## CONTENTS

**Preface** ................................................................. 9

Document Overview .................................................... 10
Related Documentation ................................................ 11
Customer Care ............................................................ 12

**Overview** .................................................................. 13

Accessing the Infoblox CLI .......................................... 14
Infoblox CLI ............................................................... 15

**CLI Commands** .......................................................... 17

ddns_add ................................................................. 21
ddns_delete ............................................................... 22
dig ........................................................................... 23
exit .......................................................................... 25
help .......................................................................... 26
ping .......................................................................... 27
reboot ......................................................................... 28
reset all ..................................................................... 29
reset arp ..................................................................... 30
reset database ........................................................... 31
reset reporting_data .................................................. 32
reset ssh_keys ........................................................... 33
restart service ............................................................ 34
rotate log .................................................................... 35
set admin_group_acl .................................................. 36
set adp ...................................................................... 37
set auto_provision ...................................................... 38
set bfd ...................................................................... 39
set bgp log ............................................................... 40
set bloxtools ............................................................. 41
set cc_mode ............................................................... 42
set certificate_auth_admins ......................................... 43
set certificate_auth_services ....................................... 44
set connection_limit .................................................. 45
set debug ................................................................. 46
set default_revert_window ....................................... 47
set default_route ......................................................... 48
set delete_tasks_interval ........................................... 49
set dhcpd_recv_sock_buf_size ....................................... 50
set dns ................................................................. 51
set dns-accel .......................................................... 52
set dns_rtl .............................................................. 53
set dscp ................................................................. 55
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>set enable_match_recursive_only</td>
<td>56</td>
</tr>
<tr>
<td>set forced Autosync</td>
<td>57</td>
</tr>
<tr>
<td>set grid Upgrade</td>
<td>58</td>
</tr>
<tr>
<td>set ibtrap</td>
<td>60</td>
</tr>
<tr>
<td>set interface</td>
<td>61</td>
</tr>
<tr>
<td>set ip_rate_limit</td>
<td>63</td>
</tr>
<tr>
<td>set ipam_web ui</td>
<td>65</td>
</tr>
<tr>
<td>set ipv6_disable_on_dad</td>
<td>66</td>
</tr>
<tr>
<td>set ipv6_neighbor</td>
<td>67</td>
</tr>
<tr>
<td>set ipv6_ospf</td>
<td>68</td>
</tr>
<tr>
<td>set ipv6_status</td>
<td>69</td>
</tr>
<tr>
<td>set lcd keys or set lcd</td>
<td>71</td>
</tr>
<tr>
<td>set lcd_settings</td>
<td>72</td>
</tr>
<tr>
<td>set lcd_settings hwident</td>
<td>73</td>
</tr>
<tr>
<td>set license</td>
<td>74</td>
</tr>
<tr>
<td>set lines</td>
<td>75</td>
</tr>
<tr>
<td>set log_txn_id</td>
<td>76</td>
</tr>
<tr>
<td>set lom</td>
<td>77</td>
</tr>
<tr>
<td>set lower_case_ptr_dname</td>
<td>78</td>
</tr>
<tr>
<td>set membership</td>
<td>79</td>
</tr>
<tr>
<td>set mgm attached</td>
<td>80</td>
</tr>
<tr>
<td>set mld_version_1</td>
<td>81</td>
</tr>
<tr>
<td>set monitor dns</td>
<td>82</td>
</tr>
<tr>
<td>set monitor dns alert</td>
<td>83</td>
</tr>
<tr>
<td>set ms_dns_reports_sync_interval</td>
<td>84</td>
</tr>
<tr>
<td>set named_recv_sock_buf_size</td>
<td>85</td>
</tr>
<tr>
<td>set network</td>
<td>86</td>
</tr>
<tr>
<td>set nogrid</td>
<td>89</td>
</tr>
<tr>
<td>set nomastergrid</td>
<td>90</td>
</tr>
<tr>
<td>set nosafemode</td>
<td>91</td>
</tr>
<tr>
<td>set ospf</td>
<td>92</td>
</tr>
<tr>
<td>set phonehome</td>
<td>93</td>
</tr>
<tr>
<td>set port_mac_addr</td>
<td>94</td>
</tr>
<tr>
<td>set promote_master</td>
<td>95</td>
</tr>
<tr>
<td>set prompt</td>
<td>97</td>
</tr>
<tr>
<td>set recursion_query_timeout</td>
<td>98</td>
</tr>
<tr>
<td>set remote_console</td>
<td>99</td>
</tr>
<tr>
<td>set reporting_cert</td>
<td>100</td>
</tr>
<tr>
<td>set reporting_cluster_maintenance_mode</td>
<td>101</td>
</tr>
<tr>
<td>set revert_grid</td>
<td>102</td>
</tr>
<tr>
<td>set safemode</td>
<td>103</td>
</tr>
<tr>
<td>set scheduled</td>
<td>104</td>
</tr>
<tr>
<td>set security</td>
<td>105</td>
</tr>
<tr>
<td>set session_timeout</td>
<td>106</td>
</tr>
<tr>
<td>set smartnic_monitor-mode</td>
<td>107</td>
</tr>
<tr>
<td>set snmptrap</td>
<td>108</td>
</tr>
<tr>
<td>set ssl_tls_ciphers</td>
<td>109</td>
</tr>
<tr>
<td>Command</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>set ssl_tls_protocols</td>
<td>111</td>
</tr>
<tr>
<td>set ssl_tls_settings</td>
<td>112</td>
</tr>
<tr>
<td>set static_route</td>
<td>113</td>
</tr>
<tr>
<td>set support_access</td>
<td>115</td>
</tr>
<tr>
<td>set sysName</td>
<td>116</td>
</tr>
<tr>
<td>set temp_license</td>
<td>117</td>
</tr>
<tr>
<td>set term</td>
<td>120</td>
</tr>
<tr>
<td>set thresholdtrap</td>
<td>121</td>
</tr>
<tr>
<td>set traffic_capture</td>
<td>123</td>
</tr>
<tr>
<td>set txn_trace</td>
<td>125</td>
</tr>
<tr>
<td>set wins_forwarding</td>
<td>126</td>
</tr>
<tr>
<td>show admin_group_acl</td>
<td>128</td>
</tr>
<tr>
<td>show adp</td>
<td>129</td>
</tr>
<tr>
<td>show arp</td>
<td>130</td>
</tr>
<tr>
<td>show auto_provision</td>
<td>131</td>
</tr>
<tr>
<td>show bfd_details</td>
<td>132</td>
</tr>
<tr>
<td>show bgp</td>
<td>133</td>
</tr>
<tr>
<td>show bloxtools</td>
<td>134</td>
</tr>
<tr>
<td>show capacity</td>
<td>135</td>
</tr>
<tr>
<td>show cc_mode</td>
<td>136</td>
</tr>
<tr>
<td>show certificate_auth_admins</td>
<td>137</td>
</tr>
<tr>
<td>show certificate_auth_services</td>
<td>138</td>
</tr>
<tr>
<td>show config</td>
<td>139</td>
</tr>
<tr>
<td>show connections</td>
<td>140</td>
</tr>
<tr>
<td>show connection_limit</td>
<td>141</td>
</tr>
<tr>
<td>show cpu</td>
<td>142</td>
</tr>
<tr>
<td>show date</td>
<td>143</td>
</tr>
<tr>
<td>show debug</td>
<td>144</td>
</tr>
<tr>
<td>show default_route</td>
<td>145</td>
</tr>
<tr>
<td>show delete_tasks_interval</td>
<td>146</td>
</tr>
<tr>
<td>show dhcp_gss_tsig</td>
<td>147</td>
</tr>
<tr>
<td>show dhcpd_recv_sock_buf_size</td>
<td>150</td>
</tr>
<tr>
<td>show dhcpv6_gss_tsig</td>
<td>151</td>
</tr>
<tr>
<td>show disk</td>
<td>152</td>
</tr>
<tr>
<td>show dns</td>
<td>153</td>
</tr>
<tr>
<td>show dns-accel</td>
<td>154</td>
</tr>
<tr>
<td>show dns-accel-cache</td>
<td>155</td>
</tr>
<tr>
<td>show dns_gss_tsig</td>
<td>156</td>
</tr>
<tr>
<td>show dns_rrl</td>
<td>157</td>
</tr>
<tr>
<td>show dscp</td>
<td>158</td>
</tr>
<tr>
<td>show dtc_geoip</td>
<td>159</td>
</tr>
<tr>
<td>show enable_match_recursive_only</td>
<td>160</td>
</tr>
<tr>
<td>show file</td>
<td>161</td>
</tr>
<tr>
<td>show hardware_status</td>
<td>163</td>
</tr>
<tr>
<td>show hwid</td>
<td>164</td>
</tr>
<tr>
<td>show ibtrap</td>
<td>165</td>
</tr>
<tr>
<td>show interface</td>
<td>166</td>
</tr>
<tr>
<td>show ip_rate_limit</td>
<td>168</td>
</tr>
</tbody>
</table>
show ipv6_bgp ................................................................. 169
show ipv6_disable_on_dad ............................................. 171
show ipv6_neighbor ...................................................... 172
show ipv6_ospf ............................................................. 173
show lcd ................................................................. 174
show lcd_info ......................................................... 175
show lcd_settings ...................................................... 176
show license ............................................................ 177
show license_uid ....................................................... 182
show license_pool_container ......................................... 183
show log ................................................................. 184
show logfiles ........................................................... 186
show log_txn_id ........................................................ 187
show lom ................................................................. 188
show lower_case_ptr_dname .......................................... 189
show memory ........................................................... 190
show mld_version ....................................................... 191
show monitor ........................................................... 192
show monitor_dns_alert ............................................... 193
show monitor_dns_alert_status ...................................... 194
show named_recv_sock_buf_size ..................................... 195
show network .......................................................... 196
show ntp ................................................................. 197
show ospf ............................................................... 198
show phonehome ........................................................ 200
show query_capture .................................................. 201
show recursion_query_timeout ....................................... 205
show remote_console .................................................. 206
show reporting_cluster_maintenance_mode ....................... 207
show routes ............................................................. 208
show scheduled ........................................................ 209
show security .......................................................... 210
show session_timeout .................................................. 211
show smartnic .......................................................... 212
show snmp .............................................................. 213
show ssl_tls_ciphers .................................................. 214
show ssl_tls_protocols ............................................... 215
show ssl_tls_settings ................................................ 216
show static_routes ..................................................... 217
show status ............................................................. 218
show support_access .................................................. 219
show tech-support ..................................................... 220
show thresholdtrap ..................................................... 221
show traffic_capture_status ......................................... 222
show txn_trace ........................................................ 223
show upgrade_compatible ............................................ 224
show upgrade_history ................................................ 225
show uptime ........................................................... 226
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show version</td>
<td>227</td>
</tr>
<tr>
<td>show vpn_cert_dates</td>
<td>228</td>
</tr>
<tr>
<td>show wins_forwarding</td>
<td>229</td>
</tr>
<tr>
<td>shutdown</td>
<td>230</td>
</tr>
<tr>
<td>snmpget</td>
<td>231</td>
</tr>
<tr>
<td>snmpwalk</td>
<td>232</td>
</tr>
<tr>
<td>traceroute</td>
<td>233</td>
</tr>
</tbody>
</table>
Preface

This guide explains the Infoblox CLI (Command Line Interface) commands that you can use to configure and manage the NIOS appliance.

This preface describes the content and organization of this guide, how to find additional product information, and how to contact technical support. It comprises the following sections:

- **Document Overview** on page 10
  - **Documentation Organization** on page 10
  - **Conventions** on page 10
- **Related Documentation** on page 11
- **Customer Care** on page 12
  - **User Accounts** on page 12
  - **Software Upgrades** on page 12
  - **Technical Support** on page 12
Document Overview

This guide explains the CLI (Command Line Interface) commands that you can use to configure and manage the NIOS appliance from a remote terminal. For the latest Infoblox documentation, visit the Infoblox Support web site at https://support.infoblox.com/.

Documentation Organization

This guide covers the following topics.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Explains how to access the Infoblox CLI using a console port or SSHv2 client. This topic also describes the CLI conventions and outlines the basic CLI commands.</td>
</tr>
<tr>
<td>CLI Commands</td>
<td>Explains the function and usage of each command, and provides an example of the command usage and expected results.</td>
</tr>
</tbody>
</table>

Conventions

This guide follows the Infoblox documentation style conventions, as listed in the following table.

<table>
<thead>
<tr>
<th>Style</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>screen</td>
<td>Indicates session text or system information displayed on the screen.</td>
</tr>
<tr>
<td>boldface screen</td>
<td>Signifies command line entries that you type.</td>
</tr>
<tr>
<td>italic screen</td>
<td>Signifies variables that you enter for your configuration, such as file names and group names.</td>
</tr>
</tbody>
</table>

CLI syntax uses conventions that are unique to documenting command line tools. The following table provides a list of syntax delimiters and their meanings.

<table>
<thead>
<tr>
<th>Item</th>
<th>Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>{} brackets</td>
<td>Indicates a mandatory feature.</td>
</tr>
<tr>
<td>[] brackets</td>
<td>Indicates an optional feature.</td>
</tr>
<tr>
<td></td>
<td>pipe symbol</td>
</tr>
</tbody>
</table>
Variables

Infoblox uses the following variables to represent the values of the configurations that exist on your appliance. You should substitute the variables with the actual values that match your site configuration.

<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>dns_view</td>
<td>DNS view</td>
</tr>
<tr>
<td>filter_name</td>
<td>Filter name</td>
</tr>
<tr>
<td>grid_master</td>
<td>Grid master</td>
</tr>
<tr>
<td>grid_member</td>
<td>Grid member</td>
</tr>
<tr>
<td>hostname</td>
<td>Host name of an independent appliance</td>
</tr>
<tr>
<td>id_grid</td>
<td>Grid name</td>
</tr>
<tr>
<td>ip_addr</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>member</td>
<td>Grid member name</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>numerical</td>
<td>Numerical entry</td>
</tr>
<tr>
<td>zone</td>
<td>DNS zone</td>
</tr>
</tbody>
</table>

Related Documentation

Other Infoblox documentation:
- Infoblox CLI Guide
- Infoblox API Documentation
- Infoblox WAPI Documentation
- Infoblox CSV Import Reference
- Infoblox Installation Guide for the Trinzic 100 Appliance
- Infoblox Installation Guide for the 800 Series Platforms
- Infoblox Installation Guide for the 805 Series Platforms
- Infoblox Installation Guide for the 1400 Series Platforms
- Infoblox Installation Guide for the 1405 Series Platforms
- Infoblox Installation Guide for the 2200 Series Platforms
- Infoblox Installation Guide for the 2205 Series Platforms
- Infoblox Installation Guide for the 4000 Series Platforms
- Infoblox Installation Guide for the Infoblox-4010 Appliance
Customer Care

This section addresses user accounts, software upgrades, 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 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. This may cause you to lose all existing data on the appliance. You can create new administrator accounts, with or without superuser privileges. For more information, refer to the Infoblox NIOS Administrator Guide.

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.
Overview

This chapter explains how to access the Infoblox CLI (Command Line Interface) and introduces the CLI commands. This chapter is organized into the following sections:

- **Accessing the Infoblox CLI** on page 14
  - **Console Port Access** on page 14
  - **SSHv2 Client Access** on page 14
- **Infoblox CLI** on page 15
  - **CLI commands** on page 15
  - **Using CLI Help** on page 16
Accessing the Infoblox CLI

You can access the Infoblox CLI from a management system. The management system is the computer from which you configure and monitor the NIOS appliance. You can access the Infoblox CLI from the management system directly through a serial cable or remotely across an Ethernet network.

- Console port access—Access the Infoblox CLI through a direct console connection from your management system to the appliance.
- SSHv2 client access—Accessing the Infoblox CLI remotely by making an SSHv2 connection across an Ethernet network.

**Note:** Only superusers can log in to the appliance through a console connection.

Console Port Access

You can access the Infoblox CLI by using a terminal emulation program from the management system through a direct console connection.

To access the Infoblox CLI through the console port:

1. Connect a serial cable from the console port on your management system to the console port on the appliance. The appliance has a male DB-9 console port on its front panel.
2. Use the following connection settings to launch an emulation session through a serial terminal emulation program such as Hilgraeve Hyperterminal® (provided with the Windows® operating systems):
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: Xon/Xoff
3. Use the following default user name and password to log in to the Infoblox appliance:
   - admin
   - infoblox

   **Note:** User names and passwords are case-sensitive.

SSHv2 Client Access

You can access the Infoblox CLI from a remote management system. You must first enable remote console access before you can remotely access the Infoblox CLI. By default, remote console access (SSHv2 access) is disabled on the Infoblox appliance.

You can enable remote console access on the Infoblox appliance through either the Infoblox GUI or the CLI.

To enable remote console access through the Infoblox GUI:

1. Make an HTTPS or console connection to the appliance and log in to the appliance.
2. For a Grid member or Grid Master, complete the following:
   1. From the Grid tab, select the Grid Manager tab, and then click Grid Properties -> Edit from the Toolbar.
   2. In the Grid Properties editor, select the Security tab, and then select Enable Remote Console Access.
   3. Click Save & Close.
For an independent appliance, complete the following:

1. From the System tab, select the System Manager tab, and then click System Properties → Edit from the Toolbar.
2. In the System Properties editor, select the Security tab, and then select Enable Remote Console Access.
3. Click Save & Close.

To enable remote console access through the CLI:

1. From the command line, enter the following after the Infoblox > prompt:
   ```
   set remote_console
   ```
2. Enter `y` at the Enable remote console access (grid-level)? (y or n): prompt.
3. Confirm the settings.

After you enable the remote console access, you can access the Infoblox CLI from a remote location using an SSHv2 client.

To access the Infoblox CLI using an SSHv2 client:

1. On the management system, open a remote console connection through an SSHv2 client.
2. In a shell window or terminal window, log in with an account that has superuser privileges.
3. Enter the user name and host name or IP address of the appliance. For example:
   ```
   ssh admin@192.168.1.2
   ```
4. Optionally, you can launch a graphical SSHv2 client and enter the information in the appropriate fields.

---

**Infoblox CLI**

The Infoblox CLI allows you to configure and monitor the appliance from a remote console using a set of commands. Some administrative tasks, such as resetting the appliance, can be done only through the CLI. The CLI commands does not support IDNs. These commands display IDN data in punycode only. For more information about IDN, refer to the Infoblox Administrator Guide.

**CLI commands**

The basic Infoblox CLI commands are alphabetically listed in the following table.

<table>
<thead>
<tr>
<th>CLI Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Displays the help information.</td>
</tr>
<tr>
<td>ddns_add</td>
<td>Sends DDNS updates to add records.</td>
</tr>
<tr>
<td>ddns_delete</td>
<td>Sends DDNS updates to delete records.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes specific files.</td>
</tr>
<tr>
<td>dig</td>
<td>Performs a DNS lookup and prints the results.</td>
</tr>
<tr>
<td>exit</td>
<td>Exits the command interpreter.</td>
</tr>
<tr>
<td>help</td>
<td>Displays the help information.</td>
</tr>
<tr>
<td>ping</td>
<td>Sends ICMP ECHO requests to verify that the host is functioning properly.</td>
</tr>
<tr>
<td>quit</td>
<td>Exits the command interpreter.</td>
</tr>
<tr>
<td>reboot</td>
<td>Reboots the Infoblox appliance.</td>
</tr>
<tr>
<td>reset</td>
<td>Resets the system settings.</td>
</tr>
</tbody>
</table>
The reset, set, and show commands each have related commands. To view a complete list of the related commands on the remote console, go to the command prompt and enter help set or help show. For information on all available commands, see CLI Commands on page 17.

### Using CLI Help

You can display a list of available CLI commands by typing `help` at the command prompt. For example:

```
> help

?       Display help
delete  Delete files
dig     Perform a DNS lookup and print the results
exit    Exit command interpreter
help    Display help
ping    Send ICMP ECHO
quit    Exit command interpreter
reboot  Reboot device
reset   Reset system settings
set     Set current system settings
show    Show current system settings
shutdown Shutdown device
traceroute Route path diagnostic
ddns_add Send DDNS update to add a record
ddns_delete Send DDNS update to delete a record
rotate  Rotate files
```

To view a detailed explanation about a CLI command and its syntax, type `help <command>` after the command prompt. For example:

```
> help rotate

Synopsis:
    rotate log [ syslog | debug | audit | ifmapserver]
    rotate file groupname filename [ filename2, filename3, ...]

Description:
    Rotates the specified log file, up to 10 previous.
    logfiles will be preserved
```
# CLI Commands

This chapter provides information about all Infoblox CLI commands, and is organized in alphabetical order as shown in the following table.

<table>
<thead>
<tr>
<th>Commands</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>ddns_add</td>
<td>21</td>
</tr>
<tr>
<td>ddns_delete</td>
<td>22</td>
</tr>
<tr>
<td>dig</td>
<td>23</td>
</tr>
<tr>
<td>exit</td>
<td>25</td>
</tr>
<tr>
<td>help</td>
<td>26</td>
</tr>
<tr>
<td>ping</td>
<td>27</td>
</tr>
<tr>
<td>reboot</td>
<td>28</td>
</tr>
<tr>
<td>reset all</td>
<td>29</td>
</tr>
<tr>
<td>reset arp</td>
<td>30</td>
</tr>
<tr>
<td>reset database</td>
<td>31</td>
</tr>
<tr>
<td>reset reporting_data</td>
<td>32</td>
</tr>
<tr>
<td>reset ssh_keys</td>
<td>33</td>
</tr>
<tr>
<td>restart service</td>
<td>34</td>
</tr>
<tr>
<td>rotate log</td>
<td>35</td>
</tr>
<tr>
<td>set admin_group_acl</td>
<td>36</td>
</tr>
<tr>
<td>set adp</td>
<td>37</td>
</tr>
<tr>
<td>set automatic_provision</td>
<td>38</td>
</tr>
<tr>
<td>set bfd</td>
<td>39</td>
</tr>
<tr>
<td>set bgp log</td>
<td>40</td>
</tr>
<tr>
<td>set bloxtools</td>
<td>41</td>
</tr>
<tr>
<td>set cc_mode</td>
<td>42</td>
</tr>
<tr>
<td>set certificate_auth_admins</td>
<td>43</td>
</tr>
<tr>
<td>set certificate_auth_services</td>
<td>44</td>
</tr>
<tr>
<td>set connection_limit</td>
<td>45</td>
</tr>
<tr>
<td>set debug</td>
<td>46</td>
</tr>
<tr>
<td>set default_revert_window</td>
<td>47</td>
</tr>
<tr>
<td>set default_route</td>
<td>48</td>
</tr>
<tr>
<td>set delete_tasks_interval</td>
<td>49</td>
</tr>
<tr>
<td>set dhcpd_recv_sock_buf_size</td>
<td>50</td>
</tr>
<tr>
<td>set dns</td>
<td>51</td>
</tr>
<tr>
<td>set dns-accel</td>
<td>52</td>
</tr>
<tr>
<td>set dns_rrl</td>
<td>53</td>
</tr>
<tr>
<td>set dscp</td>
<td>55</td>
</tr>
<tr>
<td>set enable_match_recursive_only</td>
<td>56</td>
</tr>
<tr>
<td>set forced_autosync</td>
<td>57</td>
</tr>
<tr>
<td>set grid_upgrade</td>
<td>58</td>
</tr>
<tr>
<td>set ibtrap</td>
<td>60</td>
</tr>
<tr>
<td>set interface</td>
<td>61</td>
</tr>
<tr>
<td>set ip_rate_limit</td>
<td>63</td>
</tr>
<tr>
<td>set ipam_web_ui</td>
<td>65</td>
</tr>
<tr>
<td>set ipv6_disable_on_dad</td>
<td>66</td>
</tr>
<tr>
<td>set ipv6_neighbor</td>
<td>67</td>
</tr>
<tr>
<td>set ipv6_ospf</td>
<td>68</td>
</tr>
<tr>
<td>set ipv6_status</td>
<td>69</td>
</tr>
<tr>
<td>set lcd keys or set lcd</td>
<td>71</td>
</tr>
<tr>
<td>set lcd_settings</td>
<td>72</td>
</tr>
<tr>
<td>set lcd_settings hwident</td>
<td>73</td>
</tr>
<tr>
<td>set license</td>
<td>74</td>
</tr>
<tr>
<td>Commands</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td><code>set lines</code></td>
<td>75</td>
</tr>
<tr>
<td><code>set log_txn_id</code></td>
<td>76</td>
</tr>
<tr>
<td><code>set lom</code></td>
<td>77</td>
</tr>
<tr>
<td><code>set lower_case_ptr_dname</code></td>
<td>78</td>
</tr>
<tr>
<td><code>set membership</code></td>
<td>79</td>
</tr>
<tr>
<td><code>set mgm attached</code></td>
<td>80</td>
</tr>
<tr>
<td><code>set mld_version_1</code></td>
<td>81</td>
</tr>
<tr>
<td><code>set monitor dns</code></td>
<td>82</td>
</tr>
<tr>
<td><code>set monitor dns_alert</code></td>
<td>83</td>
</tr>
<tr>
<td><code>set ms_dns_reports_sync_interval</code></td>
<td>84</td>
</tr>
<tr>
<td><code>set named_recv_sock_buf_size</code></td>
<td>85</td>
</tr>
<tr>
<td><code>set network</code></td>
<td>86</td>
</tr>
<tr>
<td><code>set nogrid</code></td>
<td>89</td>
</tr>
<tr>
<td><code>set nomastergrid</code></td>
<td>90</td>
</tr>
<tr>
<td><code>set nosafemode</code></td>
<td>91</td>
</tr>
<tr>
<td><code>set ospf</code></td>
<td>92</td>
</tr>
<tr>
<td><code>set phonehome</code></td>
<td>93</td>
</tr>
<tr>
<td><code>set promote_master</code></td>
<td>95</td>
</tr>
<tr>
<td><code>set prompt</code></td>
<td>97</td>
</tr>
<tr>
<td><code>set recursion_query_timeout</code></td>
<td>98</td>
</tr>
<tr>
<td><code>set remote_console</code></td>
<td>99</td>
</tr>
<tr>
<td><code>set reporting_cert</code></td>
<td>100</td>
</tr>
<tr>
<td><code>set reporting_cluster_maintenance_mode</code></td>
<td>101</td>
</tr>
<tr>
<td><code>set revert_grid</code></td>
<td>102</td>
</tr>
<tr>
<td><code>set safemode</code></td>
<td>103</td>
</tr>
<tr>
<td><code>set scheduled</code></td>
<td>104</td>
</tr>
<tr>
<td><code>set security</code></td>
<td>105</td>
</tr>
<tr>
<td><code>set session_timeout</code></td>
<td>106</td>
</tr>
<tr>
<td><code>set smartnic monitor-mode</code></td>
<td>107</td>
</tr>
<tr>
<td><code>set snmptrap</code></td>
<td>108</td>
</tr>
<tr>
<td><code>set ssl_tls_ciphers</code></td>
<td>109</td>
</tr>
<tr>
<td><code>set ssl_tls_protocols</code></td>
<td>111</td>
</tr>
<tr>
<td><code>set static_route</code></td>
<td>113</td>
</tr>
<tr>
<td><code>set support_access</code></td>
<td>115</td>
</tr>
<tr>
<td><code>set sysName</code></td>
<td>116</td>
</tr>
<tr>
<td><code>set temp_license</code></td>
<td>117</td>
</tr>
<tr>
<td><code>set term</code></td>
<td>120</td>
</tr>
<tr>
<td><code>set thresholdtrap</code></td>
<td>121</td>
</tr>
<tr>
<td><code>set traffic_capture</code></td>
<td>123</td>
</tr>
<tr>
<td><code>set txns</code></td>
<td>125</td>
</tr>
<tr>
<td><code>set wins_forwarding</code></td>
<td>126</td>
</tr>
<tr>
<td><code>show admin_group_acl</code></td>
<td>128</td>
</tr>
<tr>
<td><code>show adp</code></td>
<td>129</td>
</tr>
<tr>
<td><code>show arp</code></td>
<td>130</td>
</tr>
<tr>
<td><code>show auto_provision</code></td>
<td>131</td>
</tr>
<tr>
<td><code>show bfd details</code></td>
<td>132</td>
</tr>
<tr>
<td><code>show bloxtools</code></td>
<td>134</td>
</tr>
<tr>
<td><code>show bgp</code></td>
<td>133</td>
</tr>
<tr>
<td><code>show capacity</code></td>
<td>135</td>
</tr>
<tr>
<td><code>show cc_mode</code></td>
<td>136</td>
</tr>
<tr>
<td><code>show certificate_auth_admins</code></td>
<td>137</td>
</tr>
<tr>
<td><code>show certificate_auth_services</code></td>
<td>138</td>
</tr>
<tr>
<td><code>show config</code></td>
<td>139</td>
</tr>
<tr>
<td><code>show connections</code></td>
<td>140</td>
</tr>
<tr>
<td><code>show connection_limit</code></td>
<td>141</td>
</tr>
<tr>
<td><code>show cpu</code></td>
<td>142</td>
</tr>
<tr>
<td><code>show date</code></td>
<td>143</td>
</tr>
<tr>
<td><code>show debug</code></td>
<td>144</td>
</tr>
<tr>
<td><code>show default_route</code></td>
<td>145</td>
</tr>
<tr>
<td><code>show delete_tasks_interval</code></td>
<td>146</td>
</tr>
<tr>
<td><code>show dhcp_gss_tsig</code></td>
<td>147</td>
</tr>
<tr>
<td><code>show dhcpd_recv_sock_buf_size</code></td>
<td>150</td>
</tr>
<tr>
<td><code>show dhcpv6_gss_tsig</code></td>
<td>151</td>
</tr>
<tr>
<td><code>show disk</code></td>
<td>152</td>
</tr>
</tbody>
</table>
### Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>set ssl_tls_settings</code></td>
<td>112</td>
</tr>
<tr>
<td><code>show dns-accel</code></td>
<td>154</td>
</tr>
<tr>
<td><code>show dns-accel-cache</code></td>
<td>155</td>
</tr>
<tr>
<td><code>show dns_gss_tsig</code></td>
<td>156</td>
</tr>
<tr>
<td><code>show dns_rrl</code></td>
<td>157</td>
</tr>
<tr>
<td><code>show dscp</code></td>
<td>158</td>
</tr>
<tr>
<td><code>show dtc_geoip</code></td>
<td>159</td>
</tr>
<tr>
<td><code>show enable_match_recursive_only</code></td>
<td>160</td>
</tr>
<tr>
<td><code>show file</code></td>
<td>161</td>
</tr>
<tr>
<td><code>show hardware_status</code></td>
<td>163</td>
</tr>
<tr>
<td><code>show hwid</code></td>
<td>164</td>
</tr>
<tr>
<td><code>show ibtrap</code></td>
<td>165</td>
</tr>
<tr>
<td><code>show interface</code></td>
<td>166</td>
</tr>
<tr>
<td><code>show ip_rate_limit</code></td>
<td>168</td>
</tr>
<tr>
<td><code>show ipv6_bgp</code></td>
<td>169</td>
</tr>
<tr>
<td><code>show ipv6_disable_on_dad</code></td>
<td>171</td>
</tr>
<tr>
<td><code>show ipv6_neighbor</code></td>
<td>172</td>
</tr>
<tr>
<td><code>show ipv6_ospf</code></td>
<td>173</td>
</tr>
<tr>
<td><code>show lcd</code></td>
<td>174</td>
</tr>
<tr>
<td><code>show lcd_info</code></td>
<td>175</td>
</tr>
<tr>
<td><code>show lcd_settings</code></td>
<td>176</td>
</tr>
<tr>
<td><code>show license</code></td>
<td>177</td>
</tr>
<tr>
<td><code>show license_uid</code></td>
<td>182</td>
</tr>
<tr>
<td><code>show license_pool_container</code></td>
<td>183</td>
</tr>
<tr>
<td><code>show log</code></td>
<td>184</td>
</tr>
<tr>
<td><code>show logfiles</code></td>
<td>186</td>
</tr>
<tr>
<td><code>show log_txn_id</code></td>
<td>187</td>
</tr>
<tr>
<td><code>show lom</code></td>
<td>188</td>
</tr>
<tr>
<td><code>show lower_case_ptr_dname</code></td>
<td>189</td>
</tr>
<tr>
<td><code>show memory</code></td>
<td>190</td>
</tr>
<tr>
<td><code>show mld_version</code></td>
<td>191</td>
</tr>
<tr>
<td><code>show monitor</code></td>
<td>192</td>
</tr>
<tr>
<td><code>show monitor dns alert</code></td>
<td>193</td>
</tr>
<tr>
<td><code>show ntp</code></td>
<td>197</td>
</tr>
<tr>
<td><code>show ntp_cache</code></td>
<td>198</td>
</tr>
<tr>
<td><code>show osfp</code></td>
<td>199</td>
</tr>
<tr>
<td><code>show output</code></td>
<td>200</td>
</tr>
<tr>
<td><code>show phonehome</code></td>
<td>201</td>
</tr>
<tr>
<td><code>show recursion_query_timeout</code></td>
<td>205</td>
</tr>
<tr>
<td><code>show remote_console</code></td>
<td>206</td>
</tr>
<tr>
<td><code>show reporting_cluster_maintenance_mode</code></td>
<td>207</td>
</tr>
<tr>
<td><code>show routes</code></td>
<td>208</td>
</tr>
<tr>
<td><code>show scheduled</code></td>
<td>209</td>
</tr>
<tr>
<td><code>show security</code></td>
<td>210</td>
</tr>
<tr>
<td><code>show smartnic</code></td>
<td>212</td>
</tr>
<tr>
<td><code>show static_routes</code></td>
<td>217</td>
</tr>
<tr>
<td><code>show status</code></td>
<td>218</td>
</tr>
<tr>
<td><code>show support_access</code></td>
<td>219</td>
</tr>
<tr>
<td><code>show tech-support</code></td>
<td>220</td>
</tr>
<tr>
<td><code>show thresholdtrap</code></td>
<td>221</td>
</tr>
<tr>
<td><code>show traffic_capture_status</code></td>
<td>222</td>
</tr>
<tr>
<td><code>show txnn_trace</code></td>
<td>223</td>
</tr>
<tr>
<td><code>show upgrade_compatible</code></td>
<td>224</td>
</tr>
<tr>
<td><code>show upgrade_history</code></td>
<td>225</td>
</tr>
<tr>
<td><code>show uptime</code></td>
<td>226</td>
</tr>
<tr>
<td><code>show version</code></td>
<td>227</td>
</tr>
<tr>
<td><code>show vpn_cert_dates</code></td>
<td>228</td>
</tr>
<tr>
<td><code>shutdown</code></td>
<td>230</td>
</tr>
<tr>
<td><code>snmpget</code></td>
<td>231</td>
</tr>
<tr>
<td><code>snmpwalk</code></td>
<td>232</td>
</tr>
</tbody>
</table>
### Commands

<table>
<thead>
<tr>
<th>show monitor dns alert status on page 194</th>
<th>traceroute on page 233</th>
</tr>
</thead>
</table>

*CLI Commands*

Infoblox CLI Guide (Rev. A) NIOS 8.2


**ddns_add**

The `ddns_add` command sends DDNS updates to the appliance when you add new resource records. To use this command, ensure that you have properly configured the appliance for DDNS updates. For information, refer to the *Infoblox NIOS Administrator Guide*. To update a record that contains IDN, you must enter the domain name in punycode. The appliance retains the record in punycode and does not convert punycode to IDN.

**Syntax**

```
ddns_add <domain-name> <ttl> <type> <data> [keyname:secret]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-name</td>
<td>The FQDN of the resource record being added. For example, if the name of the record is <code>dns1</code> and the forward-mapping zone name is <code>corp100.com</code>, the FQDN is <code>dns1.corp100.com</code>. For an IDN, use the punycode representation of the IDN. For example, if the name of the record is <code>域</code> and the forward-mapping zone name is <code>corp100.com</code>, the FQDN is <code>xn--cjs.corp100.com</code>.</td>
</tr>
<tr>
<td>ttl</td>
<td>The TTL value (in seconds) of the new resource record.</td>
</tr>
<tr>
<td>type</td>
<td>The record type of the new resource record. For example, enter <code>A</code> for an <code>A</code> record and <code>PTR</code> for a <code>PTR</code> record.</td>
</tr>
<tr>
<td>data</td>
<td>The RDATA of the resource record. For an IDN, use the punycode representation of the IDN. For example, enter the IP address of an <code>A</code> record or the domain name of a <code>PTR</code> record.</td>
</tr>
<tr>
<td>[keyname:secret]</td>
<td>The TSIG key name and the secret for sending DDNS updates. You must enter the TSIG key name and shared secret if the DNS zone to which the record belongs is configured with a TSIG key.</td>
</tr>
</tbody>
</table>

**Example**

```
Infoblox > ddns_add dns1.corp100.com 20 A 10.0.0.11
```
**ddns_delete**

The `ddns_delete` command sends DDNS updates to the appliance when you delete existing resource records. To use this command, ensure that you have properly configured the appliance for DDNS updates. For information, refer to the *Infoblox NIOS Administrator Guide*. To delete a record that contains IDN, you must enter the domain name in punycode.

**Syntax**

```
ddns_delete <domain-name> [type[keyname:secret]]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-name</td>
<td>The FQDN of the resource record being deleted. For example, if the name of the record is <code>dns1</code> and the forward-mapping zone name is <code>corp100.com</code>, the FQDN is <code>dns1.corp100.com</code>. For an IDN, use the punycode representation of the IDN. For example, if the name of the record is <code>域</code> and the forward-mapping zone name is <code>corp100.com</code>, the FQDN is <code>xn--cjs.corp100.com</code>.</td>
</tr>
<tr>
<td>type</td>
<td>The record type of the resource record. For example, enter <code>A</code> for an A record and <code>PTR</code> for a PTR record. This is optional.</td>
</tr>
<tr>
<td>[keyname:secret]</td>
<td>The TSIG key name and the secret for sending DDNS updates. You must enter the TSIG key name and shared secret if the DNS zone to which the record belongs is configured with a TSIG key.</td>
</tr>
</tbody>
</table>

**Example**

```
Infoblox > ddns_delete dns1.corp100.com
```
dig

The `dig` command performs a DNS lookup on a specified server and displays the results. You can also use the `inverse` command to perform a reverse DNS lookup. This command displays IDN data in punycode, if any, for the specified server. If you specify IP address of the Microsoft server in this command, the IDN data is displayed in `\xyz` format.

Syntax

```
dig [@server_address] <hostname> [type] [opt...]
dig [@server_address] <ip-address> inverse
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>server_address</code></td>
<td>The IP address of the host on which you want to perform a DNS lookup.</td>
</tr>
<tr>
<td><code>hostname</code></td>
<td>The name of the host on which you want to perform a DNS lookup.</td>
</tr>
<tr>
<td><code>ip-address</code></td>
<td>The IP address of the host on which you want to perform a DNS lookup.</td>
</tr>
<tr>
<td><code>type</code></td>
<td>You can enter any of the following for the object type (case sensitive): a,</td>
</tr>
<tr>
<td></td>
<td>a6, aaaa, afsdb, any, apl, axfr, cert, cname, dhcid, div,</td>
</tr>
<tr>
<td></td>
<td>dname, dnskey, ds, gpos, hinfo, hip, ipseckey, isdn, ixfr, key, keydata,</td>
</tr>
<tr>
<td></td>
<td>kx, loc, maila, mailb, mb, md, mf, mg, minfo, mr, mx, naptr, none, ns,</td>
</tr>
<tr>
<td></td>
<td>nsap, nsap_ptr, nsec, nsec3, nsec3param, null, nxt, opt, ptr, px, rp,</td>
</tr>
<tr>
<td></td>
<td>rrsig, rt, sig, soa, spf, srv, sshfp, tkey, tsig, txt, unspec, wks, and</td>
</tr>
<tr>
<td></td>
<td>x25. <strong>The default is</strong> a.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><code>opt</code></th>
<th>You can enter one or more of the following options:</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>\-x</code></td>
<td>(specifies the in-addr lookup)</td>
</tr>
<tr>
<td><code>\-b address</code></td>
<td>(specifies the binding to the source address)</td>
</tr>
<tr>
<td><code>\-y name:key</code></td>
<td>(specifies the named base64 tsig key)</td>
</tr>
<tr>
<td><code>+vc</code></td>
<td>(enables the TCP mode)</td>
</tr>
<tr>
<td><code>+norecurse</code></td>
<td>(disables the recursive mode)</td>
</tr>
<tr>
<td><code>+short</code></td>
<td>(disables everything except the short forms of answers)</td>
</tr>
<tr>
<td><code>+nssearch</code></td>
<td>(searches all the authoritative nameservers)</td>
</tr>
<tr>
<td><code>+trace</code></td>
<td>(traces all the delegations from the root)</td>
</tr>
<tr>
<td><code>+cdflag</code></td>
<td>(requests the server not to perform a DNSSEC validation)</td>
</tr>
<tr>
<td><code>+dnssec</code></td>
<td>(requests the server to send DNSSEC records)</td>
</tr>
<tr>
<td><code>+multiline</code></td>
<td>(displays records in multiple lines)</td>
</tr>
</tbody>
</table>
Examples

Perform a DNS lookup

Infoblox > dig @10.0.2.60 www.infoblox.com a

: <<>> DiG 9.6.1-p3 <<>> @10.0.2.60 -x www.infoblox.com a
: <1 server found>
: :: global options: +cmd
: :: Got answer:
: :: ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45283
: :: flags: qr aa rd ra: QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
: :: QUESTION SECTION:
: :: ANSWER SECTION:
: infoblox.com 600 IN A 128.242.99.236

:: Query time: 2 msec
:: SERVER: 10.0.2.60#53<10.0.2.60>
:: WHEN: Fri Feb 26 14:06:00 2010
:: MSG SIZE rcvd: 64

Perform a reverse DNS lookup

Infoblox > dig @10.0.2.60 inverse

: <<>> DiG 9.6.1-p3 <<>> @10.0.2.60 inverse
: <1 server found>
: :: global options: +cmd
: :: Got answer:
: :: ->>HEADER<<- opcode: QUERY status: NXDOMAIN, id: 37916
: :: flags: qr rd ra: QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
: :: QUESTION SECTION:
: :: AUTHORITY SECTION:
: . 10800 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2010022601 1800 900 604800 86400

:: Query time: 132 msec
:: SERVER: 10.0.2.60#53<10.0.2.60>
:: WHEN: Thu Feb 25 11:20:09 2010
:: MSG SIZE rcvd: 100
exit

The **exit**(quit) command terminates the command line interface and halts the CLI session.

**Syntax**

`exit, quit`

Both commands produce the same results. There are no arguments for either command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Terminates the current CLI session.</td>
</tr>
<tr>
<td>quit</td>
<td>Terminates the current CLI session.</td>
</tr>
</tbody>
</table>

**Examples**

Infoblox > **exit**
Good Bye
Connection to `<IP address>` closed.

Infoblox > **quit**
Good Bye
Connection to `<IP address>` closed.
help

The help command displays information about a specified CLI command. If you do not specify a command, a list of all available commands is shown.

Syntax

```
help [command]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>command</td>
<td>A variable that you substitute with any CLI command to display a description of the function and a synopsis of its usage.</td>
</tr>
</tbody>
</table>

Examples

Display a list of commands

```
Infoblox > help
```

Command Summary

```
? Display help
delete Delete files
dig Perform a DNS lookup and print the results
exit Exit command interpreter
help Display help
ping Send ICMP ECHO
quit Exit command interpreter
reboot Reboot device
reset Reset system settings
set Set current system settings
show Show current system settings
shutdown Shutdown device
traceroute Route path diagnostic
ddns_add Send DDNS update to add a record
ddns_delete Send DDNS update to delete a record
rotate Rotate files
```

Display details for a single command

```
Infoblox > help exit
```

Synopsis:

```
exit, quit
```

Description:

```
Exits the command interpreter. There are no arguments to exit.
```
**ping**

The `ping` command verifies if a remote IPv4/IPv6 host is functioning and accessible across the network. When you execute the `ping` command, it sends five (default) sequential ICMP ECHO requests to the host and displays the results.

**Syntax**

```
ping {hostname | ip_address} [ opt ]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>The name of the remote host that you want to verify.</td>
</tr>
<tr>
<td>ip_address</td>
<td>The IP address of the remote host that you want to verify.</td>
</tr>
<tr>
<td>opt</td>
<td>• <code>numerical</code> (specifies to not interpret the IP address as a DNS name)</td>
</tr>
<tr>
<td></td>
<td>• <code>src_addr</code> (specifies the starting or “from” address)</td>
</tr>
<tr>
<td></td>
<td>• <code>v6</code> (specifies you are using an IPv6 hostname)</td>
</tr>
<tr>
<td></td>
<td>• <code>broadcast</code> (allows pinging to a broadcast address)</td>
</tr>
<tr>
<td></td>
<td>• <code>ttl &lt;hops&gt;</code> (specifies the time-to-live setting for outgoing packets)</td>
</tr>
<tr>
<td></td>
<td>• <code>packetsize &lt;bytes&gt;</code> (specifies the number of data bytes to send)</td>
</tr>
<tr>
<td></td>
<td>• <code>count &lt;packets&gt;</code> (specifies number of echo_requests packets sent, default is 5, maximum is 250)</td>
</tr>
</tbody>
</table>

**Examples**

**Valid host**

```
Infoblox > ping 10.1.1.1
pinging 10.1.1.1
PING 10.1.1.1 (10.1.1.1) 56(84) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=1 ttl=64 time=0.295 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=64 time=0.102 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=64 time=0.155 ms
64 bytes from 10.1.1.1: icmp_seq=4 ttl=64 time=0.211 ms
64 bytes from 10.1.1.1: icmp_seq=5 ttl=64 time=0.265 ms
--- 10.1.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.335/0.562/1.245/0.343 ms
```

**Invalid host**

```
Infoblox > ping jsparrow
pinging jsparrow
ping: unknown host jsparrow
```
**reboot**

The `reboot` command halts and then restarts the appliance. Use this command as a last measure when the appliance appears to be hung. Rebooting the appliance clears the cache and resets the system.

**Syntax**

```
reboot
```

There are no arguments for this command.

**Example**

```
Infoblox > reboot
REBOOT THE SYSTEM? (y or n) y
```
**reset all**

The `reset all` command clears the NIOS appliance of database, configuration, and network settings. It then re-establishes the factory settings with the default IP address, gateway, and subnet mask.

The `reset all licenses` command clears database, configuration, and network settings. It also clears all licensing information from the appliance before re-establishing the factory settings.

The `reset all auto_provision` command clears database, configuration, and network settings. It also re-enables auto-provisioning and a dynamic IP address is assigned to the appliance.

**Note:** No previous data remains on the appliance after using these commands.

**Syntax**

```
reset all [licenses | auto_provision]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>licenses</td>
<td>Specifies the removal of all licenses during the process of re-establishing the factory settings on the appliance.</td>
</tr>
<tr>
<td>auto_provision</td>
<td>Auto-provisioning is re-enabled and a dynamic IP address is assigned after re-establishing the factory settings on the appliance.</td>
</tr>
</tbody>
</table>

**Examples**

**Re-establish factory settings**

```
Infoblox > reset all
```

The entire system will be reset to default settings.

WARNING: THIS WILL ERASE ALL DATA AND LOG FILES THAT HAVE BEEN CREATED ON THIS SYSTEM.

ARE YOU SURE YOU WANT TO PROCEED? (y or n): y

**Re-establish factory settings and remove all licenses**

```
Infoblox > reset all licenses
```

The entire system will be reset to default settings and all licenses will be removed.

WARNING: THIS WILL ERASE ALL DATA AND LOG FILES THAT HAVE BEEN CREATED ON THIS SYSTEM.

ARE YOU SURE YOU WANT TO PROCEED? (y or n): y

**Re-establish factory settings and re-enable auto-provisioning**

```
Infoblox > reset all auto_provision
```

The entire system will be reset to default settings and system will try to obtain a dynamic address.

WARNING: THIS WILL ERASE ALL DATA AND LOG FILES THAT HAVE BEEN CREATED ON THIS SYSTEM.

ARE YOU SURE YOU WANT TO PROCEED? (y or n): y
**reset arp**

The `reset arp` command clears the ARP (Address Resolution Protocol) cache. The ARP maps IP addresses to the hardware MAC addresses and logs them in a table which is stored in the cache. Over time, the IP address leases expire and are assigned to new devices (MAC addresses). Infoblox recommends that you periodically clear this cache to maintain valid mappings between IP addresses and MAC addresses.

**Syntax**

`reset arp`

This command has no arguments.

**Example**

```
Infoblox > reset arp
ARP cache cleared.
```
reset database

The `reset database` command removes configuration files and DNS and DHCP data from the NIOS appliance database. However, the network and licensing information remains intact. The network settings of the appliance include the IP address and subnet mask for the appliance, the IP address of the gateway, the host name, and the remote access setting.

You can use this command to diagnose problems such as the following:

- Misplacing the administrator account and password.
- Preserving the log files when clearing the database.

The `reset database auto_provision` command resets the NIOS appliance to default settings, re-enables auto-provisioning, and a dynamic IP address is assigned to the appliance.

Syntax

```
reset database [auto_provision]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto_provision</td>
<td>Auto-provisioning is re-enabled and a dynamic IP address is assigned after resetting the database of appliance.</td>
</tr>
</tbody>
</table>

Reset the database

Infoblox > `reset database`

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

Do you wish to preserve basic network settings? (y or n) **y**

Reset the database and re-enable auto-provisioning

Infoblox > `reset database auto_provision`

The entire system will be reset to default settings and system will try to obtain a dynamic address.

**WARNING:** THIS WILL ERASE ALL DATA AND LOG FILES THAT HAVE BEEN CREATED ON THIS SYSTEM. ARE YOU SURE YOU WANT TO PROCEED? (y or n): **y**
reset reporting_data

The reset reporting_data command resets all reporting data.

Syntax

reset reporting_data

This command has no arguments.

Example

Infoblox > reset reporting_data
WARNING: THIS WILL RESET ALL REPORTING DATA.
DO YOU WANT TO PROCEED? (y or n): y
ARE YOU SURE YOU WANT TO PROCEED? (y or n): y
reset ssh_keys

The reset ssh_keys command resets the SSH keys of the system.

Syntax

    reset ssh_keys

This command has no arguments.

Example

    Infoblox > reset ssh_keys
    The system's SSH keys were reset.
**restart service**

Use the **restart service** command to restart services on a member. You can start individual service on the member, provided that the service is enabled. Note that you can use this command to restart services only on single independent appliances and the active nodes of HA pairs. You cannot use this command on the Grid Master.

**Syntax**

```
restart service [dhcp | dns | tftp | http-fd | ftp | ntp | bloxTools | captive_portal]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp</td>
<td>Restart the DHCP service</td>
</tr>
<tr>
<td>dns</td>
<td>Restart the DNS service</td>
</tr>
<tr>
<td>tftp</td>
<td>Restart the TFTP service</td>
</tr>
<tr>
<td>http-fd</td>
<td>Restart the HTTP file distribution service</td>
</tr>
<tr>
<td>ftp</td>
<td>Restart the FTP service</td>
</tr>
<tr>
<td>ntp</td>
<td>Restart the NTP service</td>
</tr>
<tr>
<td>bloxTools</td>
<td>Restart the bloxTools service</td>
</tr>
<tr>
<td>captive_portal</td>
<td>Restart the captive portal service</td>
</tr>
</tbody>
</table>

**Examples**

```
Infoblox > restart service dhcp
```
rotate log

The `rotate log` command rolls, or rotates, specified log files. When the audit log, syslog file, and IF-MAP log each reaches its maximum size, the NIOS 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. The maximum file size is 100 MB for the audit log, 300 MB for the syslog file, and 120 MB for the IF-MAP log.

Files are compressed during the rotation process, adding a .gz extension following the numerical increment (file.#.gz). The first file starts with .0 and subsequent file extensions are incremented by one until it reaches nine. 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. When the eleventh file is started, the last log file (file.9.gz) is deleted, and subsequent files are renumbered accordingly.

When the debug log file reaches its maximum size, which is 300 MB, the appliance rotates it, but does not compress it. The appliance retains only one previous debug log file to which it adds a .old extension.

This command is useful for diagnostic purposes. To export a file to the management system for viewing, you can include it in the support bundle.

To download the support bundle:

1. From the Grid tab or System tab, select the Grid Manager tab or System Manager tab, and then click **Download -> Support Bundle** from the Toolbar.
2. Select all options to include configuration and core file information in the output file, then save the tar file to a secure location on the management system.

Syntax

```plaintext
rotate log {syslog | debug | audit | ifmapserver}
rotate file groupname filename [filename2, filename3, ...]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>syslog</td>
<td>Syslog file</td>
</tr>
<tr>
<td>debug</td>
<td>Debug log file</td>
</tr>
<tr>
<td>audit</td>
<td>Audit log file</td>
</tr>
<tr>
<td>ifmapserver</td>
<td>IF-MAP log file (for Infoblox Orchestration Servers only)</td>
</tr>
</tbody>
</table>

Examples

```
Infoblox > rotate log debug
The selected log file has been rotated to infoblox.log.0.gz

Infoblox > rotate log audit
The selected log file has been rotated to audit.log.0.gz

Infoblox > rotate log ifmapserver
The previous ifmapserver log has successfully been rotated
```
set admin_group_acl

Use the `set admin_group_acl disable` command to disable ACL settings for a specific admin group. You will receive an error message when you try to disable a non-existing admin group.

Syntax

```
set admin_group_acl disable <Admin Group name>
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Disables ACL settings for a specific admin group.</td>
</tr>
</tbody>
</table>

**Examples**

```
Infoblox > set admin_group_acl disable some group
ACL setting for 'some group' was disabled.
Infoblox > set admin_group_acl disable nonexistinggroup
Invalid name.
```
**set adp**

The `set adp` command enables or disables ADP (Advanced DNS Protection) on the supported platform. You can use this command only if Threat Protection (hardware based) or Threat Protection (software add-on) licenses are installed on the platform.

**Syntax**

```
set adp
```

**Commands for Threat Protection (software add-on):**

- `set adp log <level>`: Use this command to set the threat protection log level, where log level is between 0 (emergency) and 6 (info). The default value is 6 (info).
- `set adp log <emergency|alert|critical|error|warning|notice|info>`: Use this command to set the threat protection log level.
- `set adp monitor-mode <on|off>`: Use this command to enable or disable the threat protection monitor mode on the respective member and DNS Cache Acceleration feature on an IB-4030 appliance. The default value is off.

**Syntax**

```
set adp log <level>
set adp log <emergency|alert|critical|error|warning|notice|info>
set adp monitor-mode <on|off>
```

**Commands for Threat Protection (hardware-based):**

- `set adp log <level>`: Use this command to set the threat protection log level, where log level is between 0 (emergency) and 7 (debug). The default value is 6 (info).
- `set adp log <emergency|alert|critical|error|warning|notice|info|debug>`: Use this command to set the threat protection log level.
- `set adp monitor-mode <on|off>`: Use this command to enable or disable the threat protection monitor mode on the respective member. The default value is off.

**Syntax**

```
set adp log <level>
set adp log <emergency|alert|critical|error|warning|notice|info|debug>
set adp monitor-mode <on|off>
```
set auto_provision

The set auto_provision command enables and disables auto-provisioning for the NIOS appliance. You cannot enable auto-provisioning for an appliance if a static IP address is already set for an appliance. Note that auto-provisioning can be enabled only on single appliances. To view the status of auto-provisioning for a NIOS appliance, see show auto_provision on page 131.

Syntax

```
set auto_provision {on | off}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Enables auto-provisioning on an appliance.</td>
</tr>
<tr>
<td>off</td>
<td>Disables auto-provisioning on an appliance.</td>
</tr>
</tbody>
</table>

Examples

**Turn on auto-provisioning on an appliance**

```
Infoblox > set auto_provision on
```

**Turn off auto-provisioning on an appliance**

```
Infoblox > set auto_provision off
```
**set bfd**

You can use the `set bfd` command to set the BFD logging level. The default logging level is ‘informational’. Changing the BFD logging level might cause disruption in advertising due to `bfdd.conf` change. To view the detailed BFD session details, see `show bfd details` on page 132.

**Syntax**

```
set bfd log [ debugging | informational | notifications | warnings | errors |
critical | alerts | emergencies ]
```

This command has no arguments.

**Example**

```
Infoblox > set bfd log debugging
```
**set bgp log**

The `set bgp log` command sets the verbosity level of the BGP routing services and writes statistical information to the syslog. The information in syslog can be helpful for diagnostic purposes. When viewing the syslog file, lines with names such as `bgp statistics` are the BGP statistical information. To view information about the BGP protocol running on the member, see `show bgp` on page 133.

**Note:** To use this command, the NSQ software package must be installed.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debugging</td>
<td>The verbosity level at which you select to write BGP statistics to syslog.</td>
</tr>
<tr>
<td>informational</td>
<td></td>
</tr>
<tr>
<td>notifications</td>
<td></td>
</tr>
<tr>
<td>warnings</td>
<td></td>
</tr>
<tr>
<td>errors</td>
<td></td>
</tr>
<tr>
<td>critical</td>
<td></td>
</tr>
<tr>
<td>alerts</td>
<td></td>
</tr>
<tr>
<td>emergencies</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
Infoblox > set bgp log
```
**set bloxtools**

You can use the `set bloxtools` command to permanently remove the bloxTools environment and all its data from the appliance. You can also use this command to clear only the user uploaded data and reset the bloxTools environment to the factory default.

**WARNING:** When you use this command, bloxTools data is permanently removed from the appliance.

To view the bloxTools status, see *show bloxtools* on page 134.

You can download a copy of the existing bloxtools data using an FTP or SFTP client before you use this command to permanently delete the data. For information, refer to the *Infoblox NIOS Administrator Guide*.

**Note:** bloxTools data files are not automatically removed when the bloxTools environment is disabled. You must use this command to manually delete bloxTools data.

**Syntax**

```
set bloxtools reset {all | data}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Clears all bloxtools related files, which include both the system and data files. You can use this argument to remove the entire bloxtools environment and its data from your appliance.</td>
</tr>
<tr>
<td>data</td>
<td>Clears only the user uploaded data that is related to bloxTools and reset the bloxTools environment to the factory default.</td>
</tr>
</tbody>
</table>

**Examples**

**Delete all bloxtools data files**

```
Infoblox > set bloxtools reset all
This will erase all Bloxtools data permanently.
Do you want to proceed? (y or n): y
Are you sure you want to do this (y or n):
Bloxtools reset.
```

**Delete bloxtools user data**

```
Infoblox > set bloxtools reset data
This will erase all Bloxtools data permanently.
Do you want to proceed? (y or n): y
Are you sure you want to do this (y or n):
Bloxtools reset.
```
set cc_mode

You can use the `set cc_mode` command to set the Common Criteria mode. To enable or disable Common Criteria configuration, connect to the CLI console, and then enter the `set cc_mode` command. This command will restart the system when it exits the Common Criteria mode. If the system is enabled for Common Criteria, it will reboot in order to go through boot time self tests. You can use this command only on the Grid Master. The setting is propagated to all Grid members. You must restart the members after the configuration change. You can use the `reset all` command to clear the Common Criteria mode. For information about `reset all`, see `reset all` on page 29.

**Note:** Factory reset must be done before using the Common Criteria mode.

**Syntax**

```
set cc_mode
```

This command has no arguments.

**Examples**

```
Infoblox > set cc_mode
Enable Common Criteria mode (grid-level)? (y or n): y
New Common Criteria Mode Settings:
    Common Criteria mode enabled: Yes
    is this correct? (y or n): y
Please refer to the Guidance Documentation Supplement Appendix of the NIOS Administrator Guide for the requirements to operate a grid in a common criteria compliant manner.
The system will be rebooted to place it into common criteria mode.
Are you sure you want to continue (y or n): y

SYSTEM REBOOTING!

Connection to 10.35.111.3 closed.
```
set certificate_auth_admins

Use the `set certificate_auth_admins` command to disable the certificate authentication service and allow users to log in without validation. Note that when you disable the certificate authentication service, the appliance terminates administrative sessions for all admin users.

**Syntax**

```
set certificate_auth_admins disable username
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>Disables certificate authentication service and allows users to log in without validation.</td>
</tr>
</tbody>
</table>

**Examples**

```
Infoblox > set certificate_auth_admins disable admin
Certificate authentication for 'admin' was disabled.
```
**set certificate_auth_services**

Use the `set certificate_auth_services disable name` command to disable a specific certificate authentication service. You will receive an error message when you try to disable a non-existing certificate authentication service.

**Syntax**

```
set certificate_auth_services disable name
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Disables specified certificate authentication service.</td>
</tr>
</tbody>
</table>

**Examples**

```
Infoblox > set certificate_auth_services disable name
Certificate authentication for 'name' was disabled.
Infoblox > set certificate_auth_services disable DoD CaC
Certificate Authentication Service for 'DoD CaC' was disabled.
Infoblox > set certificate_auth_services disable Some Name
Invalid Name.
```
set connection_limit

You can use the set connection_limit command to set the per client IP address maximum connection limit for the following protocols: HTTP and HTTPS. Note that maximum connections here refer to the network level connections, not application level connections. For example, an HTTPS connection limit of 4 means that there can be a maximum of four TCP connections between any given client IP address and the appliance using the HTTPS protocol. Valid values are from 0 to 2147483647, where 0 means no limit. The default value is 20 for all protocols.

**Note:** Setting a low connection limit may have a negative effect on client functionality. For example, some versions of the Firefox browser require at least four TCP connections to function correctly with the appliance. Setting an HTTPS connection limit below four may result in certain browser issues.

To view the current connection limit, see show connection_limit on page 141.

**Syntax**

set connection_limit {http | https}

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>http</td>
<td>Setting maximum connection limit for the HTTP protocol. Valid values are from 0 to 2147483647. The default value is 20.</td>
</tr>
<tr>
<td>https</td>
<td>Setting maximum connection limit for the HTTPS protocol. Valid values are from 0 to 2147483647. The default value is 20.</td>
</tr>
</tbody>
</table>

**Examples**

**Set the Per Client Address Maximum Connection Limit for the HTTP Protocol**

Infoblox > set connection_limit http 150
set debug

The `set debug` command enables and disables debug logging for the NIOS appliance. Debug logging is the most extensive and verbose logging that is available on the appliance. It captures all levels of messaging. The output is written into the debug log file. For information on how to view this output, see `show log` on page 184.

Use this command to capture specific occurrences. However, only use it for short periods of time. Do not leave it running for extended periods of time. Due to the amount of data that is captured, leaving this feature running for any length of time can affect the performance of the appliance. For this reason, it is best to use this command during non-peak hours.

**Note:** Infoblox recommends that you turn debug logging off, unless Infoblox Support specifically directs you to turn this feature on. If you leave debug logging turned on, it can cause performance issues.

**Syntax**

```
set debug {on | off}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies debug logging for all services as enabled or disabled.</td>
</tr>
<tr>
<td>on</td>
<td>Enables debug logging.</td>
</tr>
<tr>
<td>off</td>
<td>Disables debug logging.</td>
</tr>
</tbody>
</table>

**Examples**

**Enable debugging**

```
Infoblox > set debug all on
Enabled debug logging for: all
```

**Disable debugging**

```
Infoblox > set debug all off
Disabled debug logging for: all
```
**set default_revert_window**

Use the `set default_revert_window` command to configure the Grid default time window for reverting a member after it was upgraded from NIOS 6.4.0 to a later release. Note that you can only change the default value on the Grid Master. When you change the default value, the new revert window affects only the members that have not been upgraded.

**Syntax**

```
set default_revert_window hours
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hours</td>
<td>The number of hours configured for the default revert window. The minimum value is 1 and the maximum is 48. The default is 24.</td>
</tr>
</tbody>
</table>

**Example**

```
Infoblox > set default_revert_window 36
Member revert window is currently: 24h
Member Revert Window being changed to 36 hours
Is this correct? (y or n): y
Member Revert Window change will only affect members which are not yet upgraded.

Member Revert Window is changed.
```
**set default_route**

The `set default_route` command allows you to configure the default gateway for the NIOS appliance. You can set the gateway address of LAN1 or LAN2 as the default route. You can also specify the IPv4 or IPv6 gateway address. You can also set an optional VLAN gateway address and make it the default route.

**Syntax**

```
set default_route LAN1|LAN2
set default_route IPv4gateway [IPv6gateway] | IPv6gateway [IPv4gateway]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN1</td>
<td>Specifies the LAN1 gateway address.</td>
</tr>
<tr>
<td>LAN2</td>
<td>Specifies the LAN2 gateway address.</td>
</tr>
<tr>
<td>IPv4gateway</td>
<td>Specifies the IPv4 gateway address.</td>
</tr>
<tr>
<td>IPv6gateway</td>
<td>Specifies the IPv6 gateway address.</td>
</tr>
</tbody>
</table>

**Example**

```
Infoblox > set default_route LAN1
Infoblox > set default_route LAN2
Infoblox > set default_route 10.35.0.1 2620:10a:6000:2400::1
Infoblox > set default_route 2620:10a:6000:2400::1
```
set delete_tasks_interval

Use the `set delete_tasks_interval` command to configure the time interval the appliance waits until it deletes completed and rejected tasks from the system. Grid Manager displays these tasks in the Task Manager tab until they are deleted from the system. By default, Grid Manager displays these tasks for 14 days. You can configure this time interval. Valid values are from 1 to 30 days.

Use the `show delete_tasks_interval` command to view the current time interval. For information, see `show delete_tasks_interval` on page 146.

**Syntax**

```
set delete_tasks_interval days
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>days</td>
<td>The number of days completed and rejected tasks are displayed in the Task Manager tab before they are deleted. The minimum value is 1 and the maximum is 30. The default is 14.</td>
</tr>
</tbody>
</table>

**Example**

```
Infoblox > set delete_tasks_interval 25
Current delete tasks interval is 14 days
The delete tasks interval has been changed to 25 days
Is this correct? (y or n): y
The delete tasks interval has been changed.
```
set dhcpd_recv_sock_buf_size

You can use the `set dhcpd_recv_sock_buf_size` command to tune the DHCP receive socket buffer memory. The DHCP receive socket buffer holds DHCP packets that are queued on the UDP (User Datagram Protocol) port from the NIC (Network Interface Controller). This command is useful when you want to increase the DHCP receive buffer size to accommodate occasional burst traffic and high volume DHCP requests. Use the `show dhcpd_recv_sock_buf_size` to view the current buffer size.

**Note:** Ensure that you use this command only when you are dealing with burst traffic situations in high volume deployments.

**Syntax**

```
set dhcpd_recv_sock_buf_size N [120 <= N <= 8192, 1536=default]
```

**Examples**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>N</code></td>
<td>The number of kilobytes to which you want to set the BIND receive socket buffer size. The minimum is 120 kilobytes and the maximum is 8192. The default is 1536.</td>
</tr>
</tbody>
</table>

Infoblox > `set dhcpd_recv_sock_buf_size 1500`

DHCP service restart is required in order for the changed value to take effect.
set dns

The `set dns` command enables you to control the DNS cache. You can flush the cache file of a DNS view or flush a particular entry from a cache file. You can also flush a specific domain and its subdomains from the DNS cache. In addition, you can schedule an inbound zone transfer from an external primary server. This command displays IDN data in punycode. You can also use this command to delete cache files from the default DNS view for DNS cache acceleration on IB-FLEX.

Syntax

```
set dns flush all [dns_view]
set dns flush name name [dns_view]
set dns transfer zone [dns_view]
set dns flush tree <part-of-domain-name> [dns_view]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Flushes the cache file from the default view.</td>
</tr>
<tr>
<td>dns_view</td>
<td>Specifies a particular DNS view.</td>
</tr>
<tr>
<td>name</td>
<td>Flushes the specific entry from the cache.</td>
</tr>
<tr>
<td>zone</td>
<td>Specifies the zone for the inbound transfer from an external primary server.</td>
</tr>
<tr>
<td>tree &lt;part-of-domain-name&gt;</td>
<td>Flushes the specified domain and its subdomains from the DNS cache. For example, if you enter the domain name corp100.com, then the specified domain and its subdomains such as <a href="http://www.corp100.com">www.corp100.com</a>, corp100.com, x.corp100.com, etc. are cleared from the DNS cache.</td>
</tr>
</tbody>
</table>

Example

Flush the cache file from the default DNS view

```
Infoblox > set dns flush all
```

Flush the specified domain and its subdomains from the default DNS view

```
Infoblox > set dns flush tree xyz.com default
```
set dns-accel

The set dns-accel command enabled you to set certain parameters for the DNS Cache Acceleration feature. This command is available for:

• IB-4030 appliances only when the DNS Cache Acceleration license is present.
• IB-FLEX only if the Flex Grid Activation license is present in the Grid.

Syntax

```
set dns-accel log <level>
set dns-accel log <emergency|alert|critical|error|warning|notice|info|debug>
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level</td>
<td>The DNS Cache Acceleration log level, where log level is between 0 and 7, and the default value is 6.</td>
</tr>
<tr>
<td>&lt;emergency</td>
<td>alert</td>
</tr>
</tbody>
</table>

Example

```
Infoblox > set dns-accel log 2
Infoblox > set dns-accel log notice
```
**set dns_rrl**

Use the `set dns_rrl` command to configure RRL (Response Rate Limiting) settings for the Grid or members. Changes made using this command are applied immediately to an active DNS resolver, although there could be replication delays for Grid Master configuration of other members. Use the `show dns_rrl` on page 157 to view the current RRL settings.

**Syntax**

```
set dns_rrl enable
set dns_rrl disable
set dns_rrl [member <hostname> | view <viewname>] [override|inherit]
set dns_rrl [member <hostname> | view <viewname>] [enable|disable]
set dns_rrl [member <hostname> | view <viewname> | grid]
    [responses_per_second <number>|disable] [window <number>|default]
    [slip <number>|default|disable] [logging enable|disable|default]
    [log_only true|false|default]
```

**Note:** The `set dns_rrl` command accepts the `member`, `view`, and `grid` options only on the Grid Master.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Enable RRL with previously configured values.</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>Disable RRL.</td>
</tr>
<tr>
<td><code>member &lt;hostname&gt;</code></td>
<td>The FQDN of the Grid member.</td>
</tr>
<tr>
<td><code>view &lt;viewname&gt;</code></td>
<td>The name of the DNS view.</td>
</tr>
<tr>
<td>`override</td>
<td>inherit`</td>
</tr>
<tr>
<td><code>responses_per_second &lt;number&gt;</code></td>
<td>The number of DNS responses per second for the RRL. Valid values are from 1 to 1000. Although the BIND default is 0, which means there is no limit or RRL is disabled, you cannot set this to 0 in NIOS. Use the “disable” argument to disable this feature. The default is 100.</td>
</tr>
<tr>
<td>`window &lt;number&gt;</td>
<td>default`</td>
</tr>
<tr>
<td>`slip &lt;number&gt;</td>
<td>default</td>
</tr>
<tr>
<td>`logging enable</td>
<td>disable</td>
</tr>
</tbody>
</table>
Examples

Configure the Grid RRL settings on the Grid Master

Infoblox > set dns_rrl responses_per_second 100 log_only false window default slip 2 logging disable

Note: You can also execute the above command on a Grid member to change the RRL settings for that member.

Override the Grid RRL settings on a Grid member

Infoblox > set dns_rrl corp100.com override responses_per_second 300 log_only false window 200 slip 3

Inherit the Grid RRL settings on a Grid member

Infoblox > set dns_rrl corp100.com inherit

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log_only</td>
<td>Set this to true to test the RRL settings without dropping any requests. Set this to false to enable RRL. The default is false.</td>
</tr>
</tbody>
</table>
**set dscp**

Use the `set dscp` command to configure the DSCP value, which determines the PHBs (per-hop behaviors) on DiffServ compliant nodes and enables priorities of services to be assigned to network traffic. When you set the DSCP value, the appliance implements QoS (quality of service) rules based on your configuration so you can effectively classify and manage your critical network traffic. Note that on an appliance, all outgoing IP traffic on all interfaces uses the same DSCP value. You can configure this value for the Grid. You can also override the Grid setting for individual members.

DSCP is supported on both IPv4 and IPv6 transports. This feature is currently supported on the following Infoblox appliances: Trinzic 2210, Trinzic 2220, and Infoblox-4010. For information about these appliances, refer to the respective installation guides.

**Syntax**

```
set dscp grid [value]
set dscp member [value]
set dscp member inherit
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>The DSCP value. You can enter a value from 0 to 63. The default is 0 and it represents the lowest priority.</td>
</tr>
</tbody>
</table>

**Example**

**Set the Grid DSCP value**

```
Infoblox > set dscp grid 32
```

**Override the Grid DSCP value for a specific member**

```
Infoblox > set dscp member 20
```

**Inherit the Grid DSCP value**

```
Infoblox > set dscp member inherit
```
set enable_match_recursive_only

Use the set enable_match_recursive_only command to enable or disable the match-recursive-only option for a specific DNS view on a specific Grid member. You can also use the match-recursive-only option in combination with the Match Clients and Match Destinations settings to restrict and filter client access for specific DNS views on specific Grid members. For information about how to use these features, refer to the Infoblox NIOS Administrator Guide.

If you want to enable this setting for a DNS view, ensure that the Enable Recursion setting is enabled for the DNS view on the specified member.

To check the status of this setting for all DNS views on a Grid member, use the show enable-match-recursive-only CLI command. For information, see show enable_match_recursive_only on page 160.

Syntax

set enable_match_recursive_only <true|false|inherit> [dns_view]

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;true</td>
<td>false</td>
</tr>
<tr>
<td>dns_view</td>
<td>Optional parameter to specify the DNS view. If this parameter is omitted, the setting affects only the default DNS view. If the specific Grid member does not serve the default DNS view, you will receive an error message by omitting this parameter.</td>
</tr>
</tbody>
</table>

Example

Infoblox > set enable_match_recursive_only true (affects default DNS view only if default DNS view is served by member)
Infoblox > set enable_match_recursive_only true external
Infoblox > set enable_match_recursive_only false corp100sales
Infoblox > set enable_match_recursive_only inherit external
set forced_autosync

The `set forced_autosync` command forces a Grid member to automatically synchronize with the Grid Master when there is a join attempt to the Grid. This command can be used as an emergency workaround when a Grid is in a staged upgrade, and a Grid member that is waiting to be upgraded loses its database. In this situation, when the member attempts to rejoin the Grid, the rejoin will fail and you may use this command to synchronize the Grid member with the Grid Master.

Syntax

```
set forced_autosync
```

This command has no arguments.

Example

```
Infoblox > set forced_autosync
```
set grid_upgrade

The `set grid_upgrade` command enables you to set Grid upgrade properties. You can use this command to force a scheduled upgrade to end immediately, or to force Grid members that have not yet upgraded to upgrade immediately.

Syntax

```
set grid_upgrade [forced_end | forced_upgrade]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>forced_end</td>
<td>Ends a scheduled upgrade that is currently running.</td>
</tr>
<tr>
<td>forced_upgrade</td>
<td>Forces Grid members that have not yet upgraded to upgrade immediately.</td>
</tr>
</tbody>
</table>

Example

**When no scheduled upgrade is currently active**

Infoblox > `set grid_upgrade forced_complete`

No scheduled upgrade currently active.

**When a scheduled upgrade is active**

Infoblox > `set grid_upgrade forced_complete`

This will force all upgrade groups to trigger an immediate upgrade, this may effect grid services.

Do you want to proceed with an immediate upgrade of all groups (Y/N) ? y

Are you sure (Y/N) ? y

Upgrading all groups immediately.

**When a scheduled upgrade is currently paused**

Infoblox > `set grid_upgrade forced_complete`

Upgrade is currently paused, please un-pause the upgrade before triggering this operation.

**When no scheduled upgrade is active**

Infoblox > `set grid_upgrade forced_end`

No active scheduled upgrade.

**When a scheduled upgrade is active**

Infoblox > `set grid_upgrade forced_end`

This will force all upgrade groups to end upgrade immediately, all incomplete groups members will be logged-off the grid to perform an auto-sync of software with the grid this operation should only be used in an emergency situation to end a scheduled upgrade as it will result in member service outage until the operation is completed.

Do you want to proceed (Y/N) ? y

Are you sure (Y/N) ? y

Ending upgrade schedule and logging out incomplete group members for an auto-sync.
When a scheduled upgrade is currently paused
Infoblox > `set grid_upgrade forced_end`
Upgrade schedule is currently paused, please un-pause the upgrade schedule before triggering this operation.
set ibtrap

The `set ibtrap` command allows you to specify whether the appliance sends SNMP notifications (traps) and email notifications to the configured trap receivers and email recipients for the specified event category.

**Syntax**

```
set ibtrap [category] snmp [true|false] email [true|false]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>category</td>
<td>The event category that triggers the trap and/or email notification. Valid values are: Fan, Bloxtools, Disk, Memory, CPU, MGM, HSM, Login, PowerSupply, FTP, TFTP, HTTP, NTP, DNS, DHCP, RootFS, Database, RAID, HA, MSServer, Backup, Clear, SNMP, LCD, SSH, SerialConsole, ENAT, Network, Cluster, Controld, OSPF, OSPF6, IFMAP, BGP, CaptivePortal, DuplicateIP, License, System, Syslog, DiscoveryConflict, Reporting, FDUsage, OCSPResponders, DisconnectedGrid, LBDevice, LDAPServers, RIRSWIP</td>
</tr>
<tr>
<td>snmp</td>
<td>Specify true to send SNMP traps. Otherwise, specify false.</td>
</tr>
<tr>
<td>email</td>
<td>Specify true to send email notifications. Otherwise, specify false.</td>
</tr>
</tbody>
</table>

**Example**

```
Infoblox > set ibtrap FTP snmp true email true
```
set interface

The `set interface` command allows you to configure the speed and duplex settings of the network interfaces (MGMT, HA, LAN, and LAN2) on single independent appliances only. You cannot configure the network interface settings of appliances after they join a Grid or become HA pairs.

You can use `set interface mgmt` to enable the MGMT port and configure its IP address, netmask, and gateway address. You can configure either IPv4 address, IPv6 address or both for the MGMT interface of the appliance. Once the MGMT port is enabled, you can use the command to configure the speed and duplex settings of the MGMT port. You can also use `set interface mgmt off` to disable the MGMT port.

Use the `show interface` command to view the interface settings.

**Syntax**

```
set interface [lan|ha|lan2] speed [auto|10M|100M|1000M] duplex {auto|half|full}
set interface mgmt [speed [auto|10M|100M|1000M] duplex {auto|half|full}]
set interface mgmt off
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lan</td>
<td>Specifies the LAN interface.</td>
</tr>
<tr>
<td>ha</td>
<td>Specifies the HA interface.</td>
</tr>
<tr>
<td>speed</td>
<td>Specifies the speed of the incoming line rate in Mbps, or allows the appliance to automatically match the line speed.</td>
</tr>
<tr>
<td>auto</td>
<td>Specifies the duplex speed:</td>
</tr>
<tr>
<td>10M</td>
<td>100M</td>
</tr>
<tr>
<td>duplex</td>
<td>• Automatically adjusts the speed</td>
</tr>
<tr>
<td>half</td>
<td>• Sets it at half speed</td>
</tr>
<tr>
<td>full</td>
<td>• Set it at full speed</td>
</tr>
<tr>
<td>mgmt</td>
<td>Specifies the management interface.</td>
</tr>
<tr>
<td>mgmt off</td>
<td>Disables the management system interface.</td>
</tr>
</tbody>
</table>

**Note:** If this port is not being used, it should be set to off for security reasons.

**Examples**

**Enable and configure IPv4 address for the MGMT interface**

```
Infoblox > set interface mgmt
Enable Management port? (y or n): y
Enter Management IP address: 10.36.1.157
Enter Management netmask [Default: 255.255.255.0]: 255.255.0.0
Enter Management gateway address [Default: 10.36.0.1]:
Configure Management IPv6 network settings? (y or n): n
Restrict Support and remote console access to MGMT port? (y or n): n
Management Port Setting:
  Management Port Enabled: true
  Management IP address: 10.36.1.157
  Management netmask: 255.255.0.0
```
CLI Commands

Management Gateway address: 10.36.0.1
Restrict Support and remote console access to MGMT port:false
  Is this correct? [ y or n]: y
  Are you sure? (y or n): y
The management port settings have been updated.

Enable and configure IPv6 address for the MGMT interface

Infoblox > set interface mgmt
Enable Management port? (y or n): y
Enter Management IP address: 2620:010A:6000:2400::6508
Enter Management IPv6 Prefix Length [Default: none]: 64
Enter Management IPv6 gateway address [Default: none]: 2620:010A:6000:2400::0001
Configure Management IPv4 network settings? (y or n): n
Restrict Support and remote console access to MGMT port? (y or n): n
  Management IPv6 address: 2620:10a:6000:2400::6508/64
  Management IPv6 Gateway address: 2620:10a:6000:2400::1
  Restrict Support and remote console access to MGMT port: false
  Is this correct? (y or n): y
  Are you sure? (y or n): y
The management port settings have been updated.

Specify the MGMT interface speed after the port is enabled

Infoblox > set interface mgmt speed 10M duplex full
Setting Management interface speed to: 10M and duplex to: full
  Is this correct? [ y or n]: y
The network interface settings have been updated.

Specify the LAN interface speed

Infoblox > set interface lan speed 10M duplex full
Setting LAN interface speed to: 10M and duplex to: full
  Is this correct? [ y or n]: y
The network interface settings have been updated.

Specify the HA interface speed

Infoblox > set interface ha speed 100M duplex half
Setting HA interface speed to: 100M and duplex to: half
  Is this correct? [ y or n]: y
The network interface settings have been updated.

Note: This command is not supported on vNIOS appliances.
**set ip_rate_limit**

The `set ip_rate_limit` commands enable and disable rate limiting UDP traffic from source port 53, configure rate limiting rules that control the traffic, and remove rate limiting rules. Once you enable rate limiting, the current rate limiting rules take effect.

This command is useful when you want to mitigate cache poisoning on your DNS server by limiting the UDP traffic or blocking connections from source port 53.

**Syntax**

```
set ip_rate_limit {on | off}
set ip_rate_limit remove {source all | all | source ip-address[/mask]}
set ip_rate_limit add source {all | ip_address[/mask]} limit 0
set ip_rate_limit add source {all | ip_address[/mask]} limit packets/m [burst burst_packets]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Enables rate limiting from UDP port 53.</td>
</tr>
<tr>
<td>off</td>
<td>Disables rate limiting from UDP port 53.</td>
</tr>
<tr>
<td>add source</td>
<td>Configures the rate limiting rules.</td>
</tr>
<tr>
<td>all</td>
<td>Enter <strong>all</strong> or <strong>0.0.0.0</strong> if you want to limit all traffic from all sources.</td>
</tr>
<tr>
<td>ip_address/mask</td>
<td>Enter the IP address, and optionally the netmask, from which you want to limit the UDP traffic on port 53.</td>
</tr>
<tr>
<td>limit packets</td>
<td>Enter the number of packets per minute that you want to receive from the source.</td>
</tr>
<tr>
<td>burst burst_packets</td>
<td>Optionally, enter <strong>burst</strong> and the number of packets for burst traffic. Burst is the maximum number of packets accepted.</td>
</tr>
<tr>
<td>remove</td>
<td>Removes rate limiting rules from all sources or an existing host on UDP port 53.</td>
</tr>
<tr>
<td>source all</td>
<td>Removes the rate limiting rule that limits traffic from all sources on UDP port 53.</td>
</tr>
<tr>
<td>all</td>
<td>Removes all of the rate limiting rules from all sources on UDP port 53.</td>
</tr>
<tr>
<td>source ip-address/mask</td>
<td>Removes the existing rules for an existing host.</td>
</tr>
</tbody>
</table>
Examples

Turn on rate limiting

Infoblox > set ip_rate_limit on
Enabling rate limiting will discard packets and may degrade performance.
Are you sure? (y or n):

Turn off rate limiting

Infoblox > set ip_rate_limit off

Block all traffic from host 10.10.1.1

Infoblox > set ip_rate_limit add source 10.10.1.1 limit 0

Limit the traffic to five packets per minute from host 10.10.1.2/24, with an allowance for burst of 10 packets

Infoblox > set ip_rate_limit add source 10.10.1.2/24 limit 5/m burst 10

Remove the rate limiting rule from host 10.10.1.1/24

Infoblox > set ip_rate_limit remove source 10.10.1.1/24
**set ipam_web_ui**

The `set ipam_web_ui` command enables and disables Grid Manager on vNIOS appliances on Cisco. For information about Grid Manager, refer to the *Infoblox Administrator Guide*.

**Syntax**

```
set ipam_web_ui
```

This command has no arguments.

**Example**

```
Infoblox > set ipam_web_ui
```
set ipv6_disable_on_dad

The `set ipv6_disable_on_dad` command enables or disables IPv6 on an interface if a duplicate IPv6 address is detected.

**Syntax**

```
set ipv6_disable_on_dad {on | off}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Enables IPv6 on an interface.</td>
</tr>
<tr>
<td>off</td>
<td>Disables IPv6 on an interface.</td>
</tr>
</tbody>
</table>

**Examples**

**Turn on IPv6 on an interface**

```
Infoblox > set ipv6_disable_on_dad on
WARNING: This operation will reboot the system.
Do you want to proceed? (y or n): y
SYSTEM REBOOTING!
```

```
Infoblox > set ipv6_disable_on_dad on
Already on, nothing do be done
```

**Turn off IPv6 on an interface**

```
Infoblox > set ipv6_disable_on_dad off
WARNING: This operation will reboot the system.
Do you want to proceed? (y or n): y
SYSTEM REBOOTING!
```
**set ipv6_neighbor**

The `set ipv6_neighbor` command enables definition of an IPv6 neighbor for any of the following: LAN1, LAN2 or MGMT. `set ipv6_neighbor` also allows deletion of an existing IPv6 neighbor entry on the specified interface. For adding a new neighbor entry, the second required argument is for the link-local MAC address ID of the neighboring interface for the specified LAN/LAN2/MGMT port.

Another form of this command allows the flushing of specific or general IPv6 neighbor values from the specified interface. Prefixes and polled neighbor states can also be specified and combined in a statement.

**Syntax**

```
set ipv6_neighbor {add|clear} {LAN|LAN2|MGMT} [all] [prefix] ipv6-address ll_address [state]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6_address</td>
<td>The IPv6 address of the neighboring interface.</td>
</tr>
<tr>
<td>ll_address</td>
<td>The 48-bit link-local MAC ID of the neighboring interface. Argument is re-</td>
</tr>
<tr>
<td></td>
<td>quired for addition of a new IPv6 neighbor entry for the interface.</td>
</tr>
<tr>
<td>[all]</td>
<td>Optional argument to clear the entire list of IPv6 entries for the specified</td>
</tr>
<tr>
<td></td>
<td>interface.</td>
</tr>
<tr>
<td>[prefix]</td>
<td>Optional argument needed if all entries are to be flushed for an IPv6 pre-</td>
</tr>
<tr>
<td></td>
<td>fix. CIDR mask is required as part of the address specification.</td>
</tr>
<tr>
<td>[state]</td>
<td>Optional argument needed if entries of a specific type are to be flushed</td>
</tr>
<tr>
<td></td>
<td>or defined for an IPv6 prefix. Permitted values for the <code>state</code> argument in-</td>
</tr>
<tr>
<td></td>
<td>clude the following: <code>permanent</code>, <code>noarp</code>, <code>reachable</code>, and <code>stale</code>.</td>
</tr>
</tbody>
</table>

**Example**


Infoblox > `set ipv6_neighbor clear LAN prefix 2001:db8:12:256::/64 stale`

Infoblox > `set ipv6_neighbor clear LAN all`
**set ipv6_ospf**

The `set ipv6_ospf` command writes statistical information to syslog. This command provides informational data that can be helpful for diagnostic purposes. Setting the log level for OSPFv3 is the only configuration that can be done for the routing protocol in the NIOS CLI. The statistical information is written (dumped) to syslog. When viewing the syslog file, lines with names such as `ipv6_ospf statistics` are the OSPF statistical information. Use the `show ipv6_ospf` command to view the OSPF settings.

Syslog level describes the types of messages that are sent to syslog. You can identify the syslog information by using the `level` option.

**Note:** To use this command, the NSQ software package must be installed.

**Syntax**

```
set ipv6_ospf log {level}
```

**Argument | Description**

| level | Writes OSPF statistics to syslog with a specific associated level. The supported log levels are: debugging, informational, notifications, warnings, errors, critical, alerts, and emergencies. |

**Example**

```
Infoblox > set ipv6_ospf log alerts
```
**set ipv6_status**

The `set ipv6_status` command enables or disables IPv6 on all interfaces.

**Syntax**

```
set ipv6_status {enable | disable}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables IPv6 on all interfaces.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables IPv6 on all interfaces.</td>
</tr>
</tbody>
</table>

**Example**

Infoblox > `set ipv6_status enable`

WARNING: This operation will restart the product
Do you want to proceed? (y or n): y

Infoblox > `show interface`

MGMT:

IP Address: 10.36.111.3     MAC Address: 00:0C:29:70:D5:F5
Mask: 255.255.0.0          Broadcast: 10.36.255.255
MTU: 1500                   Metric: 1
IPv6 Link: fe80::20c:29ff:fe70:d5f5/64
IPv6 Status: Enabled
Negotiation: Disabled
Speed: 1000M                Duplex: Full
Status: UP BROADCAST RUNNING MULTICAST

Statistics Information
Received
packets: 25                 bytes: 1518 (1.4 KiB)
errors: 0                    dropped: 0
overruns: 0                  frame: 0

Transmitted
packets: 3                   bytes: 218 (218.0 b)
errors: 0                    dropped: 0
overruns: 0                  carrier: 0
Collisions: 0                Txqueuelen: 1000

Infoblox > `set ipv6_status disable`

WARNING: This operation will disable IPv6 communication
Do you want to proceed? (y or n): y
Infoblox > **show interface**

MGMT:

- **IP Address:** 10.36.111.3
- **MAC Address:** 00:0C:29:70:D5:F5
- **Mask:** 255.255.0.0
- **Broadcast:** 10.36.255.255
- **MTU:** 1500
- **Metric:** 1

IPv6 Link:
- **IPv6 Status:** Disabled
- **Negotiation:** Disabled
- **Speed:** 1000M
- **Duplex:** Full
- **Status:** UP BROADCAST RUNNING MULTICAST

Statistics Information

Received:
- **packets:** 606
- **bytes:** 66780 (65.2 KiB)
- **errors:** 0
- **dropped:** 0
- **overruns:** 0
- **frame:** 0

Transmitted:
- **packets:** 10
- **bytes:** 540 (540.0 b)
- **errors:** 0
- **dropped:** 0
- **overruns:** 0
- **carrier:** 0
- **Collisions:** 0
- **Txqueuelen:** 1000
set lcd keys or set lcd

The `set lcd keys` or `set lcd` command enables and disables the LCD input keys. Turning off the LCD input keys prevents anyone from manually changing the IP address on the NIOS appliance. Infoblox recommends this practice as a security measure for remote appliances.

Syntax

```
set lcd keys {off | on}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>off</td>
<td>Disables the LCD input keys on the appliance.</td>
</tr>
<tr>
<td>on</td>
<td>Re-enables the LCD input keys on the appliance.</td>
</tr>
</tbody>
</table>

Examples

**Disable the lcd keys**

```
Infoblox > set lcd keys
```

**Enable the lcd keys**

```
Infoblox > set lcd keys on
Turning ON the LCD display...
```

**Note:** You cannot enable or disable the LCD input keys on vNIOS appliances. You can configure the LCD input keys only on a Grid Master. On a vNIOS appliance, the `set lcd keys` or `set lcd` command generates an error.
set lcd_settings

The `set lcd_settings` command enables you to set the display settings of an LCD. You can specify the number of seconds after which the LCD screen must reduce the brightness if there is no keypad activity and specify the brightness level. You can also use this command to set the UID (unit identification) button on Trinzic appliances. For more information, see `set lcd_settings hwident`.

**Syntax**

```
set lcd_settings autodim <seconds>
set lcd_settings brightness <level>
set lcd_settings hwident [on | off]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;seconds&gt;</td>
<td>Sets the number of seconds after which the LCD screen should automatically dim. The auto-dim value should be in the range of 5 to 3600.</td>
</tr>
<tr>
<td>&lt;level&gt;</td>
<td>Sets the brightness of the LCD screen. Brightness levels are from 1 to 10.</td>
</tr>
</tbody>
</table>

**Example**

```
Infoblox > set lcd_settings autodim 8
Infoblox > set lcd_settings brightness 5
```
set lcd_settings hwident

The `set lcd_settings hwident` command enables and disables the UID (unit identification) button on Trinzic appliances. When you enable the UID button, the LCD panel on the front panel blinks and the UID LED on the rear panel glows blue. In a rack environment, the UID feature allows you to easily identify the appliance when moving between the front and rear of the rack.

Syntax

```
set lcd_settings hwident {off | on}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>off</td>
<td>Disables the UID feature on the Trinzic appliance.</td>
</tr>
<tr>
<td>on</td>
<td>Enables the UID feature on the Trinzic appliance.</td>
</tr>
</tbody>
</table>

Examples

Disable the UID feature

```
Infoblox > set lcd_settings hwident off
Turning ON the UID feature
```

Enable the UID feature

```
Infoblox > set lcd_settings hwident on
Turning ON the UID feature
```

Note: You cannot enable or disable the UID feature on vNIOS appliances. You can configure the UID feature only on Trinzic appliances. On a vNIOS appliance, the `set lcd_settings hwident` command generates an error.
set license

The `set license` command installs a license upon entering a valid license string. You must send an email request to Infoblox to receive a unique license string for your NIOS appliance. Copy the string directly from the email, and then use CTRL + V to insert it after the CLI command prompt. Use the `show license` command to view the license settings. This command is used to install both static (per member) and Grid-wide licenses.

**Note:** You can install a temporary 60-day license that allows your system to be fully functional while waiting to receive your permanent license. For more information, see `set temp_license` on page 117.

**Syntax**

```
set license
```

This command has no arguments.

**Example**

```
Infoblox > set license
Enter license string: EQAAAAKS4n90WFGNUSirwvyUT9/z
Install license? (y or n): y
Infoblox > set license
Enter license string: HQAAALsakOzDKirMdaUsG2Yfk/j0BkhoFjhVFETu36dJ
Install license? (y or n): y

License (grid-wide) is installed.
```

The UI needs to be restarted in order to reflect this license change.

```
Restart UI now, this will log out all UI users? (y or n): y
```
set lines

The **set lines** command specifies the number of lines that the appliance displays when you execute a **show** command during a session. The default is 20 lines. You can also configure permanent page settings or enter zero (0) to set paging off.

**Syntax**

```
set lines [num | permanent]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>num</td>
<td>The number of lines the appliance displays when you execute a <strong>show</strong> command.</td>
</tr>
<tr>
<td>permanent</td>
<td>Configures permanent page settings.</td>
</tr>
</tbody>
</table>

**Examples**

**Set the number of lines displayed on each page to 4:**

```
Infoblox > set lines 4
Number of scroll lines set to 4.
Infoblox > show log
May 31 13:30:05 (none) syslog-ng[892]: syslog-ng version 1.6.11 starting
May 31 13:30:05 (none) kernel: Linux version 2.6.17.4 (root@build-aslan) (gcc version 3.2.1) #1 SMP Fri May 18 19:44:21 EDT 2013
May 31 13:30:05 (none) kernel: BIOS-provided physical RAM map:
May 31 13:30:05 (none) kernel: BIOS-e820: 0000000000000000 - 000000000009f800 (usable)

Enter <return> for next page or q<return> to go back to command line.
```

**Turn paging off for this session:**

```
Infoblox > set lines 0
Number of scroll lines set to 0.
```

**Set a permanent line number:**

```
Infoblox > set lines permanent 24
Number of scroll lines set to 24.
```
**set log_txn_id**

The `set log_txn_id` command enables or disables the display of DHCP transaction IDs in syslog messages. By default, DHCP transaction ID logging is enabled. When you enable DHCP transaction ID logging, the appliance displays transaction IDs for the following packets:

- DHCPDISCOVER
- DHCPREQUEST
- DHCPRELEASE
- DHCPDECLINE
- DHCPINFORM

In Grid Manager, the transaction IDs are appended to the end of the corresponding syslog messages with a prefix of “TransID.” You can view this information in the **Administrator** tab -> **Logs** tab -> **Syslog** tab of Grid Manager.

When you enable this feature, you must restart DHCP service for the feature to take effect. When you disable this feature, you must perform a force restart services for the change to take effect. Use the `show log_txn_id` to display the current status of DHCP transaction ID logging.

**Syntax**

```
set log_txn_id (ON|OFF)
```

**Example**

**Enable DHCP transaction ID logging on an appliance**

```
Infoblox > set log_txn_id ON
DHCP Transaction id logging turned ON
DHCP force restart services is required in order for the changed value to take effect
```

**Disable DHCP transaction ID logging on an appliance**

```
Infoblox > set log_txn_id OFF
DHCP Transaction id logging turned OFF
DHCP force restart services is required in order for the changed value to take effect
```

**Sample syslog messages in the Syslog tab of Grid Manager:**

When DHCP transaction ID logging is on:

```
2013-03-25T09:39:41+00:00 daemon (none) dhcpd[14434]: info DHCPINFORM from 10.0.0.199
via 10.120.20.182 TransID 78563412: not authoritative for subnet 10.0.0.0
```

When DHCP transaction ID logging is off:

```
2013-03-25T09:39:39+00:00 daemon (none) dhcpd[14434]: info DHCPREQUEST for 10.0.0.199
from cc:bb:cc:dd:ee:ff (dhcp-10-0-0-199) via 10.120.20.182
```

---

**Argument** | **Description**
--- | ---
ON | Enables DHCP transaction ID logging on an appliance.
OFF | Disables DHCP transaction ID logging on an appliance.
The `set lom` command configures the LOM (Lights Out Management) settings for the IPMI interface. To view the current network settings for the IPMI interface, use the `show lom` command.

### Syntax

```
set lom
```

This command has no arguments.

### Example

```
Infoblox > set lom
Enter LOM IP address: 10.1.1.22
Enter LOM netmask: 255.255.255.0
Enter gateway address [Default: 10.34.10.1]:
LOM network settings:
  IP address: 10.34.10.42
  Netmask:255.255.255.0
  Gateway address: 10.34.10.1
Is this correct? (y or n): y
Are you sure? (y or n): y
```
**`set lower_case_ptr_dname`**

The `set lower_case_ptr_dname` command converts all the domain names in uppercase characters to lowercase for PTR records. You can execute this command at the Grid level, member level, or the DNS view level.

**Syntax**

```
set lower_case_ptr_dname grid (on|off)
set lower_case_ptr_dname view <view-name> (on|off) [override_grid (on|off)]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On</td>
<td>Enables the appliance to convert all the domain names in uppercase to lowercase for PTR records.</td>
</tr>
<tr>
<td>off</td>
<td>Disables the conversion option. The domain names in PTR records will remain intact.</td>
</tr>
<tr>
<td>&lt;view-name&gt;</td>
<td>Specify the DNS view name.</td>
</tr>
<tr>
<td>&lt;view-name&gt; on</td>
<td>Enables the conversion option at the DNS view level. If you enable the conversion option at both the Grid and DNS view level, the conversion option is enabled.</td>
</tr>
<tr>
<td>&lt;view-name&gt; off</td>
<td>Disables the conversion option at the DNS view level.</td>
</tr>
<tr>
<td>override_grid on</td>
<td>Overrides the conversion option set at the Grid level. If you enable the conversion option at the DNS view level and disable at the Grid level, the conversion option is enabled.</td>
</tr>
<tr>
<td>override_grid off</td>
<td>Inherits the conversion option set at the Grid level. If you enable the conversion option at the DNS view level and disable at the Grid level, the conversion option is enabled.</td>
</tr>
</tbody>
</table>

**Example**

```
Infoblox > set lower_case_ptr_dname grid on
Infoblox > set lower_case_ptr_dname grid on
Restart the DNS service in order for changes to take effect

Infoblox > set lower_case_ptr_dname view default off override_grid on
Restart the DNS service in order for changes to take effect
```
set membership

The set membership command specifies a Grid for the NIOS appliance. Use this command when the network address has been set (see set network on page 86) and you want to put the appliance in a Grid. You can join an IPv4 appliance to an IPv4-only or a dual mode Grid and an IPv6 appliance to an IPv6-only or a dual mode Grid. If the IP address is acceptable to the Grid Master, use this command to join the Grid. You can specify either an IPv4 or an IPv6 address of the Grid Master. If you need to re-address the appliance, use the set network command.

Note: When you join a dual mode Grid member to a dual mode Grid, you can enter IPv4 address of the Grid Master if the Grid communication protocol for the Grid member is set as IPv4 and you can enter IPv6 address of the Grid Master if the Grid communication protocol for the Grid member is set as IPv6. For information about setting the communication protocol for a dual mode appliance, refer to the Infoblox Administrator Guide.

Syntax

set membership

This command has no arguments.

Example

Infoblox > set membership
Join status: No previous attempt to join a Grid.
Enter new Grid Master VIP: 10.1.1.22
Enter Grid Name [Default Infoblox]: DaveyJones
Enter Grid Shared Secret: L0ck37
Join Grid as member with attributes:
Join Grid Master VIP: 10.1.1.22
Grid Name: DaveyJones
Grid Shared Secret: L0ck37
WARNING: Joining a Grid will replace all the data on this node!
Is this correct? (y or n): y
Are you sure? (y or n): y
set mgm attached

The set mgm attached command forces a Grid to attach to a Master Grid. Use this command only if a Grid is in the Attached state on the Multi-Grid Manager and Detached on the Grid Manager. This command recovers the Grid status when it is out of sync with the Grid status on the Multi-Grid Manager.

**Syntax**

```
set mgm attached [MGM IP Address] [Port Number]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGM IP Address</td>
<td>IP address of the Master Grid</td>
</tr>
<tr>
<td>Port Number</td>
<td>Port number of the Master Grid</td>
</tr>
</tbody>
</table>

**Example**

The following example uses the `set mgm attached` command.

```
Console connect [@ Grid IP address]
Infoblox > set maintenancemode
Maintenance Mode > set mgm attached [MGM IP address] [Port Number]
This command will force the Grid to get attached.
Are you sure you want to continue? (y or n): y
```
**set mld_version_1**

The `set mld_version_1` command sets the IPv6 MLD (Multicast Listener Discovery) protocol to version 1, as described in RFC 2710, *Multicast Listener Discovery for IPv6*. MLD enables the appliance to detect multicast listeners on its directly attached links and discover which multicast addresses are of interest.

The appliance runs MLD version 2, as described in RFC 3810, *Multicast Listener Discovery Version 2 for IPv6*, by default. MLD version 2 is interoperable with version 1.

**Syntax**

```
set mld_version_1
```

This command has no arguments.

**Example**

```
Infoblox > set mld_version_1
Current MLD version: 2
Set Multicast Listener Discovery Version 1? (y or n): y
New MLD Settings:
  Use MLD version 1: Yes
  Is this correct? (y or n): y
MLD version: 1 is saved to database.
MLD version is set for IPv6.
```
**set monitor dns**

The `set monitor dns` command enables network monitoring for DNS. Once enabled, you can do the following:

- View the average latency of authoritative and non-authoritative replies to DNS queries in 1, 5, 15, and 60 minute time intervals. Use the `show monitor` command to view the DNS network data.
- Monitor invalid DNS responses from UDP port 53. Use the `show monitor dns alert status` command to view the DNS alert status.

This command is useful when troubleshooting DNS and network issues.

**Note:** This command is not supported for IPv6 in NIOS 7.0 and later releases. When you enable DNS network monitoring, there is a significant impact on DNS query performance.

**Syntax**

```
set monitor dns {on | off}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Enables network monitoring for DNS.</td>
</tr>
<tr>
<td>off</td>
<td>Disables network monitoring for DNS.</td>
</tr>
</tbody>
</table>

**Examples**

**Turn on DNS network monitoring**

```
Infoblox > set monitor dns on
Turning On DNS Network Monitoring...
```

**Turn off DNS network monitoring**

```
Infoblox > set monitor dns off
Turning Off DNS Network Monitoring...
```
set monitor dns alert

The `set monitor dns alert` commands enable DNS alert monitoring and set the thresholds for invalid DNS responses. After you enable DNS alert monitoring, the appliance monitors the UDP traffic on port 53 for recursive DNS queries, and then reports invalid DNS responses on UDP ports that are not open and with mismatched TXIDs. You must enable DNS network monitoring when you enable DNS alert monitoring. For information, see the `set monitor dns` command.

You can also configure the thresholds for invalid DNS responses. When the number of invalid responses exceeds the thresholds, the appliance logs the event and sends SNMP traps and notifications, if previously enabled. The default thresholds for both invalid ports and invalid TXIDs are 50%. You can configure the thresholds either as absolute packet counts or as percentages of the total traffic during a one minute time interval.

This command is useful for monitoring possible cache poisoning. Use the `show monitor dns alert status` command to view invalid port and invalid TXID data.

**Note:** This command is not supported for IPv6 in NIOS 7.0 and later releases.

**Syntax**

```
set monitor dns alert {on | off}
set monitor dns alert modify {port | txid} over threshold_value {packets | percent}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Enables DNS alert monitoring.</td>
</tr>
<tr>
<td>off</td>
<td>Disables DNS alert monitoring.</td>
</tr>
<tr>
<td>modify</td>
<td>Sets the thresholds for invalid DNS responses.</td>
</tr>
<tr>
<td>port</td>
<td>Enter <code>port</code> to set the threshold for invalid ports.</td>
</tr>
<tr>
<td>txid</td>
<td>Enter <code>txid</code> to set the threshold for invalid TXIDs.</td>
</tr>
<tr>
<td>threshold_value</td>
<td>Enter the number of packets or percentage for the threshold.</td>
</tr>
<tr>
<td>packets</td>
<td>Enter <code>packets</code> if you want to set the threshold as a total packet count.</td>
</tr>
</tbody>
</table>
| percent          | Enter `percentage` if you want to set the threshold as a percentage of the total traffic. For a percentage-based threshold, the appliance does not generate a threshold crossing event if the traffic level is less than 100 packets per minute.

**Examples**

**Turning on and off DNS alert monitoring**

```
Infoblox > set monitor dns alert on
Infoblox > set monitor dns alert off
```

**Triggering a DNS alert when the percentage of invalid DNS responses on UDP ports exceeds 70% per minute**

```
Infoblox > set monitor dns alert modify port over 70 percent
```

**Triggering a DNS alert when the total packet count of invalid DNS responses with mismatched TXIDs is over 100 packets per minute**

```
Infoblox > set monitor dns alert modify txid over 100 packets
```
set ms_dns_reports_sync_interval

You can use the `set ms_dns_reports_sync_interval` command to specify the time interval at which the DNS reporting data from the Microsoft server is synchronized with the NIOS appliance.

Syntax

```
set ms_dns_reports_sync_interval <MS Server IP address> <seconds>
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MS Server IP address&gt;</td>
<td>Specify the IP address of the Microsoft server.</td>
</tr>
<tr>
<td>&lt;seconds&gt;</td>
<td>Specify the time interval in seconds at which the DNS reporting data from</td>
</tr>
<tr>
<td></td>
<td>the Microsoft server is synchronized with the NIOS appliance. The default</td>
</tr>
<tr>
<td></td>
<td>synchronization interval is 15 seconds.</td>
</tr>
</tbody>
</table>

Example

```
Infoblox > set ms_dns_reports_sync_interval 10.102.30.2 14
Current DNS reports sync interval is 15 second(s).
The DNS reports sync interval will be changed to 14 second(s).
Is this correct? (y or n): y
The DNS reports sync interval has been changed to 14 second(s).
```
set named_recv_sock_buf_size

You can use the `set named_recv_sock_buf_size` command to tune the BIND receive socket buffer memory to a maximum of 8 MB. The DNS receive socket buffer holds BIND packets that are queued on the UDP (User Datagram Protocol) port from the NIC (Network Interface Controller). This command is useful when you want to increase the BIND receive buffer size to accommodate occasional burst traffic and high volume DNS recursive queries. Note that the same buffer is also used for updates and non-recursive queries. Use the `show named_recv_sock_buf_size` to view the current buffer size.

**Note:** Ensure that you use this command only when you are dealing with burst traffic situations in high volume deployments.

**Syntax**

```
set named_recv_sock_buf_size [N]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>The number of kilobytes to which you want to set the BIND receive socket buffer size. The minimum is 120 kilobytes and the maximum is 8192. The default is 1536.</td>
</tr>
</tbody>
</table>

**Example**

**Set the BIND receive socket buffer size to 5000 KB**

```
Infoblox > set named_recv_sock_buf_size 5000
Infoblox >
```
**set network**

The `set network` command specifies an address for a NIOS appliance so that it can join a network, with the option of joining a Grid. You can configure either IPv4 address, IPv6 address, or both for a NIOS appliance. If the appliance is configured with an IPv6 address, it can join a Grid using the IPv6 address of the Grid Master. Use the `show network` command to view the network settings.

`set network` supports configuration of both IPv4 and IPv6 interface addresses.

**Syntax**

```bash
set network
```

This command has no arguments.

**Example**

**Specifying an IPv4 address**

```bash
Infoblox > set network
NOTICE: All HA configuration is performed from the GUI. This interface is used only to configure a standalone node or to join a grid.
Enter IP address:10.35.1.104
Enter netmask [Default: 255.255.255.0]:
Enter gateway address [Default: 10.35.0.1]:
Enter VLAN tag [Default: Untagged]:
Enter DSCP value [Default: Inherited from Grid: 0]:
NOTICE: Additional IPv6 interface can be configured only via GUI.
Configure IPv6 network settings? (y or n):n
Become grid member? (y or n): n

New Network Settings:
   IPv4 address: 10.35.1.104
   IPv4 Netmask: 255.255.255.0
   IPv4 Gateway address: 10.35.0.1
   IPv4 VLAN tag: Untagged
   IPv4 DSCP Value: Inherited from Grid: 0

Old IPv4 Network Settings:
   IPv4 address: 192.168.1.2
   IPv4 Netmask: 255.255.255.0
   IPv4 Gateway address: 192.168.1.1
   IPv4 VLAN tag: Untagged
   IPv4 DSCP Value: Inherited from Grid: 0
```

**Specifying an IPv6 address**

```bash
Infoblox > set network
NOTICE: All HA configuration is performed from the GUI. This interface is used only to configure a standalone node or to join a grid.
Enter IP address : 2620:10a:6000:2400::168
Enter IPv6 Prefix Length [Default: none]: 64
Enter IPv6 gateway [Default: none]: 2620:10a:6000:2400::1
```
set network

Enter VLAN tag [Default: Untagged]:
Enter DSCP value [Default: Inherited from Grid: 0]
Configure IPv4 network settings? (y or n): n
Become grid member? (y or n): n

New Network Settings:
IPv6 address: 2620:10a:6000:2400::168/64
IPv6 Gateway address: 2620:10a:6000:2400::1
IPv6 VLAN tag: Untagged
IPv6 DSCP Value: Inherited from Grid: 0

Specifying both IPv4 and IPv6 address

Infoblox > set network
NOTICE: All HA configuration is performed from the GUI. This interface is used only to configure a standalone node or to join a grid.
Enter IP address : 10.35.1.104
Enter netmask [Default: 255.255.255.0]: 255.255.0.0
Enter gateway address [Default: 10.35.0.1]:
Enter VLAN tag [Default: Untagged]:
Enter DSCP value [Default: Inherited from Grid: 0]
Configure IPv6 network settings? (y or n): y
Enter IPv6 address [Default: none]: 2620:10A:6000:2400::168
Enter IPv6 Prefix Length [Default: none]: 64
Enter IPv6 gateway [Default: none]: 2620:10A:6000:2400::1
Enter VLAN tag [Default: Untagged]:
Enter DSCP value [Default: 30]:
Become grid member? (y or n): n

New Network Settings:
IPv4 address: 10.35.1.104
IPv4 Netmask: 255.255.0.0
IPv4 Gateway address: 10.35.0.1
IPv4 VLAN tag: Untagged
IPv4 DSCP Value: Inherited from Grid: 0
IPv6 address: 2620:10a:6000:2400::168/64
IPv6 Gateway address: 2620:10a:6000:2400::1
IPv6 VLAN tag: Untagged
DSCP value: 30

Old IPv4 Network Settings:
IPv4 address: 192.168.1.2
IPv4 Netmask: 255.255.255.0
IPv4 Gateway address: 192.168.1.1
IPv4 VLAN tag: Untagged
IPv4 DSCP Value: Inherited from Grid: 0
Note: After you confirm your network settings, the Infoblox application automatically restarts.

After configuring the network settings, you cannot change the type of network connectivity of the appliance through CLI. For example, if the appliance is configured in IPv4-only mode, then you can change only the IPv4 interface settings through CLI. But the type of network connectivity for the appliance can be changed through GUI.
**set nogrid**

The `set nogrid` command removes the specified member from the current Grid. Execute this command from the Grid member. This command is valid only on a member.

**Note:** Infoblox recommends that you use this command only in an emergency, such as when the network is down between the master and the member. Otherwise, you should configure the member to leave the Grid using the GUI on the Grid Master.

**Syntax**

```
set nogrid
```

This command has no arguments.

**Example**

```
Infoblox > set nogrid
```

The normal method to configure a node to leave a Grid is to use the GUI on the Grid Master. This method is only used for emergencies (e.g., network is down from the master to this node).

Is this such an emergency? **y**

The current node will become a standalone machine, with default values for Grid settings.

Are you sure? (y or n) **y**

The network settings have been updated.
set nomastergrid

In a Multi-Grid environment, the `set nomastergrid` command enables a Grid to leave the current Master Grid. This command is valid only on the Multi-Grid Master.

Syntax

```plaintext
set nomastergrid
```

This command has no arguments.

Example

```plaintext
Infoblox > set nomastergrid
This grid is going to leave master grid
        Are you sure? (y or n): y
Grid is not joined to a master grid. Exiting without making any change
```
set nosafemode

The `set nosafemode` command disables safe mode on the NIOS appliance by re-enabling DNS and DHCP services. For more information, see `set safemode` on page 103.

Syntax

```
set nosafemode
```

This command has no arguments.

Example

```
Infoblox > set nosafemode
```
set ospf

The **set ospf** command writes statistical information to syslog. This command provides informational data that can be helpful for diagnostic purposes. The statistical information is written (dumped) to syslog. When viewing the syslog file, lines with names such as `ospf statistics` are the OSPF statistical information. Use the `show ospf` command to view the OSPF settings.

Syslog level describes the types of messages that are sent to syslog. You can identify the syslog information by using the **level** option.

**Note:** To use this command, the NSQ software package must be installed.

**Syntax**

```
set ospf log {level}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level</td>
<td>Writes OSPF statistics to syslog with a specific associated level. The supported log levels are: debugging, informational, notifications, warnings, errors, critical, alerts, and emergencies.</td>
</tr>
</tbody>
</table>

**Example**

```
Infoblox > set ospf log alerts
```
The `set phonehome` command enables a Grid Master or an independent appliance to email reports monthly and after each upgrade to Infoblox Technical Support and other specified recipients. The reports provide status and event information about the Grid or independent appliance and its services. The report is an XML document that includes the following information:

- The phone home feature version.
- The report type, such as periodic and test.
- The time of the report.
- The Infoblox Support ID that was assigned to the account.
- Information about the Grid, such as its NIOS version, name, VIP, Grid Master hostname, LAN IP, and the number of Grid members and appliances in the Grid.
- The upgrade history of the Grid.
- Information about each Grid member, such as the hostname, IP address, status, role (such as standalone, master), and if the member is an HA pair. If the member is a peer in a DHCP failover association, the report also includes the DHCP failover status.
- Hardware information, such as the hardware type, serial number, HA status, and uptime.
- Information about the interfaces, such as the interface name and IP addresses.
- Resource usage information, such as CPU and system temperature, and CPU, database, disk, and memory usage.

**Syntax**

```
set phonehome {on | off}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Enables the appliance to send status and event reports to specified recipients.</td>
</tr>
<tr>
<td>off</td>
<td>Disables the function to send reports.</td>
</tr>
</tbody>
</table>

**Examples**

**Turning on the phone home feature**

```
Infoblox > set phonehome on
```

**Turning off the phone home feature**

```
Infoblox > set phonehome off
```
**set port_mac_addr**

The `set port_mac_addr` command enables or disables MAC address spoofing on a LAN1 or LAN2 interface. Note that you cannot execute the command `set port_mac_addr` on a virtual appliance that is running Software ADP. To execute the command, change `set port_mac_addr` through the Hypervisor when the virtual appliance is powered off.

**Syntax**

```
set port_mac_addr on [LAN1|LAN2] <IP> <MAC>
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Enables the MAC address spoofing on an interface.</td>
</tr>
<tr>
<td>off</td>
<td>Disables the MAC address spoofing on an interface.</td>
</tr>
<tr>
<td>LAN1</td>
<td>LAN2</td>
</tr>
<tr>
<td>&lt;IP&gt;</td>
<td>IP address of the LAN1 or LAN2 interface.</td>
</tr>
<tr>
<td>&lt;MAC&gt;</td>
<td>Specifies the MAC address.</td>
</tr>
</tbody>
</table>

**Examples**

**Turning on the port_mac_addr**

```
Infoblox > set port_mac_addr on LAN1 2.2.2.2
```

**Turning off the port_mac_addr**

```
Infoblox > set port_mac_addr off LAN1
```
**set promote_master**

The `set promote_master` command specifies a NIOS appliance as the new Grid Master in the case of a Grid Master failure. The new Grid Master then alerts all the Grid members to redirect their traffic to it. If you have configured multi-site reporting cluster, you can modify the primary reporting site. For information about reporting clusters, refer to the *Infoblox NIOS Administrator Guide*.

You can do one of the following to promote a master candidate to a Grid Master:

- Immediately notify all Grid members about the promotion.
- Set a sequential notification to provide wait time for Grid members to join the new Grid Master. Staggering the restarts of Grid members can minimize DNS outages. The sequential order for Grid members to join the new Grid Master begins with the old Grid Master and then the Grid members in FQDN order. The default delay time is 120 seconds. You can configure the delay time from a minimum of 30 seconds up to 600 seconds.

For this command to be effective, you must have previously specified an appliance as the Grid Master candidate. Then when you lose the Grid Master, you can remotely (SSH) log in to the Grid Master candidate and execute this command.

*Note:* When the previous Grid Master comes back on line, it automatically joins the Grid as a master candidate.

**Syntax**

```
set promote_master
```

This command has no arguments.

**Examples**

```
Infoblox > set promote_master
Do you want a delay between notification to Grid members? (y or n): n

Enter `n` to promote the master candidate and send notifications to all Grid members immediately. The appliance displays the following:

This action will immediately promote master candidate to become the Grid Master. This feature is designed to be used primarily for disaster recovery.
Are you sure you want to do this? (y or n): y
The current member will become the Grid Master.
Are you really sure you want to do this? (y or n): y
Member promotion beginning on this member.

Enter `y` to promote the master candidate to the Grid Master immediately and specify the delay time for the Grid members to join the new Grid Master. The appliance displays the following:

```
Set delay time for notification to Grid members? [Default: 120s]: 200
```

This action will immediately promote master candidate to become the Grid Master. This feature is designed to be used primarily for disaster recovery.
Are you sure you want to do this? (y or n): y
The current member will become the Grid Master. The Grid members will be notified sequentially with a delay of 200 seconds.
Are you really sure you want to do this? (y or n): y

If you have configured multi-site reporting cluster, the appliance displays all the reporting sites in the order of priority you have configured. For example if you have configured the following reporting sites: site 4(priority 1), site 2 (priority 2), site 1(priority 3), and site 3 (priority 4)
Infoblox > `set promote_master`
Do you want a delay between notification to Grid members? (y or n): n
Primary reporting site candidates (in order of priority):
   1. site4 (Existing primary reporting site)
   2. site2
   3. site1
   4. site3
Please enter new primary reporting site (1-2) or 'c' to continue without changing primary reporting site: 5

The appliance displays the following error when you enter value incorrectly:

`ERROR`: Please enter a valid choice or 'c' to continue without changing the primary reporting site.

Please enter new primary reporting site (1-2) or 'c' to continue without changing primary reporting site: c

This action will immediately promote this member to become the grid master. This feature is designed to be used primarily for disaster recovery.

Are you sure you want to do this? (y or n): y
The current member will become the grid master.
Are you really sure you want to do this? (y or n): y
Master promotion beginning on this member
Good Bye

To change the primary reporting site:

Infoblox > `set promote_master`
Do you want a delay between notification to Grid members? (y or n): n
Primary reporting site candidates (in order of priority):
   1. site4 (Existing primary reporting site)
   2. site2
   3. site1
   4. site3
Please enter new primary reporting site (1-4) or 'c' to continue without changing primary reporting site: 2
Are you sure you want to do this? (y or n): y
The current member will become the grid master.
Are you really sure you want to do this? (y or n): y
Master promotion beginning on this member
Good Bye

The new priority order of reporting sites will be:
site2 (Existing primary reporting site)
site4
site1
site3
**set prompt**

Use the `set prompt` command to change the prompt to the host name, user@host name, host IP address, or user@host IP address. Note that the prompt displayed in the command line interface (CLI) can be set only on the active Grid Master node. Once you execute the `set prompt` command, the prompt displayed for all Grid members is set accordingly and you can see the prompt when you log in to the CLI for each Grid member.

**Syntax**

```
set prompt {hostname | user@hostname | ip | user@ip | default}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>Sets the prompt to the host name of the computer from which you access the appliance.</td>
</tr>
<tr>
<td>user@hostname</td>
<td>Sets the prompt to the user name@ the host name of the computer from which you access the appliance.</td>
</tr>
<tr>
<td>ip</td>
<td>Sets the prompt to the IP address of the host.</td>
</tr>
<tr>
<td>user@ip</td>
<td>Sets the prompt to the user name@ the IP address of the host.</td>
</tr>
<tr>
<td>default</td>
<td>Sets the prompt to “Infoblox &gt;”.</td>
</tr>
</tbody>
</table>

**Example**

```
Infoblox > set prompt user@hostname
admin@infoblox >
admin@infoblox > set prompt user@ip
admin@172.31.1.254 >
```
**set recursion_query_timeout**

Use the `set recursion_query_timeout` command to configure the maximum time allowed for a recursive query to wait for a response before timing out. Setting the timeout value to 0 returns to the default timeout behavior, which is to wait at least 30 seconds and up to 40 seconds before timing out.

**Note:** When you enable this on an HA pair, ensure that you run the command and set the same values on both nodes of the HA pair. No service restart is required when you use this command.

This command is designed to mitigate phantom domain attacks. For more information about this, refer to the *Infoblox NIOS Administrator Guide*.

**Syntax**

```
set recursion_query_timeout <timeout>
set recursion_query_timeout 0
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeout</td>
<td>The maximum time allowed for a recursive query to wait for a response before timing out. Valid values are 10 to 30, inclusive.</td>
</tr>
<tr>
<td>0</td>
<td>Returns to default timeout behavior, which is to wait at least 30 seconds and up to 40 seconds under certain circumstances.</td>
</tr>
</tbody>
</table>

**Example**

```
Infoblox > set recursion_query_timeout 30
```
The `set remote_console` command enables and disables access to the NIOS appliance using a remote console. Use the `show remote_console` command to view the remote console settings.

**Note:** Infoblox recommends that you close any port that is not being used, for security reasons. An open, unused port offers the potential for unwanted access to your network.

**Syntax**

```
set remote_console
```

This command has no arguments.

**Example**

```
Infoblox > set remote_console
Enable remote console access (Grid level)? (y or n): y
New remote console access settings:
Remote console access enabled: Yes
Is this correct? (y or n): y
```
set reporting_cert

In a Grid with a reporting server, you can use the set reporting_cert command to generate a new set of SSL certificates on all forwarders and the indexer. You can use this command only on the Grid Master.

Syntax

    set reporting_cert

This command has no arguments.

Example

    Infoblox > set reporting_cert
    Generate new reporting certificate? (y or n): y
    Reporting certificates generated.
**set reporting_cluster_maintenance_mode**

Use the `set reporting_cluster_maintenance_mode` command to enable the Grid Master to prevent from rolling the reporting data from the buckets stored on a peer node. This helps you avoid data loss due to network issues or any problem with the connection between the peer nodes. Note that you can run this command only on the Grid Master.

**Syntax**

```
set reporting_cluster_maintenance_mode [on|off]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Enables the cluster maintenance mode. When you enable this feature, the Grid Master stops the rolling of reporting data from peer nodes.</td>
</tr>
<tr>
<td>off</td>
<td>Disables the cluster maintenance mode.</td>
</tr>
</tbody>
</table>

**Example**

```
Maintenance Mode > set reporting_cluster_maintenance_mode on
Reporting cluster maintenance mode is enabled
Can be run only on the grid master.
When reporting cluster maintenance mode is enabled replication factor or search factor policies will not be enforced.
```
**set revert_grid**

Use the `set revert_grid` command to revert to a version of software that was running previously on a Grid or on an independent appliance or HA pair. Be aware that when you revert to this software, any configurations made to the currently running software are lost. You can back up the current data before you revert so that you can later determine what configuration changes are missing.

**Syntax**

```
set revert_grid
```

This command has no arguments.

**Example**

```
Infoblox > set revert_grid
```
set safemode

The `set safemode` command disables DNS and DHCP services. Use this command to troubleshoot a NIOS appliance with unreliable services.

This command restarts all the services, including DNS and DHCP. DNS and DHCP remain active only long enough to write `named.conf` and `dhcp.conf` files. These services then shut down. All other services remain functional. This allows you to review the `named.conf` and `dhcp.conf` files to determine and alleviate the cause of the appliance distress.

Once you have determined the problem, you can reinstate DNS and DHCP services using the `set nosafemode` command.

**Syntax**

```
set safemode
```

This command has no arguments.

**Example**

```
Infoblox > set safemode
```
**set scheduled**

Use the `set scheduled` command to specify the number of times per hour the appliance checks if the services need a restart when the task scheduling feature is enabled. You must manually restart services or schedule a restart of services for the scheduled change to take effect.

You can set the value from 0 to 60, and the default value is 60. When you set the value to 0, the appliance turns off the restart feature.

Use the `show scheduled` to view the number of times per hour the appliance checks whether a restart of services is required.

**Syntax**

```
set scheduled task restarts [0-60]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-60</td>
<td>The number of times per hour the appliance checks if the services need a restart when the task scheduling feature is enabled. You can enter any number from 0 to 60. The default is 60. A value of 0 turns off the restart feature.</td>
</tr>
</tbody>
</table>

**Example**

Enter the following command to enable the appliance to check 10 times per hour whether the services need a restart:

```
Infoblox > set scheduled task restarts 10
```

The appliance checks 10 times per hour if the services must be restarted, which is every six minutes of the hour. For example, if you enter the command at 3:15 p.m., the appliance checks if the services must be restarted every six minutes starting at the hour (3:00 p.m.). Therefore, the next checks are at 3:18, 3:24, 3:30, 3:36, 3:42, 3:48, 3:54, and 4:00 p.m.
**set security**

The *set security* command allows you to specify IP or network addresses that can access the appliance through the GUI. The appliance denies access to addresses that are not specified. Use the *show security* command to view the security settings.

**Syntax**

```
set security
```

This command has no arguments.

**Example**

In the following example, security is enabled to restrict access to the NIOS appliance (through the GUI) to the IP address range 10.1.1.1:

```
Infoblox > set security
Enable security? (y or n): y
Enter access IP range: 10.1.1.1
Enter access netmask (Default: 255.255.255.0): 255.255.255.0
New security settings:
  Security enabled: Yes
  IP range: 10.1.1.1
Is this correct? (y or n): y
Do you wish to enter additional access range? (y or n): n
```
set session_timeout

Use the `set session_timeout` command to specify how long a session remains open when there is no user activity. Use the `show session_timeout` command to view the session_timeout setting.

**Syntax**

```
set session_timeout
```

This command has no arguments.

**Example**

```
Infoblox > set session_timeout
Current GUI/CLI timeout is 60000 seconds (16:40:00)

WARNING: Changing the session timeout will cause GUI users to be logged out.
New GUI/CLI session timeout (in seconds, 0 to abort)? 90000
```
**set smartnic monitor-mode**

The `set smartnic monitor-mode` command enables and disables monitor mode for the Threat Protection service. This is disabled by default. When monitor mode is enabled, the appliance logs DNS packets (instead of dropping them) that would have been blocked by threat protection rules. This information is recorded in the audit log. Note that you can enable or disable monitor mode only for individual members. You cannot set this configuration at the Grid level.

To view whether monitor mode is enabled or disabled for the Threat Protection service, see `show smartnic` on page 212.

**Syntax**

```
set smartnic monitor-mode {on|off}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Enables monitor mode for the Threat Protection service.</td>
</tr>
<tr>
<td>off</td>
<td>Disables monitor mode for the Threat Protection service.</td>
</tr>
</tbody>
</table>

**Examples**

**Enable debugging**

```
Infoblox > set smartnic monitor-mode on
```

**Disable debugging**

```
Infoblox > set smartnic monitor-mode off
```
set snmptrap

The `set snmptrap` command sends SNMP traps to the trap receiver you specify. You can use the optional `v3` command to generate SNMPv3 traps. For information about SNMP, see Chapter 6, Monitoring with SNMP in the Infoblox NIOS Administrator Guide.

Use the `show snmp` command to get information about SNMP objects.

**Syntax**

```
set snmptrap variable {name of an SNMP variable, in dotted or symbolic format} address {the address of the trap receiver} [v3] [snmpuser]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name of an SNMP variable</td>
<td>The name or OID (object ID) of the SNMP object. For example, you can enter <code>sysName.0</code> or <code>.1.3.6.1.4.1.2021.11.53.0</code>.</td>
</tr>
<tr>
<td>address of the trap receiver</td>
<td>The IPv4 or IPv6 address of the management system that receives SNMP traps.</td>
</tr>
<tr>
<td>snmpuser</td>
<td>The user name of the SNMPv3 user account. This is optional. If you do not provide a user name, the appliance uses the first SNMPv3 user on the list.</td>
</tr>
</tbody>
</table>

**Examples**

**Sending SNMP traps to a specific trap receiver**

Enter the following on the appliance:

```
Infoblox > set snmptrap variable sysName.0 address 10.0.0.11
```

The appliance sends the following acknowledgement to the trap receiver:

```
2011-02-23 23:02:51 10.0.0.11 [UDP: [10.0.0.11]:35597->[10.0.0.11]]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (42) 0:00:00.42
SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-MIB::sysName.0
2011-02-23 23:02:53 10.0.0.11 [UDP: [10.0.0.11]:52367->[10.0.0.11]]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (42) 0:00:00.42
SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-MIB::sysName.0
```

**Sending SNMP traps using SNMPv3**

Enter the following on the appliance:

```
Infoblox > set snmptrap variable sysName.0 localhost v3 SNMPv3User1
```

The appliance sends the following acknowledgement to the trap receiver:

```
2011-02-07 01:08:19 localhost [UDP: [127.0.0.1]:41884->[127.0.0.1]]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (42) 0:00:00.42
SNMPv2-MIB::snmpTrapOID.0 = OID: DISMAN-EVENT-MIB::sysName.0
```

Enter the following on the appliance:

```
Infoblox > set snmptrap variable sysName.0 localhost v3 SNMPv3User1
```

The appliance sends the following to the trap receiver in the event of a process failure:

```
SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.7779.3.1.11.12.1.0
SNMPv2-SMI::enterprises.7779.3.1.11.12.1.0 = STRING: "192.168.1.2"
SNMPv2-SMI::enterprises.7779.3.1.11.12.2.2.0 = INTEGER: 5
SNMPv2-SMI::enterprises.7779.3.1.11.12.5.0 = STRING: "named"
SNMPv2-SMI::enterprises.7779.3.1.11.12.4.0 = INTEGER: 20
SNMPv2-SMI::enterprises.7779.3.1.11.12.11.0 = STRING: "A named daemon monitoring failure has occurred."
```
The `set ssl_tls_ciphers` command allows you to enable or disable the SSL/TLS cipher suites. You can enable any specific cipher suite or all the cipher suites. The default cipher suites are enabled in a specific order. However, you can change this default order. Note that you cannot disable all the cipher suites. At least one cipher suite must be enabled.

The default cipher suites are enabled in the following order:

1. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
2. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
3. TLS_DHE_RSA_WITH_AES_128_CBC_SHA
4. TLS_DHE_RSA_WITH_AES_256_CBC_SHA
5. TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
6. TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
7. TLS_RSA_WITH_AES_128_GCM_SHA256
8. TLS_RSA_WITH_AES_128_CBC_SHA
9. TLS_RSA_WITH_AES_128_CBC_SHA256
10. TLS_RSA_WITH_3DES_EDE_CBC_SHA
11. TLS_RSA_WITH_AES_256_GCM_SHA384
12. TLS_RSA_WITH_AES_256_CBC_SHA256
13. TLS_RSA_WITH_AES_256_CBC_SHA256

You can also enable the following cipher suites that are disabled by default:

- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256

You can use the `show ssl_tls_ciphers` command to view the enabled SSL/TLS cipher suites. For information, see `show ssl_tls_ciphers` on page 214.

**Syntax**

```
set ssl_tls_ciphers enable suite_name [ position ]
set ssl_tls_ciphers disable position
set ssl_tls_ciphers enable_all
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the cipher suites.</td>
</tr>
<tr>
<td>suite_name</td>
<td>Specifies the name of a particular cipher suite.</td>
</tr>
<tr>
<td>all</td>
<td>Enables all cipher suites.</td>
</tr>
<tr>
<td>position</td>
<td>Specifies the position of a cipher suite.</td>
</tr>
</tbody>
</table>
CLI Commands

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disables the cipher suites.</td>
</tr>
</tbody>
</table>

Examples

Enable all cipher suites

```
Infoblox > set ssl_tls_ciphers enable_all
All cipher suites were enabled
The following services need to be restarted manually: GUI
```

Enable a specific cipher suite

```
Infoblox > set ssl_tls_ciphers enable TLS_RSA_WITH_RC4_128_SHA 8
TLS_RSA_WITH_RC4_128_SHA was enabled
The following services need to be restarted manually: GUI
```

Disable a specific cipher suite

```
Infoblox > set ssl_tls_ciphers disable 8
TLS_RSA_WITH_RC4_128_SHA was disabled
The following services need to be restarted manually: GUI
```
set ssl_tls_protocols

The `set ssl_tls_protocols` command allows you to enable or disable the SSL/TLS protocols. You can enable any one or all of the following protocols: TLSv1.0, TLSv1.1, or TLSv1.2. By default, TLSv1.0 is enabled. Note that you cannot change the SSL/TLS protocol when the SSL/TLS setting is set to default mode. You must set the SSL/TLS setting to the override mode in order to change the SSL/TLS protocol. For information about SSL/TLS settings, see `set ssl_tls_settings` on page 112.

You can use the `show ssl_tls_protocols` command to view the enabled SSL/TLS protocols. For information, see `show ssl_tls_protocols` on page 215.

Syntax

```
set ssl_tls_protocols [ enable | disable ] [ TLSv1.0 | TLSv1.1 | TLSv1.2 ]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the SSL/TLS protocols.</td>
</tr>
<tr>
<td>TLSv1.0</td>
<td>Enables the TLSv1.0 protocol.</td>
</tr>
<tr>
<td>TLSv1.1</td>
<td>Enables the TLSv1.1 protocol.</td>
</tr>
<tr>
<td>TLSv1.2</td>
<td>Enables the TLSv1.2 protocol.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the SSL/TLS protocols. Note that you cannot disable all the SSL/TLS protocols. At least one protocol must be enabled.</td>
</tr>
</tbody>
</table>

Examples

**Enable TLSv1.2 protocol**

```
Infoblox > set ssl_tls_protocols enable TLSv1.2
TLSv1.2 was enabled. Current configurations is: TLSv1.0 TLSv1.1 TLSv1.2
The following services need to be restarted manually: GUI
```

**Disable TLSv1.0 protocol**

```
Infoblox > set ssl_tls_protocols disable TLSv1.0
TLSv1.0 was disabled. Current configuration: TLSv1.1 TLSv1.2
The following services need to be restarted manually: GUI
```


set ssl_tls_settings

You can use the `set ssl_tls_settings` command to override or restore the default SSL/TLS settings. When the SSL/TLS settings are set to the override mode, you can modify the default SSL/TLS protocols and ciphers. When the SSL/TLS settings are set to the default mode, you cannot override the default SSL/TLS protocols and ciphers. The appliance uses the default SSL/TLS protocols and ciphers. Use the `show ssl_tls_settings` on page 216 to see whether SSL/TLS settings are set to the default or override mode.

**Syntax**

```
set ssl_tls_settings [default | override]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default</code></td>
<td>Sets the default mode for SSL/TLS settings. When the SSL/TLS settings is set to the default mode, the appliance uses the default SSL/TLS protocols and ciphers.</td>
</tr>
<tr>
<td><code>override</code></td>
<td>Sets the override mode for SSL/TLS settings. When the SSL/TLS settings is set to the override mode, the appliance overrides the default SSL/TLS protocols and ciphers.</td>
</tr>
</tbody>
</table>

**Example**

```
Infoblox > set ssl_tls_settings override
```

The following services need to be restarted manually: GUI
**set static_route**

Use the *set static_route* command to configure static routes on your appliance. You can create new IPv4 and IPv6 static routes, move static route to a desired position in the list of static routes, move static routes up and down in the list, or move static route at a specific position up or down in the list of static routes. You can also delete an existing static route, delete static routes at a specific position, or delete all existing static routes for IPv4, IPv6 or both protocols. Use the *show static_routes* command to view the current configuration of static routes on your appliance.

**Syntax**

```
set static_route add network/cidr gateway [position]
set static_route move network/cidr gateway new-position
set static_route move network/cidr gateway (up|down)
set static_route move (v4|v6) old-position new-position
set static_route move (v4|v6) old-position (up|down)
set static_route delete network/cidr gateway
set static_route delete (v4|v6) position
set static_route delete (all|v4|v6)
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add network/cidr gateway [position]</td>
<td>Creates a new static route and optionally specifies its position in the list of static routes.</td>
</tr>
<tr>
<td>move network/cidr gateway new-position</td>
<td>Moves a static route to a new position in the list of static routes.</td>
</tr>
<tr>
<td>move network/cidr gateway [up</td>
<td>down]</td>
</tr>
<tr>
<td>move (v4</td>
<td>v6) [old-position] [new-position]</td>
</tr>
<tr>
<td>move (v4</td>
<td>v6) [old-position] (up</td>
</tr>
<tr>
<td>delete network/cidr gateway</td>
<td>Deletes an existing static route.</td>
</tr>
<tr>
<td>delete (v4</td>
<td>v6) [position]</td>
</tr>
<tr>
<td>delete (all</td>
<td>v4</td>
</tr>
</tbody>
</table>

**Examples**

**Adding a new static route**
```
Infoblox > set static_route add 10.6.112.0/24 10.6.42.1
Infoblox > set static_route add 2001:1234:5678::/112 2001:1234::42
```

**Moving a static route to a new position in the list of static routes**
```
Infoblox > set static_route move 10.6.112.0/24 10.6.42.1 5
Infoblox > set static_route move 2001:1234:5678::/112 2001:1234::42 6
```
CLI Commands

Moving a static route up or down in the list of static routes

```
Infoblox > set static_route move 10.6.112.0/24 10.6.42.1 up
Infoblox > set static_route move 10.6.112.0/24 10.6.42.1 down
Infoblox > set static_route move 2001:1234:5678::/112 2001:1234::42 up
Infoblox > set static_route move 2001:1234:5678::/112 2001:1234::42 down
```

Moving an IPv4 or IPv6 static route from its current position to a new position in the list of static routes

```
Infoblox > set static_route move v4 1 12
Infoblox > set static_route move v6 1 12
```

Moving an IPv4 or IPv6 static route up or down from its current position in the list of static routes

```
Infoblox > set static_route move v4 12 up
Infoblox > set static_route move v6 12 up
Infoblox > set static_route move v4 1 down
Infoblox > set static_route move v6 1 down
```

Deleting an existing static route

```
Infoblox > set static_route delete 10.6.112.0/24 10.6.42.1
Infoblox > set static_route delete 2001:1234:5678::/112 2001:1234::42
```

Deleting an IPv4 or IPv6 static route at a specific position in the list of static routes

```
Infoblox > set static_route delete v4 1
Infoblox > set static_route delete v6 2
```

Deleting all IPv4 static routes

```
Infoblox > set static_route delete v4
```

Deleting all IPv6 static routes

```
Infoblox > set static_route delete v6
```

Deleting all IPv4 and IPv6 static routes

```
Infoblox > set static_route delete all
```
set support_access

The `set support_access` command enables and disables support access. This feature is disabled (off) by default. Enabling this feature allows Infoblox Support (Tier 3 access) to perform root level diagnostics on an appliance that is in severe distress. A special key is required to access the appliance at root level, and only Infoblox Support (Tier 3) can generate this key.

**Note:** Once the problem has been resolved, Infoblox recommends that you turn off this port. Any open port that is not in use can become a security risk.

**Syntax**

```
set support_access
```

This command has no arguments.

**Example**

```
Infoblox > set support_access
Enable support access (Grid level)? (y or n): y
   New support access settings:
   Support access enabled: Yes
   Is this correct? (y or n): y
```
**set sysName**

You can use the `set sysName` command to set the FQDN (fully qualified domain name) of the appliance to allow configured SNMP management system to query the sysName value. If the appliance is an HA pair, you can use the `name2` command to set the FQDN of node 2 of the HA pair.

**Syntax**

```
set sysName name1 [name2]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name1</td>
<td>The FQDN of the appliance.</td>
</tr>
<tr>
<td>name2</td>
<td>The FQDN of node 2 of an HA pair.</td>
</tr>
</tbody>
</table>

**Examples**

**Setting the FQDN of the appliance**

Enter the following on the appliance:

```
Infoblox > set sysName eng.corp100.com
```

**Setting the FQDNs of an HA Pair**

Enter the following on the appliance:

```
Infoblox > set sysName active.corp100.com passive.corp100.com
```
The `set temp_license` command generates and installs a temporary 60-day license for a fully functional NIOS appliance and IBOS (Infoblox Orchestration Server), or a temporary 90-day license for an IF-MAP Starter Kit on a VMware virtual appliance. Depending on the appliance model, the list of temporary licenses varies. Use the `show license` command to view the license settings.

Infoblox supports cloud API calls to set temporary licenses for **Threat Protection (Software add-on)** and **Threat Protection Update** licenses.

<table>
<thead>
<tr>
<th>To install temporary license(s) for...</th>
<th>Select...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS and DHCP services</td>
<td><strong>DNSone (DNS, DHCP)</strong></td>
<td>Installs DNS and DHCP licenses</td>
</tr>
<tr>
<td>DNS and DHCP services with Grid</td>
<td><strong>DNSone with Grid (DNS, DHCP, Grid)</strong></td>
<td>Installs DNS, DHCP, and Grid licenses</td>
</tr>
<tr>
<td>DHCP services with Grid</td>
<td><strong>Network Services for Voice (DHCP, Grid)</strong></td>
<td>Installs DHCP and Grid licenses</td>
</tr>
<tr>
<td>NIOS services</td>
<td><strong>Add NIOS License</strong></td>
<td>Installs a NIOS license for SoT (Son of Trinzic) 2016 hardware appliances.</td>
</tr>
<tr>
<td>DNS services</td>
<td><strong>Add DNS Server license</strong></td>
<td>Installs a DNS license</td>
</tr>
<tr>
<td>DHCP services</td>
<td><strong>Add DHCP Server license</strong></td>
<td>Installs a DHCP license</td>
</tr>
<tr>
<td>Grid</td>
<td><strong>Add Grid license</strong></td>
<td>Installs a Grid license</td>
</tr>
<tr>
<td>IF-MAP service on an IBOS</td>
<td><strong>Add IF-MAP Service license</strong></td>
<td>You cannot install other services, such as DNS and DHCP, on an IBOS.</td>
</tr>
<tr>
<td>Microsoft server management</td>
<td><strong>Add Microsoft management license</strong></td>
<td>You can install other licenses with the Microsoft management license.</td>
</tr>
<tr>
<td>VMware virtual appliance</td>
<td><strong>Add vNIOS license</strong></td>
<td>For VMware virtual appliances only. You can install other licenses with the vNIOS license.</td>
</tr>
<tr>
<td>Load balancer services</td>
<td><strong>Add Load Balancer license</strong></td>
<td>Installs a load balancer license</td>
</tr>
<tr>
<td>IF-MAP federation</td>
<td><strong>Add IF-MAP Federation license</strong></td>
<td>Installs a 90-day temporary IF-MAP federation license.</td>
</tr>
<tr>
<td>Multi-Grid management</td>
<td><strong>Add Multi-Grid Management license</strong></td>
<td>Installs a Multi-Grid license for Multi-Grid management</td>
</tr>
<tr>
<td>DNS Traffic Control</td>
<td><strong>Add DNS Traffic Control license</strong></td>
<td>Installs a DNS Traffic Control license</td>
</tr>
<tr>
<td>Query Redirection</td>
<td><strong>Add Query Redirection license</strong></td>
<td>Installs a query redirection license</td>
</tr>
<tr>
<td>Security Ecosystem</td>
<td><strong>Add Security Ecosystem license</strong></td>
<td>Installs a Security Ecosystem license on any Grid member</td>
</tr>
<tr>
<td>Threat Analytics</td>
<td><strong>Add Threat Analytics license</strong></td>
<td>Installs a Threat Analytics license</td>
</tr>
<tr>
<td>Reporting service</td>
<td><strong>Add Reporting license</strong></td>
<td>Installs a license on the reporting server</td>
</tr>
</tbody>
</table>
CLI Commands

**Syntax**

```
set temp_license
```

This command has no arguments.

**Example**

Installing a temporary license on the NIOS appliance:

```
Infoblox > set temp_license
1. DNSone (DNS, DHCP)
2. DNSone with Grid (DNS, DHCP, Grid)
3. Network Services for Voice (DHCP, Grid)
4. Add NIOS license
5. Add DNS Server license
6. Add DHCP Server license
7. Add Grid license
8. Add Microsoft management license
9. Add IF-MAP Federation license
10. Add Multi-Grid Management license
11. Add Load Balancer license
12. Query Redirection license
13. Add Reporting license
14. Add DNS Traffic Control license
15. Add Security Ecosystem license
16. Add Response Policy Zones license
17. Add FireEye license
18. Add Cloud Network Automation license
19. Add Threat Analytics license
Select license (1-19) or q to quit:
1. IB-V805
2. IB-V815
3. IB-V825
4. IB-V1405
5. IB-V1415
6. IB-V1425
7. IB-V2205
```
8. IB-V2215
9. IB-V2225
10. IB-V4005
11. IB-V4015
12. IB-V4025

Installing a temporary license on the Trinzic Reporting VM-800 Appliance:

```
Infoblox > set temp_license
1. Add Grid license
2. Add vNIOS license
3. Add Reporting license
Select license (1-3) or q to quit:
```

Installing a temporary Flex Grid Activation license on the NIOS appliance:

```
Infoblox > set temp_license
1. DNSone (DNS, DHCP)
2. DNSone with Grid (DNS, DHCP, Grid)
3. Network Services for Voice (DHCP, Grid)
4. Add NIOS License
5. Add DNS Server license
6. Add DHCP Server license
7. Add Grid license
8. Add Microsoft management license
9. Add Multi-Grid Management license
10. Add Query Redirection license
11. Add Response Policy Zones license
12. Add FireEye license
13. Add DNS Traffic Control license
14. Add Cloud Network Automation license
15. Add Security Ecosystem license
16. Add Flex Grid Activation license
Select license (1-16) or q to quit:
```

Installing a temporary Software ADP license on the NIOS appliance:

```
Infoblox > set temp_license
1. DNSone (DNS, DHCP)
2. DNSone with Grid (DNS, DHCP, Grid)
3. Network Services for Voice (DHCP, Grid)
4. Add DNS Server license
5. Add DHCP Server license
6. Add Grid license
7. Add vNIOS license
8. Add Query Redirection license
9. Add Threat Protection (Software add-on) license
10. Add Threat Protection Update license
11. Add Response Policy Zones license
12. Add FireEye license
13. Add DNS Traffic Control license
14. Add Cloud Network Automation license
15. Add Security Ecosystem license
16. Add Threat Analytics license
17. Add Flex Grid Activation license
Select license (1-17) or q to quit:
**set term**

Use the `set term` command to set the correct terminal type for future commands in the current session.

**Syntax**

```
set term
```

This command has no arguments.

**Example**

```
Infoblox > set term vt100
```
**set thresholdtrap**

Use the `set thresholdtrap` command to enable the SNMP trap for CPU usage and to configure the trigger and reset values of the trap. The CPU usage trap is disabled by default. When you use this command to change the trigger and reset values, you enable the trap and the appliance sends and resets traps based on the configured values. When CPU usage of an appliance exceeds the trigger threshold for 15 seconds, the appliance sends a “CPU usage above threshold value” trap. After the appliance sends the “CPU usage above threshold value” trap, it sends a “CPU usage OK” trap when the CPU usage dips below the reset threshold.

Use the `show thresholdtrap` command to view the current settings of the CPU usage trap. Note that the CPU usage trap is disabled by default, and the trigger value is set at 100 and reset value at 0. For information about Infoblox SNMP traps, refer to the *Infoblox NIOS Administrator Guide*.

**Syntax**

```
set thresholdtrap {type} trigger {value} reset {value}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>type</code></td>
<td>The type of threshold trap. Enter <code>CpuUsage</code> to enable the CPU usage trap and set the trigger and reset values. Valid values are: <code>NetworkCapacity</code>, <code>DBObjects</code>, <code>Disk</code>, <code>Memory</code>, <code>Rootfs</code>, <code>CpuUsage</code>, <code>Reporting</code>, <code>ReportingVolume</code>, <code>FDUsage</code></td>
</tr>
<tr>
<td><code>value (for trigger)</code></td>
<td>The trigger value of the SNMP trap. When CPU usage exceeds this value, the appliance sends a “CPU usage above threshold value” trap.</td>
</tr>
<tr>
<td><code>value (for reset)</code></td>
<td>The reset value of the SNMP trap. When CPU usage dips below this value, the appliance sends a “CPU usage OK” trap. Ensure that the reset value is smaller than the trigger value.</td>
</tr>
</tbody>
</table>

**Example**

**Enabling the CPU usage trap and set the trigger and reset values**

```plaintext
Infoblox > set thresholdtrap CpuUsage trigger 80 reset 71
Infoblox >
```

When CPU usage exceeds 80% of capacity for 15 seconds, the appliance sends the “CPU usage above threshold value” trap. The appliance sends the “CPU usage OK” trap when CPU usage dips below the reset value of 71. Following is a sample SNMP output of this example:

```
SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.7779.3.1.1.1.1.1.3.0
SNMPv2-SMI::enterprises.7779.3.1.1.1.2.1.0 = STRING: "10.35.107.9"
SNMPv2-SMI::enterprises.7779.3.1.1.1.2.3.0 = STRING: "cpu_usage"
SNMPv2-SMI::enterprises.7779.3.1.1.1.2.6.0 = INTEGER: 100
SNMPv2-SMI::enterprises.7779.3.1.1.1.2.7.0 = INTEGER: 80
SNMPv2-SMI::enterprises.7779.3.1.1.1.2.8.0 = INTEGER: 71
SNMPv2-SMI::enterprises.7779.3.1.1.1.2.11.0 = STRING: "CPU usage above threshold value."
SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.7779.3.1.1.1.1.3.0
SNMPv2-SMI::enterprises.7779.3.1.1.1.2.1.0 = STRING: "10.35.107.9"
SNMPv2-SMI::enterprises.7779.3.1.1.1.2.3.0 = STRING: "cpu_usage"
SNMPv2-SMI::enterprises.7779.3.1.1.1.2.6.0 = INTEGER: 5
```
SNMPv2-SMI::enterprises.7779.3.1.1.1.2.7.0 = INTEGER: 80
SNMPv2-SMI::enterprises.7779.3.1.1.1.2.8.0 = INTEGER: 71
SNMPv2-SMI::enterprises.7779.3.1.1.1.2.11.0 = STRING: "CPU usage OK."
set traffic_capture

The set traffic_capture command allows you to capture the traffic for one or all of the ports on a NIOS appliance and save the traffic capture in a file. To capture traffic, the NIOS appliance must have a minimum of 500 MB of free disk space; otherwise, the traffic capture might fail.

The NIOS appliance saves all traffic it captures in a .cap file and compresses it into a .tar.gz file. The size of the .cap file is limited to 4 GB for Infoblox-4010, Infoblox-4030, Infoblox-4030-10GE, and PT-4000, and the size is limited to 1 GB for all other NIOS appliances. In Grid Manager, you can download the traffic capture file after the traffic capture stops by navigating to the Grid tab -> Grid Manager tab -> Members tab -> and click Traffic Capture from the Toolbar. To view information about the traffic capture running on the member, see show traffic_capture_status on page 222.

You can also transfer the traffic capture file to remote hosts either using FTP or SCP. You cannot transfer the traffic capture files when the traffic capture is in progress. Note that this operation may take a long time to complete.

Syntax

```
set traffic_capture on [port <all|lan1|lan2|mgmt|ha>] [vlan <id>] [duration <seconds>] [filter 'valid-tcpdump-filter-expression'] [with-rolling]
set traffic_capture off
set traffic_capture transfer [ftp|scp] <server-ip> <user-name> <user-password> [dest <file_name>]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Starts the traffic capture.</td>
</tr>
<tr>
<td>off</td>
<td>Stops the traffic capture after you have started it.</td>
</tr>
<tr>
<td>port</td>
<td>Specifies the port for which you want to capture the traffic:</td>
</tr>
<tr>
<td>all</td>
<td>• Captures traffic on all ports.</td>
</tr>
<tr>
<td>lan1</td>
<td>• Captures traffic on the LAN1 port.</td>
</tr>
<tr>
<td>lan2</td>
<td>• Captures traffic on the LAN2 port.</td>
</tr>
<tr>
<td>mgmt</td>
<td>• Captures traffic on the MGMT port.</td>
</tr>
<tr>
<td>ha</td>
<td>• Captures traffic on the HA port.</td>
</tr>
</tbody>
</table>

The default is LAN1. Note that if you have enabled the LAN2 failover feature, the LAN1 and LAN2 ports generate the same output. (For information about the LAN2 failover feature, see the About Port Redundancy section in the Infoblox NIOS Administrator Guide.)

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan &lt;id&gt;</td>
<td>Captures traffic for the vLAN interface on LAN1 or LAN2.</td>
</tr>
<tr>
<td>duration &lt;seconds&gt;</td>
<td>Specifies the duration in seconds for which you want the traffic capture to run. The default is 1800 seconds.</td>
</tr>
<tr>
<td>filter</td>
<td>Allows you to set the “tcpdump&quot; filter for traffic capture.</td>
</tr>
<tr>
<td>'valid-tcpdump-filter-expression'</td>
<td></td>
</tr>
<tr>
<td>with-rolling</td>
<td>Enables rolling of traffic capture file. When the traffic capture file reaches the maximum size limit, the appliance automatically saves the file into a new file and continues capturing the traffic. The appliance can save up to 4 traffic capture files.</td>
</tr>
<tr>
<td>transfer</td>
<td>Allows you to transfer the traffic capture file to an FTP server or a SCP server.</td>
</tr>
<tr>
<td>ftp</td>
<td>Transfers the traffic capture file to an FTP server.</td>
</tr>
</tbody>
</table>
CLI Commands

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scp</td>
<td>Transfers the traffic capture file to an SCP server.</td>
</tr>
</tbody>
</table>

**Example**

**Start the traffic capture**

```
Infoblox > set traffic_capture on
Traffic capture started successfully.
```

**Stop the traffic capture**

```
Infoblox > set traffic_capture off
Traffic capture stopped successfully.
```

**Start the traffic capture on a specific port**

```
Infoblox > set traffic_capture on port lan1
Traffic capture started successfully.
```

**Specify the traffic capture filter**

```
Infoblox > set traffic_capture on port lan1 filter 'host 10.32.2.34'
Traffic capture started successfully.
```

```
Infoblox > set traffic_capture on port lan1 filter 'net 192.168.0.0/24'
Traffic capture started successfully.
```

For information about valid tcpdump filter expressions, refer to [https://wiki.wireshark.org/CaptureFilters](https://wiki.wireshark.org/CaptureFilters).

**Transfer traffic capture file to an FTP server**

```
Infoblox > set traffic_capture transfer ftp 10.120.20.239 frtest Infoblox123 dest /home/rpadasalagi/ftp_back.tar.gz
```

WARNING: This operation may take a long time to complete
Do you want to proceed? (y or n): y

**Transfer traffic capture file to an SCP server**

```
set traffic_capture transfer scp 10.120.20.239 frtest - dest /home/test/scp_back.tar.gz
```

Enter password:
WARNING: This operation may take a long time to complete
Do you want to proceed? (y or n): y

**WARNING:** When you use the `set traffic_capture transfer` command, the user password is logged in the history. In order to avoid exposure of the user password, you can enter dash (-) instead of the actual password in the `<user-password>` field. You can enter the password when the appliance prompts for the password.
**set txn_trace**

The `set txn_trace` command enables and disables database transaction logging for the NIOS appliance. Enabling database transaction logging allows you to identify the processes that causes database utilization. To view the status of database transaction logging for the NIOS appliance, see `show txn_trace` on page 223.

**Syntax**

```
set txn_trace {on|off}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Enables database transaction logging for the NIOS appliance.</td>
</tr>
<tr>
<td>off</td>
<td>Disables database transaction logging for the NIOS appliance.</td>
</tr>
</tbody>
</table>

**Examples**

Enable DB transaction log for an appliance

```
Infoblox > set txn_trace on
```

Disable DB transaction log for an appliance

```
Infoblox > set txn_trace off
```

Backup the current `ib_db_txn_trace_log` file.
**set wins_forwarding**

Use the `set wins_forwarding` command to configure the appliance to forward WINS packets to Microsoft DNS and DHCP servers. You can enable or disable this feature for the entire Grid or override Grid-level settings for specific Grid members. To configure Grid level setting, you must execute this command on the Grid Master.

To view information about the current packet forwarding configuration, see `show wins_forwarding` on page 229.

**Syntax**

```
set wins_forwarding grid|member
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>grid</td>
<td>Configures all members in the Grid to enable or disable the forwarding of WINS packets to Microsoft DNS and DHCP servers. Grid-level setting can be set only on the Grid Master.</td>
</tr>
<tr>
<td>member</td>
<td>Overrides the Grid settings to enable or disable packet forwarding for a specific Grid member.</td>
</tr>
</tbody>
</table>

**Examples**

**Enable packet forwarding for the Grid**

Infoblox > `set wins_forwarding grid`

This command will change default settings for WINS packets forwarding (will affect members inheriting grid settings). Continue? (y or n): y

Enable WINS packets forwarding? (y or n): y

Enter default WINS server IP: 1.0.0.123

Select output interface from the list:
1. MGMT
2. LAN
3. LAN2
4. VIP

WINS packets forwarding is enabled. WINS packets will be forwarded to "1.0.0.123".

**Override Grid-level packet forwarding configuration for a specific Grid member**

Infoblox > `set wins_forwarding member`

WINS forwarding on grid level is enabled. WINS server IP is 1.0.0.123.

Override grid level settings? (y or n): y

Enable WINS packets forwarding on this member? (y or n): y

Enter WINS server IP: 1.0.0.321

Select output interface from the list:
1. MGMT
2. LAN
3. LAN2
4. VIP

WINS packets forwarding is enabled. WINS packets will be forwarded to "1.0.0.321".
Disable packet forwarding for the Grid

Infoblox > set wins_forwarding grid
This command will change default settings for WINS packets forwarding (will affect members inheriting grid settings). Continue? (y or n): y
   Enable WINS packets forwarding? (y or n): n

   WINS packets forwarding was disabled on grid level.

Overriding Grid-level configuration and disable packet forwarding for a specific Grid member

Infoblox > set wins_forwarding member
WINS forwarding on grid level is enabled. WINS server IP is 1.0.0.123.

   Override grid level settings? (y or n): y
   Enable WINS packets forwarding on this member? (y or n): n
   WINS packets forwarding is disabled for this member.
**show admin_group_acl**

The `show admin_group_acl` command displays admin groups that have ACL settings.

**Syntax**

```
show admin_group_acl
```

This command has no arguments.

**Example**

The following example shows the response when none of the admin groups have enabled ACL settings.

```
Infoblox > show admin_group_acl
None of Admin Groups have enabled ACL settings.
```
show adp

The `show adp` command displays ADP (Advanced Threat Protection) details on the supported platform. You can use this command only if **Threat Protection** (hardware based) or **Threat Protection (Software add-on)** licenses are installed on the platform.

**Syntax**

```
show adp
```

This command has no arguments.

**Example**

```
Infoblox > show adp
Threat Protection:    Enabled
Threat Protection monitor mode: Disabled
Threat Protection event stats: CRITICAL=0 MAJOR=0 WARNING=0 INFORMATIONAL=2
Log level:            6(Info)
```
show arp

The `show arp` command displays ARP (Address Resolution Protocol) data to view mappings. This allows you to see if the current state matches the mappings. If the mappings are out of date, use the `reset arp` command. This command is also useful for troubleshooting network connectivity issues.

**Syntax**

```
show arp
```

This command has no arguments.

**Example**

The following example shows the IP address (10.1.1.1), MAC address (00:04:96:1D:19:80), and type of connection (ethernet).

```
Infoblox > show arp
? (10.1.1.1) at 00:04:96:1D:19:80 [ether] or LAN
```
**show auto_provision**

The `show auto_provision` command shows the state of auto-provisioning for an appliance. It displays whether auto-provisioning is enabled or disabled for an appliance.

**Syntax**

```
show auto_provision
```

This command has no arguments.

**Example**

```
Infoblox > show auto_provision
Auto Provision is enabled

Infoblox > show auto_provision
Auto Provision is disabled
```
show bfd details

The `show bfd details` command displays the detailed BFD session details. For information about how to set the logging level, see `set bfd` on page 39.

**Syntax**

```
show bfd details
```

This command has no arguments.

**Example**

```
Infoblox > show bfd details
OutAddr NeighAddr LD/RD Holdown(mult) State Int
10.34.54.68 10.34.54.16 2/4 300(3) Up bond0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 100000, MinRxInt: 100000, Multiplier: 3
Received MinRxInt: 100000, Received Multiplier: 3
Holdown (hits): 300(0), Hello (hits): 100(1638)
Authentication: None
    Last Sequence Number: Rx: 0, Tx: 1566182577
Rx Count: 1638
Tx Count: 1686
Last packet: Version: 1  - Diagnostic: 0
    State bit: Up  - Demand bit: 0
    Poll bit: 0  - Final bit: 0
    Multiplier: 3  - Length: 24
    My Discr: 2  - Your Discr: 4
    Min tx interval: 100000  - Min rx interval: 100000
Min Echo interval: 100000
```
The `show bgp` command displays information about the BGP configuration on the appliance, reachability information about neighbors, and BGP routes to destinations. You can specify the command with or without an argument. A command without an argument defaults to `show bgp route`.
For information about how to write statistical information to syslog, see `set bgp log` on page 40.

**Syntax**

```
show bgp {route | neighbor | summary | config}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route</td>
<td>Displays the BGP routing table.</td>
</tr>
<tr>
<td>summary</td>
<td>Displays the BGP protocol summary.</td>
</tr>
<tr>
<td>neighbor</td>
<td>Displays information about all known BGP neighbors.</td>
</tr>
<tr>
<td>config</td>
<td>Displays the running BGP configuration file.</td>
</tr>
</tbody>
</table>

**Example**

The following examples are for illustration only. The actual output varies based on the Quagga version.

```
Infoblox > show bgp route
BGP table version is 0, local router ID is 50.0.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete
              Network          Next Hop     Metric  LocPrf  Weight  Path
*          i  10.0.1.0/24  10.0.1.1     0    100   0     ?
*>         i  10.0.2.99     11    32768     ?
*          i  10.0.2.0/24  10.0.1.99   2    100   0     ?
*>         i  0.0.0.0       1     32768     ?
*          i  50.0.1.1/32  10.0.1.1   0    100   0     i
*>         i  10.0.2.99    1011    32768     ?
*          i  50.0.1.2/32  0.0.0.0     1    32768     ?
*>         i  0.0.0.0       0     32768     i
...
```

```
Infoblox > show bgp summary
BGP router identifier 50.0.1.2, local AS number 65001
RIB entries 25, using 1600 bytes of memory
Peers 2, using 5024 bytes of memory
Neighbor  V  AS  MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.0.1.1   4  65001  89  85  0  0  0  01:11:27  10
100.0.2.4  4  65004  57  53  0  0  0  00:46:37  5
Total number of neighbors 2
```
show bloxtools

The `show bloxtools` command displays the operational status of the bloxTools service and the usage percentage for the CPU, memory and disk resources.

**Syntax**

```plaintext
show bloxtools
```

This command has no arguments.

**Example**

Following is an example of the output displayed when you execute the command and bloxTools is enabled and its services are running:

```
Infoblox > show bloxtools
bloxTools status: enabled(GREEN)
CPU: 1%, Memory: 21%, Hard Disk: 0%
```
show capacity

The `show capacity` command displays database capacity limits for your NIOS appliance. This allows you to see the object counts and types on a member. This command is useful to see the amount of data is assigned to a member and how that relates to the member’s specified capacity.

Syntax

```
show capacity
```

This command has no arguments.

Example

```
Infoblox > show capacity
Hardware Type = IB-2000
Database Capacity = 1200000 "objects"
Objects Present = 112466 (9 percent used)

<table>
<thead>
<tr>
<th>Count Area</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>16638</td>
<td>dns bind_a</td>
</tr>
<tr>
<td>15000</td>
<td>dns bind_cname</td>
</tr>
<tr>
<td>1000</td>
<td>dns bind_mx</td>
</tr>
<tr>
<td>19392</td>
<td>dns bind_ns</td>
</tr>
<tr>
<td>15501</td>
<td>dns bind_ptr</td>
</tr>
<tr>
<td>836</td>
<td>dns bind_soa</td>
</tr>
<tr>
<td>500</td>
<td>dns bulk_host</td>
</tr>
<tr>
<td>5000</td>
<td>dns dhcp_host</td>
</tr>
<tr>
<td>385</td>
<td>dns dhcp_member</td>
</tr>
<tr>
<td>322</td>
<td>dns dhcp_range</td>
</tr>
<tr>
<td>1538</td>
<td>dns fixed_address</td>
</tr>
<tr>
<td>5000</td>
<td>dns host</td>
</tr>
<tr>
<td>5000</td>
<td>dns host_address</td>
</tr>
<tr>
<td>5000</td>
<td>dns host_alias</td>
</tr>
<tr>
<td>265</td>
<td>dns network</td>
</tr>
<tr>
<td>263</td>
<td>dns shared_network_item</td>
</tr>
<tr>
<td>500</td>
<td>dns srg_zone_linking</td>
</tr>
<tr>
<td>840</td>
<td>dns zone</td>
</tr>
<tr>
<td>18018</td>
<td>dns zone_cluster_secondary_server</td>
</tr>
<tr>
<td>537</td>
<td>dns zone_ext_secondary_server</td>
</tr>
<tr>
<td>208</td>
<td>Grid product_license</td>
</tr>
</tbody>
</table>

Note: Counts per object type not displayed unless at least 100 of that type exist.
show cc_mode

The `show cc_mode` command displays the Common Criteria settings.

**Syntax**

```
show cc_mode
```

This command has no arguments.

**Example**

```
Infoblox > show cc_mode
Common Criteria Mode Setting:
Common Criteria Mode Enabled (grid-level): Yes
```
show certificate_auth_admins

The `show certificate_auth_admins` command displays whether the certificate authentication service is enabled for admins.

Syntax

`show certificate_auth_admins`

This command has no arguments.

Example

```
Infoblox > show certificate_auth_admins
Certificate authentication is enabled for next admins:
   admin
   ...
   [username]
```
show certificate_auth_services

The `show certificate_auth_services` command displays the list of certificate authentication services that are used as effective authorization policies.

Syntax

   show certificate_auth_services

This command has no arguments.

Example

   Infoblox > show certificate_auth_services
   Effective Certificate Authentication Services:
       DoD CaC
       [service name]
show config

The `show config` command displays the DNS or DHCP configuration files, named.conf and dhcpd.conf respectively.

**Syntax**

```
show config {dns | dhcp}
```

- `show config` displays the contents of named.conf and dhcp.conf files. You can page through the output 10 lines at a time.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns</td>
<td>Displays the dns.conf file.</td>
</tr>
<tr>
<td>dhcp</td>
<td>Displays the dhcp.conf file.</td>
</tr>
</tbody>
</table>

**Example**

```
Infoblox > show config dns
   include "/infoblox/var/named_conf";
   options {
      zone-statistics yes;
      directory "/infoblox/var/named_conf";
      version "";
      recursion no;
      listen-on {127.0.0.1; 10.0.0.0;}
      query-source address 10.0.0.0;
   }
   Enter <return> to continue with More lines or enter q<return> to go back to the command line.

Infoblox > show config dhcp
   local-address 10.0.0.0.;
   server-identifier 10.0.0.0;
   ddns-update-style interim;
   authoritative;
   option domain-name "corp100.com";
   mini-lease-time 43200;
   max-lease-time 43200;
   ping-check false;
   log-facility daemon;
   Enter <return> to continue with More lines or enter q<return> to go back to the command line.
```
show connections

The **show connections** command shows the active Internet connections for the NIOS appliance. Use this command to investigate connectivity issues or processes that may have stopped running.

**Syntax**

```
show connections
```

This command has no arguments.

**Example**

The following example provides information on:

- **Proto**: Active protocol, TCP or UDP
- **Recv-Q**: Packets received
- **Send-Q**: Packets sent
- **Local Address**: Host name and type of connection
- **Foreign Address**: IP address of the system connected to the appliance
- **State**: State of the connection

```
Infoblox > show connections
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 localhost:kdm:*:*LISTEN
tcp 0 0 localhost:cluster-disk:*:*LISTEN
tcp 0 0 localhost:localdo:domain:*:*LISTEN
tcp 0 0 localhost:domain:*:*LISTEN
tcp 0 0 localhost:rndc:*:*LISTEN
tcp 0 0 infoblox:localdom:https:*:*LISTEN
tcp 0 0 localhost:https:*:*LISTEN
tcp 0 0 infoblox:localdom:https10.1.1.1:arbotext-lm ESTABLISHED
Enter <return> to continue with More lines or enter q<return> to go back to the command line.
```
show connection_limit

You can use the `show connection_limit` command to display the per client IP address maximum connection limit for the following protocols: HTTP and HTTPS. Note that maximum connections here refer to the network level connections, not application level connections. For example, an HTTPS connection limit of 4 means that there can be a maximum of four TCP connections between any given client IP address and the appliance that are concerned using the HTTPS protocol.

To set the maximum connection limit, see `set connection_limit` on page 45.

Syntax

```
show connection_limit {http | https}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>http</td>
<td>The maximum connection limit for the HTTP protocol.</td>
</tr>
<tr>
<td>https</td>
<td>The maximum connection limit for the HTTPS protocol.</td>
</tr>
</tbody>
</table>

Examples

**Showing the Per Client Address Maximum Connection Limit for the HTTP Protocol**

```
Infoblox > show connection_limit http
Current http connection limit: 150
```
show cpu

The `show cpu` command displays the processor and memory statistics for the NIOS appliance. This command tells you how busy the appliance is and indicates if an appliance is not performing properly.

Syntax

```
show cpu
```

This command has no arguments.

Example

The following example provides information on:

- `swpd`: Amount of virtual memory (swap space) used
- `free`: Amount of available memory
- `idle`: Amount of idle memory
- `buff`: Amount of memory used as buffers (I/O)
- `cache`: Amount of memory used as cache (kernel used memory)
- `swap`
  - `si`: Amount of memory paged in (per/sec) from swap or the file system
  - `so`: Amount of memory swapped out
- `io`: Disk input/output
  - `bi`: Blocks (4K each) received from a block appliance
  - `bo`: Blocks sent to a block appliance
- `system`
  - `in`: Number of hardware interrupts per second—measures how busy the CPU is
  - `cs`: Number of context switches per second—measures how busy the CPU is
- `cpu`: Measures (%) of CPU used in each of these areas—the total equals 100%
  - `us`: Percentage of CPU used running the Infoblox product and other non-kernel processes
  - `sy`: Percentage of CPU used running kernel processes
  - `id`: Percentage of CPU that is currently idle
  - `wa`: Percentage of CPU spent waiting for disk I/O

Note: If the combined io (bi and bo) and cpu wa values are high, it is a sign that the system is overloaded.

```
Infoblox > show cpu
----------memory------------------ --swap--- ---io---- ---system-- ------cpu-------
swpd free idle buff cache si so bi bo in cs us sy id wa st
0 984024 15432 51932 916660 0 0 0 42 61 94 3 2 95 0 0
```
show date

The `show date` command displays the current date, time zone, and time of a NIOS appliance. Use this command if you log in to an appliance from a different time zone. This command is helpful when dealing with a Grid that comprises multiple appliances in multiple time zones.

**Syntax**

```
show date
```

This command has no arguments.

**Example**

```
Infoblox > show date
Tue Aug 16:24:19 EDT 2006
```
show debug

The `show debug` command shows whether debug logging is on or off. When on, debug logging captures all traffic and processes on the NIOS appliance. Due to the verbose nature and the extent of the information captured, these log files grow at a rapid rate. For information on how to turn on or off the debug logging, see `set debug` on page 46.

Note: Infoblox recommends that you turn off debug logging unless Infoblox Support specifically directs you to turn on this feature. If left on, debug logging can cause performance issues.

Syntax

```
show debug
```

This command has no arguments.

Example

```
Infoblox > show debug
Debug logging status : enabled

Infoblox > show debug
Debug logging status : disabled
```

For information on viewing the output of the debug log file, see `show log` on page 184.
show default_route

The `show default_route` command displays the default gateway settings for the NIOS appliance. For information on how to change your default route settings, see `set default_route` on page 48.

**Syntax**

```
show default_route
```

This command has no arguments.

**Example**

```
Infoblox > show default_route
Gateway for the default route: LAN1
IPv4 default Gateway: 10.35.0.1
IPv6 default Gateway: 2620:10a:6000:2400::1
```
show delete_tasks_interval

The `show delete_tasks_interval` command shows the time interval the appliance waits until it deletes the completed and rejected tasks from the system. Once the tasks are removed, they are no longer displayed in the Task Manager tab of Grid Manager. The default interval is 14 days. For information about how to configure this time interval, see `set delete_tasks_interval` on page 49.

**Syntax**

```plaintext
show delete_tasks_interval
```

This command has no arguments.

**Example**

```plaintext
Infoblox > show delete_tasks_interval
show delete_tasks_interval
Current delete tasks interval is 25 days
```
**show dhcp_gss_tsig**

The `show dhcp_gss_tsig` commands provide information about an Infoblox DHCP server that is configured to send GSS-TSIG authenticated DDNS updates to an AD integrated DNS server. You can use these commands to verify your configuration and troubleshoot potential issues. You can also test whether the appliance can communicate with the Key Distribution Center (KDC) and the DNS server.

**Syntax**

```
show dhcp_gss_tsig config
show dhcp_gss_tsig keytab
show dhcp_gss_tsig test dns {ns-ip}
show dhcp_gss_tsig test kdc {kdc-ip} {principal}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>Displays configuration information and runs tests to verify the configuration.</td>
</tr>
<tr>
<td>keytab</td>
<td>Displays information about the keytab file that is in use by the appliance.</td>
</tr>
<tr>
<td>test dns</td>
<td>Tests the configuration by verifying that the destination DNS server is reachable. You must enter the IP address of the destination DNS server.</td>
</tr>
<tr>
<td>test kdc</td>
<td>Tests the configuration by obtaining a test Ticket Granting Ticket (TGT) from the configured KDC. You must specify the following:</td>
</tr>
<tr>
<td></td>
<td>• IP address of the AD domain controller that hosts the KDC for the domain</td>
</tr>
<tr>
<td></td>
<td>• The Kerberos principal you specified when you generated the keytab file, in the following format: <code>username/instance@REALM</code></td>
</tr>
<tr>
<td></td>
<td>— <code>username/instance</code>: The AD user name for the NIOS appliance and the FQDN of the appliance. This entry must be the same on the AD domain controller and the Infoblox appliance.</td>
</tr>
<tr>
<td></td>
<td>— <code>REALM</code>: The Kerberos realm in uppercase.</td>
</tr>
</tbody>
</table>

**Examples**

**Displaying GSS-TSIG configuration information and run a test**

The `show dhcp_gss_tsig config` command displays the following information:

- Whether DHCP and GSS-TSIG dynamic DNS updates are enabled on the appliance
- The system time in UTC
- Information about the KDC, principal, and domain

After it displays information, the appliance can test if it can obtain a TGT from the KDC and provides information about that transaction. Note that the TGT is for test purposes only and does not affect the data used by DHCP and DNS.

It can also test the external zones that are supposed to receive the DDNS updates as follows:

- Verify if the external zones specified in the member’s network view match the member’s domain
- Query the name server IP address for the address of the FQDN from the DNS principal
• Query the name server for the SOA of the zone. It displays a warning if the name server does not respond or if the result does not list the FQDN from the DNS principal as authoritative.

```
Infoblox > show dhcp_gss_tsig config
System time: Tue Oct 21 16:01:43 UTC 2008

DHCP GSS-TSIG configuration for this member:
  KDC address              10.34.123.4
  KDC IP                   10.34.123.4
  Member principal  jdoe/anywhere@CORP100.LOCAL
  Member domain            CORP100.LOCAL
  GSS-TSIG                 enabled
  DDNS updates             enabled
  DHCP service             enabled

Test KDC using member configuration? (y or n): y
Requesting TGT for jdoe/anywhere@CORP100.LOCAL from KDC 10.34.123.4...
Successfully obtained test TGT.
Credentials cache: FILE:/tmp/krb5_cache.18338
  Principal: jdoe/anywhere@CORP100.LOCAL
  Cache version: 4
  Server: krbtgt/CORP100.LOCAL@CORP100.LOCAL
  Client: jdoe/anywhere@CORP100.LOCAL
  Ticket etype: arcfour-hmac-md5, kvno 2
  Ticket length: 957
  Auth time:  Oct 21 12:00:52 2008
  End time:   Oct 21 13:00:52 2008
  Ticket flags: initial, pre-authenticated
  Addresses: addressless
  Successful test. Test TGT destroyed.

This member is configured to update the following zones:
  corp100 on 10.34.123.4 as dns/ns-corp100.corp100.local

Test configured zones? (y or n): y

Next zone is corp100 on 10.34.123.4.
Test this zone? (y or n): y
Testing external zone corp100 on NS 10.34.123.4...
DNS principal is dns/ns-corp100.corp100.local.
Derived FQDN is ns-corp100.corp100.local.
FQDN resolves to nameserver IP.
SOA for corp100 has MNAME ns-corp100.corp100.local.
Nameserver is authoritative for zone.
Zone corp100 appears valid.
```
Displaying information about the keytab

The `show dhcp_gss_tsig keytab` command displays the current keytab.

```
Infoblox > show dhcp_gss_tsig keytab
Vno   Type         Principal
 7    des-cbc-md5  jdoe/instance@CORP100.LOCAL
```

Verifying the DNS server

The `show dhcp_gss_tsig test dns` command verifies the destination DNS server by performing a reverse lookup of the IP address.

```
Infoblox > show dhcp_gss_tsig test dns 10.34.123.4
Querying DNS server 10.34.123.4...
Server responded.

Probable DNS principal: dns/ns-corp100.corp100.local
```

Obtaining a test TGT from the KDC

When you use the `show dhcp_gss_tsig test kdc` command, the appliance tries to obtain a TGT from the KDC using the specified principal. It provides information about the transaction and upon successful completion, deletes the test TGT.

```
Infoblox > show dhcp_gss_tsig test kdc 10.34.123.4 jdoe/instance@CORP100.LOCAL
Requesting TGT for jdoe/instance@CORP100.LOCAL from KDC 10.34.123.4...
Successfully obtained test TGT.

Credentials cache: FILE:/tmp/krb5_cache.12000
  Principal: jdoe/instance@CORP100.LOCAL
  Cache version: 4

Server: krbtgt/CORP100.LOCAL@CORP100.LOCAL
Client: jdoe/instance@CORP100.LOCAL
Ticket etype: arcfour-hmac-md5, kvno 2
Ticket length: 957
Auth time:  Oct 21 12:30:01 2008
End time:   Oct 21 13:30:01 2008
Ticket flags: initial, pre-authenticated
Addresses: addressless

Successful test. Test TGT destroyed.
```
show dhcpd_recv_sock_buf_size

The `show dhcpd_recv_sock_buf_size` displays the current DHCP receive socket buffer size. The default is 1,536 kilobytes. For information about how to set the receive socket buffer size, see `set dhcpd_recv_sock_buf_size` on page 50.

Syntax

```
show dhcpd_recv_sock_buf_size
```

This command has no arguments.

Examples

For NIOS Appliances

```
Infoblox > show dhcpd_recv_sock_buf_size
DHCP 'dhcpd' UDP receive socket buffer size: 1500 KB
```
The `show dhcpv6_gss_tsig` commands provide information about an Infoblox DHCP server for IPv6 that is configured to send GSS-TSIG authenticated DDNS updates to an AD integrated DNS server. You can use these commands to verify your configuration and troubleshoot potential issues. You can also test whether the appliance can communicate with the Key Distribution Center (KDC) and the DNS server.

**Syntax**

```
show dhcpv6_gss_tsig config
show dhcpv6_gss_tsig keytab
show dhcpv6_gss_tsig test dns {ns-ip}
show dhcpv6_gss_tsig test kdc {kdc-ip} {principal}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>Displays configuration information and runs tests to verify the configuration.</td>
</tr>
<tr>
<td>keytab</td>
<td>Displays information about the keytab file that is in use by the appliance.</td>
</tr>
<tr>
<td>dns</td>
<td>Tests the configuration by verifying that the destination DNS server is reachable. You must enter the IP address of the destination DNS server.</td>
</tr>
</tbody>
</table>
| kdc           | Tests the configuration by obtaining a test Ticket Granting Ticket (TGT) from the configured KDC. You must specify the following:  
  - IP address of the AD domain controller that hosts the KDC for the domain  
  - The Kerberos principal you specified when you generated the keytab file, in the following format: `username/instance@REALM`  
    - `username/instance`: The AD user name for the NIOS appliance and the FQDN of the appliance. This entry must be the same on the AD domain controller and the Infoblox appliance.  
    - `REALM`: The Kerberos realm in uppercase. |
show disk

The show disk command displays the disk space that is used. Use this command to verify the amount of free disk space on the NIOS and vNIOS virtual appliances. Infoblox recommends that you regularly check the available disk space. Clear off outdated logs to maintain maximum available disk space. You should not allow the disk to become completely full because this can be detrimental to the performance of the appliance.

Syntax

show disk

This command has no arguments.

Examples

For NIOS Appliances

Infoblox > show disk
Available disk space: 207G
Disk space used: 4%
Infoblox >

For vNIOS Virtual Appliances

Infoblox > show disk
Available disk space: 53G
Disk space used: 5%
Overall disk capacity: 120G
Infoblox >
show dns

The `show dns` command displays DNS query statistics for all DNS views. It also displays the recursive cache for the specified DNS views. This command displays IDN data in punycode.

**Syntax**

```
show dns [stats | cache [wait_time ntime][dns_view...]]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stats</td>
<td>Displays DNS query statistics for all DNS views. You can also use this command to display DNS query statistics for all the DNS views of DNS cache acceleration on IB-FLEX.</td>
</tr>
<tr>
<td>ntime</td>
<td>The maximum time (from 1 to 600 seconds) to wait for the cache file to be ready.</td>
</tr>
<tr>
<td>cache dns_view</td>
<td>Specifies the DNS views for which you want to display the recursive cache.</td>
</tr>
</tbody>
</table>

**Example**

```
Infoblox > show dns stats
success 10
referral 0
nxrrset 0
nxdomain 0
recursion 0
failure 10
```
**show dns-accel**

The `show dns-accel` command displays DNS Cache Acceleration information. This command is available for:

- IB-4030 appliances only when the **DNS Cache Acceleration** license is present.
- IB-FLEX only if the **Flex Grid Activation** license is present in the Grid.

**Syntax**

```
show dns-accel
```

**Example**

```
Infoblox > show dns-accel
Log level: 2 (Critical)
Cache: Enabled
Minimum cached TTL: 1
Maximum cached lifetime: 86400
Cache hit count: 0
Cache miss count: 0
DNS query stats: SUCCESS=0 NXDOMAIN=0 NXRRSET=0 FAILURE=0 REFERRAL=0
System UDP DNS query count: LAN1=0 LAN2=0 MGMT=0 HA=0
System UDP DNS response count: 0

Infoblox > show dns-accel
Log level: 5 (Notice)
Cache: Enabled
Minimum cached TTL: 1
Maximum cached lifetime: 86400
Cache hit count: 0
Cache miss count: 0
DNS query stats: SUCCESS=0 NXDOMAIN=0 NXRRSET=0 FAILURE=0 REFERRAL=0
System UDP DNS query count: LAN1=0 LAN2=0 MGMT=0 HA=0
System UDP DNS response count: 0
```
show dns-accel-cache

The `show dns-accel-cache` command enables you to view the cache for DNS Cache Acceleration. It fetches and displays new acceleration cache data. For existing files, it displays data from the previous collection, if present. This command is available for:
- IB-4030 appliances only when the **DNS Cache Acceleration** license is present.
- IB-FLEX only if the Flex Grid Activation license is present in the Grid.

**Syntax**

```
show dns-accel-cache
```

**Example**

```
Infoblox > show dns-accel-cache
Cache is empty
```
**show dns_gss_tsig**

The `show dns_gss_tsig` commands provide information about an Infoblox DNS server that is configured to receive GSS-TSIG authenticated DDNS updates from a DHCP server. You can use these commands for diagnostic purposes and to troubleshoot issues.

**Syntax**

```
show dns_gss_tsig counters [crypto]| keytab
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>counters</td>
<td>Displays information from the internal counters, which are non-persistent and reset to zero when services are restarted. It displays the number of TKEY (transaction key) requests the Infoblox DNS server has accepted and the number of GSS-TSIG authenticated DDNS updates received. If you specify <code>crypto</code>, the display includes the number of successful and failed attempts to establish a security by context, by encryption type.</td>
</tr>
<tr>
<td>keytab</td>
<td>Displays information about the DNS keytab files that are in use by the appliance.</td>
</tr>
</tbody>
</table>

**Example**

```
Infoblox > show dns_gss_tsig keytab
        Vno | Type               | Principal                  |
        4   | des-cbc-md5        | DNS/ns1.local.test@TEST.LOCAL |
```
show dns_rrl

The `show dns_rrl` command provides information about the Grid or member DNS RRL (Response Rate Limiting) settings. You can use the `set dns_rrl` command to configure the DNS RRL settings. For more information, see `set dns_rrl` on page 53.

Syntax

```
show dns_rrl [member <hostname> | view <viewname> | grid]
```

**Note:** The `show dns_rrl` command accepts the `member` option only on the Grid Master.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>member &lt;hostname&gt;</td>
<td>The FQDN of the Grid member.</td>
</tr>
<tr>
<td>view &lt;viewname&gt;</td>
<td>The name of the DNS view.</td>
</tr>
<tr>
<td>grid</td>
<td>Show RRL settings for the Grid.</td>
</tr>
</tbody>
</table>

Examples

```
Infoblox > show dns_rrl grid
Grid RRL configuration:
  responses_per_second: 200
  window: 15 (default)
  slip: 3
  log_only: false (default)

Grid logging configuration:
  log rate-limit: true (default)
```
show dscp

The `show dscp` command provides information about the Grid and member DSCP values in both decimal and hexadecimal formats. You can use the `set dscp` command to configure the DSCP value. For more information, see `set dscp` on page 55.

Syntax

```
show dscp
```

This command has no arguments.

Examples

For a Grid:

```
Infoblox > show dscp
Grid Level: 30 (0x1e)
Member Level: Override grid setting
              20 (0x14)

Infoblox > show dscp
Grid Level: 30 (0x1e)
Member Level: Use grid setting
```

For an independent appliance:

```
Infoblox > show dscp
DSCP: 28 (0x1c)
```
show dtc_geoip

The show dtc_geoip command provides information about the GeoIP labels that are available in the current MaxMind location database for the respective IP address. You can run this command only if you have installed the DNS Traffic Control license. For more information about DNS Traffic Control, refer to the Infoblox NIOS Administrator Guide.

Syntax

show dtc_geoip <ip-address>

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Valid IPv4/IPv6 address of the host.</td>
</tr>
</tbody>
</table>

Examples

Infoblox > show dtc_geoip 54.243.36.49
Continent = North America
Country = United States
Subdivision = Virginia

Infoblox > show dtc_geoip 2607:f8b0:400a:804::1012
Continent = North America
Country = United States
Subdivision = Atlanta
**show enable_match_recursive_only**

Use the `show enable_match_recursive_only` command to view the status of the match-recursive-only option for all DNS views on a specific Grid member. For information about how to use the match-recursive-only feature, see `set enable_match_recursive_only` on page 56, and also refer to the *Infoblox NIOS Administrator Guide*.

The `show enable_match_recursive_only` command reports one of three possible states:

- **True**: The DNS view is set to use the match-recursive-only setting to restrict and filter client access for the view.
- **False**: The DNS view does not use the match-recursive-only setting.
- **Inherit**: The default, where the DNS view inherits its match-recursive-only setting from the Grid.

**Syntax**

```
show enable_match_recursive_only
```

This command has no arguments.

**Example**

```
Infoblox > show enable_match_recursive_only
View 'default': false
View 'dnsview1': true
View 'external': inherit
```
show file

The **show file** command displays specified groups and files that you can access for diagnostic purposes. You can page through the display 10 lines at a time. Use this command to view files after you enable the bloxTools Environment service.

**Syntax**

```
show file {groups | group}
show file group file1 [file2 ...] [follow]
```

If you use the **show file** command without any arguments, it displays all the files that you can manage with this command. If you use the groups argument, a list of all groups is shown.

If you use the **show file** command with a **group** argument but no **file**, it displays a list of all the files in the specified group. If you use the **show file** command with **group** and **file** arguments, you can specify a real-time (live) view of the file—the same as the using `tail -f` arguments. You can interrupt the display by pressing `Enter`.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groups</td>
<td>Displays a list of available groups.</td>
</tr>
<tr>
<td>group</td>
<td>Displays a list of files for the specified group.</td>
</tr>
<tr>
<td>group file1 [file2 ...]</td>
<td>Displays the specified (group) files.</td>
</tr>
<tr>
<td>follow</td>
<td>Displays the contents of the file live, in real-time.</td>
</tr>
</tbody>
</table>

**Examples**

**Viewing bloxTools Files**

```
Infoblox > show file bloxtools portal_access
Showing file /storage/web-portal/udata/logs/access.log

Infoblox > show file bloxtools portal_error
Showing file /storage/web-portal/udata/logs/error.log

[Thu Sep 04 11:07:59 2008] [warn] RSA server certificate CommonName (CN) 'www.infoblox.com' does NOT match server name!? 
[Thu Sep 04 11:08:03 2008] [notice] Digest: generating secret for digest authentication ...
[Thu Sep 04 11:08:04 2008] [warn] RSA server certificate CommonName (CN) 'www.infoblox.com' does NOT match server name!? 
[Thu Sep 04 11:08:04 2008] [notice] Apache/2.2.6 (Unix) mod_ssl/2.2.6 OpenSSL/0.9.8h DAV/2 mod_perl/2.0.3 Perl/v5.8.8 configured -- resuming normal operations 
[Thu Sep 04 11:11:34 2008] [warn] RSA server certificate CommonName (CN) 'www.infoblox.com' does NOT match server name!? 
[Thu Sep 04 11:11:39 2008] [notice] Digest: generating secret for digest authentication ...
[Thu Sep 04 11:11:39 2008] [notice] Digest: done
[Thu Sep 04 11:11:40 2008] [warn] RSA server certificate CommonName (CN) 'www.infoblox.com' does NOT match server name!? 
[Thu Sep 04 11:11:40 2008] [notice] Apache/2.2.6 (Unix) mod_ssl/2.2.6 OpenSSL/0.9.8h DAV/2 mod_perl/2.0.3 Perl/v5.8.8 configured -- resuming normal operations
```
Infoblox > **show file bloxtools portal_log**
Showing file /storage/web-portal/udata/logs/syslog.log
Sep 4 11:07:55 (none) kernel: Linux version 2.6.17.4 (root@buildvm2) (gcc version 3.2.1) #1 Thu Aug 28 02:20:30 EDT 2008
Sep 4 11:07:55 (none) kernel: On node 0 totalpages: 32768
Sep 4 11:07:55 (none) kernel: Built 1 zonelists
Sep 4 11:07:55 (none) kernel: Kernel command line: root=/dev/root rootflags=hostfs rootfstype=hostfs
ubdb=/storage/web-portal/swapfile
ubdc=/storage/web-portal/storagefile mem=128M eth0=tuntap,uml_htap0 con0=null con1=pts con2=pts
Sep 4 11:07:55 (none) kernel: PID hash table entries: 1024 (order: 10, 4096 bytes)
Sep 4 11:07:55 (none) kernel: Dentry cache hash table entries: 16384 (order: 4, 65536 bytes)
Sep 4 11:07:55 (none) kernel: Inode-cache hash table entries: 8192 (order: 3, 32768 bytes)
Sep 4 11:07:55 (none) kernel: Memory: 124372k available
Sep 4 11:07:55 (none) kernel: Calibrating delay loop... 1648.23 BogoMIPS (lpj=8241152)
Sep 4 11:07:55 (none) syslog-ng[699]: syslog-ng starting up; version='2.0.6'
Sep 4 11:07:55 (none) kernel: Mount-cache hash table entries: 512
Enter <return> to continue with More lines or enter q<return> to proceed to the next file
show hardware_status

The show hardware_status command displays information about the various hardware components of a NIOS appliance. It displays the power supply status, fan speed, the CPU temperature, and status of the RAID array (for the Infoblox-2000 only).

Syntax

show hardware_status

This command has no arguments.

Example

The following example displays the status of an Infoblox-2000.

```
Infoblox > show hardware_status
Power:    Power OK
Fan1:     5075 RPM
Fan2:     4927 RPM
Fan3:     4787 RPM
CPU1_TEMP: +42.0 C
CPU2_TEMP: +48.0 C
SYS_TEMP:    +49 C
RAID_ARRAY: OPTIMAL
RAID_BATTERY: OK READY Yes 103 HOURS
```

The following are notes about the output:

- **POWER**: Displays the status of the power supply. The Infoblox-1552, -1552-A and -2000 have redundant power supplies. If one power supply fails, the line displays POWER FAIL. To find out which power supply failed, check the LEDs of the power supplies.
- **Fan1, Fan2, Fan3**: Displays the fan speed. The Infoblox-2000 has three fans, therefore the sample output displays the speed of each fan. If a fan is not functioning, the output displays 0 RPM.
- **CPU1 TEMP, CPU2 TEMP**: Displays the CPU temperature.
- **SYS TEMP**: Displays the operating temperature of the appliance.
- **RAID ARRAY**: Displays the status of the RAID array of an Infoblox-2000. If at least one disk is not functioning properly, this line indicates that the RAID array is degraded and lists the disks which are online. It also indicates when the RAID array is rebuilding. If there is a disk mismatch, this line indicates so and lists all the RAID disks and their disk types.
- **RAID BATTERY**: This line reports the status of the disk controller backup battery. It includes the following information:
  - Charge status: Displays either OK or CHARGING.
  - Ready status: Displays either READY YES or READY NO.
  - Hours: Displays the estimated number of hours remaining on the battery.

**Note:** This command is not supported on vNIOS appliances on Riverbed and VMware. The vNIOS appliance displays `No sensors present` when you enter this command.
**show hwid**

The `show hwid` command displays the hardware ID. The information provided by this command is required for acquiring a new license.

**Syntax**

```
show hwid
```

This command has no arguments.

**Example**

```
Infoblox > show hwid
Hardware ID: 4dcef037e91a403fe05e10ecd241
```
show ibtrap

The `show ibtrap` command displays whether SNMP traps and email notifications are enabled for the specified event category.

Syntax

```
show ibtrap [category]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>category</td>
<td>Valid values are: Fan, Bloxtools, Disk, Memory, CPU, MGM, HSM, Login, PowerSupply, FTP, TFTP, HTTP, NTP, DNS, DHCP, RootFS, Database, RAID, HA, MSServer, Backup, Clear, SNMP, LCD, SSH, SerialConsole, ENAT, Network, Cluster, Controld, OSPF, IFMAP, BGP, CaptivePortal, DuplicateIP, License, System, Syslog, DiscoveryConflict, ReportingVolume, DisconnectedGrid</td>
</tr>
</tbody>
</table>

Example

```
Infoblox > show ibtrap Fan
Trap Category: Fan
snmp: true
email: false
```
show interface

The `show interface` command displays network interface details. The information reveals how the NIOS appliance is connected to the network. It shows line rate, broadcast address, and whether packets are being dropped. This information allows you to check the status, find the MAC address of an appliance, and provides statistics on the quality of the network signal. This command also displays whether IPv6 is enabled. On the Infoblox-250, -550-A, -1050-A, -1550-A, -1552-A, -2000, and -2000-A appliances, the appliance displays information about the LAN2 port as well. It also displays the bonded interface information when NIC bonding is enabled in the NIOS appliance.

For information about how to change your interface settings, see `set interface` on page 61.

**Syntax**

`show interface [name | all]`

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Displays information about a specific interface. Enter one of the following: <code>lan</code>, <code>lan2</code>, <code>ha</code>, <code>mgmt</code>, or <code>loopback</code>.</td>
</tr>
<tr>
<td>all</td>
<td>Displays information about all interfaces.</td>
</tr>
</tbody>
</table>

**Example**

The following example illustrates how you can use the `show interface` command to view the IP address and MAC address of an appliance, and its network connection details. Note that when you manually configure the speed and duplex of an interface, the appliance communicates only the settings. When you configure the Speed/Duplex settings at 1000M/Full, auto-negotiating is required and the appliance displays `Enabled` instead of `Enabled (Speed/Duplex configured by user)` in the **Negotiation** field, as shown in the following example. Statistical information is also provided on the packets received and transmitted, as well as any errors that have occurred. Lack of packet activity can be a sign of connectivity problems, dropped packages, overruns, or collisions.

```
Infoblox > show interface
LAN:
   IP Address:  10.34.33.11      MAC Address: 00:30:48:98:63:AD
   Mask:        255.255.255.0    Broadcast:   10.34.33.255
   MTU:         1500             Metric:      1
   IPv6 Link:          fe80::230:48ff:fe98:63ad/64
   IPv6 Status:        Enabled
   Negotiation: Enabled
   Speed:       1000M            Duplex:      Full
   DSCP Value:      30
   Status:      UP BROADCAST RUNNING MULTICAST

Statistics Information
   Received
       packets:  24812        bytes:    11660993 (11.1 Mb)
       errors:   0            dropped:  0
       overruns: 0            frame:    0
   Transmitted
       packets:  23148        bytes:    11493844 (10.9 Mb)
       errors:   0            dropped:  0
       overruns: 0            carrier:  0
   Collisions: 0            Txqueuelen: 1000
```
LAN2:

IP Address: 10.1.1.35   MAC Address: 00:30:48:98:63:AF
Mask: 255.255.255.0   Broadcast: 10.1.1.255
MTU: 1500     Metric: 1
IPv6 Link: fe80::230:48ff:fe98:63af/64
Negotiation: Enabled
Speed: 1000M   Duplex: Full
Status: UP BROADCAST RUNNING MULTICAST

Statistics Information
Received
   packets: 11  bytes: 836 (836.0 b)
   errors: 0    dropped: 0
   overruns: 0   frame: 0
Transmitted
   packets: 0    bytes: 0 (0.0 b)
   errors: 0    dropped: 0
   overruns: 0   carrier: 0
   Collisions: 0    Txqueuelen: 1000

Enter <return> to continue with More lines or enter q<return> to go back to command line
**show ip_rate_limit**

The `show ip_rate_limit` command displays the current rate limiting rules. You configure rate limiting rules to limit access or block connections from external sources. The rules take effect immediately when you enable rate limiting. For information on rate limiting and on how to configure rate limiting rules, see `set ip_rate_limit` on page 63.

**Syntax**

```
show ip_rate_limit
```

This command has no arguments.

**Example**

**Viewing the current rate limiting rules**

```
IP rate limiting is enabled.
Source    Limit       Burst
10.10.1.1  0 packets/minute  0 packets
10.10.1.2  5 packets/minute  5 packets
10.10.2.1/24  5 packets/minute  10 packets
all      5000 packets/minute  5000 packets
```
**show ipv6_bgp**

The `show ipv6_bgp` command displays the local NIOS appliance’s IPv6 BGP configuration, reachability information about neighbors, and BGP routes to destinations. You can specify the command with or without an argument. A command without an argument defaults to `show bgp route`. For information about how to write statistical information to syslog, see `set bgp log` on page 40.

**Syntax**

```
show ipv6_bgp {route | neighbor | summary | config}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route</td>
<td>Displays the BGP routing table.</td>
<td>Displays the BGP protocol summary.</td>
</tr>
<tr>
<td>summary</td>
<td>Displays information about all known BGP neighbors. If only IPv4 BGP information is available, this command option displays IPv4 information.</td>
<td>Displays the running BGP configuration file, including all IPv4 and IPv6 configuration, prefix lists and access-lists.</td>
</tr>
<tr>
<td>neighbor</td>
<td>Displays the BGP protocol summary.</td>
<td>Displays the running BGP configuration file, including all IPv4 and IPv6 configuration, prefix lists and access-lists.</td>
</tr>
</tbody>
</table>

If no applicable information is available (for example, the current device has no IPv6 BGP configuration and hence no IPv6 BGP neighbor information), you are returned to the NIOS CLI prompt.

**Example**

```
Infoblox > show ipv6_bgp summary
BGP router identifier 10.34.1.179, local AS number 1
RIB entries 3, using 288 bytes of memory
Peers 1, using 4560 bytes of memory

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.34.1.178     4    10  192542  240631        0    0    0 02:45:16        0

Total number of neighbors 1
```

```
Infoblox > show ipv6_bgp neighbor
BGP neighbor is 2001:1938:BA8::22AA:1, remote AS 10, local AS 1, external link
BGP version 4, remote router ID 10.36.1.66
BGP state = Established, up for 02:11:21
Last read 14:34:06, hold time is 16, keepalive interval is 4 seconds
Neighbor capabilities:
  4 Byte AS: advertised and received
  Route refresh: advertised and received(old & new)
  Address family IPv4 Unicast: advertised and received
  Address family IPv6 Unicast: advertised and received
Message statistics:
  Inq depth is 0
  Outq depth is 0
  Sent   Rcvd
  Opens: 118  25
```
Notifications: 13 88
Updates: 219 0
Keepalives: 239773 192022
Route Refresh: 0 0
Capability: 0 0
Total: 240123 192135

Enter <return> for next page or q<return> to go back to command line.
Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
   NEXT_HOP is always this router
   Community attribute sent to this neighbor(both)
   Inbound path policy configured
   Outbound path policy configured
   Incoming update prefix filter list is *DEFAULT
   Outgoing update prefix filter list is *ANYCAST
   0 accepted prefixes

For address family: IPv6 Unicast
   Community attribute sent to this neighbor(both)
   0 accepted prefixes

Connections established 73; dropped 72
Last reset 02:13:50, due to BGP Notification send
Local host: 10.34.1.179, Local port: 179
Foreign host: 10.34.1.178, Foreign port: 43135
Nexthop: 10.34.1.179
Nexthop global: 2001:db8:a22:1b0::3
Nexthop local: fe80::230:48ff:febc:9503
BGP connection: non shared network
Read thread: on  Write thread: off
**show ipv6_disable_on_dad**

The `show ipv6_disable_on_dad` command displays whether IPv6 is disabled, when a duplicate IPv6 address is detected, on the corresponding interface.

**Syntax**

```
show ipv6_disable_on_dad
```

**Examples**

```
Infoblox > show ipv6_disable_on_dad
Disable IPv6 if duplicate IPv6 address detected: off

Infoblox > show ipv6_disable_on_dad
Disable IPv6 if duplicate IPv6 address detected: on
```
show ipv6_neighbor

The `show ipv6_neighbor` command displays the status, IPv6 address and link-local address (normally, the MAC address of the neighboring port) of the IPv6 neighbor for the specified NIOS appliance interface–LAN, LAN2 or MGMT.

Syntax

    show ipv6_neighbor <lan|lan2|mgmt>

If no applicable information is available (for example, the current device has no IPv6 configuration and hence no IPv6 neighbor information), you are returned to the NIOS CLI prompt.

Example

    Infoblox > show ipv6_neighbor lan
    fe80::204:96ff:fe1d:1980 lladdr 00:04:96:1d:19:80 router STALE
show ipv6_ospf

The `show ipv6_ospf` command displays configuration and statistical information about the OSPFv3 protocol (if any) running on the NIOS appliance. For information on changing OSPF log settings, see `set ipv6_neighbor` on page 67.

Syntax

```
show ipv6_ospf {route | interface | database | neighbor | configuration}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route</td>
<td>Displays the OSPF routing table, as determined by the most recent SPF calculation.</td>
</tr>
<tr>
<td>interface</td>
<td>Displays the state and configuration on all interfaces configured with OSPF.</td>
</tr>
<tr>
<td>database</td>
<td>Displays all OSPF database information.</td>
</tr>
<tr>
<td>neighbor</td>
<td>Displays the OSPF neighbor information.</td>
</tr>
<tr>
<td>configuration</td>
<td>Displays the running OSPF configuration file.</td>
</tr>
</tbody>
</table>

Examples

```
Infoblox > show ipv6_ospf
OSPFv3 Routing Process (0) with Router-ID 10.34.1.179
Running 11d03:14:41
Number of AS scoped LSAs is 2
Number of areas in this router is 1
Area 0.0.0.61
    Number of Area scoped LSAs is 4
    Interface attached to this area: eth1

Infoblox > show ipv6_ospf interface
eth1 is up, type BROADCAST
    Interface ID: 11
    Internet Address:
        inet : 10.34.1.179/29
        inet6: 2001:db8:a22:1b0::3/64
        inet6: fe80::230:48ff:febc:9503/64
    Instance ID 0, Interface MTU 1500 (autodetect: 1500)
    MTU mismatch detection: enabled
    Area ID 0.0.0.61, Cost 1
    State BDR, Transmit Delay 1 sec, Priority 1
    Timer intervals configured:
        Hello 10, Dead 40, Retransmit 5
    DR: 255.1.1.1 BDR: 10.34.1.179
    Number of I/F scoped LSAs is 2
        0 Pending LSAs for LSUpdate in Time 00:00:00 [thread off]
        0 Pending LSAs for LSAck in Time 00:00:00 [thread off]

eth2 is down, type BROADCAST
```
show lcd

The `show lcd` command displays whether the LCD keys are turned on or off.

**Syntax**

```
show lcd
```

This command has no arguments.

**Example**

```
Infoblox > show lcd
No LCD present
```
show lcd_info

The `show lcd_info` command displays status, CPU temperature, network settings, version, hardware ID, and licensing information. It also displays the bonded interface information when NIC bonding is enabled in the NIOS appliance. This command combines the output of the following CLI commands: `show status`, `show temperature`, `show network`, and `show license`.

**Syntax**

```
show lcd_info
```

This command has no arguments.

**Example**

```
Infoblox > show lcd_info
Grid Status: ID Grid Master
HA Status:      Not Configured

CPU_TEMP:  +45.5 C

Current network settings:
IP Address:                 10.35.0.20
Network Mask:               255.255.255.0
Gateway Address:            10.35.0.1
HA enabled:                 false
Grid Status:             Master of Infoblox Grid

Version         : 4.2r2-0
Hardware ID     : 553a25c34f45e4a2a2349d996ae1285

License Type    : Grid
Expiration Date : 05/31/2009
License String  : GQAAAL8oY9e0uah3MkKfPdLXrWDTs5D4p3UerF8=

License Type    : DNS
Expiration Date : Permanent
License String  : EQAAAL4oZM7r+K+zctvOPdLUpH3V

License Type    : Grid Maintenance
Expiration Date : 05/31/2009
License String  : GwAAALQveMG2uqbuM8iReNLV4C/Q/5Lw6yxQ/V7Pdg==

License Type    : NIOS Maintenance
Expiration Date : 05/31/2009
License String  : GwAAALQveMG2uqbuM8iReNLV4C/Q/5Lw6yxQ/LvMjg==

License Type    : DHCP
Expiration Date : Permanent
License String  : EgAAAL4udMK65OLibpafI2+y/S6A5Q==
```

**Note:** This command is not supported on vNIOS appliances on Riverbed and VMware. On a Riverbed platform, the `show lcd_info` command generates network settings and licensing information, but not the hardware information. The `No sensors present` message is displayed in place of the hardware information.
show lcd_settings

The `show lcd_settings` command displays the value of these fields: lcd_autodim/lcd_brightness/lcd_hwident.

Syntax

```
show lcd_settings
```

This command has no arguments.

Example

```
Infoblox > show lcd_settings
LCD settings can not be configured.
```
The `show license` command displays information about the licenses installed on NIOS appliances, vNIOS appliances, and Orchestration Servers. For information, refer to the *Infoblox NIOS Administrator Guide*. You can use this command to view licenses that were transferred from one vNIOS on VMware appliance to another. For information on how to set your licenses, see `set license` on page 74.

This command displays Grid-wide licenses when you specify `gridwide` or `all` arguments. Without any arguments, the static licenses for the member are displayed.

### Syntax

```
show license [all | csv | gridwide | revoked]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all product licenses in a Grid.</td>
</tr>
<tr>
<td>csv</td>
<td>Displays all product licenses in a Grid in csv format.</td>
</tr>
<tr>
<td>gridwide</td>
<td>Displays Grid-wide licenses in a Grid.</td>
</tr>
<tr>
<td>revoked</td>
<td>Displays vNIOS licenses that were transferred from one vNIOS appliance to another.</td>
</tr>
</tbody>
</table>

### Examples

#### Showing product licenses installed on a NIOS appliance

```
Infoblox > show license
```

```
Version : 4.3r2-5
Hardware ID : 6ddd3618a43027fddb3b3ca9a29077a7

License Type : NIOS Maintenance
Expiration Date : 05/13/2009
License String : GwAAAAsiM/VsmcoYLM主持c8f6T7L7HDdR+HeL6U1WA==

License Type : Grid
Expiration Date : 05/13/2009
License String : GAAAAA1KONBms0BL3Ai9M8bpmPKoHLUC+HEfPM=

License Type : DNS
Expiration Date : Permanent
License String : EAAAAAEjL/oe28NFbWlz8M0arW7M

License Type : DHCP
Expiration Date : Permanent
License String : EgAAAAEfjP/ZPx44UCQpi7IW9D2Z9g==

License Type : Grid Maintenance
Expiration Date : 05/13/2009
License String : GwAAA4uJfVHhdENA2Yrsc8f6T7L7HDdR+HeLfE2UQ==
```

#### Showing product licenses installed on a NIOS Discovery Probe appliance

```
Infoblox > show license
```

```
Version : 6.9.0-271002
Hardware ID : 564d5d736f92734270264e24bd7f34ea
```
CLI Commands

License Type : Grid
Expiration Date : 12/21/2015
License String : GgAAALb+k/nMu+ts7UIw7sK1+7B70RJDDrqZXR8

License Type : vNIOS (model ND-V1400)
Expiration Date : 12/21/2015
License String : HAAAAAKX+jvPNt6sx4hV9oMT5+LJ70gZDCFabHOUm4tA=

License Type : Discovery
Expiration Date : 12/21/2015
License String : GQAAALf5lP/Rvfx351t+6Ir7+P010xNBQf6cCeU=

**Showing product licenses installed on an Infoblox Orchestration Server**

Infoblox > show license

Version : 5.x-86034
Hardware ID : 6ddd3618a43027fdbb3b3ca9a29077a7

License Type : IF-MAP Service
Expiration Date : 05/04/2010
License String : FAAAAAwtMedDlo5fICEi84MbpXPPpHCI

**Showing product licenses of all Grid members in csv format**

Infoblox > show license csv

<table>
<thead>
<tr>
<th>public_ip,license_type,exp_date,license_string</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.18,DNS,Permanent,EQAAAAKS4n90WFGNUSirwwyUT9/z</td>
</tr>
<tr>
<td>10.0.0.18,Grid Maintenance,05/21/2009,EwAAAA4ujFVHhdENA2Yrs8b6T3J7HDdR+HeLfQ2Cq==</td>
</tr>
<tr>
<td>10.0.0.18,Grid,05/21/2009,GwAAAA226HAtBkPFPyfzg/yVRSzZI2x0kYKoPb22g==</td>
</tr>
<tr>
<td>10.0.0.18,NIOS Maintenance,01/21/2009,GwAAAAiV/nAGGljQEDv0h/yVRSzZI2x0kYKoPb22g==</td>
</tr>
<tr>
<td>10.0.0.18,DHCP,Permanent,EgAAAAEjP/ZFx44UcSqi7JW9D229g==</td>
</tr>
<tr>
<td>10.0.0.18,DNS,05/21/2009,EgAAAAKU8nM1RbcTWK63rHYFoymQO==</td>
</tr>
<tr>
<td>10.0.0.22,Grid Maintenance,05/21/2009,GwAAAA4ujFVHhdENA2Yrs8b6T3J7HDdR+HeLfQ2Cq==</td>
</tr>
<tr>
<td>10.0.0.22,Grid,05/21/2009,GwAAAA226CftBkPFPyfzg/yVRSzZI2x0kYKoPb22g==</td>
</tr>
<tr>
<td>10.0.0.22,NIOS Maintenance,05/21/2009,GwAAAAiV/nAGGljQEDv0h/yVRSzZI2x0kYKoPb22g==</td>
</tr>
<tr>
<td>10.0.0.22,DHCP,Permanent,EgAAAAEjP/ZFx96UcSqi7JW9D229g==</td>
</tr>
</tbody>
</table>

**Showing vNIOS on VMware licenses that were transferred**

Infoblox > show license revoked

Public IP | License Type | Exp Date | Replaced Hardware ID |
----------|--------------|----------|----------------------|
10.34.196.221 | Grid | Permanent | 564dc31965c24cc2eb7ab2955e10e1c0 |
License String
PQAAADUCMoaGagzzTP0jgMU8FjNONq8dY2Ux527eLxDjCxyqsaL3woZgtPdEzhTgV+4Xk+OEYvmWk3rUf9s1Q

10.34.196.221 vNIOS (550) Permanent 564dc31965c24cc2eb7ab2955e10e1c0
AgAAACYCL4yH210r7Qvu0d1xRzAWLqtRdXQ39z+LKEW5DhjrrseLjgwfg9bZEzL1ljWkqOEN9zQD4wsRU=

**Showing product licenses, including a transferred vNIOS license**

Infoblox > show license

Version : 5.1r4-111576-ul
Hardware ID : 564d636db7a4892b1065c1d9493673a4

License Type : DHCP
Expiration Date : Permanent
License String : EgAAADQEJZ0IN0/mEqkqgMU8WjBFtQ==
License Type : DNS
Expiration Date : Permanent
License String : EQAAADQCNZ/2KwK3DuRynIhwA2MG

License Type : Grid
Expiration Date : Permanent
Revoked Hardware ID : 564dc31965c24cc2eb7ab2955e10e1c0
License String : PQAAADUCmoaGagzzTP0jgMU8FjNONq8dY2Ux527eLxDjCxyxqsaL3woZgtPdEz
License String : P0AAADzK2KqIRqJ3C1/Hc+X+QbXZfP+2R5I=

License Type : MS Management
Expiration Date : Permanent
License String : GwAAADDfGY6Vv/b/9WvU6w4A8FjNONq8dfHB9pm+JeA==

License Type : NIOS Maintenance
Expiration Date : Permanent
License String : GgAAAD4FKZCraQvqT/ct2YhtCn4fKuJMYDl19T7Z

License Type : vNIOS (550)
Expiration Date : Permanent
Revoked Hardware ID : 564dc31965c24cc2eb7ab2955e10e1c0
License String : OgAAACYCL4yHZlOrQ7Vu0dlxRzAWLqtRdXQ39z+LKEw5DsJgwrseLJgwfg9b2Ez
License String : OgAAACqQ00kWkE9qQ9+Q5CIvGe4QZdQdR=

vNIOS: CPU cores detected: 1 - [License allows: 1]
vNIOS: CPU frequency detected: 1200MHz - [License allows: 1200MHz]
vNIOS: System memory detected: 2048MB - [License allows: 2048MB]

Showing all product licenses in a Grid
Infoblox > show license all
Public IP       License Type                Kind      Exp Date   Replaced Hardware ID License String
10.34.12.200    Grid                        Static    01/27/2017 GQAAAN75s+oj6JImWMxz2c8VyGvYoQ3y2i60L3Y=
10.34.12.200    DHCP                        Static    Permanent EgAAAN/j7/30ec6bWhZb4g8Tlh7Fg==
10.34.12.200    DNS                         Static    Permanent EAAAA/s//GlZYfScSUlc8WvFesu
10.34.12.210    DNS                         Static    Permanent EQAAAN0m9pKz23n6iHLrlWhVRW
10.34.12.210    DHCP                        Static    Permanent EgAAAN0gY9btyC29myWMvXa3AcD6Q==
10.34.12.210    Grid                        Static    Permanent GgAAAN0m3wM6mOjqDrWvXajwIevdQ7U0THhL0
10.34.12.220    Grid                        Static    11/28/2016 GgAAAGq4nPRV7i2S03s7qM9vaokCkg6eUcC/g
10.34.12.220    vNIOS (model ND-V1400)    Static    11/28/2016 HAAAANm4gf5UJ/jsRQsoKJ09fiokz6kgeu/WY57vO2w=
10.34.12.220    Discovery                   Static    11/28/2016 GQAAAGm/m/JyLa+tQVS77wx/LLmktJyfeOTdsw=

Showing Grid-wide licenses in a Grid
Infoblox > show license gridwide
License Type Exp Date License String
Security Ecosystem Permanent HQAAALsakOzDKirMdaUsG2Yfk/j0BkhoFjhvFfEtu36dJ
Showing Grid-wide licenses in a Grid when an Flex Grid Activation License is installed

```
Infoblox > show license
Version : 8.0.0-347398
Hardware ID : 0800201605040013

License Type : Grid
Expiration Date : 04/20/2017
License String : GQAAADmh7ID3wf0qOe98xJnJ79mgh004FM2wrE=

License Type : DHCP
Expiration Date : Permanent
License String : EgAAADin+5X5nL4/Z7t83dShvpfzxA=

License Type : DNS
Expiration Date : Permanent
License String : EQAAADih65mogPNue/YtwZnL58Sm
```

```
Infoblox > show license all
Public IP License Type Kind Exp Date Replaced Hardware ID License String
Flex Grid Activation Grid-wide 02/19/2017 JAAAAPwgn32cIJa1oBqYtcfxdVn71rlvRTO1cjljzoXvn9yga2g==
10.35.5.176 Grid Static 04/20/2017 GQAAADmh7ID3wf0qOe98xJnJ79mgh004FM2wrE=
10.35.5.176 DHCP Static Permanent EgAAADin+5X5nL4/Z7t83dShvpfzxA==
10.35.5.176 DNS Static Permanent EQAAADih65mogPNue/YtwZnL58Sm
10.35.105.10 Grid Static 02/19/2017 GgAAAOgU19juLjevCfnnAfIKoTGz4RzoxRz7mjdO
10.35.105.10 vNIOS (model IB-VM-1410) Static 02/19/2017 GgAAAPsUytLvInTyBq2jTPRGoT+z4gjPzowG5z5g
10.35.105.10 Threat Protection (Software add-on) Static 02/19/2017 FQAAAP4N/Mn8nTyBq2jTPRGoT+z5018xQ==
10.35.105.10 Threat Protection Update Static 02/19/2017 FgAAAPkK/M7/PnDn3TuCrcbEoDn4oRo1Zg=
10.35.105.10 DHCP Static 02/19/2017 FAAAAlSwM3gb3G6s6XmAvb2Hdp3T54xvo
10.35.105.10 DNS Static 02/20/2017 EwAAAOKU0MGtajn0SuCoApd7Guu5U0=
```

Showing all licenses in a Grid when Software ADP is installed

```
Infoblox > show license
Version : 8.1.0-348290
Hardware ID : 564d6d00229a6cd6d197ffcd1383e37b

License Type : Grid
Expiration Date : 03/10/2017
License String : GgAAAN8Cp2mr0u/Es9xNAGCAeAvdy+7J5L/704mo

License Type : vNIOS (model IB-VM-1410)
Expiration Date : 03/10/2017
License String : GgAAAMwCumOq3qyVvIgBTWfMeAzydPr4ueth4Cm
```
show license

vNIOS: System memory detected: 8192MB - [License allows: 8192MB]

License Type : Threat Protection (Software add-on)
Expiration Date : 03/10/2017
License String : FQAAAMkbjHip3qyYvIgBTWfMeAzdzb2etQ==

License Type : Threat Protection Update
Expiration Date : 03/10/2017
License String : FgAAAM4cjH+swOGc9cUAASn0eOqWhbiatQ=

License Type : DNS
Expiration Date : 03/10/2017
License String : EwAAAN4CoHDol+Gc8MUDAWLNVjAz78=

License Type : DHCP
Expiration Date : 03/10/2017
License String : FAAAAN4EsHylk6jR8YlNA2XNfkeXwOnJ
**show license_uid**

The `show license_uid` command displays the license UID of the Grid. The UID is required when requesting Grid-wide licenses. The UID that the appliance returns is the same as the License Pool Container UID that is used for obtaining dynamic licenses.

**Syntax**

```
show license_uid
```

This command has no arguments.

**Examples**

```
Infoblox > show license_uid
The grid-wide license unique ID (same as LPC_UID): e51f90527dce4708bc1ada576286d26a
```
show license_pool_container

The `show license_pool_container` command displays the license UID that is required when obtaining dynamic licenses for vNIOS virtual appliances.

Syntax

```
show license_pool_container
```

This command has no arguments.

Examples

```
Infoblox > show license_pool_container
The Unique ID of the License Pool Container (LPC_UID): e51f90527dce4708bc1ada576286d26a
```
show log

The **show log** command displays a specified log file. It is helpful for obtaining diagnostic information. The syslog file is shown by default if no log is specified. The IF-MAP log displays all the IF-MAP protocol related events. It contains the XML messages communicated between Infoblox Orchestration Server and the clients.

**Syntax**

```
show log [ syslog | debug | audit | ifmapclient | ifmapserver ] <log num> [ tail <num> | follow/regex/ ]
```

Use this command to display the contents of a specified log file.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>syslog</td>
<td>Displays the syslog log file.</td>
</tr>
<tr>
<td>debug</td>
<td>Displays the debug log file.</td>
</tr>
<tr>
<td>audit</td>
<td>Displays the audit log file.</td>
</tr>
<tr>
<td>ifmapclient</td>
<td>Displays the IF-MAP log on the DHCP server when it is configured as an IF-MAP client.</td>
</tr>
<tr>
<td>ifmapserver</td>
<td>Displays the IF-MAP log on Infoblox Orchestration Server.</td>
</tr>
<tr>
<td>log num</td>
<td>Allows you to view rolled logs by specifying a number from 0 to 9. You can use this option when you display the syslog file, audit log, and ifmap log.</td>
</tr>
<tr>
<td>tail &lt;num&gt;</td>
<td>Shows the last num lines from the log file or, if no number is specified, the last 10 lines are displayed.</td>
</tr>
<tr>
<td>/regex/</td>
<td>Matches the pattern specified in regex and displays the matched lines from the selected log file. To insert &quot;/&quot; in the search pattern, use escape sequence . The search string starts at the first forward slash (/) ends at the second forward slash (/), and ignores the remaining. For information about regular expressions, see Appendix B, Regular Expressions, in the Infoblox Administrator Guide.</td>
</tr>
</tbody>
</table>

**Examples**

**Displaying syslog file**

```
Infoblox > show log syslog
Aug 23 17:48:50 (none) syslog-ng[894]: new configuration initialized
Aug 23 17:48:50 (none) kernel: ip_conntrack version 2.4 (8183 buckets, 65464 max) - 224 bytes per conntrack
Aug 23 17:48:54 (none) kernel: ADDRCONF(NETDEV_UP): eth1: link is not ready
Aug 23 17:48:56 (none) kernel: e1000: eth1: e1000_watchdog: NIC Link is Up 1000 Mbps Full Duplex
Aug 23 17:48:56 (none) kernel: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
Aug 23 17:48:58 (none) ntpd[31091]: ntpd 4.1.2@1.892 Fri Aug 4 17:14:23 EDT 2006 (1)
Aug 23 17:48:58 (none) ntpd[31091]: signal_no_reset: signal 13 had flags 400000
Aug 23 17:48:58 (none) ntpd[31091]: precision = 11 usec
Aug 23 17:48:58 (none) ntpd[31091]: kernel time discipline status 0040
Aug 23 17:48:58 (none) ntpd[31091]: frequency initialized 0.000 from /usr/conf/ntp.drift
Enter <return> to continue with More lines or enter q<return> to go back to command line
```
Displaying the last five lines of the debug log file

Infoblox > show log debug tail 5
[2006/08/23 17:48:49.346] (30748 /infoblox/one/bin/init_database) db_local.c:347
$db_database_local_create_env(): cache_size: 134217728
[2006/08/23 17:48:49.739] (30748 /infoblox/one/bin/init_database) init_database.c:45
main(): Database initialized: /data/rep
[2006/08/23 17:48:49.812] (30749 /infoblox/one/bin/db_import_3x) main.c:360
main(): Starting db_import: importing from /infoblox/one/factory_defaults
[2006/08/23 17:48:49.899] (30749 /infoblox/one/bin/db_import_3x) partition_bitmap.c:208
onedb_recalculate_partition_bitmaps(): Begin partitioning phase
[2006/08/23 17:48:49.900] (30749 /infoblox/one/bin/db_import_3x) partition_bitmap.c:283
onedb_recalculate_partition_bitmaps(): Total of 2 object(s) partitioned, committing database

Matching a pattern in a log file

Infoblox > show log syslog /ntpd/
7:Aug 23 17:48:58 (none) ntpd[31091]: signal_no_reset: signal 13 had flags 4000000
8:Aug 23 17:48:58 (none) ntpd[31091]: precision = 11 usec
9:Aug 23 17:48:58 (none) ntpd[31091]: kernel time discipline status 0040
10:Aug 23 17:48:58 (none) ntpd[31091]: frequency initialized 0.000 from /usr/conf/ntp.drift
11:Aug 23 17:48:58 (none) ntpd[31091]: frequency initialized 0.000 from /usr/conf/ntp.drift
13:Aug 23 17:50:13 (none) ntpd[31091]: ntpd exiting on signal 15
19:Aug 23 17:50:23 (none) ntpd[32623]: signal_no_reset: signal 13 had flags 4000000
20:Aug 23 17:50:23 (none) ntpd[32623]: precision = 9 usec

Displaying the IF-MAP log file

Infoblox > show log ifmapserver
2010-03-16T17:48:04 REQUEST "client1" PUBLISH: info <?xml version="1.0"
encoding="UTF-8"?><env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/
xmlns:ifmap="http://www.trustedcomputinggroup.org/2006/IFMAP/1"
xmlns:meta="http://www.trustedcomputinggroup.org/2006/IFMAP-METADATA/1"
xmlns:wsdl="http://www.trustedcomputinggroup.org/2008/IFMAP/1/ifmap.wsdl"
xmlns:meta3="www.stan.com2"
<ifmap:session-id>28baf7e3d84db248097e976bf0dce9c2</ifmap:session-id>
</SOAP-ENV:Header> <SOAP-ENV:Body> <ifmap:publish> <update> <link> <identifier> <ip-address
value="10.0.0.5"/> </identifier> <identifier> <mac-address value="56:b1:19:3b:48:0d"/>
</link> <metadata> <meta:ip-mac cardinality="singleValue">
<start-time>2009-10-27T00:00:00</start-time> <end-time>2009-10-28T00:00:00</end-time>
</SOAP-ENV:Envelope>
2010-03-16T17:48:04 RESPONSE "client1" PUBLISH: info <?xml version="1.0"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:meta="http://www.trustedcomputinggroup.org/2006/IFMAP-METADATA/1"
xmlns:wsdl="http://www.trustedcomputinggroup.org/2008/IFMAP/1/ifmap.wsdl"
xmlns:meta3="www.stan.com2"
<ifmap:session-id SOAP-ENV:mustUnderstand="1"> 28baf7e3d84db248097e976bf0dce9c2
validation="BaseOnly" /> <publishReceived/> </ifmap:response>
</SOAP-ENV:Body></SOAP-ENV:Envelope>
show logfiles

The show logfiles command displays log files and their respective sizes. You can use this command to gather information on log file sizes, and determine how quickly they are growing. This is useful for managing disk space, as it helps you determine when to download or rotate files. On Infoblox Orchestration Server, this command also displays the IF-MAP log file size.

Syntax

show logfiles

This command has no arguments.

Examples

On a NIOS appliance

Infoblox > show logfiles
Logfiles present on the system
-----------------------------
audit.log 8 k
infoblox.log 26327 k
messages 46 k
messages.0.gz 10 k

On Infoblox Orchestration Server

Infoblox > show logfiles
Logfiles present on the system
-----------------------------
audit.log 10 k
ifmapd.log 27 k
ifmapd.log.0.gz 2 k
ifmapd.log.1.gz 10 k
infoblox.log 353 k
messages 85 k
**show log_txn_id**

The `show log_txn_id` command displays whether DHCP transaction ID logging is on or off. By default, DHCP transaction ID logging is enabled. Use the `set log_txn_id` to enable or disable logging of DHCP transaction IDs.

**Syntax**

    show log_txn_id

This command has no arguments.

**Example**

    Infoblox > show log_txn_id
    DHCP Transaction id logging turned OFF
The `show lom` command displays the LOM (Lights Out Management) settings for the IPMI interface. To configure the network settings for the IPMI interface, use the `set lom` command.

**Syntax**

```
show lom
```

This command has no arguments.

**Example**

```
Infoblox > show lom
LOM for Grid: enabled
LOM for member: enabled (inherit)

Network settings:
IP Address: 10.34.10.42
Subnet Mask: 255.255.255.0
Default Gateway IP: 10.34.10.1

Users:
```
show lower_case_ptr_dname

The `show lower_case_ptr_dname` command displays information about whether the option to convert the domain names in uppercase characters to lowercase for PTR records is on or off. For information about how to enable this conversion option, see `set lower_case_ptr_dname` on page 78.

**Syntax**

```
show lower_case_ptr_dname
```

This command has no arguments.

**Examples**

```
Infoblox > show lower_case_ptr_dname
show lower_case_ptr_dname
default view: on, override_grid: on, grid: off, effective: on
```

For more than one DNS view

```
Infoblox > show lower_case_ptr_dname
show lower_case_ptr_dname
default view: on, override_grid: on, grid: off, effective: on
custom view: off, override_grid: off, grid: off, effective: off
```
show memory

The `show memory` command displays memory statistics on used and available buffers and cache. Poor performance can be an indicator that the memory is full. If your NIOS appliance is not performing as it should, use this command to verify whether or not the appliance is experiencing a memory problem. If so, Infoblox recommends that you call Infoblox Support.

Syntax

```
show memory
```

This command has no arguments.

Example

```
Infoblox > show memory

          total   used   free   buffers   cached
Mem:      1032852  309904   722948   32864    242060
Swap:     2047992    0  2047992
Total:    3080844  309904  2770940
```
**show mld_version**

The `show mld_version` command displays the version of the MLD (Multicast Listener Discovery) protocol that is running on the appliance. The appliance runs MLD version2 by default, but you can enable it to run MLD version 1 instead. (For information, see `set mld_version_1`) Note that MLDv2 is interoperable with MLDv1.

**Syntax**

```
show mld_version
```

This command has no arguments.

**Example**

```
Infoblox > show mld_version
Current Multicast Listener Discovery Setting:
  MLD Version: 2
```
show monitor

The `show monitor` command displays current network monitoring data, when network monitoring for DNS is turned on. This command also provides information on the average latency of authoritative and non-authoritative replies to DNS queries. Latency is the time it takes for a packet to cross a network connection, from sender to receiver.

**Note:** You must turn on network monitoring for DNS to view this data. For more information, see `set monitor dns` on page 82.

**Syntax**

```
show monitor
```

This command has no arguments.

**Examples**

The following example for Network Monitoring for DNS shows information on the interval times in minutes, the latency (in milliseconds), and the number of queries.

**Viewing network monitoring for DNS data**

```
Infoblox > show monitor
Network Monitoring for DNS is ON
Data last updated: Tue Sep 12 19:05:51 2006
Authoritative          Interval (min)  Latency (usec)  Number of queries
1                      2              3
5                      3              20
15                     3              65
60                     3              300
Non Authoritative      Interval (min)  Latency (usec)  Number of queries
1                      2              2
5                      3              10
15                     3              55
60                     3              150
```

**When network monitoring for DNS is off**

```
Infoblox > show monitor
Network Monitoring for DNS is OFF
```
show monitor dns alert

The show monitor dns alert command displays the current DNS alert thresholds. The appliance displays the default thresholds (50% for both invalid ports and invalid TXIDs) if you have not configured new thresholds for the DNS alerts.

Syntax

    show monitor dns alert

This command has no arguments.

Example

Viewing DNS alert thresholds

    Infoblox > show monitor dns alert
    DNS Network Monitoring is enabled.
    Alerting is enabled.
    DNS Alert         Threshold (per minute)
    ================  =========================
    port             over 70% of packets
    txid             over 100 packets
show monitor dns alert status

The `show monitor dns alert status` command displays the current status of invalid DNS responses that arrive on DNS ports that are not open and have mismatched TXIDs (DNS transaction ID). You can view the alert status to identify the primary source of invalid DNS responses. The appliance displays historical alert counts and up to five primary sources that generate invalid DNS responses.

**Syntax**

```
show monitor dns alert status
```

This command has no arguments.

**Example**

**Viewing DNS alert status**

```
Infoblox > show monitor dns alert status
Data last updated: Mon Oct 6 14:47:12 2008
DNS Alert 1m  5m  15m  60m  24h  Ever
============================================
port  8  12  12  12  12  12
Txid  8  12  12  12  12  12
```

There were 80 DNS responses seen in the last minute.
10% were to an invalid port.
10% had an invalid TXID.

Primary sources of invalid responses:
4.4.4.4 (unknown) sent 4
2.2.2.2 (unknown) sent 3
7.7.7.7 (unknown) sent 1
show named_recv_sock_buf_size

The `show named_recv_sock_buf_size` command displays the current BIND receive socket buffer size. The default is 1,536 kilobytes. For information about how to set the receive socket buffer size, see `set named_recv_sock_buf_size` on page 85.

Syntax

```
show named_recv_sock_buf_size
```

This command has no arguments.

Example

```
Infoblox > show named_recv_sock_buf_size
DNS 'named' UDP receive socket buffer size: 5000
```
show network

The show network command displays the current network settings for the NIOS appliance and status with respect to a Grid. For information on how to change your network settings, see set network on page 86.

Syntax

    show network

This command has no arguments.

Example

    Infoblox > show network
    Current LAN1 network settings:
    IP Address: 10.34.33.11
    Network Mask: 255.255.255.0
    Gateway Address: 10.34.33.1
    VLAN Tag: 110
    DSCP Value: 23
    IPv6 Address: 2620:010A:6000:2400:0000:0000:0000:6508/64
    IPv6 VLAN Tag: Untagged
    IPv6 DSCP Value: Inherited
    HA enabled: false
    Grid Status: Member of Infoblox Grid

    Current LAN2 Port Settings:
    LAN2 Port enabled: true
    NIC failover for LAN1 and LAN2 enabled: false
    LAN2 IP Address: 10.1.1.35
    LAN2 Netmask: 255.255.255.0
    LAN2 Gateway: 10.1.1.1
**show ntp**

The `show ntp` command displays a list of the peers of the NTP server, along with status information about each peer.

**Syntax**

```
show ntp
```

This command has no arguments.

**Example**

```
Infoblox > show ntp

remote           refid      st  t when poll reach  delay  offset  jitter
==============================================================================
*LOCAL(1)        LOCAL(1)        12 1   47   64  377    0.000    0.000 0.008
```

When you execute the `show ntp` command, the NIOS appliance displays the following information:

- **remote**: The IP address of the remote peer.
- **refid**: Identifies the reference clock.
- **st**: The stratum of the remote peer.
- **t**: The type of the peer, such as local, unicast or broadcast.
- **when**: When the last packet was received.
- **poll**: The polling interval, in seconds.
- **reach**: The reachability register, in octal numerals.
- **delay**: The current estimated delay, in seconds.
- **offset**: The offset of the peer clock relative to the local clock, in milliseconds.
- **jitter**: The estimated time error of the system clock.
show ospf

The `show ospf` command displays configuration and statistical information about the OSPF protocol that is running on the NIOS appliance. For information on how to change your OSPF settings, see `set ospf` on page 92.

Syntax

```
show ospf {route | interface | database | neighbor | configuration}
```

The `show ospf` command displays information about the OSPF configuration on the appliance, reachability information about neighbors, and OSPF routes to destinations. You can specify the command with or without arguments.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route</td>
<td>Displays the OSPF routing table, as determined by the most recent SPF calculation.</td>
</tr>
<tr>
<td>interface</td>
<td>Displays the state and configuration on all interfaces configured with OSPF.</td>
</tr>
<tr>
<td>database</td>
<td>Displays all OSPF database information.</td>
</tr>
<tr>
<td>neighbor</td>
<td>Displays the OSPF neighbor information.</td>
</tr>
<tr>
<td>configuration</td>
<td>Displays the running OSPF configuration file.</td>
</tr>
</tbody>
</table>

Examples

```
Infoblox > show ospf interface
eth0 is down
    OSPF not enabled on this interface
eth1 is up
    Internet Address 172.32.0.61/24, Broadcast 172.32.0.255, Area 0.0.0.0
    Router ID 172.32.0.61, Network Type BROADCAST, Cost: 100
    Transmit Delay is 1 sec, State DROther, Priority 0
    Designated Router (ID) 172.32.0.110, Interface Address 172.32.0.254
    No backup designated router on this network
    Timer intervals configured, Hello 10, Dead 40, Wait 3, Retransmit 5
    Hello due in 00:00:01
    Neighbor Count is 1, Adjacent neighbor count is 1
lo is up
    Internet Address 172.16.10.10/32, Area 0.0.0.0
    Router ID 172.32.0.61, Network Type LOOPBACK, Cost: 100
    Transmit Delay is 1 sec, State Loopback, Priority 0
    No designated router on this network
    No backup designated router on this network
    Timer intervals configured, Hello 10, Dead 40, Wait 3, Retransmit 5
    Hello due in inactive
    Neighbor Count is 0, Adjacent neighbor count is 0
```
Infoblox > `show ospf route`

======== OSPF network routing table ========
N  172.16.10.10/32  [100] area: 0.0.0.0
directly attached to lo
N  172.32.0.0/24  [100] area: 0.0.0.0
directly attached to eth1

======== OSPF router routing table ========

======== OSPF external routing table ========
show phonehome

The show phonehome command displays the settings of the phone home feature on the appliance.

Syntax

    show phonehome

This command has no arguments.

Example

    Infoblox > show phonehome
    Phone home enabled <Grid wide>: Yes
    Send to Infoblox Support: Yes
    Support ID: 8561
    Address to send to:
        support@infoblox.com
**show query_capture**

The `show query_capture` command displays the captured DNS queries that are stored locally on the appliance. You can use filters to restrict the DNS queries to specific time and date range, client FQDNs, and IP addresses. Note that the time zone in the CLI console is the time zone of the Grid member.

**Note:** Using multiple CLI commands to filter data for the appliances with large number of captured DNS queries and responses can significantly affect the system performance, protocol performance, and CLI command performance.

**Syntax**

```
show query_capture tail [<num>]
follow [[fqdn /regex/] [ip /regex/ | grep /regex/]]
[[fqdn /regex/] [ip /regex/ | grep /regex/]] [after [date] time]
[before [date] time]
```

You can specify the command with or without arguments. If you use the `show query_capture` command without any arguments, it displays queries from the current capture file. If you use the `show query_capture` command with `follow`, `tail`, `before`, `after`, `fqdn`, and `ip` arguments, you can view queries for a specific data and time range, queries sent from the client FQDNs, and IP addresses.

**Note:** A capture file for logging DNS queries and responses is compressed every 10 minutes or when it reaches 100 MB in size, whichever comes sooner. A new current file is created when a capture file is compressed. If you are running the `show query_capture` command with `follow` or `tail` when a new capture file is created, the CLI console may return an error indicating that `captured-dns-xxxxxx` has become inaccessible: No such file or directory. In these situations, you must execute the CLI command again.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tail &lt;num&gt;</td>
<td>Shows the last <code>num</code> lines from the capture file. If you do not specify a number, only the last ten lines are displayed.</td>
</tr>
<tr>
<td>follow</td>
<td>Displays continuously the lines till the end of the capture file as lines are appended. In addition, you can use 'follow' with '/regex/' to search for FQDNs, IP addresses, and regular expressions.</td>
</tr>
<tr>
<td>before [date] time</td>
<td>Displays captured DNS queries before the specified date time starting with the oldest saved log file. Make sure that you specify the date (optional for today's date) in the day-month-year format (example: 25-oct-2014), and time in hour:minutes:seconds format (example: 10:09:30).</td>
</tr>
<tr>
<td>after [date] time</td>
<td>Displays captured DNS queries after the specified date time until the end of the current log file. The CLI console will not display DNS queries when you specify the current date and time or a future date and time. Make sure that you specify the date (optional for today's date) in the day-month-year format (example: 02-aug-2014), and time in hour:minutes:seconds format (example: 10:09:30).</td>
</tr>
</tbody>
</table>
CLI Commands

Examples

Infoblox > show query_capture

09-Aug-2014 09:55:50.872 client 10.35.1.136#57722: query: aaaa80.1852a_95.com IN AAAA + (10.35.3.96)
09-Aug-2014 09:55:50.872 client 10.35.1.136#57722: query: aaaa81.1852a_95.com IN AAAA + (10.35.3.96)
09-Aug-2014 09:55:50.872 client 10.35.1.136#57722: query: aaaa79.1852a_95.com IN AAAA + (10.35.3.96)
09-Aug-2014 09:56:07.322 client 10.35.1.136#57722: query: aaaa82.1852a_95.com IN AAAA + (10.35.3.96)
09-Aug-2014 09:56:07.322 client 10.35.1.136#57722: query: aaaa84.1852a_95.com IN AAAA + (10.35.3.96)
09-Aug-2014 09:56:07.322 client 10.35.1.136#57722: query: aaaa85.1852a_95.com IN AAAA + (10.35.3.96)
09-Aug-2014 09:56:07.323 client 10.35.1.136#57722: query: aaaa86.1852a_95.com IN AAAA + (10.35.3.96)
09-Aug-2014 09:56:07.323 client 10.35.1.136#57722: query: aaaa87.1852a_95.com IN AAAA + (10.35.3.96)
09-Aug-2014 09:56:07.323 client 10.35.1.136#57722: query: aaaa88.1852a_95.com IN AAAA + (10.35.3.96)

Infoblox > show query_capture before 09-Aug-2014 05:00:00

Note that the filtering options require significant CPU resources, which may affect service performance. Infoblox recommends that you use this command only when necessary.

09-Aug-2014 09:55:50.872 client 10.35.1.136#57722: query: aaaa80.1852a_95.com IN AAAA + (10.35.3.96)
09-Aug-2014 09:55:50.872 client 10.35.1.136#57722: query: aaaa81.1852a_95.com IN AAAA + (10.35.3.96)
09-Aug-2014 09:55:50.872 client 10.35.1.136#57722: query: aaaa79.1852a_95.com IN AAAA + (10.35.3.96)
09-Aug-2014 09:56:07.322 client 10.35.1.136#57722: query: aaaa82.1852a_95.com IN AAAA + (10.35.3.96)
09-Aug-2014 09:56:07.322 client 10.35.1.136#57722: query: aaaa84.1852a_95.com IN AAAA + (10.35.3.96)
09-Aug-2014 09:56:07.322 client 10.35.1.136#57722: query: aaaa85.1852a_95.com IN AAAA + (10.35.3.96)
09-Aug-2014 09:56:07.323 client 10.35.1.136#57722: query: aaaa86.1852a_95.com IN AAAA + (10.35.3.96)
09-Aug-2014 09:56:07.323 client 10.35.1.136#57722: query: aaaa87.1852a_95.com IN AAAA + (10.35.3.96)
09-Aug-2014 09:56:07.323 client 10.35.1.136#57722: query: aaaa88.1852a_95.com IN AAAA + (10.35.3.96)
show query_capture

05-Aug-2014 13:31:29.057 client 10.35.112.5#40027: query: mx82.2000a_42.com IN MX +
(10.35.3.148)

Infoblox > show query_capture after 11-Aug-2014 09:00:00

Note that the filtering options require significant CPU resources, which may affect service performance. Infoblox recommends that you use this command only when necessary.

18-Aug-2014 05:44:22.589 client 10.35.3.148#36662: query: 1.0.0.127.in-addr.arpa IN PTR +E (10.35.3.148)
18-Aug-2014 05:45:22.470 client 10.35.3.148#56373: query: 1.0.0.127.in-addr.arpa IN PTR +E (10.35.3.148)
20-Aug-2014 06:45:25.330 client 10.35.3.148#35366: query: hal.2000a_1.com IN SOA +ED
(127.0.0.1)

Infoblox > show query_capture fqdn /2000a_1.com/

Note that the filtering options require significant CPU resources, which may affect service performance. Infoblox recommends that you use this command only when necessary.

20-Aug-2014 06:45:22.352 client 10.35.3.148#35366: query: hal.2000a_1.com IN SOA +ED
(127.0.0.1)
20-Aug-2014 06:45:22.352 client 10.35.3.148#35366: query: 2000a_1.com IN SOA +ED
(127.0.0.1)
20-Aug-2014 06:45:25.330 client 10.35.3.148#35366: query: hal.2000a_1.com IN SOA +ED
(127.0.0.1)

Infoblox > show query_capture fqdn /2000a_1.com/ grep /SOA/

Note that the filtering options require significant CPU resources, which may affect service performance. Infoblox recommends that you use this command only when necessary.

20-Aug-2014 07:54:29.457 client 10.35.3.148#35366: query: hal.2000a_1.com IN SOA +ED
(127.0.0.1)
20-Aug-2014 07:54:29.457 client 10.35.3.148#35366: query: 2000a_1.com IN SOA +ED
(127.0.0.1)
admin.infoblox.com. 503 10800 3600 2419200 900;

Infoblox > show query_capture after 18-Aug-2014 05:05:05 before 18-Aug-2014 06:05:05

Note that the filtering options require significant CPU resources, which may affect service performance. Infoblox recommends that you use this command only when necessary.
18-Aug-2014 05:05:22.342 client 10.35.3.148#50669: query: 1.0.0.127.in-addr.arpa IN PTR +E (10.35.3.148)
18-Aug-2014 05:06:22.402 client 10.35.3.148#35534: query: 1.0.0.127.in-addr.arpa IN PTR +E (10.35.3.148)
18-Aug-2014 05:07:22.338 client 10.35.3.148#43846: query: 1.0.0.127.in-addr.arpa IN PTR +E (10.35.3.148)
18-Aug-2014 05:08:22.498 client 10.35.3.148#50606: query: 1.0.0.127.in-addr.arpa IN PTR +E (10.35.3.148)
18-Aug-2014 05:53:22.359 client 10.35.3.148#56078: query: 1.0.0.127.in-addr.arpa IN PTR +E (10.35.3.148)
18-Aug-2014 05:54:22.281 client 10.35.3.148#60212: query: 1.0.0.127.in-addr.arpa IN PTR +E (10.35.3.148)
18-Aug-2014 05:55:22.368 client 10.35.3.148#35600: query: 1.0.0.127.in-addr.arpa IN PTR +E (10.35.3.148)
**show recursion_query_timeout**

The `show recursion_query_timeout` command displays the maximum time allowed for a recursive query to wait for a response before timing out.

You can use the `set recursion_query_timeout` command to configure the recursion query timeout value. For information, see `set recursion_query_timeout` on page 98. Setting the timeout value to 0 returns to the default timeout behavior, which is to wait at least 30 seconds and up to 40 seconds before timing out.

**Note:** When you enable this on an HA pair, ensure that you run the command and set the same values on both nodes of the HA pair. No service restart is required when you use this command.

These commands are designed to mitigate phantom domain attacks. For more information about this, refer to the *Infoblox NIOS Administrator Guide*.

**Syntax**

```
show recursion_query_timeout
```

**Example**

```
Infoblox > show recursion_query_timeout
Recursion query timeout (in seconds): Default (30)
```
### show remote_console

The `show remote_console` command displays remote console access settings. This command allows you to see if remote console access is enabled without accessing the GUI. You can set this option at the member level and the Grid level. For information on how to change your `remote_console`, see `set remote_console` on page 99.

#### Syntax

```
show remote_console
```

This command has no arguments.

#### Example

```
Infoblox > show remote_console
current remote console access settings:
Remote console access enabled (Grid-level):   true
```
show reporting_cluster_maintenance_mode

The `show reporting_cluster_maintenance_mode` command displays the cluster maintenance mode settings. For information about how to enable the reporting clustering mode, see `set reporting_cluster_maintenance_mode` on page 101.

**Syntax**

```
show reporting_cluster_maintenance_mode
```

This command has no arguments.

**Example**

```
Maintenance Mode > show reporting_cluster_maintenance_mode
Reporting cluster maintenance mode is enabled
```
**show routes**

The `show routes` command displays the current IPv4 and IPv6 routing information on the NIOS appliance and organizes the information according to the interface. This command is a valuable diagnostic tool for connectivity issues.

**Syntax**

```
show routes
```

This command has no arguments.

**Example**

In the following example, `default` specifies the direct connection to the interface and the static routes are represented (in this example) in bold. You specify static routes by manually entering them through the GUI.

```
Infoblox > show routes
From LAN:
10.34.33.0/24 dev eth1  scope link
default via 10.34.33.1 dev eth1

From LAN2:
10.1.1.0/24 dev eth3  scope link
default via 10.1.1.1 dev eth3

From IPv4 main route table:
10.34.33.0/24 dev eth1  proto kernel  scope link  src 10.34.33.11
10.1.1.0/24 dev eth3  proto kernel  scope link  src 10.1.1.35
default via 10.34.33.1 dev eth1

From IPv6 main route table:
fe80::/64 dev eth1  metric 256  expires 21257697sec mtu 1500 advmss 1440 metric10 4294967295
fe80::/64 dev eth3  metric 256  expires 21334065sec mtu 1500 advmss 1440 metric10 4294967295
ff00::/8 dev eth1  metric 256  expires 21257697sec mtu 1500 advmss 1440 metric10 4294967295
ff00::/8 dev eth3  metric 256  expires 21334065sec mtu 1500 advmss 1440 metric10 4294967295
default via fe80::204:96ff:fe1d:1980 dev eth1  proto kernel  metric 1024  expires 1661sec mtu 1500 advmss 1440 metric10 64
default via fe80::204:96ff:fe1d:1980 dev eth3  proto kernel  metric 1024  expires 1661sec mtu 1500 advmss 1440 metric10 64
unreachable default dev lo  proto none  metric -1  error -101 metric10 255
```
show scheduled

Use the `show scheduled` command to view the number of times per hour the appliance checks if the services need a restart when the scheduling task feature is enabled. The appliance restarts services only when the execution of a scheduled task requires a service restart.

Use the `set scheduled` command to configure the value. You can set the value from 0 to 60, and the default value is 60. A value of 0 turns off the restart feature.

**Syntax**

```
show scheduled task restarts
```

This command has no argument.

**Example**

```
Infoblox > show scheduled task restarts
Number of restarts per hour: 4
```
show security

The `show security` command shows the current security settings and whether access to the NIOS appliance through the GUI is restricted. For more information, see `set security` on page 105.

Syntax

```
show security
```

This command has no arguments.

Example

```
Infoblox > show security
current security settings:
  Access restricted: false
```
show session_timeout

The `show session_timeout` command shows how long a session remains open when there is no user activity. For more information, see `set session_timeout` on page 106.

Syntax

```
    show session_timeout
```

This command has no arguments.

Example

```
Infoblox > show session_timeout
Current GUI/CLI timeout is 31536000 seconds (8760:00:00)
```
show smartnic

The `show smartnic` command shows whether monitor mode for the Threat Protection service and DNS Cache Acceleration feature on an IB-4030 appliance is on or off. When on, monitor mode for the Threat Protection service is enabled and the appliance logs DNS packets (instead of dropping them) that would have been blocked by threat protection rules. This information is recorded in the audit log.

For information on how to disable monitor mode for the Threat Protection service, see `set smartnic monitor-mode` on page 107.

**Syntax**

```
show smartnic
```

This command has no arguments.

**Example**

```
Infoblox > show smartnic
Firmware version: 3.8.1 Jul 21, 2014,
Log level: 6
Failed cores: None
Threat Protection: Enabled
Threat Protection monitor mode: Disabled
Threat Protection event stats: CRITICAL=0 MAJOR=0 WARNING=0 INFORMATIONAL=575349
```
show snmp

The `show snmp` command shows information about the SNMP object that you specify. You can enter the SNMP object name or OID. This command is similar to the SNMP “get” operation. You can use the optional v3 command to get the information using SNMPv3. For information about SNMP, see Chapter 6, Monitoring with SNMP in the Infoblox NIOS Administrator Guide.

Use the `set snmptrap` command to send SNMP traps to management systems you specify.

**Syntax**

```
show snmp variable {name of an SNMP variable, in dotted or symbolic format} v3
{snmpuser}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name of an SNMP variable</td>
<td>The name or OID (object ID) of the SNMP object you want to retrieve. For example, you can enter <code>sysName.0</code> or <code>1.3.6.1.4.1.7779.3.1.1.2.1.1.0</code>.</td>
</tr>
<tr>
<td>snmpuser</td>
<td>The user name of the SNMPv3 user account. This is optional. If you do not provide a user name, the appliance uses the first SNMPv3 user on the list.</td>
</tr>
</tbody>
</table>

**Examples**

**Displaying the host name**

```
Infoblox > show snmp variable sysName.0
SNMPv2-MIB::sysName.0 = STRING: ib-10-34-61-253.infoblox.com
```

**Displaying the CPU temperature**

```
Infoblox > show snmp variable .1.3.6.1.4.1.7779.3.1.1.2.1.1.0
IB-PLATFORMONE-MIB::ibCPUTemperature.0 = STRING: +40.75 C
```

**Displaying the host name using SNMPv3**

```
Infoblox > show snmp variable sysName.0 v3 SNMPv3User1
SNMPv2-MIB::sysName.0 = STRING: ib-10-34-10.42.infoblox.com
```
**show ssl_tls_ciphers**

The `show ssl_tls_ciphers` command shows the SSL/TLS ciphers that are enabled for the NIOS appliance. You can use the `set ssl_tls_ciphers` command to enable or disable the cipher suites. For information, see `set ssl_tls_ciphers` on page 109.

**Syntax**

```
show ssl_tls_ciphers
```

This command has no arguments.

**Example**

```
Infoblox > show ssl_tls_ciphers
1. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 enabled
2. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 enabled
3. TLS_DHE_RSA_WITH_AES_128_CBC_SHA enabled
4. TLS_DHE_RSA_WITH_AES_256_CBC_SHA enabled
5. TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 enabled
6. TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 enabled
7. TLS_RSA_WITH_AES_128_GCM_SHA256 enabled
8. TLS_RSA_WITH_AES_128_CBC_SHA enabled
9. TLS_RSA_WITH_AES_128_CBC_SHA256 enabled
10. TLS_RSA_WITH_3DES_EDE_CBC_SHA disabled
11. TLS_RSA_WITH_AES_256_GCM_SHA384 enabled
12. TLS_RSA_WITH_AES_256_CBC_SHA enabled
13. TLS_RSA_WITH_AES_256_CBC_SHA256 enabled
    TLS_DHE_DSS_WITH_AES_256_CBC_SHA disabled
    TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA disabled
    TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA disabled
    TLS_DH_RSA_WITH_AES_128_CBC_SHA disabled
    TLS_RSA_WITH_RC4_128_SHA disabled
    TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 disabled
    TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 disabled
    TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 disabled
    TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 disabled
```
show ssl_tls_protocols

The show ssl_tls_protocols command shows the SSL/TLS protocols that are enabled for the NIOS appliance. You can use the set ssl_tls_protocols command to enable or disable SSL/TLS protocols. For information, see set ssl_tls_protocols on page 111.

Syntax

    show ssl_tls_protocols

This command has no arguments.

Example

Displaying the enabled SSL/TLS protocols

    Infoblox > show ssl_tls_protocols
    TLSv1.0 TLSv1.1 TLSv1.2
show ssl_tls_settings

The **show ssl_tls_settings** command shows whether SSL/TLS settings are set to the default or override mode. You can use the **set ssl_tls_settings** command to change the SSL/TLS settings. For information, see **set ssl_tls_settings** on page 112.

**Syntax**

```
show ssl_tls_settings
```

This command has no arguments.

**Example**

```
Infoblox > show ssl_tls_settings
SSL/TLS settings: default.
Use 'ssl_tls_protocols' and 'ssl_tls_ciphers' to see current settings.
```
**show static_routes**

Use the `show static_routes` command to display the current static route configuration on your appliance. To configure static routes, use the `set static_route` command.

You can also use the `show routes` command to view the current IPv4 and IPv6 routing information on the NIOS appliance and how the information is organized according to the interfaces.

**Syntax**

```
show static_routes [v4|v6]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>v4</td>
<td>v6</td>
</tr>
</tbody>
</table>

**Examples**

**Displaying IPv4 Static Routes**

```
Infoblox > show static_routes v4
Position | Destination | Gateway
1 | 1.1.1.1/32 | 192.168.1.11
2 | 1.1.1.2/32 | 192.168.1.12
3 | 1.1.1.11/32 | 192.168.1.21
4 | 1.1.1.3/32 | 192.168.1.13
5 | 1.1.1.4/32 | 192.168.1.14
6 | 1.1.1.5/32 | 192.168.1.15
7 | 1.1.1.6/32 | 192.168.1.16
8 | 1.1.1.7/32 | 192.168.1.17
9 | 1.1.1.8/32 | 192.168.1.18
10 | 1.1.1.9/32 | 192.168.1.19
11 | 1.1.1.10/32 | 192.168.1.20
```

**Displaying IPv6 Static Routes**

```
Infoblox > show static_routes v6
Position | Destination | Gateway
```
show status

The `show status` command shows the Grid and HA status. You can use this command to gather information about the current state of a Grid.

Syntax

```
show status
```

This command has no arguments.

Example

**Status of Grid Master**

```
Infoblox > show status
Grid Status: ID Grid Master
HA Status: Not Configured
```

**Status of HA member**

```
Infoblox > show status
Grid Status: ID Grid Member
HA Status: Active
Hostname: member1.infoblox.com
Grid Master IP: 10.35.113.15
```

**Note:** If the Grid member uses IPv6 communication protocol to join a dual mode Grid, then IPv6 address of the Grid Master is displayed.
show support_access

The `show support_access` command shows whether the support_access function is enabled. By default, the support_access function is disabled. For more information on the support_access function, see `set support_access` on page 115.

Syntax

    show support_access

This command has no arguments.

Example

    Infoblox > show support_access
    current support access settings:
        Support access enabled (Grid-level): true
show tech-support

The `show tech-support` command displays output for all show commands. It is a labor saving command that allows you to view the information provided by all the `show` commands. Using the `log` argument allows you to save the output to a log file that is included in the support bundle.

**Syntax**

```
show tech-support [log]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log</td>
<td>Saves the output to a log file that is included in the support bundle.</td>
</tr>
</tbody>
</table>

**Example**

```
Infoblox > show tech-support
Current date and time: Thu Aug 24 14:06:01 EDT 2008
Up time : 19:29
Version : 4.3r2
Hardware ID : 4dcef037e91a403fe05e10ecd241

License Type : Grid
Expiration Date : 12/20/2009
License String : GgAAADJj2t2zLRv8GJ7/Ua4wkRcbnS6Vp5V5RxizS

License Type : DNS
Expiration Date : Permanent
License String : EQAAADNj3cWUB/FCZaaFa8JoT5ev

License Type : DHCP
Expiration Date : Permanent

License Type : Grid Maintenance
Expiration Date : 12/20/2009
License String : HAAAADxo18rNWEmKtG6ndKsJpRYqS1r4xJU1n6C6bE=

License Type : NIOS Maintenance
Expiration Date : 12/20/2006
License String : HAAAADlkwcrmRfgfJLXaLsJpRYqS1r4xJUiiXWseE=

Version : 4.3r2
SN : 000100e081277a69
REVERT version is: N/A
No upgrade history found for this box.
```
show thresholdtrap

The `show thresholdtrap` command displays the trigger and reset values of the SNMP trap for CPU usage. The CPU usage trap is disabled by default, and the trigger value is set at 100 and reset value at 0. For information about how to configure the trigger and reset values, see `set thresholdtrap` on page 121.

Syntax

show thresholdtrap {type}

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>The type of threshold trap. Enter <code>CpuUsage</code> to display the trigger and reset values of the CPU usage trap. The trap is disabled by default, and the trigger value is set at 100 and reset value at 0.</td>
</tr>
</tbody>
</table>

Example

Infoblox > `show thresholdtrap CpuUsage`
Trap type: `CpuUsage`
trigger: 80
reset: 71
**show traffic_capture_status**

The `show traffic_capture_status` command displays the status of traffic capture on the NIOS appliance. You can use the `set traffic_capture` command to start or stop the traffic capture on a NIOS appliance. For more information, see `set traffic_capture` on page 123.

**Syntax**

```
  show traffic_capture_status
```

This command has no arguments.

**Example**

```
Infoblox > show traffic_capture_status
Traffic capture is stopped.
3277072 bytes captured.
```
show txn_trace

The `show txn_trace` command displays whether database transaction logging is enabled or disabled for the NIOS appliance.

**Syntax**

```
show txn_trace
```

This command has no arguments.

**Example**

```
Infoblox > show txn_trace
txn_trace set to on

Infoblox > show txn_trace
txn_trace set to off
```
show upgrade_compatible

The `show upgrade_compatible` command shows whether your Grid can be upgraded to a later NIOS release. Use this command to check if a Grid is compatible with a later NIOS release before you upgrade. For information about appliances that are compatible with the release, refer to the latest release notes.

Syntax

```
show upgrade_compatible [major-number.minor-number]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>major-number.minor-number</td>
<td>The NIOS release to which you want to upgrade your Grid. You must enter the release number in #.# format.</td>
</tr>
</tbody>
</table>

Examples

```
Infoblox > show upgrade_compatible 6.0
The Grid is compatible with release 6.0.

Infoblox > show upgrade_compatible 5.1r3
The release number format must be major number.minor number, such as 6.0.

Infoblox > show upgrade_compatible 6.0
Hardware Type(model)  Node IP        Status
NA                  10.35.1.213   bloxTools Enabled
IB-1000             10.35.1.213   Not Compatible
IB-RSP2(250)        10.35.1.28    Require Riverbed version >= 5.5.3
```

The Grid is not compatible with release 6.0.
show upgrade_history

The `show upgrade_history` command displays the upgrade history of the NIOS appliance, showing how many times the appliance has been upgraded and the versions for each upgrade. It also shows the revert version—the version that you can go back to—which is the version of the software the appliance was (last) running prior to the most recent upgrade.

Syntax

```
show upgrade_history
```

This command has no arguments.

Example

```
Infoblox > show upgrade_history
REVERT version is: 4.0r1
[2006/08/14 19:05:48] Upgraded to: 4.0r2-4-06070517
```
show uptime

The `show uptime` command displays the uptime (hours and minutes) of the NIOS appliance since the last reboot. In a test environment, this command can be used as a metric. In a production environment, this command is of less use since the appliance remains continually functional.

**Syntax**

```
show uptime
```

This command has no arguments.

**Example**

```
Infoblox > show uptime
Up time : 19:33
```
show version

The `show version` command displays the current version of the NIOS software that is installed on the NIOS appliance. You can use this information when performing an upgrade to determine what version of the software to upgrade to.

Syntax

```
show version
```

This command has no arguments.

Example

```
Infoblox > show version
Version : 4.0r2
SN      : 000100e081277a69
Hotfix  : N/A
```
**show vpn_cert_dates**

Use the `show vpn_cert_dates` command to display the start and end dates of the Infoblox appliance certificate. This information is also included in the Support Bundle.

**Syntax**

```
show vpn_cert_dates
```

This command has no arguments.

**Example**

The following is an example of the command:

```
Infoblox > show vpn_cert_dates
Start Date=Dec 13 11:00:00 2003 GMT
End Date=May 20 11:00:00 2019 GMT
```
show wins_forwarding

Use the show wins_forwarding command to display the current configuration for WINS packet forwarding for the Grid or a specific Grid member.

For information about how to configure WINS packet forwarding to Microsoft servers, see set wins_forwarding on page 126.

Syntax

    show wins_forwarding

This command has no arguments.

Examples

Execute the command on the Grid member that inherited the Grid settings

    Infoblox > show wins_forwarding
    Grid level WINS forwarding: enabled
    Grid level WINS default server IP: 10.35.0.123

    Member level WINS forwarding: Use grid setting

Execute the command on the Grid member that overrode the Grid settings

    Infoblox > show wins_forwarding
    Grid level WINS forwarding: Enabled
    Grid level WINS default server IP: 10.35.0.123
    Member level output interface: LAN2

    Member level WINS forwarding: Override grid setting
    Member level forwarding: Enabled
    Member level WINS server IP: 10.35.0.321
    Member level output interface: MGMT

Execute the command on the Grid member that overrode the Grid settings and packet forwarding was disabled

    Infoblox > show wins_forwarding
    Grid level WINS forwarding: Enabled
    Grid level WINS default server IP: 10.35.0.123
    Member level output interface: LAN

    Member level WINS forwarding: Override grid setting
    Member level forwarding: Disabled
shutdown

The `shutdown` command halts the NIOS appliance. The appliance is designed to operate continuously. However, if you want to halt the appliance you can do so with the `shutdown` command.

**Note:** Once you shutdown the appliance using this command, you must manually bring it back up.

**Syntax**

```
shutdown
```

This command has no arguments.

**Example**

The following example uses the `shutdown` command.

```
Infoblox > shutdown
SHUT DOWN THE SYSTEM? [y or n] y
```

**Note:** On a Riverbed Services Platform (RSP), the `shutdown` command restarts the Riverbed device instead of halting it. Infoblox recommends that you use the Riverbed `no rsp enable` command to perform a shutdown.
**snmpget**

Fetches the information from a discovered device’s SNMP data. You specify the IP address or hostname and the SNMP Object ID (also often referred to as an SNMP variable) or its dotted numeric equivalent as defined in the device MIB.

**Syntax**

```
snmpget <hostname or IP address> <SNMP OID>
```

**Example**

The following example uses the `snmpget` command, specifying the IP address of a device discovered by NIOS, along with the standard Object ID `sysName.0` to look up the hostname string for a device. You will need the community string or privacy key to fetch the information.

```
Infoblox > snmpget 172.22.53.5 sysName.0
Enter SNMP Version (1, 2c or 3): 2c
Enter SNMP community string: *******
Created directory: /var/lib/net-snmp/cert_indexes
Created directory: /var/lib/net-snmp/mib_indexes
SNMPv2-MIB::sysName.0 = STRING: DEVsw08
```
**snmpwalk**

Obtain a tree of information from a network device, using automatic SNMP GETNEXT commands. In the NIOS administrative shell version of the `snmpwalk` command, you can specify the SNMP version, the community string, and the desired Root Object ID (OID).

**Syntax**

```
snmpget <hostname or IP address> <SNMP OID>
```

**Example**

The following example lists a partial output from querying the root Object ID for a Cisco Nexus 5K switch (this technique is also useful for looking up other Object IDs within a particular device):

```
Infoblox > snmpwalk 172.22.33.5 1.3
Enter SNMP Version (1, 2c or 3): 2c
Enter SNMP community string: ********
SNMPv2-MIB::sysDescr.0 = STRING: Cisco NX-OS(tm) n5000, Software (n5000-uk9), Version 5.1(3)N2(1b), RELEASE SOFTWARE Copyright (c) 2002-2011 by Cisco Systems, Inc. Device Manager Version 5.2(1), Compiled 8/31/2012 17:00:00
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.12.3.1.3.798
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (165293061) 19 days, 3:08:50.61
SNMPv2-MIB::sysContact.0 = STRING: who@where
SNMPv2-MIB::sysName.0 = STRING: DEVsw03
SNMPv2-MIB::sysLocation.0 = STRING: snmplocation
SNMPv2-MIB::sysServices.0 = INTEGER: 70
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (40) 0:00:00.40
SNMPv2-MIB::sysORID.1 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.2 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.3 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.5 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORDescr.1 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.2 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORDescr.3 = STRING: The SNMP Management Architecture MIB.
```
traceroute

The `traceroute` command displays information on the route IPv4/IPv6 packets. You can use this command to determine the path of an IPv4/IPv6 query. This command provides information on the path packets travel and the time it takes to reach the IPv4/IPv6 destination address.

Syntax

```
traceroute {hostname | ip_address} [ opt ]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>Fully qualified domain name</td>
</tr>
<tr>
<td>ip_address</td>
<td>Valid IPv4/IPv6 address of the host</td>
</tr>
<tr>
<td>opt</td>
<td>Can be any of the following:</td>
</tr>
<tr>
<td></td>
<td>• <code>numerical</code> (specifies to not interpret the IP address as a DNS name)</td>
</tr>
<tr>
<td></td>
<td>• <code>src_addr</code> (specifies the starting or “from” address)</td>
</tr>
<tr>
<td></td>
<td>• <code>ICMP</code> (specifies to use <code>ping</code>)</td>
</tr>
<tr>
<td></td>
<td>• <code>v6</code> (specifies IPv6 hostname)</td>
</tr>
</tbody>
</table>

Example

The following example shows you how to use the traceroute command.

```
Infoblox > traceroute 10.1.1.1
traceroute to 10.1.1.1 (10.1.1.1), 30 hops max, 40 byte packets
  1 10.1.1.5 (10.1.1.5)  1.951 ms  1.637 ms  1.734 ms
  2 10.1.1.1 (10.1.1.1)  0.248 ms  0.284 ms  0.239 ms
```