## Contents

**Preface** ............................................................... 11

Document Overview .................................................. 12
  Documentation Conventions ........................................ 12
Related Documentation ................................................ 13
Customer Care .......................................................... 14
  User Accounts ....................................................... 14
  Software Upgrades ................................................ 14
  Technical Support .................................................. 14

**Chapter 1 Multi-Grid Manager** .................................. 15

Management System Requirements .................................. 17
  Supported Browsers ............................................... 17
  Browser Limitations .............................................. 18
About Multi-Grid Manager ............................................. 19
  Admin Permissions for Multi-Grid Manager ...................... 19
  Logging in to Multi-Grid Manager ............................... 19
SSL (Secure Sockets Layer) Protocol ............................. 20
Managing Certificates ................................................ 21
  Generating Self-Signed Certificates ............................ 21
  Generating Certificate Signing Requests ....................... 22
  Uploading Certificates ......................................... 22
  Downloading Certificates ...................................... 22
  Managing Intermediate Certificates ............................ 23
About the Multi-Grid Manager Interface .......................... 24
  System Messages .................................................. 24
  Security and Informational Banners ............................. 25
  Running Tasks ...................................................... 25
  Global Search ...................................................... 25
  Finder Panel ......................................................... 25
  Toolbar Panel ....................................................... 25
  Help Panel .......................................................... 25
  Wizards and Editors .............................................. 26
  Tooltips .............................................................. 26
Customizing Multi-Grid Manager .................................... 27
  Creating a Login Banner ......................................... 27
  Setting Your User Profile ....................................... 27
  Viewing Validated Users ......................................... 28
Working with Tables .................................................. 29
  Customizing Tables ............................................... 29
  Selecting Objects in Tables ..................................... 29
  Modifying Data in Tables ........................................ 31
Finding and Restoring Data .......................................... 32
  Using the Finder Panel .......................................... 32
  Using Filters ....................................................... 34
  Using Quick Filters .............................................. 34
  Using Global Search ............................................. 36
  Using the Go To Function ........................................ 37
# Contents

<table>
<thead>
<tr>
<th>Chapter 2 The Dashboard</th>
<th>Chapter 3 Smart Folders</th>
<th>Chapter 4 Managing Administrators</th>
</tr>
</thead>
<tbody>
<tr>
<td>About the Dashboard</td>
<td>About Smart Folders</td>
<td>About Admin Accounts</td>
</tr>
<tr>
<td>All Grids Status</td>
<td>Global Smart Folders</td>
<td>About Administrative Permissions</td>
</tr>
<tr>
<td>Master Grid Member Status</td>
<td>My Smart Folders</td>
<td>Managing Admin Groups and Admin Roles</td>
</tr>
<tr>
<td>My Commands</td>
<td>Creating Smart Folders</td>
<td>Modifying Admin Groups and Roles</td>
</tr>
<tr>
<td>Grid Status</td>
<td>Viewing and Modifying Data in Smart Folders</td>
<td>Deleting Admin Groups and Roles</td>
</tr>
<tr>
<td>Grid Connection Status</td>
<td>Modifying Smart Folders</td>
<td>Viewing Admin Groups</td>
</tr>
<tr>
<td></td>
<td>Deleting Smart Folders</td>
<td>Viewing Admin Roles</td>
</tr>
<tr>
<td></td>
<td>Saving a Copy of a Smart Folder</td>
<td>Viewing Admin Group Assignments</td>
</tr>
<tr>
<td></td>
<td>Printing and Exporting Data in Smart Folders</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exporting New CSV Jobs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Modifying CSV Export Jobs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exporting CSV Export Jobs</td>
<td></td>
</tr>
<tr>
<td>Exporting Displayed Data</td>
<td>Modifying CSV Import Jobs</td>
<td>Viewing Admin Group Assignments</td>
</tr>
<tr>
<td>Printing from Multi-Grid Manager</td>
<td>Deleting Uploaded Jobs</td>
<td></td>
</tr>
<tr>
<td>Multilingual Support</td>
<td>Downloads Files</td>
<td></td>
</tr>
<tr>
<td>UTF-8 Supported Fields</td>
<td>Creating a Data File for Import</td>
<td></td>
</tr>
<tr>
<td>UTF-8 Support Limitations</td>
<td>Configuring Import Options</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Viewing CSV Import Jobs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Modifying CSV Import Jobs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Deleting Admin Groups and Roles</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Viewing Admin Groups</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Viewing Admin Roles</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Viewing Admin Group Assignments</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
</tr>
<tr>
<td>52</td>
</tr>
<tr>
<td>53</td>
</tr>
<tr>
<td>54</td>
</tr>
<tr>
<td>56</td>
</tr>
<tr>
<td>57</td>
</tr>
<tr>
<td>58</td>
</tr>
<tr>
<td>59</td>
</tr>
<tr>
<td>60</td>
</tr>
<tr>
<td>60</td>
</tr>
<tr>
<td>61</td>
</tr>
<tr>
<td>63</td>
</tr>
<tr>
<td>65</td>
</tr>
<tr>
<td>67</td>
</tr>
<tr>
<td>68</td>
</tr>
<tr>
<td>68</td>
</tr>
<tr>
<td>69</td>
</tr>
<tr>
<td>69</td>
</tr>
<tr>
<td>70</td>
</tr>
<tr>
<td>70</td>
</tr>
<tr>
<td>71</td>
</tr>
<tr>
<td>71</td>
</tr>
<tr>
<td>71</td>
</tr>
<tr>
<td>72</td>
</tr>
<tr>
<td>72</td>
</tr>
</tbody>
</table>
## Contents

**Chapter 6 Managing Grids** ......................................................... 119

Managing Grids ......................................................... 121
Synchronizing Grids ......................................................... 122
Restricting Synchronization on Managed Grids .......................... 122
Adding a Grid ........................................................ 123
Configuring the Grid on the Multi-Grid Master .......................... 123
Generating the Join Key and File ......................................... 123
Joining a Grid to the Master Grid ........................................ 124
Leaving the Master Grid .................................................. 124
Managing Disconnected Grids .................................... 125
Attaching a Grid Immediately .......................................... 125
Schedule Attaching a Grid ............................................ 126
Detaching a Grid Immediately ......................................... 126
Schedule Detaching a Grid ............................................. 127
Monitoring Grids .......................................................... 128
Visualization Tab ......................................................... 128
Viewing the Node Tree ................................................ 130
Listing Grids ............................................................. 132
Removing a Grid ........................................................ 132
Setting Grid Properties .................................................. 133
Upgrading Grids .......................................................... 134
Uploading and Viewing Software Versions ............................. 134
Upgrading Software ...................................................... 135
Pushing Software ........................................................ 135
Distributing Software Upgrade Files .................................. 136
Testing Software Upgrades ........................................... 136
Performing Software Upgrades ....................................... 136
Managing Grid Templates ............................................... 137
About Snapshots ........................................................ 139

**Chapter 7 Network Management** ............................................. 143

Network Management ....................................................... 144
About Network Blocks ................................................... 145
Viewing IPv4 and IPv6 Networks ..................................... 145
IPv4 and IPv6 Network Maps .......................................... 145
IPv4 and IPv6 Network Lists .......................................... 148
Managing IPv4 and IPv6 Networks .................................... 149
Adding IPv4 and IPv6 Networks ...................................... 149
Modifying IPv4 and IPv6 Networks .................................. 150
Resizing IPv4 Networks ............................................... 150
Entering Extensible Attribute Values .................................. 150
Restricting Synchronization ............................................ 151

**Chapter 8 Managing Master Grid Operations** ........................... 153

Managing Time Settings ................................................. 155
Changing Time and Date Settings ..................................... 155
Chapter 9 Managing Software and Configuration Files ............................................. 205
Managing Upgrade Groups ......................................................................................... 206
Adding Upgrade Groups ............................................................................................ 206
Modifying Upgrade Groups ....................................................................................... 207
Viewing Upgrade Groups ......................................................................................... 207
Deleting Upgrade Groups ......................................................................................... 208
Viewing Software Versions ....................................................................................... 208
Upgrading Software .................................................................................................. 209
Lite Upgrades ........................................................................................................... 209
Uploading Software .................................................................................................. 209
Distributing Software Upgrade Files ....................................................................... 210
Managing Distributions ............................................................................................ 210
Testing Software Upgrades ....................................................................................... 213
Performing Software Upgrades ............................................................................... 213
Monitoring Distribution and Upgrade Status .......................................................... 217
Reverting to the Previously Running Software Version .......................................... 219
Backing Up and Restoring Configuration Files ....................................................... 219
Back Up Files ........................................................................................................... 219
Automatically Backing Up Data Files .................................................................... 220
Manually Backing Up Data Files .............................................................................. 222
Downloading Backup Files ....................................................................................... 222
Restoring Backup Files ............................................................................................ 223
Downloading Backup Files from a Different Appliance ........................................... 224
Chapter 10 Monitoring the Master Grid ................................................................. 227
Viewing Master Grid Status ...................................................................................... 228
Device Status ............................................................................................................ 228
CPU Usage ................................................................................................................ 229
Disk Usage ................................................................................................................ 229
LAN1/LAN2 Ports, HA Port, and MGMT Port ......................................................... 229
Memory Usage ......................................................................................................... 230
NTP Synchronization ............................................................................................... 230
MGM Service .......................................................................................................... 230
Grid Connection ....................................................................................................... 231
Replication ................................................................................................................. 231
Power Supply ............................................................................................................ 231
RAID ......................................................................................................................... 232
RAID Battery ............................................................................................................ 232
Viewing Hardware Status ........................................................................................ 233
Using a Syslog Server ............................................................................................... 234
Specifying Syslog Servers ....................................................................................... 234
Configuring Syslog for Master Grid Members ....................................................... 235
Viewing the Syslog ................................................................................................... 236
Searching in the Syslog ............................................................................................. 236
Downloading the Syslog File ...................................................................................... 237
Monitoring Tools ...................................................................................................... 237
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC Compliance</td>
<td></td>
</tr>
<tr>
<td>Appendix A Grid Manager Icons</td>
<td>307</td>
</tr>
<tr>
<td>Appendix B Regular Expressions</td>
<td>313</td>
</tr>
<tr>
<td>Appendix C Product Compliance</td>
<td>315</td>
</tr>
<tr>
<td>Power Safety Information</td>
<td>316</td>
</tr>
<tr>
<td>AC</td>
<td>316</td>
</tr>
<tr>
<td>DC</td>
<td>316</td>
</tr>
<tr>
<td>Agency Compliance</td>
<td>317</td>
</tr>
<tr>
<td>FCC</td>
<td>317</td>
</tr>
<tr>
<td>Canadian Compliance</td>
<td>317</td>
</tr>
<tr>
<td>VCCI</td>
<td>318</td>
</tr>
<tr>
<td>RFC Compliance</td>
<td>318</td>
</tr>
<tr>
<td>DNS RFC Compliance</td>
<td>318</td>
</tr>
<tr>
<td>DHCP RFC Compliance</td>
<td>321</td>
</tr>
<tr>
<td>DHCPv6 RFC Compliance</td>
<td>321</td>
</tr>
<tr>
<td>IDN (Internationalized Domain Names) RFC Compliance</td>
<td>322</td>
</tr>
</tbody>
</table>
Appendix D Open Source Copyright and License Statements .................. 323

GNU General Public License ................................................................. 325
GNU Lesser General Public License ...................................................... 328
Apache Software License, Version 2.0 .................................................. 334
perl Artistic License ......................................................................... 339
ISC BIND Copyright ....................................................................... 340
ISC DHCP Copyright ................................................................. 341
Julian Seward Copyright ............................................................ 341
Carnegie Mellon University Copyright ........................................... 342
Thai Open Source Software Center Copyright .................................. 343
Ian F. Darwin Copyright ............................................................... 343
Lawrence Berkeley Copyright ......................................................... 344
MIT Kerberos Copyright ............................................................... 344
BSD License ................................................................. 345
David L. Mills Copyright ............................................................. 346
OpenLDAP License ............................................................... 346
OpenSSL License ................................................................. 347
VIM License ................................................................. 348
ZLIB License ................................................................. 350
Wietse Venema Copyright ............................................................ 350
ECLIPSE SOFTWARE ................................................. 350
Eclipse Public License - v 1.0 ......................................................... 351
AOP Alliance (Java/J2EE AOP standards) ........................................ 355
Open JDK ................................................................. 355
TASM ................................................................. 363
Distributed Computing Laboratory, Emory University ......................... 364
COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) .... 364
The FreeType Project LICENSE ....................................................... 368
The Independent JPEG Group’s JPEG software .................................. 372
Net-SNMP ................................................................. 374
The PHP License, version 3.01 ......................................................... 379
INFO-ZIP ................................................................. 381
MIT License ................................................................. 382
Ehcache ................................................................. 383
Cybox ................................................................. 383
Dateutil ................................................................. 384
Importlib ................................................................. 385
Libtaxii ................................................................. 385
Mixbox ................................................................. 386
Stix ................................................................. 386
PSF License Agreement for Python 2.6 ............................................. 387
PSF License Agreement for Python 3.5.0 ........................................... 388

Index ................................................................. 389
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:

- **Document Overview** on page 12
  - **Documentation Conventions** on page 12
- **Related Documentation** on page 13
- **Customer Care** on page 14
  - **User Accounts** on page 14
  - **Software Upgrades** on page 14
  - **Technical Support** on page 14
Document Overview

This guide describes how to configure and manage the Master Grid using NIOS 8.2. It was last updated on July 21, 2017. For updated documentation, visit our Support site at https://support.infoblox.com.

Documentation Conventions

The text in this guide follows the following style conventions.

<table>
<thead>
<tr>
<th>Style</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong></td>
<td>• Indicates anything that you input in the user interface, by clicking, choosing, selecting, typing, or by pressing on the keyboard.</td>
</tr>
<tr>
<td></td>
<td>• Indicates the field names in the user interface.</td>
</tr>
<tr>
<td><strong>input</strong></td>
<td>Signifies command line entries that you type.</td>
</tr>
<tr>
<td><strong>variable</strong></td>
<td>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 the Multi-Grid Manager and Grid Manager, such as the Add Network wizard or the Master Grid Properties editor.</td>
</tr>
</tbody>
</table>

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>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>domain_name</td>
<td>Domain name</td>
</tr>
<tr>
<td>directory</td>
<td>Directory name</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 appliance</td>
</tr>
<tr>
<td>ip_addr</td>
<td>IPv4 or IPv6 address</td>
</tr>
<tr>
<td>member</td>
<td>Grid member name</td>
</tr>
<tr>
<td>multi-grid_master</td>
<td>Name of the Multi-Grid Master</td>
</tr>
<tr>
<td>master_grid_member</td>
<td>Name of a Master Grid member</td>
</tr>
<tr>
<td>netmask</td>
<td>Subnet mask</td>
</tr>
<tr>
<td>network</td>
<td>IP address of a network</td>
</tr>
<tr>
<td>network_view</td>
<td>Network view</td>
</tr>
<tr>
<td>port</td>
<td>Number of a port; predefined for certain protocols</td>
</tr>
</tbody>
</table>
### Related Documentation

Infoblox technical documentation uses an arrow “->” to represent navigation through the user interface. For example, to edit an admin group, the description is as follows:

From the **Administration** tab, select the **Administrators** tab -> **Groups** tab -> **admin_group** check box, and then click the Edit icon.

### Related Documentation

Other Infoblox appliance documentation:
- *Infoblox CLI Guide*
- *Infoblox API Documentation*
- *Infoblox CSV Import Reference*
- *Infoblox NIOS Administrator Guide*
- *Infoblox IBOS Administrator Guide*
- *Infoblox Installation Guide for the Trinzic 800 Appliances*
- *Infoblox Installation Guide for the Trinzic 1400 Appliances*
- *Infoblox Installation Guide for the Trinzic 2200 Appliances*
- *Infoblox Installation Guide for the Infoblox-4010 Appliance*
- *Infoblox Installation Guide for the Infoblox-4030 Appliance*
- *Quick Start Guide for Installing vNIOS Software on Riverbed Services Platforms*
- *Quick Start Guide for Installing vNIOS Software on Cisco Application eXtension Platforms*
- *Infoblox Installation Guide for Installing vNIOS on VMware*
- *Quick Start Guide for Installing vIBOS Software on VMware Platforms*
- *Infoblox Safety Guide*

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>scheduled_task</code></td>
<td>Scheduled task</td>
</tr>
<tr>
<td><code>server_group</code></td>
<td>Name of a group of servers</td>
</tr>
<tr>
<td><code>shared_network</code></td>
<td>Shared network</td>
</tr>
<tr>
<td><code>service</code></td>
<td>One of the services available from Multi-Grid Manager</td>
</tr>
</tbody>
</table>
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 Chapter 4, Managing Administrators, on page 63.

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.
Chapter 1  Multi-Grid Manager

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

• Management System Requirements  on page 17
  — Supported Browsers  on page 17
  — Browser Limitations  on page 18
• About Multi-Grid Manager  on page 19
  — Admin Permissions for Multi-Grid Manager  on page 19
  — Logging in to Multi-Grid Manager  on page 19
• SSL (Secure Sockets Layer) Protocol  on page 20
• Managing Certificates  on page 21
  — Generating Self-Signed Certificates  on page 21
  — Generating Certificate Signing Requests  on page 22
  — Uploading Certificates  on page 22
  — Downloading Certificates  on page 22
  — Managing Intermediate Certificates  on page 23
• About the Multi-Grid Manager Interface  on page 24
  — System Messages  on page 24
  — Security and Informational Banners  on page 25
  — Global Search  on page 25
  — Finder Panel  on page 25
  — Toolbar Panel  on page 25
  — Help Panel  on page 25
  — Wizards and Editors  on page 26
  — Tooltips  on page 26
  — Running Tasks  on page 25
• Customizing Multi-Grid Manager  on page 27
  — Creating a Login Banner  on page 27
  — Setting Your User Profile  on page 27
  — Viewing Validated Users  on page 28
• Working with Tables  on page 29
  — Customizing Tables  on page 29
— Selecting Objects in Tables on page 29
— Modifying Data in Tables on page 31

• Finding and Restoring Data on page 32
— Using the Finder Panel on page 32
— Using Filters on page 34
— Using Quick Filters on page 34
— Using Global Search on page 36
— Using the Go To Function on page 37

• About CSV Import on page 38
— CSV Import Limitations on page 38
— Configuring Import Options on page 39
— Viewing CSV Import Jobs on page 41
— Modifying CSV Import Jobs on page 42
— Deleting Uploaded Jobs on page 42
— Downloading Files on page 42
— Creating a Data File for Import on page 43
— Managing CSV Export Jobs on page 44
— Modifying CSV Export Jobs on page 44

• Exporting Displayed Data on page 45
• Printing from Multi-Grid Manager on page 45
• Multilingual Support on page 45
— UTF-8 Supported Fields on page 46
— UTF-8 Support Limitations on page 47
Management System Requirements

The management system is the computer from which you access Multi-Grid Manager. 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><strong>GUI ACCESS</strong></td>
<td>• Minimum System:</td>
</tr>
<tr>
<td>• See Supported Browsers on page 17 for</td>
<td>1.4 GHz CPU with 1 GB RAM available to</td>
</tr>
<tr>
<td>details.</td>
<td>the product GUI, and 256 Kbps connectivity</td>
</tr>
<tr>
<td><strong>CLI ACCESS</strong></td>
<td>to NIOS appliance</td>
</tr>
<tr>
<td>• Secure Socket Shell (SSH) client that</td>
<td>• Recommended System:</td>
</tr>
<tr>
<td>supports SSHv2</td>
<td>2.0 GHz (or higher) dual core CPU with 2</td>
</tr>
<tr>
<td>• Terminal emulation program, such as</td>
<td>GB RAM available for the product GUI, and</td>
</tr>
<tr>
<td>minicom or Hilgraeve Hyperterminal®</td>
<td>network connectivity to NIOS appliance</td>
</tr>
<tr>
<td></td>
<td>• Monitor Resolution:</td>
</tr>
<tr>
<td></td>
<td>1024 x 768 (minimum)</td>
</tr>
<tr>
<td></td>
<td>1280 x 800 or better (recommended)</td>
</tr>
</tbody>
</table>

**Supported Browsers**

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

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 Multi-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*</td>
</tr>
<tr>
<td></td>
<td>Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x</td>
</tr>
</tbody>
</table>
Multi-Grid Manager

| Red Hat® Enterprise Linux 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 |
|-----------------------------|--------------------------------------------------------|
| Apple® Mac OS X 10.9.x      | 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 |
| Apple® Mac OS X 10.8.x      | 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 |
| Apple® Mac OS X 10.7.x      | 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 |
| Apple® Mac OS X 10.6.x      | 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 |

**Note:** *Multi-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 “fakepath” 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 [http://msdn.microsoft.com/en-us/library/ms535128.aspx](http://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 Multi-Grid Manager

Multi-Grid Manager is the web interface that you use to configure your Master Grid and to manage your Grids and networks. It provides a number of tools, such as the following:

- Use the Dashboard to monitor your Master Grids and managed Grids, and to provides access to frequently-used commands. For more information, see Chapter 2, The Dashboard, on page 49.
- Use Smart Folders to organize your data based on criteria you specify. For more information, see Chapter 3, Smart Folders, on page 55.
- The Grid maps provide graphical views of the Master Grid and managed Grids in addition to status information, so you can quickly assess the status of the Grids and their services. For more information, see Chapter 6, Managing Grids, on page 119.
- The IPv4 and IPv6 network maps and lists provide views of your networks, so you can quickly evaluate IP address usage and understand how your network resources are being utilized. For more information, see Chapter 7, Network Management, on page 143.
- Tools such as the Finder panel, filters, and global search help you quickly find the information you need. For information, see About the Multi-Grid Manager Interface on page 24.

Admin Permissions for Multi-Grid Manager

Superusers have unrestricted access to Multi-Grid Manager. Limited-access users though, require read-only or read-write permission to the data that they want to manage through Multi-Grid Manager. Multi-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. For information about user accounts and administrative permissions, see Chapter 4, Managing Administrators, on page 63.

Logging in to Multi-Grid Manager

To log in to Multi-Grid Manager:

1. Open an Internet browser window and enter https://<IP address or hostname of your NIOS appliance>. The Multi-Grid Manager login page appears.
2. Enter your user name and password, and then click Login or press Enter. The default user name is admin and the default password is infoblox.
3. Read the Infoblox End-User License Agreement and click I Accept to proceed. Multi-Grid Manager displays the Dashboard, your home page in Multi-Grid Manager. For information about the Dashboard, see Chapter 2, The Dashboard, on page 49.

Tip: You can customize the text that appears on the Multi-Grid Manager login page. To do so, see Creating a Login Banner on page 27.
SSL (Secure Sockets Layer) Protocol

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) to secure the connection between a client and server. SSL provides server authentication and encryption. The NIOS appliance supports SSL versions 2 and 3.

When a client first connects to a server, it starts a series of message exchanges, called the SSL 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, 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.

A server generates two distinct but related keys: a public key and a private key. During the SSL 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 use the random value to generate the master secret, which they in turn use to generate symmetric keys. The client and server end the handshake when they exchange messages indicating that they are using the symmetric keys to encrypt further communications.

*Figure 1.2 SSL Handshake*
Managing 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.com, 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.

Because you connect to the Master Grid through the Multi-Grid Master, ensure that you always select the Multi-Grid Master when you perform any of the following tasks:

- Generate another self-signed certificate with the correct hostname and save it to the certificate store of your browser. For information, see Generating Self-Signed Certificates.
- Request a CA-signed certificate with the correct hostname and load it on the NIOS appliance. For information, see Generating Certificate Signing Requests on page 22.
- When you receive the certificate from the CA, import it to the appliance, as described in Uploading Certificates on page 22.
- Download the certificate from a trusted CA, as described in Downloading Certificates on page 22.

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.

To generate a self-signed certificate:

1. From the Master Grid tab, select the Members tab -> multi-grid_master check box, and then click HTTPS Cert -> Generate Self-signed Certificate from the Toolbar.
2. In the Generate Self-Signed Certificate dialog box, complete the following:
   - **Key Size**: Select either 2048 or 1024 for the length of the public key.
   - **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 Uploading Certificates on page 22.

To generate a CSR:
1. From the Master Grid tab, select Members -> multi-grid_master check box.
2. From the Toolbar, click HTTPS Cert -> Create Signing Request.
3. In the Create Certificate Signing Request dialog box, enter the following:
   - **Key Size**: Select either 2048 or 1024 for the length of the public/private key pair.
   - **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 Email Address**: Enter the email address of the appliance administrator.
   - **Comment**: Enter information about the certificate.
4. 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.

To import a certificate:
1. From the Master Grid tab, select the Members tab -> multi-grid_master check box, and then click 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. To download a certificate:
1. From the Master Grid tab, select the Members tab -> multi-grid_master check box, and then click 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.
Managing Intermediate 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.

To upload and manage intermediate certificates:

1. From the Master Grid tab, select the Members tab → multi-grid_master check box, and then click HTTPS Cert → Manage Intermediate Certificate from the Toolbar.

2. When the CA Certificate dialog box displays with the list of uploaded CA certificates, you can do the following:
   - Import a certificate by clicking the Add icon. In the Upload dialog box, click Select and navigate to where the certificate is located and click Open, and then click Upload.
   - Remove a certificate by selecting it and clicking the Delete icon.
   - Print the data or export it in .csv format.
**About the Multi-Grid Manager Interface**

Multi-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 Multi-Grid Manager. It identifies common elements of the interface and features that you can use:

*Figure 1.3  Multi-Grid Manager Interface*

---

**System Messages**

Multi-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. Multi-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

Multi-Grid Manager displays security and informational banners 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 on page 117 and Configuring Informational Banner on page 117.

Running Tasks

When you execute a task, Multi-Grid Manager automatically runs it in the background, so you can navigate to other tabs and perform other functions while Multi-Grid Manager completes the task.

The Task Icon indicates if a task is running. The icon becomes yellow if the task has been pending or running for over 10 minutes. It becomes red if the task fails to execute. If there is an active task, the icon becomes animated or active.

You can click the Task Icon to view detailed information about the tasks in the Task viewer. You can sort the tasks in ascending or descending order by column and use filters to narrow down the list. The Task viewer also provides an option to automatically clean up tasks after a specific number of days or weeks. Multi-Grid Manager displays a message at the top of the interface when the task is completed successfully or if the task fails.

Global Search

Use Global Search to find data. Multi-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 on page 36.

Finder Panel

The Finder panel appears on all pages in Multi-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.
- **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. For information, see Using the Finder Panel on page 32.

Toolbar Panel

The vertical Toolbar 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 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

Multi-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.

Tooltips

Tooltips display the function of each button. Hover your mouse over a button or icon to display its label.
Customizing Multi-Grid Manager

You can customize different elements of Multi-Grid Manager to better suit the needs of your organization and to facilitate the completion of tasks.

Creating a Login Banner

Multi-Grid Manager displays a statement at the top of the Login screen (a banner message). You can change this statement to better suit your organization. For example, you can post security warnings or provide user-friendly information. A login banner message can be up to 3000 characters long.

To create a login banner:
1. From the Master Grid tab, select either Members or Licenses.
2. From the Toolbar, click Master Grid Properties -> Edit.
3. In the Master 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.
4. Save the configuration.

Setting Your User Profile

Multi-Grid Manager creates and stores a user profile for each admin user. Each user profile contains information about your admin group and admin type. You can modify information in your user profile any time after the initial login. You can set the following in your user profile:

- Change your password to facilitate future logins and add your email address for reference.
- Specify the amount of data Multi-Grid Manager can display in a table or in 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 Multi-Grid Manager.
- Specify the time zone Multi-Grid Manager uses to convert all displayed time values, such as the last login time. You can set the time zone to Auto-detect so Multi-Grid Manager sets the time zone based on the time zone of your browser. But if Multi-Grid Manager cannot automatically determine the time zone when you log in, it sets the time zone to UTC (Coordinated Universal Time) standard. In this case, you can manually change the time zone.
- Validate your credentials on the applicable managed Grids, so you can access them from Multi-Grid Manager without having to log in to them each time.

Note that when multiple users log in to Multi-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 information about configuring admin accounts and admin groups, see Chapter 4, Managing Administrators, on page 63.

To set up your user profile:
1. Select any tab in Multi-Grid Manager, and then click User Profile from the Toolbar.
2. In the User Profile editor, complete the following:
   - Name: Displays the name of the admin user.
   - Type: Displays your user type. This can be Local or Remote. The local admin accounts are stored in the local database, and the remote admin accounts are stored on another server, such as a RADIUS server. Multi-Grid Manager automatically deletes remote user profiles if the users have not logged in for more than six months.
   - Master Grid Group: Displays the admin group to which your account belongs. The admin group determines your administrative permissions. Only superusers can define admin groups for the Master Grid.
— **Grid Groups**: The table displays the Grids that you can access through a single sign on to Multi-Grid Manager.

— **Set Password**: If you are a local user, you can enter a new password for your account. If you are a remote user, you do not see this field.

— **Retype Password**: Enter the same password.

— **Email Address**: Enter your email address. Note that this address simply provides contact information. By default, this field is blank.

— **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.

— **Time Zone**: Select the time zone used to convert all displayed time values. The default is **Auto-detect time zone**.

— **Grid Credentials**: Click Validate to validate your credentials to other Grids so you can access them from Multi-Grid Manager without having to log in to each of them.

In the **User Validation Panel** dialog box, select the check box of the applicable Grids, complete the following, and then click Validate:

— User Name: Enter the user name you use to log in to the selected Grid.

— Password: Enter the password.

You can also select the check box of a Grid and click Ignore to instruct Multi-Grid Manager to skip validation for the Grid. You are then prompted to log in to the Grid every time you try to access it from Multi-Grid Manager. Use this option only for Grids that you don't have to access from Grid Manager.

---

**Note**: The user mapping settings are not preserved after you apply Snapshot/Template to a Grid, back up the current configuration or restore backup to a Grid, and promote a Master candidate. After you perform these activities, you need to validate your credentials.

---

The Master Grid displays validated users and their corresponding Grids in the Administration tab ➔ User Mapping tab described in the next section, **Viewing Validated Users**.

3. Save the configuration.

**Viewing Validated Users**

Only admins with superuser accounts can view the list of validated users. To view the list of validated users and their Grids:

1. From the Administration tab, select the **Administrators** tab ➔ User Mapping tab.

2. Multi-Grid Manager displays the following information about each validated user on the Master Grid:

   — **User**: The user type.
   
   — **Grid User**: The name of the admin account.
   
   — **Grid**: The name of the Grid to which the user is validated.
   
   — **Group**: The name of the admin group on the specified Grid.
   
   — **Validated**: The status of the validation. This can be Ignored or Yes.

You can do the following in this panel:

- Select an admin account and click the Delete icon to delete it. The user must then log in to each Grid.
- 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** on page 34.
Working with Tables

Multi-Grid Manager uses dynamic tables to display information. The following section describe how to customize tables and how to select and edit their data.

Customizing Tables

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:
1. In the table, mouse over to a header title and click the down arrow key.
2. Select Columns > Edit Columns.
3. 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.
4. 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.

Multi-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, Multi-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. Multi-Grid Manager displays a message that indicates the total number of selected rows on the page. You can deselect a specific row by clearing its check box. You can also click a row (not the check box) in the table to select the item and deselect the others.

You can also click Select all objects in the dataset to select all rows in the entire table. You can then click Clear Selection to deselect the rows.
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

Multi-Grid Manager provides tools for organizing and quickly retrieving IP address data.

Using the Finder Panel

The Finder panel appears on all pages in Multi-Grid Manager. The panel is expanded by default. 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 information, see My Smart Folders on page 57.
- Bookmarks: Contains bookmarked objects, such as networks and IP addresses. For information, see Using Bookmarks.
- 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 information, see Managing Third Party URL Links on page 32.

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.

Using Bookmarks

The Bookmarks section displays objects for which you have created bookmarks. You can create bookmarks for objects such as networks and admin groups. To bookmark an object, navigate to its page and click the Bookmark icon at the top of the page. 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. 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. Multi-Grid Manager removes the bookmark.

Managing Third Party URL Links

In the URL Links section, you can add the URL links of frequently used third party portals and destination pages. For example, you can add the URL of a trouble ticket system and quickly access the portal once you are logged in to the Infoblox GUI. When you click an existing URL link, Multi-Grid Manager displays the destination page in a new browser window. You can also modify and delete existing URL links in this section.

On the appliance, only superusers have permissions to fully manage the URL links. Superusers can create URL links and make them globally available to all users. If you have limited-access permissions, you can only add URL links for your own use. You cannot share the links with other users.
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 page you want to add. The appliance supports valid URL entries that contain up to 2000 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.
   - Logo: Click Upload to add a logo to the URL. The appliance displays the logo in 16x16 pixels. Click Reset to Default to use the default logo.
4. Save the configuration.

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 and save it.

Deleting URL Links
To permanently delete a 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 type and amount of data displayed in a specific panel by adding filter criteria. When you add filter criteria, Multi-Grid Manager 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, 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 on page 34.

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 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”.

To use a filter:
1. In a panel, click Show Filters 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. Multi-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.
   - 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.
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. Multi-Grid Manager displays only the filtered data in the panel.
   or
   Click Toggle Filter Off to have the appliance list all data without applying filter criteria.

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. 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. For information about filters, see Using Filters on page 34.
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 on page 34.
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 on page 34.
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 Adding 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 then 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.
- Click Toggle Filter Off or Reset in the filter section.
- Delete a quick filter, as described in Deleting Quick Filters.

Deleting Quick Filters

1. In a panel that supports filters, click Show Filters, and then select the quick filter you want to delete from the Quick Filter drop-down list.
2. In the filter section, click the Delete icon next to the filter name.
3. In the Delete Quick Filter dialog box, click Yes to permanently delete the quick filter.
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 enter a search value and define filter criteria to refine the search. Multi-Grid Manager supports regular expressions in global search. Multi-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 Multi-Grid Manager.

**Note:** Depending on the size of your database, global search may take a long time to complete. Multi-Grid Manager times out when queries or searches take longer than 120 seconds. To expedite searches, use filters to refine the search criteria.

To search globally:

1. Click the global search icon on the navigation bar.
2. In the Search dialog box, do the following:
   - In the first 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 use regular expressions in the search value. For information, see Appendix B, "Regular Expressions", on page 313.
   - In the Type drop-down list, select an object type, comment, or an extensible attribute (fields with a gray background) as the filter criterion. Multi-Grid Manager displays all the supported fields in the drop-down list. The default is Type. Multi-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.
   - 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.
   - 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. Multi-Grid Manager searches all object types when you use the default.
3. Optionally, click the + icon to add another filter. You can add up to 10 filter rules.
4. After you finish defining filters, click Apply or press Enter.

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

- **Name:** The name of the matching object and its path, 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, 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.
- **Matched Value:** 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.
- **IP Address:** The IP address of the matching object. When you click the IP address link, Multi-Grid Manager displays the corresponding IP address panel from which you can view detailed information.

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. Multi-Grid Manager stores the search results until you reset the search parameters or log out.
Editing Matching Objects in Search Results

Multi-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 Multi-Grid Manager displays the path.
   Multi-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.
   Multi-Grid Manager deletes the selected objects from the database. Most deleted objects are stored in the Recycle Bin.

You can print search results. You can also export search results in CSV (comma separated value) format.

Using the Go To Function

You can use the Go to function to quickly locate an object, such as a network. 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. Multi-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.
   Multi-Grid Manager completes the operation based on the selected object.
About CSV Import

Use **CSV Import** to import IPAM data (networks, network containers) through Grid Manager. You can use this feature to migrate or add new data, overwrite existing data, or merge new data with existing data. Only superusers can perform CSV imports and exports.

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. For more information about CSV import, refer to the *Infoblox CSV Import Reference.*

To import a data file:

1. Create a data file if you do not already have one, as described in *Creating a Data File for Import* on page 43.
2. Configure import options. For information, see *Configuring Import Options* on page 39.

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.**

To access **CSV Job Manager,** from the **Data Visualization** tab, click **CSV Job Manager** from the Toolbar and select jobs Manager, click **CSV Import** in the IPAM Task Pack.

You can do the following in **CSV Import:**

- Add, override, merge, or custom data through the imported CSV file, as described in *Configuring Import Options* on page 39.
- Verify the content in the CSV file, as described in *Configuring Import Options* on page 39.
- View a list of CSV import jobs, as described in *Creating a Data File for Import* on page 43.
- Add and start CSV import jobs, upload data files, stop CSV imports, or edit the options of the uploaded file, as described in *Modifying CSV Import Jobs* on page 42.
- Delete uploaded jobs, as described in *Deleting Uploaded Jobs* on page 42.
- Download the following: imported files, import errors, import results, or snapshots, as described in *Downloading Files* on page 42.
- 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:** The list of CSV import jobs are not restored when you restore a backup file or when you promote a master candidate.

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.
- 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.
- Only editable data can be imported.
• 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.
• 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.
• 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.
• 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.

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, and custom. 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 Visualization 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
   
   — 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 _NEW_XXX fields in the data file.
   
   — Merge: Select this to add values from the imported CSV file to the existing columns in the database that do
     not have any data. It does not overwrite the existing data, even if the data file contains new values for
     certain fields. If you want to overwrite values in the required fields, you must include the required fields and
     the corresponding _NEW_XXX fields in the data file.
   
   — Delete: Select this to delete the rows in the imported CSV file from the database.
   
   — Custom: Select this to apply custom import actions for individual data rows in your CSV file. When
     preparing the CSV file for import with the Custom option, add an IMPORT-ACTION column to the file and
     specify a custom import action for each data row. Use the following abbreviations for import actions: ‘I’

   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.
- **File name**: 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**.
- **On Error**: The option you have selected.

6. Click **Test** to verify the content in your CSV file. Click **Yes** in the **Test CSV Import for Replace Operation** 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.
   - **File name**: The name of the CSV file you have selected.
   - **Separator**: The separator you have selected for your CSV file. The default value is **Comma**.
   - **On Error**: 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 errors** 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.

### Viewing CSV Import Jobs

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

1. From the **Data Visualization** 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.
   - **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**.
   - **File Size**: The size of the imported CSV file.
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 Configuring Import Options on page 39.

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

1. From the Data Visualization 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 update, click the Action icon and select Edit.
3. In Edit - CSV Import Job, select a type of import and perform the operations mentioned in Configuring Import Options on page 39.
4. Click Download to download the uploaded file, snapshot file, or the results file. For more information, see Downloading Files on page 42.
5. Click Save & Close to save the changes.

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 Visualization 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:

1. From the Data Visualization tab, click CSV Job Manager from the Toolbar.
2. In the CSV Job Manager wizard, do one of the following:
   - Select CSV Import and select the import job that you want to download, click the Action icon and select Download.
   - 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. Click the arrow beside the Download option and select one of the following:
     - 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.

### 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. You can create one CSV file to update data of multiple object types (Network and Network Container), as illustrated in [CSV File Example 1](#). In this example, you define the field names you want to modify for the two object types in rows 1 and 2. You then include the corresponding data as shown in rows 3 to 4. For detailed information about CSV Import, refer to the [Infoblox CSV Import Reference](#).

**Table 1.1 CSV File Example 1**

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HEADER-MGMNETWORK</td>
<td>GRID*</td>
<td>NETWORK_VIEW*</td>
<td>ADDRESS*</td>
</tr>
<tr>
<td>2</td>
<td>HEADER-IS_Container</td>
<td>DISABLED</td>
<td>COMMENT</td>
<td>EA-&lt;VALUE&gt;</td>
</tr>
<tr>
<td>3</td>
<td>NETWORK</td>
<td>SubGrid</td>
<td>Default</td>
<td>10.176.80.255</td>
</tr>
<tr>
<td>4</td>
<td>True</td>
<td>True</td>
<td></td>
<td>EA-Site1</td>
</tr>
</tbody>
</table>

### Exporting New CSV Jobs

You can use the [Global CSV Export Wizard](#) to export multiple objects at once. You can export network containers and networks to a single CSV file through Grid Manager.

To export network containers and networks data:

1. From the [Data Visualization](#) 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 networks are selected by default.
   - **Network:** Select this check box to select all networks and network containers that are listed.
3. Click [Export Data](#) to start the export process. In the [Start global CSV Export](#) 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 [CSV Global Export progress](#) 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 Visualization** 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 Visualization** 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 📀. 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 *Downloading Files* on page 42.

4. Click the New CSV Export job icon to export a new job. For more information, see *Exporting New CSV Jobs* on page 43.

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.

To export data:

1. From Multi-Grid Manager, navigate to the panel that contains the data you want to export. For example, if you want to export the list of IPv4 networks, select the Data Visualization tab -> IPv4 -> List.
2. Click the Export icon.
3. In the Export dialog box, click Start. Multi-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 Multi-Grid Manager to use the same method for future exports. When you select this check box, Multi-Grid Manager does not display the Opening .csv dialog box in the future.
6. Click OK.

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

Printing from Multi-Grid Manager

In Multi-Grid Manager, you can print information from panels and pages that support the Print function. Multi-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 Customizing Tables on page 29.

To print:

1. Click the Print icon. You must allow pop-up windows in your browser for printing. Multi-Grid Manager displays a separate browser window.
2. Click Print.

   Multi-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 input fields in Multi-Grid Manager. 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 Multi-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 Multi-Grid Manager.
- 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.
- 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.
- The Infoblox CLI does not support UTF-8 encoding.
Chapter 2  The Dashboard

The Dashboard provides a quick view of your Master Grid and its managed Grids. This chapter includes the following sections:

- *About the Dashboard* on page 50
- *All Grids Status* on page 51
- *Master Grid Member Status* on page 52
- *My Commands* on page 52
- *Grid Status* on page 53
- *Grid Connection Status* on page 54
About the Dashboard

The Dashboard is your home page on Multi-Grid Manager. It provides easy access to tasks and to the status of your Master Grid and its managed Grids. It provides various widgets for viewing and managing data. You can add all or some of the following widgets to your Dashboard:

- All Grids Status
- Master Grid Member Status on page 52
- My Commands on page 52
- Grid Status on page 53
- Grid Connection Status on page 54

Note that you must have at least read-only permission to the objects that a widget displays. You are allowed to select and place the widget on the Dashboard, however, it will not display any information without read-only permission.

To add widgets to your Dashboard:

1. Click Add Content.
   Multi-Grid Manager displays thumbnails of the available widgets.
2. Select and drag a widget to the desired location on your Dashboard.

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

You can click Turn Auto Refresh On at the top of the Dashboard to periodically refresh the contents of all widgets. This feature is turned off by default to optimize the performance of Multi-Grid Manager.

Widgets have the following icons:

- 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 the Dashboard.
All Grids Status

The All Grids widget provides status information about the Grids managed by the Multi-Grid Master. You can configure the widget to display information about all Grids or only Grids that have service warnings or errors. To modify the All Grids widget, click the Configure icon:

- **Select Smart Folder:** By default, Multi-Grid Manager displays all Grids in the system-defined All Grids Smart Folder. Click this to select another Smart Folder that contains Grids.

Select one of the following:
- **Show all grids** (this is the default)
- **Only show grids with service warnings or errors**

The All Grids widget displays the following information about each Grid:

- **Grid Name:** The name of the Grid. Click it to display the Grid Dashboard. The calendar icon indicates an attach or detach operation is scheduled
- **Grid Master Name:** The hostname of the Grid Master.
- **Grid Status:** The current status of the Grid, which can be one of the following:
  - **Offline:** The Grid is offline
  - **Working:** The Grid is operational.
  
  Click the Grid status to display the Grid Manager tab of the Grid.
- **Grid Connection Status:** The current connection status of the Grid. Current status will be displayed in one of the following ways:
  - **Attaching:** The attach operation is in progress.
  - **Attached:** The Grid is attached to the Master Grid.
  - **Attach Failed:** The attach operation has failed.
  - **Detaching:** The detach operation is in progress.
  - **Detached:** The Grid is detached from the Master Grid.
  - **Detach Failed:** The detach operation has failed.
  - **Snapshot Failed:** The Master Grid failed to capture the snapshot.
- **Version:** The version of NIOS that the Grid is running.
- **Upgrade Status:** The upgrade status of the Grid.
**Master Grid Member Status**

The *Master Grid Member Status* widget provides status information about the system resources and services of a Master Grid member. You can add a *Master Grid Member Status* widget to your Dashboard for each member that you want to monitor. You can then configure the widget to display additional information and specify how the information is displayed.

The status of the external storage FTP server can be one of the following:

- **Green**: The external storage server is connected and the storage capacity is below the threshold limit. Also, the last operation on the external storage is successful.
- **Yellow**: The external storage server is connected but the storage capacity is above the configured threshold limit and below 100%.
- **Red**: Cannot connect to the external storage because of some operational issue or the external storage server might be full.
- **Gray**: The external storage server is not configured or is disabled.

To edit the *Master Grid Member Status* widget, click the **Configure** icon and do the following:

- Click **Select Member** to select a member for display. The widget can display the following information:
  - **Show Role**: Click to display whether the appliance is the Multi-Grid Master, Multi-Grid Master candidate, or a Master Grid member.
  - **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:
    - **Standalone**: The member is a single appliance.
    - **HA OK**: The 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.
  - **Show System Uptime**: Click to display the duration of time (days, hours, and minutes) that the member has been up and running.

- **Statistics**: Select the data that you want to display and its format:
  - **CPU Usage**: 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.
  - **Network Usage**: Click to display the percentage of networks that are managed by the member. Select either **Pie** or **Bar** for the display format.
  - **Disk Usage**: Click to display the percentage of the data partition on the hard disk drive that is in use. Select either **Pie** or **Bar** for the display format.
  - **System Temperature**: Click to display the system temperature, if available. Select to display the temperature in either **Celsius** or **Fahrenheit**.
  - **CPU Temperature**: Click to display the CPU temperature, if available. Select to display the temperature in either **Celsius** or **Fahrenheit**.

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

**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.

To edit the *My Commands* widget, click the **Configure** button 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.
Grid Status

The Grid Status widget provides status information about the managed Grids. You can add a widget for each managed Grid.

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

- **Show all grid members** (this is the default)
- **Only show members with service warnings or errors**

In the upper section of the widget, Multi-Grid Manager displays the overall status of the Grid, which is represented by 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.

This section also displays the overall operational status of the DNS, DHCP, NTP, FTP, TFTP, HTTP (File Distribution), and bloxTools services that are currently running on the Grid.

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

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

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.

You can click a member link to view the detailed status of the selected member. Grid Manager displays the Grid tab ➔ Member tab.
Grid Connection Status

The **Grid Connection Status** widget provides statistical information about the Grid connection status and external storage space. You can configure the widget to display information and specify how the information is displayed.

Click the Configure icon to modify the Grid Connection Status widget and do the following:

- **External Storage**: Select the External Storage check box to view the used space in the external storage in percentage. Select either **Pie** or **Bar** for the display format.
- **Failed Attach**: Select the Failed Attach check box to view the number of failed attach operations.
- **Failed Detach**: Select the Failed Detach check box to view the number of failed detach operations.
- **Failed Snapshots**: Select the Failed Snapshots check box to view the number of failed attempts by the Multi-Grid Manager to complete the snapshot operation.

The **Grid Connection Status** widget also displays the following information:

- In the Grid Connection Status section:
  - **Online Grids**: Number of Grids that are online.
  - **Offline Grids**: Number of Grids that are offline.
  - **Detached/Attached Grids**: Number of Grids that are attached or detached.
  - **Grid Slots Available**: Number of Grids that can be joined to the Multi-Grid Manager before the maximum is reached.

- In the Storage Space Available section:
  - **% Used**: Space used in the external storage server in percentage.
  - **% Available**: Space available in the external storage server in percentage.

- In the Failed Attach section, you can click the **Failed Attach** link to view the Grids tab -> List tab and display the list of Grids that failed to attach.

- In the Failed Detach section, you can click the **Failed Detach** link to view the Grids tab -> List tab and display the list of Grids that failed to detach.

- In the Failed Snapshots section, you can click the **Failed Snapshots** link to view the Grids tab -> List tab and display the list of Grids that failed to complete the Snapshot operation.
Chapter 3  Smart Folders

This chapter explains how to create and use Smart Folders to organize your Grid and core network services data. It includes the following sections:

- **About Smart Folders** on page 56
  - **Global Smart Folders** on page 57
  - **My Smart Folders** on page 57
- **Creating Smart Folders** on page 58
- **Viewing and Modifying Data in Smart Folders** on page 59
- **Modifying Smart Folders** on page 60
- **Deleting Smart Folders** on page 60
- **Saving a Copy of a Smart Folder** on page 60
- **Printing and Exporting Data in Smart Folders** on page 61
About Smart Folders

Use Smart Folders to organize your Grid and IPAM data. Depending on your administrative roles and business needs, you can filter your data by object types, names, or extensible attributes, 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, Multi-Grid Manager 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 on page 59.

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. 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 on page 58. 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.

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 and manage global Smart Folders. For information, see Global Smart Folders on page 57. You can create personal Smart Folders as well as links to global Smart Folders in My Smart Folders. For information, see My Smart Folders on page 57.

Each Smart Folder you create can contain up to 2,000 objects. When the number of objects exceeds 2,000, Multi-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.

Figure 3.1 Creating Smart Folders

1. From Multi-Grid Manager, define extensible attributes. It annotates core network services data in the database.
2. Create a Smart Folder with filter criteria set to specific objects and values. You can also group the results by specifying the Group By rules.
3. The appliance searches objects that match the filter criteria, and groups the objects by the Group By rules. Multi-Grid Manager displays the folder contents in a hierarchical view.
To create Smart Folders:

1. Determine how you want to organize your 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 Using Extensible Attributes on page 168.

   **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 on page 58.

### 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. You can also save a local copy of an existing folder, depending on your administrative permissions. For more information, see Saving a Copy of a Smart Folder on page 60.

Multi-Grid Manager displays a list of global Smart Folders in the list panel.

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. You can create up to 200 Smart Folders, including 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 more information, see Saving a Copy of a Smart Folder on page 60. 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.

Multi-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 more information, see Using the Finder Panel on page 32.

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 that are in the folder. Only the Smart Folder is deleted.
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 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. Multi-Grid Manager displays a hierarchical view of the data using the Group By rules you define. By default, the appliance does not include objects that do not contain any attribute values. If you opt to include objects that do not contain attribute values, the appliance may take longer to process the request.

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

   If you logged in with a superuser account, click the Global Smart Folders tab to create a global Smart Folder.
3. 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.
   
   — Include objects with no values for the Group By attributes: Select this to include objects that do not contain values in the selected attributes when you group your Smart Folder results using the Group By rules. The appliance may take longer to include these objects in the results table when you select this option. To achieve better performance, clear this check box.
   
   — In the first drop-down list, select a field as the filter. You can select a network view as the filter. Multi-Grid Manager highlights extensible attributes in gray. You can also group the default data by adding a Group By rule without adding a filter. The default filter is “Type equals Grid”.
   
   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. The default is Grid if you select Type in the first field. Multi-Grid Manager displays all the managed Grids in the results table.
   
   — 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 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. Multi-Grid Manager displays the filtered data in the results table.

5. Click Save to save the Smart Folder.
Viewing and Modifying Data in Smart Folders

After you set up a Smart Folder, Multi-Grid Manager searches for matching objects based on the filter criteria you specified for the folder. Multi-Grid Manager also groups the objects by the Group By rules you specify. If you 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, Multi-Grid Manager sorts and displays the first 2,000 objects. It also displays a message at the top of the panel. In this case, you might want to redefine your filter criteria to further refine the filtered data in your Smart Folders.

Multi-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, Multi-Grid Manager displays all the Smart Folders in a flat list. Use 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 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 on page 31.

In the Smart Folder data panel, Multi-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, Multi-Grid Manager displays all the objects in the results table. If you select to include objects with no attribute values, Multi-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. Multi-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. Multi-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 more information, see Printing from Multi-Grid Manager on page 45 and Exporting Displayed Data on page 45.
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 on page 58.

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 your local copy is not updated.
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. Multi-Grid Manager saves the folder copy in My Smart Folders when you save the folder copy in this tab.
   or
   The *Save Smart Folder Copy* 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 *Exporting Displayed Data* on page 45 and *Printing from
Multi-Grid Manager* on page 45.
Chapter 4  Managing Administrators

This chapter describes the various tasks associated with setting up admin groups, admin roles, admin accounts, and permissions for the Master Grid. It contains the following sections:

- **About Admin Accounts** on page 65
- **About Admin Groups** on page 67
  - Creating Superuser Admin Groups on page 68
  - Creating Limited-Access Admin Groups on page 683
- **About Admin Roles** on page 69
  - Creating Admin Roles on page 69
- **Managing Admin Groups and Admin Roles** on page 70
  - Modifying Admin Groups and Roles on page 70
  - Deleting Admin Groups and Roles on page 71
  - Viewing Admin Groups on page 71
  - Viewing Admin Roles on page 71
  - Viewing Admin Group Assignments on page 72
- **About Administrative Permissions** on page 72
  - Defining Global Permissions on page 73
  - Defining Object Permissions on page 73
  - Applying Permissions and Managing Overlaps on page 75
  - Managing Permissions on page 77
- **Authenticating Administrators** on page 80
- **Creating Local Admins** on page 80
  - Modifying and Deleting Admin Accounts on page 81
- **About Remote Admins** on page 81
- **Authenticating Using RADIUS** on page 83
  - Remote RADIUS Authentication on page 84
  - Configuring a RADIUS Authentication Server Group on page 84
  - Managing the RADIUS Server List on page 86
  - Disabling RADIUS Servers on Multi-Grid Master on page 86
  - Configuring Remote RADIUS Servers on page 86
  - Authorization Groups Using RADIUS on page 87
  - Accounting Activities Using RADIUS on page 87
Managing Administrators

- Authenticating Admin Accounts Using Active Directory on page 88
  - Admin Authentication Using Active Directory on page 89
  - Configuring an Active Directory Authentication Service Group on page 89
  - Managing the Domain Controller List on page 90
  - Disabling Domain Controllers on page 90
- Authenticating Admin Accounts Using TACACS+ on page 91
  - TACACS+ Accounting on page 92
  - Configuring TACACS+ on page 92
  - Configuring a TACACS+ Authentication Server Group on page 92
- Defining the Authentication Policy on page 94
  - Configuring a List of Authentication Services on page 94
  - Configuring a List of Remote Admin Groups on page 94
- Authenticating Admins Using Two-Factor Authentication on page 95
- Changing Password Length Requirements on page 100
- Notifying Administrators on page 100
- Administrative Permissions for the Master Grid on page 101
- Administrative Permissions for Disconnected Grids on page 103
- Administrative Permissions for Scheduling Tasks on page 102
- Administrative Permissions for IPAM Resources on page 104
  - Administrative Permissions for IPv4 and IPv6 Networks on page 104
About Admin Accounts

A user must have an admin account to log in to the Master Grid. 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 on page 67. On the Master Grid, you must be a superuser to manage admin permissions. For information, see About Administrative Permissions on page 72.

When an admin connects to the Master Grid 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 appliance can authenticate users that are stored on its local database as well as users stored remotely on an Active Directory domain controller or a RADIUS server. The group from which the admin receives privileges and properties is stored locally.

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></th>
<th>Master Grid</th>
<th>RADIUS server or AD Domain Controller</th>
</tr>
</thead>
</table>
| **To store admin accounts locally** | • Use the default admin group (“admin-group”) or define a new group  
• Set the privileges and properties for the group  
• Add admin accounts to the group | | |
| **To store admin accounts remotely** | • Configure communication settings with a RADIUS server or an Active Directory domain controller  
If you use admin groups on the RADIUS server or Active Directory domain controller:  
• Use an existing admin group or define a new one  
• Set the privileges and properties for the group  
If you do not use admin groups on the RADIUS server:  
• Assign an admin group as the default | • Configure communication settings with the appliance  
If you use admin groups:  
• Import Infoblox VSAs (vendor-specific attributes) (if RADIUS)  
• Define an admin group with the same name as that on the appliance  
• Define admin accounts and link them to an admin group  
If you do not use admin groups:  
• Define admin accounts |

The admin policy defines how the appliance authenticates the admin: with the local database, RADIUS, or Active Directory. You must add RADIUS or Active Directory as one of the authentication methods in the admin policy to enable that authentication method for admins. See Defining the Authentication Policy on page 94 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**

Complete the following tasks to create an admin account:

1. Use the default admin group or create an admin group. See About Admin Groups on page 67.
2. Define the administrative permissions of the admin group. See About Administrative Permissions on page 72.
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 on page 80.
   - To configure the appliance to authenticate the admin account stored remotely, see About Remote Admins on page 81.
About Admin Groups

All administrators must belong to an admin group. The permissions and properties that you set for a group apply to the administrators that you assign to that group.

There are two types of admin groups:

- **Superuser** – Superuser admin groups provide their members with unlimited access and control of all the operations that an 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 their console, GUI, and API. In addition, only superusers can create admin groups. The Master Grid superusers can manage permissions of all Master Grid objects and synchronized objects from all managed Grids.

- **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.

All limited-access admin groups require either Read-only or Read/Write permission to access certain resources, such as IPv4 and IPv6 networks, 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 an admin group.

Complete the following tasks to assign permissions directly to an admin group:

1. Create an admin group, as described in *Creating Limited-Access Admin Groups* on page 68.
2. Assign permissions to the admin group, as described in *About Administrative Permissions* on page 72.

Complete these tasks to assign admin roles to an admin group:

1. Create an admin role, as described in *About Admin Roles* on page 69.
2. Define permissions for the newly created admin role, as described in *Creating Admin Roles* on page 69.
3. Create an admin group and assign the role to the group, as described in *Creating Limited-Access Admin Groups* on page 68.

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* on page 80.
- For remote admins, see *About Remote Admins* on page 81.
Creating Superuser Admin Groups

Superusers have unlimited access to the Master Grid. They can perform all the operations that the Master Grid provides. 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 appliance loses connectivity to the remote admin databases such as RADIUS servers or AD domain controllers.

There is a default superuser admin group (admin-group). 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.
   - **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.
4. Optionally, click Next to add extensible attributes to the admin group. For information, see Using Extensible Attributes on page 168.
5. Save the configuration.

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 on page 80.
- Assign the superuser group to remote admins. For information, see About Remote Admins on page 81.

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 an 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 Multi-Grid Manager GUI and the API (application programming interface) to configure the appliance.
  - **GUI**: Select this to allow the admin group to use the GUI.
  - **API**: Select this to allow the admin group to use the API.

4. Optionally, click **Next** to add or delete extensible attributes for this admin group. For information, see *Using Extensible Attributes* on page 168.

5. Save the configuration.

---

**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. You can create 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 *Using Extensible Attributes* on page 168.
4. Click **Next** and select one of the following:
   - **Save & Add Permissions**: Save the entry and add permissions to the role. Multi-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* on page 72.
   - **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 Using Extensible Attributes on page 168.

3. Save the configuration.
   The appliance displays the new role in the Roles tab.

After you create roles, you can do the following:

• Define their permissions. For information and guidelines on defining permissions, see About Administrative Permissions on page 72.
• Assign roles to admin groups, as described in Creating Limited-Access Admin Groups on page 68.

---

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.
   — Roles: Modify the data as described in Creating Limited-Access Admin Groups on page 68.
   — Extensible Attributes: Add and delete extensible attributes that are associated with the admin group. You can also modify the values of the extensible attributes. For information, see Using Extensible Attributes on page 168.

3. Save the configuration.
Deleting Admin Groups and Roles

You can remove any admin group as long as it is not your own admin group or the last admin group. You can also delete any admin role. The appliance puts the deleted roles in the Recycle Bin, if enabled.

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.

To delete an admin role:
1. From the Administration tab, select the Administrators tab -> Roles tab -> admin_role check box, and then click the Delete icon.
2. In the Delete Confirmation dialog box, click Yes.

Viewing Admin Groups

You can view the list of admin groups that are currently in the Master Grid. To view admin groups, from the Administration tab, select the Administrators tab -> Groups tab.

Multi-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 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 on page 34.
- 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 on page 31.
- Print or export the data.

Viewing Admin Roles

You can view the list of admin roles that are currently in the Master Grid. To view admin roles, from the Administration tab, select the Administrators tab -> Roles tab.

Multi-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.
- 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 on page 31.
- 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 on page 34.
• 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.
   Multi-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. On the Master Grid, only superuser admins can manage permissions. Limited-access users cannot grant permissions to any admin groups or roles.

The following are permissions superuser admins 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 Master Grid objects and all synchronized objects of the managed Grids. Superusers can grant permissions to objects at the global and object levels. They also have full privileges to all managed Grids so they can create networks and delegate them to the Grids. For information, see Adding IPv4 and IPv6 Networks on page 149. Limited-access admin groups however must have either Read-only or Read/Write permission assigned in order to perform tasks on any supported objects.

Besides defining permissions for Master Grid objects, superusers can also define permissions for synchronized objects that are configured on managed Grids. When managed Grids synchronize objects with the Master Grid, all permissions associated with the objects are also synchronized. Though you cannot modify the original permissions of a synchronized object, you can assign new permissions that you can then later assign to local users in the Master Grid. Note that new permissions defined for the Master Grid can only be used for local users in the Master Grid. They do not affect the original permissions defined in the managed Grid.

When you log in to the Master Grid, you inherit the permissions of the admin group to which you belong. The superuser admin can grant you additional permissions to specific objects. When you validate your user account with other users of specific managed Grids, not only can you access the Grids through SSO (Single Sign On), you also adopt the permissions of the users of the Grids you have validated, plus your local permissions from the Master Grid. For information about validating users, see Setting Your User Profile on page 27.

You can define user permissions at a global level, such as for all IPv4 and IPv6 networks. You can also define permissions at a more granular level, such as for a specific IPv4 network. For information, see Defining Global Permissions and Defining Object Permissions on page 73.

When you set permissions that overlap with existing permissions, Multi-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 Applying Permissions and Managing Overlaps on page 75.
Defining Global Permissions

You can define the following permission types at the global level:

- **IPAM Permissions**: Permissions to all network views, which give you permissions to all IPv4 and IPv6 networks.
- **Master Grid Permissions**: Permissions to all Master Grid members and the Scheduled Tasks permission.
- **Grids Permissions**: Permissions to all managed Grids in the Master Grid.

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.
   
   or
   
   For an admin role: From the Administration tab, select the Administrators tab -> Permissions tab -> admin_role in the Roles table, and then click the Add icon -> Global Permissions from the Create New Permission area or select Add -> Global Permissions from the Toolbar.

2. Multi-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 permission you want to configure from the Permission Type drop-down list. Depending on your selection, Multi-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. Multi-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.

Defining Object Permissions

You can add permissions to specific objects, such as the Comment field or a specific IPv4 network, 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. 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.

You can define permissions for the following object types:

- **Grid**: Permissions to the matching managed Grids.
- **IPv4 Networks**: Permissions to the matching IPv4 networks.
- **IPv6 Networks**: Permissions to the matching IPv6 networks.
- **Member**: Permissions to the matching Master Grid members.
- **IPv4 and IPv6 Networks**: Permissions to all matching IPv4 and IPv6 networks.

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. Multi-Grid Manager displays the Create Object Permissions wizard. For an admin group, the appliance displays the selected 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. Click Select Object(s). Multi-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.

Multi-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 on page 75.

You can also set permissions for specific objects from the objects themselves. For example, to define permissions for all IPv4 networks, navigate to the Multi-Grid Master 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 Master Grid tab -> Members tab -> Multi-Grid Master 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.
Applying Permissions and Managing Overlaps

In the Master Grid, 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 Network1 admin group tries to access the 10.0.0.0/16 IPv4 network. The appliance first checks if the Network1 admin group has permission defined for the network. If there is none, then the appliance checks the roles assigned to Network1. If there is no permission defined for the 10.0.0.0/16 network, the appliance continues checking for permissions in the order listed in Table 4.2. The appliance uses the first permission it finds.

<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. 10.0.0.0/16 network</td>
<td>a. Network1 admin group</td>
</tr>
<tr>
<td>2. All IPv4 networks in a specific network view of a Grid</td>
<td>b. Role 1, Role, 2, Role 3...</td>
</tr>
<tr>
<td>3. The specific network view of a Grid</td>
<td></td>
</tr>
<tr>
<td>4. All IPv4 networks in a specific Grid</td>
<td></td>
</tr>
<tr>
<td>5. All IPv4 networks</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 4.3, if an admin group has Read/Write permissions to Grid1 and all IPv4 networks, and a role assigned to it is denied permission to all IPv6 networks, the appliance provides Read/Write access to IPv4 networks in GRID1, but denies access to all IPv6 networks in Grid1.

| Table 4.3 Directly-Assigned Permissions and Roles |
|---|---|
| **Permissions** | **Effective permissions** |
| Permissions assigned to the admin group on the Master Grid | Read/Write to all IPv4 networks |
| Read/Write to Grid1 | |
| Permission inherited from an admin role on the Master Grid | Deny to all IPv6 networks |
| Effective permissions | Read/Write to all IPv4 networks in Grid1 |
| Deny to all IPv6 networks in Grid1 | |

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 4.4, the first role assigned to the admin group has Read-Only permission to the 10.0.0.0/24 IPv4 network in Grid1, and the second role has Read/Write permission to the same network. The appliance applies the permission from the first admin role.
When managed Grids synchronize objects with the Master Grid, all permissions associated with the objects are synchronized. Though you cannot change the synchronized permissions, you can inherit the synchronized permissions if you validate a user of the Grid to which the objects belong. The appliance takes into account both the Master Grid permissions and the synchronized permissions. As illustrated in Table 4.5, as an admin user, you are assigned permissions to specific networks at the Master Grid level. You also inherit the synchronized permissions of the networks from the managed Grid because you have user validation to that Grid. As a result, your effective permissions to these networks are a combination of the Master Grid permissions and the synchronized permissions of the managed Grid. Note that the Grid Master permissions supersede the managed Grid permissions when there is an overlapped permission.

### Table 4.5 Master Grid and Managed Grid permissions

<table>
<thead>
<tr>
<th>Permission 1</th>
<th>Permission 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Grid permissions</td>
<td>Read/Write to 10.0.0.0/8</td>
</tr>
<tr>
<td>Read/Write to 20.0.0.0/8</td>
<td>Read/Write to 10.0.0.0/8</td>
</tr>
<tr>
<td>Read/Write to 30.0.0.0/16</td>
<td>Read/Write to 10.0.0.0/8</td>
</tr>
<tr>
<td>Read/Write to 40.0.0.0/8</td>
<td>Read/Write to 10.0.0.0/8</td>
</tr>
<tr>
<td>Synchronized permissions of the managed Grid</td>
<td>Deny to 10.0.0.0/8</td>
</tr>
<tr>
<td>Read-only to 10.0.0.0/8</td>
<td>Deny to 10.0.0.0/8</td>
</tr>
<tr>
<td>Read-only to 20.0.0.0/16</td>
<td>Deny to 20.0.0.0/16</td>
</tr>
<tr>
<td>Read-only to 30.0.0.0/8</td>
<td>Deny to 30.0.0.0/8</td>
</tr>
<tr>
<td>Read-only to 40.0.0.0/8</td>
<td>Deny to 40.0.0.0/8</td>
</tr>
<tr>
<td>Effective permissions</td>
<td>Read/Write to 10.0.0.0/8</td>
</tr>
<tr>
<td>Read/Write to 20.0.0.0/8 (except the /16 network)</td>
<td>Read/Write to 10.0.0.0/8</td>
</tr>
<tr>
<td>Read-only to 20.0.0.0/16</td>
<td>Read/Write to 20.0.0.0/8 (except the /16 network)</td>
</tr>
<tr>
<td>Read-only to 30.0.0.0/8 (except the /16 network)</td>
<td>Deny to 20.0.0.0/16</td>
</tr>
<tr>
<td>Read/Write to 30.0.0.0/16</td>
<td>Deny to 30.0.0.0/8 (except the /16 network)</td>
</tr>
<tr>
<td>Read/Write to 40.0.0.0/8</td>
<td>Read/Write to 30.0.0.0/16</td>
</tr>
<tr>
<td>Read/Write to 40.0.0.0/8</td>
<td>Read/Write to 40.0.0.0/8</td>
</tr>
</tbody>
</table>

If you validate a user of a specific Grid through Multi-Grid Manager, you inherit the permissions of the user that you validate on that Grid. When you access the Grid through Multi-Grid Manager, you can perform specific tasks based on the permissions of the validated user of the Grid. You can also view a complete list of users that you have validated through Multi-Grid Manager, and find out the specific admin groups to which the admin users of the corresponding Grids belong. For information about how to view this information, see Viewing Validated Users on page 28.
You can also 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, Multi-Grid Manager displays a warning message and the See Conflicts link on which you click to view the overlapped permissions. For information, see Viewing Overlapped Permissions on page 77. 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 on page 68.

Viewing Overlapped Permissions

When you click See Conflicts to view overlapping permissions, Multi-Grid Manager displays the following information in the Permission Overlap dialog box:

- **Resource**: The name of the object or resource.
- **Type**: The object type.
- **Permission**: The permission granted. This can be Read/Write, Read-Only, or Deny.
- **Inherited From**: Indicates the source from which the permission is inherited.
- **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.
- **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 on page 77.
- Modify the permissions, as described in Modifying Permissions on page 79.
- Delete the permission, as described in Deleting Permissions on page 79.

Viewing Permissions

Only superusers can view the permissions of all admin groups, including the synchronized permissions.

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. Multi-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.
   - **Resource**: The name of the object, such as All IPv4 Networks.
   - **Resource Type**: The object type, such as Network View.
   - **Permission**: The defined permission for the resource.

When you click Show All for Admins, Groups, and Roles, Multi-Grid Manager displays all the Master Grid and synchronized 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

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
   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 Edit icon.
4. In the Manage Global Permissions or Create Object permissions editor, select the new permission: Read/Write, Read-Only or Deny for the resource.
5. Save the configuration.

Deleting Permissions

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 appliance supports the following authentication methods: local database, RADIUS, and Active Directory. 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 on page 80.

If you want to authenticate admins using RADIUS and Active Directory in addition to local authentication, then you must define those services on the appliance and define the admin authentication policy. For information, see About Remote Admins on page 81.

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 appliance in case the remote servers become unreachable.

Creating Local Admins

When you create an admin account, you must specify the 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 of Multi-Grid Manager. The appliance can use the time zone that it automatically detects from the management system that the admin uses to log in. Alternatively, you can override the time zone auto-detection feature and specify the time zone.

To create an admin account and add it to an admin group:

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 Basic wizard, complete the following:
   — Login: Enter a name for the administrator. This is the username that the administrator uses to log in.
   — Password: Enter a password for the administrator to use when logging in.
   — Confirm Password: Enter the same password.
   — 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, Multi-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.
   — 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 Using Extensible Attributes on page 168.
5. Save the configuration.
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 on page 80.
   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.
   — 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 Using Extensible Attributes on page 168.
3. Save the configuration.

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

You can configure the appliance to authenticate admins whose user credentials are stored on a RADIUS server, AD domain controller, or TACACS+ server.

To authenticate admins using RADIUS, Active Directory or TACACS+, you must define those services on the appliance and define the admin policy. The admin policy lists which authentication services to use and in what order.

The authentication policy also lists the local admin groups that match the remote admin groups. If you configured admin groups on the remote authentication server, you must configure admin groups with the same names on the appliance so it can assign remote admins to the correct group. If you did not configure admin groups on the remote authentication server, you must configure a default group for remote admins on the appliance.

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.
If authentication succeeds, the appliance determines the admin’s privileges based on the admin group of the admin. It 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 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 4.2* illustrates the authentication and authorization process for remote admins.

*Figure 4.2* Authenticating Remote Admins

1. An admin enters his user name and password to log in to the appliance.
2. The appliance checks the admin policy for the first authentication service, which is a RADIUS service. The appliance sends an Access-Request packet to the RADIUS server.
3. The appliance responds with an Access-Reject package because the admin’s user name and password are not in its database.
4. The appliance tries the next authentication service on the list, which is an Active Directory (AD) service. It sends a request to the AD server.
5. The AD server responds with an Access-Reject package because the admin’s user name and password are not in its database. The TACACS+ server finds the user name and password in its database and sends an access accept together with the admin’s group memberships.
6. The appliance matches one of the admin’s groups with a group in the admin policy.
7. The appliance allows the admin to log in and applies the privileges of the IT-BLDG2.
8. User Name Member Of
   - admin10 IT-Bldg1
   - IT-Bldg2
To configure the appliance to authenticate admins against a RADIUS server and an AD controller:

- Configure the RADIUS and AD authentication services. For information about the RADIUS authentication service, see Authenticating Using RADIUS. For information about the AD authentication service, see Authenticating Admin Accounts Using Active Directory on page 88.
- Configure admin groups that match those on the remote server. Optionally, specify a default admin group. For information about admin groups, see About Admin Groups on page 67.
- Configure the admin policy, as described in Defining the Authentication Policy on page 94.

**Note:** Infoblox strongly recommends that even 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 appliance in case the remote servers become unreachable.

---

**Authenticating Using RADIUS**

RADIUS provides authentication, accounting, and authorization functions. The appliance supports authentication using the following RADIUS servers: FreeRADIUS, Microsoft, Cisco, and Funk.

You must be a superuser to configure admin accounts and RADIUS server properties on the appliance.

When you configure the appliance to authenticate administrators using a RADIUS server, the appliance acts similarly to a network access server (NAS), which is a RADIUS client that sends authentication and accounting requests to the RADIUS server. Figure 4.3 illustrates the authentication process.

*Figure 4.3 Authentication using a RADIUS server*

1. A user makes an HTTPS connection to the appliance and sends a user name and password.
2. The appliance checks the remote admin policy and selects RADIUS as the authentication method.
3. The appliance sends an Access-Request packet to the RADIUS server.
4a. If the RADIUS server authenticates the user, it sends back an Access-Accept packet. The appliance lets the user log in and applies the authorization profile.
4b. If the RADIUS server rejects the authentication request, it sends back an Access-Reject packet. The appliance does not allow the user to log in.
Remote RADIUS Authentication

When you configure the appliance for remote authentication with a RADIUS server, you must specify the authentication method of the RADIUS server. Specify 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 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 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.

To configure the appliance to authenticate administrators using a RADIUS server, you must configure admin accounts and groups for these administrators on the RADIUS server. Then, on the appliance, you must do the following:

- Configure an authentication server group for RADIUS.
- Define admin groups and specify their privileges and settings. The names must match admin group names defined on the RADIUS server. The appliance applies these privileges and settings to users that belong to those groups on the RADIUS server. See About Admin Groups on page 67 for information about defining admin groups.
- If there are no admin groups defined on the RADIUS server, designate an admin group as the default group. See About Admin Groups on page 67 for information about defining a default admin group.
- Add the RADIUS service to the list of admin authentication services in the admin policy, and add the admin groups that match those on the RADIUS server. See Defining the Authentication Policy on page 94 for more information about configuring admin 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.

After you add a RADIUS server to the 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 on the appliance:

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 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 appliance and the RADIUS server use to encrypt and decrypt their messages. This shared secret is a value that is known only to the 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 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 appliance from trying to connect to this server.

— Click **Test** to test the configuration. If the 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.

— **Authentication:** Optionally, modify the authentication settings. These settings apply to all RADIUS servers that you configure on the 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 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.

  — **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 accounting RADIUS server. The default is 1000.

  — **Mode:** Specifies how the appliance contacts the RADIUS servers. The default is Ordered List. Do not change this value; Ordered List is the only mode that the appliance uses when it uses a RADIUS server group to authenticate remote admins. In this mode, the appliance 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.

  — **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.
Managing the RADIUS Server 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 appliance attempts to contact a RADIUS server. You can change the order of the list, as follows:

1. From the Administration tab, click the Authentication Server Groups tab -> RADIUS Services subtab, select the server_group check box and click the Edit icon.

2. In the RADIUS Servers table, do the following:
   - To move a server up the list, select it and click the up arrow.
   - To move a server down the list, select it and click the down arrow.
   
   You can also delete a RADIUS server by selecting a RADIUS server from the RADIUS Servers table and clicking the Delete icon.

3. Save the configuration.

Disabling RADIUS Servers on Multi-Grid Master

You can disable a RADIUS server if, for example, the connection to the server is down and you want to stop the appliance from trying to connect to this server.

To disable a RADIUS server:

1. From the Administration tab, click the Authentication Server Groups tab -> RADIUS Services subtab, select the server_group check box and click the Edit icon.

2. In the RADIUS Service editor, select the check box of the server you want to disable in the RADIUS Servers section, and then click the Edit icon.

3. In the RADIUS Servers section, select Disable.

4. Save the configuration.

Configuring Remote RADIUS Servers

In addition to setting up the appliance to communicate with a RADIUS server, you must also set up the remote RADIUS server to communicate with the 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 appliance:

- Authentication Port
- Accounting Port
- Domain Name/IP Address of the appliance
- Shared Secret Password
- Vendor Types
Authenticating Using RADIUS

Configuring Admin Groups on the Remote RADIUS Server

Infoblox supports admin accounts on one or more RADIUS servers. To set up admins and associate them with an admin group on a remote RADIUS server, do the following:

- 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 a local admin group on the appliance (or use an existing group)
- Define a remote admin group—with the same name as the group defined on the appliance—on the RADIUS server
- Associate one or more remote admin accounts on the RADIUS server with the remote admin group

Refer to the documentation for your RADIUS server for more information.

Configuring Admin Accounts on the Remote RADIUS Server

To set up remote admin accounts on a RADIUS server and apply the privileges and properties of the admin group on the appliance, do the following:

- Define the admin group on the appliance, and then add it to the admin policy. Note that the names of the remote admin group and the admin group on the appliance must match. You can also define a default admin group. See Defining the Authentication Policy on page 94 for more information on configuring admin policies and remote admin group lists.
- On the RADIUS server:
  - Create one or more admin accounts.
  - 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.

When an administrator whose account is stored on a RADIUS server attempts to log in to an appliance, the appliance forwards the user name and password for authentication to the RADIUS server. When the server successfully authenticates the administrator and it responds to the appliance without specifying an admin group, the appliance applies the privileges and properties of the default admin group to that administrator. Refer to the documentation for your RADIUS server for more information.

Authorization Groups Using RADIUS

You can specify authorization privileges for an admin group on the appliance only. The appliance ignores authorization settings from the RADIUS server. Therefore, you must configure all admin groups on the appliance, regardless of where the admin accounts that belong to those groups are stored—on the appliance or on the RADIUS server. For information about specifying superuser and limited-access authorization privileges, see Creating Superuser Admin Groups on page 68 and Creating Limited-Access Admin Groups on page 68.

Then you must add those admin groups to the authentication policy. For more information, see Defining the Authentication Policy on page 94.

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. For information, see Managing the RADIUS Server List on page 86.
Authenticating Admin Accounts Using Active Directory

Active Directory™ (AD) is a distributed directory service that is a repository for user information. The appliance can authenticate admin accounts by verifying user names and passwords against Active Directory. If the admin account does not exist on the AD domain controller, or if the user name and password do not match entries on the domain controller, the appliance checks the authentication policy for the next authentication service to try. However, if the appliance verifies the username and password successfully, it grants access. In addition, the 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.

You must be logged in to the appliance as a superuser to configure the AD authentication service. Figure 4.4 illustrates the Active Directory authentication process.

*Figure 4.4 Authentication Using a Domain Controller*

1. A user makes an HTTPS connection to the appliance and sends an account name and password.
2. The appliance checks the authentication policy to determine which authentication service to use. The authentication policy specifies an AD authentication service.
3. The appliance sends an authentication request to the first domain controller in the AD server group. The appliance also requests the group membership information of the admin.
4a. Authentication is successful. The domain controller successfully authenticates the admin user. The group membership information for the administrator is sent to the appliance. The first group in the list that matches the groups returned by the domain controller is assigned to the admin, along with the associated permissions after that admin logs in.
4b. Authentication is unsuccessful. The domain controller sends back a deny access result to the appliance. No group membership information is sent.

The appliance lets the user log in and applies the authorization profile.
The appliance grants all permissions specific to the administrator based on the group membership sent from the domain controller associated with the admin account. If there is no group membership information for the admin, the default group is assigned (if configured).

The appliance does not allow the user to log in.
Admin Authentication Using Active Directory

To configure the appliance to authenticate administrators using Active Directory, you must first configure user accounts on the domain controller. Then, on the appliance, do the following:

- Configure an AD authentication server group on the appliance and add one or more AD domain controllers to the group. For information about configuring an AD authentication service group for admins, see Configuring an Active Directory Authentication Service Group.
- If you configured admin groups on the AD controller, you must create those same groups on the 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 appliance assigns admins to the default group if none of the admin groups on the 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 on page 67.
- 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 on page 94 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 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 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 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 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 appliance from trying to connect to this server.
     - Click Test to test the configuration. If the 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.
   - Timeout(s): The number of seconds that the appliance waits for a response from the specified authentication server. The default is 5.

Multi-Grid Manager Administrator Guide (Rev. A) ||| 89
— **Comment**: Enter additional information about the service.
— **Disable**: Select this to retain an inactive AD authentication service profile.

4. Save the configuration.

**Managing the Domain Controller List**

This list determines the order in which the appliance attempts to contact a domain controller. You can change the order of the list, as follows:

1. From the **Administration** tab, click the **Authentication Server Groups** tab → **Active Directory Services** subtab, select the **server_group** check box and click the **Edit** icon.
2. In the **Domain Controllers** table, do the following:
   — To move a server up the list, select it and click the up arrow.
   — To move a server down the list, select it and click the down arrow.
   You can also delete a domain controller by selecting the controller from the Domain Controllers table and clicking the Delete icon.
3. Save the configuration.

**Disabling Domain Controllers**

You can disable an AD domain controller if, for example, the connection to the server is down and you want to stop the appliance from trying to connect to this server. When you disable a server, the appliance keeps the configuration of the domain controller.

To disable a domain controller:

1. From the **Administration** tab, click the **Authentication Server Groups** tab → **Active Directory Services** subtab, select the **server_group** check box and click the Edit icon.
2. In the **Edit Domain Controller** section, select **Disable**.
3. Save the configuration.
You can configure the Multi-Grid Master 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 the Multi-Grid Master, 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, The Multi-Grid Master can match the group name with the group in the authentication policy and automatically assign the admin to that group.

Figure 4.5 illustrates the TACACS+ authentication and authorization process when PAP/CHAP authentication is used.

**Figure 4.5 TACACS+ Authentication**

1. A user makes an HTTPS connection to the appliance and sends an account name and password.
2. The appliance checks the authentication policy, which specifies the TACACS+ authentication server group.
3. The appliance sends an AUTHENTICATION START message with the user’s credentials.
4a. The TACACS+ server sends an AUTHENTICATION REPLIy indicating the admin was successfully authenticated.
4b. The appliance sends an AUTHORIZATION REQUEST with the attribute-value string for the “Infoblox” service.
    - The TACACS+ server sends an AUTHORIZATION RESPONSE indicating authorization succeeded and includes the custom attribute “Infoblox-admin-group”.
4c. The appliance sends an AUTHENTICATION REQUEST with the attribute-value string for the “Infoblox” service.
    - The TACACS+ server sends an AUTHENTICATION REPLY indicating the admin was successfully authenticated.
4d. The appliance sends an AUTHORIZATION REQUEST with the attribute-value string for the “Infoblox” service.
    - The TACACS+ server sends an AUTHORIZATION RESPONSE indicating authorization succeeded and includes the custom attribute “Infoblox-admin-group”.
4e. The appliance sends an AUTHENTICATION REQUEST with the attribute-value string for the “Infoblox” service.
    - The TACACS+ server sends an AUTHENTICATION REPLY indicating the admin was successfully authenticated.

The appliance allows the user to log in and assigns it to the admin group in the authentication policy that matches the group in the custom attribute.

If the appliance does not find a matching group in the authentication policy, it assigns the user to the default admin group.

The appliance does not allow the user to log in.
TACACS+ Accounting

When you enable TACACS+ accounting, the Multi-Grid Master 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. The Multi-Grid Master 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, the Multi-Grid Master 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 the Multi-Grid Master 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 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 on the Multi-Grid Master, 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 Multi-Grid Master:

- 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 Multi-Grid Master that matches the user group on the TACACS+ server. Note that the 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 on page 67.
- In the authentication policy, add the newly configured TACACS+ server group and the TACACS+ admin group name. See Defining the Authentication Policy on page 94 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. the Multi-Grid Master sends authentication requests to the TACACS+ servers in the order they are listed. The Multi-Grid Master sends authentication requests to the first server on the list. If that server is unreachable or generates an error, then the Multi-Grid Master sends the request to the next server in the list that has not been previously queried, and so on. The Multi-Grid Master 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 appliance and the TACACS+ server use to encrypt and decrypt messages.

— **Connection Interface:** The interface on the appliance that is used to connect to the authentication server group. You can use either the LAN or MGMT interface.

— **Enable Accounting:** Select this to enable the Multi-Grid Master to send accounting information to the TACACS+ server.

— **Disable Server:** Select this to prevent queries from being sent to this server. You can retain the configuration, but disable the service.

Click **Test** to test the configuration. Click **Add** to add the TACACS+ server to the list.

When you add multiple TACACS+ servers, the appliance lists the servers in the order you added them. This list also determines the order in which the appliance attempts to contact a TACACS+ server. You can move a server up or down the list by selecting it and clicking the up or down arrow.

— **Authentication/Authorization:** Optionally, modify the authentication and authorization settings. These settings apply to all TACACS+ servers that you configure on the 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 the appliance 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.
Defining the Authentication Policy

The authentication policy defines which authentication services 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 Services

To enable the Multi-Grid Master to use multiple authentication services, you must define a prioritized list of services 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 service.
3. Select one of the following in the Add Authentication Service section:
   - RADIUS: Select this to add the RADIUS authentication service, and then select a service from the drop-down list.
   - Active Directory: Select this to add the AD authentication service, and then select a service from the drop-down list.
   - TACACS+: Select this to add the TACACS+ authentication service, and then select a service from the drop-down list.
4. Click Add.
   You can reorder the list by selecting an authentication service and moving it up or down the list using the arrow keys.

Configuring a List of Remote Admin Groups

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. You can also define a default admin group to which the appliance 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 domain controller or the RADIUS 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. From the Map the remote admin group to the local group in this order section, click the Add icon.
3. In the Admin Group Selector dialog box, select an admin group, and then click the Select icon. 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.

To assign a user to a specific admin group if the remote admin group is not found, select Assign User to this Group if Remote Admin Group cannot be found, and then click Select. In the Admin Group Selector dialog box, select an admin group, and then click the Select icon.
Authenticating Admins Using Two-Factor Authentication

Multi-Grid Manager can authenticate users, such as U.S. Department of Defense CAC users, with smart cards that contain X.509 client certificates. The status of these certificates is stored remotely on OCSP responders. You can configure NIOS to use the two-factor authentication method to authenticate these users. 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. Finally, NIOS validates the status of the client certificate through the OCSP service. Note that you cannot add OCSP validation as part of the authentication policy. You must first configure the authentication policy, and then configure and enable the OCSP service for the two-factor authentication to take effect. For information about how to set up an authentication policy, see Managing the Domain Controller List on page 90.

OCSP is an internet protocol that validates certificate status for X.509 digital certificates that are assigned to specific admins. For more information about OCSP, refer to RFC 2560 at 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 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 before a smart card admin can access the appliance.

Figure 4.5 illustrates the two-factor authentication and authorization process.
Managing Administrators

1. User inserts a smart card, establishes a successful SSL/TLS client authenticated HTTPS connection to the appliance (through the client certificate and private key from the smart card), and sends a username, password, and client certificate.

2. The appliance checks the authentication policy.

3. Based on the authentication policy, the appliance sends authentication messages to the corresponding servers.

4a. Authentication servers send responses indicating the admin is successfully authenticated.

4b. Authentication servers send messages indicating authentication and/or authorization is unsuccessful.

5. The appliance sends a request that contains the admin certificate serial number to the OCSP responder to request for client certificate status.

Multi-Grid Manager allows the admin to log in and assigns it to the admin group that matches the smart card user and applies the authorization profile.

6a. The OCSP responder returns a "good" certificate status indicating authentication is successful. In a Direct trust model, the appliance uses the OCSP responder certificate to validate the OCSP reply. In a Delegated trust model, it uses the CA certificate to validate the reply.

6b. The OCSP responder returns a "revoked" or "unknown" certificate status indicating authentication is unsuccessful.
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 on page 70. To configure two-factor authentication, consider the following:

- You must first set up an OCSP authentication server group and enable it.
- You can configure only one OCSP authentication server group that contains one or multiple OCSP responders to which Multi-Grid Manager 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 on page 65.
2. Upload the CA (Certificate Authority) certificate, as described in About CA Certificates on page 65. 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 an OCSP authentication server group and enable it, as described in Configuring the OCSP Authentication Server Group on page 97.

Note that once you save the OCSP authentication server group configuration, the appliance terminates administrative sessions for all admin users. After you enable the OCSP 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 the OCSP Authentication Server Group

To configure and enable the OCSP authentication service, complete the following:

1. From the Administration tab, click the Authentication Server Groups tab.
2. Click the OCSP Services subtab and click the Add icon.
3. In the Add OCSP Service wizard, complete the following:
   - Name: Enter a name for the service.
   - 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**: 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 OCSP service is disabled and two-factor authentication is no longer in effect.

Click **Add** to save the configuration and add the responder to the table. You can add multiple OCSP responders for failover purposes. You can use the up and down arrows to place the responders in the order you desire. The appliance tries to connect with the first responder on the list. If the connection fails, it tries the next responder on the list, and so on. Grid Manager displays the following for each responder:

— **Responder**: The FQDN or the IP address of the OCSP responder.
— **Comment**: Information you entered about the OCSP responder.
— **Port**: The port number on the OCSP responder to which the appliance sends authentication requests.
— **Disable**: Indicates whether the responder is disabled or not. Note that you must enable at least one responder to enable the OCSP service.

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. The default is 1 second. You can select the time unit from the drop-down list.

— **Retries**: Enter the number of times the appliance tries to connect to the responders after a failed attempt. The default is 5.

— **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 30 seconds. This is the time interval that NIOS waits before it tries to contact the responder again since the last attempt when the appliance could not connect with the responder or when the responder did not send a reply within the configured response timeouts and retry attempts.

— **Trust Model**: From the drop-down list, select **Direct** or **Delegated** 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**.

— **SSH Remote Console Authentication**: Select a method for admins to log in to the appliance through the CLI. From the drop-down list, select **No Login** to disable SSH remote connection through CLI, or select **Login no Certificate** to authenticate admins using their user names and passwords without authenticating their client certificates through the OCSP service. The default is **No Login**.

**Note**: To enable SSH remote console authentication, you must also enable remote console access in the Grid or member settings.

— **Enable Superuser login when all responders are unavailable**: Select this check box to enable superuser login when all OCSP responders are unavailable. As long as the superusers are authenticated through the configured authentication policy, enabling this allows superusers to log in to the appliance if all OCSP responders were disconnected or did not reply within the configured response timeouts and retry attempts.

— **Comment**: Enter useful information about the OCSP authentication service.

— **Disable**: Select this to retain an inactive OCSP authentication service profile.

**Note** that enabling the OCSP 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 CN...
(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.

Viewing the OCSP Authentication Server Group

To view the OCSP authentication server group, complete the following:

1. From the Administration tab, click the Authentication Server Groups tab.
2. Grid Manager displays the following about the OCSP authentication server group:
   - Name: The name of the OCSP server group.
   - Comment: Comments about the OCSP server group

You can also display the following column:
   - Disabled: Indicates if the OCSP server group is enabled or disabled.

You can do the following in this tab:

- Sort the data in ascending or descending order by column.
- Select the OCSP server group and click the Edit icon to modify data, or click the Delete icon to delete it.
- Print and export the data in this tab.

Create a bookmark for this page.
Changing Password Length Requirements

Password length requirements control how long a password must be for an 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 Multi-Grid Manager tab, and then select Grid Properties -> Edit from the Toolbar.
2. In the Grid Properties editor, select the Security tab.
3. Enter a number from 4 to 64 in the Minimum Password Length field.
4. Save the configuration.

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. 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 on page 253.

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.

To notify an administrator:
1. From the Master Grid tab, select the Members tab -> multi-grid master check box, and then select Master Grid Properties -> Edit from the Toolbar.
2. In the Master 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 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 appliance. In this case, specify the DNS name or IP address of a different SMTP server that does accept email from the 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.
### Administrative Permissions for the Master Grid

*Table 4.6* lists some of the common tasks admins can perform and their required permissions. All the permission tables in this chapter use the following definitions:

- **RW** = Read/Write permission
- **RO** = Read-only permission

*Table 4.6 Master Grid Permissions*

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Master Grid members</th>
<th>All Managed Grids</th>
<th>Specific Managed Grid</th>
<th>All Network Views</th>
<th>Scheduling Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Master Grid members</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scheduling tasks for all supported objects</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add a managed Grid</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify or delete a managed Grid</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upgrade a managed Grid</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Administrative Permissions for Scheduling Tasks

You can schedule tasks, such as adding IPv6 networks, for a future date and time. To schedule tasks, you must first enable the scheduling feature, and then define administrative permissions for admin groups and admin roles. 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 the Scheduling Tasks permission.

Superusers can do the following:

• Enable and disable task scheduling
• 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 on page 73. 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>
<thead>
<tr>
<th>Tasks</th>
<th>Scheduling Tasks</th>
<th>All Master Grid members</th>
<th>All Managed Grids</th>
<th>All IPv4 Networks</th>
<th>All IPv6 Networks</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>
<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>
<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:

Note that the appliance deletes all pending scheduled tasks when superusers disable task scheduling. 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 Disconnected Grids

*Table 4.8* lists some of the common tasks admins can perform and their required permissions.
All the permission tables in this chapter use the following definitions:
- **RW** = Read/Write permission
- **RO** = Read-only permission

*Table 4.8 Administrative Permissions for Disconnected Grids*

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Multi-Grid Manager Permission on Master Grid</th>
<th>Multi-Grid Manager Permission on Grid</th>
<th>Synchronized Grid Permission</th>
<th>Scheduling Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform attach and detach</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Schedule attach and detach</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visualization view, list view, and perform cancel operation</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Launch Snapshot Manager, list view</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Launch Apply Template and select template</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Launch Snapshot Manager, select a Grid, export, and print</td>
<td>RO</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add snapshot</td>
<td>RO</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apply snapshot</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete snapshot</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clone snapshot to template</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Launch Delta Viewer and select snapshot</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delta Viewer, view difference between two snapshots</td>
<td>RO</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Launch Apply Template dialog and select templates</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apply templates</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grid Templates - view, delete, export, and print Grid templates</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add Grid templates</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure external storage FTP server</td>
<td>RW</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:

- IPv4 networks
- IPv6 networks

The appliance applies permissions for IPAM resources hierarchically. 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. Permissions at more specific levels override global permissions.

Administrative Permissions for IPv4 and IPv6 Networks

Limited-access admin groups can access IPv4 and IPv6 networks only if their administrative permissions are defined. You can grant Read-only or Read/Write permission, or deny access to networks.

Notes that on the Master Grid, if you want to perform certain tasks on a synchronized network, you must have permissions to both the managed Grid to which the network belongs and to the network itself. For example, to view a synchronized network, you must have at least a Read-only permission to the managed Grid and Read-only permission to the network. If you want to modify a synchronized network, you must have Read/Write permission to both the managed Grid and the network.

The following table lists the tasks admins can perform and the required permissions for synchronized IPv4 and IPv6 networks on the Master Grid.

Table 4.9 Network Permissions

<table>
<thead>
<tr>
<th>Tasks</th>
<th>All Managed Grids</th>
<th>Specific Managed Grid</th>
<th>All Network Views</th>
<th>Specific IPv4 Network Container or Network</th>
<th>Specific IPv6 Network Container or Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>View and search for all IPv4 and IPv6 networks</td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resize IPv4 networks</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add and modify IPv4 networks</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add and modify IPv6 networks</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 5 Configuring a Master Grid

To deploy a Master Grid, it is important to understand what it is, how to create a Multi-Grid Master and add members, and how to manage the Master Grid. This chapter explains these tasks in the following sections:

- **About the Master Grid** on page 106
  - Creating a Multi-Grid Master on page 107
- **Creating a Multi-Grid Master** on page 107
  - Master Grid Setup Wizard on page 107
  - Creating an HA Multi-Grid Master on page 107
  - Creating a Single Multi-Grid Master on page 110
- **Adding Master Grid Members** on page 113
  - Joining a Master Grid on page 115
- **Managing a Master Grid** on page 116
  - Changing the Master Grid Properties on page 116
  - Removing a Master Grid Member on page 117
  - Promoting a Master Candidate on page 118
### About the Master Grid

A Master Grid is similar to an Infoblox Grid, except that the sole purpose of the Master Grid is to manage multiple Grids. It synchronizes status and IPAM information with its managed Grids, so you can view and manage data across multiple Grids from the Master Grid.

A Master Grid contains one Multi-Grid Master and one or more members. The Multi-Grid Master and its members can be single appliances or HA (High Availability) pairs. The Master Grid members cannot run any protocol, such as DNS or DHCP. Their only role in the Master Grid is that of Multi-Grid Master candidates. An appliance or HA pair that joins a Master Grid that already has a Multi-Grid Master automatically becomes a Multi-Grid Master candidate.

Communications between the Master Grid and its members are through an encrypted VPN tunnel, the same as in an Infoblox Grid. For details on Grid communications, refer to the *NIOS Administrator Guide*.

A Master Grid can include Infoblox appliances and vNIOS appliances. A vNIOS appliance is a non-Infoblox hardware platform running the vNIOS software package. You can configure Infoblox appliances and vNIOS appliances for VMware as Multi-Grid Masters or members. You can configure the other vNIOS appliances as grid members only. For information, refer to the *Infoblox NIOS Administrator Guide*.

NIOS and vNIOS appliances support different numbers of Grids. The maximum number of Grids that a Master Grid can support is based on the member with the lowest capacity. Note that when an appliance joins a Master Grid, the Multi-Grid Master checks if the platform type can support the number of currently managed Grids. If it cannot, then the join attempt is rejected.

The Multi-Grid Master is the only member in the Master Grid that runs the multi-grid management service that synchronizes data with the managed Grids. If the Multi-Grid Master is an HA pair, then the service runs on the active node only. If an HA failover occurs during a synchronization, the failing node immediately aborts the synchronization. The new active node resumes the next synchronization.

A Multi-Grid Master candidate does not run this service until it is promoted to Multi-Grid Master. The Multi-Grid Master replicates its database to all its members so that they have all the data they need in case of a candidate promotion. For more information about the Grid synchronization process, see *Synchronizing Grids* on page 122.

To connect to the Master Grid, you make a secure connection to Multi-Grid Manager. From Multi-Grid Manager, you can configure and manage the Master Grid. *Figure 5.1* illustrates the basic operations in multi-Grid management.

*Figure 5.1 Grid Synchronization and Database Replication*

---

The administrator makes a secure connection to the Multi-Grid Master to manage and monitor its Grids.

---

The Grid Masters of the managed Grids synchronize their status and IPAM data with the Multi-Grid Master...

---

...and the Multi-Grid Master replicates the entire database to the Multi-Grid Master candidate.
Creating a Multi-Grid Master

To create a Master Grid, you first create a Multi-Grid Master and then add members. Although the Multi-Grid Master can be a single appliance (a “single Multi-Grid Master”), a more resilient design is to use an HA pair (an “HA Multi-Grid Master”) to provide hardware redundancy. (For information about Infoblox HA pairs, refer to the NIOS Administrator Guide. You can create a Master Grid in either IPv4 or dual mode (IPv4 and IPv6). An IPv4 Master Grid uses IPv4 as the Grid communication protocol and a dual mode Master Grid uses IPv4 or IPv6 as the communication protocol.

Note that the appliances in the Master Grid must have the Multi-Grid Management license installed and cannot have any other licenses installed, such as IF-MAP or DNS/DHCP. vNIOS appliances must have vNIOS and Multi-Grid Management license installed.

Note: For information about enabling and using the MGMT port, the Infoblox GUI, and SSH, see Using the MGMT Port on page 183, Logging in to Multi-Grid Manager on page 19, and Enabling Remote Console Access on page 175.

Master Grid Setup Wizard

The Master Grid Setup Wizard simplifies configuring a Master Grid. You can use it to configure an HA or single Multi-Grid Master and to join appliances to the Master Grid. The Master Grid Setup Wizard appears when you first log in to the appliance. After that, you can access it at anytime by expanding the Toolbar and clicking Master Grid Properties -> Setup Wizard.

Creating an HA Multi-Grid Master

You can create an HA Multi-Grid Master in either IPv4 or dual mode. An IPv4 HA Master uses IPv4 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 Master Grid Setup Wizard to configure them as Nodes 1 and 2 to form an HA Multi-Grid Master.

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):

- 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 auto-negotiate the optimal settings, see Ethernet Port Usage on page 177 for steps you can take to resolve the problem.
Configuring a Master Grid

Putting 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 Infoblox--1050-A, -1550-A, -1552-A, -1852-A, -2000-A, and -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.

   **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.

**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.

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 Multi-Grid Manager* on page 19.

3. Review the End-User License Agreement and click I Accept.

   The Master Grid Setup wizard appears.

4. On the first screen, select Configure a Master Grid and click Next.

5. On the next screen, specify the Master Grid properties and click Next:

   - **Master Grid Name:** Enter a text string that the two appliances use to authenticate each other when establishing a VPN tunnel between them. The default Master 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.
   - **Show Password:** Select this to display the password. Clear the check box to conceal the password.
   - **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 Multi-Grid Master.
     - **IPv4:** Select this to configure an IPv4 HA Multi-Grid Master.
   - **Is the super 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.

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 Multi-Grid Master. For IPv4 HA Multi-Grid Master, specify the network information for VIP (IPv4), Node1 HA (IPv4), Node2 HA (IPv4), Node1 LAN1 (IPv4), and Node2 LAN1 (IPv4) interfaces.
     For a dual mode HA Multi-Grid Master, if you select IPv4 as the protocol for HA communications, 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) interfaces.
For a dual mode HA Multi-Grid Master, if you select IPv6 as the protocol for HA communications, 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.

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 Master Grid and indicate whether the Master Grid synchronizes its time with an NTP (Network Time Protocol) server.
   - If you choose to enable NTP, click the Add icon when the NTP Server table appears 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.
   - **Next**.

9. 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 Master 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 Multi-Grid Master.

10. 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.
2. Log in using the default user name and password **admin** and **infoblox**.
3. Review the End-User License Agreement and click **I Accept**.
Configuring a Master Grid

The Master Grid Setup wizard appears.

4. On the first screen, select Join Existing Master Grid and click Next.

5. On the next screen, specify the Master Grid properties and click Next.
   - Master 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 Master Grid name you entered for node 1.
   - Multi-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.

7. 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 setup of the HA Multi-Grid Master is complete. From now on, when you make an HTTPS connection to the HA pair, use the VIP address.

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 Multi-Grid Manager, and by making an SSHv2 connection to the LAN 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 LAN or MGMT port on the active and passive nodes.

The communication protocol for all the services in a dual mode (IPv4 and IPv6) HA Master Grid is the same protocol as the one used for VRRP advertisements. For example, if you select IPv4 in the Send HA and Grid Communication 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 Grid. For information, see Changing the Communication Protocol for a Dual Mode Member on page 114.

Creating a Single Multi-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 Multi-Grid Master. You can create a single Grid Master in either IPv4 or dual mode (IPv4 and IPv6). Infoblox recommends frequent backups if the Multi-Grid Master is a single appliance, and there is no master candidate. For information about which vNIOS appliance supports configuration as a single Multi-Grid Master, refer to the NIOS Administrator Guide.

Setting up an appliance as a single Multi-Grid Master is very easy. You can use the Master Grid Setup Wizard to create a single Multi-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 Multi-Grid Master using the Master 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 LAN 1 port on the appliance to a switch on the network.

   **Note:** The Ethernet ports on the Infoblox-1050-A, -1550-A, -1552-A, -1852-A, -2000-A, and -4010 appliances are autosensing, so you can use either a straight-through or cross-over Ethernet cable for this connection.

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.
A certificate warning appears 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, which does not match the destination IP address you entered in step 3. To stop the warning message 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 on page 21.

5. Log in using the default user name admin and password Infoblox.

6. Review the End-User License Agreement and click I Accept.

The Master Grid Setup wizard appears.

7. On the first screen, select Configure a Master Grid and click Next.

8. On the next screen, specify the Master Grid properties and click Next:

   - Master Grid Name: Enter a text string that the Multi-Grid Master and appliances joining the Master Grid use to authenticate each other when establishing a VPN tunnel between them. The default Master Grid name is Infoblox.
   - Shared Secret: Enter a text string that the Multi-Grid Master and appliances joining the Master 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 from the drop-down list:
     - IPv4 and IPv6: Select this to configure a dual mode HA Multi-Grid Master.
     - IPv4: Select this to configure an IPv4 HA Multi-Grid Master.
   - Is the Super Grid Master an HA pair?: Select No.

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 Master Grid. For IPv4 Master Grid, specify the network information for LAN1 (IPv4) port and for a dual mode Master Grid, 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: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.

   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.
Configuring a Master Grid

- **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. It displays all settings supported by the hardware type. For information, see **Modifying Ethernet Port Settings** on page 181.

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 Multi-Grid Master and indicate whether the Multi-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. You can enter IP addresses for multiple NTP servers.
   - If you choose to disable NTP, set the date and time for the appliance.

12. 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 **Master 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 Multi-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 Multi-Grid Master is complete. From now on, when you make an HTTPS connection to the appliance, use its new IP address.

In a dual mode Master Grid, 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 Member** on page 114.
Adding Master Grid Members

You can add single appliances and HA pairs to a Master Grid, forming single members and HA members respectively. You can configure Master Grid members in either IPv4 or dual mode (IPv4 and IPv6). New members inherit all settings that you set at the Master Grid level unless you override them at the member level. Master Grid members automatically become Multi-Grid Master candidates and do not run protocols, such as DNS and DHCP. Note that appliances you configure as Master Grid members must have the Multi-Grid management license installed.

The process for adding either a single appliance or HA pair to a Master Grid involves the following steps:

1. Configuring the member on the Multi-Grid Master.
2. Joining the appliance or HA pair to the Master Grid. This includes defining the VIP or IP address of the Multi-Grid Master, the Master Grid name, and the shared secret on the single appliance or HA pair. If an appliance or HA pair cannot join the Master 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 Removing a Master Grid Member on page 117.

When an appliance joins a Master Grid, the Multi-Grid Master checks if the platform type supports the same number of Grids than those that are currently managed by the Master Grid. If the platform type supports less, the member is rejected. Because all Master Grid members are Master candidates, data replication occurs automatically after a member joins the Master Grid.

Note: An appliance or an HA pair that joins a Master Grid, automatically becomes a Multi-Grid Master candidate and you cannot disable the appliance from being a Master candidate. In such case, you cannot change the type of network connectivity for both Master Grid and Grid member.

Configuring a Member on the Multi-Grid Master

1. From the Master Grid tab, select the Members tab.
2. Expand the Toolbar and click Add -> Master Grid Member.
   - Member Type: Specify the appliance type of the 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 Master Grid.
   - Time Zone: If the member is in a different time zone from the Master Grid, click Override and select a time zone.
   - Comment: Type a comment that provides some useful information about the appliance, such as its location.
   - Multi-Grid Master Candidate: This check box is selected by default and is not configurable.
3. Enter the following information about the member that you are adding to the Master Grid and click Next:
   - Type of Network Connectivity: Select the type of network connectivity for the member from the drop-down list:
     - IPv4 and IPv6: Select this to configure a dual mode member.
     - IPv4: Select this to configure an IPv4 member.
   - Standalone Member: Select this check box if the member is a single appliance.
   - High Availability Pair: Select this check box if the member is an HA pair.
     - 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 Master Grid.
   - Required Ports and Addresses: This table lists the network interfaces based on the type of network connectivity. For IPv4 member, specify the network information for LAN1 (IPv4) port and for a dual mode member, specify the network information for both LAN1 (IPv4) and LAN1 (IPv6).
Configuring a Master Grid

1. Specify the network information for VIP (IPv4), Node1 HA (IPv4), Node2 HA (IPv4), Node1 LAN1 (IPv4), and Node2 LAN1 (IPv4) interfaces.

2. 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 (IPv6), Node1 LAN1 (IPv6), and Node2 LAN1 (IPv6) interfaces.

3. 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 (IPv4), Node1 LAN1 (IPv4), Node2 LAN1 (IPv4), VIP (IPv6), Node1 LAN1 (IPv6), and Node2 LAN1 (IPv6) ports.

The VIP address and the IP addresses for all the ports must be in the same subnet.

- **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:** 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. For information, see **Modifying Ethernet Port Settings** on page 181.

- **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.

4. Optionally, define extensible attributes. For information, see **Using Extensible Attributes** on page 168.

5. Save the configuration.

The communication protocol for all the services in a dual mode (IPv4 and IPv6) Master Grid member is set to IPv4, by default. But for a dual mode (IPv4 and IPv6) HA member, the communication protocol is the same as the one that is used for VRRP advertisements. For example, if you select IPv4 in the **Send HA and Grid Communications 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 member. For information see, **Changing the Communication Protocol for a Dual Mode Member** on page 114.

### Changing the Communication Protocol for a Dual Mode Member

You can change the default communication protocol for a dual mode Master Grid member. You can force the Master Grid member to use a specific protocol to join the Master Grid 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 member:

1. From the **Master Grid** tab, select the **Members** tab -> member check box -> Edit icon.
2. In the **Master Grid Member 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 member 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:
Adding Master Grid Members

— **Always use this Communications Protocol for:** For a Master Grid, you can select either IPv4 or IPv6 from the Reporting drop-down list. This setting will force the Master Grid to use the specified communication protocol for reporting service. For a member, you can select either IPv4 or IPv6 from the Grid and Reporting drop-down list. This setting will force the 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 a Master Grid

Grid members can join the Master Grid using IPv4 protocol in an IPv4-only Grid and in a dual mode Grid, the Grid members may join the Master Grid using IPv4 or IPv6. 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.

To join a single appliance or an HA pair to a Master Grid:

1. Log in to the appliance or HA pair that you want to add to the Master Grid. The appliance or HA pair must be online and able to reach the Multi-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 Join Grid dialog box, enter the following:
   - **Virtual IP of Grid Master**: Type the VIP address of the HA Multi-Grid Master or the LAN address of the single Multi-Grid Master.
   - **Grid Name**: Type the name of the Master Grid.
   - **Grid Shared Secret**: Type the shared secret of the Master Grid.
   - **Use MGMT port to join Grid**: If you have already enabled the MGMT port, 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 Master Grid, log in to the Multi-Grid Master and navigate to the Master Grid tab -> Members tab. This panel lists the Master Grid members. Check the icon in the Status column of the newly added member. (green = the appliance has joined the Master Grid and is functioning properly; yellow = the appliance is in the process of joining the Master Grid; red = the appliance has not joined the Master Grid). You can also use the CLI command `set membership` to join an appliance to a Master Grid.
Managing a Master Grid

After you configure a Multi-Grid Master and add members, you might need to perform the following tasks:

- **Changing the Master Grid Properties**
- **Removing a Master Grid Member** on page 117
- **Promoting a Master Candidate** on page 118

### Changing the Master Grid Properties

You can change some properties, such as the Master Grid name, its shared secret, and the port number of the VPN tunnels that the Master 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 Master Grid:

1. From the Master Grid tab, expand the Toolbar and select Master Grid Properties -> Edit.
2. In the Master Grid Properties editor, select the General tab, and then modify any of the following:
   - **Master Grid Name**: Type the name of the Master Grid. The default name is Infoblox.
   - **Shared Secret**: Type a shared secret that all Master Grid members use to authenticate themselves when joining the Master 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. For afternoon and evening hours, use the integers 13-24.
   - **Master Grid Communications Port**: Type the port number that the members use when communicating with the Multi-Grid Master through encrypted VPN tunnels. The default port number is 1194.
   - **Enable Recycle Bin**: This option is enabled by default and cannot be disabled.
   - **Audit Logging**: Select one of the following:
     - **Detailed**: This is automatically selected and cannot be modified. 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.
     - **Enable GUI Redirect from Member** check box to allow the appliance to redirect the Infoblox GUI from a Grid member to the Grid Master.
3. Save the configuration.

If you changed the VPN port number, time zone, date or time, Multi-Grid Manager displays a warning indicating that a product restart is required. Click Yes to continue, and then log back in to Multi-Grid Manager after the application restarts.

You can set additional operational properties for the Master Grid. For more information, see Chapter 8, Managing Master Grid Operations, on page 153.
Configuring Security Level Banner

Only superusers are able to configure and enable this 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 Multi-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. Multi-Grid Manager automatically uses an appropriate contrasting text font color that goes with the banner color.

To configure the advanced security level banner for the Multi-Grid Manager:

1. From the **Master Grid** tab, select the Master Grid.
2. Expand the Toolbar and select **Master Grid Properties -> Edit**.
3. In the **Master Grid Properties Editor panel**, 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 list. If necessary using the drop-down list, select the required color for the security level banner.
   - **Classification Message**: Enter the message you want to display in the security banner. You can enter up to 250 characters.
5. Save the configuration.

Security banner appears on the header and footer of all pages of Multi-Grid Manager including the Login screen.

Configuring Informational Banner

Only superusers are able to configure and enable this 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 Multi-Grid Manager screen. You can publish the banner information you want and set the banner color. Multi-Grid Manager automatically uses an appropriate contrasting text font color that goes with the banner color.

To configure the advanced informational banner for a Multi-Grid Manager:

1. From the **Master Grid** tab, select the Master Grid.
2. Expand the Toolbar and select **Master Grid Properties -> Edit**.
3. In the **Master Grid Properties Editor panel**, 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 list. If necessary using the drop-down list, select the required color for the informational banner.
   - **Message**: Enter the message you want to display in the informational banner. You can enter up to 250 characters.
5. Save the configuration.

Informational banner appears on the header of the Multi-Grid Manager.

Removing a Master Grid Member

You might want or need to remove a member from the Master Grid, perhaps to disable it or to add it to a Grid.

To remove a member, from the **Master Grid** tab, select the **Members** tab -> **master_grid_member** check box, and click the Delete icon.
Promoting a Master Candidate

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.
```

Note that if the current Multi-Grid Master synchronizes with a Grid during the master candidate promotion, the newly promoted Multi-Grid Master will not have the data that was synchronized during the master promotion. To avoid this, you can disable the Grids before promoting the master candidate and then enable them again after the promotion.

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.
2. At the prompt, enter the command:
   ```
   set promote_master
   ```
   The appliance restarts. The GUI is unavailable until the master promotion is complete.
3. Log in to the Multi-Grid Manager GUI on the new Multi-Grid Master.
4. From the Master Grid tab, select the Members tab.
5. Look at the IP address of the master in the IP Address column to ensure it is the master candidate that you promoted.
6. To verify the new master is operating properly, check the icons in the Status column. Also, select the Multi-Grid Master, and then click the Detailed Status icon in the table toolbar.
   You can also check the status icons of the master candidates to verify that they are all connected to the new master.

**Note:** There can be a mismatch in the Grid status when you promote a master candidate during the attach operation. Use CLI command, `set mgm attached` to force the Grid to attach and synchronize the Grid status.
Chapter 6  Managing Grids

You can manage multiple Grids from the Master Grid. This chapter explains how to add Grids to a Master Grid, and how to monitor and manage them. This chapter includes the following sections:

• Managing Grids on page 121
  — Synchronizing Grids on page 122
  — Restricting Synchronization on Managed Grids on page 122
• Adding a Grid on page 123
  — Configuring the Grid on the Multi-Grid Master on page 123
  — Generating the Join Key and File on page 123
  — Joining a Grid to the Master Grid on page 124
• Managing Disconnected Grids on page 125
  — Attaching a Grid Immediately on page 125
  — Schedule Attaching a Grid on page 126
  — Detaching a Grid Immediately on page 126
  — Schedule Detaching a Grid on page 127
• Monitoring Grids on page 128
  — Visualization Tab on page 128
  — Viewing the Node Tree on page 130
  — Listing Grids on page 132
  — Removing a Grid on page 132
• Setting Grid Properties on page 133
• Upgrading Grids on page 134
  — Uploading and Viewing Software Versions on page 134
  — Upgrading Software on page 135
  — Pushing Software on page 135
  — Distributing Software Upgrade Files on page 136
  — Testing Software Upgrades on page 136
  — Performing Software Upgrades on page 136
• Managing Grid Templates on page 137
  — Adding Grid Templates on page 137
  — Applying Templates on page 138
  — Deleting Templates on page 138
• About Snapshots on page 139
— Managing Snapshot Information on page 139
— Adding Snapshot to a Grid on page 140
— Saving Snapshot as a Template on page 140
— Cloning Snapshots on page 140
— Delta Viewer on page 141
— Applying Snapshots on page 141
— Deleting Snapshots on page 142
— Disabling Snapshots Synchronization on page 140
Managing Grids

The Master Grid provides centralized management of multiple Grids. After you create a Master Grid, you can then add the Grids that you want to manage. After a Grid joins a Master Grid, the Multi-Grid Master automatically starts synchronizing status and IPAM data with the Grid Master in real time. You can then monitor the status of your Grids and configure network data from the Master Grid. As shown in the example in Figure 6.1, an admin logs in to Multi-Grid Manager to manage four independent Grids and its global network.

Figure 6.1 Multi-Grid Management

The Master Grid can manage Grids running NIOS versions that are different from the Master Grid. The oldest version must be no more than three versions earlier than the NIOS version running on the Master Grid. The Master Grid must run the most recent NIOS version among its managed Grids.

Note that when you add a Grid to a Master Grid, you can manage a Grid in strict delegation mode to restrict the IP address space of the managed Grid. When you manage a Grid in this mode, the Grid admin cannot perform any network operation that results in the creation of additional network space. This includes creating a network or network container that is not entirely included in an existing network or network container in the network view and resizing any top level network container. Besides this, adding a Grid to a Master Grid does not restrict the operations of a Grid. An admin can still access and configure the Grid from its Grid Master.

The Master Grid provides a Single Sign On feature that allows you to automatically sign in to selected Grids from the Master Grid, without having to log in to each one. To use this feature, you must first validate your credentials for each of the Grids you need to access in your User Profile. For more information, see Setting Your User Profile on page 27.
Synchronizing Grids

When a Grid joins a Master Grid, the Multi-Grid Master establishes a VPN connection with the Grid Master and starts synchronizing data from the Grid Master. The Multi-Grid Master synchronizes monitoring and upgrade status data, including the status of the Grid members and the services that they are running. It also synchronizes IPAM data from the Grid, including the network views, network containers, networks, and extensible attribute definitions. If the Grid manages Microsoft DHCP servers, the synchronized DHCP data from the Microsoft servers is synchronized to the Master Grid as well. When you back up a Master Grid, the backup contains all data synchronized from the managed Grids.

After the initial synchronization, the Multi-Grid Master synchronizes only the data that has been modified since the last successful synchronization. You can view the synchronization status of a Grid by navigating to the Grids tab. For more information, see Monitoring Grids on page 128.

Synchronization occurs only between the Multi-Grid Master and the Grid Master. If there is a master promotion in a managed Grid, the new Grid Master notifies the Multi-Grid Master that it is the new Grid Master. All data communication between the Multi-Grid Master and a Grid Master is encrypted and goes through a VPN tunnel. The Multi-Grid Master can perform multiple synchronizations concurrently with all the Grid Masters of its managed Grids. The Multi-Grid Master synchronizes regularly with a Grid Master to ensure the Master Grid has the most current data.

In addition, some operations on the Grid can trigger a synchronization, such as the addition or update of a member in the Grid, the addition of update of a network view, network container or network, and the update of extensible attributes. Note that the network connection may cause some delays in the synchronization and this may cause some inconsistencies. For example, Grid Manager could display a message indicating that a network already exists when you try to add a network.

Restricting Synchronization on Managed Grids

You can restrict synchronization of selected network views, network containers, networks, and extensible attributes by using the Disable Sync to MGM option on the Grid Masters of the managed Grids. You use this option to restrict certain networks and networking information by not sharing it with the Multi-Grid Master. In addition, you can prevent the Multi-Grid Master from having access to the snapshots of the managed Grids. When you disable synchronization, all synchronized data is deleted and future synchronization is disabled.

Note: The Disable Sync to MGM check box is available only on the managed Grid when it remains joined with the Multi-Grid Master.

When you disable synchronization on a parent object, the synchronization is restricted on all its child objects. You cannot override this setting (you cannot enable synchronization) on the child object. However, you can disable synchronization at the child object if you have not restricted (disable) synchronization at the parent level. For example, if you disable synchronization at the network view level, then the synchronization is disabled for all the network containers and networks that are added to this network view. You cannot override this settings and enable synchronization at the network level.

You can restrict synchronization on the following:

- Network views, IPv4 or IPv6 network containers and networks, as described in Restricting Synchronization on page 151.
- Extensible attributes, as described in Viewing Extensible Attributes on page 166.
- Snapshots, as described in Disabling Snapshots Synchronization on page 140.
Adding a Grid

When you add a Grid to a Master Grid, you can set it to strict delegation mode. In this mode, the Master Grid allocates and address block to the Grid, and the Grid admins are then allowed to create networks only within and below the assigned address block. This restriction applies so long as the Grid is managed by the Master Grid.

In addition, you can set the name of the Grid from the Master Grid; and if this name is different from the current name of the Grid, Multi-Grid Manager gives you the option to select either name or specify a new one.

The basic steps necessary to add a Grid to a Master Grid are as follows:

1. From the Multi-Grid Master:
   - Configure the Grid on the Multi-Grid Master, as described in the next section, Configuring the Grid on the Multi-Grid Master.
   - Generate the Join Key and Join File, and download the file. For more information, see Generating the Join Key and File.
2. From the Grid Master, start the join operation. For more information, see Joining a Grid to the Master Grid.

Configuring the Grid on the Multi-Grid Master

To preprovision a Grid on the Master Grid:

1. Log in to the Multi-Grid Master.
2. From the Grids tab, expand the Toolbar and click Add -> Add Grid Wizard.
3. In the Add Grid wizard, complete the following:
   - Name: Enter a name for the Grid that you are adding.
   - Comment: Optionally, enter additional information about the Grid.
   - Strict Delegation Mode: Select this option to restrict the address space within which the Grid admins can create networks.
   - Disable: Select this to disable the Grid. This allows you to preprovision the Grid and then enable it at a later time.
4. Optionally, define extensible attributes. For information, see About Extensible Attributes on page 164.
5. Save the configuration.

Generating the Join Key and File

The Join file is a binary file that contains encrypted information that the Master Grid requires before it allows a Grid to join it. The Master Grid uses the Join Key to decrypt the Join file.

To generate the join key and file:

1. Log in to the Multi-Grid Master.
2. From the Grids tab, expand the Toolbar and click Add -> Add Grid Wizard.
3. Click Download to download the Join Key file from the Multi-Grid Master. You must later upload it to the Grid Master of the Grid that is joining the Master Grid.
4. Additionally, copy the Join Key because you will need to type or paste it when you upload the Join Key file to the Grid Master.
5. Click OK to close the Join Key dialog.

Note that a Join file is valid up to four hours after it is generated.
Joining a Grid to the Master Grid

To join the Grid to the Master Grid:

1. Log in to the Grid Master of the Grid.
2. Navigate to the Grid -> Grid Manager tab.
3. Expand the Toolbar and click Master Grid -> Join.
4. In the Add Master Grid wizard, complete the following:
   - Multi-Grid Master Hostname/IP Address: Type the VIP address of the HA Multi-Grid Master or the LAN address of the single Multi-Grid Master. You can also enter the hostname of the Multi-Grid Master.
   - Multi-Grid Master Port Number: The Multi-Grid Master synchronizes data with the Grid Master through encrypted VPN tunnels. You can change the default source and destination UDP port number for VPN tunnels, which is 1194.
   - Join Key File: Click Select to upload the join file generated by the Master Grid.
   - Join Key: You can type or paste the key generated by the Multi-Grid Master.
   - Disable: Select this to disable the configuration at this time.
5. Save the configuration to begin the join operation.

If the Grid name you entered in the Master Grid is different from the actual Grid name, Multi-Grid Manager displays a confirmation dialog requesting that you select either of the names or enter a new one.

You can then log into Multi-Grid Manager to verify that the Grid has successfully joined the Master Grid. To view the Join status of the Grid, navigate to the Grids -> List tab. For more information, see Listing Grids on page 132.

From Multi-Grid Manager, you can do the following:

- View the Grids in different views. For more information, see Monitoring Grids on page 128.
- Set some Grid properties. For more information, see Setting Grid Properties on page 133.
- Upgrade the Grids. For more information, see Upgrading Grids on page 134.
- View and manage the network space of the Grids. For more information, see Chapter 7, Network Management, on page 143.

Leaving the Master Grid

You can perform the Leave operation after you join a Grid.

To leave the Master Grid:

1. Log in to the Grid Master of the Grid.
2. Navigate to the Grid -> Grid Manager tab.
3. Expand the Toolbar and click Master Grid -> Leave.
   Grid is completely disassociated from the Master Grid.
Managing Disconnected Grids

You can now manage a large number of Grids using the attach and detach operations. Grid(s) that are detached from the Multi-Grid Master remain operational. You can attach and detach at any point of time. Grid does not contact Master Grid when it is disconnected. In this state, there will be no communication between the Grid and the Master Grid, but it remains joined with the Master Grid. You can again attach the Grid to the Multi-Grid Master to re-establish communication. Establishing connection between a Grid and a Master Grid is termed as attach and disconnecting their connection is termed as detach.

You need to have appropriate permissions to perform the attach and detach operations. For more information on permissions, [Administrative Permissions for Disconnected Grids](#) on page 103. You must first validate your credentials against a Grid in your User Profile to gain appropriate access permissions. For more information, see [Setting Your User Profile](#) on page 27. Validating your credentials against a Grid allows you to perform the attach and detach operations in the Multi-Grid Manager.

You can save a copy of the Grid data during the attach and detach operation as a snapshot. These snapshots are stored on an external storage server. For more information, see [Managing External Storage Server](#) on page 170. You can also save a snapshot as a template and apply to a Grid to reset its configuration. You can manage snapshot information using Snapshot Manager. For more information, see [About Snapshots](#) on page 139.

The maximum number of Grids that a Master Grid can support for attach and detach operation is based on the NIOS appliance model. An error message is displayed to indicate that you are not allowed to continue attach operation further. The Master Grid logs an entry with the Grid name, date, and time if you try to attach beyond the maximum limit.

**Table 6.1 NIOS appliances and the number of Grids it supports**

<table>
<thead>
<tr>
<th>Appliance Model</th>
<th>Total Capacity</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>IB-4010</td>
<td>500</td>
<td>Manage concurrently 250 attached Grids and 250 detached Grids. You can attach a maximum of 250 Grids at a time. Examples of attach/detach combinations include: 100 attached + 400 detached OR you can perform 100 attached + 100 detached (in this case 300 available Grids)</td>
</tr>
<tr>
<td>IB-1420</td>
<td>50</td>
<td>Manage concurrently 25 attached Grids and 25 detached Grids. You can attach a maximum of 25 Grids at a time. Examples of attach/detach combinations include: 10 attached + 20 detached (in this case 20 available Grids)</td>
</tr>
<tr>
<td>IB-1550 A/</td>
<td>50</td>
<td>Manage concurrently 25 attached Grids and 25 detached Grids. You can attach a maximum of 25 Grids at a time. Examples of attach/detach combinations include: 10 attached + 20 detached (in this case 20 available Grids)</td>
</tr>
<tr>
<td>IB-1552 A/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IB-VM-1550</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Attaching a Grid Immediately**

Before attaching a Grid, make sure that the Grid is joined with the Master Grid and it is working. For more information, see [Joining a Grid to the Master Grid](#) on page 124.

Do the following to attach a Grid to a Master Grid:

1. Log in to the Master Grid.
2. From the Grid tab, select the List tab.
3. In the toolbar, move the pointer on the Attach drop down list and then click Immediate.
4. In the Immediate Attach Confirmation message box, click OK to begin the attach operation.

   The Connection Status displays Attaching when the attach operation is in progress. This status continues till the attach operation fails or succeeds. The Connection Status column in the Grid panel updates to Attached to confirm that the appliance has successfully attached to the Master Grid.
Tip: Alternatively, you can use the Action icon to perform Attach.

**Schedule Attaching a Grid**

You can schedule the attach operation for a future date and time.

1. Log in to the Master Grid.
2. From the Grid tab, select the List tab.
3. In the toolbar, move the pointer on the Attach drop down list and then click Schedule.
4. In the Schedule Grid Attach panel, complete the following:
   - **Attach Now**: Select this to have the appliance perform the task when you save the entry.
   - **Attach Later**: Select this to schedule the task for a later date and time. This is selected by default when there is no scheduled task associated with the object. Complete the following:
     - **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. 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 Multi-Grid Manager.
     - **Duration**: Enter the duration and specify the unit of duration. Select either Days or Hours from the drop-down list to specify the duration format. The connection status will be Attaching through this duration. The actual connection status will be displayed only after this duration. This is useful when connectivity to the Grid may not be available immediately. However, it will be available at some period of time during the duration period.
5. Click Schedule Attach.

Tip: Alternatively, you can use the Action icon to perform Schedule Attach.

**Detaching a Grid Immediately**

You can detach an attached Grid. Ensure that the Grid is online and attached. Do the following to detach a Grid from a Master Grid:

1. Log in to the Master Grid.
2. From the Grid tab, select the List tab.
3. In the toolbar, move the pointer on the Detach drop down list and then click Immediate.
4. In the Immediate Detach Confirmation message box, click OK to begin the detach operation.

The Connection Status will display Detaching when the detach operation is in progress. The Connection Status column in the Grid panel will be updated to Detached to confirm that the appliance has successfully Detached from the Master Grid.

**Note:** If you perform the Leave operation in the Grid Manager while it is detached from the Multi-Grid Manager, the Connection Status in the Multi-Grid Manager will be Detached. To attach this Grid again, you first join the Grid to the Multi-Grid Master and then perform the attach operation. For more information, see Leaving the Master Grid on page 124.
Schedule Detaching a Grid

You can schedule the detach operation for a future date and time.

1. Log in to the Master Grid.
2. From the Grid tab, select the List tab.
3. In the toolbar, move the pointer on the Detach drop down list and then click Schedule.
4. In the Schedule Grid Detach panel, complete the following:
   - **Detach Now**: Select this to have the appliance perform the task when you save the entry.
   - **Detach Later**: Select this to schedule the task for a later date and time. This is selected by default when there is no scheduled task associated with the object. Complete the following:
     - **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. 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 Multi-Grid Manager.
     - **Duration**: Enter the duration and specify the unit of duration. Select either Days or Hours from the drop-down list to specify the duration format. The connection status will be Detaching through this duration. The actual connection status will be displayed only after this duration. This is useful when connectivity to the Grid may not be available immediately. However, it will be available at some period of time during the duration period.
5. Click Schedule Detach.

**Tip**: Alternatively, you can use the Action icon to perform Detach and Schedule Detach.

Connection Status

The Connection Status column indicates the operational status of the Grid and a general description of its current operation. The status icon can be one of the following:

<table>
<thead>
<tr>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>The appliance is either Attached or Detached.</td>
</tr>
<tr>
<td>Blue</td>
<td>The appliance is connecting or detaching with its Multi-Grid Master.</td>
</tr>
<tr>
<td>Red</td>
<td>Failed operation. The appliance is offline, is not licensed, is upgrading or downgrading, or is shutting down or failed to capture snapshot.</td>
</tr>
</tbody>
</table>
Monitoring Grids

Multi-Grid Manager provides different ways to view and monitor your Grids. You can view the overall status of your managed Grids or view individual Grid status through the widgets on your Dashboard. You can also navigate to the Grids tab -> Visualization tab, which provides graphical views of the Grids, and the List tab, which lists the managed Grids.

Visualization Tab

When you navigate to Grids -> Visualization, Multi-Grid Manager displays each Grid, including the Master Grid, as a rectangular tile. The first tile represents the Master Grid, and the remaining tiles represent each Grid, arranged in alphanumeric order. Each tile provides pertinent data points at-a-glance and provides options for editing Grid properties, viewing the node tree, and logging in to an individual Grid. Figure 6.2 shows the typical layout of the Visualization tab.

Figure 6.2 Visualization Tab
The Master Grid tile provides the following information:

- Master Grid name
- Type of Multi-Grid Master (standalone or HA)
- The number of Grids managed by the Master Grid
- The Status icon represents the status of the most critical members in the Master Grid. When all members are running properly, the overall Master Grid status is green. When one of the members has operational problems, the overall Master Grid status is red.
- The External Storage icon represents the connection availability of the external storage server. When the connection is available, the External Storage icon is in green. When it is disabled or not connected, the status icon is in gray. When there is any operational issues, the External Storage icon is in red.

Each Grid tile provides the following information:

- Grid name
- Type of Grid Master (standalone or HA)
- Number of members, networks and network containers managed by the Grid
- The status of each protocol running on the Grid
- The Status icon represents the status of the most critical members in the Grid. When all the members are running properly, the overall Grid status is green. When one of the member has operational problems, the overall Grid status is red. When the Grid has not joined the Master Grid, the status icon is grey.
- The Sync Status icon indicates the synchronization status between the Grid and Master Grid. It can be one of the following:
  - Green: The Grid is connected to the Master Grid and the synchronization process is running properly.
  - Yellow: The Grid is connected to the Master Grid, but it has been 300 seconds since the last synchronization.
  - Red: The Grid is connected to the Master Grid, but 600 seconds have passed since the last synchronization, the connection failed, or the join operation failed between the Master Grid and Grid. You can view the syslog to obtain details.
  - Black: The Grid has not synchronized with the Master Grid.
- The connection status of the Grid with the Master Grid. This can be Attached or Detached.
- Last Sync Time: The date and time the Grid last synchronized with the Master Grid.

In addition, you can do the following from each tile:

- Click the Single Sign On icon to sign in to the Grid. Note that you can automatically sign in to the Grid, only if you have validated your admin account for that Grid. For information about validating your account, see Setting Your User Profile on page 27.
- Click the Edit icon to set Grid properties. For more information, see Setting Grid Properties on page 133
- Click the Node Tree icon to display the Node Tree for that particular Grid. For more information, see Viewing the Node Tree on page 130.

Above the tiles, you can do the following:

- Click Turn Auto Refresh On to periodically refresh the node tree. This feature is turned off by default. You can click the Refresh icon to update the contents of the node tree.
- Click the Visualization icon to open a new browser window for the Visualization tab. This allows you to keep a separate browser window open so you can always check the status of your Grids as you perform other tasks. You can click the Refresh icon to refresh the status of the Grids or turn on Auto Refresh.
**Viewing the Node Tree**

When you click the Node Tree icon of the Master Grid or a managed Grid, Multi-Grid Manager displays a node tree. In the Master Grid tree, the Multi-Grid Master is the root node at the center and it is connected to the Grid Masters of its managed Grids. Each Grid, in turn, is a subtree with its Grid Master at the center, connected to its members. You can then click a Grid Master to re-center the tree on that node.

The left panel displays the tile of the Grid Master that is at the center of the node tree. For information about the tile, see *Visualization Tab* on page 128. You can click Back to display the Grid tiles. *Figure 6.3* displays the typical layout of the node tree, with the Multi-Grid Master at the center of the tree.

*Figure 6.3 Node Tree*

In the node tree, the shape of the icons indicate the role of the member in the Master Grid or Grid:

- **Square:** Grid Master
- **Ellipse:** Grid Members
- **Circles:** Master 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 Multi-Grid Master with online Grid Masters, and Grid Masters with online Grid members.
- **Thick White Line:** Connects Grid Masters with Grid Master Candidates.
- **Dashed Line Connector:** Connects Grid Masters with offline Grid members or Grid Master candidates.

Above the node tree, you can do the following:

- Click **Turn Auto Refresh On** to periodically refresh the node tree. This feature is turned off by default. You can click the **Refresh** icon to update the contents of the node tree.
- Click the **Visualization** icon to open a new browser window for the Visualization tab. This allows you to keep a separate browser window open so you can always check the status of your Grids as you perform other tasks. You can click the **Refresh** icon to refresh the status of the Grids or turn on Auto Refresh.

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 following information for each type of node.

For the Multi-Grid Master:

- The name of the Multi-Grid Master.
- Indicates if the Multi-Grid Master is a standalone or an HA pair. If it’s an HA pair, indicates the status.
- The number of Grids managed by the Master Grid.

For the Multi-Grid Master Candidate:

- The name of the Multi-Grid Master.
- Indicates if the Multi-Grid Master is a standalone or an HA pair. If it’s an HA pair, indicates the status.
- The number of Grids managed by the Master Grid.

For the Grid Master of each Grid:

- **Grid Name**
- **Numbers of Members in Grid**
- **Status of each protocol running on the Grid**
- **Grid Status**
- **Synchronization status between the Grid and Master Grid, which can be:**
  - **Green:** The Grid is connected to the Master Grid and the synchronization process is running properly.
  - **Yellow:** The Grid is connected to the Master Grid, but it has been 300 seconds since the last synchronization.
  - **Red:** The Grid is connected to the Master Grid, but 600 seconds have passed since the last synchronization, the connection failed, or the join operation failed between the Master Grid and Grid. You can view the syslog to obtain details.
  - **Black:** The Grid has not synchronized with the Master Grid.
- Displays the connection status between the Grid and Master Grid. This can be **Attaching**, **Detaching**, **Attached**, **Detached**, **Attach Failed**, and **Detach Failed**.
- **The upgrade status of the Grid.**
- **The number of networks and network containers in the Grid**
- **The last date and time the Grid synchronized with the Master Grid**

For a Member:

- **Member name**
- **Standalone or HA**
- **HA Status if HA pair**
- **Status of each protocol running on that member**
Listing Grids

Navigate to Grids -> List tab to view a list of the Grids managed by the Master Grid. This panel displays the following information about each Grid:

- **Grid Name**: The name of the Grid.
- **Grid Master Name**: The hostname of the Grid Master.
- **Grid Master Address**: The VIP or LAN IP address of the Grid Master.
- **Status**: The status of the Grid.
- **Connection Status**: The connection status of the Grid with the Master Grid. This can be Attaching, Attached, Attach Failed, Detaching, Detached, Detach Failed, and Snapshot Failed. For more information, see Connection Status on page 127.
- **Service Status**: Overall status of the services on the Grid.
- **Last Sync Date/Time**: The last date and time the Grid synchronized with the Master Grid.
- **Members**: The number of members in the Grid.
- **Networks**: The number of networks managed by the Grid.
- **Network Containers**: The number of network containers in the Grid.
- **Comment**: Comments that were entered for the Grid.
- **Site**: Values that were entered for this pre-defined extensible attribute.
- **Disabled**: Indicates if the Grid is disabled.

**Note:** When you upgrade, the Grid data (number of members, networks and containers) displays 0 for the first time until the data is synchronized. Grid data displays the actual values after the database synchronization.

You can click the Add icon to add a Grid to the Master Grid, and you can also select a Grid and do the following:

- Click the Single Sign On icon to sign in to the Grid. Note that you can automatically sign into the Grid, only if you have validated your admin account for that Grid. For information about validating your account, see Setting Your User Profile on page 27.
- Click the Grid check box to view its audit log or syslog.
- Click the Edit icon to set Grid properties. For more information, see Setting Grid Properties on page 133.
- Click the Delete icon to remove it from the Master Grid.
- Click the Join icon to generate the Join key and file.
- Click the Attach icon to attach a Grid. For more information, see Attaching a Grid Immediately on page 125.
- Click the Detach icon to detach a Grid. For more information, see Detaching a Grid Immediately on page 126.
- Click the Snapshot Manager icon to launch the Snapshot Manager wizard. For more information, see Managing Snapshot Information on page 139.
- Click the Export icon to export the list in .csv format.
- Click the Print icon to print the list.

Removing a Grid

Removing a Grid from a Master Grid has no effect on the Grid’s data. It just disables the ability to view and manage the Grid from the Master Grid. In addition, if the Grid was managed in strict delegation mode, this restriction is removed as well.

To remove a Grid from the Master Grid:
1. From the Grids -> List tab, select the Grid check box and click the Delete icon.
2. Click Yes, when the confirmation dialog appears.
Setting Grid Properties

After you add a Grid, you can generate its Join Key file as described in Adding a Grid on page 123. You can also set its delegation mode to restrict the address space of the managed Grids. When you enable strict delegation mode, the Grid admins can create networks only within and below the network block of the Master Grid.

1. From the Grids -> Visualization tab -> Node Tree, select the Grid Master. When it moves to the center of the node, expand the Toolbar and click the Edit icon.
   
   From Grids -> List tab, select the Grid and click the Edit icon.

2. In the General Basic tab of the Grid editor, you can do the following:
   
   - **Name**: You can change the Grid name.
   
   - **Join Key and Expiration**: If the Grid has not joined the Master Grid and a Join key was generated, this field displays the Join key and its expiration date and time. Otherwise, it displays a message indicating that the Grid has joined the Master Grid.
   
   - **Join Key File**: If the Grid has not joined the Master Grid, you can click Generate to generate the Join Key, and then click Download to download the key.
   
   - **Comment**: Optionally, enter additional information about the Grid.
   
   - **Strict Delegation Mode**: Select this option to restrict the address space within which the Grid admins can create networks. If the Master Grid admin allocates an address block to the Grid, then the admins of the Grid can create networks within and below the address block.
   
   - **Grid Master IP Address/ FQDN**: Displays the IP address of the Grid when it is joined to a Master Grid. You can change it to FQDN.
   
   - **Attach Port**: Displays the attach port number when a Grid is joined to a Master Grid. The default value of attach port is 21195.
   
   You need to manually update the Grid Master IP Address/ FQDN field in the Multi-Grid Manager in the following scenarios:
   
   - Modify Grid Master IP when Grid is detached
   - Promote a Grid master candidate when Grid is detached
   - When Grid is behind a NAT device

   **Note**: 21195 is the default port number of a Grid and cannot be changed on the Grid. Only superusers can change this port number on the Multi-Grid Manager when there is an address and/or port translation between Multi-Grid Master and the Grid.

   - **Disable**: Select this to disable synchronization between the Grid and Master Grid. Setting the Disable option has no effect on the Grid data or its services. Setting this option terminates any ongoing synchronization and the Multi-Grid Master closes the VPN connection to the Grid Master.

3. In the Snapshot tab, you can configure the information to be captured in a snapshot. You can modify these settings at any point of time. Do the following to configure the information to be captured in a snapshot:

   - **Snapshot on Attach**: Select the Disabled check box to disable capturing the snapshot when a Grid is attached to the Master Grid. Clear the check box to capture snapshot.
   
   - **Snapshot on Detach**: Select the Disabled check box to disable capturing the snapshot when a Grid is detached from the Master Grid. Clear the check box to capture snapshot.
   
   In the Include in Snapshot section, select the check box to include the following information in the attached snapshots:
   
   - **Lease History**: Select this check box to include lease history details of a Grid.
   
   - **Syslogs**: Select this check box to include system log files.
   
   - **Distributed Files**: Select this check box to include file distribution details of a Grid.
   
   - **bloxTools partition**: Select this check box to include bloxTools partition information.
4. In the **Extensible Attributes** tab, you can add and delete extensible attributes that are associated with a Grid. You can also modify the values of extensible attributes. For information, see *About Extensible Attributes* on page 164.

5. The **Permissions** tab appears only if you belong to a superuser admin group. For information, see *About Administrative Permissions* on page 72.

6. Save the configuration.

### Upgrading Grids

From Multi-Grid Manager, you can upgrade the Master Grid and manage the upgrade process of the managed Grids. You can also drill down to an individual Grid and manage its upgrade details.

Note that upgrading the Master Grid has no effect on the Grids. If the Master Grid upgrades and this results in any managed Grid becoming unmanageable due to a mismatched version, the upgrade and test upgrades will fail.

### Uploading and Viewing Software Versions

A Master Grid can store up to 10 NIOS versions in its repository and push any of them to a Grid. In addition, before you upgrade, downgrade, or revert a Grid to a different software version, you can view its current software version, the image you have uploaded, and the available version to which you can revert.

#### Uploading NIOS Software

To upload a NIOS version to the repository:

1. From the **Grids -> Upgrades/Repository -> Repository** tab, click the Add icon.
2. In the **Upload** dialog box, click **Select** to navigate to the NIOS binary file, and then click **Upload**. Multi-Grid Manager uploads the file and adds it to the list of files in the **Repository** tab.

#### Viewing the Repository

To view information about each NIOS version that was uploaded to the Master Grid:

1. From the **Grid** tab, select **Upgrades/Repository -> Repository** tab.
2. Multi-Grid Manager displays the following information:
   - **File Name**: The file name of the NIOS binary file that was uploaded.
   - **Size**: The NIOS file size. You can compare this with the value displayed on the Infoblox support web site.
   - **Checksum**: The MD5 checksum of the file. You can compare this with the value displayed on the Infoblox support web site.
   - **Date Modified**: The date the file was last uploaded.

You can also do the following:

- Click the Add icon to upload a NIOS binary file.
- Select a NIOS file and click the Delete icon to remove the file from the system.
- Print and export the data in this tab.
Viewing Upgrade Information

To view software information:
1. From the Grid tab, select Upgrades/Repository -> Upgrades tab.
2. Multi-Grid Manager displays the following Information:
   - Upgrade Status: Displays one of the following:
     - Uploading: NIOS is being uploaded to the Grid Master or being pushed by Multi-Grid Manager.
     - Distributing: Displays the current status of distribution, if the Grid is in distribution mode.
     - Testing: If an upgrade test is in progress, or if the test succeeded or failed.
     - Upgrading: When selected, it displays the Upgrade tab of the appropriate Grid.
     - Scheduled: When selected, it displays the Upgrade Schedule dialog at the Grid level.
     - Paused: The upgrade was halted temporarily.
   - Grid Upgrade Management: Select this to automatically log in to Grid Manager and display the Upgrade tab of the Grid in a new browser window.
   - Running Version: The NIOS version that the Grid is currently running.
   - Upgrade Date: The date of the last upgrade to the displayed NIOS version.
   - Alternative Version: This is the alternative version of the Grid, if one exists.
   - Site: Displays the value of this predefined extensible attribute.

Upgrading Software

After you store the new upgrade files in the repository, complete the following tasks to upgrade a Grid.

- Upload the new software to the Grid Master, as described in Pushing Software.
- Distribute the software upgrade files, as described in Distributing Software Upgrade Files on page 136.
- Optionally, test the upgrade, as described in Testing Software Upgrades on page 136.
- Perform the software upgrade, as described in Performing Software Upgrades on page 136.

Before upgrading, Infoblox recommends that all Grid members are 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.

Pushing Software

To upload NIOS software from the Multi-Grid Master to the Grid Master:
1. From the Grids tab, select the Upgrades/Repository -> Upgrades tab.
2. Select the check box of the Grid you are upgrading and click Push Now to start the upload immediately or Schedule Push to schedule the upload for a later time.
3. When Multi-Grid Manager displays the NIOS versions that are in the repository, select the version to upload.

If you try to push a NIOS version that cannot be managed by the Master Grid, Multi-Grid Manager displays a warning message. If you try to push software to more than one Grid, Multi-Grid Manager displays a warning message that it may impact network performance.

The Grid Master 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.
**Distributing Software Upgrade Files**

Distributing the software upgrade files involves unpacking the software files and loading the new software. Note that starting the distribution disables the Grid 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.

**Distributing Software Immediately**

To distribute the software upgrade throughout the Grid immediately:

1. From the Grids tab, select the Upgrades/Repository -> Upgrades tab, and then click the Distribute icon-> Distribute Now from the Toolbar.
2. In the confirmation dialog box, click Yes to start the distribution. The appliance distributes the upgrade files and displays the status of the distribution in the Upgrade Status column.

**Scheduling Distributions**

To schedule the distribution, you must have validated your account with the Grid so you can automatically sign in to the Grid Master and schedule its upgrade.

To schedule a software distribution:

1. Select the grid check box, and then select the Distribution drop-down menu -> Schedule Distribution. Multi-Grid Manager automatically logs you in to the Grid Master.
2. In the Grid -> Upgrade tab, select Distribute -> Schedule Distribution in the Toolbar. Multi-Grid Manager automatically signs in to the Grid. Multi-Grid Manager automatically logs you in to Grid Manager, which displays the Grid -> Upgrade tab. For information about scheduling distributions for the Grid, refer to the dynamic Help page or the NIOS Administrator Guide.

**Testing Software Upgrades**

After you successfully distribute a software upgrade to a 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 version and the software upgrade. The test does not affect services and you can perform other administrative tasks during the upgrade test.

To start an upgrade test on a Grid:

- From the Grids tab, select the Upgrades/Repository -> Upgrades tab, and then click the Test Upgrade icon. After you start an upgrade test, you can view its status in the Upgrade Status column.

**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 and Restoring Configuration Files on page 219.

When upgrading to software releases that are Upgrade Lite compatible, you can schedule the Master Grid upgrade as described in Scheduling Upgrades on page 137.
Managing Grid Templates

Upgrading Immediately

You cannot schedule upgrades to releases that are not Upgrade Lite compatible. The Master Grid members must upgrade at the same time when upgrading to these releases. For Upgrade Lite compatible releases, you can schedule the upgrade as described in Scheduling Upgrades on page 137, or upgrade the Master Grid at the same time.

To upgrade a Master Grid immediately:

1. From the Grids tab, select the Upgrades/Repository -> Upgrades tab.
2. Select the Grid check box, and then select the Upgrade drop-down menu -> Upgrade Now.

The Grid upgrades immediately and if there is an active upgrade schedule, it becomes inactive.

Scheduling Upgrades

To schedule an upgrade, you must have validated your account with the Grid so you can automatically sign in to the Grid Master and schedule its upgrade. To schedule an upgrade:

1. From the Grids tab, select the Upgrades/Repository -> Upgrades tab.
2. Select the grid check box, and then select the Upgrade drop-down menu -> Schedule Upgrade.

Multi-Grid Manager automatically logs you in to Grid Manager, which displays the Grid -> Upgrade tab. For information about upgrading the Grid, refer to the dynamic Help page or the NIOS Administrator Guide.

Managing Grid Templates

Only superusers are able to create and apply Grid templates. A snapshot can be saved as a template for creating multiple Grids of the same DNS, DHCP and IPAM configuration. A template is a file containing the data of a Grid at a given point of time. A Grid template consists of the following:

- Grid database (mandatory information)
- Audit log information (mandatory information)
- Optionally, it can contain distributed files information and lease history

Note: The audit log and lease history information is not preserved when snapshot is converted to a template.

For more information on permissions, see Administrative Permissions for Disconnected Grids on page 103. You must first validate your credentials against a Grid in your User Profile to gain appropriate access permissions. For more information, see Setting Your User Profile on page 27.

Validating your credentials against a Grid allows you to perform the following tasks from the Multi-Grid Master:

- Add a Grid template, as described in Adding Grid Templates on page 137.
- Apply a template, as described in Applying Templates on page 138.
- Delete a template, as described in Deleting Templates on page 138.

Adding Grid Templates

1. From the Grids tab, select the Grid Templates tab.
2. Click Add.
3. Click Select to open the Grid Selector wizard and select a Grid.
4. In the Name text box, enter the template name.
5. Click Save.

The template will be available in the Grid Templates panel.
Applying Templates

You can apply a template to reset all the data of a Grid. When you apply a template, you have the option to use the passwords available in the template to login to the Grid or reset password when you login to the Grid. When you apply a template to a Grid, all the delegated tasks related to that Grid is deleted from the Task Viewer.

**WARNING:** Multi-Grid Master will not check the database capacity of a Grid. It is possible to apply a template that will cause the Grid to be over capacity.

To apply a template:
1. From the **Grids** tab, select the **Grid Templates** tab.
2. Click **Apply Template**.
3. From the Select Template drop down list, select a template you want to apply.
4. From the Maintain current password on reset drop down list, do the following:
   - select Yes to use the passwords available in the template.
   - select No to force the users existing in the template to reset their password at the first login on the reset Grid. Selecting this also enables the global password reset. Any new user created on the Grid should change their password at the first login.

Deleting Templates

To delete a Grid template:
1. From the **Grids** tab, select the **Grid Templates** tab.
2. Select the template you want to remove and click **Delete**.
3. In the Delete Confirmation (Grid Template) dialog box, click **Yes**.
   Grid template is removed from the Grid Templates panel.
About Snapshots

When a Grid is attached or detached, a snapshot of the Grid's current state is captured and stored on an external FTP server. You can use these snapshots to reset the Grid to a known state on failure. You can also save snapshot as a template and use it to create multiple Grids of the same DNS, DHCP and IPAM configuration. The snapshot is captured during the attach and detach operations and manually. All the snapshots are stored on an external storage FTP server and can be retrieved at any point of time. The external storage must be up and running to complete the snapshot process. A snapshot archive file is saved as a tar file in the external storage server. This file is not encrypted, however, sensitive information such as passwords are. The Multi-Grid Master follows a definite file format structure to store archive files. For more information, see File Formats in Archives on page 172 and Naming Format of a Snapshot File on page 172.

The **Failed Snapshot** status occurs when there is no:

- connection between the Master Grid and the external storage server
- space in the external storage server for the snapshot

**Note:** During the attach or detach operation if the snapshot fails, the attach or detach operation will also fail. The Multi-Grid Manager logs the event in the syslog.

Managing Snapshot Information

Snapshots are captured only if the external storage server is configured and enabled. If it is not configured or enabled, the **Snapshot Manager** wizard displays an error message when you try to perform any action in the wizard. For more information on external storage server, see Managing External Storage Server on page 170. Make sure you have appropriate permissions to perform the tasks listed below. For more information on permissions, Administrative Permissions for Disconnected Grids on page 103. You must first validate your credentials against a Grid in your User Profile to gain appropriate access permissions. For more information, see Setting Your User Profile on page 27.

Validating your credentials against a Grid allows you to perform the following tasks from the Multi-Grid Master:

- Manually add a snapshot, as described in Adding Snapshot to a Grid on page 140.
- Save a snapshot as a template, as described in Saving Snapshot as a Template on page 140.
- Create a duplicate copy of a snapshot, as described in Cloning Snapshots on page 140.
- View the difference between two snapshots, as described in Delta Viewer on page 141.
- Apply snapshot to a Grid to reset its configuration, as described in Applying Snapshots on page 141.
- Delete a snapshot, as described in Deleting Snapshots on page 142.

**Tip:** Alternatively, you can use the Action icon to perform the above tasks.

You can do the following in the Snapshot Manager wizard:

- Download: Download the snapshot list.
- Export: Export the data in .csv file.
- Print: Print the snapshot list.
Adding Snapshot to a Grid
You can manually add a snapshot and save snapshot as a template. Make sure that the external storage server is up and running. You cannot add or save a snapshot if a Grid is offline.

To manually add a snapshot:
1. Login to the Master Grid.
2. From the Grid tab, click the List tab.
3. Select a Grid and click the Snapshot Manager icon.
4. Click Add.
5. In the Name text box, enter the name of the snapshot.
6. Click the drop down list in the Save icon and click Save as Snapshot.
   The snapshot will be added manually to the list.

Saving Snapshot as a Template
The audit log and lease history information is not preserved when a snapshot is converted to a template.

1. Login to the Master Grid.
2. From the Grid tab, click the List tab.
3. Select a Grid and click the Snapshot Manager icon.
4. Click Add.
5. In the Name text box, enter the name of the template.
6. Click the list in the Save icon and click Save as Template to save as a template.
   The saved template will be available in the Grid Templates panel.

Cloning Snapshots
You can duplicate an existing snapshot and save it as a template. The snapshot will have a copy of the Grid data. The data in a snapshot is based on the settings in the Snapshot tab of the Grid Editor wizard. You can clone a snapshot only if the external storage server is up and running.

To clone a snapshot:
1. Log in to the Master Grid.
2. From the Grid tab, click the List tab.
3. Select a Grid and click the Snapshot Manager icon.
4. Click Clone.
5. In the Name text box, enter the name of the template.
6. Click Save as Template to save it as a template.
   The saved template will be available in the Grid Templates panel.

Disabling Snapshots Synchronization
You can disable synchronization of snapshots from the managed Grids to the Multi-Grid Master.

To disable synchronization of snapshots of the managed Grid:
1. Log in to the managed Grid. Make sure that the Grid remains joined with the Multi-Grid Master.
2. From the Grid tab, select the Grid Manager tab.
3. Expand the Toolbar and select Grid Properties → Edit.
4. In the Security tab, do the following:
— **Disable database snapshot sync to MGM:** Select this check box to disable the synchronization of snapshots from the managed Grid to the Multi-Grid Master. This option is available only when the managed Grid remains joined with the Multi-Grid Master.

5. Save the configuration.

**Delta Viewer**

Delta Viewer displays the difference between two snapshots taken at different periods of time. You can view difference if the external storage is up and running. In the Snapshot Manager wizard, you are able to select two different snapshots and launch the Delta Viewer wizard. The Delta Viewer wizard displays the difference between the selected snapshots. Make sure that you select two different snapshots. You can download the delta results in the .tar.gz format (zip file) to your local folder

**Note:** There is a small possibility that some of the audit records may not be replicated from the previous Active node to the new one during an HA failover. Therefore, you may not be able to view these records in the Delta Viewer.

To view the difference between two snapshots:

1. Login to the Master Grid.
2. From the Grid tab, click the List tab.
3. Select a Grid and click the Snapshot Manager icon.
4. Click Delta Viewer.
5. From the Base Snapshot drop down list, select a snapshot.
6. From the Delta Snapshot drop down list, select another snapshot. This snapshot cannot be older than the snapshot selected in the Base Snapshot.
7. Optionally, you can click Clear Selections to clear the data in the drop down list.
8. You can view the following information:
   — **Timestamp:** The date, time, and time zone the task was performed. The time zone is the time zone configured on the Master Grid.
   — **Admin:** The admin user who performed the task.
   — **Action:** The action performed. This can be CREATED, MODIFIED, DELETED, and CALLED. Note: CALLED function will filter name that contains GET, CHECK, TEST, and FETCH.
   — **Message:** Detailed information about the event.
   — **Object Type:** The object type of the object involved in this task.
   — **Object Name:** The name of the object involved in this task.

**Applying Snapshots**

You can apply a snapshot to a Grid to reset its configuration. When you apply a snapshot, you can either use the passwords available in the snapshot to login to the Grid or reset password when you login to the Grid. When you apply snapshot to a Grid, all the delegated tasks related to that Grid is deleted from the Task Viewer.

Do the following to apply a snapshot:

1. Login to the Master Grid.
2. From the Grid tab, click the List tab.
3. Select a Grid and click the Snapshot Manager icon.
4. Select a snapshot.
5. Click Apply Snapshot.
6. From the Maintain current password on reset drop down list, do one of the following:
   — select Yes to use the passwords available in the template.
— Select No to force the users existing in the template to reset their password at the first login on the reset Grid. Selecting this also enables the global password reset. Any new user created on the Grid should change their password at the first login.

Deleting Snapshots

You cannot schedule the deletion of a snapshot.  
To delete a snapshot:

1. Login to the Master Grid.
2. From the Grid tab, click the List tab.
3. Select a Grid and click the Snapshot Manager icon.
4. Click Delete.
5. Click Yes in the Delete Confirmation message dialog box.
Chapter 7  Network Management

This chapter describes how to manage the network spaces managed by the Master Grid. It also explains how to view real-time network data about your entire network space and delegate networks to a Grid or multiple Grids. It contains the following sections:

- **Network Management** on page 144
  - About Network Blocks on page 145
- **Viewing IPv4 and IPv6 Networks** on page 145
  - IPv4 and IPv6 Network Maps on page 145
  - IPv4 and IPv6 Network Lists on page 148
- **Managing IPv4 and IPv6 Networks** on page 149
  - Adding IPv4 and IPv6 Networks on page 149
  - Modifying IPv4 and IPv6 Networks on page 150
  - Resizing IPv4 Networks on page 150
  - Entering Extensible Attribute Values on page 150
  - Restricting Synchronization on page 151
Network Management

Multi-Grid management provides the tools you need to view and manage the entire network space of your enterprise through the Master Grid. The Infoblox IPAM (IP address management) implementation of the Master Grid offers a network-centric approach so you can track and manage network usage in each Grid that is managed by the Master Grid. Through Multi-Grid Manager, not only can you manage your entire network space, you can also drill down to individual Grids through SSO (Single Sign On) to perform IPAM and other DNS and DHCP tasks. For information about IPAM, DNS, and DHCP, refer to the Infoblox NIOS Administrator Guide.

In Multi-Grid Manager, you can visualize IPv4 and IPv6 networks of all Grids or selected Grids managed by the Master Grid in a map or list view. The map view provides an overview of the network spaces of the managed Grids, and the list view gives an alternate hierarchical view of all the corresponding networks in table format. Through these views, you can evaluate the number of networks each Grid has, their relative sizes, and the network spaces you have left for each Grid. You can also identify overlapping networks across multiple Grids and decide whether you want to adjust or resize the networks in those Grids. Based on the information, you can decide whether to add and delegate a network to a managed Grid or Grids. When necessary, you can customize a map view to display specific networks of specific Grids that you select, and then save the map for future use.

In the map view, Multi-Grid Manager displays network blocks to represent individual network spaces. A network block can contain other network blocks, network containers, and leaf networks. For information about network blocks, see About Network Blocks. In this view, you can use the zoom function to magnify or reduce a network block to view its contents. You can also access the corresponding Grid of each network through SSO without logging in to the Grid each time. For information about SSO, see Viewing Validated Users on page 28.

You can do the following in the Data Visualization tab of Multi-Grid Manager:

- View your IPv4 and IPv6 networks of all managed Grids in the Master Grid. For information, see IPv4 and IPv6 Network Maps on page 145 and IPv4 and IPv6 Network Lists on page 148.
- Create IPv4 and IPv6 networks and delegate them to a managed Grid or Grids. For information, see Adding IPv4 and IPv6 Networks on page 149.
- Resize an IPv4 network that is not currently managed by a Grid member. For information, see Resizing IPv4 Networks on page 150.
- Use the zoom function to magnify or reduce specific network spaces. For information, see Zooming In and Out on page 147.
- Create custom network maps of specific Grids they you want to manage. For information, see Managing Custom Network Maps on page 147.
- Restrict synchronization of network views, network containers, and networks with the Multi-Grid Manager. For information, see Restricting Synchronization on page 151.
About Network Blocks

Multi-Grid Manager uses network blocks to group IPv4 and IPv6 network blocks, network containers and leaf networks in the Map panels. A network block is a block of networks that can contain other network blocks, network containers, and leaf 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 7.1 illustrates the IPv4 20.0.0.0/8 network, which is a network block with two network containers, 20.8.0.0/13 and 20.72.0.0/13. The 20.8.0.0/13 network container has two leaf networks, 20.8.0.0/16 and 20.9.0.0/16. The 20.72.0.0/13 network container has one leaf network, 20.72.0.0/16.

Figure 7.1  IPv4 Network Block

From Multi-Grid Manager, you can use the Zoom In function to drill down to the two network containers, 20.8.0.0/13 and 20.7.0.0/13, in the network block 20.0.0.0/8, and then continue to drill down to the corresponding leaf networks. For information about the zoom function, see Zooming In and Out on page 147.

Viewing IPv4 and IPv6 Networks

In Multi-Grid Manager, you use the IPv4 and IPv6 network Map and List panels to view and manage the network infrastructure of your entire enterprise. By default, the Map panel provides a graphical view of all your networks in all the managed Grids. You can also select specific Grids to view their networks and then create a custom map of the view and save it for future use. The network list is an alternative view of the network hierarchy of the Grids that are managed by the Master Grid. It displays all networks of all Grids in table format.

You can always switch your view of the network infrastructure between the Map and List panels. For information about each panel, see IPv4 and IPv6 Network Maps and IPv4 and IPv6 Network Lists on page 148.

IPv4 and IPv6 Network Maps

The IPv4 and IPv6 network maps provide a high-level view of the respective networks of the Grids that are managed by the Master Grid. You can use network maps to design and plan your network infrastructure, configure and manage individual networks, and evaluate their utilization. The maps provide an overview of the network spaces of the managed Grids so you can evaluate the number of networks each Grid has, their relative sizes, and the network spaces you have left for each Grid. You can also access individual Grids through Multi-Grid Manager and use IPAM to manage IP addresses for each Grid. For information about IPAM, refer to the Infoblox NIOS Administrator Guide.

The IPv4 and IPv6 maps display network spaces across a maximum of eight rows, depending on the sizes of the networks. Multi-Grid Manager automatically scales the maps so that they can display all networks of all Grids in your enterprise. You can also identify overlapped networks across multiple Grids as well as multiple smaller networks.

Based on the information, you can decide whether to add and delegate a network to a managed Grid or resize a network. You can also customize the map to display only the networks of the Grids that you select or manage, and then save the map for future use.
Depending on the size of the networks, the maps display network blocks in their respective colors across multiple rows. The color-coded network blocks are defined as follows:

- Network blocks that belong to a specific Grid are displayed in the same color so you can quickly identify the networks that belong to the same Grid.
- Overlapped networks across multiple Grids are displayed in a black and white color pattern.
- Very small and multiple networks are displayed in a red dotted bar.

By default, the appliance automatically selects a network color for each Grid. To change the color, click the color box next to the Grid name, and then select a color from the chart. The appliance changes the color of all corresponding network blocks based on your selection.

As illustrated in Fig. Figure 7.2, the IPv4 Map panel presents a complete view of the entire network space of all managed Grids, including the different types of networks that are in it and their unused address spaces. Each color-coded block represents a network block, overlapped networks, 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. Therefore, you can quickly evaluate how many and what type of networks are in your Grids, their relative sizes, utilization, and how much space you have left.

As you mouse over areas of the map, Multi-Grid Manager displays network information about the area. The Map panel also has a zoom feature that allows you to enlarge or reduce your view of a particular area.

*Figure 7.2 IPv4 Network Map*
Displaying Network Information

As shown in Figure 7.2, you can get more information about a network block by hovering your mouse over a network block. A tooltip displays the following information about the network:

- The network address and netmask
- The name of the managed Grid
- The network view to which the network address belongs

The tooltip also display an Access icon. When you click the Access icon, you can access the Grid to which the network belongs. If you have configured user validation to this Grid, you can access this Grid without logging in to the Grid. For information about SSO, see Viewing Validated Users on page 28.

Zooming In and Out

Use the zoom function to enlarge and reduce your view of a selected network area. When you zoom in on an area until it reaches the last possible zoom level, the Zoom In icon in the task bar is disabled. After you zoom in on an area, you can click the Zoom Controller icon to track where you have 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 zoom in to a selected network block:
1. Click the Zoom In icon in the task bar.
2. In the map, 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. Release the mouse button when you reach the end point.
   The map displays a magnified view of the selected area after you release the mouse button. As you mouse over the zoomed in area, the tooltip displays IP information about it.

You can do the following after you zoom in to a network block:

- Select an area and zoom in again.
- Select a network and click the Edit icon to edit its properties.
- Click the Zoom Out icon to zoom out of the current network. Each time you click the zoom out icon, the map zooms out one level and the Zoom Controller is updated accordingly.
- If you want to access the Grid to which the network belongs, click the Access icon in the tooltip. You can access the GUI of the Grid through a separate browser. You do not need to enter user credentials to log in to the Grid if you have configured user validation for SSO.

Managing Custom Network Maps

You can create new custom network maps by selecting specific Grids and network views so Multi-Grid Manager displays only the networks of the selected Grids and network views. By default, Multi-Grid Manager selects all managed Grids and network views and displays all the networks. You can do the following about network maps:

- Create new network maps: You can select the check boxes of the Grids and network views you want Multi-Grid Manager to display, and then click Save as next to the Custom Map drop-down list to create a new custom map.
- Update existing maps: After you create a custom map, you can change the map by adding or deleting specific Grids and network views, and then save the changes.
- Delete existing maps: You can select a specific custom map and delete it.

To create a new custom network map:
1. From the Data Visualization tab, select the IPv4 or IPv6 Map panel.
2. Select the Grids and network views you want to include in the map view, and then click Save as.
3. In the Save Custom Map dialog box, do the following:
   - Custom Map Name: Enter the name of the custom map.
   - Set as a global custom map: Select this to make this map globally available to all users.
4. Save the configuration.
To update an existing map:
1. From the Custom Map drop-down list, select the map you want to update. Multi-Grid Manager displays the networks of the custom map.
2. Make changes by adding or deleting Grids and network views, and then click Save.
3. In the Save Custom Map dialog box, select Set as a global custom map if you want to make this map globally available to all users. Otherwise, click Yes to save the changes to the selected map. If you click No, you can save the changes as another custom map. Multi-Grid Manager keeps the current map and add another map with the changes you just made.
4. Save the configuration.

To delete a custom map:
1. From the Custom Map drop-down list, select the map you want to delete, and then click Delete.
2. In the Delete Confirmation Custom Map dialog box, click Yes. Multi-Grid Manager deletes the selected map.

Performing Other Tasks in Map Panels

From the Map panels, you can do the following:
- Add a new IPv4 or IPv6 network and delegate it to a Grid or Grids, as described in Adding IPv4 and IPv6 Networks on page 149.
- Zoom in on specific areas, as described in Zooming In and Out on page 147.
- Validate user credentials for SSO, as described in Viewing Validated Users on page 28.
- Select a network and add or modify extensible attributes and permissions, as described in Entering Extensible Attribute Values on page 150.
- Click the Refresh icon to refresh the Map view.
- Select a network and edit its properties, as described in Modifying IPv4 and IPv6 Networks on page 150.
- Switch to the List view of the network. For information, see IPv4 and IPv6 Network Lists on page 148

IPv4 and IPv6 Network Lists

The IPv4 and IPv6 network lists are alternate views of the network hierarchies managed by the Master Grid. By default, the List panels display all networks of all Grids in table format. A network list displays only the first-level network blocks. It does not show further descendant or network containers. When select and open a network block from the List panel, you can view its child networks by accessing its corresponding Grid. Multi-Grid Manager opens a separate browser from which you can access the Grid.

If the number of networks exceeds the maximum page size of the table, this panel displays the information on multiple pages. You can use the page navigation buttons at the bottom of the table to navigate through the pages of networks.

This panel displays the following information:
- **Network Block**: The network address and netmask.
- **Grid**: The name of the Grid managed by the Master Grid, or the Grid to which the network block belongs.
- **Network View**: The network view to which the network block belongs.
- **Comment**: Information about the network block.
- **Site**: The value entered for this pre-defined attribute.

You can select all available extensible attributes of each Grid for display. You can also use filters to filter the network list so it displays only the networks you want to see. For example, you can enter “Network Block begins with 7.0” as the filter criteria to view only the network addresses that begin with 7.0. Note that extensible attributes are those with a gray background in the list of available filter fields.
Filtering Network Lists

You can filter the network list so it displays only the networks you want to see. You can filter the list based on certain parameters, such as network blocks, comments, or any available extensible attributes. When you expand the list of available fields you can use for the filter, the extensible attributes are those with a gray background.

You can also create a quick filter to save frequently used filter criteria, as follows:

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.

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].

Performing Other Tasks in List Panels

You can do the following in this panel:

- Add a new IPv4 network and delegate it to a Grid or Grids, as described in Adding IPv4 and IPv6 Networks on page 149.
- 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 on page 31.
- Sort the list of networks in ascending or descending order by column.
- Print and export the data in this panel.
- Click the Refresh icon to refresh the List view.

Managing IPv4 and IPv6 Networks

Adding IPv4 and IPv6 Networks

To add an IPv4 or IPv6 network to a specific Grid or Grids:

1. From the Data Visualization tab, select the IPv4 or IPv6 Map or List panel, and then click the Add icon.
2. In the Add Network wizard, do the following:
   - IPv6 Prefix: This is displayed only if you are adding an IPv6 network. If you are adding an IPv6 network using a previously defined global IPv6 prefix, you can select it from the list.
   - Address: Enter the network address.
   - Netmask: Adjust the netmask slider to a fixed netmask for this network address.
   - Comment: Enter useful information about the network address.
   - Disable for DHCP: Select the check box to disallow the converted network from being usable under DHCP.

   **Note:** The Disable for DHCP check box enables or disables DHCP for the network.

3. Click Next and complete the following to delegate the new network to an existing Grid or Grids:
   - Grid: Select the Grid to which you want to delegate the newly created network.
   - Network View: Select the network view to which you want to delegate the network.
   Click + to delegate the same network to another Grid and network view.
4. Click Next to add extensible attributes, as described in Entering Extensible Attribute Values on page 150.
   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.
5. Save the configuration.
**Modifying IPv4 and IPv6 Networks**

You can modify existing network settings, with the exception of the network address and subnet mask.

To modify an IPv4 or IPv6 network:

1. From the Data Visualization tab, select the IPv4 or IPv6 Map or List panel, and then click the Edit icon.
2. The IPv4 Network or IPv6 Network editor provides the following tabs from which you can modify data:
   - **General**: Modify the network settings as described in *Adding IPv4 and IPv6 Networks* on page 149.
   - **Extensible Attributes**: Modify extensible attributes as described in *Entering Extensible Attribute Values* on page 150.
   - **Permissions**: Modify the permissions of the network as described in *Modifying Permissions* on page 79.
3. Save the configuration.

**Resizing IPv4 Networks**

You can resize an IPv4 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 or IPv6 network when the operation does not affect existing objects in the network. You can resize an existing network only if the network is not assigned to a Grid member. 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.

To resize a network:

1. From the Data Visualization tab, select the IPv4 or IPv6 Map or List panel.
2. Drill down to the network you want to resize, select the network, and then click Resize from the Toolbar. Note that you can only resize networks that are not currently assigned to a Grid member.
3. 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.
4. Click OK.

**Entering Extensible Attribute Values**

Multi-Grid Manager displays the required extensible attributes, if any. You must enter values for all required attributes. For more information about extensible attributes, see *About Extensible Attributes* on page 164.

In this step, you can do the following:

- Enter values for extensible attributes
- Add attributes
- Delete non-required attributes

To enter values for extensible attributes:

1. Click the Value column of the attribute.
2. Depending on the required attribute type, either enter or select a value for the attribute from the Value column. You must enter values for all required attributes.
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:
1. Click the check box beside the attribute you want to delete.
2. Click the Delete icon.

To delete all attributes:
1. Click the check box beside Attribute Name.
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.

## Restricting Synchronization

You can restrict synchronization of network views, network containers, and networks from the managed Grid to the Multi-Grid Master. You can do this when you are configuring or modifying them.

### Restricting Synchronization for Network Views

To restrict synchronization when adding a new network view:
1. Log in to the managed Grid. Make sure that the Grid remains joined with the Multi-Grid Master.
2. From the Administration tab, select the Network Views tab, and then click the Add icon.
3. In the Network View wizard, do the following:
   - Disable sync to MGM: Select this check box to disable synchronization. This will restrict the synchronization of all objects that are associated with this network view.
4. Save the changes.

To restrict synchronization when modifying network views:
1. Log in to the managed Grid. Make sure that the Grid remains joined with the Multi-Grid Master.
2. From the Administration tab, select the Network Views tab → network_view check box, and then click the Edit icon.
3. In the Network View editor, select the General tab and complete the following:
   - 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.
4. Save the changes.
Restricting Synchronization on IPv4 and IPv6 Networks

When you configure IPv4 or IPv6 networks on the managed Grid, you can enable or disable synchronization, or inherit settings from the parent object. You cannot override the settings at the child level if you have already restricted synchronization at the parent level. You may receive an error message when you try to enable synchronization at the child level after disabling synchronization at the parent level.

To restrict synchronization while configuring IPv4 or IPv6 networks:

1. Log in to the managed Grid. Make sure that the Grid remains joined with the Multi-Grid Master.
2. From the Data Management tab -> IPAM tab.
3. From the Add drop-down menu, select IPv4 Network or IPv6 Network.
4. In the Add Network wizard, select one of the following:
   — Add Network Container: Select this to add a network container.
   — Add Network: Select this to add a network.
5. Click Next and 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.
   — Use Inherited Setting: Select this to inherit synchronization settings from the parent object.
6. Save the changes.

To restrict synchronization while modifying IPv4 or IPv6 networks:

1. Log in to the managed Grid. Make sure that the Grid remains joined with the Multi-Grid Master.
2. 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.
3. The IPv4 Network editor contains the following basic tabs from which you can modify data:
   — General 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.
     — Disable sync to MGM: Click Override and select this check box to disable synchronization of the selected network with the Multi-Grid Master. Note that you can override only when you have not disabled synchronization at the parent level.
4. Save the changes.
Chapter 8  Managing Master Grid Operations

Managing the operations of the Master Grid involves defining system parameters such as time, security, and port settings. This chapter describes how to set these operational parameters and how to set up a static route when the Master Grid can send and receive traffic through multiple gateways. This chapter includes the following sections:

- Managing Time Settings on page 155
  - Changing Time and Date Settings on page 155
  - Changing Time Zone Settings on page 155
- Using NTP for Time Settings on page 156
  - Authenticating NTP on page 156
  - Multi-Grid Master and Members as NTP Clients on page 158
  - Configuring the Master Grid to Use NTP on page 159
  - Configuring a Master Grid Member to Use NTP on page 160
- Scheduling Tasks on page 161
  - Scheduling Additions and Modifications on page 161
  - Viewing Scheduled Tasks on page 161
  - Icons for Scheduled Tasks on page 162
  - Rescheduling Tasks on page 163
  - Guidelines for Upgrading, Backing Up, and Restoring the Database on page 164
- About Extensible Attributes on page 164
  - Configuring Extensible Attributes on page 165
  - Using Extensible Attributes on page 168
  - Editing Multiple Extensible Attribute Values on page 168
  - Grouping and Ungrouping Extensible Attributes on page 169
- Managing External Storage Server on page 170
  - Configuring External Storage on page 173
  - Testing External Storage Connection on page 174
  - Disabling External Storage Sever on page 174
- Managing Security Operations on page 175
  - Enabling Support Access on page 175
  - Enabling Remote Console Access on page 175
  - Permanently Disabling Remote Console and Support Access on page 175
  - Restricting GUI/API Access on page 175
— Enabling HTTP Redirection on page 175
— Modifying the Session Timeout Setting on page 176
— Disabling the LCD Input Buttons on page 176
— Configuring Security Features on page 176

• Ethernet Port Usage on page 177
  — Modifying Ethernet Port Settings on page 181

• Using the LAN2 Port on page 181
  — About NIC Redundancy on page 181
  — Configuring the LAN2 Port on page 183

• Using the MGMT Port on page 183
  — Appliance Management on page 184
  — Master Grid Communications on page 186

• Setting Static Routes on page 189

• Enabling DNS Resolution on page 193

• Managing Licenses on page 194
  — Obtaining and Adding Licenses on page 194
  — Obtaining Temporary Licenses on page 195
  — Viewing Licenses on page 195
  — Backing Up Licenses on page 196
  — Removing Licenses on page 196

• Shutting Down, Rebooting, and Resetting on page 196
  — Rebooting an Appliance on page 196
  — Shutting Down an Appliance on page 197
  — Resetting an Appliance on page 197

• Managing the Disk Subsystem on the Infoblox-2000-A and -4010 on page 199
  — About RAID 10 on page 199
  — Evaluating the Status of the Disk Subsystem on page 200
  — Disk Drive Front Panel LEDs on page 201
  — Replacing a Failed Disk Drive on page 202
  — Disk Array Guidelines on page 202
Managing Time Settings

You can define the date and time settings for your Multi-Grid Master 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 Master Grid.

Note: You cannot manually set the date and time if the NTP service is enabled.

To set the time and date for the Master Grid using the Master Grid Properties editor:
1. From the Master Grid tab, click Master Grid Properties -> Edit from the Toolbar.
2. In the General tab of the Master 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.

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 the Master 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 in the Master Grid, 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:
1. From the Master Grid tab, click Master Grid Properties -> Edit from the Toolbar.
2. In the General tab of the editor, select the appropriate time zone.
3. Save the configuration.
Using NTP for Time Settings

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 the Multi-Grid Master to function as an NTP client that synchronizes its clock with an NTP server. 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 appliance can synchronize its clock. For a list of these servers, you can access http://www.ntp.org.

The Multi-Grid Master and its members can function as NTP clients that synchronize their clocks with external NTP servers. You can configure the Multi-Grid Master and its members to use their own external NTP servers.

Authenticating NTP

To prevent intruders from interfering with the time services on your network, you can authenticate communications between the Multi-Grid Master or member and a public NTP server, and between the Multi-Grid Master or member and external NTP clients.

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 8.1 on page 157, 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 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 appliance. When you configure the 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 8.1  NTP Client Administrator Obtaining Secret Key from NTP Server Administrator
Multi-Grid Master and Members as NTP Clients

You can configure a Multi-Grid Master or a Master Grid member as an NTP client that synchronizes its system clock with an external NTP server.

When you enable the 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 the 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 on page 156.

In the Master Grid, you can configure the Multi-Grid Master and Master Grid members to synchronize their clocks with external NTP servers, as shown in Figure 8.2. If you configure the NTP server at the Master Grid level, all members (including the Multi-Grid Master) inherit the settings. For information, see Configuring the Master Grid to Use NTP on page 159.

Figure 8.2 Master Grid as NTP Client

The Multi-Grid Master uses three public NTP servers to calibrate its clock to the correct time. It uses symmetric key cryptography to authenticate NTP messages.

All NTP communications with the Master Grid go through encrypted VPN tunnels.

Master Grid Member 2 synchronizes its clock with a public NTP server.
Configuring the Master Grid to Use NTP

In the Master Grid, the Multi-Grid Master and members can synchronize their clocks with external NTP servers. In an HA pair, the active node communicates directly with an external NTP server. The passive node then synchronizes its clock with the active node.

To configure the Master Grid to use NTP, perform the following tasks:

- If you want to enable authentication between the appliance and NTP servers, you must specify the authentication keys before enabling the NTP service. For information, see Adding NTP Authentication Keys.
- Enable the NTP service on the Master Grid and specify one or more external NTP servers. For information, see Enabling the NTP Service on page 159.

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 Master Grid. You can also override authentication keys at the Multi-Grid Master and member levels.

To add NTP authentication keys:

1. Master Grid: From the Master Grid tab, select the Multi-Grid Master, expand the Toolbar and click NTP -> NTP Master Grid Config.
   Member: From the Master Grid tab, select the Members tab -> master_grid_member check box. Expand the Toolbar and click NTP -> NTP Master Grid Member Config.
   To override an inherited property, click Override next to it and complete the appropriate fields.
2. 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.
     - MD5 in ASCII format (M): The key is a 1-31 character ASCII string using MD5 (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.
     - DES in ASCII format (A): The key is a DES key written as a 1-8 character ASCII string.
     - DES in NTP format (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.
   - **String**: The key data used to calculate the MAC. The format depends on the Key Type you select.
3. Click Save to save the entry and keep the editor open so you can enable the Master Grid to synchronize its time with external NTP servers, as described in Enabling the NTP Service on page 159.

Note that if you enter a new key, the appliance checks if the key already exists in the key list. If the key exists, but either the key type or key string does not match, the appliance sends an error message.

After you enter an authentication key, you can modify or delete it. Note that you cannot delete a key that an NTP server references. You must first delete all NTP servers that reference that key and then delete the key.

Enabling the NTP Service

To enable the Master Grid to synchronize its time with external NTP servers:

1. From the Master Grid tab, select the Member tab -> multi-grid_master check box, expand the Toolbar and click NTP -> NTP Master Grid Config.
2. In the Master Grid Properties editor, select Synchronize the Master Grid with these External NTP Servers.
3. Click the Add icon in the External NTP Servers table.
4. In the Add NTP Server dialog box, enter the following information, and then click Add.

   — **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 appliance can resolve the NTP server host name, click Resolve Name. You must have a DNS name resolver configured. For information, see Enabling DNS Resolution on page 193.

   — **Enable Authentication:** Select this option to enable authentication of NTP communications between the external NTP server and the appliance (the Multi-Grid Master or Master Grid member or the active node in an HA pair).

   **Note:** To prevent intruders from interfering with the time services on your network, you can authenticate communications between a Master Grid member and an external NTP server, as well as between a Master Grid member and external NTP clients. NTP communications within the Master Grid go through an encrypted VPN tunnel, so you do not have to enable authentication between the Multi-Grid Master and Master Grid members.

   — **Authentication Key:** Select a key that you previously entered, and then click OK. For information, see Adding NTP Authentication Keys on page 159.

5. Save the configuration.

### Configuring a Master Grid Member to Use NTP

To configure the Multi-Grid Master or member to synchronize its time with external NTP servers:

1. From the **Master Grid** tab, select the **Members** tab -> **master_grid_member** check box.
2. Expand the Toolbar and click **NTP** -> **NTP Master Grid Member Config**.
3. In the **Master Grid Member Properties** editor, do the following:

   — **Synchronize this Member with other NTP Servers:** Select this option to enable this Master 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.

4. Click Override, and then click the Add icon in the External NTP Servers table.
5. In the Add NTP Server dialog box, enter the following information, and then click Add.

   — **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 appliance can resolve the NTP server host name, click Resolve Name. You must have a DNS name resolver configured. For information, see Enabling DNS Resolution on page 193.

   — **Enable Authentication:** Select this check box to enable authentication of NTP communications between the external NTP server and the member in the Master Grid.

   **Note:** To prevent intruders from interfering with the time services on your network, you can authenticate communications between a Master Grid member and an external NTP server, as well as between a member and external NTP clients. NTP communications within the Master Grid go through an encrypted VPN tunnel, so you do not have to enable authentication between the Multi-Grid Master and members.

   — **Authentication Key:** Select a key that you previously entered, and then click OK. For information, see Adding NTP Authentication Keys on page 159.

6. Save the configuration.

### Managing External NTP Servers

You can specify multiple NTP servers for failover purposes. The appliance attempts to connect to the NTP servers in the order they are listed. 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.
Scheduling Tasks

You can schedule tasks, such as adding networks, for a future date and time. The scheduling feature is useful when you want to add or modify an object 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. Only superusers can view, reschedule, and delete all scheduled tasks. Limited-access admins can reschedule and delete only their scheduled tasks. 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.

Scheduling Additions and Modifications

You can schedule the addition and modification of an object. For example, you can schedule the delegation of a network to a managed Grid. After you schedule a task, administrators cannot modify the object associated with the scheduled task until after the appliance executes the task.

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:
   - Now: Select this to have the appliance perform the task when you save the entry. This is selected by default when there is no scheduled task associated with the object.
   - Later: Select this to schedule the task for a later date and time. Complete the following:
     - 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 Multi-Grid Manager.
4. Save the configuration.

Viewing Scheduled Tasks

After you schedule a task, you can view the pending task in the Scheduled Tasks viewer. Multi-Grid Manager also displays a Schedule icon next to the associated object, 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 or if you are a superuser. In the corresponding editor, the Schedule icon is green when there is a pending scheduled task. For information, see Icons for Scheduled Tasks on page 162.

The appliance logs the scheduled tasks in the audit log and displays the pending tasks in the Scheduled Tasks viewer. By default, Multi-Grid Manager sorts the pending tasks with the earliest scheduled start times. The Scheduled Tasks viewer displays the pending scheduled tasks that the admin is allowed to view. Superusers can view all scheduled tasks, and limited-access admins can view their own scheduled tasks. For information, see Scheduled Tasks Viewer on page 161.

Scheduled Tasks Viewer

To view pending scheduled tasks:

1. From the Administration tab, select the Scheduling tab.
2. Multi-Grid Manager displays the following information for each task:
Managing Master Grid Operations

- **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.
- **Affected Object**: The name of the object that is associated with the task. For example, if the task involves a network, it displays the network address.
- **Object Type**: The object type, such as **Delegated Task**.
- **Action**: The operation the appliance performs in this task. The value can be one of the following:
  - Add: Addition
  - Modify: Modification
  - Delete: Deletion
- **Task Details**: 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 also select **Task ID** for display. The appliance assigns a task ID to a scheduled task in chronological order.

You can do the following in this viewer:

- Sort the tasks in ascending or descending order by column, except for **Task Details**.
- Use the filters or the Search function to locate a specific scheduled task.
- 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 the task, cancel the scheduling of task, or execute the task immediately.

**Icons for Scheduled Tasks**

Multi-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 8.3**. 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 Multi-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, Multi-Grid Manager does not display the **Scheduled Deletion** dialog box when you click the icon.

**Figure 8.3  Icon for a Scheduled Task**

In an editor, Multi-Grid Manager displays the Schedule icon in green to indicate a pending scheduled task associated with the corresponding object, as shown in **Figure 8.4**. 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** on page 163.
Rescheduling Tasks

Superusers can reschedule any scheduled task. Limited-access admins can reschedule only the tasks that they scheduled, depending on their permissions. When you reschedule a task, Multi-Grid Manager displays the object or operation configuration in the 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.

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 the Scheduled Tasks viewer:

1. From the Administration tab, select the Scheduling 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.

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 Schedule Deletion 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.

Canceling Scheduled Tasks

To cancel a scheduled task:

1. From the Administration tab, select the Scheduling 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.
Guidelines for Upgrading, Backing Up, and Restoring the Database

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

- Upgrade the NIOS software: In a full upgrade, all scheduled tasks are deleted. In a lite upgrade, scheduled tasks are not deleted.
- Back up the database: All scheduled tasks are backed up for troubleshooting purpose.
- Restore the database: The scheduled tasks are not restored.
- Promote a member to a Multi-Grid Master: After the promotion, all scheduled tasks that are past due are executed immediately.
- Revert the NIOS software image: After the revert, all scheduled tasks that are past due are executed immediately.

About Extensible Attributes

You can use extensible attributes to capture additional information about the objects managed by the Master Grid. The Multi-Grid Manager wizards and editors that are used to add and edit objects contain an **Extensible Attributes** tab that you can customize. You can specify the attributes that users can manage in this tab for each object, so you can collect and track data specific to your organization. You can even specify required attributes, and restrict the values that users can enter for each attribute.

**Note:** Only superusers can configure extensible attributes.

You can specify different extensible attributes for each type of object. For example, you can configure the attribute Site for an IPv4 network, and the attribute Department for admin groups.

When you configure an 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
- The objects associated with the attribute, such as networks.
- Whether the appliance makes an entry in the audit log each time an object with the attribute is added or modified.

After you configure the attributes of an object, the attributes become available in the **Extensible Attributes** tab of the wizard and editor of the object. Users then add or edit the attribute values, according to your configuration. Users can also specify attributes when searching for data and add attributes as columns in the tables of Multi-Grid Manager. For information about adding columns to tables, see **Customizing Tables** on page 29.

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.

The Infoblox appliances provide the following predefined attributes that you can customize:

- Region
- Country
- State
- Site
- Building
- VLAN
When you use a predefined attribute, you can edit 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 on page 167.

You can also create your own attributes, as described in Adding Extensible Attributes on page 165.

Multi-Grid Manager displays all available extensible attributes of the Master Grid and managed Grids. You can group attributes in a manner that is easy for you to manage. For example, you can group all the Country attributes from all managed Grids so you have a group of attributes that report information about countries in different Grids. Note that you can only group extensible attributes with the same attribute types and from different Grids, and you cannot group extensible attributes from the Master Grid. For more information about grouping and ungrouping extensible attributes, see Grouping and Ungrouping Extensible Attributes on page 169.

Configuring Extensible Attributes

To configure extensible attributes, follow these procedures:

- Identify the data that you want to track. For example, when you want to identify the manufacturers of your network devices, you can create an extensible attribute to track this information.
- Decide which predefined extensible attributes you want to use, if any, and edit them.
- Define new attributes.

Adding Extensible Attributes

To add a new extensible attribute in the Master Grid:

1. In 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.
       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.
     - Email: Select this when the attribute is used for email addresses. Email addresses are entered in the format user@domain.com.
Managing Master Grid Operations

URL: Select this when the attribute is used for tracking URLs (Uniform Resource Locators). URLs must be entered in a valid format.

Date: Select this when the attribute is used for dates. The date value is in YYYY-MM-DD format.

Comment: Enter additional information about the attribute. You can enter up to 256 UTF-8 characters.

4. Click Next.

Allow multiple values: Select this check box if you want to allow multiple values for this attribute to be set on an object. You cannot change this value for predefined attributes.

Default Value: Enter the default value that the appliance displays for the attribute. Leave this blank if there is no default value for this attribute. If the attribute type is String, you can enter up to 256 UTF-8 characters. If the attribute type is List, the value must be one of the list values and can be up to 64 UTF-8 characters.

Attribute is Required in the GUI: Select this to require users to enter a value for this attribute when adding or modifying the corresponding object in the GUI. When you configure an attribute as a required field, users must enter a value for this attribute when they configure the objects that are associated with the attribute.

Restrict to Specific Object Types: Select this check box if you want to associate the attribute with specific object types. If you do not select this check box, the appliance associates this attribute with all the supported object types. For predefined attributes, you can restrict the attribute only to the object type Network.

Click the Add icon and select the object type with which you want to associate the attribute. By default, the appliance associates an extensible attribute with all the supported object types.

Log Attribute Values When Objects are Updated: Select this check box if you want the appliance to make an entry in the audit log each time an object with this attribute is added or modified. When you select attribute values for audit, they are included in all the audit log entries. For information about the audit log, see Using the Audit Log on page 237.

5. Save the configuration.

Multi-Grid Manager adds the attribute to the Extensible Attributes tab of the wizard and editor of the specified object types.

Viewing Extensible Attributes

To view extensible attributes, from the Administration tab, select the Extensible Attributes tab. The panel displays the following information:

- **Name:** The name of the extensible attribute.
- **Grid:** The name of the Master Grid or managed Grid to which the extensible attribute belongs.
- **Type:** The type of data defined by the attribute.
- **Comment:** Information about the extensible attribute.
- **Required:** Indicates whether users are required to complete this field.
- **Restricted to Objects:** The objects that are associated with the attribute. The defaults are IPv4 and IPv6 networks.

**Note:** All extensible attribute groups are highlighted with a purple background.

You can do the following in this panel:

- Click the Group icon to group specific extensible attributes. Note that you cannot group extensible attributes configured for Master Grid or within the same Grid. Click the Ungroup icon to remove extensible attributes from a group or delete an existing group of extensible attributes. For information, see Grouping and Ungrouping Extensible Attributes on page 169.
- Select an extensible attribute configured for Master Grid and click the Edit icon to modify data, or click the Delete icon to delete it. You cannot modify or delete extensible attributes configured for managed Grids. When you click the Edit icon, only read-only properties are displayed.
- Click the Permissions icon to configure permissions for the admin account.
- 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 on page 34.
• Modify some of the Master Grid 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 on page 31.
• Print or export the data.

Modifying Extensible Attributes
You can modify predefined attributes so they capture the information that you need. When you modify an attribute, all objects using the modified attributes are updated.

To modify an extensible attribute:
1. From 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 the step 4 of Adding Extensible Attributes on page 165.
5. Save the configuration.

Disabling Synchronization of Extensible Attributes
You can disable synchronization of extensible attributes from the managed Grid to the Multi-Grid Master.
1. Log in to the managed Grid. Make sure that the Grid remains joined with the Multi-Grid Master.
2. From the Administration tab, select the Extensible Attributes tab -> Extensible Attribute check box, and then click the Edit icon.
3. In the Additional Properties tab of the Extensible Attributes editor, select the Disable sync to MGM check box. By default, this check box is not selected. The Disable sync to MGM check box is displayed only if the managed Grid remains joined with the Multi-Grid Master.
4. Save the changes.

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.
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.

Multi-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, you can do the following:
- Enter values for extensible attributes
- Add attributes
- 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.

To add attributes:
1. Click the Add icon. Multi-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:
1. Click the check box beside the attribute you want to delete.
2. Click the Delete icon.

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.

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 networks, and view and modify their extensible attributes all at once.

Note that Multi-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 on page 29.
2. Expand the Toolbar and click Extensible Attributes.
Multi-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, Multi-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*.
  
  An attribute can have multiple rows if it allows multiple values. Multi-Grid Manager displays the values that all objects have in common, if any. Otherwise, it displays *Multiple Values*.
- **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.

Multi-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 *Exporting Displayed Data* on page 45.

### Grouping and Ungrouping Extensible Attributes

In Multi-Group Manager, you can create a new group of extensible attributes or add extensible attributes to an existing group. Note that you can only group extensible attributes that are configured for different Grids, but not those configured for the same Grid or for the Master Grid. You can also remove specific extensible attributes from a group or delete the group. Note that when you remove all attributes from a group, only the group is deleted, not the attributes.

To group extensible attributes, complete the following:

1. From the **Administration** tab, select the **Extensible Attributes** tab.
2. Select extensible attributes you want to add to a group, and then click **Group** from the Toolbar.
3. In the **Grouping** dialog box, complete the following:
   - **Select existing group**: Select an existing group from the drop-down list.
   - **Create a new group**: Select this to add a new group of extensible attributes. Enter the name of the group.
   - Click the Add icon to add the extensible attributes to the group. In the *Select Extensible Attribute* dialog box, select the extensible attributes you want to add, and then click **OK**. Click **Group** to group the extensible attributes.

To delete extensible attributes from a group or delete a group, complete the following:

1. From the **Administration** tab, select the **Extensible Attributes** tab.
2. Select an extensible attribute group, and then click **Ungroup** from the Toolbar.
3. In the **UnGroup** dialog box, select the extensible attributes you want to remove from the group.
4. Click **UnGroup**.

**Note:** When you select all the extensible attributes and click **UnGroup**, the group is deleted.
Managing External Storage Server

You can configure and monitor an external storage FTP server. Only superusers can configure the external storage server. Using external storage, you can store and retrieve snapshots and templates. The external storage is accessible only through FTP. The FTP protocol supports passive or active modes automatically. No other protocol is supported for the interaction between Multi-Grid Master and external storage server. Multi-Grid Manager supports Apache FTP server and Windows 2008 R2 FTP server. Only the Grid Master interacts with the external storage server.

Note: Make sure that the data in the external storage system is secure. The Multi-Grid Manager cannot protect and secure data in the external storage server. Also, you can configure only one external storage server for one Multi-Grid Manager.

External Storage Requirements

A home directory should exist in the external storage server and the FTP user with read/ write permission should be able to perform the following in the home directory:

- create, delete, and change directory
- list files and directory
- create, rename, and delete a file

File Operations in External Storage

Multi-Grid Master automatically uploads a file when snapshot is captured for attach or detach operation. The following operations on the external storage is logged on the Multi-Grid Master:

- storing a file (operation, filename, temporary filename used during upload)
- deleting a file (operation, filename)

Backing Up Data

Multi-Grid Manager backups do not include the content of the external storage. You have to set up a backup mechanism for the backup of the external storage server. Infoblox recommends to take external storage backup along with the Multi-Grid Manager backup.

The external storage backup should include:

- all the files in the infoblox/MGM/[uuid]/ directory, where uuid is the 16 character long hexadecimal string, which is unique and tied to the Multi-Grid Manager.
- file path relative to the home directory with infoblox/MGM/[uuid]/ prefix.
- permissions and ownership of the files.

Best practice to restore a backup data is to first restore the external storage backup and then restore a Multi-Grid Manager backup. Note that the Multi-Grid Manager restore operation points to the external storage specified in the Multi-Grid Manager backup, which should match with the external storage being used to restore the external storage content. When you restore a backup, it restores all the files at the root of the home directory on the external storage. Permissions and ownership of the files are also restored as defined in the backup.

File Hierarchy

All directories and files are stored in the directory: infoblox/MGM/[uuid]/ where [uuid] is the unique identifier of the Multi-Grid Manager. This prevents multiple Multi-Grid Managers configured to use the same storage and home directory to collide. The directory is relative to the home directory configured through FTP to connect to the external storage.

Note: Tampering any file in the home directory can result in unavailability of the tampered files in the Multi-Grid Manager that uses this directory.
Managing External Storage Server

**External Storage Space Limit**

You can define a maximum space limit on the external storage. It defines the maximum space available to Multi-Grid Manager to store files on the storage. The maximum space limit is defined as a number of bytes which is compared against the sum of all the files stored under the `infoblox/MGM/[uuid]/` directory.

You can set the maximum space limit to a larger value, in which case Multi-Grid Manager is limited to the total space of the external storage. Multi-Grid Manager does not delete any data even if the size of the space used on the external storage is above the maximum space limit. In addition, it does not enforce a maximum file size, but is subjected to the maximum file size supported by the file system used by the external storage.

**Monitoring External Storage Server**

You can monitor the connectivity and space usage of the external storage server.

The status 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="green.png" alt="Green" /></td>
<td>Green</td>
<td>You can connect to the external storage server and the storage capacity is below the threshold limit. Also, the last operation on the external storage is successful.</td>
</tr>
<tr>
<td><img src="yellow.png" alt="Yellow" /></td>
<td>Yellow</td>
<td>You can connect to the external storage server but the storage capacity is above the configured threshold limit and it is below 100%.</td>
</tr>
<tr>
<td><img src="red.png" alt="Red" /></td>
<td>Red</td>
<td>Due to one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cannot connect to the external storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• can connect to the external storage but login failed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• storage capacity is above the limit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• can connect to the external storage and successfully login but last operation has failed</td>
</tr>
<tr>
<td><img src="gray.png" alt="Gray" /></td>
<td>Gray</td>
<td>The external storage server is not configured or it is disabled.</td>
</tr>
</tbody>
</table>

**About Archive Files**

The snapshots and templates are stored in the same file format. A snapshot or a template is stored in a single file with the following characteristics:

- archive file is a tar file
- archive is not encrypted
- archive contains the following files:
  - descriptor file and descriptor signature file
  - audit log archive file and audit log signature file
  - Grid backup file and Grid backup signature file
  - Optionally, an archive file can also have the following information based on the settings in the Snapshot tab of the Grid Editor wizard:
    - file distribution data. If file distribution data is available, then it is stored in the Grid backup file.
    - lease history archive file and lease history signature file.
    - syslog archive per appliance and each syslog archive followed by its signature file. Grids that are offline will have 0 byte file.
File Formats in Archives

- Audit Log Archive - Stored as audit_log.tar.gz. This archive has a gzip of the current and rolled Grid audit logs.
- Grid Backup - Stored as backup.bak.gz. This archive has a gzip of the original Grid backup. The original Grid backup follows the same format as regular NIOS backup obtained from the Grid. It contains the file distribution content and bloxtools data if snapshot is configured to include it.
- Lease History Archive - Stored as lease_history.gz. This archive has a gzip of the Grid CSV export of the lease history data.
- Syslog Archive - Stored as syslog-[member]-[role].tgz, where [member] is the FQDN of the member from which the syslog is extracted, [role] is either active or passive and allows to find out from what appliance the syslog is extracted in case the member is an HA pair. When the member is a single appliance, the [role] is always active. This is a tar gzip of the current and rolled syslog files of a Grid. If a Grid goes offline, the tar file contain only a single empty file named offline.
- Signature Files - Multi-Grid Manager uses signature files to verify the integrity of the data.

Locating Snapshots and Templates

All snapshots and templates are stored on the external storage FTP server.

- Templates are stored in the templates subdirectory of the directory infoblox/MGM.[uuid]/
- The snapshots are organized for a Grid and are stored in the subdirectory infoblox/MGM.[uuid]/
  where, <uuid>
  — uuid is a unique 16 character long hexadecimal string tied to the Grid.
  — For each subdirectory, an empty companion file exists in infoblox/MGM.[uuid]/, defined as follows:
  — <uuid>.<Grid>
    where, uuid is a unique 16 character long hexadecimal string tied to the Grid as known by Multi-Grid Manager and <Grid> is the Grid name as known by Multi-Grid Manager.
  — any non ACII or printable character or space in the Grid name is replaced with an underscore.

Note: The Grid name may not always be consistent with the Grid name on the Multi-Grid Manager. It updates Grid name once in every hour.

Naming Format of a Snapshot File

The snapshot file name will be in the format <uuid>-<type>-<Grid>-<date>.tar
where,
  — uuid - unique ID to identify a Grid.
  — type - attach (for attach snapshots), detach (for detach snapshots) and manual (for manual snapshots).
  — Grid - Grid name at the time of capturing a snapshot. Any non ACII or printable character are replaced with an underscore. Spaces are replaced with an underscore. This value is constant and does not change when the Grid name is changed, either in Master Grid or on the Grid.
  — Date - Timestamp of the snapshot operation in the YYYYMMDD-HHMMSS. Timestamp is UTC and it is the time at which the Multi-Grid Manager started the snapshot operation.

Note: The tar file becomes unusable if it is changed.
Configuring External Storage

Only superusers are able to configure an external storage server. All the configuration changes made to the external storage are logged in the audit log of the Multi-Grid Manager. You can modify the configuration only when the external storage server is disabled. The configured password is masked in the audit log entry.

The snapshots are not captured when:

- the external storage server is full.
- there is no connectivity between external storage server and Multi-Grid Manager.

You can view how much space is being used and how much free space you have on the external storage server through the Grid Connection Status widget on your Dashboard. For more information, see Grid Connection Status on page 54. You can also view the space details using the Detailed Status icon. The external server space usage is not updated in the real time. Some of the operations might fail if the external storage space is full and Multi-Grid Manager might not have updated it. When the external storage server space reaches the maximum value, the snapshots are not captured and the connection status is updated accordingly. The Master Grid logs an entry to indicate that the snapshots are not captured because there was no space in the external storage server.

You can allocate space, define the maximum number of snapshots to be captured for the attach and detach operations, test the storage connection and disable the external storage server using the External Storage Editor wizard:

To configure an external storage server:

1. Log in to the Multi-Grid Master.
2. From the Master Grid tab, select the Members tab.
3. On the vertical toolbar, click External Storage.
4. In the Server Address text box, enter the FTP server IP address. This can be IPv4 or IPv6 address or FQDN.
5. In the Server Port text box, enter the port number of the FTP server.
6. In the Server Login text box, enter the login user name.
7. In the Server Password text box, enter the server password.
8. Do the following to define storage space:
   - In the Maximum Available Storage Space text box, enter the maximum available storage space. Select the unit of the storage space. You can select GB gigabyte or TB terabyte.
   - In the Maximum Snapshots per Grid text box, enter the maximum number of snapshots you want to store in the external space for a Grid. When you decrease the set value, the Multi-Grid Manager automatically deletes the excess snapshots. For example: If you specify 10, the system will capture 10 snapshots. After this number, Multi-Grid Manager deletes the first record and saves the 11th snapshot.
   - In the Maximum Detach Snapshots per Grid text box, enter the maximum number of detach snapshots you want to store in the external space for a grid. For example: If you specify 10, the system will capture 10 snapshots. After this number, Multi-Grid Manager deletes the first record and saves the 11th snapshot.
9. Optionally, you can click Test Storage Connection to test the server connection.
10. Click Save to save the configuration.
Testing External Storage Connection

It is a good practice to test the external storage server connection to ensure that the external storage is initialized. Infoblox recommends you to test whenever you modify the external storage configuration. The Grid Master logs all the test results in the syslog and also captures error in case of test failure.

1. Log in to the Multi-Grid Master.
2. From the Master Grid tab, select the Members tab.
3. From the External Storage drop down list, click Test.
4. In the External Storage Test, do the following:
   - Server Address: Enter the IP address of the server.
   - In the Server Port text box, enter the port number of the server.
   - In the Server Login text box, enter the login user name.
   - In the Server Password text box, enter the server password.
5. Click Test to check the connection of the server. A message is displayed about the availability of the server.

You can also test the availability while configuring the server in the External Storage Editor using the Test Storage Connection option.

Disabling External Storage Server

You can disable the connection between the external storage server and the Master Grid at any point of time. The snapshot is not captured when you disable the external storage server. An error message is displayed to indicate that the external storage server is not enabled. The Master Grid logs an entry to indicate that the snapshot is not captured because the external storage server was disabled. The snapshot is captured only when the external storage server is enabled and connection between the server and the Multi-Grid Manager is restored.

To disable the external storage server:
1. Log in to the Multi-Grid Master.
2. From the Master Grid tab, select the Members tab, and then click External Storage.
3. Select the Disable check box.
4. Click Save to save the configuration.

When you disable the external storage server, you cannot do the following:
- Perform operation relying on the storage
- Retrieve or store data (snapshot or template)
- List data from the external storage
- Store file on Multi-Grid Manager
- Monitor the external storage
- Schedule any detach or attach operation

Multi-Grid Manager stops using the external storage server when it is disabled or reconfigured. However, files stored on the external storage server are preserved. Multi-Grid Manager uses the existing data when it is reconfigured to the external storage that has already been used.
Managing Security Operations

The Master Grid provides certain security-related features. The following sections describe the different security-related features that you can set. For information about how to configure these features, Configuring Security Features on page 176.

Enabling Support Access

Infoblox Technical Support might need access to the Master Grid to troubleshoot problems. This function enables an SSH (Secure Shell) daemon that only Infoblox Technical Support can access. If you have any questions, contact Infoblox Technical Support at support@infoblox.com. By default, this option is disabled.

Enabling Remote Console Access

This function 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.

Permanently Disabling Remote Console and Support Access

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.

Restricting GUI/API Access

You can specify the IP addresses from which administrators are allowed to access the Master Grid. When the 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 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.

Enabling HTTP Redirection

You can enable the Master Grid to redirect administrative connection requests using HTTP to the secure HTTPS protocol. When you disable redirection, the appliance ignores any administrative connection requests not using HTTPS. By default, the 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 Multi-Grid Manager 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 Multi-Grid Manager 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 the appliance to change the IP 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 the appliance administrators and you do not want anyone to be able to make changes through the LCD.

Configuring Security Features

To configure security features for the Master Grid:

1. Multi-Grid Master: From the Master Grid tab, click Master Grid Properties → Edit from the Toolbar.
   or
   Member: From the Master Grid tab, select the Members tab → master_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 Security tab, complete the following:
   - Session Timeout(s): This field is in the Master 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 Master Grid Properties editor only. Specify the minimum number of characters allowed for an admin password.
   - Redirect HTTP to HTTPS: This field is in the Master Grid Properties editor only. Select this option to have the appliance redirect HTTP connection requests to HTTPS.
   - Restrict GUI/API Access: This field is in the Master Grid Properties editor only. To restrict access to the GUI and API, select this option and click the Add icon. To allow administrative access to the GUI and API from a single IP address, enter the IP address in the Address field. Note that if you specify an address 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.

   To restrict administrative access to the GUI and API to a subnet, enter the network address in the Address field. Note that if you specify a subnet 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.

   - 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.
   - Enable Support Access: Select this check box to enable an SSH (Secure Shell) daemon that only Infoblox Technical Support can access.
   - Restrict Remote Console and Support Access to the MGMT 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 nodes. 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 the appliance to change the IP address settings of the LAN port. Clear this check box to disable this function.

3. Save the configuration.

---

### Ethernet Port Usage

The Ethernet ports on the appliance perform different functions, which vary depending on deployment and configuration choices. The Ethernet ports that transmit and receive traffic to the appliance are as follows:

- **LAN1 port** – This is the default port for single appliances and passive nodes in HA pairs. All deployments use the LAN port for management services if the MGMT port is disabled.

- **LAN2 port** – The LAN2 port is not enabled by default. 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 appliance on which you want to enable the port. The LAN2 port is available on Infoblox-250-A, 550-A, -1050-A, -1550-A, -1552-A, -1852-A, -2000-A, and -4010 appliances. For information about how to use the LAN2 port, see *Using the LAN2 Port* on page 181.

- **HA port** – This is the default port for the active node of an HA pair.

- **MGMT port** – If the MGMT port is enabled, the appliance uses it for many types of management services (see Table 8.3 on page 178 for specific types).

*Table 8.1* displays the type of traffic per port for both Multi-Grid Master and members. For a more detailed list of the different types of traffic, see *Table 8.3* on page 178.

### Table 8.1 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 Multi-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 Multi-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 Multi-Grid Master</td>
<td>No</td>
<td>–</td>
<td>Disabled</td>
<td>LAN1</td>
<td>LAN1</td>
<td>LAN1</td>
<td>LAN1</td>
</tr>
<tr>
<td>HA Master 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 Master 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 Master 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>HA Multi-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 Multi-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 Multi-Grid Master</td>
<td>No</td>
<td>–</td>
<td>Enabled</td>
<td>LAN1</td>
<td>LAN1 or MGMT</td>
<td>MGMT</td>
<td>MGMT</td>
</tr>
<tr>
<td>HA Master 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 Master 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>
</tbody>
</table>
Table 8.2 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 Port</th>
<th>LAN2 Port</th>
<th>Database Synchronization</th>
<th>Core Network Services</th>
<th>Management Services</th>
<th>GUI Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Master 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>
</tbody>
</table>

HA Multi-Grid Master
- Active
- Passive

Single Multi-Grid Master
- –

HA Master Grid Member
- Active
- Passive

To see the service port numbers and the source and destination locations for traffic that can go to and from the appliance, see **Table 8.3**. 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 8.3 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</td>
<td>LAN1 or MGMT on Master Grid member</td>
<td>VIP on HA Multi-Grid Master, or LAN1 on single master</td>
<td>17 UDP</td>
<td>2114</td>
<td>2114</td>
<td>Initial key exchange for establishing VPN tunnels Required for Master Grid</td>
</tr>
<tr>
<td>Service</td>
<td>SRC IP</td>
<td>DST IP</td>
<td>Proto</td>
<td>SRC Port</td>
<td>DST Port</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------</td>
<td>---------------------------------------</td>
<td>-------</td>
<td>---------------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>VPN</td>
<td>LAN1 or MGMT on Master Grid member</td>
<td>VIP on HA Multi-Grid Master, or LAN1 on single master</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 Master Grids with new DNSone 3.2 installations and 5002 for Master Grids upgraded to DNSone 3.2; the port number is configurable Required for Master Grid</td>
</tr>
<tr>
<td>RADIUS Authentication</td>
<td>NAS (network access server)</td>
<td>LAN1 or VIP</td>
<td>17 UDP</td>
<td>1024 – 65535</td>
<td>1812</td>
<td>For proxying RADIUS Authentication-Requests. The default destination port number is 1812, and can be changed to 1024 – 63997. When configuring an HA pair, ensure that you provision both LAN IP addresses on the RADIUS server.</td>
</tr>
<tr>
<td>RADIUS Accounting</td>
<td>NAS (network access server)</td>
<td>LAN1 or VIP</td>
<td>17 UDP</td>
<td>1024 – 65535</td>
<td>1813</td>
<td>For proxying RADIUS Accounting-Requests. The default destination port number is 1813, and can be changed to 1024 – 63998.</td>
</tr>
<tr>
<td>RADIUS Proxy</td>
<td>LAN1 or VIP</td>
<td>RADIUS home server</td>
<td>17 UDP</td>
<td>1814</td>
<td>1024 -&gt; 63997 (auth), or 1024 -&gt; 63998 (acct)</td>
<td>Required to proxy requests from RADIUS clients to servers. The default source port number is 1814, and although it is not configurable, it is always two greater than the port number for RADIUS authentication.</td>
</tr>
<tr>
<td>ICMP Dst Unreachable</td>
<td>VIP, LAN1, LAN2, or MGMT, or UNIX-based client</td>
<td>LAN1, LAN2, or UNIX-based client</td>
<td>1 ICMP Type 3</td>
<td>–</td>
<td>–</td>
<td>Required to respond to the UNIX-based traceroute tool to determine if a destination has been reached</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>1 ICMP Type 0</td>
<td>–</td>
<td>–</td>
<td>Required for response from ICMP echo request (ping)</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>1 ICMP Type 8</td>
<td>–</td>
<td>–</td>
<td>Required to send pings and respond to the Windows-based traceroute tool</td>
</tr>
<tr>
<td>ICMP TTL Exceeded</td>
<td>Gateway device (router or firewall)</td>
<td>Windows client</td>
<td>1 ICMP Type 11</td>
<td>–</td>
<td>–</td>
<td>Gateway sends an ICMP TTL exceeded message to a Windows client, which then records router hops along a data path</td>
</tr>
<tr>
<td>Service</td>
<td>SRC IP</td>
<td>DST IP</td>
<td>Proto</td>
<td>SRC Port</td>
<td>DST Port</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------</td>
<td>---------------------------------------------</td>
<td>-------</td>
<td>----------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>NTP</td>
<td>LAN1 on active node of Multi-Grid Master or LAN1 of a single appliance</td>
<td>NTP server</td>
<td>17 UDP</td>
<td>1024 → 65535</td>
<td>123</td>
<td>Required to synchronize Master Grid and TSIG authentication. Optional for synchronizing logs among multiple appliances</td>
</tr>
<tr>
<td>SMTP</td>
<td>LAN1, LAN2, or VIP</td>
<td>Mail server</td>
<td>6 TCP</td>
<td>1024 → 65535</td>
<td>25</td>
<td>Required if SMTP alerts are enabled</td>
</tr>
<tr>
<td>SNMP</td>
<td>NMS (network management system) server</td>
<td>VIP, LAN1, LAN2, or MGMT</td>
<td>17 UDP</td>
<td>1024 → 65535</td>
<td>161</td>
<td>Required for SNMP management</td>
</tr>
<tr>
<td>SNMP Traps</td>
<td>MGMT or VIP on Multi-Grid Master or HA pair</td>
<td>NMS server</td>
<td>17 UDP</td>
<td>1024 → 65535</td>
<td>162</td>
<td>Required for SNMP trap management. Uses MGMT (when enabled) or VIP on Multi-Grid Master or HA pair</td>
</tr>
<tr>
<td>SSHv2</td>
<td>Client</td>
<td>LAN1, LAN2, VIP, or MGMT on the appliance</td>
<td>6 TCP</td>
<td>1024 → 65535</td>
<td>22</td>
<td>Administrators can make an SSHv2 connection to the LAN1, LAN2, VIP, or MGMT port. Optional for management.</td>
</tr>
<tr>
<td>Syslog</td>
<td>LAN1, LAN2, or MGMT of the appliance</td>
<td>syslog server</td>
<td>17 UDP</td>
<td>1024 → 65535</td>
<td>514</td>
<td>Required for remote syslog logging</td>
</tr>
<tr>
<td>Traceroute</td>
<td>LAN1, LAN2, or UNIX-based appliance</td>
<td>VIP, LAN1, LAN2, or MGMT, or client</td>
<td>17 UDP</td>
<td>1024 → 65535</td>
<td>33000 → 65535</td>
<td>The appliance responds with ICMP type code 3 (port unreachable)</td>
</tr>
<tr>
<td>TFTP Data</td>
<td>LAN1 or MGMT</td>
<td>TFTP server</td>
<td>17 UDP</td>
<td>1024 → 65535</td>
<td>69, then 1024 → 63999</td>
<td>For contacting a TFTP server during database and configuration backup and restore operations</td>
</tr>
<tr>
<td>HTTP</td>
<td>Management System</td>
<td>VIP, LAN1, or MGMT</td>
<td>6 TCP</td>
<td>1024 → 65535</td>
<td>80</td>
<td>Required if the HTTP-redirect option is set on the Master Grid properties security page</td>
</tr>
<tr>
<td>HTTPS/SSL</td>
<td>Management System</td>
<td>VIP, LAN1, or MGMT</td>
<td>6 TCP</td>
<td>1024 → 65535</td>
<td>443</td>
<td>Required for administration through the GUI</td>
</tr>
</tbody>
</table>
Modifying Ethernet Port Settings

By default, the 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 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 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 appliance and on the switch to make 1000-Mbps full-duplex connections.

To change Ethernet port settings:

1. From the Master Grid tab, select the Members tab -> master_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 on page 183.

2. In the Network tab of the Master Grid Member Properties editor, the Required Ports and Addresses table lists the network settings that were configured.
   
   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. You cannot configure port settings for vNIOS appliances.

3. Save the configuration.

   Note: The port settings on the connecting switch must be identical to those you set on the appliance.

Using the LAN2 Port

The LAN2 port is a 10/100/1000Base-T Ethernet connector on the front panel of Infoblox-250-A, -550-A, -1050-A, -1550-A, -1552-A, -1852-A, and -2000-A, and -4010 appliances. The LAN2 port is not enabled by default. By default, an 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 Multi-Grid Master or 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 enable the NIC redundancy feature, which groups the LAN1 and LAN2 ports into one logical interface. The LAN1/LAN2 grouping can be activated for IPv4 only. Alternatively, you can configure the LAN2 port on a different IP network than LAN1, and enable the LAN2 port to provide other services. For information about these features, see the following sections:

- For information about the LAN2 failover feature, see About NIC Redundancy.
- For information about configuring the LAN2 port, see Configuring the LAN2 Port on page 183.

Note that you cannot use the LAN2 port to access the GUI and the API, or to connect to the Multi-Grid Master. This can impact the ability of other appliances to communicate with the Multi-Grid Master.

About NIC Redundancy

You can configure the LAN2 port to provide redundancy and additional fault tolerance in your network. NIC (Network Interface Controller) redundancy is transparently supported for IPv4. When you enable NIC redundancy, the LAN1 and LAN2 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 and LAN2 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. The other port becomes active only when the previously active port fails.

The LAN1 and LAN2 ports share the IP address of the LAN1 port; the port that is currently active owns the IP address. When you enable services on the appliance, clients send their service requests to the LAN1 port IP address and receive replies from it as well. The port supports the services and features supported on the LAN1 port as listed in Table 8.2 and Table 8.3.

As shown in Figure 8.5, the member is connected to the Multi-Grid Master through its MGMT port, 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 enable NIC redundancy on a single appliance. You cannot enable this feature on an HA pair.

Figure 8.5  Using the LAN2 Failover Feature

To enable the LAN2 port failover feature:

1. From the Master Grid tab, select the Members tab -> master_grid_member check box, and then click the Edit icon.

2. In the Network -> Basic tab of the Master Grid Member Properties editor, click the Add icon of the Additional Ports and Addresses table and select LAN2 (Failover).

   Multi-Grid Manager adds the LAN2 (Failover) entry to the table with the address information filled in. You cannot enter a separate IP address for the LAN2 port because the LAN1 and LAN2 ports share the IP address of the LAN1 port.

3. Save the configuration.

   The Detailed Status panel displays the status of both the LAN1 and LAN2 ports.
Configuring the LAN2 Port

You can configure both IPv4 and IPv6 addresses for the LAN2 port of an IPv4 and a dual mode (IPv4 and IPv6) Grid member.

To configure the LAN2 port:

1. From the Master Grid tab, select the Members tab -> master_grid_member check box, and then click the Edit icon.
2. In the Network -> Basic tab of the Master Grid Member Properties 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 or prefix length for IPv6 address. The prefix length ranges from 2 to 127.
   - Gateway: Type the default gateway for the LAN2 port.
   - 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 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.
   - LAN2 Virtual Router ID (if HA): If the appliance is in an HA pair, enter a VRID number.
3. Save the configuration.

Using the MGMT Port

The MGMT (Management) port is a 10/100/1000Base-T Ethernet connector on the front panel of an Infoblox-250-A, -550-A, -1050-A, -1550-A, -1552-A, -2000-A, and -4010 appliance. It allows you to isolate the following types of traffic from other types of traffic on the LAN and HA ports:

- Appliance Management on page 184
- Master Grid Communications on page 186

For information about what types of traffic qualify as appliance management and Master Grid communications, see Table 8.3 on page 178.

Note: The MGMT port currently does not support NTP, NAT, or TFTP.

Some 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 8.4 Supported MGMT Port Uses for Various appliance Configurations

<table>
<thead>
<tr>
<th>Appliance Configuration</th>
<th>Appliance Management</th>
<th>Master Grid Communications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Grid Master</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Multi-Grid Master Candidate</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>HA Master Grid Member</td>
<td>*</td>
<td>✓</td>
</tr>
<tr>
<td>Single Master Grid Member</td>
<td>*</td>
<td>✓</td>
</tr>
</tbody>
</table>
* Although you manage all Master Grid members through the Multi-Grid Master, if you enable the MGMT port on common Master 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 8.4 because it cannot provide redundancy through the use of a VIP. A Multi-Grid Master that is an HA pair needs the redundancy that a VIP interface on the HA port provides for Master Grid communications. Because the MGMT port does not support a VIP and thus cannot provide redundancy, Multi-Grid Masters (and potential Multi-Grid Masters) do not support Master Grid communications on the MGMT port.

The MGMT port is not enabled by default. By default, the 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 enable the MGMT port through the Infoblox GUI, as explained in the following sections.

**Appliance Management**

You can restrict administrative access to the 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 appliance through a dedicated switch (which is not connected to the rest of the network). *Figure 8.6* shows how an appliance separates appliance management traffic from network protocol services. Note that the LAN port is on a different subnet from the MGMT port.
Similarly, you can restrict management access to the Multi-Grid Master to only those members connected to the MGMT ports of the active and passive nodes of the Multi-Grid Master.

To enable the MGMT port on the Multi-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 Master Grid tab, select the Members tab -> master_grid_member check box, and then click the Edit icon.
2. In the Network -> Basic tab of the Master 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.

   Multi-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 Multi-Grid Master, and in the rows of the two nodes for an HA Multi-Grid Master:

   — **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 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.

5. In the Network -> Advanced tab, make sure that the Enable VPN on MGMT Port check box is not selected.
6. Save the configuration.
7. Log out of Multi-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 Multi-Grid Manager GUI is now accessible through the MGMT port on the 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 Multi-Grid Manager.
12. Check the Detailed Status panel of the Master Grid member to make sure the status icons are green.

Master Grid Communications

You can isolate all communications in the Master Grid to a dedicated subnet as follows:
- For Master Grid communications from the Multi-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 Multi-Grid Master can use its MGMT port for Master Grid communications. (This restriction applies equally to master candidates.)
- Master Grid members connect to the Multi-Grid Master through their MGMT ports.

This ensures that all database synchronization and Master Grid maintenance operations are inaccessible from other network elements while the Master Grid members provide network protocol services on their LAN ports. Figure 8.7 shows how members communicate with the Multi-Grid Master over a dedicated subnet.
The private network (10.1.1.0/24) is reserved for Master Grid communications between the Multi-Grid Master and all Master Grid members, and for appliance management between the management system and the Multi-Grid Master.

The Master Grid members connect to the private network through their MGMT ports*. They connect to the public network through their LAN and HA ports (using a VIP).

* Only the active node of an HA Master Grid member connects to the Multi-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 Master Grid before continuing Master Grid communications with the Multi-Grid Master on behalf of the HA Master Grid member.

The Multi-Grid Master and master candidate connect to the private network using a VIP on their HA ports.
Enabling Master Grid Communications over the MGMT Port for Existing Members

To enable the MGMT port for Master Grid communications on an existing single or HA Master Grid member:

1. Log in to the Multi-Grid Master with a superuser account.
2. From the Master Grid tab, select the Members tab -> master_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 on page 183.

3. In the Network -> Basic tab of the Master 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 and IPv6 addresses for the MGMT port. Multi-Grid Manager adds a row for the MGMT port. For an HA pair, it adds two rows, one for each node.
5. Enter the following in the row of the MGMT port for a single Multi-Grid Master or member, and in the rows of the two nodes for an HA Multi-Grid Master:
   - **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 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.
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.
   - **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 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.
8. Save the configuration.
   The master communicates the new port settings to the member, which immediately begins using them. The member stops using its LAN port for Master Grid communications and begins using the MGMT port.
9. To confirm that the member still has Master Grid connectivity, check that the status icons for that member are green.
### Setting Static Routes

When you put the 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 8.8 on page 189, the appliance is in the DMZ behind a firewall and connects to the rest of the network through the DMZ interface on the firewall.

**Figure 8.8 Single Default Route**

![Diagram of single default route]

The default route points all traffic from the LAN or LAN1 port on the appliance to the DMZ interface (1.2.2.1) on the firewall. The appliance responds to all queries from the Internet and internal network by sending its responses to the DMZ interface (1.2.2.1) on the firewall. The appliance only needs a single default route to the firewall. The firewall then routes the traffic where it needs to go.

When the 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 8.9.
To resolve the problem illustrated in Figure 8.9 on page 190, 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 8.10.

**Figure 8.10 Properly Routed Traffic**

The default route points all traffic from the appliance to the DMZ interface (1.2.2.1) on firewall-1.

**Default route:**
- **Network:** 0.0.0.0
- **Netmask:** 0.0.0.0
- **Gateway:** 1.2.2.1

Traffic from the Internet reach the appliance through firewall-1, and the appliance sends its replies back through firewall-1.

Traffic from the internal network reach the appliance through firewall-2, but because there is only one default route, the appliance erroneously sends information to the DMZ interface (1.2.2.1) on firewall-1.

A second route on the appliance points traffic destined for 10.1.1.0/24 to the DMZ interface (1.2.2.2) on firewall-2.

**Route to:**
- **Network:** 10.1.1.0
- **Netmask:** 255.255.255.0
- **Gateway:** 1.2.2.2
 Whenever you want the 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 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 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 appliance uses the MGMT port when directing traffic to that gateway.

**Figure 8.11 Static Routes for the LAN and MGMT Ports**

![Diagram showing static routes](image)

The need for routes can apply to any type of traffic that originates from the appliance, such as SNMP traps, ICMP echo replies, Infoblox GUI management, and Master 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**

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 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.
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 the Master Grid:

1. **Multi-Grid Master:** From the Master Grid tab, click **Master Grid Properties** → **Edit** from the Toolbar.
   
   **Member:** From the Master Grid tab, select the Members tab → `master_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 **Master Grid Properties** or **Master Grid Member Properties** editor, select the **DNS Resolver** tab, and then enter the following:
   
   — **Enable DNS Resolver:** Select the check box to enable the 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 of the servers to which the appliance sends queries. The appliance attempts 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 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 “corp100.com” and “hq.corp100.com” in the domain group list, then the appliance sends a query for “as1.corp100.com” and another query for “as1.hq.corp100.com” to the preferred or alternate name server.
     
     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.**
Managing Master Grid Operations

Managing Licenses

Licenses come pre-installed on the appliance according to the software packages you ordered at the time of purchase. If you wish to upgrade an existing appliance with the Multi-Grid Management license, you must contact Infoblox Technical Support and follow the procedures in Viewing Licenses on page 195.

On a vNIOS virtual appliance, you can install licenses when you deploy the appliance. You must install both the Multi-Grid Management and vNIOS licenses on a vNIOS appliance. You can transfer the valid licenses of a vNIOS appliance on VMware from one ESX/ESXi server to another. For more information, refer to the Infoblox Installation Guide for vNIOS Software on VMware.

There are three types of licenses:

- **Maintenance licenses** – Examples: Grid (or Keystone) maintenance licenses. The duration of maintenance licenses are one, two, or three years. You can obtain these licenses from your Infoblox sales representative.
- **Service licenses** – Examples: Multi-Grid Management licenses. These are permanent licenses. You can obtain these licenses from your Infoblox sales representative.
- **Temporary licenses** – You can enable temporary licenses through the CLI command `set temp_license`.

Before a maintenance license or a temporary license expires, 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 Infoblox Technical Support.

Obtaining and Adding Licenses

A valid Multi-Grid Management license is required for deploying a Master Grid. You can upgrade existing NIOS and vNIOS appliances to use a Multi-Grid Management license. To upgrade your licenses, contact Infoblox Technical Support.

When you receive a new license key, it is in CSV (comma separated values) format with the following information: serial number, hardware ID, license type, end date, and license string. You can either upload the file to the appliance or copy the information and paste it in the text field of the Licenses tab of the Infoblox GUI. Note that you must copy the entire string—serial number, hardware ID, license type, end date, and license string—and save it to the text field.

To add a license:

1. From the Master Grid tab, select the Licenses tab and click the Add icon.
2. Do one of the following:
   - **Upload License File**: Click Select File and navigate to the license file.
   - **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.
Obtaining 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 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 the Master Grid, you must log in to the Multi-Grid Master to view license information from Multi-Grid Manager. If you have transferred licenses from one vNIOS on VMware appliance to another, you can view information about the new and replaced licenses.

In this panel, 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 on page 34.

To view license information:
1. Log in to Multi-Grid Manager on the Multi-Grid Master.
2. Select the Master Grid tab -> Licenses tab. The appliance displays the following information:
   - **Name**: The name of the appliance.
   - **HA**: Indicates whether the appliance is an HA pair.
   - **Address**: The IP address of the appliance.
   - **Hardware ID**: The unique hardware ID of the appliance. The ID is highlighted in red if the license on the appliance was removed.
   - **Type**: The type of license installed.
   - **Type Context**: Depending on the license type, this field is blank or displays the attribute Model, which indicates that the vNIOS license supports a specific vNIOS virtual appliance model. The model supported is displayed in the Type Details field. This field is blank if the license does not control any attribute type.
   - **Type Details**: Information about the attribute that the license monitors. This field can display the model of the vNIOS virtual appliance, such as IB-VM-550 or IB-VM-1050.
   - **Expiration**: The expiration date of the license.
   - **Replaced Hardware ID**: The hardware ID of the appliance whose license was removed.
Back Up Licenses

You can back up the licenses installed on the appliance, in case you need to re-install them at a later time. Infoblox recommends backing up the licenses before removing any of them.

When you back up the licenses, Multi-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 the Backup Licenses icon in the toolbar.
   Multi-Grid Manager generates a CSV file that contains all the licenses. You can then open the file or save it to a specified location.

Remove Licenses

You can remove licenses and reset the appliance to its factory default settings. For example, if you have an appliance running the DNSone package with the Grid upgrade, but you want to use it as a Multi-Grid Master, 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.

this should be used with great caution as it can render an appliance unusable if the wrong license is removed

To remove a license:
1. From the Master Grid tab, select the Licenses tab.
2. Select the license and click the Delete icon.
   Check the license that you are about to remove. Note that removing the wrong license can render an appliance unusable.
3. Click Yes when the confirmation dialog appears.
4. Close the browser window and log in to the Infoblox GUI.

Shutting Down, Rebooting, and Resetting

To reboot and shut down an appliance, you can use Multi-Grid Manager or the Infoblox CLI. To reset an appliance, you must use the Infoblox CLI.

Rebooting an Appliance

You can reboot a single appliance, a single node in an HA pair, or both nodes in an HA pair.

To reboot an appliance:
1. From the Master Grid tab, select the Members tab -> master_grid_member check box.
2. Click Control -> Reboot from the Toolbar.
   — For an HA pair, choose whether to boot one node (and which one) or both nodes, and then click OK.
Depending on the browser you use, Multi-Grid Manager may display a dialog box that indicates the system is unavailable during a restart or reboot.

To reboot a single appliance using the CLI:
1. Log in to the Infoblox CLI using a superuser account for the appliance that you intend to reboot.
2. Enter the following CLI command: reboot
Shutting Down an Appliance

Under normal circumstances, you do not need to turn off or shut down an appliance. It is designed to operate continuously. However, if you want to turn off an appliance, use the GUI or the CLI to shut down the appliance, instead of just turning off the power switch. Before shutting down a remote appliance, make sure you can restart it. You cannot restart the system using the GUI.

**Note:** If there is a disruption in power when the appliance is operating, the appliance automatically reboots itself when power is restored.

To shut down an appliance:
1. From the Master Grid tab, select the Members tab -> master_grid_member check box.
2. Click Control -> Shutdown from the Toolbar.
   - For an HA pair, choose whether to shut down one node (and which one) or both nodes, and then click OK.
   
   The appliance shuts down. The fans might continue to operate until the appliance cools down.

To shut down an appliance using the CLI:
1. Log in to the Infoblox CLI using a superuser account.
2. Enter the following CLI command: `shutdown`

Resetting an Appliance

There are three ways to reset an appliance:
- **Resetting the Database** on page 197
- **Resetting an Appliance to Factory Settings** on page 198
- **Resetting an Appliance to Factory Settings and Removing Licenses** on page 198

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 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.corp100.com
   Remote Console Access: true
   The entire database will be erased.

   Do you wish to preserve basic network settings? (y or n)

3. 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 an Appliance to Factory Settings

You can reset the 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 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 an Appliance to Factory Settings and Removing Licenses

You can also reset the 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 appliance regenerates the certificates and replaces them.

To reset the 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-2000-A and -4010

Among its many features, the Infoblox-2000-A and 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 on page 202.

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 8.12. 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 8.12  RAID 10 Array Configuration

When evaluating a fault on the Infoblox-2000-A and -4010, it is best to think of the disk subsystem as a single, integrated unit with four components, rather than four independent disk drives. For information, see Evaluating the Status of the Disk Subsystem on page 200.
Evaluating the Status of the Disk Subsystem

You can monitor the disk subsystem through Multi-Grid Manager, 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-2000-A or -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

RAID_ARRAY: OPTIMAL
RAID_BATTERY: OK READY Yes 103 HOURS
```

The `Detailed Status` panel provides a detailed status report on the appliance and service operations. To see a detailed status report:

- From the `Master Grid` tab, select the `Members` tab -> `master_grid_member` check box -> Detailed Status icon in the table toolbar.

The RAID icons indicate the status of the RAID array on the Infoblox-2000-A and -4010.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="green.png" alt="Green" /></td>
<td>Green</td>
<td>The RAID array is in an optimal state.</td>
</tr>
<tr>
<td><img src="yellow.png" alt="Yellow" /></td>
<td>Yellow</td>
<td>A new disk was inserted and the RAID array is rebuilding.</td>
</tr>
<tr>
<td><img src="red.png" alt="Red" /></td>
<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>
</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. The disk type of the Infoblox-2000-A can be one of the following:

- IB-Type 1: Infoblox supported disk type
- IB-Type 2: Infoblox supported disk type
- Unk: Unknown disk type that Infoblox does not support

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 the disk type 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-2000-A are located on the right side of the appliance front panel. To the right of each drive, there is an LED that displays the status of each drive. The front panel LCD scrolls and displays the disk array status every 20 seconds. *Table 8.5* lists the disk drive LEDs.

*Table 8.5  Infoblox-2000-A Disk Drive LEDs*

<table>
<thead>
<tr>
<th>LED Color</th>
<th>Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Disk operating normally</td>
<td>None</td>
</tr>
<tr>
<td>Yellow</td>
<td>Disk read/write activity</td>
<td>Disk is functioning normally or is synchronizing if recently inserted.</td>
</tr>
<tr>
<td>Dark</td>
<td>Disk has failed or not inserted</td>
<td>Verify the failure in the GUI or CLI. Remove the disk and replace with a functional disk drive. Note that the drive rebuilds with its twin.</td>
</tr>
</tbody>
</table>

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 8.6* lists the disk drive LED combinations and the states they represent.

*Table 8.6  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>On</td>
<td>Off</td>
<td>The drive is online but it is not currently active.</td>
</tr>
<tr>
<td>Blinking regularly</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-2000-A and -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 Multi-Grid Manager, front panel LCD, or CLI.
2. If the activity light is green or blinking yellow, make sure you have identified the correct drive. There are conditions where a drive could be in the process of failing and still be green or yellow.

   **Note:** Do not remove a correctly functioning drive.

3. Push in the latch for the drive and pull the release lever out towards you.
4. When the drive disengages, wait about 30 seconds for the disk to completely stop spinning.
5. Slide it out of the slot.

Replacement drives are shipped as a complete unit, ready to insert into the appliance. There is no preparation required. To install a replacement drive, follow this procedure:

1. Insert the replacement drive into the drive bay slot.
2. 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.
3. 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.
4. 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 observe the following guidelines:

- Remove only one disk at a time. Do not remove two or more disks from the appliance at the same time. Removing two or more disks at the same time might result in an appliance failure and require an RMA of the appliance. This rule applies to both powered and powered down appliances.
- If the status of the array is degraded, remove the failed or failing disk drive only. Do not remove an optimally functioning drive.
- If your acceptance procedure requires a test of the RAID hot swap feature, remove only one disk drive at a time. You can remove a second disk only after you replace the first disk and the array completes its rebuilding process.
- Do not remove a disk drive if the array is rebuilding. This could result in an appliance failure. Verify the status of the array before removing a disk drive.
- Use the following procedure to remove a spinning disk:
  1. Unlatch and pull the disk about two cm (one inch) to disengage contact.
  2. Wait about 30 seconds for the disk to completely stop spinning.
  3. Remove the disk and handle it with care. Do not drop the disk or ship it loosely in a carton.
- You can hot swap a drive while the appliance remains in production.
• There are some conditions that may require powering down the appliance to replace a failed unit. This normally happens if the RAID controller detects an error that could damage the array. If you insert a replacement drive into a live array and the controller doesn't recognize the drive, power down the appliance.

• If you inadvertently remove the wrong disk drive, do not immediately remove the disk drive that you originally intended to remove. Verify the status of the array and replace the disk drive that you removed earlier before removing another drive. Removing a second drive could render the appliance inoperable.

• Older appliances have an audio alarm buzzer that sounds if a drive fails. The alarm automatically stops about 20 seconds after a functional disk has been inserted into the array.

• All disks in the RAID array should have the same disk type for the array to function properly.

• In the unlikely event that two disk drives fail simultaneously and the appliance is still operational, remove and replace the failed disk drives one at a time.

• Rebuild time depends on a number of factors, such as the system load and Master Grid replication activities. On very busy appliances (over 90% utilization), the disk rebuild process can take as long as 40 hours. On a Multi-Grid Master serving a very large Master Grid, expect the rebuild process to take at least 24 hours.

• Replace a failed or mismatched disk only with a replacement disk shipped from Infoblox. When you request a replacement disk, report the disk type displayed in the Detailed Status panel of the GUI or the Infoblox part number on the disk.
Chapter 9  Managing Software and Configuration Files

This chapter explains how to manage upgrade groups and perform software upgrades and downgrades for the Master Grid. It also describes how to back up and restore configuration files. It includes the following sections:

- Managing Upgrade Groups  on page 206
  - Adding Upgrade Groups  on page 206
  - Modifying Upgrade Groups  on page 207
  - Viewing Upgrade Groups  on page 207
  - Deleting Upgrade Groups  on page 208
- Viewing Software Versions  on page 208
- Upgrading Software  on page 209
  - Lite Upgrades  on page 209
  - Uploading Software  on page 209
  - Distributing Software Upgrade Files  on page 210
  - Managing Distributions  on page 212
  - Testing Software Upgrades  on page 213
  - Performing Software Upgrades  on page 213
  - Monitoring Distribution and Upgrade Status  on page 217
- Reverting to the Previously Running Software Version  on page 219
- Backing Up and Restoring Configuration Files  on page 219
  - Backing Up Files  on page 219
  - Automatically Backing Up Data Files  on page 220
  - Manually Backing Up Data Files  on page 222
  - Downloading Backup Files  on page 222
  - Restoring Backup Files  on page 223
  - Downloading Backup Files from a Different Appliance  on page 224
- Downloading Support Bundles  on page 225
Managing Software and Configuration Files

Managing Upgrade Groups

To minimize the impact of Master Grid upgrades on your system operations, you can organize Master Grid members into upgrade groups and schedule their software distributions. This is useful, for example, in a large Master Grid spanning multiple time zones where there are fluctuating network and downtime considerations at the various locations. Note that you can also schedule their upgrades if the software upgrade is an Upgrade Lite compatible release. For information, see Lite Upgrades on page 209.

Infoblox provides two default upgrade groups:

- **Grid Master** — After you configure the Multi-Grid Master, it automatically becomes the only member of this group. You cannot modify or delete this group.
- **Default** — This is the default upgrade group to which the appliance automatically assigns Master 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 on page 207.

Multi-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 Master Grid and on individual Master Grid 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 on page 207.
- View upgrade group information, as described in Viewing Upgrade Groups on page 207.
- Delete an upgrade group, as described in Deleting Upgrade Groups on page 208.

Adding Upgrade Groups

When you create an upgrade group, you select the Master 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 Master Grid member can belong to only one upgrade group.

To add an upgrade group:

1. From the Master 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 Multi-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. Multi-Grid Manager adds a row to the Member Assignment table.
— Click **Select**. In the *Member Selector* dialog box, select the Master Grid 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 Master Grid member in the list determines the time zone of the group when you schedule the distribution and upgrade. Therefore, Multi-Grid Manager displays the time zone of the first Master Grid member in the list. (For information about setting time zones, see *Setting Your User Profile* on page 27.)

5. Save the configuration.

**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 **Master 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* on page 206.
   — **Member Assignment**: Add or delete members as described in *Adding Upgrade Groups* on page 206.
4. Save the configuration.

**Viewing Upgrade Groups**

In the **Upgrade** tab, Multi-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 Master Grid 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* on page 212.) 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* on page 212.

To view the upgrade groups in the Master Grid:

1. From the **Master Grid** tab, select the **Upgrade** tab, and then click **Toggle Group List View**.
   Multi-Grid Manager displays the Multi-Grid-Master at the top of the list. All other upgrade groups are listed alphabetically after the Multi-Grid-Master. You can click the arrow next to a group to view members in the group.
2. Multi-Grid Manager displays the following:
   — **Member**: The name of the member.
   — **Group**: The name of the upgrade group to which the member belongs.
   — **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.
Managing Software and Configuration Files

— **IP Address**: The IP address of the member.
— **Running Version**: The 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* on page 34.

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. Multi-Grid Manager displays a warning before deleting an upgrade group.

To delete an upgrade group:
1. From the **Master 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 software version, you can view the current software version that is running on the Master Grid, the image you have uploaded, and the available version to which you can revert. Multi-Grid Manager displays the software information in the **Upgrade** tab.

To view software information:
1. From the **Master Grid** tab, select the **Upgrade** tab.
2. Multi-Grid Manager displays the following in the Grid Version Information section:
   — **Running**: The software version that is currently running on the Master Grid.
   — **Uploaded**: The latest image file you have uploaded and is available for distribution.
   — **Distribution**: The software version used for distribution or is available for distribution.
   — **Revert**: The 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**: Multi-Grid Manager leaves a field empty when there is no available software for the specific function.

Multi-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 Software

Infoblox frequently releases updated 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 a Master Grid.

- Upload the new software to the Multi-Grid Master, as described in Uploading Software.
- Distribute the software upgrade files, as described in Distributing Software Upgrade Files on page 210.
- Optionally, test the upgrade, as described in Testing Software Upgrades on page 213.
- Perform the software upgrade, as described in Performing Software Upgrades on page 213.

Before upgrading, Infoblox recommends that all Master Grid members in the Master Grid be connected to the network and operating normally. If one or more members are offline when you upgrade the Master Grid, they automatically receive the distributed software and upgrade when they join the Master Grid or come back online.

Before you upgrade to a later release, use the `show upgrade_compatible` command to check if your Master 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.

Lite Upgrades

Whenever possible, the appliance uses the lite upgrade mode to speed up the upgrade process. A lite upgrade occurs when there are incremental changes to the 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 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. You can schedule a lite upgrade, but you cannot test a lite upgrade. The appliance disables the testing function for lite upgrades.

Uploading Software

After you download the software upgrade to your management station, upload it to the Multi-Grid Master, as follows:

1. From the Master 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 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 software upgrade to an HA Multi-Grid Master, only the active node receives the software. The passive node does not. Therefore, if the Multi-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 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 Master 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 Multi-Grid Master distributes the software upgrade to each member in the Master Grid, including itself. As an alternative to scheduling the Master Grid distribution (see Scheduling Distributions on page 210), you can distribute the software upgrade throughout the Master Grid immediately, as follows:

1. From the Master 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 on page 212.

Note that starting a manual distribution cancels a scheduled distribution.

Scheduling Distributions

When you schedule a distribution, you schedule the distribution of the Multi-Grid Master as well as the upgrade groups, including the Default group. The Multi-Grid Master distribution must always occur before the distribution of the upgrade groups.

To schedule a software distribution:

1. From the Master 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 it 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 Multi-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 Multi-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 Multi-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 Master Grid time zone, the appliance converts the time you enter here based on the Master 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 Master Grid. (For information about selecting the Master Grid and member time zones, see Managing Time Settings on page 155.)

      — Admin Local Time: Displays the Multi-Grid Master distribution start date and time in the time zone of the administrator, as explained in Creating Local Admins on page 80.
— 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 groups**: Select After Grid Master to start the distribution immediately after the completion of the Multi-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 Master 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 Master Grid and member time zones, see Managing Time Settings on page 155.) 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 on page 206.
  — **Admin Local Time**: Displays the start date and time in the time zone of the administrator, as explained in Creating Local Admins on page 80.
  — **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 on page 207.

3. Save the configuration.
   Multi-Grid Manager confirms that the schedule is saved and indicates whether the distribution schedule is active.

   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 Master Grid distribution starts:

- The appliance checks if a 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 Multi-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 Multi-Grid Master, it is the active node that uploads the file to a backup partition and unpacks the contents.
  — The Multi-Grid Master (or active node of the HA Multi-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 Multi-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 Multi-Grid Master.
  — After the active node of an HA member receives the software, it then distributes it to the passive node.
Managing Distributions

After you start a distribution, you can pause, resume, or stop it. For information, see Pausing and Resuming Distributions on page 212 and Stopping Distributions on page 212. Multi-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.

To skip a member from a distribution:
1. From the Master 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. Multi-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 Multi-Grid Master has completed its distribution, you can upgrade the Master Grid immediately. This forces members that do not have a complete distribution to synchronize their releases with the Multi-Grid Master.
- If the Multi-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 Master Grid upgrade starts as scheduled, as long as the Multi-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 Multi-Grid Master, you can test an upgrade on the Multi-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 version and the software upgrade. The test does not affect services and you can perform other administrative tasks during the upgrade test.

To start an upgrade test:

• From the Master 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 or reboots the Multi-Grid Master, or if an HA failover occurs on the Multi-Grid Master during the upgrade test, the appliance automatically stops the test. The appliance always resets the status of the Master 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 on page 213.

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 on page 219.

When upgrading to software releases that are Upgrade Lite compatible, you can schedule the Master Grid upgrade as described in Scheduling Upgrades on page 214.

Upgrading Immediately

You cannot schedule upgrades to releases that are not Upgrade Lite compatible. The Master Grid members must upgrade at the same time when upgrading to these releases. For Upgrade Lite compatible releases, you can schedule the upgrade as described in Scheduling Upgrades on page 214, or upgrade the Master Grid at the same time.

To upgrade a Master Grid immediately:

• From the Master Grid tab, select the Upgrade tab, and then click Upgrade -> Upgrade Now from the Toolbar. The Master Grid upgrades immediately and if there is an active upgrade schedule, it becomes inactive.
Managing Software and Configuration Files

Scheduling Upgrades

When you schedule the upgrade of a Master Grid to an Upgrade Lite compatible release, you schedule the upgrade for the Multi-Grid Master and the upgrade groups, including the Default group. The Multi-Grid Master must always upgrade before the upgrade groups. To schedule an upgrade:

1. From the Master 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 Multi-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 Multi-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 Multi-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 Master Grid time zone, the appliance converts the time you enter here based on the Master 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 Master Grid. (For information about setting the Master Grid and member time zones, see Managing Time Settings on page 155.)
     - **Admin Local Time**: Displays the Multi-Grid Master upgrade date and start time in the time zone of the administrator, as explained in Creating Local Admins on page 80.
   - In the upgrade group table, specify the following for each upgrade group by clicking the corresponding field in each row:
     - **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 Multi-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.
     - **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 Master 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 Master Grid and member time zones, see Managing Time Settings on page 155.) 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 on page 206.
     - **Admin Local Time**: Displays the data and time in the time zone of the administrator, as explained in Creating Local Admins on page 80.
   - **Distribute to 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 on page 207.
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.

Otherwise, the appliance confirms that the schedule is saved and indicates whether the upgrade schedule is active.

**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 Master 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.

Multi-Grid Manager immediately upgrades the selected group.

**Upgrade Process**

When an upgrade starts, Multi-Grid Manager checks if the nodes of an HA Multi-Grid Master have the same software version on their alternate partitions. If they do not have the same software version, the upgrade process stops. Multi-Grid Manager displays an error message and if it is a scheduled upgrade, Multi-Grid Manager deactivates the schedule as well. Otherwise, the upgrade process continues. During the upgrade, if a Master Grid member has not completed its distribution, it automatically resynchronizes with the Multi-Grid Master after the Multi-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 Master Grid members upgrade, including when HA pairs fail over, is shown in *Figure 9.2* (for an HA Multi-Grid Master) and *Figure 9.2* on page 217 (for a single Multi-Grid Master).
Figure 9.1 Upgrade Sequence for an HA Multi-Grid-Master and Members

1. The passive node (Node 2) of the Multi-Grid Master upgrades.
2. The Multi-Grid Master fails over from Node 1 to Node 2. At this point, the active Multi-Grid Master (Node 2) is using the upgraded code. All other nodes, including the passive node (Node 1) and all Master Grid members, rejoin the newly updated active node (Node 2). Since the version on these nodes does not match that of the active Multi-Grid Master, the nodes are directed to
3. Node 1 (now passive) of the Multi-Grid Master upgrades. The passive node (Node 2) of the HA member and the single Master Grid member upgrade.
4. The HA Master Grid member fail overs from Node 1 to Node 2.
5. Node 1 (now passive) of the HA member upgrades.

Note: Master Grid members that do not have the correct version on their alternate partitions due to an incomplete distribution automatically resynchronize the version with the Multi-Grid Master, and then upgrade.
The Multi-Grid Manager session terminates when the HA Multi-Grid Master fails over from Node 1 to Node 2, or when the single Multi-Grid Master reboots and goes offline.

During a scheduled upgrade, the Master Grid members that have not upgraded yet can join the Master Grid and function normally until their scheduled upgrade time. When the upgrade finishes, the upgrade schedule is set to inactive.

**Monitoring Distribution and Upgrade Status**

During a distribution or an upgrade, Multi-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 Master Grid tab -> Upgrade tab.

When you perform a distribution or an upgrade, the status bar displays the overall Master 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 Multi-Grid Manager session terminates when an HA Multi-Grid Master fails over from Node 1 to Node 2, or when a single Multi-Grid Master reboots and goes offline. You can log back in to the appliance after the upgrade.

**Master Grid and Member Status**

You can view the distribution and upgrade process status at the Master Grid and member level. To view the process status, from the Master Grid tab, select the Upgrade tab, and then click Toggle Member List View.

The status bar displays the status of the overall Master 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.

Multi-Grid Manager displays the following information for each member:

- **Member:** The name of the Master 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).
• **IP Address:** The IP address of the member.
• **Running Version:** The software version that is currently running on the member.
• **Alternate Version:** Displays the 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, Multi-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.
• **Timestamp:** The date, time, and time zone of the status displayed.
• **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 Master Grid tab, select the Upgrade tab, and then click Toggle Group List View. Multi-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 Master Grid member.
- **Status:** The current member status. This can be Running (green) or Offline (red).
- **IP Address:** The IP address of the member appliance.
- **Running Version:** The software version that is currently running on the member.
- **Distribution Status:** The current distribution status. For an upgrade group, Multi-Grid Manager displays a progress bar to indicate the overall percentage of completion. For a member, Multi-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 Master Grid tab, select the Upgrade tab, and then click Toggle Member List View.
2. Select a member and then click the Detailed Status icon.

Multi-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; Multi-Grid Manager displays a description of the problem.
- **Yellow:** A warning message.

When the selected Master Grid member is an HA pair, Multi-Grid Manager displays the status information for both nodes. The panel remains open until you close it or select a different member.
Reverting to the Previously Running Software Version

You can revert to a version of software that was previously running on your appliance. The 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 Master Grid tab, select the Upgrade tab. Note that once you start distributing a new version after an upgrade, you cannot revert to a previous version.

Be aware that when you revert to this software, changes made since the Master Grid was last upgraded are lost.

To revert to a version of software previously running on a the Master Grid:

- From the Master Grid tab, select the Upgrade tab, and then click Revert from the Toolbar.

  Multi-Grid Manager displays a warning indicating that the revert process disrupts Master Grid services. Read the warning carefully, and then click Yes to confirm your decision to revert.

Backing Up and Restoring Configuration 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. You can also download a backup file to your workstation. The backup file is a .bak file that contains the configuration settings, data set, and TFTP files.

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 on page 220
- Manually Backing Up Data Files on page 222
- Restoring Backup Files on page 223
- Downloading Backup Files from a Different Appliance on page 224

Note: Infoblox highly recommends that you always back up the current configuration file before upgrading, restoring, or reverting the software on the appliance.

Backing Up Files

You can back up system files 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 on page 223. 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 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.
Managing Software and Configuration 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: Infoblox_year_month_day_time. For example, a file name of Infoblox_2008_11_30_23_00 means that the file is backed up on November 30th, 2008 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 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. 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.

Automatically Backing Up Data Files

Infoblox recommends that you back up your configuration files regularly, and the easiest way to accomplish this task is to configure the appliance to back up the configuration file automatically. You can choose when and how often files are backed up: weekly, daily, or hourly. When you automatically back up a configuration file on the appliance, the file is named in the format Infoblox_year_month_day_time. The default time for an automatic backup is 3:00 AM. Configuration files should be backed up during the slowest period of network activity.

To automatically back up a database file on the Multi-Grid Master or member:

1. From the Master Grid tab, select the Members 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.
   - 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` on a Linux system, or `c:\archive\backups` on a Microsoft Windows system. 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 Multi-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 Multi-Grid Master creates a backup file. For example, enter 5 if you want the Multi-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.
  - **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` on a Linux system, or `c:\archive\backups` on a Microsoft Windows system. 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.
  - **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.
  - **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` on a Linux system, or `c:\archive\backups` on a Microsoft Windows system. 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.
  - **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.

— **Multi-Grid Master (Local):** Back up to a local directory on the Multi-Grid Master. This is the default.

By default, the Multi-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 Master Grid and saving it locally on an hourly basis increases the turnover of files stored on the Multi-Grid Master. Backing it up hourly to a remote server increases the overall amount of traffic on your network.

3. Save the configuration.

### Manually Backing Up Data Files

You can manually back up a data file in addition to scheduling your backups.

To back up manually:

1. From the **Master Grid** tab, select the **Members** 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` on a Linux server, or `c:\archive\backups\Infoblox_2009_10_20_15_30` on a Microsoft Windows server.
     - **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` on a Linux server, or `c:\archive\backups\Infoblox_2009_10_20_15_30` on a Microsoft Windows server.
     - **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 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` on a Linux server, or `c:\archive\backups\Infoblox_2009_10_20_15_30` on a Microsoft Windows server.
     - **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.

3. 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 **Master Grid** tab, select the **Members** tab, and then click **Backup -> Manage Local Backup** from the Toolbar. Multi-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/backups/Infoblox_2009_10_20_15_30` on a Linux server, or `c:\archive\backups\Infoblox_2009_10_20_15_30` on a Microsoft Windows server.
   — **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/backups/Infoblox_2009_10_20_15_30` on a Linux server, or `c:\archive\backups\Infoblox_2009_10_20_15_30` on a Microsoft Windows server.
   — **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/backups/Infoblox_2009_10_20_15_30` on a Linux server, or `c:\archive\backups\Infoblox_2009_10_20_15_30` on a Microsoft Windows server.
   — **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 to an appliance running the same version as that of the appliance from which the backup file originates. You can also restore a backup file from an appliance running one version to an appliance running a later version, as long as the upgrade from the earlier version to the later version is supported.

**Note:** You cannot attach a Grid when you restore a backup file of earlier version to a Grid that is detached from Multi-Grid Master. Join the Grid again to perform the attach operation. For more information, see **Attaching a Grid Immediately** on page 125.

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** on page 224.

You must log in with a superuser account to back up and restore files.

There are 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.

To restore a backup file to the same appliance:

1. From the **Master Grid** tab, select the **Members** 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.
Managing Software and Configuration Files

- **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` on a Linux server, or `c:\archive\backups\Infoblox_2009_10_20_15_30` on a Microsoft Windows server.
  - **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` on a Linux server, or `c:\archive\backups\Infoblox_2009_10_20_15_30` on a Microsoft Windows server.
  - **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.

- **Multi-Grid Master (Local)**: Restore from a local directory on the Multi-Grid Master. In the Backup Set table, select the file you want to restore.

3. 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.

4. Close your current browser window, wait a few minutes, and then reconnect to the appliance.

### Downloading Backup Files from a Different Appliance

When you “force restore” an appliance, you download a backup file from one appliance to a different appliance. In a Master Grid, you can download the backup file from the Multi-Grid Master and “force restore” it to a different appliance. This is useful when you want to replace an appliance that may have operational issues, or to test or troubleshoot issues.

For example, you can force restore the backup file of a Multi-Grid Master that is in one environment, such as a production environment, to an appliance in another environment, such as a lab or test environment, for troubleshooting purposes. Note, though, that if a master candidate promotion occurs in the lab, the newly promoted Multi-Grid Master will try to contact the managed Grids in the production environment. The managed Grids could then start synchronizing their data to the newly promoted Multi-Grid Master in the lab, and stop synchronizing with the Multi-Grid Master in the production environment.

To avoid this, remove the managed Grids from the lab Master Grid immediately after you force restore the backup file of the Multi-Grid Master to the appliance in the lab. Then if the appliance is promoted to Multi-Grid Master, it will not try to synchronize with the Grids in the production environment.

To restore a backup file to the same appliance or Multi-Grid Master, use the Restore function as described in Restoring Backup Files on page 223.

To download a backup file from one appliance to a different appliance:

1. From the **Master Grid** tab, select the **Members** 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 on page 223.

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 appliance.
**Downloading Support Bundles**

When you need assistance troubleshooting an 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 each member in the Master 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.

To download a support bundle:

1. From the **Master Grid** tab, select the **Members** tab -> **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.

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 10 Monitoring the Master Grid

This chapter describes the status icons that indicate the state of the Multi-Grid Master and members, database capacity, Ethernet ports, and HA replication. It also explains how to use the various logs and the traffic capture tool to monitor the Master Grid members.

This chapter contains the following sections:

- **Viewing Master Grid Status** on page 228
  - **Device Status** on page 228
  - **Disk Usage** on page 229
  - **CPU Usage** on page 229
  - **LAN1/LAN2 Ports, HA Port, and MGMT Port** on page 229
  - **Memory Usage** on page 230
  - **NTP Synchronization** on page 230
  - **Power Supply** on page 231
  - **Replication** on page 231
  - **RAID** on page 232
  - **RAID Battery** on page 232
  - **Viewing Hardware Status** on page 233

- **Using a Syslog Server** on page 234
  - **Specifying Syslog Servers** on page 234
  - **Configuring Syslog for Master Grid Members** on page 235
  - **Viewing the Syslog** on page 236
  - **Searching in the Syslog** on page 236
  - **Downloading the Syslog File** on page 237

- **Monitoring Tools** on page 237
  - **Using the Audit Log** on page 237
  - **Viewing the Replication Status** on page 239
  - **Using the Traffic Capture Tool** on page 240
  - **Using the Capacity Report** on page 241
  - **Using the Phone Home Feature** on page 241
Monitoring the Master Grid

Viewing Master Grid Status

You can monitor the overall status, such as the Multi-Grid management service and memory usage of the Master Grid, using the Master Grid Member Status widget on the Dashboard. For information, see About the Dashboard on page 50.

You can also view the status of the Master Grid members from the Master Grid tab. To view the Master Grid member status, from the Master Grid tab, select the Members tab. Multi-Grid Manager displays information about the Multi-Grid Master and members. When all the Master Grid members are running properly, the status is green.

Multi-Grid Manager can display the following information:

- **Name**: The name of the Multi-Grid Master or member.
- **HA**: Indicates whether the member is an HA pair. If the member is an HA pair, Multi-Grid Manager displays the status of the HA pair.
- **Status**: The current status of the member.
- **IPv4 Address**: The IP address of the appliance, or the VIP of an HA pair.
- **Hardware Type**: The hardware type of the member appliance.
- **Serial Number**: The serial number of the appliance.
- **DB Utilization**: The percentage of the database that is currently in use.
- **Comments**: Information about the member.
- **Site**: The location to which the member belongs. This is one of the predefined extensible attributes.

To view detailed status, select a member check box, and then click the Detailed Status icon. Multi-Grid Manager displays the Detailed Status panel. If the selected member is an HA pair, Multi-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.

For information about detailed status of the managed Grids, see Monitoring Grids on page 128.

Device Status

The status icon indicates the operational status of the Master 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>🟢</td>
<td>Green</td>
<td>The appliance is operating normally in a “Running” state.</td>
</tr>
<tr>
<td>🟠</td>
<td>Yellow</td>
<td>The appliance is connecting or synchronizing with its Multi-Grid Master.</td>
</tr>
<tr>
<td>🔴</td>
<td>Red</td>
<td>The appliance is offline, is not licensed, is upgrading or downgrading, or is shutting down.</td>
</tr>
</tbody>
</table>

The following are descriptions that may appear: Running, Offline, Error, and Warning.
CPU Usage

Multi-Grid Manager displays the current percentage of the CPU usage on the selected Master Grid member. The maximum is 100%. 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>Under 90% capacity</td>
</tr>
<tr>
<td>🟢️</td>
<td>Yellow</td>
<td>Between 90% and 95% capacity</td>
</tr>
<tr>
<td>⚠️</td>
<td>Red</td>
<td>Over 95% capacity</td>
</tr>
</tbody>
</table>

Disk Usage

Multi-Grid Manager displays the percentage of the data partition of the hard disk drive that is currently in use on the selected Master Grid member. It also displays the percentage of usage. 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>Under 85% of the capacity is currently in use.</td>
</tr>
<tr>
<td>🟢️</td>
<td>Yellow</td>
<td>Between 85% and 95% of the capacity in use.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Red</td>
<td>Over 95% of the capacity in use.</td>
</tr>
</tbody>
</table>

LAN1/LAN2 Ports, HA Port, and MGMT Port

Multi-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>✅️</td>
<td>Green</td>
<td>The port is properly connected to a network. Multi-Grid Manager displays the IP address of the network.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Red</td>
<td>The port is not able to make a network connection.</td>
</tr>
<tr>
<td>⬅️</td>
<td>Gray</td>
<td>The port is disabled.</td>
</tr>
</tbody>
</table>
Memory Usage

Multi-Grid Manager displays the current percentage of system memory in use on the selected Master Grid member. It also describes whether the usage is OK or not. 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>Green</td>
<td>Under 90% capacity.</td>
</tr>
<tr>
<td>🟡</td>
<td>Yellow</td>
<td>Between 90% and 95% capacity.</td>
</tr>
<tr>
<td>🟥</td>
<td>Red</td>
<td>Over 95% capacity.</td>
</tr>
</tbody>
</table>

NTP Synchronization

The status icon indicates the operational status of the current NTP synchronization status of the Master Grid member.

<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>

MGM Service

The status icon indicates the status of the synchronization processes between the Multi-Grid Master and the managed Grids. This is displayed for the Multi-Grid Master only.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢</td>
<td>Green</td>
<td>All services related to Multi-Grid management are running properly.</td>
</tr>
<tr>
<td>🟡</td>
<td>Yellow</td>
<td>The status of the Multi-Grid management service is not reported.</td>
</tr>
<tr>
<td>🟥</td>
<td>Red</td>
<td>At least one of the services related to Multi-Grid management is not running.</td>
</tr>
</tbody>
</table>
Grid Connection

The status icon indicates the status of the overall connectivity of the Master Grid and managed Grids. This is displayed for the Multi-Grid Master only.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>All managed Grids are connected.</td>
<td></td>
</tr>
<tr>
<td>Yellow</td>
<td>The status of the connection is not reported.</td>
<td></td>
</tr>
<tr>
<td>Red</td>
<td>At least one of the managed Grids is not connected properly.</td>
<td></td>
</tr>
</tbody>
</table>

Replication

The status icon indicates the replication status between the Multi-Grid Master and the members. This is displayed for the Master Grid members only.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>The replication is operating normally in a “Running” state.</td>
<td></td>
</tr>
<tr>
<td>Yellow</td>
<td>The Master Grid member is connecting or synchronizing with its Multi-Grid Master.</td>
<td></td>
</tr>
<tr>
<td>Red</td>
<td>The Master Grid member is offline, is not licensed, is upgrading or downgrading, or is shutting down.</td>
<td></td>
</tr>
</tbody>
</table>

Power Supply

The Infoblox-1552-A, -1852-A, -2000-A, and -4010 have 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>Green</td>
<td>The power supplies are functioning properly.</td>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
</tbody>
</table>
RAID

For the Infoblox-2000-A and -4010, Multi-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. Multi-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>![Green]</td>
<td>Green</td>
<td>The RAID array or the disk is functioning properly.</td>
</tr>
<tr>
<td>![Yellow]</td>
<td>Yellow</td>
<td>A new disk has been inserted and the RAID array is rebuilding.</td>
</tr>
<tr>
<td>![Red]</td>
<td>Red</td>
<td>The RAID array or the disk is degraded. At least one disk in the array is not functioning properly. Multi-Grid Manager lists the disks that are online. Replace only the disks that are offline.</td>
</tr>
</tbody>
</table>

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. The disk type of the Infoblox-2000-A can be one of the following:

- IB-Type 1: Infoblox supported disk type
- IB-Type 2: Infoblox supported disk type
- Unk: Unknown disk type that Infoblox does not support

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-2000-A and -4010.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Green]</td>
<td>Green</td>
<td>The battery is charged. The description indicates the estimated number of hours of charge remaining on the battery.</td>
</tr>
<tr>
<td>![Yellow]</td>
<td>Yellow</td>
<td>The battery is charging.</td>
</tr>
<tr>
<td>![Red]</td>
<td>Red</td>
<td>The battery is not charged.</td>
</tr>
</tbody>
</table>
Viewing Hardware Status

You can view the link activity and connection speed of an Ethernet port by looking at its Link/Act and Speed LEDs on the appliance. The status the LEDs convey through their color and illumination (steady glow or blinking) are presented in the following tables.

### For Infoblox-2000-A Appliances

<table>
<thead>
<tr>
<th>MGMT and HA Ports</th>
<th>Label</th>
<th>Color</th>
<th>Port Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link/Act</td>
<td>Steady Orange</td>
<td>Link is up but inactive</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Blinking Orange</td>
<td>Link is up and active</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dark</td>
<td>Link is down</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LAN Ports</th>
<th>Label</th>
<th>Color</th>
<th>Port Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link/Act</td>
<td>Steady Green</td>
<td>Link is up but inactive</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Blinking Green</td>
<td>Link is up and active</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dark</td>
<td>Link is down</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MGMT, HA, and LAN Ports</th>
<th>Label</th>
<th>Color</th>
<th>Port Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>Steady Amber</td>
<td>1000 Mbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Steady Green</td>
<td>100 Mbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dark</td>
<td>10 Mbps</td>
<td></td>
</tr>
</tbody>
</table>

### For Infoblox-1050-A, -1550-A, -1552-A, and -1852-A Appliances

<table>
<thead>
<tr>
<th>Label</th>
<th>Color</th>
<th>Port Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link/Act</td>
<td>Steady Green</td>
<td>Link is up but inactive</td>
</tr>
<tr>
<td></td>
<td>Blinking Green</td>
<td>Link is up and active</td>
</tr>
<tr>
<td></td>
<td>Dark</td>
<td>Link is down</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Speed</th>
<th>Color</th>
<th>Port Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steady Amber</td>
<td>1000 Mbps</td>
<td></td>
</tr>
<tr>
<td>Steady Green</td>
<td>100 Mbps</td>
<td></td>
</tr>
<tr>
<td>Dark</td>
<td>10 Mbps</td>
<td></td>
</tr>
</tbody>
</table>
Using a Syslog Server

Syslog is a widely used mechanism for logging system events. The 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 an appliance to send the messages to one or more external syslog servers for later analysis. Syslog messages provide information about appliance operations and processes. The appliances include syslog messages generated by the bloxTools service. 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, the 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 a .gz extension following the numerical increment (file.#.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 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.

This section includes the following topics:

- Specifying Syslog Servers on page 234
- Configuring Syslog for Master Grid Members on page 235
- Viewing the Syslog on page 236
- Searching in the Syslog on page 236
- Downloading the Audit Log on page 239

Specifying Syslog Servers

To configure the appliance to send messages to a syslog server:

1. From the Master Grid tab, select the Members tab, and then click Master Grid Properties -> Edit from the Toolbar.
2. In the Master Grid Properties editor, select the Monitoring tab, and then complete the following:

   Syslog
   - 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.
   - Multi-Grid Manager displays the current syslog servers in the table. To define a new syslog server, click the Add icon. Multi-Grid Manager adds a row to the table. Enter the following by clicking each field in the row:
     - Address: Enter the IP address of a syslog server.
     - Transport: From the drop-down list, select whether the appliance uses TCP or UDP to connect to the external syslog server.
     - Interface: From the drop-down list, select the interface through which the appliance sends syslog messages to the syslog server.
     - Source: From the drop-down list, select which syslog messages the appliance sends to the external syslog server:
       - Internal: The appliance sends syslog messages that it generates.
Using a Syslog Server

- **External**: The appliance sends syslog messages that it receives from other devices, such as syslog servers and routers.
- **Any**: The appliance sends both internal and external syslog messages.
  - **Port**: Enter the destination port number. The default is 514.
  - **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**.
    - **emerg**: Panic or emergency conditions. The system may be unusable.
    - **alert**: Alerts, such as NTP service failures, that require immediate actions.
    - **crit**: Critical conditions, such as hardware failures.
    - **err**: Error messages, such as client update failures and duplicate leases.
    - **warning**: Warning messages, such as missing keepalive options in a server configuration.
    - **notice**: Informational messages regarding routine system events, such as “starting BIND”.
    - **info**: Informational messages, such as DHCPACK messages and discovery status.
    - **debug**: Messages that contain information for debugging purposes, such as changes in the latency timer settings and AD authentication failures for specific users.

- **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.

### Configuring Syslog for Master Grid Members

You can override the Master Grid 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.

To configure syslog parameters for a Master Grid member:

1. From the **Master Grid** tab, select the **Members** tab -> **master_grid_member** check box, and then click the **Edit** icon.
2. In the **Master Grid Member Properties** editor, select the **Monitoring** tab -> **Basic** tab, click **Override** in the Syslog section, and then complete the fields as described in **Specifying Syslog Servers** on page 234.
   In addition to storing the system log on a Master 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**: Click the Add icon. Multi-Grid Manager adds a row to the table. Complete the following:
  — **Allow Access From**: Enter the IP address and subnet mask of the appliance or network.

4. Save the configuration.

## 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 Master 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), Multi-Grid Manager displays the following in the **Syslog** viewer:
   - **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.

   **Note**: If the selected member is an HA pair, Multi-Grid Manager displays the syslog in two tabs—**Active** and **Passive**. Click the corresponding tab to view the syslog for each node.

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** on page 34.
- 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.
Monitoring Tools

You can use the audit log, the replication status, the traffic capture tool, and the capacity report in the Master Grid to monitor administrative activities and capture traffic for diagnostic purposes.

This section includes the following topics:

- Using the Audit Log
- Viewing the Replication Status  on page 239
- Using the Traffic Capture Tool  on page 240
- Using the Capacity Report  on page 241
- Using the Phone Home Feature  on page 241

Using the Audit Log

The audit log contains a record of all Infoblox administrative activities. It provides detailed information about the following changes:

- 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.
- Action performed, such as DELETED (deleting an object) or CREATED (adding an object).
- Object type of the object involved in the task. This is not displayed by default, but you can select this for display.
- Object name
- Detailed information about the performed task

The appliance logs the following successful operations:

- Logins to Multi-Grid Manager and the API.
- Logout events, including when users log out by clicking the Logout button, when the Multi-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 appliance reboots.
- Scheduled tasks such as adding an A record or modifying a fixed address.

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.
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 (\texttt{file.\#.gz}). The sequential incrementation goes from zero through nine. When the eleventh file is started, the tenth log file (\texttt{file.9.gz}) is deleted, and subsequent files are renumbered accordingly. For example, the current log file moves to \texttt{file.0.gz}, the previous \texttt{file.0.gz} moves to \texttt{file.1.gz}, and so on through \texttt{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 \texttt{show logfiles} command.

To enable audit log rolling:
1. From the Master Grid tab, select the Members tab, and then click Master Grid Properties \rightarrow Edit from the Toolbar.
2. In the Master 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 Master Grid tab, select the Members tab, and then click Master Grid Properties \rightarrow Edit from the Toolbar.
2. In the Master Grid Properties editor, select the General tab, and then select one of the following:
   
   \begin{itemize}
   \item \textbf{Audit Logging:}
   \begin{itemize}
   \item \textbf{Detailed:} This is the default type. When you select this, Multi-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.
   \item \textbf{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.
   \end{itemize}
   \end{itemize}

Viewing the Audit Log

To view an audit log:

1. From the Administration tab, select the Logs tab \rightarrow 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), Multi-Grid Manager displays the following in the Audit Log Viewer:

\begin{itemize}
\item \textbf{Timestamp:} The date, time, and time zone the task was performed. The time zone is the time zone configured on the member.
\item \textbf{Admin:} The admin user who performed the task.
\item \textbf{Action:} The action performed. This can be CALLED, CREATED, DELETED, LOGIN_ALLOWED, LOGIN_DENIED, MESSAGE, and MODIFIED.
\item \textbf{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.
\item \textbf{Object Name:} The name of the object involved in this task.
\item \textbf{Message:} Detailed information about the performed task.
\end{itemize}

You can also do the following in the log viewer:

\begin{itemize}
\item Toggle between the single line view and the multi-line view for display.
\item Navigate to the next or last page of the file using the paging buttons.
\item Refresh the audit log view.
\item Click the Follow icon to have the appliance automatically refresh the log every five seconds.
\item Download the log.
\item Clear the contents of the audit log.
\item 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.
\end{itemize}
• Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 34.
• 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 Master Grid members and the Multi-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 Master Grid tab, select the Members tab, and then click Replication Status View.

Multi-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 Multi-Grid Master to the Master Grid member.
• Last Send: The timestamp of the last replication information sent by the Multi-Grid Master.
• Receive Queue: The size of the queue from the member to the Multi-Grid Master.
• Last Receive: The timestamp of the last replication information sent received by the Multi-Grid Master.
• Member Replication Status: The replication status between the member and the Multi-Grid Master. Multi-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. Multi-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 Multi-Grid Master.
   — Red: The member is offline, is not licensed, is upgrading or downgrading, or is shutting down.
• IP Address: The IP address of the appliance.
• Hardware Type: The hardware type of the appliance, such as IB-1550-A.
• Serial Number: The serial number of the appliance.
Monitoring the Master Grid

- **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, Multi-Grid Manager displays the status of the HA pair.
- **Hardware Model**: The hardware model of the appliance.

You can do the following:

- Use filters to narrow down the list.
- Create a quick filter to save frequently used filter criteria. For information, see *Using Quick Filters* on page 34.
- 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* on page 31.
- Edit the properties of a member.
  - Click the check box beside a member, and then click the Edit icon.
- Delete a member.
  - Click the check box beside a member, and then click the Delete icon.
- Export or print the list.

**Using the Traffic Capture Tool**

You can capture the traffic on one or all of the ports on the appliance, and then view it using a third-party network protocol analyzer application, such as the Wireshark – Network Protocol Analyzer™.

The 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.

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 traffic analyzer application.

**Note**: The 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.

To capture traffic on a member:

1. From the Master Grid tab, select the Members tab, and then click Traffic Capture from the Toolbar.
2. In the Traffic Capture dialog box, complete the following:
   - **Member**: Multi-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, Multi-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.
     - **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 appliance only captures traffic that is addressed to it.
   - **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. **Uncompressed Capture File Size**: Click **Download** to download the captured traffic after the capture stops. Navigate to where you want to save the file, rename it if you want, and then click **OK** or **Save**. You cannot download the traffic report when the tool is running. Multi-Grid Manager updates the size of the report when the capture tool is running.

5. Use terminal window commands (Linux) or a software application (such as StuffIt™ or WinZip™) to extract the contents of the .tar.gz file.

6. 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 the Multi-Grid Master or a Master 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 Master Grid tab, select the Members tab -> master_grid_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 Master Grid Master or Master Grid Master Candidate.
- **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 report categorizes object types you can manage through the appliance. It displays the following information for each object type:

- **Object Type**: The type of objects that are supported by the Master Grid, such as Admin or Grid Email Address. 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 a specific object type.

You can print the object type information or export it to a CSV file.

### Using the Phone Home Feature

Administrators with superuser accounts can configure a Multi-Grid Master or member 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 version, name, VIP, Multi-Grid Master hostname, LAN IP, and the number of Master Grid members and appliances in the Grid.
- The upgrade history of the Grid.
- Information about each Master 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 on page 100, the appliance sends the phone home reports to the relay server as well.

To configure the Multi-Grid Master to email status reports:

1. From the Master Grid tab, select the Members tab, and then click Master Grid Properties -> Edit from the Toolbar.
2. In the Master Grid Properties editor, select the Phone Home tab, and then complete the following:
   - Enable Phone Home: Select this check box.
   - Support ID (numeric): Enter the Infoblox Support ID that was assigned to your account. It must be a number with four to 6 digits. This field is required if you are sending the reports to Infoblox Technical Support.
   - 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.
3. Save the configuration.
Chapter 11  Monitoring with SNMP

This chapter describes how you can use SNMP (Simple Network Management Protocol) to monitor the Master Grid. It contains the following sections:

- **Understanding SNMP** on page 244
  - About SNMPv1 and SNMPv2 on page 245
  - About User-Based Security Model in SNMPv3 on page 245

- **Configuring SNMP** on page 245
  - Configuring SNMPv3 Users on page 246
  - Modifying SNMPv3 Users on page 247
  - Deleting SNMPv3 Users on page 247
  - Accepting Queries on page 247
  - Adding Trap Receivers on page 248
  - Setting SNMP System Information on page 249
  - Testing the SNMP Configuration on page 249

- **SNMP MIB Hierarchy** on page 250
  - MIB Objects on page 251
  - System Object IDs on page 251

- **Infoblox MIBs** on page 253
  - Loading the Infoblox MIBs on page 253
  - ibTrap MIB on page 255
  - ibPlatformOne MIB on page 279
  - ibDHCPOne MIB on page 294
  - ibDNSOne MIB on page 302
Understanding SNMP

You can use SNMP (Simple Network Management Protocol) to manage network devices and monitor their processes. An SNMP-managed device, such as an Infoblox 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 11.1 SNMP Overview

The 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 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 on page 245.

About User-Based Security Model in SNMPv3

SNMPv3 adds security and remote configuration enhancements to SNMPv1 and SNMPv2. The 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 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 Encryptions Standard) as the encryption methods for SNMPv3 users. For information, see Configuring SNMP on page 245.

Configuring SNMP

You can configure the appliance to receive SNMP queries from specific management systems and send SNMP traps to specific trap receivers. The appliance supports SNMPv1, SNMPv2, and SNMPv3. You can set up either SNMPv1/SNMPv2 or SNMPv3, or all of them for the Master Grid. You can also override the Master Grid settings at a member level.

To configure SNMPv1 and SNMPv2 on the appliance, do the following:

- Enable the appliance to accept queries, as described in Accepting Queries on page 247.
- Specify the management systems to which the appliance sends traps, as described in Adding Trap Receivers on page 248.
- Specify system information using managed objects in MIB-II, the standard MIB defined in RFC 1213. For information, see Setting SNMP System Information on page 249.
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 on page 246. After you set up an SNMPv3 user, you can modify and delete it. For information, see Modifying SNMPv3 Users on page 247 and Deleting SNMPv3 Users on page 247.
- Enable the appliance to accept queries, as described in Accepting Queries on page 247.
- Specify the management systems to which the appliance sends traps, as described in see 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 on page 249.

### 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 on page 245.

To configure an SNMPv3 user:

1. From the Administration tab, select the Administrators tab -> 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 RFC1321, 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 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 on page 168.
4. Save the configuration.
Modifying SNMPv3 Users

1. From the Administration tab, select the Administrators tab → 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 on page 246.
   — 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 on page 168.
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 Administrators tab → 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 the 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 on page 246.

To configure an appliance to accept SNMP queries:

1. From the Master Grid tab, click Master Grid Properties → Edit from the Toolbar.
   or
   From the Master Grid tab, select the Members tab → master_grid_member, and then click the Edit icon.
2. In the Master Grid Properties or Master Grid Member Properties editor, select the SNMP tab. To override Master Grid settings, click Override in the Master 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 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 Master Grid. You can also override the Master Grid settings at the member level.

To enable the appliance to send traps and to add trap receivers, do the following:

1. From the **Master Grid** tab, click **Master Grid Properties** -> **Edit** from the Toolbar.
   
   or
   
   From the **Master Grid** tab, select the **Members** tab -> **master_grid_member**, and then click the **Edit** icon.

2. In the **Master Grid Properties** or **Master Grid Member Properties** editor, select the **SNMP** tab. To override Master Grid settings, click **Override** in the **Master 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 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. Multi-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. Multi-Grid Manager displays the **SNMPv3 User Selector** dialog box. Click the name of the SNMPv3 user in the dialog box. Multi-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.

   In the Trap Receiver table, Multi-Grid Manager displays the following information about the trap receivers:

   — **Address**: The IP 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 Master Grid and specific members. You can also override the Master Grid values at a member level.

To enter system information:

1. From the Master Grid tab, click Master Grid Properties -> Edit from the Toolbar.
   
   or

2. From the Master Grid tab, select the Members tab -> master_grid_member, and then click the Edit icon.

3. In the Master Grid Properties or Master Grid Member Properties editor, select the SNMP tab. To override Master Grid settings, click Override in the Master Grid Member Properties editor.

4. 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.

Testing the SNMP Configuration

After you configure SNMP on the appliance, you can do the following to test your SNMP configuration:

• From the Master Grid tab, select the Members tab -> master_grid_member, 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 11.2* 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 11.2*, 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.

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 the appliances send, and the ibPlatformOne, ibDNSOne, and ibDHCPOne MIBs provide information about the appliance. For detailed information about these MIBS, see *Infoblox MIBs* on page 253.

*Figure 11.2 MIB Hierarchy*
MIB Objects

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 the 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>
<tr>
<td>DESCRIPTION</td>
<td>&quot;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'.&quot;&quot;</td>
</tr>
</tbody>
</table>
Table 11.1 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 11.1 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>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>1101</td>
<td>ib1000</td>
<td>Infoblox-1000 appliances</td>
</tr>
<tr>
<td>1102</td>
<td>ib1200</td>
<td>Infoblox-1200 appliances</td>
</tr>
<tr>
<td>1103</td>
<td>ib500</td>
<td>Infoblox-500 appliances</td>
</tr>
<tr>
<td>1201</td>
<td>ib550</td>
<td>Infoblox-550 appliances</td>
</tr>
<tr>
<td>1202</td>
<td>ib1050</td>
<td>Infoblox-1050 appliances</td>
</tr>
<tr>
<td>1203</td>
<td>ib1550</td>
<td>Infoblox-1550 appliances</td>
</tr>
<tr>
<td>1204</td>
<td>ib1552</td>
<td>Infoblox-1552 appliances</td>
</tr>
<tr>
<td>1205</td>
<td>ib2000</td>
<td>Infoblox-2000 appliances</td>
</tr>
<tr>
<td>1206</td>
<td>ib250</td>
<td>Infoblox-250 appliances</td>
</tr>
<tr>
<td>1207</td>
<td>ib1220</td>
<td>Infoblox-1220 appliances</td>
</tr>
<tr>
<td>1301</td>
<td>ib550a</td>
<td>Infoblox-550-A appliances</td>
</tr>
<tr>
<td>1302</td>
<td>ib1050a</td>
<td>Infoblox-1050-A appliances</td>
</tr>
<tr>
<td>1303</td>
<td>ib1550a</td>
<td>Infoblox-1550-A appliances</td>
</tr>
<tr>
<td>1304</td>
<td>ib1552a</td>
<td>Infoblox-1552-A appliances</td>
</tr>
<tr>
<td>1305</td>
<td>ib1852a</td>
<td>Infoblox-1852-A appliances</td>
</tr>
<tr>
<td>1306</td>
<td>ib250a</td>
<td>Infoblox-250-A appliances</td>
</tr>
<tr>
<td>1307</td>
<td>ib2000a</td>
<td>Infoblox-2000-A appliances</td>
</tr>
<tr>
<td>1421</td>
<td>ib4010</td>
<td>Infoblox-4010 appliances</td>
</tr>
</tbody>
</table>
Infoblox MIBs

You can configure the appliance as an SNMP-managed device so that an SNMP management station can send queries to the appliance and retrieve information from its MIBs. Note that you can download all Infoblox MIBs from Multi-Grid Manager, including MIBs that are specific to DNS and DHCP operations. Perform the following tasks to access the Infoblox MIBs:

1. Configure the appliance to accept queries, as described in Configuring SNMPv3 Users on page 246.
2. Load the MIB files onto the management system. To obtain the latest Infoblox MIB files:
   a. From the Master Grid tab, select the Members tab -> master_grid_member check box, 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 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 listed:

1. IB-SMI-MIB.txt
2. IB-TRAP-MIB.txt
3. IB-PLATFORMONE-MIB.txt
4. IB-DNSONE-MIB.txt
5. IB-DHCPONE-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

Infoblox 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/.

For SNMP traps to function properly, you must download the following NET-SNMP MIBs directly from 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.
Monitoring with SNMP

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 Definitions of Managed Objects for BGP-4. You must enable and configure the SNMP trap receiver on the Multi-Grid member for the member to send SNMP traps. For information, see SNMP MIB Hierarchy on page 250.

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

Infoblox appliances send SNMP traps when events, internal process failures, or critical service failures occur. The ibTrap MIB defines the types of traps that the appliance sends and the value that each MIB object represents. The Infoblox SNMP traps report objects which the ibTrap MIB defines. *Figure 11.3* 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 the 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 11.3  ibTrapOne MIB Structure*
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 the appliance sends:

```
0:00:10.80 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.7779.3.1.1.1.4.0
SNMPv2-SMI::enterprises.7779.3.1.1.1.2.1.0 = STRING: "10.35.1.156"
SNMPv2-SMI::enterprises.7779.3.1.1.2.3.0 = STRING: "ntp_sync"
SNMPv2-SMI::enterprises.7779.3.1.1.2.9.0 = INTEGER: 15
SNMPv2-SMI::enterprises.7779.3.1.1.2.10.0 = INTEGER: 16
SNMPv2-SMI::enterprises.7779.3.1.1.2.11.0 = STRING: "The NTP service is out of synchronization."
```

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)` on page 266.

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 7779.3.1.1.2.1.0)**
  - The statement `7779.3.1.1.2.1.0 = STRING: "10.35.1.156"` tells you the IP address of the appliance on which the trap occurred.

- **ibObjectName (OID 7779.3.1.1.2.3.0)**
  - The statement `7779.3.1.1.1.2.3.0 = STRING: "ntp_sync"` 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 7779.3.1.1.2.9.0)**
  - The statement `7779.3.1.1.1.2.9.0 = INTEGER: 15` 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 7779.3.1.1.2.10.0)**
  - The statement `7779.3.1.1.1.2.10.0 = INTEGER: 16` 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 7779.3.1.1.2.11.0)**
  - 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 appliance can send. There are five types of SNMP traps. Table 11.2 describe the types of traps and their objects in the ibTrapOneModule tree.

Table 11.2  ibTrapOneModule

<table>
<thead>
<tr>
<th>OID</th>
<th>Trap Type</th>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1.1.1.1.0</td>
<td>Equipment Failure</td>
<td>ibEquipmentFailureTrap</td>
<td>The appliance generates this trap when a hardware failure occurs. This trap includes the following objects: • ibNodeName • ibTrapSeverity • ibObjectName (equipment name) • ibProbableCause • ibTrapDesc For a list of trap descriptions, see Equipment Failure Traps on page 266.</td>
</tr>
<tr>
<td>3.1.1.1.1.2.0</td>
<td>Processing and Software Failure</td>
<td>ibProcessingFailureTrap</td>
<td>The appliance generates this trap when a failure occurs in one of the software processes. This trap includes the following objects: • ibNodeName • ibTrapSeverity • ibSubsystemName • ibProbableCause • ibTrapDesc For a list of trap descriptions, see Processing and Software Failure Traps on page 267.</td>
</tr>
<tr>
<td>OID</td>
<td>Trap Type</td>
<td>MIB Object</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3.1.1.1.3.0</td>
<td>Threshold Crossing</td>
<td>ibThresholdCrossingEvent</td>
<td>The appliance generates this trap when any of the following events occur:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• System memory or disk usage exceeds 90%.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• A problem occurs when the Grid Master replicates its database to its Grid members.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• DHCP address usage crosses a watermark threshold. For more information about tracking IP address usage, see Chapter 7, Network Management, on page 143.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• The number or percentage of the DNS security alerts exceeds the thresholds of the DNS security alert triggers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This trap includes the following objects:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ibNodeName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ibObjectName (threshold name)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ibCurThresholdValue</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ibThresholdHigh</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ibThresholdLow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ibTrapDesc</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For a list of trap descriptions, see Threshold Crossing Traps on page 272.</td>
</tr>
</tbody>
</table>
### Infoblox MIBs

**NIOS 8.2 Multi-Grid Manager Administrator Guide (Rev. A)  259**

<table>
<thead>
<tr>
<th>OID</th>
<th>Trap Type</th>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1.1.5.0</td>
<td>Process Started and Stopped</td>
<td>ibProcStartStopTr</td>
<td>The appliance generates this type of trap when any of the following events occur:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• When you enable HTTP redirection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• When you change the HTTP access setting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• When you change the HTTP session time out setting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• When a failover occurs in an HA pair configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This trap includes the following objects:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ibNodeName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ibSubsystemName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ibTrapDesc</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For a list of possible trap descriptions, see <a href="#">Process Started and Stopped Traps</a> on page 278.</td>
</tr>
</tbody>
</table>
Monitoring with SNMP

Trap Binding Variables (OID 3.1.1.1.2)

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 11.3 describes the objects in the ibNotificationVarBind module.

Table 11.3 ibNotificationVarBind (OID 3.1.1.1.2)

Note: The OIDs shown in the following table do not include the prefix “.1.3.6.1.4.1.7779.”.

<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) on page 261 for details.</td>
</tr>
</tbody>
</table>
| 3.1.1.1.2.3.0  | 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. |
| 3.1.1.1.2.4.0  | ibProbableCause (Integer) | The probable cause of the trap. See ibProbableCause Values on page 262 for the definitions of each value.                                  |
| 3.1.1.1.2.5.0  | 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 3.1.1.1.2.9.0) on page 263 for definitions. |
| 3.1.1.1.2.6.0  | ibCurThresholdValue (Integer) | The current value of the threshold counter. This object is used in the Threshold Crossing traps.                                               |
| 3.1.1.1.2.7.0  | ibThresholdHigh (Integer)  | The value for 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. This object is used in Threshold Crossing traps. |
| 3.1.1.1.2.8.0  | ibThresholdLow (Integer)   | 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. This object is used in Threshold Crossing traps. For additional information, see BGP4 MIB on page 254. |
| 3.1.1.1.2.9.0  | 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) on page 265 for definitions of each value. |
Infoblox MIBs

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>Undetermined</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 3.1.1.2.4.0)

*Table 11.5* lists the values that are associated with the object `ibProbableCause` (OID 3.1.1.2.4.0). These values provide information about the events, such as software failures, that trigger traps.

#### Table 11.4  *ibProbableCause Values*

<table>
<thead>
<tr>
<th>Value</th>
<th><code>OID 3.1.1.2.4.0</code> <code>ibProbableCause</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td><code>ibClear</code></td>
</tr>
<tr>
<td>1</td>
<td><code>ibUnknown</code></td>
</tr>
<tr>
<td>2</td>
<td><code>ibPrimaryDiskFailure</code></td>
</tr>
<tr>
<td>3</td>
<td><code>ibFanFailure-old</code></td>
</tr>
<tr>
<td>4</td>
<td><code>ibPowerSupplyFailure</code></td>
</tr>
<tr>
<td>5</td>
<td><code>ibDBFailure</code></td>
</tr>
<tr>
<td>6</td>
<td><code>ibApacheSoftwareFailure</code></td>
</tr>
<tr>
<td>7</td>
<td><code>ibSerialConsoleFailure</code></td>
</tr>
<tr>
<td>11</td>
<td><code>ibControldSoftwareFailure</code></td>
</tr>
<tr>
<td>12</td>
<td><code>ibUpgradeFailure</code></td>
</tr>
<tr>
<td>13</td>
<td><code>ibSNMPDFailure</code></td>
</tr>
<tr>
<td>15</td>
<td><code>ibSSHDSoftwareFailure</code></td>
</tr>
<tr>
<td>16</td>
<td><code>ibNTPDSoftwareFailure</code></td>
</tr>
<tr>
<td>17</td>
<td><code>ibClusterdSoftwareFailure</code></td>
</tr>
<tr>
<td>18</td>
<td><code>ibLCDSoftwareFailure</code></td>
</tr>
<tr>
<td>19</td>
<td><code>ibDHCPdSoftwareFailure</code></td>
</tr>
<tr>
<td>20</td>
<td><code>ibNamedSoftwareFailure</code></td>
</tr>
<tr>
<td>21</td>
<td><code>ibAuthServerGroupDown</code></td>
</tr>
<tr>
<td>22</td>
<td><code>ibAuthServerGroupUp</code></td>
</tr>
<tr>
<td>24</td>
<td><code>ibNTLMSoftwareFailure</code></td>
</tr>
<tr>
<td>25</td>
<td><code>ibNetBIOSDaemonFailure</code></td>
</tr>
<tr>
<td>26</td>
<td><code>ibWindowBindDaemonFailure</code></td>
</tr>
<tr>
<td>27</td>
<td><code>ibTFTPDSoftwareFailure</code></td>
</tr>
<tr>
<td>29</td>
<td><code>ibBackupSoftwareFailure</code></td>
</tr>
<tr>
<td>30</td>
<td><code>ibBackupDatabaseSoftwareFailure</code></td>
</tr>
<tr>
<td>31</td>
<td><code>ibBackupModuleSoftwareFailure</code></td>
</tr>
<tr>
<td>32</td>
<td><code>ibBackupSizeSoftwareFailure</code></td>
</tr>
<tr>
<td>33</td>
<td><code>ibBackupLockSoftwareFailure</code></td>
</tr>
<tr>
<td>34</td>
<td><code>ibHTTPFileDistSoftwareFailure</code></td>
</tr>
</tbody>
</table>
### Table 11.5: ibSubsystemName Values (OID 3.1.1.1.2.9.0)

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>ibOSPFSoftwareFailure</td>
</tr>
<tr>
<td>36</td>
<td>ibAuthDHCPNamedSoftwareFailure</td>
</tr>
<tr>
<td>37</td>
<td>ibFan1Failure</td>
</tr>
<tr>
<td>38</td>
<td>ibFan2Failure</td>
</tr>
<tr>
<td>39</td>
<td>ibFan3Failure</td>
</tr>
<tr>
<td>40</td>
<td>ibFan1OK</td>
</tr>
<tr>
<td>41</td>
<td>ibFan2OK</td>
</tr>
<tr>
<td>42</td>
<td>ibFan3OK</td>
</tr>
<tr>
<td>44</td>
<td>ibFTPSoftwareFailure</td>
</tr>
<tr>
<td>46</td>
<td>ibPowerSupplyOK</td>
</tr>
<tr>
<td>47</td>
<td>ibWebUISoftwareFailure</td>
</tr>
<tr>
<td>49</td>
<td>ibADAgentSyncFailure</td>
</tr>
<tr>
<td>50</td>
<td>ibIFMAPSoftwareFailure</td>
</tr>
<tr>
<td>51</td>
<td>ibCaptivePortalSoftwareFailure</td>
</tr>
<tr>
<td>52</td>
<td>ibDuplicateIPAddressFailure</td>
</tr>
<tr>
<td>53</td>
<td>ibBGPSoftwareFailure</td>
</tr>
<tr>
<td>54</td>
<td>ibRevokedLicense</td>
</tr>
<tr>
<td>2029</td>
<td>ibHSMGroupFailure</td>
</tr>
<tr>
<td>2030</td>
<td>ibHSMGroupOK</td>
</tr>
<tr>
<td>3001</td>
<td>ibRAIDIsOptimal</td>
</tr>
<tr>
<td>3002</td>
<td>ibRAIDIsDegraded</td>
</tr>
<tr>
<td>3003</td>
<td>ibRAIDIsRebuilding</td>
</tr>
<tr>
<td>3004</td>
<td>ibRAIDStatusUnknown</td>
</tr>
<tr>
<td>3005</td>
<td>ibRAIDBatteryIsOK</td>
</tr>
<tr>
<td>3006</td>
<td>ibRAIDBatteryFailed</td>
</tr>
</tbody>
</table>

**ibSubsystemName Values (OID 3.1.1.2.9.0)**

*Table 11.5* lists the values that are associated with the object `ibSubsystemName (OID 3.1.1.2.9.0)`. These values provide information about the subsystems that trigger the traps.
<table>
<thead>
<tr>
<th>Value</th>
<th>OID 3.1.1.1.2.9.0</th>
<th>ibSubsystemName</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Uses the original ibObjectName and ibSubsystemName when the trap is cleared.</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Db_jnld</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>httpd</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>serial_console</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>controld</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Snmpd</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Sshd</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Ntpd</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Clusterd</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Lcd</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Dhcpd</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Named</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>NTLM</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Netbiosd</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Winbindd</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Tftpd</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>HTTPd</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>OSPF</td>
<td></td>
</tr>
</tbody>
</table>
ibPreviousState (OID 3.1.1.1.2.9.0) and ibCurrentState (OID 3.1.1.1.2.10.0)

The ibPreviousState object indicates the state of the appliance before the event triggered the trap. The ibCurrentState object indicates the current state of the appliance. Table 11.6 shows the message and description for each state.

Table 11.6  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 appliance is connected to the Master Grid.</td>
</tr>
<tr>
<td>5</td>
<td>grid-disconnected</td>
<td>The appliance is not connected to the Master Grid.</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-snapshopting</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 sync.</td>
</tr>
<tr>
<td>17</td>
<td>ms-server-up</td>
<td>The Microsoft server is online.</td>
</tr>
<tr>
<td>18</td>
<td>ms-server-down</td>
<td>The Microsoft server is offline.</td>
</tr>
<tr>
<td>19</td>
<td>ms-service-up</td>
<td>The Microsoft service connection is up.</td>
</tr>
<tr>
<td>20</td>
<td>ms-service-down</td>
<td>The Microsoft service connection is down.</td>
</tr>
<tr>
<td>21</td>
<td>nac-server-group-down</td>
<td>The NAC authentication server group is down.</td>
</tr>
<tr>
<td>22</td>
<td>nac-server-group-up</td>
<td>The NAC authentication server group is up.</td>
</tr>
<tr>
<td>23</td>
<td>mgm-service-up</td>
<td>The connection between the Master Grid and managed Grids is up.</td>
</tr>
<tr>
<td>24</td>
<td>mgm-service-down</td>
<td>The connection between the Master Grid and managed Grids is down.</td>
</tr>
<tr>
<td>2029</td>
<td>hsm-group-failure</td>
<td>The HSM operation failed.</td>
</tr>
<tr>
<td>2030</td>
<td>hsm-group-up</td>
<td>The HSM operation is functioning properly.</td>
</tr>
</tbody>
</table>
**ibTrapDesc (OID 3.1.1.1.2.11.0)**

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><code>ibTrapDesc OID 3.1.1.1.2.11.0</code></th>
<th><code>ibTrapServerity OID 3.1.1.1.2.2</code></th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary Drive Full</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary drive is full.</td>
<td>Major</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>
</tbody>
</table>

**Fan Monitoring**

<table>
<thead>
<tr>
<th><code>Fan &lt;n&gt;</code> Failure has occurred.</th>
<th>Minor</th>
<th>The specified fan failed. The fan number &lt;n&gt; can be 1, 2, or 3.</th>
<th>Inspect the specified fan for mechanical or electrical problems.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Fan &lt;n&gt;</code> is OK.</td>
<td>Informational</td>
<td>The specified fan is functioning properly. The fan number &lt;n&gt; can be 1, 2, or 3.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

**Power Supply Failure: monitored at 1 minute**

<table>
<thead>
<tr>
<th><code>A power supply failure has occurred.</code></th>
<th>Major</th>
<th>The power supply failed.</th>
<th>Inspect the power supply for the possible cause of the failure.</th>
</tr>
</thead>
</table>
### RAID monitoring, at 1 minute interval

<table>
<thead>
<tr>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>A RAID battery failure has occurred.</td>
<td>The system RAID battery failed. The alert light is red. Inspect the battery for the possible cause of the failure.</td>
</tr>
<tr>
<td>The system’s RAID battery is OK.</td>
<td>The system RAID battery is charging and functioning properly. The alert light changed from red to green. No action is required.</td>
</tr>
<tr>
<td>Unable to retrieve RAID array state!</td>
<td>The appliance failed to retrieve the RAID array state. The alert light is red. 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>The RAID system is functioning at an optimal state. No action is required.</td>
</tr>
<tr>
<td>The system’s RAID array is in a degraded state.</td>
<td>The RAID system is degrading. Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>The system’s RAID array is rebuilding.</td>
<td>The RAID system is rebuilding. No action is required.</td>
</tr>
</tbody>
</table>

### Processing and Software Failure Traps

<table>
<thead>
<tr>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>A named daemon monitoring failure has occurred.</td>
<td>The named process failed. Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>A DHCP daemon monitoring failure has occurred.</td>
<td>The dhcpd process failed. Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>An SSH daemon failure has occurred.</td>
<td>The sshd process failed. Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>An NTP daemon failure has occurred.</td>
<td>The ntpd process failed. Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Cluster Daemon Failure</td>
<td></td>
</tr>
<tr>
<td>Description/Cause</td>
<td>Recommended Actions</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>A cluster daemon failure has occurred.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>An LCD daemon failure has occurred.</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>
<tr>
<td>An Apache software httpd failure, monitored every 2 minutes</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>An Infoblox serial console failure has occurred.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>A controld failure has occurred.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>An SNMP server failure has occurred.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>An TFTP daemon failure has occurred.</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>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>An HTTP file distribution daemon failure has occurred.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>An auth named server failure has occurred.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>An OSPF quagga Processes (zebra &amp; ospfd)</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>ibTrapDesc OID 3.1.1.1.2.11.0</td>
<td>ibTrapServerity OID 3.1.1.1.2.2</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Backup Failure</td>
<td></td>
</tr>
</tbody>
</table>
| Backup failed.              | Not implemented               | 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     |                               |                  |                   |
| Database backup failed.     | Not implemented               | The db_dump process failed.  | Review the syslog file to identify the possible cause of this problem. |
| Backup Module Failure       |                               |                  |                   |
| Backup File Size Exceeded  |                               |                  |                   |
| File size exceeded the quota. Backup failed. | Not implemented | The backup failed because the file size exceeded the limit of 5GB. | Limit the size of the backup file to less than 5GB. |
| Another backup is in progress. Backup will not be performed. | Not implemented | The backup failed because of an attempt to back up or merge files while another backup or restore was in progress. | Wait until the backup or restore is complete before starting another backup. |
## Monitoring with SNMP

### Watchdog Process Monitoring

<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.2.11.0</th>
<th>ibTrapServerity OID 3.1.1.1.2.2</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
</table>
| WATCHDOG: <registered client name> failed on <server IP address> | Critical | The watchdog process detected a registered client failure on a specific server. The <registered client name> could be one of the following:  
• Clusterd_timeout  
• DB_Sentinel  
• Process_Manager  
• Clusterd_monitor  
• Disk_monitor | Review the syslog file to identify the possible cause of this problem. |

### Microsoft Server

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft server hostname has failed.</td>
<td>Major</td>
</tr>
<tr>
<td>Microsoft server hostname is OK.</td>
<td>Informational</td>
</tr>
</tbody>
</table>

### Microsoft DNS/DHCP Service

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Service connection to Microsoft DNS server hostname has failed.</td>
<td>Major</td>
</tr>
<tr>
<td>Service connection to Microsoft DHCP server hostname has failed.</td>
<td>Major</td>
</tr>
<tr>
<td>Service connection to Microsoft DNS server hostname is OK.</td>
<td>Informational</td>
</tr>
<tr>
<td>Service connection to Microsoft DHCP server hostname is OK.</td>
<td>Informational</td>
</tr>
</tbody>
</table>

### NAC Authentication Server Group

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NAC Authentication server group is down.</td>
<td>Major</td>
</tr>
<tr>
<td>ibTrapDesc OID 3.1.1.1.2.11.0</td>
<td>ibTrapServerity OID 3.1.1.1.2.2</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>NAC Authentication server group is up.</td>
<td>Informational</td>
</tr>
</tbody>
</table>
## Threshold Crossing Traps

<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.2.11.0</th>
<th>ibObjectName OID 3.1.1.1.2.3.0</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Memory Usage</td>
<td>memory</td>
<td>The appliance ran out of memory. The appliance encountered this problem when one of the following occurred:</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The total free memory on the appliance was less than or equal to 0%.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The total physical memory was less than the total free memory.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The percentage of free memory compared to the total physical memory was less than 5%, and the free swap percentage was less than 80%.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Free memory = free physical RAM + free cache buffers. The high threshold for swap pages is 3,200.
<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.11.0</th>
<th>ibObjectName OID 3.1.1.1.2.3.0</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
</table>
| System memory usage is over 90%. | memory | The memory usage on the appliance exceeded 90%. 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. | Review the syslog file to identify the possible cause of this problem. |
| System memory is OK. | memory | The memory usage on the system is back to normal from the previous state. | No action is required. |

**Note:** Free memory = free physical RAM + free cache buffers. The high threshold for swap pages is 3,200.
<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.2.11.0</th>
<th>ibObjectName OID 3.1.1.1.2.3.0</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Hard Drive Usage (monitored every 30 seconds)</td>
<td>System primary hard disk usage is over 90%.</td>
<td>The primary hard disk usage exceeded 90%. The alert light is yellow.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td></td>
<td>Primary drive is full.</td>
<td>The primary hard disk usage exceeded 95%. The alert light is red.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td></td>
<td>Primary drive usage is OK.</td>
<td>The primary hard disk usage is 85% or lower. The alert light is green.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>
| Replication Statistics Monitoring | Grid queue replication problem. | For send trap: Cluster_Send_Queue  
For receive trap: Cluster_Recv_Queue | 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. |
<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.2.11.0</th>
<th>ibObjectName OID 3.1.1.1.2.3.0</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DHCP Range Threshold Crossing</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP threshold crossed:</td>
<td>Threshold</td>
<td>The system encountered this problem when one of the following conditions occurred:</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Member: &lt;DHCP server node VIP&gt;</td>
<td></td>
<td>• The address usage in the DHCP range was greater than the high watermark.</td>
<td></td>
</tr>
<tr>
<td>Network: &lt;network&gt;/</td>
<td></td>
<td>• The address usage in the DHCP range was less than the low watermark.</td>
<td></td>
</tr>
<tr>
<td>&lt;network view&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Range: &lt;DHCP range&gt;/</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;network view&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High Watermark: &lt;high</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>watermark percentage&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(95% by default)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low Watermark: &lt;low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>watermark percentage&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(0% by default)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current Usage: &lt;current usage</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>percentage&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Leases: &lt;number of</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>active leases&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Available Leases: &lt;number of</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>available leases&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Addresses: &lt;total</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>addresses&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DHCP DDNS Updates Deferred</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP DNS updates deferred:</td>
<td>Threshold</td>
<td>The DNS updates were deferred because of DDNS update errors.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Retried at least once:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;number of retries&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum number of deferred</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>updates since start of</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>problem episode (or restart):</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;max number&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Database Capacity Usage

<table>
<thead>
<tr>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Over 85% database capacity used.</td>
<td>Increase the database capacity.</td>
</tr>
<tr>
<td>Database capacity used is OK.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

### DNS Monitor

For invalid ports: “dns_security_port”
For invalid TXIDs: “dns_security_txid”

DNS security alert. There were `actual` DNS responses to {invalid ports | 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 arrive on invalid ports or 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 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.

1. Review the following:
   - DNS alert status
   - syslog file
2. Limit access or block connections from the primary sources.
# Object State Change Traps

<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.2.11.0</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Shutdown</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shutting down services due to database snapshot.</td>
<td>The appliance is shutting down its services while synchronizing the database with the grid master.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Shutting down services due to database snapshot.</td>
<td>The appliance is shutting down its services while synchronizing the database with the grid master.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><strong>Network Interfaces Monitoring</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LAN port link is down. Please check the connection.</td>
<td>The LAN port is up, but the link is down.</td>
<td>Check the LAN link connection.</td>
</tr>
<tr>
<td>HA port link is down. Please check the connection.</td>
<td>The HA port is up, but the link is down.</td>
<td>Check the HA link connection.</td>
</tr>
<tr>
<td>MGMT port link is down. Please check the connection.</td>
<td>The MGMT port is enabled, but the link is down.</td>
<td>Check the MGMT link connection.</td>
</tr>
<tr>
<td>LAN port link is up.</td>
<td>The LAN port link is up and running.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>HA port link is up.</td>
<td>The HA port link is up and running.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>MGMT port link is up.</td>
<td>The MGMT port link is up and running.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><strong>HA State Change from Initial to Active</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The node has become ACTIVE.</td>
<td>A node in an HA pair becomes active. The HA pair starts up.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><strong>HA State Change from Passive to Active</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The node has become ACTIVE.</td>
<td>The node changed from a passive to an active node.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><strong>HA State Change from Initial to Passive</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The node has become PASSIVE.</td>
<td>A node in an HA pair becomes passive. The HA pair starts up, and the node is not a grid master candidate.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>
### Node Connected to Grid

<table>
<thead>
<tr>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The grid member is connected to the grid master.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

### NodeDisconnected to Grid

<table>
<thead>
<tr>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The grid member is not connected to the grid master.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

### Replication State Monitoring

<table>
<thead>
<tr>
<th>Trap Description</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ha-replication-online (13)</code></td>
<td>The HA replication is online.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><code>ha-replication-offline (14)</code></td>
<td>The HA replication is offline.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

### NTP is out of sync, monitored every 30 seconds

<table>
<thead>
<tr>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The NTP server is out of synchronization.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>

### Process Started and Stopped Traps

<table>
<thead>
<tr>
<th>Trap Description</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Httpd Start</code></td>
<td>The httpd process started.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><code>Httpd Stop</code></td>
<td>The httpd process stopped.</td>
<td>No action is required.</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 11.4* 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* on page 281.
- *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 *ibNetwork Monitor* on page 282.
- *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 appliance.
- *ibSerialNumber (IbString)* provides the serial number of the Infoblox hardware platform.
- *ibNiosVersion (IbString)* provides the version of the software.
- *ibSystemMonitor* provides information about the CPU and memory utilization of the appliance. For information, see *ibSystemMonitor* on page 289.

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* on page 289.
- *ibMemberNode1ServiceStatusTable* provides status of the system and hardware services on a queried appliance. For information, see *ibMemberNode1ServiceStatusTable* on page 292.
- *ibMemberNode2ServiceStatusTable* 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 *ibMemberNode2ServiceStatusTable* on page 292.
Figure 11.4 *ibPlatformOne MIB Structure*

(3.1.1.2) ibPlatformOne MIB

(3.1.1.2.1) ibPlatformOneModule

(3.1.1.2.1.1) ibCPUTemperature

(3.1.1.2.1.2) ibClusterReplicationStatusTable → *ibClusterReplicationStatusTable Objects* on page 281

(3.1.1.2.1.3) ibNetworkMonitor → *ibNetworkMonitor Objects* on page 283

(3.1.1.2.1.4) ibHardwareType

(3.1.1.2.1.5) ibHardwareId

(3.1.1.2.1.6) ibSerialNumber

(3.1.1.2.1.7) ibNiosVersion

(3.1.1.2.1.8) ibSystemMonitor → *ibSystemMonitor Objects* on page 289

(3.1.1.2.1.9) ibMemberServiceStatusTable → *ibMemberServiceStatusTable Objects* on page 290

(3.1.1.2.1.10) ibMemberNode1ServiceStatusTable → *ibMemberNode1ServiceStatusTable Objects* on page 292

(3.1.1.2.1.11) ibMemberNode2ServiceStatusTable → *ibMemberNode2ServiceStatusTable Objects* on page 293
ibClusterReplicationStatusTable

ibClusterReplicationStatusTable (object ID 3.1.1.2.1.2.1) provides information about the Master Grid replication status. For information about Infoblox SNMP traps, see `ibTrapDesc (OID 3.1.1.1.2.11.0)` on page 266.

*Figure 11.5* shows the sub branches of `ibClusterReplicationStatusTable`.

*Figure 11.5*  *ibClusterReplicationStatusTable Objects*

![Diagram of ibClusterReplicationStatusTable](image)

*Table 11.7* provides information about the `ibClusterReplicationStatusTable` objects.

*Table 11.7*  *ibClusterReplicationStatusTable Objects*

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ibClusterReplicationStatusEntry</code></td>
<td>A conceptual row that provides information about the Master 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><code>ibNodeIPAddress (IblpAddr)</code></td>
<td>IP address of a grid member.</td>
</tr>
<tr>
<td><code>ibNodeReplicationStatus (IbString)</code></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><code>ibNodeQueueFromMaster (Integer)</code></td>
<td>“Sent” queue size from master.</td>
</tr>
<tr>
<td><code>ibNodeLastRepTimeFromMaster (IbString)</code></td>
<td>Last sent time from master.</td>
</tr>
<tr>
<td><code>ibNodeQueueToMaster (Integer)</code></td>
<td>“Receive” queue size from master.</td>
</tr>
<tr>
<td><code>ibNodeLastRepTimeToMaster (IbString)</code></td>
<td>Last receive time from master.</td>
</tr>
</tbody>
</table>
ibNetwork Monitor

As shown in Figure 11.6, the ibNetwork Monitor has one subtree, ibNetworkMonitorDNS, that branches out into the following:

- **ibNetworkMonitorDNSActive** (Integer) reports on whether DNS latency monitoring is enabled. 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* on page 285.

- **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* on page 286.

- **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)
    - **ibNetworkMonitorDNSSecurityInvalidTxidAndPortCount** (Counter)

For information, see *Table 11.10* on page 287.
Figure 11.6 *ibNetWorkMonitor Objects*

```
(3.1.1.2.1.3)
ibNetworkMonitor
   ↓
(3.1.1.2.1.3.1)
ibNetworkMonitorDNS
      ↓
(3.1.1.2.1.3.1.1)
ibNetworkMonitorDNSActive

(3.1.1.2.1.3.1.2)
ibNetworkMonitorDNSNonAA

(3.1.1.2.1.3.1.3)
ibNetworkMonitorDNSAA

(3.1.1.2.1.3.1.4)
ibNetworkMonitorDNSSecurity
      ↓
(3.1.1.2.1.3.1.4.1)
ibNetworkMonitorDNSSecurityInvalidPort

(3.1.1.2.1.3.1.4.2)
ibNetworkMonitorDNSSecurityInvalidTxid

(3.1.1.2.1.3.1.4.3)
ibNetworkMonitorDNSSecurityInvalidPortOnly

(3.1.1.2.1.3.1.4.4)
ibNetworkMonitorDNSSecurityInvalidTxidOnly

(3.1.1.2.1.3.1.4.5)
ibNetworkMonitorDNSSecurityInvalidTxidAndPort
```
Figure 11.7 \textit{ibNetworkMonitorDNSNonAA} and \textit{ibNetworkMonitorDNSAA} Subtrees

\begin{verbatim}
(3.1.1.2.1.3.1)
ibNetworkMonitorDNS
   \downarrow
(3.1.1.2.1.3.2)
ibNetworkMonitorDNSNonAA
   \downarrow
(3.1.1.2.1.3.2.1)
ibNetworkMonitorDNSNonAAT1
      \downarrow
(3.1.1.2.1.3.2.1.1)
ibNetworkMonitorDNSNonAAT1AvgLatency
(3.1.1.2.1.3.2.1.2)
ibNetworkMonitorDNSNonAAT1Count
   \downarrow
(3.1.1.2.1.3.2.2)
ibNetworkMonitorDNSNonAAT5
      \downarrow
(3.1.1.2.1.3.2.2.1)
ibNetworkMonitorDNSNonAAT5AvgLatency
(3.1.1.2.1.3.2.2.2)
ibNetworkMonitorDNSNonAAT5Count
   \downarrow
(3.1.1.2.1.3.2.3)
ibNetworkMonitorDNSNonAAT15
      \downarrow
(3.1.1.2.1.3.2.3.1)
ibNetworkMonitorDNSNonAAT15AvgLatency
(3.1.1.2.1.3.2.3.2)
ibNetworkMonitorDNSNonAAT15Count
   \downarrow
(3.1.1.2.1.3.2.4)
ibNetworkMonitorDNSNonAAT60
      \downarrow
(3.1.1.2.1.3.2.4.1)
ibNetworkMonitorDNSNonAAT60AvgLatency
(3.1.1.2.1.3.2.4.2)
ibNetworkMonitorDNSNonAAT60Count
   \downarrow
(3.1.1.2.1.3.2.5)
ibNetworkMonitorDNSNonAAT1440
      \downarrow
(3.1.1.2.1.3.2.5.1)
ibNetworkMonitorDNSNonAAT1440AvgLatency
(3.1.1.2.1.3.2.5.2)
ibNetworkMonitorDNSNonAAT1440Count

(3.1.1.2.1.3.3)
ibNetworkMonitorDNSAA
   \downarrow
(3.1.1.2.1.3.3.1)
ibNetworkMonitorDNSAAT1
      \downarrow
(3.1.1.2.1.3.3.1.1)
ibNetworkMonitorDNSAAT1AvgLatency
(3.1.1.2.1.3.3.1.2)
ibNetworkMonitorDNSAAT1Count
   \downarrow
(3.1.1.2.1.3.3.2)
ibNetworkMonitorDNSAAT5
      \downarrow
(3.1.1.2.1.3.3.2.1)
ibNetworkMonitorDNSAAT5AvgLatency
(3.1.1.2.1.3.3.2.2)
ibNetworkMonitorDNSAAT5Count
   \downarrow
(3.1.1.2.1.3.3.3)
ibNetworkMonitorDNSAAT15
      \downarrow
(3.1.1.2.1.3.3.3.1)
ibNetworkMonitorDNSAAT15AvgLatency
(3.1.1.2.1.3.3.3.2)
ibNetworkMonitorDNSAAT15Count
   \downarrow
(3.1.1.2.1.3.3.4)
ibNetworkMonitorDNSAAT60
      \downarrow
(3.1.1.2.1.3.3.4.1)
ibNetworkMonitorDNSAAT60AvgLatency
(3.1.1.2.1.3.3.4.2)
ibNetworkMonitorDNSAAT60Count
   \downarrow
(3.1.1.2.1.3.3.5)
ibNetworkMonitorDNSAAT1440
      \downarrow
(3.1.1.2.1.3.3.5.1)
ibNetworkMonitorDNSAAT1440AvgLatency
(3.1.1.2.1.3.3.5.2)
ibNetworkMonitorDNSAAT1440Count
\end{verbatim}
**Table 11.8** describes the objects in `ibNetworkMonitorDNSNonAA`. You can send queries to retrieve values for these objects.

**Table 11.8  *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><code>ibNetworkMonitorDNSNonAAT5AvgLatency (Integer)</code></td>
<td>Indicates the average latency in microseconds of nonauthoritative replies to queries in the last five minutes.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSNonAAT5Count (Integer)</code></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><code>ibNetworkMonitorDNSNonAAT15</code></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><code>ibNetworkMonitorDNSNonAAT15AvgLatency (Integer)</code></td>
<td>Indicates the average latency in microseconds of nonauthoritative replies to queries in the last 15 minutes.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSNonAAT15Count (Integer)</code></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><code>ibNetworkMonitorDNSNonAAT60</code></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><code>ibNetworkMonitorDNSNonAAT60AvgLatency (Integer)</code></td>
<td>Indicates the average latency in microseconds of nonauthoritative replies to queries in the last 60 minutes.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSNonAAT60Count (Integer)</code></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><code>ibNetworkMonitorDNSNonAAT1440</code></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><code>ibNetworkMonitorDNSNonAAT1440AvgLatency (Integer)</code></td>
<td>Indicates the average latency in microseconds of nonauthoritative replies to queries in the last 24 hours.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSNonAAT1440Count (Integer)</code></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 11.9 describes the objects in `ibNetworkMonitorDNSAA`. You can send queries to retrieve values for these objects.

### Table 11.9 `ibNetworkMonitorDNSAA` Objects

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ibNetworkMonitorDNSAAT1</code></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><code>ibNetworkMonitorDNSAAT1AvgLatency</code></td>
<td>Indicates the average latency in microseconds of authoritative replies to queries in the last minute.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSAAT1Count</code></td>
<td>Indicates the number of queries used to calculate the average latency of authoritative replies in the last minute.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSAAT5</code></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><code>ibNetworkMonitorDNSAAT5AvgLatency</code></td>
<td>Indicates the average latency in microseconds of authoritative replies to queries in the last five minutes.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSAAT5Count</code></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><code>ibNetworkMonitorDNSAAT15</code></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><code>ibNetworkMonitorDNSAAT15AvgLatency</code></td>
<td>Indicates the average latency in microseconds of authoritative replies to queries in the last 15 minutes.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSAAT15Count</code></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><code>ibNetworkMonitorDNSAAT60</code></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><code>ibNetworkMonitorDNSAAT60AvgLatency</code></td>
<td>Indicates the average latency in microseconds of authoritative replies to queries in the last 60 minutes.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSAAT60Count</code></td>
<td>Indicates the number of queries used to calculate the average latency of authoritative replies in the last 60 minutes.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSAAT1440</code></td>
<td>File that contains the objects for monitoring the average latency of authoritative replies to queries in the last 24 hours.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSAAT1440AvgLatency</code></td>
<td>Indicates the average latency in microseconds of authoritative replies to queries in the last 24 hours.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSAAT1440Count</code></td>
<td>Indicates the number of queries used to calculate the average latency of authoritative replies in the last 24 hours.</td>
</tr>
</tbody>
</table>
Table 11.10 describes the objects in ibNetworkMonitorDNSSecurity. You receive SNMP traps with these objects when you enable the following:

- SNMP traps
- DNS network monitoring
- DNS alert monitoring

Table 11.10  ibNetworkMonitorDNSSecurity Objects

<table>
<thead>
<tr>
<th>Object Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidPort</td>
<td>Tracks the number of invalid DNS responses that arrive on invalid ports. This object contains a subtree with six objects that track invalid ports within a certain time interval. For information, see Table 11.11.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTxid</td>
<td>Tracks the number of invalid TXIDs (DNS transaction IDs). For information about invalid TXIDs, see . This object contains a subtree with six objects that track invalid TXIDs within a certain time interval. For information, see Table 11.12.</td>
</tr>
</tbody>
</table>
| ibNetworkMonitorDNSSecurityInvalidPortOnly (Counter) | Tracks the number of DNS responses with both of the following conditions:  
- Arrive on invalid ports  
- Have valid TXIDs |
| ibNetworkMonitorDNSSecurityInvalidTxidOnly (Counter) | Tracks the number of DNS responses with both of the following conditions:  
- Arrive on valid ports  
- Have Invalid TXIDs |
| ibNetworkMonitorDNSSecurityInvalidPortCount (Counter) | Tracks the total number of invalid DNS responses that arrive on invalid ports. |
| ibNetworkMonitorDNSSecurityInvalidTxidCount (Counter) | Tracks the total number of DNS responses that have invalid DNS transaction IDs. |
| ibNetworkMonitorDNSSecurityInvalidTxidAndPort (Counter) | Tracks the number of DNS responses with both of the following conditions:  
- Arrive on invalid ports  
- Have invalid TXIDs |
**Table 11.11** describes the objects in ibNetworkMonitorDNSSecurityInvalidPort.

### Table 11.11  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>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 11.12** describes the objects in ibNetworkMonitorDNSSecurityInvalidTid.

### Table 11.12  ibNetworkMonitorDNSSecurityInvalidTid Objects

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTid1 (Integer)</td>
<td>Tracks the number of DNS responses that have invalid DNS transaction IDs in the last one minute.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTid5 (Integer)</td>
<td>Tracks the number of DNS responses that have invalid DNS transaction IDs in the last five minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTid15 (Integer)</td>
<td>Tracks the number of DNS responses that have invalid DNS transaction IDs in the last 15 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTid60 (Integer)</td>
<td>Tracks the number of DNS responses that have invalid DNS transaction IDs in the last 60 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTid1440 (Integer)</td>
<td>Tracks the number of DNS responses that have invalid DNS transaction IDs in the last 24 hours.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTidCount (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 11.4*, `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 11.8 ibSystemMonitor Objects*

**ibMemberServiceStatusTable**

As shown in *Figure 11.9*, `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 `ibMemberServiceStatusTable` on page 289.
- `ibServiceStatus` (Integer) reports the status of the Infoblox services. For a list of service status, see *Service Status* on page 290.
- `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 `ibMemberNode1ServiceStatusTable` and `ibMemberNode2ServiceStatusTable` that display system and hardware status on the queried appliance. For information, see `ibMemberNode1ServiceStatusTable` on page 292 and `ibMemberNode2ServiceStatusTable` on page 292.
**Figure 11.9 ibMemberServiceStatusTable Objects**

![Diagram of ibMemberServiceStatusTable objects](image)

**Service Status**

When you query the service status on an appliance, the response includes the status of the services. *Table 11.13* shows the values and descriptions of the status. Note that for internal Master Grid operations, the NTP service is always in the “working” state even if it has been disabled through the Infoblox GUI.

*Table 11.13*  *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>

**System and Hardware Service Names**

*Table 11.14* lists the values and descriptions of the system and hardware services that appear in ibMemberServiceStatusTable, ibMemberNode1ServiceStatusTable, and ibMemberNode2ServiceStatusTable.

*Table 11.14*  *Values of ibServiceNames*

<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>TFTP file distribution</td>
</tr>
<tr>
<td>5</td>
<td>http-file-dist</td>
<td>HTTP file distribution</td>
</tr>
<tr>
<td>Value</td>
<td>Description</td>
<td>Definition</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>6</td>
<td>ftp</td>
<td>FTP file distribution</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 service</td>
</tr>
<tr>
<td>9</td>
<td>node-status</td>
<td>Node 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 1 port</td>
</tr>
<tr>
<td>12</td>
<td>enet-lan2</td>
<td>LAN 2 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>Virtual memory</td>
</tr>
<tr>
<td>17</td>
<td>replication</td>
<td>Replication process</td>
</tr>
<tr>
<td>18</td>
<td>db-object</td>
<td>Database usage</td>
</tr>
<tr>
<td>19</td>
<td>raid-summary</td>
<td>Summary of the RAID array</td>
</tr>
<tr>
<td>20</td>
<td>raid-disk1</td>
<td>Disk 1 of the RAID array (for Infoblox-2000, -2000-A, and -4010)</td>
</tr>
<tr>
<td>21</td>
<td>raid-disk2</td>
<td>Disk 2 of the RAID array (for Infoblox-2000, -2000-A, and -4010)</td>
</tr>
<tr>
<td>22</td>
<td>raid-disk3</td>
<td>Disk 3 of the RAID array (for Infoblox-2000, -2000-A, and -4010)</td>
</tr>
<tr>
<td>23</td>
<td>raid-disk4</td>
<td>Disk 4 of the RAID array (for Infoblox-2000, -2000-A, and -4010)</td>
</tr>
<tr>
<td>24</td>
<td>fan1</td>
<td>FAN 1 status</td>
</tr>
<tr>
<td>25</td>
<td>fan2</td>
<td>FAN 2 status</td>
</tr>
<tr>
<td>26</td>
<td>fan3</td>
<td>FAN 3 status</td>
</tr>
<tr>
<td>27</td>
<td>power-supply</td>
<td>Power supply</td>
</tr>
<tr>
<td>28</td>
<td>ntp-sync</td>
<td>NTP service synchronization</td>
</tr>
<tr>
<td>29</td>
<td>cpu1-temp</td>
<td>CPU 1 temperature</td>
</tr>
<tr>
<td>30</td>
<td>cpu2-temp</td>
<td>CPU 2 temperature</td>
</tr>
<tr>
<td>31</td>
<td>sys-temp</td>
<td>System temperature</td>
</tr>
<tr>
<td>32</td>
<td>raid-battery</td>
<td>RAID battery</td>
</tr>
<tr>
<td>33</td>
<td>cpu-usage</td>
<td>CPU usage</td>
</tr>
<tr>
<td>34</td>
<td>ospf</td>
<td>Anycast using OSPF</td>
</tr>
<tr>
<td>35</td>
<td>bgp</td>
<td>Anycast using BGP</td>
</tr>
<tr>
<td>36</td>
<td>mgm-service</td>
<td>Multi-Grid management service</td>
</tr>
<tr>
<td>37</td>
<td>subgrid-conn</td>
<td>Connection between the Master Grid and managed Grid</td>
</tr>
<tr>
<td>38</td>
<td>network-capacity</td>
<td>Network capacity</td>
</tr>
</tbody>
</table>
Monitoring with SNMP

ibMemberNode1ServiceStatusTable

As shown in Figure 11.10, ibMemberNode1ServiceStatusTable (object ID 3.1.1.2.1.10) has one subtree, ibMemberNode1ServiceStatusEntry, which contains the following objects:

- ibMemberNode1ServiceName (String) reports the names of the system and hardware services. For a list of service names, see Service Names on page 290.
- ibMemberNode1ServiceStatus (Integer) reports the status of the services. For a list of service status, see Service Status on page 290.
- ibMemberNode1ServiceDesc (String) describes the details of the status.

ibMemberNode1ServiceStatusTable 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 ibMemberNode2StatusTable to get the status of the passive node. For information, see ibMemberNode2ServiceStatusTable on page 292.

Note: For an independent appliance and the passive node of an HA pair, no information is returned when you query ibMemberNode2ServiceStatusTable.

Figure 11.10  ibMemberNode1ServiceStatusTable Objects

ibMemberNode2ServiceStatusTable

As shown in Figure 11.11, ibMemberNode2ServiceStatusTable (object ID 3.1.1.2.1.11) has one subtree, ibMemberNode2ServiceStatusEntry, which contains the following objects:

- ibMemberNode2ServiceName (String) reports the names of the system and hardware services. For a list of service names, see .
- ibMemberNode2ServiceStatus (Integer) reports the status of the services. For a list of possible service status, see Service Status on page 290.
- ibMemberNode2ServiceDesc (String) describes details of the status.

ibMemberNode2ServiceStatusTable 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 11.11  *ibMemberNode2ServiceStatusTable Objects*

```
(3.1.1.2.1.11)
ibMemberNode2ServiceStatusTable

(3.1.1.2.1.11.1)
ibMemberNode2ServiceStatusEntry

(3.1.1.2.1.11.1.1)
ibMemberNode2ServiceName

(3.1.1.2.1.11.1.2)
ibMemberNode2ServiceStatus

(3.1.1.2.1.11.1.3)
ibMemberNode2ServiceDesc
```
**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 11.12* 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* on page 295.
- ibDHCPStatistics maintains counters for different types of packets. For information, see *ibDHCPStatistics* on page 296.
- 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* on page 297.

*Figure 11.12  ibDHCPModule*
**ibDHCPSubnetTable**

`ibDHCPSubnetTable` provides statistical data about the DHCP operations of the appliance. It contains the following objects:

**Table 11.15 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>
<tr>
<td>ibDHCPSubnetNetworkAddress (IbIpAddr)</td>
<td>The subnetworks, in IP address format, that have IP addresses for lease. A subnetwork may have many address ranges for lease.</td>
</tr>
<tr>
<td>ibDHCPSubnetNetworkMask (IbIpAddr)</td>
<td>The subnet mask in dotted decimal format.</td>
</tr>
<tr>
<td>ibDHCPSubnetPercentUsed (Integer)</td>
<td>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.</td>
</tr>
</tbody>
</table>

Following is an example of the table as viewed through a MIB browser:

**Figure 11.13 MIB Browser View 1**
**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 11.16  *ibDHCPStatistics*

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibDhcpTotalNoOfDiscovers</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</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</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</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</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</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</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</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</td>
<td>The total number of DHCP messages other than those used in negotiation, such as DHCPFORCE 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 11.17  *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 11.14* 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* on page 299.
- **ibDHCPv6Statistics** maintains counters for different types of packets. For information, see *ibDHCPv6Statistics* on page 300.
- **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* on page 301.

*Figure 11.14  ibDHCPv6Module*
ibDHCPv6SubnetTable

ibDHCPv6SubnetTable provides statistical data about the DHCPv6 operations of the appliance. It contains the following objects:

Table 11.18  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 11.19 ibDHCPv6Statistics

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibDhcpv6TotalNoOfSolicits (Counter)</td>
<td>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.</td>
</tr>
<tr>
<td>ibDhcpv6TotalNoOfRequests (Counter)</td>
<td>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.</td>
</tr>
<tr>
<td>ibDhcpv6TotalNoOfReleases (Counter)</td>
<td>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.</td>
</tr>
<tr>
<td>ibDhcpv6TotalNoOfAdvertises (Counter)</td>
<td>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.</td>
</tr>
<tr>
<td>ibDhcpv6TotalNoOfReplies (Counter)</td>
<td>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.</td>
</tr>
<tr>
<td>ibDhcpv6TotalNoOfRenews (Counter)</td>
<td>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.</td>
</tr>
<tr>
<td>ibDhcpv6TotalNoOfRebinds (Counter)</td>
<td>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.</td>
</tr>
<tr>
<td>ibDhcpv6TotalNoOfDeclines (Counter)</td>
<td>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.</td>
</tr>
<tr>
<td>ibDhcpv6TotalNoOfInformationRequests (Counter)</td>
<td>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.</td>
</tr>
<tr>
<td>ibDhcpv6TotalNoOfOthers (Counter)</td>
<td>The total number of DHCP messages other than those used in negotiation.</td>
</tr>
</tbody>
</table>
ibDHCPv6DDNSSStats

ibDHCPv6DDNSSStats monitors the average latency for the DHCPv6 DDNS updates in microseconds and the number of timeouts during different time intervals. The ibDHCPv6DDNSSStats module contains the following objects:

*Table 11.20  ibDHCPStatistics*

<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 statistical information about the DNS processes and about the views and zones in the database. Figure 11.15 illustrates the structure of the ibDNSOne MIB. (Note that the OIDs shown in the illustration do not include the prefix 1.3.6.1.4.1.7779.) The ibDNSOne MIB contains four subtrees, ibZoneStatisticsTable, ibZonePlusViewStatisticsTable, ibDDNSUpdateStatistics, and ibBindZoneTransferCount (Counter64).

Figure 11.15 ibDNSOne MIB
**ibZoneStatisticsTable**

ibZoneStatisticsTable provides statistical data about the DNS operations on the appliance. The syntax of these objects 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 11.21 ibZoneStatisticsTable*

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibBindZoneName (IbString)</td>
<td>DNS Zone name.</td>
</tr>
<tr>
<td>ibBindZoneSuccess (Counter64)</td>
<td>The number of successful responses since the DNS process started.</td>
</tr>
<tr>
<td>ibBindZoneReferral (Counter64)</td>
<td>The number of DNS referrals since the DNS process started.</td>
</tr>
<tr>
<td>ibBindZoneNxRRset (Counter64)</td>
<td>The number of DNS queries received for non-existent records.</td>
</tr>
<tr>
<td>ibBindZoneNxDomain (Counter64)</td>
<td>The number of DNS queries received for non-existent domains.</td>
</tr>
<tr>
<td>ibBindZoneRecursion (Counter64)</td>
<td>The number of queries received using recursion since the DNS process started.</td>
</tr>
<tr>
<td>ibBindZoneFailure (Counter64)</td>
<td>The number of failed queries since the DNS process started.</td>
</tr>
</tbody>
</table>

**ibZonePlusViewStatisticsTable**

ibZonePlusViewStatisticsTable provides statistical data about DNS views and their zones. It contains the following objects:

*Table 11.22 ibZonePlusViewStatisticsTable*

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibBindZonePlusViewName (IbString)</td>
<td>The zone name. The first one in the default view is the global summary statistics. Index name for global statistics is “summary.”</td>
</tr>
<tr>
<td>ibBindZonePlusViewSuccess (Counter64)</td>
<td>Number of successful responses since the DNS process started.</td>
</tr>
<tr>
<td>ibBindZonePlusViewReferral (Counter64)</td>
<td>Number of DNS referrals</td>
</tr>
<tr>
<td>ibBindZonePlusViewNxRRset (Counter64)</td>
<td>Number of DNS queries received for non-existent records.</td>
</tr>
</tbody>
</table>
Monitoring with SNMP

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibBindZonePlusViewNxDomain</td>
<td>Number of DNS queries received for non-existent domains. (Counter64)</td>
</tr>
<tr>
<td>ibBindZonePlusViewRecursion</td>
<td>Number of DNS recursive queries received (Counter64)</td>
</tr>
<tr>
<td>ibBindZonePlusViewFailure</td>
<td>Number of failed queries (Counter64)</td>
</tr>
<tr>
<td>ibBindViewName</td>
<td>View name. This is blank for default view (IbString)</td>
</tr>
</tbody>
</table>

Following is an example of the table as viewed through a MIB browser:

*Figure 11.16 MIB Browser View*
**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 11.23  ibDDNSUpdateStatistics*

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibDDNSUpdateSuccess (Counter64)</td>
<td>The number of successful dynamic DNS updates.</td>
</tr>
<tr>
<td>ibDDNSUpdateFailure (Counter64)</td>
<td>The number of all failed dynamic DNS updates, excluding those reported by the ibDDNSUpdateReject object.</td>
</tr>
<tr>
<td>ibDDNSUpdateReject (Counter64)</td>
<td>The number of dynamic DNS updates that failed because they were denied by the DNS server.</td>
</tr>
<tr>
<td>ibDDNSUpdatePrerequisiteReject (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 ibDDNSUpdateFailure object.</td>
</tr>
</tbody>
</table>

**ibBindZoneTransferCount**

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).
Appendix A 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="Active User" /></td>
<td>Active User</td>
<td>Indicates a user is active on the Microsoft server.</td>
</tr>
<tr>
<td><img src="Image" alt="Add" /></td>
<td>Add</td>
<td>Adds an object</td>
</tr>
<tr>
<td><img src="Image" alt="Add Bookmark" /></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="Arrow (Down)" /></td>
<td>Arrow (Down)</td>
<td>Moves an object down in a list</td>
</tr>
<tr>
<td><img src="Image" alt="Arrow (Up)" /></td>
<td>Arrow (Up)</td>
<td>Moves an object up in a list</td>
</tr>
<tr>
<td><img src="Image" alt="Clear" /></td>
<td>Clear</td>
<td>Clears the status of an object</td>
</tr>
<tr>
<td><img src="Image" alt="Clock" /></td>
<td>Clock</td>
<td>Displays a drop-down list for time</td>
</tr>
<tr>
<td><img src="Image" alt="Delete" /></td>
<td>Delete</td>
<td>Deletes an object</td>
</tr>
<tr>
<td><img src="Image" alt="Disabled" /></td>
<td>Disabled</td>
<td>Indicates a disabled object</td>
</tr>
<tr>
<td><img src="Image" alt="Download" /></td>
<td>Download</td>
<td>Downloads a file or data</td>
</tr>
<tr>
<td><img src="Image" alt="Edit" /></td>
<td>Edit</td>
<td>Displays the corresponding editor for modifying object configurations</td>
</tr>
<tr>
<td><img src="Image" alt="Edit" /></td>
<td>Edit</td>
<td>Displays the corresponding editor for modifying object configurations</td>
</tr>
<tr>
<td>Icon</td>
<td>Icon Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><img src="image" alt="execute_now_icon" /></td>
<td>Execute Now</td>
<td>Executes a scheduled task immediately</td>
</tr>
<tr>
<td><img src="image" alt="export_icon" /></td>
<td>Export</td>
<td>Exports data in the current panel</td>
</tr>
<tr>
<td><img src="image" alt="extensible_attribute_icon" /></td>
<td>Extensible Attribute</td>
<td>Configures extensible attributes for the selected object</td>
</tr>
<tr>
<td><img src="image" alt="flat_view_icon" /></td>
<td>Flat View</td>
<td>Displays a list of objects in a flat view</td>
</tr>
<tr>
<td><img src="image" alt="help_icon" /></td>
<td>Help</td>
<td>Displays information about an object</td>
</tr>
<tr>
<td><img src="image" alt="hierarchy_icon" /></td>
<td>Hierarchy</td>
<td>Displays objects in a hierarchical view</td>
</tr>
<tr>
<td><img src="image" alt="import_icon" /></td>
<td>Import</td>
<td>Imports a file or data</td>
</tr>
<tr>
<td><img src="image" alt="import_job_manager_icon" /></td>
<td>Import Job Manager</td>
<td>Imports CSV data</td>
</tr>
<tr>
<td><img src="image" alt="information_icon" /></td>
<td>Information</td>
<td>Displays informational data about an object</td>
</tr>
<tr>
<td><img src="image" alt="locked_icon" /></td>
<td>Locked</td>
<td>Indicates a locked object</td>
</tr>
<tr>
<td><img src="image" alt="microsoft_server_icon" /></td>
<td>Microsoft Server</td>
<td>Indicates a Microsoft server</td>
</tr>
<tr>
<td><img src="image" alt="pause_icon" /></td>
<td>Pause</td>
<td>Pauses a function</td>
</tr>
<tr>
<td><img src="image" alt="print_icon" /></td>
<td>Print</td>
<td>Prints the information in the current panel</td>
</tr>
<tr>
<td><img src="image" alt="restart_processing_icon" /></td>
<td>Restart/ Processing</td>
<td>Restarts services on the appliances or indicates a request is in progress.</td>
</tr>
<tr>
<td><img src="image" alt="refresh_icon" /></td>
<td>Refresh</td>
<td>Refreshes the current page or table</td>
</tr>
<tr>
<td><img src="image" alt="report_icon" /></td>
<td>Report</td>
<td>Displays a report, such as the capacity report</td>
</tr>
<tr>
<td><img src="image" alt="search_icon" /></td>
<td>Search</td>
<td>Searches for specific objects</td>
</tr>
<tr>
<td><img src="image" alt="selected_object_icon" /></td>
<td>Selected object</td>
<td>Selects an object in a table for a specific function</td>
</tr>
<tr>
<td><img src="image" alt="start_icon" /></td>
<td>Start</td>
<td>Starts a process</td>
</tr>
<tr>
<td><img src="image" alt="stop_icon" /></td>
<td>Stop</td>
<td>Stops a process</td>
</tr>
<tr>
<td><img src="image" alt="unlocked_icon" /></td>
<td>Unlocked</td>
<td>Indicates an unlocked object</td>
</tr>
<tr>
<td><img src="image" alt="user_profile_icon" /></td>
<td>User Profile</td>
<td>Configures a user profile</td>
</tr>
<tr>
<td><img src="image" alt="user_icon" /></td>
<td>User</td>
<td>Indicates a user has logged out of the Microsoft server.</td>
</tr>
<tr>
<td>Icon</td>
<td>Icon Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>![View Icon]</td>
<td>View</td>
<td>Lists data in the current panel or lists detailed status about an object</td>
</tr>
<tr>
<td>![Warning Icon]</td>
<td>Warning</td>
<td>Indicates a warning message</td>
</tr>
</tbody>
</table>

The following icons appear in the **Data Management** tab:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon Name</th>
<th>Description</th>
<th>Tab/Table/Panel</th>
</tr>
</thead>
</table>
| ![Configure Icon] | Configure | • Configures DHCP properties  
• Configures File Distribution properties  
• Configures Licenses | **Data Management** tab → **DHCP** tab → Toolbar  
**Data Management** tab → **DHCP** tab → Toolbar  
Grid → **Grid Manager** tab → Toolbar |
| ![Conflict Icon] | Conflict | Indicates an IP address conflict | **Data Management** tab → **IPAM** tab → Net Map |
| ![Convert Icon] | Convert | Converts an object | **Data Management** tab → **IPAM** tab → network → IP Map → Toolbar |
| ![Discovery Icon] | Discovery | Performs a network discovery | **Data Management** tab → **IPAM** tab → Toolbar |
| ![Force HA Failover Icon] | Force HA Failover | Forces an HA failover | **Data Management** tab → **DHCP** tab → Toolbar |
| ![Force Recovery Icon] | Force Recovery | Forces a recovery | **Data Management** tab → **DHCP** tab → **Members** tab → **Failover Associations** tab → Toolbar |
| ![Grid Manager Icon] | Grid Manager | Indicates the Grid Master | **Data Management** tab → **DHCP** tab → **Members** tab  
**Data Management** tab → **IPAM** tab |
| ![Grid Manager Candidate Icon] | Grid Manager Candidate | Indicates the Grid Master candidate | **Data Management** tab → **DHCP** tab → **Members** tab  
**Data Management** tab → **IPAM** tab |
| ![Grid Member Icon] | Grid Member | Indicates the Grid member | **Data Management** tab → **DHCP** tab → **Members** tab  
**Data Management** tab → **IPAM** tab |
<p>| ![Join Icon] | Join | Joins networks | <strong>Data Management</strong> tab → <strong>IPAM</strong> tab → network → Toolbar |
| ![Key-signing Key Rollover Icon] | Key-signing Key Rollover | Indicates the key-signing key that is due to rollover | <strong>Data Management</strong> tab → <strong>DNS</strong> tab |
| ![Leaf Network Icon] | Leaf Network | Indicates a leaf network | <strong>Data Management</strong> tab → <strong>IPAM</strong> tab or <strong>DHCP</strong> tab |
| ![Disabled Leaf Network Icon] | Disabled Leaf Network | Indicates a disabled leaf network | <strong>Data Management</strong> tab → <strong>IPAM</strong> tab or <strong>DHCP</strong> tab |</p>
<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon Name</th>
<th>Description</th>
<th>Tab/Table/Panel</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Microsoft Server icon" /></td>
<td>Microsoft Server</td>
<td>Indicates a Microsoft server</td>
<td>Data Management tab → DHCP tab → Members tab → Data Management tab → IPAM tab</td>
</tr>
<tr>
<td><img src="image" alt="Multi-Ping icon" /></td>
<td>Multi-Ping</td>
<td>Pings all the addresses in a network</td>
<td>Data Management tab → IPAM tab → IP Map → Toolbar</td>
</tr>
<tr>
<td><img src="image" alt="Network Container icon" /></td>
<td>Network Container</td>
<td>Indicates a non-cloud network container</td>
<td>Data Management tab → IPAM tab or DHCP tab</td>
</tr>
<tr>
<td><img src="image" alt="Network icon" /></td>
<td>Network</td>
<td>Indicates a non-cloud network</td>
<td>Data Management tab → IPAM tab or DHCP tab</td>
</tr>
<tr>
<td><img src="image" alt="Network Container (for Cloud platform appliance) icon" /></td>
<td>Network Container (for Cloud platform appliance)</td>
<td>Indicates a cloud network container</td>
<td>Cloud tab → Networks tab or Data Management tab → IPAM tab or DHCP tab</td>
</tr>
<tr>
<td><img src="image" alt="Network (for Cloud platform appliance) icon" /></td>
<td>Network (for Cloud platform appliance)</td>
<td>Indicates a cloud network</td>
<td>Cloud tab → Networks tab or Data Management tab → IPAM tab or DHCP tab</td>
</tr>
<tr>
<td><img src="image" alt="Network (Disabled) icon" /></td>
<td>Network (Disabled)</td>
<td>Indicates a disabled network</td>
<td>Data Management tab → IPAM tab or DHCP tab</td>
</tr>
<tr>
<td><img src="image" alt="Microsoft Network icon" /></td>
<td>Microsoft Network</td>
<td>Indicates a network with Microsoft servers</td>
<td>Data Management tab → IPAM tab or DHCP tab</td>
</tr>
<tr>
<td><img src="image" alt="Infoblox Network icon" /></td>
<td>Infoblox Network</td>
<td>Indicates a network with Infoblox appliances</td>
<td>Data Management tab → IPAM tab or DHCP tab</td>
</tr>
<tr>
<td><img src="image" alt="Ping icon" /></td>
<td>Ping</td>
<td>Pings an IP address</td>
<td>Data Management tab → IPAM tab → IP Map → Toolbar</td>
</tr>
<tr>
<td><img src="image" alt="Properties icon" /></td>
<td>Properties</td>
<td>Configures Grid DNS properties</td>
<td>Data Management tab → DNS tab → Toolbar</td>
</tr>
<tr>
<td><img src="image" alt="Reclaim icon" /></td>
<td>Reclaim</td>
<td>Reclaims an IP address</td>
<td>Data Management tab → IPAM tab → IP Map → Toolbar</td>
</tr>
<tr>
<td><img src="image" alt="Resize icon" /></td>
<td>Resize</td>
<td>Resizes a network</td>
<td>Data Management tab → IPAM tab → network → Toolbar</td>
</tr>
<tr>
<td><img src="image" alt="Resolve Conflict icon" /></td>
<td>Resolve Conflict</td>
<td>Resolves an IP address conflict</td>
<td>Data Management tab → IPAM tab → IP Map → Toolbar</td>
</tr>
<tr>
<td><img src="image" alt="Set Partner Down icon" /></td>
<td>Set Partner Down</td>
<td>Sets partner down</td>
<td>Data Management tab → DHCP tab → Members tab → Failover Associations tab → Toolbar</td>
</tr>
<tr>
<td><img src="image" alt="Split Network icon" /></td>
<td>Split Network</td>
<td>Splits a network</td>
<td>Data Management tab → IPAM tab → network → Toolbar</td>
</tr>
<tr>
<td><img src="image" alt="DNSSEC status icon" /></td>
<td>DNSSEC status</td>
<td>Displays status for DNSSEC</td>
<td>Data Management tab → DNS tab → Toolbar</td>
</tr>
<tr>
<td><img src="image" alt="Secondary Zone Status icon" /></td>
<td>Secondary Zone Status</td>
<td>Displays status for the secondary zone</td>
<td>Data Management tab → DNS tab</td>
</tr>
<tr>
<td><img src="image" alt="Zoom In icon" /></td>
<td>Zoom In</td>
<td>Zooms in to the selected network</td>
<td>Data Management tab → IPAM tab → Net Map</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></td>
<td>Smart Folder</td>
<td>Lists a smart folder</td>
<td>Smart Folders tab</td>
</tr>
<tr>
<td></td>
<td>Smart Folder (Group By)</td>
<td>Lists smart folders in a group-by list</td>
<td>Smart Folders tab</td>
</tr>
<tr>
<td></td>
<td>Smart Folder (Link)</td>
<td>Indicates a link to the smart folder</td>
<td>Smart Folders tab and other selectors</td>
</tr>
</tbody>
</table>

### The following icons appear in the **Grid** tab:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon Name</th>
<th>Description</th>
<th>Tab/Table/Panel</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Backup</td>
<td>Backs up the configuration file and database</td>
<td>Grid tab → Grid Manager tab → Toolbar</td>
</tr>
<tr>
<td></td>
<td>Restore</td>
<td>Restores the configuration file and database</td>
<td>Grid tab → Grid Manager tab → Toolbar</td>
</tr>
<tr>
<td></td>
<td>bloxTools</td>
<td>Performs bloxTools services</td>
<td>Grid tab → Grid Manager tab → Toolbar</td>
</tr>
<tr>
<td></td>
<td>Certificate</td>
<td>Creates, generates, uploads, or downloads an HTTPS certificate</td>
<td>Grid tab → Grid Manager tab → Toolbar</td>
</tr>
<tr>
<td></td>
<td>Control</td>
<td>Restarts, reboots, or shuts down a member</td>
<td>Grid tab → Grid Manager tab → Members tab → member → Toolbar</td>
</tr>
<tr>
<td></td>
<td>Manage Services</td>
<td>Manages member services</td>
<td>Grid tab → Grid Manager tab → Members tab → member</td>
</tr>
<tr>
<td></td>
<td>Syslog</td>
<td>Displays the syslog file</td>
<td>Grid tab → Grid Manager tab → Members tab → member → Toolbar</td>
</tr>
<tr>
<td></td>
<td>Traffic Capture</td>
<td>Captures the traffic report on a member</td>
<td>Grid tab → Grid Manager tab → Members tab → member → Toolbar</td>
</tr>
</tbody>
</table>

### 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></td>
<td>Execute Now</td>
<td>Executes a scheduled task immediately</td>
<td>Administration tab → Scheduling tab → Toolbar</td>
</tr>
<tr>
<td></td>
<td>Overlap</td>
<td>Shows overlapping permissions</td>
<td>Administration tab → Permissions tab</td>
</tr>
</tbody>
</table>
### 312  Multi-Grid Manager Administrator Guide (Rev. A) NIOS 8.2

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>⭐</td>
<td>Bookmarks</td>
<td>Lists all bookmarked objects</td>
</tr>
<tr>
<td>🗑</td>
<td>Recycle Bin</td>
<td>Lists all deleted objects</td>
</tr>
<tr>
<td>🗄</td>
<td>Smart Folders</td>
<td>Lists all smart folders</td>
</tr>
<tr>
<td>🌐</td>
<td>URL Links</td>
<td>Adds URL links</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>📊</td>
<td>Traffic Management Visualizer</td>
<td>Views GLB object map</td>
</tr>
<tr>
<td>🍀</td>
<td>DNS View Mapping</td>
<td>Maps NIOS DNS view to GLB DNS view</td>
</tr>
</tbody>
</table>

The following icons appear in Multi-Grid Manager:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>⚙</td>
<td>Apply Template</td>
<td>Applies templates</td>
</tr>
<tr>
<td>📦</td>
<td>Delta Viewer</td>
<td>Views snapshots</td>
</tr>
<tr>
<td>🌐</td>
<td>External Storage</td>
<td>Access external storage</td>
</tr>
</tbody>
</table>
# Appendix B 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</td>
<td>e)y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Matches either the regular expression before or after the vertical bar</td>
<td>a</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>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”, “aabc”, “aaabc”, and so on.</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”, such as “abc”, “aabc”, “aaabc”, and so on.</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>Matches the beginning of a text string</td>
<td>^c</td>
<td>Matches any string beginning with “c”, such as “cat”.</td>
</tr>
<tr>
<td>$</td>
<td>Matches the end of a text string</td>
<td>com$</td>
<td>Matches any string ending with “com”, such as “Infoblox.com”.</td>
</tr>
</tbody>
</table>
| [ ]              | Matches any character specified in the brackets | [03] [abcd] [15a-d] | Matches “0” or “3”.  
 |                  |                                              |          | Matches “a”, “b”, “c”, or “d”.  
 |                  |                                              |          | Matches “1”, “5”, “a”, “b”, “c”, or “d”.  |
### Regular Expressions

<table>
<thead>
<tr>
<th>Special character</th>
<th>Purpose</th>
<th>Example</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[ n-n ]</code></td>
<td>Matches single characters contained in the specified range, including the start and end points</td>
<td><code>[0-3]</code></td>
<td>Matches 0, 1, 2, and 3.</td>
</tr>
<tr>
<td><code>[a-f]</code></td>
<td></td>
<td></td>
<td>Matches a, b, c, d, e, and f.</td>
</tr>
<tr>
<td><code>{m,n}</code></td>
<td>Matches the preceding expression at least m but not more than n times.</td>
<td><code>a</code></td>
<td>Matches “aaa”, “aaaa”, and “aaaaa”.</td>
</tr>
</tbody>
</table>

**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 C 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** on page 316
  - *AC* on page 316
  - *DC* on page 316
- **Agency Compliance** on page 317
  - *FCC* on page 317
  - *Canadian Compliance* on page 317
  - *VCCI* on page 318
- **RFC Compliance** on page 318
  - *DNS RFC Compliance* on page 318
  - *DHCP RFC Compliance* on page 321
  - *DHCPv6 RFC Compliance* on page 321
  - *IDN (Internationalized Domain Names) RFC Compliance* on page 322
**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 USA 120V 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 terminations should be the appropriate size for the wires and should clamp both the insulation and conductor.*
AGENCY COMPLIANCE

The Infoblox appliance is compliant with these EMI and safety agency regulations:

Table C.1 Agency Regulation Compliance

<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 on page 318
  - DHCP RFC Compliance on page 321
  - DHCPv6 RFC Compliance on page 321
  - IDN (Internationalized Domain Names) RFC Compliance on page 322

DNS RFC Compliance

The NIOS appliance complies with the following DNS RFCs:

Table C.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>RFC Number</td>
<td>RFC Title</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</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>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 1327 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>RFC Number</td>
<td>RFC Title</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------</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>2671</td>
<td>Extension Mechanisms for DNS (EDNS0)</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>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>
<tr>
<td>4033</td>
<td>DNS Security Introduction and Requirements</td>
</tr>
<tr>
<td>4034</td>
<td>Resource Records for the DNS Security Extensions</td>
</tr>
<tr>
<td>4035</td>
<td>Protocol Modifications for the DNS Security Extensions</td>
</tr>
<tr>
<td>4641</td>
<td>DNSSEC Operational Practices</td>
</tr>
<tr>
<td>4956</td>
<td>DNS Security (DNSSEC) Opt-In</td>
</tr>
<tr>
<td>4986</td>
<td>Requirements Related to DNS Security (DNSSEC) Trust Anchor Rollover</td>
</tr>
<tr>
<td>5155</td>
<td>DNSSEC Hashed Authenticated Denial of Existence</td>
</tr>
<tr>
<td>5702</td>
<td>Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC</td>
</tr>
<tr>
<td>5936</td>
<td>DNS Zone Transfer Protocol (AXFR)</td>
</tr>
<tr>
<td>6147</td>
<td>DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers</td>
</tr>
</tbody>
</table>
DHCP RFC Compliance

The appliance complies with the following DHCP RFCs:

Table C.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</td>
</tr>
<tr>
<td>1534</td>
<td>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 C.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>
<tr>
<td>3319</td>
<td>Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers</td>
</tr>
</tbody>
</table>
**IDN (Internationalized Domain Names) RFC Compliance**

The appliance complies with the following IDN RFCs:

*Table C.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>Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework</td>
</tr>
<tr>
<td>5891</td>
<td>Internationalized 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>Internationalized 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 D 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 on page 325
- GNU Lesser General Public License on page 328
- Apache Software License, Version 2.0 on page 334
- ISC BIND Copyright on page 340
- ISC DHCP Copyright on page 341
- Julian Seward Copyright on page 341
- Carnegie Mellon University Copyright on page 342
- Thai Open Source Software Center Copyright on page 343
- Ian F. Darwin Copyright on page 343
- Lawrence Berkeley Copyright on page 344
- MIT Kerberos Copyright on page 344
- BSD License on page 345
- David L. Mills Copyright on page 346
- OpenLDAP License on page 346
- OpenSSL License on page 347
- VIM License on page 348
- ZLIB License on page 350
- Wietse Venema Copyright on page 350
- ECLIPSE SOFTWARE on page 350
- Eclipse Public License - v 1.0 on page 351
- AOP Alliance (Java/J2EE AOP standards) on page 355
- OpenJDK on page 355
• TASM on page 363
• Distributed Computing Laboratory, Emory University on page 364
• COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) on page 364
• The FreeType Project LICENSE on page 368
• The Independent JPEG Group’s JPEG software on page 372
• Net-SNMP on page 374
• The PHP License, version 3.01 on page 379
• INFO-ZIP on page 381
• MIT License on page 382
• Ehcache on page 383
• Cybox on page 383
• Dateutil on page 384
• Importlib on page 385
• Libtaxii on page 385
• Mixbox on page 386
• Stix on page 386
• PSF License Agreement for Python 2.6 on page 387
• PSF License Agreement for Python 3.5.0 on page 388
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 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.

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 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

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 of use, 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 re-link 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 such 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 Library's 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 specify that version instead if
you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the
ordinary GNU General Public License applies to all subsequent copies and derivative works
made from that copy.

This option is useful when you wish to copy part of the code of the Library into a
program that is not a library.

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 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 customer's 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 these 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 modify 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. This must be distributed under the terms of the Sections above.

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, distribute, 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), 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 Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library 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 Library.

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.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library 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.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser 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 Library 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 Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.
14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, 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

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "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 LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. 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 LIBRARY 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 LIBRARY (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 LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

"Licensor" 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 to Licensor 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 within 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 damages.

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 Package’s 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 Package’s 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 Nominium, 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.
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;

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 documentation and/or other materials
   provided with the distribution.
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, 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 BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS "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 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/)"
 *
 * 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/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "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 OpenSSL PROJECT 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 product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com). This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 */
VIM LICENSE

COPYING
Vim is Charityware. You can use and copy it as much as you like, but you are encouraged to make a donation to orphans in Uganda. Please read the file "runtime/doc/uganda.txt" for details.

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 Makefile) 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 ICDF web site, available at these mirrors:
http://icdf-holland.org/
http://www.vim.org/icdf/
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, plus 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 1). 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 RECPIENT'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
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 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
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.

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 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.
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;

   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

   1.13. You (or Your) means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License. For legal entities, You includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, control means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

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.

Sun Microsystems, Inc. is the initial license steward and may publish revised and/or new versions of this License from time to time. Each version will be given a distinguishing version number. Except as provided in Section 4.3, no one other than the license steward has the right to modify this License.

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 version 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-infringing. 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 any 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 character 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 not apply to liability for death or personal injury resulting from such party's negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to you.

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. 2.274-7014(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:

```none
"""
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
Open Source Copyright and License Statements

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 FREETYPE 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 FREETYPE 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 any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage 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, ltconfig, 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
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 UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL,
INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING
FROM THE 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.

--- Part 2: Networks Associates Technology, Inc copyright notice (BSD) ------

Copyright (c) 2001-2003, Networks Associates Technology, 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 the Networks Associates Technology, 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 3: Cambridge Broadband Ltd. copyright notice (BSD) ------

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.
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.

* The name of Cambridge Broadband Ltd. 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.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

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 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 (c) Fabasoft R&D Software GmbH & Co KG, 2003
oss@fabasoft.com
Author: Bernhard Penz <bernhard.penz@fabasoft.com>
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 one 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>.

PHP includes the Zend Engine, freely available at

This is version 2007-Mar-4 of the Info-ZIP license.
The definitive version of this document should be available at
ftp://ftp.info-zip.org/pub/infozip/license.html indefinitely and

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:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois,
Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth,
Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz,
David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko,
Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs,
Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda,
Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren,
Rich Wales, Mike White.

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.
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.

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, 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.

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.
Index

A
Active Directory
- authenticating admins 88
adding members to Master Grid 113, 125
admin groups 67
- defining permissions 72
- managing 70
admin roles 69
admins
- authenticating 80
- authenticating using Active Directory 88
- authenticating using RADIUS 83
- authenticating using TACACS+ 91
defining admin policy 94
notifying 100
password length 100
appliance status
- viewing 228, 233
audit log
- configuring 237
- sending to syslog 235

B
backing up
- guidelines for scheduled tasks 164
backup files
- creating and restoring for Master Grid 219
bookmarks 32
browsers
- limitations 18

capacity report 241
capture traffic 240
certificates
- generating a certificate signing request 22
- generating self-signed 21
- importing 22
columns
- editing 29
CPU usage status 229
CSV import 38

D
Dashboard 19, 49
detailed status
- viewing 228
DHCPv6 RFC Compliance 321
Disabling the LCD Input Buttons 176
Disconnected Grids 125
disk usage status 229
distributing software
- Master Grid 210
- to Grids 136
DNS resolvers 193
documentation
- related technical documents 13

E
Ethernet ports 177
exporting data 45
- capacity report 241
- from Smart Folders 61
extensible attributes
- 164–169
- in wizards and editors 168
Smart Folders 56
UTF-8 encoding 46

F
filters
- in global search 36
- search criteria 34
- using for Smart Folders 56
viewing permissions list 78
Finder panel 19, 25, 32
force restore
- Master Grid 224
FTP
- backup files 219
- UTF-8 encoding for file names 46

G
global search 36
- exporting results 45
Grid status
- all managed Grids 51
- listing Grids 132
- managed Grid 53, 54
- node tree 130
- Visualization tab 128
Grid Templates 137
Grids
- joining a Master Grid 123
- removing from Master Grid 132
- setting properties 133
- synchronizing with Master Grid 122
- upgrading 134
H

hardware and software requirements 17
hardware status 233
Help panel 25
high availability (HA) pair
  configuring Multi-Grid Master 107
  rebooting 196
HTTP
  redirecting to HTTPS 175
  restricting access to appliance 175
HTTPS
  defined 20

I

IDNA RFC Compliance 322
importing CSV files 38
Infoblox-1552, -1552-A
  power supply status 231
Infoblox-1852-A
  power supply status 231
Infoblox-2000, -2000-A
  power supply status 231
  RAID status 232
Informational Banner Messages 117

L

LAN2 ports
  configuring 181
  viewing status 229
languages
  supporting multiple 45
licenses
  activating 194
  managing 194
  removing 196, 198
local admins 80
Locating Snapshots and Templates 172
logging in
  creating a banner 27
  login options 27
  steps 19
login banner 27
  UTF-8 encoding 46
logs
  audit log 237
  replication 239
  syslog 234
  traffic capture 240

M

Master Grid
  adding Grids 123
  adding members 113, 125
  configuring NTP 159
  configuring syslog 234
  configuring upgrade groups 206
  distributing software 210
  distribution and upgrade status 217
  member status 52
node tree 130
promoting master candidate 118
removing a Grid 132
removing a member 117
replication status 231
restricting access 175
setting date, time, time zone 155
setting time zone 155
synchronizing Grids 122
Visualization tab 128
Master Grid members
  configuring NTP 160
  configuring syslog 235
  distribution and upgrade status 217
memory usage status 230
MGMT port
  static routes 191
  using 183
  viewing status 229
MIBs
  SNMP 250
Multi-Grid Manager
  overview 19
  setting timeout 176
Multi-Grid Master
  configuring 107
  promoting master candidate 118
  scheduled tasks after promoting 164

N

network list 148
network maps 19
  creating custom 147
  IPv4 and IPv6 networks 145
networks
  about blocks 145
  managing IPv4 and IPv6 149
  resizing 150
NIOS appliance
  managing licenses 194
  rebooting 196
  resetting 197
  restricting HTTP access 175
  shutting down 197
NIOS software
  reverting 219
  upgrading 209
NIOS versions
  uploading 134
  uploading to a Grid 135
  viewing 134, 208
NTP
   adding an authentication key 159
   authenticating 156
   using for appliances 156
   viewing status 230

P
passwords
   length for admins 100
permissions
   applying 75
   Dashboard widgets 50
   defining for admin groups 72
   defining for objects 73
   defining global 73
   for common tasks 101
   overview 72
phone home 241
ports
   configuring VPN 116
   LAN2 181
   MGMT 183
   viewing status 229
printing data 45
   capacity report 241
   in Smart Folders 61

R
RADIUS
   authenticating admins 83
RAID
   monitoring status 232
rebooting 196
remote admins
   authenticating 81
   authenticating using RADIUS 83
   creating admin groups for 94
remote console access
   enabling and disabling 175
replication status
   viewing 239
resetting NIOS appliances 197
resizing networks 150
restoring backup files 223
restoring database
   guidelines for scheduled tasks 164
reverting
   guidelines for scheduled tasks 164

S
scheduling tasks 161
search
   global 36
   setting filters 34
Security Banner Messages 117
shutting down 196
Smart Folders 55–61
   Finder panel 32
Snapshot 139
Snapshot File Naming Format 172
SNMP 243–305
   Infoblox MIBs 250
software and hardware requirements 17
software distribution 136
sorting data 29
SSH
   remote console access 175
   restrict access to MGMT port 188
SSL
   certificates 20–22
   overview 20
static routes
   configuring 189
superusers
   configuring admin groups 68
   configuring extensible attributes 164
   defining global Smart Folders 57
support bundles
   downloading 225
syslog 234–237
   exporting 45
system time
   setting date and time 155
   using NTP 156

T
tables
   customizing 29
   printing data 45
   selecting objects 29
TACACS+
   authenticating admins 91
tasks
   scheduling 161
technical support
   download support bundle 225
   enabling and disabling access 175
   restrict access to MGMT port 188
testing upgrades 136, 213
TFTP
   backup files 219
   UTF-8 encoding for file names 46
time zone
   setting for Master Grid 116, 155
timeout, setting 176
toolbar 25
tooltips 26
traffic capture tool 240
Index

U

upgrade test 136, 213
upgrading 209
  configuring upgrade groups 206
  guidelines for scheduled tasks 164
  upgrading a Grid 136
  uploading NIOS software 209
  UTF-8 encoding
    multilingual support 45