Infoblox Administrator Guide

NIOS 5.1
for Infoblox Core Network Services Appliances
# Preface

- Document Overview.................................................................................. 24
  - Documentation Conventions................................................................. 24
- What's New ............................................................................................... 26
- Related Documentation............................................................................. 27
- Customer Care .......................................................................................... 28
  - User Accounts......................................................................................... 28
  - Software Upgrades................................................................................ 28
  - Technical Support................................................................................... 28

# Part 1 Appliance GUI

## Chapter 1 Infoblox Grid Manager ............................................................ 31

- Management System Requirements......................................................... 33
  - Supported Browsers............................................................................... 33
  - Browser Limitations.............................................................................. 34
- About Grid Manager................................................................................ 35
  - Admin Permissions for Grid Manager.................................................... 35
  - Logging in to the GUI........................................................................... 35
- Setting Login Options............................................................................. 36
  - Specifying the Grid Name and Hostname.............................................. 36
  - Managing Certificates.......................................................................... 36
  - Creating a Login Banner....................................................................... 36
  - Changing the Password and Email Address......................................... 36
  - Specifying the Table Size.................................................................... 37
  - Setting the Browser Time Zone............................................................. 37
- SSL (Secure Sockets Layer) Protocol....................................................... 38
- Managing Certificates............................................................................ 39
  - Generating Self-Signed Certificates....................................................... 39
  - Generating Certificate Signing Requests............................................. 40
  - Uploading Certificates......................................................................... 40
  - Downloading Certificates.................................................................... 41
- About the Grid Manager Interface........................................................ 42
  - System Messages.................................................................................. 42
  - Breadcrumbs Navigation........................................................................ 43
  - Global Search......................................................................................... 43
  - Finder Panel.......................................................................................... 43
  - Toolbar Panel........................................................................................ 43
  - Help Panel............................................................................................. 43
  - Wizards and Editors.............................................................................. 43
  - Tooltips................................................................................................. 43
  - Customizing Tables............................................................................... 44
  - Selecting Objects in Tables................................................................... 44
- Finding and Restoring Data.................................................................... 46
  - Using the Finder Panel.......................................................................... 46
  - Using Filters.......................................................................................... 49
  - Using Global Search............................................................................... 49
  - Using the Go To Function..................................................................... 51
- About Long Running Tasks ..................................................................... 52
  - Running Tasks in the Background........................................................ 52
  - Monitoring Long Running Tasks.......................................................... 53

# Documentation Conventions

- Technical Support.................................................................................... 28
- User Accounts.......................................................................................... 28
Chapter 2 The Dashboard ................................................................. 55

About the Dashboard ........................................................................ 56
  Grid Status .................................................................................... 57
  Member Status (System Status) ....................................................... 58
  DNS Statistics ............................................................................... 59
  Ranges Over Threshold .................................................................. 60
  Failover Associations Status ........................................................... 60
  DHCP Statistics ............................................................................ 60
  Network Statistics .......................................................................... 61
  Networks Over Threshold ............................................................... 62
  Discovery Status ........................................................................... 62
  My Commands ................................................................................ 63
  DDNS Statistics ........................................................................... 63
  System Activity Monitor ................................................................. 63
  File Distribution Statistics ............................................................. 64
  Active WebUI Users ....................................................................... 64
  Microsoft Servers Status Widget .................................................... 65

Chapter 3 Smart Folders ................................................................. 67

About Smart Folders .......................................................................... 68
  Global Smart Folders ...................................................................... 69
  My Smart Folders ........................................................................... 69
Creating Smart Folders .................................................................... 70
Viewing and Modifying Data in Smart Folders ................................ 71
Modifying Smart Folders .................................................................. 72
Deleting Smart Folders .................................................................... 72
Saving a Copy of a Smart Folder ....................................................... 72
Printing and Exporting Data in Smart Folders .................................. 73

PART 2 APPLIANCE ADMINISTRATION

Chapter 4 Managing Administrators ............................................... 77

About Admin Accounts ..................................................................... 79
About Admin Groups ........................................................................ 81
  Creating Superuser Admin Groups ............................................... 82
  Creating Limited-Access Admin Groups ........................................ 82
About Admin Roles ........................................................................... 84
  Creating Admin Roles ................................................................... 84
Managing Admin Groups and Admin Roles ..................................... 85
  Modifying Admin Groups and Roles ............................................. 85
  Deleting Admin Groups and Roles ................................................. 86
Viewing Admin Groups .................................................................... 86
Viewing Admin Roles ....................................................................... 86
Viewing Admin Group Assignments ................................................ 86
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Administrative Permissions</td>
<td>87</td>
</tr>
<tr>
<td>Defining Global Permissions</td>
<td>88</td>
</tr>
<tr>
<td>Defining Object Permissions</td>
<td>88</td>
</tr>
<tr>
<td>Applying Permissions and Managing Overlaps</td>
<td>91</td>
</tr>
<tr>
<td>Managing Permissions</td>
<td>93</td>
</tr>
<tr>
<td>Authenticating Administrators</td>
<td>95</td>
</tr>
<tr>
<td>Creating Local Admins</td>
<td>95</td>
</tr>
<tr>
<td>Modifying and Deleting Admin Accounts</td>
<td>96</td>
</tr>
<tr>
<td>About Remote Admins</td>
<td>97</td>
</tr>
<tr>
<td>Authenticating Using RADIUS</td>
<td>99</td>
</tr>
<tr>
<td>Remote RADIUS Authentication</td>
<td>100</td>
</tr>
<tr>
<td>Configuring a RADIUS Authentication Server Group</td>
<td>100</td>
</tr>
<tr>
<td>Managing the RADIUS Server List</td>
<td>102</td>
</tr>
<tr>
<td>Disabling RADIUS Servers on NIOS</td>
<td>102</td>
</tr>
<tr>
<td>Configuring Remote RADIUS Servers</td>
<td>102</td>
</tr>
<tr>
<td>Configuring Admin Groups on the Remote RADIUS Server</td>
<td>103</td>
</tr>
<tr>
<td>Configuring Remote Admin Accounts on the Remote RADIUS Server</td>
<td>103</td>
</tr>
<tr>
<td>Authorization Groups Using RADIUS</td>
<td>103</td>
</tr>
<tr>
<td>Accounting Activities Using RADIUS</td>
<td>103</td>
</tr>
<tr>
<td>Authenticating Admin Accounts Using Active Directory</td>
<td>104</td>
</tr>
<tr>
<td>Admin Authentication Using Active Directory</td>
<td>105</td>
</tr>
<tr>
<td>Configuring an Active Directory Authentication Service Group</td>
<td>105</td>
</tr>
<tr>
<td>Managing the Domain Controller List</td>
<td>106</td>
</tr>
<tr>
<td>Disabling Domain Controllers</td>
<td>106</td>
</tr>
<tr>
<td>Defining the Authentication Policy</td>
<td>107</td>
</tr>
<tr>
<td>Configuring a List of Authentication Methods</td>
<td>107</td>
</tr>
<tr>
<td>Configuring a List of Remote Admin Groups</td>
<td>107</td>
</tr>
<tr>
<td>Changing Password Length Requirements</td>
<td>108</td>
</tr>
<tr>
<td>Notifying Administrators</td>
<td>109</td>
</tr>
<tr>
<td>Administrative Permissions for Common Tasks</td>
<td>110</td>
</tr>
<tr>
<td>Administrative Permission for the Grid</td>
<td>111</td>
</tr>
<tr>
<td>Administrative Permissions for Grid Members</td>
<td>111</td>
</tr>
<tr>
<td>Administrative Permissions for Network Discovery</td>
<td>112</td>
</tr>
<tr>
<td>Administrative Permissions for Scheduling Tasks</td>
<td>113</td>
</tr>
<tr>
<td>Administrative Permissions for Microsoft Servers</td>
<td>114</td>
</tr>
<tr>
<td>Administrative Permissions for IPAM Resources</td>
<td>115</td>
</tr>
<tr>
<td>Administrative Permissions for IPv4 and IPv6 Networks</td>
<td>115</td>
</tr>
<tr>
<td>Administrative Permissions for Hosts</td>
<td>115</td>
</tr>
<tr>
<td>Administrative Permissions for DNS Resources</td>
<td>116</td>
</tr>
<tr>
<td>Administrative Permissions for DNS Views</td>
<td>117</td>
</tr>
<tr>
<td>Administrative Permissions for Zones</td>
<td>118</td>
</tr>
<tr>
<td>Administrative Permissions for Resource Records</td>
<td>119</td>
</tr>
<tr>
<td>Administrative Permissions for Shared Record Groups</td>
<td>120</td>
</tr>
<tr>
<td>Administrative Permissions for DHCP Resources</td>
<td>121</td>
</tr>
<tr>
<td>Administrative Permissions for Network Views</td>
<td>122</td>
</tr>
<tr>
<td>Administrative Permissions for Networks and Shared Networks</td>
<td>123</td>
</tr>
<tr>
<td>Administrative Permissions for Fixed Addresses and Reservations</td>
<td>125</td>
</tr>
<tr>
<td>Administrative Permissions for DHCP Ranges</td>
<td>126</td>
</tr>
<tr>
<td>Administrative Permissions for DHCP Templates</td>
<td>127</td>
</tr>
<tr>
<td>Administrative Permissions for MAC Address Filters</td>
<td>128</td>
</tr>
<tr>
<td>Administrative Permissions for the DHCP Lease History</td>
<td>129</td>
</tr>
<tr>
<td>Administrative Permissions for File Distribution Services</td>
<td>130</td>
</tr>
</tbody>
</table>
# Chapter 5 Deploying a Grid

- Introduction to Grids ......................................................... 133
- Grid Communications ....................................................... 134
- NAT Groups ................................................................... 135
- Automatic Software Version Coordination ............................ 138
- Grid Bandwidth Considerations ........................................... 140
- About HA Pairs ................................................................ 142
  - Planning for an HA Pair .................................................... 142
  - About HA Failover ............................................................ 143
  - VRRP Advertisements ......................................................... 144
- Creating a Grid Master ......................................................... 145
  - Port Numbers for Grid Communication ............................... 147
  - Grid Setup Wizard ............................................................. 147
  - Creating an HA Grid Master ................................................. 147
  - Creating a Single Grid Master .............................................. 150
- Adding Grid Members ......................................................... 152
  - Adding a Single Member .................................................... 152
  - Adding an HA Member ....................................................... 153
- Joining Appliances to a Grid .................................................. 154
- Configuration Example: Configuring a Grid ......................... 155
  - Cable All Appliances to the Network and Turn On Power .... 157
  - Create the Grid Master ....................................................... 157
  - Define Members on the Grid Master ................................. 159
  - Join Appliances to the Grid ................................................ 160
  - Import DHCP Data ............................................................ 162
  - Import DNS Data ............................................................... 163
  - Using the Wizard ............................................................... 164
  - After Using the Wizard ....................................................... 166
- Managing a Grid ................................................................. 167
  - Changing Grid Properties .................................................. 167
  - Setting the MTU for VPN Tunnels ....................................... 168
  - Removing a Grid Member ................................................... 168
  - Promoting a Master Candidate ............................................ 168
- Grid Bandwidth Considerations ............................................ 140
- Automatic Software Version Coordination ............................ 138
- Grid Communications ......................................................... 134
- VRRP Advertisements ......................................................... 144

# Chapter 6 Deploying Independent Appliances

- Independent Deployment Overview ....................................... 171
  - System Manager GUI ......................................................... 174
- Deploying a Single Independent Appliance ............................ 175
  - Method 1 – Using the LCD ................................................... 176
  - Method 2 – Using the CLI .................................................... 176
  - Method 3 – Using the Infoblox NIOS Startup Wizard ............... 177
- Configuration Example: Deploying a NIOS Appliance as a Primary DNS Server ........................................... 179
  - Cable the Appliance to the Network and Turning On Power .... 180
  - Specifying Initial Network Settings .................................... 180
  - Specifying Appliance Settings ............................................. 180
  - Defining a NAT Address ..................................................... 181
  - Enabling Zone Transfers on the Legacy Name Server ............ 182
  - Importing Zone Data on an Independent Appliance .......... 182
  - Designating the New Primary on the Secondary Name Server (at the ISP Site) ........................................ 185
  - Configuring NAT and Policies on the Firewall ..................... 185
- Deploying an Independent HA Pair ......................................... 186
  - Using the Infoblox NIOS Startup Wizard to Configure an HA Pair ...................................................... 186
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Example: Configuring an HA Pair for Internal DNS and DHCP Services</td>
<td>189</td>
</tr>
<tr>
<td>Cabling Appliances to the Network and Turning On Power</td>
<td>190</td>
</tr>
<tr>
<td>Specifying Initial Network Settings</td>
<td>191</td>
</tr>
<tr>
<td>Specifying Appliance Settings</td>
<td>191</td>
</tr>
<tr>
<td>Enabling Zone Transfers</td>
<td>193</td>
</tr>
<tr>
<td>Importing Zone Data</td>
<td>193</td>
</tr>
<tr>
<td>Defining Networks, Reverse-Mapping Zones, DHCP Ranges, and Infoblox Hosts</td>
<td>193</td>
</tr>
<tr>
<td>Defining Multiple Forwarders</td>
<td>196</td>
</tr>
<tr>
<td>Enabling Recursion on External DNS Servers</td>
<td>196</td>
</tr>
<tr>
<td>Modifying the Firewall and Router Configurations</td>
<td>197</td>
</tr>
<tr>
<td>Enabling DHCP and Switching Service to the NIOS Appliance</td>
<td>198</td>
</tr>
<tr>
<td>Managing and Monitoring</td>
<td>198</td>
</tr>
<tr>
<td>Verifying the Deployment</td>
<td>199</td>
</tr>
<tr>
<td>Single Independent Appliance</td>
<td>199</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>199</td>
</tr>
<tr>
<td>Infoblox Tools for Migrating Data</td>
<td>200</td>
</tr>
<tr>
<td><strong>Chapter 7 Managing Appliance Operations</strong></td>
<td>201</td>
</tr>
<tr>
<td>Managing Time Settings</td>
<td>203</td>
</tr>
<tr>
<td>Changing Time and Date Settings</td>
<td>203</td>
</tr>
<tr>
<td>Changing Time Zone Settings</td>
<td>203</td>
</tr>
<tr>
<td>Monitoring Time Services</td>
<td>204</td>
</tr>
<tr>
<td>Using NTP for Time Settings</td>
<td>205</td>
</tr>
<tr>
<td>Authenticating NTP</td>
<td>206</td>
</tr>
<tr>
<td>NIOS Appliance as NTP Client</td>
<td>208</td>
</tr>
<tr>
<td>Configuring a Grid to Use NTP</td>
<td>209</td>
</tr>
<tr>
<td>Configuring Grid Members to Use NTP</td>
<td>211</td>
</tr>
<tr>
<td>NIOS Appliance as NTP Server</td>
<td>212</td>
</tr>
<tr>
<td>Configuring a NIOS Appliance as an NTP Server</td>
<td>213</td>
</tr>
<tr>
<td>Monitoring NTP</td>
<td>215</td>
</tr>
<tr>
<td>Scheduling Tasks</td>
<td>216</td>
</tr>
<tr>
<td>Scheduling Additions and Modifications</td>
<td>217</td>
</tr>
<tr>
<td>Scheduling Appliance Operations</td>
<td>217</td>
</tr>
<tr>
<td>Scheduling Deletions</td>
<td>217</td>
</tr>
<tr>
<td>Viewing Scheduled Tasks</td>
<td>218</td>
</tr>
<tr>
<td>Rescheduling Tasks</td>
<td>220</td>
</tr>
<tr>
<td>Guidelines for Upgrading, Backing Up, and Restoring the Database</td>
<td>221</td>
</tr>
<tr>
<td>About Extensible Attributes</td>
<td>222</td>
</tr>
<tr>
<td>Configuring Extensible Attributes</td>
<td>223</td>
</tr>
<tr>
<td>Using Extensible Attributes</td>
<td>225</td>
</tr>
<tr>
<td>Managing Security Operations</td>
<td>227</td>
</tr>
<tr>
<td>Enabling Support Access</td>
<td>227</td>
</tr>
<tr>
<td>Enabling Remote Console Access</td>
<td>227</td>
</tr>
<tr>
<td>Permanently Disabling Remote Console and Support Access</td>
<td>227</td>
</tr>
<tr>
<td>Restricting GUI/API Access</td>
<td>227</td>
</tr>
<tr>
<td>Enabling HTTP and GUI Redirections</td>
<td>227</td>
</tr>
<tr>
<td>Modifying the Session Timeout Setting</td>
<td>228</td>
</tr>
<tr>
<td>Disabling the LCD Input Buttons</td>
<td>228</td>
</tr>
<tr>
<td>Configuring Security Features</td>
<td>228</td>
</tr>
<tr>
<td>Enabling and Disabling GUI Redirection</td>
<td>229</td>
</tr>
<tr>
<td>Ethernet Port Usage</td>
<td>230</td>
</tr>
<tr>
<td>Modifying Ethernet Port Settings</td>
<td>235</td>
</tr>
</tbody>
</table>
Using the LAN2 Port ................................................................. 236
  About NIC Redundancy ...................................................... 237
  Configuring the LAN2 Port ................................................. 238
  Enabling DHCP on LAN2 .................................................... 238
  Enabling DNS on LAN2 ..................................................... 239
Using the MGMT Port ............................................................ 240
  Appliance Management ...................................................... 241
  Grid Communications ....................................................... 243
  DNS Services ................................................................. 245
Setting Static Routes ............................................................ 247
Enabling DNS Resolution ..................................................... 251
Managing Licenses ............................................................... 252
  Obtaining and Adding Licenses ........................................... 252
  Obtaining Temporary Licenses .......................................... 253
  Viewing Licenses ............................................................ 253
  Backing Up Licenses ....................................................... 253
  Removing Licenses .......................................................... 254
Shutting Down, Rebooting, and Resetting a NIOS Appliance ....... 255
  Rebooting a NIOS Appliance .............................................. 255
  Shutting Down a NIOS Appliance ....................................... 255
  Resetting a NIOS Appliance ............................................. 255
Managing the Disk Subsystem on the Infoblox-2000 and -2000-A ... 257
  About RAID 10 ............................................................... 257
  Evaluating the Status of the Disk Subsystem ......................... 258
  Appliance Front Panel ..................................................... 259
  Replacing a Failed Disk Drive .......................................... 259
  Disk Array Guidelines ..................................................... 260
Restarting Services ............................................................. 261
  Canceling a Scheduled Restart ........................................ 263

Chapter 8 File Distribution Services ........................................ 265

  About File Distribution .................................................... 266
  Configuring the TFTP Service ............................................ 267
  Configuring the FTP Service ............................................. 267
  Configuring the HTTP Service ........................................... 268
  Configuring Access Control Lists ..................................... 268
  Modifying Access Control Lists ....................................... 269
Managing File Distribution Services ....................................... 270
  Starting and Stopping File Distribution Services .................. 270
  Monitoring File Distribution Services ................................ 270
Managing Files and Directories ............................................. 271
  Configuring File Distribution Storage Settings ...................... 271
  Adding Directories ......................................................... 271
  Modifying Directories .................................................... 271
  Uploading Files ............................................................ 272
  Viewing Directories ....................................................... 272
Chapter 9 Managing NIOS Software and Configuration Files

Managing Upgrade Groups ................................................................. 274
  Adding Upgrade Groups ................................................................ 274
  Modifying Upgrade Groups ........................................................... 275
  Viewing Upgrade Groups ............................................................... 276
  Deleting Upgrade Groups .............................................................. 276
Viewing Software Versions ............................................................... 277
Upgrading NIOS Software ............................................................... 278
  Lite Upgrades .............................................................................. 278
  Uploading NIOS Software ............................................................ 278
  Distributing Software Upgrade Files .......................................... 279
  Managing Distributions ............................................................... 281
  Testing Software Upgrades ......................................................... 282
  Performing Software Upgrades .................................................. 282
  Monitoring Distribution and Upgrade Status ................................ 287
Downgrading Software ...................................................................... 288
Reverting to the Previously Running Software Version .................... 289
Backing Up and Restoring Configuration Files .................................. 290
  Backing Up Files ....................................................................... 289
  Automatically Backing Up Data Files ........................................... 290
  Manually Backing Up Data Files ................................................. 292
  Downloading Backup Files .......................................................... 292
  Restoring Backup Files ............................................................... 293
  Downloading Backup Files from a Different Appliance .................. 294
Downloading Support Bundles .......................................................... 295

Chapter 10 Monitoring the Appliance .............................................. 297
Viewing Appliance Status ............................................................... 298
  Grid Status .............................................................................. 298
  Member Status ......................................................................... 298
  Viewing Hardware Status ............................................................ 303
Monitoring Services ......................................................................... 304
  Service Status ......................................................................... 304
  Monitoring Grid Services ............................................................ 304
  Monitoring Member Services ...................................................... 305
Using a Syslog Server ....................................................................... 306
  Specifying Syslog Servers .......................................................... 306
  Configuring Syslog for Grid Members ......................................... 307
  Setting DNS Logging Categories ............................................... 308
  Viewing the Syslog ..................................................................... 309
  Searching in the Syslog ............................................................. 309
  Downloading the Syslog File ....................................................... 309
Monitoring Tools ............................................................................ 310
  Using the Audit Log .................................................................... 310
  Viewing the Replication Status .................................................... 312
  Using the Traffic Capture Tool ..................................................... 312
  Using the Capacity Report ......................................................... 313
  Using the Phone Home Feature .................................................. 314
  Monitoring DNS Transactions ..................................................... 315
  Viewing DNS Alert Indicator Status .......................................... 317
  Configuring DNS Alert Thresholds .............................................. 318
Chapter 19 DNSSEC ................................................................. 543

About DNSSEC ................................................................. 544
  DNSSEC Resource Records .................................................. 545
  DNSKEY Resource Records ............................................... 546
  RRSIG Resource Records .................................................. 548
  NSEC/NSEC3 Resource Records ......................................... 549
  NSEC3PARAM Resource Records ....................................... 550
  DS Resource Records ........................................................ 551

Configuring DNSSEC on a Grid ............................................ 552

Enabling DNSSEC ............................................................. 554

Setting DNSSEC Parameters ................................................ 555
  About the DNSKEY Algorithm ........................................... 555
  About Key Rollovers ....................................................... 555
  RRSIG Signatures .......................................................... 556
  Configuring DNSSEC Parameters ...................................... 557

Signing a Zone ...................................................................... 558

Managing Signed Zones ....................................................... 560
  Importing a Keyset ........................................................... 560
  Exporting Trust Anchors .................................................... 561
  Checking Key-Signing Keys ............................................... 561
  Rolling Key-Signing Keys .................................................. 561
  Unsigning a Zone ............................................................. 562
  Deleting and Restoring Signed Zones ................................... 562

Configuring Grid Members to Support DNSSEC as Secondary Servers ...................................................... 563

Configuring Recursion and Validation for Signed Zones ................................................................. 564
  Enabling Recursion and Validation for Signed Zones ................. 564
  Enabling DNSSEC Validation ............................................. 565
Chapter 20 Configuring IP Routing Options ............................................. 567
  Multiple IP Addresses on an Interface .................................................. 568
    IP Addresses on an Interface ............................................................. 568
    Configuring IP Addresses on the Loopback Interface ......................... 568
    Advertising Loopback IP Addresses to the Network ......................... 569
    Configuration Example: Configuring IP Addresses on the Loopback Interface 569
  Anycast Addressing ................................................................. 570
    Network Communication Types ......................................................... 570
    OSPF ................................................................. 572
    Configure OSPF on an Interface ..................................................... 572
    Configure an Anycast Address on an Interface ................................ 574

PART 4 DHCP

Chapter 21 Infoblox DHCP Services ...................................................... 577
  About Infoblox DHCP Services .......................................................... 578
  Configuring DHCP Overview ............................................................. 579
    DHCP Configuration Checklist ......................................................... 581
  About DHCP Inheritance ................................................................. 582
    Overriding DHCP Properties .......................................................... 583
    Viewing Inherited Values ............................................................... 583
  UTF-8 Encoding ................................................................. 587

Chapter 22 Managing DHCP Data .......................................................... 589
  About Network Views ................................................................. 591
    Adding Network Views ................................................................. 592
    Modifying Network Views ............................................................. 593
    Deleting Network Views ............................................................... 593
  About DHCP Networks ................................................................. 594
    Adding IPv4 Networks ................................................................. 594
    Viewing IPv4 Networks ................................................................. 596
    Modifying IPv4 Networks ............................................................. 597
    Associating Networks with Zones .................................................. 598
    Viewing the Networks Associated with a Zone ................................ 599
    Deleting IPv4 Networks ............................................................... 599
  About Shared Networks ................................................................. 600
    Adding Shared Networks ............................................................... 600
    Viewing Shared Networks ............................................................. 601
    Modifying Shared Networks .......................................................... 601
    Deleting Shared Networks ............................................................ 602
  About DHCP Data ................................................................. 603
    Guidelines for the Next Available IP Address .................................... 603
  Configuring DHCP Address Ranges .................................................... 604
    Adding DHCP Ranges ................................................................. 604
    Viewing DHCP Ranges ................................................................. 605
    Modifying DHCP Ranges ............................................................. 606
    Deleting DHCP Ranges ............................................................... 607
    Excluding Addresses from DHCP Ranges and Templates ..................... 607
# Chapter 23 Configuring DHCP Services

- About Configuring DHCP Services ...................................................... 618
- Configuring General DHCP Properties .................................................. 619
- Configuring UTF-8 Encoding for Hostnames .......................................... 620
- Configuring DHCP Lease Times .......................................................... 621
  - Keeping Leases in Deleted Networks and Ranges ................................... 622
  - Controlling Lease Assignments ......................................................... 622
- Configuring Ping Settings ................................................................... 623
- Configuring BOOTP Properties ............................................................ 625
- About DHCP Options ......................................................................... 626
  - DHCP Option Data Types ................................................................. 627
  - Configuring DHCP Options ............................................................... 628
  - Defining Option Spaces .................................................................. 628
  - Configuring Custom DHCP Options .................................................. 629
  - Applying DHCP Options .................................................................. 629
  - Configuration Example: Defining a Custom Option ............................... 631
  - Defining Option 60 Match Rules ....................................................... 632
  - About the DHCP Relay Agent Option (Option 82) ............................... 633
- Configuring Thresholds for DHCP Ranges .............................................. 634
- Configuring DHCP Logging .................................................................. 637
- About IF-MAP ...................................................................................... 638
  - Configuring a Grid to Support IF-MAP ............................................... 638
  - Purging Data from the IF-MAP Server ............................................... 639
- Starting DHCP Services on a Member .................................................... 639
- Viewing DHCP Member Status ................................................................. 640
  - Viewing DHCP Configuration Files .................................................... 641

# Chapter 24 Managing DHCP Templates

- About DHCP Templates ........................................................................ 644
- About DHCP Range Templates ............................................................ 645
  - Adding DHCP Range Templates ......................................................... 645
  - Modifying DHCP Range Templates ..................................................... 646
- About Fixed Address/Reservation Templates ........................................ 647
  - Adding Fixed Address/Reservation Templates ...................................... 647
  - Modifying Fixed Address/Reservation Templates .................................. 648
Chapter 30 Managing Microsoft DNS Services ........................................ 741
Managing Microsoft DNS Servers ......................................................... 742
Synchronizing DNS Data ................................................................. 742
Synchronizing with Multiple Servers .................................................. 743
Managing Synchronized DNS Data ...................................................... 744
Adding Zones to Microsoft Servers ..................................................... 745
Setting Zone Properties ................................................................. 746
Deleting and Restoring Synchronized Zones ........................................ 747
Managing Resource Records in Synchronized Zones ............................ 748
Synchronizing Updates ................................................................. 750
Synchronizing AD-Integrated Zones ..................................................... 753
Resolving Conflicts ................................................................. 753
Viewing Members and Managed Servers .......................................... 754
Specifying Forwarders for Microsoft Servers ..................................... 754
Disabling and Removing Microsoft DNS Servers ............................... 755

Chapter 31 Managing Microsoft DHCP Services ................................. 757
Managing Microsoft DHCP Servers .................................................. 758
Synchronizing DHCP Data ............................................................ 758
Viewing Synchronized Leases ......................................................... 759
Managing Synchronized DHCP Data .................................................. 760
Adding and Managing Scopes ......................................................... 760
Adding Fixed Addresses/Microsoft Reservations ................................. 766
About Superscopes .......................................................................... 768
Synchronizing Updates ................................................................. 770
Managing Microsoft DHCP Servers .................................................. 771
Viewing Members and Managed DHCP Servers ................................ 771
Setting Microsoft DHCP Server Properties ...................................... 772
Controlling the DHCP Service of a Microsoft Server ......................... 773
Disabling and Removing Microsoft DHCP Servers ............................. 773
Modifying DHCP Server Assignments .............................................. 773

Part 6 IPAM Management

Chapter 32 IP Address Management .................................................... 777
IP Address Management .................................................................. 779
About Network Containers ............................................................ 780
Deleting Network Containers .......................................................... 781
Managing IPv4 Networks .................................................................. 782
Network Map .................................................................................. 783
Network List .................................................................................. 787
Adding IPv4 Networks ..................................................................... 787
Modifying IPv4 Networks ............................................................. 787
Deleting IPv4 Networks ................................................................. 788
Resizing IPv4 Networks .................................................................. 788
Splitting IPv4 Networks into Subnets ................................................ 788
Joining IPv4 Networks ................................................................. 789
PART 7 Reference

Appendix A Grid Manager Icons ................................................................. 827

Appendix B Regular Expressions ................................................................. 833
Supported Expressions for Search Parameters ............................................. 833

Appendix C vNIOS Appliance Limitations ................................................... 835
vNIOS for Cisco ......................................................................................... 836
vNIOS for Riverbed .................................................................................. 837
vNIOS for VMware .................................................................................. 837

Appendix D Product Compliance ................................................................. 839
Power Safety Information ......................................................................... 840
AC ........................................................................................................... 840
DC .......................................................................................................... 840
Agency Compliance .................................................................................. 841
FCC ......................................................................................................... 841
Canadian Compliance ............................................................................. 841
VCCI ........................................................................................................ 842
RFC Compliance ..................................................................................... 843
DNS RFC Compliance .............................................................................. 843
DHCP RFC Compliance ......................................................................... 845

Appendix E Open Source Copyright and License Statements ...................... 847
GNU General Public License ...................................................................... 849
GNU Lesser General Public License ......................................................... 852
Apache Software License, Version 2.0 ......................................................... 858
perl Artistic License .................................................................................. 863
ISC BIND Copyright ................................................................................. 864
ISC DHCP Copyright .............................................................................. 865
Julian Seward Copyright .......................................................................... 866
Carnegie Mellon University Copyright ...................................................... 866
Thai Open Source Software Center Copyright ......................................... 867
Ian F. Darwin Copyright ........................................................................... 868
Lawrence Berkeley Copyright .................................................................. 869
MIT Kerberos Copyright .......................................................................... 869
BSD License .............................................................................................. 870
David L. Mills Copyright ........................................................................... 871
OpenLDAP License .................................................................................... 871
OpenSSL License ...................................................................................... 872
VIM License .............................................................................................. 873
ZLIB License ............................................................................................. 875
Wietse Venema Copyright ........................................................................ 875
ECLIPSE SOFTWARE .............................................................................. 876
Eclipse Public License - v 1.0 ................................................................... 876
Preface

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

- **Document Overview** on page 24
  - **Documentation Conventions** on page 24
- **What's New** on page 26
- **Related Documentation** on page 27
- **Customer Care** on page 28
  - **User Accounts** on page 28
  - **Software Upgrades** on page 28
  - **Technical Support** on page 28
**DOCUMENT OVERVIEW**

This guide describes how to configure and manage NIOS appliances using NIOS 5.1r4. It was last updated on February 16, 2011. For updated documentation, visit our Support site at http://www.infoblox.com/en/support/support-center-login.html

**Documentation Conventions**

The text in this guide follows the following style conventions.

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

**Variables**

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>a_record</td>
<td>A record</td>
</tr>
<tr>
<td>aaaa_record</td>
<td>AAAA record</td>
</tr>
<tr>
<td>admin_group</td>
<td>Name of a group of administrators</td>
</tr>
<tr>
<td>admin_name</td>
<td>Name of the appliance administrator</td>
</tr>
<tr>
<td>addr_range</td>
<td>IP address range</td>
</tr>
<tr>
<td>dhcp_template</td>
<td>DHCP template</td>
</tr>
<tr>
<td>domain_name</td>
<td>Domain name</td>
</tr>
<tr>
<td>directory</td>
<td>Directory name</td>
</tr>
<tr>
<td>failover_association</td>
<td>Failover association</td>
</tr>
<tr>
<td>filter_name</td>
<td>Name of a DHCP filter</td>
</tr>
<tr>
<td>fixed_address</td>
<td>Fixed address</td>
</tr>
<tr>
<td>fixed_address_template</td>
<td>Fixed address template</td>
</tr>
<tr>
<td>grid</td>
<td>Grid name</td>
</tr>
<tr>
<td>grid_master</td>
<td>Grid Master</td>
</tr>
<tr>
<td>grid_member</td>
<td>Grid Member</td>
</tr>
<tr>
<td>hostname</td>
<td>Host name of an independent appliance</td>
</tr>
<tr>
<td>Variable</td>
<td>Value</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>host_record</td>
<td>Host record</td>
</tr>
<tr>
<td>ifmap_client</td>
<td>IF-MAP client</td>
</tr>
<tr>
<td>ip_addr</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>lease</td>
<td>IP address of a lease</td>
</tr>
<tr>
<td>mac_filter</td>
<td>Name of a MAC filter</td>
</tr>
<tr>
<td>match_rule</td>
<td>Name of a match rule</td>
</tr>
<tr>
<td>member</td>
<td>Grid member name</td>
</tr>
<tr>
<td>ms_server</td>
<td>Microsoft server</td>
</tr>
<tr>
<td>netmask</td>
<td>Subnet mask</td>
</tr>
<tr>
<td>network</td>
<td>IP address of a network</td>
</tr>
<tr>
<td>network_access_server</td>
<td>Name of a NAS</td>
</tr>
<tr>
<td>network_template</td>
<td>Network template</td>
</tr>
<tr>
<td>network_view</td>
<td>Network view</td>
</tr>
<tr>
<td>option_space</td>
<td>DHCP option space</td>
</tr>
<tr>
<td>policy</td>
<td>Name of a policy on RADIUSone</td>
</tr>
<tr>
<td>policy_group</td>
<td>Name of a Policy Group</td>
</tr>
<tr>
<td>port</td>
<td>Number of a port; predefined for certain protocols</td>
</tr>
<tr>
<td>ptr_record</td>
<td>PTR record</td>
</tr>
<tr>
<td>reservation</td>
<td>Reservation</td>
</tr>
<tr>
<td>roaming_host</td>
<td>Roaming host</td>
</tr>
<tr>
<td>scheduled_task</td>
<td>Scheduled task</td>
</tr>
<tr>
<td>server_group</td>
<td>Name of a group of servers</td>
</tr>
<tr>
<td>shared_network</td>
<td>Shared network</td>
</tr>
<tr>
<td>service</td>
<td>One of the services available from Grid Manager</td>
</tr>
<tr>
<td>template</td>
<td>DHCP template</td>
</tr>
<tr>
<td>dns_view</td>
<td>DNS view</td>
</tr>
<tr>
<td>zone</td>
<td>DNS zone</td>
</tr>
</tbody>
</table>

**Navigation**

Infoblox technical documentation uses an arrow “→” to represent navigation through the user interface. For example, to edit a fixed address, the description is as follows:

From the **Data Management** tab, select the **DHCP** tab → **Networks** tab → **Networks** → **network** → **fixed_address** check box, and then click the Edit icon.
What’s New

The following sections are new or have been updated in this version of this guide:

- **Lease Scavenging**: You can enable member DHCP servers to automatically delete free and backup leases that remain in the database beyond a specified period of time. When you enable this feature, the appliance permanently deletes the free and backup leases, and you can no longer view or retrieve the lease information. For more information, see *Scavenging Leases* on page 672.

- **Synchronization with Microsoft Servers**: With this release, there is an option to create a Microsoft user account that does not require Administrator Group rights to synchronize Microsoft servers. For more information, see *Setting Microsoft Server Credentials* on page 731.

- **IPv6 Support for NIC Redundancy**: This release supports both IPv4 and IPv6 addresses for NIC (Network Interface Controller) redundancy using the LAN2 port. For more information, see *About NIC Redundancy* on page 237.
Related Documentation

Other Infoblox appliance documentation:

- Infoblox CLI Guide
- Infoblox API Documentation
- Infoblox IBOS Administrator Guide
- Infoblox-500, Infoblox-1000 and Infoblox-1200 Quick Start
- Infoblox User Guide for the Infoblox-1050, 1550, and 1552 Appliances
- Infoblox User Guide for the Infoblox-500, -550 Appliance
- Infoblox Installation Guide for the Infoblox-550, -1050, -1550, and -1552 Appliances
- Infoblox installation Guide for the Infoblox-1852-A Appliance
- Infoblox Installation Guide for the Infoblox-250 Appliance
- Infoblox Installation Guide for the Infoblox-250-A Appliance
- Infoblox Installation Guide for the Infoblox-2000 Appliance
- Infoblox Installation Guide for the Infoblox-2000-A Appliance
- Quick Start Guide for Installing vNIOS Software on Riverbed Services Platforms
- Quick Start Guide for Installing vNIOS Software on Cisco Application eXtension Platforms
- Quick Start Guide for Installing vNIOS Software on VMware Platforms
- Quick Start Guide for Installing vIBOS Software on VMware Platforms
- Infoblox Safety Guide

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

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

**User Accounts**

The Infoblox appliance ships with a default user name and password. Change the default `admin` account password immediately after the system is installed to safeguard its use. Make sure that the NIOS appliance has at least one administrator account with superuser privileges at all times, and keep a record of your account information in a safe place. If you lose the `admin` account password, and did not already create another superuser account, the system will need to be reset to factory defaults, causing you to lose all existing data on the NIOS appliance. You can create new administrator accounts, with or without superuser privileges. For more information, see *Managing Administrators* on page 77.

**Software Upgrades**


**Technical Support**

Part 1 Appliance GUI

This section provides basic information about the Infoblox appliance, including a description of the user interface and information about basic configuration tasks. It includes the following chapters:

- Chapter 1, *Infoblox Grid Manager*, on page 31
- Chapter 2, *The Dashboard*, on page 55
- Chapter 3, *Smart Folders*, on page 67
Chapter 1  Infoblox Grid Manager

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

- **Management System Requirements** on page 33
  - Supported Browsers on page 33
  - Browser Limitations on page 34
- **About Grid Manager** on page 35
  - Admin Permissions for Grid Manager on page 35
  - Logging in to the GUI on page 35
- **Setting Login Options** on page 36
  - Specifying the Grid Name and Hostname on page 36
  - Managing Certificates on page 36
  - Creating a Login Banner on page 36
  - Changing the Password and Email Address on page 36
  - Specifying the Table Size on page 37
  - Setting the Browser Time Zone on page 37
- **SSL (Secure Sockets Layer) Protocol** on page 38
- **Managing Certificates** on page 39
  - Generating Self-Signed Certificates on page 39
  - Generating Certificate Signing Requests on page 40
  - Downloading Certificates on page 41
  - Uploading Certificates on page 40
- **About the Grid Manager Interface** on page 42
  - System Messages on page 42
  - Breadcrumbs Navigation on page 43
  - Global Search on page 43
  - Finder Panel on page 43
  - Toolbar Panel on page 43
  - Help Panel on page 43
  - Wizards and Editors on page 43
— **Tooltips** on page 43
— **Customizing Tables** on page 44
— **Selecting Objects in Tables** on page 44

- **Finding and Restoring Data** on page 46
  — **Using the Finder Panel** on page 46
  — **Using Filters** on page 49
  — **Using Global Search** on page 49
  — **Using the Go To Function** on page 51

- **About Long Running Tasks** on page 52
  — **Running Tasks in the Background** on page 52
  — **Monitoring Long Running Tasks** on page 53

- **Printing from Grid Manager** on page 53
- **Exporting Data from Grid Manager** on page 53
- **Multilingual Support** on page 54
  — **UTF-8 Supported Fields** on page 54
  — **UTF-8 Support Limitations** on page 54
**Management System Requirements**

The management system is the computer from which you configure and manage the NIOS appliance. The management system must meet the following requirements.

*Figure 1.1 Software and Hardware Requirements for the Management System*

<table>
<thead>
<tr>
<th>Management System Software Requirements</th>
<th>Management System Hardware Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>• See Supported Browsers on page 33 for details.</td>
<td>• Minimum System: 1.4 GHz CPU with 1 GB RAM available to the product GUI, and 256 Kbps connectivity to NIOS appliance</td>
</tr>
<tr>
<td>• CLI ACCESS</td>
<td>• Recommended System: 2.0 GHz (or higher) dual core CPU with 2 GB RAM available for the product GUI, and network connectivity to NIOS appliance</td>
</tr>
<tr>
<td>• Secure Socket Shell (SSH) client that supports SSHv2</td>
<td>• Monitor Resolution: 1024 x 768 (minimum)</td>
</tr>
<tr>
<td>• Terminal emulation program, such as minicom or Hilgraeve Hyperterminal®</td>
<td>1280 x 800 or better (recommended)</td>
</tr>
</tbody>
</table>

**Supported Browsers**

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

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Supported Browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 7®</td>
<td>Microsoft Internet Explorer® 8.x</td>
</tr>
<tr>
<td></td>
<td>Mozilla Firefox® 3.5.x and 3.6.x</td>
</tr>
<tr>
<td></td>
<td>Google Chrome™ 5.x</td>
</tr>
<tr>
<td>Microsoft Windows Vista®</td>
<td>Microsoft Internet Explorer 7.x</td>
</tr>
<tr>
<td>Microsoft Windows XP®(SP2+)</td>
<td>Microsoft Internet Explorer 7.x and 8.x</td>
</tr>
<tr>
<td></td>
<td>Mozilla Firefox 3.5.x and 3.6.x</td>
</tr>
<tr>
<td></td>
<td>Google Chrome 5.x</td>
</tr>
<tr>
<td>Red Hat® Enterprise Linux® 5.0 and higher</td>
<td>Mozilla Firefox 3.5.x and 3.6.x</td>
</tr>
<tr>
<td>Apple® OS X® 10.5.x</td>
<td>Safari 4.x</td>
</tr>
<tr>
<td>Apple OS X 10.6.x</td>
<td>Safari 5.x</td>
</tr>
<tr>
<td></td>
<td>Google Chrome 5.x</td>
</tr>
</tbody>
</table>

To enhance performance on Internet Explorer 7.x and 8.x browsers, Infoblox recommends that you install the Google Chrome Frame™ plug-in. For more information, refer to [http://code.google.com/chrome/chromeframe/](http://code.google.com/chrome/chromeframe/).
Browser Limitations

- When you use Internet Explorer 7 or 8 without installing the latest updates, Grid Manager may stop loading a page when you navigate from one tab to another or when you use the back navigation button to go back to a previous page. To solve this problem, you can press Ctrl+F5 to refresh the browser or install the latest updates.

- When you use the zoom function in Internet Explorer 7 running on Microsoft Windows XP, Grid Manager may not properly display some pop up windows. This is a known issue in Internet Explorer 7.

- In Internet Explorer 8, Grid Manager does not display the directory path of an uploaded file. Instead, it displays “fakepath” in place of the directory path. To resolve this issue, you can add Grid Manager as a trusted site or enable the “Include local directory path when uploading files to a server” feature in the browser. For information, refer to the MSDN documentation at http://msdn.microsoft.com/en-us/library/ms535128.aspx.

- When you use FireFox to access Grid Manager, tooltips do not display for disabled drop-down menu items. In addition, when you run a large query of smart folders, Grid Manager may display a warning message about “Unresponsive Script”. Click Continue to proceed.

- Depending on the browser you use, Grid Manager may display a dialog box that indicates the system is unavailable during a system restart or reboot.

- Infoblox strongly recommends that you do not log in to Grid Manager from different browser windows using the same user account. Depending on the browser you use, it may cache user information in one session and apply it to another session. This can cause inconsistent behaviors within the browser sessions.
About Grid Manager

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

- Use Smart Folders to organize your data based on criteria you specify. For information, see Smart Folders on page 67.
- The network and IP address maps and lists provide views of your networks and IP addresses, so you can quickly evaluate IP address usage and understand how your network resources are being utilized. You can quickly determine which IP addresses are in use, when they were allocated, and to which devices they were assigned. For information, see Managing IPv4 Networks on page 782.
- Customize the Dashboard to monitor your grid and networks. The Dashboard also provides access to frequently-used commands and the network discovery feature. You can run network discoveries to identify IP address conflicts and troubleshoot network issues. For information, see The Dashboard on page 55.
- Tools such as the Finder panel, filters, and global search help you quickly find the information you need. For information, see Finding and Restoring Data on page 46.
- Use wizards to quickly create new networks and resource records. Editors allow you to configure additional operational parameters. For information, see Wizards and Editors on page 43.

Before you can use Grid Manager, you must install and configure the NIOS appliance as described in the installation guide that shipped with your product. You can then access Grid Manager using one of the supported browsers. For information, see Supported Browsers on page 33.

Admin Permissions for Grid Manager

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

Note that superusers must configure admin groups and accounts in the Grid Manager application of the NIOS appliance. In Grid Manager, superusers can set and change permissions for specific objects, such as IPv4 networks, IPv6 networks, and resource records. For information about user accounts and administrative permissions, see Managing Administrators on page 77.

Logging in to the GUI

Before you log in to Grid Manager, ensure that you have installed your NIOS appliance as described in the installation guide or user guide that shipped with your products and configured it accordingly.

To log in to Grid Manager:

1. Open an Internet browser window and enter https://<IP address or hostname of your NIOS appliance>. The Grid Manager login page appears. For information, see Supported Browsers on page 33.
2. Enter your user name and password, and then click Login or press Enter. The default user name is admin and the default password is infoblox.
3. Read the Infoblox End-User License Agreement and click I Accept to proceed. Grid Manager displays the Dashboard, your home page in Grid Manager. For information about the Dashboard, see The Dashboard on page 55.

Tip: You can customize the text that appears on the Grid Manager login page. To do so, see Creating a Login Banner on page 36.
**SETTING LOGIN OPTIONS**

Grid Manager provides several options that you can set to facilitate the login process.

**Specifying the Grid Name and Hostname**

To define the default hostname that appears when the login prompt displays:

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

**Managing Certificates**

You can manage CA (Certificate Authority) and server certificates on the NIOS appliance. You can import certificates, select and view their details, or remove them. To manage certificates, see *Managing Certificates* on page 39.

**Creating a Login Banner**

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

To create a login banner:

1. From the Grid tab, select the Grid Manager tab, and then click Grid Properties -> Edit from the Toolbar.
2. In the Grid Properties editor, select the Security tab, and then select Enable Login Banner. In the text field, enter the text that you want displayed on the login screen.
3. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and continue to edit.

**Changing the Password and Email Address**

Grid Manager creates and stores a user profile for each admin user. Each user profile contains information about the admin group and admin type assigned to the user. You can modify information in your user profile any time after the initial login. You can change your password to facilitate future logins and add your email address for reference.

Note that when multiple users log in to Grid Manager using the same admin account, they share the same user profile and preference settings, such as the widget, table size and column settings, independent of their browser settings. Instead of using the same admin account for multiple users, you can add multiple users to the same admin group so they can share the same permissions. For information about configuring admin accounts and admin groups, see *Managing Administrators* on page 77.

To change your password and email address:

1. Select any tab in Grid Manager, and then click **User Profile** from the Toolbar.
2. In the User Profile editor, complete the following:
   - **Name**: Displays your user name.
   - **Last Login**: Displays the timestamp of your last login.
   - **Type**: Displays your user type. There are two user types: **Local** and **Remote**. The local admin accounts are stored in the database of the appliance, and the remote admin accounts are stored on another server, such as a RADIUS server. Grid Manager automatically deletes remote user profiles if the users have not logged in for more than six months.
— **Group**: Displays the admin group to which your account belongs. The admin group determines your administrative permissions. Only superusers can define admin groups through Grid Manager.
— **Set Password**: If you are a local user, you can enter a new password for your account. If you are a remote user, you do not see this field.
— **Retype Password**: Enter the same password.
— **Email Address**: Enter your email address. Note that this address simply provides contact information. By default, this field is blank.

3. Click **Save & Close**.

### Specifying the Table Size

You can specify the amount of data Grid Manager can display in a table or a single list view. You can improve the display performance by setting a smaller table size. The setting you specify here applies to all tables in Grid Manager.

To specify table size:

1. Select any tab in Grid Manager, and then click **User Profile** from the Toolbar.
2. In the **User Profile** editor, complete the following:
   — **Table Size**: Specify the number of lines of data you want a table or a single list view to contain. You can set the number of lines from 10 to 256. The default is 20.
3. Click **Save & Close**.

### Setting the Browser Time Zone

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

To manually set the time zone of your browser:

1. Select any tab in Grid Manager, and then click **User Profile** from the Toolbar.
   
The **User Profile** editor displays your user name, user type, and admin group.
2. In the **User Profile** editor, complete the following:
   — **Time Zone**: Select the time zone Grid Manager uses to convert all displayed time values. The default is **Auto-detect time zone**. You must select a specific time zone when Grid Manager cannot automatically detect the time zone of your browser.
3. Click **Save & Close**.
SSL (Secure Sockets Layer) Protocol

When you log in to the NIOS appliance, your computer makes an HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer protocol) connection to the NIOS appliance. HTTPS is the secure version of HTTP, the client-server protocol used to send and receive communications throughout the Web. HTTPS uses SSL (Secure Sockets Layer) to secure the connection between a client and server. SSL provides server authentication and encryption. The NIOS appliance supports SSL versions 2 and 3.

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

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

The server and the client use the random value to generate the master secret, which they in turn use to generate symmetric keys. The client and server end the handshake when they exchange messages indicating that they are using the symmetric keys to encrypt further communications.

Figure 1.2 SSL Handshake

Client contacts the NIOS appliance and recommends certain parameters, such as SSL version, cipher settings, and session-specific data.

The appliance either agrees or recommends other parameters. It also sends its certificate which contains its public key.

Client encrypts random number with the public key and sends it to the appliance. The appliance uses its private key to decrypt the message.

The client and the appliance generate the master secret, and then the symmetric keys.

The client and the appliance agree to encrypt all messages with symmetric keys.

The client and the appliance send all their messages through the SSL tunnel which uses the cipher settings and encryption to secure their connection.
MANAGING CERTIFICATES

The NIOS appliance generates a self-signed certificate when it first starts. A self-signed certificate is signed by the subject of the certificate, and not by a CA (Certificate Authority). This is the default certificate. When your computer first connects to the NIOS appliance, it sends this certificate to authenticate itself to your browser.

Because the default certificate is self-signed, your browser does not have a trusted CA certificate or a cached NIOS appliance server certificate (saved from an earlier connection) to authenticate the NIOS appliance certificate. Also, the hostname in the default certificate is www.infoblox.com, which is unlikely to match the hostname of your NIOS appliance. Consequently, messages appear warning that the certificate is not from a trusted certifying authority and that the hostname on the certificate is either invalid or does not match the name of the site that sent the certificate. Either accept the certificate just for this session or save it to the certificate store of your browser.

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

- Generate another self-signed certificate with the correct hostname and save it to the certificate store of your browser. For information, see Generating Self-Signed Certificates.
- Request a CA-signed certificate with the correct hostname and load it on the NIOS appliance. For information, see Generating Certificate Signing Requests on page 40.
- When you receive the certificate from the CA, import it to the appliance, as described in Uploading Certificates on page 40.
- Download the certificate from a trusted CA, as described in Downloading Certificates on page 41.

Generating Self-Signed Certificates

You can replace the default certificate with a self-signed certificate that you generate. When you generate a self-signed certificate, you can specify the correct hostname and change the public/private key size, enter valid dates and specify additional information specific to the NIOS appliance. If you have multiple appliances, you can generate a certificate for each appliance with the appropriate hostname.

To generate a self-signed certificate:

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

   or

   Infoblox Orchestration Server with the dedicated certificate feature enabled: From the Data Management tab, select the IF-MAP tab, and then click IF-MAP Service Certificate -> Generate Self-signed Certificate from the Toolbar.

2. In the Generate Self-Signed Certificate dialog box, complete the following:
   - **Key Size**: Select either 2048 or 1024 for the length of the public key.
   - **Days Valid**: Specify the validity period of the certificate.
   - **Common Name**: Specify the domain name of the NIOS appliance. You can enter the FQDN (fully qualified domain name) of the appliance.
   - **Organization**: Enter the name of your company.
   - **Organizational Unit**: Enter the name of your department.
   - **Locality**: Enter a location, such as the city or town of your company.
   - **State or Province**: Enter the state or province.
   - **Country Code**: Enter the two-letter code that identifies the country, such as US.
   - **Admin E-mail Address**: Enter the email address of the appliance administrator.
   - **Comment**: Enter information about the certificate.

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

**Generating Certificate Signing Requests**

You can generate a CSR (certificate signing request) that you can use to obtain a signed certificate from your own trusted CA. Once you receive the signed certificate, you can import it in to the NIOS appliance, as described in Uploading Certificates on page 40.

To generate a CSR:

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

   or

   Infoblox Orchestration Server with the dedicated certificate feature enabled: From the Data Management tab, select the IF-MAP tab, and then click IF-MAP Service Certificate -> Create Signing Request from the Toolbar.

2. In the Create Certificate Signing Request dialog box, enter the following:
   - **Key Size**: Select either 2048 or 1024 for the length of the public/private key pair.
   - **Common Name**: Specify the domain name of the NIOS appliance. You can enter the FQDN of the appliance.
   - **Organization**: Enter the name of your company.
   - **Organizational Unit**: Enter the name of your department.
   - **Locality**: Enter a location, such as the city or town of your company.
   - **State or Province**: Enter the state or province.
   - **Country Code**: Enter the two-letter code that identifies the country, such as US.
   - **Admin E-mail Address**: Enter the email address of the appliance administrator.
   - **Comment**: Enter information about the certificate.

3. Click OK.

**Uploading Certificates**

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

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

To import a certificate:

1. Grid: From the Grid tab, select the Grid Manager tab -> Members tab -> member check box, and then click HTTPS Cert -> Upload Certificate from the Toolbar.

   or

   Infoblox Orchestration Server with the dedicated certificate feature enabled: From the Data Management tab, select the IF-MAP tab, and then click IF-MAP Service Certificate -> Upload Certificate from the Toolbar.

2. Navigate to where the certificate is located and click Open.

3. If the appliance already has an existing HTTPS certificate, the new certificate replaces the existing one. In the Replace HTTPS Certificate Confirmation dialog box, click Yes.

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

You can download the current certificate or a self-signed certificate, as described in Generating Self-Signed Certificates on page 39.

To download a certificate:

1. Grid: From the Grid tab, select the Grid Manager tab -> Members tab -> member check box, and then click HTTPS Cert -> Download Certificate from the Toolbar.
   or
   Infoblox Orchestration Server with the dedicated certificate feature enabled: From the Data Management tab, select the IF-MAP tab, and then click IF-MAP Service Certificate -> Download Certificate from the Toolbar.

2. Navigate to where you want to save the certificate, enter the file name, and then click Save.
ABOUT THE GRID MANAGER INTERFACE

Grid Manager provides an easy-to-use interface that simplifies core network services management. Its navigational tools enable you to quickly move through the application and retrieve the information you need. You can customize different elements in your workspace, and hide and display panels as you need them. It also provides different types of Help, so you can immediately access the information you need to complete your tasks. Figure 1.3 illustrates the typical layout of Grid Manager. It identifies common elements of the interface and features that you can use:

Figure 1.3 Grid Manager Interface

System Messages
Breadcrumbs Navigation
Long Running Task
Global Search
Finder Panel
Workspace
Toolbar
Help panel

System Messages

Grid Manager displays system messages at the top of the screen. In wizards and editors, it displays messages at the top as well.

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

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

Global Search

Use Global Search to find data. Grid Manager searches the entire NIOS database for data that matches the criteria you specify. For additional information on Global Search, see Using Global Search on page 49.

Finder Panel

The Finder panel appears on all pages in Grid Manager. It provides the following tools:
- Smart Folders: Use smart folders to organize your data according to criteria that you specify.
- Bookmarks: Stores data that you have marked for easy retrieval.
- Recycle Bin: Stores deleted objects that you can either restore or permanently remove.
You can resize, collapse, and expand the Finder panel. For information, see Using the Finder Panel on page 46.

Toolbar Panel

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

Help Panel

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

Wizards and Editors

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

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

Tooltip

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

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

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

To sort the data displayed in a table, click the header title. You can click the header title again to reverse the sort order. Alternatively, you can do the following:
1. In the table, mouse over to a header title and click the down arrow key.
2. Select Sort Ascending or Sort Descending.

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

Grid Manager displays the selected column in the table.

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

Selecting Objects in Tables

In a table, Grid Manager displays data on multiple pages when the number of items to be displayed exceeds the maximum number of items that can be displayed on one page. Use the navigational buttons at the bottom of the table to page through the display.

You can select multiple rows in a table. For example, in a Windows browser, you can do the following to select multiple rows:

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

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

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

In a table, when you select all the objects for deletion, the objects that are not deleted from the database remain in the table after the operation is completed.
Figure 1.4 Select All in a Table

Click this link to select all rows on all pages.

Click this check box to select all rows on this page only.

Use these navigational buttons to page through the display.
**Finding and Restoring Data**

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

**Using the Finder Panel**

The *Finder* panel appears on all pages in Grid Manager. The panel is expanded by default. The *Finder* panel provides easy access to the following:

- **Smart Folders**: Contains a hierarchical list of smart folders that are available in My Smart Folders. For information, see *My Smart Folders* on page 69.
- **Bookmarks**: Contains bookmarked objects, such as networks and IP addresses. For information, see *Bookmarks*.
- **Recycle Bin**: Contains deleted objects that can be restored or permanently removed. For information, see *Recycle Bin* on page 47.

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

**Bookmarks**

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

You can do the following in Bookmarks:

- Access a bookmarked object
- Edit the name of a bookmark
- Delete a bookmark

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

You can arrange the order of the bookmarked objects by dragging and dropping the objects in the *Finder* panel.

To edit the name of a bookmark:

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

To delete a bookmark:

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

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

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

On a NIOS appliance, only superusers have permissions to fully manage the Recycle Bin. If you have limited-access permissions, you can view, restore, and permanently remove only the objects that you deleted. On an Infoblox IF-MAP server, only superusers can fully manage the Recycle Bin. Limited-access admins cannot view or restore IF-MAP clients from the Recycle Bin.

You can do the following in the Recycle Bin:

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

Enabling and Disabling the Recycle Bin

To enable or disable the Recycle Bin:

1. From the Grid tab, select the Grid Manager tab, and then click Grid Properties -> Edit from the Toolbar.
2. In the Grid Properties Editor, select the General tab, and then complete the following:
   - Select Enable Recycle Bin to enable the Recycle Bin
   - Deselect Enable Recycle Bin to disable the Recycle Bin.
3. Select one of the following:
   - Save & Close: Save the entry and close the editor.
   - Save: Save the entry and continue to edit.

Viewing Objects in the Recycle Bin

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

The Recycle Bin does not display all deleted objects; it can display up to 15 of the most recently deleted objects. When the Recycle Bin contains objects that are not displayed in the Finder panel or multiple objects that have the same name, the Show All button appears. Click the button to display the Recycle Bin dialog box that contains detailed information about each deleted object. When you have multiple deleted objects that use the same name, you may want to view detailed information about the deleted objects before taking any action. You can remove and restore selected objects and empty the Recycle Bin in the Recycle Bin dialog box.
To view detailed information about deleted objects:
1. In the Finder panel, expand Recycle Bin.
2. Click Show All.
   Grid Manager displays the Recycle Bin dialog box that contains the following information for each object:
   - Name: The short name of the object. For example, the short names for fixed addresses and reservations are their IP addresses.
   - Type: The object type.
   - Parent/Container: The parent object or parent container to which the object belongs.
   - Admin: The admin name of the user who deleted the object.
   - Data: The data that the object contains, if any.
   - Network View: The network view to which the object belongs.
   - Time: The time stamp when the object was deleted.
   To close the dialog box, click Close.

Restoring Objects from the Recycle Bin
You can restore deleted objects from the Recycle Bin only if you enable the Recycle Bin, and only if you select an object in the panel. You can restore only one object at a time. Deleted objects are stored in the Recycle Bin until you delete them or empty the bin.
To restore items from the Recycle Bin:
1. In the Finder panel, expand Recycle Bin.
2. Select the object you want to restore.
3. Click the Restore icon.
   Grid Manager restores the object to its corresponding container or configuration. You can confirm the restoration by checking that the object does not appear in the Recycle Bin any longer, and that it is reestablished in the appropriate panel in the GUI.

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

Emptying the Recycle Bin
You can permanently delete the contents of the Recycle Bin, if enabled. Only superusers can empty the Recycle Bin. Because the Recycle Bin can grow large, you can periodically empty the Recycle Bin to free up disk space.
To empty the Recycle Bin:
1. In the Finder panel, expand Recycle Bin.
2. Click Empty.
   Grid Manager displays the Confirm Empty Recycle Bin dialog box to confirm that you wish to empty the Recycle Bin.
3. Click Yes.
Using Filters

You can control the amount and the kind of data displayed in a specific panel by adding filter criteria. When you add filter criteria, the appliance screens the data based on your filter rules and displays only the information that matches the rules. To narrow your search for specific information, you can add up to 10 filter rules. In some panels, such as the DHCP Networks tab, you can switch between viewing information with and without the filter criteria by toggling the filter on or off.

You can also use filters to find objects that have failed an operation. When you try to modify multiple objects with the same extensible attribute, the appliance may not modify all of the selected objects. For information, see Editing Multiple Extensible Attribute Values on page 226. For example, after you modify the extensible attribute “Building” with new value “West”, you can find the objects that are not updated by defining a filter with “Building” “does not equal” “West”.

To use filters:
1. In a panel, click Show Filters to enable the function.
2. In the filter section, complete the following:
   - In the first drop-down list, select a field such as an object name, comment, or an extensible attribute (fields with a gray background) as the filter criterion. Grid Manager displays only the supported fields.
   - In the operator drop-down list, select an operator for the filter criterion. Depending on what you select in the first filter field, this list displays the relevant operators for the selection.
   - In the value field, enter or select the attribute value for the first filter field. Depending on what you select for the first two filter fields, you can either enter a value or select an attribute from a drop-down list. For example, if you select an extensible attribute in the first filter field, you can enter the attribute value here.
3. Optionally, click the + icon to add another filter rule. You can add up to 10 filter rules.
4. Click Apply to apply the rules
   or
   Click Reset to clear the filter criteria.

To view information with or without the filter criteria:
- Click Toggle Filter On to apply filter criteria to the displayed data. Grid Manager displays only the filtered data in the panel.
- or
- Click Toggle Filter Off to have the appliance list all data without applying filter criteria.

Using Global Search

You can use the global search function to search the entire NIOS database for data that matches a specific value and filter criteria. You can enter a search value and define filter criteria to refine the search. Grid Manager supports regular expressions in global search. Grid Manager can display up to 500 search results. When search results exceed 500, a warning message appears and you may want to refine your search. Search results remain in the Search dialog box until you reset the search parameters or log out of Grid Manager.

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

To search globally:
1. Click the global search icon on the navigation bar.
2. In the Search dialog box, do the following:
   - In the first field, enter the value that you want your search results to match. For example, if you want to search for hostnames that contain “Infoblox”, enter Infoblox in this field. You can also use regular expressions in the search value. For information, see Regular Expressions on page 833.
3. Optionally, click the + icon to add another filter. You can add up to 10 filter rules.

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

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

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

You can click **Reset** to clear the search results and start a new search. You can also click the Refresh icon to refresh the search results. Grid Manager stores the search results until you reset the search parameters or log out.

### Editing Matching Objects in Search Results

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

To edit an object in the Results table:

1. In the Results table, select the object check box.
2. Click the Open or Edit icon. You can also click the link of an object if Grid Manager displays the path.

   Grid Manager displays the object in the corresponding editor depending on the type of object you selected.
3. Edit the properties of the object in the editor.
4. Save your changes.
Deleting Matching Objects in Search Results

You can delete one or multiple matching objects in the search Results table.

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

Grid Manager deletes the selected objects from the database. Most deleted objects are stored in the Recycle Bin. For information, see Recycle Bin on page 47.

You can print search results. You can also export search results in CSV (comma separated value) format. For information, see Printing from Grid Manager on page 53 and Exporting Data from Grid Manager on page 53.

Using the Go To Function

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

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

Grid Manager completes the operation based on the selected object.
About Long Running Tasks

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

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

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

The appliance supports the following long running tasks:
- Restoring the database
- Backing up the database
- Backing up licenses
- Signing DNS zones
- Unsinging DNS zones
- Exporting DS records and trust anchors
- Deleting all objects in a table or dataset
- Modifying multiple extensible attributes
- Viewing DNS and DHCP configuration properties
- Downloading the following:
  - Audit logs
  - Syslog files
  - Support bundles
  - SNMP MIB files
  - NTP keys
  - HTTPS certificates
  - Traffic capture

Running Tasks in the Background

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

You can run the following tasks in the background:
- Signing DNS zones
- Unsinging DNS zones
- Modifying multiple extensible attributes
- Deleting all objects in a table or dataset

To run a task in the background:

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

You can view the progress of the task by clicking the progress bar at the top of the interface. For information, see Monitoring Long Running Tasks on page 53.
Monitoring Long Running Tasks

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

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

Printing from Grid Manager

In Grid Manager, you can print information from panels and pages that support the Print function. Grid Manager prints data one page at a time. The amount of data that is displayed in a specific panel depends on the table size configuration that you set in your user profile. For information, see Specifying the Table Size on page 37.

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

Exporting Data from Grid Manager

You can export certain information, such as global search results and syslog file, in CSV (comma separated value) format from panels and pages that support the Export function.

To export data:
1. Click the Export icon.
2. In the Export dialog box, click Start. Grid Manager displays a message about the time required to export data could be long depending on the amount of data.
3. Click Download when the export is finished.
4. Depending on your browser and operating system, you may need to do one of the following in the Opening .csv dialog box:
   — Open with: Select a program with which you want to open the .csv file.
   — Save to Disk: Select this if you want to save the .csv file to your local computer.
   — Do this automatically for files like this from now on: Select this check box if you want Grid Manager to use the same method for future exports. When you select this check box, Grid Manager does not display the Opening .csv dialog box in the future.
5. Click OK.
   Depending on the selected option, Grid Manager opens the file using the program you select, or saves the file to your local computer.
**Multilingual Support**

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

- Hostnames for Microsoft Windows clients that support Microsoft Windows code pages. For information, see Configuring UTF-8 Encoding for Hostnames on page 620.
- Input fields through Grid Manager. For information, see UTF-8 Supported Fields.

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

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

**UTF-8 Supported Fields**

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

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

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

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

**UTF-8 Support Limitations**

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

- Object names that have data restrictions due to their usage outside of the Infoblox database do not support UTF-8 encoding. For example, IP addresses, DNS names, and Active Directory domain names.
- When importing a database, most of the ASCII control characters cannot be encoded. This might cause failures in upgrades or database restore operations.
- Search is based on the Unicode standard. Depending on the language, you might not be able to perform a case-sensitive search.
- Binary data is encoded as text.
- UTF-8 encoding does not fully support regular expressions. It matches constant strings. However, it does not encode characters that are inside square brackets or followed by regular expressions such as *, ?, or +.
- You can use UTF-8 characters to authenticate both the User Name and Password through the Infoblox GUI, but not through the Infoblox CLI.
- The Infoblox CLI does not support UTF-8 encoding.
Chapter 2   The Dashboard

The Dashboard provides a quick view of your grid and core network services data. This chapter includes the following sections:

- **About the Dashboard** on page 56
  - Grid Status on page 57
  - Member Status (System Status) on page 58
  - DNS Statistics on page 59
  - Ranges Over Threshold on page 60
  - Failover Associations Status on page 60
  - DHCP Statistics on page 60
  - Network Statistics on page 61
  - Networks Over Threshold on page 62
  - Discovery Status on page 62
  - My Commands on page 63
  - DDNS Statistics on page 63
  - System Activity Monitor on page 63
  - File Distribution Statistics on page 64
  - Active WebUI Users on page 64
  - Microsoft Servers Status Widget on page 65
The Dashboard

**ABOUT THE DASHBOARD**

The Dashboard is your home page on Grid Manager. It provides easy access to tasks and to the status of your grid and networks. It provides various widgets for viewing and managing data. Widgets are the building blocks of your Dashboard. They provide information about different aspects of your grid and networks. For example, the *Member Status* widget provides general information about a grid member, and the *Network Statistics* widget provides data for a specified network.

You can select the widgets that you need and configure them to provide relevant data. From the Dashboard, you can access your most common tasks and monitor your IP address infrastructure. You can add all or some of the following widgets to your Dashboard depends on whether you are managing a grid, an independent appliance, or an Infoblox Orchestration server:

- Grid Status
- Member Status (System Status)
- DNS Statistics
- Ranges Over Threshold
- Failover Associations Status
- DHCP Statistics
- Network Statistics
- Networks Over Threshold
- Discovery Status
- My Commands
- DDNS Statistics
- System Activity Monitor
- File Distribution Statistics
- Active WebUI Users
- Microsoft Servers Status Widget

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

To add widgets to your Dashboard:

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

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

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

Widgets have the following icons:

- **Refresh**: Click to update the content of the widget. Each widget contains a status bar at the bottom that displays the last date and time it was updated.
- **Configure**: Click to hide and show the configuration options of the widget.
- **Toggle**: Click to minimize and restore the widget.
- **Close**: Click to remove the widget from the Dashboard.
Grid Status

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

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

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

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

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

This section also displays the overall operational status of the DNS, DHCP, NTP, FTP, TFTP, HTTP (File Distribution), bloxTools, and Captive Portal services that are currently running on the grid. The status icon can be one of the following:

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

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

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

When you select **Only show members with service warnings or errors**, the widget displays only the members that have service errors. The widget does not display any data in the member table if all the services on all members are running properly.

You can click a member link to monitor the detailed status of the selected member. Grid Manager displays the Grid tab -> Member tab. For information, see Member Status on page 298.
Member Status (System Status)

The Member Status widget provides status information about the system resources and services of a grid member. The System Status widget provides the operational status about an independent appliance. Add a Member Status widget to your Dashboard for each grid member that you want to monitor. The widget always displays the services that a grid member is running. You can then configure it to display additional information and specify how the information is displayed.

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

- **For Member Status widget only**: Click **Select Member** to select a grid member for display.
- **Select the information you want to display**:
  - **Show Role**: For Member Status widget only. Click to display whether the appliance is a grid master, grid master candidate, or grid member. An independent appliance does not have a Grid license installed.
  - **Show Hardware Type**: Click to display the appliance hardware model.
  - **Show HA Status**: Click to display whether the appliance is part of an HA pair. It displays one of the following:
    - **Standalone**: The grid member is an independent appliance.
    - **HA OK**: The grid member is part of an HA pair that is functioning properly.
    - **HA Broken**: The appliance is part of an HA pair that is not operating properly. You can check the logs to determine the problem.
  - **Show System Uptime**: Click to display the duration of time (days, hours, and minutes) that the grid member has been up and running.
- **Statistics**: Select the data that you want to display and its format:
  - **CPU**: Click to display the percentage of CPU that is in use. Select either Dial or Bar for the display format.
  - **Memory**: Click to display the current percentage of memory that is in use. Select either Dial or Bar for the display format.
  - **Database**: Click to display the percentage of the database that is in use. Select either Pie or Bar for the display format.
  - **Disk**: Click to display the percentage of the data partition on the hard disk drive in use. Select either Pie or Bar for the display format.
  - **System Temperature**: Click to display the system temperature. Depending on the hardware model, the system temperature may not be available. Select to display the temperature in either **Celsius** or **Fahrenheit**.
  - **CPU Temperature**: Click to display the CPU temperature. Depending on the hardware model, the CPU temperature may not be available. Select to display the temperature in either **Celsius** or **Fahrenheit**.

Click the Configuration icon again to hide the configuration panel after you complete the modification.
Grid Manager displays the hostname of the appliance at the top of the widget. You can click the name link to view detailed information about the appliance. It also displays the service status of the following: FTP, TFTP, HTTP (File Distribution), DNS, DHCP, NTP, bloxTools, Captive Portal, and IF-MAP (for IF-MAP server only) in the Services section. The service status can be one of the following:

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

The widget also displays the statistics you specified, such as CPU usage, memory and database usage, in the format you selected.

**DNS Statistics**

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

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

- Click *Select Member*. In the *Member Selector* dialog box, choose a grid member to display statistics for all its stub zones and authoritative zones.
- or
- Click *Select Zone*. In the *Zone Selector* dialog box, choose a DNS zone to display statistics for that zone only.

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

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

The widget displays the following information:

- **DNS Responses** tab: Displays a pie chart and the total number of each type of message. It also displays the total number of full and incremental zone transfers that the grid member performed.
- **Responses per Second** tab: Displays a line graph that tracks the DNS responses received per second, within an hour. The time is displayed according to the time zone specified in the User Profile. If the auto-detect time zone option is enabled and Grid Manager cannot determine the browser time zone, then the time is displayed in UTC format. You can mouse over the graph to display the coordinates of any point in the graph.
The Dashboard

Ranges Over Threshold

The *Ranges Over Threshold* widget enables you to monitor DHCP range usage from your Dashboard. It lists the DHCP ranges that are allocated above a specified threshold and thus may warrant your attention. The default threshold is 75%. For information, see *Configuring Thresholds for DHCP Ranges* on page 634. Note that the appliance highlights disabled DHCP ranges in gray.

The widget displays the DHCP ranges with utilization percentages that surpass the threshold.

To configure the *Ranges Over Threshold* widget, click the Configure icon and do the following:

- **Network View**: Select a network view in which you want to monitor the DHCP ranges. This field is displayed only when you have more than one network view.
- **Threshold**: Enter a new threshold value. The default is 75%

In addition, you can do the following:

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

Failover Associations Status

The *Failover Associations Status* widget enables you to monitor the status of the failover associations from your Dashboard. It lists all the failover associations in the grid and displays their names and status. The widget also displays the primary and secondary servers in the association. When you click a failover association link or a status link, Grid Manager displays the Failover Association section where you can get detailed information about the failover association. For information, see *Monitoring Failover Associations* on page 660.

In addition, you can do the following:

- Click the Export button to export the list of failover associations to a file in CSV format.
- Click the Refresh button to refresh the data in the list.

DHCP Statistics

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

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

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

- **Select Member**: In the *Member Selector* dialog box, select a grid member from the list.
- **Graph Configuration**: Select which messages you want to track in the *Messages per Second* graph.
  - **Discovers**: The number of DHCPDISCOVER messages that the grid member received from DHCP clients. A DHCP client broadcasts a DHCPDISCOVER message to obtain an IP address.
  - **Offers**: The number of DHCPOFFER messages that the grid member sent to DHCP clients. If the grid member has an IP address that it can allocate to the DHCP client that sent the DHCPDISCOVER message, the grid member responds with a DHCPOFFER message that includes the IP address and configuration information.
  - **Requests**: The number of DHCPREQUEST messages that the grid member received from DHCP clients. A DHCP client sends DHCPREQUEST messages when it selects a lease, connects to the network, and if it renews the lease.
  - **Acks**: The number of DHCPACK messages that the grid member sent to DHCP clients. When the grid member receives a DHCPREQUEST message, it responds with a DHCPACK message to confirm the IP address selected by the DHCP client.
  - **Nacks**: The number of DHCPNACK messages that the grid member sent to DHCP clients. The grid member sends a DHCPNACK message when a DHCP client requests an IP address that is not valid for the network.
— **Declines**: The number of DHCPDECLINE messages that the grid member received. DHCP clients send DHCPDECLINE messages to a DHCP server when it discovers that the IP address offered by a DHCP server is already in use.

— **Informs**: The number of DHCPINFORM messages that the grid member received. A client that did not receive its IP address from the DHCP server can send it a DHCPINFORM message to retrieve configuration parameters, such as the IP addresses of DNS servers in the network.

— **Releases**: The number of DHCPRELEASE messages that the grid member received. A DHCP client sends a DHCPRELEASE message when it terminates its lease and releases its IP address.

The widget displays the following information:

- **DHCP Messages** tab: Displays a pie chart and the totals for each type of DHCP message. It also displays the number of Deferred Updates, which are DDNS update requests from clients to defer applying a delete operation to a zone.

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

### Network Statistics

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

Add a **Network Statistics** widget to your Dashboard for each network that you want to monitor. You can monitor both IPv4 and IPv6 networks.

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

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

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

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

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

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

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

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

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

**Networks Over Threshold**

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

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

To configure the *Networks Over Threshold* widget, click the Configure icon, and then complete the following:

- **Network View:** This field appears only if you have more than one network view. Select the network view in which you want to monitor the threshold.
- **Threshold:** Enter a new threshold value. The default is 75%.
- **Type:** Select IPAM Utilization or DHCP Utilization. For information, see *Managing DHCP Data* on page 589.

In addition, you can do the following:

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

**Discovery Status**

The appliance can run an IP discovery to detect and obtain information about active hosts in specified networks. It can also run a VM discovery to detect virtual entities on VMware vSphere servers. For information about the discovery process, see *Chapter 33, Network Discovery,* on page 805.

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

- Click the Start button to start a discovery process.
- Click the Pause button to temporarily pause the process.
- Click the Stop button to stop the process.

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

The widget displays the following information about the discovery process:

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

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

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

• **Conflicts**: The number of discovered hosts that have a MAC address conflict or are part of a configured DHCP range, but do not have a fixed address or lease record and are not part of an exclusion range.

**My Commands**

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

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

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

**DDNS Statistics**

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

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

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

• Click **Select Member**. In the *Member Selector* dialog box, select a grid member from the list.

• **Graph Configuration**: Select which updates you want to track in the **Updates per Second** graph:

  — **Success**: The number of DDNS update requests that succeeded.
  — **Prerequisite Reject**: The number of DDNS update requests that were rejected because the prerequisite conditions specified in the request were not met.
  — **Reject**: The number of DDNS update requests that were rejected by the DNS service.
  — **Failure**: The number of DDNS update requests that failed.

The widget displays the following information:

• **DDNS Updates** tab: Displays totals for each type of update.

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

**System Activity Monitor**

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

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

• Click **Select Member**. In the *Member Selector* dialog box and select a grid member from the list.

• **CPU**: Select which type of CPU usage you want to track:

  — **User**: The CPU usage of user applications, such as programs and libraries.
  — **System**: The CPU usage of the kernel and drivers.
  — **Idle**: The percentage of CPU that is not in use.

• **System Memory**: Select which portion of the system memory you want to track:

  — **Real Memory Used**: The physical RAM usage.
The Dashboard

- **Swap Used**: The swap area usage. The swap area is the disk area that temporarily holds a process memory image.

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

- **NIC Settings**: Select the port on which you want to measure network traffic: LAN, LAN2, HA, or MGMT.

The System Activity Monitor widget displays a tab for each resource: CPU, System Memory, and NIC Usage. Each tab contains a line graph that tracks the resource utilization per second. The graph in the CPU tab tracks the percentage of CPU usage. The graph in the System Memory tab tracks the memory utilization percentage. The graph in the NIC Usage tab tracks either bytes or packets per second.

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

### File Distribution Statistics

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

The service status displays one of the following:

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

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

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

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

The File Distribution Statistics widget displays the following information:

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

### Active WebUI Users

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

You can add only one Active WebUI Users widget to the Dashboard. You must have a superuser account to add this widget to the Dashboard.

It displays the following information about each user:

- **User ID**: The user name.
- **Source Address**: The IP address of the management station the user used to connect to Grid Manager.
- **Logged In Since**: The date and time the user logged in.
- **Idle Time**: The number of minutes the user has not had any activity on Grid Manager.
- **User Agent**: The system used to access Grid Manager, such as the browser version and platform information.

You can sort the columns and hide or display each one. You can also export the list to a .csv file.
Microsoft Servers Status Widget

The *Microsoft Servers Status* widget displays the operational status of each Microsoft server managed by the grid. Grid Manager displays this widget only when at least one member in the grid has a Microsoft management license. You can configure this widget to display the status of all Microsoft servers or only those with warnings and errors. To modify the *Microsoft Servers Status* widget, click the Configure icon and select one of the following:

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

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

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

The DNS service status can be one of the following:

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

- **DHCP**: The status of the DHCP service on the Microsoft server.

The DHCP service status can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Green]</td>
<td>Green</td>
<td>The DHCP service is functioning properly.</td>
</tr>
<tr>
<td>![Red]</td>
<td>Red</td>
<td>The DHCP service is stopped.</td>
</tr>
<tr>
<td>![Yellow]</td>
<td>Yellow</td>
<td>The DHCP service is starting or stopping.</td>
</tr>
<tr>
<td>![Gray]</td>
<td>Gray</td>
<td>Management of the Microsoft DHCP server is disabled.</td>
</tr>
</tbody>
</table>
Chapter 3  Smart Folders

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

- *About Smart Folders* on page 68
  - *Global Smart Folders* on page 69
  - *My Smart Folders* on page 69
- *Creating Smart Folders* on page 70
- *Viewing and Modifying Data in Smart Folders* on page 71
- *Modifying Smart Folders* on page 72
- *Deleting Smart Folders* on page 72
- *Saving a Copy of a Smart Folder* on page 72
- *Printing and Exporting Data in Smart Folders* on page 73
About Smart Folders

Use smart folders to organize your core network services data. Depending on your administrative roles and business needs, you can filter your data by object types, names, extensible attributes, and discovered data such as conflicts, unmanaged data, or the virtual entity data, and then place the filtered results in a smart folder. You can also group the filtered results by defining up to 10 extensible attributes as the Group By rules. For example, you can create a smart folder that contains all the networks you manage in Belgium, and then group the networks by building number, as illustrated in Figure 3.1.

Once you set up a smart folder, the appliance displays up-to-date information based on your filter and grouping criteria each time you access the folder. You can also view and modify object information in the folder. For information, see Viewing and Modifying Data in Smart Folders on page 71. With smart folders, you can organize your data in a meaningful way and quickly obtain the information you need to perform specific tasks without searching the entire database.

**Figure 3.1 Creating Smart Folders**

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

Before you set up your smart folders, decide how you want to organize your data. You can specify search and Group By criteria to help you group information in a meaningful way. Note that a smart folder becomes invalid when you delete an extensible attribute that the folder uses as a filter or Group By criterion. You must redefine the extensible attribute and reconfigure the folder criteria to validate the smart folder.

In Grid Manager, you can create smart folders in both the Global Smart Folders and My Smart Folders panels. In Global Smart Folders, you can create smart folders to which other administrators can create links. Only administrators with superuser accounts can create, edit, and delete global smart folders. For information, see Global Smart Folders on page 69. You can create personal folders as well as links to global smart folders in My Smart Folders. For information, see My Smart Folders on page 69.

Each smart folder you create can contain up to 2,000 objects. When the number of objects exceeds 2,000, Grid Manager sorts and displays the first 2,000 objects only. It also displays a warning message at the top of the panel. In this case, you may want to redefine your filter criteria to further refine the filtered data in your smart folders.
To create smart folders, follow these procedures:

1. Determine how you want to organize your core network services data.

2. Identify the fields that you want to use to group networks or define extensible attributes for the data that you want to track. For information about extensible attributes, see About Extensible Attributes on page 222.

   **Note:** Infoblox strongly recommends that you use **Type** as one of the filter criteria to improve system performance.

3. Create smart folders in either the My Smart Folders or Global Smart Folders panel. For information, see Creating Smart Folders on page 70.

### Global Smart Folders

You can create global smart folders to share among administrators. You must log in as a superuser account to create, edit, and delete global smart folders. All other users have read-only access to global smart folders. You can create as many folders as you need in Global Smart Folders. You can also save a local copy of an existing folder, depending on your administrative permissions. For information, see Saving a Copy of a Smart Folder on page 72.

Grid Manager displays a list of global smart folders in the list panel.

When you log in as a superuser and mouse over a global smart folder, the following icons appear:

- **Information**: Displays information about the selected smart folder. Information includes comments and filter criteria for the folder. It also displays the Group By rules.
- **Edit**: Click this icon to edit the definition and filter criteria for the smart folder.
- **Create link**: Click this icon to create a link to the smart folder. The link to this folder is placed in My Smart Folders.
- **Delete**: Click this icon to delete the smart folder. This operation does not affect the objects that are in the folder. Only the smart folder is deleted.

### My Smart Folders

In My Smart Folders, you can create personal smart folders and links to global smart folders. You can create up to 200 smart folders, including links to global smart folders. When you create links to global smart folders, you can only view information in the folders. However, you can create a local copy of the global smart folder in its current state for editing purposes. Note that when the original global smart folder is updated, information in your local copy is not updated. For information, see Saving a Copy of a Smart Folder on page 72. When you delete a link to a global smart folder in this tab, only the link is deleted. There is no impact on the information in the original global smart folder.

Grid Manager displays a list of smart folders in the list panel. The same list of smart folders is also displayed in the Finder panel. For information, see Using the Finder Panel on page 46.

When you mouse over a smart folder in the list panel, the following icons appear:

- **Information**: Displays information about the selected smart folder. Information includes comments and filter criteria of the folder. It also displays how you grouped the filtered data.
- **Edit**: Click this icon to edit the definition and filter criteria for the smart folder.
- **Delete**: Click this icon to delete the smart folder. This operation does not affect the objects or networks that are in the folder. Only the smart folder is deleted.
Creating Smart Folders

You can create personal smart folders in My Smart Folders. You can also create global folders to share among administrators in Global Smart Folders when you log in as a superuser account. Each time you access a smart folder, you obtain up-to-date information about the core network services data that match the filter criteria you set for the folder. Grid Manager displays a hierarchical view of the smart folder using the Group By rules you define.

To create a smart folder:

1. Click the Smart Folders tab.
2. Click the My Smart Folders tab to create a personal smart folder. 
   or
   If you logged in with a superuser account, click the Global Smart Folders tab to create a global smart folder.
3. Click Create.
4. In the Smart Folder data panel, complete the following:
   - Name: Enter the name of the smart folder.
   - Comment: Optionally, enter additional information about the smart folder.
   - In the first drop-down list, select a field as the filter. You can select a network view or a record type as the filter. Grid Manager highlights extensible attributes in gray. You can also group the default data by adding a Group By rule without adding a filter. The default filter is “Type equals Network/Zone/Range/Member”.
     Note: Infoblox strongly recommends that you use Type as the first filter criterion to improve system performance.
   - In the second drop-down list, select an operator for the filter.
   - Enter or select a value for the selected field and operator. Depending on the field and operator that you select, the field can be a text or an integer field. It can also be a drop-down list or a calendar widget. The default is Network/Zone/Range/Member if you select Type in the first field. Grid Manager displays all the networks, zones, DHCP ranges, and members in the results table.
   - Optionally, click + to add another filter. You can also click Apply to view the filtered data in the results table.
   - Optionally, select the Group Results check box to organize the filtered data. You can also disable a Group By filter by deselecting the check box.
   - From the Group by drop-down list, select an extensible attribute by which you want to group the filtered data. For example, if you want to group the filtered data by building number, you can select Building from the drop-down list. To add additional Group By rules, click the + icon, and then select a field from the drop-down list. You can apply up to 10 Group By rules. You can also delete a rule by selecting the rule and clicking the - icon.
   - When you finish adding all filter criteria and Group By rules, click Apply. Grid Manager displays the filtered data in the results table. Note that in the Name field, the appliance highlights disabled DHCP objects in gray. A DHCP object can be a DHCP range, fixed address, reservation, host configured for DHCP, or roaming host with an allocated IP address.
5. Click Save to save the smart folder.
**Viewing and Modifying Data in Smart Folders**

After you set up a smart folder, the appliance searches for matching objects based on the filter criteria you specified for the folder. Grid Manager also groups the objects by the Group By rules you specify. Each smart folder you create can contain up to 2,000 objects. When the number of objects exceeds 2,000, Grid Manager sorts and displays the first 2,000 objects and a message at the top of the panel. In this case, you may want to redefine your filter criteria to further refine the filtered data in your smart folders.

Grid Manager displays smart folders hierarchically in a tree view based on your Group By rules in the following:

- Smart Folder section in the Finder panel
- Selectors from which you can select a smart folder

In the smart folder list panel however, Grid Manager displays all the smart folders in a flat list.

In the smart folder data panel, Grid Manager displays the first hierarchical level of the smart folder based on your Group By rules. If you do not configure any Group By rule, Grid Manager displays all the objects in the data panel.

Depending on your Group By rules, you can view detailed information about the objects by clicking the object link and drilling down to the lowest hierarchical level, and then opening an object. To go back to a previous hierarchical view, click the link of the corresponding level in the breadcrumb.

To view detailed information about an object:

1. In the Smart Folder data panel, click the object link until you drill down to the last hierarchical level of the folder.
2. Grid Manager displays the following information:
   - **Name:** The name or IP address of the object. The appliance highlights disabled DHCP objects in gray. A DHCP object can be a DHCP range, fixed address, reservation, host configured for DHCP, or roaming host with an allocated IP address.
   - **Comment:** Information about the object.
   - **Type:** The object type.
   - **Site:** The site to which the object belongs. This is one of the predefined extensible attributes.

   You can also select other available extensible attributes for display, and sort the data in ascending or descending order by column.

3. Select an object check box, and then do one of the following:
   - Click the Open icon to display the data in the network list or IP address list.
   - Click the Edit icon to modify or schedule the modification of the object configuration. Grid Manager displays the corresponding editor depending on the object you select.
   - Click the Delete icon to delete the object or click the Schedule Deletion icon to schedule the deletion of the object.

You can also print or export the data in this panel. For information, see *Infoblox Grid Manager* on page 31.
**Modifying Smart Folders**

After you create a smart folder, you can modify its filter and grouping criteria. To modify a smart folder:

1. Go to **Smart Folders**.
2. Click **My Smart Folders** to modify personal smart folders.
   or
   Click **Global Smart Folders** to modify global smart folders if you logged in with a superuser account.
3. Mouse over to the smart folder that you want to modify.
4. Click the Edit icon. You can also click the Edit icon next to the name of the smart folder in the data panel.
5. Make the appropriate changes in the Smart Folder data panel as described in *Creating Smart Folders* on page 70.

**Deleting Smart Folders**

You can delete personal smart folders in My Smart Folders. However, you must log in as a superuser account to delete global smart folders.

To delete a smart folder:

1. Click the **Smart Folders** tab.
2. Click the **My Smart Folders** tab to delete personal smart folders.
   or
   Click the **Global Smart Folders** tab to delete global smart folders.
3. Mouse over to the smart folder that you want to delete.
4. Click the Delete icon. In the **Delete Smart Folder** dialog box, click **Yes**.

**Saving a Copy of a Smart Folder**

You can make a copy of an existing smart folder, add or change filter criteria, and then rename the folder accordingly. You can also create a local copy of the global smart folder in its current state for editing purposes. In My Smart Folders, you can save a folder copy only in My Smart Folders. In Global Smart Folders however, you can save a folder copy in either My Smart Folders or Global Smart Folders. You must have superuser permissions to save a global smart folder copy in Global Smart Folders. Note that when the original global smart folder is updated, information in your local copy is not updated.

To save a copy of a smart folder:

1. Click **My Smart Folders** to save a folder copy in this tab.
   or
   Click **Global Smart Folders** to save a folder copy in either this tab or My Smart Folders. To save a smart folder copy in Global Smart Folders, log in as a superuser account.
2. Select the smart folder that you want to save as a copy.
3. Click **Save copy as**.
4. Grid Manager saves the folder copy in My Smart Folders when you save the folder copy in this tab.
   or
   The Save Smart Folder As dialog box appears when you perform this function in Global Smart Folders. Select
   one of the following:
   — **My Smart Folders**: Saves the copy in My Smart Folders.
   — **Global Smart Folders**: Saves the copy in Global Smart Folders.
   Click OK.

   **Note**: For the folder copy, the appliance appends the word Copy to the original name of the smart folder. You can
   change the name of the folder at anytime by editing the folder.

---

**PRINTING AND EXPORTING DATA IN SMART FOLDERS**

You can print the list of networks that are on the current smart folder page, or you can export all the data in CSV
(comma separated value) format. For information, see *About Long Running Tasks* on page 52 and *Exporting Data from
Grid Manager* on page 53.
PART 2 APPLIANCE ADMINISTRATION

This section provides information about configuring and managing a grid or an independent appliance. It includes the following chapters:

- Chapter 4, Managing Administrators, on page 77
- Chapter 5, Deploying a Grid, on page 131
- Chapter 6, Deploying Independent Appliances, on page 171
- Chapter 7, Managing Appliance Operations, on page 201
- Chapter 8, File Distribution Services, on page 265
- Chapter 9, Managing NIOS Software and Configuration Files, on page 273
- Chapter 10, Monitoring the Appliance, on page 297
- Chapter 11, Monitoring with SNMP, on page 321
- Chapter 12, bloxTools Environment, on page 375
Chapter 4  Managing Administrators

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

- **About Admin Accounts** on page 79
- **About Admin Groups** on page 81
  - *Creating Superuser Admin Groups* on page 82
  - *Creating Limited-Access Admin Groups* on page 82
- **About Admin Roles** on page 84
  - *Creating Admin Roles* on page 84
- **Managing Admin Groups and Admin Roles** on page 85
  - *Modifying Admin Groups and Roles* on page 85
  - *Deleting Admin Groups and Roles* on page 86
  - *Viewing Admin Groups* on page 86
  - *Viewing Admin Roles* on page 86
  - *Viewing Admin Group Assignments* on page 86
- **About Administrative Permissions** on page 87
  - *Defining Global Permissions* on page 88
  - *Defining Object Permissions* on page 88
  - *Applying Permissions and Managing Overlaps* on page 91
  - *Managing Permissions* on page 93
- **Authenticating Administrators** on page 95
- **Creating Local Admins** on page 95
  - *Modifying and Deleting Admin Accounts* on page 96
- **About Remote Admins** on page 97
- **Authenticating Using RADIUS** on page 99
  - *Remote RADIUS Authentication* on page 100
  - *Configuring a RADIUS Authentication Server Group* on page 100
  - *Managing the RADIUS Server List* on page 102
  - *Disabling RADIUS Servers on NIOS* on page 102
  - *Configuring Remote RADIUS Servers* on page 102
  - *Configuring Admin Groups on the Remote RADIUS Server* on page 103
  - *Configuring Remote Admin Accounts on the Remote RADIUS Server* on page 103
  - *Authorization Groups Using RADIUS* on page 103
  - *Accounting Activities Using RADIUS* on page 103
Managing Administrators

- Authenticating Admin Accounts Using Active Directory on page 104
  - Admin Authentication Using Active Directory on page 105
  - Configuring an Active Directory Authentication Service Group on page 105
  - Managing the Domain Controller List on page 106
  - Disabling Domain Controllers on page 106
- Defining the Authentication Policy on page 107
  - Configuring a List of Authentication Methods on page 107
  - Configuring a List of Remote Admin Groups on page 107
- Changing Password Length Requirements on page 108
- Notifying Administrators on page 109
- Administrative Permissions for Common Tasks on page 110
- Administrative Permission for the Grid on page 111
  - Administrative Permissions for Grid Members on page 111
  - Administrative Permissions for Network Discovery on page 112
  - Administrative Permissions for Scheduling Tasks on page 113
  - Administrative Permissions for Microsoft Servers on page 114
- Administrative Permissions for IPAM Resources on page 115
  - Administrative Permissions for IPv4 and IPv6 Networks on page 115
  - Administrative Permissions for Hosts on page 115
- Administrative Permissions for DNS Resources on page 116
  - Administrative Permissions for DNS Views on page 117
  - Administrative Permissions for Zones on page 118
  - Administrative Permissions for Resource Records on page 119
  - Administrative Permissions for Shared Record Groups on page 120
- Administrative Permissions for DHCP Resources on page 121
  - Administrative Permissions for Network Views on page 122
  - Administrative Permissions for Networks and Shared Networks on page 123
  - Administrative Permissions for Fixed Addresses and Reservations on page 125
  - Administrative Permissions for DHCP Ranges on page 126
  - Administrative Permissions for DHCP Templates on page 127
  - Administrative Permissions for MAC Address Filters on page 128
  - Administrative Permissions for the DHCP Lease History on page 129
- Administrative Permissions for File Distribution Services on page 130
About Admin Accounts

A user must have an admin account to log in to the NIOS appliance. Each admin account belongs to an admin group, which contains roles and permissions that determine the tasks a user can perform. For information, see About Admin Groups on page 81.

When an admin connects to the appliance and logs in with a username and password, the appliance starts a two-step process that includes both authentication and authorization. First, the appliance tries to authenticate the admin using the username and password. Second, it determines the authorized privileges of the admin by identifying the group to which the admin belongs. It grants access to the admin only when it successfully completes this process.

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

The tasks involved in configuring administrator accounts locally and remotely are listed in Table 4.1.

Table 4.1 Storing Admin Accounts Locally and Remotely

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

The admin policy defines how the appliance authenticates the admin: with the local database, RADIUS, or Active Directory. You must add RADIUS or Active Directory as one of the authentication methods in the admin policy to enable that authentication method for admins. See Defining the Authentication Policy on page 107 for more information about configuring the admin policy.
Figure 4.1 illustrates the relationship of local and remote admin accounts, admin policy, admin groups, and permissions and properties.

**Figure 4.1 Privileges and Properties Applied to Local and Remote Admin Accounts**

Complete the following tasks to create an admin account:

1. Use the default admin group or create an admin group. See About Admin Groups on page 81.
2. Define the administrative permissions of the admin group. See About Administrative Permissions on page 87.
3. Create the admin account and assign it to the admin group.
   - To add the admin account to the local database, see Creating Local Admins on page 95.
   - To configure the appliance to authenticate the admin account stored remotely, see About Remote Admins on page 97.
About Admin Groups

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

There are three types of admin groups:

- **Superuser** – Superuser admin groups provide their members with unlimited access and control of all the operations that a NIOS appliance performs. There is a default superuser admin group, called `admin-group`, with one superuser administrator, `admin`. You can add users to this default admin group and create additional admin groups with superuser privileges. Superusers can access the appliance through its console, GUI, and API. In addition, only superusers can create admin groups.

- **Limited-Access** – Limited-access admin groups provide their members with read-only or read/write access to specific resources. These admin groups can access the appliance through the GUI, API, or both. They cannot access the appliance through the console.

- **Default** – When upgrading from previous NIOS releases, the appliance converts the ALL USERS group to the Default Group when the ALL USERS Group contains admin accounts. The appliance does not create the Default Group if there is no permission in the ALL USERS group. The permissions associated with the ALL USERS group are moved to a newly created role called Default Role. Supported in previous NIOS releases, the ALL USERS group was a default group in which you defined global permissions for all limited-access users. This group implicitly included all limited-access users configured on the appliance.

All limited-access admin groups require either read-only or read/write permission to access certain resources, such as grid members, and DNS and DHCP resources, to perform certain tasks. Therefore, when you create an admin group, you must specify which resources the group is authorized to access and their level of access.

Only superusers can create admin groups and define their administrative permissions. There are two ways to define the permissions of an admin group. You can create an admin group and assign permissions directly to the group, or you can create roles that contain permissions and assign the roles to an admin group.

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

1. Create an admin group, as described in `Creating Limited-Access Admin Groups` on page 82.
2. Assign permissions to the admin group, as described in `About Administrative Permissions` on page 87.

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

1. Create an admin role, as described in `About Admin Roles` on page 84.
2. Define permissions for the newly created admin role, as described in `Creating Admin Roles` on page 84.
3. Create an admin group and assign the role to the group, as described in `Creating Limited-Access Admin Groups` on page 82.

After you have created admin groups and defined their administrative permissions, you can assign administrators to the group.

- For local admins, see `Creating Local Admins` on page 95.
- For remote admins, see `About Remote Admins` on page 97.
Creating Superuser Admin Groups

Superusers have unlimited access to the NIOS appliance. They can perform all the operations that the appliance provides. There are some operations, such as creating admin groups and roles, that only superusers can perform.

Note that there must always be one superuser admin account, called “admin”, stored in the local database to ensure that at least one administrator can log in to the appliance in case the NIOS appliance loses connectivity to the remote admin databases such as RADIUS servers or AD domain controllers.

There is a default superuser admin group (admin-group). You can create additional superuser admin groups, as follows:

1. From the Administration tab, select the Administrators tab -> Groups tab, and then click the Add icon.
2. In the Add Admin Group wizard, complete the following:
   - **Name**: Enter a name for the admin group.
   - **Comment**: Enter useful information about the group, such as location or department.
   - **Disable**: Select this to retain an inactivated profile for this admin group in the configuration. For example, you may want to define a profile for recently hired administrators who have not yet started work. Then when they do start, you simply need to clear this check box to activate the profile.
3. Click **Next** and complete the following:
   - **Superusers**: Select this to grant the admin accounts that you assign to this group full authority to view and configure all types of data and perform all tasks.
4. Optionally, click **Next** to add extensible attributes to the admin group. For information, see *Managing Extensible Attribute Values* on page 72.
5. Select one of the following:
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and continue to edit.
   - **Save & New**: Save the entry and open a new wizard.

You can do one of the following after you create a superuser admin group:

- Add local admins to the superuser group. For information, see *Creating Local Admins* on page 95.
- Assign the superuser group to remote admins. For information, see *About Remote Admins* on page 97.

Creating Limited-Access Admin Groups

When you create a limited-access admin group, you can assign roles to it. The group then inherits the permissions of its assigned roles. In addition, you can assign permissions directly to the group. Only superusers can create admin groups.

To create a limited-access admin group:

1. From the Administration tab, select the Administrators tab -> Groups tab, and then click the Add icon.
2. In the Add Admin Group wizard, complete the following:
   - **Name**: Enter a name for the admin group.
   - **Comment**: Enter useful information about the group, such as location or department.
   - **Disable**: Select this to retain an inactivated profile for this admin group in the configuration. For example, you may want to define a profile for recently hired administrators who have not yet started work. Then when they do start, you simply need to clear this check box to activate the profile.
3. Click **Next** and complete the following:
   - **Superusers**: Clear this check box to create a limited-access admin group.
   - **Roles**: Optionally, click the Add icon to add an admin role to the admin group. In the *Role Selector* dialog box, select the roles you want to assign to the admin group, and then click the Select icon. Use Shift+click and Ctrl+click to select multiple admin roles. You can assign up to 21 roles to an admin group. The appliance displays the selected roles in the list box.
When an admin group is assigned multiple roles, the appliance applies the permissions to the group in the order the roles are listed. Therefore if there are overlapped permissions among the roles, the appliance uses the permission from the role that is listed first and ignores the others. You can reorder the list by selecting a role and clicking the arrow keys to move the role up and down the list. To delete a role, select it and click the Delete icon.

— **Allowed Interfaces:** Specify whether the admin group can use the Grid Manager GUI and the API (application programming interface) to configure the appliance.
  — **GUI:** Select this to allow the admin group to use the GUI.
  — **API:** Select this to allow the admin group to use the API.

4. Optionally, click **Next** to add or delete extensible attributes for this admin group. For information, see *Managing Extensible Attribute Values* on page 72.

5. Select one of the following:
   — **Save & Close:** Save the entry and close the wizard.
   — **Save & Edit:** Save the entry and continue to edit.
   — **Save & New:** Save the entry and open a new wizard.
ABOUT ADMIN ROLES

An admin role is a group of permissions that you can apply to one or more admin groups. Roles allow you to quickly and easily apply a suite of permissions to an admin group. You can define roles once and apply them to multiple admin groups. The appliance contains the following system-defined admin roles:

- **DHCP Admin**: Provides read/write access to all network views, all DHCP MAC filters, all grid members, and all Microsoft servers that are managed by the grid. It also provides read-only access to all DHCP templates and DHCP lease history.
- **DNS Admin**: Provides read/write access to all grid members, all Microsoft servers that are managed by the grid, all shared record groups, and all DNS views.
- **File Distribution Admin**: Provides read/write access to grid file distribution properties.
- **Grid Admin**: Provides read/write access to all DNS views, all shared record groups, all members, all Microsoft servers that are managed by the grid, all network views, all DHCP MAC filters, all DHCP templates, DHCP lease history, Grid File distribution properties, network discovery, and task scheduling.

You can assign these system-defined roles to admin groups and create additional roles based on the job functions in your organization. If you are creating a role that has similar permissions to an existing role, you can copy the role and then make the necessary modifications to the new role. Thus you do not have to create each new role from scratch. You can assign up to 21 roles to an admin group, and you can assign a role to more than one admin group. When you make a change to a role, the appliance automatically applies the change to that role in all admin groups to which the role is assigned.

Creating Admin Roles

There are two ways to create an admin role. You can create a new role and define its permissions, or you can copy an existing role and redefine the configuration for the new role.

To create a new role from scratch:

1. From the Administration tab, select the Administrators tab -> Roles tab, and then click the Add icon.
2. In the Add Role wizard, complete the following:
   - **Name**: Enter a name for the role.
   - **Comment**: Enter useful information about the role. For example, if you are creating a role for IT personnel, you can put the information here.
   - **Disable**: Select this to retain an inactivated profile for this admin role in the configuration.
3. Optionally, click Next to add extensible attributes to this role. For information, see Managing Extensible Attribute Values on page 72.
4. Click Next and select one of the following:
   - **Save & Add Permissions**: Save the entry and add permissions to the role. Grid Manager displays the Permissions tab with the newly created role selected. You can then add permissions to this role. For information, see About Administrative Permissions on page 87.
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and continue to edit.
   - **Save & New**: Save the entry and open a new wizard.
To copy an existing role:

1. From the Administration tab, select the Administrators tab -> Roles tab -> admin_role check box, and then click Clone from the Toolbar.

2. The Copy Role editor provides the following tabs from which you can modify data for the new role:
   - General: Enter the name and information about the new role. You can also disable the role in this tab.
   - Admin Groups: Displays a list of admin groups that are currently using this role. You cannot modify the list.
   - Extensible Attributes: Add and delete extensible attributes that are associated with the admin role. You can also modify the values of the extensible attributes. For information, see Managing Extensible Attribute Values on page 72.

3. Click Save & Close or Save to save the new role.

The appliance displays the new role in the Roles tab.

After you create roles, you can do the following:

- Define their permissions. For information and guidelines on defining permissions, see About Administrative Permissions on page 87.
- Assign roles to admin groups, as described in Creating Limited-Access Admin Groups on page 82.

---

**MANAGING ADMIN GROUPS AND ADMIN ROLES**

After you create an admin group or an admin role, you can view, modify, and delete it.

**Modifying Admin Groups and Roles**

To modify an admin group:

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

2. The Admin Group editor provides the following tabs from which you can modify data:
   - General: You can modify the following data.
     - Name: Modify the name of the admin group.
     - Comment: Enter useful information about the group, such as location or department.
     - Disable: Select this to retain an inactivated profile for this admin group in the configuration. For example, you may want to define a profile for recently hired administrators who have not yet started work. Then when they do start, you simply need to clear this check box to activate the profile.
   - Roles: Modify the data as described in Creating Limited-Access Admin Groups on page 82.
   - Extensible Attributes: Add and delete extensible attributes that are associated with the admin group. You can also modify the values of the extensible attributes. For information, see Managing Extensible Attribute Values on page 72.

3. Click Save & Close or Save to save the changes.
Deleting Admin Groups and Roles

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

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

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

Viewing Admin Groups

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

Grid Manager displays the following information:
- **Name**: The name of the admin group.
- **Superuser**: Indicates whether the admin accounts that you assign to this group have full authority to view and configure all types of data. The value can be Yes or No.
- **Comment**: The information about the admin group.

You can select the additional fields, Disabled and Site, for display. You can also sort the data in ascending or descending order by column.

Viewing Admin Roles

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

Grid Manager displays the following information:
- **Name**: The name of the admin role.
- **System**: Indicates whether the admin role is system defined or not. The value can be Yes or No.
- **Comment**: The information about the admin role.

You can select the additional fields, Disabled and Site, for display. You can also sort the data in ascending or descending order by column.

Viewing Admin Group Assignments

After you define permissions for an admin role, you can assign it to multiple admin groups. You can view the list of admin groups to which an admin role is assigned, as follows:
1. From the Administration tab, select the Administrators tab -> Roles tab -> admin_group check box, and then click the Edit icon.
2. In the Role editor, select the Admin Groups tab.

Grid Manager displays the list of admin groups to which the role is assigned.
About Administrative Permissions

You can assign permissions to admin roles which you then assign to admin groups, or you can assign permissions directly to an admin group. The following are permissions you can grant admin groups and roles:

- **Read/Write (RW):** Allows admins to add, modify, delete, view, and search for a resource.
- **Read-Only (RO):** Allows admins to view and search for a resource. Admins cannot add, modify, or delete the resource.
- **Deny:** Prevents admins from adding, modifying, deleting, and viewing a resource. This is the default permission level for all resources.

By default, the superuser group (admin-group) has full access to all the following groups of resources. However, limited-access admin groups must have either read-only or read/write permission to access the following resources in order to perform certain tasks.

- **Grid members:** Includes grid members, Microsoft servers that are managed by the grid, network discovery, and task scheduling.
- **IPAM resources:** Includes network views, IPv4 and IPv6 networks, and host records.
- **DHCP resources:** Includes network views, IPv4 networks, host records, DHCP ranges, DHCP fixed addresses/reservations, Mac filters, shared networks, DHCP templates, lease history, and roaming hosts.
- **DNS resources:** Includes DNS views, DNS zones, host records, bulk hosts, all DNS resource records, and all shared records.
- **File distribution resources:** Includes grid-level file distribution properties.

You can define permissions at a global level; for example, for all DNS views or all DHCP networks in the database. You can also define permissions at a more granular level, such as a specific zone, network, and even an individual database object, such as a resource record or fixed address. You can configure global permissions and object permissions for default and custom admin groups and roles, but you cannot define permissions for the factory default roles, such as DHCP Admin.

The appliance applies permissions hierarchically in a parent-child structure. When you define a permission to a resource, the permission applies to all the other resources and objects contained within that resource. For example, if you grant an admin group read/write permission to a network, it automatically has read/write permission to all objects in the network. However, you can override the network-level permission by setting a different permission, read-only or deny, for a fixed address. Permissions to a grid member apply to all zones and resource records served by that grid member, and permissions to a network view apply to all DHCP resources within that view. To override permissions set at a higher level, you must define permissions at a more specific level. To define permissions for a more specific level, see the following:

- Permissions for common tasks, as described in Administrative Permissions for Common Tasks on page 110.
- Permissions for the grid and grid members, as described in Administrative Permission for the Grid on page 111.
- Permissions for IPAM resources, such as IPv6 networks, as described in Administrative Permissions for IPAM Resources on page 115.
- Permissions for DNS resources, such as DNS views and A records, as described in Administrative Permissions for DNS Resources on page 116.
- Permissions for DHCP resources, such as network views and fixed addresses, as described in Administrative Permissions for DHCP Resources on page 121.
- Permissions for file distribution services, as described in Administrative Permissions for File Distribution Services on page 130

When you set permissions that overlap with existing permissions, Grid Manager displays a warning about the overlaps. You can view detailed information and find out which permissions the appliance uses and which ones it ignores. For information, see Applying Permissions and Managing Overlaps on page 91.
Defining Global Permissions

You can define permissions at a global level for an admin group or admin role. To define global permissions:

1. For an admin group: From the Administration tab, select the Administrators tab → Permissions tab → admin_group in the Groups table, and then click the Add icon → Global Permissions from the Create New Permission area or select Add → Global Permissions from the Toolbar.

or

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

2. Grid Manager displays the Manage Global Permissions editor. For an admin group, the appliance displays the selected admin group in the Group Permission field. For an admin role, the appliance displays the selected admin role in the Role Permission field. You can also select a different group or role from the drop-down list.

3. Select the resources that you want to configure from the Permission Type drop-down list. Depending on your selection, Grid Manager displays the corresponding resources for the selected permission type in the table.

4. Select Read/Write, Read-Only, or Deny for the resources you want to configure. By default, the appliance denies access to resources if you do not specifically configure them.

5. Optionally, select additional resources from the Permission Type drop-down list. Grid Manager appends the new resources to the ones that you have already configured. Define the permissions for the resources you select.

6. Click Save & Close or Save to save the permissions.

Defining Object Permissions

You can add permissions to specific objects for selected admin groups or roles. When you add permissions to objects, you can select multiple objects with the same or different object types. When you select multiple objects with the same object type, you can apply permissions to the selected objects as well as the sub object types that are contained in the selected objects. As described in Figure 4.2, when you select five DNS forward-mapping authoritative zones, the appliance displays the object type “AuthZone” for all the zones. Since all five DNS zones are of the same object type, you can also apply permissions to all the resource records in these zones. The appliance displays the resources in the resource section of the Create Object Permissions editor. You can choose one or more of the resources to which you want to apply permissions.
When you select multiple objects with more than one object type, you can add permissions to the selected objects as well as to the sub object types that are common among the selected objects. For example, when you select three DNS forward-mapping authoritative zones and two IPv4 reverse-mapping authoritative zones as illustrated in Figure 4.3, you can apply permissions to all the DNS zones as well as to the CNAME, DNAME, and host records in these zones because CNAME, DNAME, and host records are the common sub object types in these zones.

**Figure 4.2 Selecting Multiple Objects with the Same Object Type**

1. You select five forward-mapping authoritative DNS zones that have resource records such as A records, Hosts, and CNAME records.
2. Since all DNS zones have the same object type, you can apply object permissions to all the DNS zones as well as to all the resource records in the DNS zones.
3. The appliance displays the common resources in the **Resources in Selected Objects** column.

When you select multiple objects with more than one object type, you can add permissions to the selected objects as well as to the sub object types that are common among the selected objects. For example, when you select three DNS forward-mapping authoritative zones and two DNS IPv4 reverse-mapping authoritative zones as illustrated in Figure 4.3, you can apply permissions to all the DNS zones as well as to the CNAME, DNAME, and host records in these zones because CNAME, DNAME, and host records are the common sub object types in these zones.

**Figure 4.3 Multiple Objects with Common Sub Object Types**

When you select three DNS forward-mapping authoritative zones and two IPv4 reverse-mapping authoritative zones, you can apply object permissions to all the DNS zones as well as the CNAME, DNAME and Host records in these DNS zones.
To define object permissions for an admin group or role:

1. For an admin group: From the Administration tab, select the Administrators tab \(\rightarrow\) Permissions tab \(\rightarrow\) admin_group in the Groups table, and then click the Add icon \(\rightarrow\) Object Permissions from the Create New Permission area or select Add \(\rightarrow\) Object Permissions from the Toolbar.
   
   or

   For an admin role: From the Administration tab, select the Administrators tab \(\rightarrow\) Permissions tab \(\rightarrow\) admin_role in the Roles table, and then click Add icon \(\rightarrow\) Object Permissions from the Create New Permission area or select Add \(\rightarrow\) Object Permissions from the Toolbar.

2. Grid Manager displays the Create Object Permissions wizard. For an admin group, the appliance displays the selected group in the Group Permission field. For an admin role, the appliance displays the selected admin role in the Role Permission field. You can also select a different group or role from the drop-down list.

3. Click Select Object(s). Grid Manager displays the Object Selector dialog box.

4. In the Object Selector dialog box, complete the following:
   - Enter a value or partial value of an object in the first field. This field is not case-sensitive. For example, if the object to which you want to define permissions contains “Infoblox”, enter Infoblox here.
   - Select the object type for which you are searching in the Type drop-down list. By default, the appliance searches all object types.
   - In the operator drop-down list, select an operator for the filter criteria. Depending on what you select in the first filter field, this list displays the relevant operators for the selection.
   - In the value field, enter or select the attribute value for the first filter field. Depending on what you select for the first two filter fields, you can either enter a value or select a value from a drop-down list.

5. Click Search. The appliance lists all matching objects in the table. You can select multiple object types by clicking the Add icon to add more filter criteria. You can also click Reset to clear all entries.

6. Select the check boxes of the objects to which you are defining permissions, and then click the Select icon.

7. In the Create Object Permissions wizard, do the following:
   - **Object**: Displays the name of the selected object. When you select multiple objects, the appliance displays Multiple here. Mouse over to the information icon to view the list of objects to which you are defining permissions.
   - **Object Type**: Displays the object type of the selected object. When you select more than one object type, the appliance displays Multiple here.
   - **Resource**: Displays the selected objects. When you select more than one object type, the appliance displays Multiple Selected Objects here. Mouse over to the information icon to view the list of objects to which you are defining permissions. Grant the resources an appropriate permission: Read/Write, Read Only, or Deny.

8. After you apply permissions to the selected objects, select one of the following:
   - **Save**: Save the entry and continue to edit.
   - **Save & Close**: Save the entry and close the wizard.

Grid Manager displays a warning message when the permissions you define here overlap with other permissions in the system. Click See Conflicts to view the overlapping permissions in the Permissions Conflict dialog box. For information, see Applying Permissions and Managing Overlaps on page 91.
You can also set permissions for specific objects from the objects themselves. For example, to define permissions for a particular grid member, navigate to that grid member and define its permissions.

To define the permissions of a specific object:

1. Navigate to the object. For example, to define permissions for a particular network, from the Data Management tab, select the IPAM tab -> network check box, and then click the Edit icon.

2. In the editor, select the Permissions tab, and then do one of the following:
   - Click the Add icon to add permission to the object. In the Admin Group/Role Selector dialog box, select an admin group or role to which you want to assign the permission, and then click the Select icon.
   - Modify the permission and resource type of a selected admin group or role.
   - Select an admin group or role and click the Delete icon to delete it.

3. Select one of the following:
   - Save: Save the entry and continue to edit.
   - Save & Close: Save the entry and close the editor.

Applying Permissions and Managing Overlaps

When an admin tries to access an object, the appliance checks the permissions of the group to which the admin belongs. Because permissions at more specific levels override those set at a higher level, the appliance checks object permissions hierarchically—from the most to the least specific. In addition, if the admin group has permissions assigned directly to it and permissions inherited from its assigned roles, the appliance checks the permissions in the following order:

1. Permissions assigned directly to the admin group.
2. Permissions inherited from admin roles in the order they are listed in the Roles tab of the Admin Group editor.

For example, an admin from the DNS1 admin group tries to access the a1.test.com A record in the test.com zone in the Infoblox default view. The appliance first checks if the DNS1 admin group has a permission defined for the a1.test.com A record. If there is none, then the appliance checks the roles assigned to DNS1. If there is no permission defined for the a1.test.com A record, the appliance continues checking for permissions in the order listed in Table 4.2. The appliance uses the first permission it finds.

Table 4.2  Permission Checking

<table>
<thead>
<tr>
<th>The appliance checks object permissions from the most to the least specific, as listed.</th>
<th>For each object, the appliance checks permissions in the order listed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. a1.test.com A record</td>
<td>a. DNS1 admin group</td>
</tr>
<tr>
<td>2. A records in test.com</td>
<td>b. Role 1, Role 2, Role 3...</td>
</tr>
<tr>
<td>3. test.com</td>
<td></td>
</tr>
<tr>
<td>4. All zones in the default view</td>
<td></td>
</tr>
<tr>
<td>5. Default view</td>
<td></td>
</tr>
<tr>
<td>6. All A records</td>
<td></td>
</tr>
<tr>
<td>7. All zones</td>
<td></td>
</tr>
<tr>
<td>8. All DNS views</td>
<td></td>
</tr>
</tbody>
</table>

An admin group that is assigned multiple roles and permissions can have overlaps among the different permissions. As stated earlier, the appliance uses the first permission it finds and ignores the others. For example, as shown in Table 4.3, if an admin group has read/write permission to all A records in the test.com zone and a role assigned to it is denied permission to test.com, the appliance provides read/write access to A records in the test.com zone, but denies access to the test.com zone and all its other resource records.
Table 4.3  Directly-Assigned Permissions and Roles

<table>
<thead>
<tr>
<th>Permission assigned to the admin group</th>
<th>Read/Write to all A records in the test.com zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permission inherited from an admin role</td>
<td>Deny to the test.com zone</td>
</tr>
<tr>
<td><strong>Effective permissions</strong></td>
<td>Deny to the test.com zone</td>
</tr>
<tr>
<td></td>
<td>Read/Write to all A records in test.com zone</td>
</tr>
<tr>
<td></td>
<td>Deny to all other resource records in test.com zone</td>
</tr>
</tbody>
</table>

If the group has multiple roles, the appliance applies the permissions in the order the roles are listed. If there are overlaps in the permissions among the roles, the appliance uses the permission from the role that is listed first. For example, as shown in Table 4.4, the first role assigned to the admin group has read-only permission to all A records in the test.com zone and the second role has read/write permission to the same records. The appliance applies the permission from the first admin role.

Table 4.4  Multiple Roles

<table>
<thead>
<tr>
<th>Role 1 permission</th>
<th>Read-only to all A records in the test.com zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role 2 permission</td>
<td>Read/Write to all A records in test.com zone</td>
</tr>
<tr>
<td></td>
<td>Read/Write to all MX records in test.com zone</td>
</tr>
<tr>
<td><strong>Effective permissions</strong></td>
<td>Deny to the test.com zone</td>
</tr>
<tr>
<td></td>
<td>Read-only to all A records in the test.com zone</td>
</tr>
<tr>
<td></td>
<td>Read/Write to all MX records in test.com zone</td>
</tr>
</tbody>
</table>

You can check for overlapped permissions when you add permissions to roles and to admin groups, and when you assign roles to an admin group. When you create a permission that overlaps with existing permissions, Grid Manager displays a warning message and the See Conflicts link on which you click to view the overlapped permissions. For information, see Viewing Overlapping Permissions on page 93. You can also use the quick filter Overlaps to filter overlapped permissions, the appliance lists permissions that overlap with other permissions. If you want to change the permission the appliance uses, you must change the order in which the roles are listed or change the permissions that are directly assigned to the admin group. For information, see Creating Limited-Access Admin Groups on page 82.
Viewing Overlapping Permissions

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

- **Resource**: The name of the object or resource.
- **Type**: The object type.
- **Permission**: The permission granted. This can be Read/Write, Read-Only, or Deny.
- **Inherited From**: Indicates the source from which the permission is inherited.
- **Conflict Status**: Indicates whether the permission is being used or ignored. In a permission overlap, the group permission always overrides the role permission if both permissions are set at the same level (global or object). However, if the permissions are set at different levels, the permission at a more specific level overrides that set at a higher level.
- **Role/Group Name**: The name of the admin group or admin role.

You can click the arrow key next to the resource to view the permission that is being ignored in the overlap.

Managing Permissions

After you define permissions for an admin group and role, you can do the following:

- View the permissions, as described in Viewing Permissions on page 93.
- Modify the permissions, as described in Modifying Permissions on page 94.
- Delete the permission, as described in Deleting Permissions on page 94.

Viewing Permissions

Only superusers can view the permissions of all admin groups.

To view the permissions of an admin group or role:

1. From the Administration tab, select the Administrators tab -> Permissions tab.
2. For an admin group: Select an admin group in the Groups table.
   or
   For an admin role: Select an admin role in the Roles table.
3. Grid Manager displays the following information in the Permissions table:
   - **Group/Role**: The name of the admin group or role.
   - **Permission Type**: The type of permissions. This can be DHCP Permissions, DNS Permissions, File Distribution Permissions, Grid Permissions, or IPAM Permissions.
   - **Resource**: The name of the object. For example, this field displays All Hosts if you have defined permissions for all the hosts in the grid.
   - **Resource Type**: The object type. For example, this can be Host, PTR record, or Shared Network.
   - **Permission**: The defined permission for the resource.

When you click Show All for Admins, Groups, and Roles, Grid Manager displays all the admin accounts, admin groups, and admin roles in their respective tables.

Filtering the List of Permissions

You can filter the permissions you want to view by selecting one of the following from the quick filter menu:

- **Effective Permissions**: Select to view only the permissions that the appliance is using for this group. The permissions that were ignored due to overlaps are not listed in this view.
- **Overlaps**: Select to view only the overlapped permissions.
- **All Configured Permissions**: Select to view all permissions.
Modifying Permissions

You can modify the permissions of user-defined admin roles and admin groups. You cannot modify the permissions of system-defined admin roles. When you change the permissions of a role that has been assigned to multiple admin groups, the appliance automatically applies the change to the role in all admin groups to which it is assigned.

To modify the existing permissions of a role or an admin group:

1. From the Administration tab, select the Administrators tab -> Permissions tab.
2. For an admin group: Select an admin group in the Groups table.
   or
   For an admin role: Select an admin role in the Roles table.
3. In the Permissions table, select the resource that you want to modify, and then click the Edit icon.
4. In the Manage Global Permissions or Create Object permissions editor, select the new permission: Read/Write, Read-Only or Deny for the resource.
5. Select one of the following:
   — Save: Save the entry and continue to edit.
   — Save & Close: Save the entry and close the editor.

Deleting Permissions

You can remove permissions from user-defined admin roles and admin groups. You cannot remove permissions from system-defined admin roles. When you remove permissions from a role, they are removed from the role in all admin groups to which the role is assigned. You can remove a permission from a group as long as it is not inherited from a role. You cannot remove permissions that are inherited from a role.

To delete a permission:

1. From the Administration tab, select the Administrators tab -> Permissions tab.
2. For an admin group: Select an admin group in the Groups table.
   or
   For an admin role: Select an admin role in the Roles table.
3. In the Permissions table, select the resource that you want to modify, and then click the Delete icon.
4. In the Delete Permission Confirmation dialog box, click Yes.
AUTHENTICATING ADMINISTRATORS

The NIOS appliance supports the following authentication methods: local database, RADIUS, and Active Directory. The appliance can use any combination of these authentication methods. It authenticates admins against its local database by default. Therefore, if you want to use local authentication only, you must configure the admin groups and add the local admin accounts, as described in Creating Local Admins on page 95.

If you want to authenticate admins using RADIUS and Active Directory in addition to local authentication, then you must define those services on the appliance and define the admin authentication policy. For information, see About Remote Admins on page 97.

Note: If you are using remote authentication, you must always have at least one local admin in a local admin group to ensure connectivity to the NIOS appliance in case the remote servers become unreachable.

CREATING LOCAL ADMINs

When you create an admin account, you must specify the name, password, and admin group of the administrator. You can also control in which time zone the appliance displays the time in the audit log and the DHCP and IPAM tabs of Grid Manager, such as the DHCP Lease History and DHCP Leases panels. The appliance can use the time zone that it automatically detects from the management system that the admin uses to log in. Alternatively, you can override the time zone auto-detection feature and specify the time zone.

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

1. Log in as a superuser.
2. From the Administration tab, select the Administrators tab -> Admins tab, and then click the Add icon.
   or
   From the Administration tab, select the Administrators tab -> Groups tab -> admin_group, and then click the Add icon.
3. In the Add Administrator Basic wizard, complete the following:
   — Login: Enter a name for the administrator. This is the username that the administrator uses to log in.
   — Password: Enter a password for the administrator to use when logging in.
   — Confirm Password: Enter the same password.
   — Email Address: Enter the email address for this administrator. The appliance uses this email address to send scheduling notifications.
   — Admin Group: Click Select to specify an admin group. If there are multiple admin groups, Grid Manager displays the Admin Group Selector dialog box from which you can select one. An admin can belong to only one admin group at a time.
   — Comment: Enter useful information about the administrator.
   — Disable: Select this check box to retain an inactive profile for this administrator in the configuration. For example, you might want to define a profile for a recently hired administrator who has not yet started work. Then when he or she does start, you simply need to clear this check box to activate the profile.
4. Optionally, click Next to add extensible attributes to the admin account. For information, see Managing Extensible Attribute Values on page 72.
5. Select one of the following:
   — Save & Close: Save the entry and close the wizard.
   — Save & Edit: Save the entry and continue to edit.
   — Save & New: Save the entry and open a new wizard.
Modifying and Deleting Admin Accounts

You can modify and delete admin accounts that you create, but you can only partially modify the default superuser account “admin”—and only when you are logged in as a superuser account. Furthermore, because there must always be a superuser account on the appliance, you can only remove the default “admin” account after you create another superuser account.

To modify an admin account:

1. From the Administration tab, select the Administrators tab → Admins tab → admin_account check box, and then click the Edit icon.
   
or
   From the Administration tab, select the Administrators tab → Groups tab → admin_group → admin_account check box, and then click the Edit icon.

2. The Administrator editor provides the following tabs from which you can modify data:
   
   — **General**: In the General Basic tab, modify data of the admin account as described in Creating Local Admins on page 95.
   
   In the General Advanced tab, complete the following:
   
   — **Time Zone**: Select a time zone from the drop-down list if you want to specify the time zone for the administrator. By default, the appliance automatically detects the time zone from the management system that the administrator uses to connect to the appliance. The appliance uses this time zone when it displays the timestamps for relevant data.
   
   — **Extensible Attributes**: Add and delete extensible attributes that are associated with the admin account. You can also modify the values of the extensible attributes. For information, see Managing Extensible Attribute Values on page 72.

3. Select one of the following:
   
   — **Save & Close**: Save the entry and close the editor.
   
   — **Save**: Save the entry and continue to edit.

To delete an admin account:

1. From the Administration tab, select the Administrators tab → Admins tab → admin_account check box, and then click the Delete icon.
   
   or
   
   From the Administration tab, select the Administrators tab → Groups tab → admin_group → admin_account check box, and then click the Delete icon.

2. In the Delete Confirmation dialog box, click Yes.
**About Remote Admins**

You can configure the NIOS appliance to authenticate admins whose user credentials are stored on a RADIUS server or AD domain controller. The appliance can authenticate users against more than one authentication server, and supports remote and local authentication.

To authenticate admins using RADIUS and Active Directory, you must define those services on the appliance and define the admin policy. The admin policy lists which authentication methods to use and in what order. It also lists admin groups that you have configured on the appliance and to which you can assign remote admins. An admin inherits its privileges from its admin group; therefore, all admins must be assigned to an admin group. If you configured admin groups on the remote authentication server, the group names on the remote authentication server must match the group names on the NIOS appliance so the appliance can assign an admin to the correct group. If you did not configure admin groups on the remote authentication server, you must configure a default group for remote admins on the NIOS appliance.

When an admin logs in with a user name and password, the appliance uses the first method listed in the admin policy to authenticate the admin. If authentication fails, the appliance tries the next method listed. It tries each method on the list until it is successful or all methods fail. If all methods fail, then the appliance denies access to the appliance.

If authentication succeeds, the NIOS appliance determines the admin’s privileges based on the admin group of the admin. It tries to match the admin group names in the order in which they are listed in the admin policy to any groups received from the remote server. If it finds a match, the NIOS appliance applies the privileges of that group to the admin and allows access. If the appliance does not find a match, then it applies the privileges of the default group. If no default group is defined, then the appliance denies access. *Figure 4.4* illustrates the authentication and authorization process for remote admins.

*Figure 4.4  Authenticating Remote Admins*

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

- Configure the RADIUS authentication service and AD authentication service. For information about the RADIUS authentication service, see Authenticating Using RADIUS. For information about the AD authentication service, see Authenticating Admin Accounts Using Active Directory on page 104.
- Configure admin groups that match those on the remote server. Optionally, specify a default admin group. For information about admin groups, see About Admin Groups on page 81.
- Configure the admin policy, as described in Defining the Authentication Policy on page 107.

**Note:** Infoblox strongly recommends that even if you are using remote authentication, you must always have at least one local admin in a local admin group to ensure connectivity to the appliance in case the remote servers become unreachable.
Authenticating Using RADIUS

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

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

When you configure the appliance to authenticate administrators using a RADIUS server, the appliance acts similarly to a network access server (NAS), which is a RADIUS client that sends authentication and accounting requests to the RADIUS server. Figure 4.5 illustrates the authentication process.

Figure 4.5 Authentication using a RADIUS server

1. A user makes an HTTPS connection to the NIOS appliance and sends a user name and password.
2. The appliance checks the remote admin policy and selects RADIUS as the authentication method.
3. The appliance sends an Access-Request packet to the RADIUS server.
4a. If the RADIUS server authenticates the user, it sends back an Access-Accept packet.
4b. If the RADIUS server rejects the authentication request, it sends back an Access-Reject packet.

The appliance lets the user log in and applies the authorization profile.

The appliance does not allow the user to log in.
Remote RADIUS Authentication

When you configure the NIOS appliance for remote authentication with a RADIUS server, you must specify the authentication method of the RADIUS server. Specify PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol).

PAP tries to establish the identity of a host using a two-way handshake. The client sends the user name and password in clear text to the NIOS appliance. The appliance uses a shared secret to encrypt the password and sends it to the RADIUS server in an Access-Request packet. The RADIUS server uses the shared secret to decrypt the password. If the decrypted password matches a password in its database, the user is successfully authenticated and allowed to log in.

With CHAP, when the client tries to log in, it sends its user name and password to the NIOS appliance. The appliance then creates an MD5 hash of the password together with a random number that the appliance generates. It then sends the random number, user name, and hash to the RADIUS server in an Access-Request package. The RADIUS server takes the password that matches the user name from its database and creates its own MD5 hash of the password and random number that it received. If the hash that the RADIUS server generates matches the hash that it received from the appliance, then the user is successfully authenticated and allowed to log in.

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

- Configure an authentication server group for RADIUS.
- Define admin groups and specify their privileges and settings. The names must match admin group names defined on the RADIUS server. The NIOS appliance applies these privileges and settings to users belonging to those groups on the RADIUS server. See About Admin Groups on page 81 for information about defining admin groups.
- If there are no admin groups defined on the RADIUS server, designate an admin group as the default group. See About Admin Groups on page 81 for information about defining a default admin group.
- Add RADIUS service to the list of admin authentication methods in the admin policy to enable RADIUS authentication. See Defining the Authentication Policy on page 107 for more information about configuring admin policy.

Configuring a RADIUS Authentication Server Group

You can add multiple RADIUS servers to the group for redundancy. When you do, the appliance tries to connect to the first RADIUS server on the list and if the server does not respond within the maximum retransmission limit, then it tries the next RADIUS server on the list.

After you add a RADIUS server to the NIOS appliance, you can validate the configuration. The appliance uses a pre-defined username and password when it tests the connection to the RADIUS server. The pre-defined user name is “infoblox_test_user” and the password is “infoblox_test_password“. Do not use these as your administrator username and password.

To configure a RADIUS authentication server group on the NIOS appliance:

1. From the Administration tab, click the Authentication Server Groups tab.
2. Click the Add icon in the RADIUS Services subtab.
3. In the Add RADIUS Authentication Service wizard, complete the following:
   - **Name**: Enter the name of the server group.
   - **RADIUS Servers**: Click the Add icon and enter the following:
     - **Server Name or IP Address**: Enter the FQDN or the IP address of the RADIUS server that is used for authentication.
     - **Comment**: Enter additional information about the RADIUS server.
     - **Authentication Port**: The destination port on the RADIUS server. The default is 1812. This field is required only if you do not enable accounting on the RADIUS server. This field is not required if you enable accounting to configure an accounting-only RADIUS server.
— **Authentication Type**: Select the authentication method of the RADIUS server from the drop-down list. You can specify either PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol). The default is PAP.

— **Shared Secret**: Enter the shared secret that the NIOS appliance and the RADIUS server use to encrypt and decrypt their messages. This shared secret is a value that is known only to the NIOS appliance and the RADIUS server.

— **Enable Accounting**: Select this to enable RADIUS accounting for the server so you can track an administrator's activities during a session. When you enable accounting, you must enter a valid port number in the **Accounting Port** field.

— **Accounting Port**: The destination port on the RADIUS server. The default is 1813.

— **Connect through Management Interface**: Select this so that the NIOS appliance uses the MGMT port for administrator authentication communications with just this RADIUS server.

— **Disable server**: Select this to disable the RADIUS server if, for example, the connection to the server is down and you want to stop the NIOS appliance from trying to connect to this server.

— **Click Test** to test the configuration. If the NIOS appliance connects to the RADIUS server using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the RADIUS server, the appliance displays a message indicating an error in the configuration.

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

  — **Timeout(s)**: Specify the number of seconds that the appliance waits for a response from the RADIUS server.

  — **Retries**: Specify how many times the appliance attempts to contact an authentication RADIUS server. The default is 5.

If you have configured multiple RADIUS servers for authentication and the NIOS appliance fails to contact the first server in the list, it tries to contact the next server, and so on.

— **Accounting**: Optionally, modify the Accounting settings.

  — **Timeout(s)**: Specify the number of seconds that the appliance waits for a response from the RADIUS server.

  — **Retries**: Specify how many times the appliance attempts to contact an accounting RADIUS server. The default is 1000.

— **Mode**: Specifies how the appliance contacts the RADIUS servers. The default is Ordered List. Do not change this value as Ordered List is the only mode that the appliance uses when it uses a RADIUS server group to authenticate remote admins. In this mode, the appliance always selects the first RADIUS server in the list when it sends an authentication request. It queries the next server only when the first server is considered down.

— **Comment**: Enter useful information about the RADIUS service.

— **Disable**: Select this to disable RADIUS authentication for the servers listed in the table.

4. Select one of the following:

  — **Save & Close**: Save the entry and close the wizard.

  — **Save & Edit**: Save the entry and continue to edit.

  — **Save & New**: Save the entry and open a new wizard.

Note that the following fields in the wizard do not apply to this feature: Enable NAC Filter, Cache Time to Live, and Recovery Interval. They are used with the NAC Integration feature described in *Chapter 28, Authenticated DHCP*, on page 693.
Managing the RADIUS Server List

When you add multiple RADIUS servers, the appliance lists the servers in the order you added them. This list also determines the order in which the NIOS appliance attempts to contact a RADIUS server. You can change the order of the list, as follows:

1. From the Administration tab, click the Authentication Server Groups tab -> RADIUS Services subtab, select the server_group check box and click the Edit icon.
2. In the RADIUS Servers table, do the following:
   — To move a server up the list, select it and click the up arrow.
   — To move a server down the list, select it and click the down arrow.
You can also delete a RADIUS server by selecting a RADIUS server from the RADIUS Servers table and clicking the Delete icon.
3. Select one of the following:
   — Save & Close: Save the entry and close the editor.
   — Save & Edit: Save the entry and continue to edit.
   — Save & New: Save the entry and open a new editor.

Disabling RADIUS Servers on NIOS

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

To disable a RADIUS server:

1. From the Administration tab, click the Authentication Server Groups tab -> RADIUS Services subtab, select the server_group check box and click the Edit icon.
2. In the RADIUS Service editor, select the check box of the server you want to disable in the RADIUS Servers section, and then click the Edit icon.
3. In the RADIUS Servers section, select Disable.
4. Select Save & Close or Save to save your changes.

Configuring Remote RADIUS Servers

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

Note: If you have two Infoblox appliances in an HA pair, enter both the members of the HA pair as separate access appliances and use the LAN or MGMT IP address of both appliances (not the VIP address), if configured.

Depending on your particular RADIUS server, you can configure the following RADIUS server options to enable communication with the NIOS appliance:

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

Configuring Admin Groups on the Remote RADIUS Server

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

- Import Infoblox VSAs (vendor-specific attributes) to the dictionary file on the RADIUS server
- For third-party RADIUS servers, import the Infoblox vendor file (the Infoblox vendor ID is 7779)
- Define a local admin group on the NIOS appliance (or use an existing group)
- Define a remote admin group—with the same name as the group defined on the NIOS appliance—on the RADIUS server
- Associate one or more remote admin accounts on the RADIUS server with the remote admin group

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

Configuring Remote Admin Accounts on the Remote RADIUS Server

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

- Define an admin group on the NIOS appliance and specify it as the default group. You define admin groups for remote admins within the admin policy. See Defining the Authentication Policy on page 107 for more information on configuring remote admin policies and remote admin group lists.
- On the RADIUS server:
  - Create one or more admin accounts.
  - Add and activate a policy for the admin accounts, but do not associate the policy with a policy group that contains an infoblox-group-info attribute.

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

Authorization Groups Using RADIUS

You can specify authorization privileges for an admin group on the NIOS appliance only. The appliance ignores authorization settings from the RADIUS server. Therefore, you must configure all admin groups on the NIOS appliance, regardless of where the admin accounts that belong to those groups are stored—on the NIOS appliance or on the RADIUS server. For information about specifying superuser and limited-access authorization privileges, see Creating Superuser Admin Groups on page 82 and Creating Limited-Access Admin Groups on page 82.

Accounting Activities Using RADIUS

You can enable the accounting feature on the RADIUS server to track whether an administrator has initiated a session. After an administrator successfully logs in, the appliance sends an Accounting-Start packet to the RADIUS server. For information, see Managing the RADIUS Server List on page 102.
Managing Administrators

**AUTHENTICATING ADMIN ACCOUNTS USING ACTIVE DIRECTORY**

Active Directory™ (AD) is a distributed directory service that is a repository for user information. The NIOS appliance can authenticate admin accounts by verifying user names and passwords against Active Directory. If the admin does not exist on the AD domain controller, or if the user name and password do not match entries on the domain controller, the NIOS appliance denies access to the admin. However, if the NIOS appliance verifies the username and password successfully, it grants access. In addition, the NIOS appliance queries the AD domain controller for the group membership information of the admin. The appliance matches the group names from the domain controller with the admin groups on its local database. It then authorizes services and grants the admin privileges, based upon the matching admin group on the appliance.

You must be logged in to the NIOS appliance as a superuser to configure the AD authentication service. **Figure 4.6** illustrates the Active Directory authentication process.

*Figure 4.6 Authentication Using a Domain Controller*

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

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

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

- Configure an AD authentication server group on the appliance and add one or more AD domain controllers to the group. For information about configuring an AD authentication service group for admins, see Configuring an Active Directory Authentication Service Group.
- If you configured admin groups on the AD controller, you can create those same groups on the NIOS appliance and specify their privileges and settings. Note that the admin group names must match those on the AD domain controller. You can specify a default group as well. The NIOS appliance assigns admins to the default group if none of the admin groups on the NIOS appliance match the admin groups on the AD domain controller or if there are no other admin groups configured. For information about configuring group permissions and privileges, see About Admin Groups on page 81.
- Enable Active Directory authentication by adding Active Directory to the list of authentication methods in the admin policy. The appliance refers to this list in the admin policy to determine which authentication method to use and in what order. See Defining the Authentication Policy on page 107 for more information about configuring an admin policy.

Configuring an Active Directory Authentication Service Group

You can configure multiple AD servers for redundancy. When you do, the appliance tries to connect to the first AD server on the list and if the server does not respond within the maximum retransmission limit, then it tries the next AD server on the list.

You can add multiple domain controllers for failover purposes. The NIOS appliance tries to connect with the first domain controller on the list. If it is unable to connect, it tries the next domain controller on the list, and so on.

To configure an Active Directory authentication server group on the NIOS appliance:

1. From the Administration tab, click the Authentication Server Groups tab.
2. Click the Active Directory Services subtab and click the Add icon.
3. In the Add Active Directory Authentication Service wizard, complete the following:
   - Name: Enter a name for the service.
   - Active Directory Domain: Enter the AD domain name.
   - Domain Controllers: Click the Add icon and complete the following to add an AD domain controller:
     - Server Name or IP Address: Enter the FQDN or the IP address of the AD server that is used for authentication.
     - Comment: Enter additional information about the AD server.
     - Authentication Port: Enter the port number on the domain controller to which the appliance sends authentication requests. The default is 389.
     - Encryption: Select SSL from the drop-down list to transmit through an SSL (Secure Sockets Layer) tunnel. When you select SSL, the appliance automatically updates the authentication port to 636. Infoblox strongly recommends that you select this option to ensure the security of all communications between the NIOS appliance and the AD server. If you select this option, you must upload a CA certificate from the AD server. Click CA Certificates to upload the certificate. In the CA Certificates dialog box, click the Add icon, and then navigate to the certificate to upload it.
     - Connect through Management Interface: Select this so that the NIOS appliance uses the MGMT port for administrator authentication communications with just this AD server.
     - Disable server: Select this to disable an AD server if, for example, the connection to the server is down and you want to stop the NIOS appliance from trying to connect to this server.
     - Test: Click to test the configuration. If the NIOS appliance connects to the domain controller using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the server, the appliance displays a message indicating an error in the configuration.
   - Click Add to add the domain controller to the group.
Managing Administrators

- **Timeout:** The number of seconds that the NIOS appliance waits for a response from the specified authentication server. The default is 5.
- **Comment:** Enter additional information about the service.
- **Disable:** Select this to retain an inactive AD authentication service profile.

4. Select one of the following:
   - **Save & Close:** Save the entry and close the wizard.
   - **Save & Edit:** Save the entry and continue to edit.
   - **Save & New:** Save the entry and open a new wizard.

### Managing the Domain Controller List

When you add multiple AD domain controllers, the appliance lists the servers in the order you add them. This list also determines the order in which the NIOS appliance attempts to contact a server. You can change the order of the list, as follows:

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

2. In the **Domain Controllers** table, do the following:
   - To move a server up the list, select it and click the up arrow.
   - To move a server down the list, select it and click the down arrow.

   You can also delete a domain controller by selecting the controller from the Domain Controllers table and clicking the Delete icon.

3. Select one of the following:
   - **Save & Close:** Save the entry and close the editor.
   - **Save & Edit:** Save the entry and continue to edit.
   - **Save & New:** Save the entry and open a new editor.

### Disabling Domain Controllers

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

To disable a domain controller:

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

2. In the **Edit Domain Controllers** section, select **Disable**.

3. Select **Save & Close** or **Save** to save your changes.
Defining the Authentication Policy

After you configure the properties of each authentication service you want to use, you must then define the admin authentication policy. The policy defines which authentication methods the appliance uses to authenticate admins, and in what order. By default, the appliance defines a “Local Admin” rule for authenticating users using the local database. You cannot modify or delete this default rule.

Configuring a List of Authentication Methods

You can configure a list of authentication methods, and prioritize each method in the list. The appliance uses the first method on the list. If unsuccessful, the appliance uses the next method on the list, and so on.

To configure a list of authentication methods for remote admins:

1. From the Administration tab, select the Administrators tab -> Authentication Policy tab.
2. From the Authenticate users against these services in this order section, click the Add icon to add an authentication service.
3. Select one of the following in the Add Authentication Service section:
   - RADIUS: Select this to add the RADIUS authentication service.
   - Active Directory: Select this to add an AD authentication service, and then select the service you want to add from the drop-down list.
4. Click Add.
   You can reorder the list by selecting an authentication method or service and moving it up or down the list using the arrow keys next to the list.

Configuring a List of Remote Admin Groups

You can configure a list of admin groups for remote admins, and prioritize each group by moving them up or down within the list. You can add remote admin groups in addition to the default group. When the appliance receives information that an admin belongs to one or more groups, the appliance selects the first group in the list that matches, and assigns that group to the admin. If no groups are returned by the domain controller or the RADIUS server, the default group is assigned (if specified).

To configure the remote admin group list:

1. From the Administration tab, select the Administrators tab -> Authentication Policy tab.
2. From the Map the remote admin group to local group in this order section, click the Add icon to add an admin group to the list.
3. In the Admin Group Selector dialog box, select an admin group, and then click the Select icon. Use Shift+click and Ctrl+click to select multiple admin groups.
   You can reorder the list by selecting an admin group and moving it up or down the list using the arrow keys next to the list.

To assign a user to a specific admin group if the remote admin group is not found, select Assign User to this Group if Remote Admin Group cannot be found, and then click Select. In the Admin Group Selector dialog box, select an admin group, and then click the Select icon.
Changing Password Length Requirements

Password length requirements control how long a password must be for a NIOS appliance admin account. Increasing this value reduces the likelihood of hackers gaining unauthorized access.

To change password length requirements:

1. From the Grid tab, select the Grid Manager tab, and then select Grid Properties → Edit from the Toolbar.
2. In the Grid Properties editor, select the Security tab.
3. Enter a number from 4 to 64 in the Minimum Password Length field.
4. Click the Save & Close or Save to save your changes.
Notifying Administrators

You can notify individual administrators about system status through email, or notify a group of people using an alias email address. If you have configured DNS resolution on your network, the E-mail relay configuration function is not required. If you did not configure the settings on the DNS Resolver section, you must enter a static IP address of the target system in the Relay Name/IP Address field. The appliance sends e-mail to administrators when certain events occur. Here is a list of events that trigger e-mail notifications:

- Changes to link status on ports and online/offline replication status
- Events that generate traps, except for upgrade failures (ibUpgradeFailure). For a list of events, see Infoblox MIBs on page 326

The appliance attempts to send the email notification once after an event. It does not try to send the notification again, if the first attempt fails. Infoblox recommends that you use the Test Email settings button to test the email settings and to verify that the recipient received the notification.

You can define the email settings at the grid and member levels.

Grid Level

To notify an administrator of an independent appliance or a grid:

1. From the Grid tab, select the Grid Manager tab, and then select Grid Properties → Edit from the Toolbar.
2. In the Grid Properties editor, select the Email tab, and then complete the following:
   - Enable Email notification: Select this.
   - Email address: Enter the email address of the administrator. Use an email alias to notify multiple people.
   - Use SMTP Relay: Select this if the NIOS appliance must send email to an intermediary SMTP (Simple Mail Transfer Protocol) server that relays it to the SMTP server responsible for the domain name specified in the email address. Some SMTP servers only accept email from certain other SMTP servers and might not allow email from the NIOS appliance. In this case, specify the DNS name or IP address of a different SMTP server that does accept email from the NIOS appliance and that will then relay it to the SMTP server that can deliver it to its destination. Clear this if it is unnecessary to use an email relay server.
   - SMTP Relay Name or Address: If you have configured DNS resolution, enter the DNS name of the relay server.
     If DNS resolution is not configured, enter the IP address of the relay server.
3. Optionally, click Test Email settings to confirm this feature is operating properly.
4. Click the Save & Close or Save to save your changes.

Member Level

To define email settings for a member:

1. From the Grid tab, select the Grid Manager tab → member check box, and then select the Edit icon.
2. In the Grid Member Properties editor, select the Email tab, and then click Override to override grid-level settings.
3. Complete the email configuration as described in Grid Level on page 109.
## Administrative Permissions for Common Tasks

*Table 4.5* lists some of the common tasks admins can perform and their required permissions. All the permission tables in this chapter use the following definitions:

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

*KTable 4.5 Permissions for Common Tasks*

<table>
<thead>
<tr>
<th>Tasks</th>
<th>All Grid Members</th>
<th>Grid Member(s)</th>
<th>All DNS Views</th>
<th>All DNS Zones</th>
<th>All Shared Record Groups</th>
<th>All Resource Records</th>
<th>All Network Views</th>
<th>All Networks</th>
<th>Specific Network(s)</th>
<th>DHCP Range(s)</th>
<th>Fixed Addresses</th>
<th>Scheduling Task</th>
<th>Network Discovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>For Grid and Members</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure a grid member</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restart services for an entire grid</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restart services on a grid member</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initiate and control network discovery on all networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scheduling tasks for all supported objects</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>For DNS resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete DNS views</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for DNS views</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete DNS zones with assigned members</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for DNS zones with assigned members</td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete all resource records</td>
<td>RW</td>
<td></td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for all resource records</td>
<td>RO</td>
<td></td>
<td></td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>For DHCP Resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete network views and their associated DNS views</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View network properties and statistics</td>
<td>RO</td>
<td></td>
<td></td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete networks with assigned members</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete networks without assigned members</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete DHCP ranges in a specific network with assigned members</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete fixed addresses in a specific network without assigned members</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Administrative Permission for the Grid**

By default, the grid master denies access to grid members when a limited-access admin group does not have defined permissions. You can grant an admin group read-only or read/write permission, or deny access to all grid members or you can grant permission to specific grid members, as described in *Applying Permissions and Managing Overlaps* on page 91.

**Note:** Only superusers can modify DNS and DHCP grid properties.

The following sections describe the types of permissions that you can set with grid permissions:

- *Administrative Permissions for Grid Members* on page 111
- *Administrative Permissions for Network Discovery* on page 112
- *Administrative Permissions for Scheduling Tasks* on page 113
- *Administrative Permissions for Microsoft Servers* on page 114

**Administrative Permissions for Grid Members**

*Table 4.6* lists the tasks admins can perform and the required permissions for grid members.

*Table 4.6  Grid Member Permissions*

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid Member(s)</th>
<th>DNS Views</th>
<th>DNS Zones</th>
<th>Networks</th>
<th>DHCP Ranges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign members to DNS zones</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign members to networks</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign members to DHCP ranges</td>
<td>RW</td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure member properties</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add a member to a Match Members list of a DNS view</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete a view with members in a Match Members list</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View DNS and DHCP member properties</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and download syslog</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View DNS and DHCP configuration file</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View network statistics</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restart grid DNS and DHCP services</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Administrative Permissions for Network Discovery

Limited-access admin groups can initiate a discovery and manage discovered data based on their administrative permissions.

You can set global permissions for network discovery as described in Defining Global Permissions on page 88. The following table lists the tasks admins can perform and the required permissions for network discovery.

Table 4.7 Permissions for Network Discovery

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Network Discovery</th>
<th>DNS Zones</th>
<th>Networks Selected for Discovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiate and control a discovery on selected networks</td>
<td>RW</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>View discovered data</td>
<td></td>
<td>RO</td>
<td></td>
</tr>
<tr>
<td>Add unmanaged data to existing hosts, and resolve conflicting IP addresses</td>
<td></td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>Convert unmanaged data to a host, fixed address, reservation, A record, or PTR record</td>
<td>RW</td>
<td>RW</td>
<td></td>
</tr>
</tbody>
</table>
Administrative Permissions for Scheduling Tasks

You can schedule tasks, such as adding hosts or modifying fixed addresses, for a future date and time. To schedule tasks, you must first enable the scheduling feature at the grid level, and then define administrative permissions for admin groups and admin roles. For information, see Scheduling Tasks on page 216. Only superusers can enable and disable this feature and grant scheduling permissions to admin groups. Limited-access admin groups can schedule tasks only when they have scheduling permissions.

Superusers can do the following:

- Enable and disable task scheduling at the grid level
- Grant and deny scheduling permissions to admin groups and admin roles
- Schedule tasks for all supported object types
- Reschedule and delete any scheduled task

You can set global permissions to schedule tasks as described in Defining Global Permissions on page 88. The following table lists the tasks admins can perform and the required permissions. Users with read/write permission to scheduling can view, reschedule, and delete their own scheduled tasks.

Table 4.8 Scheduling Task Permissions

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Scheduling Task</th>
<th>All Networks</th>
<th>All DNS Views</th>
<th>All Shared Record Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule the addition, modification, and deletion of all supported object types</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>View, reschedule, and delete scheduled tasks</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>Convert unmanaged data to a host, fixed address, reservation, A record, or PTR record</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To schedule tasks for specific resources, admins must have Read/Write permission to scheduling tasks, plus the required permissions to the supported resources. For information about permissions for specific resources, see the following:

- Grid members—See Administrative Permission for the Grid on page 111.
- DNS resources—See Administrative Permissions for DNS Resources on page 116.
- DHCP resources—See Administrative Permissions for DHCP Resources on page 121.

Note that the appliance deletes all pending scheduled tasks when superusers disable task scheduling at the grid level. The appliance deletes an admin’s scheduled tasks when superusers do the following:

- Set the scheduling permission of admin groups and roles to “Deny”
- Delete or disable an admin group or an admin role
- Delete or disable local admins
- Delete the scheduling permission from any admin group or admin role that contains users with pending scheduled tasks
- Change the admin group of a limited-access admin
Administrative Permissions for Microsoft Servers

By default, only superusers can add Microsoft servers as managed servers to the grid. Limited-access admins can add and manage Microsoft servers from the grid based on their administrative permissions.

The following table lists the tasks admins can perform and the required permissions. Note that only superusers can add a Microsoft server to a name server group.

Table 4.9 Microsoft Server Permissions

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Microsoft Server(s)</th>
<th>Grid Member(s)</th>
<th>Network Views</th>
<th>DNS Views</th>
<th>DNS Zones</th>
<th>Resource Records</th>
<th>Networks</th>
<th>DHCP Ranges</th>
<th>Superscopes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign Microsoft server to member</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign a network view to the Microsoft server</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign a DNS view to the Microsoft server</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign Microsoft server as primary or secondary to DNS zones</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove a Microsoft server as the primary or secondary server of a zone</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove a zone from a Microsoft server</td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit zones and resource records of Microsoft servers</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign a Microsoft server to a network</td>
<td>RW</td>
<td></td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign a Microsoft server to a DHCP range</td>
<td>RW</td>
<td></td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove a network served by a Microsoft server</td>
<td>RW</td>
<td></td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove a DHCP range (scope) from a Microsoft server</td>
<td>RW</td>
<td></td>
<td></td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add, modify and remove Microsoft superscopes</td>
<td>RW</td>
<td></td>
<td></td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clear leases from Microsoft server</td>
<td>RW</td>
<td></td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit Microsoft server properties</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Microsoft server properties</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and download Microsoft logs</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start/Stop DNS or DHCP on the Microsoft server</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove a Microsoft server from the grid</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Administrative Permissions for IPAM Resources

Limited-access admin groups can access certain IPAM resources only if their administrative permissions are defined. By default, the appliance denies access when a limited-access admin group does not have defined permissions. You can grant admin groups read-only or read/write permission, or deny access to the following IPAM resources:

- Network views
- IPv4 networks
- IPv6 networks
- Hosts

The appliance applies permissions for IPAM resources hierarchically. Permissions to a network view apply to all networks and resources in that view. You can also grant an admin group broad permissions to IPAM resources, such as read/write permission to all IPv4 networks and IPv6 networks in the database. In addition, you can grant permission to a specific host in a network. Permissions at more specific levels override global permissions.

The following sections describe the types of permissions that you can set for IPAM resources:

- Administrative Permissions for Network Views on page 122
- Administrative Permissions for IPv4 and IPv6 Networks on page 115
- Administrative Permissions for Hosts on page 115

Administrative Permissions for IPv4 and IPv6 Networks

Limited-access admin groups can access IPv4 and IPv6 networks only if their administrative permissions are defined. Permissions for a network apply to all its DNS and DHCP resources, if configured. To override network-level permissions, you must define permissions for specific objects within the networks.

You can grant read-only or read/write permission, or deny access to networks, as follows:

- All IPv4 or IPv6 networks—Global permission that applies to all networks in the database.
- A specific network—Network permissions apply to its properties and to all DNS and DHCP resources. This overrides global permissions.

Administrative Permissions for Hosts

A host record can contain both DNS and DHCP attributes if you configure them. When applying administrative permissions to host records, the permissions apply to all relevant DNS and DHCP resources within the host records.

You can define global permissions to all hosts. To override global permissions, you must define permissions for specific hosts.

You can grant read-only or read/write permission, or deny access to host records, as follows:

- All hosts—Global permission that applies to all host records in the grid.
- A specific host—Object permission that applies only to a selected host.
Administrative Permissions for DNS Resources

You can grant roles and admin groups read-only or read/write permission, or deny access to the following DNS resources:

- DNS Views
- DNS Zones
- Hosts
- Bulk Hosts
- A records
- AAAA records
- CNAME records
- DNAME records
- MX records
- PTR records
- SRV records
- TXT
- Hosts
- Bulk Hosts
- Shared Record Groups
- Shared A records
- Shared AAAA records
- Shared MX records
- Shared SRV records
- Shared TXT records

The appliance applies permissions for DNS resources hierarchically. Permissions to a DNS view apply to all zones and resource records in that view. Permissions for a zone apply to all its subzones and resource records, and resource record permissions apply to those resource records only. To override permissions set at higher level, you must define permissions at a more specific level. To assign permissions, see Applying Permissions and Managing Overlaps on page 91.

The following sections describe the different types of permissions that you can set for DNS resources:

- Administrative Permissions for DNS Views on page 117
- Administrative Permissions for Zones on page 118
- Administrative Permissions for Resource Records on page 119
Administrative Permissions for DNS Views

Limited-access admin groups can access DNS views, including the default view, only if their administrative permissions are defined. Permissions to a DNS view apply to all its zones and resource records. To override view-level permissions, you must define permissions for its zones and resource records. For example, you can grant an admin group read-only permission to a view and read/write permission to all its zones. This allows the admins to display the view properties, but not edit them, and to create, edit and delete zones in the view.

You can grant read-only or read/write permission, or deny access to DNS views, as follows:

- All views—Global permission that applies to all DNS views in the database.
- A specific view—Applies to its properties and its zones, if you do not define zone-level permissions. This overrides the global view permissions.
- All zones in a view—if you do not define permissions for zones, they inherit the permissions of the view they are in.

For information on setting permissions for a view and its zones, see Applying Permissions and Managing Overlaps on page 91.

The following table lists the tasks admins can perform and the required permissions for DNS views.

Table 4.10 Permissions for DNS Views

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid Member(s)</th>
<th>All DNS Views</th>
<th>Specific DNS View</th>
<th>All DNS Zones</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete DNS views</td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete DNS zones with assigned members</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete DNS zones without assigned members</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify and delete a specific DNS view</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete DNS zones, subzones, and resource records in a specific DNS view</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add grid members to a Match Members list of a DNS view</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete a DNS view with grid members in a Match Members list</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View DNS view properties, DNS zones, and resource records</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View DNS zone properties, subzones, and resource records</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restart services from the DNS tab</td>
<td>RO</td>
<td></td>
<td></td>
<td>RW</td>
</tr>
</tbody>
</table>
Administrative Permissions for Zones

By default, zones inherit administrative permissions from the DNS view in which they reside. You can override view-level permissions by setting permissions for specific zones. Permissions set for a zone are inherited by its subzones and resource records. To override zone-level permissions, set permissions for specific subzones and resource records.

For example, you can grant an admin group the following permissions:

• Read-only to a zone and to all its A, AAAA, and PTR records
• Read/Write permission to all MX and SRV records in the zone
• Deny to all the other resource records—CNAME, DNAME, TXT, host, and bulk host

You can grant read-only or read/write permission, or deny access to zones as follows:

• All zones —Global permission that applies to all zones in all views.
• All zones in a view—Permissions at this level override the global permissions.
• A specific zone—Applies to the zone properties and resource records, if you do not define permissions for its resource records. This overrides global and view-level permissions. If you delete a zone and re-parent its subzone, the subzone inherits the permissions of the new parent zone.
• Each resource record type in a zone—For example, you can define permissions for all A records and for all PTR records in a zone. If you do not define permissions for resource records, they inherit the permissions of the zone in which they reside.

For information on setting permissions for zones and resource records, see Applying Permissions and Managing Overlaps on page 91.

The following table lists the tasks admins can perform and the required permissions for zones.

Table 4.11 DNS Zone Permissions

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid Member(s)</th>
<th>Specific DNS View</th>
<th>All DNS Zones</th>
<th>Specific DNS Zone</th>
<th>Resource Records</th>
<th>Shared Record Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete zones, subzones and resource records with assigned members</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete zones, subzones and resource records without assigned members</td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lock and unlock a zone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete a zone with assigned grid members</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete all zones, subzones, and resource records in a specific view</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign a name server group (member) to a zone</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete a zone with name server groups assigned</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign a shared record group to a zone</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View zone properties, subzones, and resource records of a specific zone</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search for zones, subzones, and resource records in a specific DNS view</td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Copy resource records from one zone to another: Source zone</td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Copy resource records from one zone to another: Destination Zone</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Administrative Permissions for Resource Records

Resource records inherit the permissions of the zone to which they belong. You can override zone-level permissions by setting permissions for specific resource records.

You can grant read-only or read/write permission, or deny access to resource records as follows:

- Each resource record type in all zones and in all views—Global permission that applies to all resource records of the specified type; for example, all A records in the database.
- Each resource record type in a zone—Permissions at this level override global permissions.
- A specific resource record—Overrides zone-level permissions.

For information on setting permissions for resource records, see Applying Permissions and Managing Overlaps on page 91. The following table lists the tasks admins can perform and the required permissions for resource records.

Table 4.12 DNS Resources

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Resource Record Type</th>
<th>Specific Resource Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete resource records for a specified type, such as all A records or all PTR records</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>View resource records for a specified type only</td>
<td>RO</td>
<td>RO</td>
</tr>
<tr>
<td>Search for records of a specified type</td>
<td>RO</td>
<td>RO</td>
</tr>
<tr>
<td>View a specific resource record</td>
<td>RO</td>
<td>RO</td>
</tr>
<tr>
<td>View, modify, and delete a specific resource record</td>
<td>RW</td>
<td>RW</td>
</tr>
</tbody>
</table>

The following are additional guidelines:

- Only admins with read/write permission to bulk host records and read/write permission to reverse zones can create bulk host records and automatically add reverse-mapping zones.
- To create host records, admins must have read/write permission to the network and zone of the host.
- Admins must have read-only permission to the host records in a zone to view the Host Name Compliance Report. Admins must have read/write permission to the resource records in a zone to modify host names that do not comply with the host policy.
Administrative Permissions for Shared Record Groups

By default, only superusers can add, edit, and delete shared record groups. Limited-access admin groups can access shared record groups, only if their administrative permissions are defined.

You can set different permissions for a shared record group and for each type of shared resource record in the group. For example, you can grant a role or an admin group the following permissions:

- Read-only to a shared record group and to all its shared A and AAAA records
- Read/Write permission to all the shared MX and SRV records in the shared record group
- Deny to the TXT records

You can grant read-only or read/write permission, or deny access to shared record groups, as follows:

- All shared record groups—Global permission that applies to all shared record groups in the database.
- A specific shared record group—Overrides global permissions.
- Each shared record type in all shared record groups — The shared resource record types include shared A records, shared AAAA records, shared MX records, shared SRV records, and shared TXT resource records.
- Each shared record type in a shared record group—Permissions at this level override global permissions.
- A specific shared record—Overrides zone-level permissions.

Note the following guidelines:

- Shared record group permissions override zone permissions.
- Even if a zone is locked, superusers and limited-access users with read/write access can still edit or delete a shared record in the zone.

For information on setting permissions for shared record groups, see Applying Permissions and Managing Overlaps on page 91. The following table lists the tasks admins can perform and the required permissions for shared record groups.

Table 4.13 Permissions for Shared Record Groups

<table>
<thead>
<tr>
<th>Tasks</th>
<th>All Shared Record Groups</th>
<th>Specific Shared Record Group</th>
<th>Specific Record Type</th>
<th>Specific DNS Zone</th>
<th>Specific Shared Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete shared record groups</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify and delete a shared record group</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View a shared record group</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete shared records for a specific type</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View or search for shared records of a specific type</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete shared records for a specific type in a specified shared record group</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View shared records for a specific type in a specified shared record group only</td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete a shared record</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View a specific shared record</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign a shared record group to DNS zones</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Administrative Permissions for DHCP Resources

Limited-access admin groups can access certain DHCP resources only if their administrative permissions are defined. By default, the appliance denies access when a limited-access admin group does not have defined permissions. You can grant admin groups read-only or read/write permission, or deny access to the following DHCP resources:

- Network views
- IPv4 Networks
- Hosts
- DHCP ranges
- DHCP Fixed addresses
- DHCP Reservations
- MAC address filters
- Shared networks
- Network templates
- DHCP range templates
- Fixed address templates
- DHCP lease history
- Roaming hosts

You can grant an admin group broad permissions to DHCP resources, such as read/write permission to all networks and shared networks in the database. In addition, you can grant permission to specific resources, such as a specific network, a DHCP range, or an individual IP address in a network. Permissions at more specific levels override global permissions.

The following sections describe the different types of permissions that you can set for DHCP resources:

- Administrative Permissions for Network Views on page 122
- Administrative Permissions for Networks and Shared Networks on page 123
- Administrative Permissions for Fixed Addresses and Reservations on page 125
- Administrative Permissions for DHCP Ranges on page 126
- Administrative Permissions for DHCP Templates on page 127
- Administrative Permissions for MAC Address Filters on page 128
- Administrative Permissions for the DHCP Lease History on page 129
Administrative Permissions for Network Views

Limited-access admin groups can access network views, including the default network view, only if they have read-only or read/write permission to a specific network view or to all network views. Permissions granted to a network view apply to all its networks, shared networks, DHCP ranges and fixed addresses.

You can grant admin groups read-only or read/write permission, or deny access to network views as follows:

- All network views—Global permission that applies to all network views in the database.
- A specific network view—Permission to a specific network view applies to the properties you set in the Network View editor, and to all the networks and shared networks in the network view. This overrides the global permission to all network views. When you configure permissions for a network view, you can also set permissions for the following:
  - All networks in the selected network view—If you do not define permissions for networks, they inherit the permissions of their network view.
  - All shared networks in a specific network view—If you do not define permissions for shared networks, they inherit the permissions of their network view.

Note that you can grant an admin group read-only or read/write permission to specific networks in a network view, without granting them permission to that network view. For information, see Administrative Permissions for Networks and Shared Networks on page 123.

For information on how to define permissions for network views, see Applying Permissions and Managing Overlaps on page 91.

The following table lists the tasks admins can perform and the required permissions for network views.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>All DNS Views</th>
<th>Specific DNS View</th>
<th>All Network Views</th>
<th>Specific Network View</th>
<th>All Networks</th>
<th>All Shared Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create and delete network views and their associated DNS views</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create and delete a network view and its associated DNS views</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete networks and shared networks in all network views</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete networks and shared networks in a network view</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View the properties of all network views</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View network statistics of all network views</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for all networks and shared networks</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View the properties of a network view</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for networks and shared networks in a network view</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expand and join networks</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expand and join networks in a specific network view</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete networks, DHCP ranges and fixed addresses in a specific network view</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View network statistics and properties of all networks in a network view</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Administrative Permissions for Networks and Shared Networks

Limited-access admin groups can access networks, including shared networks, only if their administrative permissions are defined. Permissions for a network apply to all its DHCP ranges and fixed addresses. To override network-level permissions, you must define permissions for specific DHCP ranges and fixed addresses. For example, you can grant an admin group read-only permission to a network, read/write permission to its DHCP ranges, and read-only permission to its fixed addresses.

You can grant read-only or read/write permission, or deny access to networks, as follows:

- All networks—Global permission that applies to all networks in the database.
- All shared networks—Global permission that applies to all shared networks in the database.
- A specific network—Network permissions apply to its properties and to all DHCP ranges, fixed addresses and hosts in the network, if they do not have permissions defined. This overrides global permissions.
- All DHCP ranges in a network—if you do not define permissions for DHCP ranges, they inherit the permissions of the network in which they reside.
- All fixed addresses in a network—if you do not define permissions for fixed addresses, they inherit the permissions of the network in which they reside.

To define permissions for a specific network and its DHCP ranges and fixed addresses, see Applying Permissions and Managing Overlaps on page 91.

The following table lists the tasks admins can perform and the required permissions for networks.
### Table 4.15 Network Permissions

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid Member(s)</th>
<th>All Networks</th>
<th>Specific Network</th>
<th>Specific DNS Zone</th>
<th>All DHCP Ranges</th>
<th>All Fixed Addresses</th>
<th>Network Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete networks, DHCP ranges, and fixed addresses without assigned</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>grid members</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete networks, DHCP ranges, and fixed addresses with assigned</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>grid members</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign a grid member to a specific network and its DHCP ranges</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expand and join networks</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create networks from templates</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RO</td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete a network</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View network properties and statistics, and search for DHCP ranges and fixed addresses</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>in a specific network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete DHCP ranges and fixed addresses in a specific network</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create and split a network and automatically create a reverse DNS zone</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete shared networks</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View shared networks</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete DHCP ranges with an assigned member in a specific network</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete DHCP ranges</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for DHCP ranges in a specific network</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete fixed addresses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RO</td>
<td></td>
</tr>
<tr>
<td>View and search for fixed addresses in a specific network</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Administrative Permissions for Fixed Addresses and Reservations

Fixed addresses and reservations inherit the permissions of the networks in which they reside. You can override network-level permissions by defining permissions for fixed addresses.

You can grant read-only or read-write permission, or deny access to fixed addresses, as follows:

- All fixed addresses/reservations—Global permission that applies to all fixed addresses and reservations in the database.
- All fixed addresses/reservations in a network—Permissions at this level override global permissions. If you do not define permissions for fixed addresses and reservations, they inherit the permissions of the network in which they reside.
- A single fixed address/reservation—Overrides global and network-level permissions.

For information on setting permissions for fixed addresses, see Applying Permissions and Managing Overlaps on page 91.

The following table lists the tasks admins can perform and the required permissions for fixed addresses.

Table 4.16 Permissions for Fixed Addresses/Reservations

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Specific Network</th>
<th>All Fixed Addresses/Reservations</th>
<th>Specific Fixed Address/Reservation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete fixed addresses/reservations</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete fixed addresses/reservations in specific a network</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify and delete a fixed address/reservation</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for all fixed addresses/reservations</td>
<td>RO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for fixed addresses/reservations in a network</td>
<td>RO</td>
<td>RO</td>
<td></td>
</tr>
<tr>
<td>View and search for a fixed address/reservation</td>
<td>RO</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Administrative Permissions for DHCP Ranges

DHCP ranges inherit the permissions of the networks in which they reside. You can override network-level permissions by defining permissions for DHCP ranges. You can read-only or read/write permission, or deny access to DHCP address ranges, as follows:

- All DHCP ranges—Global permission that applies to all DHCP ranges in the database.
- All DHCP ranges in a network—Permissions at this level override global permissions. If you do not define permissions for DHCP ranges, they inherit the permissions of the network in which they reside.
- A single DHCP range—Overrides global and network-level permissions.

For information on setting permissions for DHCP ranges, see Applying Permissions and Managing Overlaps on page 91. The following table lists the tasks admin can perform and the required permissions for DHCP ranges.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid Member(s)</th>
<th>Specific Network</th>
<th>All DHCP Ranges</th>
<th>Specific DHCP Range</th>
<th>MAC Address Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete DHCP ranges with an assigned member or a failover association</td>
<td>RW</td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete DHCP ranges in a network with assigned members</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify and delete a DHCP range with an assigned member</td>
<td>RW</td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for all DHCP ranges with an assigned member</td>
<td>RO</td>
<td></td>
<td>RO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for DHCP ranges in a network with assigned members</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for a DHCP range with an assigned member</td>
<td>RO</td>
<td></td>
<td>RO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for a DHCP range without an assigned member</td>
<td>RO</td>
<td></td>
<td>RO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apply relay agent and option filters to a DHCP range</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apply a MAC address filter to a DHCP range</td>
<td></td>
<td></td>
<td>RW</td>
<td>RO</td>
<td></td>
</tr>
</tbody>
</table>
Administrative Permissions for DHCP Templates

There are three types of DHCP templates—network, DHCP range, and fixed address/reservation templates. To access any of these templates, a limited-access admin group must have read-only permission to the template. Limited-access admin groups cannot have read/write permission to the templates. Only superusers can create, modify and delete network, DHCP range, and fixed address templates. An admin group with read-only permission to the DHCP templates can view them and use them to create networks, DHCP ranges and fixed addresses, as long as they have read/write permissions to those DHCP resources as well.

You can set global read-only permission that applies to all DHCP templates, and you can set permissions to specific templates as well.

For information on setting permissions, see Applying Permissions and Managing Overlaps on page 91. The following table lists the tasks admins can perform and the required permissions for DHCP templates.

Table 4.18 Permissions for DHCP Templates

<table>
<thead>
<tr>
<th>Tasks</th>
<th>DHCP Templates</th>
<th>All Networks</th>
<th>All DHCP Ranges</th>
<th>All Fixed Addresses/Reservations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create networks from templates</td>
<td>RO</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create DHCP ranges from templates</td>
<td>RO</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create fixed addresses/reservations from templates</td>
<td>RO</td>
<td></td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>View templates</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note the following additional guidelines:

- DHCP range templates and fixed address templates do not inherit their permissions from network templates. You must set permissions for each type of template.
- An admin group can create a network using a network template that includes a DHCP range template and a fixed address template, even if it has no permission to access the DHCP range and fixed address templates.
Administrative Permissions for MAC Address Filters

Limited-access admin groups can access MAC address filters only if their administrative permissions are defined. The appliance denies access to MAC address filters for which an admin group does not have defined permissions.

You can grant read-only or read/write permission, or deny access to MAC address filters as follows:

- All MAC address filters in the database
- A specific MAC address filter

For information on setting permissions, see Applying Permissions and Managing Overlaps on page 91. The following table lists the tasks admins can perform and the required permissions for MAC address filters.

*Table 4.19 Permissions for MAC Filters*

<table>
<thead>
<tr>
<th>Tasks</th>
<th>All MAC Address Filters</th>
<th>Specific MAC Address Filter</th>
<th>Specific DHCP Ranges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete MAC address filters</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete MAC address entries for a MAC address filter</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify and delete a MAC address filter</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apply a MAC address filter to a DHCP range</td>
<td>RO, RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete a MAC address filter from a DHCP range</td>
<td>RO, RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View MAC address filters and their MAC address entries</td>
<td>RO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View a MAC address filter and its MAC address entries</td>
<td>RO</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Administrative Permissions for the DHCP Lease History

A limited-access admin group can view and export the DHCP lease history if it has read-only permission to the DHCP lease history. Permissions to the DHCP lease history are different from the network permissions. Therefore, an admin group can access the DHCP lease history, regardless of its network permissions. Note that only superusers can import a DHCP lease history file.

To define permissions for the DHCP lease history:

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

2. Complete the following in the Manage Global Permissions dialog box:
   - Permission Type: Select DHCP Permissions from the drop-down list.
   - In the table, select Read/Write, Read-only, or Deny for All DHCP Lease History.

3. Click Save & Close or Save to save the permissions.
Administrative Permissions for File Distribution Services

You can restrict access to the TFTP, HTTP and FTP services provided by the appliance. By default, the appliance denies access to the TFTP, HTTP and FTP services, unless an admin group has their administrative permissions defined.

You can grant read-only or read/write permission, or deny access to the following resources:
- Grid File Distribution Properties—Applies to the grid and its members, directories, and files. You can set this from the Administrators perspective only.
- Member File Distribution Properties—Applies to the grid member properties only.
- A specific directory—Applies to the directory and its files.

For information on setting permissions, see Applying Permissions and Managing Overlaps on page 91. The following table lists the tasks admins can perform and the required permissions for file distribution services.

Table 4.20 Permissions for File Distribution Services

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid File Distribution Properties</th>
<th>Member Distribution Properties</th>
<th>Specific Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create and remove directories and files</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify the grid and member file distribution properties</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View the grid and member file distribution properties, directories, and files</td>
<td>RO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify the member file distribution properties</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View the member file distribution properties</td>
<td>RO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add and delete a directory, subdirectories, and files in the directory</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View a directory and its subdirectories and files</td>
<td>RO</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 5  Deploying a Grid

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

- **Introduction to Grids** on page 133
  - *Grid Communications* on page 134
  - *NAT Groups* on page 135
  - *Automatic Software Version Coordination* on page 138
  - *Grid Bandwidth Considerations* on page 140
- **About HA Pairs** on page 142
  - *Planning for an HA Pair* on page 142
  - *About HA Failover* on page 143
  - *VRRP Advertisements* on page 144
- **Creating a Grid Master** on page 145
  - *Port Numbers for Grid Communication* on page 147
  - *Grid Setup Wizard* on page 147
  - *Creating an HA Grid Master* on page 147
  - *Creating a Single Grid Master* on page 150
- **Adding Grid Members** on page 152
  - *Adding a Single Member* on page 152
  - *Adding an HA Member* on page 153
  - *Joining Appliances to a Grid* on page 154
- **Configuration Example: Configuring a Grid** on page 155
  - *Cable All Appliances to the Network and Turn On Power* on page 157
  - *Create the Grid Master* on page 157
  - *Define Members on the Grid Master* on page 159
  - *Join Appliances to the Grid* on page 160
  - *Import DHCP Data* on page 162
  - *Import DNS Data* on page 163
  - *Using the Wizard* on page 164
  - *After Using the Wizard* on page 166
• Managing a Grid on page 167
  — Changing Grid Properties on page 167
  — Setting the MTU for VPN Tunnels on page 168
  — Removing a Grid Member on page 168
  — Promoting a Master Candidate on page 168
Introduction to Grids

A grid is a group of two or more NIOS appliances that share sections of a common, distributed, built-in database and which you configure and monitor through a single, secure point of access: the grid master. A grid can include Infoblox appliances and vNIOS appliances. A vNIOS appliance is a non-Infoblox hardware platform running the vNIOS software package. (Supported platforms are Riverbed Steelhead appliances running the Riverbed Services Platforms, Cisco AXP service modules in Integrated Services Routers, Cisco SRE-V, and VMware ESX and ESXi server platforms.) You can configure Infoblox appliances and vNIOS appliances for VMware as grid masters, grid master candidates, and grid members. You can configure other vNIOS appliances as grid members only. For information, see Supported vNIOS Appliance Configurations on page 835. Figure 5.1 shows the basic concept of a grid and database distribution (or “replication”).

Figure 5.1 Grid and Partitioned Database Replication

Note: In addition to the VPN tunnel securing administrative traffic to the grid master, all grid communications between the grid master and grid members pass through encrypted VPN tunnels (not shown).

The grid master can be either an HA master or a single master; that is, an HA (high availability) pair or a single appliance. Similarly, a grid member can be either a single member or an HA member. You can add single appliances and HA pairs to a grid, forming single members and HA members respectively. A single grid member can be either an Infoblox appliance or a vNIOS appliance. An HA grid member can be a pair of Infoblox appliances or vNIOS appliances. For information, see Supported vNIOS Appliance Configurations on page 835.

The grid master communicates with every grid member in a hub-and-spoke configuration. For an HA member, the grid master communicates with the active node, which in turn communicates with the passive node, as shown in Figure 5.2.
When adding vNIOS appliances to a grid, you centralize the management of core network services of the virtual appliances through the grid master. vNIOS appliances support most of the features of the Infoblox NIOS software, with some limitations as described in Appendix C, "vNIOS Appliance Limitations", on page 835.

For additional information specific to each platform, refer to the Installation Guide for vNIOS Software on Cisco Application eXtension Platforms, the Installation Guide for vNIOS Software on Riverbed Services Platforms, and the Installation Guide for vNIOS Software on VMware Platforms.

By default, grid communications use the UDP transport with a source and destination port of 1194. This port number is configurable. For a port change to take effect, one of the following must occur: the HA master fails over, the single master reboots, or the grid restarts services.

After adding an appliance or HA pair to a grid, you no longer access the Infoblox GUI on that appliance. Instead, you access the GUI running on the grid master. Although you can create multiple administrator accounts to manage different services on various grid members, all administrative access is through the grid master. So even if someone has administrative privileges to a single grid member, that administrator must access the GUI running on the grid master to manage that member.

You can access the Infoblox GUI through an HTTPS connection to one of the following IP addresses and ports on the grid master:

- The VIP address, which links to the HA port on the active node of an HA grid master
- The IP address of the LAN port on a single grid master
- The IP address of the MGMT port (if enabled) of the active node of an HA or single grid master. See Using the MGMT Port on page 240.

**Grid Communications**

The grid master synchronizes data among all grid members through encrypted VPN tunnels. The default source and destination UDP port number for VPN tunnels is 1194. You can continue using the default port number or change it. For example, if you have multiple grids, you might want each grid to use a different port so that you can set different firewall rules for each. Whatever port number you choose to use for the VPN tunnels in a grid, all the tunnels in that grid use that single port number.

Before an appliance or HA pair forms a tunnel with the master, they first authenticate each other using the Challenge-Response Authentication Mechanism (CRAM). The source and destination port number for this traffic is 2114. During the CRAM handshake, the master tells the appliance or HA pair what port number to use when building the subsequent VPN tunnel.
Another type of traffic, which flows outside the tunnels, is the VRRP (Virtual Router Redundancy Protocol) advertisements that pass between the active and passive nodes in an HA pair. The VRRP advertisements act like heartbeats that convey the status of each node in an HA pair. If the active node fails, the passive node becomes active. The VIP (virtual IP) address for that pair then shifts from the previously active node to the currently active node.

**NAT Groups**

NAT groups are necessary if the grid master is behind a NAT appliance and there are members on both sides of that NAT appliance. Any members on the same side as the master go into the same NAT group as the master and use their interface addresses for grid communications with each other. Grid members on the other side of that NAT appliance do not go in the same NAT group as the master and use the master’s NAT address for grid communications. These other members outside the NAT appliance can—but do not always need to be—in a different NAT group. To see when NAT groups become necessary for grid communications, compare Figure 5.4 below with Figure 5.5 and Figure 5.6 on page 137.
**Figure 5.4  NAT without NAT Groups**

The grid members use the addresses in **bold** for grid communications through their LAN ports.

In this case, there is no need for NAT groups. The master (Member 1) always uses its NAT address (10.1.1.10) when communicating with the grid members. Also, if you ever promote Member 3 to master, it only has to use its NAT address (10.3.3.30) to communicate with the other grid members. Whichever appliance is master (Member 1 or Member 3), there is no other member behind the same NAT appliance with which it needs to use its interface address.

**Note:** A single or HA member using its MGMT port for grid communications cannot be separated from the grid master behind a NAT appliance. For more information, see *Using the MGMT Port* on page 240.

**Figure 5.5  Grid Master in NAT Group**

Members 2 – 5 use the addresses in **black bold** for grid communications. Members 1 and 6 use their interface addresses in **underlined blue bold**.

The master (Member 1) uses its interface address (192.168.1.10) for grid communications with Member 6 and its NAT address (10.1.1.10) when communicating with the other grid members. Member 6 uses its interface address (192.168.1.60) when communicating with the master. If Member 3 (a master candidate) ever became the grid master, then both Members 1 and 6 would use their NAT addresses when communicating with it.
The same use of NAT groups that applies to a grid master also applies to master candidates. If there are no other members behind the same NAT appliance as a master candidate, then the master candidate does not need to be in a NAT group. It always uses its NAT address for grid communications. If another member is behind the same NAT appliance as the master candidate, then both the candidate and that member need to be in the same NAT group so that—if the candidate becomes master—they can use their interface addresses to communicate with each other (see Figure 5.6).

Figure 5.6 Grid Master and Master Candidate in NAT Groups

Although some members might not need to be in a NAT group, it is good practice to put all members in NAT groups in anticipation of adding or rearranging grid members within the network. For example, in Figure 5.4 – Figure 5.6, Member 4 did not need to be in a NAT group until it became configured as a master candidate in Figure 5.6. At that point, because Member 5 is also behind the same NAT appliance as Member 4, it became necessary to create NAT Group 2 and add Members 4 and 5 to it. Similarly, if you add another member behind the NAT appliance in front of Member 3, then you must create a new NAT group and add Member 3 and the new member to it. Always using NAT groups can simplify such changes to the grid and ensure that NAT appliances never interrupt grid communications.

To create a NAT group:
1. From the Grid tab, select the Grid Manager tab.
2. Expand the Toolbar and select Grid Properties -> Edit.
3. In the Grid Properties editor, select the NAT Groups tab.
4. Click the Add icon, and enter a name in the Name field and optionally, a comment in the Comment field.
5. Select one of the following:
   - Save & Close: Save the entry and close the editor.
   - Save: Save the entry and keep the editor open.
To add members to the NAT group:

1. From the Grid tab, select the Grid Manager tab -> Members tab.
2. Select a grid member and click the Edit icon.
3. In the Grid Member Properties editor, select the Network -> Advanced tab and complete the following
   - **Enable NAT compatibility**: Select this check box.
   - **NAT Group**: From the drop-down list, select the NAT group you previously created.
   - **NAT Addresses**: For a single grid master or member, enter the address configured on the NAT appliance that maps to the interface address of the LAN port. A single master or member that serves DNS uses this NAT address for grid communications and—if it serves DNS—DNS messages.
     For an HA grid master or member, enter the address configured on the NAT appliance that maps to its VIP address. An HA master uses its VIP NAT address when communicating with grid members. An HA member that serves DNS uses its VIP NAT address for its DNS messages. It uses its LAN port NAT address for grid communications.
   - **Node 1 (if HA)**
     - **NAT IP Address**: Enter the address configured on the NAT appliance that maps to the interface address of the LAN port on Node 1. When Node 1 of an HA member is active, it uses its NAT address for grid communications.
   - **Node 2 (if HA)**
     - **NAT IP Address**: Enter the address configured on the NAT appliance that maps to the interface address of the LAN port on Node 2. When Node 2 of an HA member is active, it uses its NAT address for grid communications.
4. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.

**Automatic Software Version Coordination**

When you add an appliance or HA pair to a grid as a new member, it is important that it is running the same version of software as the other members in the grid. Infoblox provides two methods for coordinating the software version:

- **Manual Upgrade and Downgrade**: Before adding an appliance or HA pair to a grid, you can manually upgrade or downgrade the software on the appliance or HA pair to the version used by the rest of the grid.
- **Automatic Upgrade and Downgrade**: The grid master automatically compares the software version of each appliance attempting to enter a grid with that in use by the rest of grid. If the versions do not match, the grid master downloads the correct version to the new appliance or HA pair.

**Note:** The grid master checks the software version every time an appliance or HA pair joins the grid. The software version check occurs during the initial join operation and when a member goes offline and then rejoins the grid.
When a single appliance attempts to join the grid for the first time, the following series of events takes place:

1. The appliance establishes an encrypted VPN tunnel with the grid master.
2. The master detects that the software version on the appliance is different from that in the rest of the grid. For example, the appliance is running NIOS 4.3r6-3 software but the rest of the grid is running NIOS 5.0r1 software.
3. The appliance downloads the NIOS 5.0r1 software from the grid master.
4. After the upgrade is complete, the NIOS application automatically restarts.
5. After the appliance reboots, it again contacts the grid master and step 1 is repeated. Because the software versions now match, the appliance can complete its attempt to join the grid.

When an HA pair attempts to join the grid for the first time, the following series of events takes place:

1. The active node of the HA pair establishes an encrypted VPN tunnel with the grid master.
2. The master detects that the software version on the node is different from that in the rest of the grid. For example, the active node is running NIOS 4.3r6-3 software but the rest of the grid is running NIOS 5.0r1 software.
3. The appliance downloads the NIOS 5.0r1 software from the grid master.
4. After the upgrade is complete, the NIOS application automatically restarts. This causes an HA failover.
5. The new active node (which was previously the passive node) attempts to join the grid, repeating steps 1 – 4.
6. When the NIOS application on the currently active node restarts, there is another failover, and the currently passive node becomes active again.
7. The active node again contacts the grid master and step 1 is repeated. Because the software versions now match, it can complete its attempt to join the grid.
Grid Bandwidth Considerations

Infoblox grid technology relies upon database replication for its core functionality. When designing a grid, it is important to consider the amount of traffic generated by this replication and the overall number of grid members. Other communication between grid members (such as log retrieval and monitoring functions) occurs as well. All of this traffic is securely communicated between the grid master and grid members through encrypted VPN tunnels.

One component of the traffic through the tunnels is database replication traffic. There are three types to consider:

- **Complete database replication to a master candidate** — Occurs when a master candidate joins or rejoins a grid. The grid master sends the complete database to a master candidate so that it has all the data it needs if it ever becomes promoted from member to master.

- **Partial database replication** — Occurs when an appliance or HA pair joins or rejoins the grid as a regular member (which is not configured as a master candidate). The grid master sends it the section of the database that mainly applies just to the member.

- **Ongoing database updates** — Occurs as changes are made to the grid configuration and data. The grid master sends all ongoing database updates to master candidates and individual member-specific updates to regular members.

  If there are no or very few DNS dynamic updates, and no or very few DHCP lease offers and renewals issued, then this type of replication traffic is minimal.

  If there are many DDNS (dynamic DNS) updates (many per second) and/or many DHCP lease offers and renewals (many per second), then the replication traffic is the largest component of the VPN traffic among grid members.

**Note:** A grid master replicates data to single members and to the active node of HA members. The active node then replicates the data to the passive node in the HA pair.

At a minimum, there must be 256 Kbps (kilobits per second) bandwidth between the grid master and each member, with a maximum round-trip delay of 500 milliseconds. For ongoing database updates, the amount of data sent or received is 15 Kb for every DDNS update, and 10 Kb for every DHCP lease offer/renew. The baseline amount for heartbeat and other maintenance traffic for each member is 2 Kbps. Measure the peak DNS and DHCP traffic you see in your network to determine the bandwidth needed between the grid master and its members for this activity.

For example, you might decide to place your grid members in the locations shown in *Figure 5.6* on page 137.
In this example, the grid master is optimally placed in the Data Center West. There are a total of seven members: the HA grid master, three HA members, and three single members. If all the members are master candidates, the grid master replicates all changes to the other six members. Assuming that the master receives 20 dynamic updates per minute and 40 DHCP lease renewals per minute, the calculation for grid bandwidth is:

\[
\begin{align*}
\text{20 DDNS updates/minute/60 secs} & = 0.333 \text{ DDNS updates/sec} \times 15 \text{ Kb} \times 6 \text{ members} = 30 \text{ Kbps} \\
\text{40 DHCP leases/minute/60 secs} & = 0.666 \text{ DHCP leases/sec} \times 10 \text{ Kb} \times 6 \text{ members} = 40.2 \text{ Kbps} \\
\text{2 Kbps of grid maintenance traffic} & = 12 \text{ Kbps} \\
\text{Total} & = 82.2 \text{ Kbps}
\end{align*}
\]

Another component is the upgrade process. See *Upgrading NIOS Software* on page 278 for more information. Bandwidth requirements, database size, and update rate determine the maximum size of the grid you can deploy. Based on the various factors discussed above, you can determine the amount of bandwidth your grid needs. If your calculations exceed the available bandwidth, then you might need to modify your deployment strategy, perhaps by splitting one large grid into two or more smaller ones.

**Note:** This calculation does not take into account existing traffic other than DNS and DHCP services, so factor and adjust accordingly.

For international networks, because of bandwidth and delay requirements, a geographical grouping of grid members might be the best approach. For example, if you have a global presence, it may make the most sense to have a North American grid, a South American grid, a European grid, and an Asia/Pacific grid.
About HA Pairs

You can configure two appliances as an HA (high availability) pair to provide hardware redundancy for core network services. An HA pair can be a grid master, a grid member, or an independent appliance. The two nodes that form an HA pair—identified as Node 1 and Node 2—are in an active/passive configuration. The active node receives, processes, and responds to all service requests. The passive node constantly keeps its database synchronized with that of the active node, so it can take over services if a failover occurs. A failover is the reversal of the active/passive roles of each node; that is, when a failover occurs, the previously active node becomes passive and the previously passive node becomes active.

The appliance uses the following components in the HA functionality:

- **bloxSYNC**: An Infoblox proprietary mechanism for secure, real-time synchronization of the database that maintains the data, system configuration, and protocol service configuration between the two nodes. With bloxSYNC, the nodes continuously synchronize changes of their configurations and states. When a failover occurs, the passive node can quickly take over services. For information, see *About HA Failover* on page 143.

- **VRRP (Virtual Router Redundancy Protocol)**: An industry-standard, MAC-level HA failover mechanism. VRRP utilizes the concept of an active and passive node that share a single VIP (virtual IP) address. When the active node that owns the VIP becomes unavailable, the passive node takes over the VIP and provides network core services. For information about VRRP, refer to RFC3768, *Virtual Router Redundancy Protocol (VRRP)* and *VRRP Advertisements* on page 144.

Using bloxSYNC and VRRP combined, if the active node fails or is taken offline for maintenance purposes, the passive node assumes the VIP and continues to respond to requests and services with minimal interruption. You can deploy an HA pair as a grid master, a grid member, and an independent HA pair. To deploy an independent HA pair, see *Deploying an Independent HA Pair* on page 186. To deploy an HA grid master, see *Creating a Grid Master* on page 145.

Planning for an HA Pair

To achieve high availability, the HA and LAN ports on both the active and passive nodes are connected to switches on the same network or VLAN. Both nodes in an HA pair share a single VIP address and a virtual MAC address so they can appear as a single entity on the network. As illustrated in *Figure 5.9*, the VIP and virtual MAC addresses link to the HA port on each node. Select five IP addresses on the same network before you configure an HA pair, as follows:

- **VIP**: For core network services and for management purposes when the MGMT port is disabled. Both nodes share the same VIP.
- **Node 1 HA (active)**: Source IP for the VIP and VRRP advertisements
- **Node 1 LAN (active)**: For management through SSHv2 and listens for VRRP advertisements from the HA port
- **Node 2 HA (passive)**: Listens for VRRP advertisements
- **Node 2 LAN (passive)**: Source IP for SSL VPN to the VIP of the active node and receives bloxSYNC from the VIP

*Figure 5.9 HA Pair*
About HA Failover

The appliance supports HA through bloxHA™, which provides a robust failover mechanism. As described in Planning for an HA Pair on page 142, both nodes in an HA pair share a single VIP address and a virtual MAC address. The node that is currently active is the one whose HA port owns the VIP address and virtual MAC address. When a failover occurs, these addresses shift from the HA port of the previous active node to the HA port of the new active node, as illustrated in Figure 5.10.

Figure 5.10 VIP Address and Virtual MAC Address and HA Failover

After an HA failover occurs, Node 2 becomes the active node. Because Node 2 is now active, it now owns the VIP address and virtual MAC address.
VRRP Advertisements

VRRP advertisements are periodic announcements of the availability of the HA node linked to the VIP. The two nodes in an HA pair include a VRID (virtual router ID) in all VRRP advertisements and use it to recognize VRRP advertisements intended for themselves. Only another appliance on the same subnet configured to use the same VRID responds to the announcements. The active node in an HA pair sends advertisements as multicast datagrams every second. It sends them from its HA port using the source IP address of the HA port (not from the VIP address) and the source MAC address 00:00:5e:00:01:vrrp_id. The last two hexadecimal numbers in the source MAC address indicate the VRID number for this HA pair. For example, if the VRID number is 143, then the source MAC address is 00:00:5e:00:01:8f (8f in hexadecimal notation = 143 in decimal notation).

The destination MAC and IP addresses for all VRRP advertisements are 01:00:5e:00:00:12 and 224.0.0.18. Because a VRRP advertisement is a multicast datagram that can only be sent within the immediate logical broadcast domain, the nodes in an HA pair must be in the same subnet together.

As illustrated in Figure 5.11, when you configure an HA pair, only the appliance configured to listen for VRRP advertisements with the same VRID number processes the datagrams, while all other appliances ignore them. The passive node in an Infoblox HA pair listens for these on its HA port and the active node listens on its LAN port. If the passive node does not receive three consecutive advertisements or if it receives an advertisement with the priority set to 0 (which occurs when you manually perform a forced failover or request the active node to restart, reboot, or shut down), it changes to the active state and assumes ownership of the VIP address and virtual MAC address.

If both nodes go offline, the one that comes online first becomes the active node. If they come online simultaneously, or if they enter a dual-active state—that is, a condition arises in which both appliances assume an active role and send VRRP advertisements, possibly because of network issues—then the appliance with the numerically higher VRRP priority becomes the active node. The priority is based on system status and events.

If both nodes have the same priority, then the appliance whose HA port has a numerically higher IP address becomes the active node. For example, if the IP address of the HA port on Node 1 is 10.1.1.80 and the IP address of the HA port on Node 2 is 10.1.1.20, then Node 1 becomes the active node.

For more information about VRRP, see RFC 3768, Virtual Router Redundancy Protocol (VRRP).

If both nodes have the same priority, then the appliance whose HA port has a numerically higher IP address becomes the active node. For example, if the IP address of the HA port on Node 1 is 10.1.1.80 and the IP address of the HA port on Node 2 is 10.1.1.20, then Node 1 becomes the active node.

For more information about VRRP, see RFC 3768, Virtual Router Redundancy Protocol (VRRP).

Figure 5.11  VRRP Advertisements with a Unique VRID

After you finish configuring Node 1 of the HA pair to use VRID 143—a number that is unique for this subnet—it starts listening for VRRP advertisements with that VRID. When it does not receive any for three seconds, it becomes the active node in the HA pair and begins multicasting VRRP advertisements with a VRID 143 from its HA port.

Any device on that subnet that is not configured to listen for VRRP advertisements with VRID 143 drops the packet.

After you finish configuring Node 2 to join the HA pair, it initiates a connection with Node 1. The two appliances establish a VPN tunnel between themselves, using the HA connection name and shared secret to authenticate each other. Node 2 downloads the database from Node 1 and learns its VRID. Node 2 then begins listening for VRRP advertisements on its HA port. When it receives an advertisement from Node 1, Node 2 recognizes it and becomes the passive node.
CREATING A GRID MASTER

To create a grid, you first create a grid master and then add members. Although the grid master can be a single appliance (a “single master”), a more resilient design is to use an HA pair (an “HA master”) to provide hardware redundancy. For information about HA pairs, see About HA Pairs on page 142. The basic procedure for forming two appliances into an HA master is shown in Figure 5.12. All Infoblox hardware platforms, except for the Infoblox-250 and -250-A, support configuration as a grid master or grid master candidate. For information about which vNIOS appliance supports configuration as a grid master, see Supported vNIOS Appliance Configurations on page 835.

Figure 5.12 Initially Configuring a Pair of Appliances as a Grid Master

1. Connect your management system to a switch and set its IP address to 192.168.1.3.
2. Connect Node 1 to the switch, log in to its default IP address (192.168.1.2), check that a Grid license is installed, and configure the following:
   - VIP address, netmask, gateway
   - Hostname
   - HA and LAN addresses of Node 1
   - HA and LAN addresses of Node 2
   - VRID (virtual router ID)
   - NTP settings
   - Grid name
   - Shared secret

3. After you configure Node 1, it listens for three seconds for VRRP advertisements containing its VRID number. When it does not receive any, it assumes the active role in the HA pair and starts sending advertisements.

   Note: For more information about VRRP advertisements, see VRRP Advertisements on page 144.

4. Connect Node 2 to the switch, log in to its default IP address (192.168.1.2), check that a Grid license is installed, and configure the following:
   - VIP address (for Node 1)
   - LAN address, netmask, gateway
   - Hostname
   - Grid name
   - Shared secret

   Note: Because you do not set the VRID for Node 2, it cannot listen for VRRP advertisements yet. It learns its VRID after it joins the grid and downloads the database from Node 1. Then, when Node 2 receives an advertisement containing its VRID from Node 1, it assumes the passive role in the HA pair.

5. After you configure Node 2, it contacts the VIP address on Node 1 and initiates a key exchange using the shared secret. The nodes then construct an encrypted VPN tunnel to secure grid communications.

After the two nodes form an HA pair, Node 2 initiates a key exchange and creates an encrypted VPN tunnel with Node 1. The two nodes communicate between the VIP interface linked to the HA port on Node 1 and the LAN port on Node 2. The initialization of VPN communications between the two nodes is shown in Figure 5.13 on page 146.
After the nodes establish a VPN tunnel between themselves, Node 1 sends Node 2 its entire database (its configuration settings and service data). Because the configuration contains the VRID (virtual router ID) for the HA pair, Node 2 starts listening for VRRP advertisements containing that VRID number. Because Node 1 is already sending such advertisements, Node 2 receives one and assumes the passive role in the HA pair.

After the initial transmission of its database, Node 1 continues to send Node 2 real-time database updates through the VPN tunnel.

Node 1 maintains the synchronization of the database throughout the grid—which, at this point, has no other members—sends VRRP advertisements indicating its physical and network health, and—if configured to do so—provides network services. Node 2 maintains a state of readiness to assume mastership in the event of a failover. You can see the flow of HA- and grid-related traffic from ports on the active node to ports on the passive node in Figure 5.14. This illustration also shows the ports that you can use for management traffic and network service.
From the management system, you can manage the active node of the HA master by making an HTTPS connection to the VIP interface and using the GUI, and by making an SSHv2 connection to the LAN port (and MGMT port, if enabled) and using the CLI. If you enable the MGMT port on an HA pair, you can make an HTTPS connection through the MGMT port on the active node, and you can make an SSHv2 connection through the LAN or MGMT port on the active and passive nodes.

**Note:** For information about enabling and using the MGMT port, the Infoblox GUI, and SSH, see *Using the MGMT Port* on page 240, *Logging in to the GUI* on page 35, and *Enabling Remote Console Access* on page 227.

---

**Port Numbers for Grid Communication**

If connectivity between grid members must pass through a firewall, the firewall policies must allow the initial key exchange and subsequent VPN traffic to pass. The key exchange uses UDP with a source and destination port of 2114. VPN traffic uses UDP with a default source and destination port of 1194. The VPN port number is configurable.

To configure the VPN port number:

1. From the Grid tab, select the Grid Manager tab.
2. Expand the Toolbar and click Grid Properties -> Edit.
3. In the General tab of the Grid Properties editor, type a new port number in the VPN Port field.
4. Click Save & Close.

After changing the port number, you must restart grid services.

A member and master first perform a handshake to authenticate each other and exchange encryption keys. Then they build an encrypted VPN tunnel between themselves. The member typically initiates both of these connections. The master only initiates a key exchange if you manually promote a member to the role of master (see *Promoting a Master Candidate* on page 168). *Figure 5.13* on page 146 shows the typical connection exchange and default port usage not only between the two nodes forming an HA pair but also between a member and master when the member joins a grid. The member and master key exchange occurs when an appliance joins a grid, during master promotion, and when a member reconnects to a grid after becoming disconnected. At all other times, grid-related communications occur through encrypted VPN tunnels.

**Grid Setup Wizard**

The Grid Setup Wizard simplifies configuring a grid. You can use it to configure an HA or single grid master and to join appliances to a grid. The Grid Setup Wizard appears when you first log in to the appliance. After that, you can access it at anytime as follows:

1. From the Grid tab, select the Grid Manager tab -> Members tab.
2. Expand the Toolbar and click Grid Properties -> Setup (Grid Setup Wizard).

**Creating an HA Grid Master**

To create a grid, you first create a grid master and then add members. Although you can define a single appliance as a grid master, using an HA pair provides hardware redundancy for this vital component of a grid. The following procedure explains how to put two NIOS appliances on the network and use the Grid Setup Wizard to configure them as Nodes 1 and 2 to form an HA grid master. For information about which vNIOS appliance supports configuration as an HA grid master, see *Supported vNIOS Appliance Configurations* on page 835.
Deploying a Grid

Configuring the Connecting Switch

To ensure that VRRP (Virtual Router Redundancy Protocol) works properly, configure the following settings at the port level for all the connecting switch ports (HA, LAN1, and LAN2):

- Trunking: Disable
- EtherChannel: Disable
- IGMP Snooping: Disable
- Port Channeling: Disable
- Speed and Duplex settings: Match these settings on both the Infoblox appliance and switch
- Disable other dynamic and proprietary protocols that might interrupt the forwarding of packets

**Note:** By default, a NIOS appliance automatically negotiates the optimal connection speed and transmission type (full or half duplex) on the physical links between its LAN1, HA, and MGMT ports and the Ethernet ports on the connecting switch. If the two appliances fail to auto-negotiate the optimal settings, see *Modifying Ethernet Port Settings* on page 235 for steps you can take to resolve the problem.

Putting Both Appliances on the Network

1. Connect the power cable from each NIOS appliance to a power source and turn on the power. If possible, connect the appliances to separate power circuits. If one power circuit fails, the other might still be operative.
2. Connect Ethernet cables from the LAN1 port and the HA port on each appliance to a switch on the network.

**Note:** The Ethernet ports on the Infoblox-250, -250-A, -550, -550-A, -1050, -1050-A, -1550, -1550-A, -1552, -1552-A, 1852-A, -2000, and -2000-A appliances are autosensing, so you can use either a straight-through or cross-over Ethernet cable for these connections.

3. Use the LCD on one appliance or make a console connection to it, and configure the network settings of its LAN1 port so that it is on the local subnet and you can reach it on the network.

**Note:** For details about using the LCD and console, refer to the installation guide that shipped with your product.

4. Similarly, configure the LAN1 port on the other appliance so that it is in the same subnet as the first appliance.
5. Connect your management system to the network so that it can reach the IP addresses of the LAN1 ports.

HA Master – Node 1

1. On your management system, open a browser window, and connect to https://ip_addr, where ip_addr is the address of the LAN1 port on Node 1.
2. Log in using the default user name and password admin and infoblox. For detailed information about logging in to the GUI, see *Logging in to the GUI* on page 35.
3. Review the End-User License Agreement and click I Accept.
   The Grid Setup wizard appears.
4. On the first screen, select Configure a Grid Master and click Next.
5. On the next screen, specify the grid properties and click Next:
   - **Grid Name:** Enter a text string that the two appliances use to authenticate each other when establishing a VPN tunnel between them. The default grid name is Infoblox.
   - **Shared Secret:** Enter a text string that both appliances use as a shared secret to authenticate each other when establishing a VPN tunnel between them. The default shared secret is test.
   - **Show Password:** Select this to display the password. Clear the check box to conceal the password.
— **Hostname**: Enter a valid domain name for the appliance.
— **Is the Grid Master an HA pair?**: Select Yes.

6. On the next screen, specify the network properties and click **Next**:
   — **Virtual Router ID**: Enter the VRID (virtual router ID). This must be a unique VRID number—from 1 to 255—for this subnet.
   — **Required Ports and Addresses**: Enter information about the following interfaces: VIP, Node 1 HA and LAN ports, Node 2 HA and LAN ports. Some fields are prepopulated by Grid Manager based on the existing configuration of the appliance. All fields are required.
   — IP address and subnet mask
   — IP address of the gateway for the subnet on which the interfaces are set. This is the same for all interfaces.
   — Select the port setting from the drop-down list. It displays all settings supported by the hardware type.

7. Optionally, enter a new password and click **Next**. The password must be a single string (no spaces) that is at least four characters long.

8. Select the time zone of the grid master and indicate whether the grid master synchronizes its time with an NTP (Network Time Protocol) server.
   — If you choose to enable NTP, click the Add icon and enter the IP address of an NTP server. You can enter IP addresses for multiple NTP servers.
   — If you choose to disable NTP, set the date and time for the appliance.
   — Click **Next**.

9. The last screen displays the settings you specified in the previous panels of the wizard. Verify that the information is correct and click **Finish**. The application restarts after you click **Finish**.

**Note:** The Grid Setup wizard provides options such as not changing the default password and manually entering the time and date. However, changing the password and using an NTP server improve security and accuracy (respectively), and so these choices are presented here.

Record and retain this information in a safe place. If you forget the shared secret, you need to contact Infoblox Technical Support for help. When you add an appliance to the grid, you must configure it with the same grid name, shared secret, and VPN port number that you configure on the grid master.

10. Close the management window.
    The configuration for Node 1 is complete.
HA Master – Node 2
1. On your management system, open a new browser window, and connect to https://ip_addr, where ip_addr is the address of the LAN1 port on Node 2.
2. Log in using the default user name and password admin and infoblox.
3. Review the End-User License Agreement and click I Accept.
   The Grid Setup wizard appears.
4. On the first screen, select Join Existing Grid and click Next.
5. On the next screen, specify the grid properties and click Next
   — Grid Name: Enter a text string that the two appliances use to authenticate each other when establishing a VPN tunnel between them. This must match the grid name you entered for node 1.
   — Grid Master’s IP Address: Enter the same VIP you entered for node 1.
   — Shared Secret: Enter a text string that both appliances use as a shared secret to authenticate each other when establishing a VPN tunnel between them. This must match your entry in node 1.
6. On the next screen verify the IP address settings of the member and click Next
7. The last screen displays the settings you specified in the previous panels of the wizard. Verify that the information is correct and click Finish.
   The setup of the HA master is complete. From now on, when you make an HTTPS connection to the HA pair, use the VIP address.

Creating a Single Grid Master
Although using an HA master is ideal because of the hardware redundancy it provides, you can also use a single appliance as the grid master. Infoblox recommends frequent backups if the grid master is a single appliance, and there is no master candidate. For information about which vNIOS appliance supports configuration as a single grid master, see Supported vNIOS Appliance Configurations on page 835.
Setting up an appliance as a single grid master is very easy. If the appliance has the DNSOne package with the Grid upgrade, it is already a grid master. You simply need to define the network settings for its LAN1 port. The various procedures for defining the network settings for the LAN1 port of a single independent appliance apply here as well; that is, you can use any of the following procedures to define the network settings for the LAN1 port of the appliance that you want to make a single grid master:
• LCD – See Method 1 – Using the LCD on page 176.
• Console port – Method 2 – Using the CLI on page 176.
You can also use the NIOS Grid Setup Wizard to create a single grid master. In addition to providing a simple method accompanied by helpful information, the setup wizard allows you to change the admin password and configure time settings for the appliance.

Using the Setup Wizard
To create a single grid master using the Grid Setup wizard:
1. Connect the power cable from the NIOS appliance to a power source and turn on the power.
2. Connect an Ethernet cable from the LAN 1 port on the appliance to a switch on the network.

3. If you have not changed the default IP address (192.168.1.2/24) of the LAN1 port through the LCD or CLI—and the subnet to which you connect the appliance does not happen to be 192.168.1.0/24—put your management system in the 192.168.1.0/24 subnet and connect an Ethernet cable between your management system and the NIOS appliance.
4. Open a web browser and make an HTTPS connection to the IP address of the LAN1 port. To reach the default IP address, enter: https://192.168.1.2.

Several certificate warnings appear during the login process. This is normal because the preloaded certificate is self-signed (and, therefore, is not in the trusted certificate stores in your browser) and has the hostname www.infoblox.com, which does not match the destination IP address you entered in step 3. To stop the warning messages from occurring each time you log in to the GUI, you can generate a new self-signed certificate or import a third-party certificate with a common name that matches the FQDN (fully qualified domain name) of the appliance. For information about certificates, see Managing Certificates on page 36.

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

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

The Grid Setup wizard appears.

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

8. On the next screen, specify the grid properties and click Next:
   - Grid Name: Enter a text string that the grid master and appliances joining the grid use to authenticate each other when establishing a VPN tunnel between them. The default grid name is Infoblox.
   - Shared Secret: Enter a text string that the grid master and appliances joining the grid use as a shared secret to authenticate each other when establishing a VPN tunnel between them. The default shared secret is test.
   - Show Password: Select this to display the password. Clear the check box to conceal the password.
   - Hostname: Enter a valid domain name for the appliance.
   - Is the Grid Master an HA pair?: Select No.

9. On the next screen, configure the network settings and click Next:
   - Host Name: Enter a valid domain name for the appliance.
   - IP Address: Displays the IP address of the LAN port.
   - Subnet Mask: Displays the subnet mask of the LAN port.
   - Gateway: Displays the IP address of the gateway of the subnet on which the LAN port is set.
   - Port Settings: Select the port setting from the drop-down list. It displays all settings supported by the hardware type. For information, see Modifying Ethernet Port Settings on page 235.

10. Optionally, enter a new password and click Next. The password must be a single hexadecimal string (no spaces) that is at least four characters long.

11. Select the time zone of the grid master and indicate whether the grid master synchronizes its time with an NTP (Network Time Protocol) server, and then click Next.
   - If you choose to enable NTP, click the Add icon and enter the IP address of an NTP server. You can enter IP addresses for multiple NTP servers.
   - If you choose to disable NTP, set the date and time for the appliance.

12. The last screen displays the settings you specified in the previous panels of the wizard. Verify that the information is correct and click Finish. The application restarts after you click Finish.

   **Note:** The Grid Setup wizard provides options such as not changing the default password and manually entering the time and date. However, changing the password and using an NTP server improve security and accuracy (respectively), and so these choices are presented here.

   Record and retain this information in a safe place. If you forget the shared secret, you need to contact Infoblox Technical Support for help. When you add an appliance to the grid, you must configure it with the same grid name, shared secret, and VPN port number that you configure on the grid master.

The last screen of the setup wizard states that the changed settings require the appliance to restart. When you click Finish, the appliance restarts.

The setup of the single master is complete. From now on, when you make an HTTPS connection to the appliance, use its new IP address.
**Deploying a Grid**

**Adding Grid Members**

You can add single appliances and HA pairs to a grid, forming single members and HA members respectively. A single grid member can be either an Infoblox appliance or a vNIOS appliance. For information about which vNIOS appliance supports configuration as an HA grid member, see Supported vNIOS Appliance Configurations on page 835.

You can also define an HA member on the grid master and then add two individual NIOS appliances to the grid as Node 1 and Node 2 to complete the HA member you defined on the master.

New members inherit all settings that you create at the grid level unless you override them at the member level.

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

1. Configuring the member on the grid master. In addition to defining the network and appliance settings for a member, you can also configure service settings before you join the appliance or HA pair to the grid.

2. Joining the appliance or HA pair to the grid. This includes defining the VIP or IP address of the grid master, the grid name, and the shared secret on the single appliance or HA pair. If an appliance or HA pair cannot join the grid because of MTU (maximum transmission unit) limitations on its network link, you can reduce the MTU that the master uses when communicating with it. See Setting the MTU for VPN Tunnels on page 168.

If the grid master is behind a NAT device and there are members on both sides of that NAT device, you must create a NAT group, as described in NAT Groups on page 135.

**Adding a Single Member**

The basic steps necessary to add a single member are as follows:

1. Define the network settings of the LAN port of the single appliance on the grid master.

2. Initiate the join grid operation during which you specify the VIP or IP address of the grid master, the grid name, and the shared secret on the single appliance. For information, see Joining Appliances to a Grid on page 154.

In addition, you can configure on the grid master the service settings such as DNS zones and records, DHCP networks and address ranges, and so on for a member before or after you join the appliance to the grid. The basic steps for adding a single member are presented below.

For information on how to configure a vNIOS appliance as a grid member, refer to the Quick Start Guide for Installing vNIOS Software on Riverbed Services Platforms, the Quick Start Guide for Installing vNIOS Software on Cisco Application eXtension Platforms, and the Quick Start Guide for Installing vNIOS Software on VMware Platforms.

**Configuring a Single Member on the Grid Master**

1. From the Grid tab, select the Grid Manager tab -> Members tab.

2. Expand the Toolbar and click Add -> Add Grid Member.

3. In the Add Grid Member wizard, enter the following and click Next:

   - **Member Type**: Specify the appliance type of the grid member. If the member is an Infoblox appliance, select Infoblox, which is the default. For a vNIOS appliance, select Cisco, Riverbed, or Virtual NIOS for VMware.

   - **Host Name**: Type the FQDN (fully qualified domain name) of the appliance that you are adding to the grid.

   - **Time Zone**: If the grid member is in a different time zone from the grid, click Override and select a time zone.

   - **Comment**: Type a comment that provides some useful information about the appliance, such as its location.

   - **Master Candidate**: Select this option to designate this appliance as a master candidate. For supported vNIOS appliances, see Supported vNIOS Appliance Configurations on page 835.
4. Enter the following information about the member that you are adding to the grid and click **Next**:
   - **Standalone Member**: Select this option.
   - **Address**: Type the IP address of the LAN1 port.
   - **Subnet Mask**: Choose the netmask for the subnet to which the LAN1 port connects.
   - **Gateway**: Type the IP address of the default gateway of the subnet to which the LAN1 port connects.
   - **Port Settings**: The default is automatic. You can select another port setting from the drop-down list. For information, see *Modifying Ethernet Port Settings* on page 235.

5. Optionally, define extensible attributes. For information, see *About Extensible Attributes* on page 222.

6. Do one of the following:
   - Click **Save & Edit** to add the single member to the grid and launch the editor. You can configure additional properties, such as the MTU size, or add the member to a NAT group.
   - Click **Save & New** to add the single member to the grid and launch the wizard again to add another member.
   - Click **Save & Close** to add the single member to the grid and close the wizard.

**Adding an HA Member**

The basic steps necessary to add an HA member are as follows:

1. Define the network settings of the HA pair on the grid master.
2. Initiate the join grid operation, during which you specify the VIP or IP address of the grid master, the grid name, and the shared secret on the HA pair. For information, see *Joining Appliances to a Grid* on page 154.

In addition, on the grid master you can configure the service settings such as DNS zones and records, DHCP networks and address ranges, and so on for a member before or after you join the HA pair to the grid. The basic steps for adding an HA member are presented below.

**Note:** The procedure for adding an HA pair to a grid when it uses the MGMT port of the active node for grid communications differs slightly from that described below. See *Grid Communications* on page 243.

**Configuring an HA Member on the Grid Master**

1. From the Grid tab, select the Grid Manager tab -> Members tab.
2. Expand the Toolbar and click Add -> Add Grid Member.
3. In the Add Grid Member wizard, enter the following and click **Next**:
   - **Member Type**: Specify the appliance type of the grid member. If the member is an Infoblox appliance, select Infoblox, which is the default. For a vNIOS appliance on VMware, select Virtual NIOS.
   - **Host Name**: Type the FQDN (fully qualified domain name) for the HA member.
   - **Time Zone**: If you want the grid member to have a different time zone, click Override and select a time zone.
   - **Comment**: Type a comment that provides some useful information about the appliance, such as its location.
   - **Master Candidate**: select this check box to designate this appliance as a master candidate. For supported vNIOS appliances, see *Supported vNIOS Appliance Configurations* on page 835.

4. Enter the following information about the member that you are adding to the grid and click **Next**:
   - **High Availability Pair**: Select this option.
   - **Virtual Router ID**: Enter a unique VRID number—from 1 to 255—for the local subnet.
   - **Required Ports and Addresses**: Enter information about the following interfaces: VIP, Node 1 HA and LAN ports, Node 2 HA and LAN ports. The VIP address and the IP addresses for all the ports must be in the same subnet. All fields are required.
   - **IP address and subnet mask**
   - **IP address of the gateway for the subnet on which the interfaces are set. This is the same for all interfaces.**
Deploying a Grid

1. Select the port setting from the drop-down list. It displays all settings supported by the hardware type. For information, see Modifying Ethernet Port Settings on page 235.

5. Optionally, define extensible attributes. For information, see Using Extensible Attributes on page 225.

6. Do one of the following:
   - Click Save & Edit to add the HA member to the grid and launch the editor. You can configure additional properties, such as the MTU size, or add the member to a NAT group.
   - Click Save & New to add the HA member to the grid and launch the wizard again to add another member.
   - Click Save & Close to add the HA member to the grid and close the wizard.

Joining Appliances to a Grid

You can use the Grid Setup Wizard or access the Join Grid dialog box to join appliances to a grid. The Grid Setup Wizard launches when you first log in to an appliance. You can also launch it from the Toolbar as described in Grid Setup Wizard on page 147.

To join a single appliance and HA pair to a grid using the Grid Manager GUI:

1. Log in to the appliance or HA pair that you want to add to the grid. The appliance or HA pair must be online and able to reach the grid master.

2. From the Grid tab, select the Grid Manager tab -> Members tab.

3. Expand the Toolbar and click Join Grid.

4. In the Join Grid dialog box, enter the following:
   - Virtual IP of Grid Master: Type the VIP address of the HA grid master or the LAN address of the single grid master for the grid to which you want to add the appliance.
   - Grid Name: Type the name of the grid.
   - Grid Shared Secret: Type the shared secret of the grid.
   - Use MGMT port to join grid: If you have already enabled the MGMT port (see Grid Communications on page 243), this option becomes available. Select it to connect to the grid through the MGMT port.

5. Click OK to begin the join operation.

To confirm that the appliance has successfully joined the grid, log in to the grid master and navigate to the Grid tab, select the Grid Manager -> Members tab. This panel lists the grid members. Check the icon in the Status column of the newly added member. (green = the appliance has joined the grid and is functioning properly; yellow = the appliance is in the process of joining the grid; red = the appliance has not joined the grid). You can also use the CLI command set network to join an appliance to a grid.

To join a single appliance and HA pair to a grid using the Grid Setup Wizard:

1. Log in to the appliance or HA pair that you want to add to the grid. The appliance or HA pair must be online and able to reach the grid master.

2. From the Grid tab, select the Grid Manager tab -> Members tab.

3. Expand the Toolbar and click Grid Properties -> Setup (Grid Setup Wizard).

4. On the next screen, specify the grid properties and click Next
   - Grid Name: Enter a text string that the two appliances use to authenticate each other when establishing a VPN tunnel between them. This must match the grid name you entered for node 1.
   - Grid Master's IP Address: Enter the same VIP you entered for node 1.
   - Shared Secret: Enter a text string that both appliances use as a shared secret to authenticate each other when establishing a VPN tunnel between them. This must match your entry in node 1.

5. On the next screen verify the IP address settings of the member and click Next
6. The last screen displays the settings you specified in the previous panels of the wizard. Verify that the information is correct and click Finish.

To confirm that the appliance has successfully joined the grid, log in to the grid master and navigate to the Grid tab, select the Grid Manager -> Members tab. This panel lists the grid members. Check the icon in the Status column of the newly added member. (green = the appliance has joined the grid and is functioning properly; yellow = the appliance is in the process of joining the grid; red = the appliance has not joined the grid). You can also use the CLI command `set network` to join an appliance to a grid.

---

**Configuration Example: Configuring a Grid**

In this example, you configure seven NIOS appliances in a grid serving internal DHCP and DNS for an enterprise with the domain name `corp100.com`. There are four sites: HQ and three branch offices. A hub-and-spoke VPN tunnel system connects the sites, with HQ at the hub. The distribution and roles of the NIOS appliances at the four sites are as follows:

- **HQ site (four appliances in two HA pairs):**
  - HA grid master – hidden primary DNS server
  - HA member – secondary DNS server and DHCP server for HQ

- **Site 1 (two appliances in an HA pair):** HA member – secondary DNS server and DHCP server for Site 1

- **Site 2 (one appliance):** single member – secondary DNS server and DHCP server for Site 2

**Note:** When adding an Infoblox appliance to an existing grid, you must first check whether the grid is running the minimum required software release of the appliance. For information, refer to the document, *Minimum Required Release Software for Hardware Platforms*, that was shipped with your product.

To create a grid, you first create a grid master and then add members. The process involves these three steps:

1. Configuring two appliances at HQ as the grid master. See *Create the Grid Master* on page 157.
2. Logging in to the grid master and defining the members that you want to add to the grid; that is, you configure grid member settings on the grid master in anticipation of later joining those appliances to the grid. See *Define Members on the Grid Master* on page 159.
3. Logging in to the individual appliances and configuring them so that they can reach the grid master over the network and join the grid. See *Join Appliances to the Grid* on page 160.

After creating the grid and adding members, you use the Data Import Wizard to import DHCP and DNS data from legacy servers. See *Import DHCP Data* on page 162 and *Import DNS Data* on page 163.

Finally, you transition DHCP and DNS service from the legacy servers to the Infoblox grid members. See *Enable DHCP and Switch Service to the Grid* on page 167.
Deploying a Grid

Figure 5.15 Network Diagram
Cable All Appliances to the Network and Turn On Power

Cable the NIOS appliances to network switches. After cabling each appliance to a switch and connecting it to a power source, turn on the power. For information about installing and cabling the appliance, refer to the user guide or installation guide that ships with the product.

1. At HQ and Site 1, connect Ethernet cables from the LAN1 and HA ports on the appliances in each HA pair to a switch, connect the appliances to power sources, and turn on the power for each appliance.

   **Note:** When connecting the nodes of an HA pair to a power source, connect each node to a different power source if possible. If one power source fails, the other might still be operative.

2. At Site 2, connect an Ethernet cable from the LAN1 port on the single appliance to a switch, connect the appliance to a power source, and turn on the power for that appliance.

Create the Grid Master

Configure two appliances at HQ to be the two nodes that make up the HA pair forming the grid master.

Grid Master – Node 1

1. By using the LCD or by making a console connection to the appliance that you want to make Node 1 of the HA pair for the grid master, change the default network settings of its LAN1 port to the following:
   - IP Address: 10.0.1.6
   - Netmask: 255.255.255.0
   - Gateway: 10.0.1.1

2. Connect your management system to the HQ network, open a browser window, and connect to https://10.0.1.6.

3. Log in using the default user name and password **admin** and **infoblox**.

4. Review the End-User License Agreement and click I Accept. The Grid Setup Wizard appears.

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

6. Specify the grid properties:
   - **Grid Name:** Enter **corp100**.
   - **Shared Secret:** Enter **Mg1kW17d**.
   - **Show Password:** Clear the check box to conceal the password.
   - **Hostname:** Enter **ns1.corp100.com**.
   - **Is the Grid Master an HA pair?** Select Yes.

7. Specify the network properties and click Next:
   - **Virtual Router ID:** Enter **143**.
   - **Required Ports and Addresses:** Enter the following to set up the HA pair:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Address</th>
<th>Subnet Mask</th>
<th>Gateway</th>
<th>Port Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP</td>
<td>10.0.1.10</td>
<td>255.255.255.0</td>
<td>10.0.1.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node 1 HA</td>
<td>10.0.1.7</td>
<td>255.255.255.0</td>
<td>10.0.1.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node 2 HA</td>
<td>10.0.1.9</td>
<td>255.255.255.0</td>
<td>10.0.1.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node 1 LAN</td>
<td>10.0.1.6</td>
<td>255.255.255.0</td>
<td>10.0.1.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node 2 LAN</td>
<td>10.0.1.8</td>
<td>255.255.255.0</td>
<td>10.0.1.1</td>
<td>Automatic</td>
</tr>
</tbody>
</table>
8. Enter a new password: `1n85w2IF`. Retype it and click Next.
9. Complete the following:
   - **Time zone**: Select *(UTC – 8:00 Pacific Time (US and Canada), Tijuana)*
   - Enable NTP, click the Add icon and enter the IP address of the NTP server: `3.3.3.3`
10. Click Finish.
    When you click Finish, the Infoblox GUI application restarts.

**Grid Master – Node 2**

1. By using the LCD or by making a console connection to the appliance that you want to make Node 2 of the HA pair for the grid master, change the default network settings of its LAN1 port to the following:
   - IP Address: `10.0.1.8`
   - Netmask: `255.255.255.0`
   - Gateway: `10.0.1.1`
2. In the login window, type `10.0.1.8` in the Hostname field.
3. Log in using the default user name and password `admin` and `infoblox`.
4. From the Grid tab, select the Grid Manager tab -> Members tab -> member check box.
5. Expand the Toolbar and click Join Grid and specify the following:
   - Virtual IP of Grid Master: `10.0.1.10`.
   - Grid Name: Enter `corp100`.
   - Grid Shared Secret: Enter `Mg1kW17d`.
6. Confirm the configuration, and then on the last screen of the wizard, click Finish.
    The HTTPS session terminates, but the login window remains open.
7. In the login window, type `10.0.1.10` (the VIP address for the grid master) in the Hostname field.
8. Log in using the default user name `admin` and the password `1n85w2IF`.
9. To check the status of the two nodes of the HA grid master, navigate to the Grid tab, select the Grid Manager -> Members tab. This panel lists the grid members. Check the icon in the Status column of the grid master. (green = the appliance has joined the grid and is functioning properly; yellow = the appliance is in the process of joining the grid; red = the appliance has not joined the grid). You can also use the CLI command `set network` to join an appliance to a grid. Check that the status indicators are all green in the Detailed Status panel.

During the joining process, an appliance passes through the following four phases:
1. Offline – the state when a grid member—in this case, the second node of the HA pair composing the grid master—is not in contact with the active node of the master
2. Connecting – the state when an appliance matching a member configuration contacts the master to join the grid and negotiates secure communications and grid membership
3. Synchronizing – the master transmits its entire database to the member
4. Running — the state when a member is in contact with the master and is functioning properly

**Note:** Depending on the network connection speed and the amount of data that the master needs to synchronize with the member, the process can take from several seconds to several minutes to complete.
Define Members on the Grid Master

Before logging in to and configuring the individual appliances that you want to add to the grid, define them first on the grid master.

HQ Site – HA Member

1. From the Grid tab, select the Grid Manager -> Members tab.
2. Expand the Toolbar and click Add -> Add Grid Member.
3. In the Add Grid Member wizard, complete the following and click Next:
   - Host Name: Enter ns2.corp100.com.
   - Comment: Enter HQ Site - ns2.corp100.com.
4. Enter the following information about the member that you are adding to the grid and click Save & Close:
   - High Availability Pair: Select this option.
   - Virtual Router ID: 210
   - Required Ports and Addresses:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Address</th>
<th>Subnet Mask</th>
<th>Gateway</th>
<th>Port Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP</td>
<td>10.0.2.10</td>
<td>255.255.255.0</td>
<td>10.0.2.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node 1 HA</td>
<td>10.0.2.7</td>
<td>255.255.255.0</td>
<td>10.0.2.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node 2 HA</td>
<td>10.0.2.9</td>
<td>255.255.255.0</td>
<td>10.0.2.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node 1 LAN</td>
<td>10.0.2.6</td>
<td>255.255.255.0</td>
<td>10.0.2.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node 2 LAN</td>
<td>10.0.2.8</td>
<td>255.255.255.0</td>
<td>10.0.2.1</td>
<td>Automatic</td>
</tr>
</tbody>
</table>

Site 1 – HA Member

1. From the Grid tab, select the Grid Manager tab -> Members tab.
2. Expand the Toolbar and click Add -> Add Grid Member.
3. In the Add Grid Member wizard, enter the following and click Next:
   - Host Name: Enter ns3.site1.corp100.com
   - Comment: Enter Site 1 - ns3.site1.corp100.com
4. Specify the following information about the member that you are adding to the grid and click Save & Close:
   - High Availability Pair: Select this option.
   - Virtual Router ID: Enter 111.
   - Required Ports and Addresses:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Address</th>
<th>Subnet Mask</th>
<th>Gateway</th>
<th>Port Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP</td>
<td>10.1.1.10</td>
<td>255.255.255.0</td>
<td>10.1.1.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node 1 HA</td>
<td>10.1.1.7</td>
<td>255.255.255.0</td>
<td>10.1.1.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node 2 HA</td>
<td>10.1.1.9</td>
<td>255.255.255.0</td>
<td>10.1.1.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node 1 LAN</td>
<td>10.1.1.6</td>
<td>255.255.255.0</td>
<td>10.1.1.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node 2 LAN</td>
<td>10.1.1.8</td>
<td>255.255.255.0</td>
<td>10.1.1.1</td>
<td>Automatic</td>
</tr>
</tbody>
</table>
Site 2 – Single Member

1. From the Grid tab, select the Grid Manager -> Members tab.
2. Expand the Toolbar and click Add -> Add Grid Member.
3. In the Add Grid Member wizard, enter the following and click Next:
   - Host Name: ns4.site2.corp100.com
   - Comment: Site 2- ns4.site2.corp100.com
4. Specify the following information about the member that you are adding to the grid and click Next:
   - Standalone Member: Select this option.
   - Address: Enter 10.2.1.10.
   - Subnet Mask: Enter 255.255.255.0.
   - Gateway: Enter 10.2.1.1.
   - Port Settings: Select AUTOMATIC.
5. Click Save & Close.
6. Log out from the grid master.

Join Appliances to the Grid

To complete the process of adding appliances to the grid, log in to and configure each individual appliance so that it can contact the grid master.

HQ Site – HA Grid Member (Node 1)

Make a console connection to the appliance that you want to make Node 1 in the HA pair, and enter the following:

   Infoblox > set network
   NOTICE: All HA configuration is performed from the GUI. This interface is used only to configure a standalone node or to join a grid.
   Enter IP address: 10.0.2.6
   Enter netmask [Default: 255.255.255.0]:
   Enter gateway address [Default: 10.0.2.1]:
   Become grid member? (y or n): y
   Enter Grid Master VIP: 10.0.1.10
   Enter Grid Name: corp100
   Enter Grid Shared Secret: Mg1kW17d
   New Network Settings:
   IP address: 10.0.2.6
   Netmask: 255.255.255.0
   Gateway address: 10.0.2.1
   Join grid as member with attributes:
      Grid Master VIP: 10.0.1.10
      Grid Name: corp100
      Grid Shared Secret: Mg1kW17d
   WARNING: Joining a grid will replace all the data on this node!
   Is this correct? (y or n): y
   Are you sure? (y or n): y

The Infoblox application restarts. After restarting, the appliance contacts the grid master and joins the grid as Node 1.
**HQ Site – HA Member (Node 2)**

Make a console connection to the appliance that you want to make Node 2 in the HA pair, and enter exactly the same data you entered for Node 1 except that the IP address is 10.0.2.8.

After the application restarts, the appliance contacts the grid master and joins the grid as Node 2, completing the HA member configuration for the HQ site.

**Site 1 – HA Grid Member (Node 1)**

Make a console connection to the appliance that you want to make Node 1 in the HA pair at Site 1, and use the `set network` command to configure its basic network and grid settings. Use the following data:

- IP Address: 10.1.1.6
- Netmask: 255.255.255.0
- Gateway: 10.1.1.1
- Grid Master VIP: 10.0.1.10
- Grid Name: corp100
- Grid shared secret: Mg1kW17d

The Infoblox application restarts. After restarting, the appliance contacts the grid master and joins the grid as Node 1.

**Site 1 – HA Grid Member (Node 2)**

Make a console connection to the appliance that you want to make Node 2 in the HA pair at Site 1, and enter exactly the same data you entered for Node 1 except that the IP address is 10.1.1.8.

After the application restarts, the appliance contacts the grid master and joins the grid as Node 2, completing the HA member configuration for Site 1.

**Site 2– Single Grid Member**

Make a console connection to the appliance that you want to make Node 1 in the HA pair at Site 1, and use the `set network` command to configure its basic network and grid settings. Use the following data:

- IP Address: 10.2.1.10
- Netmask: 255.255.255.0
- Gateway: 10.2.1.1
- Grid Master VIP: 10.0.1.10
- Grid name: corp100
- Grid shared secret: Mg1kW17d

The Infoblox application restarts. After restarting, the appliance contacts the grid master and joins the grid.

To check the status of all the grid members, log in to the grid master at 10.0.1.10, and from the Grid tab, select the Grid Manager tab -> Members tab, select 10.0.1.10 and click the Detailed Status icon. Check that the status indicators are all green in the Detailed Status panel. As an appliance joins a grid, it passes through the following phases: Offline, Connecting, (Downloading Release from Master), Synchronizing, and Running.)

**Note:** Depending on the network connection speed and the amount of data that the master needs to synchronize with the member, the process of joining a grid can take from several seconds to several minutes to complete.

The grid setup is complete.
Import DHCP Data

The Data Import Wizard is a software tool that you can download from the Infoblox Support site to your management system. With it, you can import data from legacy DHCP and DNS servers to NIOS appliances. In this example, you use it to import both DHCP and DNS data to the grid master at 10.0.1.10, which then uses the database replication mechanism to send the imported data to other grid members. In the wizard, you also specify which grid members serve the imported data. The wizard supports various types of DHCP formats, such as the following:

- ISC DHCP
- Lucent VitalQIP
- Microsoft
- Nortel NetID
- CSV (comma-separated values); you can also import IPAM data in CSV format

In this example, all the DHCP data is in standard ISC DHCP format.

Importing DHCP Data for HQ and Site 2

1. Save the DHCP configuration file from your legacy DHCP server at 10.0.2.20 to a local directory.
2. Visit www.infoblox.com/support, log in with your support account, and download the Data Import Wizard. The Data Import Wizard application downloads to a container within a Java sandbox on your management system and immediately launches, displaying the Welcome page.
3. After reading the information in the left panel, click Next.
4. Select Import to Infoblox Appliance, enter the following, and then click Next:
   - Hostname or IP address: 10.0.1.10
   - Username: admin
   - Password: 1n85w2IF
5. Select the following, and then click Next:
   - What kind of data would you like to import? DHCP/IPAM
   - Which legacy system are you importing from? ISC DHCP
   - Which appliance will be serving this data? 10.0.2.10
6. Type the path and file name of the DHCP configuration file saved from the legacy server, and then click Next.
   or
   Click Browse, navigate to the file, select it, click Open, and then click Next.
7. In the Global DHCP Configuration table, double-click the Value cell for the domain-name-servers row, and change the IP addresses to 10.0.2.10.
8. When satisfied with the data, click Import.
   You can view the status of the importation process and a summary report in the Data Import Wizard Log.
9. To enable DDNS updates, log in to the grid master, from the Data Management tab, select the DHCP tab, expand the Toolbar and click Grid DHCP Configuration.
10. In the DDNS -> Basic tab of the Grid DHCP Properties editor, select Enable DDNS Updates.
11. Click Save & Close.
12. To check the imported DHCP configuration file, from the Data Management tab, select the DHCP tab, -> Members tab -> 10.0.2.10 - check box. Expand the Toolbar and click View DHCP Configuration.
13. In the DHCP configuration file, check that all the imported subnets are present, and navigate to the beginning of the file and check that you see the ddns-updates on statement. (If you see ddns-updates off, enable DDNS updates for the grid as explained in steps 9–12.)
Importing DHCP Data for Site 1
1. Repeat the steps in Importing DHCP Data for HQ and Site 2, saving the DHCP configuration file from your legacy DHCP server at 10.1.1.20, and importing it to the grid master at 10.0.1.10 for the member with IP address 10.1.1.10 to serve.
2. Check the imported DHCP configuration file by logging in to the grid master and from the Data Management tab, select the DHCP tab → Members tab → 10.1.1.10 -check box. Expand the Toolbar and click View DHCP Configuration.

Importing DHCP Data for Site 3
1. Repeat the steps in Importing DHCP Data for HQ and Site 2, saving the DHCP configuration file from your legacy DHCP server at 10.1.1.20, and importing it to the grid master at 10.0.1.10 for the member with IP address 10.3.1.10 to serve.
2. After the importation process completes, check the imported DHCP configuration file by logging in to the grid master and from the Data Management tab, select the DHCP tab → Members tab → 10.3.1.10 -check box. Expand the Toolbar and click View DHCP Configuration.

Import DNS Data
Using the Infoblox Data Import Wizard, import DNS data from the legacy hidden primary server at 10.0.1.5 to the new hidden primary server at 10.0.1.10 (the grid master). There are three phases to this task:

• Before Using the Wizard:
  — Save the named.conf file from the legacy server to a file in a local directory on your management system.
  — Enable the legacy server to perform zone transfers to the NIOS appliance.
  — Configure three name server groups for the grid, and allow the grid master/hidden primary DNS server at 10.0.1.10 to receive DDNS updates from the grid members at 10.0.2.10, 10.1.1.10, and 10.3.1.10. These members act as secondary DNS servers and DHCP servers.
• Using the Wizard on page 164: Define the source, destination, and type of DNS data in the DNS configuration file (named.conf) that you want to import.
• After Using the Wizard on page 166: Check the imported DNS configuration file.

In this example, all the DNS data is in BIND 9 format. The Data Import Wizard supports various types of DNS formats, such as the following:
• BIND 4, 8, and 9
• Microsoft
• Lucent VitalQIP
• Nortel NetID

Before Using the Wizard
You must set up the legacy server and grid master before using the Data Import Wizard.

Legacy Server
1. Log in to the legacy name server at 10.0.1.5 and save the named.conf file, which contains all the DNS settings that you want to import into the Infoblox name server, to a local directory on your management system.
2. On the legacy server, enable zone transfers to the NIOS appliance.
**Infoblox Grid Master – DDNS Updates**

1. Log in to the grid master at 10.0.1.10, and from the Data Management tab, select the DNS tab -> Members tab -> 10.0.1.10 check box and select the Edit icon.

2. In the Member DNS Configuration editor, select the Updates -> Basic tab and enter the following:
   - Select Override.
   - Allow updates from: Click the Add icon and select IPv4 Address. Enter 10.0.2.10 in the Name field of the new row.

3. Click the Add icon again and add 10.1.1.10 and 10.2.1.10 as IP addresses from which you allow DDNS updates.

4. Click Save & Close.

**Note:** When all DNS servers are members in the same grid, the members use database replication to synchronize all their data—including DNS zone data. You can change the default behavior so that grid members use zone transfers instead. In this example, grid members use database replication.

**Infoblox Grid Master – Name Server Groups**

1. From the Data Management tab, select the DNS tab -> Name Server Groups tab.

2. Click the Add icon to open the Add Name Server Group wizard.

3. Enter the following:
   - Name Server Group Name: HQ-Group

4. Click the Add icon and add the following:
   - Grid Primary: ns1.corp100.com; Stealth: Select this check box.
   - Grid Secondary: ns2.corp100.com; Grid replication (recommended): Select this check box.

5. Click Save & New.

6. Repeat steps 2 to 4 to create another group. Name it Site1-Group, and use ns1.corp100.com as the hidden primary server, ns3.site1.corp100.com as a secondary server, and grid replication for zone updates.

7. Repeat steps 2 to 4 to create another group. Name it Site2-Group, and use ns1.corp100.com as the hidden primary server, ns4.site2.corp100.com as a secondary server, and grid replication for zone updates.

**Using the Wizard**

While progressing through the Data Import Wizard, you must define the source, destination, and type of DNS data that you want to import. You then make some simple modifications to the data and import it.

**Defining the Source, Destination, and Type of DNS Data**

1. Launch the Data Import Wizard.

2. After reading the information in the left panel of the welcome page, click Next.

3. Select Import to Infoblox Appliance, enter the following, and then click Next:
   - Hostname or IP address: 10.0.1.10
   - Username: admin
   - Password: 1n85w2IF

   The Data Import Wizard Log opens in a separate window behind the wizard. Leave it open while you continue.

4. Select the following, and then click Next:
   - What kind of data would you like to import? DNS
   - Which legacy system are you importing from? BIND 9
   - Which appliance will be serving this data? 10.0.1.10
5. Select the following, and then click **Next**:
   - What BIND 9 DNS configuration file would you like to use? Click **Browse**, navigate to the named.conf file you saved from the legacy server, select it, and then click **Open**.
   - What type of BIND 9 DNS data do you want to import? **DNS zone information and DNS record data**
   - Where is the BIND 9 DNS record data? **Zone transfer(s) from a DNS server; 10.0.1.5**

The wizard displays two tables of data. The upper table contains global DNS server configuration parameters. The lower table contains zone configurations.

The Data Import Wizard Log presents a summary listing the number of views, zones, and DNS records in the configuration file.

### Modifying DNS Data

While importing data from the legacy DNS server, you cancel the importation of global configuration settings, and apply the name server groups you created in **Before Using the Wizard** on page 163 to the zones you want to import.

1. In the Global DNS Configuration table, select all rows by clicking the top row and then SHIFT+clicking the bottom row.
2. Right-click the selected rows to display the **Set Import Options** dialog box, select **Do not import**, and then click **Apply**.
3. In the DNS Zones table, clear the **Import** check box for the default view.
4. Select **corp100.com, lab.corp100.com** and all the corresponding reverse-mapping zones.

   **Tip:** You can use SHIFT+click to select multiple contiguous rows and CTRL+click to select multiple noncontiguous rows.

5. Right-click the selected rows, and then select **Set Import Options**.
6. In the **Set Import Options** dialog box, enter the following, and then click **Apply**:
   - Set Zone Type: No change
   - Set Import Option: No change
   - Set View: default
   - Set Member: HQ-Group master

7. Select **site1.corp100.com** and all the reverse-mapping zones with 1 in the second octet in the zone name (1.1.10.in-addr.arpa, 2.1.10.in-addr.arpa, 3.1.10.in-addr.arpa, and so on).
8. Right-click the selected rows, and select **Set Import Options**.
9. In the **Set Import Options** dialog box, make the same selections as in **Step 6**, but choose **Site1-Group master** from the Set Member drop-down list.
10. Similarly, select **site2.corp100.com** and all the reverse-mapping zones with 2 in the second octet in the zone name.
11. Right-click the selected rows, and select **Set Import Options**.
12. In the **Set Import Options** dialog box, make the same selections as in **Step 6**, but choose **Site2-Group master** from the Set Member drop-down list.
Importing DNS Data

1. Click **Import**.
   The wizard imports the global DNS parameters and zone-specific configuration settings from the named.conf file and performs a zone transfer of the data from the legacy server.

2. Use the Data Import Wizard Log to monitor progress and review results afterward.
   The log lists all the zones that the wizard imports and concludes with a total of all the successfully and unsuccessfully imported zones.

   **Note:** If the wizard is unable to import a zone, an error message with an explanation appears in the log.

3. To close the Data Import Wizard, click **Exit**. This closes the Data Import Wizard Log as well.

After Using the Wizard

After you import data, you must restart services on the grid master and delete the A records for the legacy servers from the corp100.com zone. You can also confirm that the imported data is correct and complete by checking the DNS configuration and the forward- and reverse-mapping zones.

1. Log in to the grid master (10.0.1.10), select the **Grid** tab, expand the Toolbar, and then click the **Restart Services** icon.

   **Note:** When importing data through the wizard rather than entering it through the GUI, the Restart Services icon does not change to indicate you must restart service for the appliance to apply the new data. Still, restarting service on the grid master is necessary for the imported configuration and data to take effect.

2. To remove A records for the legacy servers, from the **Data Management** tab, select **DNS** tab -> **Zones** tab -> **corp100.com**.

3. Expand the Records section, select the following A records in the corp100.com zone, and then click the **Delete** icon:
   - ns1 (for 10.0.1.5)
   - ns2 (for 10.0.2.5)
   - ns3.site1.corp100 (for 10.1.1.5)
   - ns4.site3.corp100 (for 10.2.1.5)

4. Remove the respective A records for legacy servers from the site1.corp100 and site3.corp100 subzones.

5. To check the imported DNS configuration file, from the **Data Management** tab, select **DNS** tab -> **Members** tab -> **10.0.1.10** check box. Expand the Toolbar and click **View** -> **View DNS Configuration**.

   **Note:** If you do not see the imported DNS configuration file, make sure you enabled DNS and restarted services.

6. Scroll through the DNS configuration log to check that each imported zone has an **allow-update** statement like the following one for the 10.1.10.in-addr.arpa reverse-mapping zone:

   ```
   zone "10.1.10.in-addr.arpa" in {
       ...
       allow-update { key DHCP_UPDATER; 10.0.2.10; 10.1.1.10; 10.2.1.10; };
       ...
   };
   ```
Enable DHCP and Switch Service to the Grid

Finally, you must enable DHCP service on the three grid members at 10.0.2.10, 10.1.1.10, and 10.2.1.10, and switch DNS and DHCP service from the legacy DNS and DHCP servers to them.

1. Log in to the grid master (10.0.1.10) and from the Data Management tab, select the DHCP tab -> Members tab -> 10.0.2.10 check box. Expand the Toolbar and click Start.
2. Repeat step 1 to enable DHCP on 10.1.1.10 and 10.3.1.10.

Note: DNS service is enabled by default.

The grid members are ready to serve DHCP and DNS, and send DDNS updates.

3. Take the legacy DHCP and DNS servers offline.

MANAGING A GRID

After you configure a grid master and add members, you might need to perform the following tasks:

- Changing Grid Properties
- Setting the MTU for VPN Tunnels on page 168
- Removing a Grid Member on page 168
- Promoting a Master Candidate on page 168

Changing Grid Properties

You can change a grid name, its shared secret, and the port number of the VPN tunnels that the grid uses for communications. If you make such changes after populating a grid with members, all current members will lose grid connectivity and you will have to rejoin them to the grid manually.

To modify the properties of a grid:

1. From the Grid tab, select the Grid Manager tab.
2. Expand the Toolbar and select Grid Properties -> Edit.
3. In the Grid Properties editor, select the General tab, and then modify any of the following:
   - Grid Name: Type the name of a grid. The default name is Infoblox.
   - Shared Secret: Type a shared secret that all grid members use to authenticate themselves when joining the grid. The default shared secret is test.
   - Shared Secret Retype: Type the shared secret again to confirm its accuracy.
   - Time Zone: Choose the applicable time zone from the drop-down list.
   - Date: Click the calendar icon to select a date or enter the date in YYYY/MM/DD format.
   - Time: Click the clock icon to select a time or enter the time in HH:MM:SS format. For afternoon and evening hours, use the integers 13-24.
   - VPN Port: Type the port number that the grid members use when communicating with the grid master through encrypted VPN tunnels. The default port number is 1194. After changing the port number, you must restart grid services or reboot the single master or the active node of an HA master (which forces an HA failover). For more information, see Port Numbers for Grid Communication on page 147.
   - Enable Recycle Bin: Select the check box to enable the Recycle Bin. The Recycle Bin stores deleted items when the user deletes grid, DNS, or DHCP configuration items. Enabling the Recycle Bin allows you to undo deletions and to restore the items on the appliance at a later time. If you do not enable this feature, deleted items from the GUI are permanently removed from the database.
Deploying a Grid

— **Audit Logging**: Select one of the following:
  — **Detailed**: This is the default type. It is automatically selected. It provides detailed information on all administrative changes such as the date and time stamp of the change, administrator name, changed object name, and the new values of all properties.
  — **Brief**: Provides information on administrative changes such as the date and time stamp of the change, administrator name, and the changed object name. It does not show the new value of the object.

4. Click **Save & Close** to save your changes.
5. If you changed the VPN port number, click the **master** check box, expand the Toolbar and click **Restart Services**.

**Setting the MTU for VPN Tunnels**

You can configure the VPN MTU (maximum transmission unit) for any appliance with a network link that does not support the default MTU size (1500 bytes) and that cannot join a grid because of this limitation. If an appliance on such a link attempts to establish a VPN tunnel with a grid master to join a grid, the appliance receives a PATH-MTU error, indicating that the path MTU discovery process has failed. For information about the MTU discovery process, see RFC 1191, *Path MTU Discovery*.

To avoid this problem, you can set a VPN MTU value on the grid master for any appliance that cannot link to it using a 1500-byte MTU. When the appliance contacts the master during the key exchange handshake that occurs during the grid-joining operation, the master sends the appliance the MTU setting to use.

To set the VPN MTU for a grid member:
1. From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab -> **grid_member** check box -> **Edit** icon.
2. Select the **Network** -> **Advanced** tab of the **Grid Member Properties** editor.
3. In the **VPN MTU** field, enter a value between 600 and 1500.
4. Click **Save & Close** to save the VPN MTU settings for this member.

**Removing a Grid Member**

You might want or need to remove a member from a grid, perhaps to disable it or to make it an independent appliance or an independent HA pair. Before you remove a member, make sure that it is not assigned to serve any zones or networks.

To remove a grid member, from the **Grid** tab, select the **Grid Manager** tab -> **Members** tab -> **grid_member** check box, and click the **Delete** icon.

**Promoting a Master Candidate**

To be able to promote a master candidate, you must have previously designated a grid member as a master candidate before anything untoward happens to the current master. When adding or modifying a grid member, select the **Master Candidate** option in the **General** tab of the **Grid Member Properties** editor for that member. Before promoting a master candidate, check your firewall rules to ensure that the new master can communicate with all the grid members. For information, see Grid Communications on page 134.

To promote a master candidate, you can make a direct serial connection to the console port on the active node of an HA candidate or to the console port on a single candidate. You can also make a remote serial connection (using SSH v2) to the candidate. Enter the following Infoblox CLI command to promote a master candidate: `set promote_master`.

**Note**: For information about making a serial connection, see Method 2 – Using the CLI on page 176.
To promote a master candidate, do the following:

1. Establish a serial connection (through a serial console or remote access using SSH) to the master candidate.

2. At the prompt, enter the command:
   ```
   set promote_master
   ```
   The appliance restarts. The GUI is unavailable until the master promotion is complete.

3. Log in to the Infoblox Grid Manager GUI on the new master using the VIP address for an HA master or the IP address of the LAN1 port for a single master.

4. From the Grid tab, select the Grid Manager tab.

5. Look at the IP address of the master in the IP Address column to ensure it is the member you promoted.

6. To verify the new master is operating properly, check the icons in the Status column. Also, select the master, and then click the Detailed Status icon in the table toolbar.
   You can also check the status icons of the grid members to verify that all grid members have connected to the new master. If any have not, you can check your firewall rules and log into to CLI of those members to investigate.
Chapter 6  Deploying Independent Appliances

This chapter explains how to deploy single independent appliances and independent HA pairs. Independent appliances run NIOS without the grid upgrade and are deployed independently from a grid. This chapter includes the following sections:

- **Independent Deployment Overview** on page 173
  - System Manager GUI on page 174

- **Deploying a Single Independent Appliance** on page 175
  - Method 1 – Using the LCD on page 176
  - Method 2 – Using the CLI on page 176
  - Method 3 – Using the Infoblox NIOS Startup Wizard on page 177

- **Configuration Example: Deploying a NIOS Appliance as a Primary DNS Server** on page 179
  - Cabling the Appliance to the Network and Turning On Power on page 180
  - Specifying Initial Network Settings on page 180
  - Specifying Appliance Settings on page 180
  - Defining a NAT Address on page 181
  - Enabling Zone Transfers on the Legacy Name Server on page 182
  - Importing Zone Data on an Independent Appliance on page 182
  - Designating the New Primary on the Secondary Name Server (at the ISP Site) on page 185
  - Configuring NAT and Policies on the Firewall on page 185

- **Deploying an Independent HA Pair** on page 186
  - Using the Infoblox NIOS Startup Wizard to Configure an HA Pair on page 186

- **Configuration Example: Configuring an HA Pair for Internal DNS and DHCP Services** on page 189
  - Cabling Appliances to the Network and Turning On Power on page 190
  - Specifying Initial Network Settings on page 191
  - Specifying Appliance Settings on page 191
  - Enabling Zone Transfers on page 193
  - Importing Zone Data on page 193
  - Defining Networks, Reverse-Mapping Zones, DHCP Ranges, and Infoblox Hosts on page 193
  - Defining Multiple Forwarders on page 196
  - Enabling Recursion on External DNS Servers on page 196
  - Modifying the Firewall and Router Configurations on page 197
Deploying Independent Appliances

- Enabling DHCP and Switching Service to the NIOS Appliance on page 198
- Managing and Monitoring on page 198
- Verifying the Deployment on page 199
  - Single Independent Appliance on page 199
  - Independent HA Pair on page 199
- Infoblox Tools for Migrating Data on page 200
INDEPENDENT DEPLOYMENT OVERVIEW

You can deploy the NIOS appliance as a grid member in an Infoblox grid or independently as a standalone deployment. Grids offer many advantages for large organizations while independent deployments can be sufficient for smaller sites. For example, if your ISP hosts one name server to respond to external DNS queries, you can deploy a single independent NIOS appliance as the other name server, as shown in Figure 6.1.

Figure 6.1 Single Independent Appliance as a DNS Server

Using primary and secondary name servers provides DNS protocol redundancy, and configuring two DHCP servers as DHCP failover peers provides DHCP protocol redundancy. However, you can only have hardware redundancy if you deploy appliances in an HA (high availability) pair. Should the active node in an HA pair fail, the passive node becomes active and begins serving data, as shown in Figure 6.2. For more information about HA pairs, see About HA Pairs on page 142.

Figure 6.2 Independent HA Pair
System Manager GUI

When you deploy an independent appliance, you use System Manager to manage the appliance. Though other chapters in this guide contain information that assumes a grid deployment and describes the Grid Manager GUI, most of the configuration procedures are applicable to an independent appliance, with the following differences:

- In the Dashboard, there is no Grid Status widget, and the Members Status widget in Grid Manager is the System Status widget in System Manager.
- Functions related to a grid, such as joining a grid and managing grid licenses, do not exist in System Manager.
- The grid related tabs and functions in Grid Manager are the system related tabs and functions in System Manager.
- Functions related to the Members tab in Grid Manager appear in the Nodes tab or the Toolbar of another subtab in System Manager.

For example, the following navigation path for a grid:

- From the Grid tab, select the Grid Manager tab -> Members tab -> member check box, and then click HTTPS Cert -> Download Certificate from the Toolbar.

is the following for an independent appliance:

- From the System tab, select the System Manager tab -> Nodes tab, and then click HTTPS Cert -> Download Certificate from the Toolbar.
Deploying a Single Independent Appliance

To deploy a single independent NIOS appliance, you cable its LAN1 port to the network and change its default IP settings so that it can connect to its surrounding IP address space. The default LAN settings are as follows:

- IP address: 192.168.1.2
- Netmask: 255.255.255.0
- Gateway: 192.168.1.1

When deploying a single independent appliance, you can use one of the following methods to set up the initial configuration:

- **Method 1 – Using the LCD**
  - Requirements: Physical access to a powered up NIOS appliance.
  - Advantage: You do not need any other equipment.

- **Method 2 – Using the CLI**
  - Requirements: A serial connection from your management system to the console port on the NIOS appliance. You can also enable remote console access so that you can use the CLI over a network connection. For information, see Enabling Remote Console Access on page 139.
  - Advantage: You do not need to change the IP address of the management system to connect to the NIOS appliance.

- **Method 3 – Using the Infoblox NIOS Startup Wizard**
  - Requirements: An HTTPS connection from your management system to the LAN1 port on the NIOS appliance.
  - Advantage: The wizard provides step-by-step guidance for changing not only the IP settings for the LAN1 port, but also changing the appliance host name and admin password, setting the system clock, and—if using NTP (Network Time Protocol)—enabling the NIOS appliance to be an NTP client.

Note that you can configure network settings using the Startup wizard any time after you have configured the appliance. To start the wizard, from System Manager, select the System tab, and then click System Properties → Startup Wizard from the Toolbar.

After you configure the network settings on a single independent appliance, you can migrate data from legacy DNS and DHCP servers to the NIOS appliance. Several tools and methods are available for migrating data and configuration settings. For a list of the available options, see Infoblox Tools for Migrating Data on page 200.
Method 1 – Using the LCD

Some of the NIOS appliances have an LCD and navigation buttons on the front panel that allow you to view system status and license information as well as configure network settings for the LAN1 port.

You can deploy a single independent NIOS appliance by setting its LAN1 port IP address, netmask, and gateway through the LCD. This is the simplest method because you do not need anything other than a physical access to the appliance to complete the initial configuration.

1. Connect the power cable from the NIOS appliance to a power source and turn on the power.
   At startup, the Infoblox logo appears in the LCD on the front panel of the appliance. Then the LCD scrolls repeatedly through a series of display screens.

2. To change the network settings for the LAN1 port, press one of the navigation buttons.
   The LCD immediately goes into the input mode, in which you can enter the IP address, netmask, and gateway for the LAN1 port.

3. Use the navigation buttons to enter an IP address, netmask, and gateway address for the LAN1 port.

4. Cable the LAN1 port of the NIOS appliance to a network as described in the installation guide that shipped with your product.

Method 2 – Using the CLI

You can use the Infoblox CLI to make an initial network configuration through the `set network` command. To access the CLI, make a direct serial connection from your management system.

1. Connect a console cable from the console port on your workstation to the male DB-9 console port on the NIOS appliance.
   The DB-9 pin assignments follow the EIA232 standard. You can use the RJ-45 rollover cable and two female RJ-45-to-female DB-9 adapters that ship with the appliance, or a female DB-9-to-female DB-9 null modem cable.
2. Use a serial terminal emulation program, such as Hilgraeve Hyperterminal® (provided with Windows® operating systems), to launch a session. The connection settings are:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: Xon/Xoff

3. Log in to the appliance using the default username and password (admin and infoblox).

4. At the Infoblox command prompt, enter `set network` to change the network settings, such as the IP address, netmask, and gateway for the LAN1 port.

   **Note:** In the following example, the variable `ip_addr1` is the IP address of the LAN1 port and `ip_addr2` is the IP address of the gateway for the subnet on which you set the `ip_addr1` address.

   ```
   Infoblox > set network
   NOTICE: All HA configuration is performed from the GUI. This interface is used only to configure a standalone node or to join a grid.
   Enter IP address: ip_addr1
   Enter netmask: [Default: 255.255.255.0]: netmask
   Enter gateway address [Default: n.n.n.1]: ip_addr2
   Become grid member? (y or n): n
   ```

   After you confirm your network settings, the Infoblox application automatically restarts.

5. Cable the LAN1 port to a network as described in *Independent Appliance Cabling Using the LAN or Serial Port* on page 833.

**Method 3 – Using the Infoblox NIOS Startup Wizard**

When you first make an HTTPS connection to a NIOS appliance, the Infoblox NIOS Startup Wizard guides you through the deployment options and basic network settings. You can also change the password of the superuser (admin) and set up the system clock.

Note that you can configure network settings using the Startup wizard any time after you have configured the appliance. To start the wizard, from Grid Manager, select the System tab, and then click System Properties -> Startup Wizard from the Toolbar.

To make an HTTPS connection to the appliance, you must be able to reach its IP address from your management system.

Note: If you have already set the IP address of the LAN1 port through the LCD or CLI so that you can reach it over the network—and you have already cabled the appliance to the network—you can skip the first step.

1. If you have not changed the default IP address (192.168.1.2/24) of the LAN1 port through the LCD or CLI—and the subnet to which you connect the appliance is not 192.168.1.0/24—put your management system in the 192.168.1.0/24 subnet and connect an Ethernet cable between your management system and the NIOS appliance.

2. Open an Internet browser window and enter `https://<IP address of the appliance>` to make an HTTPS connection. For information about supported browsers, see *Supported Browsers* on page 33.

   Several certificate warnings may appear during the login process because the preloaded certificate is self-signed and has the hostname www.infoblox.com, which may not match the destination IP address you entered in step 1. To stop the warning messages from occurring each time you log in to Grid Manager, you can generate a new self-signed certificate or import a third-party certificate with a common name that matches the FQDN (fully qualified domain name) of the appliance. For information, see *Managing Certificates* on page 51.
3. Enter the default username and password (admin and infoblox) on the Grid Manager login page, and then click **Login** or press Enter. For information, see *Accessing the Infoblox GUI* on page 41.

4. Read the Infoblox End-User License Agreement, and then click **I Accept** to proceed. Grid Manager may take a few seconds to load your user profile.

5. In the **NIOS Startup wizard**, select **Configuring a standalone appliance**. To configure an independent HA pair, see *Deploying an Independent HA Pair* on page 186.

6. Click **Next** and complete the following to configure network settings:
   - **Host Name**: Enter a valid domain name for the appliance.
   - **IP Address**: Displays the IP address of the LAN1 port.
   - **Subnet Mask**: Displays the subnet mask of the LAN1 port.
   - **Gateway**: Displays the IP address of the gateway of the subnet on which the LAN1 port is set.
   - **Port Settings**: Select the port settings from the drop-down list. The list contains all the settings supported by the hardware model. The default is **Automatic**. The appliance automatically detects the port settings.

7. Click **Next** and complete the following to set admin password:
   - **Yes**: To change the default password.
   - **No**: To keep the default password. Infoblox recommends that you change the default password. When you select **Yes**, complete the following:
     - **Password**: Enter a password for the superuser admin account. The password must be a single alphanumeric string without spaces and at least four characters long. The password is case-sensitive.
     - **Retype Password**: Enter the same password.

8. Click **Next** and complete the following to configure time settings:
   - **Time Zone**: Select the applicable time zone from the drop-down list. The default is **(UTC) Coordinated Universal Time**.
   - **Would you like to enable NTP?**:
     - Select **Yes** to synchronize the time with external NTP servers, and then click the Add icon. Grid Manager adds a row to the NTP Server table. Click the row and enter either the IP address or the resolvable host name of an NTP server. You can view a list of public NTP servers at ntp.isc.org.
     - Select **No** to specify the time settings for the appliance.
       - **Date**: Enter the date in YYYY-MM-DD format. You can also click the calendar icon to select a date from the calendar widget.
       - **Time**: Enter the time in HH:MM:SS AM/PM format. You can also click the clock icon to select a time from the drop-down list.

9. Click **Next** to view the summary of the configuration. Review the information and verify that it is correct. You can change the information you entered by clicking **Previous** to go back to a previous step.

10. Click **Finish**.
    The appliance restarts and disconnects Grid Manager.
Configuration Example: Deploying a NIOS Appliance as a Primary DNS Server

In this example, you configure the NIOS appliance as a primary DNS server for corp100.com. Its FQDN (fully-qualified domain name) is ns1.corp100.com. The interface IP address of the LAN1 port is 10.1.5.2/24. Because this is a private IP address, you must also configure the firewall to perform NAT (network address translation), mapping the public IP address 1.1.1.2 to 10.1.5.2. Using its public IP address, ns1 can communicate with appliances on the public network. The FQDN and IP address of the external secondary DNS server are ns2.corp100.com and 2.2.2.2. The ISP hosts this server.

The primary and secondary servers answer queries for the following public-facing servers in the DMZ:

- www.corp100.com
- mail.corp100.com
- ftp.corp100.com

When you create the corp100.com zone on the NIOS appliance, you import zone data from the legacy DNS server at 10.1.5.3.

Figure 6.5 Example 1 Network Diagram

The NIOS appliance is the primary DNS server for the corp100.com domain. It answers queries from the Internet for the three public-facing servers in the DMZ network:

- www.corp100.com
- mail.corp100.com
- ftp.corp100.com
Cabling the Appliance to the Network and Turning On Power

Connect an Ethernet cable from the LAN1 port of the NIOS appliance to a switch in the DMZ network and turn on the power. For information about installing and cabling the appliance, refer to the user guide or installation guide that ships with the product.

Specifying Initial Network Settings

Before you can configure the NIOS appliance through Grid Manager, you must be able to make a network connection to it. The default network settings of the LAN1 port are 192.168.1.2/24 with a gateway at 192.168.1.1 (the HA and MGMT ports do not have default network settings). To change these settings to suit your network, use either the LCD or the console port.

In this example, you change the IP address/netmask of the LAN1 port to 10.1.5.2/24, and the gateway to 10.1.5.1.

LCD

The NIOS appliance has an LCD and navigation buttons on its front panel.

At startup, the Infoblox logo appears in the LCD on the front panel of the appliance. Then the LCD scrolls repeatedly through a series of display screens.

1. To change the network settings from the default, press one of the navigation buttons.
   
   The LCD immediately goes into input mode, in which you can enter the IP address, netmask, and gateway for the LAN1 port.

2. Use the navigation buttons to enter the following information:
   
   — IP Address: 10.1.5.2
   — Netmask: 255.255.255.0
   — Gateway: 10.1.5.1

Specifying Appliance Settings

When you make the initial HTTPS connection to the NIOS appliance, the NIOS Startup Wizard guides you through the basic deployment of the appliance on your network. Use the wizard to enter the following information:

• Deployment: single independent appliance
• Host name: ns1.corp100.com
• Password: SnD34n534
• NTP (Network Time Protocol) server: 3.3.3.3; time zone: (UMT – 8:00 Pacific Time (US and Canada), Tijuana

1. Open an Internet browser window and enter **https://10.1.5.2**.

2. Accept the certificate when prompted.

   Several certificate warnings may appear during the login process. This is normal because the preloaded certificate is self-signed and has the hostname www.infoblox.com, which does not match the destination IP address you entered in step 1. To stop the warning messages from occurring each time you log in to Grid Manager, you can generate a new self-signed certificate or import a third-party certificate with a common name that matches the FQDN (fully-qualified domain name) of the appliance. This is a very simple process. For information about certificates, see **Managing Certificates** on page 51.

3. Enter the default username and password (admin and infoblox) on the Grid Manager login page, and then click **Login** or press Enter. For information, see **Accessing the Infoblox GUI** on page 41.

4. Read the Infoblox End-User License Agreement, and then click **I Accept** to proceed. Grid Manager may take a few seconds to load your user profile.

5. In the **NIOS Startup wizard**, select **Configuring a standalone appliance**.
6. Click **Next** and complete the following to configure network settings:
   - **Host Name:** Enter `ns1.corp100.com`.
   - **IP Address:** Enter `10.1.5.2` as the IP address for the LAN1 port.
   - **Subnet Mask:** Enter `255.255.255.0` as the subnet mask for the LAN1 port.
   - **Gateway:** Enter `10.1.5.1` as the gateway of the subnet on which the LAN1 port is set.
   - **Port Settings:** Use the default value **Automatic**.

7. Click **Next** and complete the following to set admin password:
   - **Would you like to set admin password?:** Click **Yes**.
   - **Password:** Enter `SnD34n534`.
   - **Retype Password:** Enter `SnD34n534` again.

8. Click **Next** and complete the following to configure the time settings:
   - **Time Zone:** Select **UMT – 8:00 Pacific Time (US and Canada), Tijuana** from the drop-down list.
   - **Would you like to enable NTP?:** Select **Yes** to synchronize the time with external NTP servers, and then click the Add icon. Grid Manager adds a row to the NTP Server table. Click the row and enter `3.3.3.3` in the NTP Server field.

9. Click **Next** to view the summary of the configuration. Review the information and verify that it is correct. You can change the information you entered by clicking **Previous** to go back to a previous step.

10. Click **Finish**.

### Defining a NAT Address

Because the firewall translates the public IP address 1.1.1.2 to the interface IP address 10.1.5.2, all DNS queries originating outside the firewall use 1.1.1.2 (not 10.1.5.2) to reach the NIOS appliance. Accordingly, you must configure the appliance to indicate to other external DNS servers that its address is 1.1.1.2.

To define a NAT address:

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, click the **Network -> Advanced** tab, and then complete the following:
   - **Enable NAT compatibility:** Select this check box.
   - **NAT Address:** Click the LAN row in the table, and then enter the NAT (V)IP address `1.1.1.2` in the **Address** field.

3. Click **Save & Close**.

The glue record is an A record for a name server. The appliance automatically generates the A record for `ns1.corp100.com` using either the interface address or NAT address (if configured). To verify that the A record uses the NAT address (1.1.1.2) instead of the interface address (10.1.5.2):

1. From the **Data Management** tab, select the **DNS** tab, and then click **System DNS Properties** from the Toolbar.

2. In the **System DNS Properties** editor, click the **DNS Views** tab, and then complete the following:
   - **Address of Member Used in DNS Views:** In the table, click the **Interface** field in the default row.
   - From the **Interface** drop-down list, select **NAT IP address**. Grid Manager displays the NAT IP address.

3. Click **Save & Close**.
Enabling Zone Transfers on the Legacy Name Server

To allow the appliance to import zone data from the legacy server 10.1.5.3, you must configure the legacy server to allow zone transfers to the appliance at 10.1.5.2.

Legacy BIND Server

1. Open the named.conf file using a text editor and change the allow-transfer statement as shown below:

   For All Zones — To set the allow-transfer statement as a global statement in the named.conf file for all zones:
   ```
   options {
   zone-statistics yes;
   directory "/var/named/named_conf";
   version "";
   recursion yes;
   listen-on { 127.0.0.1; 10.1.5.3; };
   ...
   allow-transfer {10.1.5.2; };
   transfer-format many-answers;
   };
   ```

   For a Single Zone — To set the allow-transfer statement in the named.conf file for the corp100.com zone:
   ```
   zone "corp100.com" in {
   type master;
   allow-transfer {10.1.5.2; };
   notify yes;
   }
   ```

2. After editing the named.conf file, restart DNS service on the appliance for the change to take effect.

Legacy Windows 2000/2003 Server

1. Click Start -> All Programs -> Administrative Tools -> DNS.
2. Click + (for ns1) -> + (for Forward Lookup Zones) -> corp100.com.
3. Right-click corp100.com, and then select Properties -> Zone Transfers.
4. On the Zone Transfers page in the corp100.com Properties dialog box, enter the following:
   - Allow zone transfers: Select this.
   - Only to the following servers: Select this.
   - IP address: Enter 10.1.5.2, and then click Add.
5. To save the configuration and close the corp100.com Properties dialog box, click OK.

Importing Zone Data on an Independent Appliance

You can import zone data from a legacy server or manually enter it. When you import both forward-mapping and reverse-mapping zone data, the NIOS appliance automatically creates Infoblox host records if corresponding A and PTR records are present. You can then modify the host records to add MAC addresses. However, if you only import forward-mapping zone data, the NIOS appliance cannot create host records from just the A records. In that case, because you cannot later convert A records to host records, it is more efficient to create the corp100.com zone, and define host records manually.

Infoblox host records are data models that represent IP devices within the Infoblox semantic database. The NIOS appliance uses a host object to define A, PTR, and CNAME resource records in a single object as well as a DHCP fixed address if you include a MAC address in the host object definition. The host object prevents costly errors because you only maintain a single object for multiple DNS records and a DHCP fixed address. Therefore, it is advantageous to use host records instead of separate A, PTR, and CNAME records.
Configuration Example: Deploying a NIOS Appliance as a Primary DNS Server

Note: If you only have forward-mapping zones on your legacy servers and you want to add reverse-mapping zones and automatically convert A records to host records in the imported forward-mapping zones and create reverse host records in corresponding reverse-mapping zones, create the reverse-mapping zones on the NIOS appliance and then import the forward-mapping zones data. The NIOS appliance automatically converts the imported A records to host records in the forward-mapping zones and creates reverse host records in the reverse-mapping zones.

You also have the option of using the Data Import Wizard for loading DNS and DHCP data. For large data sets, this option is an efficient approach. To download the Data Import Wizard, visit www.infoblox.com/import/.

In this example, when you create the corp100.com forward-mapping zone, you import zone data for the existing corp100.com zone from the legacy server at 10.1.5.3. When you create the 1.1.1.0/24 reverse-mapping zone, you also import the reverse-mapping zone records from the legacy server. After the appliance has both the forward- and reverse-mapping zone data, it converts the A and PTR records to Infoblox host records.

Creating a Name Server Group

1. Open an Internet browser window, enter https://10.1.5.2, and then log in to Grid Manager using the username admin and password SnD34n534.
2. From the Data Management tab, select the DNS tab -> Name Server Groups tab, and then click the Add icon to create a name server group.
3. In the Name Server Group wizard, complete the following:
   — Name: Enter Corp100 as the group name.
   — Name Servers: Click the Add icon -> Primary.
     — In the Add Primary section, Grid Manager displays the host name of the independent appliance. Click Add. Grid Manager adds the independent system as the primary server.
   — Click the Add icon -> External Secondary.
     — In the Add External Secondary section, complete the following:
       — Name: Enter ns2.corp100.com.
       — Address: Enter 2.2.2.2.
       — Stealth: Clear this check box.
     — Click Add. Grid Manager adds the external secondary to the name server group.
4. Click Save & Close.

Creating a Forward-Mapping Zone

Note: To import zone data, you must first create a zone and save it.

1. To create an authoritative zone, from the Data Management tab, select the DNS tab -> Zones tab, and then click the Add icon -> Authoritative Zone.
2. In the Add Authoritative Zone wizard, select Add an authoritative forward-mapping zone.
3. Click Next and complete the following:
   — Name: Enter corp100.com.
   — Comment: Enter DNS zone.
4. Click Next to assign a name server group to the zone.
5. Click the Zones tab, select the corp100.com check box, and then click the Edit icon.
6. In the Authoritative Zone editor, select the Name Servers tab, and then complete the following:
   — Use this name server group: Select this, and then select Corp100 from the drop-down list.
7. Click Save & Close.
**Importing Zone Data**

1. To import zone data to the corp100.com zone that you created earlier, click the Zones tab, select the corp100.com check box, and then click Import Zone from the Toolbar.

2. In the Import Zone editor, complete the following:
   - **Address**: Enter the IP address 10.1.5.3 from which you want to import zone data.
   - **Automatically create hosts from A records**: Select this to enable the appliance to create host records from the imported A records.

3. Click Import.

4. After successfully importing the zone data, click corp100.com in the Zones tab.
   You can see all the imported forward-mapping zone data in the Records panel. Because you have not yet imported the reverse-mapping zone data, most of the records appear as A records.

5. To import the reverse-mapping zone data, from the Zones tab, click the Add icon -> Authoritative Zone.

6. In the Add Authoritative Zone wizard, select Add an authoritative IPv4 reverse-mapping zone.

7. Click Next and complete the following:
   - **IPv4 Network**: Enter 1.1.1.0.
   - **Netmask**: Select 24 from the drop-down list.
   - **Comment**: Enter Reverse-mapping zone.

8. Click Save & Close.

9. To assign a name server group to the reverse-mapping zone, click the Zones tab, select the 1.1.1.in-addr.arpa check box, and then click the Edit icon.

10. In the Authoritative Zone editor, select the Name Servers tab, and then complete the following:
    - **Use this name server group**: Select this, and then select Corp100 from the drop-down list.

11. Click Save & Close.

12. To import reverse-mapping zone data, click the Zones tab, select the corp100.com check box, and then click Import Zone from the Toolbar.

13. In the Import Zone editor, complete the following:
    - **Address**: Enter 10.1.5.3 from which you want to import zone data.
    - **Automatically create hosts from A records**: Select this to enable the appliance to create host records from the imported A records.

14. Click Import.

15. After successfully importing the zone data, click 1.1.1.in-addr.arpa in the Zones tab.
   You can see all the imported reverse-mapping zone data in the Records panel.

16. Click corp100.com in the Forward Mapping Zones list.
    Because you have now imported both the forward- and reverse-mapping zone data, most of the records appear as host records.

17. Finally, you must remove the ns1 host record for the legacy server (value 1.1.1.3). To remove it, select the ns1 check box (the host record for 1.1.1.3), and then click the Delete icon.
Designating the New Primary on the Secondary Name Server (at the ISP Site)

In this example, the external secondary name server is maintained by an ISP, so you must contact your ISP administrator to change the IP address of the primary (or master) name server. (If you have administrative access to the secondary name server, you can make this change yourself.)

Because a firewall performing NAT exists between the secondary and primary name servers, specify the NAT address 1.1.1.2 for the primary name server instead of 10.1.5.2.

**Secondary BIND Server**

1. Open the named.conf file using a text editor and set ns1 (with NAT address 1.1.1.2) as the primary (or master) from which ns2 receives zone transfers in the named.conf file for the corp100.com zone:

   ```
   zone "corp100.com" in {
   type slave;
   masters {1.1.1.2;};
   notify yes;
   file "/var/named/db.corp100.com";
   }
   ```

2. After editing the named.conf file, restart DNS service for the change to take effect.

**Secondary Windows 2000/2003 Server**

1. Click **Start** -> **All Programs** -> **Administrative Tools** -> **DNS**.
2. Click + (for ns2) -> + (for Forward Lookup Zones) -> corp100.com.
3. Right-click corp100.com, and then select **Properties** -> **General**.
4. On the **General** page in the corp100.com Properties dialog box, enter the following:
   - **Zone file name**: corp100.com.dns
   - **IP address**: Enter **1.1.1.2**, and then click **Add**.
   - In the IP Address field, select **1.1.1.3** (the NAT IP address of the legacy DNS server), and then click **Remove**.
5. To save the configuration and close the corp100.com Properties dialog box, click **OK**.

**Configuring NAT and Policies on the Firewall**

Change the NAT and policy settings on the firewall to allow bidirectional DNS traffic to and from ns1.corp100.com and NTP traffic from ns1.corp100.com to the NTP server at 3.3.3.3.

For example, enter the following commands on a juniper firewall running ScreenOS 4.x or later:

```bash
set address dmz ns1 10.1.5.2/32
set address untrust ntp_server 3.3.3.3/32
set interface ethernet1 mip 1.1.1.2 host 10.1.5.2
set policy from dmz to untrust ns1 any dns permit
set policy from untrust to dmz any mip(1.1.1.2) dns permit
set policy from dmz to untrust ns1 ntp_server ntp permit
```

At this point, the new DNS server can take over DNS service from the legacy server. You can remove the legacy server and unset any firewall policies permitting traffic to and from 10.1.5.3.
Deploying Independent Appliances

DEPLOYING AN INDEPENDENT HA PAIR

To deploy an independent HA pair, you cable the HA and LAN1 or LAN2 ports to the network and configure the IP settings for these ports and the VIP address within the same subnet. For information about HA pairs, see About HA Pairs on page 142.

The default LAN1 or LAN2 settings are as follows:
- IP address: 192.168.1.2
- Netmask: 255.255.255.0

You can configure an HA pair using the Infoblox NIOS Startup Wizard.
- Requirements: HTTPS connections from your management system to the Ethernet ports on the two appliances.
- Advantage: The startup wizard provides step-by-step guidance for configuring the network settings of the VIP address and HA and LAN (or LAN1) ports on both nodes, for setting the host name, admin password, and system clock, and—if using NTP (Network Time Protocol)—for enabling the HA pair as an NTP client.

Using the Infoblox NIOS Startup Wizard to Configure an HA Pair

When you first make an HTTPS connection to the NIOS appliance, the Infoblox NIOS Startup Wizard guides you through various deployment options, basic network settings, and opportunities for changing the password of the superuser admin and for setting the system clock.

Configuring the Connecting Switch

To ensure that VRRP (Virtual Router Redundancy Protocol) works properly, configure the following settings at the port level for all the connecting switch ports (HA, LAN1, and LAN2):
- Trunking: Disable
- EtherChannel: Disable
- IGMP Snooping: Disable
- Port Channeling: Disable
- Speed and Duplex settings: Match these settings on both the Infoblox appliance and switch
- Disable other dynamic and proprietary protocols that might interrupt the forwarding of packets

Note: By default, a NIOS appliance automatically negotiates the optimal connection speed and transmission type (full or half duplex) on the physical links between its LAN1, HA, and MGMT ports and the Ethernet ports on the connecting switch. If the two appliances fail to auto-negotiate the optimal settings, see Modifying Ethernet Port Settings on page 148 for steps you can take to resolve the problem.

Putting Both Nodes on the Network

1. Use one of the methods described in Deploying a Single Independent Appliance on page 175 to configure the network settings of the LAN1 port of each node so that they are on the same subnet and you can reach them across the network.
2. Cable the LAN1 port and the HA port on each node to the network switch.

Note: The Ethernet ports on the Infoblox-250, -250-A, -550, -550-A, -1050, -1050-A, -1550, -1550-A, -1552, -1552-A, 1852-A and -2000 appliances are autosensing, so you can use either a straight-through or cross-over Ethernet cable for these connections.
3. Cable your management system to the network switch.
Configuring Node 1

1. Open an Internet browser window and enter `https://<the IP address of the appliance>` to make an HTTPS connection to the first node. For information about supported browsers, see supported browsers on page 33. Several certificate warnings may appear during the login process because the preloaded certificate is self-signed and has the hostname www.infoblox.com, which may not match the destination IP address you entered in step 1. To stop the warning messages from occurring each time you log in to Grid Manager, you can generate a new self-signed certificate or import a third-party certificate with a common name that matches the FQDN (fully qualified domain name) of the appliance. For information, see Managing Certificates on page 51.

2. Enter the default username and password (admin and infoblox) on the Grid Manager login page, and then click Login or press Enter. For information, see Accessing the Infoblox GUI on page 41.

3. Read the Infoblox End-User License Agreement, and then click I Accept to proceed. Grid Manager may take a few seconds to load your user profile.

4. In the NIOS Startup wizard, select Configuring an HA pair. Click Yes for the first appliance of the HA pair.

5. Click Next and complete the following to configure network settings:
   - Host Name: Enter a valid domain name for the node.
   - HA Pair Name: Enter a name for the HA pair. The default name is Infoblox.
   - Shared Secret: Enter the shared secret that both nodes use to authenticate each other when establishing a VPN tunnel for ensuing bloxSYNC traffic. The default shared secret is test.
   - Show Password: Select this to display the shared secret. Clear it to conceal the shared secret.

6. Click Next and complete the following to set properties for the first node:
   - Virtual Router ID: Enter the VRID (virtual router ID). This must be a unique VRID number—from 1 to 255—for this subnet.
   - Required Ports and Addresses: Enter information for the interfaces VIP, Node 1 HA, Node 2 HA, Node 1 LAN, and Node 2 LAN. Some fields are prepopulated by Grid Manager based on the existing configuration of the appliance. All fields are required. Click the empty fields and complete the following information:
     - Address: IP address of the interface.
     - Subnet Mask: The subnet mask of the interface.
     - Gateway: The IP address of the gateway for the subnet on which the interfaces are set. This is the same for all interfaces.
     - Port Settings: Select the port settings from the drop-down list. The list contains all settings supported by the hardware model. The default is Automatic. The appliance automatically detects the port settings.

7. Click Next and complete the following to set admin password:
   - Yes: To change the default password.
   - No: To keep the default password.
   If you select Yes, complete the following:
     - Password: Enter a password for the superuser admin account. The password cannot contain spaces and it must be at least four characters long. The password is case-sensitive.
     - Retype Password: Enter the same password.

8. Click Next and complete the following to configure time settings:
   - Time Zone: Select the applicable time zone from the drop-down list. The default is (UTC) Coordinated Universal Time.
   - Would you like to enable NTP?:
     - Select Yes to synchronize the time with external NTP servers. Click the Add icon. Grid Manager adds a row to the NTP Server table. Click the row and enter either the IP address or the resolvable host name of an NTP server. You can view a list of public NTP servers at ntp.isc.org.
     - Select No to specify a date and time.
Deploying Independent Appliances

— **Date:** Enter the data in YYYY-MM-DD format. You can also click the calendar icon to select a date from the calendar widget.
— **Time:** Enter the time in HH:MM:SS AM/PM format. You can also click the clock icon to select a time from the drop-down list.

9. Click **Next** to view the summary of the configuration. Review the information and verify that it is correct. You can change the information you entered by clicking **Previous** to go back to a previous step.

10. Click **Finish**.

### Configuring Node 2

1. Open an Internet browser window and enter `https://<the IP address of the appliance>` to make an HTTPS connection to the second node. For information about supported browsers, see **Supported Browsers** on page 33.

   Several certificate warnings may appear during the login process because the preloaded certificate is self-signed and has the hostname www.infoblox.com, which may not match the destination IP address you entered in step 1. To stop the warning messages from occurring each time you log in to Grid Manager, you can generate a new self-signed certificate or import a third-party certificate with a common name that matches the FQDN (fully qualified domain name) of the appliance. For information, see **Managing Certificates** on page 51.

2. Enter the default username and password (admin and infoblox) on the Grid Manager login screen, and then click **Login** or press Enter. For information, see **Accessing the Infoblox GUI** on page 41.

3. Read the Infoblox End-User License Agreement, and then click **I Accept** to proceed. Grid Manager may take a few seconds to load your user profile.

4. In the **NIOS Startup wizard**, select **Configuring an HA pair** to configure an independent HA pair. Click **No** to configure the second node of the HA pair.

5. Click **Next** and complete the following to configure network settings:
   — **HA Virtual IP address:** Enter the VIP (virtual IP) address and its netmask.
   — **HA Pair Name:** Enter a name for the HA pair. The default name is **Infoblox**. Ensure that you use the same name as the first node.
   — **Shared Secret:** Enter a text string that both nodes use as a shared secret to authenticate each other when establishing a VPN tunnel. The default shared secret is test. This must be the same shared secret that you entered on the first appliance.
   — **Show Password:** Click this to display the shared secret. Clear it to conceal the shared secret.

6. Click **Next**, and then complete the following to set properties for the second appliance:
   — **IP Address:** Enter the IP address of the appliance.
   — **Subnet Mask:** Enter the subnet mask of the appliance.
   — **Gateway:** Enter the IP address of the gateway of the subnet of the interface.

7. Click **Next** to view the summary of the configuration. Review the information and verify that it is correct. You can change the information you entered by clicking **Previous** to go back to a previous step.

8. Click **Finish**.

The setup of the HA pair is complete. When you next make an HTTPS connection to the HA pair, use the VIP address.
**Configuration Example: Configuring an HA Pair for Internal DNS and DHCP Services**

In this example, you set up an HA pair of NIOS appliances to provide internal DNS and DHCP services. The HA pair answers internal queries for all hosts in its domain (corp100.com). It forwards internal queries for external sites to ns1.corp100.com at 10.1.5.2 and ns2.corp100.com at 2.2.2.2. It also uses DHCP to provide dynamic and fixed addresses.

The HA pair consists of two appliances (nodes). The IP addresses of the VIP (virtual IP) address of the HA pair and the HA and LAN1 ports on each node, are as follows:

<table>
<thead>
<tr>
<th>HA Pair IP Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP 10.1.4.10 (the address that the active node of the HA pair uses)</td>
</tr>
<tr>
<td><strong>Node 1</strong></td>
</tr>
<tr>
<td>• LAN1 10.1.4.6</td>
</tr>
<tr>
<td>• HA 10.1.4.7</td>
</tr>
</tbody>
</table>

The virtual router ID number for the HA pair is 150. The ID number must be unique for this network segment. When you create the corp100.com zone on the HA pair, you import DNS data from the legacy server at 10.1.4.11.
Cabling Appliances to the Network and Turning On Power

Connect Ethernet cables from the LAN1 and HA ports on both NIOS appliances to a switch in the server network and turn on the power for both appliances. For information about installing and cabling the appliance, refer to the user guide or installation guide that ships with the product.
Specifying Initial Network Settings

Before you can configure the appliances through Grid Manager, you must be able to make a network connection to them. The default network settings of the LAN1 port are 192.168.1.2/24 with a gateway at 192.168.1.1 (the HA and MGMT ports do not have default network settings). To change these settings, you can use the LCD or make a console connection to each appliance.

Node 1

Using the LCD or console port on one of the appliances, enter the following information:

- IP Address: 10.1.4.6 (for the LAN1 port)
- Netmask: 255.255.255.0
- Gateway: 10.1.4.1

Node 2

Using the LCD or console port on the other appliance, enter the following information:

- IP Address: 10.1.4.8 (for the LAN1 port)
- Netmask: 255.255.255.0
- Gateway: 10.1.4.1

After you confirm your network settings, the Infoblox GUI application automatically restarts.

Specifying Appliance Settings

When you make the initial HTTPS connection to a NIOS appliance, the Infoblox NIOS Startup Wizard guides you through the basic deployment of the appliance on your network. To set up an HA pair, you must connect to and configure each appliance individually.

Node 1

1. Open an Internet browser window and enter https://10.1.4.6.
2. Accept the certificate when prompted.
   Several certificate warnings may appear during the login process. This is normal because the preloaded certificate is self-signed and has the hostname www.infoblox.com, which does not match the destination IP address you entered in step 1. To stop the warning messages from occurring each time you log in to Grid Manager, you can generate a new self-signed certificate or import a third-party certificate with a common name that matches the FQDN (fully-qualified domain name) of the appliance. This is a very simple process. For information about certificates, see Managing Certificates on page 51.
3. Enter the default username and password (admin and infoblox) on the Grid Manager login page, and then click Login or press Enter. For information, see Accessing the Infoblox GUI on page 41.
4. Read the Infoblox End-User License Agreement, and then click I Accept to proceed. Grid Manager may take a few seconds to load your user profile.
5. In the NIOS Startup wizard, select Configuring an HA pair. Click Yes to configure the first appliance.
6. Click Next and complete the following to configure network settings:
   - Host Name: Enter ns3.corp100.com.
   - HA Pair Name: Use the default name Infoblox.
   - Shared Secret: Enter 37eeT1d.
7. Click **Next** and complete the following to set properties for the first node:
   - **Virtual Router ID**: Enter 150.
   - **Required Ports and Addresses**: In the table, click the empty fields and enter the following information for each corresponding interface:
     - **VIP**: 10.1.4.10
     - **Node 1 HA**: 10.1.4.7
     - **Node 2 HA**: 10.1.4.9
     - **Node 1 LAN**: 10.1.4.6
     - **Node 2 LAN**: 10.1.4.8
     - **Subnet Mask**: 255.255.255.0
     - **Gateway**: 10.1.4.1

   **Note**: Some fields are prepopulated by Grid Manager based on the existing configuration of the appliance. All fields are required.

8. Click **Next** and complete the following to set admin password:
   - **Would you like to set admin password?**: Click No.

9. Click **Next** and complete the following to configure time settings:
   - **Time Zone**: Select **UMT – 8:00 Pacific Time (US and Canada), Tijuana** from the drop-down list.
   - **Would you like to enable NTP?**: Select Yes to synchronize the time with external NTP servers, and then click the Add icon. Grid Manager adds a row to the NTP Server table. Click the row and enter 3.3.3.3 in the NTP Server field.

10. Click **Next** to view the summary of the configuration. Review the information and verify that it is correct. You can change the information you entered by clicking **Previous** to go back to a previous step.
11. Click **Finish**.

**Node 2**

1. From the **System** tab, select the **System Manager** tab, and then click **System Properties -> Setup Wizard** from the Toolbar.

2. In the **NIOS Startup wizard**, select **Configuring an HA pair** to configure an independent HA pair. Click No for configuring node 2 of the HA pair.

3. Click **Next**, and then complete the following to configure network settings:
   - **HA Virtual IP address**: Enter 10.1.4.10.
   - **HA Pair Name**: Use the default name Infoblox.
   - **Shared Secret**: Enter 37eeT1d.
   - **Show Password**: Click this to display the shared secret.

4. Click **Next**, and then complete the following to set properties for the second appliance:
   - **IP Address**: Enter 10.1.4.8.
   - **Subnet Mask**: Enter 255.255.255.0.
   - **Gateway**: Enter 10.1.4.1.

5. Click **Next** to view the summary of the configuration. Review the information and verify that it is correct. You can change the information you entered by clicking **Previous** to go back to a previous step.

6. Click **Finish**.

The setup of the HA pair is complete. From now on, when you make an HTTPS connection to the HA pair, use the VIP address 10.1.4.10.
Enabling Zone Transfers

To allow the NIOS appliance to import zone data from the legacy server at 10.1.4.11, you must configure the legacy server to allow zone transfers to the appliance at 10.1.4.10.

Legacy BIND Server

1. Open the named.conf file using a text editor and change the allow-transfer statement to allow zone transfers to the appliance at 10.1.4.10. For a sample of the required changes to the named.conf file, see Legacy BIND Server on page 182.
2. After editing the named.conf file, restart DNS service for the change to take effect.

Legacy Windows 2000/2003 Server

Navigate to the corp100.com Properties dialog box, and add 10.1.4.10 to the list of IP addresses to which you want to allow zone transfers. For more detailed navigation and configuration instructions, see Legacy Windows 2000/2003 Server on page 182.

Importing Zone Data

You can import zone data from a legacy server to an independent HA pair, as described in Importing Zone Data on an Independent Appliance on page 182. Use the following information:

- Forward-mapping zone: corp100.com
- Import zone from: 10.1.4.11
- Reverse-mapping zone: 1.1.1.0

Defining Networks, Reverse-Mapping Zones, DHCP Ranges, and Infoblox Hosts

In this task, you enter data manually. For large data sets, you have the option of using the Data Import Wizard for loading DNS and DHCP configurations and data to make the process more efficient. To download the Data Import Wizard, visit www.infoblox.com/import/.

Networks

You can create all the subnetworks individually (which in this example are 10.1.1.0/24, 10.1.2.0/24, 10.1.4.0/24, and 10.1.5.0/24), or you can create a parent network (10.1.0.0/16) that encompasses all the subnetworks and then use the Infoblox split network feature to create the individual subnetworks automatically. The split network feature accomplishes this by using the IP addresses that exist in the forward-mapping zones to determine which subnets it needs to create. This example uses the split network feature. For information about creating networks, see Configuring a DHCP Network on page 505.

1. From the Data Management tab, select the IPAM tab, and then click Add -> Add IPv4 Network from the Toolbar.
2. In the Add Network wizard, complete the following:
   - Address: 10.1.0.0
   - Netmask: Use the netmask slider to select the /16 (255.255.0.0) netmask.
3. Click Next to select a server. Click the Add icon. Grid Manager displays ns3.corp100.com in the table.
4. Click Save & Close.
5. In the IPAM tab, select the 10.1.0.0/16 check box, and then select Split from the Toolbar.
6. In the *Split Network* dialog box, complete the following:
   - **Subnetworks**: Move the slider to 24.
   - **Immediately Add**: Select *Only networks with ranges and fixed addresses*.
   - **Automatically create reverse-mapping zones**: Select this check box.

7. Click **OK**.

   The appliance creates the following 24-bit subnets for the imported Infoblox hosts:
   - 10.1.1.0/24
   - 10.1.2.0/24
   - 10.1.4.0/24
   - 10.1.5.0/24

8. From the IPAM tab, click the **10.1.1.0/24** check box, and then click the Edit icon.

9. In the **DHCP Network** editor, enter information in the following tabs:
   - **General**
     - **Comment**: MGT
   - **Server Assignment**
     - Add ns3.corp100.com as a server.

10. Click **Save & Close**.

11. To modify the other networks, repeat steps #8 – 10 for each network and use the following information:
   - **10.1.2.0/24 Network**:
     - **Comment**: Dev
     - **Server Assignment**: ns3.corp100.com
   - **10.1.4.0/24 Network**:
     - **Comment**: Server
     - **Server Assignment**: ns3.corp100.com
   - **10.1.5.0/24 Network**:
     - **Comment**: DMZ
     - **Server Assignment**: ns3.corp100.com

**DHCP Ranges**

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **10.1.1.0/24**, and then click **Add** -> **DHCP Range** from the Toolbar.

2. In the **Add Range** wizard, complete the following:
   - **Start**: 10.1.1.10
   - **End**: 10.1.1.50

3. Click **Next**, and then select **Server**, Grid Manager displays ns3.corp100.com as the assigned member.

4. Click **Save & Close**.

5. In the **Networks** tab, click **10.1.2.0/24**, and then click **Add** -> **DHCP Range** from the Toolbar.

6. In the **Add Range** wizard, complete the following:
   - **Start**: 10.1.2.10
   - **End**: 10.1.2.50

7. Click **Next**, and then select **Server**, Grid Manager displays ns3.corp100.com as the assigned member.

8. Click **Save & Close**.
**Infoblox Hosts**

Defining both a MAC and IP address for an Infoblox host definition creates a DHCP host entry—like a fixed address—that you can manage through the host object. To add a MAC address to each host record that the appliance created when you imported forward- and reverse-mapping zone records:

1. From the **Data Management** tab, select the **IPAM** tab -> 10.1.1.0/24 -> 10.1.1.2.
2. In the **Related Objects** tab, select the check box of the host record, and then click the Edit icon.
3. In the **Host Record** editor, select the check box of the host record, and then click the **Edit** icon.
   - **MAC Address**: 00:00:00:aa:aa:aa
4. Click **Save & Close**.
5. Follow steps 1 – 4 to modify hosts with the following information:
   - **printer2**
     - IP Address: 10.1.2.2
     - MAC Address: 00:00:00:bb:bb:bb
   - **storage1**
     - IP Address: 10.1.4.2
     - MAC Address: 00:00:00:dd:dd:dd
   - **storage2**
     - IP Address: 10.1.4.3
     - MAC Address: 00:00:00:dd:dd:dd
   - **proxymail**
     - IP Address: 10.1.4.4
     - MAC Address: 00:00:00:ee:ee:ee
   - **proxyweb**
     - IP Address: 10.1.4.5
     - MAC Address: 00:00:00:ee:ee:ee
   - **www**
     - IP Address: 10.1.5.5
     - MAC Address: 00:00:00:ff:ff:ff
   - **mail**
     - IP Address: 10.1.5.6
     - MAC Address: 00:00:00:ff:ff:ff
   - **ftp**
     - IP Address: 10.1.5.7
     - MAC Address: 00:00:00:ff:ff:ff
   - **www**
     - IP Address: 10.1.5.8
     - MAC Address: 00:00:00:ff:ff:ff
Defining Multiple Forwarders

Because ns3.corp100.com is an internal DNS server, you configure it to forward DNS queries for external DNS name resolution to the primary and secondary DNS servers—ns1.corp100.com at 10.1.5.2 and ns2.corp100.com at 2.2.2.2.

1. From the Data Management tab, select the DNS tab, and then select System DNS Properties from the Toolbar.
2. In the System DNS Properties editor, click the Add icon in the Forwarders tab. Grid Manager adds a row to the table. Complete the following:
   - Address: Type 2.2.2.2. Click Add again to add another forwarder.
   - Address: Type 10.1.5.2.
3. Click Save & Close.

Each of the forwarders is assigned a random response time. The appliance sends the initial outbound query to the forwarder that has the lowest response time. If the first forwarder does not reply, the appliance tries the one with the next lowest random response time. The appliance adjusts and keeps track of the response times of the forwarders, and uses the quicker one for future queries. If the quicker forwarder does not respond, the appliance then uses another one.

Enabling Recursion on External DNS Servers

Because the HA pair forwards outbound queries to the two external DNS servers ns1.corp100.com (10.1.5.2) and ns2.corp100.com (2.2.2.2) for resolution, you must enable recursion on those servers. When a DNS server employs recursion, it queries other DNS servers for a domain name until it either receives the requested data or an error that the requested data cannot be found. It then reports the result back to the server that queried—in this case, the internal DNS server ns3.corp100.com (10.1.4.10), which in turn reports back to the DNS client.

Infoblox Server in the DMZ Network (ns1.corp100.com, 10.1.5.2)

1. From the Data Management tab, select the DNS tab, and then click System DNS Properties from the Toolbar.
2. In the System DNS Properties editor, select the Allow Recursion check box from the Queries tab, and then click the Add icon -> IPv4 Address. Grid Manager adds a row to the Allow recursive queries from table. Complete the following:
   - Permission: Select Allow from the drop-down list.
   - Name: Enter 10.1.1.52.
3. Click Save & Close.

BIND Server at ISP Site (ns2.corp100.com, 2.2.2.2)

1. Open the named.conf file using a text editor and change the recursion and allow-recursion statements to allow recursive queries from 1.1.1.8 (the NAT address of ns3).

   ```
   options {
     zone-statistics yes;
     directory "/var/named/named_conf";
     version "";
     recursion yes;
     listen-on { 127.0.0.1; 2.2.2.2; };
     ...
     allow-recursion {1.1.1.8;};
     transfer-format many-answers;
   }
   ...
   ```
2. After editing the named.conf file, restart DNS service for the change to take effect.
Windows 2000/2003 Server at ISP Site (ns2.corp100.com, 2.2.2.2)

1. Click **Start** -> **All Programs** -> **Administrative Tools** -> **DNS**.
2. Right-click **ns3**, and then select **Properties** -> **Advanced**.
3. On the **Advanced** page in the **ns3 Properties** dialog box, clear the **Disable recursion** check box.
4. To save the configuration change and close the **ns3 Properties** dialog box, click **OK**.

Modifying the Firewall and Router Configurations

Configure the firewall and router in your internal network to allow the following DHCP, DNS, and NTP traffic:

- To allow messages to pass from the DHCP clients in the DMZ—the web, mail, and FTP servers—to ns3 in the Server network, configure policies and DHCP relay agent settings on the firewall.
- To forward DHCP messages from DHCP clients in the MGT and Dev networks to ns3 in the Server network, configure relay agent settings on the router.
- To translate the private IP address of ns3 (10.1.4.10) to the public IP address (1.1.1.8) when forwarding DNS queries from ns3 to ns2, set a MIP (mapped IP) address on the firewall.
- To allow DNS queries from ns3 to ns1 and ns2 and NTP traffic from ns3 to the NTP server, configure firewall policies.

**Firewall**

For example, enter the following commands on a Juniper firewall running ScreenOS 4.x or later:

**DHCP Relay Configuration**

- `set address trust ns3 10.1.4.10/32`
- `set interface ethernet2 dhcp relay server-name 10.1.4.10`
- `set policy from dmz to trust ns1 ns3 DHCP-Relay permit`

**DNS Forwarding**

- `set interface ethernet1 mip 1.1.1.8 host 10.1.4.10`
- `set policy from trust to untrust ns3 ns2 dns permit`
- `set policy from trust to dmz ns3 ns1 dns permit`

**NTP**

- `set policy from dmz to untrust ns1 ntp_server ntp permit`

**Router**

For example, enter the following commands on a Cisco router running IOS for release 12.x or later:

**DHCP Relay Configuration**

- `interface ethernet1`
  - `ip helper-address 10.1.4.10`
- `interface ethernet2`
  - `ip helper-address 10.1.4.10`
Enabling DHCP and Switching Service to the NIOS Appliance

With the Infoblox in place and the firewall and router configured for relaying DHCP messages, you can switch DHCP service from the legacy DHCP server at 10.1.4.11 to the HA pair at 10.1.4.10 (VIP address).

**Tip:** To minimize the chance of duplicate IP address assignments during the transition from the legacy DHCP server to the appliance, shorten all lease times to a one-hour length in advance of the DHCP server switch. Then, when you take the legacy DHCP server offline, the DHCP clients quickly move to the new server when their lease renewal efforts fail and they broadcast DHCPDISCOVER messages. To determine how far in advance you need to shorten the lease length, find the longest lease time (for example, it might be two days). Then change the lease length to one hour at a slightly greater interval of time before you plan to switch DNS service to the appliance (for example, three days before the switch over). By changing the lease length this far in advance, you can be sure that all DHCP leases will be one-hour leases at the time of the switch-over. If the longest lease length is longer—such as five days—and you want to avoid the increased amount of traffic caused by more frequent lease renewals over a six-day period, you can also employ a stepped approach: Six days before the switch-over, change the lease lengths to one-day leases. Then two days before the switch-over, change them to one-hour leases.

1. Open an Internet browser window, enter `https://10.1.4.10`, and then log in to the appliance using the username `admin` and password `SnD34n534`.
2. From the Data Management tab, select the DHCP tab, and then click Start from the Toolbar.
3. In the Start Member DHCP Service dialog box, click Yes.
   The HA pair is ready to provide DHCP service to the network.
4. Take the legacy DHCP server at 10.1.4.11 offline.
   When the DHCP clients are unable to renew their leases from the legacy DHCP server, they broadcast DHCPDISCOVER messages to which the new DHCP server responds.

Managing and Monitoring

Infoblox provides tools for managing IP address usage and several types of logs to view events of interest and DHCP and DNS data. After configuring the appliance, you can use the following resources to manage and monitor IP address usage, DNS and DHCP data, and administrator and appliance activity.

**IPAM (IP Address Management)**

IPAM offers the following services:

- Simple IP address modification — Within a single IP address-centric data set, you can modify the Infoblox host, DHCP, and DNS settings associated with that IP address.
- Address type conversion — Through IPAM functionality, you can make the following conversions:
  - Currently active dynamic addresses to fixed addresses, reserved addresses, or Infoblox hosts.
  - Fixed addresses to reservations or hosts.
  - Reservations to hosts.
- Device classification — You can make detailed descriptions of appliances in DHCP ranges and appliances defined as Infoblox hosts and as fixed addresses.
- Three distinct views of IP address usage — To monitor the usage of IP addresses on your network, you can see the following different views:
  - High-level overall network view: From the Data Management tab, select the IPAM tab -> member. You can view the network usage in the Net Map or List view. You can also drill down to specific IP address to get detailed information.
  - DHCP lease history records: From the Data Management tab, select the DHCP tab -> Leases tab -> Lease History.
Verifying the Deployment

After you deploy a single independent appliance or HA pair, you can make an HTTPS connection to it, log in, and check its status.

Single Independent Appliance

From the Dashboard, check the appliance status in the System Status widget. For information, see Member Status (System Status) on page 58.

- If the Status icon is green, the appliance has a network connection and is operating properly.
- If the Status icon is red, there is a problem. To determine what it is, look at the system log file for this appliance by selecting the Administration tab -> Logs tab -> Syslog.

Independent HA Pair

1. Make an HTTPS connection to the VIP address of the HA pair, log in, and check the status of both nodes.
2. From the Dashboard, check the appliance status in the System Status widget. For information, see Member Status (System Status) on page 58.
   - If the Status icon is green, both nodes have connectivity with each other and are operating properly.
   - If the Status icon is yellow, the two nodes are in the process of forming an HA pair.
   - If the Status icon is red, the passive node is offline or there is a problem. To determine what it is, look at the system log file by selecting the Administration tab -> Logs tab -> Syslog. You can also gather information from the System tab -> System Manager tab. For information, refer to the online Help.
INFOBLOX TOOLS FOR MIGRATING DATA

Typically, the next step after cabling a single independent appliance to a network and configuring its network settings—or cabling two independent appliances to a network and configuring them as an HA pair—is to import data from legacy DNS, DHCP, and TFTP servers. Infoblox provides several tools to accomplish this:

- The Infoblox Data Import Wizard is a useful tool that simplifies the importation of DNS, DHCP and IPAM (IP address management), and TFTP settings and data into a NIOS appliance. For large data sets, this option is an efficient approach. To download the Data Import Wizard, visit www.infoblox.com/import/.

- You can use prewritten Infoblox Perl API scripts or write your own scripts to ease the execution of large and repetitive operations such as importing data for large numbers of networks and zones. To download script packs, log in to http://www.infoblox.com/en/support/support-center-login.html, and navigate to the Downloads section. Each script has a corresponding HTML Help file. For a more general introduction to using the Infoblox API, refer to the Infoblox API Documentation, which is available in the Technical Library section of the Infoblox Support site.

- For smaller DNS data sets, you can use the zone import feature, which allows you to import data on a per-zone basis (see Importing Zone Data on page 394).
Chapter 7  Managing Appliance Operations

Managing the operations of a NIOS appliance involves defining system parameters such as time, security, and port settings. This chapter describes how to set these operational parameters and how to set up a static route when the NIOS appliance can send and receive traffic through multiple gateways. The tasks covered in this chapter include:

- **Managing Time Settings** on page 203
  - *Changing Time and Date Settings* on page 203
  - *Changing Time Zone Settings* on page 203
  - *Monitoring Time Services* on page 204
- **Using NTP for Time Settings** on page 205
  - *Authenticating NTP* on page 206
  - *NIOS Appliance as NTP Client* on page 208
  - *Configuring a Grid to Use NTP* on page 209
  - *Configuring Grid Members to Use NTP* on page 211
  - *NIOS Appliance as NTP Server* on page 212
  - *Configuring a NIOS Appliance as an NTP Server* on page 213
  - *Monitoring NTP* on page 215
- **Scheduling Tasks** on page 216
  - *Scheduling Additions and Modifications* on page 217
  - *Scheduling Appliance Operations* on page 217
  - *Scheduling Deletions* on page 217
  - *Viewing Scheduled Tasks* on page 218
  - *Rescheduling Tasks* on page 220
  - *Guidelines for Upgrading, Backing Up, and Restoring the Database* on page 221
- **About Extensible Attributes** on page 222
  - *Configuring Extensible Attributes* on page 223
  - *Using Extensible Attributes* on page 225
- **Managing Security Operations** on page 227
  - *Enabling Support Access* on page 227
  - *Enabling Remote Console Access* on page 227
  - *Permanently Disabling Remote Console and Support Access* on page 227
  - * Restricting GUI/API Access* on page 227
  - *Enabling HTTP and GUI Redirections* on page 227
  - *Modifying the Session Timeout Setting* on page 228
Managing Appliance Operations

- Disabling the LCD Input Buttons on page 228
- Configuring Security Features on page 228

- Ethernet Port Usage on page 230
  - Modifying Ethernet Port Settings on page 235

- Using the LAN2 Port on page 236
  - About NIC Redundancy on page 237
  - Configuring the LAN2 Port on page 238
  - Enabling DHCP on LAN2 on page 238
  - Enabling DNS on LAN2 on page 239

- Using the MGMT Port on page 240
  - Appliance Management on page 241
  - Grid Communications on page 243
  - DNS Services on page 245

- Setting Static Routes on page 247

- Enabling DNS Resolution on page 251

- Managing Licenses on page 252
  - Obtaining and Adding Licenses on page 252
  - Obtaining Temporary Licenses on page 253
  - Viewing Licenses on page 253
  - Backing Up Licenses on page 253
  - Removing Licenses on page 254

- Shutting Down, Rebooting, and Resetting a NIOS Appliance on page 255
  - Rebooting a NIOS Appliance on page 255
  - Shutting Down a NIOS Appliance on page 255
  - Resetting a NIOS Appliance on page 255

  - About RAID 10 on page 257
  - Evaluating the Status of the Disk Subsystem on page 258
  - Appliance Front Panel on page 259
  - Replacing a Failed Disk Drive on page 259
  - Disk Array Guidelines on page 260

- Restarting Services on page 261
  - Canceling a Scheduled Restart on page 263
Managing Time Settings

You can define the date and time settings for your NIOS appliance using the Infoblox Appliance Startup Wizard. Alternatively, you can set the date and time of the appliance anytime after you first configure it if you did not do so using the startup wizard or if you need to change it if, for example, you move an appliance from a location in one time zone to a location in a different time zone. To set the date and time of the appliance, you can either manually enter the values or configure the appliance to synchronize its time with a public NTP server.

Changing Time and Date Settings

If you do not use the NTP service, you can set the date and time for a grid.

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

To set the time and date for a grid using the Grid Properties editor:

1. From the Grid tab, select the Grid Manager tab, expand the Toolbar and click Grid Properties -> Edit.
2. In the General tab of the Grid Properties editor, complete the following:
   - Date: Click the calendar icon to select a date or enter the date in YYYY-MM-DD format.
   - Time: Click the clock icon to select a time or enter the time in HH:MM:SS format. For afternoon and evening hours, use the integers 13-24.
3. Click Save.

Note: Changing the date and time resets the application and terminates the management session.

Changing Time Zone Settings

Whether you enable NTP (Network Time Protocol) or manually configure the date and time, you must always set the time zone manually. You can set the time zone for a grid, which then applies to all members. If different members are in different time zones, you can choose the time zone that applies to most members at the grid level, and then override the setting for the remaining members.

Note: Changing the time zone does not reset the application nor does it terminate the management session.

To set the time zone for a grid or member:

1. Grid: From the Grid tab, select the Grid Manager tab, expand the Toolbar and click Grid Properties -> Edit. Member: From the Grid tab, select the Grid Manager tab -> Members tab -> grid_member check box, and then click the Edit icon.
   To override an inherited property, click Override next to it and complete the appropriate fields.
2. In the General tab of the editor, select the appropriate time zone.
3. Select one of the following:
   - Save & Close: Save the entry and close the editor.
   - Save: Save the entry and keep the editor open.
Monitoring Time Services

In a grid, the grid master and its members use an internal NTP daemon to synchronize their time. It is not user-configurable and functions regardless of how you set the time on the grid master. The Detailed Status panel contains an NTP Synchronization icon so you can monitor the internal NTP daemon that runs within a grid to ensure the time among its members is synchronized.

To display the Detailed Status panel, from the Grid tab, select the Grid Manager tab -> Members tab -> grid_member check box, and then click the Detailed Status icon in the table toolbar of the Members panel.

The following are descriptions of the NTP status icons in the Detailed Status panel:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green" /></td>
<td>Green</td>
<td>The NTP service is running properly.</td>
</tr>
<tr>
<td><img src="image" alt="Yellow" /></td>
<td>Yellow</td>
<td>The appliance is synchronizing its time.</td>
</tr>
<tr>
<td><img src="image" alt="Red" /></td>
<td>Red</td>
<td>The NTP service is not running properly. View the corresponding description for additional information.</td>
</tr>
</tbody>
</table>
Using NTP for Time Settings

Note: vNIOS grid members on Cisco do not support the NTP service. vNIOS grid members on Riverbed can be NTP clients only.

NTP (Network Time Protocol) is a standard protocol that system clocks use to ensure their time is always accurate. Appliances that use NTP try to get their time as close as possible to UTC (Coordinated Universal Time), the standard timescale used worldwide. NTP uses UDP (User Datagram Protocol) on port 123 for communications between clients and servers.

NTP is based on a hierarchy where reference clocks are at the top. Reference clocks use different methods such as special receivers or satellite systems to synchronize their time to UTC. NTP servers on the first level of the hierarchy synchronize their time with the reference clocks, and serve time to clients as well. Each level in the hierarchy is a stratum; stratum-0 is a reference clock. Stratum-1 servers synchronize their clocks with reference clocks. Stratum-2 servers synchronize their clocks with stratum-1 servers, and so forth. The stratum number indicates the number of levels between the NTP server and the reference clock. A higher stratum number could indicate more variance between the NTP server and the reference clock.

You can configure a NIOS appliance to function as an NTP client that synchronizes its clock with an NTP server. NTP clients typically use time information from at least three different sources to ensure reliability and a high degree of accuracy. There are a number of public NTP servers on the Internet with which the NIOS appliance can synchronize its clock. For a list of these servers, you can access http://www.ntp.org.

In a grid, the grid master and grid members can function as NTP clients that synchronize their clocks with external NTP servers. They can in turn function as NTP servers to other appliances in the network. This allows you to deploy multiple NTP servers to ensure accurate and reliable time across the network. To configure the grid master and grid members as NTP clients, you must first enable the NTP service and configure external NTP servers at the grid level. You can then configure the grid master and grid members to override the grid-level NTP servers and use their own external NTP servers. A grid member synchronizes its clock with the grid master if you do not configure it to use external NTP servers.
Managing Appliance Operations

Figure 7.1 Infoblox Appliances as NTP Servers

Stratum-1 NTP servers use reference clocks to synchronize their time to UTC (Coordinated Universal Time).

In this example, the grid master—as an NTP client—synchronizes its time with stratum-1 NTP servers. The grid master also functions as a stratum-2 NTP server to Grid Member 1. NTP messages between the grid master and Grid Member 1 go through encrypted VPN tunnels.

As an NTP client, Grid Member 1 synchronizes its clock with the grid master. It also functions as a stratum-3 NTP server to external devices on its network.

Authenticating NTP

To prevent intruders from interfering with the time services on your network, you can authenticate communications between a NIOS appliance and a public NTP server, and between a NIOS appliance and external NTP clients. NTP communications within the grid go through an encrypted VPN tunnel, so you do not have to enable authentication between members in a grid.

NTP uses symmetric key cryptography, where the server and the client use the same algorithm and key to calculate and verify a MAC (message authentication code). The MAC is a digital thumbprint of the message that the receiver uses to verify the authenticity of a message.

As shown in Figure 7.2, the NTP client administrator must first obtain the secret key information from the administrator of the NTP server. The server and the client must have the same key ID and data. Therefore, when you configure the NIOS appliance as an NTP client and want to use authentication, you must obtain the key information from the administrator of the external NTP server and enter the information on the NIOS appliance. When you configure a NIOS appliance as an NTP server, you must create a key and send the key information to clients in a secure manner. A key consists of the following:

- **Key Number**: A positive integer that identifies the key.
- **Key Type**: Specifies the key format and the algorithm used to calculate the MAC (message authentication code) of a message.
  - **M**: The key is a 1-31 character ASCII string using MD5 (Message Digest).
  - **S**: The key is a 64-bit hexadecimal number in DES (Data Encryption Standard) format. The high order 7 bits of each octet form the 56-bit key, and the low order bit of each octet is given a value so that the octet maintains odd parity. You must specify leading zeros so the key is exactly 16 hexadecimal digits long and maintains odd parity.
- A: The key is a DES key written as a 1-8 character ASCII string.
- N: The key is a 64-bit hexadecimal number in NTP format. It is the same as the S format, but the bits in each octet have been rotated one bit right so the parity bit is in the high order bit of the octet. You must specify leading zeros and odd parity must be maintained.

- Key String: The key data used to calculate the MAC. The format depends on the Key Type you select.

When the NTP client initiates a request for time services to the NTP server, it creates the MAC by using the agreed upon algorithm to compress the message and then encrypts the compressed message (which is also called a message digest) with the secret key. The client appends the MAC to the message it sends to the NTP server. When the NTP server receives the message from the client, it performs the same procedure on the message — it compresses the message it received, encrypts it with the secret key and generates the MAC. It then compares the MAC it created with the MAC it received. If they match, the server continues to process and respond to the message. If the MACs do not match, the server ignores the message.

*Figure 7.2 NTP Client Administrator Obtaining Secret Key from NTP Server Administrator*

NTP server administrator sends the secret key information to the NTP client administrator, who adds the key to the NTP client. When the NTP client sends a request for time services to the NTP server, it uses the agreed upon algorithm and secret key to create the MAC (message authorization code). It then sends the MAC and message to the NTP server.

NTP server uses the agreed upon algorithm and secret key to create the MAC. It compares this MAC with the MAC it received. If they match, the server responds to the request of the client for time services. If the MACs do not match, the server ignores the message from the client.
NIOS Appliance as NTP Client

You can configure an independent NIOS appliance, a grid master, or any grid member in a grid as an NTP client that synchronizes its system clock with an external NTP server.

When you enable a NIOS appliance to function as an NTP client, you must specify at least one NTP server with which the appliance can synchronize its clock. Infoblox recommends that you specify multiple NTP servers that synchronize their time with different reference clocks and that have different network paths. This increases stability and reduces risk in case a server fails. For a list of public NTP servers, you can access www.ntp.org.

When you specify multiple NTP servers, the NTP daemon on the appliance determines the best source of time by calculating round-trip time, network delay, and other factors that affect the accuracy of the time. NTP periodically polls the servers and adjusts the time on the appliance until it matches the best source of time. If the difference between the appliance and the server is less than five minutes, the appliance adjusts the time gradually until the clock time matches the NTP server. If the difference in time is more than five minutes, the appliance immediately synchronizes its time to match that of the NTP server.

To secure communications between a NIOS appliance and an NTP server, you can authenticate communications between the appliance and the NTP server. When you configure authentication, you must obtain the key information from the administrator of the NTP server and enter the key on the appliance. For information, see Authenticating NTP on page 206.

In a grid, you can configure the grid master and grid members to synchronize their clocks with external NTP servers. When you enable the NTP service on the grid, the grid master automatically functions as an NTP server to the grid members. A grid member can synchronize its time with the grid master, an external NTP server, or another grid member. When grid members synchronize their times with the grid master, the grid master and its members send NTP messages through an encrypted VPN tunnel, as shown in Figure 7.3. When a grid member synchronizes its time with another grid member, the NTP messages are not sent through a VPN tunnel.

Figure 7.3 Grid Master as NTP Client
Using NTP for Time Settings

Using NTP for Time Settings

Configuring a Grid to Use NTP

In a grid, the grid master and grid members can synchronize their clocks with external NTP servers. They then forward the clock time to other appliances in the network. Likewise, in an independent HA pair, the active node communicates directly with an external NTP server. The passive node then synchronizes its clock with the active node.

In a grid, you must first enable the NTP service and configure external NTP servers at the grid level before you configure the grid master and grid members as NTP clients.

To configure a grid master as an NTP client, perform the following tasks:

- If you want to enable authentication between the grid members and NTP servers, you must specify the authentication keys before enabling the NTP service. You can specify authentication keys at the grid and member levels. For information, see Adding NTP Authentication Keys.
- Enable the NTP service on the grid and specify one or more external NTP servers. For information, see Enabling the NTP Service on page 210.

Adding NTP Authentication Keys

To enable authentication between the appliance and the NTP servers, add the authentication keys before enabling the NTP service on the grid. You can specify authentication keys at the grid and member levels.

To add NTP authentication keys:

1. **Grid**: From the Grid tab, select the Grid Manager tab, expand the Toolbar and click NTP -> NTP Grid Config.
   
   **Member**: From the Grid tab, select the Grid Manager tab -> Members tab -> grid_member check box. Expand the Toolbar and click NTP -> NTP Member Config.

   To override an inherited property, click Override next to it and complete the appropriate fields.

   1. Click the Add icon in the NTP Keys section and enter the following information.
      
      - **Key Number**: A positive integer that identifies a key.
      - **Type**: Specifies the key format and the algorithm used to calculate the MAC (message authentication code) of a message.
        
        - **MD5 in ASCII format (M)**: The key is a 1-31 character ASCII string using MD5 (Message Digest).
        - **DES in hex format (S)**: The key is a 64-bit hexadecimal number in DES (Data Encryption Standard) format. The high order 7 bits of each octet form the 56-bit key, and the low order bit of each octet is given a value so that the octet maintains odd parity. You must specify leading zeros so the key is exactly 16 hexadecimal digits long and maintains odd parity.
        - **DES in ASCII format (A)**: The key is a DES key written as a 1-8 character ASCII string.
        - **DES in NTP format (N)**: The key is a 64-bit hexadecimal number in NTP format. It is the same as the S format, but the bits in each octet have been rotated one bit right so the parity bit is in the high order bit of the octet. You must specify leading zeros and odd parity must be maintained.
      - **String**: The key data used to calculate the MAC. The format depends on the Key Type you select.

   2. Click **Save** to save the entry and keep the editor open so you can enable the grid to synchronize its time with external NTP servers, as described in Enabling the NTP Service.

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

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

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

1. From the Grid tab, select the Grid Manager tab, expand the Toolbar and click NTP -> NTP Grid Config.
2. In the Grid NTP Properties editor, select Synchronize the Grid with NTP Servers.
3. Click the Add icon in the External NTP Servers table.
4. In the Add NTP Server dialog box, enter the following information, and then click Add.
   - **NTP Server**: Enter either the IP address or the resolvable host name of an NTP server. You can view a list of public NTP servers at ntp.isc.org. To check whether the DNS server can resolve the NTP server host name, click Resolve Name. You must have a DNS name resolver configured. For information, see Enabling DNS Resolution on page 251. 
   - **Enable Authentication**: Select this option to enable authentication of NTP communications between the external NTP server and the NIOS appliance (the grid master or grid member in a grid, an independent NIOS appliance, or the active node in an independent HA pair).

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

   - **Authentication Key**: Select a key that you previously entered, and then click OK. For information, see Adding NTP Authentication Keys on page 209.

5. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.
Configuring Grid Members to Use NTP

To configure grid members to synchronize their time with external NTP servers:

1. From the Grid tab, select the Grid Manager tab → Members tab → grid_member check box.
2. Expand the Toolbar and click NTP → NTP Member Config.
3. In the Member NTP Configuration editor, do the following:
   - Synchronize this Member with other NTP Servers: Select this option to enable this grid member to use external NTP servers. When you select this check box, you must enter at least one external NTP server for the member.
   - Exclude Grid Master as NTP Server: Select this option if you want to exclude the grid master from being one of the time sources. By default, the appliance automatically configures the grid master as the backup NTP server for a grid member. When the member cannot reach any of its configured NTP servers, it uses the grid master as the NTP server.
4. Click Override, and then click the Add icon in the External NTP Servers table.
5. In the Add NTP Server dialog box, enter the following information, and then click Add.
   - NTP Server: Enter either the IP address or the resolvable host name of an NTP server. You can view a list of public NTP servers at ntp.isc.org. To check whether the DNS server can resolve the NTP server host name, click Resolve Name. You must have a DNS name resolver configured. For information, see Enabling DNS Resolution on page 251.
   - Enable Authentication: Select this check box to enable authentication of NTP communications between the external NTP server and the NIOS appliance (the grid master or grid member in a grid, an independent NIOS appliance, or the active node in an independent HA pair).
     Note: To prevent intruders from interfering with the time services on your network, you can authenticate communications between a grid member and an external NTP server, as well as between a grid member and external NTP clients. NTP communications within the grid go through an encrypted VPN tunnel, so you do not have to enable authentication between the grid master and grid members.
   - Authentication Key: Select a key that you previously entered, and then click OK. For information, see Adding NTP Authentication Keys on page 209.
6. Select one of the following:
   - Save & Close: Save the entry and close the editor.
   - Save: Save the entry and keep the editor open.

Managing External NTP Servers

You can specify multiple NTP servers for failover purposes. The NIOS appliance attempts to connect to the NTP servers in the order they are listed. A grid member uses the grid master as the NTP server when it cannot reach any of its external NTP servers.

You can change the order of the list by selecting an NTP server and dragging it to its new location or by clicking the up and down arrows. You can add and delete servers and modify their information as well.
NIOS Appliance as NTP Server

After you enable NTP on a grid, the grid members—including the grid master—can function as NTP servers to clients in different segments of the network. Similarly, after you enable NTP on an independent appliance or an HA pair, and it synchronizes its time with an NTP server, you can configure it to function as an NTP server as well.

To configure a NIOS appliance as an NTP server, perform the following tasks:

- Enable the appliance as an NTP server.
- Enable authentication between the appliance and its NTP clients.
- Optionally, specify which clients can access the NTP service of the appliance.
- Optionally, specify which clients can use ntpq to query the appliance.
Using NTP for Time Settings

Configuring a NIOS Appliance as an NTP Server

You can configure a grid member—including the grid master—or an independent appliance or HA pair to function as an NTP server. When you enable a NIOS appliance to function as an NTP server, you can enable authentication between a NIOS appliance functioning as an NTP server and its NTP clients. When you enable authentication, you must specify the keys that the appliance and its clients must use for authentication. In a grid, you can enter NTP authentication keys at the grid level so that all the members can use them to authenticate their clients. You can also enter keys at the member level, if you want that member to use different keys from those set at the grid level. After you enter the keys, you can download the key file and distribute the file to the NTP clients.

To enable an appliance as an NTP server and authenticate NTP traffic between a NIOS appliance and an NTP client, perform the following tasks:

- Enable an appliance as an NTP server and define authentication keys. For information, see Enabling an Appliance as an NTP Server on page 213.
- Optionally, define NTP access control. For information, see Defining NTP Access Control on page 214.

Enabling an Appliance as an NTP Server

To enable an appliance as an NTP server and add authentication keys:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> grid_member check box.
2. Expand the Toolbar and click NTP -> NTP Member Config.
3. In the Member NTP Properties editor, do the following:
   - Enable this Member as an NTP Server: Select this option to configure a grid master or a grid member as an NTP server.
   - Click Override in the NTP Keys section to enter NTP authentication keys at the member level. The member uses these keys when acting as an NTP server and authenticates requests from NTP clients. Clear the check box to use the grid-level authentication keys.
4. Click Add in the NTP Keys section. For information, see Adding NTP Authentication Keys on page 209.
5. Click Save & Close.

After you enter the authentication keys, you can download the key file (usually called ntp.keys) and distribute it to NTP clients as follows:

1. Grid: From the Grid tab, select the Grid Manager tab.
2. In the Opening ntp.keys dialog box, save the file, and then click OK.
3. Distribute this to the NTP clients using a secure transport.
Defining NTP Access Control

The NTP access control list specifies which clients can use a NIOS appliance as an NTP server. If you do not use the access control list, then the NIOS appliance allows access to all clients.

In addition, the NIOS appliance can accept queries from clients using ntpq, the standard utility program used to query NTP servers about their status and operational parameters. You can specify from which clients the NIOS appliance is allowed to accept ntpq queries. The appliance does not accept ntpq queries from any client, by default.

To specify which clients can access the NTP service of a NIOS appliance and from which clients a NIOS appliance can accept ntpq queries:

1. **Grid**: From the **Grid** tab, select the **Grid Manager** tab, expand the Toolbar and click **NTP -> Grid NTP Configuration**.
   **Member**: From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab -> **grid_member** check box. Expand the Toolbar and click **NTP -> NTP Member Config**.
   To override an inherited property, click **Override** next to it and complete the appropriate fields.

2. In the **Access Control** tab of the **Grid or Member NTP Properties** editor, click the **Add** icon and select an item to add:
   - **IPv4 Address**: The appliance allows a client from a single IP address to use its NTP service. The appliance accepts ntpq queries from specific NTP clients. Enter the IP address in the **Address** field.
   - **IPv4 Network**: The appliance also allows clients from a subnet to use its NTP service. It also accepts ntpq queries from a subnet. Enter the network address and netmask in the **Address** field.
   - **Any Address/Network**: The appliance allows clients from any address to use its NTP service.

3. In the **Service** column, select one of the following:
   - **Time + NTP Control**: Select this to allow the specified IP address or network to use the NTP service and to enable the appliance to accept ntpq queries.
   - **Time Only**: Select this to allow the specified IP address or network to use the NTP service.

4. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.
Monitoring NTP

When you enable the grid to synchronize its time with external NTP servers, you can monitor the status of the NTP service by checking the NTP status icons in the Member Services panel. To access the panel, from the Grid tab, select the Grid Manager tab -> Members tab -> grid_member check box, and then select the Manage Member Services icon in the table toolbar of the Members tab.

The following are descriptions of the NTP status icons in the Members Services panel. The type of information that can appear in the Description column corresponds to the SNMP trap messages. For information about the Infoblox SNMP traps, see Chapter 11, Monitoring with SNMP, on page 321.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green" /></td>
<td>Green</td>
<td>The NTP service is enabled and running properly.</td>
</tr>
<tr>
<td><img src="image" alt="Yellow" /></td>
<td>Yellow</td>
<td>The NTP service is enabled, and the appliance is synchronizing its time.</td>
</tr>
<tr>
<td><img src="image" alt="Red" /></td>
<td>Red</td>
<td>The NTP service is enabled, but it is not running properly or is out of synchronization.</td>
</tr>
<tr>
<td><img src="image" alt="Gray" /></td>
<td>Gray</td>
<td>The NTP service is disabled.</td>
</tr>
</tbody>
</table>
Scheduling Tasks

You can schedule tasks, such as adding DNS zones, modifying fixed addresses, and restarting services, for a future date and time. The scheduling feature is useful when you want to add, modify, or delete a record, or schedule a network discovery at a desired date and time. Using this feature, you can streamline your day-to-day operations. For example, you can schedule the deletion of records that you use for testing when the test time is up. You can also reassign an IP address to a fixed address when the location of the server to which the fixed address is assigned changes from one network to another.

You can schedule the addition, modification, and deletion for the following objects:

- DNS zones (authoritative, forward, stub, and delegated)
- DNS views
- DNS resource records (except SOA records)
- Hosts
- Bulk hosts
- Shared records
- Shared record groups
- Networks
- Network containers
- Shared networks
- DHCP ranges
- Fixed addresses
- Reservations
- Roaming hosts

You can also schedule the following operations:

- Network discoveries
- Service restarts

Only superusers can view, reschedule, and delete all scheduled tasks. Limited-access admins can reschedule and delete only their scheduled tasks. The appliance sends email notifications to local admins, except for those who do not have email addresses, when email notification is enabled for the admins and any of the following happens:

- A superuser schedules a task, and another superuser reschedules or deletes the task.
- A limited-access admin schedules a task, and a superuser reschedules or deletes the task.
- A superuser or a limited-access admin schedules a task, and the task fails.

Superusers can also grant scheduling permissions to other admin groups. When the scheduling permission is added or inherited from an admin role, limited-access admin groups can schedule tasks. For information, see Administrative Permissions for Network Discovery on page 112.
Scheduling Additions and Modifications

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

To schedule an addition or a modification:
1. Add or modify a record following the instructions described in this guide.
2. Click the Schedule icon at the top of the corresponding wizard or editor.
3. In the Schedule Change panel, complete the following:
   - **Now**: Select this to have the appliance perform the task when you save the entry. This is selected by default when there is no scheduled task associated with the object.
   - **Later**: Select this to schedule the task for a later date and time. Complete the following:
     - **Date**: Enter a date in YYYY-MM-DD (year-month-day) format. The appliance displays today's date. You can also click the calendar icon to select a date from the calendar widget.
     - **Time**: Enter a time in hh:mm:ss AM/PM (hours:minutes:seconds AM or PM) format. You can also select a time from the drop-down list by clicking the time icon.
     - **Time Zone**: Select a time zone for the scheduled date and time from the drop-down list. This field displays the time zone of the browser that the admin uses to log in to Grid Manager.
4. Select one of the following:
   - **Save & Close**: Save the entry and close the wizard or editor.
   - **Save & New**: Save the entry and open a new wizard.

Scheduling Appliance Operations

The appliance supports the scheduling of the following operations:
- Network discoveries—For information, see Chapter 33, Network Discovery, on page 805.
- Service restarts—For information, see Restarting Services on page 261.

Scheduling Deletions

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

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

The appliance performs the deletion at the scheduled date and time.
Viewing Scheduled Tasks

After you schedule a task, you can view the pending task in the Scheduled Tasks viewer. Grid Manager also displays a Schedule icon next to the associated object, except for the addition of an object. You can click the icon to view the configuration and schedule. You can also reschedule the task if you are the owner of the task or if you are a superuser. In the corresponding editor, the Schedule icon is green when there is a pending scheduled task. For information, see Icons for Scheduled Tasks on page 219.

The appliance logs the scheduled tasks in the audit log and displays the pending tasks in the Scheduled Tasks viewer. By default, Grid Manager sorts the pending tasks with the earliest scheduled start times. The Scheduled Tasks viewer displays the pending scheduled tasks that the admin is allowed to view. Superusers can view all scheduled tasks, and limited-access admins can view their own scheduled tasks. For information, see Scheduled Tasks Viewer on page 218.

When you schedule a network discovery or a service restart, you can view the pending tasks related to the operation if you have the applicable permissions. You can also reschedule or delete existing tasks. For information, see Pending Tasks for Operations on page 220.

Scheduled Tasks Viewer

To view pending scheduled tasks:

1. From the Administration tab, select the Scheduling tab.
2. Grid Manager displays the following information for each task:
   - Scheduled Time: The date, time, and time zone when the appliance executes the task.
   - Submitted Time: The date, time, and time zone when the task was submitted.
   - Submitter: The admin who scheduled the task.
   - Affected Object: The name of the object that is associated with the task. For example, if the task involves an A record, this field displays the domain name of the record. If it is a fixed address, it displays the IP address of the fixed address.
   - Object Type: The object type. For example, the appliance can display A Record or Fixed Address.
   - Action: The operation the appliance performs in this task. The value can be one of the following:
     - Add: Addition
     - Modify: Modification
     - Delete: Deletion
     - Network Discovery
     - Restart Services: A service restart for either the grid or a member.
   - Task Details: The message that appears in the audit log.

By default, the appliance sorts the tasks by Scheduled Time starting with the earliest scheduled start time. You can also select Task ID for display. The appliance assigns a task ID to a scheduled task in chronological order.

You can do the following in this viewer:
- Sort the tasks in ascending or descending order by column, except for Task Details.
- Use the filter or Search function to locate a specific scheduled task.
- Export and print the information in the table.
- Control the display of information in the panel by toggling between a single-line view and a multi-line view.
- Reschedule the task, cancel the scheduling of task, or execute the task immediately.
Icons for Scheduled Tasks

Grid Manager displays a scheduled task icon next to an object that is associated with a scheduled task (except for the addition of an object), as shown in Figure 7.5. When you mouse over the icon, an informational dialog box appears displaying the type of action, the date and time of the scheduled task, and the person who scheduled the task.

You can click the icon and Grid Manager displays the corresponding editor (for modification) or the Scheduled Deletion dialog box (for deletion) in the read-only mode. If you are viewing a task that you scheduled, you can modify and save the schedule, but you cannot modify the configuration of the object. If you are not the owner of a scheduled modification or a superuser, you can only view the information. You cannot reschedule the task. If you are not the owner of a scheduled deletion or a superuser, Grid Manager does not display the Scheduled Deletion dialog box when you click the icon.

Figure 7.5 Icon for a Scheduled Task

In the editor, Grid Manager displays the Schedule icon in green to indicate a pending scheduled task associated with the corresponding object, as shown in Figure 7.6. You can click the Schedule icon to view the date and time of the scheduled task. You can also reschedule the task if you have the applicable permissions. For information, see Rescheduling Tasks on page 220.

Figure 7.6 Scheduling Icon Indicating a Pending Task
Pending Tasks for Operations

You can view all pending tasks for a network discovery or service restart in the Scheduled Tasks viewer if you have the applicable permissions. For information, see Scheduled Tasks Viewer on page 218. You can also view the pending tasks in their corresponding editors.

To view the pending tasks in an editor:

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

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

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

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

3. Grid Manager displays the following information in the Scheduled Tasks viewer:
   - **Scheduled Time:** The date, time, and time zone when the appliance executes the task.
   - **Submitted Time:** The date, time, and time zone when the task was submitted.
   - **Submitter:** The admin who scheduled the task.
   - **Task Details:** The message that appears in the audit log.

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

- Sort the tasks in ascending or descending order by column, except for Task Details.
- Reschedule a selected task. For information, see Rescheduling Tasks Associated with Operations on page 221.
- Delete a selected task by selecting the task check box and clicking the Delete icon.
- Export and print the information in the table.

Rescheduling Tasks

Superusers can reschedule any scheduled task. Limited-access admins can reschedule only the tasks that they scheduled, depending on their permissions. When you reschedule a task, Grid Manager displays the object or operation configuration in the read-only mode. You can modify the date and time to reschedule the task. However, you cannot modify the configuration of the object or operation.

Rescheduling Tasks Associated with Objects

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

To reschedule a task from the Scheduled Tasks viewer:

1. From the Administration tab, select the Scheduling tab -> scheduled_task check box, and then click the Reschedule icon.

2. In the Reschedule dialog box, modify the date and time when you want the appliance to execute the task. You can select Now to execute the task when you save the entry.

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

**Rescheduling Tasks Associated with Operations**

To reschedule a network discovery or a service restart:
1. From the Administration tab, select the Scheduling tab -> scheduled_task check box, and then click the Reschedule icon.
   Or
   Navigate to the operation and click the Schedule icon at the top of the wizard. In the Schedule Change panel, select Click here to view/manage the scheduled items. Grid Manager displays all scheduled tasks related to the operation in the Scheduled Tasks viewer. Select the task check box, and then click the Reschedule icon.
2. Grid Manager displays detailed information about the task in the Reschedule dialog box.
3. Modify the date and time when you want the appliance to execute the task. You can also select Now to execute the task when you save the entry.
4. Click Save & Close or Save.

**Canceling Scheduled Tasks**

To cancel a scheduled task:
1. From the Administration tab, select the Scheduling tab -> scheduled_task check box, and then click the Delete icon.
2. In the Confirm Delete Request dialog box, click Yes.
   The appliance deletes the scheduled task and does not perform the scheduled operation. Therefore, no change is made to any record after you delete a scheduled task.

**Guidelines for Upgrading, Backing Up, and Restoring the Database**

You should take into consideration the impact on scheduled tasks when you perform any of the following:
- Upgrade the NIOS software: In a full upgrade, all scheduled tasks are deleted. In a lite upgrade, scheduled tasks are not deleted.
- Back up the NIOS database: All scheduled tasks are backed up for troubleshooting purpose.
- Restore the database: The scheduled tasks are not restored.
- Promote a grid member to a grid master: After the promotion, all scheduled tasks that are past due are executed immediately.
- Revert the NIOS software image: After the revert, all scheduled tasks that are past due are executed immediately.
ABOUT EXTENSIBLE ATTRIBUTES

You can use extensible attributes to capture additional information about the objects managed by NIOS appliances. The Grid Manager wizards and editors that are used to add and edit objects, such as admin groups, DNS views, and DHCP networks, contain an Extensible Attributes tab that you can customize. You can specify the attributes that users can manage in this tab for each object, so you can collect and track data specific to your organization. You can even specify required attributes, and restrict the values that users can enter for each attribute.

Note: Only superusers can configure extensible attributes.

For example, Figure 7.7 illustrates a network with different device types. Each device is represented as a host in the NIOS appliance database. You can configure Device Type, Location and Owner as required attributes for hosts. Then when admins add hosts, they will be required to enter values for these attributes in the Extensible Attributes tab of the Add Host wizard.

Figure 7.7 Using Extensible Attributes to Define Network Devices

You can specify different extensible attributes for each type of object. For example, you can configure the attribute Site for fixed addresses and hosts, and the attribute Department for admin groups. When you configure an attribute, you can specify the following:

- The type of data that admins enter, such as text strings, integers, or email addresses. You can also restrict admins to a list of values.
- Whether admins can enter multiple values
- A default value
- Whether the attribute is required
About Extensible Attributes

- The objects associated with the attribute, such as admin groups, DNS views, or DHCP networks.
- Whether the appliance makes an entry in the audit log each time an object with the attribute is added or modified.

After you configure the attributes of an object, the attributes become available in the Extensible Attributes tab of the wizard and editor of the object. Users then add or edit the attribute values, according to your configuration. Users can also specify attributes when searching for data and add attributes as columns in the tables of Grid Manager. For example, you can add the Site attribute as a column in the Records panel of the Zones tab. For information about adding columns to tables, see Customizing Tables on page 44.

Users can also group objects in smart folders according to their attributes. For example, a user can create a smart folder that contains all networks in a certain site.

NIOS appliances provide the following predefined attributes that you can customize:

- Region
- Country
- State
- Site
- Building
- VLAN

When you use a predefined attribute, you can edit it and change its name, but you cannot change the type of data it accepts. You can also delete predefined attributes that you do not use. All predefined attributes accept text strings. You can define other settings though, as described in Modifying Extensible Attributes on page 225.

You can also create your own attributes, as described in Adding Extensible Attributes on page 223.

Configuring Extensible Attributes

To configure extensible attributes, follow these procedures:

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

Adding Extensible Attributes

To add a new extensible attribute:

1. In the Administration tab, select the Extensible Attributes tab.
2. Click the Add icon on any of the toolbars.
3. In the Add Extensible Attribute wizard, complete the following:
   - **Name**: Enter the name of the attribute. This is a required field and is case-sensitive. You can enter up to 128 UTF-8 characters.
   - **Type**: Specify the type of data that you want to capture for an object. Select one of the following:
     - **String**: Select this when the attribute is used to define string values, such as names. When you select this type, the wizard displays the Number of Characters field where you can enter the minimum and maximum number of characters that users can enter.
     - **List**: Select this when you want to define a list of values for the attribute. Users can then select a value from this list. For example, if you want to restrict an attribute to five specific values, you can define the attribute as a List and then list the five values in the List Values section. When a user uses the attribute, they are limited to selecting from one of the five values.

When you select **List**, the wizard displays the List of values table, where you add the allowed values. These values appear in the drop-down list when a user defines the attribute. Click the Add icon to enter values in the table. You can enter up to 64 UTF-8 characters for each value.
You can also modify list values at a later time. When you modify list values, all object attributes using the modified values are updated to the new values.

You can also delete values from the list. Note that when you delete a list value, all attributes using the deleted values are removed from the objects. For objects with multiple attribute values, only the deleted values are removed.

You can also move a value up or down in the list.

- **Integer**: Select this when the attribute is used to track whole numbers, such as serial numbers. When you select this type, the wizard displays the **Value Limits** fields where you can enter the range of allowed values. Note that you cannot change your entries in the **Value Limits** fields if you modify the attribute at a later date.

- **Email**: Select this when the attribute is used for email addresses. Email addresses are entered in the format `user@domain.com`.

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

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

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

4. Click **Next**.

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

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

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

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

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

- **Log Attribute Values When Objects are Updated**: Select this check box if you want the appliance to make an entry in the audit log each time an object with this attribute is added or modified. When you select attribute values for audit, they are included in all the audit log entries. For information about the audit log, see **Using the Audit Log** on page 310

5. Click **Save & Close**.

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

### Viewing Extensible Attributes

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

- **Name**: The name of the extensible attribute.
- **Type**: The type of data defined by the attribute.
- **Comment**: Comments entered for the extensible attribute.
- **Required**: Indicates whether users are required to complete this field.
- **Restricted to Objects**: The object types that are associated with the attribute.
Modifying Extensible Attributes

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

To modify an extensible attribute:
1. In the Administration tab, select the Extensible Attributes tab.
2. Select the attribute and click the Edit icon.
3. In the General tab of the Extensible Attributes editor, you can only change the name of the attribute. You cannot change the data type. The data type for predefined attributes is string.
4. In the Additional Properties tab, you can modify any of the fields described in the step 4 of Adding Extensible Attributes on page 223.
5. Click Save & Close.

Deleting Extensible Attributes

When you delete an extensible attribute, the appliance removes the attribute. All the attribute values set on the selected object types are removed from those objects. Once deleted, the attribute no longer exists in the system.

Deleted attributes are not moved to the Recycle Bin. This operation might take a long time depending on the amount of data that needs to be deleted.

To delete extensible attributes:
1. In the Administration tab, select the Extensible Attributes tab.
2. Select the attribute and click the Delete icon.
3. When the confirmation dialog box appears, click Yes.

Using Extensible Attributes

After a superuser admin configures the attributes of an object, they become available in the wizard and editor of the object. This section describes how users can then add and manage the attributes that were configured.

Grid Manager displays the required extensible attributes in the Extensible Attribute tab. You must enter values for all required attributes. If an object does not have required attributes, you can add the available optional attributes.

In the Extensible Attribute tab of an object, such as a network or host record, you can do the following:
- Enter values for extensible attributes
- Add attributes
- Delete optional attributes

To enter values for the extensible attributes of an object:
1. Open the editor of the object. For example, to enter values for the attributes of a network, select it and click its Extensible Attributes tab.
2. Click the Value column of the attribute. You must enter values for all required attributes.
3. Depending on the required attribute type, either enter or select a value for the attribute from the Value column.

To add attributes:
1. Click the Add icon. Grid Manager adds a row to the table with the default attribute displayed.
2. Click the default attribute and expand the list of available attributes.
3. Select an attribute from the drop-down list.
4. Enter or select a value for the attribute from the Value column.

To delete an attribute:
1. Click the check box beside the attribute you want to delete.
2. Click the Delete icon.
Managing Appliance Operations

To delete all attributes:
1. Click the **Attribute Name** check box.
2. Click the Delete icon.

**Note:** You can delete only attributes that are not required. If you have one or more required attributes, you cannot use the delete all function.

To save your changes, click **Save & Close**.

**Editing Multiple Extensible Attribute Values**

You can also manage the extensible attributes of multiple objects at the same time. For example, you can select several zones, and view and modify their extensible attributes all at once.

Note that Grid Manager may not apply the changes you made to all the selected objects. It applies the change to objects that meet the following criteria:

- You have read/write permission to the object.
- The selected object is not locked by another user or does not have a scheduled pending task.
- If the attribute was restricted to certain object types, the object must be one of those types.

To edit multiple extensible attribute values:
1. Select the objects whose extensible attributes you want to modify. You can select specific objects or select all objects in a dataset, as described in *Selecting Objects in Tables* on page 44.
2. Expand the Toolbar and click **Extensible Attributes**.
   Grid Manager displays the *Multi-Select Edit Extensible Attributes* dialog box which lists the extensible attributes of the selected objects. It displays the following information for each attribute:
   - **Attribute Name:** This field displays the name of the extensible attribute associated with the selected object.
   - **Value:** If the selected objects have the same value for the attribute, Grid Manager displays that value in this field. If the selected objects have different values for the attribute or if some have values and others do not, this field displays *Multiple Values*.
     An attribute can have multiple rows if it allows multiple values. Grid Manager displays the values that all objects have in common, if any. Otherwise, it displays *Multiple Values*.
   - **Required:** This field displays *Yes* if the attribute is required in at least one object associated with the attribute. It displays *No* if the attribute is not required in any of the objects.
3. You can do the following:
   - Change the value of an attribute. Depending on the attribute type, select the value and either enter a new value or select one from the drop-down list.
   - Add an attribute to the selected objects. Click the Add icon. In the **Attribute Name** field of the new row, select an attribute from the list of available attributes and specify its value. If the attribute that you added was configured as a required attribute, the **Required** field displays *Yes*. Otherwise, it displays *No*.
   - Delete an attribute. You can delete an attribute if it is not required. Select the attribute and click the Delete icon.
4. Click **OK** when you are finished modifying the extensible attributes.

Grid Manager applies your changes to the applicable objects. This operation might take a long time, depending on the amount of data being modified. You can choose to run this operation in the background, as described in *About Long Running Tasks* on page 52.
MANAGING SECURITY OPERATIONS

The grid provides certain security-related features. The following sections describe the different security-related features that you can set. For information about how to configure these features, see Configuring Security Features on page 228.

Enabling Support Access

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

Enabling Remote Console Access

This function makes it possible for a superuser admin to access the Infoblox CLI from a remote location using an SSH (Secure Shell) v2 client. The management system must have an SSH v2 client to use this function. After opening a remote console connection using an SSH client, log in using a superuser name and password. By default, this option is disabled. Note that only superusers can log in to the appliance through a console connection.

Permanently Disabling Remote Console and Support Access

You can permanently disable remote console (Secure Shell v2) access for appliance administration and for Infoblox Technical Support to perform remote troubleshooting. Disabling this type of access might be required in a high-security environment.

WARNING: After permanently disabling remote console and support access, you cannot re-enable them! Not even resetting an appliance to its factory default settings can re-enable them.

Restricting GUI/API Access

You can specify the IP addresses from which administrators are allowed to access the NIOS appliance. When the NIOS appliance receives a connection request, it tries to match the source IP address in the request with IP addresses in the list. If there is at least one item in the HTTP Access Control list and the source IP address in the request does not match it, the NIOS appliance ignores the request.

Caution: If you specify an address or network other than the one from which you are currently accessing the appliance, when you save your configuration, you will lose your administrative session and be unable to reconnect.

Enabling HTTP and GUI Redirections

You can enable the NIOS appliance to redirect administrative connection requests using HTTP to the secure HTTPS protocol. When you disable redirection, the NIOS appliance ignores any administrative connection requests not using HTTPS. By default, the NIOS appliance does not redirect HTTP connection requests to HTTPS. When you change this setting, the application restarts and your management session terminates.

You can also enable and disable the redirection of the Infoblox GUI from a grid member to the grid master. You can configure this for the grid and override the grid setting at the member level. When you enable this feature together with the HTTP to HTTPS redirection, the GUI redirection takes precedence. For information about how to configure the redirection of the Infoblox GUI, see Enabling and Disabling GUI Redirection on page 229.
Modifying the Session Timeout Setting

You can set the length of idle time before an administrative session to the Infoblox GUI times out. The default timeout value is 600 seconds (10 minutes).

If a user does not interact with the application for the specified time, the appliance displays a message that a timeout has occurred. Click OK to restart the GUI session.

**Note:** If you change the session timeout value, the new setting takes effect only after you log out and log back in.

Disabling the LCD Input Buttons

By default, the LCD input function is enabled, which allows you to use the LCD buttons on the front panel of a NIOS appliance to change the IP address settings of the LAN port. You can disable this function if the appliance is in a location where you cannot restrict access exclusively to NIOS appliance administrators and you do not want anyone to be able to make changes through the LCD.

Configuring Security Features

You can manage only certain features at the member level. To configure security features for the grid or an individual member:

1. **Grid:** From the Grid tab, select the Grid Manager tab, expand the Toolbar and click Grid Properties -> Edit.
   
   **Member:** From the Grid tab, select the Grid Manager tab -> Members tab -> grid_member check box, and then click the Edit icon.

   To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the Security tab, complete the following:
   
   — **Session Timeout(s):** This field is in the Grid Properties editor only. Enter a number between 60 and 31536000 seconds (one minute – one year) in the Session Timeout field. The default session timeout is 600 seconds (10 minutes).
   
   — **Minimum Password Length:** This field is in the Grid Properties editor only. Specify the minimum number of characters allowed for an admin password.
   
   — **Redirect HTTP to HTTPS:** This field is in the Grid Properties editor only. Select this option to have the appliance redirect HTTP connection requests to HTTPS.
   
   — **Restrict GUI/API Access:** This field is in the Grid Properties editor only. To restrict access to the GUI and API, select this option and click the Add icon. To allow administrative access to the GUI and API from a single IP address, enter the IP address in the **Address** field. Note that if you specify an address other than the one from which you are currently accessing the appliance, when you save your configuration, you will lose your administrative session and be unable to reconnect.
   
   To restrict administrative access to the GUI and API to a subnet, enter the network address in the **Address** field. Note that if you specify a subnet other than the one from which you are currently accessing the appliance, when you save your configuration, you will lose your administrative session and be unable to reconnect.

   — **Enable Remote Console Access:** Select this option to enable superuser admins to access the Infoblox CLI from a remote location using SSH (Secure Shell) v2 clients. You can set this at the grid and member levels.

   — **Enable Support Access:** Select this check box to enable an SSH (Secure Shell) daemon that only Infoblox Technical Support can access. You can set this at the grid and member levels.

   — **Restrict Remote Console and Support Access to the MGMT Port:** This field is in the Grid Member Properties editor only. Select this check box to restrict SSH (Secure Shell) v2 access to the MGMT port only. This restricts Infoblox Technical Support and remote console connections—both of which use SSH v2—to just the MGMT port. For an HA pair, you can make an SSH v2 connection to the MGMT port on both the active and passive nodes.

   Clear the check box to allow SSH v2 access to both the MGMT and LAN ports.
— **Permanently Disable Remote Console and Support Access:** This field is in the *Grid Properties* editor only. Select this option to permanently disable remote console (Secure Shell v2) access for appliance administration and for Infoblox Technical Support.

— **Enable LCD Input:** Select this check box to allow use of the LCD buttons on the front panel of a NIOS appliance to change the IP address settings of the LAN port. Clear this check box to disable this function. You can set this at the grid and member levels.

3. Select one of the following:
   — **Save & Close:** Save the entry and close the editor.
   — **Save:** Save the entry and keep the editor open.

### Enabling and Disabling GUI Redirection

1. **Grid:** From the *Grid* tab, select the *Grid Manager* tab, expand the Toolbar and click *Grid Properties* → *Edit*.

2. **Member:** From the *Grid* tab, select the *Grid Manager* tab → *Members* tab → *grid_member* check box, and then click the Edit icon.

2. In the *Grid Properties* or *Grid Member Properties* editor, select the *General* tab → *Advanced* tab, and then complete the following:
   — **Enable GUI Redirect from Member:** Select this check box to enable the redirection of the Infoblox GUI from a member to the grid master. To override the grid setting for a member, click *Override*. Clear this check box to disable the feature.

3. Select one of the following:
   — **Save & Close:** Save the entry and close the editor.
   — **Save:** Save the entry and keep the editor open.
**Ethernet Port Usage**

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

- **LAN1 port** – This is the default port for single independent appliances, single grid members, and passive nodes in HA pairs. All deployments use the LAN port for management services if the MGMT port is disabled.
- **LAN2 port** – The LAN2 port is not enabled by default. By default, an appliance uses the LAN1 port (and HA port when deployed in an HA pair). To enable and configure the LAN2 port, you must have read/write permission to the grid member on which you want to enable the port. The LAN2 port is available on Infoblox-250, 250-A, 550-A, -1050-A, -1550-A, -1552-A, -1852-A, -2000, and -2000-A appliances.
- **HA port** – This is the default port for the active grid master node and the active node in an independent HA pair.
- **MGMT port** – If the MGMT port is enabled, the NIOS appliance uses it for many types of management services (see Table 7.3 on page 232 for specific types).

*Table 7.1* displays the type of traffic per port for both grid and independent deployments. For a more detailed list of the different types of traffic, see *Table 7.3* on page 232.

*Table 7.1 Appliance Roles and Configuration, Communication Types, and Port Usage*

<table>
<thead>
<tr>
<th>Appliance Role</th>
<th>HA Pair</th>
<th>HA Status</th>
<th>MGMT Port</th>
<th>Database Synchronization</th>
<th>Core Network Services</th>
<th>Management Services</th>
<th>GUI Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>HA Grid Master</td>
<td>Yes</td>
<td>Active</td>
<td>Disabled</td>
<td>VIP on HA</td>
<td>VIP on HA</td>
<td>LAN1</td>
<td>VIP on HA</td>
</tr>
<tr>
<td>HA Grid Master</td>
<td>Yes</td>
<td>Passive</td>
<td>Disabled</td>
<td>LAN1</td>
<td>–</td>
<td>LAN1</td>
<td>–</td>
</tr>
<tr>
<td>Single Grid Master</td>
<td>No</td>
<td>–</td>
<td>Disabled</td>
<td>LAN1</td>
<td>LAN1</td>
<td>LAN1</td>
<td>LAN1</td>
</tr>
<tr>
<td>HA Grid Member</td>
<td>Yes</td>
<td>Active</td>
<td>Disabled</td>
<td>LAN1</td>
<td>VIP on HA</td>
<td>LAN1</td>
<td>–</td>
</tr>
<tr>
<td>HA Grid Member</td>
<td>Yes</td>
<td>Passive</td>
<td>Disabled</td>
<td>LAN1</td>
<td>–</td>
<td>LAN1</td>
<td>–</td>
</tr>
<tr>
<td>Single Grid Member</td>
<td>No</td>
<td>–</td>
<td>Disabled</td>
<td>LAN1</td>
<td>–</td>
<td>LAN1</td>
<td>–</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>Yes</td>
<td>Active</td>
<td>Disabled</td>
<td>VIP on HA</td>
<td>VIP on HA</td>
<td>LAN1</td>
<td>VIP on HA</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>Yes</td>
<td>Passive</td>
<td>Disabled</td>
<td>LAN1</td>
<td>–</td>
<td>LAN1</td>
<td>–</td>
</tr>
<tr>
<td>Single Independent</td>
<td>No</td>
<td>–</td>
<td>Disabled</td>
<td>–</td>
<td>–</td>
<td>LAN1</td>
<td>–</td>
</tr>
<tr>
<td>HA Grid Master</td>
<td>Yes</td>
<td>Active</td>
<td>Enabled</td>
<td>VIP on HA</td>
<td>VIP on HA</td>
<td>MGMT</td>
<td>MGMT</td>
</tr>
<tr>
<td>HA Grid Master</td>
<td>Yes</td>
<td>Passive</td>
<td>Enabled</td>
<td>LAN1</td>
<td>–</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>Single Grid Master</td>
<td>No</td>
<td>–</td>
<td>Enabled</td>
<td>LAN1</td>
<td>LAN1 or MGMT</td>
<td>MGMT</td>
<td>MGMT</td>
</tr>
<tr>
<td>HA Grid Member</td>
<td>Yes</td>
<td>Active</td>
<td>Enabled</td>
<td>LAN1 or MGMT</td>
<td>VIP on HA</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>HA Grid Member</td>
<td>Yes</td>
<td>Passive</td>
<td>Enabled</td>
<td>LAN1 or MGMT</td>
<td>–</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>Single Grid Member</td>
<td>No</td>
<td>–</td>
<td>Enabled</td>
<td>LAN1 or MGMT</td>
<td>–</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>Yes</td>
<td>Active</td>
<td>Enabled</td>
<td>VIP on HA</td>
<td>VIP on HA</td>
<td>MGMT</td>
<td>MGMT</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>Yes</td>
<td>Passive</td>
<td>Enabled</td>
<td>LAN1</td>
<td>–</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>Single Independent</td>
<td>No</td>
<td>–</td>
<td>Enabled</td>
<td>–</td>
<td>–</td>
<td>LAN1 or MGMT</td>
<td>MGMT</td>
</tr>
</tbody>
</table>
Table 7.2 Appliance Roles and Configuration, Communication Types, and Port Usage for Appliances with LAN2 Ports

<table>
<thead>
<tr>
<th>Appliance Role</th>
<th>HA Status</th>
<th>MGMT Port</th>
<th>LAN2 Port</th>
<th>Database Synchronization</th>
<th>Core Network Services</th>
<th>Management Services</th>
<th>GUI Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>HA Grid Master</td>
<td>Active</td>
<td>Disabled</td>
<td>Enabled</td>
<td>VIP on HA</td>
<td>VIP on HA</td>
<td>LAN1 or LAN2</td>
<td>VIP on HA</td>
</tr>
<tr>
<td>HA Grid Master</td>
<td>Passive</td>
<td>Disabled</td>
<td>Enabled</td>
<td>LAN1</td>
<td>–</td>
<td>LAN1 or LAN2</td>
<td>–</td>
</tr>
<tr>
<td>Single Grid Master</td>
<td>–</td>
<td>Disabled</td>
<td>Enabled</td>
<td>LAN1</td>
<td>LAN1 and/or LAN2</td>
<td>LAN1 or LAN2</td>
<td>LAN1</td>
</tr>
<tr>
<td>HA Grid Member</td>
<td>Active</td>
<td>Disabled</td>
<td>Enabled</td>
<td>LAN1</td>
<td>–</td>
<td>LAN1 or LAN2</td>
<td>–</td>
</tr>
<tr>
<td>HA Grid Member</td>
<td>Passive</td>
<td>Disabled</td>
<td>Enabled</td>
<td>LAN1</td>
<td>–</td>
<td>LAN1 or LAN2</td>
<td>–</td>
</tr>
<tr>
<td>Single Grid Member</td>
<td>–</td>
<td>Disabled</td>
<td>Enabled</td>
<td>LAN1</td>
<td>LAN1 and/or LAN2</td>
<td>LAN1 or LAN2</td>
<td>–</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>Active</td>
<td>Disabled</td>
<td>Enabled</td>
<td>VIP on HA</td>
<td>VIP on HA</td>
<td>LAN1 or LAN2</td>
<td>VIP on HA</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>Passive</td>
<td>Disabled</td>
<td>Enabled</td>
<td>LAN1</td>
<td>–</td>
<td>LAN1 or LAN2</td>
<td>–</td>
</tr>
<tr>
<td>Single Independent</td>
<td>–</td>
<td>Disabled</td>
<td>Enabled</td>
<td>–</td>
<td>LAN1 and/or LAN2</td>
<td>LAN1 or LAN2</td>
<td>LAN1</td>
</tr>
<tr>
<td>HA Grid Master</td>
<td>Active</td>
<td>Enabled</td>
<td>Enabled</td>
<td>VIP on HA</td>
<td>VIP on HA</td>
<td>MGMT</td>
<td>MGMT</td>
</tr>
<tr>
<td>HA Grid Master</td>
<td>Passive</td>
<td>Enabled</td>
<td>Enabled</td>
<td>LAN1</td>
<td>–</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>Single Grid Master</td>
<td>–</td>
<td>Enabled</td>
<td>Enabled</td>
<td>LAN1</td>
<td>LAN1, LAN2 and/or MGMT</td>
<td>MGMT</td>
<td>MGMT</td>
</tr>
<tr>
<td>HA Grid Member</td>
<td>Active</td>
<td>Enabled</td>
<td>Enabled</td>
<td>LAN1 or MGMT</td>
<td>VIP on HA</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>HA Grid Member</td>
<td>Passive</td>
<td>Enabled</td>
<td>Enabled</td>
<td>LAN1 or MGMT</td>
<td>–</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>Single Grid Member</td>
<td>–</td>
<td>Enabled</td>
<td>Enabled</td>
<td>LAN1 or MGMT</td>
<td>LAN1, LAN2 and/or MGMT</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>Active</td>
<td>Enabled</td>
<td>Enabled</td>
<td>VIP on HA</td>
<td>VIP on HA</td>
<td>MGMT</td>
<td>MGMT</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>Passive</td>
<td>Enabled</td>
<td>Enabled</td>
<td>LAN1</td>
<td>–</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>Single Independent</td>
<td>–</td>
<td>Enabled</td>
<td>Enabled</td>
<td>–</td>
<td>LAN1, LAN2 and/or MGMT</td>
<td>MGMT</td>
<td>MGMT</td>
</tr>
</tbody>
</table>

To see the service port numbers and the source and destination locations for traffic that can go to and from a NIOS appliance, see Table 7.3. This information is particularly useful for firewall administrators so that they can set policies to allow traffic to pass through the firewall as required.

**Note:** The colors in both tables represent a particular type of traffic and correlate with each other.
<table>
<thead>
<tr>
<th>Service</th>
<th>SRC IP</th>
<th>DST IP</th>
<th>Proto</th>
<th>SRC Port</th>
<th>DST Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Exchange</td>
<td>LAN1 or MGMT on grid member</td>
<td>VIP on HA grid master, or LAN1 on single master</td>
<td>17 UDP</td>
<td>2114</td>
<td>2114</td>
<td>Initial key exchange for establishing VPN tunnels Required for Grid</td>
</tr>
<tr>
<td>VPN</td>
<td>LAN1 or MGMT on grid member</td>
<td>VIP on HA grid master, or LAN1 on single master</td>
<td>17 UDP</td>
<td>1194 or 5002, or 1024 -&gt; 63999</td>
<td>1194 or 5002, or 1024 -&gt; 63999</td>
<td>Default VPN port 1194 for grids with new DNSone 3.2 installations and 5002 for grids upgraded to DNSone 3.2; the port number is configurable Required for Grid</td>
</tr>
<tr>
<td>DHCP</td>
<td>Client</td>
<td>LAN1, LAN2, VIP, or broadcast on NIOS appliance</td>
<td>17 UDP</td>
<td>68</td>
<td>67</td>
<td>Required for DHCP service</td>
</tr>
<tr>
<td>DHCP</td>
<td>LAN1, LAN2 or VIP on NIOS appliance</td>
<td>Client</td>
<td>17 UDP</td>
<td>67</td>
<td>68</td>
<td>Required for DHCP service</td>
</tr>
<tr>
<td>DHCP Failover</td>
<td>LAN1, LAN2 or VIP on Infoblox DHCP failover peer</td>
<td>LAN1, LAN2 or VIP on Infoblox DHCP failover peer</td>
<td>6 TCP</td>
<td>519</td>
<td>519</td>
<td>Required for DHCP failover</td>
</tr>
<tr>
<td>DHCP Failover</td>
<td>VIP on HA grid master or LAN1 or LAN2 on single master</td>
<td>LAN1, LAN2 or VIP on grid member in a DHCP failover pair</td>
<td>6 TCP</td>
<td>1024 -&gt; 65535</td>
<td>7911</td>
<td>Informs functioning grid member in a DHCP failover pair that its partner is down Required for DHCP failover</td>
</tr>
<tr>
<td>DDNS Updates</td>
<td>LAN1, LAN2, or VIP</td>
<td>LAN1, LAN2, or VIP</td>
<td>17 UDP</td>
<td>1024 -&gt; 65535</td>
<td>53</td>
<td>Required for DHCP to send DNS dynamic updates</td>
</tr>
<tr>
<td>DNS Transfers</td>
<td>LAN1, LAN2, VIP, or MGMT, or client</td>
<td>LAN1, LAN2, VIP, or MGMT, or client</td>
<td>6 TCP</td>
<td>53, or 1024 -&gt; 65535</td>
<td>53</td>
<td>For DNS zone transfers, large client queries, and for grid members to communicate with external name servers Required for DNS</td>
</tr>
<tr>
<td>DNS Queries</td>
<td>Client</td>
<td>LAN1, LAN2, VIP, or broadcast on NIOS appliance</td>
<td>17 UDP</td>
<td>53, or 1024 -&gt; 65535</td>
<td>53</td>
<td>For DNS queries Required for DNS</td>
</tr>
<tr>
<td>NTP</td>
<td>NTP client</td>
<td>VIP, LAN1 or LAN2</td>
<td>17 UDP</td>
<td>1024 -&gt; 65535</td>
<td>123</td>
<td>Required if the NIOS appliance is an NTP server</td>
</tr>
</tbody>
</table>
### Ethernet Port Usage

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

By default, the NIOS appliance automatically negotiates the optimal connection speed and transmission type (full or half duplex) on the physical links between the 10/100Base-T and 10/100/1000Base-T ports on the NIOS appliance and the Ethernet ports on a connecting switch. It is usually unnecessary to change the default auto-negotiation setting; however, you can manually configure connection settings for a port if necessary.

Occasionally, for example, even though both the NIOS appliance and the connecting switch support 1000-Mbps (megabits per second) full-duplex connections, they might fail to auto-negotiate that speed and type, and instead connect at lower speeds of either 100 or 10 Mbps using potentially mismatched full- and half-duplex transmissions. If this occurs, first determine if there is a firmware upgrade available for the switch. If so, apply the firmware upgrade and test the connection. If that does not resolve the issue, manually set the ports on the NIOS appliance and on the switch to make 1000-Mbps full-duplex connections.

To change Ethernet port settings:

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

   **Note:** You must enable the MGMT port before modifying its port settings. See Using the MGMT Port on page 240.

2. In the Network tab of the Grid Member Properties editor, the Required Ports and Addresses table lists the network settings that were configured.

   — **Port Settings:** Choose the connection speed that you want the port to use. You can also choose the duplex setting. Choose **Full** for concurrent bidirectional data transmission or **Half** for data transmission in one direction at a time. You cannot configure port settings for vNIOS appliances.

3. Select one of the following:

   — **Save & Close:** Save the entry and close the editor.
   — **Save:** Save the entry and keep the editor open.

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


**Using the LAN2 Port**

**Note:** This feature is not supported on vNIOS grid members for Cisco and Riverbed.

The LAN2 port is a 10/100/1000Base-T Ethernet connector on the front panel of Infoblox-250, -250-A, -550-A, -1050-A, -1550-A, -1552-A, -1852-A, -2000, and -2000-A appliances. The LAN2 port is not enabled by default. By default, an appliance uses the LAN1 port (and HA port when deployed in an HA pair). To enable and configure the LAN2 port, you must have read/write permission to the grid member on which you want to enable the port. When you enable the LAN2 port and SNMP, the appliance sends traps from this port for LAN2 related events.

You can configure the LAN2 port in different ways. You can enable the NIC redundancy feature, which groups the LAN1 and LAN2 ports into one logical interface. The LAN1/LAN2 grouping can be activated for both IPv4 and IPv6. Note that this feature is not supported on an HA pair. For information, see *About NIC Redundancy* on page 237. You can enable the LAN2 port on the active or passive node of an HA pair. For information about the LAN2 port configuration and usage on an HA pair, see *Table 7.2* on page 231.

Alternatively, you can configure the LAN2 port on a different IP network than LAN1, and enable the LAN2 port to provide DNS and DHCP services. For information about these features, see the following sections:

- For information about configuring the LAN2 port, see *Configuring the LAN2 Port* on page 238.
- For information about enabling the LAN2 port to provide DHCP services, see *Enabling DHCP on LAN2* on page 238.
- For information about enabling the LAN2 port to provide DNS services, see *Enabling DNS on LAN2* on page 239.

Note that you cannot use the LAN2 port to access the GUI or to connect to the grid.
About NIC Redundancy

You can configure the LAN2 port to provide redundancy and additional fault tolerance in your network. NIC (Network Interface Controller) redundancy is transparently supported for both IPv4 and IPv6. When you enable NIC redundancy, the LAN1 and LAN2 ports are grouped into one logical interface. They share one IP address and appear as one interface to the network. Then, if a link to one of the ports fails or is disabled, the appliance fails over to the other port, avoiding a service disruption.

You can connect the LAN1 and LAN2 ports to the same switch or to different switches, but they must be on the same VLAN. One port is active and the other port is idle at all times. The other port becomes active only when the previously active port fails.

The LAN1 and LAN2 ports share the IP address of the LAN1 port; the port that is currently active owns the IP address. When you enable services on the appliance, such as DNS and DHCP, clients send their service requests to the LAN1 port IP address and receive replies from it as well. The port supports the services and features supported on the LAN1 port as listed in Table 7.2 and Table 7.3. Note that you cannot enable the NIC redundancy feature if the LAN2 port is serving DNS or DHCP.

As shown in Figure 7.8, the appliance is connected to the grid through its MGMT port, and the LAN1 and LAN2 ports are connected to the same switch. The LAN1 and LAN2 port share the IP address of the LAN1 port, which is 1.1.1.5. In the illustration, LAN1 is the active port.

You can enable NIC redundancy on a single independent appliance or grid member. You cannot enable this feature on an HA pair.

Figure 7.8  Using the LAN2 Port for NIC Redundancy

The LAN1 and LAN2 ports share the LAN1 IP address. Only 1 port is active at anytime. Failover may be active for either IPv4 or IPv6 addresses.

Clients send service requests and replies to the LAN1 IP address.
To enable NIC redundancy:

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

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

   Grid Manager adds the LAN2 (Failover) entry to the table with the address information filled in, including IPv6 information if applicable. You cannot enter a separate IP address for the LAN2 port because the LAN1 and LAN2 ports share the IP address of the LAN1 port.

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

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

### Configuring the LAN2 Port

Before you enable the LAN2 port to provide DHCP and DNS services, you must specify its IP address and other properties.

To configure the LAN2 port:

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

2. In the Network -> Basic tab of the Grid Member Properties editor, click the Add icon of the Additional Ports and Addresses table and select LAN2. Enter the following:

   - **Address**: Type the IP address for the LAN2 port, which must be in a different subnet from that of the LAN1 and HA ports.
   - **Subnet Mask**: Specify an appropriate subnet mask.
   - **Gateway**: Type the default gateway for the MGMT port.
   - **Port Settings**: Choose the connection speed that you want the port to use. You can also choose the duplex setting. Choose Full for concurrent bidirectional data transmission or Half for data transmission in one direction at a time. Select Automatic to instruct the NIOS appliance to negotiate the optimum port connection type (full or half duplex) and speed with the connecting switch automatically. This is the default setting. You cannot configure port settings for vNIOS appliances.
   - **LAN2 Virtual Router ID (if HA)**: If the appliance is in an HA pair, enter a VRID number.

3. Click Save & Close to save the entry and close the editor.

### Enabling DHCP on LAN2

You can configure an appliance to provide DHCP services through the LAN1 port only, the LAN2 port only, or both the LAN1 and LAN2 ports. Note that when you enable both ports, they must be connected to different subnets.

After you configure the LAN2 port, you can enable DHCP services on the LAN2 port as follows:

1. From the Data Management tab, select the DHCP tab -> Members tab -> grid_member check box, and then click the Edit icon.

2. In the General -> Basic tab of the Member DHCP Configuration editor, select the Enable DHCP service on LAN2 port check box.

3. Select one of the following:

   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.

4. Click Restart to restart services.
Enabling DNS on LAN2

If you enable DNS on an appliance, it always serves DNS on the LAN1 port. Optionally, you can configure the appliance to provide DNS services through the LAN2 port as well. For example, the appliance can provide DNS services through the LAN1 port for internal clients on a private network, and DNS services through the LAN2 port for external clients on a public network.

After you configure the LAN2 port, you can enable DNS services on the LAN2 port as follows:

1. From the Data Management tab, select the DNS tab → Members tab → grid_member check box, and then click the Edit icon.
2. In the General → Basic tab of the Member DNS Configuration editor, do the following:
   - Enable DNS service on LAN2 port: Select this check box.
   - Automatically create glue A and PTR records for LAN2’s address: The NIOS appliance can automatically generate A (address) and PTR records for a primary name server whose host name belongs to the name space of the zone. Select this check box to enable the appliance to automatically generate an A and PTR record.
3. In the General → Advanced tab, select one of the following from the Send queries from and the Send notify messages and zone transfer request from drop-down lists:
   - VIP: The appliance uses the IP address of the HA port as the source for queries, notifies, and zone transfer requests.
   - MGMT: The appliance uses the IP address of the MGMT port as the source for queries, notifies, and zone transfer requests.
   - LAN2: The appliance uses the IP address of the LAN2 port as the source for queries, notifies, and zone transfer requests.
   - Any: The appliance chooses which port to use as the source for queries, notifies, and zone transfer requests.

   The Send queries from drop-down list also includes loopback IP addresses that you configured. You can select a loopback address as the source for queries.
4. Select one of the following:
   - Save & Close: Save the entry and close the editor.
   - Save: Save the entry and keep the editor open.
5. Click Restart to restart services.
Using the MGMT Port

Note: This feature is not supported on vNIOS grid members for Riverbed and Cisco.

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

- Appliance Management on page 241
- Grid Communications on page 243
- DNS Services on page 245

For information about what types of traffic qualify as appliance management, grid communications, and DNS services, see Table 7.3 on page 232.

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

Some NIOS appliance deployment scenarios support more than one concurrent use of the MGMT port. The following table depicts MGMT port uses for various appliance configurations.

Table 7.4 Supported MGMT Port Uses for Various appliance Configurations

<table>
<thead>
<tr>
<th>Appliance Configuration</th>
<th>Appliance Management</th>
<th>Grid Communications</th>
<th>DNS Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Independent Appliance</td>
<td>✓</td>
<td>Not Applicable</td>
<td>✓</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>✓</td>
<td>Not Applicable</td>
<td>✓</td>
</tr>
<tr>
<td>Grid Master</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Grid Master Candidate</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>HA Grid Member</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Single Grid Member</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

* Although you manage all grid members through the grid master, if you enable the MGMT port on common grid members, they can send syslog events, SNMP traps, and e-mail notifications, and receive SSH connections on that port.

Infoblox does not support MGMT port usage for some appliance configurations (indicated by the symbol ✗ in Table 7.4) because it cannot provide redundancy through the use of a VIP. A grid master that is an HA pair needs the redundancy that a VIP interface on the HA port provides for grid communications. Similarly, DNS servers in an HA pair need that redundancy to answer DNS queries. Because the MGMT port does not support a VIP and thus cannot provide redundancy, grid masters (and potential grid masters) do not support grid communications on the MGMT port.

In addition, NIOS appliances in an HA pair support DNS services on the active node only (indicated by the symbol ◆ in Table 7.4). Only the active node can respond to queries that it receives. If a DNS client sends a query to the MGMT port of the node that happens to be the passive node, the query can eventually time out and fail.
The MGMT port is not enabled by default. By default, a NIOS appliance uses the LAN port (and HA port when deployed in an HA pair). You must log in using a superuser account to enable and configure the MGMT port. You can enable the MGMT port through the Infoblox GUI, as explained in the following sections.

**Appliance Management**

You can restrict administrative access to a NIOS appliance by connecting the MGMT port to a subnet containing only management systems. This approach ensures that only appliances on that subnet can access the Infoblox GUI and receive appliance management communications such as syslog events, SNMP traps, and e-mail notifications from the appliance.

If you are the only administrator, you can connect your management system directly to the MGMT port. If there are several administrators, you can define a small subnet—such as 10.1.1.0/29, which provides six host IP addresses (10.1.1.1–10.1.1.6) plus the network address 10.1.1.0 and the broadcast address 10.1.1.7—and connect to the NIOS appliance through a dedicated switch (which is not connected to the rest of the network). Example 7.9 shows how an independent appliance separates appliance management traffic from network protocol services. Note that the LAN port is on a different subnet from the MGMT port.

*Figure 7.9 Appliance Management from One or More Management Systems*

Similarly, you can restrict management access to a grid master to only those appliances connected to the MGMT ports of the active and passive nodes of the grid master.
To enable the MGMT port on an independent appliance or grid master for appliance management and then cable the MGMT port directly to your management system or to a network forwarding appliance such as a switch or router:

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

2. In the Network -> Basic tab of the Grid Member Properties editor, add the MGMT port to the Additional Ports and Addresses table as follows:

   3. Click the Add icon and select MGMT.

   Grid Manager adds a row for the MGMT port. For an HA pair, it adds two rows, one for each node.

4. Enter the following in the row of the MGMT port for a single grid master or independent appliance, and in the rows of the two nodes for an HA grid master or independent HA pair:

   - **Address**: Type the IP address for the MGMT port, which must be in a different subnet from that of the LAN and HA ports.
   - **Subnet Mask**: Specify an appropriate subnet mask for the number of management systems that you want to access the appliance through the MGMT port.
   - **Gateway**: Type the default gateway for the MGMT port. If you need to define any static routes for traffic originating from the MGMT port—such as SNMP traps, syslog events, and email notifications—destined for remote subnets beyond the immediate subnet, specify the IP address of this gateway in the route.
   - **Port Settings**: Choose the connection speed that you want the port to use. You can also choose the duplex setting. Choose **Full** for concurrent bidirectional data transmission or **Half** for data transmission in one direction at a time. Select **Automatic** to instruct the NIOS appliance to negotiate the optimum port connection type (full or half duplex) and speed with the connecting switch automatically. This is the default setting. You cannot configure port settings for vNIOS appliances.

5. In the Network -> Advanced tab, make sure that the Enable VPN on MGMT Port check box is not selected.

6. Click Save & Close to save the entry and close the editor.

7. Log out of Grid Manager.

8. Cable the MGMT port to your management system or to a switch or router to which your management system can also connect.

9. If your management system is in a subnet from which it cannot reach the MGMT port, move it to a subnet from which it can.

   The Infoblox Grid Manager GUI is now accessible through the MGMT port on the NIOS appliance from your management system.

10. Open an Internet browser window and enter the IP address of the MGMT port as follows: \textit{https://\textlangle IP address of MGMT port\textrangle}.

11. Log in to Grid Manager.

12. Check the Detailed Status panel of the grid member to make sure the status icons are green.
Grid Communications

You can isolate all grid communications to a dedicated subnet as follows:

- For grid communications from the grid master, which can be an HA pair or a single appliance, the master uses either the VIP interface on the HA port of its active node (HA master) or its LAN port (single master). Neither a single nor HA grid master can use its MGMT port for grid communications. (This restriction applies equally to master candidates.)
- Common grid members connect to the grid master through their MGMT port.

This ensures that all database synchronization and grid maintenance operations are inaccessible from other network elements while the common grid members provide network protocol services on their LAN ports. Figure 7.10 shows how grid members communicate to the master over a dedicated subnet.

*Only the active node of an HA member connects to the grid master. The passive node communicates just with the active node. If there is an HA failover, the newly promoted active node must first join the grid before continuing grid communications with the grid master on behalf of the HA member.*
Enabling Grid Communications over the MGMT Port for Existing Grid Members

To enable the MGMT port for grid communications on an existing single or HA grid member:

1. Log in to the grid master with a superuser account.
2. From the Grid tab, select the Grid Manager tab -> Members tab -> grid_member check box, and then click the Edit icon.

   **Note:** You must enable the MGMT port before modifying its port settings. See *Using the MGMT Port* on page 240.

3. In the Network -> Basic tab of the Grid Member Properties editor, add the MGMT port to the Additional Ports and Addresses table as follows:

4. Click the Add icon and select MGMT.

   Grid Manager adds a row for the MGMT port. For an HA pair, it adds two rows, one for each node.

5. Enter the following in the row of the MGMT port for a single grid master or independent appliance, and in the rows of the two nodes for an HA grid master or independent HA pair:
   
   — **Address:** Type the IP address for the MGMT port, which must be in a different subnet from that of the LAN and HA ports.
   
   — **Subnet Mask:** Specify an appropriate subnet mask for the number of management systems that you want to access the appliance through the MGMT port.
   
   — **Gateway:** Type the default gateway for the MGMT port. If you need to define any static routes for traffic originating from the MGMT port—such as SNMP traps, syslog events, and email notifications—destined for remote subnets beyond the immediate subnet, specify the IP address of this gateway in the route.
   
   — **Port Settings:** Choose the connection speed that you want the port to use. You can also choose the duplex setting. Choose **Full** for concurrent bidirectional data transmission or **Half** for data transmission in one direction at a time. Select **Automatic** to instruct the NIOS appliance to negotiate the optimum port connection type (full or half duplex) and speed with the connecting switch automatically. This is the default setting. You cannot configure port settings for vNIOS appliances.

6. In the Network -> Advanced tab, select the **Enable VPN on MGMT Port** check box.

7. In the Security tab, do the following:
   
   — **Restrict Remote Console and Support Access to MGMT Port:** Select this check box to restrict SSH (Secure Shell) v2 access to the MGMT port only. This restricts Infoblox Technical Support and remote console connections—both of which use SSH v2—to just the MGMT port. For an HA pair, you can make an SSH v2 connection to the MGMT port on both the active and passive nodes.

   Clear the check box to allow SSH v2 access to both the MGMT and LAN ports. For an HA pair, you can make an SSH v2 connection to the MGMT and LAN ports on both the active and passive nodes.

8. Click **Save & Close** to save the entries and close the editor.

   The master communicates the new port settings to the member, which immediately begins using them. The member stops using its LAN port for grid communications and begins using the MGMT port.

9. To confirm that the member still has grid connectivity, check that the status icons for that member are green on the *Detailed Status* and *Grid* panels.
DNS Services

You can configure a single independent appliance or single grid member to provide DNS services through the MGMT port in addition to the LAN port. For example, the appliance can provide DNS services through the MGMT port for internal clients on a private network, and DNS services through the LAN port for external clients on a public network. While providing DNS services on the MGMT port, you can still use that port simultaneously for appliance management. Figure 7.11 shows a management system communicating with a single independent appliance through its MGMT port while the appliance also provides DNS services on that port to a private network. Additionally, the appliance provides DNS services to an external network through its LAN port.

Figure 7.11  DNS Services on the LAN and MGMT Ports, and appliance Management on the MGMT Port

Like a single independent appliance, a single grid member can also support concurrent DNS traffic on its MGMT and LAN ports. However, because you manage all grid members through the grid master, a grid member only uses an enabled MGMT port to send SNMP traps, syslog events, and email notifications, and to receive SSH connections. In addition, the active node of an HA pair can provide DNS services through its MGMT port. To use this feature, you must enable DNS services on the MGMT ports of both nodes in the HA pair and specify the MGMT port IP addresses of both nodes on the DNS client as well, in case there is a failover and the passive node becomes active. Note that only the active node can respond to queries that it receives. If a DNS client sends a query to the MGMT port of the node that happens to be the passive node, the query can eventually time out and fail.

To enable DNS services on the MGMT port of an appliance:

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

   Note: You must enable the MGMT port before modifying its port settings. See Using the MGMT Port on page 240.

2. In the Network -> Basic tab of the Grid Member Properties editor, add the MGMT port to the Additional Ports and Addresses table as follows:

3. Click the Add icon and select MGMT.

   Grid Manager adds a row for the MGMT port. For an HA pair, it adds two rows, one for each node.
4. Enter the following in the row of the MGMT port for a single grid master or independent appliance, and in the rows of the two nodes for an HA grid master or independent HA pair:
   - **Address**: Type the IP address for the MGMT port, which must be in a different subnet from that of the LAN and HA ports.
   - **Subnet Mask**: Specify an appropriate subnet mask for the number of management systems that you want to access the appliance through the MGMT port.
   - **Gateway**: Type the default gateway for the MGMT port. If you need to define any static routes for traffic originating from the MGMT port—such as SNMP traps, syslog events, and email notifications—destined for remote subnets beyond the immediate subnet, specify the IP address of this gateway in the route.
   - **Port Settings**: Choose the connection speed that you want the port to use. You can also choose the duplex setting. Choose Full for concurrent bidirectional data transmission or Half for data transmission in one direction at a time. Select Automatic to instruct the NIOS appliance to negotiate the optimum port connection type (full or half duplex) and speed with the connecting switch automatically. This is the default setting. You cannot configure port settings for vNIOS appliances.

5. Click **Save & Close** to save your settings for the MGMT port.

6. From the **Data Management** tab, select the **DNS** tab -> **Members** tab -> *grid_member* check box, and then click the **Edit** icon.

7. In the **General** -> **Basic** tab of the **Member DNS Configuration** editor, do the following:
   - **Enable DNS service on MGMT port**: Select this check box.

8. In the **General** -> **Advanced** tab, select one of the following from the **Send queries from** and the **Send notify messages and zone transfer requests from** drop-down lists:
   - **VIP**: The appliance uses the IP address of the HA port as the source for queries, notifies, and zone transfer requests.
   - **MGMT**: The appliance uses the IP address of the MGMT port as the source for queries, notifies, and zone transfer requests.
   - **LAN2**: The appliance uses the IP address of the LAN2 port as the source for queries, notifies, and zone transfer requests.
   - **Any**: The appliance chooses which port to use as the source for queries, notifies, and zone transfer requests.

   The **Send queries from** drop-down list also includes loopback IP addresses that you configured. You can select a loopback address as the source for queries.

9. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.

To see that the appliance now also serves DNS on the MGMT port:

1. From the **Data Management** tab, select the **DNS** tab -> **Members** tab -> *grid_member* check box.

2. Expand the Toolbar and click **View** -> **View DNS Configuration**.

3. Check that the IP address of the MGMT port appears in the address match list in the listen-on substatement.
**SETTING STATIC ROUTES**

When you put the NIOS appliance on a segment of the network where there is a single path to and from it, a single default route is sufficient. For example, in *Figure 7.12* on page 247, the appliance is in the DMZ behind a firewall and connects to the rest of the network through the DMZ interface on the firewall. For example, when hosts send DNS queries from the Internet and the internal network to the appliance and when the appliance replies to those hosts, the firewall takes care of all the routing.

**Note:** This feature is not supported on vNIOS grid members for Riverbed and Cisco.

*Figure 7.12  Single Default Route*

When the NIOS appliance is on a segment of the network where there are multiple gateways through which traffic to and from the appliance can flow, a single default route is insufficient. For an example, see *Figure 7.13*.
To resolve the problem illustrated in Figure 7.13 on page 248, add a second route pointing traffic destined for 10.1.1.0/24 to use the gateway with IP address 1.2.2.2 on firewall-2. This is shown in Figure 7.14.
Whenever you want the NIOS appliance to send traffic through a gateway other than the default gateway, you need to define a separate route. Then, when the appliance performs a route lookup, it chooses the route that most completely matches the destination IP address in the packet header.

When you enable the MGMT port, the gateway you reference in a static route determines which port the NIOS appliance uses when directing traffic to a specified destination.

- If a route definition references a gateway that is in the same subnet as the IP and VIP addresses of the LAN (or LAN1) and HA ports, the NIOS appliance uses the LAN (or LAN1) or HA port when directing traffic to that gateway.
- If a route definition references a gateway that is in the same subnet as the MGMT port, the NIOS appliance uses the MGMT port when directing traffic to that gateway.

**Figure 7.15 Static Routes for the LAN and MGMT Ports**

```
From LAN:
1.2.2.0/24 dev eth1 scope link
10.1.1.0/24 via 1.2.2.2 dev eth1
default via 1.2.2.1 dev eth1

From MGMT:
10.1.2.0/24 dev eth0 scope link
10.1.3.0/24 via 10.1.2.1 dev eth0
default via 10.1.2.1 dev eth0

From all:
10.1.1.0/24 via 1.2.2.2 dev eth1
10.1.3.0/24 via 10.1.2.1 dev eth0
1.2.2.0/24 dev eth1 proto kernel scope link src 1.2.2.5
to 10.1.2.0/24 dev eth0 proto kernel scope link src 10.1.2.5
default via 1.2.2.1 dev eth1
```

The need for routes can apply to any type of traffic that originates from the appliance, such as DNS replies, DHCP messages, SNMP traps, ICMP echo replies, Infoblox GUI management, and grid communications.

Note: There is a route table for each port as well as a comprehensive route table. For an HA pair, the LAN port route table is duplicated for the HA port. In this illustration, the static routes are shown in green.
To set a static route, do the following:

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

2. In the Network -> Advanced tab of the Grid Member Properties editor, click the Add icon for the Static Routes table, and then enter the following:
   - **Network Address**: Type the address and netmask of the remote network to which the NIOS appliance routes traffic.
   - **Gateway Address**: Type the IP address of the gateway on the local subnet through which the NIOS appliance directs traffic to reach the remote network. The gateway address must meet the following requirements:
     - It must belong to a working gateway router or gateway switch.
     - It must be in the same subnet as the NIOS appliance.

   **Note**: Consult your network administrator before specifying the gateway address for a static route on the appliance. Specifying an invalid gateway address can cause problems, such as packets being dropped or sent to an incorrect address.

3. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.
Enabling DNS Resolution

You can specify a network server to perform domain name queries and specify up to two name servers for resolving a DNS name. You can specify the IP address of a preferred name server and that of an alternate name server, plus use a search list for performing partial name resolution.

To enable DNS resolution for a grid or for an independent appliance or HA pair:

1. **Grid:** From the Grid tab, select the Grid Manager tab, expand the Toolbar and click Grid Properties -> Edit.
   - **Member:** From the Grid tab, select the Grid Manager tab -> Members tab -> grid_member check box, and then click the Edit icon.
   - To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the Grid Properties or Member Properties editor, select the DNS Resolver tab, and then enter the following:
   - **Enable DNS Resolver:** Select the check box to enable the NIOS appliance to send DNS queries to the preferred or alternate name servers whose IP addresses you specify in the following fields.
     - Click the Add icon and enter the IP addresses of the servers to which the appliance sends queries. The appliance attempts to send queries to the servers in the order they are listed if it does not receive a response from a listed name server. To move a server up or down on the list, select it and drag it to its new location or click the up and down arrows.
   - **Search List:** You can define a group of domain names that the NIOS appliance can add to partial queries that do not specify a domain name. For example, if you define a RADIUS authentication home server as “as1”, and you list “corp100.com” and “hq.corp100.com” in the domain group list, then the NIOS appliance sends a query for “as1.corp100.com” and another query for “as1.hq.corp100.com” to the preferred or alternate name server.
     - To add a domain name, click the Add icon and type a domain name in the Search List field. To remove a domain name from the group, select it, and then click Delete.

3. Select one of the following:
   - **Save & Close:** Save the entry and close the editor.
   - **Save:** Save the entry and keep the editor open.
Managing Licenses

Licenses come pre-installed on a NIOS appliance according to the software packages you ordered at the time of purchase. If you wish to upgrade an existing appliance, you must contact Infoblox Technical Support and follow the procedures in "Obtaining and Adding Licenses" on page 252.

On a vNIOS virtual appliance, you can install licenses when you deploy the appliance. You must install both the Grid and vNIOS licenses on a vNIOS appliance for it to join a grid. You can transfer the valid licenses of a vNIOS appliance on VMware from one ESX/ESXi server to another, or from one Cisco SRE-V to another. For information, refer to the "Installation Guide for the vNIOS Software for VMware".

There are three types of licenses:

- **Maintenance licenses** – Examples: NIOS and Grid (or Keystone) maintenance licenses. The duration of maintenance licenses are one, two, or three years. You can obtain these licenses from your Infoblox sales representative.

- **Service licenses** – Examples: DNS and DHCP licenses. These are permanent licenses. You can obtain these licenses from your Infoblox sales representative.

- **Temporary licenses** – You can enable one of several sets of temporary service licenses through the CLI command `set temp_license`.

Before a maintenance license or a temporary license expires, an expiration warning appears during the GUI login process. The warning reappears during each login until you renew the license. To renew a license, contact Infoblox Technical Support.

Obtaining and Adding Licenses

A valid Grid license is required for deploying a grid with NIOS and vNIOS appliances. You can upgrade existing independent NIOS and vNIOS appliances to use a Grid license and then add them to a grid. To upgrade your licenses, contact your Infoblox Technical Support.

When you receive a new license key, it is in CSV (comma separated values) format with the following information: serial number, hardware ID, license type, end date, and license string. You can either upload the file to the appliance or copy the information and paste it in the text field of the Licenses tab of the Infoblox GUI. Note that you must copy the entire string—serial number, hardware ID, license type, end date, and license string—and save it to the text field.

To add a license:

1. From the Grid tab, select the Licenses tab and click the Add icon.
2. Do one of the following:
   - **Upload License File**: Click Select File and navigate to the license file.
   - **Paste License(s)**: Paste the license key in this text field. You must paste the entire string in CSV format: serial number, hardware ID, license type, end date, and license string. If you are pasting multiple licenses, start each string on a new line.
3. Click Save License(s).

**Note**: To transfer licenses between vNIOS on VMware appliances, refer to the "Installation Guide for the vNIOS on VMware Appliances".
Obtaining Temporary Licenses

You can use the CLI command `set temp_license` to generate and install temporary licenses. This can provide licensed features and functionality for the interim, while you wait for your permanent license to arrive.

To generate a temporary license:

1. Log in to the NIOS appliance through a remote console window. For more information on how to open a remote console window, refer to the Infoblox CLI Guide.
2. At the Infoblox command prompt, enter `set temp_license`. The appliance lists the available licenses, and you select those you need.
3. Enter the number of the licenses you want to install.
4. Confirm the selection when prompted, and the following message appears:
   
   Temporary license is installed.

Viewing Licenses

If the appliance is part of a grid, you must log in to the grid master to view license information from Grid Manager. If the appliance is an independent appliance, log in to System Manager on the appliance. If you have transferred licenses from one vNIOS on VMware appliance to another, you can view information about the new and replaced licenses.

To view license information on a NIOS or vNIOS appliance:

1. Log in to Grid Manager on the grid master or System Manager on the independent appliance.
2. Select the Grid or System tab -> Licenses tab. The appliance displays the following information:
   - Name: The name of the appliance.
   - HA: Indicates whether the appliance is an HA pair. This is either Yes or No.
   - Address: The IP address of the appliance.
   - Hardware ID: The unique hardware ID of the appliance. On a vNIOS on VMware appliance, the ID is highlighted in red if the license was transferred to another vNIOS on VMware appliance.
   - Type: The type of license installed. For example, this field displays Grid for a grid license and DHCP for a DHCP service license.
   - Type Detail: Details of the license type. For example, this field displays Model 550 for an IB-VM-550 vNIOS on VMware model.
   - Expiration: The expiration date of the license. For permanent licenses, this displays Permanent.
   - Replaced Hardware ID: The hardware ID of the vNIOS on VMware appliance whose license was transferred.

Backing Up Licenses

You can back up the licenses installed on the appliance, in case you need to re-install them at a later time. Infoblox recommends backing up the licenses before removing any of them.

When you back up the licenses, Grid Manager creates a CSV file that lists the following information for each license: serial number, hardware ID, license type, end date, license string.

To back up licenses:

1. From the Grid tab, select the Licenses tab.
2. Click the Backup Licenses icon in the toolbar.
   Grid Manager generates a CSV file that contains all the licenses. You can then open the file or save it to a specified location.
Removing Licenses

You can remove licenses and reset a NIOS appliance to its factory default settings. For example, if you have a NIOS appliance running the DNSone package with the Grid upgrade, but you want to use it as an independent appliance, you can remove the Grid license. Infoblox recommends that you back up licenses before removing them, in case you decide to reinstall them at a future time.

**Note:** This function should be used with great caution as it can render an appliance unusable if the wrong license is removed.

To remove a license:

1. From the **Grid** tab, select the **Licenses** tab.
2. Select the license and click the Delete icon.
   - Check the license that you are about to remove. Note that removing the wrong license can render an appliance unusable.
3. Click **Yes** when the confirmation dialog appears.
4. Close the browser window and log back in to the Infoblox GUI.
SHUTTING DOWN, REBOOTING, AND resetting a NIOS APPLIANCE

To reboot and shut down a NIOS appliance, you can use Grid Manager or the Infoblox CLI. To reset a NIOS appliance, you must use the Infoblox CLI.

Rebooting a NIOS Appliance

You can reboot a single NIOS appliance, a single node in an HA pair, or both nodes in an HA pair.

To reboot a single NIOS appliance or one or both nodes in an HA pair:

1. From the Grid tab, select the Grid Manager tab → Members tab → grid_member check box.
2. Expand the Toolbar and click Control → Reboot.

— For an HA pair, choose whether to boot one node (and which one) or both nodes, and then click OK.

Depending on the browser you use, Grid Manager may display a dialog box that indicates the system is unavailable during a restart or reboot.

To reboot a single NIOS appliance using the CLI:

1. Log in to the Infoblox CLI using a superuser account for the NIOS appliance that you intend to reboot.
2. Enter the following CLI command: `reboot`

Shutting Down a NIOS Appliance

Under normal circumstances, you do not need to turn off or shut down a NIOS appliance. It is designed to operate continuously. However, if you want to turn off a NIOS appliance, use the GUI or the CLI to shut down the appliance, instead of just turning off the power switch. Before shutting down a remote appliance, make sure you can restart it.

You cannot restart the system using the GUI.

Note: If there is a disruption in power when the NIOS appliance is operating, the NIOS appliance automatically reboots itself when power is restored.

To shut down a NIOS appliance:

1. From the Grid tab, select the Grid Manager tab → Members tab → grid_member check box.
2. Expand the Toolbar and click Control → Shutdown.

— For an HA pair, choose whether to shut down one node (and which one) or both nodes, and then click OK.

The NIOS appliance shuts down. The fans might continue to operate until the appliance cools down.

To shut down a NIOS appliance using the CLI:

1. Log in to the Infoblox CLI using a superuser account.
2. Enter the following CLI command: `shutdown`

Resetting a NIOS Appliance

There are three ways to reset a NIOS appliance:

- Resetting the Database on page 256
- Resetting a NIOS Appliance to Factory Settings on page 256
- Resetting the NIOS Appliance to Factory Settings and Removing Licenses on page 256

You can perform these functions only through the CLI.
Resetting the Database

You can reset the database if you lose the administrator account and password or if you want to clear the database but preserve the log files to diagnose a problem. This function removes the configuration files, and the DNS and DHCP data from the appliance database. During this procedure, you are given the option to preserve the network settings of the appliance, which are the IP address and subnet mask, the IP address of the gateway, the host name, and the remote access setting.

To reset the database:
1. Log in to the Infoblox CLI using a superuser account.
2. Enter the following CLI command: `reset database`
   The appliance then displays a message similar to the following:
   The following network settings can be restored after reset:
   - IP Address: 10.1.1.10
   - Subnet Mask: 255.255.255.0
   - Gateway: 10.1.1.1
   - Host Name: ns1.corp100.com
   - Remote Console Access: true
   The entire database will be erased.
   Do you wish to preserve basic network settings? (y or n)
3. Press the Y key to preserve the network settings or the N key to return the network settings to their default values (192.168.1.2, 255.255.255.0, 192.168.1.1).

Resetting a NIOS Appliance to Factory Settings

You can reset a NIOS appliance to its original factory settings. This removes the database, network settings, logs, and configuration files. Then, it reboots with its factory settings, which are the default user name and password, and default network settings. When you perform this procedure, the appliance does not give you the option to preserve your network settings.

Note: If you have previously imported HTTPS certificates, the appliance regenerates the certificates and replaces them.

To reset the NIOS appliance to its factory settings:
1. Log in to the Infoblox CLI using a superuser account.
2. Enter the following CLI command: `reset all`

Resetting the NIOS Appliance to Factory Settings and Removing Licenses

You can also reset a NIOS appliance to its original factory settings and remove all the licenses installed on the appliance. This removes the database, network settings, logs, configuration files, and licenses. The appliance then reboots with its factory settings, which are the default user name and password, and default network settings.

Note: If you have previously imported HTTPS certificates, the NIOS appliance regenerates the certificates and replaces them.

To reset the NIOS appliance to its factory settings and remove all its licenses:
1. Log in to the Infoblox CLI using a superuser account.
2. Enter the following CLI command: `reset all licenses`
Managing the Disk Subsystem on the Infoblox-2000 and -2000-A

Among its many features, the Infoblox-2000 and -2000-A use a RAID (Redundant Array of Independent Disks) 10 array to provide the optimum mix of high database performance and redundant data storage with recovery features in the event of disk failures. The disk array is completely self managed. There are no maintenance or special procedures required to service the disk subsystem.

Caution: Never remove more than one disk at a time from the array. Removing two or more disks at once can cause an array failure and result in an unrecoverable condition. You should replace only one disk at a time, using a replacement disk from Infoblox. For information, see Replacing a Failed Disk Drive on page 259.

About RAID 10

RAID 10 (or sometimes called RAID 1+0) uses a minimum of four disk drives to create a RAID 0 array from two RAID 1 arrays, as shown in Figure 7.16. It uses mirroring and striping to form a stripe of mirrored subsets. This means that the array combines—or stripes—multiple disk drives, creating a single logical volume (RAID 0). RAID 10 combines the high performance of RAID 0 and the high fault tolerance of RAID 1. Striping disk drives improves database write performance over a single disk drive for large databases. The disks are also mirrored (RAID 1), so that each disk in the logical volume is fully redundant.

Figure 7.16 RAID 10 Array Configuration

When evaluating a fault on the Infoblox-2000 or -2000-A, it is best to think of the disk subsystem as a single, integrated unit with four components, rather than four independent disk drives. For information, see Evaluating the Status of the Disk Subsystem on page 258.
Managing Appliance Operations

Evaluating the Status of the Disk Subsystem

You can monitor the disk subsystem through the Infoblox Grid Manager GUI, the scrolling front panel LCD display, and four front panel LEDs next to the disk drives. In addition, you can monitor the disk status by using the CLI command `show hardware_status`. The following example displays the status of an Infoblox-2000 or -2000-A using the command:

```
Infoblox > show hardware_status
POWER:    Power OK
Fan1:     7258 RPM
Fan2:     6887 RPM
Fan3:     7258 RPM
CPU1_TEMP: +20.0 C
CPU2_TEMP: +24.0 C
SYS_TEMP:    +35 C
RAID_ARRAY: OPTIMAL
RAID_BATTERY: OK READY Yes 103 HOURS
```

The `Detailed Status` panel provides a detailed status report on the appliance and service operations. To see a detailed status report:

- From the Grid tab, select the Grid Manager tab -> Members tab -> grid_member check box -> Detailed Status icon in the table toolbar.

After displaying the Detailed Status panel, you can view the status of the selected grid member. For more information on the Detailed Status panel, see Viewing Appliance Status on page 298.

The RAID icons indicate the status of the RAID array on the Infoblox-2000 or -2000-A.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="green.png" alt="Green" /></td>
<td>Green</td>
<td>The RAID array is in an optimal state.</td>
</tr>
<tr>
<td><img src="yellow.png" alt="Yellow" /></td>
<td>Yellow</td>
<td>A new disk was inserted and the RAID array is rebuilding.</td>
</tr>
<tr>
<td><img src="red.png" alt="Red" /></td>
<td>Red</td>
<td>The RAID array is degraded. At least one disk is not functioning properly. The GUI lists the disks that are online. Replace only the disks that are offline.</td>
</tr>
</tbody>
</table>

The appliance also displays the type of each disk. In the event of a disk failure, you must replace the failed disk with one that is qualified and shipped from Infoblox and has the same disk type as the rest of the disks in the array. The disk type can be one of the following:

- IB-Type 1: Infoblox supported disk type
- IB-Type 2: Infoblox supported disk type
- Unk: Unknown disk type that Infoblox does not support

All disk drives in the array must have the same disk type for the array to function properly. You can have either IB-Type 1 or IB-Type 2, but you cannot mix both in the array. When you have a mismatched disk in the array, you must promptly replace the disk with a replacement disk from Infoblox to avoid operational issues.
Appliance Front Panel

The disk drives are located on the right side of the appliance front panel. To the right of each drive there is an LED that displays the status of each drive. The front panel LCD scrolls and displays the disk array status every 20 seconds.

Table 7.5 Disk Drive LEDs

<table>
<thead>
<tr>
<th>LED Color</th>
<th>Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Disk operating normally</td>
<td>None</td>
</tr>
<tr>
<td>Yellow</td>
<td>Disk read/write activity</td>
<td>Disk is functioning normally or is synchronizing if recently inserted.</td>
</tr>
<tr>
<td>Dark</td>
<td>Disk has failed or not inserted</td>
<td>Verify the failure in the GUI or CLI. Remove the disk and replace with a functional disk drive. Note that the drive rebuilds with its twin.</td>
</tr>
</tbody>
</table>

Replacing a Failed Disk Drive

The Infoblox-2000 and -2000-A are designed to provide continuous operation in the event of a failed disk. Replace an original RAID disk only when there is a disk failure. Hot-swapping a disk drive is a simple process that does not require issuing commands or a GUI operation.

When you replace a failed disk, you must replace it with an Infoblox supplied disk. To ensure that you receive the correct replacement disk, report the disk type or part number of the failed disk. The appliance displays the disk type in the Detailed Status panel, and the Infoblox part number is printed on the disk. Installing disks that are not qualified and shipped from Infoblox could cause failures in the appliance.

To replace a disk drive, follow this procedure:

1. Identify and verify the failed drive via the Grid Manager, front panel LCD, or CLI.
2. If the activity light is green or blinking yellow, make sure you have identified the correct drive. There are conditions where a drive could be in the process of failing and still be green or yellow.
   
   **Note:** Do not remove a correctly functioning drive.

3. Push in the latch for the drive and pull the release lever out towards you.
4. When the drive disengages, wait about 30 seconds for the disk to completely stop spinning.
5. Slide it out of the slot.

Replacement drives are shipped as a complete unit, ready to insert into the appliance. There is no preparation required. To install a replacement drive, follow this procedure:

1. Insert the replacement drive into the drive bay slot.
2. Gently slide the drive into place. When you feel the release lever engage, continue applying gentle pressure to the drive while pushing the release lever towards the appliance.
3. The release lever locks into place and the LED next to the disk drive lights up. Note that if the alarm buzzer is sounding, it automatically turns off about 20 seconds after the drive is inserted.
4. The disk drive automatically goes into rebuild mode.
Disk Array Guidelines

Infoblox has designed the disk array to be completely self managed. There are no maintenance procedures required for a normally functioning disk array. Mishandling the disk array can cause an unrecoverable error and result in a failed appliance. Infoblox highly recommends that you observe the following guidelines:

- Remove only one disk at a time. Do not remove two or more disks from the appliance at the same time. Removing two or more disks at the same time might result in an appliance failure and require an RMA of the appliance. This rule applies to both powered and powered down appliances.
- If the status of the array is degraded, remove the failed or failing disk drive only. Do not remove an optimally functioning drive.
- If your acceptance procedure requires a test of the RAID hot swap feature, remove only one disk drive at a time. You can remove a second disk only after you replace the first disk and the array completes its rebuilding process.
- Do not remove a disk drive if the array is rebuilding. This could result in an appliance failure. Verify the status of the array before removing a disk drive.
- Use the following procedure to remove a spinning disk:
  1. Unlatch and pull the disk about two cm (one inch) to disengage contact.
  2. Wait about 30 seconds for the disk to completely stop spinning.
  3. Remove the disk and handle it with care. Do not drop the disk or ship it loosely in a carton.
- You can hot swap a drive while the appliance remains in production.
- There are some conditions that may require powering down the appliance to replace a failed unit. This normally happens if the RAID controller detects an error that could damage the array. If you insert a replacement drive into a live array and the controller doesn't recognize the drive, power down the appliance.
- If you inadvertently remove the wrong disk drive, do not immediately remove the disk drive that you originally intended to remove. Verify the status of the array and replace the disk drive that you removed earlier before removing another drive. Removing a second drive could render the appliance inoperable.
- Older appliances have an audio alarm buzzer that sounds if a drive fails. The alarm automatically stops about 20 seconds after a functional disk has been inserted into the array.
- All disks in the RAID array should have the same disk type for the array to function properly.
- In the unlikely event that two disk drives fail simultaneously and the appliance is still operational, remove and replace the failed disk drives one at a time.
- Rebuild time depends on a number of factors, such as the system load and grid replication activities. On very busy appliances (over 90% utilization), the disk rebuild process can take as long as 40 hours. On a grid master serving a very large grid, expect the rebuild process to take at least 24 hours.
- Replace a failed or mismatched disk only with a replacement disk shipped from Infoblox. When you request a replacement disk, report the disk type displayed in the Detailed Status panel of the GUI or the Infoblox part number on the disk.
Restarting Services

Whenever you make a change (such as add a zone, a network, or a range), you click the Restart icon to restart services. You can restart the DNS and DHCP services after you make configuration changes. You can also specify a future restart time.

You can restart services at the grid level or at the member level as described in:

- Restarting Grid Services on page 261
- Restarting Member Services on page 262

The following rules apply to superusers and limited-access users:

- You can cancel a schedule that you create to restart services. A superuser can cancel any scheduled restarts.
- Only superusers and administrators with read/write permission to all grid members can schedule a grid restart.
- When a superuser schedules a grid restart, a limited-access user cannot schedule a member-level restart.
- Limited-access users cannot cancel a superuser's scheduled changes.
- Limited-access users cannot create or modify a schedule for a grid member if a schedule for the member (created by another user) already exists.

The system writes every scheduled change action to the audit log as follows:

```
USER logon_id action service restart schedule 'schedule' on grid (or member) grid name or member node id
```

For example:

```
USER jdoe insert service restart schedule '02/20/2007 01:30:00' on grid Infoblox
USER jdoe deleted service restart schedule '02/22/2007 01:30:00' on node id 3
```

For more information on the audit log, see Using the Audit Log on page 310.

Restarting Grid Services

Only superusers and administrators with read/write permission to all grid members can schedule a grid restart. You can restart services at the grid level either simultaneously or sequentially, and also specify the restart time.

After you enter a specific date and time, the system schedules the restart at the specified time on each grid member. To restart services at the grid level:

1. From the Data Management tab, select the DHCP, DNS, or Grid tab, or select the Administration tab, and then click Restart Services from the Toolbar. The Restart Grid Services wizard appears.
2. You can specify whether the member restarts services when necessary or you can force it to restart services. Select one of the following in the Restart Grid Services section:
   - If needed: Select this to restart all active DNS and DHCP services if there are any changes requiring a service restart.
   - Force restart services: Select this to force all active services to restart, regardless of their state.
3. Select one of the following in the Restart Services on all Members section:
   - Simultaneously: Restarts the services on all of the members in a grid at the same time. This is the default option.
   - Sequentially: Restarts the services on each grid member according to the number of seconds you enter in the Sequential every (seconds) field. For example, if you enter every 10 seconds, the system restarts services on the first member, and 10 seconds later on the second member.

Impact Members and Services: Click the Poll Members icon to display the affected members and services when the system restarts. Grid Manager displays the member names and one of the following for each service:

- YES: The service is active and the system will restart the service upon execution of this task.
- NO: The service will not restart unless the Force restart services option is selected.
- DISABLED: The service is currently disabled.
4. To schedule a service restart, click the Schedule icon at the top of the wizard. In the Schedule Change panel, complete the following:
   - **Now**: Restarts services upon clicking Restart.
   - **Later**: Enter the following information to schedule all grid members to restart services at a certain date and time:
     - **Date**: Enter a date in YYYY-MM-DD (year-month-day) format. The appliance displays today's date. You can also click the calendar icon to select a date from the calendar widget.
     - **Time**: Enter a time in hh:mm:ss AM/PM (hours:minutes:seconds AM or PM) format. When you enter the time in a 24-hour format such as 23:00, Grid Manager displays 11:00:00 PM. You can also select a time from the drop-down list by clicking the time icon.
     - **Time Zone**: Select a time zone for the scheduled date and time from the drop-down list. This field displays the time zone of the browser that the admin uses to log in to Grid Manager.

5. Click Restart to restart services immediately or click Schedule Restart to schedule the restart.

**Restarting Member Services**

The member restart time always supersedes the grid restart time. If the member restart time is later than the grid restart time, then the member restarts services at its scheduled time. If the member restart time is before the grid restart time, then the member restarts services at its scheduled restart time, and again during the grid restart time.

To restart member services:

1. From the Data Management tab, select the DHCP tab → Members tab → member check box, and then click Restart Services from the Toolbar.
   or
   From the Grid tab, select the Grid Manager tab, and then select a member check box.

2. You can specify whether the member should restart services when necessary or you can force it to restart services. Select one of the following in the Restart Member Services section:
   - **If needed**: Select this to restart all active DNS and DHCP services, if there are any changes requiring a service restart.
   - **Force restart services**: Select this to force all active services to restart, regardless of their state.

   **Impacted Services**: This table displays the affected services when the system restarts. It can display one of the following for each service:
   - **YES**: The service is active and the system will restart the service upon execution of this task.
   - **NO**: The service will not restart unless the Force restart services option is selected.
   - **DISABLED**: The service is currently disabled.

3. To schedule a service restart, click the Schedule icon at the top of the editor. In the Schedule Change panel, complete the following:
   - **Now**: Restarts services immediately.
   - **Later**: Enter the following information to schedule the member to restart services at a certain date and time:
     - **Date**: Enter a date in YYYY-MM-DD (year-month-day) format. The appliance displays today's date. You can also click the calendar icon to select a date from the calendar widget.
     - **Time**: Enter a time in hh:mm:ss AM/PM (hours:minutes:seconds AM or PM) format. You can also select a time from the drop-down list by clicking the time icon.
     - **Time Zone**: Select a time zone for the scheduled date and time from the drop-down list. This field displays the time zone of the browser that the admin uses to log in to Grid Manager.

4. Click Restart to restart services immediately or click Schedule Restart to schedule the restart.
Canceling a Scheduled Restart

Limited-access users can only cancel a schedule that they created. Superusers can cancel a schedule that any user created. You can cancel scheduled restarts from the scheduled tasks viewer. For information, see Scheduled Tasks Viewer on page 218.

When you delete a scheduled restart, the system cancels the schedule to restart services on the member or grid and does not restart services.

To cancel a scheduled restart, see Canceling Scheduled Tasks on page 221.
Chapter 8  File Distribution Services

This chapter provides an overview of the file distribution services provided on the NIOS appliance. It contains the following sections:

•  About File Distribution  on page 266
  —  Configuring the TFTP Service  on page 267
  —  Configuring the FTP Service  on page 267
  —  Configuring the HTTP Service  on page 268
  —  Configuring Access Control Lists  on page 268
  —  Modifying Access Control Lists  on page 269

•  Monitoring File Distribution Services  on page 270
  —  Starting and Stopping File Distribution Services  on page 270
  —  Monitoring File Distribution Services  on page 270

•  Managing Files and Directories  on page 271
  —  Configuring File Distribution Storage Settings  on page 271
  —  Adding Directories  on page 271
  —  Modifying Directories  on page 271
  —  Uploading Files  on page 272
  —  Viewing Directories  on page 272
ABOUT FILE DISTRIBUTION

The NIOS appliance provides support for file transfers using TFTP, HTTP, and FTP. You can use Grid Manager or the API to upload files to the appliance. You can then allow specific network devices to retrieve the files using TFTP, HTTP, or FTP.

Network devices, such as VoIP phones, can use the DHCP services on the appliance for IP address assignments and use the file distribution services for IP device configuration downloads. Downloads can be accomplished with TFTP, HTTP, or FTP.

Figure 8.1 Uploading and retrieving files

You can store up to 10,000 files in binary and ASCII format on a NIOS appliance, vNIOS appliance on Cisco, or vNIOS appliance on VMware. The appliance or virtual appliance provides a total storage size of five gigabytes, with a default of 500 MB. On a grid with vNIOS appliances on Riverbed as grid members, the storage size is restricted to one gigabyte. You can create a directory structure and organize your files to match your requirements. By default, the appliance includes the files when you back up the system.

For appliances in a grid, you can configure all or some grid members for file distribution services. Upload the files to the active grid master, and it replicates the files to all potential grid masters and all members with TFTP, HTTP, or FTP enabled.

After configuring the file distribution services on the appliance, you can do the following:

- Enable, disable, and monitor the services, as described in Managing File Distribution Services on page 270.
- Modify storage space for file distribution, as described in Configuring File Distribution Storage Settings on page 271.
- Upload files to the appliance, as described in Uploading Files on page 272.
- View current files, as described in Viewing Directories on page 272.
Configuring the TFTP Service

The TFTP file distribution service is disabled on the appliance by default. To allow file distribution access using TFTP, you must specify the clients that are allowed to use the service and then enable the service on the appliance. If you do not specify this information or enable the service, the appliance denies access to all clients. The appliance provides read-only access to the files.

To configure the TFTP file distribution service on a member:

1. From the **Data Management** tab, select the **File Distribution** tab -> **Members** tab -> **member** check box, and then click the **Edit** icon.

2. In the **Member File Distribution Properties** editor, select the **TFTP** tab, and then complete the following:
   - **Listen on Port**: Enter the number of the port on which the appliance receives TFTP file distribution requests. The default is port 69.
   - **Allow file transfers from**: Configure the appliance to grant or deny permissions to TFTP file distribution requests from clients, as described in **Configuring Access Control Lists** on page 268.

3. **Save & Close** or **Save** to save the configuration.

After you configure the TFTP service, you must enable the service to allow file distribution access. For information, see **Starting and Stopping File Distribution Services** on page 270.

Configuring the FTP Service

The FTP file distribution service is disabled on the appliance by default. To allow file distribution access using FTP, you must specify the clients that are allowed to use the service and then enable the FTP service on the appliance. If you do not specify this information or enable the service, the appliance denies access to all clients. The appliance provides read-only access to the files.

To configure the FTP file distribution service on a member:

1. From the **Data Management** tab, select the **File Distribution** tab -> **Members** tab -> **member** check box, and then click the **Edit** icon.

2. In the **Member File Distribution Properties** editor, select the **FTP** tab, and then complete the following:
   - **Listen on Port**: Enter the number of the port on which the appliance receives FTP file distribution requests. The default is port 21.
   - **Login Banner**: Enter your own login banner text that appears after you establish an FTP connection or use the default (Restricted Access Only).
   - **FTP Passive Mode**: By default, this is selected to enable FTP in passive mode; otherwise, it is in active mode. An FTP connection between a client and server can be in active or passive mode. In active mode, the server initiates the data connection. In passive mode, the client initiates the data connection. Depending on your firewall policy, firewalls can block active mode connections. There is no firewall filtering in passive mode.
   - **FTP File Listing**: Select this to allow users to list files and subdirectories on the appliance.
   - **Allow file transfers from**: Configure the appliance to grant or deny permissions to FTP file distribution requests from clients, as described in **Configuring Access Control Lists** on page 268.

3. Click **Save & Close** or **Save** to save the configuration.
Configuring the HTTP Service

To allow file distribution access using HTTP, you must specify clients that can request the service and then enable the HTTP service on the appliance.

Before you enable the HTTP service, however, be aware of the following configuration rules:

- HTTP only runs on the active member of an HA pair.
- HTTP can run on the master or any member.
- HTTP always runs on the LAN port, never the MGMT port.
- HTTP to HTTPS redirect becomes non-functional if the file distribution service is enabled and all administrative access is run on the LAN port. For more information on HTTP redirect, see Enabling HTTP and GUI Redirections on page 227. For information on how to specify the MGMT port for HTTP, see Using the MGMT Port on page 240.

To configure the HTTP file distribution service on a member:

1. From the Data Management tab, select the File Distribution tab → Members tab → member check box, and then click the Edit icon.
2. In the Member File Distribution Properties editor, select the HTTP tab, and then complete the following:
   - Allow Any: This is selected by default to allow HTTP file distribution requests from any client.
   - Only these addresses: Select this to configure the access control list for allowing HTTP file distribution requests from clients, as described in Configuring Access Control Lists on page 268.
3. Click Save & Close or Save to save the configuration.

Configuring Access Control Lists

You can configure the appliance to grant or deny access to file distribution requests from specific clients by creating access control lists for the file distribution services. You can grant or deny permissions to specific IPv4 addresses and IPv4 networks. You can also grant or deny permissions to all clients. Note that for the HTTP service, you can grant permissions to all clients or specific clients, but you can deny permissions only to all clients, not specific clients.

When you grant permissions to a network for a specific file distribution service, all clients in the network have the permission to request the file distribution service. However if some IP addresses within the network should not have the permission to access files through a specific service, you can add these addresses to the access control list and deny their permissions to the service. Ensure that you list these IP addresses before the network address in the list because the appliance applies permissions to the addresses in the order they are listed. You can use the arrow keys to move the addresses up and down the list after you add them.

To configure an access control list for a file distribution service:

1. From the Data Management tab, select the File Distribution tab → Members tab → member check box, and then click the Edit icon.
2. In the Member File Distribution Properties editor, select the tab of the service to which you want to add the list.
3. In the Allow file transfers from section, click the Add icon, and then select one of the following from the drop-down list:
   - IPv4 Address: Select this to manage file access permissions for a single IP address using the file distribution service.
     Grid Manager adds a row to the table. Complete the following:
     - Permission: Select Allow to grant permission to use the file distribution service. Select Deny to deny permission to use the file distribution service. For the HTTP service, you can only grant permission to the IP address or network. IP addresses and networks that are not on the list are automatically denied access to the HTTP service.
     - Type: Grid Manager displays the address type. This can be IPv4 Address, IPv4 Network, or Any. You cannot modify this field.
     - Name: Enter the IP address here. You cannot modify this field if you select Any Address/Network from the Add menu.
— **IPv4 Network**: Select this to manage file access permissions for a specific network using the file distribution service. Grid Manager displays the *Add IPv4 Network* section. Complete the following and click the Add icon:
  — **Address**: Enter the network address you want to add to the list.
  — **Netmask**: Use the slider to choose an appropriate netmask for the network.
  — **Permissions**: Select *Allow* to grant permissions to all the clients in the network to use the file distribution service. Select *Deny* to deny permission to all the clients in the network to use the file distribution service.
  — **Any Address/Network**: Select this to accept file distribution requests from any client. This is not an option for the HTTP file distribution service.

4. Click *Save & Close* or *Save* to save the configuration.

### Modifying Access Control Lists

1. From the **Data Management** tab, select the **File Distribution** tab -> **Members** tab -> *member* check box, and then click the Edit icon.

2. In the **Member File Distribution Properties** editor, select the tab of the service to which the list belongs.

3. In the **Allow file transfers from** section, modify the fields as described in *Configuring Access Control Lists* on page 268. You can also do the following:
   - Add a new permission. For information, see *Configuring Access Control Lists* on page 268.
   - Delete a permission by selecting it and clicking the Delete icon.
   - Reorder the list by selecting a permission and clicking an arrow next to the list to move the permission up or down the list.
Managing File Distribution Services

After you configure the file distribution services, you can do the following to manage them:

- Enable or disable a file distribution service, as described in Starting and Stopping File Distribution Services on page 270.
- Monitor the current status of the services, as described in Monitoring File Distribution Services on page 270.

Starting and Stopping File Distribution Services

You can enable and disable a file distribution service on a specific grid member or on multiple members. You must have read/write permission to the members to start and stop a service on them.

To start a service on a member:

1. From the Data Management tab, select the File Distribution tab -> Members tab -> member check box, and then click the Start icon from the Toolbar. You can select multiple members by selecting their check boxes.
2. From the Start drop-down menu, select the service you want to start.
3. In the Start Service dialog box, click Yes.
   Grid Manager enables the selected service on the selected member and displays the service status in the Status column in the panel.

To stop a service on a member:

1. From the Data Management tab, select the File Distribution tab -> Members tab -> member check box, and then click the Stop icon from the Toolbar. You can select multiple members by selecting their check boxes.
2. From the Stop drop-down menu, select the service you want to stop.
3. In the Stop Service dialog box, click Yes.
   Grid Manager disables the selected service on the selected member and displays the service status in the Status column in the panel.

Note: When you enable or disable a service, there may be a short delay before Grid Manager displays the correct status.

Monitoring File Distribution Services

To view the current status of the file distribution services:

1. From the Data Management tab, select the File Distribution tab -> Members tab.
2. Grid Manager displays the following information:
   - Name: The name of the grid member.
   - Address: The IP address of the grid member.
   - Status: The overall status of the file distribution services running on the member. You can mouse over on the field to view the status of each service. This field can display one of the following:
     - Stopped: All the file distribution services are disabled.
     - Running: One or more of the file distribution services are running properly.
     - Warning: The services are functioning properly. However, there are some issues, such as storage space has reached 90%, about the services.
     - Error: One or more of the services have service issues.
   - Comment: Information about the member.
   - Site: The location to which the member belongs. This is one of the pre-defined extensible attributes.

You can sort the information in ascending or descending order by columns. You can also print and export the information in this panel.
**Managing Files and Directories**

After you configure file distribution services on grid members, you can manage files and directories in the following ways:

- Set the storage limitation for file distribution, as described in Configuring File Distribution Storage Settings on page 271.
- Create a directory structure for file distribution, as described in Adding Directories on page 271.
- Upload files to the appliance, as described in Uploading Files on page 272.
- View the uploaded files, as described in Viewing Directories on page 272.

### Configuring File Distribution Storage Settings

The maximum storage space for distributed files is five gigabytes on a grid with NIOS appliances, vNIOS appliances on Cisco, and vNIOS appliances on VMware. On a grid with vNIOS appliances on Riverbed as grid members, the maximum storage is one gigabyte. The default is 500 MB.

To change the default file distribution storage settings:

1. From the Data Management tab, select the File Distribution tab, and then click Grid File Distribution Properties from the Toolbar.
2. In the Grid File Distribution Properties editor, complete the following:
   - **Storage Limit (MB):** Enter the maximum storage space in megabytes.
   - **Include files and directories in system backup:** This is selected by default to ensure that the appliance includes the files in the backup process. You can clear this check box to improve the backup performance if you have stored these files separately on another server.
3. Click the Save & Close or Save to save the configuration.

### Adding Directories

To facilitate file management, you can create a directory structure in which you store your files.

To add a directory:

1. From the Data Management tab, select the File Distribution tab -> Files tab.
2. Click the parent directory link, and then click Add -> Directory from the Toolbar.
3. Grid Manager adds a new directory to the parent directory and gives it the default name NewDirectory.

You can modify the directory name and permissions, as described in Modifying Directories on page 271.

### Modifying Directories

To modify a directory:

1. From the Data Management tab, select the File Distribution tab -> Files tab.
2. Select the directory check box and click the Edit icon.
3. The Directory editor provides the following tabs from which you can modify data:
   - **General:** You can modify the directory name here, except for the Root directory.
   - **Permissions:** You can add or delete admin permissions in this tab. For information, see About Administrative Permissions on page 87.
4. Click the Save & Close or Save to save the configuration.

You can also select a directory and click the Delete icon to delete it.

**Note:** When you delete a directory, the appliance automatically removes all its contents as well.
Uploading Files

You can upload a maximum of 10,000 files. When you upload a file, the appliance compares the file size with the available storage. If there is enough space, it uploads the file. If uploading the file exceeds the storage limit, the appliance displays a warning message and does not upload the file. For information about file distribution storage, see Configuring File Distribution Storage Settings on page 271.

If you upload a file that has the same name and path as an existing file, the appliance automatically replaces the old file.

Note: Administrators with superuser privileges can manage uploading files. Limited-access admins with read/write permissions to specific directories can upload files to the directories. For information, see Administrative Permissions for File Distribution Services on page 130.

To upload a file:
1. From the Data Management tab, select the File Distribution tab -> Files tab.
2. Select the destination directory link.
3. Click Add -> File from the Toolbar.
4. In the Upload dialog box, navigate to the file you want to upload, click Open, and then click Upload.

Grid Manager uploads the file to the destination directory.

Viewing Directories

To view directories and file information:
1. From the Data Management tab, select the File Distribution tab -> Files tab.
2. Grid Manager displays the following information in the Root directory.
   - Name: The name of the directory or file.
   - Type: Depending on the file type, this can be Directory or File.
   - Size: The file size in B, KB, or MB depending on whether the file size crosses the unit limit or not. For example, if the file size is 1023, Grid Manager displays 1023 B. If the file size is 1025, Grid Manager displays 1 KB. For a directory, Grid Manager displays a dash (-).
   - Date Modified: The timestamp when the directory was last created or when the file was last modified.

You can view files and directories in a specific directory by clicking the directory link.

You can also do the following in this panel:
- Sort the information in ascending or descending order by columns.
- Use the breadcrumb to go to a specific directory.
- Print and export the information in this panel.
- Add a directory or a file. For information, see Adding Directories on page 271 and Uploading Files on page 272.
- Open and edit a directory. For information, see Modifying Directories on page 271.
Chapter 9  Managing NIOS Software and Configuration Files

This chapter explains how to manage upgrade groups and perform software upgrades and downgrades for NIOS appliances. It also describes how to back up and restore configuration files. It includes the following sections:

- **Managing Upgrade Groups** on page 274
  - Adding Upgrade Groups on page 274
  - Modifying Upgrade Groups on page 275
  - Viewing Upgrade Groups on page 276
  - Deleting Upgrade Groups on page 276
- **Viewing Software Versions** on page 277
- **Upgrading NIOS Software** on page 278
  - Lite Upgrades on page 278
  - Uploading NIOS Software on page 278
  - Distributing Software Upgrade Files on page 279
  - Managing Distributions on page 281
  - Testing Software Upgrades on page 282
  - Performing Software Upgrades on page 282
  - Monitoring Distribution and Upgrade Status on page 287
- **Downgrading Software** on page 288
- **Reverting to the Previously Running Software Version** on page 289
- **Backing Up and Restoring Configuration Files** on page 289
  - Backing Up Files on page 289
  - Automatically Backing Up Data Files on page 290
  - Manually Backing Up Data Files on page 292
  - Downloading Backup Files on page 292
  - Restoring Backup Files on page 293
  - Downloading Backup Files from a Different Appliance on page 294
- **Downloading Support Bundles** on page 295
Managing NIOS Software and Configuration Files

Managing Upgrade Groups

To minimize the impact of grid upgrades on your system operations, you can organize members into upgrade groups and schedule their software distributions. This is useful, for example, in a large grid spanning multiple time zones where there are fluctuating network and downtime considerations at the various locations. Note that you can also schedule their upgrades if the NIOS software upgrade is an Upgrade Lite compatible release. For information, see Lite Upgrades on page 278.

Infoblox provides two default upgrade groups:

- Grid Master — After you configure the grid master, it automatically becomes the only member of this group. You cannot modify or delete this group.
- Default — This is the default upgrade group to which the appliance automatically assigns grid members. If you do not explicitly assign a member to an upgrade group, it remains in the Default group. You cannot delete or rename this group. For information, see Modifying Upgrade Groups on page 275.

Grid Manager provides information about the upgrade group to which a member belongs. You can add or delete an upgrade group and monitor the software version that is currently running on the grid and on individual member. You can do the following:

- Add an upgrade group, as described in Adding Upgrade Groups.
- Modify an upgrade group, as described in Modifying Upgrade Groups on page 275.
- View upgrade group information, as described in Viewing Upgrade Groups on page 276.
- Delete an upgrade group, as described in Deleting Upgrade Groups on page 276.

Adding Upgrade Groups

When you create an upgrade group, you select the grid members for that group, and specify whether the software distribution and upgrade occur on all group members at the same time, or successively in the order they are listed in the group members list. A grid member can belong to only one upgrade group.

Note: Infoblox recommends that you assign DHCP failover peers to separate upgrade groups to minimize the risk of a loss in DHCP services. For example, if DHCP failover peers are in the same upgrade group and its members upgrade simultaneously, the upgrade causes a loss in DHCP services. Note that the appliance displays a warning message when you create an upgrade group that includes DHCP failover peers. To minimize the risk of a loss in DNS services, put the name servers for a zone in different upgrade groups, and assign the primary and secondary servers to separate upgrade groups.

To add an upgrade group:

1. From the Grid tab, select the Upgrade tab.
2. Click Toggle Group List View to display the list of upgrade groups, and then click the Add icon.
3. In the Add Upgrade Group wizard, complete the following:
   - Name: Enter a name for the upgrade group. The name can contain alphanumeric characters, spaces, underscores, hyphens, and dashes.
   - Distribute to Members: Select one of the following to specify how the grid master distributes software to the members in the group.
     - Simultaneously: Select this to distribute software upgrade files to all group members at the same time.
     - Sequentially: Select this to distribute software upgrade files to group members in the order they are listed in the group members list.
Managing Upgrade Groups

— **Upgrade Members**: Select one of the following to specify how the group members upgrade to the new software version.
  — **Simultaneously**: Select this to upgrade all group members at the same time.
  — **Sequentially**: Select this to upgrade group members in the order they are listed in the group members list.
— **Comment**: Enter useful information about the upgrade group, such as the location of the group.

4. Click **Next** to select members for the group. Complete the following:
   — Click the **Add** icon. Grid Manager adds a row to the Member Assignment table.
   — Click **Select**. In the **Member Selector** dialog box, select the members you want to add to the group, and then click the **Select** icon. Use Shift+click and Ctrl+click to select multiple members. Note that if you choose to distribute and upgrade members sequentially, the distribution and upgrade occur in the order the members are listed. You can reorder the list by dragging a member to a desired location or by selecting a member and using the up and down arrows next to the check box to place the member at a desired location. You can also delete a member from the list.

   **Note:** After you add a member, the appliance adds it to the group members list. The first grid member in the list determines the time zone of the group when you schedule the distribution and upgrade. Therefore, Grid Manager displays the time zone of the first grid member in the list. (For information about setting time zones, see **Managing Time Settings** on page 203.)

5. Select one of the following:
   — **Save & Close**: Save the entry and close the wizard.
   — **Save & Edit**: Save the entry and continue to edit.
   — **Save & New**: Save the entry and open a new wizard.

**Modifying Upgrade Groups**

You can modify an existing upgrade group to change the group name or how the distribution and upgrade are performed. You can also add and delete members.

To modify an upgrade group:
1. From the **Grid** tab, select the **Upgrade** tab, and then click **Toggle Group List View**.
2. Select an **upgrade_group** check box, and then click the **Edit** icon in the row. You can also click the Edit icon directly without selecting the check box.
3. The **Upgrade Group** editor provides the following tabs from which you can modify data:
   — **General**: Modify the fields as described in **Adding Upgrade Groups** on page 274.
   — **Member Assignment**: Add or delete members as described in **Adding Upgrade Groups** on page 274.
4. Click **Save & Close** or **Save**.
Viewing Upgrade Groups

In the Upgrade tab, Grid Manager lists the Grid Master group, the Default group, and other upgrade groups you have configured. You cannot modify or delete the Grid Master group. You can modify the Default group, but you cannot delete it. To view the members in a specific upgrade group, click the arrow next to the group name to expand the group. All groups are collapsed by default.

Before a distribution or upgrade starts, you can move members from one group to another, reorder the members, or remove a member from an upgrade group. The member you remove automatically joins the Default group. (For information, see Managing Distributions on page 281.) You cannot add, delete, or reorder members in an upgrade group while a distribution or upgrade is in progress. You can skip a member in an upgrade group from a distribution only before the distribution starts, or after you pause it. For information, see Pausing and Resuming Distributions on page 281.

To view the upgrade groups in a grid:
1. From the Grid tab, select the Upgrade tab, and then click Toggle Group List View.
   
   Grid Manager displays the Grid Master at the top of the list. All other upgrade groups are listed alphabetically after the Grid Master. You can click the arrow next to a group to view members in the group.

2. Grid Manager displays the following:
   - **Group**: The name of an upgrade group to which the member belongs.
   - **Member**: The name of the member.
   - **Status**: Displays the overall status of an upgrade group at the group level and individual status for each member when you expand the upgrade group. At the group level, this displays the most severe status among the members. For example, when there are three out of five members are offline, the overall status shows **3 of 5 members** in red, which means offline.
   - **IP Address**: The IP address of the member.
   - **Running Version**: The NIOS software version that is currently running on the member.
   - **Distribution Status**: The distribution status of the group.
   - **Timestamp**: The date, time, and time zone when a distribution or upgrade is complete.

You can hide some of the default columns, but you cannot sort the information in this table.

Deleting Upgrade Groups

When you delete an upgrade group, members in the upgrade group that you want to delete will be moved to the Default group. Grid Manager displays a warning before deleting an upgrade group.

To delete an upgrade group:
1. From the Grid tab, select the Upgrade tab, and then click Toggle Group List View.
2. Select an upgrade-group check box, and then click the Delete icon.
3. In the Delete Confirmation dialog box, click Yes.
Viewing Software Versions

Before you upgrade, downgrade, or revert to a different NIOS software version, you can view the current software version that is running on the grid, the NIOS image you have uploaded, and the available version to which you can revert. Grid Manager displays the software information in the Upgrade tab.

To view software information:
1. From the Grid tab, select the Upgrade tab.
2. Grid Manager displays the following in the Grid Version Information section:
   - **Running**: The NIOS software version that is currently running on the grid.
   - **Uploaded**: The latest NIOS image file you have uploaded and is available for distribution.
   - **Distribution**: The NIOS software version used for distribution or is available for distribution.
   - **Alternate Version**: The NIOS software version to which the appliance can revert.

   **Note**: Grid Manager leaves a field empty when there is no available software for the specific function.

Grid Manager automatically refreshes the Upgrade tab with the latest information and displays the timestamp in the Last Updated field below the Grid Version Information section.
Managing NIOS Software and Configuration Files

**Upgrading NIOS Software**

Infoblox frequently releases updated NIOS software. Contact Infoblox Technical Support to learn which file name to use when downloading a new upgrade file, or watch your email for periodic notifications that a new software upgrade is available. To get the latest upgrade, your local network must be capable of downloading a file from the Internet. After you download and store the new upgrade file on your local network, complete the following tasks to upgrade an Infoblox independent appliance or a grid.

- Upload the new software to the grid master, as described in *Uploading NIOS Software*.
- Distribute the software upgrade files, as described in *Distributing Software Upgrade Files* on page 279.
- Optionally, test the upgrade, as described in *Testing Software Upgrades* on page 282.
- Perform the software upgrade, as described in *Performing Software Upgrades* on page 282.

Before upgrading, Infoblox recommends that all members in the grid be connected to the network and operating normally. If one or more members are offline when you upgrade the grid, they automatically receive the distributed software and upgrade when they join the grid or come back online.

**Note:** You cannot upgrade directly to NIOS 5.x from NIOS releases less than 4.2r4. Refer to the release notes for the appropriate upgrade and revert paths.

Before you upgrade to a later NIOS release, use the `show upgrade_compatible` command to check if your grid is compatible with the release. For information about using this command, refer to the *Infoblox CLI Guide*.

**Caution:** Do not attempt to add or remove a member, or convert an HA pair to single members or vice versa during a distribution or upgrade.

**Lite Upgrades**

Whenever possible, the appliance uses the lite upgrade mode to speed up the upgrade process. A lite upgrade occurs when there are incremental changes to the software that do not require any change to the database. The appliance can perform a lite upgrade only if the format of the database between the existing NIOS version and the upgrade version is the same.

In general, when you upgrade from a patch release to another patch release, you are performing a lite upgrade. You can schedule a lite upgrade, but you cannot test a lite upgrade. The appliance disables the testing function for lite upgrades.

**Uploading NIOS Software**

After you download the NIOS software upgrade to your management station, upload it to the grid master, as follows:

1. From the **Grid** tab, select the **Upgrade** tab, and then click **Upload** in the panel or from the Toolbar.
2. Navigate to the directory where you have stored the NIOS software upgrade, and then click **Open** or **Upload**.
   
   The appliance uploads the file and displays the status of the upload in the status bar. You can click the Stop icon in the status bar to stop the upload. Ensure that you do not navigate away from the **Upgrade** tab until after the upload is complete. Otherwise, the upload process stops.

**Note:** When you upload the NIOS software upgrade to an HA grid master, only the active node receives the software. The passive node does not. Therefore, if the grid master fails over before a distribution starts, you must upload the software again. If you do not, the distribution fails because the new active node does not have the uploaded software.
Distributing Software Upgrade Files

Distributing the software upgrade files involves unpacking the software files and loading the new software. When you perform a distribution, the NIOS appliance loads the new software code into an alternate disk partition, which overwrites any previously saved version of code that is already there. Therefore starting the distribution disables the appliance from reverting to a release prior to the current version.

The time this process takes depends on the number of appliances to which the software is distributed; the more appliances, the longer it takes. Therefore, you might want to schedule the grid distribution during times when your network is less busy. You can distribute the software immediately or schedule the distribution of any software upgrade file, even if it is not Upgrade Lite compatible.

Distributing Software Immediately

The grid master distributes the software upgrade to each member in the grid, including itself. As an alternative to scheduling the grid distribution (see Scheduling Distributions on page 279), you can distribute the software upgrade throughout the grid immediately, as follows:

1. From the Grid tab, select the Upgrade tab, and then click Distribute -> Distribute Now from the Toolbar.
2. In the confirmation dialog box, click Yes to start the distribution.

   The distribution starts and if there is an active distribution scheduled, the appliance changes its status to inactive. The appliance distributes the upgrade files and displays the status of the distribution in the status bar. You can pause, resume, or stop the distribution by clicking the corresponding icon in the status bar. For information, see Managing Distributions on page 281.

   Note that starting a manual distribution cancels a scheduled distribution.

Scheduling Distributions

When you schedule a distribution, you schedule the distribution of the grid master as well as the upgrade groups, including the Default group. The grid master distribution must always occur before the distribution of the upgrade groups.

To schedule a software distribution:

1. From the Grid tab, select the Upgrade tab, and then click Distribute -> Schedule Distribution from the Toolbar.
2. In the Schedule Distribution editor, complete the following:
   - **Activate Distribution Schedule**: Select this to enable the distribution schedule. Clear it if you are creating a distribution schedule you plan to activate at a later date. You can configure and save information in this editor even when you deactivate a scheduled distribution.
   - **Grid Master Distribution Start Information**: Enter a grid master distribution date, time, and time zone. The distribution date and time must be before those of the upgrade groups.
     - **Date**: Enter a start date of the grid master distribution in YYYY-MM-DD (year-month-day) format. You can click the calendar icon to select a date from the calendar widget.
     - **Time**: Enter a start time of the grid master distribution in hh:mm:ss AM/PM (hour:minute:second in AM or PM) format. You can also select a time from the drop-down list.
     - **Time Zone**: Select a time zone that applies to the start time you enter. If this time zone is different from the grid time zone, the appliance converts the time you enter here based on the grid time zone, after you save this schedule. When you display this schedule again, it displays the converted time. Selecting the time zone here does not affect any time zone settings in the grid. (For information about selecting the grid and member time zones, see Managing Time Settings on page 203.)
     - **Admin Local Time**: Displays the grid master distribution start date and time in the time zone of the administrator, as explained in Creating Local Admins on page 95.
In the upgrade group table, specify the following for each upgrade group by clicking the corresponding field in each row:

- **Start Distribution**: Specify when the distribution occurs. Select one of the following from the drop-down list:
  - **Date/Time**: Select this to configure the distribution start date, time, and time zone.
  - **After group**: Select **After Grid Master** to start the distribution immediately after the completion of the grid master distribution. Select an upgrade group that must complete its distribution before the group you are configuring. When you select this option, you cannot enter a date, time, and time zone.

  **Date, Time, and Time Zone** are enabled only when you select **Date/Time** for **Start Distribution**.

- **Date**: Enter a distribution start date in YYYY-MM-DD (year-month-day) format. You can click the calendar icon to select a date from the calendar widget.

- **Time**: Enter a distribution start time in hh:mm:ss AM/PM (hour:minute:second in AM or PM) format. You can select a time from the drop-down list.

- **Time Zone**: By default, the appliance displays the time zone of the first grid member in the Upgrade Group. You can change this time zone if you want to enter the time using a different time zone. After you save the schedule though, the appliance converts the time you entered to the time zone of the upgrade group, if it is different. (For information about setting the grid and member time zones, see **Managing Time Settings** on page 203.) To change the default time zone of the upgrade group, change the time zone of the first group member, as explained in **Adding Upgrade Groups** on page 274.

- **Admin Local Time**: Displays the start date and time in the time zone of the administrator, as explained in **Creating Local Admins** on page 95.

- **Distribute to Members**: Indicates whether the distribution within the group occurs simultaneously or sequentially. You cannot edit this field here. You define this when you create the upgrade group. To change this setting, see **Modifying Upgrade Groups** on page 275.

3. Select **Save & Close** or **Save**.

Grid Manager confirms that the schedule is saved and indicates whether the distribution schedule is active. It also displays a warning message if an upgrade group contains members in the same DHCP failover association.

Note that the appliance does not save the schedule and displays an error message if the schedule contains the following:

- Circular dependencies between upgrade groups. For example, the distribution of Group A is scheduled after Group B, and the distribution of Group B is scheduled after Group A.
- The distribution time is in the past.

Software Distribution Process

The following series of events occur after a grid distribution starts:

- The appliance checks if a NIOS software upgrade was uploaded.
  - If the upgrade files are not uploaded, the distribution stops. The appliance displays an error message and if the distribution is scheduled, the appliance deactivates the distribution schedule.
  - If the upgrade files are uploaded, the distribution proceeds.

- A single grid master uploads the file to a backup partition and unpacks the contents, which overwrites any existing backup software that might have been there. For an HA grid master, it is the active node that uploads the file to a backup partition and unpacks the contents.
  - The grid master (or active node of the HA grid master) sends a command to all nodes that are online to copy their database and software to a backup software partition.
  - For an HA grid master, the active node sends the command to the passive node as well.
  - The nodes perform resynchronization on their backup partition, retrieving only the changed files from the grid master.
  - After the active node of an HA member receives the software, it then distributes it to the passive node.
When the distribution successfully completes, the appliance updates the distribution status and sets the schedule, if configured, to inactive. The new software is now staged on all member appliances and is ready for use. Grid Manager displays the software version in the Distribution field in the Grid Version Information section.

Managing Distributions

After you start a distribution, you can pause, resume, or stop it. For information, see Pausing and Resuming Distributions on page 281 and Stopping Distributions on page 281. Grid Manager displays the status of the overall distribution as well as the status of individual members. You can view this information in the Upgrade tab.

Pausing and Resuming Distributions

The following are some operational guidelines for performing a distribution:

- You cannot create new upgrade groups, add members to a group, or remove members from a group after a distribution starts.
- You can skip a member that is currently offline from a distribution. When both nodes of an HA pair are online, the skip member function is not available.

To pause a distribution:

1. From the Grid Distribution Status bar, click the Pause icon.
2. When the appliance displays a confirmation dialog box, click Yes to pause the distribution.

To skip a member from a distribution:

1. From the Grid tab, click the Upgrade tab, and then click Toggle Member List View.
2. Select a member check box, and then click Skip Member from the Toolbar. Grid Manager automatically skips the distribution of software to the members that are offline.

To resume a distribution:

1. From the Grid Distribution Status bar, click the Resume icon.
2. When the appliance displays a confirmation dialog box confirming that you want to resume the distribution, click Yes to continue.

Members that have not completed or started distributions that were scheduled at an earlier time resume the distribution.

Stopping Distributions

You can stop a distribution immediately, for example, if there are offline members and you do not want to wait for them to come back online, or if you realize that you have uploaded the wrong software version. When you stop a distribution, you can do the following:

- If the grid master has completed its distribution, you can upgrade the grid immediately. This forces members that do not have a complete distribution to synchronize their releases with the grid master.
- If the grid master does not have a valid distribution, you can restart the distribution.
- Upload another software upgrade.

Ending a distribution does not affect the upgrade schedule, if configured. The grid upgrade starts as scheduled, as long as the grid master completes its distribution.

To stop a distribution:

1. From the Grid Distribution Status bar, click the Stop icon.
2. When the appliance displays a confirmation dialog box confirming that you want to stop the distribution, click Yes to continue.
Testing Software Upgrades

After you successfully distribute a software upgrade to the grid master, you can test an upgrade on the grid master before actually implementing it. This allows you to resolve potential data migration issues before the actual upgrade. The length of time the upgrade test takes depends on the amount of data and the difference between the current NIOS version and the software upgrade. The test does not affect NIOS services and you can perform other administrative tasks during the upgrade test.

To start an upgrade test:

- From the Grid tab, select the Upgrade tab, and then click Test Upgrade from the Toolbar. Test upgrade is enabled only for a major upgrade (not an Upgrade Lite compatible upgrade).

After you start an upgrade test, you can view its status in the status bar. You can also stop it at anytime.

To stop an upgrade test:

- From the Grid Upgrade Test Status bar, click the Stop icon.

Note that if an admin restarts the grid services or reboots the grid master, or if an HA failover occurs on the grid master during the upgrade test, the appliance automatically stops the test. The appliance always resets the status of the grid to “Distributed” when it stops the upgrade test.

If the appliance encounters an error during the test, it stops the test and displays a message in the Upgrade Status panel indicating that the upgrade test failed and the reason for the failure, such as a data translation error or data import error. You can review the syslog for specific error messages before downloading the Support Bundle and contacting Infoblox Technical Support.

After the test successfully finishes, the appliance displays a message confirming that the test upgrade is complete. You can then perform the actual upgrade as described in Performing Software Upgrades on page 282.

Performing Software Upgrades

Performing a software upgrade involves rebooting the appliances and then running the new software. Essentially, each appliance switches between the two software partitions on its system, activating the staged software and saving the previously active software and database as backup.

**Note:** Before you upgrade the software, Infoblox recommends that you back up the current configuration and database. For information, see Backing Up Files on page 289.

When upgrading to software releases that are Upgrade Lite compatible, you can schedule the grid upgrade as described in Scheduling Upgrades on page 283.

Upgrading Immediately

You cannot schedule upgrades to releases that are not Upgrade Lite compatible. The grid members must upgrade at the same time when upgrading to these releases. For Upgrade Lite compatible releases, you can schedule the upgrade as described in Scheduling Upgrades on page 283, or upgrade the grid at the same time.

To upgrade a grid immediately:

- From the Grid tab, select the Upgrade tab, and then click Upgrade -> Upgrade Now from the Toolbar.

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

When you schedule the upgrade of a grid to an Upgrade Lite compatible release, you schedule the upgrade for the grid master and the upgrade groups, including the Default group. The grid master must always upgrade before the upgrade groups. To schedule an upgrade:

1. From the Grid tab, select the Upgrade tab, and then click Upgrade→Schedule Upgrade from the Toolbar.
2. In the Upgrade Schedule editor, complete the following:
   - **Activate Upgrade Schedule**: Select this to enable the upgrade schedule. Clear it if you are creating an upgrade schedule that you plan to activate at a later date. You can configure and save information in this editor even when you deactivate a distribution.
   - **Grid Master Upgrade Start Information**: Enter a grid master upgrade date, time, and time zone. The date and time must be before those of the upgrade groups.
     - **Date**: Enter a start date of the grid master upgrade in YYYY-MM-DD (year-month-day) format. You can click the calendar icon to select a date from the calendar widget.
     - **Time**: Enter a start time of the grid master upgrade in hh:mm:ss AM/PM (hour:minute:second in AM or PM) format. You can select a time from the drop-down list.
     - **Time Zone**: Select a time zone that applies to the start time you enter. If this time zone is different from the grid time zone, the appliance converts the time you enter here based on the grid time zone, after you save the schedule. When you display this schedule again, it displays the converted time. Selecting the time zone here does not affect any time zone settings in the grid. (For information about setting the grid and member time zones, see Managing Time Settings on page 203.)
   - **Admin Local Time**: Displays the grid master upgrade date and start time in the time zone of the administrator, as explained in Creating Local Admins on page 95.
   - In the upgrade group table, specify the following for each upgrade group by clicking the corresponding field in each row:
     - **Start Upgrade**: Specify when the upgrade occurs. Select one of the following from the drop-down list:
       - **Date/Time**: Select this to configure the upgrade start date, time, and time zone.
       - **After <group>**: Select After Grid Master to start the distribution immediately after the completion of the grid master distribution. Select an upgrade group that must complete its distribution before the group you are configuring. If you select this option, you cannot enter a date, time, and time zone.
       - **Date**: Enter an upgrade start date in YYYY-MM-DD (year-month-day) format. You can click the calendar icon to select a date from the calendar widget.
       - **Time**: Enter an upgrade start time in hh:mm:ss AM/PM (hour:minute:second in AM or PM) format. You can select a time from the drop-down list.
       - **Time Zone**: By default, the appliance displays the time zone of the first grid member in the Upgrade Group. You can change this time zone, if you want to enter the time using a different time zone. After you save the schedule though, the appliance converts the time you entered to the time zone of the upgrade group, if it is different. (For information about setting the grid and member time zones, see Managing Time Settings on page 203.) To change the default time zone of an upgrade group, change the first group member in the Upgrade Group list, as explained in Adding Upgrade Groups on page 274.
       - **Admin Local Time**: Displays the data and time in the time zone of the administrator, as explained in Creating Local Admins on page 95.
       - **Distribute to Members**: Indicates whether the upgrade within the group occurs simultaneously or sequentially. You cannot edit this field here. You define this when you create the upgrade group. To change this setting, see Modifying Upgrade Groups on page 275.
   - **Date, Time, and Time Zone** are enabled only when you select Date/Time for Start Upgrade.
3. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and continue to edit.
The appliance does not save the schedule and displays an error message if the schedule contains the following:

- Circular dependencies between upgrade groups; for example, the upgrade of Group A is scheduled after Group B, and the upgrade of Group B is scheduled after Group A.
- The upgrade time is in the past.

Otherwise, the appliance confirms that the schedule is saved and indicates whether the upgrade schedule is active. It also displays a warning message if an upgrade group contains members in the same DHCP failover association.

**Upgrading Groups Immediately**

After you schedule an upgrade with multiple upgrade groups, you can choose to immediately upgrade an upgrade group that has not been upgraded yet. This function is available only for scheduled upgrades.

To upgrade an upgrade group now:

1. From the **Grid** tab, select the **Upgrade** tab, and then click **Toggle Group List View**.
2. In the Group List view, click the Upgrade Group Now icon in the upgrade group row. Grid Manager immediately upgrades the selected group.
Upgrade Process

When an upgrade starts, Grid Manager checks if the nodes of an HA grid master have the same NIOS software version on their alternate partitions. If they do not have the same software version, the upgrade process stops. Grid Manager displays an error message and if it is a scheduled upgrade, Grid Manager deactivates the schedule as well. Otherwise, the upgrade process continues. During the upgrade, if a grid member has not completed its distribution, it automatically resynchronizes with the grid master after the grid master upgrade is complete.

Due to the nature of the upgrade sequence, HA pairs fail over during the upgrade. Therefore, be aware that the active and passive nodes reverse roles. The order in which grid members upgrade, including when HA pairs fail over, is shown in Figure 9.2 (for an HA grid master) and Figure 9.2 on page 286 (for a single grid master).

Figure 9.1 Upgrade Sequence for an HA Grid Master and Grid Members

![Diagram of upgrade sequence](image)

1. The passive node (Node 2) of the grid master upgrades.
2. The grid master fails over from Node 1 to Node 2. At this point, the active grid master (Node 2) is using the upgraded code. All other nodes, including the passive node (Node 1) and all grid members, rejoin the newly updated active node (Node 2). Since the NIOS version on these nodes does not match that of the active grid master, the nodes are directed to upgrade.
3. Node 1 (now passive) of the grid master upgrades. The passive node (Node 2) of the HA member and the single grid member upgrade.
4. The HA grid member fail overs from Node 1 to Node 2.
5. Node 1 (now passive) of the HA member upgrades.

Note: Grid members that do not have the correct NIOS version on their alternate partitions due to an incomplete distribution automatically resynchronize the NIOS version with the grid master, and then upgrade.
The Grid Manager session terminates when the HA grid master fails over from Node 1 to Node 2, or when the single grid master reboots and goes offline.

During a scheduled upgrade, the grid members that have not upgraded yet can join the grid and function normally until their scheduled upgrade time. When the upgrade finishes, the upgrade schedule is set to inactive.

Figure 9.2 Upgrade Sequence for a Single Grid Master and Grid Members

1. Single grid master upgrades. All other members rejoin the newly updated grid master. Since the NIOS version on these nodes does not match that of the grid master, the nodes are directed to upgrade.

2. Node 2 (passive) of the HA member and the single member upgrade.

3. The HA member fails over from Node 1 to Node 2.

4. Node 1 (now passive) of the HA member upgrades.
Monitoring Distribution and Upgrade Status

During a distribution or an upgrade, Grid Manager displays the status of the distribution or upgrade in the status bar. It also displays the process status for each member. You can view the status in either the Member List view or Group List view from the Grid tab → Upgrade tab.

When you perform a distribution or an upgrade, the status bar displays the overall grid distribution status with a progress bar that describes the process being performed. The status bar also displays the number of members that have completed the distribution or upgrade.

A difference between a distribution and an upgrade process is that during an upgrade, the Grid Manager session terminates when an HA grid master fails over from Node 1 to Node 2, or when a single grid master reboots and goes offline. You can log back in to the appliance after the upgrade.

Grid and Member Status

You can view the distribution and upgrade process status at the grid and member level. To view the process status, from the Grid tab, select the Upgrade tab, and then click Toggle Member List View.

The status bar displays the status of the overall grid process. It contains a progress bar that indicates the percentage of completion. It also shows the number of members that have completed the process.

Grid Manager displays the following information for each member:

- **Member**: The name of the grid member.
- **Group**: The upgrade group to which the member belongs.
- **HA**: Indicates whether the member is an HA pair or not.
- **Status**: The current distribution or upgrade status. This can be Running (green) or Offline (red).
- **IP Address**: The IP address of the member.
- **Running Version**: The NIOS software version that is currently running on the member.
- **Alternate Version**: Displays the NIOS software version to which the appliance can revert.
- **Distribution/Upgrade Status**: The current distribution or upgrade status. When the distribution or upgrade is in progress, Grid Manager displays a progress bar in this field to indicate the percentage of completion.
- **Hotfix**: The name of the hotfix that was last run on the member.
- **Timestamp**: The date, time, and time zone of the status displayed.
- **Site**: The location to which the member belongs. This is one of the predefined extensible attributes.

The appliance automatically refreshes the information in this panel.

Upgrade Group Status

You can view the distribution or upgrade status of an upgrade group in the group list view. In this view, the distribution or upgrade status rolls up to the group level. You can expand an upgrade group to view the status of individual member. However, you cannot view detailed status of a selected member from this view.

To view the process status of an upgrade group, from the Grid tab, select the Upgrade tab, and then click Toggle Group List View. Grid Manager displays the following information for each member in an upgrade group:

- **Group**: The upgrade group to which the member belongs.
- **Member**: The name of the grid member.
- **Status**: The current member status. This can be Running (green) or Offline (red).
- **IP Address**: The IP address of the member appliance.
- **Running Version**: The NIOS software version that is currently running on the member.
- **Distribution Status**: The current distribution status. For an upgrade group, Grid Manager displays a progress bar to indicate the overall percentage of completion. For a member, Grid Manager displays the state of the distribution process.
- **Timestamp**: The date, time, and time zone of the status displayed.
**Detailed Status**

You can view detailed process information of a member during a distribution or an upgrade.

To view detailed process information:

1. From the Grid tab, select the Upgrade tab, and then click **Toggle Member List View**.
2. Select a member and then click the Detailed Status icon.

Grid Manager displays a panel that shows the required steps during a distribution or an upgrade. It also displays a color indicator, next to each step, to indicate the current status of each step. The color indicator can be one of the following:

   - Grey: The process has not started yet.
   - Green: The process is complete.
   - Blue: The distribution or upgrade that is in progress.
   - Red: There is an error; Grid Manager displays a description of the problem.
   - Yellow: A warning message.

When the selected member is an HA pair, Grid Manager displays the status information for both nodes. The panel remains open until you close it or select a different member.

---

**Downgrading Software**

Each Infoblox appliance model has a minimum required release of Infoblox software. Before downgrading an appliance, refer to the document, *Minimum Required Release Software for Hardware Platforms*, that shipped with your product.

The downgrade procedure is for single independent appliances only. Infoblox does not support software downgrades for grid members, but you can revert to the previous NIOS release (see the next section) on a grid master.

Caution: Although the downgrade process preserves license information and basic network settings, it does not preserve data. After you complete the downgrade procedure, all data in the database is lost.

To downgrade software on a single independent appliance running NIOS 4.0 or later:

1. From the Grid tab, select the Upgrade tab, and then click **Downgrade** from the Toolbar.
   
   Grid Manager displays a warning indicating that reverting to the current release is not possible once you start the downgrade. Read the warning carefully, and then click **Yes** to confirm your decision to downgrade.

2. In the **Choose file** dialog box, navigate to the downgrade image file, and then click **Open** to upload the file. The appliance uploads the file to the Grid Master. You cannot stop the downgrade process once you start it. Grid Manager displays the downgrade status in the status bar.
Reverting to the Previously Running Software Version

You can revert to a version of software that was previously running on your NIOS appliance. The NIOS appliance stores the previous software version in its backup software partition. You can see if there is a software version to which you can revert and its version number in the Alternate Version column in the Grid Version Information section of the Upgrade tab. To view the software version, from the Grid tab, select the Upgrade tab. Note that once you start distributing a new NIOS version after an upgrade, you cannot revert to a previous NIOS version.

Be aware that when you revert to this software, changes made since the grid was last upgraded are lost, including the new DHCP leases and other DNS changes.

To revert to a version of software previously running on a grid or on an independent appliance or HA pair:

- From the Grid tab, select the Upgrade tab, and then click Revert from the Toolbar.

  Grid Manager displays a warning indicating that the revert process disrupts grid services. Read the warning carefully, and then click Yes to confirm your decision to revert.

Backing Up and Restoring Configuration Files

You can back up your system files locally on the appliance or to your management system, or use TFTP (Trivial File Transfer Protocol), FTP (File Transfer Protocol), or SCP (Secure Copy) to back them up to a remote server. You can also download a backup file to your workstation. The backup file is a .bak file that contains the configuration settings, data set, and TFTP files.

The following sections describe how to use the backup and restore functions:

- **Backing Up Files**
- **Automatically Backing Up Data Files** on page 290
- **Manually Backing Up Data Files** on page 292
- **Restoring Backup Files** on page 293
- **Downloading Backup Files from a Different Appliance** on page 294

Note: Infoblox highly recommends that you always back up the current configuration file before upgrading, restoring, or reverting the software on the appliance.

Backing Up Files

You can back up system files periodically and on demand. You can then restore the files on the same appliance or on a different appliance. For information about restoring files, see Restoring Backup Files on page 293. You can configure the appliance to automatically back up the files on a weekly, daily, or hourly basis.

Infoblox recommends that you back up the system files during off-hours to minimize the impact on network services. By default, the automatic backup function is turned off. You must log in with a superuser account to back up files.

You can back up system files to the following:

- A local directory
- The management system that you use to operate the appliance
- A TFTP server
- An FTP server. This option requires that you have a valid username and password on the server prior to backing up files.
- An SSH server that supports SCP. This option requires that you have a valid username and password on the server prior to backing up files.
Local Backup

You can store a backup file on the appliance itself. However, Infoblox recommends that you store backup files in an alternate location. When you back up the system files locally, the appliance uses the following format to name the file: Infoblox_year_month_day_time. For example, a file name of Infoblox_2008_11_30_23_00 means that the file is backed up on November 30th, 2008 at 11:00 PM.

The appliance can save up to 20 configuration files, regardless of how often the files are saved (weekly, hourly, or daily). Ensure that you take the size of the configuration file into consideration when backing up files because the storage limit on an appliance is 5 Gb (gigabytes). If your configuration file is 500 Mb (megabytes), then the appliance can store 10 configuration files. When uploading configuration files on to a TFTP, FTP, or SCP server, you must consider the file size on that server as well.

Using TFTP

TFTP is a client-server protocol that uses UDP as its transport protocol. It does not provide authentication or encryption, therefore it does not require a username or password.

When you back up the system files to a TFTP server, you select the backup file you want to download, enter the name in which the file is stored on the TFTP server and the server IP address.

Using FTP

FTP is a client-server protocol used to exchange files over TCP-based networks. The appliance, as the FTP client, connects to a remote FTP server that you identify. When you use FTP to back up the system files, the password and file contents are transmitted in clear text and may be intercepted by other users.

When you back up the system files to an FTP server, the appliance, as the FTP client, logs on to the FTP server. You must specify the username and password the appliance uses to log on to the FTP server. The user account must have write permission to the directory to which the appliance uploads the backup file.

Using SCP

SCP is more secure than TFTP and FTP. It uses the SSH protocol to provide authentication and security. You can use SCP to back up the NIOS system files to a server running SSHv2.

When you use SCP to back up the system files to an SSH server, you must specify the username and password the appliance uses to log on to the server. The user account must have write permission to the directory to which the appliance uploads the backup file. In addition, make sure that you enter the correct IP address of the SSH server; the appliance does not check the credentials of the SSH server to which it connects.

Automatically Backing Up Data Files

Infoblox recommends that you back up your configuration files regularly, and the easiest way to accomplish this task is to configure the appliance to back up the configuration file automatically. You can choose when and how often files are backed up: weekly, daily, or hourly. When you automatically back up a configuration file on the appliance, the file is named in the format Infoblox_year_month_day_time. The default time for an automatic backup is 3:00 AM.

Configuration files should be backed up during the slowest period of network activity.

To automatically back up a database file on an independent appliance or grid master:

1. From the Grid tab, select the Grid Manager tab, and then click Backup -> Schedule Backup from the Toolbar.
2. In the Schedule Backup dialog box, select the destination of the backup file from the Backup to drop-down list:
   - TFTP: Back up system files to a TFTP server.
     - IP Address of TFTP Server: Enter the IP address of the TFTP server to which you want to back up the system files.
     - Directory Path: Enter the directory path of the file. For example, you can enter /archive/backups on a Linux system, or c:\archive\backups on a Microsoft Windows system. The directory path cannot contain spaces. The folder or directory you enter here must already exist on the specified server. Do not include the file name in the directory path.
— **Recurrence**: Select how often you want to back up the files. You can select **Weekly**, **Daily**, or **Hourly** from the drop-down list. When you select **Weekly**, complete the following:
  * **Every**: Choose a day of the week from the drop-down list.
  * **Time**: Enter a time in the hh:mm:ss AM/PM format. You can also click the clock icon and select a time from the drop-down list. The grid master creates a backup file on the selected day and time every week.

When you select **Daily**, enter a time in the hh:mm:ss AM/PM format. You can also select a time from the drop-down list.

When you select **Hourly**, complete the following:
  * **Minutes after the Hour**: Enter the minute after the hour when the grid master creates a backup file. For example, enter 5 if you want the grid master to create a backup file five minutes after the hour every hour.

— **Disable Scheduled Backup**: Select this if you want to disable automatic backups from occurring now. You can still save the settings for future use.

— **FTP**: Back up system files to an FTP server.
  — **IP Address of FTP Server**: The IP address of the FTP server.
  — **Directory Path**: Enter the directory path of the file. For example, you can enter `/archive/backups` on a Linux system, or `c:\archive\backups` on a Microsoft Windows system. The directory path cannot contain spaces. The folder or directory you enter here must already exist on the specified server. Do not include the file name in the directory path.
  — **Username**: Enter the username of your FTP account.
  — **Password**: Enter the password of your FTP account.
  — **Recurrence**: Select how often the scheduled backups should occur. You can select **Weekly**, **Daily**, or **Hourly**. For information, see TFTP.
  — **Disable Scheduled Backup**: Select this if you want to disable automatic backups from occurring now, but want to save the settings for future use.

— **SCP**: Back up system files to an SSH server that supports SCP.
  — **IP Address of SCP Server**: The IP address of the SCP server.
  — **Directory Path**: Enter the directory path of the file. For example, you can enter `/archive/backups` on a Linux system, or `c:\archive\backups` on a Microsoft Windows system. The directory path cannot contain spaces. The folder or directory you enter here must already exist on the specified server. Do not include the file name in the directory path.
  — **Username**: Enter the username of your SCP account.
  — **Password**: Enter the password of your SCP account.
  — **Recurrence**: Select how often the scheduled backups should occur. You can select **Weekly**, **Daily**, or **Hourly**. For information, see the TFTP section.
  — **Disable Scheduled Backup**: Select this if you want to disable automatic backups from occurring now. You can still save the settings for future use.

---

**Note**: When you select **FTP** or **SCP**, ensure that you have a valid username and password on the server prior to backing up the files.

— **Grid Master (Local)**: Back up to a local directory on the grid master. This is the default.

  By default, the grid master generates a backup file and saves it locally in its own storage at 3:00 AM daily. Be aware that backing up the grid and saving it locally on an hourly basis increases the turnover of files stored on the grid master. Backing it up hourly to a remote server increases the overall amount of traffic on your network.

3. Click **Save & Close**.
Manually Backing Up Data Files

You can manually back up a data file in addition to scheduling your backups.

To back up manually:

1. From the Grid tab, select the Grid Manager tab, and then click Backup → Manual Backup from the Toolbar.
2. In the Backup wizard, select the destination of the backup file from the Backup to drop-down list:
   - My Computer: Back up system files to a local directory on your computer. This is the default.
   - TFTP: Back up system files to a TFTP server.
     - Filename: Enter the directory path and the file name of the backup file. For example, you can enter /archive/backups/Infoblox_2009_10_20_15_30 on a Linux server, or c:\archive\backups\Infoblox_2009_10_20_15_30 on a Microsoft Windows server.
     - IP Address of TFTP Server: Enter the IP address of the TFTP server to which you want to back up the system files.
   - FTP: Back up system files to an FTP server.
     - Filename: Enter the directory path and the file name of the backup file. For example, you can enter /archive/backups/Infoblox_2009_10_20_15_30 on a Linux server, or c:\archive\backups\Infoblox_2009_10_20_15_30 on a Microsoft Windows server.
     - IP Address of FTP Server: The IP address of the FTP server.
     - Username: Enter the username of your FTP account.
     - Password: Enter the password of your FTP account.
   - SCP: Back up system files to an SSH server that supports SCP.
     - Filename: Enter the directory path and the file name of the backup file. For example, you can enter /archive/backups/Infoblox_2009_10_20_15_30 on a Linux server, or c:\archive\backups\Infoblox_2009_10_20_15_30 on a Microsoft Windows server.
     - IP Address of SCP Server: The IP address of the SCP server.
     - Username: Enter the username of your SCP account.
     - Password: Enter the password of your SCP account.

Note: When you select FTP or SCP, ensure that you have a valid username and password on the server prior to backing up the files.

3. Click Backup.

Downloading Backup Files

You can save an existing backup file, or create and save a new one to your local management system, a TFTP server, an FTP server, or a SCP server.

To download an existing backup file:

1. From the Grid tab, select the Grid Manager tab, and the click Backup → Manage Local Backup from the Toolbar.
   Grid Manager displays the current backup files in the Manage Local Backups dialog box.
2. To download a backup file, select the check box of a backup file, and then click the Transfer icon. You cannot select multiple files for downloading.
3. Select one of the following from the Backup to drop-down list:
   - My Computer: Backup to a local directory on your computer. This is the default.
   - TFTP: Save the backup file to a TFTP server.
     - Filename: Enter the directory path and the file name of the backup file. For example, you can enter /archive/backups/Infoblox_2009_10_20_15_30 on a Linux server, or c:\archive\backups\Infoblox_2009_10_20_15_30 on a Microsoft Windows server.
Backing Up and Restoring Configuration Files

— **IP Address of TFTP Server**: Enter the IP address of the TFTP server to which you want to save the backup file.

— **FTP**: Save the backup file to an FTP server.
  
  — **Filename**: Enter the directory path and the file name of the backup file. For example, you can enter /archive/backups/Infoblox_2009_10_20_15_30 on a Linux server, or c:\archive\backups\Infoblox_2009_10_20_15_30 on a Microsoft Windows server.

— **IP Address of FTP Server**: The IP address of the FTP server.

— **Username**: Enter the username of your FTP server account.

— **Password**: Enter the password of your FTP server account.

— **SCP**: Save the backup file to an SSH server that supports SCP.
  
  — **Filename**: Enter the directory path and the file name of the backup file. For example, you can enter /archive/backups/Infoblox_2009_10_20_15_30 on a Linux server, or c:\archive\backups\Infoblox_2009_10_20_15_30 on a Microsoft Windows server.

— **IP Address of SCP Server**: The IP address of the SCP server.

— **Username**: Enter the username of your SCP server account.

— **Password**: Enter the password of your SCP server account.

**Note**: When you select FTP or SCP, ensure that you have a valid username and password on the server prior to backing up the files.

4. Click **Transfer Copy**.

**Restoring Backup Files**

You can restore a backup file to an appliance running the same NIOS version as that of the appliance from which the backup file originates. You can also restore a backup file from an appliance running a NIOS version to an appliance running a later NIOS version as long as the upgrade from the earlier NIOS version to the later version is supported. For example, you can restore a backup file from an appliance running NIOS 4.3r6-1 to an appliance running NIOS 5.0r1-0 because upgrading from NIOS 4.3r6-1 to 5.0r1-0 is supported. However, you cannot restore a backup file from an appliance running NIOS 4.1r2-1 to an appliance running NIOS 5.0r1-0 because upgrading from NIOS 4.1r2-1 to 5.0r1-0 is not supported.

You can restore an existing backup file on the appliance from which it originates, or restore a backup file from a different appliance (referred to as a forced restore). To download a backup file from a different appliance, see *Downloading Backup Files from a Different Appliance* on page 294.

You must log in with a superuser account to back up and restore files.

There are three ways to restore a backup file:

- From a local directory or the management system you use to operate the appliance
- From a TFTP server
- From a remote server using FTP. This option requires that you have a valid username and password on the FTP server prior to performing a backup or restore.

To restore a backup file to the same independent appliance or grid master:

1. From the Grid tab, select the **Grid Manager** tab, and then click **Restore** from the Toolbar.

2. In the **Restore** dialog box, choose one of the following from the **Restore from** drop-down list:
   
   — **My Computer**: Restore a file from your local computer. This is the default.
   
   — **Filename**: Click **Select File** to navigate to the configuration file.
   
   — **TFTP**: Restore a file from a TFTP server.
   
   — **Filename**: Enter the directory path and the file name you want to restore. For example, you can enter /archive/backups/Infoblox_2009_10_20_15_30 on a Linux server, or c:\archive\backups\Infoblox_2009_10_20_15_30 on a Microsoft Windows server.
Managing NIOS Software and Configuration Files

— **IP Address of TFTP Server:** Enter the IP address of the TFTP server from which you restore the configuration file.

— **FTP:** Restore a file from an FTP server.

— **Filename:** Enter the directory path and the file name of the backup file. For example, you can enter `/archive/backups/Infoblox_2009_10_20_15_30` on a Linux server, or `c:\archive\backups\Infoblox_2009_10_20_15_30` on a Microsoft Windows server.

— **IP Address of FTP Server:** The IP address of the FTP server.

— **Username:** Enter the username of your FTP server account.

— **Password:** Enter the password of your FTP server account.

• **Grid Master (Local):** Restore from a local directory on the grid master. In the Backup Set table, select the file you want to restore.

3. Click **Restore.** In the Confirm Restore dialog box, click **Yes.**
   
   After restoring the file, the appliance restarts. The restore process overwrites all existing data. All pending scheduled tasks are not restored or reverted.

4. Close your current browser window, wait a few minutes, and then reconnect to the NIOS appliance.

### Downloading Backup Files from a Different Appliance

When you “force restore” a NIOS appliance, you download a backup file from one appliance to a different appliance.

To restore a backup file to the same appliance or grid master, use the Restore function as described in **Restoring Backup Files** on page 293.

To download a backup file from one appliance to a different appliance:

1. From the Grid tab, select the Grid Manager tab, and then click **Restore** from the Toolbar.

2. In the **Restore** wizard, do the following:
   
   — **Restore from:** Choose a source from which you restore the configuration file, as described in **Restoring Backup Files** on page 293.

3. Select **Force Restore from Different Grid** to enable the feature, and then select one of the following:
   
   — **Retain Current Grid Master IP Settings** (this is the default)
   
   — **Overwrite Grid Master IP Settings**

4. Click **Restore.** In the Confirm Restore dialog box, click **Yes.**
   
   After restoring the file, the appliance reboots. The restore process overwrites all existing data. All pending scheduled tasks are not restored or reverted.

5. Close your current browser window, wait a few minutes, and then reconnect to the NIOS appliance.
Download Support Bundles

When you need assistance troubleshooting a NIOS appliance, you can log in to the appliance as a superuser, download the support bundle of the appliance, and then send it to Infoblox Technical Support for analysis. A support bundle is a tar.gz file that contains configuration files and the appliance system files. You can download a support bundle for an independent appliance and for each member in a grid. When you download a support bundle for an HA pair, it includes the files of both nodes in the HA pair.

By default, the appliance includes the following files in the support bundle: core files, current logs, and rotated logs. Because core files can be quite large and take a significant amount of time to download, Infoblox recommends that you include core files in the support bundle only when requested by Infoblox Technical Support.

To download a support bundle:

1. From the Grid tab, select a member check box, and then click Download -> Support Bundle from the Toolbar.
2. In the Download Support Bundle dialog box, select the files you want to include in the support bundle, and then click OK:
   - Core Files: Infoblox recommends that you include these files only when requested by Infoblox Technical Support.
   - Current Logs: Infoblox recommends that you always include these files in the support bundle.
   - Rotated Logs: These are rotated logs that contain historical information.
3. Navigate to the location you want to save the file and change the file name. Do not change the .tar.gz file extension in the file name.
4. Send this file to Infoblox Technical Support.
Chapter 10 Monitoring the Appliance

This chapter describes the status icons that indicate the state of appliances, services, database capacity, Ethernet ports, HA, and grid replication. It also explains how to use the various logs and the traffic capture tool to monitor a NIOS appliance.

This chapter contains the following sections:

• **Viewing Appliance Status** on page 298
  – **Grid Status** on page 298
  – **Member Status** on page 298
  – **Viewing Hardware Status** on page 303

• **Monitoring Services** on page 304
  – **Service Status** on page 304
  – **Monitoring Grid Services** on page 304
  – **Monitoring Member Services** on page 305

• **Using a Syslog Server** on page 306
  – **Specifying Syslog Servers** on page 306
  – **Configuring Syslog for Grid Members** on page 307
  – **Setting DNS Logging Categories** on page 308
  – **Viewing the Syslog** on page 309
  – **Searching in the Syslog** on page 309
  – **Downloading the Syslog File** on page 309

• **Monitoring Tools** on page 310
  – **Using the Audit Log** on page 310
  – **Viewing the Replication Status** on page 312
  – **Using the Traffic Capture Tool** on page 312
  – **Using the Capacity Report** on page 313
  – **Using the Phone Home Feature** on page 314
  – **Monitoring DNS Transactions** on page 315
  – **Viewing DNS Alert Indicator Status** on page 317
  – **Configuring DNS Alert Thresholds** on page 318
**Viewing Appliance Status**

Grid Manager provides tools for monitoring the status of the grid, members, and services. You can monitor overall grid and member status from the Dashboard, which provides a high-level view of your grid, members and IP address data, and easy access to tasks. For information, see *The Dashboard* on page 55.

Grid Manager also displays status icons to indicate the state of appliances, services, database capacity, Ethernet ports, HA, and grid replication. For the Infoblox-1552, -1852-A, -2000, and -2000-A, Grid Manager displays status icons for the power supplies. For the Infoblox-2000 and -2000-A, Grid Manager displays icons to indicate the state of the RAID array and disk controller backup battery.

You can monitor detailed status of the grid, members, and services, and then decide how to manage them. Note that when any member or service encounters issues, the appliance sends SNMP traps. For information, see *Monitoring with SNMP* on page 321.

**Grid Status**

You can monitor the overall status of the grid using the *Grid Status* widget on the Dashboard. For information, see *Grid Status* on page 57.

You can also view the grid status from the *Grid Manager* tab. To view grid status, from the *Grid* tab, select the *Grid Manager* tab. Grid Manager displays the overall grid status and status of all grid services. The grid status represents the status of the most critical members or services in the grid. When all grid members are running properly, the overall grid status is green. When one of the members has operational problems, the overall grid status is red. Grid Manager lists all grid members in the *Members* tab so you can identify which member has issues. For information, see *Member Status*.

In addition, the service bar below the grid status lists the status of all licensed services—DHCP, DNS, TFTP, HTTP (File Distribution), FTP, NTP, bloxTools—in the grid. When you click a service link, Grid Manager displays detailed information about the selected service running on all members. For information, see *Monitoring Services* on page 304. Grid Manager also provides icons you can use to edit grid properties and bookmark the page.

**Member Status**

You can monitor the overall status, such as the memory usage and system temperature, of a grid member or an independent appliance using the *Member Status (System Status)* widget on the Dashboard. For information, see *Member Status (System Status)* on page 58.

To monitor detailed status of a member, from the *Grid* tab, select the *Grid Manager* tab -> *Members* tab.

In the *Members* tab, Grid Manager displays the grid master first and then all other members in alphabetical order. If a member is an HA pair, you can click the arrow next to the member row to view information about the active and passive nodes. Grid Manager can display the following information:

- **Name**: The name of the member.
- **HA**: Indicates whether the member is an HA pair. If the member is an HA pair, Grid Manager displays the status of the HA pair.
- **Status**: The current status of the member.
- **IP Address**: The IP address of the appliance, or the VIP of an HA pair.
- **DHCP, DNS, TFTP, HTTP, FTP, NTP, bloxTools, Captive Portal**: The status icons indicate whether these services are running properly or not. For information, see *Service Status* on page 304.
- **Hardware Type**: The hardware type of the member appliance.
- **Serial Number**: The serial number of the appliance.
- **DB Utilization**: The percentage of the database that is currently in use.
- **Comments**: Information about the member.
- **Site**: The location to which the member belongs. This is one of the predefined extensible attributes.
To view detailed status, select a member check box, and then click the Detailed Status icon. Grid Manager displays the Detailed Status panel. If the selected member is an HA pair, Grid Manager displays the information in two columns, one for the active node and the other for the passive. The Detailed Status panel provides detailed information described in the following sections.

**Appliance Status**

The status icon indicates the operational status of a grid member and a general description of its current operation. The status icon can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green" /></td>
<td>Green</td>
<td>The appliance is operating normally in a “Running” state.</td>
</tr>
<tr>
<td><img src="image" alt="Yellow" /></td>
<td>Yellow</td>
<td>The appliance is connecting or synchronizing with its grid master.</td>
</tr>
<tr>
<td><img src="image" alt="Red" /></td>
<td>Red</td>
<td>The grid member is offline, is not licensed (that is, it does not have a DNSone license with the Grid upgrade that permits grid membership), is upgrading or downgrading, or is shutting down.</td>
</tr>
</tbody>
</table>

The following are descriptions that may appear: Running, Offline, Error, and Warning.

**Disk Usage**

Grid Manager displays the percentage of the data partition of the hard disk drive that is currently in use on the selected grid member. It also displays the percentage of usage. The status icon can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green" /></td>
<td>Green</td>
<td>Under 85% of the capacity is currently in use.</td>
</tr>
<tr>
<td><img src="image" alt="Yellow" /></td>
<td>Yellow</td>
<td>Between 85% and 95% of the capacity in use.</td>
</tr>
<tr>
<td><img src="image" alt="Red" /></td>
<td>Red</td>
<td>Over 95% of the capacity in use.</td>
</tr>
</tbody>
</table>

**DB Capacity Usage**

Grid Manager displays the current percentage of the database in use on the selected grid member. For information, see *Using the Capacity Report* on page 313. The status icon can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green" /></td>
<td>Green</td>
<td>Under 85% of the database capacity is currently in use.</td>
</tr>
<tr>
<td><img src="image" alt="Yellow" /></td>
<td>Yellow</td>
<td>Over 85% of the database capacity is currently in use. When the capacity exceeds 85%, the icon changes from green to yellow.</td>
</tr>
</tbody>
</table>
**Monitoring the Appliance**

### LAN1/LAN2 Ports, HA Port, and MGMT Port

Grid Manager displays the IP address of the port. The status icons for these ports indicate the state of their network connectivity.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green" /></td>
<td>Green</td>
<td>The port is properly connected to a network. Grid Manager displays the IP address of the network.</td>
</tr>
<tr>
<td><img src="image" alt="Red" /></td>
<td>Red</td>
<td>The port is not able to make a network connection.</td>
</tr>
<tr>
<td><img src="image" alt="Gray" /></td>
<td>Gray</td>
<td>The port is disabled.</td>
</tr>
</tbody>
</table>

### LCD

The LCD status icon indicates its operational status.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green" /></td>
<td>Green</td>
<td>The LCD is functioning properly.</td>
</tr>
<tr>
<td><img src="image" alt="Yellow" /></td>
<td>Yellow</td>
<td>The LCD process is not running.</td>
</tr>
</tbody>
</table>

### Memory Usage

Grid Manager displays the current percentage of system memory in use on the selected grid member. It also describes whether the usage is OK or not. You can see more details about memory usage through the CLI command: `show memory`. The status icon can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green" /></td>
<td>Green</td>
<td>Under 90% capacity.</td>
</tr>
<tr>
<td><img src="image" alt="Yellow" /></td>
<td>Yellow</td>
<td>Between 90% and 95% capacity.</td>
</tr>
<tr>
<td><img src="image" alt="Red" /></td>
<td>Red</td>
<td>Over 95% capacity.</td>
</tr>
</tbody>
</table>

### FAN

The status icon indicates whether the fan is functioning properly. The corresponding description displays the fan speed. The status icon and fan speed are displayed for Fan1, Fan2, and Fan3.

**Note:** vNIOS appliances on Cisco and VMware do not monitor or report the fan speed.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green" /></td>
<td>Green</td>
<td>The fan is functioning properly.</td>
</tr>
<tr>
<td><img src="image" alt="Red" /></td>
<td>Red</td>
<td>The fan is not running.</td>
</tr>
</tbody>
</table>
Power Supply

The Infoblox-1552, -1552-A, -1852-A, -2000, and -2000-A have redundant power supplies. The power supply icon indicates the operational status of the power supplies.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Green</td>
<td>The power supplies are functioning properly.</td>
</tr>
<tr>
<td></td>
<td>Red</td>
<td>One power supply is not running. To find out which power supply failed, check the LEDs of the power supplies.</td>
</tr>
</tbody>
</table>

NTP Synchronization

The status icon indicates the operational status of the current NTP synchronization status.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Green</td>
<td>The NTP service is enabled and running properly.</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>The NTP service is enabled, and the appliance is synchronizing its time.</td>
</tr>
<tr>
<td></td>
<td>Red</td>
<td>The NTP service is enabled, but it is not running properly or is out of synchronization.</td>
</tr>
<tr>
<td></td>
<td>Gray</td>
<td>The NTP service is disabled.</td>
</tr>
</tbody>
</table>

CPU Temperature

This icon is always green. The description reports the CPU temperature.

**Note:** vNIOS appliances on Cisco and VMware do not monitor or report the CPU temperature.

System Temperature

This icon is always green. The description reports the system temperature.

**Note:** vNIOS appliances on Cisco and VMware do not monitor or report the system temperature.

CPU Usage

Grid Manager displays the current percentage of the CPU usage on the selected grid member. The maximum is 100%. The status icon can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Green</td>
<td>Under 90% capacity</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>Between 90% and 95% capacity</td>
</tr>
<tr>
<td></td>
<td>Red</td>
<td>Over 95% capacity</td>
</tr>
</tbody>
</table>
RAID

For the Infoblox-2000 and -2000-A, Grid Manager displays one of the following icons to indicate the status of each disk in the RAID array. Next to the status icon is a summary that includes the disk number, the operational status of the disk, and the disk type. Grid Manager also displays a RAID summary with an overall array status icon and the percentage at which the array is currently operating.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Green Icon]</td>
<td>Green</td>
<td>The RAID array or the disk is functioning properly.</td>
</tr>
<tr>
<td>![Yellow Icon]</td>
<td>Yellow</td>
<td>A new disk has been inserted and the RAID array is rebuilding.</td>
</tr>
<tr>
<td>![Red Icon]</td>
<td>Red</td>
<td>The RAID array or the disk is degraded. At least one disk in the array is not functioning properly. Grid Manager lists the disks that are online. Replace only the disks that are offline.</td>
</tr>
</tbody>
</table>

In the event of a disk failure, you must replace the failed disk with one that is qualified and shipped from Infoblox and has the same disk type as the rest of the disks in the array. The appliance displays information about mismatched disks. The disk type can be one of the following:

- IB-Type 1: Infoblox supported disk type
- IB-Type 2: Infoblox supported disk type
- Unk: Unknown disk type that Infoblox does not support

All disk drives in the array must have the same disk type for the array to function properly. You can have either IB-Type 1 or IB-Type 2, but you cannot mix both in the array. When you have a mismatched disk in the array, you must promptly replace the disk with a replacement disk from Infoblox to avoid operational issues.

RAID Battery

The icon indicates the status of the disk controller backup battery on the Infoblox-2000 or -2000-A.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Green Icon]</td>
<td>Green</td>
<td>The battery is charged. The description indicates the estimated number of hours of charge remaining on the battery.</td>
</tr>
<tr>
<td>![Yellow Icon]</td>
<td>Yellow</td>
<td>The battery is charging.</td>
</tr>
<tr>
<td>![Red Icon]</td>
<td>Red</td>
<td>The battery is not charged.</td>
</tr>
</tbody>
</table>
Viewing Hardware Status

You can view the link activity and connection speed of an Ethernet port by looking at its Link/Act and Speed LEDs on the appliance. The status the LEDs convey through their color and illumination (steady glow or blinking) are presented in the following tables.

For Infoblox-2000 and -2000-A Appliances

<table>
<thead>
<tr>
<th>MGMT and HA Ports</th>
<th>Port Status</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link/Act</td>
<td>Link is up but inactive</td>
<td>Steady Orange</td>
</tr>
<tr>
<td>Blinking Orange</td>
<td>Link is up and active</td>
<td>Blinking Orange</td>
</tr>
<tr>
<td>Dark</td>
<td>Link is down</td>
<td>Dark</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LAN Ports</th>
<th>Port Status</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link/Act</td>
<td>Link is up but inactive</td>
<td>Steady Green</td>
</tr>
<tr>
<td>Blinking Green</td>
<td>Link is up and active</td>
<td>Blinking Green</td>
</tr>
<tr>
<td>Dark</td>
<td>Link is down</td>
<td>Dark</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>MGMT, HA, and LAN Ports</th>
<th>Port Status</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link/Act</td>
<td>Link is up but inactive</td>
<td>Steady Amber</td>
</tr>
<tr>
<td>Blinking Yellow</td>
<td>Link is up and active</td>
<td>Blinking Yellow</td>
</tr>
<tr>
<td>Dark</td>
<td>Link is down</td>
<td>Dark</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Speed</th>
<th>Port Status</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link/Act</td>
<td>Link is up but inactive</td>
<td>Steady Green</td>
</tr>
<tr>
<td>Blinking Green</td>
<td>Link is up and active</td>
<td>Blinking Green</td>
</tr>
<tr>
<td>Dark</td>
<td>Link is down</td>
<td>Dark</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MGMT</th>
<th>Port Status</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link/Act</td>
<td>Link is up but inactive</td>
<td>Yellow</td>
</tr>
<tr>
<td>Blinking Yellow</td>
<td>Link is up and active</td>
<td>Blinking Yellow</td>
</tr>
<tr>
<td>Dark</td>
<td>Link is down</td>
<td>Dark</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LAN1</th>
<th>Port Status</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link/Act</td>
<td>Link is up but inactive</td>
<td>Steady Amber</td>
</tr>
<tr>
<td>Blinking Yellow</td>
<td>Link is up and active</td>
<td>Blinking Yellow</td>
</tr>
<tr>
<td>Dark</td>
<td>Link is down</td>
<td>Dark</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LAN2</th>
<th>Port Status</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link/Act</td>
<td>Link is up but inactive</td>
<td>Steady Amber</td>
</tr>
<tr>
<td>Blinking Yellow</td>
<td>Link is up and active</td>
<td>Blinking Yellow</td>
</tr>
<tr>
<td>Dark</td>
<td>Link is down</td>
<td>Dark</td>
</tr>
</tbody>
</table>

For Infoblox-250 Appliances

<table>
<thead>
<tr>
<th>Port Status</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link/Act</td>
<td>Link is up but inactive</td>
</tr>
<tr>
<td>Blinking Yellow</td>
<td>Link is up and active</td>
</tr>
<tr>
<td>Dark</td>
<td>Link is down</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Speed</th>
<th>Port Status</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link/Act</td>
<td>Link is up but inactive</td>
<td>Steady Amber</td>
</tr>
<tr>
<td>Blinking Yellow</td>
<td>Link is up and active</td>
<td>Blinking Yellow</td>
</tr>
<tr>
<td>Dark</td>
<td>Link is down</td>
<td>Dark</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Speed</th>
<th>Port Status</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link/Act</td>
<td>Link is up but inactive</td>
<td>Steady Amber</td>
</tr>
<tr>
<td>Blinking Yellow</td>
<td>Link is up and active</td>
<td>Blinking Yellow</td>
</tr>
<tr>
<td>Dark</td>
<td>Link is down</td>
<td>Dark</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Speed</th>
<th>Port Status</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link/Act</td>
<td>Link is up but inactive</td>
<td>Steady Amber</td>
</tr>
<tr>
<td>Blinking Yellow</td>
<td>Link is up and active</td>
<td>Blinking Yellow</td>
</tr>
<tr>
<td>Dark</td>
<td>Link is down</td>
<td>Dark</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Speed</th>
<th>Port Status</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link/Act</td>
<td>Link is up but inactive</td>
<td>Steady Amber</td>
</tr>
<tr>
<td>Blinking Yellow</td>
<td>Link is up and active</td>
<td>Blinking Yellow</td>
</tr>
<tr>
<td>Dark</td>
<td>Link is down</td>
<td>Dark</td>
</tr>
</tbody>
</table>
Monitoring Services

The grid or device status icon and the service icon indicates whether a service running on a member or an independent appliance is functioning properly or not.

Service Status

After you enable any of the services—DHCP, DNS, TFTP, HTTP (for file distribution), FTP, NTP, bloxTools, and Captive Portal—the appliance indicates their status as follows:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green" /></td>
<td>Green</td>
<td>The service is enabled and running properly.</td>
</tr>
<tr>
<td><img src="image" alt="Yellow" /></td>
<td>Yellow</td>
<td>The service is enabled, but there may be some issues that require attention.</td>
</tr>
<tr>
<td><img src="image" alt="Red" /></td>
<td>Red</td>
<td>The service is enabled, but it is not running properly. (A red status icon can also appear temporarily when a service is enabled and begins running, but the monitoring mechanism has not yet notified Grid Manager.)</td>
</tr>
<tr>
<td><img src="image" alt="Gray" /></td>
<td>Gray</td>
<td>The service is not configured or it is disabled.</td>
</tr>
</tbody>
</table>

Monitoring Grid Services

The status icon of a grid service represents the status of the most critical service in the grid. For example, if the grid DHCP status icon is red, the DHCP service on one of the members in the grid is not running properly. You can click the DHCP service link to view the service status of all grid members and identify which member has a service problem. You can then decide to start or stop the service, or modify the service configuration on that member.

To monitor a grid service:

1. From the Grid tab, select the Grid Manager tab, and then click a service link.
2. Grid Manager displays the following information in the Services tab:
   - **Name**: The name of the member.
   - **Service Status**: The current status of the service.
   - **IP Address**: The IP address of the appliance or the VIP of an HA pair.
   - **Comments**: Information about the member or service.
   - **Site**: The site to which the member belongs. This is one of the predefined extensible attributes. You can select available extensible attributes for display.
3. Optionally, click the Edit icon next to the service name to edit the grid properties for the service. Or
   - Select a member check box, and do one of the following:
     - Click the Edit icon to edit the member service configuration. Grid Manager displays the editor for the corresponding service. For example, when you edit the DHCP service, Grid Manager displays the Member DHCP Configuration editor.
     - Click the Start icon to start the service.
     - Click the Stop icon to stop the service.
   Grid Manager updates the service status based on your action.
Monitoring Member Services

You can view detailed service status on a selected member. Optionally, you can start and stop a service, and edit the service configuration.

To monitor a member service:

1. From the Grid tab, select the Grid Manager tab → Members tab → member check box, and then click the Manage Member Services icon.

   In the Manage Services panel, Grid Manager displays the following information:
   - **Service**: The name of the service.
   - **Status**: The current status of the service running on the member.
   - **Description**: The description of the status. Grid Manager displays the percentage of usage for the TFTP, HTTP (File Distribution), FTP, and bloxTools services.

2. Optionally, mouse over a service and do one of the following:
   - **Start/Stop Service**: Click this icon to start or stop the selected service. For example, when the DNS service is currently stopped, the appliance starts the service when you click this icon.
   - **Edit Service**: Click this icon to edit the selected service. Grid Manager displays the corresponding editor. For example, when you click the Edit Service icon for DNS, Grid Manager displays the Member DNS Configuration editor.

   Click the Refresh icon to update the service status.
Using a Syslog Server

Syslog is a widely used mechanism for logging system events. NIOS appliances generate syslog messages that you can view through the Syslog viewer and download to a directory on your management station. In addition, you can configure a NIOS appliance to send the messages to one or more external syslog servers for later analysis. Syslog messages provide information about appliance operations and processes. You can also include audit log messages and specific BIND messages among the messages the appliance sends to the syslog server.

In addition to saving system messages to a remote syslog server, a NIOS appliance also stores the system messages locally. When the syslog file reaches its maximum size, which is 300 MB for Infoblox appliances and Cisco and VMware virtual appliances, and 20 MB for Riverbed virtual appliances, the appliance automatically writes the file into a new file by adding a .0 extension to the first file and incrementing subsequent file extensions by 1.

Files are compressed during the rotation process, adding a .gz extension following the numerical increment (file.#.gz). The sequential incrementation goes from zero through nine. When the eleventh file is started, the tenth log file (file.9.gz) is deleted, and subsequent files are renumbered accordingly. For example, the current log file moves to file.0.gz, the previous file.0.gz moves to file.1.gz, and so on through file.9.gz. A maximum of 10 log files (0-9) are kept.

You can set syslog parameters at the grid and member levels. At the member level, you can override grid-level syslog settings and enable syslog proxy.

This section includes the following topics:

- Specifying Syslog Servers on page 306
- Configuring Syslog for Grid Members on page 307
- Setting DNS Logging Categories on page 308
- Viewing the Syslog on page 309
- Searching in the Syslog on page 309
- Downloading the Audit Log on page 312

Specifying Syslog Servers

To configure a NIOS appliance to send messages to a syslog server:

1. From the Grid tab, select the Grid Manager tab -> Members tab, and then click Grid Properties -> Edit from the Toolbar.

2. In the Grid Properties editor, select the Monitoring tab, and then complete the following:
   
   **Syslog**

   In addition to storing the syslog on a grid member, you can configure the grid to send the log to an external syslog server.

   - **Syslog size (MB):** Specify the maximum size for a syslog file. Enter a value between 10 and 300. The default is 300.
     
     When the syslog file reaches the size you enter here, the appliance automatically writes the file into a new file by adding a .0 extension to the first file and incrementing subsequent file extensions by 1.

   - **Log to External Syslog Servers:** Select this to enable the appliance to send messages to a specified syslog server.

   Grid Manager displays the current syslog servers in the table. To define a new syslog server, click the Add icon. Grid Manager adds a row to the table. Enter the following by clicking each field in the row:

     - **Address:** Enter the IP address of a syslog server.
     - **Transport:** From the drop-down list, select whether the appliance uses TCP or UDP to connect to the external syslog server.
     - **Interface:** From the drop-down list, select the interface through which the appliance sends syslog messages to the syslog server.
— **Source:** From the drop-down list, select which syslog messages the appliance sends to the external syslog server:
  - **Internal:** The appliance sends syslog messages that it generates.
  - **External:** The appliance sends syslog messages that it receives from other devices, such as syslog servers and routers.
  - **Any:** The appliance sends both internal and external syslog messages.
— **Port:** Enter the destination port number. The default is 514.
— **Severity:** Choose a severity filter from the drop-down list. When you choose a severity level, the appliance sends log messages with the selected level and the levels above it. The severity levels range from the lowest, **debug**, to the highest, **emerg**. For example, if you choose **debug**, the appliance sends all syslog messages to the server. If you choose **err**, the appliance sends messages with severity levels **err, crit, alert, and emerg**.
  - **emerg:** Panic or emergency conditions. The system may be unusable.
  - **alert:** Alerts, such as NTP service failures, that require immediate actions.
  - **crit:** Critical conditions, such as hardware failures.
  - **err:** Error messages, such as client update failures and duplicate leases.
  - **warning:** Warning messages, such as missing keepalive options in a server configuration.
  - **notice:** Informational messages regarding routine system events, such as “starting BIND”.
  - **info:** Informational messages, such as DHCPACK messages and discovery status.
  - **debug:** Messages that contain information for debugging purposes, such as changes in the latency timer settings and AD authentication failures for specific users.
— **Copy Audit Log Messages to Syslog:** Select this for the appliance to include audit log messages it sends to the syslog server. This function can be helpful for monitoring administrative activities on multiple appliances from a central location.
— **Syslog Facility:** This is enabled when you select **Copy audit log messages to syslog**. Select the facility that determines the processes and daemons from which the log messages are generated.

3. Select one of the following:
— **Save & Close:** Save the entry and close the editor.
— **Save:** Save the entry and continue to edit.

### Configuring Syslog for Grid Members

You can override grid-level syslog settings and enable syslog proxy for individual members. When you enable syslog proxy, the member receives syslog messages from specified devices, such as syslog servers and routers, and then forwards these messages to an external syslog server. You can also enable appliances to use TCP for sending syslog messages. Using TCP is more reliable than using UDP; this reliability is important for security, accounting, and auditing messages sent through the syslog.

To configure syslog parameters for a member:

1. From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab -> **member** check box, and then click the Edit icon.
2. In the **Grid Member Properties** editor, select the **Monitoring** tab -> **Basic** tab, click **Override** in the Syslog section, and then complete the fields as described in **Specifying Syslog Servers** on page 306.

   In addition to storing the system log on a grid member, you can configure a member to send the log to a syslog server.

3. Select the **Advanced** tab and complete the following:
   — **Enable syslog proxy:** Select this to enable the appliance to receive syslog messages from other devices, such as syslog servers and routers, and then forward these messages to an external syslog server.
   — **Enable listening on TCP:** Select this if the appliance uses TCP to receive messages from other devices. Enter the number of the port through which the appliance receives syslog messages from other devices.
Monitoring the Appliance

- **Enable listening on UDP:** Select this if the appliance uses UDP to receive messages from other devices. Enter the number of the port through which the appliance receives syslog messages from other devices.

- **Proxy Access Control:** Click the Add icon. Grid Manager adds a row to the table. Complete the following:
  - **Allow Access From:** Enter the IP address and subnet mask of the appliance or network.

4. Select one of the following:
   - **Save & Close:** Save the entry and close the editor.
   - **Save:** Save the entry and continue to edit.

### Setting DNS Logging Categories

You can specify which of the 14 BIND logging message categories you want the syslog to capture. Furthermore, you can filter these messages by severity at the grid and member levels. For information about severity types, see *Specifying Syslog Servers* on page 306.

To specify logging categories:

1. From the **Data Management** tab, select the **DNS** tab, and then click **Grid DNS Properties** from the Toolbar.
   or
   From the **Data Management** tab, select the **DNS** tab → **Members** tab → **grid_member** check box, and then click the Edit icon.

2. In the **Grid DNS Properties** or **Member DNS Properties** editor, click **Toggle Advanced Mode** if the editor is in the basic mode, select the **Logging** tab, and then complete the following:
   - **Logging Facility:** Select a facility from the drop-down list. This is the location on the syslog server to which you want to sort the DNS logging messages.
   - **Logging Category:** Select one or more of these log categories:
     - **general:** Records the BIND messages that are not specifically classified.
     - **client:** Records client requests.
     - **config:** Records the configuration file parsing messages.
     - **database:** Records BIND’s internal database processes.
     - **dnssec:** Records the DNSSEC-signed responses.
     - **lame servers:** Records bad delegation instances.
     - **network:** Records the network operation messages.
     - **notify:** Records the asynchronous zone change notification messages.
     - **queries:** Records the DNS queries. Note that selecting this category may affect the DNS query performance. Infoblox recommends that you do not log this message category for high throughput servers.
     - **resolver:** Records the DNS resolution instances, including recursive queries from resolvers.
     - **security:** Records the approved and denied requests.
     - **transfer-in:** Records zone transfer messages from the remote name servers to the appliance.
     - **transfer-out:** Records zone transfer messages from the NIOS appliance to remote name servers.
     - **update:** Records the dynamic update instances.
     - **update-security:** Records the security updates.

3. Select one of the following:
   - **Save & Close:** Save the entry and close the editor.
   - **Save:** Save the entry and continue to edit.
Viewing the Syslog

1. From the Administration tab, select the Logs tab -> Syslog tab.
2. From the drop-down list at the upper right corner, select the grid member on which you want to view the syslog.
3. Optionally, use the filters to narrow down the system messages you want to view. Click Show Filters to enable the filters. Configure the filter criteria, and then click Apply.

Based on your filter criteria (if any), Grid Manager displays the following in the Syslog viewer:

   - **Timestamp:** The date, time, and time zone of the log message. The time zone is the time zone configured on the member.
   - **Facility:** The location on the syslog server that determines the processes and daemons from which the log messages are generated.
   - **Level:** The severity of the message. This can be ALERT, CRITICAL, DEBUG, EMERGENCY, ERROR, INFO, NOTICE, or WARNING.
   - **Server:** The name of the server that logs this message, plus the process ID.
   - **Message:** Detailed information about the task performed.

**Note:** If the selected member is an HA pair, Grid Manager displays the syslog in two tabs—Active and Passive. Click the corresponding tab to view the syslog for each node.

You can also do the following in the Syslog viewer:

- Toggle between the single line view and the multi-line view for display.
- Navigate to the next or last page of the file using the paging buttons.
- Refresh the syslog output with newly logged messages.
- Click the Follow icon to have the appliance automatically refresh the log every five seconds.
- Clear the contents of the syslog.
- Print the report or export it in CSV format.
- Bookmark the syslog page.

Searching in the Syslog

Instead of paging through the syslog to locate messages, you can have the appliance search for syslog messages with certain text strings.

To search for specific messages:

- Enter a search value in the search field below the filters, and then click the Search icon.

   The appliance searches through the syslog and highlights the search value in the viewer. You can use the arrow keys next to the Search icon to locate the previous or next message that contains the search value.

Downloading the Syslog File

You can download the syslog file to a specified directory, if you want to analyze it later.

1. From the Administration tab, select the Logs tab -> Syslog tab, and then click the Download icon.
2. Navigate to a directory where you want to save the file, optionally change the file name (the default names are `node_1_sysLog.tar.gz` and `node_2_sysLog.tar.gz`), and then click OK. If you want to download multiple syslog files to the same location, rename each downloaded file before downloading the next.

**Note:** If your browser has a pop-up blocker enabled, you must turn off the pop-up blocker or configure your browser to allow pop-ups for downloading files.
Monitoring the Appliance

Monitoring Tools

You can use the audit log, the replication status, the traffic capture tool, and the capacity report in a grid or HA pair to monitor administrative activities and capture traffic for diagnostic purposes. You can also use CLI commands to monitor certain DNS transactions.

This section includes the following topics:

- Using the Audit Log
- Viewing the Replication Status on page 312
- Using the Traffic Capture Tool on page 312
- Using the Capacity Report on page 313
- Using the Phone Home Feature on page 314
- Monitoring DNS Transactions on page 315
- Viewing DNS Alert Indicator Status on page 317
- Configuring DNS Alert Thresholds on page 318
- Monitoring DNS Transactions on page 315

In addition, if grid members manage Microsoft servers, Grid Manager creates a synchronization log file for each managed Microsoft server. For information, see Viewing Synchronization Logs on page 739.

Using the Audit Log

The audit log contains a record of all Infoblox administrative activities. It provides detailed information about the following changes:

- Timestamp of the change. If you have different admin accounts with different time zone settings, the appliance uses the time zone of the admin account that you use to log in to the appliance to display the date and timestamp.
- Administrator name
- Changed object name
- New value of the object. If you change multiple properties of an object, the audit log lists all changes in a comma-separated log entry. You can also search the audit log to find the new value of an object.

The appliance logs the following successful operations:

- Logins to Grid Manager and the API.
- Logout events, including when users log out by clicking the Logout button, when the Grid Manager GUI times out, and when users are logged out due to an error.
- Write operations such as the addition, modification, and deletion of objects.
- System management operations such as service restarts and appliance reboots.
- Scheduled tasks such as adding an A record or modifying a fixed address.

Enabling Audit Log Rolling

When the audit log reaches its maximum size, which is 100 MB, the appliance automatically writes the file into a new file by adding a .0 extension to the first file and incrementing subsequent file extensions by 1. Files are compressed during the rotation process, adding a .gz extension following the numerical increment (file.#.gz). The sequential incrementation goes from zero through nine. When the eleventh file is started, the tenth log file (file.9.gz) is deleted, and subsequent files are renumbered accordingly. For example, the current log file moves to file.0.gz, the previous file.0.gz moves to file.1.gz, and so on through file.9.gz. A maximum of 10 log files (0-9) are kept. To list the audit log files and their sizes, log in to the Infoblox CLI and execute the show logfiles command.

To enable audit log rolling:

1. From the Grid tab, select the Grid Manager tab → Members tab, and then click Grid Properties → Edit from the Toolbar.
2. In the Grid Properties editor, select the Security tab, and then select Enable Audit Log Rolling.
Specifying the Audit Log Type

Select either the Detailed (default) or Brief audit log type as follows:

1. From the Grid tab, select the Grid Manager tab -> Members tab, and then click Grid Properties -> Edit from the Toolbar.
2. In the Grid Properties editor, select the General tab, and then select one of the following:
   - Detailed: This is the default type. When you select this, Grid Manager displays detailed information on all administrative changes such as the timestamp of the change, administrator name, changed object name, and the new values of all properties in the logged message.
   - Brief: Provides information on administrative changes such as the changed object name and action in the log message. The logged message does not show timestamp or admin name.

Viewing the Audit Log

To view an audit log:

1. From the Administration tab, select the Logs tab -> Audit Log tab.
2. Optionally, use the filters to narrow down the audit log messages you want to view. Click Show Filters to enable the filters. Configure the filter criteria, and then click Apply.

   Based on your filter criteria (if any), Grid Manager displays the following in the Audit Log viewer:
   - Timestamp: The date, time, and time zone the task was performed. The time zone is the time zone configured on the member.
   - Admin: The admin user who performed the task.
   - Action: The action performed. This can be CALLED, CREATED, DELETED, LOGIN_ALLOWED, LOGIN_DENIED, MESSAGE, and MODIFIED.
   - Object Type: The object type of the object involved in this task. This field is not displayed by default. You can select this for display.
   - Object Name: The name of the object involved in this task.
   - Message: Detailed information about the performed task.

You can also do the following in the log viewer:

- Toggle between the single line view and the multi-line view for display.
- Navigate to the next or last page of the file using the paging buttons.
- Refresh the audit log view.
- Click the Follow icon to have the appliance automatically refresh the log every five seconds.
- Download the log.
- Clear the contents of the audit log.
- Export or print the content of the log.

Searching in the Audit Log

Instead of paging through the audit log file to locate messages, you can have the appliance search for messages with certain text strings.

To search for specific messages:

- Enter a search value in the search field below the filters, and then click the Search icon.
  The appliance searches through the audit log file and highlights the search value in the viewer. You can use the arrow keys next to the Search icon to locate the previous or next message that contains the search value.
Monitoring the Appliance

**Downloading the Audit Log**

You can download the audit log file to a specified directory, if you want to analyze it later.

To download an audit log file:

1. From the **Administration** tab, select the **Logs** tab → **Audit Log** tab, and then click the Download icon.
2. Navigate to a directory where you want to save the file, optionally change the file name (the default name is *auditLog.tar.gz*), and then click **OK**. If you want to download multiple audit log files to the same location, rename each downloaded file before downloading the next.

**Note:** If your browser has a pop-up blocker enabled, you must turn off the pop-up blocker or configure your browser to allow pop-ups for downloading files.

**Viewing the Replication Status**

The *Replication Status* panel reports the status of the database replication between grid members and grid master, and between the two nodes in an independent HA pair. You can use this information to check the health of the grid and HA pair activity.

To view the current replication status, from the **Grid** tab, select the **Grid Manager** tab → **Members** tab, and then click **Toggle Replication Status View**.

In addition to the fields displayed in the **Members** tab, Grid Manager can display the following replication information for each member:

- **Send Queue**: The size of the queue from the grid master to the grid member.
- **Last Send**: The timestamp of the last replication information sent by the grid master.
- **Receive Queue**: The size of the queue from the grid member to the grid master.
- **Last Receive**: The timestamp of the last replication information sent received by the grid master.
- **Member Replication Status**: The replication status between the member and the grid master. Grid Manager displays the status in green when the status is fine or red when the member is offline.
- **HA Replication Status**: The HA replication status between the active and passive nodes. The status is at the node level, not at the member level. Grid Manager displays the status in red when one of the nodes is offline.
- **HA**: Indicates whether the member is an HA pair. If the member is an HA pair, Grid Manager displays the status of the HA pair.

**Using the Traffic Capture Tool**

You can capture the traffic on one or all of the ports on a NIOS appliance, and then view it using a third-party network protocol analyzer application, such as the Wireshark – Network Protocol Analyzer™.

The NIOS appliance saves all the traffic it captures in a *.cap file and compresses it into a *.tar.gz file. Your management system must have a utility that can extract the *.tar file from the *.gzip file, and an application that can read the *.cap (capture) file format.

This section explains the process of capturing traffic, and how to download the traffic capture file to your management system. After that, you can extract the traffic capture file and view it with a third-party traffic analyzer application.

**Note:** The NIOS appliance always saves a traffic capture file as *tcpdumpLog.tar.gz*. If you want to download multiple traffic capture files to the same location, rename each downloaded file before downloading the next.
To capture traffic on a member:

1. From the Grid tab, select the Grid Manager tab -> Members tab, and then click Traffic Capture from the Toolbar.
2. In the Traffic Capture dialog box, complete the following:
   - **Member**: Grid Manager displays the selected member on which you want to capture traffic. If no member is displayed or if you want to specify a different member, click Select. When there are multiple members, Grid Manager displays the Member Selector dialog box from which you can select one. You cannot capture traffic on an offline member.
   - **Interface**: Select the port on which you want to capture traffic. Note that if you enabled the LAN2 failover feature, the LAN and LAN2 ports generate the same output. (For information about the LAN2 failover feature, see About NIC Redundancy on page 237.)
     - **LAN**: Select this to capture all the traffic the LAN port receives and transmits.
     - **MGMT**: Select this to capture all the traffic the MGMT port receives and transmits.
     - **LAN2**: Select to capture all the traffic the LAN2 port (if enabled) receives and transmits.
     - **All**: Select this to capture the traffic addressed to all ports. Note that the NIOS appliance only captures traffic that is addressed to it.
   - **Seconds to run**: Specify the number of seconds you want the traffic capture tool to run.
3. Capture Control: Click the Start icon to start the capture. A warning message appears indicating that this report will overwrite the existing file. Click Yes. You can click the Stop icon to stop the capture after you start it.
4. Uncompressed Capture File Size: Click Download to download the captured traffic after the capture stops. Navigate to where you want to save the file, rename it if you want, and then click OK or Save. You cannot download the traffic report when the tool is running. Grid Manager updates the size of the report when the capture tool is running.
5. Use terminal window commands (Linux) or a software application (such as StuffIt™ or WinZip™) to extract the contents of the .tar.gz file.
6. When you see the traffic.cap file in the directory where you extract the .tar.gz file, open it with a third-party network protocol analyzer application.

### Using the Capacity Report

You can view the capacity usage and object type information of an appliance in a capacity report. The capacity report displays capacity and object type information of an independent appliance, a grid master, or a grid member. For an HA pair, the report displays information on the active node.

The top half of the panel displays a capacity summary, and the bottom half displays the object types the appliance supports and the total counts for each object type.

To view a capacity report:

- From the Grid tab, select the Grid Manager tab -> Members tab -> member check box, and then click Capacity Report from the Toolbar.

The capacity summary contains the following information:

- **Name**: The name of the appliance.
- **Role**: The role of the appliance. The value can be Grid Master, Grid Master Candidate, Grid Member, or Standalone.
- **Hardware Type**: The type of hardware. For an HA pair, the report displays the hardware type for both the active and passive nodes.
- **Object Capacity**: The maximum number of objects the appliance can support.
- **Total Objects**: The total number of objects currently in the database.
- **% Capacity Used**: The percentage of the capacity in use.
The report categorizes object types you can manage through the appliance. It displays the following information for each object type:

- **Object Type**: The type of objects. For example, DHCP Lease, Admin Group, or PTR Record. For objects that are only used for internal system operations, the report groups and shows them under **Other**.
- **Total**: The total number of objects for a specific object type.

You can print the object type information or export it to a CSV file.

### Using the Phone Home Feature

Administrators with superuser accounts can configure a grid master or an independent appliance to email reports monthly and after each upgrade to Infoblox Technical Support and other specified recipients. The reports are also included in support bundles that you download.

The reports provide status and event information about the grid or independent appliance and its services. The report is an XML document that includes the following information:

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

Note that if the appliance is configured to send email notifications to an SMTP relay server, as described in *Notifying Administrators* on page 109, the appliance sends the phone home reports to the relay server as well.

To configure the grid master to email status reports:

1. From the Grid tab, select the Grid Manager tab → Members tab.
2. Expand the Toolbar and click Grid Properties → Edit.
3. In the Grid Properties editor, select the Phone Home tab, and then complete the following:
   - **Enable Phone Home**: Select this check box.
   - **Support ID (numeric)**: Enter the Infoblox Support ID that was assigned to your account. It must be a number with four to 6 digits. This field is required if you are sending the reports to Infoblox Technical Support.
   - **Send notifications to**:
     - **Infoblox Support**: Select this to email the reports to Infoblox Technical Support.
     - **Additional email addresses**: Optionally, you can specify up to 16 additional recipients. Click the Add icon and enter the email addresses of the recipients.
   - **Send Test Report**: Click this to send a test report to the specified recipients.
4. Click Save & Close.
Monitoring DNS Transactions

The NIOS appliance provides tools for monitoring DNS transactions and mitigating cache poisoning from UDP (User Datagram Protocol) traffic on source port 53. Cache poisoning can occur when a DNS server accepts maliciously created unauthentic data. The DNS server ends up locally caching the incorrect entries and serving them to users that make the same DNS requests. In a maliciously created situation, the attacker can redirect Internet traffic from the legitimate host to another host that the attacker controls.

You can configure the appliance to track invalid DNS responses for recursive DNS queries. The appliance tracks DNS responses that arrive on invalid ports or have invalid TXIDs (DNS transaction IDs). Both invalid ports and invalid TXIDs could be indicators of cache poisoning. An invalid port is a DNS response that arrives from UDP port 53 with either one of the following conditions:

- There are no outstanding DNS requests from the port on which the response arrives.
- The TXID of the DNS response matches the TXID of an outstanding request. However, the request was sent from a port other than the port on which the response arrives.

An invalid TXID is a DNS response that arrives from UDP port 53, and the TXID does not match the TXID of an outstanding DNS request.

Figure 10.1 illustrates how the appliance detects an invalid port and an invalid TXID.

Figure 10.1 Invalid Port and Invalid TXID

Both invalid ports and invalid TXIDs could be indicators of DNS cache poisoning, although a small number of them is considered normal in situations where valid DNS responses arrive after the DNS queries have timed out. You can configure the appliance to track these indicators, and you can view their status. You can also configure thresholds for them. When the number of invalid ports or invalid TXIDs exceeds the thresholds, the appliance logs an event in the syslog file and sends an SNMP trap and e-mail notification, if you enable them. You can then configure rate limiting rules to limit incoming traffic or completely block connections from primary sources that send the invalid DNS responses.
Rate limiting is a token bucket system that accepts packets from a source based on the rate limit. You can configure the number of packets per minute that the Infoblox DNS server accepts from a specified source. You can also configure the number of packets for burst traffic, which is the maximum number of packets that the token bucket can accept. Once the bucket reaches the limit for burst traffic, it discards the packets and starts receiving new packets according to the rate limit.

The appliance monitors only UDP traffic from remote port 53 for the following reasons:
- The attacks that the appliance monitors do not happen over TCP.
- DNS responses are sent only from port 53. The appliance discards DNS responses that are sent from other ports.

To monitor invalid ports and invalid TXIDs on the Infoblox DNS server, follow these procedures:

1. Enable DNS network monitoring and DNS alert monitoring. For information, see Enabling and Disabling DNS Alert Monitoring on page 316.
2. Configure the thresholds for DNS alert indicators. For information, see Configuring DNS Alert Thresholds on page 318.
3. Enable SNMP traps and e-mail notifications. For information, see Configuring SNMP on page 373.
4. Review the DNS alert status. For information, see Viewing DNS Alert Indicator Status on page 317.
5. Identify the source of the attack by reviewing the DNS alert status, syslog file, and SNMP traps. For information on SNMP traps for DNS alerts, see Threshold Crossing Traps on page 344.

To mitigate cache poisoning, you can limit incoming traffic or completely block connections from specific sources, as follows:
- Enable rate limiting on the DNS server. For information, see Enabling and Disabling Rate Limiting from External Sources on page 319.
- Configure rate limit traffic rules from specific sources. For information, see Configuring Rate Limiting Rules on page 319.

You can verify the rate limiting rules after you configure them. For information, see Viewing Rate Limiting Rules on page 320.

Enabling and Disabling DNS Alert Monitoring

The appliance monitors only UDP traffic on port 53 for recursive queries, and then reports invalid DNS responses. DNS alert monitoring is disabled by default. For an HA pair, you must enable DNS alert monitoring on both the active and passive nodes.

To enable DNS network monitoring and DNS alert monitoring:

1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:
   ```
   set monitor dns on
   ```
   The appliance displays the following:
   ```
   Turning on DNS Network Monitoring...
   ```
3. Enter the following command:
   ```
   set monitor dns alert on
   ```
   When you enable DNS alert monitoring and DNS network monitoring is disabled, the appliance automatically enables DNS network monitoring and displays the following:
   ```
   DNS Network Monitoring is disabled. It must be enabled for alerting to function.
   Enable DNS Monitoring now? (y or n):
   ```
   You can also disable DNS network monitoring and DNS alert monitoring using the following commands:
   ```
   set monitor dns off
   set monitor dns alert off
   ```
Monitoring Tools

You can then view the alert status to identify the primary source of invalid DNS responses. For information, see Viewing DNS Alert Indicator Status on page 317.

Viewing DNS Alert Indicator Status

To view DNS alert indicator status:

1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:

   show monitor dns alert status

   The appliance displays historical alert counts and up to five primary sources that generate invalid DNS responses, as shown in the following example:

```
Data last updated: Mon Oct 6 14:47:12 2008
DNS Alert   1m   5m   15m   60m   24h   Ever
============================================
port        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

   The appliance attempts to resolve the hostnames of the sources that sent invalid responses, if the DNS resolver is enabled. If the appliance cannot resolve a hostname, it displays “unknown” as the hostname of the invalid response.
Configuring DNS Alert Thresholds

You can configure thresholds for DNS alerts to control when the appliance tracks DNS attacks on UDP port 53 and issues SNMP traps and e-mail notifications.

**Note:** Ensure that you enable SNMP traps and e-mail notifications. For information, see *Configuring SNMP* on page 373.

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

To configure DNS alert thresholds:

1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:
   ```
   set monitor dns alert modify port | txid over threshold_value packets | percent
   ```
   where
   - `port | txid` = Enter `port` to set the threshold for invalid ports, or enter `txid` to set the threshold for invalid TXIDs.
   - `threshold_value` = Enter the number of packets or percentage for the threshold.
   - `packets | percent` = Enter `packets` if you want to track the total packet count, or enter `percentage` if you want to track a percentage of the total traffic. For a percentage-based threshold, the appliance does not generate a threshold crossing event if the traffic level is less than 100 packets per minute.

   For example, if you want the appliance to send a DNS alert when the percentage of DNS responses arriving on invalid ports from UDP port 53 exceeds 70% per minute, you can enter the following command:
   ```
   set monitor dns alert modify port over 70 percent
   ```

   If you want the appliance to send a DNS alert when the total number of packets with invalid TXIDs from UDP port 53 is over 100 packets per minute, you can enter the following command:
   ```
   set monitor dns alert modify txid over 100 packets
   ```

   When there is a DNS alert, the appliance logs an event in the syslog file and sends an SNMP trap and e-mail notification if enabled.

Viewing DNS Alert Thresholds

You can view the DNS alert thresholds. The appliance displays the current thresholds. If you have not configured new thresholds, the appliance displays the default thresholds, which are 50% for both invalid port and TXID.

To view the DNS alert thresholds:

1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:
   ```
   show monitor dns alert
   ```
   The appliance displays the threshold information as shown in the following example:

   DNS Network Monitoring is enabled.
   Alerting is enabled.
   DNS Alert Threshold (per minute)
   --------------------------------------------------
   port over 70% of packets
   txid over 100 packets
Enabling and Disabling Rate Limiting from External Sources

You can mitigate cache poisoning on your DNS server by limiting the traffic or blocking connections from UDP port 53.

To enable rate limiting from sources:

1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:
   ```
   set ip_rate_limit on
   ```
   The appliance displays the following:
   ```
   Enabling rate limiting will discard packets and may degrade performance.
   Are you sure? (y or n):
   ```
   **Note:** When you enable rate limiting, the appliance discards packets based on the configured rate limiting rules. This might affect the DNS performance when the appliance discards valid DNS responses.

3. Enter `y` to enable rate limiting.

When you enable rate limiting, the appliance applies the rate limiting rules that you configured. You might want to configure the rate limiting rules before enabling rate limiting. For information on how to configure rate limiting rules, see Configuring Rate Limiting Rules on page 319.

You can also disable rate limiting by entering the following command:
```
set ip_rate_limit off
```
When you disable rate limiting, the appliance stops applying the rate limiting rules.

Configuring Rate Limiting Rules

You configure rate limiting rules to limit access or block connections from UDP port 53. The rules take effect when you enable rate limiting.

When adding rules, ensure that you do not include an IP address that matches the IP address of either the grid master or grid member. Doing this could affect VPN connectivity. To configure rate limiting rules:

1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:
   ```
   set ip_rate_limit add source all | ip_address [/mask] limit packets/m [burst burst_packets]
   ```
   where
   ```
   all | ip_address = Enter all or 0.0.0.0 if you want to limit all traffic from all sources, or enter the IP address from which you want to limit the traffic.
   [/mask] = Optionally, enter the netmask of the host from which you want to limit the traffic.
   packets = Enter the number of packets per minute that you want to receive from the source.
   [burst burst_packets] = Optionally, enter `burst` and the number of packets for burst traffic. This is the maximum number of packets accepted.
   ```

The following are sample commands and descriptions for rate limiting rules:

- To block all traffic from host 10.10.1.1, enter the following command:
  ```
  set ip_rate_limit add source 10.10.1.1 limit 0
  ```
- To limit traffic to five packets per minute from host 10.10.1.2, enter the following command:
  ```
  set ip_rate_limit add source 10.10.1.2 limit 5/m
  ```
- To limit the traffic to five packets per minute from host 10.10.2.1/24 with an allowance for burst traffic of 10 packets, enter the following command:
  ```
  set ip_rate_limit add source 10.10.2.1/24 limit 5/m burst 10
  ```
- To limit the traffic to 5000 packets per minute from all sources, enter the following command:
  ```
  set ip_rate_limit add source all limit 5000/m
  ```
**Removing Rate Limiting Rules**

You can remove the existing rate limiting rules that limit access or block connections from UDP port 53.

To remove all the existing rules:

1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:
   - To remove the rate limiting rule that limits traffic from all sources, enter:
     ```
     set ip_rate_limit remove source all
     ```
   - To remove all of the rate limiting rules from all sources, enter:
     ```
     set ip_rate_limit remove all
     ```

To remove one of the existing rules for an existing host:

1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:
   ```
   set ip_rate_limit remove source ip-address[/mask]
   ```

**Viewing Rate Limiting Rules**

You can view the existing rate limiting rules that limit access or block connections from UDP port 53 at any time.

To view rate limiting rules:

1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:
   ```
   show ip_rate_limit
   ```

The appliance displays the rules, as shown in the following example:

```
IP rate limiting is enabled.
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             5000packets/minute 5000 packets
```
Chapter 11 Monitoring with SNMP

This chapter describes how you can use SNMP (Simple Network Management Protocol) to monitor NIOS appliances in your network. It contains the following sections:

- **Understanding SNMP** on page 322
- **SNMP MIB Hierarchy** on page 323
  - **MIB Objects** on page 324
  - **System Object IDs** on page 324
- **Infoblox MIBs** on page 326
  - **Loading the Infoblox MIBs** on page 326
  - **ibTrap MIB** on page 327
  - **ibPlatformOne MIB** on page 351
  - **ibDHCPOne MIB** on page 365
  - **ibDNSOne MIB** on page 369
- **Configuring SNMP** on page 373
  - **Accepting SNMP Queries** on page 373
  - **Adding SNMP Trap Receivers** on page 373
  - **Setting System Information** on page 374
  - **Configuring SNMP for a Grid Member** on page 374
**Understanding SNMP**

You can use SNMP (Simple Network Management Protocol) to manage network devices and monitor their processes. An SNMP-managed device, such as a NIOS appliance, has an SNMP agent that collects data and stores them as objects in MIBs (Management Information Bases). The SNMP agent can also send traps (or notifications) to alert you when certain events occur within the appliance or on the network. You can view data in the SNMP MIBs and receive SNMP traps on a management system running an SNMP management application, such as HP OpenView, IBM Tivoli NetView, or any of the freely available or commercial SNMP management applications on the Internet.

*Figure 11.1 SNMP Overview*

You can configure a NIOS appliance as an SNMP-managed device. NIOS appliances support SNMP versions 1 and 2, and adhere to the following RFCs:

- RFC 3413, *Simple Network Management Protocol (SNMP) Applications*
- RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*
- RFC 1155, *Structure and identification of Management information for TCP/IP-based internets*
- RFC 2578, *Structure of Management Information Version 2 (SMIv2)*
Infoblox supports the standard MIBs defined in RFC-1213, Management Information Base for Network Management of TCP/IP-based Internets: MIB-II, in addition to implementing its own enterprise MIBs. The Infoblox MIBs are part of a universal hierarchical structure, usually referred to as the MIB tree. The MIB tree has an unlabeled root with three subtrees. Figure 11.2 illustrates the branch of the MIB tree that leads to the Infoblox enterprise MIBs. Each object in the MIB tree has a label that consists of a textual description and an OID (object identifier). An OID is a unique dotted-decimal number that identifies the location of the object in the MIB tree. Note that all OIDs begin with a dot (.) to indicate the root of the MIB tree.

As shown in Figure 11.2, Infoblox is a branch of the Enterprise subtree. IANA (Internet Assigned Numbers Authority) administers the Enterprise subtree, which is designated specifically for vendors who define their own MIBs. The IANA-assigned enterprise number of Infoblox is 7779; therefore, the OIDs of all Infoblox MIB objects begin with the prefix .1.3.6.1.4.1.7779.

The Infoblox SNMP subtree branches down through two levels, ibProduct and ibOne, to the Infoblox MIBs: ibTrap, ibPlatformOne, ibDNSOne, and ibDHCPOne. The ibTrap MIB defines the traps that NIOS appliances send, and the ibPlatformOne, ibDNSOne, and ibDHCPOne MIBs provide information about the appliance. For detailed information about these MIBs, see Infoblox MIBs on page 326.

Figure 11.2 MIB Hierarchy
MIB Objects

The Infoblox MIB objects were implemented according to the guidelines in RFCs 1155 and 2578. They specify two types of macros for defining MIB objects: OBJECT-TYPE and NOTIFICATION-TYPE. These macros contain clauses that describe the characteristics of an object, such as its syntax and its status. OBJECT-TYPE macros describe MIB objects, and NOTIFICATION-TYPE macros describe objects used in SNMP traps.

Each object in the ibPlatformOne, ibDNSOne, and ibDHCPOne MIBs contains the following clauses from the OBJECT-TYPE macro:

- **OBJECT-TYPE**: Provides the administratively-assigned name of the object.
- **SYNTAX**: Identifies the data structure of the object, such as integers, counters, and octet strings.
- **MAX-ACCESS**: Identifies the type of access that a management station has to the object. All Infoblox MIB objects provide read-only access.
- **STATUS**: Identifies the status of the object. Values are current, obsolete, and deprecated.
- **DESCRIPTION**: Provides a textual description of the object.
- **INDEX or AUGMENTS**: An object that represents a conceptual row must have either an INDEX or AUGMENTS clause that defines a key for selecting a row in a table.
- **OID**: The dotted decimal object identifier that defines the location of the object in the universal MIB tree.

The ibTrap MIB defines the SNMP traps that a NIOS appliance can send. Each object in the ibTrap MIB contains the following clauses from the NOTIFICATION-TYPE macro:

- **NOTIFICATION-TYPE**: Provides the administratively-assigned name of the object.
- **OBJECTS**: Provides an ordered list of MIB objects that are in the trap.
- **STATUS**: Identifies the status of the object. Values are current, obsolete, and deprecated.
- **DESCRIPTION**: Provides the notification information.

System Object IDs

Infoblox uses the SNMP system object identifier sysObjectID to identify Infoblox appliances. The following is a definition of sysObjectID from the SNMPv2 MIB, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*:

<table>
<thead>
<tr>
<th><strong>OBJECT-TYPE</strong></th>
<th>sysObjectID</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SYNTAX</strong></td>
<td>Object Identifier</td>
</tr>
<tr>
<td><strong>MAX-ACCESS</strong></td>
<td>read-only</td>
</tr>
<tr>
<td><strong>STATUS</strong></td>
<td>current</td>
</tr>
<tr>
<td><strong>DESCRIPTION</strong></td>
<td>&quot;The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining <code>what kind of box' is being managed. For example, if vendor </code>Flintstones,Inc.' was assigned the subtree 1.3.6.1.4.1.424242, it could assign the identifier 1.3.6.1.4.1.424242.1.1 to its `Fred Router'.&quot;</td>
</tr>
</tbody>
</table>

Table 11.1 lists the enterprise IDs and their corresponding Infoblox hardware platforms that an SNMP query can return when you request the sysObjectID value. Note that the IDs shown in the table do not include 1.3.6.1.4.1.7779.1. (the infobloxProducts prefix).

Table 11.1  sysObjectID for Infoblox Hardware

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>ibDefault</td>
<td>Default environments, such as chroot</td>
</tr>
<tr>
<td>1001</td>
<td>ibRsp2</td>
<td>vNIOS appliances on Riverbed Services Platforms</td>
</tr>
<tr>
<td>1002</td>
<td>ibCisco</td>
<td>vNIOS appliances on Cisco Application eXtension Platforms</td>
</tr>
<tr>
<td>1003</td>
<td>ibvm</td>
<td>vNIOS appliances on VMware ESX or ESXi servers</td>
</tr>
<tr>
<td>1004</td>
<td>ibvnios</td>
<td>Virtual NIOS</td>
</tr>
<tr>
<td>1101</td>
<td>ib1000</td>
<td>Infoblox-1000 appliances</td>
</tr>
<tr>
<td>1102</td>
<td>ib1200</td>
<td>Infoblox-1200 appliances</td>
</tr>
<tr>
<td>1103</td>
<td>ib500</td>
<td>Infoblox-500 appliances</td>
</tr>
<tr>
<td>1201</td>
<td>ib550</td>
<td>Infoblox-550 appliances</td>
</tr>
<tr>
<td>1202</td>
<td>ib1050</td>
<td>Infoblox-1050 appliances</td>
</tr>
<tr>
<td>1203</td>
<td>ib1550</td>
<td>Infoblox-1550 appliances</td>
</tr>
<tr>
<td>1204</td>
<td>ib1552</td>
<td>Infoblox-1552 appliances</td>
</tr>
<tr>
<td>1205</td>
<td>ib2000</td>
<td>Infoblox-2000 appliances</td>
</tr>
<tr>
<td>1206</td>
<td>ib250</td>
<td>Infoblox-250 appliances</td>
</tr>
<tr>
<td>1207</td>
<td>ib1220</td>
<td>Infoblox-1220 appliances</td>
</tr>
<tr>
<td>1301</td>
<td>ib550a</td>
<td>Infoblox-550-A appliances</td>
</tr>
<tr>
<td>1302</td>
<td>ib1050a</td>
<td>Infoblox-1050-A appliances</td>
</tr>
<tr>
<td>1303</td>
<td>ib1550a</td>
<td>Infoblox-1550-A appliances</td>
</tr>
<tr>
<td>1304</td>
<td>ib1552a</td>
<td>Infoblox-1552-A appliances</td>
</tr>
<tr>
<td>1305</td>
<td>ib1852a</td>
<td>Infoblox-1852-A appliances</td>
</tr>
<tr>
<td>1306</td>
<td>ib250a</td>
<td>Infoblox-250-A appliances</td>
</tr>
<tr>
<td>1307</td>
<td>ib2000a</td>
<td>Infoblox-2000-A appliances</td>
</tr>
</tbody>
</table>
**INFOBLOX MIBs**

You can configure a NIOS appliance as an SNMP-managed device so that an SNMP management station can send queries to the appliance and retrieve information from its MIBs. Perform the following tasks to access the Infoblox MIBs:

1. Configure a NIOS appliance to accept queries, as described in *Accepting SNMP Queries* on page 373.
2. Load the MIB files onto the management system. To obtain the latest Infoblox MIB files:
   a. From the Data Management tab, select the Grid tab -> Grid Manager tab, and then select Download -> SNMP MIBs from the Toolbar.
   b. In the Save As dialog box, navigate to a directory to which you want to save the MIBs.
   c. Click Save.
3. Use a MIB browser or SNMP management application to query the objects in each MIB.

The NIOS appliance allows read-only access to the MIBs. This is equivalent to the *Get* and *Get Next* operations in SNMP.

**Loading the Infoblox MIBs**

If you are using an SNMP manager toolkit with strict dependency checking, you must download the following Infoblox MIBs in the order they are listed:

1. IB-SMI-MIB.txt
2. IB-TRAP-MIB.txt
3. IB-PLATFORMONE-MIB.txt
4. IB-DNSONE-MIB.txt
5. IB-DHCPONE-MIB.txt

In addition, if the SNMP manager toolkit you use requires a different MIB file naming convention, you can rename the MIB files accordingly.

**NET-SNMP MIBs**

NIOS appliances support NET-SNMP (formerly UCD-SNMP), a collection of applications used to implement the SNMP protocol. The NET-SNMP MIBs provide the top-level infrastructure for the SNMP MIB tree. They define, among other things, the objects in the SNMP traps that the agent sends when the SNMP engine starts and stops. For information about NET-SNMP and the MIB files distributed with NET-SNMP, refer to [http://net-snmp.sourceforge.net/](http://net-snmp.sourceforge.net/).

For SNMP traps to function probably, you must download the following NET-SNMP MIBs directly from [http://net-snmp.sourceforge.net/docs/mibs/](http://net-snmp.sourceforge.net/docs/mibs/):

- NET-SNMP-MIB
- UCD-SNMP-MIB

**Note:** Ensure that you save the MIBs as text files in the directory to which you save all the other MIB files.
ibTrap MIB

NIOS appliances send SNMP traps when events, internal process failures, or critical service failures occur. The ibTrap MIB defines the types of traps that a NIOS appliance sends and the value that each MIB object represents. The Infoblox SNMP traps report objects which the ibTrap MIB defines. Figure 11.3 illustrates the ibTrap MIB structure. It provides the OID and textual description for each object.

Note: OIDs shown in the illustrations and tables in this section do not include the prefix .1.3.6.1.4.1.7779.

The ibTrap MIB comprises two trees, ibTrapOneModule and ibNotificationVarBind. The ibTraponeModule tree contains objects for the types of traps that a NIOS appliance sends. The ibNotificationVarBind tree contains objects that the Infoblox SNMP traps report. You cannot send queries for the objects in this MIB module. The objects are used only in the SNMP traps.

Figure 11.3 ibTrapOne MIB Structure
Monitoring with SNMP

Interpreting Infoblox SNMP Traps

Depending on the SNMP management application your management system uses, the SNMP traps you receive may list the OIDs for all relevant MIB objects from both the ibTrapOneModule and ibNotificationVarBind trees. For OIDs that have string values, the trap lists the text. For OIDs that contain integers, you can use the tables in this section to find out the values. Some SNMP management applications list only the object names and their corresponding values in the SNMP traps. Whether or not your SNMP management application lists OIDs, you can use the tables in this section to find out the corresponding value and definition for each MIB object.

The following is a sample trap a NIOS appliance sends:

```
0:00:10.80 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.7779.3.1.1.1.1.4.0
SNMPv2-SMI::enterprises.7779.3.1.1.1.2.1.0 = STRING: "10.35.1.156"
SNMPv2-SMI::enterprises.7779.3.1.1.1.2.3.0 = STRING: "ntp_sync"
SNMPv2-SMI::enterprises.7779.3.1.1.1.2.9.0 = INTEGER: 15
SNMPv2-SMI::enterprises.7779.3.1.1.1.2.10.0 = INTEGER: 16
SNMPv2-SMI::enterprises.7779.3.1.1.1.2.11.0 = STRING: "The NTP service is out of synchronization."
```

The sample trap lists the OIDs and their corresponding values that can help you identify the cause of an event or problem. To identify the possible cause and recommended actions for the trap, use the ibTrapDesc tables. For information, see ibTrapDesc (OID 3.1.1.1.2.11.0) on page 338.

You can interpret the sample trap as follows:

- **Using the `ibTrapOneModule` table**, you find out OID 7779.3.1.1.1.1.4.0 represents an Object State Change trap. This trap includes the following objects: ibNodeName, ibObjectName, ibPreviousState, ibCurrentState, and ibTrapDesc. For each object, the trap displays the OID and its corresponding value. The following is how you can interpret the rest of the trap:
  - **ibNodeName (OID 7779.3.1.1.1.2.1.0)**
    - Using the `ibNotificationVarBind (OID 3.1.1.1.2)` table, you find out OID 7779.3.1.1.1.2.1.0 represents the MIB object ibNodeName, which is the IP address of the appliance on which the trap occurred. Therefore, the statement "7779.3.1.1.1.2.1.0 = STRING: "10.35.1.156" SNMPv2-SMI::enterprises." tells you the IP address of the appliance on which the trap occurred.
  - **ibObjectName (OID 7779.3.1.1.1.2.3.0)**
    - The statement "7779.3.1.1.1.1.2.3.0 = STRING: "ntp_sync" SNMPv2-SMI::enterprises." tells you the MIB object ibObjectName, which is the name of the object for which the trap was generated, has a value of "ntp_sync" that indicates NTP synchronization issues.
  - **ibPreviousState (OID 7779.3.1.1.1.2.9.0)**
    - The statement "7779.3.1.1.1.1.2.9.0 = INTEGER: 15 SNMPv2-SMI::enterprises." tells you the MIB object ibPreviousState, which indicates the previous state of the appliance, has a value of 15. Using the ibPreviousState and ibCurrentState Values table, you know that 15 represents “ntp-sync-up”, which means the NTP server was up and running.
  - **ibCurrentState (OID 7779.3.1.1.1.1.2.10.0)**
    - The statement "7779.3.1.1.1.1.2.10.0 = INTEGER: 16 SNMPv2-SMI::enterprises." tells you the MIB object ibCurrentState, which indicates the current state of the appliance, has a value of 16. Using the ibPreviousState and ibCurrentState Values table, you know that 16 represents “ntp-sync-down”, which means the NTP server is now out of sync.
  - **ibTrapDesc (OID 7779.3.1.1.1.1.2.11.0)**
    - The last statement "7779.3.1.1.1.1.2.11.0 = STRING: "The NTP service is out of synchronization." states the description of the trap. Using the Object State Change Traps table for ibTrapDesc, you can find out the trap description and recommended actions for this problem.
Types of Traps (OID 3.1.1.1.1)

ibTrapOneModule defines the types of traps that the NIOS appliance can send. There are five types of SNMP traps. Table 11.2 describe the types of traps and their objects in the ibTrapOneModule tree.

Table 11.2  ibTrapOneModule

<table>
<thead>
<tr>
<th>OID</th>
<th>Trap Type</th>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1.1.1.0</td>
<td>Equipment Failure</td>
<td>ibEquipmentFailureTrap</td>
<td>The NIOS appliance generates this trap when a hardware failure occurs. This trap includes the following objects:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ibNodeName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ibTrapSeverity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ibObjectName (equipment name)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ibProbableCause</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ibTrapDesc</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For a list of trap descriptions, see Equipment Failure Traps on page 338.</td>
</tr>
<tr>
<td>3.1.1.1.2.0</td>
<td>Processing and Software</td>
<td>ibProcessingFailureTrap</td>
<td>The NIOS appliance generates this trap when a failure occurs in one of the software processes. This trap includes the following objects:</td>
</tr>
<tr>
<td></td>
<td>Failure</td>
<td></td>
<td>• ibNodeName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ibTrapSeverity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ibSubsystemName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ibProbableCause</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ibTrapDesc</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For a list of trap descriptions, see Processing and Software Failure Traps on page 339.</td>
</tr>
</tbody>
</table>
### 3.1.1.1.3.0 Threshold Crossing

The NIOS appliance generates this trap when any of the following events occur:
- System memory or disk usage exceeds 90%.
- A problem occurs when the grid master replicates its database to its grid members.
- DHCP address usage crosses a watermark threshold. For more information about tracking IP address usage, see Chapter 32, IP Address Management, on page 777.
- The number or percentage of the DNS security alerts exceeds the thresholds of the DNS security alert triggers.

This trap includes the following objects:
- `ibNodeName`
- `ibObjectName` (threshold name)
- `ibCurThresholdvalue`
- `ibThresholdHigh`
- `ibThresholdLow`
- `ibTrapDesc`

For a list of trap descriptions, see Threshold Crossing Traps on page 344.

### 3.1.1.1.4.0 Object State Change

The NIOS appliance generates this trap when there is a change in its state, such as:
- The link to one of the configured ports goes down, and then goes back up again.
- A failover occurs in an HA (high availability) pair configuration.
- A member connects to the grid master.
- An appliance in a grid goes offline.

This trap includes the following objects:
- `ibNodeName`
- `ibObjectName`
- `ibPreviousState`
- `ibCurrentState`
- `ibTrapDesc`

For a list of possible trap descriptions, see Object State Change Traps on page 349.

<table>
<thead>
<tr>
<th>OID</th>
<th>Trap Type</th>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
</table>
| 3.1.1.1.3.0   | Threshold Crossing | ibThresholdCrossingEvent | The NIOS appliance generates this trap when any of the following events occur:  
|               |                    |                     | - System memory or disk usage exceeds 90%.  
|               |                    |                     | - A problem occurs when the grid master replicates its database to its grid members.  
|               |                    |                     | - DHCP address usage crosses a watermark threshold. For more information about tracking IP address usage, see Chapter 32, IP Address Management, on page 777.  
|               |                    |                     | - The number or percentage of the DNS security alerts exceeds the thresholds of the DNS security alert triggers.  
|               |                    |                     | This trap includes the following objects:  
|               |                    |                     | - `ibNodeName`
|               |                    |                     | - `ibObjectName` (threshold name)
|               |                    |                     | - `ibCurThresholdvalue`
|               |                    |                     | - `ibThresholdHigh`
|               |                    |                     | - `ibThresholdLow`
|               |                    |                     | - `ibTrapDesc`
|               |                    |                     | For a list of trap descriptions, see Threshold Crossing Traps on page 344. |
| 3.1.1.1.4.0   | Object State Change | ibStateChangedEvent   | The NIOS appliance generates this trap when there is a change in its state, such as:  
|               |                    |                     | - The link to one of the configured ports goes down, and then goes back up again.  
|               |                    |                     | - A failover occurs in an HA (high availability) pair configuration.  
|               |                    |                     | - A member connects to the grid master.  
|               |                    |                     | - An appliance in a grid goes offline.  
|               |                    |                     | This trap includes the following objects:  
|               |                    |                     | - `ibNodeName`
|               |                    |                     | - `ibObjectName`
|               |                    |                     | - `ibPreviousState`
|               |                    |                     | - `ibCurrentState`
|               |                    |                     | - `ibTrapDesc`
|               |                    |                     | For a list of possible trap descriptions, see Object State Change Traps on page 349. |
### Infoblox MIBs

**3.1.1.1.5.0 Process Started and Stopped**

The NIOS appliance generates this type of trap when any of the following events occur:
- When you enable HTTP redirection.
- When you change the HTTP access setting.
- When you change the HTTP session time out setting.
- When a failover occurs in an HA pair configuration.

This trap includes the following objects:
- `ibNodeName`
- `ibSubsystemName`
- `ibTrapDesc`

For a list of possible trap descriptions, see "Process Started and Stopped Traps" on page 350.

<table>
<thead>
<tr>
<th>OID</th>
<th>Trap Type</th>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1.1.5.0</td>
<td>Process Started and Stopped</td>
<td>ibProcStartStopTrap</td>
<td>The NIOS appliance generates this type of trap when any of the following events occur:</td>
</tr>
</tbody>
</table>

- When you enable HTTP redirection.
- When you change the HTTP access setting.
- When you change the HTTP session time out setting.
- When a failover occurs in an HA pair configuration.

This trap includes the following objects:
- `ibNodeName`
- `ibSubsystemName`
- `ibTrapDesc`

For a list of possible trap descriptions, see "Process Started and Stopped Traps" on page 350.
### Trap Binding Variables (OID 3.1.1.1.2)

Each SNMP trap contains information about the event or the problem. The Infoblox SNMP traps include MIB objects and their corresponding values from the `ibNotificationVarBind` module. *Table 11.3* describes the objects in the `ibNotificationVarBind` module.

*Table 11.3* *`ibNotificationVarBind (OID 3.1.1.1.2)`*

**Note:** The OIDs shown in the following table do not include the prefix “.1.3.6.1.4.1.7779.”.

<table>
<thead>
<tr>
<th>OID</th>
<th>MIB Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1.1.2.1.0</td>
<td><code>ibNodeName</code> (DisplayString)</td>
<td>The IP address of the appliance on which the trap occurs. This may or may not be the same as the appliance that sends the trap. This object is used in all types of traps.</td>
</tr>
<tr>
<td>3.1.1.1.2.2.0</td>
<td><code>ibTrapSeverity</code> (Integer)</td>
<td>The severity of the trap. There are five levels of severity. See <em>Trap Severity (OID 3.1.1.1.2.2.0)</em> on page 333 for details.</td>
</tr>
</tbody>
</table>
| 3.1.1.1.2.3.0      | `ibObjectName` (DisplayString) | The name of the object for which the trap was generated. This is used in the Equipment Failure traps, Threshold Crossing Event traps, and the Object State Change traps. The following shows what this object represents depending on the type of traps:  
  - Equipment Failure traps: The equipment name.  
  - Threshold Crossing Event traps: The object name of the trap.  
  - State Change traps: The object that changes state. |
| 3.1.1.1.2.4.0      | `ibProbableCause` (Integer)    | The probable cause of the trap. See *`ibProbableCause Values`* on page 334 for the definitions of each value.                                 |
| 3.1.1.1.2.5.0      | `ibSubsystemName` (DisplayString) | The subsystem for which the trap was generated, such as NTP or SNMP. This object is used in the Processing and Software Failure traps and the Process Start and Stop traps. See *`ibSubsystemName Values (OID 3.1.1.1.2.9.0)`* on page 335 for definitions. |
| 3.1.1.1.2.6.0      | `ibCurThresholdValue` (Integer) | The current value of the threshold counter. This object is used in the Threshold Crossing traps.                                               |
| 3.1.1.1.2.7.0      | `ibThresholdHigh` (Integer)    | The value for the high watermark. This only applies when the appliance sends a trap to indicate that DHCP address usage is above the configured high watermark value for a DHCP address range. This object is used in Threshold Crossing traps. For additional information, see *Configuring Thresholds for DHCP Ranges* on page 634. |
| 3.1.1.1.2.8.0      | `ibThresholdLow` (Integer)     | The value for the low watermark. This only applies when the appliance sends a trap to indicate that DHCP address usage went below the configured low watermark value for a DHCP address range. This object is used in Threshold Crossing traps. For additional information, see *`ibTrap MIB`* on page 327. |
| 3.1.1.1.2.9.0      | `ibPreviousState` (Integer)    | The previous state of the appliance. This object is used in the Object State Change traps. See *`ibPreviousState (OID 3.1.1.1.2.9.0)`* and *`ibCurrentState (OID 3.1.1.1.2.10.0)`* on page 337 for definitions of each value. |
**Infoblox MIBs**

**Trap Severity (OID 3.1.1.1.2.2.0)**

The object `ibTrapSeverity` defines the severity level for each Infoblox SNMP trap. There are five levels of severity.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Undetermined</td>
</tr>
<tr>
<td>2</td>
<td>Informational: Event that requires no further action.</td>
</tr>
<tr>
<td>3</td>
<td>Minor: Event that does not require user intervention.</td>
</tr>
<tr>
<td>4</td>
<td>Major: Event that requires user intervention and assistance from Infoblox Technical Support.</td>
</tr>
<tr>
<td>5</td>
<td>Critical: Problem that affects services and system operations, and requires assistance from Infoblox Technical Support.</td>
</tr>
</tbody>
</table>

**Table 1.1**

<table>
<thead>
<tr>
<th>OID</th>
<th>MIB Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1.1.2.10.0</td>
<td><code>ibCurrentState</code> (Integer)</td>
<td>The current state of the appliance. This object is used in the Object State Change traps. See <code>ibPreviousState (OID 3.1.1.1.2.9.0)</code> and <code>ibCurrentState (OID 3.1.1.1.2.10.0)</code> on page 337 for the definition of each value.</td>
</tr>
<tr>
<td>3.1.1.1.2.11.0</td>
<td><code>ibTrapDesc</code> (DisplayString)</td>
<td>The description of the trap. This object is used in all types of traps. See <code>ibTrapDesc (OID 3.1.1.1.2.11.0)</code> on page 338 for the description, possible cause, and recommended actions for each Infoblox SNMP trap.</td>
</tr>
</tbody>
</table>
ibProbableCause Values (OID 3.1.1.2.4.0)

*Table 11.5* lists the values that are associated with the object ibProbableCause (OID 3.1.1.2.4.0). These values provide information about the events, such as software failures, that trigger traps.

<table>
<thead>
<tr>
<th>Value</th>
<th>OID 3.1.1.2.4.0</th>
<th>ibProbableCause</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>ibClear</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>ibUnknown</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>ibPrimaryDiskFailure</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ibFanFailure-old</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>ibPowerSupplyFailure</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>ibDBFailure</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>ibApacheSoftwareFailure</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>ibSerialConsoleFailure</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>ibControldSoftwareFailure</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>ibUpgradeFailure</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>ibSNMPDFailure</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>ibSSHDSoftwareFailure</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>ibNTPDSoftwareFailure</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>ibClusterdSoftwareFailure</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>ibLCDSoftwareFailure</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>ibDHCPdSoftwareFailure</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>ibNamedSoftwareFailure</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>ibAuthServerGroupDown</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>ibAuthServerGroupUp</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>ibNTLMSoftwareFailure</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>ibNetBIOSDaemonFailure</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>ibWindowBindDaemonFailure</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>ibTFTPDSoftwareFailure</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>ibBackupSoftwareFailure</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>ibBackupDatabaseSoftwareFailure</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>ibBackupModuleSoftwareFailure</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>ibBackupSizeSoftwareFailure</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>ibBackupLockSoftwareFailure</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>ibHTTPFileDistSoftwareFailure</td>
<td></td>
</tr>
</tbody>
</table>
Table 11.5 lists the values that are associated with the object `ibSubsystemName (OID 3.1.1.1.2.9.0)`. These values provide information about the subsystems that trigger the traps.

**Table 11.5 ibSubsystemName Values**

<table>
<thead>
<tr>
<th>Value</th>
<th>OID 3.1.1.1.2.9.0</th>
<th>ibSubsystemName</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>ibOSPFSoftwareFailure</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>ibAuthDHCNNamedSoftwareFailure</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>ibFan1Failure</td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>ibFan2Failure</td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>ibFan3Failure</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>ibFan1OK</td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>ibFan2OK</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>ibFan3OK</td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>ibFTPSSoftwareFailure</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>ibPowerSupplyOK</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>ibWebUISoftwareFailure</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>ibADAjentSyncFailure</td>
<td></td>
</tr>
<tr>
<td>3001</td>
<td>ibRAIDIsOptimal</td>
<td></td>
</tr>
<tr>
<td>3002</td>
<td>ibRAIDIsDegraded</td>
<td></td>
</tr>
<tr>
<td>3003</td>
<td>ibRAIDIsRebuilding</td>
<td></td>
</tr>
<tr>
<td>3004</td>
<td>ibRAIDStatusUnknown</td>
<td></td>
</tr>
<tr>
<td>3005</td>
<td>ibRAIDBatteryIsOK</td>
<td></td>
</tr>
<tr>
<td>3006</td>
<td>ibRAIDBatteryFailed</td>
<td></td>
</tr>
</tbody>
</table>

**ibSubsystemName Values (OID 3.1.1.1.2.9.0)**

Table 11.5 lists the values that are associated with the object `ibSubsystemName (OID 3.1.1.1.2.9.0)`. These values provide information about the subsystems that trigger the traps.
<table>
<thead>
<tr>
<th>Value</th>
<th>OID</th>
<th>ibSubsystemName</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td></td>
<td>serial_console</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>controld</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>Snmpd</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>Sshd</td>
</tr>
<tr>
<td>16</td>
<td></td>
<td>Ntpd</td>
</tr>
<tr>
<td>17</td>
<td></td>
<td>Clusterd</td>
</tr>
<tr>
<td>18</td>
<td></td>
<td>Lcd</td>
</tr>
<tr>
<td>19</td>
<td></td>
<td>Dhcpd</td>
</tr>
<tr>
<td>20</td>
<td></td>
<td>Named</td>
</tr>
<tr>
<td>24</td>
<td></td>
<td>NTLM</td>
</tr>
<tr>
<td>25</td>
<td></td>
<td>Netbiosd</td>
</tr>
<tr>
<td>26</td>
<td></td>
<td>Winbindd</td>
</tr>
<tr>
<td>27</td>
<td></td>
<td>Tftpd</td>
</tr>
<tr>
<td>29</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>30</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>31</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>32</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>33</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>34</td>
<td></td>
<td>HTTPd</td>
</tr>
<tr>
<td>35</td>
<td></td>
<td>OSPF</td>
</tr>
</tbody>
</table>
ibPreviousState (OID 3.1.1.1.2.9.0) and ibCurrentState (OID 3.1.1.1.2.10.0)

The ibPreviousState object indicates the state of the appliance before the event triggered the trap. The ibCurrentState object indicates the current state of the appliance. Table 11.6 shows the message and description for each state.

Table 11.6  ibPreviousState and ibCurrentState Values

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ha-active</td>
<td>The HA pair is in ACTIVE state.</td>
</tr>
<tr>
<td>2</td>
<td>ha-passive</td>
<td>The HA pair is in PASSIVE state.</td>
</tr>
<tr>
<td>3</td>
<td>ha-initial</td>
<td>The HA pair is in INITIAL state.</td>
</tr>
<tr>
<td>4</td>
<td>grid-connected</td>
<td>The appliance is connected to the grid.</td>
</tr>
<tr>
<td>5</td>
<td>grid-disconnected</td>
<td>The appliance is not connected to the grid.</td>
</tr>
<tr>
<td>6</td>
<td>enet-link-up</td>
<td>The ethernet port link is active.</td>
</tr>
<tr>
<td>7</td>
<td>enet-link-down</td>
<td>The ethernet port link is inactive.</td>
</tr>
<tr>
<td>8</td>
<td>replication-online</td>
<td>The replication is online.</td>
</tr>
<tr>
<td>9</td>
<td>replication-offline</td>
<td>The replication is offline.</td>
</tr>
<tr>
<td>10</td>
<td>replication-snapshotting</td>
<td>The replication is snapshotting.</td>
</tr>
<tr>
<td>11</td>
<td>service-up</td>
<td>The service is up.</td>
</tr>
<tr>
<td>12</td>
<td>service-down</td>
<td>The service is down.</td>
</tr>
<tr>
<td>13</td>
<td>ha-replication-online</td>
<td>The HA pair replication is online.</td>
</tr>
<tr>
<td>14</td>
<td>ha-replication-offline</td>
<td>The HA pair replication is offline.</td>
</tr>
<tr>
<td>15</td>
<td>ntp-syn-up</td>
<td>The NTP server is synchronizing.</td>
</tr>
<tr>
<td>16</td>
<td>ntp-syn-down</td>
<td>The NTP server is out of sync.</td>
</tr>
</tbody>
</table>
ibTrapDesc (OID 3.1.1.1.2.11.0)

The ibTrapDesc object lists the trap messages of all Infoblox SNMP traps. This section lists all the SNMP traps by their trap types. Each trap table describes the trap message, severity, cause, and recommended actions.

**Note:** Contact Infoblox Technical Support for assistance when the recommended actions do not resolve the problems.

### Equipment Failure Traps

<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.2.11.0</th>
<th>ibTrapSeverity OID 3.1.1.1.2.2</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary Drive Full</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary drive is full.</td>
<td>Major</td>
<td>The primary disk drive reached 100% of usage.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td><strong>Fan Monitoring</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fan &lt;n&gt; failure has occurred.</td>
<td>Minor</td>
<td>The specified fan failed. The fan number &lt;n&gt; can be 1, 2, or 3.</td>
<td>Inspect the specified fan for mechanical or electrical problems.</td>
</tr>
<tr>
<td>Fan &lt;n&gt; is OK.</td>
<td>Informational</td>
<td>The specified fan is functioning properly. The fan number &lt;n&gt; can be 1, 2, or 3.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

**Power Supply Failure: monitored at 1 minute**

| A power supply failure has occurred. | Major | The power supply failed. | Inspect the power supply for the possible cause of the failure. |
### RAID monitoring, at 1 minute interval

<table>
<thead>
<tr>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>A RAID battery failure has occurred. Major The system RAID battery failed. The alert light is red.</td>
<td>Inspect the battery for the possible cause of the failure.</td>
</tr>
<tr>
<td>The system's RAID battery is OK. Informational The system RAID battery is charging and functioning properly. The alert light changed from red to green.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Unable to retrieve RAID array state! Undetermined The appliance failed to retrieve the RAID array state. The alert light is red.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>The system's RAID array is now running in an optimal state. Informational The RAID system is functioning at an optimal state.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>The system's RAID array is in a degraded state. Major The RAID system is degrading.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>The system's RAID array is rebuilding. Minor The RAID system is rebuilding.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

### Processing and Software Failure Traps

<table>
<thead>
<tr>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>A named daemon monitoring failure has occurred. Critical The named process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>A DHCP daemon monitoring failure has occurred. Critical The dhcpd process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>An SSH daemon failure has occurred. Major The sshd process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>An NTP daemon failure has occurred. Major The ntpd process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Description/Cause</td>
<td>Recommended Actions</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td><strong>Cluster Daemon Failure</strong></td>
<td>A cluster daemon failure has occurred. Critical The clusterd process failed. Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td><strong>LCD Daemon Failure</strong></td>
<td>An LCD daemon failure has occurred. Major The LCD process failed. The alert light is yellow. 1. Inspect the LCD panel for the possible cause of this problem. 2. Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td><strong>Apache Software httpd failure, monitored every 2 minutes</strong></td>
<td>An Apache software failure has occurred. Critical The request to monitor the Apache server failed. Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td><strong>Serial Console Failure</strong></td>
<td>An Infoblox serial console software failure has occurred. Major The Infoblox serial console failed. Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td><strong>Controld Software Failure</strong></td>
<td>A controld failure has occurred. Critical The controld process failed. Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td><strong>SNMP Sub-agent Failure</strong></td>
<td>An SNMP server failure has occurred. Major The one-subagent process failed. Review the syslog file to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>
| **TFTPD and FTPD Failure** | A TFTPD daemon failure has occurred. Critical The tftpd process failed. Review the syslog file to identify the possible cause of this problem.  
An FTPD daemon failure has occurred. Critical The ftpd process failed. Review the syslog file to identify the possible cause of this problem. |
| **HTTP File Distribution, monitored at 10 second intervals** | An HTTP file distribution daemon failure has occurred. Critical The HTTP file distribution process failed. Review the syslog file to identify the possible cause of this problem. |
| **auth_named Process Failure** | An auth named server failure has occurred. Critical The auth_named server failed. Review the syslog file to identify the possible cause of this problem. |
| **DNS ONE quagga Processes (zebra & ospfd)** | An OSPF routing daemon failure has occurred. Critical Either the zebra process or the ospfd process failed. Review the syslog file to identify the possible cause of this problem. |
### Backup Failure

<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.2.11.0</th>
<th>ibTrapServerity OID 3.1.1.1.2.2</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
</table>
| Backup failed.               | Not implemented               | The backup failed. One of the following could be the cause of the failure:  
- The appliance could not access a backup directory.  
- The backup was interrupted by one of the following signals: SIGINT, SIGHUP, or SIGTERM.  
- Incorrect login or connection failure in an FTP backup.  
- The backup failed to create temporary files. | Review the syslog file to identify the possible cause of this problem. |

### Database Backup Failure

| Database backup failed. | Not implemented | The db_dump process failed. | Review the syslog file to identify the possible cause of this problem. |

### Backup Module Failure


### Backup File Size Exceeded

| File size exceeded the quota. Backup failed. | Not implemented | The backup failed because the file size exceeded the limit of 5GB. | Limit the size of the backup file to less than 5GB. |

| Another backup is in progress. Backup will not be performed. | Not implemented | The backup failed because of an attempt to back up or merge files while another backup or restore was in progress. | Wait until the backup or restore is complete before starting another backup. |
## Monitoring with SNMP

### Watchdog Process Monitoring

<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.2.11.0</th>
<th>ibTrapServerity OID 3.1.1.1.2.2</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>WATCHDOG: &lt;registered client name&gt; failed on &lt;server IP address&gt;</td>
<td>Critical</td>
<td>The watchdog process detected a registered client failure on a specific server. The &lt;registered client name&gt; could be one of the following: • Clusterd_timeout • DB_Sentinel • Process_Manager • Clusterd_monitor • Disk_monitor</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>

### Microsoft Server

<table>
<thead>
<tr>
<th>Microsoft server hostname has failed.</th>
<th>Major</th>
<th>The Microsoft server could not be reached.</th>
<th>Check that the Microsoft server is connected to the network and configured properly.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft server hostname is OK.</td>
<td>Informational</td>
<td>The Microsoft server can be reached and is functioning properly</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

### Microsoft DNS/DHCP Service

<table>
<thead>
<tr>
<th>Service connection to Microsoft DNS server hostname has failed.</th>
<th>Major</th>
<th>The Microsoft DNS service is not responding.</th>
<th>Check that the DNS service is configured and running on the Microsoft server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service connection to Microsoft DHCP server hostname has failed.</td>
<td>Major</td>
<td>The Microsoft DHCP service is not responding.</td>
<td>Check that the DHCP service is configured and running on the Microsoft server.</td>
</tr>
<tr>
<td>Service connection to Microsoft DNS server hostname is OK.</td>
<td>Informational</td>
<td>The Microsoft DNS service is responding.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Service connection to Microsoft DHCP server hostname is OK.</td>
<td>Informational</td>
<td>The Microsoft DHCP service is responding.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>ibTrapDesc OID 3.1.1.1.2.11.0</td>
<td>ibTrapSeverity OID 3.1.1.1.2.2</td>
<td>Description/Cause</td>
<td>Recommended Actions</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>-------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>NAC Authentication server group is down</td>
<td>Major</td>
<td>None of the servers in the NAC authentication server group can be reached.</td>
<td>Review the syslog.</td>
</tr>
<tr>
<td>NAC Authentication server group is up</td>
<td>Informational</td>
<td>The NAC authentication server group is responding.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>
# Threshold Crossing Traps

<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.2.11.0</th>
<th>ibObjectName OID 3.1.1.2.3.0</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Memory Usage</td>
<td>memory</td>
<td>The appliance ran out of memory. The appliance encountered this problem when one of the following occurred:</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The total free memory on the appliance was less than or equal to 0%.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The total physical memory was less than the total free memory.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The percentage of free memory compared to the total physical memory was less than 5%, and the free swap percentage was less than 80%.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The percentage of free memory compared to the total physical memory was less than 5%, plus the numbers of both swap INs and swap OUTs were greater than or equal to 3,200.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The percentage of free memory compared to the total physical memory was between 5% and 10%, the free swap percentage was greater than or equal to 80%, plus the numbers of both swap INs and swap OUTs were greater than or equal to 3,200.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The percentage of free memory compared to the total physical memory was greater than 10%, the free swap percentage was less than 80%, plus the numbers of both swap INs and swap OUTs were greater than or equal to 3,200.</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Free memory = free physical RAM + free cache buffers. The high threshold for swap pages is 3,200.
<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.2.11.0</th>
<th>ibObjectName OID 3.1.1.1.2.3.0</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
</table>
| System memory usage is over 90%. | memory | The memory usage on the appliance exceeded 90%. The appliance encountered this problem when one of the following occurred:  
• The percentage of free memory compared to the total physical memory was less than 5%, and the free swap percentage was less than 90%.  
• The percentage of free memory compared to the total physical memory was less than 5%, plus the number of swap INs was less than 3,200 and the number of swap OUTs was greater than or equal to 3,200.  
• The percentage of free memory compared to the total physical memory was between 5% and 10%, and the free swap percentage was less than 80%.  
• The percentage of free memory compared to the total physical memory was greater than 5%, plus the number of swap INs was less than 3,200 and the number of swap OUTs was greater than or equal to 3,200. | Review the syslog file to identify the possible cause of this problem. |
| **Note:** Free memory = free physical RAM + free cache buffers. The high threshold for swap pages is 3,200. | |
| System memory is OK. | memory | The memory usage on the system is back to normal from the previous state. | No action is required. |
### Primary Hard Drive Usage (monitored every 30 seconds)

<table>
<thead>
<tr>
<th>System primary hard disk usage is over 90%</th>
<th>disk usage</th>
<th>The primary hard disk usage exceeded 90%. The alert light is yellow.</th>
<th>Review the syslog file to identify the possible cause of this problem.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary drive is full.</td>
<td>disk usage</td>
<td>The primary hard disk usage exceeded 95%. The alert light is red.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Primary drive usage is OK.</td>
<td>disk usage</td>
<td>The primary hard disk usage is 85% or lower. The alert light is green.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

### Replication Statistics Monitoring

| Grid queue replication problem. | For send trap: Cluster_Send_Queue  
For receive trap: Cluster_Recv_Queue | The system encountered this problem when all of the following conditions occurred:  
• The node was online.  
• The number of the replication queue being sent from the master column was greater than 0, or the number of the queue received was greater than 0.  
• It was more than 10 minutes since the last replication queue was sent and monitored. | Review the syslog file to identify the possible cause of this problem. |

---

**ibTrapDesc**
OID 3.1.1.1.2.11.0

**ibObjectName**
OID 3.1.1.1.2.3.0

<table>
<thead>
<tr>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>No action is required.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>ibTrapDesc OID 3.1.1.1.2.11.0</td>
<td>ibObjectName OID 3.1.1.1.2.3.0</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td><strong>DHCP Range Threshold Crossing</strong></td>
<td></td>
</tr>
<tr>
<td>DHCP threshold crossed:</td>
<td></td>
</tr>
<tr>
<td>Member: &lt;DHCP server node VIP&gt;</td>
<td></td>
</tr>
<tr>
<td>Network: &lt;network&gt;/ &lt;network view&gt;</td>
<td></td>
</tr>
<tr>
<td>Range: &lt;DHCP range&gt;/ &lt;network view&gt;</td>
<td></td>
</tr>
<tr>
<td>High Watermark: &lt;high watermark percentage&gt; (95% by default)</td>
<td></td>
</tr>
<tr>
<td>Low Watermark: &lt;low watermark percentage&gt; (0% by default)</td>
<td></td>
</tr>
<tr>
<td>Current Usage: &lt;current usage percentage&gt;</td>
<td></td>
</tr>
<tr>
<td>Active Leases: &lt;number of active leases&gt;</td>
<td></td>
</tr>
<tr>
<td>Available Leases: &lt;number of available leases&gt;</td>
<td></td>
</tr>
<tr>
<td>Total Addresses: &lt;total addresses&gt;</td>
<td></td>
</tr>
</tbody>
</table>

| **DHCP DDNS Updates Deferred** | | **Threshold** | Review the syslog file to identify the possible cause of this problem. |
| DHCP DNS updates deferred: | | | |
| Retried at least once: <number of retries> | | | |
| Maximum number of deferred updates since start of problem episode (or restart): <max number> | | | |
| The DNS updates were deferred because of DDNS update errors. | | | |
### Database Capacity Usage

<table>
<thead>
<tr>
<th>Status</th>
<th>db_usage</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Over 85% database capacity used.</td>
<td>The appliance database usage exceeded 85%.</td>
<td>Increase the database capacity.</td>
</tr>
<tr>
<td>Database capacity used is OK.</td>
<td>The appliance database usage is less than 85%.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

### DNS Monitor

<table>
<thead>
<tr>
<th>Status</th>
<th>db_usage</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Monitor</td>
<td>For invalid ports: “dns_security_port” For invalid TXIDs: “dns_security_txid”</td>
<td>DNS security alert. There were actual/DNS responses to {invalid ports</td>
<td>with invalid TXID} in the last minute, comprising percent% of all responses. Primary sources: ip_address sent count, ip_address sent count. where • actual is the total number of DNS responses arrive on invalid ports or have invalid TXIDs. • percent% is the percentage of invalid DNS responses over the total number of DNS responses. • ip_address is the IP address of the primary source that generated the invalid DNS responses. • count is the number of invalid responses generated by the specified IP address. Example: DNS security alert. There were 1072 DNS responses to invalid ports in the last minute, comprising 92% of all responses. Primary sources: 10.0.0.0 sent 1058, 2.2.2.2 sent 14.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.2.11.0</th>
<th>ibObjectName OID 3.1.1.1.2.3.0</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>db_usage</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**ibTrapDesc** OID 3.1.1.1.2.11.0: This SNMP trap is generated when the database capacity usage exceeds 85%.

**ibObjectName** OID 3.1.1.1.2.3.0: The db_usage trap is used to indicate that the database usage has reached a critical level. The trap is designed to alert administrators to the potential risk of data corruption or loss due to insufficient database capacity.

**Description/Cause:** The appliance database usage exceeded 85%.

**Recommended Actions:** Increase the database capacity.

**DNS Monitor:**

- **For invalid ports:** “dns_security_port”
- **For invalid TXIDs:** “dns_security_txid”

**DNS security alert:** There were actual DNS responses to {invalid ports | with invalid TXID} in the last minute, comprising percent% of all responses. Primary sources: ip_address sent count, ip_address sent count.

**where**

- **actual** is the total number of DNS responses arrive on invalid ports or have invalid TXIDs.
- **percent%** is the percentage of invalid DNS responses over the total number of DNS responses.
- **ip_address** is the IP address of the primary source that generated the invalid DNS responses.
- **count** is the number of invalid responses generated by the specified IP address.

**Example:**

DNS security alert. There were 1072 DNS responses to invalid ports in the last minute, comprising 92% of all responses. Primary sources: 10.0.0.0 sent 1058, 2.2.2.2 sent 14.
# Object State Change Traps

<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.2.11.0</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Shutdown</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shutting down services due to database snapshot.</td>
<td>The appliance is shutting down its services while synchronizing the database with the grid master.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Shutting down services due to database snapshot.</td>
<td>The appliance is shutting down its services while synchronizing the database with the grid master.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><strong>Network Interfaces Monitoring</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LAN port link is down. Please check the connection.</td>
<td>The LAN port is up, but the link is down.</td>
<td>Check the LAN link connection.</td>
</tr>
<tr>
<td>HA port link is down. Please check the connection.</td>
<td>The HA port is up, but the link is down.</td>
<td>Check the HA link connection.</td>
</tr>
<tr>
<td>MGMT port link is down. Please check the connection.</td>
<td>The MGMT port is enabled, but the link is down.</td>
<td>Check the MGMT link connection.</td>
</tr>
<tr>
<td>LAN port link is up.</td>
<td>The LAN port link is up and running.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>HA port link is up.</td>
<td>The HA port link is up and running.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>MGMT port link is up.</td>
<td>The MGMT port link is up and running.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><strong>HA State Change from Initial to Active</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The node has become ACTIVE.</td>
<td>A node in an HA pair becomes active. The HA pair starts up.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><strong>HA State Change from Passive to Active</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The node has become ACTIVE.</td>
<td>The node changed from a passive to an active node.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><strong>HA State Change from Initial to Passive</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The node has become PASSIVE.</td>
<td>A node in an HA pair becomes passive. The HA pair starts up, and the node is not a grid master candidate.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>
### Node Connected to Grid

<table>
<thead>
<tr>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The grid member is connected to the grid master.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

### Node Disconnected to Grid

<table>
<thead>
<tr>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The grid member is not connected to the grid master.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

### Replication State Monitoring

<table>
<thead>
<tr>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ha-replication-online (13)</td>
<td>No action is required.</td>
</tr>
<tr>
<td>ha-replication-offline (14)</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

### NTP is out of sync, monitored every 30 seconds

<table>
<thead>
<tr>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The NTP server is out of synchronization.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>

### Process Started and Stopped Traps

<table>
<thead>
<tr>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The httpd process started.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>The httpd process stopped.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>
ibPlatformOne MIB

The ibPlatformOne MIB provides information about the CPU temperature of the appliance, the replication status, the average latency of DNS requests, DNS security alerts, CPU and memory utilization of the appliance, and the Infoblox service status. Figure 11.4 illustrates the structure of the PlatformOne MIB. (Note that the OIDs in the illustration do not include the prefix .1.3.6.1.4.1.7779.)

The ibPlatformOne MIB contains the following objects:

- ibCPUTemperature (IbString) tracks the CPU temperature of the appliance.
- ibClusterReplicationStatusTable provides information in tabular format about the replication status of the appliance. For information, see ibClusterReplicationStatusTable on page 353.
- ibNetworkMonitor provides information about the average latency of authoritative and nonauthoritative replies to DNS queries for different time intervals. It also provides information about invalid DNS responses that arrive on invalid ports or have invalid DNS transaction IDs. For information, see ibNetworkMonitor on page 354.
- ibHardwareType (IbString) provides information about the hardware platform. For an Infoblox appliance, it provides the model number of the Infoblox hardware platform. For vNIOS appliances, it identifies whether the hardware platform is Riverbed, Cisco, or VMware.
- ibHardwareId (IbString) provides the hardware ID of the NIOS appliance.
- ibSerialNumber (IbString) provides the serial number of the Infoblox hardware platform.
- ibNiosVersion (IbString) provides the version of the NIOS software.
- ibSystemMonitor provides information about the CPU and memory utilization of the appliance. For information, see ibSystemMonitor on page 360.

The ibPlatformOne MIB also contains the following tables that provide status of the Infoblox services as well as system and hardware services on the appliance you query:

- ibMemberServiceStatusTable provides status of the Infoblox services, such as the DNS and DHCP services, on a queried appliance. For information, see ibMemberServiceStatusTable on page 360.
- ibMemberNode1ServiceStatusTable provides status of the system and hardware services on a queried appliance. For information, see ibMemberNode1ServiceStatusTable on page 361.
- ibMemberNode2ServiceStatusTable provides status of the system and hardware services on the passive node of an HA pair if the queried appliance is the VIP or the active node of an HA pair. For independent appliances and the passive nodes of HA pairs, this table does not display any status. For information, see ibMemberNode2ServiceStatusTable on page 363.
Figure 11.4  \textit{ibPlatformOne MIB Structure}

\begin{figure}
\centering
\includegraphics[width=0.8\textwidth]{ibPlatformOne_MIB_Structure.png}
\caption{ibPlatformOne MIB Structure}
\end{figure}

(3.1.1.2) ibPlatformOne MIB
\hspace{2cm}
(3.1.1.2.1) ibPlatformOneModule
\hspace{2cm}
\vdots
\hspace{2cm}
(3.1.1.2.1.9) ibMemberServiceStatusTable \hspace{1cm} \rightarrow \textit{ibMemberServiceStatusTable Objects} on page 360
\hspace{2cm}
(3.1.1.2.1.10) ibMemberNode1ServiceStatusTable \hspace{1cm} \rightarrow \textit{ibMemberNode1ServiceStatusTable Objects} on page 362
\hspace{2cm}
(3.1.1.2.1.11) ibMemberNode2ServiceStatusTable \hspace{1cm} \rightarrow \textit{ibMemberNode2ServiceStatusTable Objects} on page 363
**ibClusterReplicationStatusTable**

*ibClusterReplicationStatusTable* (object ID 3.1.1.2.1.2.1) provides information about the grid replication status. For information about Infoblox SNMP traps, see *ibTrapDesc (OID 3.1.1.1.2.11.0)* on page 338. *Figure 11.5* shows the sub branches of *ibClusterReplicationStatusTable*.

*Figure 11.5 ibClusterReplicationStatusTable Objects*

![Diagram of ibClusterReplicationStatusTable objects]

*Table 11.7* provides information about the *ibClusterReplicationStatusTable* objects.

*Table 11.7 ibClusterReplicationStatusTable Objects*

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibClusterReplicationStatusEntry</td>
<td>A conceptual row that provides information about the grid replication status. The status indicates whether the appliance is sending replication queues, receiving queues, or having problems with the replication.</td>
</tr>
<tr>
<td>ibNodeIPAddress (IbIPAddr)</td>
<td>IP address of a grid member.</td>
</tr>
<tr>
<td>ibNodeReplicationStatus (IbString)</td>
<td>Replication status of the grid member. The replication status can be one of the following: online, offline, or snapshotting.</td>
</tr>
<tr>
<td>ibNodeQueueFromMaster (Integer)</td>
<td>“Sent” queue size from master.</td>
</tr>
<tr>
<td>ibNodeLastRepTimeFromMaster (IbString)</td>
<td>Last sent time from master.</td>
</tr>
<tr>
<td>ibNodeQueueToMaster (Integer)</td>
<td>“Receive” queue size from master.</td>
</tr>
<tr>
<td>ibNodeLastRepTimeToMaster (IbString)</td>
<td>Last receive time from master.</td>
</tr>
</tbody>
</table>
ibNetwork Monitor

As shown in Figure 11.6, the ibNetwork Monitor has one subtree, ibNetworkMonitorDNS, that branches out into the following:

- ibNetworkMonitorDNSActive (Integer) reports on whether DNS latency monitoring is enabled. This is the only object in this branch. When you send a query for this object, the appliance responds with either “active” (1) or “nonactive” (0).
- ibNetworkMonitorDNSNonAA provides information about the average latency of nonauthoritative replies to DNS queries for 1-, 5-, 15-, and 60-minute intervals. For information, see ibNetworkMonitorDNSNonAA Objects on page 356.
- ibNetworkMonitorDNSAA provides information about the average latency of authoritative replies to DNS queries for 1-, 5-, 15-, and 60-minute intervals. For information, see ibNetworkMonitorDNSAA Objects on page 357.
- ibNetworkMonitorDNSSecurity provides information about the invalid DNS responses that arrive on invalid ports or have invalid DNS transaction IDs. ibNetworkMonitorDNSSecurity branches out into the following:
  - ibNetworkMonitorDNSSecurityInvalidPort
  - ibNetworkMonitorDNSSecurityInvalidTxid
  - ibNetworkMonitorDNSSecurityInvalidPortOnly (Counter)
    - ibNetworkMonitorDNSSecurityInvalidPortCount (Counter)
  - ibNetworkMonitorDNSSecurityInvalidTxidOnly (Counter)
    - ibNetworkMonitorDNSSecurityInvalidTxidCount (Counter)
  - ibNetworkMonitorDNSSecurityInvalidTxidAndPort (Counter)
  For information, see Table 11.10 on page 358.

Figure 11.6 ibNetworkMonitor Objects
Figure 11.7  \textit{ibNetworkMonitorDNSNonAA} and \textit{ibNetworkMonitorDNSAA} Subtrees
Table 11.8 describes the objects in ibNetworkMonitorDNSNonAA. You can send queries to retrieve values for these objects.

**Table 11.8 ibNetworkMonitorDNSNonAA Objects**

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibNetworkMonitorDNSNonAAT1</td>
<td>File that contains the objects for monitoring the average latency of nonauthoritative replies to queries in the last minute.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT1AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of nonauthoritative replies to queries in the last minute.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT1Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of nonauthoritative replies in the last minute.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT5</td>
<td>File that contains the objects for monitoring the average latency of nonauthoritative replies to queries in the last five minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT5AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of nonauthoritative replies to queries in the last five minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT5Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of nonauthoritative replies in the last five minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT15</td>
<td>File that contains the objects for monitoring the average latency of nonauthoritative replies to queries in the last 15 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT15AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of nonauthoritative replies to queries in the last 15 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT15Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of nonauthoritative replies in the last 15 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT60</td>
<td>File that contains the objects for monitoring the average latency of nonauthoritative replies to queries in the last 60 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT60AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of nonauthoritative replies to queries in the last 60 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT60Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of nonauthoritative replies in the last 60 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT1440</td>
<td>File that contains the objects for monitoring the average latency of nonauthoritative replies to queries in the last 24 hours.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT1440AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of nonauthoritative replies to queries in the last 24 hours.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT1440Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of nonauthoritative replies in the last 24 hours.</td>
</tr>
</tbody>
</table>
Table 11.9 describes the objects in ibNetworkMonitorDNSAA. You can send queries to retrieve values for these objects.

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibNetworkMonitorDNSAA1</td>
<td>File that contains the objects for monitoring the average latency of authoritative replies to queries in the last minute.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAA1AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of authoritative replies to queries in the last minute.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAA1Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of authoritative replies in the last minute.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAA1</td>
<td>File that contains the objects for monitoring the average latency of authoritative replies to queries in the last minute.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAA5AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of authoritative replies to queries in the last five minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAA5Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of authoritative replies in the last five minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAA15</td>
<td>File that contains the objects for monitoring the average latency of authoritative replies to queries in the last 15 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAA15AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of authoritative replies to queries in the last 15 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAA15Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of authoritative replies in the last 15 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAA60AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of authoritative replies to queries in the last 60 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAA60Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of authoritative replies in the last 60 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAA60</td>
<td>File that contains the objects for monitoring the average latency of authoritative replies to queries in the last 60 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAA1440AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of authoritative replies to queries in the last 24 hours.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAA1440Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of authoritative replies in the last 24 hours.</td>
</tr>
</tbody>
</table>
Table 11.10 describes the objects in ibNetworkMonitorDNSSecurity. You receive SNMP traps with these objects when you enable the following:

- SNMP traps
- DNS network monitoring
- DNS alert monitoring

Table 11.10  ibNetworkMonitorDNSSecurity Objects

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidPort</td>
<td>Tracks the number of invalid DNS responses that arrive on invalid ports. For information about invalid ports, see Monitoring DNS Transactions on page 315. This object contains a subtree with six objects that track invalid ports within a certain time interval. For information, see Table 11.11.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTxid</td>
<td>Tracks the number of invalid TXIDs (DNS transaction IDs). For information about invalid TXIDs, see Monitoring DNS Transactions on page 315. This object contains a subtree with six objects that track invalid TXIDs within a certain time interval. For information, see Table 11.12.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidPortOnly (Counter)</td>
<td>Tracks the number of DNS responses with both of the following conditions:</td>
</tr>
<tr>
<td></td>
<td>• Arrive on invalid ports</td>
</tr>
<tr>
<td></td>
<td>• Have valid TXIDs</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTxidOnly (Counter)</td>
<td>Tracks the number of DNS responses with both of the following conditions:</td>
</tr>
<tr>
<td></td>
<td>• Arrive on valid ports</td>
</tr>
<tr>
<td></td>
<td>• Have Invalid TXIDs</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidPortCount (Counter)</td>
<td>Tracks the total number of invalid DNS responses that arrive on invalid ports.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTxidCount (Counter)</td>
<td>Tracks the total number of DNS responses that have invalid DNS transaction IDs.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTxidAndPort (Counter)</td>
<td>Tracks the number of DNS responses with both of the following conditions:</td>
</tr>
<tr>
<td></td>
<td>• Arrive on invalid ports</td>
</tr>
<tr>
<td></td>
<td>• Have invalid TXIDs</td>
</tr>
</tbody>
</table>
Table 11.11 describes the objects in `ibNetworkMonitorDNSSecurityInvalidPort`.

Table 11.11  *ibNetworkMonitorDNSSecurityInvalidPort Objects*

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ibNetworkMonitorDNSSecurityInvalidPort1</code> (Integer)</td>
<td>Tracks the number of invalid DNS responses that arrive on invalid ports in the last one minute.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSSecurityInvalidPort5</code> (Integer)</td>
<td>Tracks the number of invalid DNS responses that arrive on invalid ports in the last five minutes.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSSecurityInvalidPort15</code> (Integer)</td>
<td>Tracks the number of invalid DNS responses that arrive on invalid ports in the last 15 minutes.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSSecurityInvalidPort60</code> (Integer)</td>
<td>Tracks the number of invalid DNS responses that arrive on invalid ports in the last 60 minutes.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSSecurityInvalidPort1440</code> (Integer)</td>
<td>Tracks the number of invalid DNS responses that arrive on invalid ports in the last 24 hours.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSSecurityInvalidPortCount</code> (Counter)</td>
<td>Tracks the total number of invalid DNS responses that arrive on invalid ports.</td>
</tr>
</tbody>
</table>

Table 11.12 describes the objects in `ibNetworkMonitorDNSSecurityInvalidTxid`.

Table 11.12  *ibNetworkMonitorDNSSecurityInvalidTxid Objects*

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ibNetworkMonitorDNSSecurityInvalidTxid1</code> (Integer)</td>
<td>Tracks the number of DNS responses that have invalid DNS transaction IDs in the last one minute.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSSecurityInvalidTxid5</code> (Integer)</td>
<td>Tracks the number of DNS responses that have invalid DNS transaction IDs in the last five minutes.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSSecurityInvalidTxid15</code> (Integer)</td>
<td>Tracks the number of DNS responses that have invalid DNS transaction IDs in the last 15 minutes.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSSecurityInvalidTxid60</code> (Integer)</td>
<td>Tracks the number of DNS responses that have invalid DNS transaction IDs in the last 60 minutes.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSSecurityInvalidTxid1440</code> (Integer)</td>
<td>Tracks the number of DNS responses that have invalid DNS transaction IDs in the last 24 hours.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSSecurityInvalidTxidCount</code> (Counter)</td>
<td>Tracks the total number of DNS responses that have invalid DNS transaction IDs.</td>
</tr>
</tbody>
</table>
### `ibSystemMonitor`

As shown in Figure 11.4, `ibSystemMonitor` (object ID 3.1.1.2.1.2.8) has the following subtrees:

- `ibSystemMonitorCpu`: Contains `ibSystemMonitorCpuUsage` (Integer) that reports the CPU usage of the appliance.
- `ibSystemMonitorMem`: Contains `ibSystemMonitorMemUsage` (Integer) that reports the memory usage of the appliance.

*Figure 11.8  `ibSystemMonitor` Objects*

### `ibMemberServiceStatusTable`

As shown in Figure 11.9, `ibMemberServiceStatusTable` (object ID 3.1.1.2.1.2.9) has one subtree, `ibMemberServiceStatusEntry`, which contains the following objects:

- `ibServiceName` (String) reports the names of the Infoblox services. For a list of Infoblox services, see *Infoblox Services for `ibMemberServiceStatusTable`*.
- `ibServiceStatus` (Integer) reports the status of the Infoblox services. For a list of service status, see *Service Status* on page 361.
- `ibServiceDesc` (String) describes the details of the status.

`ibMemberServiceStatusTable` displays the current status of the Infoblox services on the appliance that you query. For an HA pair, this table displays the service status of the active node. If the appliance you query is the passive node of an HA pair, this table reflects the service status of the passive node, which can be “inactive” or “unknown.”

You can also query `ibMemberNode1ServiceStatusTable` and `ibMemberNode2ServiceStatusTable` that display system and hardware status on the queried appliance. For information, see *ibMemberNode1ServiceStatusTable* on page 361 and *ibMemberNode2ServiceStatusTable* on page 363.

*Figure 11.9  `ibMemberServiceStatusTable` Objects*
Infoblox MIBs

Infoblox Services for ibMemberServiceStatusTable

*Table 11.13* lists the values and descriptions of the Infoblox services that appear in *ibMemberServiceStatusTable*.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>dhcp</td>
<td>DHCP service</td>
</tr>
<tr>
<td>2</td>
<td>dns</td>
<td>DNS service</td>
</tr>
<tr>
<td>3</td>
<td>ntp</td>
<td>NTP service</td>
</tr>
<tr>
<td>4</td>
<td>radius</td>
<td>RADIUS service</td>
</tr>
<tr>
<td>5</td>
<td>tftp</td>
<td>File distribution using the TFTP service</td>
</tr>
<tr>
<td>6</td>
<td>http-file-dist</td>
<td>File distribution using the HTTP service</td>
</tr>
<tr>
<td>7</td>
<td>ftp</td>
<td>File distribution using the FTP service</td>
</tr>
<tr>
<td>8</td>
<td>bloxtools</td>
<td>bloxTools environment</td>
</tr>
</tbody>
</table>

Service Status

When you query the service status on an appliance, the response includes the status of the services. *Table 11.14* shows the values and descriptions of the status.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>working</td>
<td>The service is functioning properly.</td>
</tr>
<tr>
<td>2</td>
<td>warning</td>
<td>The service is having some issues. Check the service or hardware function and the syslog to identify the problem.</td>
</tr>
<tr>
<td>3</td>
<td>failed</td>
<td>The service failed. Review the syslog to identify the problem.</td>
</tr>
<tr>
<td>4</td>
<td>inactive</td>
<td>The service is disabled or out of service.</td>
</tr>
<tr>
<td>5</td>
<td>unknown</td>
<td>The appliance cannot detect the current status of the service.</td>
</tr>
</tbody>
</table>

*ibMemberNode1ServiceStatusTable*

As shown in *Figure 11.10*, *ibMemberNode1ServiceStatusTable* (object ID 3.1.1.2.1.2.10) has one subtree, *ibMemberNode1ServiceStatusEntry*, which contains the following objects:

- *ibMemberNode1ServiceName* (String) reports the names of the system and hardware services. For a list of service names, see *System and Hardware Services for *ibMemberNode1ServiceStatusTable* on page 362.*
- *ibMemberNode1ServiceStatus* (Integer) reports the status of the services. For a list of service status, see *Service Status* on page 361.*
- *ibMemberNode1ServiceDesc* (String) describes the details of the status.*

*ibMemberNode1ServiceStatusTable* displays the current status of the system and hardware services on the appliance that you query. For example, when you query an independent appliance, this table shows the information about the independent appliance. When you query the VIP of an HA pair, this table shows the information about the active node. For the active node of the HA pair, you can also query *ibMemberNode2StatusTable* to get the status of the passive node. For information, see *ibMemberNode2ServiceStatusTable* on page 363.
**Note:** For an independent appliance and the passive node of an HA pair, no information is returned when you query `ibMemberNode2ServiceStatusTable`.

*Figure 11.10  `ibMemberNode1ServiceStatusTable` Objects*

```
(3.1.1.2.1.10)  ibMemberNode1ServiceStatusTable
    ↓
(3.1.1.2.1.10.1)  ibMemberNode1ServiceStatusEntry
    ↓
(3.1.1.2.1.10.1.1)  ibMemberNode1ServiceName
    ↓
(3.1.1.2.1.10.1.2)  ibMemberNode1ServiceStatus
    ↓
(3.1.1.2.1.10.1.3)  ibMemberNode1ServiceDesc
```

**System and Hardware Services for `ibMemberNode1ServiceStatusTable`**

*Table 11.15* lists the values and descriptions of the system and hardware services that appear in `ibMemberNode1ServiceStatusTable`.

*Table 11.15  `ibServiceName` Values for `ibMemberNode1ServiceStatusTable`*

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>node-status</td>
<td>Node status</td>
</tr>
<tr>
<td>10</td>
<td>disk-usage</td>
<td>Disk usage</td>
</tr>
<tr>
<td>11</td>
<td>enet-lan</td>
<td>LAN 1 port</td>
</tr>
<tr>
<td>12</td>
<td>enet-lan2</td>
<td>LAN 2 port</td>
</tr>
<tr>
<td>13</td>
<td>enet-ha</td>
<td>HA port</td>
</tr>
<tr>
<td>14</td>
<td>enet-mgmt</td>
<td>MGMT port</td>
</tr>
<tr>
<td>15</td>
<td>lcd</td>
<td>LCD</td>
</tr>
<tr>
<td>16</td>
<td>memory</td>
<td>Virtual memory</td>
</tr>
<tr>
<td>18</td>
<td>db-object</td>
<td>Database usage</td>
</tr>
<tr>
<td>19</td>
<td>raid-summary</td>
<td>Summary of the RAID array</td>
</tr>
<tr>
<td>20</td>
<td>raid-disk1</td>
<td>Disk 1 of the RAID array (for Infoblox-2000 and -2000-A)</td>
</tr>
<tr>
<td>21</td>
<td>raid-disk2</td>
<td>Disk 2 of the RAID array (for Infoblox-2000 and -2000-A)</td>
</tr>
<tr>
<td>22</td>
<td>raid-disk3</td>
<td>Disk 3 of the RAID array (for Infoblox-2000 and -2000-A)</td>
</tr>
<tr>
<td>23</td>
<td>raid-disk4</td>
<td>Disk 4 of the RAID array (for Infoblox-2000 and -2000-A)</td>
</tr>
<tr>
<td>24</td>
<td>fan1</td>
<td>FAN 1 status</td>
</tr>
</tbody>
</table>
As shown in Figure 11.11, ibMemberNode2ServiceStatusTable (object ID 3.1.1.2.1.11) has one subtree, ibMemberNode2ServiceStatusEntry, which contains the following objects:

- **ibMemberNode2ServiceName (String)** reports the names of the system and hardware services. For a list of service names, see System and Hardware Services for ibMemberNode2ServiceStatusTable.
- **ibMemberNode2ServiceStatus (Integer)** reports the status of the services. For a list of possible service status, see Service Status on page 361.
- **ibMemberNode2ServiceDesc (String)** describes details of the status.

ibMemberNode2ServiceStatusTable displays the current status of the system and hardware services on the passive node of an HA pair when you query the VIP of the HA pair. For independent appliances and the passive nodes of HA pairs, this table does not display any status.

### Figure 11.11 ibMemberNode2ServiceStatusTable Objects

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>fan2</td>
<td>FAN 2 status</td>
</tr>
<tr>
<td>26</td>
<td>fan3</td>
<td>FAN 3 status</td>
</tr>
<tr>
<td>27</td>
<td>power-supply</td>
<td>Power supply</td>
</tr>
<tr>
<td>28</td>
<td>ntp-sync</td>
<td>NTP service synchronization</td>
</tr>
<tr>
<td>29</td>
<td>cpu1-temp</td>
<td>CPU 1 temperature</td>
</tr>
<tr>
<td>30</td>
<td>cpu2-temp</td>
<td>CPU 2 temperature</td>
</tr>
<tr>
<td>31</td>
<td>sys-temp</td>
<td>System temperature</td>
</tr>
<tr>
<td>32</td>
<td>raid-battery</td>
<td>RAID battery</td>
</tr>
<tr>
<td>33</td>
<td>cpu-usage</td>
<td>CPU usage</td>
</tr>
<tr>
<td>34</td>
<td>ospf</td>
<td>Anycast using OSPF</td>
</tr>
</tbody>
</table>
### System and Hardware Services for `ibMemberNode2ServiceStatusTable`

*Table 11.16* lists the values and descriptions of the system and hardware services that appear in `ibMemberNode2ServiceStatusTable`.

#### *Table 11.16  `ibServiceName` Values for `ibMemberNode2ServiceStatusTable`*

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>node-status</td>
<td>Node status</td>
</tr>
<tr>
<td>10</td>
<td>disk-usage</td>
<td>Disk usage</td>
</tr>
<tr>
<td>11</td>
<td>enet-lan</td>
<td>LAN 1 port</td>
</tr>
<tr>
<td>12</td>
<td>enet-lan2</td>
<td>LAN 2 port</td>
</tr>
<tr>
<td>13</td>
<td>enet-ha</td>
<td>HA port</td>
</tr>
<tr>
<td>14</td>
<td>enet-mgmt</td>
<td>MGMT port</td>
</tr>
<tr>
<td>15</td>
<td>lcd</td>
<td>LCD</td>
</tr>
<tr>
<td>16</td>
<td>memory</td>
<td>Virtual memory</td>
</tr>
<tr>
<td>17</td>
<td>replication</td>
<td>Replication process</td>
</tr>
<tr>
<td>18</td>
<td>db-object</td>
<td>Database usage</td>
</tr>
<tr>
<td>19</td>
<td>raid-summary</td>
<td>The summary of the RAID array</td>
</tr>
<tr>
<td>20</td>
<td>raid-disk1</td>
<td>Disk 1 of the RAID array (for Infoblox-2000 and -2000-A)</td>
</tr>
<tr>
<td>21</td>
<td>raid-disk2</td>
<td>Disk 2 of the RAID array (for Infoblox-2000 and -2000-A)</td>
</tr>
<tr>
<td>22</td>
<td>raid-disk3</td>
<td>Disk 3 of the RAID array (for Infoblox-2000 and -2000-A)</td>
</tr>
<tr>
<td>23</td>
<td>raid-disk4</td>
<td>Disk 4 of the RAID array (for Infoblox-2000 and -2000-A)</td>
</tr>
<tr>
<td>24</td>
<td>fan1</td>
<td>FAN 1 status</td>
</tr>
<tr>
<td>25</td>
<td>fan2</td>
<td>FAN 2 status</td>
</tr>
<tr>
<td>26</td>
<td>fan3</td>
<td>FAN 3 status</td>
</tr>
<tr>
<td>27</td>
<td>power-supply</td>
<td>Power supply</td>
</tr>
<tr>
<td>28</td>
<td>ntp-sync</td>
<td>NTP service synchronization</td>
</tr>
<tr>
<td>29</td>
<td>cpu1-temp</td>
<td>CPU 1 temperature</td>
</tr>
<tr>
<td>30</td>
<td>cpu2-temp</td>
<td>CPU 2 temperature</td>
</tr>
<tr>
<td>31</td>
<td>sys-temp</td>
<td>System temperature</td>
</tr>
<tr>
<td>32</td>
<td>raid-battery</td>
<td>RAID battery</td>
</tr>
<tr>
<td>33</td>
<td>cpu-usage</td>
<td>CPU usage</td>
</tr>
<tr>
<td>34</td>
<td>ospf</td>
<td>Anycast using OSPF</td>
</tr>
</tbody>
</table>
**ibDHCPOne MIB**

The ibDHCPOne MIB provides information about address usage within a subnet, DHCP lease statistics, and DHCP packet counts. *Figure 11.12* illustrates the structure of the ibDHCPOne MIB. (Note that the OIDs shown in the illustration do not include the prefix .1.3.6.1.4.1.7779.) ibDHCPOne contains the following objects:

- **ibDHCPSubnetTable** provides statistical data about the DHCP operations of the appliance. For information, see *ibDHCPSubnetTable* on page 366.
- **ibDHCPStatistics** maintains counters for different types of packets. For information, see *ibDHCPStatistics* on page 367.
- **ibDHCPDeferredQueueSize** tracks the total number of deferred DDNS updates that are currently in the queue to be retried. When DDNS updates are deferred due to timeout or server issues, the DHCP server puts these updates in this queue.
- **ibDHCPDDNSSstats** monitors the average latency for the DDNS updates in microseconds and the number of timeouts during different time intervals. For information, see *ibDHCPDDNSSstats* on page 368.

*Figure 11.12  DHCPone MIB*
**ibDHCPSubnetTable**

*ibDHCPSubnetTable* provides statistical data about the DHCP operations of the appliance. It contains the following objects:

**Table 11.17 ibDHCPSubnetTable**

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibDHCPSubnet Entry</td>
<td>File that contains the objects for monitoring DHCP operations on the appliance.</td>
</tr>
<tr>
<td>ibDHCPSubnetNetworkAddress (IpAddr)</td>
<td>The subnetworks, in IP address format, that have IP addresses for lease. A subnetwork may have many address ranges for lease.</td>
</tr>
<tr>
<td>ibDHCPSubnetNetworkMask (IpAddr)</td>
<td>The subnet mask in dotted decimal format.</td>
</tr>
<tr>
<td>ibDHCPSubnetPercentUsed (Integer)</td>
<td>The percentage of dynamic DHCP addresses leased out at this time for each subnet. Fixed addresses are always counted as leased for this calculation, if the fixed addresses are within a leased address range.</td>
</tr>
</tbody>
</table>

Following is an example of the table as viewed through a MIB browser:

*Figure 11.13 MIB Browser View 1*
**ibDHCPStatistics**

ibDHCPStatistics maintains counters for different types of packets. The counters always start with zero when you enable DHCP. Therefore the numbers reflect the total number of packets received since DHCP was enabled on the NIOS appliance. The ibDHCPStatistics module contains the following objects:

Table 11.18  *ibDHCPStatistics*

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibDhcpTotalNoOfDiscovers (Counter)</td>
<td>The number of DHCPDISCOVER messages that the appliance received. Clients broadcast DHCPDISCOVER messages when they need an IP address and network configuration information.</td>
</tr>
<tr>
<td>ibDhcpTotalNoOfRequests (Counter)</td>
<td>The number of DHCPREQUEST messages that the appliance received. A client sends a DHCPREQUEST message requesting configuration information, after it receives the DHCPOFFER message.</td>
</tr>
<tr>
<td>ibDhcpTotalNoOfReleases (Counter)</td>
<td>The number of DHCPRELEASE messages that the appliance received from its clients. A client sends a DHCP release when it terminates its lease on an IP address.</td>
</tr>
<tr>
<td>ibDhcpTotalNoOfOffers (Counter)</td>
<td>The number of DHCPOFFER messages that the appliance has sent to clients. The appliance sends a DHCPOFFER message to a client. It contains an IP address and configuration information.</td>
</tr>
<tr>
<td>ibDhcpTotalNoOfAcks (Counter)</td>
<td>The number of DHCPACK messages that the appliance sent to clients. It sends a DHCPACK message to a client to confirm that the IP address offered is still available.</td>
</tr>
<tr>
<td>ibDhcpTotalNoOfNacks (Counter)</td>
<td>The number of DHCPNACK messages that the appliance sent to clients. It sends a DHCPNACK message to withdraw its offer of an IP address.</td>
</tr>
<tr>
<td>ibDhcpTotalNoOfDeclines (Counter)</td>
<td>The number of DHCPDECLINE messages that the appliance received. A client sends a DHCPDECLINE message if it determines that an offered IP address is already in use.</td>
</tr>
<tr>
<td>ibDhcpTotalNoOfInforms (Counter)</td>
<td>The number of DHCPINFORM messages that the appliance received. A client sends a DHCPINFORM message when it has an IP address but needs information about the network.</td>
</tr>
<tr>
<td>ibDhcpTotalNoOfOthers (Counter)</td>
<td>The total number of DHCP messages other than those used in negotiation, such as DHCPFORCERENEW, DHCPKNOWN, and DHCPLEASEQUERY.</td>
</tr>
</tbody>
</table>
**ibDHCPDDNSSStats**

ibDHCPDDNSSStats monitors the average latency for the DHCP DDNS updates in microseconds and the number of timeouts during different time intervals. The ibDHCPDDNSSStats module contains the following objects:

*Table 11.19  ibDHCPDDNSSStats*

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibDHCPDDNSAvgLatency5</td>
<td>Indicates the average latency in microseconds of the DHCP DDNS updates in the last five minutes.</td>
</tr>
<tr>
<td>ibDHCPDDNSAvgLatency15</td>
<td>Indicates the average latency in microseconds of the DHCP DDNS updates in the last 15 minutes.</td>
</tr>
<tr>
<td>ibDHCPDDNSAvgLatency60</td>
<td>Indicates the average latency in microseconds of the DHCP DDNS updates in the last 60 minutes.</td>
</tr>
<tr>
<td>ibDHCPDDNSAvgLatency1440</td>
<td>Indicates the average latency in microseconds of the DHCP DDNS updates in the last 24 hours.</td>
</tr>
<tr>
<td>ibDHCPDNDSTimeoutCount5</td>
<td>The number of timeouts for the DHCP DDNS updates in the last five minutes.</td>
</tr>
<tr>
<td>ibDHCPDNDSTimeoutCount15</td>
<td>The number of timeouts for the DHCP DDNS updates in the last 15 minutes.</td>
</tr>
<tr>
<td>ibDHCPDNDSTimeoutCount60</td>
<td>The number of timeouts for the DHCP DDNS updates in the last 60 minutes.</td>
</tr>
<tr>
<td>ibDHCPDNDSTimeoutCount1440</td>
<td>The number of timeouts for the DHCP DDNS updates in the last 24 hours.</td>
</tr>
</tbody>
</table>
ibDNSOne MIB

The ibDNSOne MIB provides statistical information about the DNS processes and about the views and zones in the database. *Figure 11.14* illustrates the structure of the ibDNSOne MIB. (Note that the OIDs shown in the illustration do not include the prefix 1.3.6.1.4.1.7779.) The ibDNSOne MIB contains four subtrees, ibZoneStatisticsTable, ibZonePlusViewStatisticsTable, ibDDNSUpdateStatistics, and ibBindZoneTransferCount (Counter64).

*Figure 11.14 ibDNSOne MIB*
**ibZoneStatisticsTable**

`ibZoneStatisticsTable` provides statistical data about the DNS operations on the appliance. The syntax of these objects uses a Counter64 format. In some cases, the counter format may not be compatible with SNMP toolkits that use a 32-bit counter. Ensure that you reconfigure or update these tools to use the Counter64 format.

`ibZoneStatisticsTable` contains the following objects:

*Table 11.20  `ibZoneStatisticsTable`*

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ibBindZoneName</code> (IbString)</td>
<td>DNS Zone name.</td>
</tr>
<tr>
<td><code>ibBindZoneSuccess</code> (Counter64)</td>
<td>The number of successful responses since the DNS process started.</td>
</tr>
<tr>
<td><code>ibBindZoneReferral</code> (Counter64)</td>
<td>The number of DNS referrals since the DNS process started.</td>
</tr>
<tr>
<td><code>ibBindZoneNxRRset</code> (Counter64)</td>
<td>The number of DNS queries received for non-existent records.</td>
</tr>
<tr>
<td><code>ibBindZoneNxDomain</code> (Counter64)</td>
<td>The number of DNS queries received for non-existent domains.</td>
</tr>
<tr>
<td><code>ibBindZoneRecursion</code> (Counter64)</td>
<td>The number of queries received using recursion since the DNS process started.</td>
</tr>
<tr>
<td><code>ibBindZoneFailure</code> (Counter64)</td>
<td>The number of failed queries since the DNS process started.</td>
</tr>
</tbody>
</table>

**ibZonePlusViewStatisticsTable**

`ibZonePlusViewStatisticsTable` provides statistical data about DNS views and their zones. It contains the following objects:

*Table 11.21  `ibZonePlusViewStatisticsTable`*

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ibBindZonePlusViewName</code> (IbString)</td>
<td>The zone name. The first one in the default view is the global summary statistics. Index name for global statistics is “summary.”</td>
</tr>
<tr>
<td><code>ibBindZonePlusViewSuccess</code> (Counter64)</td>
<td>Number of successful responses since the DNS process started.</td>
</tr>
<tr>
<td><code>ibBindZonePlusViewReferral</code> (Counter64)</td>
<td>Number of DNS referrals</td>
</tr>
<tr>
<td><code>ibBindZonePlusViewNxRRset</code> (Counter64)</td>
<td>Number of DNS queries received for non-existent records.</td>
</tr>
</tbody>
</table>
**Object (Type)** | **Description**
---|---
ibBindZonePlusViewNxDomain (Counter64) | Number of DNS queries received for non-existent domains.
ibBindZonePlusViewRecursion (Counter64) | Number of DNS recursive queries received
ibBindZonePlusViewFailure (Counter64) | Number of failed queries
ibBindViewName (IbString) | View name. This is blank for default view

Following is an example of the table as viewed through a MIB browser:

*Figure 11.15  MIB Browser View*
ibDDNSUpdateStatistics

ibDDNSUpdateStatistics provides statistical data about DDNS updates. The counters always start with zero when the DNS service is restarted. They report the total numbers since the DNS service was last restarted.

ibDDNSUpdateStatistics contains the following objects:

Table 11.22  ibDDNSUpdateStatistics

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibDDNSUpdateSuccess (Counter64)</td>
<td>The number of successful dynamic DNS updates.</td>
</tr>
<tr>
<td>ibDDNSUpdateFailure (Counter64)</td>
<td>The number of all failed dynamic DNS updates, excluding those reported by the ibDDNSUpdateReject object.</td>
</tr>
<tr>
<td>ibDDNSUpdateReject (Counter64)</td>
<td>The number of dynamic DNS updates that failed because they were denied by the DNS server.</td>
</tr>
<tr>
<td>ibDDNSUpdatePrerequisiteReject (Counter64)</td>
<td>The number of dynamic DNS updates that failed because the prerequisites were not satisfied. This is also included in the total number of failures reported by the ibDDNSUpdateFailure object.</td>
</tr>
</tbody>
</table>

ibBindZoneTransferCount

ibBindZoneTransferCount (Counter64) provides the total number of successful zone transfers from an Infoblox primary or secondary DNS server to a DNS client, since the DNS service was last restarted. Note that this counter tracks the number of successful full zone transfers (AXFRs) and incremental zone transfers (IXFRs).
Configuring SNMP

Perform the following tasks to configure SNMP on the NIOS appliance:

- Enable the NIOS appliance to accept queries and define the community string that management systems must specify when they send queries to the appliance.
- Specify the management systems to which the appliance sends traps.

For a grid, you can perform these tasks at the grid and member levels. You can define SNMP settings for an entire grid, and when necessary, define different SNMP settings for a member. SNMP settings for a member override SNMP settings for a grid.

You can also set up SNMP on an independent appliance or HA pair.

Accepting SNMP Queries

You can allow specific management systems to send queries to a NIOS appliance. When you do, you must specify a community string. The appliance accepts queries only from management systems that provide the correct community string.

To configure a grid, an independent NIOS appliance, or an HA pair to accept SNMP queries:

1. From the Grid tab, select the Grid Managers tab, and then select Grid Properties -> Edit from the Toolbar.
2. In the Grid Properties editor, select the Monitoring tab, and then complete the following in the SNMP section:
   - Enable SNMP Queries: Select this for all grid members, an independent appliance, or an HA pair to accept queries from SNMP management systems.
   - Community String: Enter a text string that the management system must send together with its queries to the grid, the independent appliance, or HA pair. A community string is similar to a password in that the appliance accepts queries only from management systems that send the correct community string. Note that this community string must match exactly what you enter in the management system.
3. Click Save & Close or Save to save your settings.

Adding SNMP Trap Receivers

You can enable a NIOS appliance to send traps to specific management systems or trap receivers. It sends traps whenever certain events occur, as described in ibTrap MIB on page 327.

To configure an SNMP trap receiver for a grid, an independent appliance, or an HA pair:

1. From the Grid tab, select the Grid Managers tab, and then select Grid Properties -> Edit from the Toolbar.
2. In the Grid Properties editor, select the Monitoring tab, and then complete the following in the SNMP section:
   - Enable SNMP Traps: Select this to enable all grid members, an independent appliance, or an HA pair to send traps to specified SNMP management systems.
   - Community String: Enter a text string that the NIOS appliance sends to the management system together with its traps. Note that this community string must match exactly what you enter in the management system.
3. Click the Add icon to add an SNMP trap receiver. Grid Manager adds a row to the table. In the Address field, enter the IP address of the SNMP management system to which you want the SNMP agent on the appliance to send traps. You can enter more than one trap receiver. To remove an IP address from the list, select the address, and then click the Delete icon.
4. Click Save & Close or Save to save your settings.
Setting System Information

You can enter values for the following managed objects in MIB-II, the standard MIB defined in RFC 1213:

- sysContact
- sysLocation
- sysName
- sysDescr

After you enter these values on the appliance, administrators can send queries for these values from management systems that are allowed to send queries to the appliance.

To enter system information:

1. From the Grid tab, select the Grid Managers tab, and then select Grid Properties -> Edit from the Toolbar.
2. In the Grid Properties editor, select the Monitoring tab, and then complete the following in the SNMP section:
   - sysContact: Enter the name of the contact person for the appliance.
   - sysLocation: Enter the physical location of the appliance.
   - sysName: Enter the fully qualified domain name of the appliance.
   - sysDescr: Enter useful information about the appliance, such as the software version it is running.
3. Click Save & Close or Save to save your settings.

Configuring SNMP for a Grid Member

You can override grid-level SNMP settings for individual grid members.

To modify the SNMP settings for a grid member:

1. From the Grid tab, select the Grid Managers tab -> member check box, and then click the Edit icon.
2. In the Grid Member Properties editor, select the Monitoring tab, click Override in the SNMP section, and then complete the following:
   - Enable SNMP Queries: Select this for the member to accept queries from SNMP management systems. Clear the check box to disable the member from accepting SNMP queries.
   - Community String: Enter a text string that the management system must send together with its queries to the grid or the independent appliance or HA pair. A community string is similar to a password in that the appliance accepts queries only from management systems that send the correct community string. Note that this community string must match exactly what you enter in the management system.
   - Enable SNMP Traps: Select this to enable the grid member to send traps to specified SNMP management systems. Clear the check box to disable the member from sending SNMP traps.
   - Community String: Enter a text string that the NIOS appliance sends to the management system together with its traps. Note that this community string must match exactly what you enter in the management system.
   - Trap Receivers: Click the Add icon and type the address of an SNMP management system to which you want the SNMP agent on grid members and independent appliances to send traps. You can enter more than one trap receiver. To remove an IP address from the list, select the address, and then click the Delete icon.
   - SNMP System Information: Complete the following information:
     - sysContact: Enter the name of the contact person for the appliance.
     - sysLocation: Enter the physical location of the appliance.
     - sysName: Enter the fully qualified domain name of the appliance.
     - sysDescr: Enter useful information about the appliance, such as the software version it is running.
3. Click Save & Close or Save to save your settings.
Chapter 12 bloxTools Environment

The bloxTools environment provides a pre-installed environment for hosting custom web-based applications. This chapter includes the following sections:

- About the bloxTools Environment on page 376
  - System Requirements on page 376
- Using the bloxTools Environment on page 377
  - Configuring the Service on page 377
  - Uploading Files on page 378
  - Scheduling Tasks on page 378
- Monitoring the Service on page 379
  - Viewing the Logs on page 379
  - Viewing Detailed Status on page 379
About the bloxTools Environment

The bloxTools environment provides tools for creating custom applications that facilitate the administrative tasks in your organization. It provides a pre-installed environment for running applications using Perl, Python, PHP, CGI scripting, and Infoblox API libraries. It also includes sample applications which you can use or modify to suit your business needs. Note that no direct external remote user (telnet and ssh, for example) or shell access is available in this environment.

The bloxTools environment runs as a service on an independent appliance or on a grid master. It “borrows” resources such as CPU, memory, disk space, and networking from the host Infoblox appliance, but is logically separated from the NIOS. The logical separation ensures that any failure in the bloxTools service does not affect the other services running on the appliance.

After you enable the bloxTools service and configure its built-in file transfer services, you can upload content to the bloxTools portal using either an FTP (File Transfer Protocol) or SFTP (SSH File Transfer Protocol) client. The uploaded content is included in system backups and you can restore it from the backups.

In a grid, you upload content to the grid master, which then replicates the data and logs to all master candidates. If there is a grid master failover, the bloxTools service is automatically launched after the passive grid master takes over as the active grid master.

For more information about the bloxTools environment and to access free applications, visit http://www.infoblox.com/en/support/support-center-login.html.

Note: The bloxTools environment is not supported on vNIOS appliances on Riverbed, Cisco, and VMware.

System Requirements

Table 12.1 shows which Infoblox appliances support the bloxTools service and the memory requirement for each. The service “borrows” host resources such as CPU, memory, and disk space from the host Infoblox appliance.

Table 12.1 Memory Requirements

<table>
<thead>
<tr>
<th>Infoblox Appliance</th>
<th>Memory Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infoblox-250</td>
<td>Feature not supported</td>
</tr>
<tr>
<td>Infoblox-250-A</td>
<td></td>
</tr>
<tr>
<td>Infoblox-500</td>
<td></td>
</tr>
<tr>
<td>Infoblox-550</td>
<td>128 MB</td>
</tr>
<tr>
<td>Infoblox-1000</td>
<td></td>
</tr>
<tr>
<td>Infoblox-1050</td>
<td></td>
</tr>
<tr>
<td>Infoblox-550-A</td>
<td>128 MB to 256 MB (configurable) The default is 128 MB</td>
</tr>
<tr>
<td>Infoblox-1050-A</td>
<td></td>
</tr>
<tr>
<td>Infoblox-1200</td>
<td></td>
</tr>
<tr>
<td>Infoblox-1220</td>
<td></td>
</tr>
<tr>
<td>Infoblox-1550</td>
<td>128 MB to 512 MB (configurable) The default is 128 MB</td>
</tr>
<tr>
<td>Infoblox-1550-A</td>
<td></td>
</tr>
<tr>
<td>Infoblox-1552</td>
<td></td>
</tr>
<tr>
<td>Infoblox-1552-A</td>
<td></td>
</tr>
<tr>
<td>Infoblox-1852-A</td>
<td></td>
</tr>
<tr>
<td>Infoblox-2000</td>
<td></td>
</tr>
<tr>
<td>Infoblox-2000-A</td>
<td></td>
</tr>
</tbody>
</table>
Complete the following tasks to upload custom applications to the bloxTools environment:

1. Log in to the appliance as a superuser and configure the bloxTools service, as described in Configuring the Service.

2. Use an FTP or a SFTP client to upload content to the bloxTools environment.

In addition, you can schedule tasks as described in Scheduling Tasks on page 378, and monitor the bloxTools service as described in Monitoring the Service on page 379.

**WARNING:** Resetting the grid master using either the reset all or reset database CLI commands permanently deletes the content you uploaded to the bloxTools environment. Infoblox recommends that you backup the appliance before using any of these commands.

---

**Configuring the Service**

When you configure the bloxTools service, you can enable FTP, SFTP, and HTTPS, and set their operational parameters. FTP and SFTP are the services you use to upload data. You can disable these services when they are not in use. HTTPS must remain enabled to allow the web based bloxTools applications to run. Note that the bloxTools service uses the same SSL certificate as the host Infoblox appliance. (For information on certificates, see Managing Certificates on page 39.)

To configure the bloxTools service:

1. Log in as a superuser.

2. For the grid: From the Grid tab, select the Grid Manager tab, and then click bloxTools. In the Services tab, click Edit -> Grid bloxTools Properties from the Toolbar.

3. In the bloxTools Properties editor, complete the following:
   - **Allocated Memory (MB):** The service “borrows” host resources such as CPU, memory, and disk space from the host Infoblox appliance. The default amount of memory the appliance allocates for the bloxTools environment is 128 MB. You can change this allocation, depending on the appliance platform. See System Requirements on page 376 for the requirements and allowed values of each appliance.
   - **Enable Web Service:** Select HTTPS Port to enable users to access the applications through an HTTPS connection. The default port is 444. You can change the port number to suit your environment.
   - **Enable FTP Service:** Select FTP Port to enable the FTP service. The default port is 26. You can change the port number to suit your environment.
   - **Enable SFTP Service:** Select SFTP Port to enable the SFTP service for secure file transfer. The default port is 28. You can change the port to a number between 1024 and 63999, provided that the port is not currently used for another purpose.
   - **Login:** Enter the username for the FTP and SFTP services. The username can contain lower case letters, numbers, underscores (_), and dollar signs ($), and it must begin with a letter, not a number.
   - **Set Password:** Enter the password for the FTP and SFTP services in this field.
   - **Retype Password:** Enter the same password.

   **Note:** The password is sent as clear text when you use the FTP service. To maintain security on the Infoblox appliance, this password should be different from the password set for the Infoblox appliance.

4. Click Save & Close or Save.
Uploading Files

Use an FTP or a SFTP client to upload content, such as Perl modules, JavaScript files, PHP files, CGI files, and image files, to the bloxTools environment. You can upload a maximum of 1 GB of data. After you have uploaded content to your bloxTools environment, you should disable the FTP and SFTP services to prevent unauthorized or accidental changes.

To upload files using the FTP service:
1. Open an Internet browser window and log in to the FTP service by entering:
   ```
   ftp://grid_master_ip_addr:ftp_port
   ```
   For example, if the IP address of the grid master is 10.1.1.1 and the FTP port number is 26, enter:
   ```
   ftp://10.1.1.1:26
   ```
2. In the Authentication Required dialog box, enter the username and password. This is the username and password you entered for the FTP service in the bloxTools Environment editor on the appliance.
3. Follow the instructions provided by your FTP client to upload the files.

To upload files using the SFTP service:
1. Open a terminal window and log in to the SFTP service by entering:
   ```
   sftp -oPort=sftp_port sftp_user@grid_master_ip_addr
   ```
   For example, if the IP address of the grid master is 10.1.1.1, the login username for the SFTP service is jdoe, and the SFTP port number is 28, enter:
   ```
   sftp -oPort=28 jdoe@10.1.1.1
   ```
2. Enter the password. This is the password you entered for the SFTP service in the bloxTools Environment editor on the appliance.
3. Follow the instructions provided by your SFTP client to upload the files.

**Note:** On a computer running Microsoft Windows, you can use WinSCP as the FTP or SFTP client for uploading files.

The bloxTools environment stores the uploaded data in the /portal directory.

Scheduling Tasks

bloxTools includes support for the Perl module `Config::Crontab` so you can manage scheduler services. You can use the scheduler to execute commands in the future. You can also schedule recurring commands. For example, you can schedule the creation of a host record or schedule recurring reports. The scheduler allows default “user level” crontab access and you can use the user account “nobody” to submit commands. The grid master replicates the crontab data to the master candidates.
MONITORING THE SERVICE

Infoblox provides several tools for monitoring the bloxTools Environment. The bloxTools Environment has its own syslog service which you can access to view logs generated by the bloxTools service and its processes. The Detailed Status panel also displays the status of the bloxTools Environment.

Viewing the Logs

The bloxTools Environment generates the following logs:

- **access.log**: The Apache access log
- **error.log**: The Apache error log
- **syslog.log**: The bloxTools Environment system log

These log files are included in the support bundle. You can download the log files using FTP, and you can also use the following CLI commands to view the logs:

- Use the `show file` command to view the list of log files.
- Use the `show bloxtools` command to view the status of the bloxTools Environment.
- Use the `show file bloxtools portal_access` command to view the web portal access log.
- Use the `show file bloxtools portal_error` command to view the web portal error log.
- Use the `show file bloxtools portal_log` command to view the web portal system log.

Viewing Detailed Status

You can view the status of the bloxTools Environment from the Services tab of the Grid Manager tab. To display the Services tab, from the Grid tab, select the Grid Manager tab -> Services tab. Grid Manager displays the following information:

- **Name**: The grid member name.
- **Service Status**: Indicates the current operational status of the bloxTools Environment running on the member.
- **IP Address**: The IP address of the member.
- **Comment**: Information about the bloxTools Environment.
- **Site**: The location to which the member belongs. This is one of the predefined extensible attributes.

The service status icon indicates the operational status of the bloxTools Environment and the usage percentages for the CPU, memory and disk resources. The status icon can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gray</td>
<td>Green</td>
<td>The CPU, memory, and disk usage is below 80%.</td>
</tr>
<tr>
<td>Yellow</td>
<td>Usage of at least one of the following resources is greater than or equal to 80%: CPU, memory or disk. The description indicates the percentage of each resource.</td>
<td></td>
</tr>
<tr>
<td>Red</td>
<td>The bloxTools Environment is down, or an essential service within the bloxTools Environment has failed.</td>
<td></td>
</tr>
</tbody>
</table>
Part 3 DNS

This section describes how to configure the grid to provide DNS services. It includes the following chapters:

- Chapter 13, Infoblox DNS Service, on page 383
- Chapter 14, DNS Views, on page 391
- Chapter 15, Configuring DNS Zones, on page 403
- Chapter 16, DNS Resource Records, on page 441
- Chapter 17, Configuring DNS Services, on page 479
- Chapter 18, Configuring DDNS Updates from DHCP, on page 501
- Chapter 19, DNSSEC, on page 543
- Chapter 20, "Configuring IP Routing Options", on page 567
Chapter 13 Infoblox DNS Service

The NIOS appliance uses a standard, BIND-based DNS protocol engine. It interoperates with any other name server that complies with the DNS RFCs (see DNS RFC Compliance on page 771).

This chapter provides an overview of the DNS configuration tasks. It includes the following sections:

- Configuring DNS Overview on page 384
  - DNS Configuration Checklist on page 385
- About Inheriting DNS Properties on page 386
  - Overriding DNS Properties on page 387
- Understanding DNS for IPv6 on page 388
  - Configuring IPv6 on a Grid Member on page 389
  - Configuring DNS for IPv6 Addressing on page 390
**Configuring DNS Overview**

An overview of the DNS configuration process is outlined in the following diagram, illustrating the required steps for preparing a NIOS appliance for use:

- Begin the initial configuration of DNS for a NIOS appliance.
  - Do you want to configure grid DNS properties?
    - Yes: Configure grid DNS properties.
    - No: Configure member DNS properties.

- Begin the configuration of DNS zones and resource records.
  - Do you want to add DNS views, in addition to the default?
    - Yes: Add DNS views.
    - No: Decide on the type of zones to configure.

- Forward zone
  - Specify the IP address of the server(s) to which queries are forwarded, and select the grid member that hosts the zone.
  - Choose the primary member or specify the external primary.
  - Choose grid secondaries or specify external secondaries.
  - Add resource records.
  - Import zone data.

- Authoritative zone
  - Specify the IP address and FQDN of the authoritative name server for the zone.

- Delegated zone
  - Specify the IP address of the master server, and select the grid member that hosts the zone.

- Stub zone

- Do you want to add more zones?
  - Yes
  - No: Initial DNS configuration is complete.
DNS Configuration Checklist

The following checklist includes the major steps for configuring DNS:

Table 13.1 DNS Configuration Checklist

<table>
<thead>
<tr>
<th>Step</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decide if you want to configure DNS properties for the grid and for individual members.</td>
<td>• <em>Chapter 13, Infoblox DNS Service</em>, on page 383</td>
</tr>
<tr>
<td>Decide if you want to create a new DNS view, in addition to the default DNS view.</td>
<td>• <em>Chapter 14, DNS Views</em>, on page 391</td>
</tr>
<tr>
<td>Decide which type of DNS zone you want to configure.</td>
<td>• <em>Chapter 15, Configuring DNS Zones</em>, on page 403</td>
</tr>
<tr>
<td>Add hosts and resource records.</td>
<td>• <em>Chapter 16, DNS Resource Records</em>, on page 441</td>
</tr>
<tr>
<td>Import zone data.</td>
<td>• <em>Importing Zone Data</em> on page 419</td>
</tr>
</tbody>
</table>
**ABOUT INHERITING DNS PROPERTIES**

You can configure DNS properties at the grid, member, zone, and resource records level. The NIOS appliance applies the properties hierarchically, with the grid at the top of the hierarchy. Grid settings apply to all members in the grid, unless you override them at the member, zone, or resource record level. When you set DNS properties for a particular member, these properties override the grid properties and apply to all zones served by that member. When you set properties for a specific zone, they override the member properties and apply to the resource records in the zone. You can also override the zone properties and set properties for specific resource records.

When you configure DNS properties that contain inherited values, the appliance displays the information based on the inheritance sources. There may be times when an object can inherit properties from different sources with different settings. The following table summarizes what the appliance can display:

<table>
<thead>
<tr>
<th>When you see...</th>
<th>it means...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inherited From <code>&lt;object&gt;</code></td>
<td>the DNS property has a definite value from an inheritance source.</td>
</tr>
<tr>
<td>Inherited From Upper Level</td>
<td>the appliance cannot yet determine the inherited value or inheritance source for the DNS property.</td>
</tr>
<tr>
<td>Inherited From Multiple</td>
<td>the DNS property has the same value that it inherits from multiple sources.</td>
</tr>
<tr>
<td><strong>Settings Inherited from Multiple Ancestors, View Multiple Inheritance Scenarios</strong></td>
<td>the DNS property has different values that it inherits from multiple sources, and you can view the values and their corresponding sources by clicking the <a href="#">View Multiple Inheritance Scenarios</a> link.</td>
</tr>
</tbody>
</table>

Based on the information provided, you can then decide whether to override or keep the inherited values. You must have read/write permissions to the DNS resources to override inherited values. You can only view inherited values and paths if you have at least read-only permissions.

In the example in *Figure 13.1*, the DNS zone is served by members with different query settings.

*Figure 13.1  DNS Zone with Different Inherited Settings*
The Multiple Inheritance Viewer indicates that the two servers have different query ACLs, as shown in Figure 13.2. You can then view the Query properties of each member and edit them, or override the setting and specify values that apply to the zone only.

Figure 13.2 Multiple Inheritance Viewer

Overriding DNS Properties

DNS properties configured at the grid level apply to the entire grid. You can choose to keep the inherited properties or override them when you configure the properties for a member, zone, or resource record.

To override an inherited value:

1. In a wizard or editor, click Override next to a property to enable the configuration. The Override button changes to Inherit.
2. Enter a new value to override the inherited value.
**Understanding DNS for IPv6**

You can configure NIOS appliances to provide DNS services over IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6) networks. You can configure the grid member as a dual-mode name server, capable of sending and receiving IPv4 and IPv6 queries and responses. It can serve DNS data in response to both IPv4 and IPv6 queries. The appliance supports authoritative forward-mapping zones containing AAAA records mapping host names to IPv6 addresses, as well as authoritative reverse-mapping zones with PTR records mapping IPv6 addresses to host names.

Configuring a grid containing an IPv4 primary server and IPv6 secondary servers is not supported. You must enable IPv6 on both the primary and secondary servers within the grid to enable them to communicate with each other. Infoblox highly recommends that you enable IPv6 on your grid appliances before configuring IPv6 authoritative zones.

The NIOS appliance supports one IPv6 address per grid member. Infoblox integrates IPv6 address management into many of the same places where IPv4 addresses are entered. Data validation occurs on all IP address fields and automatic validation is done to ensure proper entry of either an IPv4 address or an IPv6 address.

The NIOS appliance supports the following DNS functions for IPv6:

- **AAAA records**—You can import, serve queries, display, add, delete, and modify AAAA records on the appliance. An AAAA record is equivalent to an IPv4 A record, relying upon a forward-mapping zone to map a hostname to an IPv6 address. A single forward-mapping zone can map names to both IPv4 and IPv6 addresses. The appliance autogenerates AAAA records for any of its interfaces that have IPv6 addresses.

- **Hosts**—You can configure IPv4 and IPv6 addresses for hosts. For information, see *Adding Host Records* on page 444.

- **ip6.arpa**—A specific domain for IPv6 is used for DNS reverse lookups called ip6.arpa. This domain maps an IPv6 address to a hostname. When you specify an IPv6 network, the appliance automatically creates the appropriate zone under ip6.arpa.

- **PTR records**—Import, serve queries, display, add, delete, and modify PTR records within an ip6.arpa reverse zone. The PTR record returns a domain name corresponding to an IPv6 address contained in the ip6.arpa zone. The appliance does not autogenerate PTR records; the user must configure PTR records manually.

- **DDNS**—The appliance supports AAAA and PTR records for DDNS (Dynamic DNS).

For more information about DNS for IPv6, see RFC 3596, *DNS Extensions to Support IP Version 6*.

**Address Structures**

IPv4 uses a 32-bit, 4-octet (each octet separated by decimals) addressing structure to designate sources and destinations within a network. Since there are 32 bits that make up the address, IPv4 can support up to 4 billion unique addresses.

An IPv6 address is a 128-bit number in colon hexadecimal notation. It consists of eight groups of four hexadecimal digits separated by colons (example: 12ab:0000:0000:0123:4567:89ab:0000:cdef). Since there are 128 bits that make up the address, IPv6 can support up to $3.4 \times 10^{38}$ unique addresses. The increase in the number of unique IPv6 addresses is one of the biggest advantages of an IPv6 implementation.

*Figure 13.3 IPv6 Address Structure*
The IPv6 address structure consists of the following:

- **Global Routing Prefix**—Global routing prefix is a (typically hierarchically-structured) value assigned to a site.
- **Subnet ID**—Subnet ID is an identifier of a link within the site.
- **Interface ID**—Interface Identifier. This portion of the address identifies the interface on the subnet. This is equivalent to the host identifier for IPv4 addresses.

When you enter an IPv6 address, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2006:0000:0000:0123:4567:89ab:0000:cdef can be shortened to 2006::123:4567:89ab:0:cdef. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The NIOS appliance displays an IPv6 address in its shortened form, regardless of its form when it was entered.

### Configuring IPv6 on a Grid Member

You can configure a grid member to support both IPv4 and IPv6 connections by configuring an IPv6 address on the member, in addition to the standard IPv4 address.

When you enable IPv6 on a member, you can manually enter the IPv6 gateway address or enable the member to automatically acquire the address from router advertisements. Routers periodically send router advertisements that contain link-layer addresses and configuration parameters. A NIOS appliance that supports IPv6 can listen for router advertisements and obtain the default gateway IP address and link MTU (maximum transmission unit). The link MTU is the maximum packet size, in octets, that can be conveyed in one transmission unit over a link. Thus you can set parameters on a router once and automatically propagate it to all attached hosts.

To configure the member to support IPv6:

1. From the **Grid** tab, select the **Grid Manager** tab -> **grid_member** check box -> Edit icon.
2. Select the **Network** -> **Basic** tab of the **Grid Member Properties** editor.
3. Click the Add icon of the Additional Ports and Addresses table, select IPv6 and complete the following:
   - **Address**: Type the IPv6 address for the grid member on the interface. An IPv6 address is a 128-bit number in colon hexadecimal notation. It consists of eight 16-bit groups of hexadecimal digits separated by colons (example: 12ab:0000:0000:0123:4567:89ab:0000:cdef).
   - **Subnet Mask**: Choose the CIDR netmask for the subnet to which the VIP address connects. The prefix length can range from 0 to 128, due to the larger number of bits in the IPv6 address.
   - **Gateway**: Do one of the following:
     - Type the IPv6 address of the default gateway of the subnet to which the VIP address connects.
     - Type **auto** to enable the appliance to acquire the IP address of the default gateway and the link MTU from router advertisements.
4. Click **Save & Close**.
Configuring DNS for IPv6 Addressing

Configuring the appliance to manage DNS services for IPv6 connections is similar to configuring DNS services for IPv4 connections. For simplicity, the IPv6 procedures are located in the same location as the corresponding procedures for IPv4 in this chapter. In most cases, the key difference within the procedure involves selecting an IPv6 mapping zone instead of an IPv4 mapping zone. You can configure the following tasks:

Table 13.2 IPv6 DNS Configuration Checklist

<table>
<thead>
<tr>
<th>Step</th>
<th>For more information</th>
</tr>
</thead>
</table>
| Create primary or secondary name servers and specify an IPv6 root server. | • About Authoritative Zones on page 404  
  • Specifying a Primary Server on page 411  
  • Specifying a Secondary Server on page 414  
  • Creating a Root Zone on page 408 |
| Configure the IPv6 zones. | • Creating an Authoritative Forward-Mapping Zone on page 405  
  • Creating an Authoritative Reverse-Mapping Zone on page 406 |
| Configure IPv6 resource records | • Managing AAAA Records on page 454  
  • Managing PTR Records on page 455 |
Chapter 14  DNS Views

DNS views enable the NIOS appliance to serve different versions of DNS data based on the host accessing it. The topics in this chapter include:

- Using Infoblox DNS Views on page 392
  - About DNS Views and Network Views on page 394
- Configuring DNS Views on page 394
  - Adding a DNS View on page 395
  - Defining Match Clients Lists on page 396
  - Copying Zone Records on page 397
  - Managing the DNS Views of a Grid Member on page 397
  - Managing Recursive DNS Views on page 398
  - Managing the Order of DNS Views on page 399
  - Managing DNS Views on page 400
- Configuration Example: Configuring a DNS View on page 401
**Using Infoblox DNS Views**

DNS views provide the ability to serve one version of DNS data to one set of clients and another version to another set of clients. With DNS views, the NIOS appliance can provide a different answer to the same DNS query, depending on the source of the query.

In *Figure 14.1*, the appliance has two views: an Internal and an External DNS view. When the appliance receives queries from DNS clients, it responds with data from either the Internal or External DNS view, depending on the source IP address. When the appliance receives a query from Client A and determines that it can resolve the query from data in the Internal view, the appliance responds with the IP address of the site in the Internal view. When the appliance receives a query from Client B and determines that it can resolve the query from data in the External view, it responds with the IP address in the External view.

*Figure 14.1 Internal and External Views*

You can configure both forward and reverse mapping zones in DNS views and provide DNS services, such as name resolution, zone transfers and dynamic DNS updates. For information about these services, see *Configuring DNS Services* on page 479.

You can provide multiple views of a given zone with a different set of records in each DNS view. In *Figure 14.2*, both views contain the corp100.com zone and the sales.corp100.com zone. The finance.corp100.com zone is only in the internal DNS view, and only internal users are allowed to access records in that zone. Resource records can also exist in multiple zones. In the example, the A records for serv1.sales.corp100.com and serv2.sales.corp100.com are in the sales.corp100.com zones in both views.

*Figure 14.2 Zone Data in Each DNS View*
You can control which clients access a DNS view through the use of a match list specifying IP addresses and/or TSIG (transaction signature) keys. When the NIOS appliance receives a request from a client, it tries to match the source IP address and/or TSIG key with its match list when determining which DNS view, if any, the client can access. After the appliance determines that a client can access a DNS view, it checks the zone level settings to determine if it can provide the service that the client is requesting.

For information on TSIG keys or defining zone transfer settings, see Enabling Zone Transfers on page 491. For more information on match lists, see Defining Match Clients Lists on page 396. For information on defining query settings, refer to Controlling DNS Queries on page 486.

Figure 14.3 illustrates how the NIOS appliance resolves a query for a domain name in a zone of a DNS view. In the example, the internal DNS view is listed before the external DNS view. Therefore, when the appliance receives a query, it checks the match list of the internal DNS view first. If it does not find the source address in the match list of the internal DNS view, it checks the match list of the external DNS view. The match list of the external DNS view allows all IP addresses.

Next, the NIOS appliance checks the zone level settings to determine if it is allowed to resolve queries from the client for domain names in that zone. After the appliance determines it is allowed to respond to queries from this client, it resolves the query and sends back the response to the client.

Figure 14.3 Query Resolution

When you create more than one DNS view, as shown in Figure 14.3, the order of the views is important. View order determines the order in which the NIOS appliance checks the match lists. In Figure 14.3, the internal DNS view is listed before the external DNS view. If the views were reversed, no hosts would receive DNS replies from the internal DNS view because the match list of the external DNS view allows replies to clients with any IP address. For information on how to order views, see Managing the DNS Views of a Grid Member on page 397.

In a grid, each grid member can host its own set of views. A grid member can serve as the primary or secondary server for multiple views of a particular zone. For information about specifying primary and secondary servers, see Assigning Zone Authority to Name Servers on page 411.
About DNS Views and Network Views

The NIOS appliance provides one default DNS view, which is always associated with the default network view. You can create additional network and DNS views. A network view is a single routing domain with its own networks. For information about network views, see About Network Views on page 591.

The default DNS view initially allows all IP addresses access, and has the same recursion setting as the grid. You can change these properties and rename the default DNS view, but you cannot delete it. When you upgrade or migrate from a name server, or an earlier version of software that does not support DNS views, the appliance places all the zones defined in the older release in the default DNS view. You can then create additional views and organize the zones in each view.

When you create a network view, the appliance automatically creates a corresponding DNS view with “default.” prepended to the name of the network view. You can rename the system-defined DNS view and configure its properties.

If an appliance contains only one network view, all DNS views are associated with that network view. If there are multiple network views, the appliance lists the network views so you can select one from the list. The appliance displays the network views only when there are multiple network views configured.

A DNS view can be in one network view only, but a network view can have multiple DNS views. If you enable dynamic DNS updates, you must specify which DNS view receives the updates. In a network view, only one DNS view can receive the dynamic DNS updates. For information, see Sending DDNS Updates to a DNS Server on page 518.

Configuring DNS Views

Following are the tasks to configure a DNS view:

1. Add a DNS view, as described in Adding a DNS View on page 395.
2. Define a Match Clients list to restrict access to the DNS view. For information, see Defining Match Clients Lists on page 396.
3. Add zones to the DNS view. You can add authoritative forward-mapping and reverse-mapping zones, as well as delegated, forward, and stub zones. For information about configuring each type of zone, see Configuring Authoritative Zones on page 404 and Configuring Delegated, Forward, and Stub Zones on page 427.

You can optionally do the following:

1. Copy resource records from one zone to another. This is useful when different DNS views have the same zone and have multiple resource records in common. For information, see Managing DNS Views on page 400.
2. Create resource records in a group and share the group among multiple zones. For information, see About Shared Record Groups on page 472.
3. Specify which interface IP address is published in the glue A record of the DNS view. For information, see Changing the Interface IP Address on page 398.
4. Manage recursive views. For information, see Managing Recursive DNS Views on page 398.
5. Manage the order of the DNS views, as this determines the order in which the NIOS appliance checks the Match Clients list. For information, see Managing the Order of DNS Views on page 399.
Adding a DNS View

You can add up to 255 DNS views. When you add a DNS view, specify the following:

- The network view in which you are creating the DNS view.
  The appliance lists the network views only when there are multiple network views. Otherwise, it automatically associates the DNS view with the default network view.
- A Match Clients list specifying the hosts allowed access to the DNS view
  If you do not define a list, the appliance allows all hosts to access the DNS view. For more information, see Defining Match Clients Lists on page 396.
- Whether recursive queries are allowed
  When a name server is authoritative for the zones in a DNS view, you can disable recursion since your name server should be able to respond to the queries without having to query other servers.
  If you want to allow a grid member to respond to recursive queries from specific IP addresses, you can create an empty DNS view, that is, one that has no zones in it, and enable recursion. For information, see Configuration Example: Configuring a DNS View on page 401

Note: This setting overrides the recursion setting at the grid and member levels.

To configure a new DNS view:

1. If there is more than one network view in the grid, select the network view in which you are creating the DNS view.
2. From the Data Management tab -> DNS tab, expand the Toolbar and click Add -> Add DNS View.
3. In the Add DNS View wizard, complete the following fields:
   - DNS View: Enter the name of the DNS view. It can be up to 64 characters long and can contain any combination of printable characters. Each DNS view must have a unique name. You cannot create two DNS views with the same name, even if they are in different network views.
   - Comment: Optionally, enter information about the DNS view. You can enter up to 256 characters.
   - Enable Recursion: This field's initial default state is inherited from the grid. It is inactive and greyed out until you click Override. After you click override, you can select or clear the check box to define a setting that applies to the DNS view only.
     Note that a DNS view actually inherits its recursion setting from the grid members that serve its zones. When you first create a DNS view though, it does not have any zones and therefore inherits its setting from the grid. After you create zones in the DNS view, Grid Manager can then determine the associated members and display the resulting inheritance. If a DNS view has multiple zones served by multiple members with different recursion settings, you can view the different settings in the Multi-Inheritance viewer.
     You can click Inherit to have the DNS view inherit its recursion setting from the grid.
   - Disable: Select this check box to disable this DNS view.
4. Select one of the following:
   - Next: Define a Match Clients list. For information, see Defining Match Clients Lists on page 396.
   - Save & Close: Save the entry and close the wizard.
   - Save & Edit: Save the entry and open the DNS View editor which provides more configuration options.
   - Save & New: Save the entry and create a new DNS view.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 25.
Defining Match Clients Lists

When you configure a DNS view, you can create a Match Clients list to identify source IP addresses and TSIG keys that are allowed or denied access to the DNS view. The NIOS appliance determines which hosts can access a DNS view by matching the source IP address or TSIG key with its Match Clients list. After the appliance determines that a host can access a DNS view, it checks the zone level settings to determine whether it can provide the service that the host is requesting for that zone.

If you do not configure a Match Clients list, then all devices are allowed access to the DNS view. However, if you configure a Match Clients list, then only those devices in the list with “Allow” permission can access the DNS view. All other devices are denied access, including grid members. Therefore, to allow a primary server of a zone to receive dynamic DNS updates from member DHCP servers, you must add the members to the Match Clients list as well.

Defining a Match Clients List for a DNS View

You can define a Match Clients list for a DNS view when you add a new DNS view (second step of the Wizard) or when you edit an existing DNS view. For information about adding a DNS view, see Adding a DNS View on page 395.

To define a Match Clients list for an existing DNS view:

1. From the Data Management tab, click the DNS tab -> Zones tab-> dns_view check box -> Edit icon.
2. Click the Match Clients tab, and then click the Add icon and select the item to add.
3. Depending on the item you selected, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows:
   - IPv4 Address: In the Name field of the new row, enter the IP address of the client. The Permission column displays Allow by default. To change it to Deny, click it to display the drop-down list and select Deny.
   - IPv4 Network: In the Add IPv4 Network panel, complete the following, and then click Add to add the network to the Match Clients list:
     - Address: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.
     - Permission: Select Allow or Deny from the drop-down list.
   - IPv6 Address: In the Name field of the new row, enter the IPv6 address of the client. The Permission column displays Allow by default. To change it to Deny, click it to display the drop-down list and select Deny.
   - IPv6 Network: In the Add IPv6 Network panel, complete the following, and then click Add to add the network to the Match Clients list:
     - Address: Enter an IPv6 network address and select the netmask from the drop-down list.
     - Permission: Select Allow or Deny from the drop-down list.
   - TSIG Key: In the Add TSIG Key panel, complete the following, and then click Add to add the TSIG key to the Match Clients list:
     - Key name: Enter a meaningful name for the key, such as a zone name or the name of a remote name server. This name must match the name of the same TSIG key on other name servers.
     - Key Data: To use an existing TSIG key, type or paste the key in the Key field. Alternatively, you can select the type of key and create a new key. By default, Grid Manager creates a 512-bit key. You can select 256-bit key or 128-bit key. Click Generate Key Data to create the new key.
     - The Permission column displays Allow by default. To change it to Deny, click it to display the drop-down list and select Deny.
   - DNS One 2.x TSIG: Select this when the other name server is a NIOS appliance running DNS One 2.x code.
   - Any Address/Network: Select this to allow or deny any IP address to access the DNS view.
4. Select one of the following:
   - **Next**: Define extensible attributes. For information, see *Using Extensible Attributes* on page 225.
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 25.

### Copying Zone Records

Different views of the same zone may have a number of records in common. If this is the case, you can copy zone records between views and zones.

**Note**: You cannot copy shared records and records that the NIOS appliance automatically creates, such as NS records and glue A records.

To copy zone records between DNS zones and views:

1. From the **Data Management** tab -> **DNS** tab, click **Copy Records** from the Toolbar.
2. In the **Copy Records** dialog box, Grid Manager displays the last selected zone or the zone from which you are copying zone records in the **Source** field. Complete the following to copy records:
   - **Destination**: Click **Select Zone** to select the destination zone. When there are multiple zones, Grid Manager displays the **Zone Selector** dialog box from which you can select one. After you select the zone, Grid Manager displays the associated DNS view.
   - **Copy All records**: Select this option to copy all the zone records, including those records not created on the NIOS appliance, such as HINFO records.
   - **Copy Specific Records**: Select this option to copy specific types of records. Select a resource record type from the **Available** column and click the right arrow to move it to the **Selected** column.
   - **Copy Options**: Select one of the following:
     - **Delete all records in destination before copying the records**: Select to delete all resource records in the destination zone before the records are copied.
     - **Overwrite existing records**: Select to overwrite existing resource records that have the same domain name owners as the records being copied.
3. Click **Copy & Close**.

**Note**: When you copy resource records between zones and there are pending scheduled tasks associated with these records, the appliance allows the copying of zone records before it executes the scheduled tasks.

### Managing the DNS Views of a Grid Member

A grid member can serve zones in different DNS views. You can manage the DNS views associated with a grid member as follows:

- You can specify which interface IP address is published in glue A records in the DNS view, as described in *Changing the Interface IP Address* on page 398.
- You can assign an empty recursive view to a member, as described in *Managing Recursive DNS Views* on page 398.
- You can control the list of DNS views as described in *Changing the Order of DNS Views* on page 399.
Changing the Interface IP Address

By default, a grid member publishes its LAN address in glue A records in the DNS view. You can change this default for each DNS view associated with a member. You can specify the NAT IP address or another IP address.

To specify the interface IP address for glue A records in a view:

1. From the Data Management tab, click the DNS tab -> Members tab -> member check box, and then click the Edit icon.
2. In the Member DNS Configuration editor, click Toggle Advanced Mode if the editor is in basic mode, and then select the DNS Views tab.
3. To change the address, click the entry in the Interface column of a DNS view, and select one of the following:
   - NAT IP Address to use the NAT address for glue A records.
   - Other to specify another address for glue A records. Enter the address in the Address field.
4. Select one of the following:
   - Save & Close: Save the entry and close the editor.
   - Save: Save the entry and keep the editor open.

Managing Recursive DNS Views

When you add a DNS view that has recursion enabled, the appliance resolves recursive queries from hosts on the Match Clients list of that view. If the DNS view contains zones and you delete those zones, the appliance retains the view in its configuration file, as long as recursion is enabled in the view. Such a view is called an empty recursive DNS view because it does not contain any zones. It enables the appliance to respond to recursive queries from the specified clients.

In a grid, all members automatically store DNS views that have recursion enabled in their configuration files. If you do not want a grid member to respond to recursive queries for clients in a particular DNS view, you can remove the view from the member’s configuration file.

To delete or retain an empty recursive DNS view in the DNS configuration file of a grid member:

1. From the Data Management tab, click the DNS tab -> Members tab -> grid_member check box -> Edit icon.
2. In the Member DNS Configuration editor, click Toggle Advanced Mode if the editor is in basic mode, and then select the DNS Views tab.
3. The Recursive Views Assigned to this Member section lists the empty recursive DNS views. Move a DNS view to the Selected column to explicitly assign the view to the grid member and include it in the DNS configuration file of the member. Move a DNS view to the Available column to remove it from the configuration file of the member. Empty recursive DNS views that you retain in the configuration file are automatically listed at the bottom of the list of DNS views. You can move them up on the list when you manually change the order of the DNS views, as described in Managing the DNS Views of a Grid Member on page 397.
4. Select one of the following:
   - Save & Close: Save the entry and close the editor.
   - Save: Save the entry and keep the editor open.
Managing the Order of DNS Views

When a member receives a query from a DNS client, it checks the Match Client lists in the order the DNS views are listed in the **Order of DNS Views** table of the **DNS Views** tab in the DNS Member editor. The NIOS appliance can order DNS views automatically, or you can order the DNS views manually. If you choose to have the appliance automatically update the order of the DNS views, it does so after each of the following events:

- Adding a DNS view to a member.
- Removing a DNS view from a member.
- Changing the address match list of a DNS view hosted by the member.

About IP Addresses and the Order of DNS Views

NIOS appliances with both IPv4 and IPv6 enabled can contain both types of addresses in the Match Clients list. When you enable IPv6 on the appliance, the order of DNS views in the GUI may be affected. Views are ordered and sorted automatically based on Match Clients lists. Views with IPv6 enabled are sorted as follows:

- If the Match Clients lists of all views contain IPv4 addresses only—The appliance orders views based on IPv4 addresses.
- If the Match Clients lists of all views contain IPv6 addresses only—The appliance orders views based on IPv6 addresses.
- If the Match Clients list of one DNS view has IPv6 addresses and all other views have IPv4 addresses—The appliance orders views based on IPv4 addresses, and the IPv6 address is given lowest priority in the ordering.
- If the Match Clients list of one DNS view has IPv4 addresses and all other DNS views have IPv6 addresses—The appliance orders DNS views based on IPv6 addresses, and the IPv4 address is given lowest priority in the ordering.
- If the Match Clients list of one DNS view has both IPv4 and IPv6 addresses—The appliance orders DNS views based on both IPv4 and IPv6 addresses, but more priority is given to the IPv4 addresses in the ordering.

*Note:* Only superusers can change the order of the views.

Changing the Order of DNS Views

To change the order of DNS views:

1. From the **Data Management** tab, click the **DNS** tab -> **Members** tab-> **grid_member** check box -> **Edit** icon.
2. In the **Member DNS Configuration** editor, click **Toggle Advanced Mode** if the editor is in basic mode, and then select the **DNS Views** tab.
3. In the Order of DNS Views section, select one of the following:
   - **Order DNS Views Automatically:** Click this to automatically order views after adding a new DNS view, removing a DNS view, or changing the match client list.
   - **Order DNS Views Manually:** This able lists the DNS views that have zones assigned to the grid member and the empty recursive views associated with the member. Select a DNS view, then click an arrow to move it up or down in the list.
4. Select one of the following:
   - **Save & Close:** Save the entry and close the editor.
   - **Save:** Save the entry and keep the editor open.
Managing DNS Views

You can list the DNS views, and then modify, disable, or remove any custom DNS view. You can modify and disable the default DNS view; however, under no circumstances can it be removed.

Listing DNS Views

After you configure additional DNS views, you can list all DNS views by navigating to the Data Management tab -> DNS tab -> Zones panel. This panel lists DNS views only after you modify the default DNS view or add a DNS view. If you never added DNS views or modified the default DNS view, this panel does not display the default DNS view. Instead, it lists the zones in the default DNS view. To display the properties of the default DNS view and edit it, use the Global Search function to locate and edit it.

Note that if you have not used Grid Manager to add a new DNS view, and you import DNS views through the Data Import Wizard or the API, you must log out and log back in to Grid Manager to display the newly imported DNS views.

For each DNS view, this panel displays the following by default:

- **Comment**: Comments that were entered for the DNS view.
- **Site**: Values that were entered for this pre-defined attribute.

You can also display the following column:

- **Disabled**: Indicates if the DNS view is enabled or disabled. Disabled DNS views are excluded from the named.conf file.

From this list, you can do the following:

- List the zones in a DNS view by clicking a DNS view name.
- Edit a DNS view, as described in the next section.
- Delete a DNS view, as described in Deleting DNS Views on page 401.

Modifying a DNS View

To modify a DNS view:

1. From the Data Management tab, click the DNS tab -> Zones tab -> dns_view check box -> Edit icon.
2. In the DNS View editor, you can do the following:
   - In the General tab, you can change any of the information you entered through the wizard. You can also disable a DNS view to temporarily block access to a DNS view. Disabling a DNS view excludes it from the named.conf file. For a description of the fields, see the online Help or Configuring DNS Views on page 394.
   - In the Match Clients tab, you can define or update a Match Clients list, as described in Defining Match Clients Lists on page 396.
   - In the DNSSEC tab, you can specify parameters for DNSSEC as described in Configuring DNSSEC on a Grid on page 552.
   - In the Root Name Servers tab, you can configure root name servers, as described in About Root Name Servers on page 494.
   - In the Extensible Attributes tab, you can modify the attributes. For information, see Using Extensible Attributes on page 225.
   - The Permissions tab displays if you logged in as a superuser. For information, see About Administrative Permissions on page 87.
3. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 25.
Deleting DNS Views

You can delete a DNS view if it is not the only view associated with a network view and if it is not selected for dynamic DNS updates. You cannot remove the system-defined default DNS view. When you remove a DNS view, the NIOS appliance removes the forward and reverse mappings of all the zones defined in the DNS view.

To delete a DNS view:
- From the Data Management tab, select the DNS tab > Zones tab > dns_view check box.
  
  To delete the DNS view immediately, click the Delete icon, and then click Yes to confirm the delete request. To schedule the deletion, click Schedule Deletion and in the Schedule Change panel, enter a date, time, and time zone. For information, see Schedule Deletion on page 25.
  
  Grid Manager moves the view to the Recycle Bin, from which you can restore or permanently delete it.

Configuration Example: Configuring a DNS View

In Figure 14.4, Member-A is a member of a grid. It is the primary name server for the corp100.com zone in the internal DNS view. It allows the IP address 192.168.10.1 and the 10.2.2.0/24 subnet access to DNS zone data in the internal DNS view. At the zone level, it allows transfers to an external secondary server, Infoblox-B, with an IP address of 192.168.10.1. Infoblox-B is a secondary server for the corp100.com zone. The process follows these steps:

1. Adding an Internal DNS View on Member-A
2. Adding a Zone to a DNS View
3. Copying Records Between DNS Zones, from the corp100.com zone in the default DNS view to the corp100.com zone in the internal DNS view
4. Verifying the Configuration

Figure 14.4 Configuring a DNS View

Adding an Internal DNS View

1. Expand the Toolbar and click Add -> Add DNS View.
2. In the Add DNS View wizard, specify the following, and then click Next:
   - Name: internal
   - Comment: internal DNS view
3. In the Match Clients panel, click Add and select IPv4 Network from the drop-down list.

Configuration Example: Configuring a DNS View

In Figure 14.4, Member-A is a member of a grid. It is the primary name server for the corp100.com zone in the internal DNS view. It allows the IP address 192.168.10.1 and the 10.2.2.0/24 subnet access to DNS zone data in the internal DNS view. At the zone level, it allows transfers to an external secondary server, Infoblox-B, with an IP address of 192.168.10.1. Infoblox-B is a secondary server for the corp100.com zone. The process follows these steps:

1. Adding an Internal DNS View on Member-A
2. Adding a Zone to a DNS View
3. Copying Records Between DNS Zones, from the corp100.com zone in the default DNS view to the corp100.com zone in the internal DNS view
4. Verifying the Configuration

Figure 14.4 Configuring a DNS View

Adding an Internal DNS View

1. Expand the Toolbar and click Add -> Add DNS View.
2. In the Add DNS View wizard, specify the following, and then click Next:
   - Name: internal
   - Comment: internal DNS view
3. In the Match Clients panel, click Add and select IPv4 Network from the drop-down list.
4. Do the following for IP addresses in the network 10.2.2.0/24:
   — Enter 10.2.2.0/24 in the in the Address field.
   — The Permission field displays Allow by default. Leave it as is.
   — Click Add.
   You will have 255 allowed client addresses in the Match Clients list when you are done.

5. Click Save & Close.

Adding a Zone to a DNS View
1. Expand the Toolbar and click Add -> Zone -> Add Auth Zone.
2. In the Add Auth Zone wizard, click Add an authoritative forward-mapping zone and click Next.
3. Specify the following, and then click Next:
   — Name: Enter corp100.com.
   — DNS View: Select Internal from the drop-down list.
4. In step 3 of the wizard, do the following:
   a. Select Use this set of name servers.
   b. Click the Add icon and select Grid Primary.
   c. Click Select Member and select Member A from the Select Grid Member dialog box.
   d. Click Add to add the grid member to the list of name servers.
   e. Click the Add icon again and select External Secondary.
   f. Enter the following information, and then click Add:
      — Name: InfobloxB
      — IP Address: 192.168.10.1
5. Click Save & Edit to display the Authoritative Zone editor and continue with the zone configuration.
6. Click Queries,
7. Click Override, and then click the Add icon and select IPv4 Network.
   — Enter 10.2.2.0/8 in the in the Address field.
   — The Permission field displays Allow by default. Leave it as is.
   — Click Add.
   This allows queries that the appliance answers from its internal DNS view.
8. Click Save & Close.

Copying Records Between DNS Zones
1. Navigate to the default DNS view and select the corp100.com zone.
2. Expand the Toolbar and click Copy Records.
3. In the Destination field, click Select Zone, and then select the corp100.com zone in the Internal DNS view.
4. Select Copy all records, and then click OK.
5. Click Save & Close.
   The records from corp100.com in the default DNS view are copied to corp100.com in the internal DNS view.

Verifying the Configuration
1. In the DNS tab, click Members and select the Member-A check box.
2. Expand the Toolbar and click View -> View DNS Configuration.
3. In the DNS Configuration File viewer, scroll through the contents of the file.
   Verify that the internal DNS view section is similar to the configuration file shown.
Chapter 15 Configuring DNS Zones

This chapter provides general information about DNS zones that you can configure and manage on the Infoblox appliance. The topics in this chapter include:

- **About Authoritative Zones** on page 404
  - Configuring Authoritative Zones on page 404
  - Creating an Authoritative Forward-Mapping Zone on page 405
  - Creating an Authoritative Reverse-Mapping Zone on page 406
  - Creating a Root Zone on page 408
  - Adding an Authoritative Subzone on page 408
  - Locking and Unlocking Zones on page 409
  - Enabling and Disabling Zones on page 409
- **About Domains and Zones** on page 410
- **Assigning Zone Authority to Name Servers** on page 411
  - Specifying a Primary Server on page 411
  - Specifying a Secondary Server on page 414
- **Using Name Server Groups** on page 417
  - Adding Name Server Groups on page 417
  - Viewing Name Server Groups on page 418
  - Applying Name Server Groups on page 418
- **Importing Zone Data** on page 419
  - About Importing Data into a New Zone on page 420
  - About Importing Data into an Existing Zone on page 420
  - Importing Data into Zones on page 420
- **Configuring Authoritative Zone Properties** on page 421
- **Removing Zones** on page 423
- **Restoring Zone Data** on page 425
- **Configuring Delegated, Forward, and Stub Zones** on page 427
  - Configuring a Delegation on page 427
  - Configuring a Forward Zone on page 428
  - Configuring Stub Zones on page 432
- **Viewing Zones** on page 440
About Authoritative Zones

An authoritative zone is a zone for which the local (primary or secondary) server references its own data when responding to queries. The local server is authoritative for the data in this zone and responds to queries for this data without referencing another server.

There are two types of authoritative zones:

- Forward-Mapping – An authoritative forward-mapping zone is an area of domain name space for which one or more name servers have the responsibility to respond authoritatively to name-to-address queries.
- Reverse-Mapping – A reverse-mapping zone is an area of network space for which one or more name servers have the responsibility to respond to address-to-name queries.

Configuring Authoritative Zones

You can configure and manage authoritative forward-mapping and IPv4 and IPv6 reverse-mapping zones on an Infoblox appliance. In a grid, an authoritative forward-mapping zone is an area of domain name space for which one or more grid members have the responsibility to respond authoritatively to name-to-address queries. The grid members can function as primary or secondary servers for the zone.

Following are the tasks to configure an authoritative zone:

1. Create the zone. The following sections explain how to create authoritative forward-mapping zones, reverse-mapping zones, subzones, and a custom root zone:
   - Creating an Authoritative Forward-Mapping Zone on page 405
   - Creating an Authoritative Reverse-Mapping Zone on page 406
   - Creating a Root Zone on page 408
2. Assign an Infoblox appliance as the primary or secondary server of the zone. For information, see Assigning Zone Authority to Name Servers on page 411.
3. Import resource records or add resource records manually. The following provides information about resource records:
   - Managing Resource Records on page 451
   - Importing Zone Data on page 419
4. Configure additional parameters. For information, see Configuring Authoritative Zone Properties on page 421.
5. Optionally, associate the zone with one or more networks. This is useful when you want to restrict the A, AAAA and host records to IP addresses from specific networks. For information, see Associating Networks with Zones on page 598.
Creating an Authoritative Forward-Mapping Zone

An authoritative forward-mapping zone is an area of domain name space for which one or more grid members have the responsibility to respond authoritatively to name-to-address queries.

**Note:** A single forward-mapping zone can map names to both IPv4 and IPv6 addresses.

To create an authoritative forward-mapping zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar, and click **Add -> Zone -> Add Auth Zone**.
2. In the **Add Authoritative Zone** wizard, click **Add an authoritative forward-mapping zone** and click **Next**.
3. Specify the following:
   - **Name**: Enter the domain name for the zone. Omit the trailing period (“.”) that signifies the root zone.
   - **DNS View**: This field displays only when there is more than one DNS view in the current network view. Select a DNS view from the drop-down list.
   - **Comment**: Enter a descriptive comment about the zone.
   - **Disable**: Click this check box to temporarily disable this zone. For information, see *Enabling and Disabling Zones* on page 409.
   - **Lock**: Click this check box to lock the zone so that you can make changes to it and prevent others from making conflicting changes. For information, see *Locking and Unlocking Zones* on page 409.
4. Select one of the following:
   - **Next**: Continue to the next steps in the wizard as follows:
     - Define the name servers for the zone. Refer to the online Help for information about this panel, or refer to the following:
       - For information on specifying primary and secondary servers, see *Assigning Zone Authority to Name Servers* on page 411.
       - For information on specifying name server groups, see *Using Name Server Groups* on page 417.
     - Define extensible attributes. For information, see *Using Extensible Attributes* on page 225.
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and open the **Authoritative Zone** editor which provides more configuration options.
   - **Save & New**: Save the entry and create another new zone.
   - Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 25.
Creating an Authoritative Reverse-Mapping Zone

An authoritative reverse-mapping zone is an area of network space for which one or more name servers—primary and secondary—have the responsibility to respond to address-to-name queries. Infoblox supports reverse-mapping zones for both IPv4 and IPv6 addresses.

**Note:** When you add an IPv4 reverse-mapping zone, the appliance automatically generates an in-addr.arpa space for the network address that you specify. When you add an IPv6 reverse-mapping zone, the appliance automatically generates an ip6.arpa space.

Specifying an RFC 2317 Prefix

**RFC 2317, Classless IN-ADDR.ARPA delegation** is an IETF (Internet Engineering Task Force) document that describes a method of delegating parts of the DNS IPv4 reverse-mapping tree that correspond to subnets smaller than a /24 (from a /25 to a /31). The DNS IPv4 reverse-mapping tree has nodes broken at octet boundaries of IP addresses, which correspond to the old classful network masks. So, IPv4 reverse-mapping zones (and delegation points) usually fall on /8, /16, or /24 boundaries.

With the proliferation of CIDR (Classless Inter-Domain Routing) support for routing, ISPs no longer assign entire /24 networks to customers that only need a handful of IPv4 addresses. In general, IPv4 address assignments no longer fall on classful boundaries. For DNS, a problem comes into play when an ISP gives a customer an address range that is smaller than a /24, but the customer also wants to be delegated the DNS reverse-mapping zone.

If the ISP gives you, for example, a subnet with a 25-bit mask, then you only have half of the /24 address range. If you configure your DNS server to be authoritative for the zone corresponding to a /24 subnet, the DNS server cannot resolve half of the possible reverse-mapping records in the zone. RFC 2317 defines an approach, considered a best practice, which addresses this issue.

**Note:** Before enabling RFC 2317 support for zones, disable forwarders for the zone, especially when any sort of delegation (including RFC 2317) is being used. If you do not, reverse lookups may fail. For more information, contact Infoblox Support for the Tech Note on RFC 2317 delegation.

Adding an IPv4 Reverse-Mapping Zone

To add an IPv4 reverse-mapping zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Zone -> Add Auth Zone.
2. In the Add Authoritative Zone wizard, click Add an authoritative IPv4 reverse-mapping zone and click Next.
3. Specify the following zone information:
   - **IPv4 Network**: Enter the IPv4 address for the address space for which you want to define the reverse-mapping zone and select a netmask from the Netmask drop-down list. Alternatively, you can specify the address in CIDR format, such as 192/8.
     
     To use an RFC 2317 prefix, select a netmask value that is between 25 to 31, inclusive. Grid Manager displays the RFC 2317 Prefix field. Enter a prefix in the text field. Prefixes can include alphanumeric characters. Though spaces are allowed, Grid Manager displays a warning when a prefix includes a space. For information, see Specifying an RFC 2317 Prefix on page 406.
   - **Name**: Enter the domain name of the reverse-mapping zone.
   - **DNS View**: This field displays only when there is more than one DNS view in the current network view. Select a DNS view from the drop-down list.
   - **Comment**: Optionally, enter additional information about the zone.
   - **Disable this zone**: Select this option to temporarily disable this zone. For information, see Enabling and Disabling Zones on page 409.
— **Lock this zone**: Select this option to lock the zone so that you can make changes to it and prevent others from making conflicting changes. For information, see *Locking and Unlocking Zones* on page 409.

4. Select one of the following:
   — **Next**: Continue to the next steps in the wizard as follows:
     — Define the name servers for the zone. Refer to the online Help for information about this panel, or refer to the following:
       • For information on specifying primary and secondary servers, see *Assigning Zone Authority to Name Servers* on page 411.
       • For information on specifying name server groups, see *Using Name Server Groups* on page 417.
     — Define extensible attributes. For information, see *Using Extensible Attributes* on page 225.
   — **Save & Close**: Save the entry and close the editor.
   — **Save & Edit**: Save the entry and launch the *Authoritative Zone* editor which provides more configuration options.
   — **Save & New**: Save the entry and create another new zone.
   or
   — Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 25.

### Adding an IPv6 Reverse-Mapping Zone

To add an IPv6 reverse-mapping zone:

1. From the *Data Management* tab, select the *DNS* tab, expand the Toolbar and click *Add -> Zone -> Add Auth Zone*.
2. In the *Add Authoritative Zone* wizard, click *Add an authoritative IPv6 reverse-mapping zone* and click **Next**.
3. Enter the following zone information:
   — Enter one of the following to identify the zone:
     — **IPv6 Network Prefix**: Enter the 128-bit IPv6 address for the address space for which you want to define the reverse-mapping zone. When you enter an IPv6 address, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2006:0000:0000:0123:4567:89ab:0000:cdef can be shortened to 2006::123:4567:89ab:0::cdef. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The NIOS appliance displays an IPv6 address in its shortened form, regardless of its form when it was entered. Choose the network prefix that defines the IPv6 network address space.
     — **Name**: Enter the domain name of the reverse-mapping zone.
     — **DNS View**: This field displays only when there is more than one DNS view in the current network view. Select a DNS view from the drop-down list.
     — **Comment**: Enter a descriptive comment about the zone.
     — **Disable**: Click this check box to temporarily disable this zone. For information, see *Enabling and Disabling Zones* on page 409.
     — **Lock**: Click this check box to lock the zone so that you can make changes to it and prevent others from making conflicting changes. For information, see *Locking and Unlocking Zones* on page 409.
4. Select one of the following:
   — **Next**: Continue to the next steps in the wizard as follows:
     — Define the name servers for the zone. Refer to the online Help for information about this panel, or refer to the following:
       • For information on specifying primary and secondary servers, see *Assigning Zone Authority to Name Servers* on page 411.
       • For information on specifying name server groups, see *Using Name Server Groups* on page 417.
     — Define extensible attributes. For information, see *Using Extensible Attributes* on page 225.
— **Save & Close**: Save the entry and close the editor.
— **Save & Edit**: Save the entry and launch the *Authoritative Zone* editor which provides more configuration options.
— **Save & New**: Save the entry and create another new zone.

or

— Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 25.

### Creating a Root Zone

The NIOS appliance allows you to create an internal root zone for your organization. When the appliance receives a query for DNS data that is not in its cache or authoritative data, it can query an internal root server after querying any specified forwarders. If you do not specify an internal root server and the appliance can access the Internet, it queries the Internet root servers. For information on root name server, see *About Root Name Servers* on page 494.

To create a root zone, create an authoritative forward-mapping zone as described in [*Creating an Authoritative Forward-Mapping Zone*](#) on page 405 and specify the following:

- Enter a period (.) in the *Name* field.
- Optionally, enter a comment.
- Select a grid member as the primary name server for the root zone.

Once created, the root zone automatically becomes the parent of all the zones under the root zone.

### Adding an Authoritative Subzone

After creating a zone, you can add more zones at the same level, or add subordinate zones (*subzones*). The subzones can be authoritative, delegated, forward, or stub. For simplicity, the zones created in this example are authoritative (as are all zones by default). For information about configuring the other zone types, see [*Configuring Delegated, Forward, and Stub Zones*](#) on page 427.

You create an authoritative zone when you assign authority for all the resource records of a particular domain to one or more name servers. You create a subzone when you assign authority for all the resource records of a subdomain to name servers. The name servers can be the same as, or different from, the name servers that serve resource records for the parent domain.

The distinction between domains and zones is that domains provide a logical structure to the DNS name space while zones provide an administrative structure. The difference between domains and subdomains and zones and subzones is that the terms *subdomains* and *subzones* reference their relationship to a parent domain or zone. With the exception of the root domain and root zone, all domains are subdomains and all zones are subzones.

You can organize a domain based on logical divisions such as type (*.com, .gov, .edu; or sales, eng, sup) or location (*.uk, .jp, .us; or hq, east, west). *Figure 15.1* on page 409 shows one way to organize the external (public) name space and the internal (private) name space for a corporation with the domain name *corp100.com*. The external name space follows standard DNS conventions. Internally, you create an individual subdomain and corresponding subzone for each department.
About Authoritative Zones

The DNS name space is logically structured into domains and subdomains.

The DNS name space is administratively structured into zones and subzones.

“.” = root domain

The procedure for adding a subzone is the same as that used to add an authoritative zone. The only difference is that you specify the subzone name in the Name field. For information about adding authoritative zones, see Configuring Authoritative Zones on page 404.

Locking and Unlocking Zones

You can lock a zone when you create or edit it to prevent other administrators from making conflicting changes. When you lock a zone, Grid Manager displays LOCKED beside the zone name when you view the records and subzones of the zone in the Zones panel. When other administrators try to make changes to a locked zone, the system displays a warning message that the zone is locked by admin_name.

You can perform dynamic updates through mechanisms such as DDNS and nsupdate on a locked zone. The system can also add auto-generated records such as glue A records and NS records to a locked zone. Locks on a zone do not impact its child zones.

Only a superuser or the administrator who locked the zone can unlock it. Locks do not expire; you must manually unlock a locked zone.

Enabling and Disabling Zones

The NIOS appliance allows you to disable and enable a zone when you create or edit it. When you disable a zone, Grid Manager removes it from the DNS configuration file, but not from the database. This feature is especially helpful when you have to move or repair the server for a particular zone. You can easily disable a zone temporarily, and then enable it after the move or repair is completed.

Note: Throughout this documentation, the trailing dot indicating the root zone is not shown, although its presence is assumed.
ABOUT DOMAINS AND ZONES

After creating a zone, you can add more zones at the same level, or add subordinate zones (subzones). The subzones can be authoritative, delegated, forward, or stub.

The distinction between domains and zones is that domains provide a logical structure to the DNS name space while zones provide an administrative structure. The difference between domains and subdomains and zones and subzones is that the terms subdomains and subzones reference their relationship to a parent domain or zone. With the exception of the root domain and root zone, all domains are subdomains and all zones are subzones.

You can organize a domain based on logical divisions such as type (.com, .gov, .edu; or sales, eng, sup) or location (.uk, .jp, .us; or hq, east, west). Figure 15.1 on page 409 shows one way to organize the external (public) name space and the internal (private) name space for a corporation with the domain name corp100.com. The external name space follows standard DNS conventions. Internally, you create an individual subdomain and corresponding subzone for each department.

Figure 15.2 Domains and Subdomains, and Forward-Mapping Zones and Subzones

On the Infoblox appliance, you can configure and manage DNS zones and subzones.
Assigning Zone Authority to Name Servers

Forward-mapping zones answer name-to-address queries, and reverse-mapping zones answer address-to-name queries. When you create an authoritative forward-mapping zone or reverse-mapping zone, you must define a name server as a primary server for that zone. A primary server contains editable zone data, which that server can send to other (secondary) servers through zone transfers. You can also create one or more secondary name servers for a zone. A secondary server for a zone receives read-only zone data from the primary server.

**Note:** The primary/secondary relationship between name servers is also called “master”/”slave”. You can enter, modify, and remove zone data on the primary (or master) server, which can then send new and modified data in a read-only form to the secondary (or slave) server. Both primary and secondary name servers are authoritative for the zone data they serve. The distinction between them is how they get their zone data.

If a zone is part of an internal DNS structure for a private network, the inclusion of a secondary DNS server is optional, though highly recommended. If a zone is part of an external DNS structure for a public network such as the Internet, then a secondary server in a different subnet from the primary server is required. This requirement provides an additional safeguard against localized network failures causing both primary and secondary name servers for a zone to become inaccessible.

In Grid Manager, you can specify the primary and secondary servers for a zone or you can specify a name server group. A name server group is a collection of one primary server and one or more secondary servers. For information on name server groups, see Using Name Server Groups on page 417.

Specifying a Primary Server

When you create a zone, the primary server can be a grid member, an external DNS server that you specify, or a Microsoft DNS server that is managed by a grid member. For information about managing Microsoft Windows DNS servers, see Chapter 29, Managing Microsoft Windows Servers, on page 727.

Although a zone typically has just one primary name server, you can specify up to ten independent servers for a single zone. When the primary server is a grid member, however, then only that member can be the primary server.

A primary server can be in stealth mode, which means that it does not respond to queries from other name servers and its NS record is not published among the zone data. Such a server is also called a “hidden primary”.

A hidden primary provides data to its secondary servers, which in turn respond to DNS queries using this data. One of several advantages of this approach is that you can take the primary server offline for administrative or maintenance reasons without causing a disruption to DNS service (within the expiration interval set for the validity of its zone data—the default is 30 days).

When you add an authoritative forward-mapping zone and assign responsibility for the zone to a primary name server whose host name belongs to the name space of the zone, the NIOS appliance automatically generates an NS (name server) record and an A (address) record for the name server. This type of A record is called a glue record because it “glues” the NS record to the IP address (in the A record) of the name server.

In Grid Manager, you can specify the primary server for a zone when you create it using the Add Authoritative Zone wizard or when you edit an existing zone using the Authoritative Zone editor. For information on how to add a new zone through the wizard, see Configuring Authoritative Zones on page 404. The following procedure describes how to access the editor of a zone.
To specify a primary server for an existing zone:

1. From the Data Management tab, select the DNS tab -> Zones tab -> zone check box, and then click the Edit icon.
2. In the Authoritative Zone editor, click Name Servers.
3. Select Use this set of name servers.
4. Click the Add icon and select one of the following options for a primary server:
   - Grid Primary: Choose this option to select a grid member as the primary server for the zone. See Specifying a Grid Primary Server on page 412.
   - Microsoft Primary: Choose this option to select a Microsoft DNS server as the primary server for the zone. See Specifying a Microsoft Primary Server on page 413.
   - External Primary: Choose this option if the appliance is in a grid and you want to specify a primary server outside the grid (“external” to the grid). See Specifying an External Primary Server on page 413.
5. Select one of the following:
   - Save & Close: Save the entry and close the editor.
   - Save: Save the entry and keep the editor open.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 25.

Specifying a Grid Primary Server

In the Add Grid Primary panel, do the following, and then click Add to add the grid member to the list of name servers for the zone as primary:

- If no member is displayed, click Select to specify a grid member. When there are multiple members, Grid Manager displays the Member Selector dialog box from which you can select a primary name server.
- Stealth: Click this to hide the NS record for the primary name server from DNS queries. The NIOS appliance does not create an NS record for the primary name server in the zone data. Clear the check box to display the NS record for the primary name server in responses to queries.

Changing the SOA Name for a Zone

If the primary name server of a zone is a grid member, the NIOS appliance allows you to change the SOA (start of authority) name that is automatically created when you initially configure the zone. For example, you might want to hide the primary server for a zone. If your appliance is named dns1.zone.tld, and for security reasons, you may want to show a secondary server called dns2.zone.tld as the primary server. To do so, you would go to dns1.zone.tld zone (being the true primary) and change the SOA to dns2.zone.tld to hide the true identity of the real primary server.

To change the SOA name for a zone:

1. From the Data Management tab, select the DNS tab -> Zones tab -> dns_view -> zone check box -> Edit icon.
2. In the Authoritative Zone editor, click Settings.
3. Click Override beside the Primary name server field and enter the new SOA name.
4. Select one of the following:
   - Save & Close: Save the entry and close the editor.
   - Save: Save the entry and keep the editor open.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 25.
Specifying a Microsoft Primary Server

You can assign a Microsoft server as the primary server of a zone when it is managed by a grid member in read/write mode. For information, see Chapter 29, Managing Microsoft Windows Servers, on page 727.

When a Microsoft server is the primary server of a zone, the zone can only support standard DNS resource records. It does not support the Infoblox record types host records, bulk host records, and shared record groups. You cannot add any of these records to the zone nor assign a DNS zone with these records to a Microsoft server as the primary server.

In the Add Grid Primary panel, do the following to assign a Microsoft primary server:

1. Complete the following:
   - Select **Use this set of name servers**.
   - Click the Add icon and select **Microsoft Primary**.

2. In the **Add Microsoft Primary** panel, do the following, and then click **Add** to add the Microsoft primary server to the list of name servers for the zone:
   - If no server is displayed, click **Select Server** to specify a Microsoft server. When there are multiple servers, Grid Manager displays the **Server Selector** dialog box from which you can select a Microsoft server. Grid Manager lists Microsoft servers that are managed in read/write mode. It does not include Microsoft servers managed in read-only mode.
   - **Information to create NS record**: Grid Manager automatically creates the NS record. After you select a server, Grid Manager populates the **Name** and **IP Address** fields. Grid Manager uses this information when it creates the NS record, unless you select **Stealth**. You can specify a different FQDN or IP address for the NS record; for example, for a multihomed server.
   - **Store the zone in Active Directory (AD Integrated Zone)**: This is enabled and selected by default only if the Microsoft server is a domain controller. Note that you can enable Active Directory integration only after the Microsoft server has been synchronized at least once because its AD ability is not known before the synchronization. This is disabled when the Microsoft server is not a domain controller.
   - **Stealth**: Select this option to hide the NS record for the primary name server from DNS queries. Grid Manager does not create an NS record for the primary name server in the zone data. Clear this option to display the NS record for the primary name server in responses to queries. Note that this option is not available for AD-integrated zones.

Specifying an External Primary Server

In the Add External Primary panel, do the following, and then click **Add** to add the external primary server to the list of name servers for the zone:

- **Name**: Type a resolvable domain name for the external primary server.
- **Address**: Type the IP address of the external primary server.
- **Stealth**: Click this check box to hide the grid external primary server from DNS queries. The NIOS appliance does not create an NS record for the grid external primary server in the zone data. Clear the check box to display the NS record for the primary name server in responses to queries.
- **Use TSIG**: To authenticate zone transfers between the local appliance and the external primary server using a TSIG (transaction signature), select this check box. Infoblox TSIGs use HMAC-MD5 hashes. These are keyed one-way hashes for message authentication codes using the Message Digest 5 algorithm. For details, see RFC 1321, The MD5 Message-Digest Algorithm, and RFC 2104, HMAC: Keyed-Hashing for Message Authentication.
  - **Key name**: Type or paste the name of the TSIG key you want to use. This must be the same name as that of the TSIG key on the external primary server.
  - **Key Data**: Type or paste a previously generated key. This key must also be present on the external primary server. You can generate a TSIG key, or obtain the TSIG key name and key from the external name server, either by accessing the server yourself or by requesting the server administrator to deliver them to you through some out-of-band mechanism. Then type or copy-and-paste the name and key into the appropriate fields.
Configuring DNS Zones

- **Use 2.x TSIG**: If you want to use TSIG authentication and the external primary name server is a NIOS appliance running DNS One 2.x code, select this check box. The local appliance generates the required TSIG key for authenticating DNS messages to and from appliances running DNS One 2.x code.

**Note**: On the appliance you configure as a secondary server for a zone, you must associate a TSIG key for each primary server to which the secondary server requests zone transfers. On the appliance you configure as a primary server for a zone, you can set a TSIG key at the grid, member, or zone level. Because the secondary server requests zone transfers, it must send a specific key in its requests to the primary server. Because the primary server responds to the requests, it can have a set of TSIG keys from which it can draw when responding. As long as the primary server can find the same TSIG key that the secondary sends it, it can verify the authenticity of the requests it receives and authenticate the responses it sends. Use NTP to synchronize the time on both name servers that use TSIG-authenticated zone transfers.

### Specifying a Secondary Server

A secondary name server is as authoritative for a zone as a primary server. Like a primary server, a secondary server answers queries from resolvers and other name servers. The main difference between a secondary and primary server is that a secondary server receives all its data from a primary server, or possibly from another secondary server that relays zone data it receives. The zone data passes from a primary to a secondary server (and possibly from that secondary server on to another secondary server). This process is called a zone transfer.

The advantage of using primary and secondary name servers is that you enter and maintain zone data in one place—on the primary server. The data is then distributed to the one or more secondary servers. Secondary servers can be grid members, external DNS servers or Microsoft DNS servers that are managed by grid members.

In Grid Manager, you can specify the secondary server for a zone when you create it using the Add Authoritative Zone wizard and when you edit an existing zone using the Authoritative Zone editor. For information on how to add a new zone through the wizard, see [Configuring Authoritative Zones](#) on page 404. The following procedure describes how to access the editor of a zone.

To specify a secondary server for an existing zone:

1. From the **Data Management** tab -> **DNS** tab -> **Zones** tab -> **zone** check box, and then click the Edit icon.
2. In the **Authoritative Zone** editor, click **Name Servers**.
3. Select **Use this set of name servers**.
4. Click the Add icon and select one of the following options:
   - **Grid Secondary**: Selects the local appliance as the secondary server (or if the appliance is deployed in a grid and you want to make a different member the secondary server). See [Adding Grid Secondaries](#) on page 415.
   - **Microsoft Secondary**: Select this option if you want to specify a managed Microsoft DNS server as a secondary server. See [Specifying Microsoft Secondary Servers](#) on page 415.
   - **External Secondary**: Select this option if the appliance is in a grid and you want to specify a secondary server outside the grid ("external" to the grid), or if the appliance is deployed independently from a grid. See [Specifying External Secondaries](#) on page 416.
5. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.
   - Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see [Scheduling Tasks](#) on page 25.
Adding Grid Secondaries

In the Add Grid Secondary panel, enter the following, and then click **Add** to add the grid secondary server to the list of name servers for the zone:

- If no member is displayed, click **Select** to specify a grid member. When there are multiple members, Grid Manager displays the **Member Selector** dialog box from which you can select a secondary name server.

- **Stealth:** Select this to hide the NS record for the secondary name server from DNS queries. The NIOS appliance does not create an NS record for this name server in the zone data. Select the check box again to display the NS record for the secondary name server in responses to queries. A secondary server in stealth mode is also known as a “hidden secondary”.

  For example, you can configure a hidden secondary when a secondary server is at a branch office with a slow connection to the rest of corporate network. Configure local hosts at the branch office to send DNS queries to the secondary server, but keep it hidden from other name servers on the rest of the network so that they do not send it queries. Instead, they use a server located in a different part of the network that has faster connection speeds.

- **Lead Secondary:** This option becomes available only after you specify the primary name server as external. When a primary server is external to a grid whose members are secondary servers, you can select this check box to designate one member as a lead secondary. The primary server sends zone transfers to the lead secondary, which distributes the zone data to the other secondary servers in the grid using zone transfers (not the grid data replication mechanism). After you designate a grid member as a lead secondary for a zone, you do not have to configure members to use the lead secondary server. All other grid members acting as secondary servers for the zone automatically use the lead secondary to get zone data. Using a lead secondary simplifies the addition, modification, and removal of other secondary servers in the grid. As long as the lead secondary remains unchanged, you need not update intervening firewall policies or the external primary server whenever you make changes to non-lead secondary grid members. This approach also reduces the amount of traffic between primary and secondary servers.

- **Update Zones Using:** This option becomes available only after you specify a grid member as the primary server.
  - **Grid Replication (recommended):** Select this check box to use grid replication to move zone data from the primary to secondary servers.
  - **DNS Zone Transfers:** Select this check box to use the DNS zone transfer process to move zone data from the primary to secondary servers.

Specifying Microsoft Secondary Servers

You can assign a Microsoft server as the primary server of a zone when it is managed by a grid member in read/write mode. For information, see *Chapter 29, Managing Microsoft Windows Servers*, on page 727.

Since Microsoft servers cannot replicate data from the grid, when a DNS zone is defined as a secondary on a Microsoft server, the Microsoft server obtains the content of the zone only through DNS zone transfers.

- In the Add Microsoft Secondary panel, do the following:
  - If no server is displayed, click **Select Server** to specify a Microsoft server. When there are multiple servers, Grid Manager displays the **Server Selector** dialog box from which you can select a Microsoft server. Grid Manager lists Microsoft servers that are managed in read/write mode. It does not include Microsoft servers managed in read-only mode.
  - **Information to create NS record:** Grid Manager automatically creates the NS record. After you select a server, Grid Manager populates the **Name** and **IP Address** fields. Grid Manager uses this information when it creates the NS record, unless you select Stealth.
  - **Stealth:** Select this option to hide the NS record for the secondary name server from DNS queries. Grid Manager does not create an NS record for this name server in the zone data. Clear this option to display the NS record for the secondary name server in responses to queries.
Specifying External Secondaries

In the Add External Secondary panel, enter the following, and then click Add to add the external secondary server to the list of name servers for the zone:

- **Name**: Enter a resolvable domain name for the external secondary server.
- **Address**: Enter the IP address of the external secondary server.
- **Stealth**: Click this check box to hide the NS record for the secondary name server from DNS queries. The NIOS appliance does not create an NS record for the secondary name server in the zone data. Select the check box again to display the NS record for the secondary name server in responses to queries.
- **Use TSIG**: To authenticate zone transfers between the local appliance and the external secondary server using a TSIG (transaction signature), select this check box. Infoblox TSIGs use HMAC-MD5 hashes. These are keyed one-way hashes for message authentication codes using the Message Digest 5 algorithm. For details, see RFC 1321, *The MD5 Message-Digest Algorithm*, and RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*.
  
  - **Key name**: Type or paste the name of the TSIG key you want to use. This must be the same name as that of the TSIG key for this zone on the external secondary server.
  - **Key**: Type or paste a previously generated key. On the external secondary server, this key must also be present and associated with this zone. You can generate a TSIG key, or you can obtain the TSIG key name and key from the external name server, either by accessing the appliance yourself or by requesting the appliance administrator to deliver them to you through some out-of-band mechanism. Then, type or copy-and-paste the name and key into the appropriate fields.
- **Use 2.x TSIG**: Select this check box to use TSIG authentication and the external secondary name server is a NIOS appliance running DNS One 2.x code. The local appliance generates the required TSIG key for authenticating DNS messages to and from appliances running DNS One 2.x code.

**Note**: On the appliance you configure as a secondary server for a zone, you must associate a TSIG key for each primary server to which the secondary server requests zone transfers. On the appliance you configure as a primary server for a zone, you can set a TSIG key at the grid, member, or zone level. Because the secondary server requests zone transfers, it must send a specific key in its requests to the primary server. Because the primary server responds to the requests, it can have a set of TSIG keys from which it can draw when responding. As long as the primary server can find the same TSIG key that the secondary sends it, it can verify the authenticity of the requests it receives and authenticate the responses it sends. Use NTP to synchronize the time on both name servers that use TSIG-authenticated zone transfers.
Using Name Server Groups

A name server group is a collection of one primary DNS server and one or more secondary DNS servers. Grouping a commonly used set of primary and secondary DNS servers together simplifies zone creation by enabling you to specify a single name server group instead of specifying multiple name servers individually. After you create a name server group, you can then assign it to serve authoritative forward-mapping and reverse-mapping zones.

**Note:** Only superusers can create and manage name server groups.

### Adding Name Server Groups

To add a name server group:

1. From the Data Management -> DNS tab, do one of the following:
   - Click the Name Server Groups tab -> Add icon -> Group -> Name Server Group.
   - From the Toolbar, click the Add icon -> Group -> Name Server Group

2. In the Name Server Group wizard, do the following:
   - **Name:** Type a name that provides a meaningful reference for this set of servers.
   - **Name Servers:** Click the Add icon and select one of the following options for every server that you are adding to the NS group:
     - **Grid Primary:** Choose this option to select a grid member as the primary server for the zone. See Specifying a Grid Primary Server on page 412.
     - **Grid Secondary:** Choose this option to select a grid member as a secondary server for the zone. See Adding Grid Secondaries on page 415.
     - **Microsoft Primary:** Choose this option to select a Microsoft server as the primary server for the zone. See Specifying a Microsoft Primary Server on page 413.
     - **Microsoft Secondary:** Choose this option to select a Microsoft server as the primary server for the zone. See Specifying Microsoft Secondary Servers on page 415.
     - **External Primary:** Choose this option if the appliance is in a grid and you want to specify a primary server outside the grid (“external” to the grid). See Specifying an External Primary Server on page 413.
     - **External Secondary:** Choose this option if the appliance is in a grid and you want to specify a secondary server outside the grid (“external” to the grid), or if the appliance is deployed independently from a grid. See Specifying External Secondaries on page 416.
   - **Default NS Group:** Select this to specify this name server group as the default.
   - **Comment:** Optionally, enter additional information about the NS group.

3. Select one of the following:
   - **Next:** Define extensible attributes. For information, see Using Extensible Attributes on page 225.
   - **Save & Close:** Save the entry and close the editor.
   - **Save & Edit:** Save the entry and launch the Name Server Group Editor which provides more configuration options.
   - **Save & New:** Save the entry and create another NS Group.

A newly created name server group appears in the Name Server Groups tab. You can then associate it with forward-mapping and reverse-mapping zones.
Viewing Name Server Groups

You can view the configured name server groups by navigating to the Data Management tab -> DNS tab -> Name Server Groups tab.

The panel displays the following information about each name server group:

- **Name**: The name of the name server group.
- **Comment**: Comments that were entered for the name server group.
- **Site**: Values that were entered for this pre-defined attribute.

You can do the following:

- **Edit the properties of a name server group.**
  - Click the check box beside a name server group, and then click the Edit icon.
- **Delete a name server group.**
  - Click the check box beside a name server group, and then click the Delete icon.
- **Export the list of grid members to a .csv file.**
  - Click the Export icon.
- **Print the list of grid members.**
  - Click the Print icon.

Applying Name Server Groups

In Grid Manager, you can assign a name server group to a zone when you first create it using the Add Authoritative Zone wizard and when you edit an existing zone using the Authoritative Zone editor. For information on creating a zone using the wizard, see Configuring Authoritative Zones on page 404. The panels used to assign a name server group to a zone are the same in the wizard or and editor. The only difference is the way you access it. The following procedure describes how to specify a name server group when editing a forward-mapping zone:

1. From the Data Management tab -> DNS tab -> Zones tab -> zone check box, and then click the Edit icon.
2. In the Authoritative Zone editor, click Name Servers.
3. Select **Use this name server group**, and then select the name server group from the drop-down list.

**Note:** If you apply a name server group to at least one zone or specify it as the default group, you cannot rename or remove it. To rename or remove a group, you must first disassociate it from all zones and unassign it as the default group.
Importing Zone Data

Importing zone information alleviates having to manually enter data through the Infoblox GUI. You can import data from existing name servers, as well as from NIOS appliances running version 3.1r4 or later. You can import existing zone data when you create a new zone and when you edit an existing zone. You can import one zone (and its subzones) at a time.

For the remainder of this section, the name server that stores the existing zone data (which is imported) is referred to as the source name server (regardless of whether it is a third-party server or another NIOS appliance). The appliance that receives the zone data is referred to as the destination appliance. The following illustration shows the import zone data process.

Figure 15.3 Importing Zone Data Process

1. Use the management system to allow zone transfers on the source DNS server to the NIOS appliance IP address (10.1.1.5)
2. Log in to the appliance and specify the IP address of the source DNS server when you create or modify a zone.
3. The appliance sends a request to import the specified zone data from the source DNS server at 10.1.1.15.
4. The source DNS server sends the specified zone(s) data listed in the zone file to the appliance.
The appliance imports zone data through a zone transfer. Therefore, the source name server must be authoritative for the zone data being imported. You must also configure the source name server to allow zone transfers to the destination appliance. On the source name server, you might need to modify the `allow-transfer` substatement to include the IP address of the destination appliance prior to importing the data. If you are importing zone data to an HA pair, use the VIP (virtual IP) address shared by the HA pair. For a single independent appliance, use the LAN IP address. If you are importing zone data to a grid, always use the IP address of the grid master.

If the source name server is an Infoblox appliance, you can configure it to allow zone transfers as described in “Enabling Zone Transfers” on page 491. Note that a NIOS appliance, acting as the primary name server for a zone, by default allows zone transfers to its secondary name servers.

### About Importing Data into a New Zone

When the appliance imports data to a newly created zone, it imports the existing A, CNAME, DNAME, SRV, TXT, MX, PTR, host, and bulk host records, but creates NS (and A records matching that NS record) and SOA records appropriate for the destination server. The NS and SOA records are auto-created when a destination appliance is specified as the primary or secondary name server for the new zone. If the imported zone has extra NS records, they are rewritten to specify the source server as an external secondary. Delegation is also added for any subzones. The subzone records are not imported.

### About Importing Data into an Existing Zone

When you import zone data into an existing zone, the zone retains the NS and SOA records automatically created when the zone was originally created and replaces all other records—A, PTR, MX, TXT, SRV, CNAME, DNAME, host, and bulk host. The local appliance also retains subzones and records in the subzones that exist locally. If there are no duplicates, the destination appliance records are retained. If the imported zone has extra NS records, those records change to designate the source server as an external secondary.

### Importing Data into Zones

In Grid Manager, you can import zone data when you create the zone using the Add Authoritative Zone wizard and when you edit an existing zone. For information on how to add a new zone through the wizard, see Configuring Authoritative Zones on page 404. The last step of the wizard provides the option to import zone data. The following procedure describes how to import data into an existing zone.

To import data into an existing zone:

1. From the Data Management tab, select the DNS tab -> Zones tab -> zone check box, and then click Import Zone in the Toolbar.

2. In the Import Zone dialog box, specify the following:
   - The IP address of the name server from which you want to import data.
   - Optionally, click the Automatically create Infoblox host records from A records check box.

3. Click Import.

   When the local server successfully imports the zone data, a Confirmation message appears. If the local server cannot import the zone data, an Error message appears, recommending that you verify the correctness of the IP address of the remote server and zone information.
Configuring Authoritative Zone Properties

A zone inherits some of its properties from the grid or from the member that serves it as a primary or secondary server. When you edit a zone, you can override properties set at the grid or member level and modify the original zone settings, as well.

To configure authoritative zone properties:

1. From the Data Management tab, select the DNS tab → Zones tab → zone check box, and then click the Edit icon.
2. In the Authoritative Zone editor, you can do the following in each tab:
   - **General**: Modify the original zone settings, except the zone name.
   - **Name Servers**: Specify primary and secondary servers as described in Assigning Zone Authority to Name Servers on page 411.
   - **Settings**: Set certain properties if the primary server is a grid member. If the zone’s primary server is an external server, then all these fields, except Don't use forwarders to resolve queries in subzones, are read-only with the information derived from the SOA record of the zone.
     - The Serial Number field displays the zone's current serial number. You can change the serial number in an SOA record only if the primary server of the zone is a grid member.
     - The serial number in the SOA record increments every time the record is modified. This serial number plays a key role when and how zone data is updated via zone transfers. The NIOS appliance allows you to change the serial number (in the SOA record) for the primary server so it is higher than the secondary server, thereby ensuring zone transfers come from the primary server (as they should).
     - Override the grid or member TTL settings as described in About Time To Live Settings on page 480.
     - Override the email settings, as described in Adding an Email Address to the SOA Record on page 481.
     - Change the primary name server that is specified in the SOA MNAME of a zone, as described in Changing the SOA Name for a Zone on page 412.
     - Select Don't use forwarders to resolve queries in subzones. You can disable forwarding for a zone so the NIOS appliance does not forward a query to another name server, for data (it does not have) that is requested in the query.
   - **Queries**: Set restrictions for queries as described in Controlling DNS Queries on page 486.
   - **Zone Transfers**: Specify to which servers zone transfers are allowed as described in Enabling Zone Transfers on page 491.
   - **Updates**: Set dynamic DNS update properties as described in Configuring DNS Servers for DDNS on page 515.
   - **Active Directory**: Set parameters to allow zones to receive GSS-TSIG authenticated DDNS updates from DHCP clients and servers in an AD domain. For information, see Supporting Active Directory on page 518.
   - **Extensible Attributes**: Define extensible attributes. For information, see Using Extensible Attributes on page 225.
   - **Permissions**: Define administrative permissions. For information, see About Administrative Permissions on page 87.

3. Click Toggle Advanced Mode if the editor is in basic mode. When the additional tabs appear, you can do the following in each tab:
   - **General**: Click the Advanced subtab and view the networks associated with the zone. This tab is visible only if the primary server is a grid member, a Microsoft server, or unassigned.
     - If a zone is associated with one or more networks, the IP addresses of its host, A and AAAA records must belong to the associated networks. You cannot change the network associations in this editor. Navigate to the DHCP Network editor of the network, to change the zone associations. For information, see Associating Networks with Zones on page 598.
   - **Host Naming**: Set restrictions for host names. For information, see Specifying Hostname Policies on page 499.
— **Shared Record Groups**: Add shared record groups to a zone. For information, see *About Shared Record Groups* on page 472.

— **DNSSEC**: Configure DNSSEC properties. For information, see *Chapter 19, DNSSEC*, on page 543.

4. Select one of the following:
   — **Save & Close**: Save the entry and close the editor.
   — **Save**: Save the entry and continue editing.
   or
   — Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 25.
### Removing Zones

When you remove a zone, the NIOS appliance moves the zone to the Recycle Bin, along with all resource records in the zone. If a zone has subzones, you can choose to remove them and their resource records or “reparent” them to the parent zone of the one you are removing. These two options are shown in Figure 15.4.

**Figure 15.4 Removing or Reparenting Subzones**

- **Removing subzones**
  - Remove subzones **eng.corp100.com** and **ftp.eng.corp100.com**.
  - When you remove subzones in **corp100.com**, the NIOS appliance removes subzones **eng.corp100.com** and **ftp.eng.corp100.com**, and all their resource records.

- **Reparenting subzones**
  - Reparent subzones **eng.corp100.com** and **ftp.eng.corp100.com** to **corp100.com**.
  - When you remove subzone **eng.corp100.com**, the NIOS appliance removes the zone and its resource records. It then reparents subzone **ftp.eng.corp100.com** to **corp100.com**. It creates a new NS record in **corp100.com** for subzone **ftp.eng.corp100.com** and possibly changes admin privileges for **ftp.eng.corp100.com**.

If you choose to reparent the subzones, be aware of the following caveats and possible effects of the reparenting:

- You cannot remove a zone and reparent its subzones if at least one of the subzones is a delegated zone. You must first remove any delegated subzones, and then you can remove the zone and reparent its subzones.
- If there are AD (Active Directory) subzones (\_msdcs, \_sites, \_tcp, \_udp, domainndszones, forestdnszones) and you opt to remove the parent zone only, the NIOS appliance reparents all subzones except the AD subzones, which it removes regardless of the removal option you specify.
- The subzone reparenting option is unavailable when you select multiple zones for removal.
- When you remove a zone and reparent its subzones, any subzone that inherited its admin access settings from its previous parent zone (as opposed to having specific access settings for the subzone) now receive their settings from its new parent zone, which might be different. See Figure 15.5.
To remove a zone:
1. From the Data Management tab, select the DNS tab → Zones tab.
2. Click the check box of the zones you want to delete.
3. Click the Delete icon.
4. In the Delete Confirmation dialog box, enter the following:
   - **Remove zone only**: Select to remove the zone and its resource records. The Infoblox appliance reparents all subzones to the parent zone of the zone that you remove. Automatically created AD (Active Directory) subzones are an exception. Even if you select **Remove zone only**, the Infoblox appliance still removes AD subzones.
   - **Remove all subzones**: Select to remove the selected zone, all its subzones, and all the resource records of the selected zone and its subzones.
5. Click **Yes**.

*Note:* Instead of removing a zone, you can also disable it. For more information, refer to *Enabling and Disabling Zones* on page 409.

Before you remove eng.corp100.com, subzone ftp.eng.corp100.com inherits a “Deny” admin access setting from eng.corp100.com. After the removal, subzone ftp.eng.corp100.com inherits “Read/Write” access from its new parent zone, corp100.com.

Note that if you set a specific “Deny” admin access privilege for subzone ftp.eng.corp100.com before removing its parent zone (eng.corp100.com), ftp.eng.corp100.com retains its specified “Deny” setting.

If you remove eng.corp100.com and … … the admin access settings for subzone ftp.eng.corp100.com change because the privileges for its new parent zone (corp100.com) are different from those of its previous parent zone (eng.corp100.com).
RESTORING ZONE DATA

After you import or delete a zone, if you want the original zone back, you can restore it using the Recycle Bin. When you import a zone for the first time, the appliance saves the zone and its resource records as a single object in the Recycle Bin. It keeps the subzones with the zone. See Restoring Zone Data After a Zone Import Example on page 425.

When you reimport data into a zone, the software saves the zones, its resource records, and the delegated subzones created by the previous import operation in the Recycle Bin. It keeps the subzones (not created during the zone import) with the zone. See Restoring Zone Data After a Zone Reimport Example on page 426.

If the zone import succeeds, the system adds resource records from the source to the target zone. It also adds delegated subzones for the source subzones. If the zone import fails, the system does not create records and delegated subzones. In either case, you can retrieve the original zone and its subzones from the Recycle Bin as follows:

1. Delete the zone using the steps described in the section Removing Zones on page 423.
2. Select Remove zone only to remove the zone and its resource records. The NIOS appliance reparents all subzones to the parent zone of the zone that you remove. Do not select Remove all subzones.
   Automatically created AD (Active Directory) subzones are an exception. Even if you select Remove zone only, the NIOS appliance still removes AD subzones.
3. In the Finder panel, click Recycle Bin.
4. Select the zone you want to restore and click the Restore icon.
   The zone is restored back to its original state. The resource records are reparented back under it.

Restoring Zone Data After a Zone Import Example

In the example shown in Figure 15.6:

1. import data from a source zone with subzones Sub x and Sub y into zone B with subzones Sub B1 and Sub B2.
   The appliance stores zone B and its resource records in the Recycle Bin.
   To retrieve zone B after the import:
2. Delete subzone B using the Remove zone only option.
   The appliance reparents subzones Sub B1 and Sub B2 to the Zone A, which is the zone above Zone B.
3. After the import, you can restore zone B from the Recycle Bin. The appliance reparents the subzones Sub B1 and Sub B2 back to zone B.

Figure 15.6 Restoring Zones After a Zone Import
Restoring Zone Data After a Zone Reimport Example

In the example shown in Figure 15.7:

1. You reimport data from the source zone with subzones Sub x and Sub y into zone B with subzones Sub B1 and Sub B2.
   
   To retrieve zone B after the import:

2. Delete the delegated subzones x and y and then remove subzone B using the **Remove zone only** option.
   
   The appliance stores zone B and its resource records and the previously-imported subzones Sub x and Sub y (as delegated subzones) in the Recycle Bin. It reparents subzones Sub B1 and Sub B2 to the zone above zone B (Zone A).

3. After the import, you can restore zone B and the subzones Sub x and Sub y from the Recycle Bin. The appliance reparents the subzones Sub B1 and Sub B2 back to zone B.

*Figure 15.7  Restoring Zones After a Zone Reimport*
Configuring Delegated, Forward, and Stub Zones

In addition to authoritative zones, the NIOS appliance allows you to configure delegated, forward, and stub zones. A delegated zone is a zone managed by (delegated to) another name server who owns the authority for the zone. A forward zone is where queries are sent before being forwarded to other remote name servers. A stub zone contains records that identify the authoritative name servers in another zone. This section covers the following topics:

- Configuring a Delegation
- Configuring a Forward Zone on page 428
- Configuring Stub Zones on page 432

Configuring a Delegation

Instead of a local name server, remote name servers (which the local server knows) maintain delegated zone data. When the local name server receives a query for a delegated zone, it either responds with the NS record for the delegated zone server (if recursion is disabled on the local server) or it queries the delegated zone server on behalf of the resolver (if recursion is enabled).

For example, there is a remote office with its own name servers, and you want it to manage its own local data. On the name server at the main corporate office, define the remote office zone as delegated, and then specify the remote office name servers as authorities for the zone. You can delegate a zone to one or more remote name servers, which are typically the authoritative primary and secondary servers for the zone. If recursion is enabled on the local name server, it queries multiple delegated name servers based on their round-trip times.

You can also configure TTL settings of auto-generated NS records and glue A and AAAA records for delegated zones in forward-mapping, IPv4 reverse-mapping, and IPv6 reverse-mapping zones. For information, see About Time To Live Settings on page 480.

The delegation must exist within an authoritative zone with a grid primary server. To create a delegation:

1. From the Data Management tab, select the DNS tab ‒ Zones tab.
2. Click the parent zone to open it.
   - Grid Manager displays the Records and Subzones tabs of the zone.
3. Click the Add icon → Zone → Add Delegation.
4. In the Add Delegation wizard, specify the following:
   - Name: This field displays a dot followed by the domain name of the current zone. Enter one or more labels before the dot to specify the domain name of the subzone.
   - DNS View: This field displays only when there is more than one DNS view in the network view. Displays the DNS view of the current zone.
   - Comment: Optionally, enter additional text about the zone.
   - Disable: Click this check box to temporarily disable this zone. For information, see Enabling and Disabling Zones on page 409
   - Lock: Click this check box to lock the zone so that you can make changes to it, and also prevent others from making conflicting changes. For information, see Locking and Unlocking Zones on page 409.
5. Click Next to define the name servers for the zone.
6. In the Name Servers panel, click the Add icon and specify the following information:
   - Name: Enter the name of a remote name server to which you want the local server to redirect queries for data for the zone. This is a name server that is authoritative for the delegated zone.
   - Address: Enter the IP address of the delegated server.
7. Select one of the following:
   — **Next**: Define extensible attributes as described in *Using Extensible Attributes* on page 225.
   — **Save & Close**: Save the entry and close the editor.
   — **Save & Edit**: Save the entry and launch the *Delegation Zone* editor which provides more configuration options.
   — **Save & New**: Save the entry and create another zone.
   or
   — Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 25.

### Configuring a Forward Zone

When you want to forward queries for data in a particular zone, define the zone as a forward zone and specify one or more name servers that can resolve queries for the zone. For example, define a forward zone so that the NIOS appliance forwards queries about a partner’s internal site to a name server, which the partner hosts, configured just for other partners to access.

**Note:** The use of a forward zone is different from that of a forwarder. (A forwarder is a name server that performs recursive lookups on behalf of the name servers that forward queries to it. For more information, see *Using Forwarders* on page 485.) A NIOS appliance forwards queries to the name server of a forward zone because the name server can resolve queries for the zone. A NIOS appliance forwards queries to a forwarder regardless of zones.

Note that a name server can have only one definition for a zone in any given DNS view; a forward zone cannot be configured on a member that already has a zone with the same domain name configured on it in the same DNS view.

To configure a forward forward-mapping zone:

1. From the *Data Management* tab, select the *DNS* tab, expand the Toolbar and click *Add -> Zone -> Add Forward Zone*.
2. In the *Add Forward Zone* wizard, click *Add a forward forward-mapping zone* and click **Next**.
3. Enter the following information, and then click **Next**:
   — **Name**: Enter the domain name of the zone for which you want the NIOS appliance to forward queries.
   — **DNS View**: This field displays only when there is more than one DNS view in the current network view. Select the DNS view of the forward zone.
   — **Comment**: Enter a descriptive comment.
   — **Disable**: Click this check box to temporarily disable this zone.
   — **Lock**: Click this check box to lock the zone so that you can make changes to it and prevent others from making conflicting changes.
4. In the *Forwarders* panel, click the Add icon and specify the servers to which the NIOS appliance forwards queries for the zone:
   — **Name**: Enter a domain name for the server to which you want the NIOS appliance to forward queries for the specified domain name.
   — **Address**: Enter the IP address of the server to which you want the NIOS appliance to forward queries.
   — Select **Use Forwarders Only** if you want the NIOS appliance to query forwarders only to resolve domain names in the zone.
5. Select one of the following:
   — **Next**: Continue to the next step where you select the appliance on which the forward zone is configured.
   — **Save & Close**: Save the entry and close the wizard.
   — **Save & Edit**: Save the entry and launch the *Forward Zone* editor.
   — **Save & New**: Save the entry and create another forward zone.
6. If you clicked **Next**, in the Name Servers section, click the Add icon, and then select the NIOS appliance on which the forward zone is configured. For an independent deployment, select the local appliance (it is the only choice). For a grid, you can select one or more grid members.

7. Select one of the following:
   - **Next**: Continue to the next step where you define extensible attributes as described in *Using Extensible Attributes* on page 225, and then optionally proceed to the next step where you define admin permissions as defined in *About Administrative Permissions* on page 87.
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and launch the Forward Zone editor which provides more configuration options.
   - **Save & New**: Save the entry and create another forward zone.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 25.

8. Click **Restart** to apply the configuration.

To configure a forward IPv4 reverse-mapping zone:

1. From the **Data Management** tab, select the **Zones** tab, expand the Toolbar and click **Add -> Zone -> Add Forward Zone**.

2. In the **Add Forward Zone** wizard, click **Add a forward IPv4 reverse-mapping zone** and click **Next**.

3. Enter the following information, and then click **Next**:
   - **IPv4 Network**: Enter the IPv4 address for the address space for which you want to define the reverse-mapping zone and select a netmask from the *Netmask* drop-down list. Alternatively, you can specify the address in CIDR format, such as 192/8. To use an RFC 2317 prefix, select a netmask value that is between 25 to 31, inclusive. Grid Manager displays the *RFC 2317 Prefix* field. Enter a prefix in the text field. Prefixes can be alphanumeric characters, without blank spaces. For information, see *Specifying an RFC 2317 Prefix* on page 406.
   or
   - **Name**: Enter the domain name of the reverse-mapping zone.
   - **DNS View**: This field displays only when there is more than one DNS view in the network view. Select a DNS view from the drop-down list.
   - **Comment**: Optionally, enter additional information about the zone.
   - **Disable**: Click this check box to temporarily disable this zone.
   - **Lock**: Click this check box to lock the zone so that you can make changes to it, and also prevent others from making conflicting changes.

4. In the **Forwarders** panel, do the following:
   - Click the Add icon and specify the servers to which the NIOS appliance forwards queries for the specified zone:
     - **Address**: Enter the IP address of the server to which you want the NIOS appliance to forward queries.
     - **Name**: Enter a domain name for the server to which you want the NIOS appliance to forward queries for the specified domain name.
   - **Select Use Forwarders Only** if you want the NIOS appliance to query forwarders only to resolve domain names in the zone.

5. Select one of the following:
   - **Next**: Continue to the next step where you select the NIOS appliance from which you want to forward queries.
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and launch the *Forward Zone* editor which provides more configuration options.
   - **Save & New**: Save the entry and create a new forward zone.
Configuring DNS Zones

6. If you clicked Next, in the Name Servers section, click the Add icon, select the NIOS appliance from which you want to forward queries. For an independent deployment, select the local appliance (it is the only choice). For a grid, you can select one or more grid members.

7. Select one of the following:
   — Next: Continue to the next step where you define extensible attributes as described in Using Extensible Attributes on page 225.
   — Save & Close: Save the entry and close the wizard.
   — Save & Edit: Save the entry and launch the Forward Zone editor which provides more configuration options.
   — Save & New: Save the entry and create a new forward zone.
   or
   — Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 25.

8. Click Restart to apply the configuration.

To configure a forward IPv6 reverse-mapping zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Zone -> Add Forward Zone.

2. In the Add Forward Zone wizard, click Add a forward IPv6 reverse-mapping zone and click Next.

3. Enter the following zone information:
   — IPv6 Network Address: Enter the 128-bit IPv6 address for the address space for which you want to define the reverse-mapping zone. When you enter an IPv6 address, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2006:0000:0000::0123:4567:89ab:0000:cdef can be shortened to 2006::123:4567:89ab:0:cdef. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The NIOS appliance displays an IPv6 address in its shortened form, regardless of its form when it was entered. Choose the network prefix that defines the IPv6 network address space.
   or
   — Name: Enter the domain name of the reverse-mapping zone.
   — DNS View: This field displays only when there is more than one DNS view in the network view. Select a DNS view from the drop-down list.
   — Comment: Enter a descriptive comment about the zone.
   — Disable: Click this check box to temporarily disable this zone.
   — Lock: Click this check box to lock the zone so that you can make changes to it, and also prevent others making conflicting changes.

4. In the Forwarders panel, do the following:
   — Click the Add icon and specify the servers to which the NIOS appliance forwards queries for the specified zone:
     — Address: Enter the IP address of the server to which you want the NIOS appliance to forward queries.
     — Name: Enter a domain name for the server to which you want the NIOS appliance to forward queries for the specified domain name.
   — Select Use Forwarders Only if you want the NIOS appliance to query forwarders only to resolve domain names in the zone.

5. Select one of the following:
   — Next: Continue to the next step where you select the NIOS appliances from which you want to forward queries.
   — Save & Close: Save the entry and close the wizard.
   — Save & Edit: Save the entry and launch the Forward Zone editor which provides more configuration options
   — Save & New: Save the entry and create a new forward zone.
6. If you clicked **Next**, in the Name Servers section, click the Add icon, select the NIOS appliances from which you want to forward queries. For an independent deployment, select the local appliance (it is the only choice). For a grid, you can select one or more grid members.

7. Select one of the following:
   - **Next**: Continue to the next step where you define extensible attributes as described in *Using Extensible Attributes* on page 225.
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and launch the *Forward Zone* editor which provides more configuration options.
   - **Save & New**: Save the entry and create a new forward zone.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 25.

8. Click **Restart** to apply the configuration.
Configuring Stub Zones

A stub zone contains records that identify the authoritative name servers in the zone. It does not contain resource records for resolving IP addresses to hosts in the zone. Instead, it contains the following records:

- SOA (Start of Authority) record of the zone
- NS (name server) records at the apex of the stub zone
- A (Address) records that map the name servers to their IP addresses

Stub zones, like secondary zones, obtain their records from other name servers. Their records are read only; therefore, administrators do not manually add, remove, or modify the records.

Stub zone records are also periodically refreshed, just like secondary zone records. However, secondary name servers contain a complete copy of the zone data on the primary server. Therefore, zone transfers from a primary server to a secondary server, or between secondary servers, can increase CPU usage and consume excessive bandwidth. A name server hosting a stub zone maintains a much smaller set of records; therefore, updates are less CPU intensive and consume less bandwidth.

When a name server hosting a stub zone receives a query for a domain name that it determines is in the stub zone, the name server uses the records in the stub zone to locate the correct name server to query, eliminating the need to query the root server.

*Figure 15.8* and *Figure 15.9* illustrate how the NIOS appliance resolves a query for a domain name for which it is not authoritative. *Figure 15.8* illustrates how the appliance resolves a query when it does not have a stub zone. *Figure 15.9* illustrates how the appliance resolves the query with a stub zone.

In *Figure 15.8*, a client sends a query for ftp.sales.corp200.com to the NIOS appliance. When the appliance receives the request from the client, it checks if it has the data to resolve the query. If the appliance does not have the data, it tries to locate the authoritative name server for the requested domain name. It sends nonrecursive queries to a root name server and to the closest known name servers until it learns the correct authoritative name server to query.

*Figure 15.8 Processing a Query without a Stub Zone*
In Figure 15.9, when the NIOS appliance receives the request for the domain name in corp200.com, it determines it does not have the resource records to resolve the query. It does, however, have a list of the authoritative name servers in the stub zone, corp200.com. The appliance then sends a query directly to the name server in corp200.com.

**Figure 15.9 Processing a Query with a Stub Zone**

2. The appliance has a corp200.com stub zone.
3. The appliance sends a query directly to a corp200.com server...
   ... which responds with a referral to the sales.corp200.com servers.
4. The appliance sends a query to a sales.corp200.com server.
   The sales.corp200.com server checks its resource records and responds with the requested data.
5. The appliance responds to the client with the requested data.
Configuring DNS Zones

Stub zones facilitate name resolution and alleviate name server traffic in your network. For example, the client in the previous examples is in corp100.com. The corp100.com and corp200.com zones are partners, and send all their communications through a VPN tunnel, as shown in Figure 15.10 on page 434. The firewall protecting corp100.com is configured to send all messages for the 10.2.2.0/24 network through the VPN tunnel. Infoblox_A hosts the stub zone for corp200.com. Therefore, when the host in corp100.com sends a query for ftp.sales.corp200.com, Infoblox_A obtains the IP address of Infoblox_B (10.2.2.7) from its stub zone records and sends the query to the firewall protecting corp100.com.

Because the destination of the query is in the 10.2.2.0/24 network, the firewall (configured to encrypt all traffic to the network) sends the request through a VPN tunnel to Infoblox_B. Infoblox_B resolves the query and sends back the response through the VPN tunnel. All name server traffic went through the VPN tunnel to the internal servers, bypassing the root servers and external name servers.

Figure 15.10  Stub Zone Configuration

In parent-child zone configurations, using stub zones also eases the administration of name servers in both zones. For example, as shown in Figure 15.10, sales.corp200.com is a child zone of corp200.com. On the corp200.com name servers, you can create either a delegated zone or a stub zone for sales.corp200.com.

When you create a delegated zone, you must first specify the name servers in the delegated zone and manually maintain information about these name servers. For example, if the administrator in sales.corp200.com changes the IP address of a name server or adds a new name server, the sales.corp100.com administrator must inform the corp200.com administrator to make the corresponding changes in the delegated zone records.

If, instead, you create a stub zone for sales.corp200.com, you set up the stub zone records once, and updates are then done automatically. The name servers in corp200.com that are hosting a stub zone for sales.corp200.com automatically obtain updates of the authoritative name servers in the child zone.

In addition, a name server that hosts a stub zone can cache the responses it receives. Therefore, when it receives a request for the same resource record, it can respond without querying another name server.

Creating Stub Zones

When you create a stub zone on the NIOS appliance, you specify the following:

- The grid member that is hosting the stub zone
  You can specify multiple appliances if you want the stub zones on multiple name servers. If you do, the appliances store identical records about the stub zone.
- The IP address of the primary server(s) that the NIOS appliance can query in the stub zone
  The primary server can be a grid member or an external primary server. If you specify multiple primary servers, the appliance queries the primary servers, starting with the first server on the list.

The primary server and the name server hosting the stub zone can belong to the same grid, as long as the authoritative zone and the stub zone are in different DNS views. You cannot configure one zone as both authoritative and stub in the same view.
After you create a stub zone, the NIOS appliance does the following:

1. It sends a query to the primary server for the SOA (Start of Authority) record of the stub zone.
   The primary server returns the SOA record.
2. Then, it sends a query for the NS (name server) records in the zone.
   The primary server returns the NS records and the A (address) records of the name servers. (These A records are also called glue records.)
   If the primary server is a NIOS appliance, you might have to manually create the A record and add it to the stub zone. A NIOS appliance that is the primary server for a zone always creates an NS record, but does not always create an A record.
   - The appliance automatically creates an A record when its host name belongs to the name space of the zone. For example, if the zone is corp100.com and the primary server host name is server1.corp100.com, the appliance automatically creates the NS and A records and sends these records when it is queried by the stub zone name server.
   - The appliance does not automatically create an A record when its host name is in a name space that is different from the zone. For example, if the zone is corp200.com and the primary server host name is server1.corp100.com, then the appliance creates the NS record only and sends it when it is queried by the stub zone name server. In this case, you must manually create the A record.

Maintaining Stub Zones

The NIOS appliance maintains the stub zone records and updates them based on the values in the SOA record as follows:

- The refresh interval indicates when the appliance sends a discrete query to the primary name server for the stub zone. The appliance learns about any changes in the stub zone and updates the NS and A records in the stub zone accordingly.
- If the update fails, the retry interval indicates when the appliance resends a discrete query.
- If the query continues to fail, the expiry value indicates when the appliance stops using the zone data.

Adding Stub Zones

To add a stub zone, you must identify the Infoblox appliance that hosts the stub zone, and provide the IP address of the primary server.

You can also add stub zones for Microsoft servers that are managed by grid members. For information, see Managing Microsoft Windows Servers on page 727.

You can configure a stub zone for forward mapping or reverse mapping zones.

To add a forward-mapping stub zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Zone -> Add Stub Zone.
2. In the Add Stub Zone wizard, click Add a stub forward-mapping zone and click Next.
3. Specify the following, and then click Next:
   - Name: Enter the name for the stub zone.
   - Comment: Enter a useful comment, such as the admin to contact for the stub zone.
   - Disable: Click this check box to temporarily disable this zone.
   - Lock: Click this check box to lock the zone so that you can make changes to it, and also prevent others from making conflicting changes.
4. In the Master Name Servers panel, click the Add icon and enter the Name and IP Address of the primary server in the stub zone, and then click Next.
   If the primary server is a grid member, you must enter the host name and IP address of the grid member. The NIOS appliance does not validate these entries. Therefore, if you change the IP address of a grid member listed here, you must update the grid member information in this list as well.
You can specify multiple primary servers for redundancy. If the primary server is a NIOS appliance, the appliance must have the Minimal Response feature disabled so it can propagate the data to the stub server. For information about the Minimal Response feature, see *Specifying Minimal Responses* on page 483.

— Optionally, click the **Don't use forwarders to resolve queries in subzones** check box to indicate that the name servers hosting the stub zone must not use forwarders to resolve queries for domain names in the stub zone or in its subzones.

5. In the **Name Servers** panel, click the Add icon and select one of the following:
   — **Add Infoblox Member**: Select this and select the grid member that hosts the stub zone.
   — **Add Microsoft Server**: Select this and select the Microsoft server that hosts the stub zone.

6. Select one of the following:
   — **Next**: Continue to the next step where you define extensible attributes as described in *Using Extensible Attributes* on page 225.
   — **Save & Close**: Save the entry and close the wizard.
   — **Save & Edit**: Save the entry and launch the **Stub Zone** editor which provides more configuration options.
   — **Save & New**: Save the entry and create a new stub zone.
   or
   — Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 25.

You can define two types of reverse-mapping stub zones, one for IPv4 addresses and one for IPv6 addresses.

To configure an IPv4 reverse-mapping stub zone:

1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Add -> Zone -> Add Stub Zone**.
2. In the **Add Stub Zone** wizard, click **Add a stub IPv4 reverse-mapping zone** and click **Next**.
3. Specify the following:
   — **IPv4 Network**: Enter the IPv4 address for the address space for which you want to define the reverse-mapping zone and select a netmask from the **Netmask** drop-down list. Alternatively, you can specify the address in CIDR format, such as 192/8.
     
     To use an RFC 2317 prefix, select a netmask value that is between 25 to 31, inclusive. Grid Manager displays the **RFC 2317 Prefix** field. Enter a prefix in the text field. Prefixes can be alphanumeric characters, without blank spaces. For information, see *Specifying an RFC 2317 Prefix* on page 406.
     
     or
   — **Name**: Enter the domain name of the reverse-mapping zone.
   — **DNS View**: This field displays only when there is more than one DNS view in the network view. Select a DNS view from the drop-down list.
   — **Comment**: Optionally, enter additional information about the zone.
   — **Disable**: Click this check box to temporarily disable this zone.
   — **Lock**: Click this check box to lock the zone so that you can make changes to it, and also prevent others from making conflicting changes.

4. In the **Master Name Servers** panel, click the Add icon and enter the **Name** and **IP Address** of the primary server in the stub zone, and then click **Next**.

If the primary server is a grid member, you must enter the host name and IP address of the grid member. The NIOS appliance does not validate these entries. Therefore, if you change the IP address of a grid member listed here, you must update the grid member information in this list as well.

You can specify multiple primary servers for redundancy. If the primary server is a NIOS appliance, the appliance must have the Minimal Response feature disabled so it can propagate the data to the stub server. For information about the Minimal Response feature, see *Specifying Minimal Responses* on page 483.

— Optionally, click the **Don't use forwarders to resolve queries in subzones** check box to indicate that the name servers hosting the stub zone should not forward queries that end with the domain name of the stub zone to any configured forwarders.
Configuring Delegated, Forward, and Stub Zones

5. In the **Name Servers** panel, click the Add icon and select one of the following:
   - **Add Infoblox Member**: Select this and select the grid member that hosts the stub zone.
   - **Add Microsoft Server**: Select this and select the Microsoft server that hosts the stub zone.

6. Select one of the following:
   - **Next**: Continue to the next step where you define extensible attributes as described in *Using Extensible Attributes* on page 225.
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and launch the **Stub Zone** editor which provides more configuration options.
   - **Save & New**: Save the entry and create a new stub zone.
   - Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 25.

To configure an IPv6 reverse-mapping stub zone:

1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Add -> Zone -> Add Stub Zone**.

2. In the **Add Stub Zone** wizard, click **Add a stub IPv6 reverse-mapping zone** and click **Next**.

3. Specify the following:
   - **IPv6 Network Prefix** and **Prefix Length**: Enter the 128-bit IPv6 address for the address space for which you want to define the reverse-mapping zone. When you enter an IPv6 address, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2006:0000:0000:0123:4567:89ab:0000:cdef can be shortened to 2006::123:4567:89ab:0:cdef. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The NIOS appliance displays an IPv6 address in its shortened form, regardless of its form when it was entered. You can enter a slash and prefix length in the **IPv6 Network Prefix** field or you can choose a value from the **Prefix Length** drop-down list.
   - **Name**: Enter the domain name of the reverse-mapping zone.
   - **DNS View**: This field displays only when there is more than one DNS view in the current network view. Select a DNS view from the drop-down list.
   - **Comment**: Enter a descriptive comment about the zone.
   - **Disable**: Click this check box to temporarily disable this zone.
   - **Lock**: Click this check box to lock the zone so that you can make changes to it and prevent others from making conflicting changes.

4. In the **Master Name Servers** panel, click the Add icon and enter the **Name** and **IP Address** of the primary server in the stub zone, and then click **Next**.

   If the primary server is a grid member, you must enter the host name and IP address of the grid member. The NIOS appliance does not validate these entries. Therefore, if you change the IP address of a grid member listed here, you must update the grid member information in this list as well.

   You can specify multiple primary servers for redundancy. If the primary server is a NIOS appliance, the appliance must have the Minimal Response feature disabled so it can propagate the data to the stub server. For information about the Minimal Response feature, see *Specifying Minimal Responses* on page 483.

   Optionally, click the **Don't use forwarders to resolve queries in subzones** check box to indicate that the name servers hosting the stub zone should not forward queries that end with the domain name of the stub zone to any configured forwarders.

5. In the **Name Servers** panel, click the Add icon and select one of the following:
   - **Add Infoblox Member**: Select this and select the grid member that hosts the stub zone.
   - **Add Microsoft Server**: Select this and select the Microsoft server that hosts the stub zone.
6. Select one of the following:
   - **Next**: Continue to the next step where you define extensible attributes as described in *Using Extensible Attributes* on page 225.
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and launch the *Stub Zone* editor which provides more configuration options.
   - **Save & New**: Save the entry and create a new stub zone.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 25.

**Viewing SOA Records**

The timer values in the SOA record determine when the stub zone records are updated.

To view zone SOA record values:

1. From the **Data Management** tab, select the **DNS** tab -> **Zones** tab -> *zone* check box, and then click the Edit icon.
2. In the **Stub Zone** editor, click **Settings** to view the following:
   - **Serial number**—The number used by stub DNS servers to check if the zone has changed. If the serial number is higher than what the stub server currently has, a query is initiated. This number is automatically increased when changes are made to the zone or its records.
   - **Primary Name Server**—The domain name for the primary DNS server for the zone. The zone should contain a matching NS record.
   - **E-mail Address**—The e-mail address of the person responsible for maintaining the zone.
   - **Refresh**—The time lapse between checks the stub server makes for changes to the zone.
   - **Retry**—The time lapse after which the stub server checks for changes if the first refresh fails.
   - **Expire**—The time period the zone remains valid after repeated failures to refresh.
   - **Default TTL**: Specifies how long a name server can cache the record.
   - **Negative-caching TTL**: Specifies how long a name server caches negative responses from the name servers that are authoritative for the zone.
3. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and continue editing.

**Configuration Example: Configuring a Stub Zone in a Grid**

This example illustrates how to configure a stub zone and assign it to a grid member. You configure a grid, Corp100, with a single grid master and grid member. The grid member, member1.corp100.com, is the primary name server for the corp100.com zone in the internal view. The grid master, gm-corp100.com, hosts the stub zone for corp100.com in the external view. Thus, when the grid master receives a query for the corp100.com zone, it sends it directly to member1.corp100.com, the primary name server for the zone.

In this example, you configure the following:

1. Turn off minimal responses on member1.corp100.com, the primary name server for the corp100.com zone. See *Disable Minimal Responses*.
2. Create the internal and external views. See *Create the Views*.
3. Create the corp100.com authoritative zone and stub zone. See *Create the Zones*. 
Disable Minimal Responses

After you create the grid, turn off minimal responses for member1.corp100.com. Disabling minimal responses ensures that member1.corp100.com propagates the required data to the server hosting the stub zone.

1. From the Data Management tab, select the DNS tab, click Members -> member1.corp100.com check box -> Edit icon.
2. In the Member DNS Configuration editor, click the General -> Basic tab.
3. Clear the Return minimal responses check box.
4. Click Save & Close.

Create the Views

Create the internal and external views. To create each view:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add DNS View.
2. In the Add DNS View wizard, enter the name of the view. In this example, enter either External or Internal.
3. Click Save & New and create the other DNS view.

Create the Zones

Create the corp100.com zone in the internal view and assign member1.corp100.com as the grid primary server:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Zone -> Add Auth Zone.
2. In the Forward Authoritative Zone wizard, do the following:
   — Select Add an authoritative forward-mapping zone and click Next.
   — Enter the zone name, corp100.com and select the Internal DNS view. Click Next.
   — Select Use this set of name servers and select member1.corp100.com as the grid primary server.
3. Click Save & Close.

After you create the zone, you can view the NS and A records which were automatically created.

Create the stub zone, corp100.com, in the external view, assign gm-corp100.com as the stub member and member1.corp100.com as the stub primary server.

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Zone -> Add Stub Zone.
2. In the Stub Zone wizard, do the following:
   — Select Add a stub forward-mapping zone and click Next.
   — Enter the name of the stub zone, corp100.com and select the External DNS view. Click Next.
   — In the Master Name Servers panel, click the Add icon and enter the following for the primary name server, and then click Next:
     Name: member1.corp100.com
     Address: 10.35.0.222
   — In the Name Servers panel, click the Add icon and select gm-corp100.com.
3. Click Save & Close.

After you create the stub zone, the server hosting the stub zone, gm-corp100.com, sends queries to the primary server, member1.corp100.com, for the SOA and NS records. member1.corp100.com then returns its NS records and A (address) records.
**Viewing Zones**

To list zones, navigate to the Data Management tab → DNS tab → Zones panel. If there is more than one DNS view in the grid, this panel lists the DNS views. Select a DNS view to list its zones. (For information, see *Listing DNS Views* on page 400.)

- Click **Toggle flat view** to display a flat list of all the zones in the view.
- Click **Toggle hierarchical view** to display only the apex zones.

This panel displays the following information for each zone, by default:

- **Name:** The domain name of the zone.
- **MS Sync Master:** When a zone is served by multiple Microsoft servers, this column shows which Microsoft server is actually performing the synchronization of that zone with the grid.
- **Type:** The zone type. Possible values are Authoritative, Forward, Stub and Delegation.
- **Comment:** Comments that were entered for the zone.
- **Site:** Values that were entered for this pre-defined attribute.

You can also display the following columns:

- **Locked:** Displays Yes when a zone is locked by an admin, and displays No when the zone is unlocked.
- **Function:** Indicates whether the zone is a forward-mapping, or an IPv4 or IPv6 reverse-mapping zone.
- **Disabled:** This field displays Yes if the zone is disabled. Otherwise, this field displays No.
- **Signed:** This field displays Yes if the zone is a DNSSEC-signed zone. Otherwise, this field displays No.

You can do the following:

- List the resource records and subzones of a DNS zone.
  - Click a DNS zone name.
- Edit the properties of a DNS zone.
  - Click the check box beside a DNS zone, and then click the Edit icon.
- Delete a DNS zone.
  - Click the check box beside a DNS zone, and then click the Delete icon.
- Export the list of DNS zones to a .csv file.
  - Click the Export icon.
- Print the list of DNS zones.
  - Click the Print icon.
Chapter 16  DNS Resource Records

This chapter provides general information about Infoblox host records and DNS resource records. The topics in this chapter include:

- **About Host Records** on page 442
  - Assigning Multiple IP Addresses to a Host on page 443
  - Adding Host Records on page 444
  - Modifying Host Records on page 445
- **About Bulk Hosts** on page 446
  - Specifying Bulk Host Name Formats on page 446
  - Before Defining Bulk Host Name Formats on page 446
  - Adding Bulk Hosts on page 449
- **Managing Resource Records** on page 451
  - Managing A Records on page 452
  - Managing NS Records on page 453
  - Managing AAAA Records on page 454
  - Managing PTR Records on page 455
  - Managing MX Records on page 456
  - Managing SRV Records on page 457
  - Managing TXT Records on page 459
  - Managing CNAME Records on page 460
  - Managing DNAME Records on page 462
  - Managing NAPTR Records on page 469
  - Modifying, Disabling, and Deleting Host and Resource Records on page 471
- **About Shared Record Groups** on page 472
  - Shared Records Guidelines on page 473
  - Configuring Shared Record Groups on page 473
  - Managing Shared Resource Records on page 475
  - Configuration Example: Configuring Shared Records on page 478
### About Host Records

Host records provide a unique approach to the management of DNS, DHCP, and IPAM data. By using host records, you can manage multiple DNS records and DHCP and IPAM data collectively, as one object on the appliance.

When you create a host record, you are specifying the name-to-address and address-to-name mappings for the IP address that you assign to the host. The Infoblox DNS server then uses this data to respond to DNS queries for the host. When the server receives a name-to-address query for the host, it responds with an A record that contains the data from the host record. Likewise, when it receives an address-to-name query for the host, the appliance responds with a PTR record that contains data from the host record. Additionally, if you specify an alias in the host record, the appliance uses this data as a CNAME record to respond to queries with the alias. It maps the alias to the canonical name and sends back a response with the canonical name and IP address of the host. Thus, a single host record is equivalent to creating A, PTR, and CNAME resource records for an IP address.

In addition, if the Infoblox DHCP server manages the IP address assigned to the host, the server uses it as a fixed address record as well. The DHCP server assigns the IP address to the host when it receives a DHCP request with the matching MAC address. Its response includes configuration information, and any DHCP options and options filters defined for the host or inherited from the network to which the fixed address belongs. You can also assign multiple IP addresses to a host, as described in [Assigning Multiple IP Addresses to a Host](#) on page 443. Note that you can modify the host record and make it a reservation, as well. For information, see [Configuring Reservations](#) on page 611.

You can define extensible attributes for a host record to further describe the device. You can include information such as its location and owner for IP address management purposes. For information about extensible attributes, see [About Extensible Attributes](#) on page 222.

Figure 16.1 illustrates how the appliance uses the host record for both DHCP and DNS.

#### Figure 16.1 Using the Host Record for DHCP and DNS

![Diagram of DHCP and DNS interaction](#)

1. The DHCP client sends its MAC address in the DHCP DISCOVER and REQUEST packets.
2. The appliance determines the network segment of the host and matches the MAC address with the Host record. It assigns the fixed address from the host record and includes the configuration settings and DHCP options inherited from the network.
3. A resolver sends a query for the IP address of ftp.corp.100.com.
4. The appliance responds with the A record of ftp.corp.100.com:
   - `ftp.corp100.com`
   - `internet address=10.1.1.7`
   - `ttl = 86400 (10)`

Note that if the zone of the host record is associated with networks, the IP addresses must belong to the associated networks. For example, if the host record is in the corp100.com zone, which is associated with 10.1.0.0/16 network, then the IP addresses of the host record must belong to the 10.1.0.0/16 network. For information about associating zones and networks, see [Associating Networks with Zones](#) on page 598.
Assigning Multiple IP Addresses to a Host

You can assign multiple IP addresses to a host depending on the function of the device. For example, you can create a host record for a router that supports three network interfaces in two different networks, and assign IP addresses to each interface, as illustrated in Figure 16.2. When the DNS server responds to DNS queries for the host, it includes an A record for each IP address.

In addition, if the IP addresses belong to different networks, they can have different DHCP configurations and options. As shown in Figure 16.2, the configuration information and DHCP options of the interface with IP address 10.31.212.3 may be different from the other two interfaces, 10.31.209.5 and 10.31.209.7, because it is in a different network.

Figure 16.2 Assigning Multiple IP Addresses to one Host Record
Adding Host Records

You can add host records from the Toolbar of the IPAM, DHCP and DNS tabs of the Data Management tab. When you create a host record, you must specify its zone and at least one IP address. If the zone of the host record is associated with one or more networks, the IP addresses must belong to one of the associated networks.

To add a host record:

1. From the IPAM, DHCP or DNS tab of the Data Management tab, expand the Toolbar.
2. Click Add and select the option to add a host record from the drop-down menu.
3. In the Add Host Record wizard, do the following:
   - **Name**: If Grid Manager displays a zone name, enter the host name here. The displayed zone name can either be the last selected zone or the zone from which you are adding the host record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box, and then enter a unique name for the host. The name you enter is prefixed to the DNS zone name that is displayed, and the complete name becomes the FQDN (fully qualified domain name) of the host. For example, if the zone name displayed is corp100.com and you enter admin, then the FQDN becomes admin.corp100.com.
   - **Enable in DNS**: This is selected by default. It enables DNS service for the host. If you clear this check box, DNS does not serve this host and you cannot assign it to a zone.
   - **DNS View**: Displays the DNS view for the host record. This appears only when you enable the host record in DNS.
   - **Host Name Policy**: Displays the host name policy of the selected zone. This appears only when you enable the host record in DNS.
   - In the **IP Addresses** section, you specify the IP addresses of the host record. Click the Add icon and do one of the following:
     - **Select Add Address** to enter an IP address.
     - **Select Next Available IPv4** to retrieve the next available IP address in a network.
       - If the host record is in a zone that has one associated network, Grid Manager retrieves the next available IP address in that network.
       - If the host record is in a zone that has multiple associated networks, the Network Selector dialog box lists the associated networks. If the zone has no network associations, the Network Selector dialog box lists the available networks. When you select a network, Grid Manager retrieves the next available IP address in that network.
       - If you want to enter a link-local IPv6 address, you must enter an IPv4 address and the host MAC address first, and then click the Add (+) icon again to enter the link-local IPv6 address. When you select the link-local IPv6 address, the MAC address is automatically filled in. For information, see Understanding DNS for IPv6 on page 388.
     - Optionally, you can delete an IP address from the host by selecting an IP address in the table and clicking the Delete icon.
       - **MAC Address**: Enter the MAC address of the network device associated with this host IP address. Note that you must enter a MAC address if DHCP is enabled for the host IP address.
       - **DHCP**: Select this to enable the DHCP services to manage the host IP address. If you do not select this option, the host IP address is not managed by the DHCP server.
       - **Comment**: Optionally, enter additional information about the host record.
       - **Disable**: Select this option to temporarily disable the host record. For example, you might want to disable a host when you need to update the network device.
4. Select one of the following:
   - Save & Close: Save the entry and close the wizard.
   - Save & Edit: Save the entry and continue editing.
   - Save & New: Save the entry and display a new wizard.
   or
   - Click Next to define extensible attributes. For information, see Using Extensible Attributes on page 225.

Modifying Host Records

To modify a host record:
1. From the Data Management tab, select the IPAM, DHCP, or DNS tab.
2. In the selected application, search for or navigate to the host record that you want to modify.
3. Select the record and click the Edit icon. Grid Manager displays the Host Record editor.
4. The Host Record editor provides the following tabs from which you can modify data:
   - General: Modify the information you entered through the wizard as described in Adding Host Records on page 444.
   - TTL: This tab displays the default TTL settings the record inherited from the grid or the DNS zone, if you enabled override TTL settings at the zone level. You can keep the default settings or override them. To override the inherited value, click Override to enable the configuration. Specify how long the record is cached. Select the time period in seconds, minutes, hours, days, or weeks from the drop-down list. To enable the record to inherit the grid or zone TTL settings, click Inherit.
   - Aliases: Click the Add icon. Grid Manager displays a new row in the table. Enter a fully qualified domain name (a CNAME record for the host) in the Aliases column. You can delete an alias by selecting the alias check box and clicking the Delete icon.
   - Discovered Data: Displays the discovered data of the host record. For information, see Viewing Data in the Discovered Data Section on page 820.
   - Extensible Attributes: You can add and delete extensible attributes that are associated with a host record. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes on page 225.
   - Permissions: This tab appears only if you belong to a superuser admin group. For information, see About Administrative Permissions on page 87.
5. Select one of the following:
   - Cancel: Cancel the entry and close the editor.
   - Save & Close: Save the entry and close the editor.
   - Save: Save the entry and continue to edit.
About Bulk Hosts

If you need to add a large number of A and PTR records, you can have the NIOS appliance add them as a group and automatically assign host names based on a range of IP addresses and the host name format you specify. Such a group of records is called a *bulk host*, which the appliance manages and displays as a single bulk host record.

Specifying Bulk Host Name Formats

Bulk host name formats provide a flexible way to define bulk host names. You create multiple bulk host formats at the grid level. Either select from the default bulk host formats or create your own. You can specify a different format for each bulk host. When you assign a bulk host name format to a bulk host in a zone, the system applies the zone’s host name policy to it.

A bulk host name consists of a prefix, a suffix, and the name of the domain to which the host belongs. The prefix can contain any printable character that complies with the zone host name policy. It can also be blank. The suffix is derived from an IP address in the bulk host IP address range.

The suffix format is a string of ASCII characters that uses $ (unpadded) or # (zero-padded) followed by 1,2,3,4 to refer to the first, second, third, or fourth IP address octet; it uses $1,$2,$3,$4 or #1,#2,#3,#4. $2 refers to the second unpadded octet and #4 refers to the fourth zero-padded octet. For example:

The prefix of a bulk host = info
IP address = 10.19.32.133
Domain name = infoblox.com.
If you specify the default four-octet format -$1-$2-$3-$4, the bulk host name is info-10-19-23-133.infoblox.com.
If you specify a custom name format such as *#1*#2*#3*#4, the bulk host name is info*10*019*023*133.infoblox.com.

Before Defining Bulk Host Name Formats

Before you specify a bulk host name format, ensure that it complies with the following rules:

- The NIOS appliance uses <prefix>-xx-xx-xx for bulk hosts. Ensure that the bulk host name does not conflict with CNAMEs, DNAMEs, or host name aliases.
- When you add a bulk host, if you enable the Automatically add reverse mapping option and there is a CNAME record in the corresponding reverse zone that conflicts with a PTR record generated by the bulk host, the bulk host insertion fails and an error message appears. For example, if there is a CNAME with the alias 15 in a reverse zone 1.168.192.in-addr.arpa and if you add a bulk host foo/192.168.1.10/192.168.1.20 with the Automatically add reverse mapping option selected, the insertion fails and an error message appears because both the bulk host and the CNAME generate a record 15.1.168.192.in-addr.arpa in the reverse zone.
- You cannot create or change a bulk host if a zone is locked by another user. If you select a different template for the grid, it changes each record associated with the bulk host.
- You can define bulk host name formats only at the grid level and override them at the bulk host level; not at the zone or bulk host object level.
- During an upgrade, the system migrates existing bulk hosts as follows:
  - If you did not customize the bulk host IP format, there is no action required. All migrated bulk hosts continue to use the grid-level default four-octet format -$1-$2-$3-$4. See Specifying Bulk Host Name Formats on page 446.
  - If you customized the bulk host IP format, the system creates a new template called Migrated Default template. All migrated bulk hosts override the grid default template and use the Migrated Default template.

Note: The NIOS appliance considers two bulk hosts that have the same prefix, start address, and end address as duplicate hosts; even if they use different bulk host formats.
### Bulk Host Name Format Rules

*Table 16.1* describes the rules that you should follow when you create bulk host name formats. It also provides examples of valid and invalid formats for each rule.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>The suffix format cannot have more than four octets.</td>
<td>-$4-$5 is invalid.</td>
</tr>
<tr>
<td>The octets must be in order.</td>
<td>-$2-$3-$4 is valid but -$3-$2-$4 is invalid.</td>
</tr>
<tr>
<td>Do not skip octets.</td>
<td>-$2-$3-$4 is valid but -$2-$4 is invalid.</td>
</tr>
<tr>
<td>Do not use a combination of both the $ and # symbols together as</td>
<td>-$2-$3-$4 is invalid.</td>
</tr>
<tr>
<td>octet references; use only one of them.</td>
<td></td>
</tr>
<tr>
<td>The suffix format must contain at least the fourth octet. You must</td>
<td>-$4 is valid but -$3 is invalid.</td>
</tr>
<tr>
<td>define at least one -$4 or -$#4.</td>
<td></td>
</tr>
<tr>
<td>The suffix format must not start with the $ character.</td>
<td>$4 is invalid.</td>
</tr>
<tr>
<td>If the suffix format uses $ references, it cannot be preceded by a</td>
<td>-$2-$3-$4</td>
</tr>
<tr>
<td>digit. You must add a non-digit prefix to each $ or # reference.</td>
<td></td>
</tr>
<tr>
<td>The \ character is the designated escape character for the $, # and</td>
<td>For the IP address 10.19.32.133, the format #-#1-#2-#3-#4 expands to</td>
</tr>
<tr>
<td>\ characters. You cannot use the $ or # symbols as separators</td>
<td>#010-019-032-133.</td>
</tr>
<tr>
<td>unless you prefix them with an escape character.</td>
<td></td>
</tr>
<tr>
<td>The bulk host name format must comply with its zone host name</td>
<td>You cannot insert a bulk host name format -?-$4 in a zone that uses</td>
</tr>
<tr>
<td>policy.</td>
<td>Allow Underscore as host name policy because the policy does not allow</td>
</tr>
<tr>
<td>The bulk host name must comply with the maximum label length.</td>
<td>you to use the ? character in the host name.</td>
</tr>
<tr>
<td>The bulk host name cannot result in an FQDN with more than 255</td>
<td>The sum of the bulk host name prefix and suffix cannot be greater than</td>
</tr>
<tr>
<td>characters.</td>
<td>63 characters. When you enter a suffix format, the NIOS appliance</td>
</tr>
<tr>
<td>The NIOS appliance computes the maximum length of the bulk host</td>
<td>determines the length of the longest bulk host defined, and checks</td>
</tr>
<tr>
<td>suffix by expanding the bulk host IP format using 255.255.255.255.</td>
<td>that the sum of the bulk host prefix and suffix length does not exceed 63 characters; if it does, an error message appears.</td>
</tr>
</tbody>
</table>

The NIOS appliance computes the maximum length of the bulk host suffix by expanding the bulk host IP format using 255.255.255.255.

For the format string -$1-$2-$3-$4, the maximum length of the suffix is 255-255-255-255; that is, 16 characters. Therefore, the maximum length of the host prefix is 47 characters.
The appliance provides four predefined formats. You can define additional formats or change the default format at the grid level only. To define new bulk host name formats:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
2. Select the Host Naming tab of the Grid DNS Properties editor.
   
   The Bulk Host Name Formats table displays four predefined name suffix formats. The following examples show the host name that each format generates for the zone test.com:
   
   
   Three Octets: -$2-$3-$4—Generates foo-168-1-15.test.com
   
   Two Octets: -$3-$4—Generates foo-1-15.test.com
   
   One Octet: -$4—Generates foo-15.test.com
   
   For the IP address 10.100.0.10, the format -$1-$2-$3-$4 generates the host name suffix -10-100-0-10. The format $1-$2-$3-$4 generates the host name suffix -10-100-0-10. The format #1-#2-#3-#4 generates the host name suffix -10-100-0-10.
   
   3. Click Add to enter the name and format of a new bulk host name format.
4. Optionally, click the Default column of a format and select Default to make it the grid default.
5. Select one of the following:
   
   — Save & Close: Save the entry and close the editor.
   
   — Save: Save the entry and keep the editor open.
About Bulk Hosts

Adding Bulk Hosts

To add a bulk host:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Host -> Add Bulk Host.
2. In the Add Bulk Host wizard, complete the following fields:

   - **Prefix**: If Grid Manager displays a zone name, enter a prefix (or series of characters) to insert at the beginning of each host name. The displayed zone name can either be the last selected zone or the zone from which you are adding the bulk host record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box, and enter a prefix for the bulk host record. You can enter any printable character that complies with the zone host name policy or you can also leave this blank.

   The sum of the bulk host prefix length and suffix length must not exceed 63 characters. When you enter a prefix, the NIOS appliance computes the maximum length of the bulk host suffix to verify that the total prefix and suffix length does not exceed 63 characters. If it does, the appliance displays an error message indicating the number of characters that you must remove to make a valid prefix.
   
   - **DNS View**: Displays the DNS view of the zone to which the bulk host records belong.
   - **Host Name Policy**: Displays the host name policy of the selected DNS zone.
   - **Name Format**: To override the default four-octet suffix format or the format set at the grid level, and specify a different format, click Override and select a host name format from the Name Formats drop-down menu.

   The Name Formats drop-down menu lists the formats **Four Octets**, **Three Octets**, **Two Octets**, and **One Octet** along with any other bulk host name formats that you have defined.
   
   - **Starting IP Address**: Enter the first IP address in the range of addresses for the group.
   - **End IP Address**: Enter the last IP address in the range of addresses for the group.
   - **Comment**: Optionally, enter additional information for this record.
   - **Automatically Add Reverse Mapping**: Click to have the appliance automatically create a PTR record for each IP address within the bulk host range.
   - **Disable**: Clear the check box to enable the record. Select the check box to disable it.

3. Select one of the following:
   
   - **Next**: Define extensible attributes for the bulk host record. For information, see Using Extensible Attributes on page 225.
   - **Save & Close**: Save the entry and close the editor.
   - **Save & Edit**: Save the entry and continue with editing.
   - **Save & New**: Save the entry and create a new bulk host record.

To modify or delete a bulk host, see Modifying, Disabling, and Deleting Host and Resource Records on page 471.
Example 1 - Responding to DNS AXFR Queries

This example shows the responses the bulk host foo/1.2.3.10/1.2.3.20 returns to DNS AXFR (Full Zone Transfers) queries.

If the bulk host uses the template -$3-$4, the query returns:

  foo-3-10.test.com
  foo-3-11.test.com
  ......  
  foo-3-20.test.com

If the bulk host uses the template -#2-#3-#4, the query returns:

  foo-002-003-010.test.com
  foo-002-003-011.test.com
  ......  
  foo-002-003-020.test.com

Example 2 - Importing Zones with Bulk Hosts

When you import zones with bulk hosts, the system selects the most specific match.

The following example can possibly match three octet, two octet, and one octet formats; however, the system selects the most specific four octet default format.

The query:

  foo-1-2-3-4 IN A 1.2.3.4
  foo-1-2-3-5 IN A 1.2.3.5

Results in the match:

  foo/1.2.3.4/1.2.3.5 (Four Octets)

Not in any of the following:

  foo-1/1.2.3.4/1.2.3.5 (Three Octets)
  foo-1-2/1.2.3.4/1.2.3.5 (Two Octets)
  foo-1-2-3/1.2.3.4/1.2.3.5 (One Octet)
MANAGING RESOURCE RECORDS

DNS resource records provide information about objects and hosts. DNS servers use these records to respond to queries for hosts and objects.

You can manage the following types of DNS resource records:

- **A (IPv4 Address)**—For information, see *Managing A Records* on page 452.
- **NS (Name server)**—For information, see *Managing NS Records* on page 453.
- **AAAA (IPv6 Address)**—For information, see *Managing AAAA Records* on page 454.
- **PTR (Pointer)**—For information, see *Managing PTR Records* on page 455.
- **MX (Mail exchanger)**—For information, see *Managing MX Records* on page 456.
- **SRV (Service location)**—For information, see *Managing SRV Records* on page 457.
- **TXT (Text)**—For information, see *Managing TXT Records* on page 459.
- **CNAME (Canonical name)**—For information, see *Managing CNAME Records* on page 460.
- **DNAME**—For information, see *Managing DNAME Records* on page 462.
Managing A Records

An A (address) record is a DNS resource record that maps a domain name to an IPv4 address. To define a specific name-to-address mapping, you can add an A record to a previously defined authoritative forward-mapping zone. If the zone is associated with one or more networks, the IP address must belong to one of the associated networks. For example, if the A record is in the corp100.com zone, which is associated with 10.1.0.0/16 network, then the IP addresses of the A record must belong to the 10.1.0.0/16 network. For information about associating zones and networks, see Associating Networks with Zones on page 598.

The appliance also supports wildcard A records. For example, you can use a wildcard A record in the corp100.com domain to map queries for names such as www1.corp100.com, ftp.corp100.com, main.corp100.com, and so on to the IP address of a public-facing web server. Note that wildcard names only apply when the domain name being queried does not match any resource record.

Adding A Records

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> Add A Record.
2. In the Add A Record wizard, do the following:
   — Name: If Grid Manager displays a zone name, enter the hostname that you want to map to an IP address. The displayed zone name can either be the last selected zone or the zone from which you are adding the host record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box and then enter the hostname. The name you enter is prefixed to the DNS zone name that is displayed, and the complete name becomes the FQDN (fully qualified domain name) of the host. For example, if the zone name displayed is corp100.com and you enter admin, then the FQDN becomes admin.corp100.com. Ensure that the domain name you enter complies with the hostname restriction policy defined for the zone. To create a wildcard A record, enter an asterisk (*) in this field.
   — DNS View: This field displays the DNS view to which the DNS zone belongs.
   — Hostname Policy: Displays the hostname policy of the zone.
   — In the IP Addresses section, click the Add icon and do one of the following:
     — Select Add Address to enter the IPv4 address to which you want the domain name to map.
     — Select Next Available IPv4 to retrieve the next available IP address in a network.
       If the A record is in zone that has associated networks, the Network Selector dialog box lists the associated networks. If the zone has no network associations, the Network Selector dialog box lists the available networks. When you select a network, Grid Manager retrieves the next available IP address in that network.
   — Comment: Optionally, enter additional information about the A record.
   — Create associated PTR record: Select this option to automatically generate a PTR record that maps the specified IP address to the hostname. A reverse-mapping zone is required for the PTR record.
   — Disable: Select this check box to disable the record. Clear the check box to enable it.
3. Select one of the following:
   — Save & Close: Save the entry and close the wizard.
   — Save & Edit: Save the entry and continue editing.
   — Save & New: Save the entry and create another A record.
   or
   — Click Next to define extensible attributes. For information, see Using Extensible Attributes on page 225.
Managing Resource Records

Modifying A Records

When you modify an A record, you can change the following information:

- In the General tab, you can change the information you previously entered through the wizard.
- The Discovered Data tab displays the following discovered data, if any, for the record:
  - MAC Address: The unique identifier of a network device. A discovery returns the MAC address for hosts that are located on the same network as the grid member that is running the discovery.
  - NetBIOS Name: The name that is returned in the NetBIOS reply or a name that you manually register for the discovered host.
  - OS: The operating system of the detected host. This value is set to Microsoft for active hosts that have a MAC address in the NetBIOS reply.
  - Last Discovered: The timestamp that indicates when the active host was last detected by a discovery.
    Note that this data can be overwritten by a subsequent discovery.

You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records on page 471.

Managing NS Records

An NS record identifies an authoritative DNS server for a domain. Each authoritative DNS server must have an NS record. Grid Manager automatically creates an NS record when you assign a grid member as the primary server for a zone. You can manually create NS records for other zones. NS records associated with one or more IP addresses are used for related A record and PTR record generation. You can configure an NS record for anycast IP addresses on the appliance. For more information about anycast, see Anycast Addressing on page 570.

Adding NS Records

To add an NS record:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> Add NS Record.
2. In the Add NS Record wizard, complete the following fields:
   - Zone: The displayed zone name can either be the last selected zone or the zone from which you are adding the NS record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box.
   - DNS View: Displays the DNS view to which the selected zone belongs.
   - Hostname Policy: Displays the hostname policy of the selected zone.
   - Name Server: Enter the host name that you want to configure as the name server for the zone.
3. Click Next to enter IP addresses for the name server.
4. In the Name Server Addresses panel, click the Add icon and complete the following fields:
   - Address: Enter the IP address of the name server.
   - Add PTR Record: This field displays Yes by default, enabling the automatic generation of a PTR record for the IP address. You can select No to disable the generation of the PTR record.
5. Select one of the following:
   - Save & Close: Save the entry and close the wizard.
   - Save & Edit: Save the entry and continue editing. Grid Manager displays the NS Record editor.
   - Save & New: Save the entry and display a new wizard.
   or
   - Click Next to define extensible attributes. For information, see Using Extensible Attributes on page 225.
Modifying and Deleting NS Records

When you modify an NS record, you can change the following information:

- In the General tab, you can change the name server name.
- In the Addresses tab, you can do the following:
  - Delete an address by selecting it and clicking the Delete icon.
  - Add an address by clicking the Add icon, and then entering the IP address and completing the Add PTR Record field.

Managing AAAA Records

An AAAA (quad A address) record maps a domain name to an IPv6 address. To define a specific name-to-address mapping, add an AAAA record to a previously defined authoritative forward-mapping zone. If the zone is associated with one or more networks, the IP address must belong to one of the associated networks. For example, if the AAAA record is in the corp100.com zone, which is associated with the 1111:0001/32 network, then the IP addresses of the A record must belong to that network. For information about associating zones and networks, see Associating Networks with Zones on page 598.

Adding AAAA Records

To create an AAAA record:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> Add AAAA Record.
2. In the Add AAAA Record wizard, complete the following:
   - Name: If Grid Manager displays a zone name, enter the hostname that you want to map to an IP address. The displayed zone name can either be the last selected zone or the zone from which you are adding the AAAA record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box, and then enter the hostname. The name you enter is prefixed to the DNS zone name that is displayed, and the complete name becomes the FQDN (fully qualified domain name) of the host. For example, if the zone name displayed is corp100.com and you enter admin, then the FQDN becomes admin.corp100.com.
   - DNS View: Displays the DNS view to which the selected DNS zone belongs.
   - Hostname Policy: Displays the hostname policy of the zone.
   - IP Address: Enter the IPv6 address to which you want the domain name to map. When you enter an IPv6 address, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2006:0000:0000:0123:4567:89ab:0000:cdef can be shortened to 2006::123:4567:89ab:0:cdef. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The NIOS appliance displays an IPv6 address in its shortened form, regardless of its form when it was entered.
   - Comment: Optionally, enter additional information about this record.
   - Disable: Clear the check box to enable the record. Select the check box to disable it.
3. Select one of the following:
   - Save & Close: Save the entry and close the wizard.
   - Save & Edit: Save the entry and continue editing.
   - Save & New: Save the entry and add another AAAA record.
   or
   - Click Next to define extensible attributes. For information, see Using Extensible Attributes on page 225.
Managing AAAA Records

When you modify an AAAA record, in the General tab, you can change the information you previously entered through the wizard. You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records on page 471.

Managing PTR Records

A PTR (pointer) record is a DNS resource record that maps an IP address to a hostname, and can only be added to a reverse-mapping zone. You must first create a reverse-mapping zone before adding a PTR record for the zone. To create a PTR record, you need to specify a domain name and a hostname.

Note: You must configure PTR records manually for IPv6 addresses. Unlike IPv4 PTR records, IPv6 PTR records are not automatically generated.

Adding PTR Records

To add a PTR record:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> Add PTR Record.
2. In the Add PTR Record wizard, do the following:
   - IP Address or Domain Name: From the drop-down list, select either IP Address or Domain Name. When you select IP Address, enter the IPv4 or IPv6 address that you want to map to a domain name. When you select Domain Name, click Select Zone to select a reverse-mapping zone, and then enter the domain name or the prefix of the domain name.
   - DNS View: If you enter an IP address, you must select the DNS view of the PTR record. If you enter a domain name, this field displays the DNS view of the selected reverse-mapping zone.
   - Name: Enter the hostname to which you want the PTR record to point. For example, www.corp100.com.
   - Comment: Optionally, enter useful information about the PTR record.
   - Disable: Select this check box to disable the record. Clear the check box to enable it.
3. Select one of the following:
   - Save & Close: Save the entry and close the wizard.
   - Save & Edit: Save the entry and continue editing.
   - Save & New: Save the entry and add another PTR record.
   - Click Next to define extensible attributes. For information, see Using Extensible Attributes on page 225.

Modifying PTR Records

When you modify a PTR record, you can change the following information:

- In the General tab, you can change the information you previously entered through the wizard.
- The Discovered Data tab displays the following discovered data, if any, for the record:
  - NetBIOS Name: The name that is returned in the NetBIOS reply or a name that you manually register for the discovered host.
  - OS: The operating system of the detected host.
  - Last Discovered: The timestamp that indicates when the active host was last detected by a discovery. This data is read-only.

You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records on page 471.
Managing MX Records

An MX (mail exchanger) record maps a domain name to a mail exchanger. A mail exchanger is a server that either delivers or forwards mail. You can specify one or more mail exchangers for a zone, as well as the preference for using each mail exchanger. A standard MX record applies to a particular domain or subdomain.

You can use a wildcard MX record to forward mail to one mail exchanger. For example, you can use a wildcard MX record in the corp100.com domain to forward mail for eng.corp100.com and sales.corp100.com to the same mail exchange, as long as the domain names do not have any matching resource record. Wildcards only apply when the domain name being queried does not match any record.

See Figure 16.3.

Figure 16.3  MX Records

The following MX records ... ... direct queries for one or more domains ... ... to the same mail exchanger:

- An MX record for the mail exchanger that answers queries for just the corp100.com domain (and its corresponding A record):
  ```
  corp100.com IN MX 0 mail1.corp100.com
  mail1.corp100.com IN A 10.2.2.10
  ```

- An MX record for just site1.corp100.com, a subdomain of corp100.com:
  ```
  site1.corp100.com IN MX 0
  mail1.corp100.com
  ```

- A wildcard MX record for the corp100.com domain:
  ```
  *.corp100.com IN MX 0 mail1.corp100.com
  ```

Note: You must also create an A record for the host defined as a mail exchanger in an MX record.

Adding MX Records

To add an MX record:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add → Record → Add MX Record.
2. In the Add MX Record wizard, complete the following fields:
   - Mail Destination: If Grid Manager displays a zone name, enter the mail destination here. The displayed zone name can either be the last selected zone or the zone from which you are adding the MX record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box, and then enter the mail destination. If you want to define an MX record for a domain whose name matches the zone you selected, leave this field blank. Grid Manager automatically adds the domain name (the same as the zone name) to the MX record. For example, if you want to create an MX record for a mail exchanger serving the corp100.com domain and you selected the corp100.com zone, leave this field empty.
   - Subdomain: Enter the domain name of the subdomain you want to define.
   - Preference: Enter the preference for using the mail exchanger.
   - Mail Exchanger: Enter the name of the mail exchanger.

If you want to define an MX record for a subdomain, enter the subdomain name. The NIOS appliance prefixes the name you enter to the domain name of the selected zone. For example, if you want to create an MX record for a mail exchanger serving site1.corp100.com—a subdomain of corp100.com—and you define the MX record in the corp100.com zone, enter site1 in this field.

If you want to define an MX record for a domain and all its subdomains, enter an asterisk (*) to create a wildcard MX record.
Managing Resource Records

- **DNS View**: Displays the DNS view of the selected zone.
- **Host Name Policy**: Displays the hostname policy of the selected zone. Ensure that the hostname you enter complies with the hostname restriction policy defined for the zone.
- **Mail Exchanger**: Enter the fully qualified domain name of the mail exchanger.
- **Preference**: Select an integer from 10 to 100, or enter a value from 0 to 65535. The preference determines the order in which a client attempts to contact the target mail exchanger.
- **Comment**: Enter a descriptive comment for this record.
- **Disable**: Clear the check box to enable the record. Select the check box to disable it.

3. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save & Edit**: Save the entry and continue editing.
   - **Save & New**: Save the entry and create a new MX record.
   or
   - Click **Next** to define extensible attributes. For information, see *Using Extensible Attributes* on page 225.

Modifying and Deleting MX Records

When you modify an MX record, in the **General** tab, you can change the information you previously entered through the wizard. You can also enter or edit information in the **TTL**, **Extensible Attributes** and **Permissions** tabs. For information on modifying and deleting resource records, see *Modifying, Disabling, and Deleting Host and Resource Records* on page 471.

Managing SRV Records

An SRV (service location) record directs queries to hosts that provide specific services. For example, if you have an FTP server, then you might create an SRV record that specifies the host which provides the service. You can specify more than one SRV record for a host. For more information about SRV records, see *RFC 2052, A DNS RR for specifying the location of services (DNS SRV)*.

Adding SRV Records

1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Add -> Record -> Add SRV Record**.
2. In the **Add SRV Record** wizard, complete the following fields:
   - **Service**: Specify the service that the host provides. You can either select a service from the list or type in a service, if it is not on the list. For example, if you are creating a record for a host that provides FTP service, select \_ftp. To distinguish the service name labels from the domain name, the service name is prefixed with an underscore.
     If the name of the service is defined in *RFC 1700, Assigned Numbers*, use that name. Otherwise, you can use a locally-defined name.
   - **Protocol**: Specify the protocol that the host uses. You can either select a protocol from the list or type in a protocol, if it is not on the list. For example, if it uses TCP, select \_tcp. To distinguish the protocol name labels from the domain name, the protocol name is prefixed with an underscore.
DNS Resource Records

— **Domain:** If Grid Manager displays a zone name, enter the name here to define an SRV record for a host or subdomain. The displayed zone name can either be the last selected zone or the zone from which you are adding the SRV record. If no zone name is displayed or if you want to specify a different zone, click **Select Zone.** When there are multiple zones, Grid Manager displays the **Zone Selector** dialog box. Click a zone name in the dialog box, and then enter the name to define the SRV record. The NIOS appliance prefixes the name you enter to the domain name of the selected zone. For example, if you want to create an SRV record for a web server whose host name is www2.corp100.com and you define the SRV record in the corp100.com zone, enter www2 in this field. To define an SRV record for a domain whose name matches the selected zone, leave this field blank. The NIOS appliance automatically adds the domain name (the same as the zone name) to the SRV record. For example, if you want to create an SRV record for the corp100.com domain and you selected the corp100.com zone, leave this field blank.

— **Priority:** Select or enter an integer from 0 to 65535. The priority determines the order in which a client attempts to contact the target host; the domain name host with the lowest number has the highest priority and is queried first. Target hosts with the same priority are attempted in the order defined in the **Weight** field.

— **Weight:** Select or enter an integer from 0 to 65535. The weight allows you to distribute the load between target hosts. The higher the number, the more that host handles the load (compared to other target hosts). Larger weights give a target host a proportionately higher probability of being selected.

— **Port:** Specify the appropriate port number for the service running on the target host. You can use standard or nonstandard port numbers, depending on the requirements of your network. You can select a port number from the list or enter an integer from 0 to 65535.

— **Target:** Enter the canonical domain name of the host (not an alias); for example, www2.corp100.com. 

**Note:** In addition, you need to define an A record mapping the canonical name of the host to its IP address.

— **Comment:** Enter a descriptive comment for the record.

— **Disable:** Clear the check box to enable the record. Select the check box to disable it.

3. Select one of the following:

— **Save & Close:** Save the entry and close the editor.

— **Save & Edit:** Save the entry and continue with editing.

— **Save & New:** Save the entry and create a new SRV record.

or

— Click **Next** to define extensible attributes. For information, see *Using Extensible Attributes* on page 225.

### Modifying and Deleting SRV Records

When you modify an SRV record, in the **General** tab, you can change the information you previously entered through the wizard. You can also enter or edit information in the **TTL, Extensible Attributes** and **Permissions** tabs. For information on modifying and deleting resource records, see *Modifying, Disabling, and Deleting Host and Resource Records* on page 471.
Managing TXT Records

A TXT (text record) record contains supplemental information for a host. For example, if you have a sales server that serves only North America, you can create a text record stating this fact. You can create more than one text record for a domain name.

Using TXT Records for SPF

SPF (Sender Policy Framework) is an anti-forgery mechanism designed to identify spam e-mail. SPF fights e-mail address forgery and makes it easier to identify spam, worms, and viruses. Domain owners identify sending mail servers in DNS. SMTP receivers verify the envelope sender address against this information, and can distinguish legitimate mail from spam before any message data is transmitted.

SPF makes it easy for a domain to say, “I only send mail from these machines. If any other machine claims that I’m sending mail from there, they’re not valid.” For example, when an AOL user sends mail to you, an email server that belongs to AOL connects to an email server that belongs to you. AOL uses SPF to publish the addresses of its email servers. When the message comes in, your email servers can tell if the server that sent the email belongs to AOL or not.

You can use TXT records to store SPF data that identifies what machines send mail from a domain. You can think of these specialized TXT records as reverse MX records that e-mail servers can use to verify if a machine is a legitimate sender of an e-mail.

**SPF Record Examples**

- corp100.com. IN TXT “v=spf1 mx -all”
- corp100.net. IN TXT “v=spf1 a:mail.corp100.com -all”
- corp100.net. IN TXT “v=spf1 include:corp100.com -all”
- corp100.net. IN TXT “v=spf1 mx -all exp=getlost.corp100.com”
- corp100.com. IN TXT “v=spf1 include:corp200.com -all”

Adding TXT Records

To add a TXT record:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> Add TXT Record.
2. In the Add TXT Record wizard, complete the following fields:
   - **Name:** If Grid Manager displays a zone name, enter the name to define a TXT record for a host or subdomain. The displayed zone name can either be the last selected zone or the zone from which you are adding the TXT record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box. Then, enter the TXT record name. The NIOS appliance prefixes the name you entered to the domain name of the selected zone. For example, if you want to create a TXT record for a web server whose host name is www2.corp100.com and you define the TXT record in the corp100.com zone, enter www2 in this field. To define a TXT record for a domain whose name matches the selected zone, leave this field empty. The NIOS appliance automatically adds the domain name (the same as the zone name) to the TXT record. For example, if you want to create a TXT record for the corp100.com domain and you selected the corp100.com zone, leave this field empty.
   - **DNS View:** Displays the DNS view of the selected zone.
   - **Text:** Enter the text that you want to associate with the record. It can contain up to 255 characters.
   - **Comments:** Enter a descriptive comment for this record.
   - **Disable:** Clear the check box to enable the record. Select the check box to disable it.
3. Select one of the following:
   — Save & Close: Save the entry and close the editor.
   — Save & Edit: Save the entry and continue with editing.
   — Save & New: Save the entry and create a new TXT record.
   or
   — Click Next to define extensible attributes. For information, see Using Extensible Attributes on page 225.

Modifying and Deleting TXT Records

When you modify a TXT record, you can change the information you previously entered in the General tab. You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records on page 471.

Managing CNAME Records

A CNAME record maps an alias to a canonical name. You can use CNAME records in both forward- and IPv4 reverse-mapping zones to serve two different purposes. (At this time, you cannot use CNAME records with IPv6 reverse-mapping zones.)

CNAME Records in Forward-Mapping Zones

In a forward-mapping zone, a CNAME record maps an alias to a canonical (or official) name. CNAME records are often more convenient to use than canonical names because they can be shorter or more descriptive. For example, you can add a CNAME record that maps the alias qa.engr to the canonical name qa.engr.corp100.com.

Note: A CNAME record does not have to be in the same zone as the canonical name to which it maps. In addition, a CNAME record cannot have the same name as any other record in that zone.

To add a CNAME record to a forward-mapping zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> Add CNAME Record.
2. In the Add CNAME Record wizard, complete the following fields:
   — Alias: If Grid Manager displays a zone name, enter the alias for the canonical name. The displayed zone name can either be the last selected zone or the zone from which you are adding the CNAME record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box, and then enter the alias name.
   — DNS View: Displays the DNS view of the selected zone.
   — Canonical Name: This field displays the domain name of either the current zone or the last selected zone. You can change the entry, which must be the complete canonical (or official) name of the host.
   — Comments: Enter a descriptive comment for this record.
   — Disable: Clear the check box to enable the record. Select the check box to disable it.
3. Select one of the following:
   — Save & Close: Save the entry and close the editor.
   — Save & Edit: Save the entry and continue with editing.
   — Save & New: Save the entry and create a new CNAME record.
   or
   — Click Next to define extensible attributes. For information, see Using Extensible Attributes on page 225.
CNAME Records in IPv4 Reverse-Mapping Zones

You can add CNAME records to an IPv4 reverse-mapping zone to create aliases to addresses maintained by a different name server when the reverse-mapping zone on the server is a delegated child zone with fewer than 256 addresses. This technique allows you to delegate responsibility for a reverse-mapping zone with an address space of fewer than 256 addresses to another authoritative name server. See Figure 16.4 and RFC 2317, Classless IN-ADDR.ARPA delegation.

Figure 16.4  CNAME Records in a Reverse-Mapping Zone

All the PTR records for Customer1 use the addresses defined as canonical names in the CNAME records on the local DNS server.

Sample PTR records:
IP Address: 1.0/127.1.1.10.in-addr.arpa
Host Name: host1.customer1.com
IP Address: 2.0/127.1.1.10.in-addr.arpa
Host Name: host2.customer1.com

You add CNAME records in the parent zone on your name server. The aliases defined in those CNAME records point to the addresses in PTR records in the child zone delegated to the other server.

When you define a reverse-mapping zone that has a netmask from /25 (255.255.255.128) to /31 (255.255.255.254), you must include an RFC 2317 prefix. This prefix can be anything, from the address range (examples: 0-127, 0/127) to descriptions (examples: first-network, customer1). On a NIOS appliance, creating such a reverse-mapping zone automatically generates all the necessary CNAME records. However, if you need to add them manually to a parent zone that has a child zone with fewer than 255 addresses:
To add a CNAME record to a reverse-mapping zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> Add CNAME Record.

2. In the Add CNAME Record wizard, complete the following fields:
   - **Alias**: If Grid Manager displays a zone name, enter the host portion of an IP address. For example, if the full IP address is 10.1.1.1 in a network with a 25-bit netmask, enter 1. (The 10.1.1.0/25 network contains host addresses from 10.1.1.1 to 10.1.1.126. The network address is 10.1.1.0, and the broadcast address is 10.1.1.127.) The displayed zone name can either be the last selected zone or the zone from which you are adding the CNAME record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box, and then enter the alias name.
   - **DNS View**: Displays the DNS view of the selected zone.
   - **Canonical Name**: This field displays the domain name of either the current zone or the last selected zone. You can save this entry or change it and enter host_ip_addr.prefix.network.in-addr.arpa (host IP address + 2317 prefix + network IP address + in-addr.arpa). For example, enter 1.0.25.1.10.in-addr.arpa. This IP address must match the address defined in the PTR record in the delegated child zone.
   - **Comments**: Enter a descriptive comment for this record.
   - **Disable**: Clear the check box to enable the record. Select the check box to disable it.

3. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save & Edit**: Save the entry and continue with editing.
   - **Save & New**: Save the entry and create a new CNAME record.
   - Click Next to define extensible attributes. For information, see Using Extensible Attributes on page 225.

### Modifying and Deleting CNAME Records

When you modify a CNAME record, you can change the information you previously entered in the General tab. You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records on page 471.

### Managing DNAME Records

A DNAME record maps all the names in one domain to those in another domain, essentially substituting one domain name suffix with the other (see RFC 2672, Non-Terminal DNS Name Redirection). For example, adding a DNAME record to the corp100.com domain mapping “corp100.com” to “corp200.com” maps name-x.corp100.com to name-x.corp200.com:

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Target Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>server1.corp100.com</td>
<td>server1.corp200.com</td>
</tr>
<tr>
<td>server2.corp100.com</td>
<td>server2.corp200.com</td>
</tr>
<tr>
<td>server3.corp100.com</td>
<td>server3.corp200.com</td>
</tr>
<tr>
<td>. . . corp100.com</td>
<td>. . . corp200.com</td>
</tr>
</tbody>
</table>
When a request arrives for a domain name to which a DNAME record applies, the NIOS appliance responds with a CNAME record that it dynamically creates based on the DNAME definition. For example, if there is a DNAME record corp100.com. DNAME corp200.com.

and a request arrives for server1.corp100.com, the NIOS appliance responds with the following CNAME record:


If responding to a name server running BIND 9.0.0 or later, the NIOS appliance also includes the DNAME record in its response, so that name server can also create its own CNAME records based on the cached DNAME definition.

The following are two common scenarios for using DNAME records:

- One company buys another and wants people using both the old and new name spaces to reach the same hosts.
- A virtual Web hosting operation offers different “vanity” domain names that point to the same server or servers.

There are some restrictions that apply to the use of DNAME records:

- You cannot have a CNAME record and a DNAME record for the same subdomain.
- You cannot use a DNAME record for a domain or subdomain that contains any subdomains. You can only map the lowest level subdomains (those that do not have any subdomains below them). For an example of using DNAME records in a multi-tiered domain structure, see Figure 16.5 on page 463.

**Figure 16.5 Adding DNAME Records for the Lowest Level Subdomains**

Corp200 buys Corp100 and wants to redirect queries for corp100.com to corp200.com; however, the multitiered structure of corp100.com prohibits a complete mapping of all its subdomains. In such a case, DNAME records provide only a partial solution.

In the case of a domain structure consisting of a single domain (no subdomains), adding a DNAME record redirects queries for every name in the domain to the target domain, as shown in Figure 16.6.
When using a DNAME record, you must copy the resource records for the source domain to the zone containing the target domain, so that the DNS server providing service for the target domain can respond to the redirected queries.

For the example in Figure 16.6, copy these records:

<table>
<thead>
<tr>
<th>Copy from corp100.com</th>
<th>to corp100.corp200.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>www1 IN A 10.1.1.10</td>
<td>www1 IN A 10.1.1.10</td>
</tr>
<tr>
<td>www2 IN A 10.1.1.11</td>
<td>www2 IN A 10.1.1.11</td>
</tr>
<tr>
<td>ftp1 IN A 10.1.1.20</td>
<td>ftp1 IN A 10.1.1.20</td>
</tr>
<tr>
<td>mail1 IN A 10.1.1.30</td>
<td>mail1 IN A 10.1.1.30</td>
</tr>
</tbody>
</table>

After copying these records to the zone containing the corp100.corp200.com domain, delete them from the zone containing the corp100.com domain.

If DNS service for the source and target domain names is on different name servers, you can import the zone data from the NIOS appliance hosting the source domain to the appliance hosting the target domain. For information about this procedure, see Importing Zone Data on page 419.

If DNS service for the source and target domain names is on the same name server and the parent for the target domain is on a different server, you can delegate DNS services for the target domain name to the name server that provided—and continues to provide—DNS service for the source domain name (see Figure 16.7 on page 465). By doing this, you can continue to maintain resource records on the same server, potentially simplifying the continuation of DNS administration.
The following tasks walk you through configuring the two appliances in Figure 16.7 to redirect queries for corp100.com to corp100.corp200.com using a DNAME record:

On the ns1.corp100.com name server, do the following:
2. Copy all the resource records for the domain or subdomain to which the DNAME record is going to apply from corp100.com to corp100.corp200.com.
3. In the corp100.com zone, delete all the resource records for the domain or subdomain to which the DNAME record is going to apply.
4. Add a DNAME record to the corp100.com zone specifying “corp100.com” as the domain and “corp100.corp200.com” as the target domain. Adding a DNAME record is explained in the next section.
5. On the ns1.corp200.com name server, add corp100.corp200.com as a delegated zone and specify ns1.corp100.com as the name server for it. See Configuring a Delegation on page 427.

DNAME Records for Forward-Mapping Zones

To add a DNAME record to a forward-mapping zone:
1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> Add DNAME Record.
2. In the Add DNAME Record wizard, complete the following fields:

Note: If you specify a subdomain in the Domain Name field when configuring a DNAME record and the subdomain is also a subzone, the DNAME record appears in the list view for the subzone, not in the list view for the parent zone selected in the process of adding the record.
— **Alias:** If Grid Manager displays a zone name, enter the name of a subdomain here. If you are adding a DNAME record for the entire zone, leave this field empty. This field is for adding a DNAME record for a subdomain within the selected zone. The displayed zone name can either be the last selected zone or the zone from which you are adding the CNAME record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box, and then enter the name of a subdomain.

— **Target:** Enter the domain name to which you want to map all the domain names specified in the Alias field.

— **Comment:** Enter identifying text for this record, such as a meaningful note or reminder.

— **Disable:** Clear the check box to enable the record. Select the check box to disable it.

3. Select one of the following:

   — **Save & Close:** Save the entry and close the editor.
   
   — **Save & Edit:** Save the entry and continue with editing.
   
   — **Save & New:** Save the entry and create a new DNAME record.
   
   or
   
   — Click **Next** to define extensible attributes. For information, see *Using Extensible Attributes* on page 225.

### DNAME Records for Reverse-Mapping Zones

You can use DNAME records to redirect reverse lookups from one reverse-mapping zone to another. You can use DNAME records for reverse-mapping zones to simplify the management of subzones for classless address spaces larger than a class C subnet (a subnet with a 24-bit netmask).

RFC 2672, *Non-Terminal DNS Name Redirection*, includes an example showing the delegation of a subzone for an address space with a 22-bit netmask inside a zone for a larger space with a 16-bit netmask:

```
$ORIGIN 0.192.in-addr.arpa.
8/22 NS ns.slash-22-holder.example.
8 DNAME 8.8/22
9 DNAME 9.8/22
10 DNAME 10.8/22
11 DNAME 11.8/22
```

The reverse-mapping zone 0.192.in-addr.arpa applies to the address space 192.0.0.0/16. Within this zone is a subzone and subdomain with the abbreviated name 8/22. (Its full name is 8/22.0.192.in-addr.arpa.) This subdomain contains its own subdomains corresponding to the 1024 addresses in the 192.0.8.0/22 subnet:

- **Subdomain 8/22 (8/22.0.192.in-addr.arpa)**
  
  — Subdomain 8.8/22 for addresses 192.0.8.0 – 192.0.8.255 (or 192.0.8.0/24)
  
  — Subdomain 9.8/22 for addresses 192.0.9.0 – 192.0.9.255 (or 192.0.9.0/24)
  
  — Subdomain 10.8/22 for addresses 192.0.10.0 – 192.0.10.255 (or 192.0.10.0/24)
  
  — Subdomain 11.8/22 for addresses 192.0.11.0 – 192.0.11.255 (or 192.0.11.0/24)

The NS record delegates authority for the reverse-mapping subzone 8/22 to the DNS server ns.slash-22-holder.example.

Finally, the DNAME records provide aliases mapping domain names that correspond to the 192.0.8.0/24, 192.0.9.0/24, 192.0.10.0/24, and 192.0.11.0/24 subnets to the respective subdomains 8.8/22, 9.8/22, 10.8/22, and 11.8/22 in the 8/22.0.192.in-addr.arpa subzone.

---

**Note:** NIOS appliances support DNAME records in reverse-mapping zones that map addresses to target zones with a classless address space larger than a class C subnet. However, NIOS appliances do not support such target zones.

You might also use DNAME records if you have a number of multihomed appliances whose IP addresses must be mapped to a single set of domain names. An example of this is shown in *Figure 16.8*. 

---
Instead of maintaining a PTR record for the IP address of each interface on every multihomed appliance, you can store all the PTR records in one reverse-mapping zone and use DNAME records in the other zones to point reverse lookups to the one set of PTR records.

**Figure 16.8 DNAME Records to Simplify DNS for Multihomed Appliances**

Note: If you specify a subdomain in the Domain Name field when configuring a DNAME record, and the subdomain is also a subzone, the DNAME record appears in the list view for the subzone, not in the list view for the parent zone that was selected when adding it.
To add a DNAME record to a reverse-mapping zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> Add DNAME Record.
2. In the Add DNAME Record wizard, complete the following fields:

   **Note:** If you specify a subdomain in the Domain Name field when configuring a DNAME record and the subdomain is also a subzone, the DNAME record appears in the list view for the subzone, not in the list view for the parent zone selected in the process of adding the record.

   - **Alias:** If Grid Manager displays a zone name, enter the name of a subdomain here. If you are adding a DNAME record for the entire zone, leave this field empty. This field is for adding a DNAME record for a subdomain within the selected zone. The displayed zone name can either be the last selected zone or the zone from which you are adding the CNAME record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box, and then enter the name of a subdomain.
   - **Target:** Type the name of the reverse-mapping zone to which you want to map all the addresses specified in the Domain Name field.
   - **Comments:** Enter identifying text for this record, such as a meaningful note or reminder.
   - **Disable:** Clear the check box to enable the record. Select the check box to disable it.

3. Select one of the following:
   - **Save & Close:** Save the entry and close the editor.
   - **Save & Edit:** Save the entry and continue with editing.
   - **Save & New:** Save the entry and create a new DNAME record.
   or
   - Click Next to define extensible attributes. For information, see Using Extensible Attributes on page 225.

**Modifying and Deleting DNAME Records**

When you modify a CNAME record, you can change the information you previously entered in the General tab. You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records on page 471.
Managing NAPTR Records

A NAPTR (Name Authority Pointer) record specifies a rule that uses a substitution expression to rewrite a string into a domain name or URI (Uniform Resource Identifier). A URI is either a URL (Uniform Resource Locator) or URN (Uniform Resource Name) that identifies a resource on the Internet.

NAPTR records are usually used to map E.164 numbers to URIs or IP addresses. An E.164 number is a telephone number, 1-555-123-4567 for example, in a format that begins with a country code, followed by a national destination code and a subscriber number. (E.164 is an international telephone numbering system recommended by the International Telecommunication Union.) Thus, NAPTR records allow us to use telephone numbers to reach devices, such as fax machines and VoIP phones, on the Internet.

To map an E.164 to a URI, the E.164 number must first be transformed into a domain name. ENUM (E.164 Number Mapping) specifies a method for converting E.164 numbers to domain names. For example, using the method specified by ENUM, the telephone number 1-555-123-4567 becomes the domain name 7.6.5.4.3.2.1.5.5.1.e164.arpa. For details about ENUM, refer to RFC 3761, The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM).

After the E.164 number is converted to a domain name, a DNS client can then perform a DNS lookup for the NAPTR records of the domain name. The following example illustrates how a DNS client processes NAPTR records.

In this example, the telephone number 1-555-123-4567 is converted to the domain name 7.6.5.4.3.2.1.5.5.1.e164.arpa. The DNS client then sends a query to the Infoblox DNS server for the NAPTR records associated with 7.6.5.4.3.2.1.5.5.1.e164.arpa. The Infoblox DNS server returns the following NAPTR record:

```plaintext
$ORIGIN 7.6.5.4.3.2.1.5.5.1.e164.arpa
IN NAPTR 10 100 "U" "sip + E2U" "$^.*$!sip:jdoe@corp100.com!" .
```

The DNS client then examines the fields in the NAPTR record as follows:

- If a DNS client receives multiple NAPTR records for a domain name, the value in the Order field determines which record is processed first. It processes the record with the lowest value first.

- The DNS client uses the Preference value when the Order values are the same. Similar to the Preference field in MX records, this value indicates which NAPTR record the DNS client should process first when the records have the same Order value. It processes the record with the lowest value first.

In the example, the DNS client ignores the Order and Preference values because it received only one NAPTR record.

- The Flag field indicates whether the current lookup is terminal; that is, the current NAPTR record is the last NAPTR record for the lookup. It also provides information about the next step in the lookup process. The flags that are currently used are:
  - U: Indicates that the output maps to a URI (Uniform Record Identifier).
  - S: Indicates that the output is a domain name that has at least one SRV record. The DNS client must then send a query for the SRV record of the resulting domain name.
  - A: Indicates that the output is a domain name that has at least one A or AAAA record. The DNS client must then send a query for the A or AAAA record of the resulting domain name.
  - P: Indicates that the protocol specified in the Service field defines the next step or phase.

If the Flag field is blank, this indicates that the client must use the resulting domain name to look up other NAPTR records.

- The Service field specifies the service and protocol that are used to communicate with the host at the domain name. In the example, the service field specifies that SIP (Session Initiation Protocol) is used to contact the telephone service.
The regular expression specifies the substitution expression that is applied to the original string of the client. In the example, the regular expression `!^.*$!sip:jdoe@corp100.com!` specifies that the domain name `7.6.5.4.3.2.1.5.5.5.1.e164.arpa` is replaced with `sip:jdoe@corp100.com`.

The regular expression in a NAPTR record is always applied to the original string of the client. It must not be applied to a domain name that resulted from a previous NAPTR rewrite.

The Replacement field specifies the FQDN for the next lookup, if it was not specified in the regular expression.

Adding a NAPTR Record

To add a NAPTR record:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> Add NAPTR Record.
2. In the Add NAPTR Record wizard, complete the following fields:
   - **Domain:** If Grid Manager displays a zone name, enter the domain name to which this resource record refers. The displayed zone name can either be the last selected zone or the zone from which you are adding the NAPTR record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box, and then enter a domain name for the record. The name you enter is prefixed to the DNS zone name that is displayed, and the complete name becomes the FQDN (fully qualified domain name) of the record. For example, if the zone name displayed is corp100.com and you enter admin, then the FQDN becomes admin.corp100.com.
   - **DNS View:** Displays the DNS view of the selected zone.
   - **Service:** Specifies the service and protocol used to reach the domain name that results from applying the regular expression or replacement. You can enter a service or select a service from the list.
   - **Flags:** The flag indicates whether the resulting domain name is the endpoint URI or if it points to another record. Select one of the following:
     - **U:** Indicates that the output maps to a URI.
     - **S:** Indicates that the resulting domain name has at least one SRV record.
     - **A:** Indicates that the resulting domain name has at least one A or AAAA record.
     - **P:** Indicates that this record contains information specific to another application. Leave this blank to indicate that the DNS client must use the resulting domain name to look up other NAPTR records. You can use the NAPTR records as a series of rules that are used to construct a URI or domain name.
   - **Order:** Select an Integer from 10 to 100, or enter a value from 0 to 65535. This value indicates the order in which the NAPTR records must be processed. The record with the lowest value is processed first.
   - **Preference:** Select an Integer from 10 to 100, or enter a value from 0 to 65535. Similar to the Preference field in MX records, this value indicates which NAPTR record should be processed first when the records have the same Order value. The record with the lowest value is processed first.
   - **REGEX:** The regular expression that is used to rewrite the original string from the client into a domain name. RFC 2915 specifies the syntax of the regular expression. Note that the appliance validates the regular expression syntax between the first and second delimiter against the Python re module, which is not 100% compatible with POSIX Extended Regular Expression as specified in the RFC. For information about the Python re module, refer to [http://docs.python.org/release/2.5.1/lib/module-re.html](http://docs.python.org/release/2.5.1/lib/module-re.html).
   - **Replacement:** This specifies the domain name for the next lookup. The default is a dot (.), which indicates that the regular expression in the **REGEX** field provides the replacement value. Alternatively, you can enter the replacement value in FQDN format.
   - **Comment:** Optionally, enter a descriptive comment for this record.
   - **Disable:** Clear the check box to enable the record. Select the check box to disable it.
Managing Resource Records

3. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save & Edit**: Save the entry and continue with editing.
   - **Save & New**: Save the entry and create a new NAPTR record.

or

   - Click **Next** to define extensible attributes. For information, see *Using Extensible Attributes* on page 225.

Modifying, Disabling, and Deleting Host and Resource Records

You can modify, disable, or delete an existing host or DNS resource record. When physical repair or relocation of a network device occurs, you can disable a record instead of deleting it. When you disable a record, the NIOS appliance does not answer queries for it, nor does it include disabled records in zone transfers and zone imports. This avoids having to delete and then add the record again. When the changes to the physical device are complete, you can simply enable the host or resource record.

To modify or disable a host or resource record:

1. Use one of the following methods to retrieve the host or resource record:
   - Perform a global search.
   - Select it from a Smart Folder.
   - From the Data Management tab, select the DNS tab -> Zones tab -> dns_view -> zone -> host_record or resource_record.

2. Select the record you want to modify and click the Modify icon.

3. In the host or resource record editor, you can do the following:
   - In the **General** tab, you can change most of the information, except for the read-only fields, such as the DNS View and Host Name Policy. You can select the **Disable** check box to disable the record.
   - In the **TTL** tab, you can modify the TTL setting. The NIOS appliance also allows you to specify TTL settings for each record. If you do not specify a TTL for a record, the appliance applies the default TTL value of the zone to each record. For information, see *About Time To Live Settings* on page 480.
   - In the **Extensible Attributes** tab, you can modify the attributes. For information, see *Using Extensible Attributes* on page 225.
   - The **Permissions** tab displays if you logged in as a superuser. For information, see *About Administrative Permissions* on page 87.

4. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.

When you delete host and resource records, Grid Manager moves them to the Recycle Bin. You can use the Recycle Bin to store deleted DNS configuration objects and selectively restore objects to the active configuration at a later time. You can also permanently remove the objects from the Recycle Bin.

**Note:** You cannot delete automatically-generated records, such as NS records and SOA records.

To delete host and resource record:

1. Perform a global search to retrieve the record you want to delete.
   - From the Data Management tab, select the DNS tab, click the Zones tab -> dns_view -> zone -> host_record or resource_record.

2. Select the record and click the Delete icon.

3. When the confirmation dialog box displays, select **Yes**.
**About Shared Record Groups**

A shared record group is a set of resource records that you can add to multiple zones. You can create resource records in a group and share the group among multiple zones. The zones handle the shared resource records as any other resource record. You can include the following types of DNS resource records in a shared record group: A, SRV, MX, AAAA, and TXT.

Using shared record groups simplifies and expedites the administration of resource records. When you create or update a shared record, the appliance automatically updates it in all associated zones. In addition, shared resource records reduce the object count in the NIOS database; instead of creating the same record in multiple zones, you can use only one shared record. For example, for 10 zones and 500 records per zone, the object count decreases from 5278 objects to 781 objects.

*Figure 16.9* shows an example of how to create and use shared records.

In this example, there are two shared record groups. One group—group1—contains the A records ftp and printer1 and the MX record mx1, and the other group—group2—contains the A record web and the MX record mx2. The resource records in group1 are shared with the internal view zones sales.corp100.com and finance.corp100.com and the external view zone sales.corp100.com. The resource records in group2 are shared with the internal view zone marketing.corp100.com and the external view zones sales.corp100.com and marketing.corp100.com.

*Figure 16.9 Creating Shared Records*
Shared Records Guidelines

The following are guidelines for using shared records:

- You can include multiple shared A, AAAA, SRV, MX and TXT resource records in a group. You cannot include NS, CNAME, DNAME, PTR, host and bulk host records.
- You can add shared records to authoritative zones only. You cannot add shared records to forward zones, stub zones, or reverse mapping zones.
- Zones that contain shared records can also contain regular DNS records (not shared).
- When you change or delete a shared resource record, it changes the canonical source of the shared record and impacts all the zones that contain the record.
- You cannot copy shared records from a zone.
- You do not need to restart the appliance when you create, delete, or modify shared records.

Configuring Shared Record Groups

Before you can create shared resource records, you must first create the group to which they belong. The shared record group serves as a container for the shared resource records. The following are the tasks to configure a shared record group:

1. Create a shared record group and associate it with the appropriate zones. See Creating a Shared Record Group on page 473.
2. Create shared A, SRV, MX, AAAA, and TXT resource records, and add them into the shared record group. See Managing Shared Resource Records on page 475.

Creating a Shared Record Group

When you create a shared record group, the only requirement is that you give it a name. You can associate it with one or multiple zones when you first create the group or at a later time, by editing the shared record group. You can associate a shared record group with authoritative zones only. Associating the shared record group with a zone adds the shared records to the zone. The zone handles the shared records like any other resource records.

To create a shared record group:

1. From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> Add icon -> Group -> Add Shared Record Group.
2. In the Add Shared Record Group wizard, specify the following:
   - **Name**: Enter the name of the shared record group. It can be up to 64 characters long and can contain any combination of printable characters. You can change the shared record group name even after you create the group. It does not impact the shared records in the group.
   - **Host Name Policy**: Click **Override** to supersede the hostname restriction policy set at the zone level or click **Inherit** to use the zone policy. This sets the hostname policy for the shared records in the group. See Specifying Hostname Policies on page 499.
   - **Comment**: Optionally, enter additional information about the shared record group.
3. Select one of the following:
   - **Next**: Associate the shared record group with zones.
   - **Save & Close**: Save the entry and close the editor.
   - **Save & Edit**: Save the entry and continue editing.
   - **Save & New**: Save the entry and create a new shared record group.
4. To associate the shared record group with at least one zone, click the Add icon in the Associated Zones panel.
5. Select a zone and click the Select icon. You can add multiple zones.
6. Select one of the following:
   - **Next**: Define extensible attributes for the zone. For information, see *Using Extensible Attributes* on page 225. After you define extensible attributes, you can save it and add resource records. For information, see *Managing Shared Resource Records* on page 475.
   - **Save & Close**: Save the entry and close the editor.
   - **Save & Edit**: Save the entry and continue with editing.
   - **Save & New**: Save the entry and create a new shared record group.

### Viewing Shared Record Groups

You can view the configured shared record groups by navigating to the **Data Management** tab -> **DNS** tab -> **Shared Record Groups** tab. Grid Manager displays the following information about each shared record group:

- **Name**: The shared record group name.
- **Comment**: Comments that were entered for the shared record group.
- **Site**: Values that were entered for this pre-defined attribute.

You can do the following:

- List the shared resource records in a shared record group.
  - Click a shared record group name.
- Edit the properties of a DNS shared record group.
  - Click the check box beside a shared record group, and then click the **Edit icon**.
- Delete a shared record group.
  - Click the check box beside a shared record group, and then click the **Delete icon**. Note that you must remove the zone associations in a shared record group before you delete it.
- Export the list of shared record groups to a .csv file.
  - Click the **Export icon**.
- Print the list of shared record groups.
  - Click the **Print icon**.

### Editing a Shared Record Group

When you edit a shared record group, you can do the following:

1. Perform a global search to retrieve the shared record group you want to modify.
   or
   From the **Data Management** tab, select the **DNS** tab -> **Shared Record Groups** tab -> *shared_record_group* check box.
2. Click the **Edit icon**.
3. In the **Shared Record Group** editor, you can do the following:
   - In the **General** tab, you can change any of the information you entered when you created it, including its name. Changing the shared record group name does not impact the shared resource records in it.
   - In the **Associated Zones** tab, you can add and delete zones.
   - In the **Extensible Attributes** tab, you can modify the attributes. For information, see *Using Extensible Attributes* on page 225.
   - The **Permissions** tab displays if you logged in as a superuser. For information, see *About Administrative Permissions* on page 87.
4. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.
Deleting Shared Record Groups

Before you delete a shared record group, you must remove the zone associations in the group; otherwise, an error message appears when you delete.

To delete a shared record group, select:
1. Perform a global search to retrieve the shared record group you want to modify.
   or
   From the Data Management tab, select the DNS tab → Shared Record Groups tab → shared_record_group check box.
2. Click the Delete icon.
3. In the Delete Confirmation dialog box, click Yes.
Grid Manager moves the shared record group to the Recycle Bin. Use the Recycle Bin feature to recover a deleted shared record group and retrieve the deleted zones. For information, see Recycle Bin on page 47.

Managing Shared Resource Records

You can create shared A, AAAA, MX, SRV and TXT records. These resource records are similar to the non-shared resource records. The DNS server uses them to respond to queries in the same way as any other resource record. A shared resource record can belong to only one shared record group. This section describes how to add shared resource records to a group and how to modify and delete them. It includes the following sections:

- Creating Shared Records on page 475
- Viewing Shared Records on page 476
- Modifying Shared Records on page 477
- Deleting Shared Records on page 477

Creating Shared Records

After you create a shared record group, you can create its resource records.

To create a shared A, AAAA, MX, SRV or TXT record and add it to a group:
1. From the Data Management tab, select the DNS tab. Expand the Toolbar and click Add → Shared Record.
   or
   From the Data Management tab, select the DNS tab → Shared Record Groups tab → shared_record_group check box.
   Click the Add icon, and then click Shared Record.
2. Select one of the following:
   - Add Shared A Record
   - Add Shared AAAA Record
   - Add Shared MX Record
   - Add Shared SRV Record
   - Add Shared TXT Record
3. Enter information in the Add Shared Record wizard that displays. See the online Help or the following for information about each resource record:
   - For information about A records, see Managing A Records on page 452.
   - For information about AAAA records, see Managing AAAA Records on page 454.
   - For information about MX records, see Managing MX Records on page 456.
   - For information about SRV records, see Managing SRV Records on page 457.
   - For information about TXT records, see Managing TXT Records on page 459.
4. Select one of the following:
   — Click **Next** to define extensible attributes for the shared record. For information, see *Using Extensible Attributes* on page 225.
   — **Save & Close**: Save the entry and close the editor.
   — **Save & Edit**: Save the entry and continue with editing.
   — **Save & New**: Save the entry and create a new shared record.

### Viewing Shared Records

You can view the shared records in a group and in a zone. To edit the shared record properties, click the shared record name and select the Edit icon.

To view the shared records in a group:

- From the **Data Management** tab, select the **DNS** tab -> **Shared Record Groups** tab and select a shared record group.

To view the shared records in a zone:

- From the **Data Management** tab, select the **DNS** tab -> **Zones** tab and select a zone.

Grid Manager lists the following information about each shared record by default:

- **Name**: The shared record name.
- **Type**: Indicates the type of resource record, such as A, AAAA, MX, SRV or TXT records. Shared records are identified as *(Shared)*.
- **Data**: The data the shared resource record provides.
- **Comment**: Comments that were entered in the resource record.
- **Site**: Displays values that were entered for this pre-defined attribute.

You can display the following additional columns:

- **TTL**: The TTL value of the shared resource record.
- **Disabled**: Indicates whether the record is disabled.

You can do the following:

- **Edit the properties of a shared resource record.**
  — Select the shared resource record, and then click the Edit icon.

- **Delete a shared resource record.**
  — Select the shared resource record, and then click the Delete icon.

- **Export the list of shared resource records to a .csv file.**
  — Click the Export icon.

- **Print the list of shared resource records.**
  — Click the Print icon.
Modifying Shared Records

You can modify, disable, or delete any shared record. When physical repair or relocation of a network device occurs, you can disable a record instead of deleting it. This alleviates having to delete, and then add the shared record again. When the changes to the physical device are complete, you can simply enable the shared record.

To modify or disable a shared record:
1. Perform a global search to retrieve the host or resource record you want to modify.
   or
   From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> shared_record_group.
2. Select the shared record you want to modify and click the Modify icon.
3. In the General tab, you can change most of the information, except for the read-only fields, such as the Host Name Policy. You can also select the Disable check box to disable the record.
   — In the TTL tab, you can modify the TTL setting. For information, see About Time To Live Settings on page 480.
   — In the Extensible Attributes tab, you can modify the attributes. For information, see Using Extensible Attributes on page 225.
   — The Permissions tab displays if you logged in as a superuser. For information, see About Administrative Permissions on page 87.
4. Select one of the following:
   — Save & Close: Save the entry and close the editor.
   — Save: Save the entry and keep the editor open.

Deleting Shared Records

To delete shared resource records:
1. Perform a global search to retrieve the record you want to delete.
   or
   From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> shared_record_group.
2. Select the shared records and click the Delete icon.
3. When the confirmation dialog box displays, select Yes.
   Grid Manager moves the shared records to the Recycle Bin, from which you can restore or permanently delete the records.
**Configuration Example: Configuring Shared Records**

The following example shows you how to configure shared records. In this example, you do the following:

- Create a shared record group: **group1**.
- Associate it with three zones: **eng.com**, **sales.com**, and **marketing.com**.
- Create an A record **www** and an MX record **mx1**.

1. Create a shared record group called **group1** and associate it with **eng.com**, **sales.com**, and **marketing.com**.
   a. From the Data Management tab, select the DNS tab → Shared Record Groups tab → Add icon → Group → Add Shared Record Group.
   b. In the first step of the **Add Shared Record Group** wizard, specify the following:
      Group Name: Enter the name of the shared record group as **group1**.
   c. Click **Next**.
   d. Click the Add icon in the Associated Zones panel.
   e. Select **eng.com** from the list of zones and click the select icon. Do the same for the **sales.com**, and **marketing.com** zones.
   f. Click **Save & Close**.

2. Add an A record **www** into **group1**.
   a. Expand the Toolbar and click Add → Shared Record > Shared A Record.
   b. In the **Add Shared A Record** wizard, specify the following:
      Name: Enter **www**.
      Shared Record Group: Select **group1** from the drop-down list.
      IP Address: Enter the IP address **10.9.1.1**.
   c. Click **Save & Close**.

3. Add an MX record **mx1** into **group1**.
   a. Expand the Toolbar and click Add → Shared Record > Shared MX Record.
   b. In the **Add Shared MX Record** wizard, specify the following:
      Mail Destination: Enter **mx1**.
      Shared Record Group: Select **group1** from the drop-down list.
      Mail Exchanger: Enter **www.infoblox.com**.
      Preference: Enter **10**.
      Comment: Enter **mail exchanger record for shared record group1**.
   c. Click **Save & Close**.
Chapter 17 Configuring DNS Services

This chapter provides general information about DNS service properties. The topics in this chapter include:

- Configuring DNS Service Properties on page 480
  - About Time To Live Settings on page 480
  - Adding an Email Address to the SOA Record on page 481
  - Notifying External Secondary Servers on page 482
  - Specifying Port Settings for DNS on page 482
  - Specifying Minimal Responses on page 483
  - Starting and Stopping the DNS Service on page 484
- Using Forwarders on page 485
  - Specifying Forwarders on page 485
- Controlling DNS Queries on page 486
  - Specifying Queriers on page 486
- Enabling Recursive Queries on page 488
  - Enabling Recursion on page 488
  - Restricting Recursive Clients on page 489
  - Enabling NXDOMAIN Redirection on page 490
- Enabling Zone Transfers on page 491
  - Configure Zone Transfers on page 491
- About Root Name Servers on page 494
  - Specifying Root Name Servers on page 494
- About Sort Lists on page 495
  - Defining a Sort List on page 495
- Configuring a DNS Blackhole List on page 497
  - Defining a DNS Blackhole List on page 497
- Specifying Hostname Policies on page 499
  - Defining Grid Hostname Policies on page 499
  - Defining Hostname Restrictions on page 500
  - Obtaining a List of Invalid Record Names on page 500
Configuring DNS Service Properties

About Time To Live Settings
You can specify TTL (time to live) settings for Infoblox host records and resource records. TTL is the time that a name server is allowed to cache data. After the TTL expires, the name server is required to update the data. Setting a high TTL reduces network traffic, but also renders your cached data less current. Conversely, setting a low TTL renders more current cached data, but also increases the traffic on your network.

You can specify global TTL settings at the grid level, for individual zones, or resource records. When you configure TTL settings for auto-generated records, the following conditions apply:
- NS records that are auto-generated for delegated name servers use TTL settings from their delegated zones.
- Auto-generated glue A and AAAA records use TTL settings from a delegated zone if the name of the name server is below the delegation point and does not belong to an authoritative child zone.
- All other auto-generated NS, A, and AAAA records continue to use TTL settings from their parent zones.
- Auto-generated PTR records do not inherit TTL settings from delegated zones. They use TTL settings from their parent zones.

When you have an RRSET (resource record set) that contains different TTL settings for each record, Grid Manager displays the actual TTL values for these records. However, in DNS responses, the appliance takes the least of the values and returns that as the TTL setting for all resource records in the RRset.

Specifying TTL Settings for a Grid
To specify global TTL settings for resource records hosted by grid members:
1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
2. In the Basic tab of the General section of the Grid DNS Properties editor, modify the following values as necessary:
   - Refresh: This interval tells secondary servers how often to send a message to the primary server for a zone to check that their data is current, and retrieve fresh data if it is not. The default is three hours.
   - Retry: This interval tells secondary servers how long to wait before attempting to recontact the primary server after a connection failure between the two occurs. The default is one hour.
   - Expire: If the secondary fails to contact the primary for the specified interval, the secondary stops giving out answers about the zone because the zone data is too old to be useful. The default is 30 days.
   - Default TTL: Specifies how long name servers can cache the data. The default is eight hours.
   - Negative-caching TTL (Time to Live): Specifies how long name servers can cache negative responses, such as NXDOMAIN responses. The default is 15 minutes.
3. Select one of the following:
   - Save & Close: Save the entry and close the editor.
   - Save: Save the entry and keep the editor open.
Specifying TTL Settings for a Zone

To specify TTL settings for host and resource records in a zone:

1. From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view -> zone check box -> Edit icon.
2. In the Authoritative Zone editor, click Settings.
3. Click Override and complete the fields as described in the preceding section, Specifying TTL Settings for a Grid.

Specifying the TTL of a Host or Resource Record

To specify the TTL setting for an Infoblox host or resource record:

1. From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view -> zone -> resource_record.
2. The TTL tab of the resource record editor displays the TTL setting the resource record inherited from the grid or zone. Click Override and enter a value. The setting is in hours by default. You can change it to seconds, minutes, days or weeks.
3. Select one of the following:
   — Save & Close: Save the entry and close the editor.
   — Save: Save the entry and keep the editor open.

Adding an Email Address to the SOA Record

If the primary name server of a zone is a grid member, you can add an administrator email address to the SOA record to help people determine who to contact about this zone.

Adding an Email Address for SOA Records in the Grid

If all zones hosted by the grid members have the same administrator, you can add the email address once for the grid. The appliance then adds the email address to the RNAME field of the SOA records of the zones.

To add an email address to the SOA records at the grid level:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
2. In the General -> Basic tab of the Grid DNS Properties editor, enter the email address in the E-mail Address (for SOA RNAME field) field.
3. Select one of the following:
   — Save & Close: Save the entry and close the editor.
   — Save: Save the entry and keep the editor open.

Adding an Email Address for the Zone SOA Record

To add an email address to the SOA record of a zone:

1. From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view -> zone check box -> Edit icon.
2. In the Authoritative Zone editor, click Settings.
3. Click Override beside the Email address (for SOA RNAME field) field and enter the email address of the zone administrator.
4. Select one of the following:
   — Save & Close: Save the entry and close the editor.
   — Save: Save the entry and keep the editor open.
**Notifying External Secondary Servers**

Grid members can use database replication to maintain up-to-date zone data sets, so the secondary servers in the grid can keep their zone data synchronized even if the primary server fails. Any external secondary servers can fall out of sync, however, if they rely only on the primary server to send notify messages when there is new zone data. Therefore all authoritative name servers in a grid (all primary and secondary servers) send notify messages to external secondary servers by default. This ensures that an external secondary name server receives notify messages when its master is a secondary name server in a grid. However, it also increases the number of notify messages.

To specify whether secondary name servers in the grid are to send notify messages to external secondary name servers:

1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Grid DNS Properties**.
2. In the **Grid DNS Properties** editor, click **Toggle Advanced Mode**.
3. When the additional tabs appear, click the **Advanced** subtab of the **General** tab.
4. Complete the following:
   - **Enable grid secondaries to notify external secondaries**: This option is enabled by default.
   - **Notify Delay**: Specify the number of seconds that the grid secondary servers delays sending notification messages to the external secondaries. The default is five seconds.
5. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.

For the external secondary servers to accept notify messages from the secondary name servers in the grid and then request zone transfers from them, you must configure the external secondary servers to use the grid secondary servers as the source of the zone transfers. This ensures that the external secondary servers continue to receive notify messages, even if the primary server is unavailable.

**Specifying Port Settings for DNS**

When requesting zone transfers from the primary server, some secondary DNS servers use the source port number (the primary server used to send the notify message) as the destination port number in the zone transfer request. If the primary server uses a random source port number when sending the notify message—that the secondary server then uses as the destination port number when requesting a zone transfer—zone transfers can fail if there is an intervening firewall blocking traffic to the destination port number.

Specifying a source port number for recursive queries ensures that a firewall allows the response. If you do not specify a source port number, the NIOS appliance sends these messages from a random port number.

When performing recursive queries, the NIOS appliance uses a random source port number above 1024 by default. The queried server responds using the source port number in the query as the destination port number in its response. If there is an intervening firewall that does not perform stateful inspection and blocks incoming traffic to the destination port number, the recursive query fails.

You can specify a source port number for notify messages to ensure the firewall allows the zone transfer request from the secondary server to the primary server. If you do not specify a source port number, the NIOS appliance sends messages from a random port number above 1024.
Specifying Source Ports

To specify port numbers and settings for queries, notify messages and zone transfer requests:

1. From the Data Management tab, select the DNS tab and click the Members tab to member check box to Edit icon.
2. In the editor, click Toggle Advanced Mode.
3. When the additional tabs appear, click the Advanced subtab of the General tab.
4. You can change the port settings as follows:
   - **Listen on these additional IP addresses**: Specify the IP addresses of interfaces on which the member can listen for queries.
   - **Send queries from**: Select the source port of the queries that the grid member sends. The drop-down list also displays loopback addresses that were configured. You can select a loopback address as the source for queries.
   - **Send notify messages and zone transfer requests from**: Select the source port of the notify messages and zone transfer requests that the grid member sends.
   - **Notify Delay**: Specify the number of seconds that the grid secondary servers delays sending notification messages to the external secondaries. The default is five seconds.
5. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.

Specifying Static Source Ports

To specify static source ports:

1. **Grid**: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
   **Member**: From the Data Management tab, select the DNS tab and click the Members tab to member check box to Edit icon.
   To override an inherited property, click Override next to it and complete the appropriate fields.
2. Complete the following:
   - **Set static source UDP port for queries (not recommended)**: This is disabled by default. Select this check box to enable it and enter the UDP port number.
   - **Set static source UDP port for notify messages**: This is disabled by default. Select this check box to enable it and enter the UDP port number.
3. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.

Specifying Minimal Responses

A NIOS appliance returns a minimal amount of data in response to a query, by default. It includes records in the authority and additional data sections of its response only when required, such as in negative responses. This feature speeds up the DNS services provided by the appliance.

To disable returning minimal responses:

1. From the Data Management tab, select the DNS tab and click the Members tab to member check box to Edit icon.
2. In the Member DNS Configuration editor, click General to Basic tab.
3. Clear the **Return minimal responses** check box
4. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and continue editing.
Starting and Stopping the DNS Service

The DNS service is enabled by default on a NIOS appliance. You can disable the DNS service for any grid member. Be aware that disabling DNS service for a member removes the NS records from it. If you later re-enable DNS service for this member, the NS records are then restored.

To disable DNS service for a grid member:
1. From the Data Management tab, select the DNS tab and click the Members tab → member check box.
2. Expand the Toolbar and click Stop to disable the DNS service or click Start to enable it.
3. When the confirmation dialog displays, click Yes.
Using Forwarders

A forwarder is essentially a name server to which all other name servers first send queries that they cannot resolve locally. The forwarder then sends these queries to DNS servers that are external to the network, avoiding the need for the other name servers in your network to send queries off-site. A forwarder eventually builds up a cache of information, which it uses to resolve queries. This reduces Internet traffic over the network and decreases the response time to DNS clients. This is useful in organizations that need to minimize off-site traffic, such as a remote office with a slow connection to a company's network.

You can select any grid member to function as a forwarder. You must configure your firewall to allow that grid member to communicate with external DNS servers. You can also configure the NIOS appliance to send queries to one or more forwarders. You can define a list of forwarders for the entire grid or for each grid member.

Specifying Forwarders

To configure a grid or member to use forwarders:

1. **Grid**: From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Grid DNS Properties**.
   **Member**: From the **Data Management** tab, select the **DNS** tab and click the **Members** tab -> **member** check box -> **Edit** icon.
   To override an inherited property, click **Override** next to it and complete the appropriate fields.

2. Click the **Forwarders** tab.

3. Click the Add icon.

4. Enter an IP address in the text field.
   — To remove a forwarder, select the IP address from the Forwarders list, and then click the Delete icon.

5. To use only forwarders on your network (and not root servers), select the **Use Forwarders Only** check box.

6. Select one of the following:
   — **Save & Close**: Save the entry and close the editor.
   — **Save**: Save the entry and continue editing.
Controlling DNS Queries

By default, the NIOS appliance responds to DNS queries from any IP address. You can create a list of queriers to which the appliance is allowed to respond; restricting it to specific networks, IP addresses, and remote servers that present specified TSIG (transaction signature) keys. When using TSIG keys, it is important that the appliances and servers involved with the authentication procedure use NTP (Network Time Protocol) for their time settings (see Using NTP for Time Settings on page 205).

In addition, you can also configure the appliance to respond to recursive queries. A recursive query requires the appliance to return requested DNS data, or locate the data through queries to other servers. Recursion is disabled by default. If you enable this feature, you can also create a list of allowed recursive queriers. For information about allowing recursion, refer to Enabling Recursive Queries on page 488.

You can create a list of allowed queriers for the grid and for individual grid members.

Specifying Queriers

To configure a list of allowed queriers for the grid or for a member:

1. **Grid**: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties. **Member**: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.

   To override an inherited property, click **Override** next to it and complete the appropriate fields.

2. Click **Queries**.

3. Depending on the item that you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows:

   - **IPv4 Address**: In the Name field of the new row, enter the IP address of the remote querier. The Permission column displays Allow by default. To change it to Deny, click it to display the drop-down list and select Deny.
   - **IPv4 Network**: In the Add IPv4 Network panel, complete the following, and then click Add to add the network to the list:
     - Address: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.
     - Permission: Select Allow or Deny from the drop-down list.
   - **IPv6 Address**: In the Name field of the new row, enter the IPv6 address of the remote server. The Permission column displays Allow by default. To change it to Deny, click it to display the drop-down list and select Deny.
   - **IPv6 Network**: In the Add IPv6 Network panel, complete the following, and then click Add to add the network to the list:
     - Address: Enter an IPv6 network address and select the netmask from the drop-down list.
     - Permission: Select Allow or Deny from the drop-down list.
   - **TSIG Key**: In the Add TSIG Key panel, complete the following, and then click Add to add the TSIG key to the list:
     - Key name: Enter a meaningful name for the key, such as a zone name or the name of the remote name server. This name must match the name of the same TSIG key on other name servers.
     - Key Data: To use an existing TSIG key, type or paste the key in the Key field. Alternatively, you can select the type of key and create a new key. By default, Grid Manager creates a 512-bit key. You can select 256-bit key or 128-bit key. Click Generate Key Data to create the new key.
     - Any Address/Network: Select to allow or disallow queries from any IP address.
4. Optionally, you can:
   — Modify an item on the list by selecting it and clicking the Edit icon.
   — Remove an item from the list by selecting it and clicking the Delete icon.
   — Move an item up or down the list. Select it and drag it to its new position, or click the up or down arrow. The appliance applies permissions to the queriers in the order they are listed.

Select one of the following:
   — **Save & Close**: Save the entry and close the editor.
   — **Save**: Save the entry and keep the editor open.
Enabling Recursive Queries

You can enable the appliance to respond to recursive queries and create a list of allowed networks, IP addresses, and remote servers that present specified TSIG (transaction signature) keys. When using TSIG keys, it is important that the appliances and servers involved with the authentication procedure use NTP (Network Time Protocol) for their time settings (see Using NTP for Time Settings on page 205).

A recursive query requires the appliance to return requested DNS data, or locate the data through queries to other servers. When a NIOS appliance receives a query for DNS data it does not have and you have enabled recursive queries, it first sends a query to any specified forwarders. If a forwarder does not respond (and you have disabled the Use Forwarders Only option in the Forwarders tab of the Member DNS Properties editor), the appliance sends a non-recursive query to specified internal root servers. If no internal root servers are configured, the appliance sends a non-recursive query to the Internet root servers. For information on specifying root name servers, see About Root Name Servers on page 494.

You can enable recursion for a grid, individual grid members, and DNS views. For information about enabling recursion in a DNS view, see Configuring DNS Views on page 394.

Enabling Recursion

To enable recursion and create a list of recursive queriers:

1. **Grid**: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties. **Member**: From the Data Management tab, select the DNS tab -> Members tab -> member check box -> Edit icon. To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the editor, click Queries.

3. Click Allow recursion, and then click the Add icon.

4. Depending on the item that you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows:
   - **IPv4 Address**: In the Name field of the new row, enter the IP address of the remote querier. The Permission column displays Allow by default. To change it to Deny, click it to display the drop-down list and select Deny.
   - **IPv4 Network**: In the Add IPv4 Network panel, complete the following, and then click Add to add the network to the list:
     - **Address**: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.
     - **Permission**: Select Allow or Deny from the drop-down list.
   - **IPv6 Address**: In the Name field of the new row, enter the IPv6 address of the remote server. The Permission column displays Allow by default. To change it to Deny, click it to display the drop-down list and select Deny.
   - **IPv6 Network**: In the Add IPv6 Network panel, complete the following, and then click Add to add the network to the list:
     - **Address**: Enter an IPv6 network address and select the netmask from the drop-down list.
     - **Permission**: Select Allow or Deny from the drop-down list.
   - **TSIG Key**: In the Add TSIG Key panel, complete the following, and then click Add to add the TSIG key to the list:
     - **Key name**: Enter a meaningful name for the key, such as a zone name or the name of the remote name server. This name must match the name of the same TSIG key on other name servers.
     - **Key Data**: To use an existing TSIG key, type or paste the key in the Key field. Alternatively, you can select the type of key and create a new key. By default, Grid Manager creates a 512-bit key. You can select 256-bit key or 128-bit key. Click Generate Key Data to create the new key.
   - **Any Address/Network**: Select to allow or disallow recursive queries from any IP address.
5. Optionally, you can:
   — Modify an item on the list by selecting it and clicking the Edit icon.
   — Remove an item from the list by selecting it and clicking the Delete icon.
   — Move an item up or down the list. Select it and drag it to its new position, or click the up or down arrow. The appliance applies permissions to the recursive queriers in the order they are listed.

6. Select one of the following:
   — **Save & Close**: Save the entry and close the editor.
   — **Save**: Save the entry and keep the editor open.

### Restricting Recursive Clients

By default, the appliance is allowed to serve up to 1000 concurrent clients that send recursive queries. You can change this default according to your business needs.

1. From the **Data Management** tab, select the **DNS** tab and click the **Members** tab → **member** check box → **Edit** icon.
2. In the **Member DNS Properties** editor, click **Toggle Advanced Mode**.
3. When the additional tabs appear, click the **Advanced** subtab of the **Queries** tab.
4. Select the **Limit number of recursive clients to** option and enter a number.
5. Select one of the following:
   — **Save & Close**: Save the entry and close the editor.
   — **Save**: Save the entry and keep the editor open.
Enabling NXDOMAIN Redirection

When a recursive DNS server receives a recursive query for DNS data it does not have, it locates the data through queries to other servers. If the DNS server receives an NXDOMAIN response from an authoritative name server, it forwards the response to the DNS client that requested the data. An NXDOMAIN response contains a “Name Error” RCODE, signifying that the domain name referenced in the query does not exist. (For information, you can refer to RFC 1035, Domain Names — Implementation and Specification.) You can configure an Infoblox DNS server to forward a DNS response with a specified IP address to the DNS client, in place of the NXDOMAIN response. This allows you to redirect DNS clients who request data for nonexistent domain names to a specific IP address. In Figure 17.1, a DNS client opens a web browser and tries to access nosuch.domain.com, a nonexistent domain name. Instead of receiving a “page not found” response, the DNS client is directed to a predefined portal at 10.1.2.3.

**Figure 17.1 NXDOMAIN Redirection**

1. A DNS client sends its DNS resolver a query for nosuch.domain.com.
2. The resolver sends the DNS server a recursive query for the A record of nosuch.domain.com.
3. The DNS server locates an authoritative server for domain.com and sends it a query for the A record of nosuch.domain.com.
4. The authoritative server for domain.com sends back an NXDOMAIN response, indicating that nosuch.domain.com does not exist.
5. The DNS server takes the NXDOMAIN response and forwards an A record with IP address 10.1.2.3 to the resolver.
6. The resolver sends the IP address 10.1.2.3 to the DNS client, which accesses the portal at 10.1.2.3.

Infoblox DNS servers intercept and redirect NXDOMAIN responses for A records only. Queries for all other records in non-existent domain names are treated as normal NXDOMAIN responses.

When DNSSEC is enabled on the Infoblox DNS server, it does not redirect DNS clients that request DNSSEC data for a non-existent domain name. Instead, it returns an authenticated negative response in the form of an NSEC or NSEC3 RR. (For information about DNSSEC, see Chapter 19, DNSSEC, on page 523.) If DNSSEC is not enabled, the appliance ignores the request for DNSSEC data and redirects the clients.

You can enable NXDOMAIN redirection at the grid and member levels. You can override or disable the settings per member. This allows you to specify a different IP address for each grid member and to define members that do not provide redirection. This is useful when you want to define a set of “opt out” servers for DNS clients that do not want to be redirected. To enable NXDOMAIN redirection:

1. **Grid**: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties. **Member**: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon. To override an inherited property, click Override next to it and complete the appropriate fields.
2. If the Grid DNS Properties or Member DNS Properties editor is in basic mode, click Toggle Advanced Mode.
3. Click NXDOMAIN and complete the following:
   - **Enable Redirection (Recursive Members Only)**: Select this option to enable recursive DNS servers in the grid to send DNS responses with a specified IP address, instead of NXDOMAIN responses, to DNS clients who send queries for nonexistent domain names.
   - **Redirect to**: Specify the IP address that the DNS server includes in the response it sends in place of an NXDOMAIN response.
4. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.
Enabling Zone Transfers

A zone transfer is the process of sending zone data across a network from one name server to another. When the primary server detects a change to its zone data, it notifies the secondary servers. The secondary servers reply by checking to see if the serial number they have for the zone is as large as the serial number for the zone on the primary server. If not, the secondary servers request a zone transfer.

In addition to receiving zone change notifications, a secondary server periodically polls the primary server to see if their zone data is in sync. In response, the primary server can send a DNS message containing just the changed zone data, or the entire data set. The first type of transfer is known as an incremental zone transfer, or IXFR. The second type of transfer is known as a full zone transfer, or AXFR.

A NIOS appliance, acting as the primary name server for a zone, allows zone transfers to secondary name servers by default. This includes all servers listed in the NS records for that zone. (Secondary name servers in a grid, however, receive updated zone data via database replication by default, as explained later in this section.) You can also specify zone transfers to other name servers, such as when migrating zone data to a new server or to a management system. You can specify one or more destinations to which the local appliance sends zone transfers. You can also specify the security and format of the transfers.

By default, grid members automatically receive updated zone data via database replication (through an encrypted VPN tunnel). You can change the default behavior to allow grid members to use zone transfers instead of grid replication.

Keep in mind that a database replication updates zone data for both the active and passive nodes of an HA member. Therefore, if there is a failover, the new active node (the previous passive node) immediately begins serving zone data with fresh information. In the case of a zone transfer, the passive node does not receive zone data until after a failover, when it becomes an HA master. At that time, it performs a zone transfer. If there is a lot of zone data, the transfer can take up to several minutes, thereby causing a break in the availability of the new HA master.

If you have HA members as secondary servers, zone transfers can result in service interruption when there is a failover. Furthermore, if the primary server is down when the HA member fails over, the new active node cannot receive zone data until the primary server comes back online.

You can use TSIG (transaction signature) keys to authenticate zone transfer requests and replies. The same key name and key value must be on the primary and secondary name servers for TSIG-authenticated zone transfers to occur. When using TSIG, it is important that both appliances involved with the authentication procedure use NTP (Network Time Protocol) for their time settings (see Using NTP for Time Settings on page 205).

You can control zone transfers at the grid, member, and zone levels. This enables you to specify a different set of servers for a grid, member and zone, if necessary.

Configure Zone Transfers

To configure zone transfers, you identify the servers to which zone data is transferred and optionally, servers to which data must not be transferred. For example, you can allow transfers to a network, but not to a specific server in the network.

You can specify a different set of servers for each grid member. For example, if certain grid members are primary servers for a zone, then you can specify the secondary servers to which that member is allowed to transfer zones.

To configure zone transfer properties:

1. Grid: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties. Member: From the Data Management tab, select the DNS tab, click the Members tab -> member check box -> Edit icon.

   Zone: From the Data Management tab, select the DNS tab, click the Zones tab -> zone check box, and then click the Edit icon.

   To override an inherited property, click Override next to it and complete the appropriate fields.

2. Select the Zone Transfers -> Basic tab to specify the name servers for the zone transfers.
3. Depending on the item that you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows:

- **IPv4 Address:** In the Name field of the new row, enter the IP address of the remote name server. The Permission column displays Allow by default. To change it to Deny, click it to display the drop-down list and select Deny.

- **IPv4 Network:** In the Add IPv4 Network panel, complete the following, and then click Add to add the network to the list:
  - Address: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.
  - Permission: Select Allow or Deny from the drop-down list.

- **IPv6 Address:** In the Name field of the new row, enter the IPv6 address of the remote server. The Permission column displays Allow by default. To change it to Deny, click it to display the drop-down list and select Deny.

- **IPv6 Network:** In the Add IPv6 Network panel, complete the following, and then click Add to add the network to the list:
  - Address: Enter an IPv6 network address and select the netmask from the drop-down list.
  - Permission: Select Allow or Deny from the drop-down list.

- **TSIG Key:** In the Add TSIG Key panel, complete the following, and then click Add to add the TSIG key to the list:
  - Key name: Enter a meaningful name for the key, such as a zone name or the name of the remote name server with which the local server authenticates zone transfer requests and replies. This name must match the name of the same TSIG key on other name servers that use it to authenticate zone transfers with the local server.
  - Key Data: To use an existing TSIG key, type or paste the key in the Key field. Alternatively, you can select the type of key and create a new key. By default, Grid Manager creates a 512-bit key. You can select 256-bit key or 128-bit key. Click Generate Key Data to create the new key.

- **DNS One 2.x TSIG:** Select this when the other name server is a NIOS appliance running DNS One 2.x code.

- **Any Address/Network:** Select to allow or deny the local appliance to send zone transfers to any IP address.

4. Optionally, you can:

- Modify an item on the list by selecting it and clicking the Edit icon.
- Remove an item from the list by selecting it and clicking the Delete icon.
- Move an item up or down the list. Select it and drag it to its new position, or click the up or down arrow.

5. Select one of the following:

- **Save & Close:** Save the entry and close the editor.
- **Save:** Save the entry and keep the editor open.

### Specifying a Zone Transfer Format

The zone transfer format determines the BIND format for a zone transfer. This provides tracking capabilities for single or multiple transfers and their associated servers.

To specify a zone transfer format:

1. **Grid:** From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.

2. **Member:** From the Data Management tab, select the DNS tab, click the Members tab -> member check box -> Edit icon.

   To override an inherited property, click Override next to it and complete the appropriate fields.

3. When the additional tabs appear, click the Advanced subtab of the Zone Transfers tab to specify the zone transfer format.
4. Select one of the following options from the **Default Zone Transfer Format** drop-down menu:
   - **many-answers** (Secondaries run BIND 8/9): includes as many records as the packet size allows
   - **one-answer** (Secondaries run BIND 4): includes one record per packet

5. To exclude servers, click the Add icon in the **Zone Transfer Format Exceptions** table and enter the IP address of the server in the Addresses field.

6. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.
**About Root Name Servers**

Root name servers contain the root zone file which lists the names and IP addresses of the authoritative name servers for each top-level zone. When a root name server receives a query for a domain name, it provides at least the names and addresses of the name servers that are authoritative for the top-level zone of the domain name.

You can configure the NIOS appliance to use Internet root name servers or custom root name servers. If you enable recursive queries and the appliance receives a recursive query it cannot resolve locally, it queries specified forwarders (if any) and then queries any root name servers you configure. If you do not specify internal root name servers and the appliance can access the Internet, it queries the Internet root name servers.

You can specify root name servers for the grid, individual members, and user-defined DNS views. You can specify root name servers for all DNS views except the default view. The default view uses either the member level root name servers (if specified) or the grid level root name servers.

Every grid member has a default view. If you want to specify root name servers for a default view, override the grid root name server setting at the member level and the default view can use the member-level setting.

**Specifying Root Name Servers**

To specify root name servers for a grid, member, or DNS view:

1. **Grid**: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
   
   **Member**: From the Data Management tab, select the DNS tab, click the Members tab -> member check box -> Edit icon.
   
   **DNS View**: From the Data Management tab, select the DNS tab, click the Zones tab-> dns_view check box -> Edit icon.

   To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the Grid DNS Properties and Member DNS Properties editors, you must click Toggle Advanced Mode.

3. When the additional tabs appear, click Root Name Servers.

4. Select one of the following options:
   
   - **Use Internet root name servers**: This option is selected by default.
   
   - **Use custom root name servers**: Click the Add icon and enter the following information when a new row appears:
     
     - **Name**: Enter a name for the root name server.
     
     - **Address**: Enter the IP address of the root name server.

5. Optionally, you can:
   
   - Select a server from the list and click the Edit icon, to modify its information.
   
   - Select a server from the list and click the Delete icon.

6. Select one of the following:
   
   - **Save & Close**: Save the entry and close the editor.
   
   - **Save**: Save the entry and continue editing.
About Sort Lists

A sort list prioritizes A and AAAA records on certain networks when those records are included in responses, sorting them to the beginning of the list in the response. For example, you can define a sort list when a server has two interfaces and you want the DNS clients to prefer one interface because it has a faster link.

When you define a sort list on the NIOS appliance, you specify the following:

- The IP address or network of the source of the query
- The IP addresses or networks that the appliance lists first in its response when it receives a query from the corresponding source address

When the NIOS appliance receives a query from the specified IP address or network and the DNS lookup produces a response with multiple addresses, the NIOS appliance sorts the addresses so that those in the sort list are at the beginning of its response.

Defining a Sort List

To define a sort list for a grid or member:

1. **Grid**: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
   **Member**: From the Data Management tab, select the DNS tab -> Members tab -> member check box -> Edit icon.

   To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the editor, click Toggle Advanced Mode.

3. When the additional tabs appear, click Sort List.

4. Click the Add icon and select either Any to define a sort list for any address and network, or Address/Network to define a sort list for a particular source IP address or network.

5. Do the following in the new row:
   - If you selected Address/Network, enter the IP address or network of the source of the query.
   - Click the Add icon beside the source IP address to add the preferred IP addresses or networks for the source. You can add as many IP addresses as necessary. When you add multiple IP addresses, you can change the order of the IP addresses. Select an IP address and drag it to its new position, or click the up or down arrow, as show in Figure 17.2.

![Figure 17.2 Sort List](image)

---

**Click this Add icon to enter a new source IP address.**

**Click + to enter the preferred IP address or network for the specified source address. Click - to remove an address from the list.**

**Click the arrow to move an address up or down on the list.**

---

**Click to expand/hide the sort list of each source address.**
6. To add another source IP address or network, click the Add icon again. You can create a separate sort list for each source IP address or network.

7. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and continue editing.
Configuring a DNS Blackhole List

The DNS blackhole feature provides the ability to specify IP and network addresses of network devices that you want to exclude from the DNS resolution process. The DNS blackhole feature is disabled by default. When enabled, the NIOS appliance does not accept queries from IP addresses in the blackhole list and does not use them to resolve queries. For example, you can add the IP addresses of name servers that are using DNS incorrectly to prevent the NIOS appliance from accepting their queries and from using them as resolvers. You can also use this feature to fix temporary network issues. For example, you can add the IP addresses of delegated servers, configured forwarders, and DHCP servers that have temporary DNS-related issues.

You can create a DNS blackhole list for the entire grid or create a separate list for each grid member. For example, if one of your grid members is behind a firewall, you might need to configure a different DNS blackhole list for this member because the clients that can access it might be mapped differently.

The appliance accepts queries from addresses and networks that are not in the blackhole list and uses the addresses and networks that are excluded from the blackhole list as resolvers. To add an IP address to the blackhole list, enter it and set its permission to “Allow”. Note that adding an IP address to the blackhole list and setting its permission to “Deny” excludes that address from the blackhole list, effectively allowing the NIOS appliance to respond to queries from that address and to use it as a resolver.

When you add a network to a DNS blackhole list, all the IP addresses in the network are excluded from the DNS resolution process. If you want to allow some IP addresses within the network, add these addresses to the list and set their permission to “Deny.” Ensure that you list these IP addresses before the network address because the appliance applies permissions to the addresses in the order they are listed. For example, when you add the network 10.10.0.0/24 to a DNS blackhole list, all 256 IP addresses in the network are put on the blackhole list. To allow DNS traffic to the IP addresses 10.10.0.55 and 10.10.0.88, add these two addresses before the network address in the DNS blackhole list, and then set their permissions to “Deny.”

Defining a DNS Blackhole List

To enable the DNS blackhole feature and configure a DNS blackhole list for a grid or member:

1. **Grid:** From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
   **Member:** From the Data Management tab, select the DNS tab, click the Members tab -> member check box -> Edit icon.
   To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the editor, click Toggle Advanced Mode.
3. When the additional tabs appear, click DNS Blackhole.
4. Select the Enable Blackhole check box to enable the DNS blackhole feature. It is disabled by default.
5. Click the Add icon to add IP addresses to the DNS blackhole list.
6. Depending on the item that you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows:
   - **IPv4 Address:** In the Name field of the new row, enter an IPv4 address. The Permission column displays Allow by default, which adds the address to the blackhole list. To change it to Deny, click it to display the drop-down list and select Deny.
   - **IPv4 Network:** In the Add IPv4 Network panel, complete the following, and then click Add to add the network to the list:
     - **Address:** Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.
     - **Permission:** Select Allow or Deny from the drop-down list.
   - **IPv6 Address:** In the Name field of the new row, enter an IPv6 address. The Permission column displays Allow by default, which adds the address to the blackhole list. To change it to Deny, click it to display the drop-down list and select Deny.
— **IPv6 Network**: In the **Add IPv6 Network** panel, complete the following, and then click **Add** to add the network to the list:
  — **Address**: Enter an IPv6 network address and select the netmask from the drop-down list.
  — **Permission**: Select **Allow** or **Deny** from the drop-down list.
  — **Any Address/Network**: Select to allow or deny DNS traffic to and from any IP address.

7. Optionally, you can:
   — Modify an item on the list by selecting it and clicking the **Edit** icon.
   — Remove an item from the list by selecting it and clicking the **Delete** icon.
   — Move an item up or down the list. Select it and drag it to its new position, or click the up or down arrow.

8. Select one of the following:
   — **Save & Close**: Save the entry and close the editor.
   — **Save**: Save the entry and keep the editor open.
Specifying Hostname Policies

You can enforce a naming policy for the hostnames of A, AAAA, Host, MX, NS, and bulk host records based on user-defined or default patterns. For MX and NS records, the hostname restrictions apply to the text in the RDATA field (right-hand side) of the resource record name.

Records that you created before you enabled the hostname checking policy need not comply with the hostname restriction that you specify.

You can select one of three preconfigured policies or define your own host naming policy with a POSIX regular expression. The policies Infoblox provides implement standard host naming restrictions according to RFC 952, DOD Internet Host Table Specification, and RFC 1123, Requirements for Internet Hosts -- Application and Support.

**Note:** The hostname restriction limits the hostname of A, AAAA, Host, MX, NS, and bulk host records only.

You can define your own hostname restriction policy at the grid level only. At the member and zone levels, you can select a predefined policy or a policy that was defined at the grid level.

Defining Grid Hostname Policies

You can define new hostname policies and set the hostname policy for all zones in the grid as follows:

1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Grid DNS Properties**.
2. In the **Grid DNS Properties** editor, click **Toggle Advanced Mode**.
3. When the additional tabs appear, click **Host Naming**.
   - The Host Name Policies section lists the following preconfigured record policies:
     - **Strict Hostname Checking**: You can only use hostnames that contain alphanumeric characters and dashes (“-”).
     - **Allow Underscore**: You can only use hostnames with alphanumeric characters, dashes, and underscores (“-” and “_”). This is the default.
     - **Allow Any**: You can use any hostname.
     Select **Default** from the drop-down list in the Default column to change the grid default hostname policy.
4. Click **Add** to define your own hostname checking policy.
5. Enter a record policy name and a regular expression string, and click **OK**. See Appendix B, “Regular Expressions”, on page 833 for definitions of regular expressions.
   - Note that Grid Manager does not validate the regular expressions that you enter. Therefore, you can inadvertently specify an invalid regular expression that might cause noncompliance errors when you create records.
6. If you select the **Strict Hostname Checking** policy, the **Apply policy to dynamic updates and inbound zone transfers (requires Strict Hostname Checking setting)** option is enabled by default. It enables the appliance to apply the policy to dynamic DNS updates and zone transfers that it receives. You can then select which action the appliance takes when it encounters names that do not conform to the policy. Select either **Fail** or **Warn**. If you select **Warn**, the appliance allows the dynamic DNS update or zone transfer, but logs a syslog message.
7. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and continue editing.
After you specify a hostname restriction policy, if you create a record name that does not comply with this policy and try to save it, an error message appears.
Defining Hostname Restrictions

You can select a hostname restriction policy for an individual grid member or zone. You can specify hostname restrictions for authoritative forward-mapping zones only. You cannot specify hostname restrictions for forward zones, stub zones, IPv4 reverse-mapping zones, and IPv6 reverse mapping zones.

To select a hostname restriction policy for a grid member or zone:

1. **Member:** From the Data Management tab, select the DNS tab, click the Members tab → member check box → Edit icon.
   - **Zone:** From the Data Management tab, select the DNS tab and click the Zones tab→ dns_view→ zone check box → Edit icon.
   - To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the **Member DNS Properties** editor, click **Toggle Advanced Mode.**

3. When the additional tabs appear, click **Host Naming.**

4. Click **Override.**

5. From the **Host Name Policy** drop-down list, select a predefined policy or a policy that was defined at the grid level.

6. If you select the Strict Hostname Checking policy, the **Apply policy to dynamic updates and inbound zone transfers (requires Strict Hostname Checking setting)** is enabled by default. It enables the appliance to apply the policy to dynamic DNS updates and zone transfers that it receives. You can then select which action the appliance takes when it encounters names that do not conform to the policy. Select either **Fail** or **Warn.** If you select **Warn,** the appliance allows the dynamic DNS update or zone transfer, but logs a syslog message.

7. Select one of the following:
   - **Save & Close:** Save the entry and close the editor.
   - **Save:** Save the entry and continue editing.

Obtaining a List of Invalid Record Names

You can retrieve a list of all record names that do not comply with the current hostname checking policy of a zone. These could be records that were created before the current host naming policy was set. In addition, if you selected the Strict Hostname Checking policy and allowed illegal hostnames in DDNS updates and inbound zone transfers with a warning, those records are listed in this report as well.

To display the Hostname Compliance report:

1. From the Data Management tab, select the DNS tab and click the Zones tab→ dns_view→ zone check box.

2. Click **Hostname Compliance.**
   - The Hostname Compliance Report for the zone displays. It lists the record name, type, value, and comment for all records that do not comply with the hostname restriction policy of the zone.

From the report, you can select a record and do the following:

- Click the Edit icon to open the record editor.
- Click the Delete icon to move it to the Recycle Bin.
Chapter 18 Configuring DDNS Updates from DHCP

DDNS (Dynamic DNS) is a method to update DNS data (A, TXT, and PTR records) from sources such as DHCP servers and other systems that support DDNS updates (for example, Windows 2000, 2003, and XP). This chapter provides conceptual information about DDNS and explains how to configure NIOS appliances running DHCP and DNS to support DDNS updates. It contains the following main sections:

- **Understanding DDNS Updates from DHCP** on page 502
- **Configuring DHCP for DDNS** on page 505
  - Enabling DDNS and Specifying a Domain Name on page 506
  - Sending Updates to DNS Servers on page 507
- **Configuring DDNS Features** on page 509
  - Resending DDNS Updates on page 509
  - Generating Host Names for DDNS Updates on page 509
  - Updating DNS for Clients with Fixed Addresses on page 509
  - About the Client FQDN Option (Option 81) on page 509
  - Configuring DDNS Features on page 511
  - Configuring DDNS Update Verification on page 512
- **Configuring DNS Servers for DDNS** on page 515
  - Enabling a DNS Server to Accept DDNS Updates on page 515
  - Forwarding Updates on page 516
- **Supporting Active Directory** on page 518
  - Sending DDNS Updates to a DNS Server on page 518
- **About GSS-TSIG** on page 519
  - Sending Secure DDNS Updates to a DNS Server in the Same Domain on page 520
  - Configuring DHCP to Send GSS-TSIG Updates in the Same Domain on page 522
  - Sending Secure DDNS Updates to a DNS Server in Another Domain on page 529
  - Configuring DHCP to Send GSS-TSIG Updates to Another Domain on page 530
  - Sending GSS-TSIG Updates to a DNS Server in Another Forest on page 532
- **Accepting DDNS Updates from DHCP Clients** on page 533
  - Supporting Active Directory and Unauthenticated DDNS Updates on page 533
- **Accepting GSS-TSIG-Authenticated Updates** on page 535
  - Configuring DNS to Receive GSS-TSIG Updates on page 537
UNDERSTANDING DDNS UPDATES FROM DHCP

DHCP supports several DNS-related options (such as options 12, 15, and 81). With DDNS (Dynamic DNS) updates, a DHCP server or client can use the information in these options to inform a DNS server of dynamic domain name-to-IP address assignments.

To set up one or more NIOS appliances for DDNS updates originating from DHCP, you must configure at least one DHCP server and one DNS server. These servers might be on the same appliance or on separate appliances. Three possible arrangements for a DHCP server to update a DNS server are shown in Figure 18.1.

*Figure 18.1 Relationship of DHCP and DNS Servers for DDNS Updates*
Here is a closer look at one setup for performing DDNS updates from a DHCP server (the steps relate to Figure 18.2):

1. When a DHCP client requests an IP address, the client sends its host name (DHCP option 12). The client also includes its MAC address in the ethernet frame header.

2. a. When the DHCP server responds with an IP address, it usually provides a domain name (DHCP option 15). The combined host name (from the client) and domain name (from the server) form an FQDN (fully qualified domain name), which the NIOS appliance associates with the IP address in the DHCP lease.

   b. The DHCP server sends the A, TXT, and PTR records of the DHCP client to the primary DNS server to update its resource records with the dynamically associated FQDN + IP address.

3. The primary DNS server notifies its secondary servers of a change. The secondary servers confirm the need for a zone transfer, and the primary server sends the updated zone data to the secondary server, completing the update.

Note: For information about zone transfers, see Enabling Zone Transfers on page 491.

Figure 18.2 DDNS Update from a DHCP Server

Update for forward-mapping zone corp100.com
A record: jsmith-xp 10.1.2.90
TXT record: jsmith-xp
"31995a5ea0681ee5d2f6e06ad0d0477e84"

Update for reverse-mapping zone
2.1.10.in-addr.arpa
PTR record: 90 - jsmith-xp.corp100.com

When the update reaches the primary server, it updates its zone data, increases the corp100.com zone serial number, and sends a NOTIFY to ns2.

When the secondary server receives the NOTIFY, it checks if ns1 has a higher serial number for corp100.com.

Because the corp100.com serial number on ns1 is higher, ns2 requests an incremental zone transfer (IXFR).

ns1 sends the changed zone data to ns2.
To enable a DHCP server to send DDNS updates to a DNS server, you must configure both servers to support the updates. First, configure the DHCP server to do the following:

- Provide what is needed to create an FQDN: add a server-generated host name to a server-provided domain name, add a server-provided domain name to a client-supplied host name, or permit the client to provide its own FQDN
- Send updates to a DNS server

Then, configure the following on the DNS server:

- Accept updates from the DHCP server, a secondary DNS server, or a DHCP client
- If the DHCP server sends updates to a secondary DNS server, configure the secondary server to forward updates to the primary DNS server

When setting up DDNS, you can determine the amount of information that DHCP clients provide to a DHCP server—and vice versa—and where the DDNS updates originate. A summary of these options is shown in Figure 18.3.

Figure 18.3  DHCP Clients and Server Providing DNS Information and Updates
You can configure the DHCP and DNS settings for DDNS at the grid level, member level, and network and zone level. By applying the inheritance model in the NIOS appliance, settings made at the grid level apply to all members in the grid. Settings you make at the member level apply to all networks and zones configured on that member. Settings made at the network and zone level apply specifically to just that network and zone. When configuring independent appliances (that is, appliances that are not in a grid), do not use the member-level settings. Instead, configure DDNS updates at the grid level to apply to all zones and, if necessary, override the grid-level settings on a per zone basis.

**Configuring DHCP for DDNS**

To configure the DHCP server to send DDNS updates to DNS servers in the grid, you must perform the following tasks:

- Enable DDNS updates and optionally specify the domain name that the DHCP server provides to DHCP clients for DDNS updates. For information, see *Enabling DDNS and Specifying a Domain Name* on page 506.
- Identify the DNS view to which the DHCP server sends DDNS updates. For information, see *Sending Updates to DNS Servers in the Grid* on page 507.

To configure the DHCP server to send DDNS updates for clients using option 81, you must perform the following tasks:

- Enable DDNS updates. For information, see *Enabling DDNS and Specifying a Domain Name* on page 506.
- Enable support for option 81 and configure how the DHCP server updates DNS. For information, see *Configuring DDNS Features* on page 511.
- Identify the zones to which the DHCP server sends DDNS updates for clients using option 81. For information, see *Sending Updates for DHCP Clients Using Option 81* on page 507.

To configure the DHCP server to send DDNS updates to external DNS servers, you must perform the following tasks:

- Enable DDNS updates. For information, see *Enabling DDNS and Specifying a Domain Name* on page 506.
- Identify the external DNS servers to which the DHCP server sends DDNS updates. For information, see *Sending Updates for Zones on an External Name Server* on page 508.

You can also enable additional features for DDNS updates. For information, see *Configuring DDNS Features* on page 509.

**Note:** Whether you deploy NIOS appliance in a grid or independently, they send updates to UDP port 53. Grid members do not send updates through a VPN tunnel; however, grid members do authenticate updates between each other using TSIG (transaction signatures) based on an internal TSIG key.
Enabling DDNS and Specifying a Domain Name

You can enable DDNS for a grid, member, shared network, network, address range, DHCP template, fixed address, and roaming host.

Before a DHCP server can update DNS, the DHCP server needs to have an FQDN-to-IP address mapping. When a DHCP client requests an IP address, it typically includes its host name in option 12 of the DHCPDISCOVER packet. You can configure the NIOS appliance to include a domain name in option 15 when it responds with a DHCPOFFER packet. You specify this domain name in the **DHCP Options Basic** tab of the Grid DHCP Configuration editor and the **Member DHCP Configuration** editor, and in the **DHCP** tab of the Network, DHCP Range and Fixed Address editors.

In addition, if you want to specify a different domain name that the appliance uses specifically for DDNS updates, you can do so for networks, address ranges, and fixed addresses, DHCP templates, and roaming hosts. The appliance combines the hostname from the client and the domain name you specify to create the FQDN that it uses to update DNS. You can also use the name of a roaming host record as the name of the client for DDNS updates.

To enable DDNS and specify a DDNS domain name:

1. **Grid:** From the Data Management tab, select the DHCP tab, expand the Toolbar and click **Grid DHCP Properties**.
   - **Member:** From the Data Management tab, select the DHCP tab and click the **Members** tab -> **Members** -> **member** check box -> Edit icon.
   - **Network:** From the Data Management tab, select the DHCP tab and click the **Networks** tab -> **Networks** -> **network** check box -> Edit icon.
   - **Address Range:** From the Data Management tab, select the DHCP tab and click the **Networks** tab -> **Networks** -> **network** -> **addr_range** check box -> Edit icon.
   - **Fixed Address:** From the Data Management tab, select the DHCP tab and click the **Networks** tab -> **Networks** -> **network** -> **ip_addr** check box -> Edit icon.
   - **Roaming Host:** From the Data Management tab, select the DHCP tab and click the **Networks** tab -> **Roaming Hosts** -> **roaming_host** -> Edit icon.
   - **Network/Address Range/Fixed Address Template:** From the Data Management tab, select the DHCP tab and click the **Templates** tab -> **DHCP_template** check box -> Edit icon.
   
   To override an inherited property, click **Override** next to it and complete the appropriate fields.

2. In the **DDNS** -> **Basic** tab, complete the following:
   - **Enable DDNS Updates:** Select this check box to enable DDNS updates.
   - **DDNS Update TTL:** You can set the TTL used for A and PTR records updated by the DHCP server. The default is shown as zero. If you do not enter a value here, the appliance by default sets the TTL to half of the DHCP lease time with a maximum of 3600 seconds. For example, a lease time of 1800 seconds results in a TTL of 900 seconds, and a lease time of 86400 seconds results in a TTL of 3600 seconds. For information about how to set the lease time, see **Configuring DHCP Lease Times** on page 621.
   - **DDNS domain name:** Specify the domain name of the network that the appliance uses to update DNS. This is available for networks, address ranges, and fixed addresses, DHCP templates, and roaming hosts only.
   - **DDNS Hostname:** Select **Override client provided hostname with roaming hostname** to use the name of the roaming host record as the name of the client for DDNS updates. This is available for roaming hosts only.
   - **Update DNS on DHCP Lease Renewal:** Select this check box to enable the appliance to update DNS when a DHCP lease is renewed.

3. Select one of the following:
   - **Save & Close:** Save the entry and close the editor.
   - **Save:** Save the entry and keep the editor open.
**Sending Updates to DNS Servers**

The DHCP server can send DDNS updates to DNS servers in the same grid and to external DNS servers. When you enable the appliance to send updates to grid members, you must specify the DNS view to be updated. If a network view has multiple DNS views, you can select only one DNS view for DDNS updates. For information about DNS views, see *Using Infoblox DNS Views* on page 392.

When you enable DDNS updates for a grid, member, shared network, network, address range, DHCP template, fixed address, or roaming host, the DHCP server sends updates to authoritative zones using the domain name (as DHCP option 15) you define in the DHCP properties. You can also define forward-mapping zones that receive DDNS updates for DHCP clients that use option 81 to define the domain name. For information, see *About the Client FQDN Option (Option 81)* on page 509. To allow DDNS updates for clients using option 81, you must first enable the support for option 81. For information, see *Configuring DDNS Features* on page 509.

**Sending Updates to DNS Servers in the Grid**

You must specify the DNS view to be updated for each network view.

To configure the DHCP server to send updates to DNS servers in the same grid:

1. If there are multiple network views in the grid, select a network view.
2. From the **Data Management** tab, select the **DHCP** tab, and then click **Configure DDNS** from the Toolbar.
3. In the **DDNS Properties** editor, complete the following:
   - **DNS View**: If a network view has more than one DNS view, this field lists the associated DNS views. From the drop-down list, select the DNS view to which the DHCP server sends DDNS updates. Otherwise, the appliance uses the default DNS view.
4. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.

   The appliance sends DDNS updates to the appropriate zones in the selected DNS view. Note that you cannot delete a DNS view that has been selected for DDNS updates. By default, the DHCP server sends DDNS updates to zones using the domain name that you define for DHCP objects, such as networks and DHCP ranges.

**Sending Updates for DHCP Clients Using Option 81**

You must specify the DNS view to be updated for each network view.

To send updates to zones for DHCP clients using option 81:

1. If there are multiple network views in the grid, select a network view.
2. From the **Data Management** tab, select the **DHCP** tab, and then click **Configure DDNS** from the Toolbar.
3. In the **DDNS Properties** editor, complete the following:
   - **DNS View**: If a network view has more than one DNS view, this field lists the associated DNS views. From the drop-down list, select the DNS view to which the DHCP server sends DDNS updates. Otherwise, the appliance uses the default DNS view.
   - **Zones to update for Option 81 Hosts**: In this section, you can define forward-mapping zones to which the DHCP server sends DDNS updates for DHCP clients that use option 81. You must first enable the support for option 81 before the DHCP server can send DDNS updates to these zones. By default, the DHCP server sends DDNS updates to zones using the domain name that you define for DHCP objects, such as networks and DHCP ranges. For clients using option 81, the DHCP server uses the domain name defined in the option.

   Click the Add icon to specify a forward-mapping zone. Note that the Forward-mapping Zone Selector dialog box displays only the DNS zones that are associated with the selected DNS view. The zones you select here are written to the dhcpd.conf file as "zone" statements with the matching TSIG key of the DNS view, so the updates are sent to the correct DNS view.
4. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.

### Sending Updates for Zones on an External Name Server

The DHCP server can send dynamic updates to an external name server that you specify. For each network view, you can specify the zone to be updated and the IP address of the primary name server for that zone. You can add information for a forward and reverse zone. The DHCP server updates the A record in the forward zone and the PTR record in the reverse zone.

You can also use TSIG (transaction signatures) or GSS-TSIG to secure communications between the servers. TSIG uses the MD5 (Message Digest 5) algorithm and a shared secret key to create an HMAC (hashed message authentication code)—sometimes called a digital fingerprint—of each update. Both the DHCP server sending the update and the DNS server receiving it must share the same secret key. Also, it is important that the time stamps on the TSIG-authenticated updates and update responses be synchronized, or the participants reject them. Therefore, use an NTP server to set the time on all systems involved in TSIG authentication operations.

To send updates to a DNS server that is external to your grid:

1. If there are multiple network views in the grid, select a network view.
2. From the **Data Management** tab, select the **DHCP** tab, expand the Toolbar and click **Configure DDNS**.
3. In the **DDNS Updates to External Zones** section of the **DDNS Properties** editor, click the Add icon. Complete the following fields in the Add External DDNS Zone panel, and then click **Add**:
   - **Zone Name**: Enter the FQDN of a valid forward-mapping or reverse-mapping zone to which the DHCP server sends the updates. Do not enter the zone name in CIDR format.
   - **DNS Server Address**: Enter the IP address of the primary name server for that zone.
   - **Security**: Select one of the following security methods:
     - **None**: Select this to use unsecured DDNS updates. This is the default.
     - **TSIG**: Select this to use the standards-based TSIG key that uses the one-way hash function MD5 to secure transfers between name servers. You can either specify an existing key or generate a new key. To specify an existing key, complete the following:
       - **Key Name**: Enter the TSIG key name. The key name entered here must match the TSIG key name on the external name server.
       - **Key String**: Type or paste the key.
       To generate a new key, select the type of key from the **Key Length** drop-down menu. By default, Grid Manager creates a 512-bit key. You can select a 256-bit key or 128-bit key. Click **Generate Key**.
     - **GSS-TSIG**: For information about using GSS-TSIG, see **About GSS-TSIG** on page 519.
4. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.
**Configuring DDNS Features**

You can enable the DHCP server to support certain DDNS features. These features affect the behavior of the DHCP server and how it handles DDNS updates. The following sections describe the different features you can set. For information about how to configure these features, see *Configuring DDNS Features* on page 511.

**Resending DDNS Updates**

You can enable the DHCP server to make repeated attempts to send DDNS updates to a DNS server. The DHCP server asynchronously updates DNS for a particular lease and sends the DHCP ACK to the client requesting the lease. If the update fails, the DHCP server still provides the lease and sends the DHCP ACK to the client. The DHCP server then continues to send the updates until it is successful or the lease of the client expires. You can change the default retry interval, which is five minutes. For information, see *Configuring DDNS Features* on page 509.

You can enable this feature for the grid and for individual grid members.

**Generating Host Names for DDNS Updates**

Some clients do not send a host name with their DHCP requests. When the DHCP server receives such a request, its default behavior is to provide a lease but not update DNS. You can configure the DHCP server to generate a host name and update DNS with this host name when it receives a DHCP REQUEST message that does not include a host name. It generates a name in the following format: `DHCP-WWW-XXX-YYY-ZZZ`, where `WWW-XXX-YYY-ZZZ` is the IP address of the lease. For example, if this feature is enabled and the DHCP server receives a DHCP REQUEST from a DHCP client with IP address 10.1.1.1 and no host name, the DHCP server generates the name dhcp-10-1-1-1 and uses this name for the DDNS update.

You can define host name settings for the grid, grid members, networks, shared networks, and DHCP address ranges.

**Updating DNS for Clients with Fixed Addresses**

By default, the DHCP server does not update DNS when it allocates a fixed address to a client. You can configure the DHCP server to update the A and PTR record of clients with a fixed address. When you enable this feature and the DHCP server adds A and PTR records for a fixed address, the DHCP server never discards the records. When the lease of the client terminates, you must delete the records manually.

You can define fixed address settings for the grid, grid members, networks, and shared networks.

**About the Client FQDN Option (Option 81)**

When a DHCP client sends DHCP DISCOVER and DHCP REQUEST messages, it can include option 81, the Client FQDN option. This option contains either the host name or FQDN (fully qualified domain name) of the client, and instructions on whether the client or the server performs the DDNS update.

The DHCP server can support this option and use the host name or FQDN that the client provides for the update. It can also allow or deny the client’s request to update DNS, according to the administrative policies of your organization. The DHCP server indicates its response in the DHCP OFFER message it sends back to the client.

**Sending Updates with Option 81 Enabled**

When you enable the DHCP server to support option 81, it uses the information provided by the client to update DNS as follows:

- When a DHCP client sends a DHCP request with option 81, it can include either the FQDN or only the host name of the client.
  - If the request includes the FQDN, the DHCP server uses this FQDN to update DNS. You can specify a list of forward-mapping zones to be updated for clients using option 81. For information, see *Configuring DDNS Features* on page 509.
— If the request includes the host name, the DHCP server provides the domain name. It combines the host name of the client and the domain name to create an FQDN for the client. It then updates DNS with the FQDN it created. (You can enter the domain name in the General page of the DHCP Properties window. For information, see 

Enabling DDNS and Specifying a Domain Name on page 506.)

• When a DHCP client sends a DHCP request with its host name (option 12), the DHCP server adds the domain name you specified to create an FQDN for the client. It then updates DNS with the FQDN it created. For information about entering the domain name, see 

Enabling DDNS and Specifying a Domain Name on page 506.

• When a DHCP client does not send a host name, the DHCP server provides a lease but does not update DNS. You can configure the DHCP server to generate a host name and update DNS as described in 

Generating Host Names for DDNS Updates on page 509.

• If multiple DHCP clients specify the same FQDN or host name, the DHCP server allocates leases to the clients, but updates DNS only for the client that first sent the request. When it tries to update DNS for the succeeding clients, the update fails.

Sending Updates from DHCP Clients or a DHCP Server
When you enable the DHCP server to support option 81, you must decide if you want the DHCP server to allow clients to update DNS. If you allow the client to update DNS, then the client updates its A record only. The DHCP server always updates the PTR records. You can configure the DHCP server as follows:

• The DHCP server can allow clients to update DNS when they send the request in option 81. This is useful for small sites where security is not an issue or in sites where clients move from one administrative domain to another and want to maintain the same FQDN regardless of administrative domain.

  If you configure the DHCP server to allow clients to perform DDNS updates, you must also configure the DNS server to accept these updates from clients. Note that multiple clients can use the same name, resulting in multiple PTR records for one client name.

  When a lease expires, the DHCP server does not delete the A record if it was added by the client.

• The DHCP server can refuse the DHCP client’s request to update DNS and always perform the updates itself. When the DHCP server updates DNS, it uses the FQDN provided by the DHCP client. Select this option if your organization requires tighter control over your network and does not allow clients to update their own records.

  If you do not enable support for option 81 and a client includes it in a DHCP request with its FQDN, the DHCP server does not use the FQDN of the client. Instead, it creates the FQDN by combining the host name from the client with the domain name specified in the Grid or Member DHCP Configuration editor.
Configuring DDNS Features

You can configure DDNS features for a grid, member, network and shared network, and DHCP address range.

To configure DDNS features:

1. **Grid:** From the Data Management tab, select the DHCP tab, expand the Toolbar and click Grid DHCP Configuration.
   
   **Member:** From the Data Management tab, select the DHCP tab and click the Members tab -> member check box -> Edit icon.

   **Network:** From the Data Management tab, select the DHCP tab and click the Networks tab -> Networks -> network check box -> Edit icon.

   **Shared Network:** From the Data Management tab, select the DHCP tab and click the Networks tab -> Shared Networks -> shared_network check box -> Edit icon.

   **DHCP Range:** From the Data Management tab, select the DHCP tab and click the Networks tab -> Networks -> network -> addr_range check box -> Edit icon.

   To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the DDNS -> Advanced tab for the grid and member, or the DDNS -> Basic tab for the network, do the following:
   
   - **Update Retry**
     - **Retry Updates When Server Becomes Available:** Select this check box.
     - **Retry interval (Minutes):** You can optionally set the retry interval. The default is five minutes.

   - **Generate Hostname**
     - **Generate Hostname if not Sent by Client:** Select this check box to enable the DHCP server to generate a hostname and update DNS with this hostname, when the DHCPREQUEST does not include a hostname.

   - **Fixed Address Updates**
     - **Update Fixed Addresses:** Select this check box to allow he DHCP server to send updates to DNS for fixed addresses.

   - **Option 81 Support**
     - **Enable Option 81 Support:** Select this to enable the support for option 81.
     - **DHCP server always updates DNS:** Select this to allow the DHCP server to update DNS, regardless of the requests from DHCP clients.
     - **DHCP server updates DNS if requested by client:** Select this to allow the DHCP server to update DNS only when requested by DHCP clients.

3. Select one of the following:
   
   - **Save & Close:** Save the entry and close the editor.
   - **Save:** Save the entry and keep the editor open.

   When a lease expires, the DHCP server removes the A and PTR records that it updated. It does not remove any records that the client updated.
Configuring DDNS Update Verification

The DHCP server can handle DDNS updates differently, depending on how stringently you configure record handling. You can configure the DHCP server to update records only after passing verification. You can adjust the way DHCP handles updates so the DHCP server updates records after passing less stringent verification requirements, or without any type of verification.

To provide a measure of protection against unintentional changes of DNS data, NIOS appliances support the generation and use of TXT records, as described in IETF draft, draft-ietf-dhc-dhcp-dns-12.txt and by the ISC (Internet Systems Consortium). When DHCP updates or deletes an A record, the corresponding TXT record is checked first to verify the authenticity of the update. The TXT record is based on a hash of the DHCID which is unique to each client, usually based in part on the MAC address. If the client requests an update to DNS, the DHCP server first checks the TXT record to verify that it matches the client that originally inserted the record. This process provides assurance that the updates are from the same client. These security checks are based upon inserting a cryptographic hash of the DHCID (DHCP Client Identifier) into a DNS TXT RR and then verifying that value before updating. For example, a sample client update adds the following records in DNS:

<table>
<thead>
<tr>
<th>oxcart.lo0.net.</th>
<th>21600</th>
<th>IN A 172.31.1.20</th>
</tr>
</thead>
<tbody>
<tr>
<td>oxcart.lo0.net.</td>
<td>21600</td>
<td>IN TXT &quot;313ce164780d34b91486b7c489ed7467e6&quot;</td>
</tr>
<tr>
<td>20.1.31.172.in-addr.arpa.</td>
<td>21600</td>
<td>IN PTR oxcart.lo0.net.</td>
</tr>
</tbody>
</table>

However, your DNS configuration might require that the NIOS appliance handle DNS record updates differently than described in draft-ietf-dhc-dhcp-dns-12.txt. Your specific requirements might benefit from less-stringent verification of the DHCID, or might require skipping verification entirely. Verification checks might cause complications in some specific cases described below:

- **Mobility**: The TXT record is based on the DHCID unique to each client and is usually based on the MAC address of the interface. Devices such as laptops that connect to both wired and wireless networks have different MAC addresses and different DHCID values for each interface. In this scenario, after either one of the network interfaces inserts a DNS record, updates are allowed from that interface only. This results in a disruption of service for DDNS updates when roaming between wired and wireless networks.

- **Migration**: The second problem occurs during a migration from non-ISC based systems to ISC systems. For example, if the user is migrating from a Microsoft-based system, the clients have A and PTR records in the DDNS updates but no TXT records. As a result, new DDNS updates fail after the migration.

- **Mixed Environments**: The final problem occurs in mixed ISC and non-ISC environments. For example, assume that both Microsoft and ISC DHCP servers update DNS records on the appliance. Since the Microsoft DHCP server does not insert the TXT records, updates from ISC-based systems fail while updates from the Microsoft DHCP server are committed into the database.
The NIOS appliance offers four modes to handle DDNS updates as described in Figure 18.4 on page 513:

**Figure 18.4  DDNS Update Verification Mode**

<table>
<thead>
<tr>
<th>Mode</th>
<th>If a Record at Lease Grant</th>
<th>Then TXT Record at Lease Grant</th>
<th>Lease Grant Action</th>
<th>Lease Expire Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard ISC</td>
<td>Exists</td>
<td>Must match</td>
<td>Delete A</td>
<td>Delete PTR</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Add A</td>
<td>Delete A, TXT if TXT matches and no other A RRs</td>
</tr>
<tr>
<td></td>
<td>No A record</td>
<td>No check</td>
<td>Add A, TXT</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Add PTR</td>
<td></td>
</tr>
<tr>
<td>Check TXT only</td>
<td>Exists</td>
<td>Must exist</td>
<td>Delete A, TXT</td>
<td>Delete PTR</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Add A, TXT</td>
<td>Delete A if TXT exists and no other A RRs</td>
</tr>
<tr>
<td></td>
<td>No A record</td>
<td>No check</td>
<td>Add A, TXT</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Add PTR</td>
<td></td>
</tr>
<tr>
<td>ISC Transitional</td>
<td>Exists</td>
<td>No check</td>
<td>Delete A, TXT if exists</td>
<td>Delete PTR</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Add A, TXT</td>
<td>Delete A, TXT if TXT matches and no other A RRs</td>
</tr>
<tr>
<td></td>
<td>No A record</td>
<td>No check</td>
<td>Add A, TXT</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Add PTR</td>
<td></td>
</tr>
<tr>
<td>No TXT record</td>
<td>Exists</td>
<td>No check</td>
<td>Delete A</td>
<td>Delete PTR, A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Add A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No A record</td>
<td>No check</td>
<td>Add A</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Add PTR</td>
<td></td>
</tr>
</tbody>
</table>

Depending on your expected usage, you must carefully consider the various options for update verification. The following section illustrates recommendations for each verification option:

- **Standard ISC**: This method is the most stringent option for verification of updates. This is the default.
- **ISC Transitional**: This method is useful during migrations from systems that do not support the TXT record to systems that are ISC-based.
- **Check TXT only**: This method is useful for the roaming laptop scenario. The NIOS appliance checks that a TXT record exists, but does not check the value of the TXT record.
- **No TXT record**: This method should be used with caution because anyone can send DDNS updates and overwrite records. This method is useful when both ISC and non-ISC-based DHCP servers and clients are updating the same zone. Infoblox recommends that you allocate a DNS zone for this authentication method, as a precaution.

**Note**: In certain situations, when a DHCP lease expires, the DHCP server might remove the TXT record even if there is no A record.
You can enable this feature at the grid level. To configure TXT record handling on the DHCP server:

1. From the **Data Management** tab, select the **DHCP** tab, expand the Toolbar and click **Grid DHCP Configuration**.
2. In the **DDNS → Advanced** tab, select one of the following from the **TXT (DHCID) Record Handling** drop-down list:
   - **Check Only**: Select this check box to enable minimal checking of DDNS updates. Specifically, A records are modified only if a TXT record exists. The NIOS appliance checks that a TXT record exists, but does not check its value.
   - **ISC**: Select this check box to enable standard ISC (Internet Systems Consortium) handling for DDNS updates. Specifically, A records are modified or deleted only if the TXT records match. This option is the default setting on the appliance.
   - **ISC Transitional**: Select this check box to enable less stringent handling of DDNS updates. Specifically, the NIOS appliance enables you to add or modify A records whether or not TXT records exist. It checks whether a TXT record exists and then processes the update. If the appliance does not find a TXT record, it adds the record.
   - **No TXT Record**: Select this check box to disable TXT record checking. Specifically, A records are added, modified, or deleted whether or not the TXT records match. No TXT records are added, and existing TXT records are ignored.
3. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and keep the editor open.
Configuring DNS Servers for DDNS

For security reasons, an Infoblox DNS server does not accept DDNS updates by default. You must specify the sources from which you want to allow the DNS server to receive updates. For protection against spoofed IP addresses, you can use TSIG (transaction signatures) to authenticate and verify updates.

TSIG uses the MD5 (Message Digest 5) algorithm and a shared secret key to create an HMAC (hashed message authentication code)—sometimes called a digital fingerprint—of each update. Both the DHCP server sending the update and the DNS server receiving it must share the same secret key. Also, it is important that the time stamps on the TSIG-authenticated updates and update responses be synchronized, or the participants reject them. Therefore, use an NTP server to set the time on all systems involved in TSIG authentication operations.

The TSIG key that you use can come from several places:
- You can use the key generation tool described in this section to create a new TSIG key to authenticate updates from the DHCP server.
- You can enter (copy and paste) a TSIG key that you previously generated for another purpose, such as for zone transfers.
- If the DHCP server is on a separate appliance and a TSIG key was previously generated on that appliance, you can enter (copy and paste) that TSIG key onto the local DNS server.

The TSIG key name and value that the DHCP and DNS servers use must be the same.

Note: Whether you deploy NIOS appliances in a grid or independently, they send updates to UDP port 53. Grid members do not send updates through a VPN tunnel. Grid members do, however, authenticate updates between them using TSIG (transaction signatures) based on an internal TSIG key.

Enabling a DNS Server to Accept DDNS Updates

You can configure the Infoblox DNS server to restrict the DHCP servers from which it is allowed to receive updates. You can set this for the grid so that all grid members are allowed to receive DDNS updates. Likewise, you can configure a DNS server to accept forwarded updates from another DNS server. These are the DNS servers from which the grid members are allowed to accept forwarded updates (see Forwarding Updates on page 516).

To configure the DNS server to accept updates:

1. Grid: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
   Member: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
   Zones: From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view -> zone check box -> Edit icon.
   To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the editor, click Updates.

3. In the Updates -> Basic tab, click the Add icon beside Allow updates from. Depending on the item that you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows:
   - IPv4 Address: In the Name field of the new row, enter the IP address of the remote server. The Permission column displays Allow by default. To change it to Deny, click it to display the drop-down list and select Deny.
   - IPv4 Network: In the Add IPv4 Network panel, complete the following, and then click Add to add the network to the list:
     - Address: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.
     - Permission: Select Allow or Deny from the drop-down list.
## Configuring DDNS Updates from DHCP

1. **IPv6 Address**: In the Name field of the new row, enter the IPv6 address of the remote server. The Permission column displays Allow by default. To change it to Deny, click it to display the drop-down list and select Deny.

2. **IPv6 Network**: In the Add IPv6 Network panel, complete the following, and then click Add to add the network to the list:
   - **Address**: Enter an IPv6 network address and select the netmask from the drop-down list.
   - **Permission**: Select Allow or Deny from the drop-down list.

3. **TSIG Key**: In the Add TSIG Key panel, complete the following, and then click Add to add the TSIG key to the list:
   - **Key name**: Type a useful name for the key, such as the name of the grid or grid member using the key, or the name of the zone being updated. The key name entered here must match the TSIG key name on the DHCP server sending the updates.
   - **Key Data**: To use an existing TSIG key, type or paste the key in the Key field. Alternatively, you can select the type of key and create a new key. By default, Grid Manager creates a 512-bit key. You can select 256-bit key or 128-bit key. Click Generate Key Data to create the new key.

4. **Any Address/Network**: Select to allow or deny updates from any IP address.

### Forwarding Updates

When a secondary DNS server receives DDNS updates, it must forward the updates to the primary server because it cannot update zone data itself. In such situations, you must enable the secondary server to receive updates from the DHCP server, and then forward them to the primary DNS server.

To configure the secondary server to accept and forward updates for all zones:

1. **Grid**: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
   - **Member**: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
   - **Zones**: From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view -> zone check box -> Edit icon.
   - To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the editor, click **Toggle Advanced Mode**.

3. When the additional tabs appear, click the Advanced subtab of the Updates tab, and then complete the following:
   - **Allow secondary name servers to forward updates**: Select this check box.
   - **Forward updates from**: This is available for a zone only. Click Add. Depending on the item that you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows:
     - **IPv4 Address**: In the Name field of the new row, enter the IP address of the remote name server. The Permission column displays Allow by default. To change it to Deny, click it to display the drop-down list and select Deny.
     - **IPv4 Network**: In the Add IPv4 Network panel, complete the following, and then click Add to add the network to the list:
       - **Address**: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.
       - **Permission**: Select Allow or Deny from the drop-down list.
— **IPv6 Address**: In the **Name** field of the new row, enter the IPv6 address of the remote name server. The **Permission** column displays **Allow** by default. To change it to **Deny**, click it to display the drop-down list and select **Deny**.

— **IPv6 Network**: In the **Add IPv6 Network** panel, complete the following, and then click **Add** to add the network to the list:
  - **Address**: Enter an IPv6 network address and select the netmask from the drop-down list.
  - **Permission**: Select **Allow** or **Deny** from the drop-down list.

— **TSIG Key**: In the **Add TSIG Key** panel, complete the following, and then click **Add** to add the TSIG key to the list:
  - **Key name**: Type a useful name for the key, such as the name of the grid or grid member using the key, or the name of the zone being updated. This key name must match the TSIG key name on the DHCP server sending the updates.
  - **Key Data**: To use an existing TSIG key, type or paste the key in the Key field. Alternatively, you can select the type of key and create a new key. By default, Grid Manager creates a 512-bit key. You can select 256-bit key or 128-bit key. Click **Generate Key Data** to create the new key.

— **Any Address/Network**: Select to allow or disallow the appliance to forward updates from any IP address.

4. Select one of the following:
   — **Save & Close**: Save the entry and close the editor.
   — **Save**: Save the entry and keep the editor open.
**Supporting Active Directory**

Active Directory™ (AD) is a distributed directory service that authenticates network users and—by working with DHCP and DNS—provides the location of and authorizes access to services running on devices in a Windows® network.

You can integrate a NIOS appliance providing DHCP and DNS services with servers running Windows 2000 Server, Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2 with the Active Directory service installed. Assuming that you already have AD set up and it is currently in use, you can migrate DHCP and DNS services away from internal operations on the AD domain controller or from other third party DHCP and DNS systems to NIOS appliances that serve DHCP and DNS.

A NIOS appliance providing DHCP and DNS services to an AD environment can send and receive DDNS updates. In addition, a NIOS appliance can use GSS-TSIG (Generic Security Service-Transaction Signatures) authentication for DDNS updates. The basic DHCP, AD, and DNS services are shown in Figure 18.5.

*Figure 18.5 DHCP, Active Directory, and DNS*

Sending DDNS Updates to a DNS Server

You can configure an Infoblox DHCP server to send unauthenticated or GSS-TSIG-authenticated DDNS updates to a DNS server in an AD domain. There are no special configurations to consider when configuring a NIOS appliance to send unauthenticated DDNS updates to the DNS server. (For information about configuring DHCP, see *Chapter 23, Configuring DHCP Services*, on page 617; and for information on configuring the DHCP server to send DDNS updates, see *Configuring DHCP for DDNS* on page 505.) For information about configuring a DHCP server to send GSS-TSIG authenticated updates, see *About GSS-TSIG* on page 519.
GSS-TSIG is used to authenticate DDNS updates. It is a modified form of TSIG authentication that uses the Kerberos v5 authentication system.

GSS-TSIG involves a set of client/server negotiations to establish a “security context”. It makes use of a Kerberos server (running on the AD domain controller) that functions as the Kerberos Key Distribution Center (KDC) and provides session tickets and temporary session keys to users and computers within an Active Directory domain. The client and server collaboratively create and mutually verify transaction signatures on messages that they exchange. Windows 2000 servers and later support DDNS updates using GSS-TSIG.

Note: For information about GSS-TSIG, see RFC 3645, Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG).

A NIOS appliance can use GSS-TSIG authentication for DDNS updates for either one of the following:

- A NIOS appliance serving DHCP can send GSS-TSIG authenticated DDNS updates to a DNS server in an AD domain whose domain controller is running Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2. The DNS server can be in the same AD domain as the DHCP server or in a different domain.
  - For information about sending secure DDNS updates to a DNS server in the same domain, see Sending Secure DDNS Updates to a DNS Server in the Same Domain on page 520.
  - For information about sending secure DDNS updates to a DNS server in a different domain, see Sending Secure DDNS Updates to a DNS Server in Another Domain on page 529.

  - For information, see Accepting GSS-TSIG-Authenticated Updates on page 535.

Note that a NIOS appliance cannot support both of these features at the same time.
Sending Secure DDNS Updates to a DNS Server in the Same Domain

An Infoblox DHCP server can send GSS-TSIG authenticated DDNS updates to a DNS server in an AD domain whose domain controller is running Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2. The DHCP server, DNS server, and domain controller are all in the same AD domain. The process by which an Infoblox DHCP server dynamically updates resource records on a DNS server using GSS-TSIG authentication is shown in Figure 18.6. In the illustration, the Kerberos Key Distribution Center (KDC) is running on an AD domain controller, which also provides DNS service.

*Figure 18.6 An Infoblox DHCP Server Sends GSS-TSIG Updates to a DNS Server*

After you enable the NIOS appliance to send GSS-TSIG authenticated updates to a DNS server, the following process occurs:

1. **Kerberos – Login, and TGT and Service Ticket Assignments**
   a. The Infoblox appliance automatically logs in to the AD/Kerberos server.
   b. The Kerberos server sends the appliance a TGT (ticket-granting ticket).
   c. Using the TGT, the appliance requests a service ticket for the DNS server.
   d. The Kerberos server replies with a service ticket for that server.
2. TKEY negotiations (GSS Handshake):
   a. The appliance sends the DNS server a TKEY (transaction key) request. A Transaction Key record establishes shared secret keys for use with the TSIG resource record. For more information, see RFC 2930, Secret Key Establishment for DNS (TKEY RR).
      The request includes the service ticket. The service ticket includes the appliance’s principal and proposed TSIG (transaction signature) key, along with other items such as a ticket lifetime and a timestamp.
   b. The DNS server responds with a DNS server-signed TSIG, which is a “meta-record” that is never cached and never appears in zone data. A TSIG record is a signature of the update using an HMAC-MD5 hash that provides transaction-level authentication. For more information, see RFC 2845, Secret Key Transaction Authentication for DNS (TSIG).
      The two participants have established a security context.

When a DHCP client sends a request for an IP address to the DHCP server, the following occurs:

3. DHCP – IP Address and Network Parameters Assignment
   a. The DHCP client requests an IP address.
   b. The DHCP server assigns an IP address, subnet mask, gateway address, DNS server address, and a domain name.

After the appliance assigns an IP address to the DHCP client, it sends the DDNS update to the DNS server as follows:

4. DDNS – Dynamic Update of the Client’s Resource Records
   c. GSS-TSIG-Authenticated DDNS Update
      1. The appliance sends an authenticated DDNS update, which may include the following resource records:
         • A – Address record
         or
         PTR – Pointer record
         • TKEY – Transaction Key record
         • TSIG – TSIG record
      2. The DNS server verifies the DDNS update and allows it to complete.
      3. The DNS server sends a GSS-TSIG-authenticated response to the appliance, confirming the update.
Configuring DHCP to Send GSS-TSIG Updates in the Same Domain

Before configuring an Infoblox DHCP server to support GSS-TSIG, you must create a user account on the Kerberos server for the appliance. Then you must export the corresponding keytab file from the Kerberos server and import it onto the NIOS appliance. Figure 18.7 illustrates the initial configuration tasks.

**Figure 18.7 Adding an Infoblox DHCP Server to an AD Environment with GSS-TSIG Support**

1. Add a user account for the Infoblox DHCP server.
2. Generate the keytab file for the DHCP server account and export it from the Kerberos server to a local directory on your management system.
3. Import the keytab file to the NIOS appliance.
4. Enable GSS-TSIG updates.
5. The DHCP server assigns IP addresses to DHCP clients that send requests for IP addresses.
6. The DHCP server sends GSS-TSIG dynamic DNS updates to the DNS server.

The Infoblox DHCP server can send GSS-TSIG-signed DDNS updates to a DNS server for one domain only, though multiple Infoblox DHCP servers can update that domain. If you want more than one Infoblox DHCP server to update a DNS domain, you can either import the same keytab file to the other Infoblox DHCP servers or generate and import a different keytab file. In a grid, each member can update a different domain.

**Note:** For GSS-TSIG authentication to work properly, the system clock times of the Infoblox DHCP server, AD domain controller and DNS server must be synchronized. One approach is to use NTP and synchronize all three devices with the same NTP servers.

To use an AD domain controller as a Kerberos Key Distribution Center, complete the following tasks on an AD/Kerberos server:

1. Add a user account for the NIOS appliance to the AD domain controller. For information, see [Creating an AD User Account](#) on page 523.
2. Generate the keytab file for the NIOS appliance account and export it from the AD domain controller to a local directory on your management system. For information, see [Generating the Keytab File](#) on page 523.

To configure a NIOS appliance to support AD and send GSS-TSIG secure DDNS updates to a DNS server, complete the following tasks on a NIOS appliance:

1. Import the keytab file from your management system to the appliance and enable GSS-TSIG dynamic updates at the grid or member level. For information, see [Enabling GSS-TSIG Authentication for DHCP](#) on page 527.
2. Configure the appliance to send GSS-TSIG dynamic updates to forward-mapping and optionally, reverse-mapping zones on the DNS server. For information, see [Creating an External Zone for GSS-TSIG Updates](#) on page 528.
Creating an AD User Account

Connect to the AD domain controller and create a user account for the NIOS appliance.

| Note: | The name that you enter in the User logon name is the name that you later use when exporting the keytab file. This is also the principal name. The text in the First name, Initials, Last name, and Full name fields is irrelevant to this task. |

The AD domain controller automatically creates a Kerberos account for this user. Note the following:

- If you define an expiration date for the user account and you later create a new account when the first one expires, the keytab for the corresponding Kerberos account changes. At that point, you must update the keytab file on the NIOS appliance (see Generating the Keytab File and Enabling GSS-TSIG Authentication for DHCP on page 527). Optionally, if your security policy allows it, you can set the user account for the NIOS appliance so that it never expires.
- If the AD domain controller is running Windows Server 2003, the user account must have the DES encryption type enabled. You can enable this either in the Account tab of the AD domain controller when you create the user account or by specifying +DesOnly when you use the Ktpass tool to generate the keytab file. For instructions, see the next section, Generating the Keytab File.

Generating the Keytab File

Use the Ktpass tool to generate the keytab file for the Kerberos account. Note that the version of the Ktpass tool that you use must match the Windows version of the domain controller. For example, if you are using a domain controller running Windows Server 2008, you must use the Ktpass tool for Windows Server 2008.

Following are the differences between generating a keytab file on a Windows Server 2003 and on a Windows Server 2008/Windows Server 2008 R2 domain controller.

- The Ktpass syntax is slightly different. On a Windows Server 2003, the principal name must include a slash. On a Windows Server 2008 or Windows Server 2008 R2, the principal name must not include a slash. After you generate the keytab file, a warning message may be displayed because the slash was excluded. (See the example in Generating the Keytab File on a Windows Server 2008/Windows Server 2008 R2.)
- A Windows Server 2003 domain controller allows you to generate a keytab file with only one key for a principal. A Windows Server 2008 or Windows Server 2008 R2 domain controller allows you to generate a keytab file with multiple keys for one principal. This is useful when the KDC has principals with multiple encryption types. When the NIOS DHCP server uses a keytab with multiple keys, it negotiates a key based on those in the configured keytab file.
Generating the Keytab File on a Windows Server 2003

The Ktpass tool is included in the Windows Server 2003 Support Tools. To generate the keytab file using the Ktpass tool:

1. Start a command prompt.
2. Enter the following command to generate the keytab file for the NIOS appliance user account:

   ```
   ktpass -princ username/instance@REALM -mapuser logon_name@REALM -pass password -out my.ktb -ptype krb5_nt_principal -crypto des-cbc-md5 +DesOnly
   ```

   For example:

   ```
   ktpass -princ dns/anywhere@CORP100.LOCAL -mapuser dns@CORP100.LOCAL -pass infoblox -out dns.ktb -ptype krb5_nt_principal -crypto des-cbc-md5 +DesOnly
   ```

   where:

   - **-princ** = Kerberos principal
     - out **username/instance**: The AD user name for the NIOS appliance and a character string. The AD user name must match the user logon name in the AD domain controller.
     - **REALM**: The Kerberos realm in uppercase. It must match the realm (or domain name) specified in the **-mapuser** option.
   
   - **-mapuser** = Maps the Kerberos principal name to the AD user account.
     - **logon_name**: The AD user name for the NIOS appliance.
     - **REALM**: The Kerberos realm in uppercase. The realm (or domain name) must be the same as that specified in the **-princ** option.
   
   - **-pass** = A new password for the AD user account. The Ktpass command changes the account password to the specified value, thus incrementing the version number of the user account and the resulting keytab file.
     - **password**: The password of the user account for the NIOS appliance.
   
   - **-out** = The name of the keytab file that is generated.
     - **my.ktb**: The name of the keytab file.
   
   - **-ptype** = Specifies the principal type. This must be **krb5_nt_principal**.
   
   - **-crypto** = Specifies the encryption type. This must be **des-cbc-md5**.
   
   +**DesOnly** = Specifies DES encryption for the account. Include this if you did not enable DES encryption for the account.

   After you execute the command to generate the keytab file, the AD domain controller displays a series of messages similar to the following to confirm that it successfully generated the keytab file:

   ```
   Targeting domain controller: ibtest-xu5nxd56.corp100.local
   Using legacy password setting method
   Successfully mapped dns/anywhere to dns.
   Key created.
   Output keytab to dns.ktb:
   Keytab version: 0x502
   keysize 56 dns/anywhere@CORP100.LOCAL ptype 1 (KR5_NT_PRINCIPAL) vno 5 etype 0x3 (DES-CBC-MD5) keylength 8 (0xbae610f11552c80b)
   ```

   **Note:** The keytab file contains highly sensitive data for the NIOS appliance account. Ensure that you store and transport its contents securely.
Generating the Keytab File on a Windows Server 2008/Windows Server 2008 R2

On a Windows Server 2008 or Windows Server 2008 R2 domain controller, the Ktpass tool supports generating a keytab file with multiple keys for a single principal. Infoblox strongly recommends that one of the keys include the encryption type DES-CBC-MD5 for compatibility purposes. Most principals use DES-CBC-MD5 and it is the most compatible encryption type with other systems, such as MIT Kerberos.

To generate the keytab file using the Ktpass tool:

1. Start a command prompt.
2. Enter the following command to generate the keytab file for the NIOS appliance user account:

   \[ \text{ktpass -princ } \text{username@REALM } \text{-mapuser } \text{logon_name@REALM } \text{-pass password } \text{-out my.tab -ptype krb5_nt_principal -crypto encryption} \]

   For example:

   \[ \text{ktpass -princ dns@CORP100.LOCAL -mapuser dns@CORP100.LOCAL -pass infoblox -out dns.tab -ptype krb5_nt_principal -crypto all} \]

   where:

   - \text{-princ} = Kerberos principal
     - \text{username}: The AD user name for the NIOS appliance. This entry must be the same on the AD domain controller and the Infoblox appliance.
     - \text{REALM}: The Kerberos realm in uppercase. It must match the realm (or domain name) specified in the \text{-mapuser} option.
   - \text{-mapuser} = Maps the Kerberos principal name to the AD user account.
     - \text{logon_name}: The AD user name for the NIOS appliance.
     - \text{REALM}: The Kerberos realm in uppercase. The realm (or domain name) must be the same as that specified in the \text{-princ} option.
   - \text{-pass} = The existing AD user account password.
     - \text{password}: The password of the user account for the NIOS appliance.
   - \text{-out} = The name of the keytab file that is generated.
     - \text{my.ktb}: The name of the keytab file.
   - \text{-ptype} = Specifies the principal type. This must be \text{krb5_nt_principal}.
   - \text{-crypto} = Specifies the encryption type. You can specify more than one encryption type or specify \text{-all} to indicate that all supported encryption types can be used.

You can optionally specify the following:

- \text{+DesOnly} = Specifies DES encryption for the account. Include this if you did not enable DES encryption for the account.
- \text{+setpass} = Sets a new AD user account password. This is required if the \text{+DesOnly} option is specified. When you use this encryption type, you must change the user’s password. Otherwise, the ticket issued for the principal becomes unusable.
  - \text{password}: The new password of the user account for the NIOS appliance.
After you execute the command to generate the keytab file, the AD domain controller displays a series of messages similar to the following to confirm that it successfully generated the keytab file:

```plaintext
Targeting domain controller: qacert.corp100.local
Using legacy password setting method
Failed to set property 'servicePrincipalName' to 'dns' on Dn 'CN=firstname lastname,CN=Users,DC=corp100,DC=local': 0x13. WARNING: Unable to set SPN mapping data.
If jdoe already has an SPN mapping installed for dns, this is no cause for concern.
Key created.
Key created.
Key created.
Key created.
Key created.
Output keytab to dns.tab:
Keytab version: 0x502
keysize 45 dns@CORP100.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 2 etype 0x1 (DES-CBC-CRC) keylength 8 (0xa7cbd091c86b0a4)
keysize 45 dns@CORP100.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 2 etype 0x3 (DES-CBC-MD5) keylength 8 (0xa7cbd091c86b0a4)
keysize 53 dns@CORP100.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 2 etype 0x17 (RC4-HMAC) keylength 16 (0xc304df2d2bf575e13b43c37030d0b50)
keysize 69 dns@CORP100.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 2 etype 0x12 (AES-256-SHA1) keylength 32 (0xe8fdd9493d114980c6369bfe56bf7fd1c4baa9b36c4bd672b4050b073ee5023)
keysize 53 dns@CORP100.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 2 etype 0x11 (AES-128-SHA1) keylength 16 (0x2c142c8d2bf575e13b43c37030d0b50)
```

**Note that the messages included the following warning:**

```plaintext
Failed to set property 'servicePrincipalName' to 'dns' on Dn 'CN=firstname lastname,CN=Users,DC=corp100,DC=local': 0x13. WARNING: Unable to set SPN mapping data.
If logon_name already has an SPN mapping installed for dns, this is no cause for concern.
```

This message displays because the principal name did not include a slash. You can ignore the warning because the AD domain controller still generates a valid keytab file, despite the warning.
Enabling GSS-TSIG Authentication for DHCP

You can enable GSS-TSIG authentication at the grid or member level. When you enable GSS-TSIG authentication, make sure that you upload the keytab file from the Kerberos account for the Infoblox DHCP server. The AD domain controller stores the keytab file in the directory in which you generated the keytab file. You can copy this file to a management system that connects to the NIOS appliance or launch the NIOS Grid Manager on the AD domain controller and import the keytab file to the NIOS appliance.

You can import keytab files to the grid or to individual members.

To enable GSS-TSIG authentication and import Keytab files:

1. **Grid:** From the Data Management tab, select the DHCP tab, expand the Toolbar and click Grid DHCP Properties.
   **Member:** From the Data Management tab, select the DHCP tab and click the Members tab -> member check box -> Edit icon.
   To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the DDNS -> Basic tab of the editor, complete the following:
   - **DDNS Updates:** Select the Enable DDNS Updates check box.
   - **DDNS Update TTL:** You can set the TTL used for A and PTR records updated by the DHCP server. The default is shown as zero. If you do not enter a value here, the appliance by default sets the TTL to half of the DHCP lease time with a maximum of 3600 seconds. For example, a lease time of 1800 seconds results in a TTL of 900 seconds, and a lease time of 86400 seconds results in a TTL of 3600 seconds. For information about how to set the lease time, see Configuring DHCP Lease Times on page 621.
   - **GSS-TSIG:** Complete the following:
     - **Enable GSS-TSIG Updates:** Select this check box.
     - **Domain Controller:** Enter the resolvable host name or IP address of the AD domain controller that hosts the Key Distribution Center (KDC) for the domain.
     - **GSS-TSIG Key:** Select the name of the keytab file you are using for the grid. This is only available if you have uploaded a keytab file.
       To upload a keytab file, click Manage Keytab Files. In the Kejtab File Manager dialog box, click the Add icon. Click Browse, navigate to the keytab file, select it, and then click Upload.
     - **Domain:** The appliance displays the name of the domain associated with the keytab file.
     - **Click Test GSS-TSIG to list the external zones to which the grid member can send secure DDNS updates.**

3. Select one of the following:
   - **Save & Close:** Save the entry and close the editor.
   - **Save:** Save the entry and keep the editor open.

Each time you export a keytab file from a Kerberos server running on Windows Server 2003, the version number of the keytab file increases incrementally. Because the version number of the keytab file that you import to the NIOS appliance must match the version that is in use on the Kerberos server, you should select the last keytab file that is exported from the Kerberos server if you have exported multiple keytab files.
Creating an External Zone for GSS-TSIG Updates

For each network view, you specify the zone to be updated, the IP address of the primary DNS server for that zone, and the security method, GSS-TSIG. The zone must be in the same AD domain as the member that is sending the updates.

You can add information for a forward and reverse zone. The DHCP server updates the A record in the forward zone and the PTR record in the reverse zone.

To enable the NIOS appliance to send dynamic updates to a DNS server using GSS-TSIG for authentication:

1. If there are multiple network views in the grid, select a network view.
2. From the Data Management tab, select the DHCP tab, expand the Toolbar and click Configure DDNS.
3. In the DDNS Updates to External Zones table of the DDNS Properties editor, click the Add icon and complete the following fields in the Add External DDNS Zone panel:
   - Zone Name: Enter the name of the zone that receives the updates. You can specify both forward-mapping and reverse-mapping zones.
   - DNS Server Address: Enter the IP address of the primary name server for that zone.
   - Security: Select GSS-TSIG.
   - AD Domain: Select the AD domain associated with the keytab file.
   - DNS Principal: The name and domain of the DNS server receiving the DDNS updates. Note that this is not the same as the Kerberos principal you specified when you generated the keytab file.
     - Use the following format when you complete this field: DNS/dns_server_fqdn@ad_domain
     - dns_server_fqdn: This is the FQDN of the DNS server. You can use the “dig” command to perform a DNS lookup to obtain the FQDN of the DNS server as it appears on the SOA record.
     - ad_domain: This is the AD domain of the DNS server.
   - Click Test GSS-TSIG to list the grid members that are allowed to send GSS-TSIG updates to the DNS server.
4. Select one of the following:
   - Save & Close: Save the entry and close the editor.
   - Save: Save the entry and keep the editor open.

Verifying the Configuration

After you configure the AD domain controller and the Infoblox DHCP server, you can view the syslog of the Infoblox DHCP server to verify if it successfully established a security context with the AD domain controller. The DHCP server displays a series of messages similar to the following:

```
dhcpd: Enabled GSS-TSIG for zone corp100. using principal jdoe/anywhere@CORP100.LOCAL.
dhcpd: GSS-TSIG security thread has started.
dhcpd: GSS-TSIG security update starting at 1222389338.
dhcpd: Acquiring GSS-TSIG credential for jdoe/anywhere@CORP100.LOCAL (good for 3568s).
dhcpd: Security context established with server 10.34.123.4 for principal jdoe/anywhere@CORP100.LOCAL (good for 568s).
dhcpd: GSS-TSIG security update complete at 1222389338. Next update in 360s.
```

In addition, you can log in to the Infoblox CLI and use the `show dhcp_gss_tsig` CLI command to troubleshoot your configuration. For information about this command, refer to the Infoblox CLI Guide.
Sending Secure DDNS Updates to a DNS Server in Another Domain

Domain and forest trust relationships provide clients authenticated access to resources in other domains. Some trusts are automatically created, such as the two-way, direct trust between parent and child domains in a forest. Other trusts must be created manually. Refer to the Microsoft Active Directory documentation for information on establishing trusts between domains.

Once a direct trust exists between two AD domains, a KDC from one domain can grant a referral to the KDC of the other domain. The Infoblox DHCP server can then use the referral to request access to services in the other domain.

In Figure 18.8, the Infoblox DHCP server in the child.corp100.com domain needs to send GSS-TSIG authenticated DDNS updates to the DNS server in its parent domain, corp100.com domain. There is an automatic two-way trust between the domains because corp100.com domain is the parent of child.corp100.com domain.

Figure 18.8 Sending Secure DDNS Updates to a DNS Server in Another Domain

After you configure the Infoblox DHCP server and AD domain controller, the following occurs:

1. Kerberos – In Same Domain
   The Infoblox DHCP server uses the TGT (ticket-granting ticket) from the AD/Kerberos server, ad.child.corp100.com, to request a service ticket for DNS/ns1.corp100.com@CORP100.COM. The Kerberos server replies with a referral ticket for the Kerberos server in the corp100.com domain, ad.corp100.com.

2. Kerberos — In the Other Domain
   The Infoblox DHCP server uses the referral ticket and requests a service ticket from ad.corp100.com for DNS/ns1.corp100.com@CORP100.COM. The Kerberos server replies with a service ticket for DNS/ns1.corp100.com@CORP100.COM.

3. TKEY Negotiations (GSS Handshake)
   The Infoblox DHCP server sends the DNS server ns1.corp100.com a TKEY (transaction key) request, which includes the service ticket. The DNS server replies with a TKEY response that includes a TSIG (transaction signature). The Infoblox appliance and the DNS server have established a security context, enabling the DHCP server to send DDNS updates to the DNS server.
Configuring DHCP to Send GSS-TSIG Updates to Another Domain

Before the DHCP server can send secure DDNS updates to a DNS server in a different domain, you must ensure that a direct trust relationship exists between the domain of the DHCP server and that of the DNS server. (For information, refer to the Active Directory documentation.)

Following are the tasks to configure the AD domain controller and the Infoblox DHCP server for secure updates to another domain. All the configuration is done on the AD domain controller for the domain of the DHCP server and on the Infoblox DHCP server:

1. Complete the following tasks on the AD domain controller for the domain of the DHCP server:
   a. Add a user account for the Infoblox DHCP server. In the configuration example, the user account is ibdhcp. For information, see Creating an AD User Account on page 523.
   b. Generate the keytab file for the Infoblox DHCP server and export it from the AD domain controller to a local directory on your management system. For the DHCP server in Figure 18.8, the principal is ibdhcp/ib.child.corp100.com@CHILD.CORP100.COM. For information, see Generating the Keytab File on page 523.

2. Complete the following tasks on the Infoblox DHCP server:
   a. Import the keytab file from your management system to the appliance and enable GSS-TSIG dynamic updates at the grid or member level. For information, see Enabling GSS-TSIG Authentication for DHCP on page 527
   b. Configure the external forward-mapping zone for the DDNS updates. Note that the DNS principal uses the domain of the DNS server, regardless of the domain of the DHCP server. For the DNS server in Figure 18.8, the DNS principal is DNS/ns1.corp100.com@CORP100.COM. For information, see Creating an External Zone for GSS-TSIG Updates on page 528.
Configuration Example

Following are the steps to configure the example shown in Figure 18.8:

On the AD domain controller:

1. Create a user account for the Infoblox DHCP server. The user account is ibdhcp.
2. Generate the keytab file and export it to your management system. If the domain controller is running Windows Server 2003:
   
   ktpass -princ ibdhcp/ib.child.corp100.com@CHILD.CORP100.COM -mapuser ibdhcp@CHILD.CORP100.COM -pass infoblox -out ibdhcp.ktb -ptype krb5_nt_principal -crypto des-cbc-md5 +desonly

On the Infoblox DHCP server:

1. Enable GSS-TSIG at the member level.
2. From the DHCP tab, click the Members tab → member check box → Edit icon.
3. In the DDNS → Basic tab of the editor, complete the following:
   
   — Override: Select this check box.
   — DDNS Updates: Select the Enable DDNS Updates check box.
   — GSS-TSIG: Select Override and complete the following:
     — Enable GSS-TSIG Updates: Select this check box.
     — Domain Controller: Enter ad.child.corp100.com. This is the KDC in the domain of the DHCP server.
     — GSS-TSIG Key: Click Manage Keytab Files. In the Keytab File Manager dialog box, click the Add icon. Click Browse, navigate to the keytab file, select it, and then click Upload. Select the keytab file that you just uploaded, ibdhcp/ib.child.corp100.com@CHILD.CORP100.COM.
     — Domain: The appliance displays the name of the domain associated with the key, which is child.corp100.com.
     — Click Test GSS-TSIG to list the external zones to which the grid member can send secure DDNS updates.
4. Click Save & Close.
5. Configure the external forward mapping zone, corp100.com.
   
   a. From the DHCP tab, expand the Toolbar and click Configure DDNS.
   b. In the DNS Updates to External Zones table of the DNS Properties editor, click the Add icon and complete the following fields in the Add External DNS Zone panel:
     — Zone Name: Enter corp100.com.
     — DNS Server Address: Enter the IP address of the primary DNS server to which the Infoblox DHCP server sends DDNS updates. In the example, the DNS server is ns.corp100.com. Therefore, enter its IP address, which is 10.23.2.24.
     — Security: Select GSS-TSIG.
       — AD Domain: Select child.corp100.com.
       — DNS Principal: Enter DNS/ns1.corp100.com@CORP100.COM.
     — Click Test GSS-TSIG to list the grid members that are allowed to send GSS-TSIG updates to the DNS server.
6. Click Save & Close.
Sending GSS-TSIG Updates to a DNS Server in Another Forest

The Infoblox DHCP server can also send secure DDNS updates to a DNS server that belongs to a domain in another forest, as long as a forest trust exists. Refer to the Microsoft Active Directory documentation for information on establishing forest trusts.

Similar to the authentication process between domains, the authentication process between forests also uses referrals. The appliance follows the referral chain until it reaches the domain controller of the domain in which the service is located. Note that forest trusts are not transitive. For example, if the DHCP server is in forest A and the DNS server is in forest C, a direct trust must exist between forest A and forest C for the DDNS updates to succeed. Having a trust between forest A and B, and between forest B and C is not sufficient.

In Figure 18.9, a trust exists between the A.Local forest and the B.Local forest. The Infoblox DHCP server in the A.Local forest needs to dynamically update the DNS server in the B.Local forest.

Figure 18.9  Sending Secure DDNS Updates to a DNS Server in Another Forest

The following authentication process occurs:

1. Kerberos – In Same Domain
   The Infoblox appliance uses the TGT (ticket-granting ticket) from the AD/Kerberos server, ad.child.corp100.com, to request a service ticket for DNS/ns1.corp200.com@CORP200.COM. The Kerberos server does not find the principal name in its domain database and after consulting the global catalog, it replies with a referral ticket for its parent domain.

2. Kerberos — Referral Chain
   The appliance contacts a domain controller in corp100.com and requests a referral to a domain controller in the corp200.com domain in B.Local Forest.
   When it receives the referral, the DHCP server contacts the domain controller and requests a service ticket for the DNS server, ns1.corp200.com. The domain controller replies with a service ticket for DNS/ns1.corp200.com@CORP200.COM.

3. TKEY Negotiations (GSS Handshake)
   The Infoblox appliance sends the DNS server ns1.corp200.com a TKEY (transaction key) request, which includes the service ticket. The DNS server replies with a TKEY response that includes a TSIG (transaction signature). The Infoblox appliance and the DNS server have established a security context.

Configuring DHCP to Send GSS-TSIG Updates to a Different Forest

Configuring the Infoblox DHCP server for dynamic updates to a DNS server in another forest is similar to the configuration used to send dynamic updates to another domain in the same forest. For information, see Configuring DHCP to Send GSS-TSIG Updates to Another Domain on page 530.
**Accepting DDNS Updates from DHCP Clients**

A NIOS appliance serving DNS can support Active Directory and accept both unauthenticated and GSS-TSIG authenticated updates from DHCP clients, DHCP servers, and AD domain controllers.

When adding a NIOS appliance that serves DNS to an AD environment, you must configure the AD/Kerberos server and NIOS appliance as follows—based on whether or not you want the DNS server to support DDNS updates using GSS-TSIG authentication:

- **AD/Kerberos Server**
  1. Enable zone transfers to the NIOS appliance.
  2. (For GSS-TSIG) Create a user account for the NIOS appliance that it can use for authentication.
  3. (For GSS-TSIG) Generate the keytab file of the DNS server and save it to your management system.

- **NIOS Appliance**
  4. (GSS-TSIG) Enable GSS-TSIG support.
  5. (GSS-TSIG) Import the keytab file of the DNS server from your management system to the NIOS appliance.
  7. Add a forward-mapping zone and give it a name matching the AD DNS zone whose resource records you want to import.
  8. Specify the domain controller from which the appliance can receive DDNS updates. An AD domain controller replicates its data among other domain controllers within its AD domain and among domain controllers in other domains.
  9. Import zone data from the specified domain controller.
  10. Enable the acceptance of DDNS updates from the AD domain controller and from the DHCP clients and servers whose addresses the DHCP server assigns. You can set this at the grid, member, and zone levels.
  11. (For GSS-TSIG) Enable acceptance of GSS-TSIG DDNS updates from the AD domain controller and from the addresses that the DHCP server assigns. You can set this at the grid, member, and zone levels.

As you can see from the above task list, adding a NIOS appliance that serves DNS to an AD environment without GSS-TSIG support involves four simple steps. To include GSS-TSIG support, there are several additional steps.

**Supporting Active Directory and Unauthenticated DDNS Updates**

Before configuring the NIOS appliance, configure the AD domain controller to permit zone transfers to the IP address of the appliance. Then on the appliance, you can do the following to configure a forward-mapping zone to support AD (Active Directory) and receive unauthenticated DDNS updates from DHCP clients, DHCP servers, and AD domain controllers.

- Create a forward-mapping zone, as described in *Creating an Authoritative Forward-Mapping Zone* on page 405. Give it a name that matches the AD DNS zone whose resource records you want to import.
- Specify the domain controllers from which the appliance can receive updates, as described in *Configuring AD Support* on page 534.
- Import the zone data from the domain controller. For information, see *Importing Data into Zones* on page 401.
- Enable the appliance to accept DDNS updates from the DHCP clients and servers whose addresses the DHCP server assigns. You can set this at the grid, member, and zone levels. For information, see *Enabling a DNS Server to Accept DDNS Updates* on page 515.
Configuring AD Support

You can configure a forward-mapping zone to support AD from the Active Directory wizard or from the Active Directory tab of the Authoritative Zone editor. This section describes both methods.

To configure AD support using the Active Directory wizard:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Configure Active Directory. Note that from the Zones tab, you must select a zone before you click Configure Active Directory.

2. In the Active Directory wizard, complete the following, and then click Next:
   - Select Zone: Click this and select a zone. The name of the zone must match the name in the AD domain controller so the zone transfer from the AD domain controller to the NIOS appliance can succeed.
   - Allow unsigned updates from Domain Controllers: Select this option.

If you configured DNS resolvers in the grid, the appliance sends DNS queries for the names and addresses of the AD domain’s domain controllers. Since the name of the zone that you selected is the same as the AD domain name on the domain controller, the appliance can then send a DNS query for the SRV records attached to the domain name. It also sends a DNS query for the A record of each domain controller to determine its IP address. The query results are listed in the next panel.

3. You can edit the list of domain controllers, if necessary. Click Next to proceed to the next step.
   - To add a domain controller, click the Add icon and specify the IP address.
   - To delete a domain controller from the list, select it and click the Delete icon.

4. Complete the following:
   - Do you want to create underscore zones to hold the records added by the Domain Controllers?
     This option allows the appliance to create the following subzones that the DNS server must have to answer AD-related DNS queries:
     _msdcs.zone
     _sites.zone
     _tcp.zone
     _udp.zone
     domaindnszones.zone
     forestdnszones.zone

     Note that these zones are automatically generated. You cannot edit these zones or import data into them. They cannot be modified, thus providing protection against forged updates.

5. Click Save & Close.

To configure AD support using the Authoritative Zone editor:

1. From the Data Management tab, select the DNS tab -> Zones tab -> zone check box -> Edit icon.

2. In the Authoritative Zone editor, select the Active Directory tab and do the following:
   - Allow unsigned updates from these Domain Controllers: Select this check box and specify the AD domain controllers from which the appliance can receive DDNS updates.
   - Automatically create underscore zones: Select this check box to automatically create the subzones.

3. Click Save & Close.

You can then import zone data, as described in Importing Data into Zones on page 401.
Accepting GSS-TSIG-Authenticated Updates

A NIOS appliance can support Active Directory and process secure GSS-TSIG-authenticated DDNS updates from DHCP clients, DHCP servers, and AD domain controllers. The process in which a DHCP client dynamically updates its resource records on a DNS server using GSS-TSIG authentication is shown in *Figure 18.10*. The illustration also shows the relationship of the clients, the DHCP server, the DNS server, and the Kerberos server (running on the AD domain controller).

**Note:** For explanations of the alphanumerically notated steps in *Figure 18.10*, see the section following the illustration.

*Figure 18.10 Authenticating DDNS Updates with GSS-TSIG*

1. **DHCP – IP Address and Network Parameters Assignment**
   a. The DHCP client requests an IP address.
   b. The DHCP server assigns an IP address, subnet mask, gateway address, and a DNS server address.
2. Active Directory – Computer and User Logins
   a. The computer sends a DNS request to locate the AD domain controller, and then logs in to the domain controller.

   **Note:** Computer accounts have passwords that the AD domain controller and computer maintain automatically. There are two passwords for each computer: a computer account password and a private key password. By default, both passwords are automatically changed every 30 days.

   b. The user manually logs in to a domain.

3. DNS – Query for the Kerberos Server
   a. The computer (or client) automatically sends a query for _kerberos._udp.dc_msdc$.$dom_name to the DNS server whose IP address it received through DHCP.

   b. The NIOS appliance replies with the name of the Kerberos server.

4. Kerberos – Login, and TGT and Service Ticket Assignments
   a. The client automatically logs in to the Kerberos server.
   b. The Kerberos server sends the client a TGT (ticket-granting ticket).
   c. Using the TGT, the AD member requests a service ticket for the DNS server.
   d. The Kerberos server replies with a service ticket for that server.

5. DDNS – Dynamic Update of the Client's Resource Records
   a. Unauthenticated DDNS Update Attempt (Refused)
      1. The client sends an unauthenticated DDNS update.
      2. The DNS server refuses the update.
   b. TKEY negotiations (GSS Handshake):
      1. The client sends the DNS server a TKEY (transaction key) request. A Transaction Key record establishes shared secret keys for use with the TSIG resource record. For more information, see RFC 2930, Secret Key Establishment for DNS (TKEY RR).
      2. The DNS server responds with a DNS server-signed TSIG, which is a “meta-record” that is never cached and never appears in zone data. A TSIG record is a signature of the update using an HMAC-MD5 hash that provides transaction-level authentication. For more information, see RFC 2845, Secret Key Transaction Authentication for DNS (TSIG).
   c. GSS-TSIG-Authenticated DDNS Update (Accepted)
      1. The client sends an authenticated DDNS update, which includes the following resource records:
         • A – Address record
         • PTR – Pointer record
         • TKEY – Transaction Key record
         • TSIG – TSIG record
      2. The DNS server authenticates the DDNS update and processes it.
      3. The DNS server sends a GSS-TSIG-authenticated response to the AD member, confirming the update.

   **Note:** For GSS-TSIG authentication to work properly, the system clock times of the Infoblox DHCP server, AD domain controller and DNS server must be synchronized. One approach is to use NTP and synchronize all three devices with the same NTP servers.
Configuring DNS to Receive GSS-TSIG Updates

You can configure an appliance to support Active Directory and accept secure DDNS updates from clients using GSS-TSIG. The initial configuration tasks are shown in Figure 18.11.

Figure 18.11 Adding a NIOS Appliance to an AD Environment with GSS-TSIG Support

1. Add a user account for the DNS server.
2. Generate the keytab file for the DNS server account and export it from the Kerberos server to a local directory on your management system.
3. Import the keytab file to the NIOS appliance.
4. Create a forward-mapping zone and import zone data from the AD domain controller. Note: Make sure that zone transfers from the AD domain controller to the NIOS appliance are enabled.
5. Optional: Create a reverse-mapping zone.
On an already functioning AD domain controller:
1. Enable zone transfers to the NIOS appliance.
2. Add a user account for the NIOS appliance serving DNS. A corresponding account on the Kerberos server is automatically created. For information, see Creating an AD User Account on page 538.
3. Export the keytab file for the NIOS appliance account from the Kerberos server to a local directory on your management system. For information, see Generating and Exporting the Keytab File on page 539.

On an Infoblox appliance:
1. Import the keytab file from your management system to the Infoblox appliance and enable GSS-TSIG authentication on the appliance. For information, see Importing the Keytab File and Enabling GSS-TSIG Authentication on page 541.
2. Configure a forward-mapping zone with the same name as the AD zone. For information, see Creating an Authoritative Forward-Mapping Zone on page 405.
3. (Optional) Create a reverse-mapping zone for the network address space that corresponds to the domain name space in the forward-mapping zone. For information, see Creating an Authoritative Reverse-Mapping Zone on page 406.
4. Import the zone data from the AD domain controller. For information, see Importing Zone Data on page 419.
5. Enable the acceptance of GSS-TSIG-signed updates from the AD controller and from the DHCP clients and servers whose addresses the DHCP server assigns. For information, see Accepting GSS-TSIG Updates on page 541.

Creating an AD User Account

Connect to the AD domain controller and create a user account for the NIOS appliance.

Note: The name you enter in the User logon name is the name that you later use when exporting the keytab file. This is also the principal name. The text in the First name, Initials, Last name, and Full name fields is irrelevant to this task.

The AD domain controller automatically creates a Kerberos account for this user with an accompanying keytab. Note the following:

- If you define an expiration date for the user account and you later create a new account when the first one expires, the keytab for the corresponding Kerberos account changes. At that point, you must update the keytab file on the NIOS appliance (see Generating and Exporting the Keytab File and Enabling GSS-TSIG Authentication on page 541). Optionally, if your security policy allows it, you can set the user account for the NIOS appliance so that it never expires.
- If the AD domain controller is running Windows Server 2003, the user account must have the DES encryption type enabled. You can enable this either in the Account tab when you create the user account or by specifying +DesOnly when you use the Ktpass tool to generate the keytab file.
Generating and Exporting the Keytab File

You can generate and export the keytab file for the Kerberos account by using the Ktpass tool. Note that the version of the Ktpass tool that you use must match the Windows version of the domain controller. For example, if you are using a domain controller running Windows Server 2008 or Windows Server 2008 R2, you must use the Ktpass tool for Windows Server 2008 or Windows Server 2008 R2.

You enter different commands for generating and exporting the keytab file, depending on whether you are generating the keytab file from a server running Microsoft Windows 2000, Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2.

Generating the Keytab on Windows 2000

To export the keytab file using a Microsoft Windows 2000 Resource Kit:

1. Start a command prompt.
2. Enter the following command to export the keytab file for the NIOS appliance user account:
   ```
   C:> ktpass -princ service_name/FQDN_instance@REALM -mapuser AD_username -pass password -out filename.keytab
   ```
   For example:
   ```
   C:> ktpass -princ DNS/ns1.corp100.com@CORP100.COM -mapuser ns1@corp100.com -pass 37Le37 -out ns1.keytab
   ```

Generating the Keytab on Windows Server 2003

The Ktpass tool is included in the Windows Server 2003 Support Tools. To export the keytab file using a Microsoft Windows 2003 Resource Kit:

1. Start a command prompt.
2. Enter the following command to export the keytab file for the NIOS appliance user account:
   ```
   ktpass -princ DNS/FQDN_instance@REALM -mapuser AD_username -pass password -out filename.keytab
   -ptype KRB5_NT_PRINCIPAL -crypto des-cbc-md5 +DesOnly
   ```
   For example:
   ```
   ktpass -princ DNS/ns1.corp100.com@CORP100.COM -mapuser ns1@corp100.com -pass 37Le37 -out ns1.keytab -ptype KRB5_NT_PRINCIPAL -crypto des-cbc-md5 +DesOnly
   ```
   where:
   - **-princ** = Kerberos principal
     - DNS = Service name in uppercase format
     - ns1.corp100.com = Instance in FQDN (fully-qualified domain name) format; this is the same as the DNS name of the NIOS appliance
     - CORP100.COM = The Kerberos realm in uppercase format; this must be the same as the AD domain name
   - **-mapuser** = Maps the Kerberos principal name to the AD user account
     - ns1@corp100.com = The AD user name for the NIOS appliance
   - **-pass** = The AD user account password
     - 37Le37 = The password of the user account for the NIOS appliance
   - **-out** = Exports the keytab file
     - ns1.keytab = The name of the keytab file
   - **-ptype** = Sets the principal type. This must be **krb5_nt_principal**.
   - **-crypto** = Specifies the encryption type. This must be **des-cbc-md5**.
   - **+DesOnly** = Specifies DES encryption for the account. Include this if you did not enable DES encryption for the account.
Generating the Keytab on Windows Server 2008/Windows Server 2008 R2

A Windows Server 2008 or Windows Server 2008 R2 domain controller allows you to generate a keytab file with multiple keys for one principal. The Infoblox DNS server accepts GSS-TSIG updates from DHCP clients that provide a Kerberos ticket for any of the keys in its configured keytab. To generate the keytab file using the Ktpass tool:

1. Start a command prompt.
2. Enter the following command to export the keytab file for the NIOS appliance user account:
   
   ```
   ktpass -princ DNS/FQDN_instance@REALM -mapuser AD_username -pass password -out filename.keytab -ptype krb5_nt_principal -crypto encryption
   ```
   
   For example:
   
   ```
   ktpass -princ DNS/ns1.corp100.com@CORP100.COM -mapuser ns1@corp100.com -pass 37Le37 -out ns1.keytab -ptype krb5_nt_principal -crypto all
   ```
   
   where:
   
   - **-princ** = Kerberos principal
     - DNS = Service name in uppercase format
     - ns1.corp100.com = Instance in FQDN format; this is the same as the DNS name of the NIOS appliance
     - CORP100.COM = The Kerberos realm in uppercase; this must be the same as the AD domain name
   - **-mapuser** = Maps the Kerberos principal name to the AD user account
     - ns1@corp100.com = The AD user name for the NIOS appliance
   - **-pass** = The AD user account password
     - 37Le37 = The password of the user account for the NIOS appliance
   - **-out** = Exports the keytab file
     - ns1.keytab = The name of the keytab file
   - **-ptype** = Sets the principal type. This must be krb5_nt_principal.
   - **-crypto** = Specifies the encryption type. You can specify more than one encryption type or specify -all to indicate that all supported encryption types can be used. Infoblox recommends that you specify the -all option to enable the Infoblox DNS server to accept GSS-TSIG updates from DHCP clients that provide a Kerberos ticket with any of the keys.

   After you execute the command to generate the keytab file, the AD domain controller displays a series of messages similar to the following to confirm that it successfully generated the keytab file:

   ```
   Targeting domain controller: qacert.qatest.local
   Using legacy password setting method
   Successfully mapped DNS/ns1.corp100.com to ns1.
   Key created.
   Key created.
   Key created.
   Key created.
   Key created.
   Output keytab to dns432.keytab:
   Keytab version: 0x502
   keysize 59 DNS/ns1.corp100.com@CORP100.COM ptype 1 (KR5_NT_PRINCIPAL) vno 2 etype 0x1 (DES-CBC-CRC) keylength 8 (0x9e15851383efae89)
   keysize 59 DNS/ns1.corp100.com@CORP100.COM ptype 1 (KR5_NT_PRINCIPAL) vno 2 etype 0x3 (DES-CBC-MD5) keylength 8 (0x9e15851383efae89)
   keysize 67 DNS/ns1.corp100.com@CORP100.COM ptype 1 (KR5_NT_PRINCIPAL) vno 2 etype 0x17 (RC4-HMAC) keylength 16 (0x644492a9cfabad73633b1d9b1f15410d)
   keysize 83 DNS/ns1.corp100.com@CORP100.COM ptype 1 (KR5_NT_PRINCIPAL) vno 2 etype 0x12 (AES256-SHA1) keylength 32 (0x69a8d5773004e3a2849d36120226f0e9dbbb984a348a5bc809546d6cc295e4e)
   keysize 67 DNS/ns1.corp100.com@CORP100.COM ptype 1 (KR5_NT_PRINCIPAL) vno 2 etype 0x11 (AES128-SHA1) keylength 16 (0x54ae8ed10194d94c5057c8f312749705)
   ```

   **Note:** The keytab file contains highly sensitive data for the NIOS appliance account. Ensure that you store and transport its contents securely.
Modifying an AD User Account

To change any AD user account information (login, password, etc):
1. Remove the previous user account from AD.
2. Create a new user for GSS-TSIG mapping.
4. Import the keytab file to the DNS server.

Importing the Keytab File and Enabling GSS-TSIG Authentication

Before you can enable GSS-TSIG authentication, you must import the keytab file from the Kerberos account for the NIOS appliance. To import the keytab file:
1. From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
2. In the Member DNS Properties editor, click Toggle Advanced Mode.
3. When the additional tabs appear, click GSS-TSIG and do the following:
   - If a principal name and version number are listed, there is a keytab file loaded on the appliance. Compare this information with that for the NIOS appliance account on the Kerberos server to make sure that they match. If there is no keytab file on the NIOS appliance or if the loaded keytab file does not match that on the Kerberos server, you must load the correct keytab file
     - Click Upload, click Browse to navigate to the keytab file, and then click Upload.
   - Enable GSS-TSIG authentication of clients: Select this check box.
4. Click Save & Close.

Each time you export a keytab file from a Kerberos server running on Windows Server 2003, the version number of the keytab file increases incrementally. Because the version number on the keytab file that you import to the NIOS appliance must match the version that is in use on the Kerberos server, you should select the last keytab file that is exported from the Kerberos server if you have exported multiple keytab files. (A Kerberos server running on Windows 2000 does not increase the version number of keytab files with each export.)

Accepting GSS-TSIG Updates

You can allow a grid or specific members or zones to accept GSS-TSIG signed updates from domain controllers and DHCP clients and servers, as follows:
1. Grid: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties. Member: From the Data Management tab, select the DNS tab -> Members tab -> member check box -> Edit icon. Zone: From the Data Management tab, select the DNS tab -> Zones tab -> zone check box -> Edit icon. To override an inherited property, click Override next to it and complete the appropriate fields.
2. Select the Updates tab and do the following in the Basic subtab:
   - Allow GSS-TSIG signed updates: Select this option.
3. Click Save & Close.

You can then use the Active Directory wizard or navigate to the Active Directory tab of the Authoritative Zone editor to enable the appliance to create underscore zones for the records hosted by domain controllers and to allow GSS-TSIG signed updates to the underscore zones.

To use the Active Directory wizard:
1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Configure Active Directory.
2. In the Configure Active Directory wizard, complete the following, and then click Next:
   - Select Zone: Click this and select a zone. The name of the zone must match the name in the AD domain controller so the zone transfer from the AD domain controller to the NIOS appliance can succeed.
   - Allow GSS-TSIG-signed (secure) updates from Domain Controllers: Select this option.
3. Complete the following:
   — **Do you want to create underscore zones to hold the records added by the Domain Controllers?**
     This option allows the appliance to create the following subzones that the DNS server must have to answer
     AD-related DNS queries:
     
     `_msdcs.zone`
     `_sites.zone`
     `_tcp.zone`
     `_udp.zone`
     `domaindnszones.zone`
     `forestdnszones.zone`
     
     Note that these zones are automatically generated. You cannot edit these zones or import data into them.
     When you allow GSS-TSIG signed updates, this option is disabled by default. GSS-TSIG provides protection
     against forged updates, eliminating the need to generate these zones that cannot be modified.

     — **Allow GSS-TSIG-signed updates to underscore zones:** This option is selected by default.

4. Click **Save & Close**.

   To use the **Authoritative Zone** editor:
   1. From the **Data Management** tab, select the **DNS** tab -> **Zones** tab -> **zone** check box -> **Edit** icon.
   2. In the **Authoritative Zone** editor, select the **Active Directory** tab and do the following:
      — **Allow unsigned updates from these Domain Controllers:** Clear this check box.
      — **Automatically create underscore zones:** (select)
        This option automatically creates the following subzones that the DNS server must have to answer
        AD-related DNS queries:
        
        `_msdcs.zone`
        `_sites.zone`
        `domaindnszones.zone`
        `forestdnszones.zone`
        
        Note that these zones are automatically generated and cannot be manually edited.

     — **Allow GSS-TSIG-signed updates to underscore zones:** This option is selected by default.
Chapter 19 DNSSEC

This chapter provides general information about DNSSEC. The topics in this chapter include:

- About DNSSEC on page 544
  - DNSSEC Resource Records on page 545
  - DNSKEY Resource Records on page 546
  - RRSIG Resource Records on page 548
  - NSEC/NSEC3 Resource Records on page 549
  - NSEC3PARAM Resource Records on page 550
  - DS Resource Records on page 551
- Configuring DNSSEC on a Grid on page 552
- Enabling DNSSEC on page 554
- Setting DNSSEC Parameters on page 555
  - About the DNSKEY Algorithm on page 555
  - About Key Rollovers on page 555
  - RRSIG Signatures on page 556
  - Configuring DNSSEC Parameters on page 557
- Signing a Zone on page 558
- Managing Signed Zones on page 560
  - Importing a Keyset on page 560
  - Exporting Trust Anchors on page 561
  - Checking Key-Signing Keys on page 561
  - Rolling Key-Signing Keys on page 561
  - Unsigning a Zone on page 562
  - Deleting and Restoring Signed Zones on page 562
- Configuring Grid Members to Support DNSSEC as Secondary Servers on page 563
- Enabling Recursion and Validation for Signed Zones on page 564
  - Enabling Recursion and Validation for Signed Zones on page 564
  - Enabling DNSSEC Validation on page 565
About DNSSEC

DNSSEC (DNS Security Extensions) provides mechanisms for authenticating the source of DNS data and ensuring its integrity. It protects DNS data from certain attacks, such as man-in-the-middle attacks and cache poisoning. A man-in-the-middle attack occurs when an attacker intercepts responses to queries and inserts false records. Cache poisoning can occur when a client accepts maliciously created data. DNSSEC helps you avoid such attacks on your networks.

DNSSEC provides changes to the DNS protocol and additional resource records (RRs) as described in the following RFCs:

- RFC 4033, DNS Security Introduction and Requirements
- RFC 4034, Resource Records for the DNS Security Extensions
- RFC 4035, DNSSEC Protocol Modifications
- RFC 4641, DNSSEC Operational Practices
- RFC 4956, DNS Security (DNSSEC) Opt-In
- RFC 4986, Requirements Related to DNS Security (DNSSEC) Trust Anchor Rollover
- RFC 5155, DNS Security (DNSSEC) Hashed Authenticated Denial of Existence
- RFC 5702, Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC

DNSSEC uses public key cryptography to authenticate the source of DNS responses and to ensure that DNS responses were not modified during transit. Public key cryptography uses an asymmetric key algorithm. With asymmetric keys, one key is used to decrypt data that was encrypted using the other key.

In DNSSEC, the primary name server of a zone generates at least one public/private key pair. It “signs” each data set in the zone by running it through a one-way hash, and then encrypting the hash value with the private key. The public key is stored in an RR type introduced by DNSSEC, the DNSKEY RR. Resolvers use the DNSKEY record to decrypt the hash value. If the hash values match, then the resolver is assured of the authenticity of the message.

In addition to the DNSKEY record, DNSSEC also introduces new RRs which DNS servers can use to authenticate the non-existence of servers, zones, or resource records. For information about the DNSSEC RRs, see DNSSEC Resource Records on page 545.

DNSSEC uses the EDNSO message extension. Resolvers include the EDNS OPT pseudo-RR with the DO (DNSSEC OK) bit set to indicate that they are requesting DNSSEC data. A DNS client or resolver sets the EDNS DO bit when it sends a query for data in a signed zone. When the DNS server receives such a query, it includes the additional DNSSEC records in its response, according to the DNSSEC standard rules. In addition, because DNSSEC messages are often large, the EDNSO message extension also provides mechanisms for handling larger DNS UDP messages.

For information about EDNS, refer to RFC 2671, Extension Mechanisms for DNS (EDNS0). For information about the DO bit, refer to RFC 3225, Indicating Resolver Support of DNSSEC.

DNSSEC also supports new data in the packet header, the CD (Checking Disabled) bit and the AD (Authenticated Data) bit. The CD bit is used by resolvers in their DNS queries and the AD bit is used by recursive name servers in their responses to queries.

A resolver can set the CD bit in its query to indicate that the name server should not validate the DNS response and that the resolver takes responsibility for validating the DNS data it receives.

A name server that has successfully validated the data in a DNS response sets the AD (Authenticated Data) bit in the message header to indicate that all resource records in its response have been validated and are authentic. Note that unless the connection between the DNS server and client has been secured, such as through TSIG, the client cannot rely on the AD bit to indicate valid data. The data could have been changed in transit between the server and client. Resolvers can trust a response with the AD bit set only if their communication channel is secure.
DNSSEC Resource Records

Following are the DNSSEC RR types:

- DNS Public Key (DNSKEY) resource records—For information, see DNSKEY Resource Records on page 546.
- Resource Record Signature (RRSIG) records—For information, see RRSIG Resource Records on page 548.
- Next Secure (NSEC/NSEC3) records—For information, see NSEC/NSEC3 Resource Records on page 549.
- NSEC3PARAM records—For information, see NSEC3PARAM Resource Records on page 550.
- Delegation Signer (DS) resource records—For information, see DS Resource Records on page 551.

For detailed information about each RR, refer to RFC 4034, Resource Records for the DNS Security Extensions and RFC 5155, DNS Security (DNSSEC) Hashed Authenticated Denial of Existence.
DNSKEY Resource Records

When an authoritative name server digitally signs a zone, it typically generates two key pairs, a zone-signing key (ZSK) pair and a key-signing key (KSK) pair. The name server uses the private key of the ZSK pair to sign each RRset in a zone. (An RRset is a group of resource records that are of the same owner, class, and type.) It stores the public key of the ZSK pair in a DNSKEY record. The name server then uses the private key of the KSK pair to sign all DNSKEY records, including its own, and stores the corresponding public key in another DNSKEY record. As a result, a zone typically has two DNSKEY records; a DNSKEY record that holds the public key of the ZSK pair, and another DNSKEY record for the public key of the KSK pair.

Note: For the remainder of this chapter, the DNSKEY record that holds the public key of the ZSK pair is referred to as the ZSK and the DNSKEY record that holds the public key of the KSK is referred to as the KSK.

The purpose of the KSK is two-fold. First, it is referenced in the Delegation Signer (DS) RR that is stored in a parent zone. The DS record is used to authenticate the KSK of the child zone, so a resolver can establish a chain of trust from the parent zone to its child zone. (For more information about the DS RR, see DS Resource Records on page 551.) Second, if a zone does not have a chain of trust from a parent zone, security aware resolvers can configure the KSK as a trust anchor; that is, the starting point from which it can build a chain of trust from that zone to its child zones.

Note that though the two key pairs, KSK and ZSK, are used in most DNSSEC environments, their use is not required by the RFCs. A zone administrator can use a single private/public key pair to sign all zone data. (Note that Infoblox appliances require two key pairs.)

Following is an example of a DNSKEY RR:

corp100.com 129600 IN DNSKEY 257 3 5 20181231235959hiZsq1gPtqIKeVuGBbAchPSdg
4vSymSx8sqzueQM4jrrjCBaQbH7VH95kdfcAPxhx
ZBvwQMgE07dxaOetwjpg0vpl6E0VOzLwWhiImw
17Xh0j1arzM8nTf1Pj+4av1KrqB1IPy3693jjChyl8sMT
0EfwwS0tEAWD7IsvtzW24cE= )

<table>
<thead>
<tr>
<th>Owner Name</th>
<th>TTL</th>
<th>Class</th>
<th>RR Type</th>
<th>Flags Field</th>
<th>Algorithm</th>
<th>Protocol</th>
<th>Public Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>corp100.com</td>
<td>129600</td>
<td>IN</td>
<td>DNSKEY</td>
<td>257</td>
<td>3</td>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

The first four fields specify the domain name of the zone that owns the key, the resource record TTL, class, and RR type. The succeeding fields are:

- **Flags Field:** In its wire format, this field is two bytes long. (The wire format is used in DNS queries and responses.) Bits 0 through 6 and 8 through 14 are reserved, and have a value of 0. Bit 7 indicates if the record holds a DNS zone key. Bit 15 is the Secure Entry Point (SEP) flag, which serves as a hint that indicates whether the DNSKEY record contains a ZSK or a KSK, as described in RFC 3757, DNSKEY RR SEP Flag. Zone administrators typically set the SEP flag of a DNSKEY record of a zone when it contains the KSK, to indicate that it can be used as a trust anchor. However, a DNSKEY record that does not have the SEP flag set can also be used as a trust anchor.

  Given the currently defined flags, in its text format, the flags field is represented as an unsigned decimal integer with the possible values of 0, 256 and 257. A value of 256 indicates that the DNSKEY record holds the ZSK and a value of 257 indicates that it contains the KSK. In general, this field contains an odd number when the DNSKEY record holds the KSK.

- **Protocol:** This always has a value of 3, for DNSSEC.
- Algorithm: Identifies the public key's cryptographic algorithm. The available types are:
  - 1 = RSA/MD5
  - 2 = Diffie-Hellman (This is not supported by BIND and Infoblox appliances.)
  - 3 = DSA
  - 4 = Reserved
  - 5 = RSA/SHA1
  - 6 = DSA/SHA1/NSEC3
  - 7 = RSA/SHA1/NSEC3
  - 8 = RSA/SHA-256
  - 10 = RSA/SHA-512
- Public Key: The public key encoded in Base64.
**RRSIG Resource Records**

A signed zone has multiple RRsets, one for each record type and owner name. (The owner is the domain name of the RRset.) When an authoritative name server uses the private key of the ZSK pair to sign each RRset in a zone, the digital signature on each RRset is stored in an RRSIG record. Therefore, a signed zone contains an RRSIG record for each RRset.

Following is an example of an RRSIG record:

```
corp100.com 86400 IN RRSIG A 5 2 86400 20181231235959 20081027145729
49890 corp100.com hiZsqlgPrtqIKevuGBbAchPSdg4vSymSxSgzqJQW64jrjCBsQbH7VH95kdfcAPxh
ZBvQ5MgE07dxoOeTpwpagQ0vl6E0V0zLwWhiImw
17XhOgJiarzMBnTFf1PJ+4av1KrcqB1Py3693j5ChyL8sMT0EfW50te5W7isvt2V2W4cE= )
```

The first four fields specify the owner name, TTL, class, and RR type. The succeeding fields are:

- **Type Covered:** The RR type covered by the RRSIG record. The RRSIG record in the example covers the A records for corp100.com.
- **Algorithm:** The cryptographic algorithm that was used to create the signature. It uses the same algorithm types as the DNSKEY record indicated in the Key Tag field.
- **Number of Labels:** Indicates the number of labels in the owner name of the signed records. There are two labels in the example, corp100 and com.
- **RRset TTL:** The TTL value of the RRset covered by the RRSIG record.
- **Expiration Time:** The signature expiration time in UTC format.
- **Inception Time:** The signature inception time in UTC format.
- **Key Tag:** The key tag value of the DNSKEY RR that validates the signature.
- **Signature Name:** The zone name of the RRset.
- **Public Key:** The Base64 encoding of the signature.
NSEC/NSEC3 Resource Records

When a name server receives a request for a domain name that does not exist in a zone, the name server sends an authenticated negative response in the form of an NSEC or NSEC3 RR. NSEC and NSEC3 records contain the next secure domain name in a zone and list the RR types present at the NSEC or NSEC3 RR's owner name. The difference between an NSEC and NSEC3 RRs is that the owner name in an NSEC3 RR is a cryptographic hash of the original owner name prepended to the name of the zone. NSEC3 RRs protect against zone enumeration.

Following is an example of an NSEC record:

```
corpl00.com 86400 IN NSEC a1.corpl00.com. NS SOA RRSIG NSEC DNSKEY
```

The first four fields specify the owner name, TTL, class and RR type. The succeeding fields are:
- Next Owner Name: In the canonical order of the zone, the next owner name that has authoritative data or that contains a delegation point NS record.
- RRsets: The RRsets that exist at the owner name of the NSEC record, which are NS, SOA, RRSIG, NSEC, and DNSKEY in the example.

Following is an example of an NSEC3 RR:

```
ule6lovi99jvlerve0e080ta34ocu39 900 IN NSEC3 1 0 100 74ae486f6ecbd29010047ad
ULJ8BVITGP50A0RMRFUPQV6A2197FIB NS SOA RRSIG DNSKEY NSEC3PARAM
```

The first field contains the hashed owner name. It is followed by the TTL, class and RR type. The fields after the RR type are:
- Algorithm: The hash algorithm that was used. The currently supported algorithm is SHA-1, which is represented by a value of 1.
- Flags Field: Contains 8 one-bit flags, of which only one flag, the Opt-Out flag, is defined by RFC 5155. The Opt-Out flag indicates whether the NSEC3 record covers unsigned delegations.
- Iterations: The number of times the hash function was performed.
- Salt Field: A series of case-insensitive hexadecimal digits. It is appended to the original owner name as protection against pre-calculated dictionary attacks.
- Next Owner Name: Displays the next hashed owner name.
- RRsets: The RR types that are at the owner name.
NSEC3PARAM Resource Records

An authoritative DNS server uses NSEC3PARAM RRs to determine which NSEC3 records it includes in its negative responses. An NSEC3PARAM RR contains the parameters that an authoritative server needs to calculate hashed owner names. As stated in RFC 5155, the presence of an NSEC3PARAM RR at a zone apex indicates that the specified parameters may be used by authoritative servers to choose an appropriate set of NSEC3 RRs for negative responses.

Following is an example of an NSEC3PARAM record:

corp100.com 900 IN NSEC3PARAM 1 0 100 74ae486f6ecbbd29010047ad

The first four fields specify the owner name, TTL, class and RR type. The succeeding fields are:

- **Algorithm**: The hash algorithm that was used. The currently supported algorithm is SHA-1, which is represented by a value of 1.
- **Flags Field**: Contains 8 one-bit flags, of which only one flag, the Opt-Out flag, is defined by RFC 5155. The Opt-Out flag indicates whether the NSEC3 record covers unsigned delegations.
- **Iterations**: The number of times the hash function was performed.
- **Salt Field**: A series of case-insensitive hexadecimal digits. It is appended to the original owner name as protection against pre-calculated dictionary attacks.
**DS Resource Records**

A DS RR contains a hash of a child zone's KSK and can be used as a trust anchor in some security-aware resolvers and to create a secure delegation point for a signed subzone in DNS servers. As illustrated in Figure 19.1, the DS RR in the parent zone corp100.com contains a hash of the KSK of the child zone sales.corp100.com, which in turn has a DS record that contains a hash of the KSK of its child zone, nw.sales.corp100.com.

**Figure 19.1**

Following is an example of the DS RR:

```
corp100.com 86400 IN DS 25924 5 1 49D2801B50E25D59440F1FF1A8012B568435
```

The first four fields specify the owner name, TTL, class and RR type. The succeeding fields are as follows:

- **Key Tag**: The key tag value that is used to determine which key to use to verify signatures.
- **Algorithm**: Identifies the algorithm of the DNSKEY RR to which this DS RR refers. It uses the same algorithm values and types as the corresponding DNSKEY RR.
- **Digest Type**: Identifies the algorithm used to construct the digest. The supported algorithms are:
  - 1 = SHA-1
  - 2 = SHA-256
- **Digest**: If SHA-1 is the digest type, this field contains a 20 octet digest. If SHA-256 is the digest type, this field contains a 32 octet digest.
Configuring DNSSEC on a Grid

You can configure the name servers in a grid to support DNSSEC. You can configure the grid master as the primary server for a signed zone and the grid members as secondary servers. (For information, see Configuring Grid Members to Support DNSSEC as Secondary Servers on page 563.) Note that only the grid master can serve as the primary server for a signed zone.

You can sign any authoritative forward-mapping or reverse-mapping zone according to the following criteria:

- The zone does not contain any bulk host records.
- DNSSEC is enabled on the grid master.
- The primary server of the zone must be a grid member. If the zone is assigned to an NS group, the primary server in the group must be a grid member that has DNSSEC enabled.

Note that you can use DNS views to separate internal and external zone data, to manage your zones more efficiently and reduce the size of the zones that require signing. For information about DNS views, see Using Infoblox DNS Views on page 384.

When you sign a zone whose primary server is a grid member, that member becomes a secondary server and the grid master becomes the hidden primary server. If the zone is assigned to an NS group, the grid master removes the association with the NS group. The previous primary server becomes a secondary server for the zone.

If a master candidate is promoted to grid master and the previous grid master was the primary server for signed zones, the new grid master becomes the hidden primary server for all signed zones. The previous grid master, which was the primary server for the zone, becomes a secondary server for the zone.

As the primary server, the grid master sends zone data to the secondary servers through zone transfers; or, if the secondary servers are grid members, the grid master transfers data to all grid members through the database replication process, by default. The grid master transfers all records in that zone, including all NSEC/NSEC3, RRSIG, DNSKEY and DS records with owner names that belong to that zone. The RRSIG RRs are included in zone transfers of the zone in which they are authoritative data. The grid master also performs incremental zone transfers to secondary servers as a result of incremental zone signings.

In addition, the grid master automatically performs an incremental signing of the zone data sets when their contents change. Incremental signing refers to signing just those parts of a zone that change when RRs are added, modified, or deleted. The grid master uses the private key of the ZSK when it incrementally signs a zone. In addition, the grid master adds, modifies or deletes the corresponding RRSIG records and the appropriate NSEC/NSEC3 records.
For example, Figure 19.2 shows a grid master as the primary server of a signed zone and its grid members as secondary servers. The grid master, ns1.corp100.com, is the hidden primary DNS server for the corp100.com zone. As the hidden primary name server for corp100.com, the grid master does not respond to queries from other name servers. Instead, it provides data to its secondary servers, ns2.corp100.com and ns3.corp100.com, which use this data to respond to DNS queries. Because the secondary servers are grid members, they receive zone data from the grid master through the grid database replication process.

The name server ns1.corp200.com is a recursive name server. It has configured the DNSKEY of the corp100.com zone as a trust anchor. Therefore, it is able to validate the data it receives when it sends a query for the corp100.com zone.

Following are the tasks to configure a signed zone:

1. Create the zone. For information, see Configuring Authoritative Zones on page 396.
   - Specify the grid master as the primary server.
2. Enable DNSSEC, as described in Enabling DNSSEC.
3. Optionally, change the default DNSSEC settings. For information, see Setting DNSSEC Parameters on page 555.
4. Sign the zone. The appliance automatically generates the DNSSEC RRs when you sign a zone. For information, see Signing a Zone on page 558.
Enabling DNSSEC

You can enable DNSSEC on a grid, individual members, and DNS views. Because only grid masters can serve as primary servers for signed zones, you must enable DNSSEC on the grid master before you can sign zones. You must also enable DNSSEC on any grid member that serves as a secondary server for signed zones.

When you enable DNSSEC on a grid, you can set certain parameters that control the DNSSEC RRs, as described in Setting DNSSEC Parameters on page 555.

When you enable DNSSEC on a grid member or DNS view, you can set parameters that affect its operations as a secondary server, as described in Configuring Grid Members to Support DNSSEC as Secondary Servers on page 563.

To enable DNSSEC on a grid, member or DNS view:

1. **Grid**: From the Data Management tab, select the DNS tab. Expand the Toolbar and click Grid DNS Properties.
   - **Member**: From the Data Management tab, select the Members tab -> member check box and click the Edit icon.
   - **DNS View**: From the Data Management tab, select the Zones tab -> dns_view check box and click the Edit icon.

2. In the editor, click **Toggle Advanced Mode**.
3. When the additional tabs appear, click **DNSSEC**.
4. In the **DNSSEC** tab, select **Enable DNSSEC**.
5. Click **Save & Close**.

---

**Enabling DNSSEC**

You can enable DNSSEC on a grid, individual members, and DNS views. Because only grid masters can serve as primary servers for signed zones, you must enable DNSSEC on the grid master before you can sign zones. You must also enable DNSSEC on any grid member that serves as a secondary server for signed zones.

When you enable DNSSEC on a grid, you can set certain parameters that control the DNSSEC RRs, as described in Setting DNSSEC Parameters on page 555.

When you enable DNSSEC on a grid member or DNS view, you can set parameters that affect its operations as a secondary server, as described in Configuring Grid Members to Support DNSSEC as Secondary Servers on page 563.

To enable DNSSEC on a grid, member or DNS view:

1. **Grid**: From the Data Management tab, select the DNS tab. Expand the Toolbar and click Grid DNS Properties.
   - **Member**: From the Data Management tab, select the Members tab -> member check box and click the Edit icon.
   - **DNS View**: From the Data Management tab, select the Zones tab -> dns_view check box and click the Edit icon.

2. In the editor, click **Toggle Advanced Mode**.
3. When the additional tabs appear, click **DNSSEC**.
4. In the **DNSSEC** tab, select **Enable DNSSEC**.
5. Click **Save & Close**.
Setting DNSSEC Parameters

The grid master uses certain default parameters when it signs a zone and generates the DNSSEC RRs. You can change these defaults for the entire grid and for individual zones, in case you want to use different parameters for certain zones. The following sections describe the different parameters that you can set:

- About the DNSKEY Algorithm
- About Key Rollovers
- RRSIG Signatures on page 556

For information on setting these parameters, see Configuring DNSSEC Parameters on page 557

About the DNSKEY Algorithm

You can select the cryptographic algorithm that the grid master uses when it generates the KSK and ZSK. By default, it uses RSA/SHA1 and generates NSEC RRs. If you want the grid master to generate NSEC3 RRs, you must select DSA/NSEC3, RSA/SHA1/NSEC3, RSA/SHA-256/NSEC3 or RSA/SHA-512/NSEC3 as the algorithm for both the KSK and ZSK.

When you select an algorithm for the KSK, the grid master automatically assigns the same algorithm to the ZSK. You can change this algorithm, but the algorithms used by the KSK and ZSK must generate the same type of NSEC record. A zone cannot contain both NSEC and NSEC3 RRs.

About Key Rollovers

To reduce the probability of their being compromised, ZSKs and KSKs must be periodically changed. The time within which a key pair is effective is its rollover period. The rollover period starts as soon as a zone is signed. After a rollover period starts, you cannot interrupt or restart it unless you unsign the zone.

Zone-Signing Key Rollover

ZSK rollovers occur automatically on the grid master, using the double signature rollover method described in RFC 4641. This method provides for a grace period, which is half of the rollover period. The default ZSK rollover period is 30 days; thus the default grace period is 15 days.

At the end of a rollover period of a ZSK, the grid master generates a new ZSK key pair. It signs the zone with the private key of the new ZSK key pair, and consequently generates new RRSIG RRs with the new signatures. However, the grid master also retains the old ZSK key pair and RRSIG RRs. Thus during the grace period, the data in the zone is signed by the private keys of both the old and new ZSKs. Their corresponding public keys (stored in DNSSEC RRs) can be used to verify both the old and new RRSIGs.

The grace period also allows the data that exists in remote caches to expire and during this time, the updated zone data can be propagated to all authoritative name servers.

The grid master removes the old ZSK and its RRSIGs when the rollover grace period elapses.

Key-Signing Key Rollover

Unlike ZSK rollovers, which occur automatically, KSK rollovers must be initiated by an admin. When the KSK rollover is overdue or is due within seven days, the grid master displays a warning when admins log in. In addition, you can also check which KSKs are due for a rollover as described in Checking Key-Signing Keys on page 561.

The grid master also uses the double signature rollover method described in RFC 4641 for KSK rollovers.

When a user initiates a KSK rollover, the grid master sets the grace period to half the KSK rollover period. It generates a new KSK, and signs the DNSKEY records with the new KSK. Thus during the grace period, the DNSKEY records are signed by the private keys of both the old and new KSKs. Both the old and the new KSKs can be used to validate the zone. The grace period allows the old keys in remote caches to expire. In addition, the admin should also export the new KSK and send it to the recursive name servers that use the KSK as trust anchors.
If the KSK rollover is for a child zone and the primary server of the parent zone is a grid member, the grid master also inserts a DS record in the parent zone for the new DNSKEY in the child zone. If the primary server of the parent zone is external to the grid, the admin must export either the DS record or the new KSK to the admin of the parent zone. For information about exporting a KSK, see Exporting Trust Anchors on page 561.

The grid master then removes the old KSK and its RRSIG records when the grace period for the KSK rollover ends.

**About Key Rollovers and DNS TTLs**

Note that the KSK and ZSK rollover intervals affect TTLs used by RRs in signed zones.

A grace period is half of the key rollover interval. For example, if the KSK rollover interval is 1 year (365 days), then the grace period is 182.5 days; if the ZSK rollover interval is 30 days, then the grace period is 15 days.

The DNSKEY RRset in the zone is assigned a TTL that is the minimum of the KSK and ZSK grace period. In the preceding example, the minimum or lowest of these is 15 days. Therefore, the TTLs used for the DNSKEY RRset are 15 days (1296000 seconds).

All other RRs in the signed zone are limited to a “zone maximum TTL,” which is the grace period of the ZSK. In the example, this is also 15 days.

When the zone is initially signed, if the TTL of an RR exceeds the zone maximum TTL, the grid master reduces the TTL to the zone maximum TTL. Additionally, the TTL settings for the signed zone are set to override; the values are inherited from the grid DNS properties at that time, and the default TTL setting is reduced to the zone maximum TTL if the grid property exceeds it. If the zone is later unsigned, the zone DNS properties remain at their overridden settings.

**RRSIG Signatures**

As shown in the sample RRSIG record in RRSIG Resource Records on page 548, the signatures have an inception and an expiration time. The default validity period of signatures in RRSIG records on the grid master is four days. You can change this default, as long as it is not less than one day or more than 3660 days. The grid master automatically renews signatures before their expiration date.
Configuring DNSSEC Parameters

To set parameters at the grid or zone level:

1. **Grid:** From the Data Management tab, select the DNS tab. Expand the Toolbar and click Grid DNS Properties. 
   **Zone:** From the Data Management tab, select the DNS tab -> Zones tab -> zone check box, and click the Edit icon. Click Override to override the parameters.

2. In the editor, click **Toggle Advanced Mode.**

3. When the additional tabs appear, click **DNSSEC.**

4. In the DNSSEC tab, complete the following:
   - **Key-signing Key:** Select the cryptographic algorithm that the grid master uses when it generates the KSK. The default is **RSA/SHA1.** Select DSA/NSEC3 RSA/SHA1/NSEC3, RSA/SHA-256/NSEC3 or RSA/SHA-512/NSEC3 to use NSEC3 instead of NSEC records in signed zones. You can also select the default key length for the KSK. Following are the valid values for each algorithm:
     - **DSA:** The minimum is 512 bits and the maximum is 1024 bits, which is also the default. The key length must be a multiple of 64.
     - **DSA/NSEC3:** The minimum is 512 bits and maximum is 1024 bits, which is also the default. The key length must be a multiple of 64.
     - **RSA/MD5:** The minimum is 512 bits, the maximum is 4096 bits, and the default is 2048 bits.
     - **RSA/SHA1:** The minimum is 512 bits, the maximum is 4096 bits, and the default is 2048 bits.
     - **RSA/SHA1/NSEC3:** The minimum is 512 bits, the maximum is 4096 bits, and the default is 2048 bits.
     - **RSA/SHA-256:** The minimum is 512 bits, the maximum is 4096 bits, and the default is 2048 bits.
     - **RSA/SHA-256/NSEC3:** The minimum is 512 bits, the maximum is 4096 bits, and the default is 2048 bits.
     - **RSA/SHA-512:** The minimum is 1024 bits, the maximum is 4096 bits, and the default is 2048 bits.
     - **RSA/SHA-512/NSEC3:** The minimum is 1024 bits, the maximum is 4096 bits, and the default is 2048 bits.
   - **Key-signing Key Rollover Interval:** The minimum value is one day and the maximum is the time remaining to January 2038. The default is one year.
   - **Zone-signing Key:** Select the cryptographic algorithm that the grid master uses when it generates the ZSK. When you select an algorithm for the KSK, the grid master automatically selects the same algorithm for the ZSK. You can change the algorithm. However, the algorithms used by the KSK and ZSK must use the same type of NSEC record. You can also select the default key length for the zone-signing key. Following are the valid values for each algorithm:
     - **DSA:** The minimum is 512 bits and the maximum is 1024 bits. The default is 768 bits.
     - **DSA/NSEC3:** The minimum is 512 bits and maximum is 1024 bits. The default is 768 bits.
     - **RSA/MD5:** The minimum is 512 bits, the maximum is 4096 bits, and the default is 2048 bits.
     - **RSA/SHA1:** The minimum is 512 bits, the maximum is 4096 bits, and the default is 1024 bits.
     - **RSA/SHA1/NSEC3:** The minimum is 512 bits, the maximum is 4096 bits, and the default is 1024 bits.
     - **RSA/SHA-256:** The minimum is 512 bits, the maximum is 4096 bits, and the default is 1024 bits.
     - **RSA/SHA-256/NSEC3:** The minimum is 512 bits, the maximum is 4096 bits, and the default is 1024 bits.
     - **RSA/SHA-512:** The minimum is 1024 bits, the maximum is 4096 bits, and the default is 1024 bits.
     - **RSA/SHA-512/NSEC3:** The minimum is 1024 bits, the maximum is 4096 bits, and the default is 1024 bits.
   - **Zone-signing Key Rollover Interval:** The minimum value is one day and the maximum is the time remaining to January 2038. The default is 30 days.
   - **Signature Validity:** Specify the signature validity period for RRSIG RRs. The minimum is one day and the maximum is 3660 days. The default signature validity interval is four days.

5. Click **Save & Close.**
#### Signing a Zone

When it signs a zone, the grid master generates new DNSKEY key pairs. As shown in Figure 19.3, it uses the private key of the ZSK to sign the authoritative RRsets in the zone, and stores the corresponding public key in a DNSKEY record. It then uses the private key of the KSK to sign the DNSKEY records and stores the corresponding public key in another DNSKEY record. It stores the private keys in the grid database and stores the public keys in the DNSKEY records in the database.

*Figure 19.3 Zone Signing Process*

The grid master also does the following:

- It inserts NSEC/NSEC3 records for each label. The use of NSEC or NSEC3 RRs depends on the algorithm you selected for the KSK and ZSK. When you select DSA/NSEC3, RSA/SHA1/NSEC3, RSA/SHA-256/NSEC3 or RSA/SHA-512/NSEC3, the grid master uses NSEC3 records in signed zones. Note that a zone cannot contain both NSEC and NSEC3 RRs. If you want to change the type of NSEC records that a zone uses, you must unsign the zone, change the algorithm for the KSK and ZSK, and then re-sign the zone.

- It increments the SOA serial number and notifies the secondary servers that there is a change to its zone data. When the secondary servers check the serial number and see that it has been incremented, the secondary servers request a zone transfer.

- If the TTL of an RR in the zone exceeds the ZSK grace period, the grid master reduces the TTL to the ZSK grace period. (For information about the grace period, see *About Key Rollovers* on page 555.) Setting a TTL value that exceeds half of the rollover period is not allowed.

- If the KSK rollover period is less than the ZSK rollover period, the grid master sets the TTL of the DNSKEY RR to the KSK rollover period.

When it signs a subzone, the grid master automatically inserts DS records for parent zones that are hosted by grid members. To sign a zone:

1. From the Data Management tab, select the DNS tab.
2. Expand the Toolbar and click DNSSEC -> Sign Zone.
3. In the Sign Zone dialog box, the displayed zone name can either be the last selected zone or the zone from which you are signing. If no zone name is displayed or if you want to select a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Select a zone, and then click Sign Zone.
4. When the confirmation dialog displays, click Yes.
To view the records of the signed zone, from the Data Management tab, select the DNS tab -> Zones tab -> zone. Expand the Records section to list the RRs of the zone, as shown in Figure 19.4.

**Figure 19.4**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
<th>Comment</th>
<th>Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOA Record</td>
<td>Serial</td>
<td>4</td>
<td>Auto-created by</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MNAME</td>
<td>infobox.broadcom</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RNAME</td>
<td>please_set_ena</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Refresh</td>
<td>1088</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Retry</td>
<td>1080</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Expire</td>
<td>2419200</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Negative</td>
<td>caching TTL 900</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RRSIG Record</td>
<td>3600</td>
<td>DNSKEY 5 1 3600 20091102188</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RRSIG Record</td>
<td>3600</td>
<td>DNSKEY 5 1 3600 20091102188</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNSKEY Record</td>
<td>43200</td>
<td>257 5 39337</td>
<td>Authenticator: RSA 1920061759</td>
<td></td>
</tr>
<tr>
<td>DNSKEY Record</td>
<td>43200</td>
<td>256 5 2145</td>
<td>Authenticator: RSA 1920061759</td>
<td></td>
</tr>
<tr>
<td>RRSIG Record</td>
<td>28800</td>
<td>SOA 5 1 28800 20091102185</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NS Record</td>
<td></td>
<td>doddemo-2.infobox</td>
<td>Auto-created by</td>
<td></td>
</tr>
<tr>
<td>RRSIG Record</td>
<td>900</td>
<td>NSEC 5 1 900 20091102185718</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSEC Record</td>
<td>900</td>
<td>host2.test NS SOA RRSIG NSEC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
MANAGING SIGNED ZONES

After you sign a zone, you can do the following:

- You can add a DS RR at the delegation point for a signed subzone when the subzone is hosted on a non-Infoblox DNS server or an Infoblox server that is part of a different grid. For information, see Importing a Keyset on page 560.
- Trust anchors can be specified as DNSKEY RRs, DS RRs, and as a BIND trusted-keys statement. You can export any of these as trust anchors. For information, see Exporting Trust Anchors on page 561.
- You must change the KSK periodically, to ensure its security. For information, see Checking Key-Signing Keys on page 561 and Rolling Key-Signing Keys on page 561
- If, for any reason, the security of the keys are compromised, you can perform an emergency replacement of both the zone-signing and key-signing keys by unsigning the zone, and then re-signing it. For information about unsigning the zone, see Unsigning a Zone on page 562.
  Note that when you re-sign a zone, the grid master generates new ZSK and KSK pairs. You must send the new DNSKEY of the KSK to resolvers that use it as a trust anchor and generate new DS records and send them to the parent zones.
- You can move a signed zone to the Recycle Bin, from where you can delete it permanently or restore it. For information, see Deleting and Restoring Signed Zones on page 562.

In addition, signed zones can accept dynamic DNS updates. For information about configuring zones to accept dynamic DNS updates, see Configuring DNS Servers for DDNS on page 515.

Importing a Keyset

A keyset is a DS RRset, or a DNSKEY RRset which is used as input to generate the DS RRset. To import a keyset:

1. From the Data Management tab, select the DNS tab.
2. Expand the Toolbar and click DNSSEC -> Import Keyset.
3. In the Import Keyset dialog box, the displayed zone name can either be the last selected zone or the zone from which you are importing the keyset. If no zone name is displayed or if you want to select a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box from which you can select a zone.
4. Paste the KSK or DS record being imported. It must be a KSK or DS record, and must belong to an immediate subzone of the zone to which the record is being imported.
5. Click Import.

If you imported a DNSKEY RRset, the grid master uses the SHA-1 algorithm to generate the DS RRset, which it adds to the parent zone. If you imported a DS RRset, the grid master adds it to the parent zone. The grid master incrementally signs the DS RRset.
Exporting Trust Anchors

A trust anchor is a DNSSEC public key which is used by security-aware resolvers as the starting point for establishing authentication chains. A trust anchor can be specified as a DNSKEY RR or a DS RR, which contains the hash of a DNSKEY RR and can also be used to create a secure delegation point for a signed subzone in DNS servers.

In BIND, trust anchors are configured using the trusted-keys directive. A trusted key is a DNSKEY RR without the TTL, class and RR type. You can export the trust anchors for the selected zone in a format that can be used in a BIND trusted-keys directive.

To export trust anchors:
1. From the Data Management tab, select the DNS tab.
2. Expand the Toolbar and click DNSSEC -> Export Trust Anchors.
3. In the Export Trust Anchors dialog box, do the following:
   - The displayed zone name can either be the last selected zone or the zone from which you are exporting trust anchors. If no zone name is displayed or if you want to select a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box from which you can select one.
   - Select one of the following: DNSKEY records, DS records, or BIND trusted-keys statement
4. Click Export.
5. Specify the location of the exported file and click OK.

If you exported DS records, the exported file contains DS records that use the SHA-1 and SHA-256 algorithms.

Checking Key-Signing Keys

To check which key-signing keys are overdue for a rollover or are due to roll over within a week:
1. From the Data Management tab, select the DNS tab.
2. Expand the Toolbar and click DNSSEC -> Check Key-Signing Keys.
3. The KSK Rollover Due dialog box lists the key-signing keys that are due to rollover. It includes the domain name of the zone, DNS view (if there are multiple DNS views), and the number of days until the rollover.
4. Click Close.

Rolling Key-Signing Keys

Unlike ZSKs, which are automatically rolled over, KSK rollovers must be initiated by an admin. You can initiate a rollover before or after a rollover period, or when you need to replace the KSK for security reasons. You can initiate a rollover at anytime, as long as a KSK rollover is not already in progress for the zone.

To roll over key-signing keys:
1. From the Data Management tab, select the DNS tab.
2. Expand the Toolbar and click DNSSEC -> Roll Over Key-Signing Key.
3. In the Roll Over Key-Signing Key dialog box, the displayed zone name can either be the last selected zone or the zone from which you are rolling over key-signing keys. If no zone name is displayed or if you want to select a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box from which you can select one.
4. Click Roll Over.

You can export the new KSK and send it to the security-aware resolvers that use it as a trust anchor.
**Unsigning a Zone**

When you need to perform an emergency key rollover, you can unsign a zone and then re-sign it to generate new ZSK and KSK key pairs. When you unsign a zone, the grid master permanently removes all automatically generated DNSSEC records in the zone and parent zone. It does not remove any DS records associated with a child zone.

To unsign a zone:

1. From the **Data Management** tab, select the **DNS** tab.
2. Expand the Toolbar and click **DNSSEC -> Unsign Zone**.
3. In the **Unsign Zone** dialog box, the displayed zone name can either be the last selected zone or the zone from which you are signing. If no zone name is displayed or if you want to select a different zone, click **Select Zone**. When there are multiple zones, Grid Manager displays the **Zone Selector** dialog box from which you can select one. After you have selected a zone, click **Unsign Zone**.
4. When the confirmation dialog displays, click **Yes**.

**Deleting and Restoring Signed Zones**

When you delete a signed zone, the grid master unsigns the zone before moving it to the Recycle Bin. Unsigning the zone effectively deletes all auto-generated DNSSEC RRs; only user-defined DS records are retained and moved to the Recycle Bin as well. The grid master also retains the ZSK and KSK in its database, until you permanently delete the zone from the Recycle Bin.

When you restore a signed zone, the grid master restores it and re-signs its data sets with the original keys, which are also restored. You can also restore the user-defined DS records. The rollover period of the ZSK and KSK starts when the zone is signed after it is restored.

To delete a signed zone:

1. From the **Data Management** tab, select the **DNS** tab -> **Zones** tab.
2. Click the check box of the zone you want to delete.
3. Click the **Delete** icon.
4. Click **Yes** to confirm the deletion.

To restore a signed zone:

1. In the **Finder** panel, expand **Recycle Bin**.
2. Select the zone you want to restore.
3. Click the **Restore** icon.
Configuring Grid Members to Support DNSSEC as Secondary Servers

Any Infoblox grid member can function as a secondary server for DNSSEC signed zones. It can receive transfers of signed zones from the grid master or an external primary server, and from other secondary servers. It can also respond to queries for DNS data in DNSSEC signed zones for which it is a secondary server.

Configuring a Secondary Server for Signed Zones

The following are the tasks to configure an appliance as a secondary server for signed zones:

1. Enable DNSSEC on the appliance. For information, see Enabling DNSSEC on page 554.
2. Configure the appliance as a secondary server for the zone. For information, see Specifying a Secondary Server on page 406.
3. If the primary server for the signed zone is external, then you must allow zone transfers to the secondary server. For information, see Enabling Zone Transfers on page 485. If the primary server is the grid master, then the secondary server receives data through the grid replication process by default.
Configuring Recursion and Validation for Signed Zones

When you enable recursion on a grid member and it receives a recursive query for DNS data it does not have, it queries remote name servers that you specified in the Grid DNS Properties or Member DNS Properties editor. It then includes the DNSSEC data it retrieved through recursion in its responses to clients that requested DNSSEC RRs. You can enable the appliance to validate the responses of these servers for certain zones. On the appliance, you specify the zones to validate and configure their DNSKEY records as trust anchors. When the appliance validates a response for a zone configured with a trust anchor or for any of its child zones, the appliance starts with the DNSKEY that you configured and proceeds recursively down the DNS tree.

In the example shown in Figure 19.5, the following was configured on the NIOS appliance:

- Forwarder with the following IP address: 10.2.2.1
- Recursion was enabled
- DNSSEC and validation were enabled
- The corp100.com zone and its DNSKEY record were configured

Figure 19.5

1. A security-aware resolver sends a recursive query for data in the corp100.com zone.
2. The appliance does not have the requested data. It sends a request to the configured forwarder, 10.2.2.1.
3. The forwarder sends the response to the NIOS appliance along with the appropriate DNSSEC RRs.
4. The appliance uses the configured DNSKEY RR of the corp100.com zone to validate the response.
5. The appliance sends the response to the DNS client. The AD bit is set to indicate that the appliance validated the data.

Enabling Recursion and Validation for Signed Zones

The following are the tasks to enable recursion and validate recursively derived data:

1. Enable DNSSEC on the appliance. For information, see Enabling DNSSEC on page 554.
2. Enable validation and configure the trust anchor of each signed zone. For information, see Enabling DNSSEC Validation on page 565. You must configure at least one trusted DNSKEY RR.
3. Enable recursion on the appliance. For information, see Enabling Recursive Queries on page 482.
4. Complete any of the following:
   - Configure the forward, delegated, stub or root zones for the signed zones. For information, see Configuring Delegated, Forward, and Stub Zones on page 419 and Creating a Root Zone on page 400.
   - Configure global forwarders and custom root name servers, if needed. For information, see Using Forwarders on page 479 and About Root Name Servers on page 488.
Enabling DNSSEC Validation

To configure trust anchors and enable Infoblox name servers to validate responses:

1. Grid: From the Data Management tab, select the DNS tab. Expand the Toolbar and click Grid DNS Properties.
   Member: From the Data Management tab, select the Members tab -> member check box and click the Edit icon.
   DNS View: From the Data Management tab, select the Zones tab -> dns_view check box and click the Edit icon.
   To override an inherited property, click Override next to the property to enable the configuration.
2. In the editor, click Toggle Advanced Mode.
3. When the additional tabs appear, click DNSSEC.
4. In the DNSSEC tab, complete the following:
   — Enable DNSSEC validation: If you allow the appliance to respond to recursive queries, you can select this check box to enable the appliance to validate responses to recursive queries for domains that you specify. You must configure the DNSKEY RR of each domain that you specify.
   — Accept expired signatures: Click this check box to enable the appliance to accept responses with signatures that have expired. Though enabling this feature might be necessary to work temporarily with zones that have not had their signatures updated in a timely fashion, note that it could also increase the vulnerability of your network to replay attacks.
   — Trust Anchors: Configure the DNSKEY record that holds the KSK as a trust anchor for each zone for which the grid member returns validated data. Click the Add icon and complete the following:
     — Zone: Enter the FQDN of the domain for which the member validates responses to recursive queries.
     — Secure Entry Point (SEP): This check box is enabled by default to indicate that you are configuring a KSK.
     — Algorithm: Select the algorithm of the DNSKEY record: RSA/SHA1 (5), DSA (3), DSA/NSEC3 (6), RSA/MD5 (1), RSA/SHA1/NSEC3 (7), RSA/SHA-256 (8), or RSA-SHA-512 (10). This must be the same algorithm that was used to generate the keys that were used to sign the zones.
     — Public Key: Paste the key into this text box.
5. Click Save & Close.
Chapter 20 Configuring IP Routing Options

You can enable and configure anycast addressing as well as configure multiple IP address on loopback interfaces on the NIOS appliance, allowing the appliance to function in different network deployments. Configuring anycast on the appliance and within your network allows you to add redundancy and improve reliability for DNS server queries. Configuring multiple IP addresses on the loopback interface assists in server migration, server consolidation, or network address change.

You can also enable DNS services after configuring multiple IP addresses on a loopback interface on the appliance. This chapter contains the following sections:

- *Multiple IP Addresses on an Interface* on page 568
  - *IP Addresses on an Interface* on page 568
  - *Configuring IP Addresses on the Loopback Interface* on page 568
  - *Advertising Loopback IP Addresses to the Network* on page 569
  - *Configuration Example: Configuring IP Addresses on the Loopback Interface* on page 569
- *Anycast Addressing* on page 570
  - *Network Communication Types* on page 570
  - *OSPF* on page 572
  - *Configure OSPF on an Interface* on page 572
  - *Configure an Anycast Address on an Interface* on page 574
**Multiple IP Addresses on an Interface**

You can configure one or more IP addresses on the loopback interface of the NIOS appliance. This section discusses the following topics:

- IP Addresses on an Interface
- Configuring IP Addresses on the Loopback Interface
- Advertising Loopback IP Addresses to the Network on page 569
- Configuration Example: Configuring IP Addresses on the Loopback Interface on page 569

**IP Addresses on an Interface**

You can configure multiple IP addresses on the loopback interface on the NIOS appliance. Enabling multiple IP addresses allows you to configure the loopback interface as the source or destination for DNS queries. Configuring multiple IP addresses on the loopback interface is helpful in different scenarios, such as DNS server migration. Consider the following scenarios where configuring multiple IP addresses on the loopback interface is beneficial:

- Consolidation of DNS servers to a smaller number of servers: You can configure these different IP addresses for multiple servers onto a single interface of a NIOS appliance during migration to minimize any downtime for users.
- Change in the network addresses of DNS servers: You can configure the appliance interface with both the current server IP address and the new IP address, minimizing any downtime during the migration to the new IP address.
- Migration of DNS servers.
- Separation of DNS traffic. You can select a loopback address as the source for DNS queries, and select another port as the source for notify message and zone transfer requests.

All the scenarios listed require a way to provide uninterrupted services during any change in the network. Configuring multiple IP addresses to the loopback interface provides the administrator tools to provide continuous service during server migration.

**Configuring IP Addresses on the Loopback Interface**

You can configure one or more IP addresses on the loopback interface of the appliance.

To configure an IP address on the loopback interface, perform the following tasks:

1. From the Grid tab, select the Grid Manager tab -> grid_member check box -> Edit icon.
2. Select the Network -> Basic tab of the Grid Member Properties editor.
3. Click the Add icon of the Additional Ports and Addresses table, select Additional Address (loopback), and complete the following:
   - **Address**: Enter the IP address you want to configure on the loopback interface.
   - **Subnet Mask**: You cannot change the netmask for the loopback interface. It is set to 255.255.255.255.
4. Click Save & Close.

To configure multiple IP addresses on the loopback interface, repeat the previous steps for each IP address you want to add.

To specify a loopback address as the source for DNS queries, see Specifying Port Settings for DNS on page 482.

**Note:** If you are configuring the interface on a grid master, the grid is temporarily disrupted upon saving the configuration and restarting services on the appliance. The grid reconnects automatically and the appliance regains the role as grid master after this short delay.
Advertising Loopback IP Addresses to the Network

Configuring multiple IP addresses on the loopback interface relies on the upstream router to populate routes to the loopback interface.

If you are configuring non-anycast addresses on the loopback interface, or you are not running OSPF within your network, you must configure the upstream router to reach the NIOS appliance through a static route. Consult your network administrator for more information about configuring static routes from the router to the additional IP addresses on the loopback interface.

Configuration Example: Configuring IP Addresses on the Loopback Interface

You can configure one or more IP addresses on the appliance interface. In this example, configure the following IP addresses on the loopback interface of the appliance: 10.1.10.1/32, 10.1.10.2/32, and 10.16.1.1/32.

Figure 20.1 Configuring an IP Address on an Interface

Configure the device with the following IP addresses on the loopback interface:
10.1.10.1/32
10.1.10.2/32
10.16.1.1/32
To configure IP addresses on the loopback interface of an appliance:

1. From the Grid tab, select the Grid Manager tab → grid_member check box → Edit icon.
2. Select the Network → Basic tab of the Grid Member Properties editor.
3. Click the Add icon of the Additional Ports and Addresses table, select Additional Address (loopback), and complete the following:
   - Address: Enter 10.1.10.1 as the IP address.
   - Subnet Mask: You cannot change the netmask for the loopback interface. It is set to 255.255.255.255.
4. Repeat step 3 to configure 10.1.10.2/32 and 10.16.1.1/32 on the loopback interface of the NIOS appliance.
5. Click Save & Close.
6. Enable DNS services for the additional IP addresses.

**ANYCAST ADDRESSING**

**Note:** This feature is not supported on vNIOS appliances on Riverbed and Cisco.

The NIOS appliance supports DNS services for anycast addresses on the loopback interface. This section provides information on the following topics:

- *Network Communication Types*
- *OSPF* on page 572
- *Configure OSPF on an Interface* on page 572
- *Configure an Anycast Address on an Interface* on page 574

**Network Communication Types**

There are primarily four types of communication utilized within a network: unicast, broadcast, multicast, and anycast. Each of the types of network communication are described in the following section, and focuses on anycast addressing:

- **Unicast** describes a one-to-one network communication between a single sender and a single recipient. The routing protocol determines the path through the network from the sender to the recipient based on the specific protocol or routing scheme. Unicast also describes the address type assigned to the recipient, used by the routing protocol to determine the path to the recipient.

- **Multicast** describes a one-to-many network communication between a single sender and a specific group of recipients. All members within the group are intended recipients and each member receives a copy of the data from the sender. Multicast also describes the address type assigned to the group of recipients, used by the routing protocol to determine the path to the group.

- **Broadcast** is similar to multicast, the exception being that data is sent to every possible destination regardless of the groups or subnetwork. There is no specific group of recipients.

- **Anycast** describes a one-to-nearest communication between a single sender and the nearest recipient within a group. The routing protocol chooses one recipient within a target group based on the routing algorithm for the specific protocol, and sends data to that recipient only.
Network routers use routing protocols such as the (OSPF) Open Shortest Path First to determine the best path to the nearest server. The NIOS appliance advertises the route information to the upstream router, a router that forwards data on the network link and determines the forwarding path to destinations. To enable anycast for DNS queries, you configure two or more DNS servers with the same anycast address on the loopback interfaces. When a DNS query is sent to this IP address, the nearest server within the group of servers configured with the IP address responds to the DNS query. In the case where the nearest server becomes unavailable, the next nearest server responds to the query. From the client perspective, anycasting is transparent and the group of DNS servers with the anycast address appears to be a single server.

**Figure 20.2 Anycast Addressing**

Anycasting for DNS provides the following benefits:

- **Improved Reliability**: Anycast provides improved reliability because DNS queries are sent to an anycast IP address configured on multiple DNS servers. If the nearest server is offline, then the next DNS server with the anycast IP address responds to the query.
- **Load Distribution**: Anycast distributes the load across multiple DNS servers.
- **Improved Performance**: The NIOS appliance uses routing protocol algorithms (such as OSPF) to advertise anycast routing information to the upstream router. The upstream router determines the best route to the nearest DNS server. Anycast enables the queries to reach the nearest server faster, as well as providing faster responses to queries.

The NIOS appliance provides the following support for DNS anycast:

- You can configure up to ten anycast IP addresses for each grid member.
- The appliance advertises routing information through OSPF. OSPF determines the nearest server to send DNS queries.
- The appliance advertises and withdraws route information based on reachability information to DNS servers sent by OSPF route advertisements. OSPF uses routing algorithms to determine the best path to servers.

For more information about anycast addressing, see RFC 1546 “Host Anycasting Service”.

---

**Anycast Query**

Anycast: In this example, the desktop sends a DNS query to 10.128.1.12, the anycast address. Many servers possess the anycast address. The routing protocol selects the nearest server and the desktop queries that server. The nearest server sends back a response after receiving the query.

- **Client**
  - europe.corp100.com

- **DNS Server (example: nslookup)**
  - europe.corp100.com
  - america.corp100.com
  - asia.corp100.com

- **10.128.1.12**

- **Internet**

A routing protocol usually determines the nearest server. In this example, the nearest DNS server is the Europe server, since the client is located in Europe.
OSPF

The OSPF routing protocol is a link-state protocol based on the Dijkstra algorithm used to calculate the shortest path to a destination address. This protocol uses a link-state database created using routing information advertised from neighbors and peers, each with costs based on the state of that link to the destination.

The NIOS appliance uses the OSPF routing protocol to advertise routes for an anycast address on the appliance to the upstream router. The upstream router uses the OSPF advertisements to determine the nearest server from a group of servers. The upstream router then can forward the query to the chosen DNS server.

Routers use this OSPF route advertisement to determine which of a group of DNS server is the nearest server. The sender queries the chosen DNS server only. In practicality, the NIOS appliance relies upon OSPF to determine the best route for DNS queries to take to the nearest DNS server.

OSPF network topologies consist of administrative domains called OSPF areas. An area is a logical collection of OSPF routers, servers and other network devices that have the same area identifier. A router within an area keeps an OSPF database for its OSPF area only, reducing the size of the database that is maintained.

You can configure authentication for OSPF advertisements to ensure that the routing information received from a neighbor is authentic and the reachability information is accurate.

To enable the appliance to support OSPF and advertising anycast addresses, you must configure the LAN(HA) interface as an OSPF advertising interface.

Note: If the NIOS appliance is part of an HA pair, the HA interface is chosen. If the appliance is not part of an HA pair, the LAN interface is chosen.

For more information about the OSPF routing protocol, see RFC 2328 “OSPFv2”.

Configure OSPF on an Interface

You can configure the LAN(HA) interface on the NIOS appliance as an OSPF advertising interface. The interface advertises the OSPF routing information out to the network so that routers can determine the best server to query. For the NIOS appliance, you must configure the LAN(HA) interface as an OSPF advertising interface, and assign an area ID on the interface to associate it with a specific area. The advertising interface sends out routing advertisements about the anycast address into the network out to upstream routers.

Note: You must configure an OSPF advertising interface on the appliance to support anycast addressing.

To configure an interface to be an OSPF advertising interface, perform the following tasks:

1. From the Grid tab, select the Grid Manager tab -> grid_member check box -> Edit icon.
2. Select the Anycast tab of the Grid Member Properties editor.
3. Click the Add icon of the OSPF Area Configuration table and enter the following information to configure the LAN(HA) interface as the OSPF advertising interface:
   - Area ID: Enter the OSPF area identifier of the network containing the upstream routers, in either an IP address format or a decimal format. All network devices configured with the same OSPF area ID belong to the same OSPF area. The area ID configured on the grid member must match the area ID of the upstream router configuration.
— **Area Type:** Select the type of OSPF area to associate with the advertising interface from the drop-down list. The area type configured on the grid member must match the area type of the upstream router configuration. The supported area types are described as follows:
  
  — **Standard:** A standard area has no restrictions on routing advertisements, and connects to the backbone area (area 0) and accepts both internal and external link-state advertisements.
  
  — **Stub:** A stub area is an area that does not receive external routes.
  
  — **Not-so-stubby:** A not-so-stubby area (NSSA) imports autonomous system (AS) external routes and sends them to the backbone, but cannot receive AS external routes from the backbone or other areas.

— **Authentication Type:** Select the authentication method to use to verify OSPF routing advertisements on the interface. The authentication type configured on the grid member must match the authentication type of the upstream router configuration. The supported authentication types are described as follows:
  
  — **None:** No authentication for OSPF advertisement.
  
  — **Simple:** A simple password for OSPF advertisement authentication, in clear text.
  
  — **MD5:** An MD5 hash algorithm to authenticate OSPF advertisements. This is the most secure option.

— **Authentication Key ID:** Enter the key identifier to use to specify the correct hash algorithm after you select MD as your OSPF authentication type. The authentication key ID configured on the grid member must match the authentication key ID of the upstream router configuration.

— **Authentication Key:** Enter the authentication password to use to verify OSPF advertisements after you select Simple or MD as your OSPF authentication type. Specify a key string between 1 to 8 characters for Simple authentication, and a string between 1 to 16 characters for MD5 authentication. The authentication key configured on the grid member must match the authentication key of the upstream router configuration.

— **Cost:** Select one of the following:
  
  — **Calculate Automatically:** Select this check box to auto generate the cost to associate with the advertising OSPF interface to the appliance. If this check box is not selected, then you specify the cost value explicitly. Calculate the cost as 100,000,000 (reference bandwidth) divided by the interface bandwidth. For example, a 100Mb interface has a cost of 1, and a 10Mb interface has a cost of 10.
  
  — **Fixed Metric:** Enter the cost to associate with the advertising OSPF interface to the appliance.

— **Hello Interval:** Specify how often to send OSPF hello advertisements out from the appliance interface, in seconds. Specify any number from 1 through 65,535. The default value is 10 seconds. The hello interval configured on the grid member must match the hello interval of the upstream router configuration.

— **Dead Interval:** Specify how long to wait before declaring that the NIOS appliance is unavailable and down, in seconds. Specify any number from 1 through 65,535. The default value is 40 seconds. The dead interval configured on the grid member must match the dead interval of the upstream router configuration.

— **Retransmit Interval:** Specify how long to wait before retransmitting OSPF advertisements from the interface, in seconds. Specify any number from 1 through 65,535. The default value is 5 seconds. The retransmit interval configured on the grid member must match the retransmit interval of the upstream router configuration.

— **Transmit Delay:** Specify how long to wait before sending an advertisement from the interface, in seconds. Specify any number from 1 through 65,535. The default value is 1 second. The transmit interval configured on the grid member must match the transmit interval of the upstream router configuration.

— **Click Add** to add the interface to the table.

4. **Click **Save & Close.**
Configure an Anycast Address on an Interface

You can configure anycast addressing on the loopback interface of the NIOS appliance by performing the following tasks:

- Specify the address as an anycast address.
- Configure the appliance to listen on the anycast address.

**Note:** Anycast addressing is supported on the loopback interface only. All other interfaces are greyed out under the Bound Interface drop-down list when you select the Anycast check box.

To enable and configure anycast addressing on the loopback interface:

1. From the Grid tab, select the Grid Manager tab -> grid_member check box -> Edit icon.
2. Select the Anycast tab of the Grid Member Properties editor.
3. Click the Add icon of the Anycast Interfaces table and complete the following:
   - **Address:** Enter the IP address you want to configure on the loopback interface.
   - **Subnet Mask:** You cannot change the netmask for the loopback interface. It is set to 255.255.255.255.
   - **Comments:** Enter a text string to help identify this interface and IP address.
4. Click Save & Close.

To enable the appliance to listen on the anycast address:

1. From the Data Management tab, click the DNS tab -> Members tab -> grid_member check box -> Edit icon.
2. In the Member DNS Properties editor, click Toggle Advanced Mode.
3. When the additional tabs appear, click the Advanced subtab of the General tab.
4. Click the Add icon in the Listen on these additional IP addresses table.
5. Specify the IP address of the loopback interface.
6. Click Save & Close.
**Part 4 DHCP**

This section describes how to configure the grid to provide DHCP services. It includes the following chapters:

- Chapter 21, *Infoblox DHCP Services*, on page 577
- Chapter 22, *Managing DHCP Data*, on page 589
- Chapter 23, *Configuring DHCP Services*, on page 617
- Chapter 24, *Managing DHCP Templates*, on page 643
- Chapter 25, *DHCP Failover*, on page 655
- Chapter 26, *Managing Leases*, on page 663
- Chapter 27, *Configuring DHCP Filters*, on page 673
- Chapter 28, "*Authenticated DHCP*", on page 693
Chapter 21 Infoblox DHCP Services

This chapter describes an overview of the Infoblox DHCP services. It contains the following sections:

- **About Infoblox DHCP Services** on page 578
- **Configuring DHCP Overview** on page 579
  - **DHCP Configuration Checklist** on page 581
- **About DHCP Inheritance** on page 582
  - **Overriding DHCP Properties** on page 583
  - **Viewing Inherited Values** on page 583
- **UTF-8 Encoding** on page 587
About Infoblox DHCP Services

DHCP (Dynamic Host Configuration Protocol) is a network application protocol that automates the assignment of IP addresses and network parameters to DHCP-configured network devices (DHCP clients). When a DHCP client connects to a network, it sends a request to obtain an IP address and configuration information from the DHCP server. The DHCP server manages a pool of IP addresses and configuration information such as default gateway, domain name, and DNS server. Depending on the configuration, the DHCP server either assigns or denies an IP address to a client request. It also sends network configuration parameters to the client.

As illustrated in Figure 21.1, when a DHCP client requests an IP address, it sends a DHCPDISCOVER message to the router, which can act as a relay agent. The router forwards the message to the DHCP server. When the DHCP server receives the DHCPDISCOVER message, it determines the network segment to which the client belongs and assigns an IP address. The DHCP server then sends a DHCPOFFER message that includes the IP address and other network configuration information. When the router receives the DHCPOFFER message, it broadcasts the message to the client that originates the DHCPDISCOVER message.

Figure 21.1  IP Address Allocation Process

You can configure a NIOS appliance as a full-featured DHCP server that assigns IP addresses to DHCP clients and manages the information about DHCP client configuration parameters. The Infoblox DHCP server complies with a number of DHCP RFCs (see Appendix A Product Compliance). To set up the appliance as a DHCP server, you configure DHCP properties and enable DHCP services on the appliance. For information about the configuration process, see Configuring DHCP Overview on page 579 and DHCP Configuration Checklist on page 581.

Note: Limited-access admin groups can access certain DHCP resources only if their administrative permissions are defined. For information on setting permissions for admin groups, see Chapter 3, Managing Administrators.
Configuring DHCP Overview

An overview of the complete DHCP configuration process is outlined in the following diagram (and continued on the next page), illustrating the main steps for preparing a NIOS appliance for use:

1. Decide how the network will be used.
   - Specify the network address and netmask.
   - Select the member(s) that provide DHCP services for this network.
   - Specify the network address and netmask.

2. Assign Member(s)
   - Create failover associations
   - Configure the DHCP failover properties

* Do not start DHCP services when configuring members until the configuration is complete.
… continued from previous page.

Yes

Define DHCP address ranges for this network.

Specify the IP address and MAC address for each fixed address.

No

Do you want to define fixed addresses for this network?

Configure the network-level DHCP properties.

Yes

Do you want to add more ranges?

No

See 1 in the previous diagram to repeat the process of adding more networks on additional members.

Yes

Do you want to add more networks?

No

See 2 in the previous diagram to repeat the process of enabling the DHCP services on additional members.

Yes

Do you have additional members to configure for DHCP?

No

Initial configuration of DHCP networks is complete.

Start the DHCP services on members.
## DHCP Configuration Checklist

The following checklist includes the major steps for configuring DHCP services:

<table>
<thead>
<tr>
<th>Step</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete the appliance configuration for each member in the grid.</td>
<td>• Managing Appliance Operations on page 201</td>
</tr>
</tbody>
</table>
| Decide if you want to configure DHCP properties for the grid and members. | • Configuring General DHCP Properties on page 619  
• Configuring DHCP Lease Times on page 621  
• Select one of the following: on page 623  
• Configuring BOOTP Properties on page 625  
• Applying DHCP Options on page 629  
• Chapter 18, Configuring DDNS Updates from DHCP, on page 501  
• Configuring Thresholds for DHCP Ranges on page 634  
• Configuring DHCP Logging on page 637  
• Configuring the Lease Logging Member on page 665 |
| Decide if you want to configure a DHCP failover association. | • Configuring Failover Associations on page 657 |
| Configure networks based on your network requirements and decide if you want to override the grid or member DHCP configuration for the networks. | • Adding IPv4 Networks on page 594  
• Modifying IPv4 Networks on page 597 |
| Decide if you want to configure fixed addresses and whether to override the upper level DHCP properties for the fixed addresses. | • Adding Fixed Addresses on page 609  
• Modifying Fixed Addresses on page 610 |
| Define DHCP ranges and decide whether to override the upper level DHCP properties for the ranges. | • Adding DHCP Ranges on page 604  
• Modifying DHCP Ranges on page 606 |
| Enable DHCP services on the member. | • Starting DHCP Services on a Member on page 639 |

**Note:** When the DHCP services are enabled, ensure that you restart services on the appliance after you make changes to any DHCP properties.
About DHCP Inheritance

When you configure DHCP properties for the grid, members, networks, shared networks, DHCP ranges, fixed addresses, reservations, host addresses, and roaming hosts, the appliance applies the configured properties hierarchically. For example, when you set DHCP properties for the grid, all DHCP objects inherit the properties from the grid unless you override them at a specific level. Properties set at the member level override grid-level settings and apply to the objects that the member serves. Properties set at the network level override member-level settings and apply to the objects within the network. Properties set for a DHCP range override those set at higher levels. You can also set specific properties that apply only to fixed addresses, reservations, host addresses, and roaming hosts.

Figure 21.2 illustrates some inheritance scenarios that can occur in a grid. As shown in the figure, the authoritative server configuration set for the grid is inherited by the members. Since Member 1 has no overrides and Member 2 overrides the authoritative server configuration, they have different DHCP configurations. Grid Manager applies DHCP properties hierarchically from the grid down. Therefore, a DHCP object below the member level can inherit DHCP properties with multiple values from multiple sources. In Figure 21.2, network 10.1.1.0/24 inherits multiple values (True and False) from the members for the authoritative server configuration. The shared network, which includes 10.1.1.0/24, inherits DHCP properties from both members. For DHCP range 10.1.1.11 - 10.1.1.50, since Member 1 is the assigned member, it inherits properties from Member 1 and the network. The fixed address 10.1.1.2 overrides the BOOTP settings and inherits the authoritative server configuration from both members and the network.

Figure 21.2 Inheritance Hierarchy in a Grid

When a DHCP property contains inherited values from different sources, the appliance displays the corresponding information when you create or modify an object. Based on the information provided, you can then decide whether to override or keep the inherited values. You must have read/write permissions to the DHCP resources to override inherited values. You can only view inherited values and paths if you have read-only permissions.
About DHCP Inheritance

Overriding DHCP Properties

DHCP properties configured at the grid level apply to the entire grid. You can choose to keep the inherited properties or override them when you configure the properties for a member, network, shared network, DHCP range, fixed address, host address, or roaming host. For example, you can override the values of DHCP properties inherited from a member and enter unique values for a network that is configured for DHCP.

To override an inherited value:

1. In a wizard or editor, click **Override** next to a property to enable the configuration. The **Override** button changes to **Inherit**.
2. Enter a new value to override the inherited value.

Viewing Inherited Values

When you configure DHCP properties that contain inherited values, the appliance displays the information based on the inheritance sources. The following table summaries what the appliance can display:

<table>
<thead>
<tr>
<th>When you see...</th>
<th>it means...</th>
<th>For details, see...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inherited From <code>&lt;object&gt;</code></td>
<td>the DHCP property has a definite value from an inheritance source.</td>
<td><strong>Simple Inheritance.</strong></td>
</tr>
<tr>
<td>Inherited From Upper Level</td>
<td>the appliance cannot determine the inherited value or inheritance source for the DHCP property.</td>
<td><strong>Unknown Inheritance</strong> on page 584.</td>
</tr>
<tr>
<td>Inherited From Multiple</td>
<td>the DHCP property has the same value that it inherits from multiple sources.</td>
<td><strong>Multiple Inheritance</strong> on page 585.</td>
</tr>
<tr>
<td>Settings Inherited from Multiple</td>
<td>the DHCP property has multiple values that it inherits from multiple sources, and you can view the values and their corresponding sources by clicking the <strong>View Multiple Inheritance Scenarios</strong> link.</td>
<td><strong>Multiple Inheritance</strong> on page 585.</td>
</tr>
</tbody>
</table>

Simple Inheritance

When a DHCP property has an inherited value from a specific source, the appliance displays the value. It also displays Inherited From `<object>` (where `<object>` can be the grid, member, network, shared network, or DHCP range) to indicate the source from which the value is inherited.

For example, when you set DHCP properties at the grid level and do not override the properties at any level, the members, networks, shared networks, DHCP ranges, fixed addresses, reservations, host addresses, and roaming hosts inherit these properties from the grid. The appliance displays the property value and Inherited From Grid Infoblox for each configured DHCP property, as shown in **Figure 21.3**.
Unknown Inheritance

In some cases, DHCP properties may not have definite inherited values and inheritance sources. The following are examples of unknown inheritance:

- The appliance cannot determine the inheritance sources of the DHCP properties in a template until you use the template to create an object.
- When a network or a DHCP range does not have an assigned member, it does not have a clear definition of an inheritance source because a network or a DHCP range inherits properties from a member.
- When individual networks in a shared network do not have member assignments, the shared network has unknown inheritance because the shared network inherits DHCP properties from a member and its networks.
- All roaming hosts have unknown inheritance because the DHCP properties can be inherited from different DHCP ranges within a network view.

In cases where the source of the inheritance is unknown, the appliance displays Inherited From Upper Level as the inheritance source. As shown in Figure 21.4, network 10.1.1.0 has unknown lease time value because it does not have any assigned member.

Figure 21.4 Unknown Inheritance
Multiple Inheritance

As illustrated in Figure 21.2, a network can have multiple inherited values and inheritance sources for DHCP properties when it is served by multiple members. When an object inherits a DHCP property from different sources, the property value can be the same from all sources or it can be different. When the value is the same, the appliance displays the value in the property field. When there are multiple values inherited from multiple paths, the appliance displays the information to indicate so.

In a grid, when two members serve the same network, the network inherits DHCP properties from both associated members. If both members have the same configured DHCP property, the network inherits the same value from both members. For example, when DHCP network 10.1.1.0 has two associated members and both members have the lease time set for 20 hours, the appliance displays the lease time value and Inherited From Multiple to indicate the value is inherited from multiple sources, as shown in Figure 21.5.

Figure 21.5 Multiple Inherited Paths with the Same Inherited Value

In the same grid with the two members serving the same network, the network inherits different values for the same properties if you override the grid configuration on one member but not on the other. For example, you can configure different PXE lease times for the members and configure a member as an authoritative DHCP server for the domain and the other not. In this case, the appliance displays Settings inherited from multiple ancestors and provides a View Multiple Inheritance Scenarios link so you can view the inherited values and paths, as shown in Figure 21.6.

Figure 21.6 Multiple Inheritance Sources with Multiple Values
For example, to view the multiple inherited values of the **Authoritative** field, click **View Multiple Inheritance Scenarios**, and the **Multiple Inheritance Viewer** displays the inherited values from the two members. Since member1.foo.net does not have a configured value for this field, the viewer displays **Not Set**, as shown in *Figure 21.7*. You can use this information to determine whether you want to keep the inherited values or configure new ones.

*Figure 21.7  Multiple Inheritance Viewer*

Another scenario of multiple inherited levels is when you have multiple DHCP properties that can inherit the same or multiple values from different sources. For example, when you configure multiple DHCP custom options, each of the options can inherit the same or multiple values from multiple paths. You can override the inherited options and configure new ones at a specific level other than the grid level. Though these options are grouped under **DHCP Custom Options**, the appliance treats each of them as a separate property. The appliance groups the inherited options at the top, as shown in *Figure 21.8*. You can override these options but you cannot delete them. For multiple values inherited from multiple sources, you can view the values in the **Multiple Inheritance Viewer** by clicking **View Inheritance**, as shown in *Figure 21.9*.

*Figure 21.8  DHCP Custom Options with Multiple Inheritance Sources*

*Figure 21.9  Multiple Inheritance Viewers for Options*

When you configure email notification for the grid or grid member from the **Data Management** tab -> **Grid** tab, the email address you enter there is inherited by the DHCP configuration for the grid, members, networks, and DHCP ranges unless you override it at a specific level. The appliance uses this email address to send notification for a DHCP range when the DHCP usage crosses either the effective watermark threshold. For information, see **Configuring Thresholds for DHCP Ranges** on page 634.
UTF-8 Encoding

When you configure the appliance as a DHCP server, the appliance supports UTF-8 encoding of host names that are encoded with Microsoft Windows code pages. You can configure the DHCP services on the appliance to convert these client host names to UTF-8 characters. The appliance stores the UTF-8 encoded host names in the database. If you also configure the DHCP services on the appliance to perform DDNS updates, the appliance sends the UTF-8 encoded host names in the DDNS updates. You can configure the UTF-8 encoding of host names at the grid DHCP service and member DHCP service levels. For information on UTF-8 encoding, see Multilingual Support on page 54.

The appliance displays the host names in their original characters in the following:

- DHCP lease history
- DHCP lease details
- IP address management
- Syslog
- Audit log
Chapter 22 Managing DHCP Data

This chapter explains how to configure and manage DHCP data. It contains the following sections:

- **About Network Views** on page 591
  - Adding Network Views on page 592
  - Modifying Network Views on page 593
  - Deleting Network Views on page 593
- **About DHCP Networks** on page 594
  - Adding IPv4 Networks on page 594
  - Viewing IPv4 Networks on page 596
  - Modifying IPv4 Networks on page 597
  - Associating Networks with Zones on page 598
  - Viewing the Networks Associated with a Zone on page 599
  - Deleting IPv4 Networks on page 599
- **About Shared Networks** on page 600
  - Adding Shared Networks on page 600
  - Viewing Shared Networks on page 601
  - Modifying Shared Networks on page 601
  - Deleting Shared Networks on page 602
- **About DHCP Data** on page 603
  - Guidelines for the Next Available IP Address on page 603
- **Configuring DHCP Address Ranges** on page 604
  - Adding DHCP Ranges on page 604
  - Viewing DHCP Ranges on page 605
  - Modifying DHCP Ranges on page 606
  - Deleting DHCP Ranges on page 607
  - Excluding Addresses from DHCP Ranges and Templates on page 607
- **Configuring Fixed Addresses** on page 608
  - Adding Fixed Addresses on page 609
  - Modifying Fixed Addresses on page 610
  - Deleting Fixed Addresses on page 610
- **Configuring Reservations** on page 611
  - Adding Reservations on page 611
  - Modifying Reservations on page 612
• Configuring Roaming Hosts on page 613
  — Enabling Support for Roaming Hosts on page 613
  — Adding Roaming Hosts on page 613
  — Viewing Roaming Hosts on page 614
  — Modifying Roaming Hosts on page 615
  — Deleting Roaming Hosts on page 615
About Network Views

A network view is a single routing domain with its own networks and shared networks. You can manage the networks in one network view independently of the other network views. Changes in one network view are not reflected in other network views. Because network views are mutually exclusive, the networks in each view can have overlapping address spaces with multiple duplicate IP addresses without impacting network integrity.

For example, two corporations, Corp 100 and Corp 200, merge. They each have their own networks and DNS domains. They also have their own private IP address spaces in the 10.0.0.0/24 network. Both corporations have DHCP and DNS servers, and use dynamic DNS updates. The DHCP servers of each corporation serve IP addresses for networks in their respective corporations. The DHCP clients in each corporation update DNS zones within their DNS domains.

They plan to migrate the networks and hosts in Corp 200 to the Corp 100 address space and the corp100.com domain. To support both networks in the meantime and to facilitate the migration, you can configure an Infoblox grid to centrally manage the networks and domains of both corporations. As shown in Figure 22.1, you can configure network views for each corporation and manage their networks independently of the other.

Member 1 serves DNS and DHCP to Corp 100. The networks of Corp 100 are contained in the corp 100 network view, which is associated with both the internal and external DNS views of the corp100.com domain. Member 2 serves DNS and DHCP to Corp 200. The networks of Corp 200 are in the corp 200 network view, which is associated with both the internal and external DNS views of the corp200.com domain. The two corporations have one overlapping network, 10.1.1.0/24.

Figure 22.1 Two Network Views Managed By a Grid
A grid member can serve one network view only, but a network view can be served by multiple grid members. DHCP failover associations must be defined within a single network view, and both the primary and secondary peer must serve the same network view.

The NIOS appliance provides one default network view. You can rename the default view and change its settings, but you cannot delete it. There must always be at least one network view in the appliance. If you do not need to manage overlapping IP address spaces in your organization, you can use the system-defined network view for all your networks. You do not need to create additional network views. But if there are overlapping IP address spaces and you need more than one network view, you can create up to 100 network views.

Each network view must be associated with at least one DNS view. The default network view is always associated with the default DNS view, which also cannot be deleted. When you create a network view, the appliance automatically creates a corresponding DNS view with the same name as the network view, but with "default" prepended to the name. You can then rename that system-defined DNS view, but you cannot delete it.

A network view can be associated with multiple DNS views (as shown in Figure 22.1), but a DNS view cannot be associated with more than one network view. Each network view must be associated with a unique set of DNS views.

You can initiate a network discovery in only one network view at a time. When you run a discovery task, the appliance sends updates to all DNS views associated with the network view. (For information about network discoveries, see Chapter 33, Network Discovery, on page 805.)

Adding Network Views

All networks must belong to a network view. You can use the default network view on the appliance and create additional network views, as needed. If you plan to enable DDNS (dynamic DNS) updates on any of the networks, DHCP ranges and fixed addresses in the network view, you must set parameters that specify which DNS view is updated for each network view.

To create a network view:

1. From the Administration tab, select the Network Views tab, and then click the Add icon.
2. In the Network View wizard, do the following:
   - **Name**: Enter the name of the network view.
   - **Comment**: Enter useful information about the network view.
3. Click Next to enter values for required extensible attributes or add optional extensible attributes for the network view. For information, see About Extensible Attributes on page 222.
4. Click Next and select one of the following:
   - **Save & Edit**: Save the entry and continue to edit.
   - **Save & New**: Save the entry and open a new wizard.
   - **Save & Close**: Save the entry and close the wizard.
   - **Configure DDNS Properties**: Configure the DNS zones that are associated with the network view to receive DDNS updates. When you select this option, the Configure DDNS Properties dialog box appears. The appliance saves the network view entry before it opens the Configure DDNS Properties dialog box. For information, see Configuring DDNS Updates from DHCP on page 501.
Modifying Network Views

1. From the Administration tab, select the Network Views tab -> network_view check box, and then click the Edit icon.

2. The Network View editor provides the following tabs from which you can edit data:
   - **General**: You can modify all the fields in this tab.
   - **Members**: This tab displays the members that provide DHCP services for the networks in this network view. You cannot modify information in this tab. It displays the following:
     - **Name**: The name of the DHCP member.
     - **IP Address**: The IP address of the DHCP member.
     - **Failover Association**: The name of the failover association to which the DHCP member belongs. If there are multiple failover associations, only the first one is displayed.
     - **Comment**: The information that you entered for the DHCP member.
     You can sort the information in the table by column. You can also print and export the information.
   - **Extensible Attributes**: Add and delete extensible attributes that are associated with a specific network view. You can also modify the values of extensible attributes. For information, see About Extensible Attributes on page 222.
   - **Permissions**: This tab displays only if you belong to a superuser admin group. For information, see Administrative Permissions for DHCP Resources on page 121.

Deleting Network Views

You can delete any network view, except for the default network view. You can delete a network view that has only one DNS view associated with it. You cannot delete a network view that has more than one DNS view associated with it. When you delete a network view, the appliance deletes all the networks and records within the network view.

To delete a network view:

1. From the Administration tab, select the Network Views tab -> network_view check box, and then click the Delete icon.

2. In the Delete Confirmation dialog box, click Yes.
   The appliance removes the network view and its associated DNS views. You can restore the network view from the Recycle Bin, if enabled. If you restore a network view, the appliance restores the associated DNS views as well. For information about the Recycle Bin, see Recycle Bin on page 47.
ABOUT DHCP NETWORKS

Before you configure a NIOS appliance to provide DHCP services, configure the grid and member DHCP properties as described in Configuring DHCP Services on page 617, and then define the networks that it serves. All networks must belong to a network view. The appliance has one default network view and unless you create additional network views, all networks belong to the default view. Note that because network views are mutually exclusive, you can create networks with overlapping IP address spaces in two different network views.

You can configure DHCP services for IPv4 networks only. However, you can configure both IPv4 and IPv6 networks for IPAM (IP Address Management). For information about IPAM, see Chapter 32, IP Address Management, on page 777.

To configure DHCP services for an IPv4 network and the resources in the network, perform the following tasks:

1. Create a network and assign it to grid members or Microsoft DHCP servers. For information, see Adding IPv4 Networks and Modifying IPv4 Networks on page 597.
2. Configure DHCP properties for the network. You can override properties set at the grid or member level and enter unique values for the network. For information, see Configuring General DHCP Properties on page 619.
3. Optionally, assign zones to a network. For information, see Associating Networks with Zones on page 598.
4. Add a DHCP range to the network and assign it to a member, a failover association, or a Microsoft DHCP server. For information, see Adding DHCP Ranges on page 604 and Modifying DHCP Ranges on page 606.
5. Optionally, add exclusions to the DHCP range for addresses that are not used for dynamic allocation. For information, see Excluding Addresses from DHCP Ranges and Templates on page 607.
6. Optionally, configure DHCP properties for the address range. You can override properties set at an upper level and enter unique values for the address range. For information, see Modifying DHCP Ranges on page 606.
7. Optionally, define filters for precise address assignments and apply them to the DHCP range. For information, see About DHCP Filters on page 674.
8. Optionally, add fixed addresses and reservations to the network and configure DHCP properties for them. For information, see About DHCP Data on page 603.

Adding IPv4 Networks

When you configure an IPv4 network, you must assign either grid members or Microsoft servers to the network. A network cannot be served by a mix of Microsoft and Infoblox DHCP servers. Multiple servers can serve a network, but grid members and Microsoft servers cannot serve the same network.

A grid member can serve only one network view. Similarly, a Microsoft server can serve only one network view. Therefore when you assign grid members to networks, you must assign the members to networks in the same network view. For information, see About Network Views on page 591.

You can configure DHCP services for IPv4 networks only.

To add an IPv4 network:

1. From the Data Management tab, select the DHCP tab.
2. If you have more than one network view in the system, select the network view in which you want to add the network.
3. Expand the Toolbar and click Add -> Network.
4. In the Add Network wizard, select one of the following and click Next:
   - Add Network: Click this to add a network from scratch.
   - Add Network using Template: To use a template, click this, and then click Select Template and select a network template. For information, see About DHCP Templates on page 644. When you use a template to create a network, the configurations of the template apply to the new network. The appliance populates the template properties in the wizard when you click Next. You can then edit the pre-populated properties, except for Netmask.
5. Complete the following and click **Next**:
   - **Address**: Enter the IP address of the network. You can enter the IP address with a CIDR block. For example, enter 10.0.0.0/24, and the netmask slider adjusts the netmask to /24. You can also enter partial IP address with a CIDR block. When you are done, Grid Manager displays the complete IP address with the CIDR block. For example, when you enter 15/24, Grid Manager displays 15.0.0.0/24 and the netmask slider adjusts the netmask to /24.
   - **Netmask**: Use the netmask slider to select the appropriate number of subnet mask bits for the network. The appliance supports /1 to /32 netmasks. Note that when you use a template that contains a fixed netmask, you cannot adjust the netmask for this network.
     Microsoft servers can serve networks with /1 to /31 netmasks. Infoblox DHCP servers can serve networks with /8 to /32 netmasks.
     Since Infoblox DHCP servers do not support /1 to /7 networks, you can assign these networks to Microsoft DHCP servers only. You can create DHCP ranges and fixed addresses within these subnets.
   - **Comment**: Enter useful information about the network, such as the name of the organization it serves.
   - **Automatically create reverse-mapping zone in view**: This function is enabled if the netmask of the network equals /8, /16, or /24. Select this to have the appliance automatically create reverse-mapping zones for the network. A reverse-mapping zone is an area of network space for which one or more name servers have the responsibility for responding to address-to-name queries. These zones are created in the DNS view assigned to receive dynamic DNS updates at the network view level.
   - **Disabled**: Select this if you do not want the DHCP server to provide DHCP services for this network at this time. This feature is useful when you are in the process of setting up the DHCP server. Clear this after you have configured the server and are ready to have it serve DHCP for this network.

6. Click **Next** and add a grid member or Microsoft server as a DHCP server for the network. A network can be served by either grid members or Microsoft servers, but not both at the same time.
   - Click the Add icon and select one of the following options:
     - **Add Infoblox Member**: Select this option to add a grid member as a DHCP server for the network. Select the grid member from the **Member Selector** dialog box. Keep in mind, DHCP properties for the network are inherited from this member. The network can be served by multiple members, but a member can serve networks in one network view only.
     or
     - **Add Microsoft Server**: Select this option to add a Microsoft server as a DHCP server for the network. Select the Microsoft server from the **Microsoft Server Selector** dialog box.

7. Click **Next** to override DHCP properties as described in *About Configuring DHCP Services* on page 618. This only applies if you are adding a network that is served by an Infoblox grid member.

8. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see *About Extensible Attributes* on page 222.

9. Select one of the following:
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and continue to edit.
   - **Save & New**: Save the entry and open a new wizard.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 216.
After you create a network, you can do the following:

- Use the split network feature to create subnets for the network. For information, see *Splitting IPv4 Networks into Subnets* on page 788.
- Use the join networks feature to create a parent network that encompasses multiple subnets into a larger network. For information, see *Joining IPv4 Networks* on page 789. You can also create a shared network for subnets that are on the same network segment.

Networks served by Microsoft servers do not support the split and join functions.

**Viewing IPv4 Networks**

You can view a list of IPv4 networks in the **DHCP** tab -> **Networks** tab -> **Networks** panel. This panel displays all IPv4 networks. It does not display IPv6 addresses. To view a complete list of IPv4 and IPv6 network, go to the **IPAM** tab. For information, see *Chapter 32, IP Address Management*, on page 777.

In the **Networks** panel, you can use filters or the **Go to** function to navigate to a specific network. You can add, delete, or edit a network. You can also monitor the DHCP utilization of a selected network.

To view IPv4 networks:

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks**.
2. Grid Manager displays the following information:
   - **Network**: The network address.
   - **Comment**: The information you entered about the network.
   - **DHCP Utilization**: The percentage of the total DHCP usage of the network. This is the percentage of the total number of DHCP hosts, fixed addresses, reservations, and active leases in the network divided by the total number of IP addresses (excluding IP addresses in the exclusion range) and all DHCP objects in the network. Note that only enabled addresses are included in the calculation. The appliance updates the utilization data approximately every 15 minutes. The utilization data is displayed in one of the following colors:
     - Red: The DHCP resources are 100% utilized.
     - Yellow: The DHCP utilization percentage is over the effective high-water mark threshold.
     - Blue: The DHCP utilization percentage is below the effective low-water mark threshold.
     - Black: The DHCP utilization percentage is at any number other than 100%, or it is not above and below any threshold.
   - **Site**: The site to which the network belongs. This is one of the predefined extensible attributes.

**Viewing Network Details**

You can view detailed information about a specific network by clicking the network link. Grid Manager displays the following information about the network:

- **IP Address**: The IP address of a DHCP object, such as a DHCP range, fixed address, reservation, host configured for DHCP, or roaming host with an allocated IP address. For a DHCP range, this field displays the start and end addresses of the range. For a host that has multiple IP addresses, each IP address is displayed separately. Note that the appliance highlights all disabled DHCP objects in gray.
- **Type**: The DHCP object type, such as **DHCP Range** or **Fixed Address**.
- **Name**: The object name. For example, if the IP address belongs to a host record, this field displays the hostname.
- **Comment**: The information you entered for the object.
- **DHCP Utilization**: The percentage of the total DHCP usage of a DHCP range. This is the percentage of the total number of fixed addresses, reservations, hosts, and active leases in the DHCP range divided by the total IP addresses in the range, excluding the number of addresses in the exclusion ranges. Note that only enabled objects are included in the calculation.
- **Site**: The site to which the DHCP object belongs. This is one of the predefined extensible attributes.
You can select the following additional columns for display:

- **Static Addresses**: Indicates whether the IP address is a static address.
- **Dynamic Addresses**: Indicates whether the IP address is a dynamically assigned address.
- **Disabled**: Indicates whether the object is disabled.
- Available extensible attributes.

You can also do the following in this panel:

- Sort the displayed data in ascending or descending order by column.
- Click **Go to IPAM View** to view information about the object in the IPAM tab.
- Add new objects, such as DHCP ranges, to the network.
- Delete or schedule the deletion of a selected object or multiple objects.
- Use filters to search for specific objects.
- Print or export the data.

**Modifying IPv4 Networks**

You can modify existing network settings and override the grid or member DHCP properties, with the exception of the network address and netmask.

To modify an IPv4 network:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon.

2. The **Network** editor contains the following basic tabs from which you can modify data:

   - **Genera Basic**: You can modify the following fields:
     - **Comment**: The information you entered for the network.
     - **Disabled**: This field is displayed only if the selected network is a network without a child network under it. You can disable and enable existing networks instead of removing them from the database, if the selected network does not have a child subnet. This feature is especially helpful when you have to move or repair the server for a particular network.

   - **Member Assignment**: Add or delete a grid member that provides DHCP services for this network. For information, see **Adding IPv4 Networks** on page 594.

   - **DHCP**: Keep the inherited DHCP properties or override them and enter unique settings for the network. For information, see **About Configuring DHCP Services** on page 618.

   - **Extensible Attributes**: Add and delete extensible attributes that are associated with a specific network. You can also modify the values of the extensible attributes. For information, see **About Extensible Attributes** on page 222.

   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see **Managing Permissions** on page 20.

3. Optionally, you can click **Toggle Advanced Mode** to display the following tabs from which you can modify advanced data.

   - **General Advanced**: You can associate zones with a network. For information, see **Associating Networks with Zones** on page 598.

   - **DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the network. For information, see **Configuring DDNS Updates from DHCP** on page 501.

   - **BOOTP**: Keep the inherited BOOTP properties or override them and enter unique settings for the network. For information, see **Configuring BOOTP Properties** on page 625.

   - **Thresholds**: Keep the inherited thresholds settings or override them and enter unique settings for the network. For information, see **Configuring Thresholds for DHCP Ranges** on page 634.

Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.
Managing DHCP Data

4. Select one of the following:
   — Save & Close: Save the entry and close the editor.
   — Save: Save the entry and continue to edit.
   or
   — Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 216.

Associating Networks with Zones

You can associate a network with DNS zones to limit the zones that admins can use when they create DNS records for IP addresses in the network. When a network is associated with one or more zones and an admin creates a DNS record for one of its IP addresses, Grid Manager allows the admin to create the DNS record in the associated zones only. For example, if you associate the 10.1.0.0/16 network with the corp100.com zone, admins are allowed to create DNS records in the corp100.com zone only for IP addresses in the 10.1.0.0/16 network.

This feature applies to A, AAAA and host records only. It does not apply to records in a shared record group. If you are creating a host record with multiple IP addresses in different networks, the networks must be associated with the zone of the host record.

If a network is not associated with a zone, admins can create DNS records for its IP addresses only in zones with no network associations as well.

You can associate a network with any authoritative zone whose primary server is a grid member or a Microsoft server, or is unassigned. You cannot associate networks with zones that have external primary servers.

You can associate a network with multiple zones, and associate a zone with more than one network. You can associate IPv4 and IPv6 network containers and networks with zones. When you associate a network container with zones, its networks inherit the zone associations. You can override the zone associations at the network level.

If you split a network, the resulting subnets inherit the zone associations. If you join networks, the resulting network retains the zone associations of the network that you selected when you performed the join operation. You can override the inherited zone associations of individual networks. Subzones do not inherit the network associations of their parent zones.

When you import data into a zone that is associated with a list of networks, the imported A, AAAA and host records must have IP addresses in the associated networks. Grid Manager does not allow you to import A, AAAA and host records with IP addresses in unassociated networks.

When you associate a network with a zone, the DNS records created before the association are not affected. But if you edit an A, AAAA or host record after the association, Grid Manager does not allow you to save the record if its IP address is not in an associated network.

To associate a network with a zone:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon.
2. In the DHCP Network editor, click Toggle Advanced Mode if the editor is in basic mode.
3. When the additional tabs appear, click the Advanced subtab of the General tab.
4. Click the Add icon and select the zone you want to associate with the network.
   — Optionally, select a default zone. When you create or edit an A, AAAA or host record from a network in the IPAM tab, Grid Manager automatically selects the default zone that is assigned to the network.
5. Select one of the following:
   — Save & Close: Save the entry and close the editor.
   — Save: Save the entry and continue to edit.
   or
   — Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 216.
Viewing the Networks Associated with a Zone

You can view the networks associated with a zone from the zone editor. The tab to display network associations in zone editors is visible only if the primary server is a grid member, a Microsoft server, or unassigned.

To view the network associations of a zone:

1. From the Data Management tab, select the DNS tab -> Zones tab -> zone check box, and then click the Edit icon.
2. In the Authoritative Zone editor, click Toggle Advanced Mode if the editor is in basic mode.
3. When the additional tabs appear, click the Advanced subtab of the General tab.

The Network Associations table lists the networks and their corresponding comments. You cannot change the network associations in this editor. Navigate to the DHCP Network editor of the network, to change the zone associations.

Deleting IPv4 Networks

When you delete a network, all of its data, including all DHCP records, subnets, and records in its subnets, is deleted from the database. Because of the potentially large loss of data that can occur when you delete a network, the appliance stores the deleted network in the Recycle Bin. You can restore a deleted network from the Recycle Bin, if enabled. You can also disable a network instead of deleting it. For information, see Modifying IPv4 Networks on page 597.

To delete a network:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> network check box, and then select Delete or Schedule Delete from the Delete drop-down menu.
2. To delete the network now, in the Delete Confirmation dialog box, click Yes. To schedule the deletion, see Scheduling Tasks on page 216.

The appliance puts the deleted network in the Recycle Bin, if enabled.
ABOUT SHARED NETWORKS

A shared network is a network segment to which you assign two or more subnets. When subnets in a shared network contain IP addresses that are available for dynamic allocation, the addresses are put into a common pool for allocation when client requests arise. When you create a shared network, the DHCP server can assign IP addresses to client requests from any subnet (that resides on the same network interface) in the shared network. For example, when you have networks A, B, and C on the same network interface and you assign them to a shared network, the DHCP server can allocate available IP addresses from any DHCP range within networks A, B, and C even when all the client requests originate from network A. When adding subnets to a shared network, ensure that the subnets are assigned to the same members to avoid DHCP inconsistencies.

Before creating a shared network, you must first create the subnets. For example, you must first create the networks 10.32.1.0 and 10.30.0.0 before designating them to a shared network.

Adding Shared Networks

To add a shared network:

1. From the Data Management tab, select the DHCP tab, and then click Add -> Shared Network from the Toolbar.
2. In the Add Shared Network wizard, do the following:
   a. Name: Enter the name of the shared network.
   b. Comment: Enter information about the shared network.
   c. Disabled: Select this if you want to enable the shared network at a later time. You can disable and enable existing networks instead of removing them from the database. This feature is especially helpful when you have to move or repair the server for a particular network.
3. Click Next and do the following to add networks:
   a. Click the Add icon.
   b. In the Select Network dialog box, select the networks that you want to include in the shared network. Ensure that the networks are served by the same grid members to avoid DHCP inconsistencies.
   c. Click the Select icon.
4. Click Next to configure or override DHCP options as described in About Configuring DHCP Services on page 618.
5. Click Next to enter values for required extensible attributes or add optional extensible attributes for the shared network. For information, see Using Extensible Attributes on page 225.
6. Select one of the following:
   a. Save & Close: Save the entry and close the wizard.
   b. Save & Edit: Save the entry and continue to edit.
   c. Save & New: Save the entry and open a new wizard.
   or
   a. Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 216.
### Viewing Shared Networks

To view shared networks:

1. From the **Data Management** tab, select the **DHCP** tab → **Networks** tab → **Shared Networks**.
2. Grid Manager displays the following information:
   - **Name**: The name of the shared network.
   - **Comment**: The information you entered about the shared network.
   - **DHCP Utilization**: The percentage of the DHCP utilization of the networks that belong to the shared network. This is the percentage of the total number of available IP addresses from all the networks that belong to the shared network versus the total number of all IP addresses in all of the networks in the shared network.
   - **Site**: The site to which the shared network belongs. This is one of the predefined extensible attributes.

You can select **Disabled** or available extensible attributes for display. You also can view detailed information about a network in a shared network by clicking the network link. For information, see **Viewing IPv4 Networks** on page 596.

### Modifying Shared Networks

To modify a shared network:

1. From the **Data Management** tab, select the **DHCP** tab → **Networks** tab → **Shared Networks** → **shared_network** check box, and then click the Edit icon.
2. The **Shared Network** editor contains the following tabs from which you can modify data:
   - **General**: Modify the fields **Name**, **Comments**, and **Disabled** as described in **Adding Shared Networks** on page 600.
   - **Networks**: Displays the networks that are currently assigned to the shared network. You can add or delete a network. To add a network, click the Add icon. In the **Select Network** dialog box, select the network you want to add. To delete an existing network, select the **network** check box, and then click the Delete icon.
   - **DHCP**: Keep the inherited DHCP properties or override them and enter unique settings for the shared network. For information, see **About Configuring DHCP Services** on page 618.
   - **Extensible Attributes**: Add and delete extensible attributes that are associated with a specific network. You can also modify the values of extensible attributes. For information, see **Using Extensible Attributes** on page 225.
   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see **Managing Permissions** on page 20.
3. Optionally, you can click **Toggle Advanced Mode** to display the following tabs from which you can modify advanced data.
   - **DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the shared network. For information, see **Chapter 18, Configuring DDNS Updates from DHCP**, on page 501.
   - **BOOTP**: Keep the inherited BOOTP properties or override them and enter unique settings for the shared network. For information, see **Configuring BOOTP Properties** on page 625.

Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.
4. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and continue to edit.
   - Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see **Scheduling Tasks** on page 216.
Deleting Shared Networks

To delete a shared network:

1. From the Data Management tab, select the DHCP tab → Networks tab → Shared Networks → shared_network check box, and then select Delete or Schedule Delete from the drop-down menu.

2. To delete the shared network now, in the Delete Confirmation dialog box, click Yes. To schedule the deletion, see Scheduling Tasks on page 216.

The appliance puts the deleted shared network in the Recycle Bin, if enabled.
About DHCP Data

After you create a network, you can define DHCP resources such as DHCP ranges, fixed addresses, reservations, host records, and roaming hosts.

In a network, you define DHCP ranges from which the DHCP server assigns IP addresses to client requests. When a DHCP client requests an IP address, the appliance allocates an address within a defined DHCP range. The DHCP client can use the assigned IP address until the lease expires. You can also apply filters to DHCP ranges to control how the DHCP server allocates IP addresses. For information about DHCP filters, see About DHCP Filters on page 674.

You can configure fixed addresses for network devices, such as routers and printers, that are not frequently moved from network to network. By creating fixed addresses for network devices, clients can reliably reach them by their domain names. Some network devices, such as web or FTP servers, can benefit from having fixed addresses for this reason. For information about fixed addresses, see Configuring Fixed Addresses on page 608. You can also reserve an IP address that is not part of a DHCP range by defining a reservation. For information about creating reservations, see Configuring Reservations on page 611.

Infoblox host records are data objects that contain DNS, DHCP, and IPAM data of the assigned addresses. You can assign multiple IP addresses to a host record. When you create a host record, you are specifying the name-to-address and address-to-name mappings for the IP addresses that you assign to the host. For information about Infoblox hosts, see About Host Records on page 442.

Roaming hosts are hosts that require dynamically assigned IP addresses and specific sets of options. You can create roaming hosts for devices, such as laptop computers and mobile phones, that require different IP addresses each time they are moved from one network to another as well as a unique set of DHCP options. The appliance assigns an IP address from the DHCP range associated with the network from which the address request originates. If the grid member does not have an associated DHCP range, the appliance does not return an IP address. A roaming host also receives DHCP options from the grid, member, network, or shared network with which it associates. For more information, see Configuring Roaming Hosts on page 613.

When you configure a fixed address, a reservation, or a host address, you can either specify an IP address or obtain the next available IP address in a specified network or DHCP range to which you have administrative permissions. The next available IP address is the first unused IP address in the network or DHCP range. The appliance searches for the next available IP address based on certain criteria. Depending on whether the appliance searches for the next available IP address in a network or in a DHCP range, it uses different criteria. For information about obtaining the next available IP address, see Guidelines for the Next Available IP Address. You can also track specific information about a network device by defining extensible attributes. Extensible attributes are fields that you define to track properties such as network locations or device models. For more information, see About Extensible Attributes on page 222.

Guidelines for the Next Available IP Address

You can obtain the next available IP address when you define a fixed address, a reservation, or a host record. The next available IP address is the first unused IP address in a specified network or DHCP range to which you have administrative permissions. The appliance follows certain rules when searching for the next available IP address in the specified network and DHCP range.

In a network, the appliance searches for the next IP address that meets all of the following criteria:

- It does not match any DNS resource record, such as an A or PTR record, that is associated with an IP address.
- It is not assigned to a DHCP fixed address or host address record.
- It is not part of any DNS bulk host record.
- It does not match any unmanaged IP address.
- It is not the network (the first) or broadcast (the last) address in the specified network.
- It is not within any DHCP range in this network.
- It is not within an exclusion range.
- It is not part of a scheduled task that involves a fixed address. For information about how to schedule a task, see Scheduling Tasks on page 216.
In a DHCP range, the appliance searches for the next IP address that meets all of the following criteria:

- It is not assigned to a DHCP fixed address or host address record.
- It does not match any unmanaged IP address.
- It is not part of an exclusion range within the DHCP range.
- It is not part of a scheduled task that involves a fixed address.
- It does not match any active DHCP lease.

**Note:** The appliance does not search for deleted leases in the Recycle Bin.

When multiple users simultaneously request for the next available IP address, the appliance returns the same unused IP address to all users. The user who first saves the task that uses the IP address gets the next available IP address. In some cases, other users get an error message telling them that the IP address is not available when they save their tasks. They can then request another unused IP address or enter a new IP address.

For information about the DHCP data that you can add to a network, see the following:

- **Configuring DHCP Address Ranges**
- **Configuring Fixed Addresses** on page 608
- **Configuring Reservations** on page 611
- **Configuring Roaming Hosts** on page 613

### Configuring DHCP Address Ranges

A DHCP range is a pool of IP addresses from which the appliance allocates IP addresses. You must add a DHCP address range in your network so the appliance can assign IP addresses to DHCP clients within the specified range. Each range is managed by a member or a failover association for address assignments. If the client is on a network that is assigned a DHCP range, the appliance assigns an available IP address from that range to the DHCP client.

You must assign a DHCP range to a grid member. Note that you can only assign DHCP ranges to members and networks that are in the same network view. If the server is an independent appliance, you must specify this appliance as the member that serves the DHCP range. You can also use a template to add a DHCP range. For information, see **About DHCP Range Templates** on page 645.

### Adding DHCP Ranges

You can add a DHCP range to a network that does not have any child network under it.

To add a DHCP range:

1. Navigate to the network to which you want to add a DHCP range, and then click Add -> DHCP Range from the Toolbar. You can also add a DHCP range from any panel in the DHCP tab.
2. In the Add Range wizard, select one of the following and click Next:
   - Add DHCP Range
   - Add DHCP Range using Template
     - Click Select Template and select the template that you want to use. Note that when you use a template to create a DHCP range, the configurations of the template apply to the new range. The appliance automatically populates the DHCP range properties in the wizard. You can then edit the pre-populated properties.
3. Complete the following:
   - **Network**: The displayed network address can either be the last selected network or the network from which you are adding the DHCP range. If no network address is displayed or if you want to specify a different network, click **Select Network**. When there are multiple networks, Grid Manager displays the *Select Network* dialog box from which you can select one.
   - **Start**: Enter the first IP address in the range available for the clients.
   - **End**: Enter the last IP address in the range available for the clients.
   - **Name**
   - **Comment**: Enter useful information about the address range.
   - **Disabled**: Select this if you do not want the DHCP server to allocate IP addresses from this DHCP range at this time. This feature is useful when you are in the process of setting up the DHCP server. Clear this after you have configured the server and are ready to have it serve DHCP for this range.

4. Click **Next** and select one of the following to provide DHCP services for the DHCP range:
   - **None**: Select this if you do not want any member to serve DHCP for this range. This is selected by default.
   - **Grid Member**: Select this if you want a grid member to serve DHCP for this DHCP range. Select a grid member from the drop-down list. The drop-down list displays only the grid members that are associated with the network to which the DHCP range belongs.
   - **Failover Association**: Select this if you want a failover association to serve DHCP for this DHCP range. Click **Select Association**. In the *DHCP Failover Association Selector* dialog box, choose a failover association, and then click the Select icon. The appliance lists failover associations that serve DHCP in the network view of the DHCP range. For information, see Chapter 25, DHCP Failover, on page 655.

5. Click **Next** to configure or override DHCP options as described in About Configuring DHCP Services on page 618.

6. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes on page 225.

7. Select one of the following:
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and continue to edit.
   - **Save & New**: Save the entry and open a new wizard.
   - or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 216.

**Viewing DHCP Ranges**

To view information about a DHCP range:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range.

2. Grid Manager displays the following information:
   - **IP Address**: The IP address of the object in the DHCP range. For exclusion ranges, this displays the start and end IP addresses. For host records with multiple IP addresses, each IP address is displayed separately. The appliance highlights disabled DHCP objects in gray. A DHCP object can be a fixed address, reservation, host configured for DHCP, or roaming host with an allocated IP address.
   - **Type**: The object type, such as Fixed Address.
   - **Name**: The object name. For example, if the IP address belongs to a host record, this field displays the hostname.
   - **Comment**: The information you entered for the object.
   - **Site**: The site to which the object belongs. This is one of the predefined extensible attributes.

You can select Disabled or available extensible attributes for display.
You can also do the following:

- Sort the data in ascending or descending order by column.
- Create a bookmark for the range.
- Delete or schedule the deletion of a selected object or multiple objects in the range.
- Use filters to search for specific objects.
- Select an object and view detailed information.
- Print or export the data.

**Modifying DHCP Ranges**

To modify a DHCP range:

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** -> **network** -> **addr_range** check box, and then click the Edit icon.

2. The **DHCP Range** editor contains the following basic tabs from which you can modify data:
   - **General**: Modify the fields, except the network address, as described in *Adding DHCP Ranges* on page 604.
   - **Member Assignment**: Modify the grid member or failover association that provides DHCP services for the DHCP range as described in *Adding DHCP Ranges* on page 604.
   - **DHCP**: Keep the inherited DHCP options or override them and enter unique settings for the DHCP range. For information, see *About Configuring DHCP Services* on page 618.
   - **Extensible Attributes**: You can add and delete extensible attributes that are associated with a specific DHCP range. You can also modify the values of extensible attributes. For information, see *Using Extensible Attributes* on page 225.
   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see *Managing Permissions* on page 20.

3. Optionally, you can click **Toggle Advanced Mode** to display the following tabs from which you can modify advanced data.
   - **DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the DHCP range. For information, see *Configuring DDNS Updates from DHCP* on page 501.
   - **BOOTP**: Keep the inherited BOOTP properties or override them and enter unique settings for the DHCP range. For information, see *Configuring BOOTP Properties* on page 625.
   - **Exclusion Ranges**: Configure a range of IP addresses that the appliance does not use to assign to clients. You can use these exclusion addresses as static IP addresses. For information, see *Excluding Addresses from DHCP Ranges and Templates*.
   - **Thresholds**: Keep the inherited thresholds settings or override them and enter unique settings for the DHCP range. For information, see *Configuring Thresholds for DHCP Ranges* on page 634.
   - **Filters**: You can add or delete DHCP filters to the range. For information, see *Applying Filters to DHCP Address Ranges* on page 687.

Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and continue to edit.
   - Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 216.
Deleting DHCP Ranges

To delete a DHCP range:
1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range check box, and then click the Delete icon.

Excluding Addresses from DHCP Ranges and Templates

Creating an exclusion range prevents the appliance from assigning the addresses in the exclusion range to clients. IP addresses in an exclusion range are excluded from the pool of IP addresses. You can use exclusions to split a DHCP range into multiple blocks of ranges. You can also use addresses in the exclusion ranges as static IP addresses for network devices such as legacy printers that do not support DHCP. An exclusion in a range can help prevent address conflicts between statically configured devices and dynamically configured devices.

To exclude addresses from a DHCP address range:
1. In the DHCP Range editor, click Toggle Advanced Mode, select the Exclusion Ranges tab, and then click the Add icon.
2. Enter the start and end addresses of the exclusion range.
3. Optionally, enter information about this exclusion range.

To exclude addresses from a DHCP range template:
1. In the DHCP Range Template editor, select the Exclusion Ranges tab, and then click the Add icon.
2. Enter the following:
   — **Offset**: An offset for an exclusion range determines the start IP address of the exclusion range. The appliance adds the offset value you enter here to the start IP address of the DHCP range created using this template. That IP address becomes the start IP address of the exclusion range.
   — **Number of Addresses**: Enter the number of IP addresses to be included in the exclusion range.
   — **Comment**: Enter useful information about the exclusion range.
**Configuring Fixed Addresses**

A fixed address represents a persistent link between an IP address and one of the following:
- MAC address
- Client identifier
- Circuit ID or remote ID in the DHCP relay agent option (option 82)

You can create fixed addresses as described in *Adding Fixed Addresses*. You can also create a fixed address when you create a host record or when you convert an active, dynamically leased address to a fixed address. For more information, see *Adding Host Records* on page 444 and *Converting DHCP Leases* on page 795.

When you create a fixed address, you must define a host identifier that the DHCP server uses to match the DHCP client. Every time the DHCP client with the matching identifier requests an IP address, the DHCP server assigns it the same address.

When a DHCP client sends a DHCPDISCOVER, it can include the MAC address or a unique client identifier as option 61 in the DHCP section of the packet. Using a client identifier is especially useful for virtualized server processes that might be moved to different hardware platforms. For information about option 61, refer to RFC2132, *DHCP Options and BOOTP Vendor Extensions*. You can select either the MAC address or client identifier as the host identifier in a fixed address. The DHCP server matches the option 61 value in the client request using either the MAC address or client identifier, depending on your configuration. When a DHCP client renews an IP address using a matching MAC address or client identifier, the DHCP server tracks the allocation of IP addresses and reserves the same IP address for the client.

When you enter a MAC address, you can use one of the following formats:
- aa:bb:cc:dd:ee:ff — Six groups of two hexadecimal digits separated by colons (-)
- aa-bb-cc-dd-ee-ff — Six groups of two hexadecimal digits separated by hyphens (-)
- aabb.ccdd.eeff — Three groups of four hexadecimal digits separated by periods (.)
- aabbcc-ddeeff — Two groups of six hexadecimal digits separated by a hyphen (-)
- aabbcddddeeff — One group of 12 hexadecimal digits without any separator

After you save the entry, the appliance displays the MAC address in the AA:BB:CC:DD:EE:FF format.

When a DHCP client requests an IP address through a DHCP relay agent, the agent adds either the circuit ID or remote ID, or both, to the DHCP relay agent information option (option 82). For information, see *About the DHCP Relay Agent Option (Option 82)* on page 633. When you select the DHCP relay agent option (circuit ID or remote ID) as the host identifier in a fixed address, the DHCP server matches the DHCP client request using either the circuit ID or the remote ID, depending on your configuration. When a DHCP client renews an IP address using a matching relay agent ID, the DHCP server tracks the allocation of IP addresses and reserves the same IP address for the client. Note that leases are not renewed at the standard renewal time (T1) when option 82 information is not available as a unicast renewal. Instead, leases are renewed at the rebinding time (T2) when renewals are sent as broadcasts to the relay agents and contain option 82 information. For information about how to configure the lease time, see *Configuring DHCP Lease Times* on page 621.
Adding Fixed Addresses

1. From the Data Management tab, select the DHCP tab.
2. Expand the Toolbar and click Add → Fixed Address.
3. In the Add Fixed Address wizard, select one of the following and click Next:
   - Add Fixed Address
   or
   - Add Fixed Address using Template
     Click Select Template and select the template that you want to use. Note that when you use a template to create a fixed address, the configurations of the template apply to the new address. The appliance automatically populates the fixed address properties in the wizard. You can then edit the pre-populated properties.
4. Complete the following:
   - Network: The displayed network address can either be the last selected network or the network from which you are adding the fixed address. If no network address is displayed or if you want to specify a different network, click Select Network. When there are multiple networks, Grid Manager displays the Select Network dialog box from which you can select one.
   - IP Address: Enter the IPv4 address for the fixed address, or click Next Available IP to obtain the next available IP address. For information about obtaining the next available IP address, see Guidelines for the Next Available IP Address on page 603.
   - If the network of the IP address is served by a grid member, Grid Manager displays the Assign IP Address by section. Select one of the following to match your criteria:
     - MAC Address: Select this to assign a fixed address to a host with the MAC address that you specify here. Enter the MAC address in the field. For MAC address format, see Configuring Fixed Addresses on page 608.
     - DHCP Client Identifier: Select this to assign a fixed address to a host with the DHCP client identifier that you specify here. In the field, enter the client identifier of the host to which you want the DHCP server to assign this IP address. The client identifier must be unique within the network.
       - Match null (\0) at beginning of DHCP client identifier: This is enabled when you select DHCP client identifier. Select this when a DHCP client sends a \000 prefixed to the DHCP client identifier. \0 is the null character. Some DHCP clients (for example, Microsoft) send the client identifier in a \000foo format (with the null character prefix instead of just foo). The client identifier for the requesting host and the client identifier stored in the appliance must match.
     - DHCP Relay Agent: Select this to assign a fixed address to a host with the circuit ID or remote ID you specify here. From the drop-down list, select Circuit ID or Remote ID, and then enter the ID in the field. For information about circuit IDs and remote IDs, see About the DHCP Relay Agent Option (Option 82) on page 633. You can enter the ID in hexadecimal format, such as ex:aa, ab, 1f:cd, or ef:23:56, or in string format, such as abcd or aa:gg. The appliance matches the value you enter here with the value sent by the DHCP client in counted octet sequence format. For information about how to use hexadecimal values, see DHCP Option Data Types on page 627. The ID is case sensitive and can contain up to 230 characters.
   - Name: Enter a name for the fixed address. This field is required if the network is served by a Microsoft server. For information, see Adding Fixed Addresses/Microsoft Reservations on page 766.
   - Comment: Optionally, enter additional information about the fixed address.
   - Disabled: Select this if you do not want the DHCP server to allocate this IP address at this time.
5. Click Next to configure or override DHCP options as described in About DHCP Options on page 626.
6. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see *Using Extensible Attributes* on page 225.

7. Select one of the following:
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and continue to edit.
   - **Save & New**: Save the entry and open a new wizard.
   
   or
   
   - Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 216.

### Modifying Fixed Addresses

To modify a fixed address:

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** -> **network** -> **fixed_address** check box, and then click the **Edit** icon.

2. The **Fixed Address** editor contains the following basic tabs from which you can modify data:
   
   - **General**: You can modify the fields, except the network address, as described in *Adding Fixed Addresses* on page 609.
   
   - **DHCP**: You can keep the inherited DHCP options or override them and enter unique settings for the fixed address. For information, see *About Configuring DHCP Services* on page 618.
   
   - **Discovered Data**: Displays the discovered data of the fixed address. For information, see *Viewing Data in the Discovered Data Section* on page 820.
   
   - **Extensible Attributes**: Add and delete extensible attributes that are associated with a specific network. You can also modify the values of extensible attributes. For information, see *Using Extensible Attributes* on page 225.
   
   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see *Managing Permissions* on page 20.

3. Optionally, you can click **Toggle Advanced Mode** to display the following tabs from which you can modify advanced data.
   
   - **DDNS**: You can keep the inherited DDNS settings or override them and enter unique settings for the fixed address. For information, see *Configuring DDNS Updates from DHCP* on page 501.
   
   - **BOOTP**: You can keep the inherited BOOTP properties or override them and enter unique settings for the fixed address. For information, see *Configuring BOOTP Properties* on page 625.

   Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Select one of the following:
   
   - **Save & Close**: Save the entry and close the editor.
   
   - **Save**: Save the entry and continue to edit.
   
   or
   
   - Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 216.

### Deleting Fixed Addresses

To delete a fixed address, from the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** -> **network** -> **fixed_address** check box, and then click the **Delete** icon.
Configuring Reservations

You can reserve an IP address so the DHCP server cannot assign it to any client. A reservation is an IP address that you exclude from DHCP use because you intend to configure the address manually on a network device. A reservation is not currently used for DHCP purposes.

To create a reservation, you can do one of the following:

- Add a reservation. For information, see Adding Reservations.
- Convert a fixed address or a dynamic address with an active lease to a reservation. For information, see Converting Objects Associated with IP Addresses on page 794.
- Define a fixed address with an IP address. For information, see Adding Fixed Addresses on page 609.

Adding Reservations

To create a reservation:

1. From the Data Management tab, select the DHCP tab.
2. Select a network view from the drop-down list.
3. Expand the Toolbar and click Add -> Reservation.
4. In the Add Reservation wizard, select one of the following and click Next:
   - Add Reservation
   or
   - Add Reservation using Template
     Click Select Template and select the template that you want to use. Note that when you use a template to create a reservation, the configurations of the template apply to the new address. The appliance automatically populates the reservation properties in the wizard. You can then edit the pre-populated properties.
5. Complete the following:
   - Network: The displayed network address can either be the last selected network or the network from which you are adding the DHCP range. If no network address is displayed or if you want to specify a different network, click Select Network. When there are multiple networks, Grid Manager displays the Select Network dialog box from which you can select one.
   - IP Address: Enter the IP address that you want to reserve for manual assignment, or click Next Available IP to obtain the next available IP address. For information about obtaining the next available IP address, see Guidelines for the Next Available IP Address on page 603.
   - Network View: Displays the network view of the reservation.
   - Comment: Optionally, enter useful information about the reservation.
   - Disabled: Select this if you do not want the DHCP server to use this reservation at this time.
6. Click Next to configure or override DHCP options as described in About Configuring DHCP Services on page 618.
7. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes on page 225.
8. Select one of the following:
   - Save & Close: Save the entry and close the wizard.
   - Save & Edit: Save the entry and continue to edit.
   - Save & New: Save the entry and open a new wizard.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 216.
Modifying Reservations

To modify a reservation:

1. From the Data Management tab, select the DHCP tab → Networks tab → Networks → network → reservation check box, and then click the Edit icon.

2. The Reservation Address editor contains the following tabs from which you can modify data:
   - General: Modify the fields, except the network address, as described in Adding Reservations on page 611.
   - DHCP: Keep the inherited DHCP options or override them and enter unique settings for the reservation. For information, see About Configuring DHCP Services on page 618.
   - Discovered Data: Displays the discovered data of the reservation. For information, see Viewing Data in the Discovered Data Section on page 820.
   - Extensible Attributes: Add and delete extensible attributes that are associated with a reservation. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes on page 225.
   - Permissions: This tab appears only if you belong to a superuser admin group. For information, see Managing Permissions on page 20.

3. Optionally, you can click Toggle Advanced Mode to display the following tabs from which you can modify advanced data.
   - DDNS: Keep the inherited DDNS settings or override them and enter unique settings for the reservation. For information, see Configuring DDNS Updates from DHCP on page 501.
   - BOOTP: You can keep the inherited BOOTP properties or override them and enter unique settings for the reservation. For information, see Configuring BOOTP Properties on page 625.

   Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Select one of the following:
   - Save & Close: Save the entry and close the editor.
   - Save: Save the entry and continue to edit.
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 216.
**Configuring Roaming Hosts**

A roaming host is a host with a dynamically assigned IP address and a specific set of properties and DHCP options. When you create a roaming host for a network device, the device can receive any dynamically assigned address from the network to which it belongs. You can create roaming hosts for devices, such as laptop computers and mobile phones, that require different IP addresses each time they are moved from one network to another and require a unique set of DHCP options.

When you configure a roaming host, you must configure it in a specific network view. If you have multiple network views, you must specify the network view to which the requesting hosts belong so the appliance can assign addresses to the hosts from the networks within the same network view. You can also match the host by its MAC address or a DHCP client identifier and specify DHCP options for the host while allowing it to receive a dynamic IP address. For information about entering MAC addresses, see Configuring Fixed Addresses on page 608.

To configure a roaming host, perform the following tasks:

- Enable support for roaming hosts at the grid level. For information, see Enabling Support for Roaming Hosts.
- Add a roaming host. For information, see Adding Roaming Hosts.
- Optionally, configure DHCP properties for the roaming host. You can override properties set for the upper levels and enter unique values for the roaming hosts. For information, see Configuring General DHCP Properties on page 619.

Do the following to manage the roaming hosts after you configure them:

- View roaming hosts. For information, see Viewing Roaming Hosts on page 614.
- Modify existing roaming hosts. For information, see Modifying Roaming Hosts on page 615.
- Delete roaming hosts that are not currently in use. For information, see Deleting Roaming Hosts on page 615.

**Enabling Support for Roaming Hosts**

You must first enable support for roaming hosts before adding them. After you enable this feature, you can only disable it after you delete all the existing roaming hosts.

To enable support for roaming hosts:

1. From the Data Management tab, select the DHCP tab.
2. Expand the Toolbar and click Grid DHCP Configuration.
3. In the General Advanced tab, select Enable support for roaming host.
4. Select Save & Close.

**Adding Roaming Hosts**

To add a roaming host:

1. From the Data Management tab, select the DHCP tab.
2. Select a network view from the drop-down list.
3. Expand the Toolbar and click Add -> Roaming Host.
4. In the Add Roaming Host wizard, select one of the following and click Next:
   - Add Roaming Host
   - Add Roaming Host using Template
     Click Select Template to create a roaming host using a fixed address/reservation template. In the DHCP Template Selector dialog box, select the template that you want to use. Note that when you use a template to create a roaming host, the configurations of the template apply to the new host. The appliance automatically populates the host properties in the wizard. You can then edit the pre-populated properties.


5. Complete the following:
   - **Name**: Enter the name of the roaming host. The name must be unique for each roaming host in a given network view.
   - **Assign IP Address by**: Select one of the following criteria on which the appliance matches when assigning an IP address to the host.
     - **MAC Address**: Select this to assign a dynamic IP address to a host, provided that the MAC address of the requesting host matches the MAC address that you specify here.
     - **DHCP Client Identifier**: Select this to assign a dynamic IP address to a host with the same DHCP client identifier that you specify here. When you select this, the **Match null (\0) at beginning of DHCP client identifier** check box is displayed. Select this when a DHCP client sends a \000 prefixed to the DHCP client identifier. \0 is the null character. Some DHCP clients (for example, Microsoft) send the client identifier in a \000foo format (with the null character prefix instead of just foo). The client identifier for the requesting host and the client identifier stored in the appliance must match.
   - **Comment**: Enter useful information about the roaming host.
   - **Disabled**: Select this if you do not want the DHCP server to use this roaming host definition. When you disable a roaming host, the host gets an IP address without the defined DHCP options.
6. Click **Next** to configure the DHCP options for the roaming host, as described in *About Configuring DHCP Services* on page 618.
7. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see *Using Extensible Attributes* on page 225.
8. Select one of the following:
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and continue to edit.
   - **Save & New**: Save the entry and open a new wizard.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 216.

**Viewing Roaming Hosts**

To view a list of roaming hosts in a specific network view:
1. From the **Data Management** tab, select the **DHCP** tab → **Networks** tab → **Roaming Hosts**.
2. From the Network View drop-down list, select the network view to which the roaming hosts belong.
3. The Grid Manager displays the following for each roaming host:
   - **Name**: The name of the roaming host.
   - **Address**: The IP address of the roaming host.
   - **Comment**: The information that you entered for the roaming host.
   - **Site**: The site to which the template belongs. This is one of the predefined extensible attributes.
You can also select **Disabled** and available extensible attributes for display.
Modifying Roaming Hosts

To edit an existing roaming host:
1. From the Data Management tab, select the DHCP tab -> Networks tab -> Roaming Hosts -> roaming_host check box, and then click the Edit icon.
2. The Roaming Host editor contains the following tabs from which you can modify data:
   - **General**: Edit the fields as described in Adding Roaming Hosts on page 613, except for the Templates field.
   - **DHCP**: Keep the inherited DHCP options or override them and enter unique settings for the roaming host. For information, see About Configuring DHCP Services on page 618.
   - **Discovered Data**: This tab displays the discovered data of the roaming host. For information, see Viewing Data in the Discovered Data Section on page 820.
   - **Extensible Attributes**: Add and delete extensible attributes that are associated with a roaming host. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes on page 225.
   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see Managing Permissions on page 20.
3. Optionally, you can click Toggle Advanced Mode to display the following tabs from which you can modify advanced data.
   - **DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the roaming host. For information, see Enabling DDNS and Specifying a Domain Name on page 506. Note that you can select Override client provided hostname with roaming hostname in this tab to use the name of the roaming host as the name of the client for DDNS updates.
   - **BOOTP**: Keep the inherited BOOTP properties or override them and enter unique settings for the roaming host. For information, see Configuring BOOTP Properties on page 625.
4. Select one of the following:
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and continue to edit.
   - **Save & New**: Save the entry and open a new wizard.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 216.

Deleting Roaming Hosts

To delete a roaming host:
1. From the Data Management tab, select the DHCP tab -> Networks tab -> Roaming Hosts -> roaming_host check box, and then select Delete or Schedule Delete from the drop-down menu.
2. To delete the roaming host now, in the Delete Confirmation dialog box, click Yes. To schedule the deletion, see Scheduling Tasks on page 216.
   The Grid Manager puts the deleted roaming host in the Recycle Bin, if enabled.
Chapter 23 Configuring DHCP Services

This chapter explains how to configure DHCP services. It contains the following sections:

- About Configuring DHCP Services on page 618
- Configuring General DHCP Properties on page 619
- Configuring UTF-8 Encoding for Hostnames on page 620
- Configuring DHCP Lease Times on page 621
  - Keeping Leases in Deleted Networks and Ranges on page 622
  - Controlling Lease Assignments on page 622
- Configuring Ping Settings on page 623
- Configuring BOOTP Properties on page 625
- About DHCP Options on page 626
  - DHCP Option Data Types on page 627
  - Configuring DHCP Options on page 628
  - Defining Option Spaces on page 628
  - Configuring Custom DHCP Options on page 629
  - Applying DHCP Options on page 629
  - Configuration Example: Defining a Custom Option on page 631
  - Defining Option 60 Match Rules on page 632
  - About the DHCP Relay Agent Option (Option 82) on page 633
- Configuring Thresholds for DHCP Ranges on page 634
- Configuring DHCP Logging on page 637
- About IF-MAP on page 638
  - Configuring a Grid to Support IF-MAP on page 638
  - Purging Data from the IF-MAP Server on page 639
- Starting DHCP Services on a Member on page 639
- Viewing DHCP Member Status on page 640
  - Viewing DHCP Configuration Files on page 641
About Configuring DHCP Services

When you configure a NIOS appliance to function as a DHCP server, you can set DHCP properties that control how the appliance operates. You can also specify configuration information the appliance includes in its DHCP messages. When a DHCP server assigns an IP address to a client, it can include information the client needs to connect to the network and communicate with other hosts and devices on the network. You can set these properties at the grid level and override them for a member, network, shared network, DHCP range, fixed address, reservation, host address, or roaming host.

When you configure a DHCP object that has inherited DHCP properties, you can either keep the inherited properties or override them. The appliance displays the inherited values and the levels from which the DHCP properties are inherited. For information, see About DHCP Inheritance on page 582.

You can configure and define the following DHCP properties:

- General properties, as described in Configuring General DHCP Properties on page 619.
- UTF-8 encoding for host names, as described in Configuring UTF-8 Encoding for Hostnames on page 620.
- DHCP lease times, as described in Configuring DHCP Lease Times on page 621.
- Ping settings, as described in Configuring Ping Settings on page 623.
- BOOTP properties, as described in Configuring BOOTP Properties on page 625.
- Custom DHCP options, as described in About DHCP Options on page 626.
- DDNS settings, as described in Chapter 18, Configuring DDNS Updates from DHCP, on page 501.
- Thresholds for DHCP ranges, as described in Configuring Thresholds for DHCP Ranges on page 634.
- DHCP logging messages, as described in Configuring DHCP Logging on page 637.
- Lease Logging member, as described in Configuring the Lease Logging Member on page 665.
- Support for publishing DHCP data to IF-MAP servers, as described in Configuring a Grid to Support IF-MAP on page 638.

Note: Limited-access admin groups can access certain DHCP resources only if their administrative permissions are defined. For information on setting permissions for admin groups, see Administrative Permissions for DHCP Resources on page 121.
### Configuring General DHCP Properties

When you configure general DHCP properties at the grid level, the configuration applies to the entire grid. Though you can set DHCP properties at the grid level, you can enable DHCP services at the member level only. Infoblox recommends that you configure the DHCP properties before you enable DHCP on the appliance. Depending on the properties, you can override some of them for the members, networks, DHCP ranges, fixed addresses, reservations, host addresses, and roaming hosts. To override an inherited DHCP property, click **Override** next to the property to enable the configuration.

To configure general properties for the grid or member:

1. **Grid**: From the **Data Management** tab, select the **DHCP** tab, and then select **Grid DHCP Configuration** from the Toolbar.
   - **Member**: From the **Data Management** tab, select the **DHCP** tab → **Members** tab → **Members** → **member** check box, and then click the **Edit** icon.

2. In the **DHCP Properties** editor, select the **General** tab and complete the following:
   - **Authoritative**: Select **DHCP server is authoritative for the domain**. Only authoritative DHCP servers can send clients DHCPNAK messages when they request invalid IP addresses. For example, a client moves to a new subnet and broadcasts a DHCPREQUEST message for its old IP address. An authoritative DHCP server responds with a DHCPNAK, causing the client to move to the INIT state and to send a DHCPDISCOVER message for a new IP address. Authoritative servers also respond to DHCPINFORM messages from clients that receive their IP addresses from the DHCP server and require additional options after the initial leases have been granted.
   - **Microsoft Clients Code Page**: From the drop-down list, select the code page with which the host names are encoded when the appliance converts the Microsoft code page encoded host names to UTF-8 characters. For information, see *UTF-8 Encoding* on page 587.

3. Click **Toggle Advanced Mode** if the editor is in basic mode. When the additional tabs appear, click the **Advanced** subtab and complete the following:
   - **Ignore Optionlist**: Select **Ignore optionlist requested by client and return all defined options** if you want the appliance to ignore the requested list of options in the DHCPREQUEST messages it receives from DHCP clients, and to include all the configured options in the DHCPACK and DHCPOFFER messages it sends back to the clients.
   - **Failover Port**: You can modify the port number that members use for failover associations. You can use any available port from 1 to 63999. The default is 647 for a new installation and 519 for an upgrade.
   - **LEASEQUERY**: Select **Allow LEASEQUERY** to enable the DHCP server to respond to DHCPLEASEQUERY messages.

4. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and continue editing.

To configure or override general DHCP properties for other DHCP objects:

1. **Network**: From the **Data Management** tab, select the **DHCP** tab → **Networks** tab → **Networks** → **network** check box, and then click the **Edit** icon.
   - **DHCP Range**: From the **Data Management** tab, select the **DHCP** tab → **Networks** tab → **Networks** → **network** → **DHCP_range** check box, and then click the **Edit** icon.
   - **Fixed Address**: From the **Data Management** tab, select the **DHCP** tab → **Networks** tab → **Networks** → **network** → **fixed_address** check box, and then click the **Edit** icon.
   - **Reservation**: From the **Data Management** tab, select the **DHCP** tab → **Networks** tab → **Networks** → **network** → **reservation** check box, and then click the **Edit** icon.
   - **Host Address**: From the **Data Management** tab, select the **DHCP** tab → **Networks** tab → **Networks** → **network** → **host_record** check box, and then click the **Edit** icon. Select the host IP address, and then click the **Edit** icon.
Configuring DHCP Services

Roaming Host: From the Data Management tab, select the DHCP tab → Networks tab → Roaming Hosts → roaming_host check box, and then click the Edit icon.

2. In the DHCP Properties editor, select the DHCP Options Basic or DHCP Basic tab and complete the following:
   - **Routers**: Click the Add icon. Grid Manager adds a row to the table. In the table, enter the IP address of the router that is connected to the same network as the DHCP client. When configuring this for a template, enter the offset value of the IP address of the router. The DHCP server includes this information in its DHCPOFFER and DHCPACK messages.
   - **Domain Name**: Enter the name of the domain for which the grid serves DHCP data. The DHCP server includes this domain name in Option 15 when it responds with a DHCPOFFER packet to a DHCPDISCOVER packet from a client. If DDNS is enabled on the DHCP server, it combines the host name from the client and this domain name to create the FQDN (fully-qualified domain name) that it uses to update DNS. For information about DDNS, see Chapter 18, Configuring DDNS Updates from DHCP, on page 501.
   - **DNS Servers**: Click the Add icon. Grid Manager adds a row to the table. In the table, enter the IP address of the DNS server to which the DHCP client sends name resolution requests. The DHCP server includes this information in the DHCPOFFER and DHCPACK messages.
   - **Broadcast Address**: Enter the broadcast IP address of the network to which the DHCP server is attached. When configuring this for a template, enter the offset value of the broadcast IP address of the network.

3. Click **Toggle Advanced Mode** if the editor is in basic mode. When the additional tabs appear, click the Advanced subtab and complete the following:
   - **Authoritative**: For networks only. Click DHCP Server is authoritative for the domain to enable the DHCP server to be authoritative for the domain.
   - **Ignore Optionlist**: Click Ignore optionlist requested by client and return all defined options if you want the appliance to ignore the requested list of options in the DHCPREQUEST messages it receives from DHCP clients, and to include all the configured options in the DHCPOFFER and DHCPACK messages it sends back to the clients.

4. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and continue editing.

**CONFIGURING UTF-8 ENCODING FOR HOSTNAMES**

The NIOS appliance supports UTF-8 encoding of hostnames for Microsoft Windows clients that support Microsoft Windows code pages. When you use the appliance as a DHCP server, you can configure the DHCP service on the appliance to convert client hostnames that are encoded with a Microsoft code page to UTF-8 encoded characters. The appliance stores the UTF-8 encoded hostnames in the database. If you also configure the DHCP service on the appliance to perform DDNS updates, the appliance sends the UTF-8 encoded hostnames in the DDNS updates.

To configure UTF-8 encoding for hostnames:

1. **Grid**: From the Data Management tab, select the DHCP tab, and then select Grid DHCP Properties from the Toolbar.

2. **Member**: From the Data Management tab, select the DHCP tab → Members tab → Members → member check box, and then click the Edit icon.

2. In the DHCP Properties editor, select the General tab and complete the following:
   - **Microsoft Clients Code Page**: From the drop-down list, select the code page with which the host names are encoded when the appliance converts the Microsoft code page encoded host names to UTF-8 characters. For information, see UTF-8 Encoding on page 587.

3. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and continue editing.
Configuring DHCP Lease Times

When you configure DHCP general properties, you can specify the length of time the DHCP server leases an IP address to a client. The default on the appliance is 12 hours, and you can change this default according to your network requirements. There are a number of factors to consider when setting the lease time for IP addresses, such as the types of resources and clients on the network, and impact to traffic and performance. With NIOS appliances, you can set lease times at different levels, based on these factors. You can set a default lease time at the grid level and then override this setting for specific members, networks, IP address ranges or fixed addresses when appropriate.

Some hosts use PXE (Preboot Execution Environment) to boot remotely from a server. When such a host starts up, it first requests an IP address so it can connect to a server on the network and download the file it needs to boot. After it downloads the file, the host reboots and sends another IP address request. To better manage your IP resources, set a different lease time for PXE boot requests. You can configure the DHCP server to allocate an IP address with a shorter lease time to hosts that send PXE boot requests, so IP addresses are not leased longer than necessary.

You can configure lease times at the grid level and override them at the member, network, DHCP range, fixed address, reservation, and host record levels. Depending on the DHCP object you are configuring, the appliance displays only the properties that apply to the object. To override an inherited DHCP property, click Override next to the property to enable the configuration. For information, see Overriding DHCP Properties on page 583.

To configure DHCP lease times:

1. **Grid**: From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar.

   **Member**: From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box, and then click the Edit icon.

   **Network**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon.

   **DHCP Range**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range check box, and then click the Edit icon.

   **Fixed Address**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> fixed_address check box, and then click the Edit icon.

   **Reservation**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> reservation check box, and then click the Edit icon.

   **Host Address**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> host_record check box, and then click the Edit icon.

   **Roaming Host**: From the Data Management tab, select the DHCP tab -> Networks tab -> Roaming Hosts -> roaming_host check box, and then click the Edit icon.

2. In the DHCP Properties editor, select the **General** tab and complete the following:

   — **Lease Time**: Enter the lease time and select the time unit from the drop-down list. The default is 12 hours.

3. In the DHCP Properties editor, click **Toggle Advanced Mode** if the editor is in basic mode. When the additional tabs appear, click the **General** tab -> **Advanced** tab and complete the following:

   — **PXE Lease Time**: Select **Enable PXE Lease Time** if you want the DHCP server to use a different lease time for PXE clients. You can specify the duration of time it takes a host to connect to a boot server, such as a TFTP server, and download the file it needs to boot. For example, set a longer lease time if the client downloads an OS (operating system) or configuration file, or set a shorter lease time if the client downloads only configuration changes. Enter the lease time for the preboot execution environment for hosts to boot remotely from a server.

4. Select one of the following:

   — **Save & Close**: Save the entry and close the editor.

   — **Save**: Save the entry and continue editing.
Keeping Leases in Deleted Networks and Ranges

You can configure the DHCP server to store leases in a deleted DHCP range for up to one week after the leases expire. When you add a new DHCP range that includes the IP addresses of these leases or assign the DHCP range to another member within the grid, the appliance automatically restores the active leases. You can configure this feature for the grid, and override the configuration for members, networks, and DHCP ranges.

To keep active leases in a deleted DHCP range:

1. **Grid:** From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar.
   **Member:** From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box, and then click the Edit icon.
   **Network:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon.
   **DHCP Range:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range check box, and then click the Edit icon.

2. In the DHCP Properties editor, click Toggle Advanced Mode if the editor is in basic mode. When the additional tabs appear, click the General tab -> Advanced tab and complete the following:
   - **Lease Deletion:** When you select Keep leases from deleted range until one week after expiration and delete a DHCP range with active leases, the appliance stores these leases for up to one week after they expire.

3. Select one of the following:
   - **Save & Close:** Save the entry and close the editor.
   - **Save:** Save the entry and continue editing.

Controlling Lease Assignments

You can set parameters to control how the DHCP server responds to lease requests within a specific DHCP range. When you set a DHCP range to deny all leases requests, the appliance does not assign IP addresses within this range to DHCP clients. This is useful when you want DHCP clients with IP addresses within this range to obtain new IP addresses when they renew their leases. When a client with an IP address within this range broadcasts a DHCPREQUEST message for its old IP address, the authoritative DHCP server responds with a DHCPNAK. This causes the client to move to the INIT state and to send a DHCPDISCOVER message for a new IP address.

You can also configure the DHCP server to assign or deny IP addresses within a DHCP range to known and unknown DHCP clients. Known clients include roaming hosts and clients with fixed addresses or DHCP host entries. Unknown clients include clients that are not roaming hosts and clients that do not have fixed addresses or DHCP host entries.

To control how the appliance assigns leases to client requests:

1. **DHCP Range:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range check box, and then click the Edit icon.

2. In the DHCP Properties editor, click Toggle Advanced Mode if the editor is in basic mode. When the additional tabs appear, click the General tab -> Advanced tab and complete the following:
   - **Allow/Deny Clients**
     - **Known Clients:** Select this check box, and then select Allow or Deny from the drop-down list to assign or deny IP addresses within this range to known DHCP clients. Known DHCP clients include roaming hosts and clients with fixed addresses or DHCP host entries. Note that the appliance cannot deny an IP address to a fixed address within this range. You must disable the fixed address if you do not want it to obtain an IP address here.
     - **Unknown Clients:** Select this check box, and then select Allow or Deny from the drop-down list to assign or deny IP addresses within this range to unknown DHCP clients. Unknown DHCP clients include clients that are not roaming hosts and clients that do not have fixed addresses or DHCP host entries.
     - **Deny Leases:** Select Deny all lease requests for this range to deny all lease requests from DHCP clients.
3. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and continue editing.

**Configuring Ping Settings**

When a DHCP client first tries to connect to a network, it broadcasts its request for an IP address. When the appliance receives such a request, it checks its record of assigned IP addresses and leases. Because there are a limited number of IP addresses available, the appliance reassigns IP addresses whose leases might have expired. Therefore, once the appliance selects a candidate IP address for lease, it sends an ICMP echo request (or ping) to the IP address to verify that it is not in use.

If the appliance receives a response, this indicates that the IP address is still in use. Note that the lease status for this IP address is **Abandoned**. The appliance then selects another candidate IP address and sends it a ping. The appliance continues this process until it finds an IP address that does not respond to the ping. The appliance then sends a DHCPOFFER message with the unused IP address to the DHCP client.

*Figure 23.1 Ping Overview*
By default, the appliance pings the candidate IP address once and waits one second for the response. You can change these default settings to better suit your environment. Though you can increase the ping or timeout value to accommodate delays caused by problems in the network, increasing any of these values increases the delay a client experiences when acquiring a lease. You can also disable the appliance from sending pings by changing the number of pings to 0.

You can define ping settings for an entire grid, and when necessary, define different ping settings for a member. Settings at the member level override settings at the grid level.

To configure ping settings:

1. **Grid:** From the Data Management tab, select the DHCP tab, and then click Grid DHCP Configuration from the toolbar.
   
   **Member:** From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box, and then click the Edit icon.

2. In the DHCP Properties editor, click **Toggle Advanced Mode** if the editor is in basic mode. When the additional tabs appear, click the General tab -> Advanced tab and complete the following:
   
   — **Number of Ping Requests:** Enter the number of pings the appliance sends to an IP address to verify that it is not in use. The range is 0 to 10, inclusive. Enter 0 to disable DHCP pings. For information, see Configuring Ping Settings on page 623.
   
   — **Ping Timeout (Seconds):** Enter the ping timeout value. The range is 1 to 5, inclusive.

3. Select one of the following:
   
   — **Save & Close:** Save the entry and close the editor.
   
   — **Save:** Save the entry and continue editing.
Configuring BOOTP Properties

You can configure the DHCP server to support clients that use BOOTP (bootstrap protocol) or that include the TFTP server name option and boot file name option in their DHCPREQUEST messages. You can specify the name or IP address of the boot server and the name of the file the host needs to boot.

You can configure the BOOTP properties at the grid level and override them for members, networks, DHCP ranges, fixed addresses, and reservations, host addresses, and roaming hosts. To override an inherited DHCP property, click Override next to the property to enable the configuration. For information, see Overriding DHCP Properties on page 583.

To configure or override BOOTP properties:

1. **Grid Level**: From the Data Management tab, select the DHCP tab, and then click Grid DHCP Configuration from the Toolbar.

   - **Member Level**: From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box, and then click the Edit icon.

   - **Network Level**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon.

   - **DHCP Range Level**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range check box, and then click the Edit icon.

   - **Fixed Address Level**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> fixed_address check box, and then click the Edit icon.

   - **Reservation**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> reservation check box, and then click the Edit icon.

   - **Host Address**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> host_record check box, and then click the Edit icon. Select the host IP address, and then click the Edit icon.

   - **Roaming Host**: From the Data Management tab, select the DHCP tab -> Networks tab -> Roaming Hosts -> roaming_host check box, and then click the Edit icon.

2. In the DHCP Properties editor, select the BOOTP tab and complete the following

   - **Deny BOOTP Requests**: Select Deny BOOTP Requests to disable the BOOTP settings and deny BOOTP boot requests.

   - Complete the following in the **BOOTP Settings** section:

     - **Boot File**: Enter the name of the boot file the client must download.

     - **Next Server**: Enter the IP address or hostname of the boot file server where the boot file is stored. Complete this field if the hosts in your network send requests for the IP address of the boot server. If the TFTP server is the NIOS appliance that is also serving DHCP, enter the IP address of the appliance.

     - **Boot Server**: Enter the name of the server on which the boot file is stored. Clients can request for either the boot server name or IP address. Complete this field if the hosts in your network send requests for the boot server name. If the TFTP server is the appliance that is also serving DHCP, enter the name of the appliance.

   **Note**: Enter values in both the **Next Server** and **Boot Server** fields if some hosts on your network require the boot server name and others require the boot server IP address.

3. Select one of the following:

   - **Save & Close**: Save the entry and close the editor.

   - **Save**: Save the entry and continue editing.
About DHCP Options

DHCP options provide specific configuration and service information to DHCP clients. These options appear as variable-length fields at the end of the DHCP messages that DHCP servers and clients exchange. For example, DHCP option 3 is used to list the available routers in the network of the client and option 6 is used to list the available DNS servers.

An option space is a collection of options. ISC (Internet Systems Consortium) DHCP has five predefined option spaces: dhcp, agent, server, nwip, and fqdn. The NIOS appliance supports only the predefined DHCP option space, which contains the industry standard options as well as additional options you can configure as needed:

- Predefined options: These are option codes 1 to 125. They are allocated by the IANA and defined by IETF standards. The DHCP server knows these standard options, and they are predefined on the server. You cannot redefine these options or delete them from the DHCP option space.
- Custom options: These are option codes 126 to 254. They are not defined by IETF standards and are available for private use. You can use these option codes to provide configuration or service information that none of the predefined options provide.

You can also create option spaces to define new groups of options. For example, you can create additional option spaces to define vendor specific options, which are encapsulated in option 43. When a DHCP client requests vendor specific options, it makes a request using the vendor identifier set in option 60 and a list of requested vendor specific options (option 43). The DHCP server then responds with the list of replies for the various options encapsulated into option 43.

Note that custom options defined in the DHCP option space are included in the options section of the DHCP messages that DHCP servers and clients exchange. Custom options defined in a user-defined option space are always encapsulated in option 43 in DHCP messages.

You can apply options globally at the grid level, or more specifically at the member, network, range, host and roaming host levels.

You can also create an option filter the appliance uses to filter address requests by the DHCP options of requesting hosts. The filter instructs the appliance to either grant or deny an address request if the requesting host matches the filter. For information, see Defining Option Filters on page 684.

The DHCP option configuration conforms to the following RFCs:

- RFC 2132, DHCP Options and BOOTP Vendor Extension
- RFC 3046, DHCP Relay Agent Information Option. The supported options include option 60 (Client Identifier), 21 (Policy Filter), 22 (Maximum Datagram Reassembly Size), 23 (Default IP Time-to-Live), and 82 (Support for Routed Bridge Encapsulation).
- RFC 3925, Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)
- RFC 2939, Procedures and IANA Guidelines for Definition of New DHCP Options and Message Types
DHCP Option Data Types

Each DHCP option is identified by a name and an option code number, and specifies a data type. The data type for some options is predefined. For example, in the DHCP option space, the data type for option 1: subnet-mask is an IP address. You cannot change the data type for this option. The data type for some options is user-defined and can be in one of the formats shown in Table 23.1.

Table 23.1 DHCP Option Data Types

<table>
<thead>
<tr>
<th>Data type</th>
<th>Specifies</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>An ASCII text string (the same as the text data type) or a list of hexadecimal characters separated by colons</td>
</tr>
<tr>
<td></td>
<td>Formatting to distinguish an ASCII text string from a hexadecimal string is important. For details, see the following section</td>
</tr>
<tr>
<td>Boolean</td>
<td>A flag with a value of either true or false (or on or off)</td>
</tr>
<tr>
<td>IP address</td>
<td>A single IP address</td>
</tr>
<tr>
<td>Array of IP addresses</td>
<td>A series of IP addresses, separated by commas</td>
</tr>
<tr>
<td></td>
<td>You can optionally include a space after each comma</td>
</tr>
<tr>
<td>Text</td>
<td>An ASCII text string</td>
</tr>
<tr>
<td>8-, 16-, or 32-bit unsigned integer</td>
<td>A numeric range of the following possible values</td>
</tr>
<tr>
<td></td>
<td>8-bit unsigned integer: from 0 to 255</td>
</tr>
<tr>
<td></td>
<td>16-bit unsigned integer: from 0 to 65,535</td>
</tr>
<tr>
<td></td>
<td>32-bit unsigned integer: from 0 to 4,294,967,295</td>
</tr>
<tr>
<td>8-, 16-, or 32-bit signed integer</td>
<td>A numeric range of the following possible values</td>
</tr>
<tr>
<td></td>
<td>8-bit signed integer: from -128 to 127</td>
</tr>
<tr>
<td></td>
<td>16-bit signed integer: from -32,768 to 32,767</td>
</tr>
<tr>
<td></td>
<td>32-bit signed integer: from -2,147,483,648 to 2,147,483,647</td>
</tr>
<tr>
<td>Domain name</td>
<td>A list of domain names, separated by spaces</td>
</tr>
</tbody>
</table>

When defining a hexadecimal string for a DHCP option (such as option 43, vendor encapsulated options), use only hexadecimal characters (0-9, a-f, or A-F) without spaces and separated by colons. The accepted form for a hexadecimal string, as presented in a regular expression, is \[0-9a-fA-F\]{1,2}(\[0-9a-fA-F\]{1,2})*

Two examples of correctly written hexadecimal strings:

- aa:de:89:1b:34
- 1C:8:22:A3 (Note that the DHCP module treats a single hexadecimal character, such as “8” as “08”.)

A few examples of incorrectly written hexadecimal strings:

- bb:4 5:d2:1f – Problem: The string erroneously includes a space between two characters (“4” and “5”).
- bb:45:d2:1g – Problem: The string erroneously includes a nonhexadecimal character (“g”).

The DHCP module treats incorrectly written hexadecimal strings as simple text strings, not hexadecimal strings. If the string appears in quotes, it is a text string.
Configuring DHCP Services

To use DHCP options, you can do the following:

- Configure one or more option spaces, as described in the next section Defining Option Spaces.
- Define custom options in the predefined DHCP option space or add options to an option space that you configured. For more information, see Configuring Custom DHCP Options on page 629.
- Specify values for the options and apply them to the grid, or to a member, network, range, fixed address, reservation, host, or roaming host. For more information, see Applying DHCP Options on page 629.

Defining Option Spaces

DHCP members support the DHCP option space by default. You can create additional option spaces to provide additional configuration or service information. Note that custom options defined in a user-defined option space are always encapsulated in option 43 in DHCP messages

To add a custom option space:

1. From the Data Management tab, select the DHCP tab -> Filters/Option Spaces tab-> Option Spaces.
2. Expand the Toolbar and click Add -> Option Space.
3. In the Option Space wizard, do the following:
   - Name: Enter the name of the option space.
   - Comment: Enter useful information about the option space.
   - Options: Click the Add icon to add options. For additional information, see the next section, Configuring Custom DHCP Options on page 629.
4. Select one of the following:
   - Save & Close: Save the entry and close the wizard.
   - Save & Edit: Save the entry and continue to edit.
   - Save & New: Save the entry and open a new wizard.

After you create an option space and add options to it, you can apply the options as described in Applying DHCP Options on page 629.
Configuring Custom DHCP Options

You can define custom options in the DHCP option space or in an option space that you configured, as follows:

1. From the Data Management tab, select the DHCP tab -> Filters/Option Spaces tab -> Option Spaces -> option_space check box, and then click the Edit icon.

2. In the Option Space editor, click the Add icon to add a custom option. In the new row, complete the following:
   - **Name:** Enter the name of the custom DHCP option.
   - **Code:** Select an option code from the drop-down list. Select a number between 126 and 254 if you are adding custom options to the DHCP option space. If you are adding custom options to an option space you configured, you can enter a number between 1 and 254.
   - **Type:** Select the option type (such as ip-address, text, boolean, and string as described in Table 23.1). For example, to create an option that defines the IP addresses of Solaris root servers, enter the name SrootIP4, select option code 126, and then select the type as ip-address.

   Click the Add icon to add more options.

3. Select one of the following:
   - **Save & Close:** Save the entry and close the editor.
   - **Save:** Save the entry and continue to edit.

Applying DHCP Options

Some options may apply to all networks and some may apply to specific ranges and even hosts. When you apply an option, you select the object to which the option is applied, such as the grid member, or network, and then specify a value for the option.

Use the following guidelines when specifying option values:

- Enter **false** or **true** for a Boolean Flag type value.
- Enter an ASCII text string, or enter a series of octets specified in hex, separated by colons.
- Separate multiple values by commas. For example, to enter multiple IP addresses for netbios-name-servers, enter a comma between each IP address.

Here are some examples of option names and correctly formatted values:

<table>
<thead>
<tr>
<th>Option name</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>option 61</td>
<td>MyPC</td>
<td>Double quotes are no longer needed for string type values</td>
</tr>
<tr>
<td>dhcp-client-identifier</td>
<td>43:4c:49:45:54:2d:46:4f:4f</td>
<td>Series of octets specified in hex, separated by colons for a Data-string type value</td>
</tr>
<tr>
<td>netbios-name-servers</td>
<td>10.1.1.5,10.1.1.10</td>
<td>Multiple IP addresses separated by commas</td>
</tr>
<tr>
<td>option-80</td>
<td>ABC123</td>
<td>Custom option number 80 set to the string ABC123.</td>
</tr>
</tbody>
</table>
To apply DHCP options:

1. **Grid**: From the Data Management tab, select the DHCP tab, and then click Grid DHCP Configuration from the Toolbar.

   **Member**: From the Data Management tab, select the DHCP tab → Members tab → Members → member check box, and then click the Edit icon.

   **Network**: From the Data Management tab, select the DHCP tab → Networks tab → Networks → network check box, and then click the Edit icon.

   **DHCP Range**: From the Data Management tab, select the DHCP tab → Networks tab → Networks → network → addr_range check box, and then click the Edit icon.

   **Fixed Address**: From the Data Management tab, select the DHCP tab → Networks tab → Networks → network → fixed_address check box, and then click the Edit icon.

   **Reservation**: From the Data Management tab, select the DHCP tab → Networks tab → Networks → network → reservation check box, and then click the Edit icon.

   **Host Address**: From the Data Management tab, select the DHCP tab → Networks tab → Networks → network → host_record check box, and then click the Edit icon. Select the host IP address, and then click the Edit icon.

   **Roaming Host**: From the Data Management tab, select the DHCP tab → Networks tab → Roaming Hosts → roaming_host check box, and then click the Edit icon.

2. In the DHCP Properties editor, select the DHCP Options or DHCP tab and complete the following:

   — The Custom DHCP Options section displays two fields. The first field displays Choose option. Click the arrow and select an option from the list. In the second field, enter a value for the selected option. Note that certain options have predefined data types and their values must be entered in a specific format. For information about the data types, see DHCP Option Data Types on page 627.

     Click + to add another option, or click - to delete an inherited option. When overriding an option, enter the new value for the selected option.

     Note that if you created an option space as described in Defining Option Spaces on page 628, this section displays a list of option spaces in the first drop-down menu, so you can select the option space of the option you want to define.

3. Select one of the following:

   — **Save & Close**: Save the entry and close the editor.

   — **Save**: Save the entry and continue to edit.
**Configuration Example: Defining a Custom Option**

In this example, you configure two custom options in the DHCP option space, and apply them to a DHCP range in the network 192.168.2.0/24.

Add the custom options to the DHCP options space:
1. From the Data Management tab, select the DHCP tab -> Filters/Option Spaces tab.
2. Click the Option Spaces subtab to display the panel, click the DHCP check box, and then click the Edit icon.
3. In the Option Space editor, click the Add icon. In the new row, complete the following:
   - Name: Enter tftp-server.
   - Code: Enter 150.
   - Type: Select array of ip-address.
4. Click the Add icon to add another option. In the new row, complete the following:
   - Name: Enter pxe-configfile.
   - Code: Enter 209.
   - Type: Select text.
5. Click Save & Close.

Enter values for the newly defined custom options and apply them to a DHCP range:
1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks subtab, and click the 192.168.2.0/24 network.
2. Click the 192.168.2.10 - 100 check box, and then click the Edit icon.
3. In the DHCP Properties editor, select the DHCP tab and complete the following in the Custom DHCP Options section:
   - From the drop-down list of options, select tftp-server (150) array of address. In the second field, enter 192.168.1.2.
   - Click + to add another option.
   - From the drop-down list of options, select pxe-configfile (209) text. In the second field, enter pxe.config, which is the file name of the boot image.
4. Click Save & Close.
5. Click Restart.

The member then includes options 150 and 209 in its DHCP messages to clients that are allocated IP addresses from the DHCP range 192.168.2.10 - 100.
Defining Option 60 Match Rules

The appliance uses option 60 (vendor-class-identifier) to forward client requests to the DHCP server for services that the clients require. You can define option 60 match rules and filter on these rules. You can set these rules for the grid and override for a member.

To define option 60 for the grid or member:

1. **Grid:** From the Data Management tab, select the DHCP tab, and then click Grid DHCP Configuration from the Toolbar.

   **Member:** From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box, and then click the Edit icon.

2. In the DHCP Properties editor, click **Toggle Advanced Mode** if the editor is in basic mode. When the additional tabs appear, click the DHCP Options tab -> Advanced tab and complete the following:

   To override the grid configuration for a member, click **Override** next to the property. Grid Manager hides the grid configuration. You can then add new values for the member.

   — **Option 60 (Vendor Class Identifier) Match Rules:** Click the Add icon if you want to add a match rule to a vendor class option. The appliance adds a row to the table. Complete the following:

     — **Option Space:** Select an option space from the drop-down list. This field appears only when you have custom option spaces. The appliance uses the default DHCP option space if you do not have custom option spaces.

     — **Match Value:** Enter the value you want the appliance to use when matching vendor class options.

     — **Is Substring:** Select this check box if the match value is a substring of the option data.

     — **Substring Offset:** Enter the number of characters at which the match value substring starts in the option data. Enter 0 to start at the beginning of the option data, enter 1 for the second position, and so on. For example, when you enter 2 here and have a match value of RAS, the appliance matches the value RAS starting at the third character of the option data.

     — **Substring length:** Enter the length of the match value. For example, if the match value is SUNW, the length is 4.

3. Select one of the following:

   — **Save & Close:** Save the entry and close the editor.

   — **Save:** Save the entry and continue to edit.
About the DHCP Relay Agent Option (Option 82)

The typical relationship between a DHCP client, relay agent, and server (that is, the NIOS appliance) on a network is as follows:

1. A DHCP client broadcasts a DHCPDISCOVER message on its network segment.
2. A DHCP relay agent on that segment receives the message and forwards it as a unicast message to one or more DHCP servers (such as NIOS appliances).
3. If the NIOS appliance accepts the address request, it responds to the relay agent with a DHCPOFFER message. If the appliance denies the request, it does not send any response in case other DHCP servers that might be involved respond instead.
4. The relay agent forwards the response to the client, usually as a broadcast message.

The situation is different for individual hosts connecting to the Internet through an ISP, usually over a circuit-switched data network.

1. A host connects to its ISP's circuit access concentration point, authenticates itself, and requests an IP address.
2. The circuit access unit relays the address request to a DHCP server, which responds with a DHCPOFFER message. To avoid broadcasting the DHCPOFFER over the network segment on which the host made the request, the relay agent sends the response directly to the host over the established circuit.

Option 82 assists the agent in forwarding address assignments across the proper circuit. When a relay agent receives a DHCPDISCOVER message, it can add one or two agent IDs in the DHCP option 82 suboption fields to the message. The two relay agent IDs are:

- **Circuit ID**: This identifies the circuit between the remote host and the relay agent. For example, the identifier can be the ingress interface number of the circuit access unit (perhaps concatenated with the unit ID number and slot number). The circuit ID can also be an ATM virtual circuit ID or cable data virtual circuit ID.
- **Remote ID**: This identifies the remote host. The ID can be the caller ID telephone number for a dial-up connection, a user name for logging in to the ISP, a modem ID, and so on. Because the remote ID is defined on the relay agent, which is presumed to have a trusted relationship with the DHCP server, and not on the untrusted DHCP client, the remote ID is also presumably a trusted identifier.

**Note**: For information about the relay agent option, refer to RFC3046, DHCP Relay Agent Information Option.

The NIOS appliance can screen address requests through a relay agent filter you set up using option 82. For information, see About Relay Agent Filters on page 682.

You can also use the relay agent information (circuit ID or remote ID) as a host identifier when configuring a fixed address, though you cannot do so in a host record. For information about how to configure a circuit ID or remote ID as an identifier, see Adding Fixed Addresses on page 609.
**Configuring Thresholds for DHCP Ranges**

Grid Manager can provide a view of the current overall DHCP address usage for the networks and DHCP ranges defined on each grid member. The view is in the form of a percent: address leases in use/total addresses for each network. Such information can indicate if there is a sufficient number of available addresses at each of these levels. It can also provide information about the distribution of address resources, indicating if there are too many unused addresses in one location while all the addresses in another are in use.

In addition to viewing the percent of addresses in use, you can also apply high and low watermarks for each DHCP range. These watermarks represent thresholds above or below which address usage is unexpected and might warrant your attention. For example, usage falling below a low watermark might indicate network issues preventing the renewal of leases. When usage for a DHCP range crosses a watermark, the appliance makes a syslog entry and—if configured to do so—sends the administrator alerts as SNMP traps and email notifications. *Figure 23.2* illustrates the relationship of allocated and available addresses to high and low watermarks in a DHCP range.

*Figure 23.2* *Overall DHCP Address Usage for a DHCP Range*

You can define watermarks at the grid, member, network, and DHCP range levels, but the appliance applies them solely to DHCP ranges. Because the appliance applies settings hierarchically in a parent-child structure, by defining watermarks once at a higher level, DHCP ranges can then inherit these settings without your needing to redefine them for each range. For example, if you set high and low watermarks for a grid, then each grid member, each network, and each DHCP range inherits these settings. However, if you override these settings at the member level, then the network and DHCP ranges for that member inherit its settings. If you override the grid member settings at the network level, then that network and any DHCP ranges within that network inherit the network-level settings. Finally, you can set high and low watermarks for an individual DHCP range, which override anything set at a higher level.

*Figure 23.3* shows different high and low watermark settings at different levels. Although you can set thresholds at four levels (grid, grid member, network, and DHCP range), the NIOS appliance applies them to DHCP ranges.
Address usage in a DHCP range can trigger an event and an email notification when it crosses a watermark. You must enable DHCP threshold and email warnings to receive events and notifications. The following are actions that do and do not trigger an address usage event and notification:

- Address usage triggers an event and the appliance sends a notification when the percentage of the allocated addresses in the DHCP range:
  - Exceeds the high watermark
  - Drops below or equals to the high watermark after exceeding it
  - Drops below the low watermark
  - Exceeds the low watermark after dropping below it

- Address usage does not trigger an event when the percentage of the allocated addresses in the DHCP range:
  - Never exceeds the low watermark
  - Initially exceeds the low watermark
  - Reaches a watermark but does not cross it

**Note:** You can effectively disable address usage events for a DHCP range by setting its high watermark at 100% and the low watermark at 0% (default setting for the low watermark). Because address usage cannot cross these watermarks, no events can occur.

You can configure the threshold settings at the grid level and override them at the member, network, and DHCP range levels. To override an inherited DHCP property, click **Override** next to the property to enable the configuration. For information, see *Overriding DHCP Properties* on page 583.
To configure thresholds:

1. **Grid**: From the Data Management tab, select the DHCP tab, and then click Grid DHCP Configuration from the Toolbar.

   **Member**: From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box, and then click the Edit icon.

   **Network**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon.

   **DHCP Range**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range check box, and then click the Edit icon.

2. In the DHCP Properties editor, select the Thresholds tab and complete the following:
   - **DHCP Thresholds**: Select Enable DHCP Thresholds to enable the DHCP threshold feature.
     - **High-water Mark**: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range exceeds this number, the appliance makes a syslog entry and—if configured to do so—sends an SNMP trap and an email notification to a designated destination. The default is 95.
     - **Low-water Mark**: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range drops below this number, the appliance makes a syslog entry and—if configured to do so—sends an SNMP trap and an email notification to a designated destination. The default is 0. Address usage must initially exceed the low-water mark threshold and then dip below it before the appliance considers low address usage an event requiring an alert.
     - **Enable SNMP Warnings**: Select this for the appliance to send an SNMP trap to the trap receiver that you define for the grid when DHCP address usage crosses a watermark threshold.
     - **Enable Email Warnings**: Select this for the appliance to send an email notification to an administrator if DHCP address usage crosses a high-water or low-water mark threshold.
     - **Email Addresses**: Click Override to override the grid administrator email address configured in the Data Management tab -> Grid tab. This address is not hierarchically inherited from the grid DHCP configuration. Click the Add icon, and then enter an email address to which you want the appliance to send email notifications when the DHCP address usage for the network crosses a threshold. You can create a list of email addresses.

3. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and continue editing.
Configuring DHCP Logging

If you have a syslog server operating on your network, you can specify in which facility you want the server to display the DHCP logging messages. You can also select the grid member on which you want to store the DHCP lease history log. For information, see Configuring the Lease Logging Member on page 665. You can configure DHCP and lease logging only on the grid and member levels.

To specify DHCP logging for the grid or member:

1. **Grid:** From the Data Management tab, select the DHCP tab, and then click Grid DHCP Configuration from the Toolbar.
   
   **Member:** From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box, and then click the Edit icon.

2. In the DHCP Properties editor, select the Logging Basic tab and complete the following:
   
   — **Syslog Facility:** From the drop-down list, select the facility that is used to tag syslog messages from the DHCP server. This facility can be used to filter messages on a central syslog server.

3. Select one of the following:
   
   — **Save & Close:** Save the entry and close the editor.
   
   — **Save:** Save the entry and continue editing.
Configuring DHCP Services

About IF-MAP

You can configure Infoblox DHCP servers to publish DHCP data to an IF-MAP server. The IF-MAP server takes real-time information from different sources and stores it in a shared database from which clients can retrieve information about network devices, their status and activities. For details about the IF-MAP protocol, refer to http://www.trustedcomputinggroup.org. For information about the Infoblox IF-MAP server, refer to the Infoblox Administrator Guide for Infoblox Orchestration Servers.

Each Infoblox DHCP server in a grid can function as an IF-MAP client, with the ability to publish lease information to an IF-MAP server. The DHCP server updates an IF-MAP server with metadata using the XML format and SOAP/HTTPS bindings specified in IF-MAP v1.1r5.

When the DHCP server grants a lease and sends the DHCPACK packet to the DHCP client, it updates the link in the IF-MAP server between the leased IP address and client MAC address with ip-mac metadata with the following attributes: start-time, end-time, and dhcp-server. The dhcp-server attribute contains the DHCP server hostname. The ip-mac metadata is attached to a link with:

- An ip-address identifier with the type attribute set to IPv4, a value attribute that contains the leased IP address, and the administrative-domain attribute set to the network view to which the IP address belongs.
- A mac-address identifier with a value attribute that contains the client MAC address. It does not have the administrative-domain attribute.

The Infoblox DHCP server also publishes data when the lease changes. When the lease is released or when an active lease expires, the DHCP server sends a publish request to delete the IP address/MAC address association information from the IF-MAP server.

Configuring a Grid to Support IF-MAP

Following are the tasks to enable DHCP servers in a grid to function as IF-MAP clients:

1. Enable IF-MAP in the grid, and specify the URL and port of the IF-MAP server.
2. Enable IF-MAP on each grid member, and specify the username and password the member uses to connect to the IF-MAP server.

To enable IF-MAP on the grid:

1. From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar.
2. In the Grid DHCP Properties editor, click the IF-MAP tab, and then complete the following:
   - Enable IF-MAP Publishing: Select this check box.
   - IF-MAP Server URL: Enter the URL of the IF-MAP server to which the grid members publish DHCP data. The URL must begin with http:// or https://; for example, https://<server_ip_addr>/ifmap.
   - IF-MAP Server Port: The default HTTP port is 80 and the default HTTPS port is 443. Optionally, you can specify a different port on the IF-MAP server.
3. Select one of the following:
   - Save & Close: Save the entry and close the editor.
   - Save: Save the entry and continue editing.

To enable an appliance to function as an IF-MAP client:

1. From the Data Management tab, select the DHCP tab -> Members tab -> member check box, and then click the Edit icon.
2. In the Member DHCP Properties editor, click the IF-MAP tab, and then complete the following:
   - Enable DHCP-IF MAP Publishing: Select this check box.
   - IF-MAP Server Username: Enter the username the member uses to connect to the IF-MAP server. This username must have been configured as a valid username on the IF-MAP server. Each member must have its own username.
   - IF-MAP Server Password: Enter the password the member uses to connect to the IF-MAP server.
3. Select one of the following:
   — **Save & Close**: Save the entry and close the editor.
   — **Save**: Save the entry and continue editing.

---

**Purging Data from the IF-MAP Server**

You can purge all data published by a specified member. To purge the data published by all members in a grid, you must purge data for each member individually.

To purge DHCP data published by a member on the IF-MAP server:

1. From the **Data Management** tab, select the **DHCP** tab -> **Members** tab, and then click **Purge IF-MAP Data** from the Toolbar.
2. In the **Purge IF-MAP Data** dialog box, Grid Manager displays the last selected grid member. To select a different member, click **Select Member**. If there are multiple members, Grid Manager displays the **Member Selector** dialog box from which you can select one. Click the member name in the dialog box, and then click **Purge** to purge the DHCP data published by the grid member.

---

**STARTING DHCP SERVICES ON A MEMBER**

After you complete the DHCP configuration, you can start DHCP services on a member.

To start DHCP services on a member:

1. From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **Members** -> **member** check box.
2. Expand the Toolbar and click **Start**.
3. In the **Start Member DHCP Service** dialog box, click **Yes**.
4. Grid Manager starts DHCP services on the selected member.

You can stop DHCP services on a member by selecting the member check box and click **Stop** from the Toolbar.
**Viewing DHCP Member Status**

You can view DHCP member status after you configure DHCP properties and start or stop DHCP services on a member. To view member status:

1. From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box.
2. Grid Manager displays the following information:
   - **Name**: The name of the grid member.
   - **Status**: The status of the DHCP services on the member. This can be one of the following:
     - **Not Running**: DHCP services have not been started on the member.
     - **Running**: The DHCP services are running properly on the member.
     - **Warning**: The member is connecting or synchronizing with its grid master.
     - **Error**: The member is offline, is not licensed (that is, it does not have a DNSOne license with the Grid upgrade that permits grid membership), is upgrading or downgrading, or is shutting down.
   - **Comment**: The information you entered for the member.
   - **DHCP Utilization**: The percentage of the total DHCP utilization of the member. This is the percentage of the total number of DHCP hosts, fixed addresses, reservations, and leases assigned to the member versus the total number of IP addresses (excluding IP addresses in the exclusion range) and all DHCP objects assigned to the member. Note that only enabled objects are included in the calculation. The appliance updates the utilization data every 15 minutes. The appliance displays the utilization data in one of the following colors:
     - **Red**: The DHCP resources are 100% utilized.
     - **Yellow**: The utilization percentage is over the effective high watermark threshold.
     - **Blue**: The utilization percentage is below the effective low watermark threshold.
     - **Black**: The utilization percentage is at any number other than 100%, or within the effective thresholds.
   - **Site**: The site to which the member belongs. This is one of the predefined extensible attributes.

You can mouse over the informational icon next to the status to view detailed information.

You can select the following additional columns for display:
- **Address**: The IP address of the member.
- **Static Addresses**: The number of static IP addresses.
- **Dynamic Addresses**: The number of dynamically assigned IP addresses.

You can view detailed information about a specific member by clicking the member link. Grid Manager displays the following information about the selected member:

- **Network**: The network assigned to the member.
- **Comment**: The information about the network.
- **DHCP Utilization**: The percentage of the DHCP usage of the network. This is the percentage of the total number of fixed addresses, reservations, hosts, and active leases on the network over the total IP addresses in the range, excluding the number of addresses on the network. Note that only enabled objects are included in the calculation.
- **Site**: The site to which the DHCP object belongs. This is one of the predefined extensible attributes.
In the member panel, you can select the following additional fields for display:

- **Disabled**: Indicates whether the member is disabled or not.
- **IPAM Utilization**: When you define a network, this is the percentage based on the IP addresses in use divided by the total addresses in the network. For example, in a /24 network, if there are 25 static IP addresses defined and a DHCP range that includes 100 addresses, the total number of IP addresses in use is 125. Of the possible 256 addresses in the network, the IPAM utilization is about 50% for this network.

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

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

- Extensible attributes that associate with the network.

You can also sort the data in ascending or descending order by column. For information, see *Customizing Tables* on page 44.

**Viewing DHCP Configuration Files**

You can view the DHCP configuration of a selected member. The format of the configuration file depends on the browser you use.

To view the DHCP configuration of a selected member:

1. From the **Data Management** tab, select the **DHCP** tab → **Members** tab → **Members** → *member* check box.
2. Expand the Toolbar and select **View DHCP Configuration**. Grid Manager displays the DHCP configuration of the selected member in a new browser. You can print and save the file using the corresponding functions in your browser.
Chapter 24  Managing DHCP Templates

This chapter explains how to configure and manage DHCP templates. It contains the following sections:

•  *About DHCP Templates*  on page 644
•  *About DHCP Range Templates*  on page 645
  —  *Adding DHCP Range Templates*  on page 645
  —  *Modifying DHCP Range Templates*  on page 646
•  *About Fixed Address/Reservation Templates*  on page 647
  —  *Adding Fixed Address/Reservation Templates*  on page 647
  —  *Modifying Fixed Address/Reservation Templates*  on page 648
•  *About Network Templates*  on page 649
  —  *Adding Network Templates*  on page 649
  —  *Modifying Network Templates*  on page 650
•  *Viewing Templates*  on page 651
•  *Deleting Templates*  on page 651
•  *Configuration Example: Creating a Network Using a Template*  on page 652
About DHCP Templates

A template contains a set of predefined properties that you use to create a DHCP range, a fixed address, a reservation, a roaming host, or a network. It is metadata that you can modify and reuse. When you create a DHCP range using a template, the range inherits the properties of the template. Using a template enables you to create objects in a quick and consistent way. For example, you can create a network template that has a fixed netmask of /24 and extensible attribute “State” set to California. You can then use the template to create networks in California that contain /24 netmasks.

There are three types of templates:

- A DHCP range template, containing DHCP range settings, such as the total number of IP addresses allocated to a range. You can add a DHCP range template to a network template. For information, see About DHCP Range Templates on page 645.

- A fixed address/reservation template, containing information for creating fixed addresses, reservations, or roaming hosts. You can add a fixed address/reservation template to a network template. For information, see About Fixed Address/Reservation Templates on page 647.

- A network template, containing basic network properties for creating networks. It is also a container that holds your DHCP range templates and fixed address/reservation templates. When you create a network using a network template, the network inherits the properties of the range and fixed address/reservation templates. You can create a network in any network view using a network template. For information, see About Network Templates on page 649.

To create a template, first decide the purpose of the template and how you may use it, and then give it a meaningful name. Since you can potentially add DHCP range and fixed address/reservation templates to a network template, create the DHCP range and fixed address/reservation templates before you create a network template. For information, see Configuration Example: Creating a Network Using a Template on page 652.

You can also modify and delete a template. Note that modifying or deleting a template does not affect existing objects created based on the template. You must be a superuser or have read/write permissions to add, modify, or delete a template. A superuser can set other admin group privileges on templates. For information, see Administrative Permissions for DHCP Templates on page 127. You can also define extensible attributes for these templates when you create them. For information, see Using Extensible Attributes on page 225.
**About DHCP Range Templates**

A DHCP range template has properties similar to those of a real DHCP range, except for the following:

- It is uniquely identified by a name.
- It can be defined independently and can be referred by multiple network templates.
- The start address and end address fields are replaced by numbers of the offset from the network start address and the number of IP addresses in the range.
- It does not have a disabled status.
- In the DHCP Options tab of a DHCP range template, the broadcast address is an address offset number rather than a broadcast IP address; network router addresses are offset numbers as well.

An offset in a DHCP range template indicates the starting IP address of the DHCP range object created from the template. For example, you can create a network template called `test_network_template` and a DHCP range template `test_range_template` linked to this network template. If the `test_range_template` has an offset value 10, when you create a 10.0.0.0/8 network using the `test_network_template`, the appliance creates a DHCP range with the starting IP address 10.0.0.10. If you create a 20.0.0.0/8 network using the `test_network_template`, the appliance creates a DHCP range with the starting IP address 20.0.0.10.

- For the exclusion range in the template, the start address and end address are replaced by the number of offsets in the DHCP range template’s start address and the number of IP addresses in the exclusion range.
- After you create a DHCP range template, you can use the template to create a DHCP range. You can also modify the template by configuring other properties, such as exclusion ranges and DHCP filters.

**Adding DHCP Range Templates**

To create a DHCP range template:

1. From the Data Management tab, select the DHCP tab.
2. Expand the Toolbar and click **Add -> Templates -> Range**.
3. In the Add DHCP Range Template wizard, do the following:
   - **Name**: Enter a name that helps identify the DHCP range template. For example, enter **Region 1 IT** if you want to use this template to create DHCP ranges for the IT department in Region 1.
   - **Offset**: An offset in a DHCP range template determines the starting IP address of the range. The appliance adds the offset value you enter here to the start IP address of the network in which you create a DHCP range using this template. That IP address becomes the start IP address of the DHCP range. For example, you specify an offset value of 25 for a 25.0.0.0/8 network using the DHCP range template, the appliance creates a DHCP range with the start IP address of 25.0.0.25 in the network.
   - **Number of Addresses**: Enter the total number of IP addresses to be included in the DHCP range.
   - **Comment**: Enter useful information about the template.
4. Click **Next** and select one of the following to provide DHCP services for the range:
   - **None**: Select this if you do not want to include member assignment information in the template.
   - **Grid Member**: Click **Select** and choose a grid member from the drop-down list.
   - **Failover Association**: Click **Select** and choose a failover association. Only failover associations that provide DHCP services in the network view of the DHCP range appear in the drop-down list.
   - **Microsoft DHCP Server**: Click **Select** and choose a Microsoft server from the drop-down list. The drop-down list displays only the servers that are associated with the network to which the DHCP range belongs.
5. Click **Next** to configure or override DHCP options as described in *About Configuring DHCP Services* on page 618.
6. Click **Next** to add or delete required and optional extensible attributes. You can add extensible attributes in the template and enter attribute values when you use the template to create a DHCP range. For information, see *Using Extensible Attributes* on page 225.
7. Select one of the following:
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and continue to edit.
   - **Save & New**: Save the entry and create a new template.

## Modifying DHCP Range Templates

To modify a DHCP range template:

1. From the **Data Management** tab, select the **DHCP** tab -> **Templates** tab -> **template** check box, and then click the **Edit** icon.

2. The **DHCP Range Template** editor contains the following tabs from which you can modify data:
   - **General**: Modify general information as described in *Adding DHCP Range Templates* on page 645.
   - **Member Assignment**: Change the grid member, failover association, or Microsoft server that provides DHCP services for this template. You can also add or delete a member or failover association. For information, see *Adding DHCP Range Templates* on page 645.
   - **DHCP**: Keep the inherited DHCP options or override them and enter unique settings for the template. For information, see *About Configuring DHCP Services* on page 618.
   - **Extensible Attributes**: Add and delete extensible attributes that are associated with this template. You can also modify the values of the extensible attributes. For information, see *Using Extensible Attributes* on page 225.
   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see *About Administrative Permissions* on page 87.

3. Optionally, you can click **Toggle Advanced Mode** to display the following tabs from which you can modify data:
   - **DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the template. For information, see *Configuring DHCP for DDNS* on page 505.
   - **BOOTP**: Keep the inherited BOOTP properties or override them and enter unique settings for the template. For information, see *Configuring BOOTP Properties* on page 625.
   - **Exclusion Ranges**: Configure a range of IP addresses that the appliance does not use for dynamic address assignments. You can use these exclusion addresses as static IP addresses. For information, see *Excluding Addresses from DHCP Ranges and Templates* on page 607.
   - **Thresholds**: Keep the inherited thresholds settings or override them and enter unique settings for the template. For information, see *Configuring Thresholds for DHCP Ranges* on page 634.
   - **Filters**: Add filters to the template. For information, see *Applying Filters to DHCP Address Ranges* on page 687.

   Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and continue to edit.

To delete a DHCP range template, see *Deleting Templates* on page 651.
About Fixed Address/Reservation Templates

A fixed address/reservation template has properties similar to a fixed address, a reservation, or a roaming host, except for the following:

- It is uniquely identified by a name.
- After you create a fixed address/reservation template, you can use the template to create fixed addresses, reservations, or roaming hosts.
- It can be defined to populate one or multiple fixed addresses, reservations, and roaming hosts. It can populate multiple objects only when it is assigned to a network template.
- It can populate multiple reservations only, not fixed addresses, if it is assigned to a network template.

Adding Fixed Address/Reservation Templates

To create a fixed address template:

1. From the Data Management tab, select the DHCP tab.
2. Expand the Toolbar and click Add -> Templates -> Fixed Address/Reservation.
3. In the Add Fixed Address/Reservation Template wizard, enter the following:
   - Name: Enter a name that helps identify the fixed address/reservation template. For example, you can enter HP Printer when you create a template that contains settings for assigning fixed addresses or reservations to HP printers.
   - Comment: Enter useful information about the template.
   - In the Optional Settings For Range of Objects section, do the following:
     - Offset: An offset in a fixed address/reservation template determines the start IP address of the object created from the template. The appliance adds the offset value you enter here to the start IP address of the network in which you create objects using this template. That IP address becomes the start IP address of the object.
     - Number of Addresses: Enter the number of IP addresses to be used as fixed addresses, reservations, or roaming hosts.

Note: The appliance uses the offset and number of addresses only when this template is used in a network template.

4. Click Next to configure or override DHCP options as described in Configuring General DHCP Properties on page 619.
5. Click Next to add or delete required and optional extensible attributes. You can add extensible attributes in the template and enter attribute values when you use the template to create a fixed address or reservation. For information, see Using Extensible Attributes on page 225.
6. Select one of the following:
   - Save & Close: Save the entry and close the wizard.
   - Save & Edit: Save the entry and continue to edit.
   - Save & New: Save the entry and create a new template.
Modifying Fixed Address/Reservation Templates

To modify a fixed address/reservation template:

1. From the Data Management tab, select the DHCP tab -> Templates tab -> template check box, and then click the Edit icon.

2. The Fixed Address/Reservation Template editor contains the following tabs from which you can modify data:
   - **General**: Modify general information for the template as described in Adding Fixed Address/Reservation Templates on page 647.
   - **DHCP**: Keep the inherited DHCP options or override them and enter unique settings for the template. For information, see About Configuring DHCP Services on page 618.
   - **Extensible Attributes**: Add and delete extensible attributes that are associated with the template. You can also modify the values of the extensible attributes. For information, see Using Extensible Attributes on page 225.
   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see About Administrative Permissions on page 87.

3. Optionally, you can click Toggle Advanced Mode to display the following tabs from which you can modify data:
   - **DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the template. For information, see Configuring DDNS Updates from DHCP on page 501.
   - **BOOTP**: Keep the inherited BOOTP properties or override them and enter unique settings for the template. For information, see Configuring BOOTP Properties on page 625.

   Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and continue to edit.

To delete a fixed address/reservation template, see Deleting Templates on page 651.
About Network Templates

A network template is similar to a real network, except for the following:

- It is uniquely identified by a name.
- It does not have a network view.
- It does not have a network container. Hierarchies such as network and subnets (split networks) do not apply to network templates.
- It does not have a network address. You enter the network address when you create an actual network from the template.
- It does not have a disabled status.
- You can add DHCP range or fixed address/reservation templates to a network template.

A network template is useful for setting up a network with fixed addresses and DHCP ranges selected from predefined information. Once the fixed address and DHCP range information is set up, the network template contains a range template list and a fixed address/reservation template list. You can select from an existing range or fixed address template and add it to the list.

Adding Network Templates

Once you create a network template, you can add a network using any existing network template (you define the IP address for the network, and the subnet mask information is inherited from the selected template).

To create a network template:
1. From the Data Management tab, select the DHCP tab.
2. Expand the Toolbar and click Add -> Templates -> Network.
3. In the Add Network Template wizard, do the following:
   - Name: Enter a name that helps identify the network template. For example, you can enter Class C if you want to configure the template for creating Class C networks.
   - Netmask: Select one of the following options:
     - Fixed: Select this and adjust the netmask slider to a fixed netmask for this network template. When you select this option, users cannot specify another netmask when they use this template to create a network. For example, if you select /24 as the fixed netmask, all networks created using this template have a /24 netmask.
     - Allow User to Specify Netmask: Select this to allow users to specify the subnet mask when creating networks using this template.
   - Comment: Enter useful information about the template.
   - Automatically create a reverse-mapping zone: This function is enabled if the fixed netmask of the template equals /8, /16, and /24, or if you select the Allow User to Specify Netmask option. Select this if you want the appliance to automatically create the corresponding reverse-mapping zone for the networks created using this template. A reverse-mapping zone is an area of network space for which one or more name servers have the responsibility for responding to address-to-name queries. These zones are created in the DNS view assigned to receive dynamic DNS updates at the network level.
Managing DHCP Templates

4. Click **Next** and do the following to assign either grid members or Microsoft DHCP servers to this network template. Ensure that you include members or Microsoft servers that are associated with other templates that you plan to add to this network template. You can assign one or multiple members to this template. However, you cannot assign a combination of NIOS grid members and vNIOS grid members to the template. You can also assign multiple Microsoft servers to a template, but you cannot assign a mix of Microsoft servers and grid members to a template.
   - Click the Add icon and select one of the following options:
     - **Add Infoblox Member**: Select this option to add a grid member as a DHCP server for the networks created using this template. Select the grid member from the **Member Selector** dialog box. Keep in mind, DHCP properties for the network are inherited from this member. Networks created using this template can be served by multiple members, but a member can serve networks in one network view only.
     - **Add Microsoft Server**: Select this option to add a Microsoft server as a DHCP server for the networks created using this template. Select the Microsoft server from the **Microsoft Server Selector** dialog box.

5. Click **Next** and do the following to include DHCP range and fixed address/reservation templates in the network template. Note that when you select a fixed address/reservation template, only reservations, not fixed addresses, are created for networks created using this template. You cannot add a fixed address/reservation template that does not contain an offset value or a total number of IP addresses for a range.
   - Click the Add icon.
   - In the **DHCP Template Selector** dialog box, choose the template that you want to include in this network template. You can choose a DHCP range or fixed address/reservation template. Use SHIFT+click and CTRL+click to select multiple templates.
   - Click the Select icon.
   - You can delete a template by selecting the template and clicking the Delete icon.

6. Click **Next** to configure or override DHCP options as described in *About Configuring DHCP Services* on page 618.

7. Click **Next** to add or delete required and optional extensible attributes. You can add extensible attributes in the template and enter attribute values when you use the template to create a network. For information, see *Using Extensible Attributes* on page 225.

8. Select one of the following:
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and continue to edit.
   - **Save & New**: Save the entry and create a new template.

### Modifying Network Templates

To modify a network template:

1. From the **Data Management** tab, select the **DHCP** tab -> **Templates** tab -> **template** check box, and then click the **Edit** icon.

2. The **Network Template** editor contains the following tabs from which you can modify data:
   - **General**: Modify general information as described in *Adding Network Templates* on page 649.
   - **Server Assignment**: Change the Microsoft servers or grid members that provide DHCP services for this template. For information, see *Adding Network Templates* on page 649.
   - **Templates**: Add or delete DHCP range and fixed address/reservation templates. For information, see *Adding Network Templates* on page 649.
   - **DHCP**: Keep the inherited DHCP options or override them and enter unique settings for the template. For information, see *About Configuring DHCP Services* on page 618.
   - **Extensible Attributes**: Add and delete extensible attributes that are associated with the template. You can also modify the values of the extensible attributes. For information, see *Using Extensible Attributes* on page 225.
— **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see *Managing Permissions* on page 93.

3. Optionally, you can click **Toggle Advanced Mode** to display the following tabs from which you can modify data:
   — **DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the template. For information, see *Configuring DDNS Updates from DHCP* on page 501.
   — **BOOTP**: Keep the inherited BOOTP properties or override them and enter unique settings for the template. For information, see *Configuring BOOTP Properties* on page 625.
   — **Thresholds**: Keep the inherited thresholds settings or override them and enter unique settings for the template. For information, see *Configuring Thresholds for DHCP Ranges* on page 634.

   Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Select one of the following:
   — **Save & Close**: Save the entry and close the editor.
   — **Save**: Save the entry and continue to edit.

---

**VIEWING TEMPLATES**

To view a list of available templates:

1. From the Data Management tab, select the DHCP tab -> Templates tab.
2. Grid Manager displays the following information:
   — **Name**: The name of the template.
   — **Type**: The template type, such as Network or Range.
   — **Comment**: The information you entered about the template.
   — **Site**: The site to which the template belongs. This is one of the predefined extensible attributes.

You can select predefined and user defined extensible attributes for display.

You can also do the following in this panel:
- Sort the displayed data in ascending or descending order by column.
- Delete a selected template or multiple templates. For information, see *Deleting Templates* on page 651.
- Use the filter or Go to function to search for specific templates.
- Select an object and edit its information.
- Print or export the data in the panel.

---

**DELETING TEMPLATES**

To delete a template:

1. From the Data Management tab, select the DHCP tab -> Templates tab -> template check box, and then click the Delete icon.
2. In the *Delete Confirmation* dialog box, click **Yes**.
**Configuration Example: Creating a Network Using a Template**

This example describes how to create a /24 network template and how to use the template to create a 192.168.2/24 network with the following configurations:

- First address 192.168.2.1 is reserved for the router
- Next 10 addresses (192.168.2.2 to 192.168.2.11) reserved for servers
- Next 10 addresses (192.168.2.12 to 192.168.2.21) reserved for printers
- Next 10 addresses (192.168.2.22 to 192.168.2.31) assigned as fixed addresses
- 100 addresses (192.168.2.32 to 192.168.2.131) reserved for workstations. The appliance assigns these dynamically.
- 10 addresses (192.168.2.42 to 192.168.2.51) are in an exclusion range. If you assigned static addresses to certain hosts in the middle of an address range template, you can exclude the addresses from the address range template so the appliance does not assign these IP addresses to clients.

*Figure 24.1* illustrates the configurations of the 192.168.2/24 network using the network template you create:

*Figure 24.1 Creating a Network Using a Template*

Use the following steps to create the sample network template (shown in *Figure 24.1*).

1. Create the following DHCP range templates. For information, see *Adding DHCP Range Templates* on page 645.
   - Server template with the following values:
     - **Name:** Servers
     - **Offset:** 2
     - **Number of Addresses:** 10
     - **Comment:** Address range 2 to 11 for Servers
   - Printer template with the following values:
     - **Name:** Printers
     - **Offset:** 12
     - **Number of Addresses:** 10
     - **Comment:** Address range 12 to 21 for printers.
Configuration Example: Creating a Network Using a Template

— Workstation template with the following values:
  — Name: Workstations
  — Offset: 32
  — Number of Addresses: 100
  — Comment: Address range 32 to 131 for DHCP on workstations
— Exclusion range with the following values. You must modify the Workstations template to add the exclusion range. For information, see Modifying DHCP Range Templates on page 646.
  — Name: Exclusion
  — Offset: 42
  — Number of Addresses: 10
  — Comment: Excluding addresses 42 to 51 from the DHCP range 32 to 131.

2. Create a fixed address/reservation template with the following values. For information, see Adding Fixed Address/Reservation Templates on page 647.
   — Name: Router
   — Comment: Fixed address template
   — Offset: 1
   — Number of Addresses: 1

3. Create a fixed address/reservation template with the following values. For information, see Adding Fixed Address/Reservation Templates on page 647.
   — Name: myFixedAddress
   — Comment: Fixed address template
   — Offset: 22
   — Number of Addresses: 10

4. Create a network template with the following values. For information, see Adding Network Templates on page 649.
   — Name: myNetworkTemplate
   — Netmask: Select /24 as the fixed subnet mask for the network
   — Comment: Network template for /24 network
   — Automatically create a reverse-mapping zone: Select this so that the NIOS appliance automatically creates the corresponding reverse-mapping zone for the network.

5. Add the DHCP range templates Servers, Printers, and Workstations to the network template.

6. Add the fixed address/reservation template myFixedAddress to the network template.

7. Add a fixed address with the following values:

8. Create a network using the network template myNetworkTemplate with the following values. For information, see Adding IPv4 Networks on page 594.
   — Address: Enter the IP address 192.168.2.0 of the network that you want to create using the template.
   — Select template: Select the network template myNetworkTemplate.

9. To verify your configuration, from the Data Management tab, select the DHCP tab -> Templates tab. Select myNetworkTemplate and click the Edit icon. In the Network Template editor, click the Templates tab. The Grid Manager displays the DHCP range templates and fixed address templates.

10. Click Restart to restart services.
Chapter 25  DHCP Failover

This chapter explains how to configure DHCP failover associations. It contains the following sections:

- **About DHCP Failover** on page 656
  - Failover Association Operations on page 656
- **Configuring Failover Associations** on page 657
  - Adding Failover Associations on page 658
- **Managing Failover Associations** on page 659
  - Modifying Failover Associations on page 659
  - Monitoring Failover Associations on page 660
  - Deleting Failover Associations on page 661
  - Setting a Peer in the Partner-Down State on page 661
  - Performing a Force Recovery on page 661
About DHCP Failover

You can create a failover association between two DHCP servers (a primary server and a secondary). When you set up a failover association, you greatly reduce DHCP service downtime if one of your DHCP servers is out of service. You can better manage IP address requests by making two servers available for DHCP services. You can also configure one of the servers to assume full DHCP services when you know the other server may go out of service for a period of time.

You can configure two NIOS appliances, or one appliance and one external server, to form a failover association. The pairing of a primary and secondary server is called a peer association. The failover peers establish a TCP connection for their communication. They share a pool of IP addresses that they allocate to hosts on their networks based on load balancing. Load balancing is a technique to split the address allocation workload evenly across the two DHCP servers. You can assign a DHCP failover association to serve DHCP ranges in a network. A DHCP failover association can serve DHCP ranges that belong to one network view only. It cannot serve ranges in different network views.

Failover Association Operations

When a host broadcasts a DHCPDISCOVER message, it includes its MAC address. Both the primary and secondary peers receive this message. To determine which server should allocate an IP address to the host, they each extract the MAC address from the DHCPDISCOVER message and perform a hash operation. Each server then compares the result of its hash operation with the configured load balancing split. The split is set to 50% by default to ensure an even split between the two servers. When the split is 50%, the primary server allocates the IP address if the hash result is between 1 and 127, and the secondary server allocates the IP address if the hash result is between 128 and 255. As a server allocates an IP address, it updates its peer so their databases remain synchronized.

As shown in Figure 25.1, when a host broadcasts a DHCPDISCOVER message, both the primary and secondary servers receive the message. They perform a hash operation on the MAC address in the DHCPDISCOVER message, and the result is 250. Since the load balancing split is 50% and the hash result is 250, the secondary server responds to the host with a DHCPOFFER message. The secondary server allocates an IP address from its assigned pool of IP addresses. It then sends a lease update message to the primary server so that the primary server knows how the address is assigned and can properly take over if the secondary server fails.

Figure 25.1 Load Balancing and IP Addresses Allocation
## Configuring Failover Associations

The following are tasks and guidelines for configuring a DHCP failover:

1. Identify the primary and secondary DHCP servers and ensure that the appliances are set up correctly for the failover association, using the following guidelines:
   - Configure a failover association using two NIOS appliances, or a NIOS appliance and an ISC DHCP compliant server.
   - One of the DHCP servers must be an independent appliance or in an Infoblox grid.
   - The DHCP servers do not have to be in the same geographic location.
   - The clocks on both servers must be synchronized. This happens automatically when both servers are on the same grid.
   - Both servers must use the same version of the DHCP configuration file. This happens automatically when both servers are on the same grid.
   - If you use firewalls on your networks, ensure that the firewalls allow TCP port 519 between the servers, and that TCP port 7911 is open for partner down operations.
   - Each pair of DHCP servers can participate in only one failover association. An appliance can participate in more than one failover association, as long as it is with a different peer.
   - Configure the same DHCP properties on the primary and secondary servers, as described in Configuring General DHCP Properties on page 619.
     - Both the primary and secondary servers must have the same operational parameters, and they must be able to receive DHCPDISCOVER messages that hosts broadcast on the networks.
     - If you change any of the DHCP failover parameters for a peer association definition, you must make the same changes on both the primary and secondary servers.

   **Note:** If both the primary and secondary servers are in a grid, you configure the properties on the failover association and the configuration applies to both servers.

2. Create a failover association and configure load balancing between the servers. For information, see Adding Failover Associations on page 658.
   - Ensure that you use the same failover association name on both the primary and secondary servers.
   - The appliance assigns default values to the failover timers. In general, these default values serve the purpose of a failover. Do not change these values unless you understand the ramifications of the changes. For example, when one of the peers in a failover association fails, the other peer goes into a COMMUNICATIONS-INTERRUPTED state, and the lease time changes to the MCLT (Maximum Client Lead Time). You should consider how the MCLT affects the lease time when a failover occurs if you want to change this value.

3. Assign the failover association to the networks and DHCP ranges in the same network view. For information, see Configuring DHCP Address Ranges on page 604.
   - If you configure a shared network, and the subnets in the shared network contain ranges served by a DHCP failover association, both the primary and secondary DHCP server must have the same shared networks defined, containing the same networks and DHCP ranges.

   **Note:** If you have multiple networks that are in a shared network and you plan to use a DHCP failover, you must use the same failover association and specify the same peers on all the networks in the shared network.

4. Enable DHCP on the primary and secondary servers AFTER you complete all the configurations. For information, see Managing Failover Associations on page 659.

   **Note:** When you set up a failover association for the first time, ensure that both servers are up and running and their databases are synchronized before they can start assigning IP addresses.
When you configure a failover association, the appliance assigns default values for timers, such as the MCLT and the maximum number of "unacked" packets. A failover may occur when some of the timers expire or when a failover peer goes out of service. When a failover occurs, the functional peer takes over and assigns IP addresses with the lease time set to the MCLT. When the server that is offline comes back online, it synchronizes its database with its peer before it starts allocating IP addresses.

### Adding Failover Associations

To add a DHCP failover association, perform the following procedures on both the primary and secondary servers:

1. From the Data Management tab, select the DHCP tab.
2. Expand the Toolbar and click Add -> Failover Association.
3. In the Add Failover Association wizard, complete the following:
   - **Name**: Enter a unique name for the failover association. The failover association name is case sensitive. Enter the same name on both the primary and secondary servers. The appliance validates the names on both servers. The names must be exactly the same. If they do not match, the failover association goes into disconnect mode.
   - **DHCP Failover Primary**: Select one of the following. The default is Grid Member.
     - **Grid Member**: Click Select member. In the Select Member dialog box, select the primary server and click the Select icon.
     - **External Server IP Address**: Select this to use an external ISC DHCP compliant server as the primary server. Enter the IP address of the primary server in the field.
   - **DHCP Failover Secondary**: Select one of the following. The default is Grid Member.
     - **Grid Member**: Click Select member. In the Select Member dialog box, select the secondary server and click the Select icon.
     - **External Server IP Address**: Select this to use an external ISC DHCP compliant server as the secondary server. Enter the IP address of the secondary server in the field.

   **Note**: You cannot select External Server IP Address for both the primary and secondary servers. One of the servers must be an independent appliance or in an Infoblox grid.

   - **Comment**: Enter useful information about the failover association.

4. Click Next and do the following to control the IP address allocation between the peers and how they switch from one to the other based on the configuration:
   - **Load Balancing Data**: Adjust the slider to determine which server should handle more IP address requests. The default is 50%. When you adjust the slider, a tooltip window displays the percentage of available IP addresses that each server can allocate. When you move the slider all the way to the left, the primary server serves zero IP address request, and the secondary server responds to all. Infoblox recommends that you use the default (50/50) to enable the primary and secondary servers to respond to IP address requests on an equal basis.
   - **Lease Deletion**: Select the following to override settings at the grid and member levels.
     - **Keep leases from deleted ranges until one week after expiration**: When you select this and delete a DHCP range with active leases, the appliance stores these leases up to one week after they expire. When you add a new DHCP range that includes the IP addresses of these active leases, the appliance automatically restores the leases.

5. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes on page 225.

6. Select one of the following:
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and continue to edit.
   - **Save & New**: Save the entry and open a new wizard.
MANAGING FAILOVER ASSOCIATIONS

After you establish a failover association, you can monitor its status periodically to ensure that it is functioning properly. You can also delete a failover association when it is not assigned to any DHCP range.

See the following sections on how to manage failover associations:

- **Modifying Failover Associations**
- **Monitoring Failover Associations** on page 660
- **Deleting Failover Associations** on page 661

Under special circumstances, you can manually adjust the configuration of a failover association. For example, when you know in advance that a peer will be out of service for an extended period of time, you can manually set the functional peer in a PARTNER-DOWN mode. This allows the functional partner to assume all leases and be able to allocate addresses to client requests in full capacity. In addition, when you suspect the databases in a failover association are not synchronized, you can consider doing a force recovery (after you consult with Infoblox Technical Support or your Infoblox representative) so the secondary server can completely rebuild its lease table with updates from the primary server.

See the following sections on how to set a peer to the partner-down mode and perform a force recovery:

- **Setting a Peer in the Partner-Down State** on page 661
- **Performing a Force Recovery** on page 661

Modifying Failover Associations

To modify a failover association:

1. From the Data Management tab, select the DHCP tab -> Members tab -> Failover Associations -> failover_association check box, and then click the Edit icon.

2. The DHCP Failover Association editor contains the following tabs from which you can modify data:

   - **General**: In the Basic tab, modify the fields as described in Adding Failover Associations on page 658. In the Advanced tab, complete the following to modify the port number you use for the failover association:
     - **Failover Port**: Click Override to enter a port number for the failover association. You can use any available port from 1 to 63999. The default is 647 for a new installation and 519 for an upgrade.
     - **Triggers**: Before editing the triggers and timers, ensure that you understand the ramifications of the changes. Improper configuration of the triggers can cause the failover association to fail. For information about the fields, see Adding Failover Associations on page 658. The following are the advanced triggers:

       - **Max Response Delay Before Failover(s)**: Specifies how much time (in seconds) can transpire before a failover occurs when a failover peer does not receive any communication from its peer. This number should be small enough that the transient network failure does not leave the servers out of communication for a long time, but big enough that the servers are not constantly connecting and disconnecting. The default is 60 seconds.

       - **Max Number of Unacked Updates**: Specifies the number of “unacked” packets the server can send before a failover occurs. The default is 10 messages.

       - **Max Client Lead Time(s)**: Specifies the length of time that a failover peer can renew a lease without contacting its peer. The larger the number, the longer it takes for the peer to recover IP addresses after moving to the PARTNER-DOWN state. The smaller the number, the more load your servers experience when they are not communicating. The default is 3600 seconds.

       - **Max Load Balancing Delay(s)**: Specifies the cutoff after load balancing is disabled. The cutoff is based on the number of seconds since a client sent its first DHCPDISCOVER message. For instance, if one of the failover peers gets into a state where it is busy responding to failover messages but is not responding to other client requests, the other peer responds to the client requests when the clients retry. This does not cause a failover. The default is three seconds.
— **Extensible Attributes**: Add and delete extensible attributes that are associated with a failover association. You can also modify the values of extensible attributes. For information, see *Using Extensible Attributes* on page 225.

**Monitoring Failover Associations**

After you configure a failover association, the peers establish a TCP connection for communication. In a normal operational state, they send keepalive messages and database updates every time they grant a lease. However, there are times when the failover association experiences problems and goes into a state other than NORMAL. You can monitor the overall state of a failover association and the individual status of the peers to verify that the servers are operating and communicating properly.

To monitor the failover association status:

1. From the **Data Management** tab, select the **DHCP** tab → **Members** tab → **Failover Associations**. Grid Manager displays the list of failover associations and their overall status.
2. To view detailed information about a failover association, select the failover_association check box, and then click the Show Status icon.
3. In the **Failover Association Status** dialog box, Grid Manager displays the overall status of the failover association and the status of both the primary and secondary servers.

The failover association can be in one of the following states:

— **OK** (green): The failover association is functioning properly.
— **DEGRADED** (yellow): The failover association is degraded when one of the peers is giving out limited addresses.
— **FAILURE** (red): The failover association is not functioning. The peers are not assigning IP addresses.

For each peer, Grid Manager displays the hostname or IP address, the status, and event date. The peer can be in one of the following states:

— **STARTUP**: The server is starting up.
— **NORMAL**: The server is in a normal operational state in which only one failover peer responds to a DHCP client.
— **COMMUNICATIONS-INTERRUPTED**: The servers are not communicating with each other. Both servers provide DHCP service to DHCP clients from which they receive DHCP requests.
— **PARTNER-DOWN**: The server assumes control of the DHCP service because its peer is out of service.
— **RECOVER**: The server is starting up and trying to get a complete update from its peer and discovers that its peer is in the PARTNER-DOWN state.
— **RECOVER-WAIT**: The server is waiting for its peer to start up in order to get a complete update.
— **RECOVER-DONE**: The server completed an update from its peer.
— **POTENTIAL-CONFLICT**: The peers are not synchronized due to an administrative error or an incorrect state transition. Check the failover configuration and correct the error.
— **CONFLICT-DONE**: This is a temporary state that the primary server enters after it received updates from the secondary server when it was in the POTENTIAL-CONFLICT state.
— **RESOLUTION-INTERRUPTED**: The server responds to DHCP clients in a limited way when it is in this state.
— **UNKNOWN**: The DHCP server is in an unknown state. The failover association is not functioning properly.
Deleting Failover Associations

You cannot delete a failover association if it is currently assigned to a DHCP range. If you want to delete a failover association, ensure that it is not assigned to any DHCP range.

To delete a failover association:

1. From the Data Management tab, select the DHCP tab -> Members tab -> Failover Associations -> failover_association check box, and then click the Delete icon.
2. In the Delete Confirmation dialog box, click Yes.
   The appliance puts the failover association in the recycle bin, if enabled.

Setting a Peer in the Partner-Down State

If one of the peers in a failover association is out of service for an extended period of time, you should consider putting the functional peer in the PARTNER-DOWN state. When you place the functional peer in the PARTNER-DOWN state, it assumes full DHCP services for the networks. Since the functional server may not receive all the updates from its peer, it extends all the leases up to the MCLT. Once the following conditions are met, the functional peer provides DHCP services autonomously:

- It has reclaimed all the leases that belonged to its peer.
- The MCLT has passed.

When the peer that is offline comes back online, it synchronizes with the functional peer and reestablishes the communication before it provides DHCP services to the clients.

**WARNING:** Before you put a peer in the partner-down state, ensure that the other peer is indeed out of service. If both the primary and secondary servers are operational when you place one of them in the partner-down mode, both servers may stop issuing leases for a minimum of time defined in the MCLT.

To set a peer in the PARTNER-DOWN state:

1. From the Data Management tab, select the DHCP tab -> Members tab -> Failover Associations -> failover_association check box.
2. Expand the Toolbar and click Set Partner Down.
3. In the Set Failover Association Partner Down dialog box, select one of the following:
   - Primary: Select this if the secondary server is out of service.
   - Secondary: Select this if the primary server is out of service.
4. Click OK.

Performing a Force Recovery

When the primary and secondary peers are not synchronized, you can perform a force recovery to set the primary server in the PARTNER-DOWN state while putting the secondary server in the RECOVER state. During a force recovery, all leases in the databases are resynchronized. When you perform a force recovery, the secondary server does not serve any DHCP leases for a minimum of the MCLT while it resynchronizes with the primary server. Before you perform a force recovery, consult with Infoblox Technical Support or your Infoblox representative to ensure that the force recovery is appropriate for the situation.

To perform a force recovery:

1. From the Data Management tab, select the DHCP tab -> Members tab -> Failover Associations -> failover_association check box.
2. Expand the Toolbar and click Force Recovery State.
3. In the Force Secondary Peer Recovery State dialog box, click OK.
   The appliance synchronizes the databases on the primary and secondary servers.
Chapter 26  Managing Leases

This chapter explains how to manage leases. It contains the following sections:

- About DHCP Leases on page 664
- Configuring the Lease Logging Member on page 665
- Configuring Fixed Address Leases For Display on page 667
- Viewing Current Leases on page 668
- Viewing Detailed Lease Information on page 669
- Viewing Lease History on page 670
- Viewing Lease Event Detailed Information on page 670
- Exporting Lease Records on page 671
- Clearing Leases on page 671
- Scavenging Leases on page 672
ABOUT DHCP LEASES

Historical DHCP lease records complement the real-time DHCP lease viewer by allowing the appliance to store and correlate DHCP lease information over the lifetime of a lease. You can see critical information such as when the appliance issued or freed an IP address, the MAC address and host name of the device that received the IP address, the grid member that supplied the lease, and the start and end dates of the lease.

You can view current leases and lease history in the Data Management -> DHCP -> Leases tab in Grid Manager. To view lease history, you must first enable lease logging at the grid level. For information, see Configuring DHCP Logging on page 637 and Configuring the Lease Logging Member. You can also export the DHCP lease history log in CSV format for archival and reporting purposes.

In the Leases tab, you can do the following:

- View current leases. For information, see Viewing Current Leases on page 668.
- View detailed information about a specific lease. For information, see Viewing Detailed Lease Information on page 669.
- View historical lease records. For information, Viewing Lease History on page 670.
- View detailed information about a lease event. For information, see Viewing Lease Event Detailed Information on page 670.
- Export current leases and lease history logs. For information, see Exporting Lease Records on page 671.
- Clear leases. For information, see Clearing Leases on page 671.

You can also use the filter and Go to functions in the lease panels to retrieve lease information for specific hosts, MAC addresses, and IP addresses. These capabilities are crucial for security auditing and for meeting new compliance regulations such as SOX and HIPAA. You can also sort the lease information by column.
Configuring the Lease Logging Member

Logging DHCP lease events makes significant CPU demands, especially when there is heavy DHCP activity. Therefore, Infoblox strongly recommends that you designate a grid member other than the master as a logging member whenever possible.

Another way to manage the increased load that logging introduces is to log selectively per grid member. For example, you might want to log DHCP leases for members serving critical parts of your network and not keep historical logs for members serving other parts.

By default, DHCP lease logging is disabled. You can enable and disable it at the grid and member levels, the member level setting overriding the grid setting. For information, see Configuring DHCP Logging on page 637.

Figure 26.1 DHCP Lease History Logging with Member Overrides

To specify lease logging for a member:

1. **Grid**: From the Data Management tab, select the DHCP tab, and then click Grid DHCP Configuration from the Toolbar.
   - **Member**: From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box, and then click the Edit icon.

2. In the **Logging** tab, complete the following:
   - **Lease Logging**: Select Enable Lease History (for grid) or Log Lease Events from DHCP Server (for member) to enable DHCP lease logging. To disable DHCP lease logging, clear the check box. You can set member overrides if you want to enable or disable lease logging per member.
   - **Send leases to**: For grid only. Click Select. In the Select Member dialog box, select the grid member on which you want to store the DHCP lease history log. Infoblox recommends that you dedicate a member other than the grid master as a logging member. If possible, use this member solely for storing the DHCP lease history log. If you do not select a member, no logging can occur.
3. Select one of the following:
   - **Save & Close**: Save the entry and close the wizard.
   - **Save**: Save the entry and continue editing.

**Note**: You cannot configure vNIOS grid members on Riverbed and Cisco as DHCP lease history logging members.
Configuring Fixed Address Leases For Display

You can configure the DHCP server to capture the hostname and lease time of a fixed address when you assign a fixed address to a client. The appliance displays the hostname, and the start and end time of each fixed address lease in the Current Leases panel in Grid Manager. You can configure this feature at the grid level only, and you cannot override the configuration at any DHCP object level.

To configure the fixed address lease feature:

1. **Grid**: From the Data Management tab, select the DHCP tab, and then select Grid DHCP Configuration from the Toolbar.

2. In the DHCP Properties editor, click Toggle Advanced Mode if the editor is in basic mode. When the additional tabs appear, click the General tab -> Advanced tab and complete the following:
   - **Fixed Address Lease**: Select Capture hostname and lease time when assigning Fixed Addresses. The appliance displays the host name, and the start and end time of each fixed address lease in the Current Leases panel. If there are multiple records (A, host, and lease) for the IP address, it also displays the information for the records.

For information about viewing current leases, see Viewing Current Leases on page 668.
**VIEWING CURRENT LEASES**

To view current leases:

1. From the Data Management tab, select the DHCP tab -> Leases tab -> Current Leases.
2. Grid Manager displays the following information:
   - **IP Address**: The IP address the appliance assigned to a DHCP client for this lease.
   - **Member/Server**: The grid member or Microsoft server that granted the lease.
   - **MAC address**: The MAC address of the DHCP client that receives this lease for an IP address.
   - **Host Name**: The host name that the DHCP client sent to the appliance using DHCP option 12.
   - **State**: The binding state of the current lease. The lease state can be one of the following:
     - **Free**: The lease is available for clients to use.
     - **Active**: The lease is currently in use by a DHCP client.
     - **Static**: The lease is a fixed address lease.
     - **Expired**: The lease was in use, but the DHCP client never renewed it, so it is no longer valid.
     - **Released**: The DHCP client returned the lease to the appliance.
     - **Abandoned**: The appliance cannot lease this IP address because the appliance received a response when pinging the address.
   - **End**: The day, date, and time when the lease ends.
   - **Start**: The day, date, and time when the lease starts.
   - **Username**: Displays the name of the user who receives the lease for the IP address. The username enables you to differentiate between guest users and authenticated users. If you log in as an authenticated user, your username is whatever you choose when you log in. If you log in as a guest, your username is First: first_name Last: last_name. For example, if your first name is John and last name is Doe and your username is jdoe, when you log in as an authenticated user, your username is jdoe. If you log in as a guest user, your username is First: John, Last: Doe.
   - **ClientID**: The DHCP client identifier (option 61) in the lease. The client sends the client identifier as option 61 in the DHCP DISCOVER and REQUEST packets, as described in RFC2132, DHCP Options and BOOTP Vendor Extensions. The client identifier is either the MAC address of the network interface card requesting the address or any string uniquely identifying the client. This field is not displayed by default.

**Note**: The dates and timestamps in the Leases tab are determined by the time zone setting of the admin account that you use to log in to the appliance.

You can do the following in this section:

- View detailed information about a current lease by selecting the check box of the lease, and then clicking the Open icon.
- Select discovered data for display by clicking **Columns -> Edit Columns** from any header. For information, see *Viewing Discovered Data* on page 819.
- Change a current lease state to **Free** by selecting the check box of a current lease, and then clicking the Delete icon.
- Print or export the information in this section.
VIEWING DETAILED LEASE INFORMATION

You can view detailed information about a specific lease.

To view detailed information of a specific lease:

1. From the Data Management tab, select DHCP tab -> Leases -> Current Leases -> lease check box, and then click the Lease Details icon.

   or

   From the Data Management tab, select the IPAM tab, drill down to the IP Map, IP List, or IP address panel, and then click Lease Details from the Toolbar.

2. In the Lease Detailed Information viewer, Grid Manager displays the fields Member, MAC address, Host, Start, End, Binding State, Username, Billing Class, as described in Viewing Current Leases on page 668, plus the following information:
   - **Lease Issue:** The date and time when the lease was issued. Displayed in the lease event details report only.
   - **Event:** The action taken. This can be one of the following: Issued, Renewed, Freed, or Abandoned. Displayed in the lease event details report only.
   - **Served by:** The member that provides DHCP services to the lease.
   - **Next Binding State:** The subsequent binding state when the current lease expires. The lease state and the next binding state can be one of the following:
     - **Free:** The lease is available for clients to use.
     - **Active:** The lease is currently in use by a DHCP client.
     - **Static:** The lease is a fixed address lease.
     - **Expired:** The lease was in use, but the DHCP client never renewed it, so it is no longer valid.
     - **Released:** The DHCP client returned the lease to the appliance.
     - **Abandoned:** The appliance cannot lease this IP address because the appliance received a response when pinging the address.
   - **Billing Class:** The billing class of the lease.
   - **Option 82 Agent ID:** The agent ID of the relay agent filter (option 82). A relay agent can append DHCP option 82, relay agent information, to a message that it forwards from a DHCP client to a DHCP server.
   - **Option 82 Circuit ID:** The circuit ID of the relay agent filter (option 82).
   - **Option 82 Remote ID:** The remote ID of the relay agent filter (option 82).
   - **Option:** Agent circuit ID and remote ID data sent by a DHCP relay agent in all DHCP options.
   - **UID:** (User ID) The client identifier that the DHCP client sends the appliance (in DHCP option 61) when it acquires the lease. Not all DHCP clients send a UID.
   - **TSFT:** (Time Sent From Partner) The time—from the point of view of a remote DHCP failover peer—when the current lease state ends.
   - **CLTT:** (Client Last Transaction Time) The time of the last transaction with the DHCP client for this lease.
   - **TSTP:** (Time Sent To Partner) The time—from the point of view of the local DHCP failover peer—that the current lease state ends.
**Viewing Lease History**

To view historical lease records:

1. From the Data Management tab, select the DHCP tab → Leases tab → Lease History.
2. Grid Manager displays a table of historical leases that have been archived in the system. You can export the information in the lease history table. You can also search by the IP address or MAC address of the lease. Grid Manager displays the following read-only information:
   - **Lease Issue**: The date and time when the lease was issued.
   - **IP Address**: The IP address of the lease.
   - **MAC**: The MAC address of the lease.
   - **Name**: The host name that the DHCP client sent to the appliance using DHCP option 12.
   - **Action**: This can be one of the following: Issued, Renewed, Freed, or Abandoned.
   - **User Name**: The name of the user who received the lease for the IP address.
   - **Start**: The start date of the lease.
   - **Stop**: The end date of the lease.
   - **Member/Server**: The DHCP member or Microsoft server that granted the lease.

You can do the following in this section:

- View the lease event detailed information of a historical lease by selecting the check box of a lease, and then clicking the Open icon.
- Print or export the information in this section.

**Viewing Lease Event Detailed Information**

You can view detailed information about a historical lease record by clicking the lease in the Data Management tab → DHCP tab → Leases tab → Lease History. Grid Manager displays the event, the date and time when the event occurred, plus detailed information about the historical lease record. For information about the fields, see Viewing Detailed Lease Information on page 669.

You can also export and print the information in this panel. For information, see Exporting Lease Records on page 671.
**EXPORTING LEASE RECORDS**

The DHCP lease history log holds a maximum of 100,000 entries. After that maximum is reached, the appliance begins deleting entries, starting with the oldest. To archive DHCP lease history logs, you can export them and save them as CSV (comma separated variables) files. You do not need to export the entire log. You can selectively export a section of the log, such as the lease events for a single day.

As a conservative approach to archiving DHCP lease data, Infoblox recommends exporting the log on a daily basis, perhaps through API (application programming interface) scripting. By exporting the daily log entries every day over a certain period of time and then opening the exported files with a spreadsheet program, you can see the number of entries for each day. You can then estimate how often you need to export the log to ensure that you save all of the entries before the log fills up (at 100,000 entries). As a result, you might discover that you need to export the log more or less frequently than once a day to archive all the records.

A limited-access admin group can view and export the DHCP lease history if it has read-only permission to the DHCP lease history. For information on setting permissions for the DHCP lease history, see Administrative Permissions for the DHCP Lease History on page 104.

To export DHCP current leases or a lease history log:
1. From the Data Management tab, select the DHCP tab → Leases tab → Current Leases or Lease History.
2. Click the Export icon.
3. In the Export dialog box, click Start.
4. Click Download when the export is complete. Ensure that you turn off the pop-up blocker in your browser.
5. In the File Download dialog box, select the appropriate action to either open or save the CSV file.

**CLEARING LEASES**

To clear a lease, you must have read/write permissions to the leases you want to clear. You can only clear leases that have the status of “Active” and “Backup”. You cannot clear leases that have other status.

To clear a lease:
1. From the Data Management tab, select the DHCP tab → Leases tab → Current Leases or Lease History → lease.
2. Expand the Toolbar and select Clear Lease. Grid Manager clears the selected leases.
**Scavenging Leases**

You can enable member DHCP servers to automatically delete free and backup leases that remain in the database beyond a specified period of time. When you enable this feature, the appliance permanently deletes the free and backup leases, and you can no longer view or retrieve the lease information.

Note that the period of time that you specify is the number of days or weeks after the expiration date of a lease, not its release date. For example, you specify a time period of 5 days when you enable this feature. If the lease time of an IP address is ten days, but the lease is released after only five days, the appliance still deletes the lease from the database after 15 days.

You can enable this option globally at the grid level, and more specifically for a member, shared network, network or DHCP range. You can also enable this option for a network template or DHCP range template.

| Note: | If you plan to enable this feature after upgrading from a previous NIOS version, Infoblox recommends that you enable it during off-peak hours, as it may impact DHCP services. |

To enable the option to automatically delete free and backup leases:

1. **Grid**: From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar.
   
   **Member**: From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box, and then click the Edit icon.
   
   **Network**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon.
   
   **Shared Network**: From the Data Management tab, select the DHCP tab -> Networks tab -> Shared Networks -> shared_network check box, and then click the Edit icon.
   
   **DHCP Range**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range check box, and then click the Edit icon.
   
   **Range or Network Template**: From the Data Management tab, select the DHCP tab -> Templates tab -> template check box, and then click the Edit icon.

2. In the DHCP Properties editor, select the Advanced subtab of the DHCP or General tab, and then complete the following:
   
   **DHCP Lease Scavenging**: Select the Scavenge free/backup leases that persist longer than check box and specify the number of days or weeks that free and backup leases remain in the database before they are automatically deleted.

3. Save the configuration and click Restart if it displays at the top of the screen.
Chapter 27 Configuring DHCP Filters

This chapter explains how to configure DHCP filters. It contains the following sections:

- **About DHCP Filters** on page 674
  - IP Address Allocation on page 674
  - IP Address Allocation Using Filters on page 677
- **About MAC Address Filters** on page 680
  - Defining MAC Address Filters on page 680
  - Adding MAC Address Filter Items on page 681
- **About Relay Agent Filters** on page 682
  - Defining Relay Agent Filters on page 683
- **About Option Filters** on page 684
  - Defining Option Filters on page 684
  - Adding Match Rules on page 685
  - Configuring User Class Filters on page 686
- **Applying Filters to DHCP Address Ranges** on page 687
- **Managing DHCP Filters** on page 688
  - Modifying DHCP Filters on page 688
  - Viewing DHCP Filters on page 689
  - Deleting Filters on page 690
- **Configuration Example: Using Option Filters** on page 691
Configuring DHCP Filters

**About DHCP Filters**

You can use DHCP filters to control how the appliance allocates IP addresses. DHCP filters screen requesting hosts by matching MAC addresses, relay agent identifiers, or DHCP options. If you configure DHCP servers in the grid to send authentication requests to a RADIUS authentication server group, you can also filter requests by matching the authentication results. (For information about this feature, see Chapter 28, Authenticated DHCP, on page 693.)

When you define DHCP filters, you classify DHCP clients based on the information provided by the clients or by the RADIUS server. When you apply the filters to DHCP ranges, the appliance either grants or denies address requests based on your configuration. For example, you can use DHCP filters to screen unmanaged hosts on a network by denying their address requests. If you have multiple DHCP address ranges on the same network and you want to assign IP addresses from specific address ranges to specific hosts, you can use filters to screen the address assignments. For information, see IP Address Allocation.

The appliance supports the following filters:

- **MAC address filters** that use MAC addresses as matching criteria for granting or denying address requests. For information, see About MAC Address Filters on page 680.
- **Relay agent filters** that identify remote hosts by matching the relay agent identifiers in the DHCPDISCOVER messages. For information, see About Relay Agent Filters on page 682.
- **Option filters** that classify hosts by matching the DHCP options and values sent by the requesting hosts. For information, see About Option Filters on page 684.
- **NAC filters** that use authentication results from a RADIUS authentication server group as matching criteria for granting or denying address requests. For information, see Chapter 28, Authenticated DHCP, on page 693.

Unlike MAC address and relay agent filters, you can use option filters to define DHCP options clients can receive. Note that all DHCP clients with matching criteria receive the DHCP options defined in an option filter, regardless of the networks in which the DHCP clients reside and whether the option filter is applied to a DHCP range or not. The DHCP options defined for the option filter supersede those defined at the member, network, and DHCP range levels. For information, see About Option Filters on page 684.

**IP Address Allocation**

When a DHCP client requests an IP address, the NIOS appliance draws an address from an address range associated with the network segment for that client. Because you define that range, you can thereby control the IP address (within the defined range) and the associated TCP/IP settings that the client receives.

In Figure 27.1, three hosts—each in a different subnet—request an IP address. Each one broadcasts a DHCPDISCOVER message, which includes its MAC address. When the router, which also functions as a DHCP relay agent, receives the message, it adds the IP address of the interface on which the message arrives and forwards the message to the DHCP server—or servers—previously configured on the router. When the NIOS appliance receives the message, it uses the ingress interface IP address of the router to determine the network segment to which the host belongs and associates the MAC address of the requesting host with an IP address from an address range for that network.
The NIOS appliance replies to DHCPREQUEST messages by sending DHCPOFFER messages through the relay agent to the requesting hosts, as shown in Figure 27.2 on page 676.
Configuring DHCP Filters

Figure 27.2 Requesting Addresses – DHCPOFFER Messages

The addressing scheme depicted in Figure 27.1 on page 675 and Figure 27.2 is fairly simple: each network has a single address range. Consequently, address assignments are fairly straightforward. However, if you have multiple address ranges in the same network and you want to assign addresses from specific address ranges to specific hosts, you must screen the address assignments through the use of filters. If you do not apply a filter, the NIOS appliance assigns addresses from the highest address range to the lowest range and within each range from the highest address to the lowest address. That is, the appliance chooses the range with the highest addresses first (that is, closest to 255) and begins assigning addresses exclusively from that range, starting with the highest address and finishing with the lowest (closest to 0). When all the addresses from that range are in use, it then begins assigning addresses from the next highest range, and so on, finishing with the range with the lowest addresses. This is shown in Figure 27.3 on page 677.

Note: After the DHCP server runs for a while, it assigns leases based on when it last used addresses, and not just on their positions in the range.
You can configure a NIOS appliance as a full-featured DHCP server that assigns IP addresses to DHCP clients and manages the information about DHCP client configuration parameters. The Infoblox DHCP server complies with a number of DHCP RFCs (see Appendix A Product Compliance). To set up the appliance as a DHCP server, you configure DHCP properties and enable DHCP services on the appliance. For information about the configuration process, see Configuring DHCP Overview on page 579 and DHCP Configuration Checklist on page 581.

**Note:** Limited-access admin groups can access certain DHCP resources only if their administrative permissions are defined. For information on setting permissions for admin groups, see Chapter 3, Managing Administrators.

### IP Address Allocation Using Filters

To control the assignment of addresses from specific address ranges to specific hosts, the NIOS appliance provides the following filters:

- A MAC address filter to which you add MAC addresses as filter criteria.
- A relay agent filter with configured circuit ID and remote ID as specified by the relay agent (DHCP option 82).
- An option filter in which you specify DHCP options and matching values.
- A NAC filter in which you specify authentication results from a RADIUS authentication server group as filter criteria. For information about NAC filters, see About NAC Filters on page 723.

When the appliance receives an address request, it checks if the request matches a filter. If it does not, the appliance assigns an address from the address range with the highest available IP address. If the request matches one or more filters for a range, the appliance applies the following rules:

- If there are grant address filters applied to that range, the request must match one of the filters or the appliance does not grant an address from that range.
- If there are deny address filters applied to that range, the request must not match any of the filters. If the request matches a deny filter, the appliance does not grant an address from that range.
- If an address range has a combination of grant and deny filters, the request must:
  - Match a grant filter
  - Not match a deny filter

---

**Figure 27.3 Multiple Address Ranges without Filters**

The NIOS appliance assigns addresses to both hosts from the same address range—first to Host A, and then to Host B.

1. Host A receives 10.1.1.200
2. Host B receives 10.1.1.199

If more hosts request addresses, the appliance continues to assign them from address range 2—next address being 10.1.1.198, then 10.1.1.197, and so on—until all the addresses in that range are in use.

Then the appliance starts assigning addresses from address range 1, starting at 10.1.1.80, and stopping at 10.1.1.20.

The NIOS appliance assigns addresses to both hosts from the same address range—first to Host A, and then to Host B.
Two rules govern the behavior of the appliance in relation to DHCP filters:

1. The appliance checks if any data in an address request (the MAC address of the client, and DHCP options 77 and 82) matches any filters applied to an address range.

2. The appliance checks for available addresses in the address ranges containing the highest addresses first. (“Highest” means closest to 255.255.255.255, and “lowest” means closest to 0.0.0.0.)

These two rules can work in coordination. For example, when the appliance receives an address request, it first checks if the request matches any filter. If it matches more than one filter assigned to different address ranges, the appliance first applies the filter that belongs to the range with the highest IP addresses. If that address does not grant an address lease (because the filter action is Deny or all address leases in that range are already in use), the appliance then applies the matching filter for the range with the next higher set of IP addresses. If the appliance still has not granted a lease from either of the address ranges whose filters match data in the request and there are unfiltered address ranges, the appliance attempts to assign an address from one of these ranges, again beginning with the range having the highest IP addresses. Figure 27.4 presents an example illustrating the sequence in which the appliance assigns addresses when a request matches a MAC address filter. For information about MAC address filters, see About MAC Address Filters on page 680.

Figure 27.4 DHCP Address Assignment with Multiple Filters
The following explains how the NIOS appliance applies filters to DHCP address requests:

<table>
<thead>
<tr>
<th>If</th>
<th>then</th>
</tr>
</thead>
<tbody>
<tr>
<td>the appliance receives a request that matches a filter for one</td>
<td>it applies the action specified in the filter for that address range. If it does not assign an address from that range (the action is <em>deny</em> or the action is <em>grant</em> but all addresses in that range are in use), the appliance then checks if it can assign an address from an unfiltered address range (if there are any), starting with the range with the highest addresses first, as shown in Figure 27.3 on page 677.</td>
</tr>
<tr>
<td>address range,</td>
<td></td>
</tr>
<tr>
<td>the same filter applies to multiple address ranges and the appliance</td>
<td>it checks the address range with the highest IP addresses matching</td>
</tr>
<tr>
<td>receives an address request matching that filter,</td>
<td>that filter. If the appliance does not assign an address from that range, it checks the filtered address range with the next highest IP addresses, and so on. If it still has not assigned an address, the appliance starts checking unfiltered address ranges (if there are any), again beginning with the range with the highest address first.</td>
</tr>
<tr>
<td>multiple filters for the same address range conflict with each</td>
<td>the filter denying the lease takes precedence. For example, if a</td>
</tr>
<tr>
<td>other (one filter grants a lease and another denies it) and a</td>
<td>requesting client matches both a MAC address filter (granting a lease) and a user class filter (denying a lease) for the same address range, the appliance denies the lease. When faced with a choice to either allow or deny a lease based on equal but contradictory filters, the appliance takes the more secure stance of denying it.</td>
</tr>
<tr>
<td>requesting client matches both filters,</td>
<td></td>
</tr>
</tbody>
</table>
Configuring DHCP Filters

**About MAC Address Filters**

The appliance can filter an address request by the MAC address of a requesting host. The filter instructs the appliance either to grant or deny the address request if the requesting host matches the filter.

You can configure a MAC address filter or specific MAC addresses within a filter to expire after a certain amount of time has passed. Filter expiration is useful in situations where you want to keep filters running against updated MAC addresses. The permission to use the MAC addresses assigned to an IP address may become invalid after a certain period of time. For example, you can use a MAC address filter to restrict the right to use MAC addresses assigned to IP addresses for visiting guests or temporary workers. You can avoid removing invalid addresses from address filters manually by configuring the appliance to expire filters or to expire specific addresses within filters.

To apply a MAC address filter to an address range:

1. Define a MAC address filter. For information, see **Defining MAC Address Filters**.
2. Add a MAC address to the filter. For information, see **Adding MAC Address Filter Items** on page 681.
3. Apply the filter to a DHCP address range, and specify that if the MAC address of a requesting host matches the filter definition, the appliance either grants or denies the address assignment. For information, see **Applying Filters to DHCP Address Ranges** on page 687.

**Defining MAC Address Filters**

To define a MAC address filter:

1. From the Data Management tab, select the DHCP tab.
2. Expand the Toolbar and click Add -> Filter.
3. In the Add Filter wizard, complete the following:
   - **Name**: Enter a meaningful name for the filter. For example, if you want to filter address requests by department, you can name one filter “Marketing”, another “Finance”, and so on.
   - **Comment**: Enter useful information about the filter.
   - **Filter Type**: Select MAC Address from the drop-down list.
4. Click Next and complete the following to configure the expiration setting:
   - **Default MAC Address Expiration**
     Select one of the following to configure the expiration setting for the filter:
     - **Never Expires**: Select this if you want the MAC address filter to never expire. This is selected by default.
     - **Automatically Expires in**: Select this if you want the filter to expire after a specific time frame. You can specify the time in seconds, minutes, hours, or days.
     The filter expiration time you configure here affects how long the DHCP server grants a lease to a client. It has an upper limit of 15 minutes on the lease time you configure for the grid. For example, if both the filter expiration time and the lease time are less than 15 minutes, the appliance uses the lease time. If both the filter expiration time and lease time are greater than 15 minutes, the appliance uses the filter expiration time. If the filter expiration time is less than 15 minutes and the lease time is greater than 15 minutes, the DHCP server grants a lease for 15 minutes. If the filter expiration time is greater than 15 minutes and the lease time is less than 15 minutes, the appliance uses the lease time.
     - **Select Enforce Expiration Times** to enable expiration.
5. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see **Using Extensible Attributes** on page 225.
6. Select one of the following:
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and continue to edit.
   - **Save & New**: Save the entry and open a new wizard.
Adding MAC Address Filter Items

To add a MAC address to a MAC address filter:

1. From the Data Management tab, select the DHCP tab.
2. Expand the Toolbar and click Add -> MAC Address Filter Item.
3. In the Add MAC Address Filter Item wizard, complete the following:
   - MAC Address Filter: Click Select Filter. In the DHCP Filter Selector dialog box, select the MAC address filter to which you want to add a MAC address, and then click the Select icon. If you are adding a MAC address to a filter that you have selected in the Filters panel, Grid Manager displays the selected filter in this field.
   - MAC Address: Enter the MAC address in one of the following formats: aa:bb:cc:dd:ee:ff, aa-bb-cc-dd-ee-ff, aabb.ccdd.eeff, aabbcc-ddeeff, and aabbccddeeff. The appliance displays the address in the AA:BB:CC:DD:EE:FF format. You can also enter a vendor prefix in the three hexadecimal format using the same separators supported in the MAC address format. For example, you can enter aa.bb.cc as the vendor prefix. The appliance displays AA:BB:CC.
   - Comment: Enter useful information about the filter item.
   - Expiration Time
     MAC addresses in a filter stay valid until you explicitly configure them to expire. You can enable expiration for specific MAC addresses in the filter. Select one of the following:
     - Never Expires: Select this if you want the MAC address to never expire. This is selected by default.
     - Expires on: Select this and specify the Date and Time for the expiration. The fields display the current date and time. If you have already configured an expiration time for the filter, the appliance displays the time here by adding the filter expiration time to the current time. For example, if the expiration time for the filter is two days and the current date is June 6, 2009, the appliance displays June 8, 2009 in the Date field.
4. Click Next and select one of the following to configure user registration (optional):
   - Register as User: Select this and enter a username in the field.
   - Register as Guest: Select this and enter the first name, middle name, last name, email address, and phone number of the guest user.

The appliance displays the information you enter here in the lease viewers.
5. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes on page 225.
6. Select one of the following:
   - Save & Close: Save the entry and close the wizard.
   - Save & Edit: Save the entry and continue to edit.
   - Save & New: Save the entry and open a new wizard.

After you define a MAC address filter and add MAC addresses to it, you can assign the filter to a DHCP range. The appliance filters IP address requests based on the filter criteria. For information, see Applying Filters to DHCP Address Ranges on page 687.
**About Relay Agent Filters**

The NIOS appliance can filter an address request by the circuit ID and remote ID of a requesting host. The filter instructs the appliance either to grant or deny an address request if the requesting host matches the filter. For information about the DHCP relay agent option, see *About the DHCP Relay Agent Option (Option 82)* on page 633. Option 82 assists the agent in forwarding address assignments across the proper circuit. When a relay agent receives a DHCPDISCOVER message, it can add one or two agent IDs (circuit ID and remote ID) in the DHCP option 82 suboption fields to the message, as illustrated in Figure 27.5. If the agent ID strings match those defined in a relay agent filter applied to a DHCP address range, the appliance either assigns addresses from that range or denies the request based on the configured parameters.

*Figure 27.5  Relay Agent Filtering*

To apply a relay agent filter to an address range:

1. Define a relay agent filter. For information, see *Defining Relay Agent Filters*.
2. Apply the filter to a DHCP address range, and specify that if the circuit ID or remote ID of a requesting host matches the filter definition, the appliance either grants or denies the address assignment. For information, see *Applying Filters to DHCP Address Ranges* on page 687.
3. Define the access privileges of limited-access admin group for relay agent filters. For information, see *Managing Administrators* on page 90.
Defining Relay Agent Filters

To define a relay agent filter:

1. From the **Data Management** tab, select the **DHCP** tab.
2. Expand the Toolbar and click **Add -> Filter**.
3. In the **Add Filter** wizard, complete the following:
   - **Name**: Enter a meaningful name for the filter. For example, you can enter the IP address or the name of the router acting as the relay agent.
   - **Comment**: Enter useful information about the filter.
   - **Filter Type**: Select **Relay Agent** from the drop-down list.
4. Click **Next** to define the relay agent ID type. If you apply both ID types, the relay agent must provide both identifiers when submitting a DHCP address request.
   - Select one of the following for both **Circuit ID** and **Remote ID**:
     - **Any**: Select this and the filter matches any of the circuit identifiers for remote hosts. You cannot select this for both circuit ID and remote ID at the same time.
     - **Not Set**: Select this and no circuit identifier is set for remote hosts.
     - **Matches Values**: Select this and enter the circuit ID or remote ID. You can enter the ID in hexadecimal format, such as ex:aa, ab, 1f:cd, or ef:23:56, or in string format, such as abcd or aa:gg. The appliance matches the value you enter here with the value sent by the DHCP client in counted octet sequence format.
5. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see **Using Extensible Attributes** on page 225.
6. Select one of the following:
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and continue to edit.
   - **Save & New**: Save the entry and open a new wizard.

After you define a relay agent filter, you can assign it to a DHCP range. The appliance responds to address requests based on the filter criteria. For information, see **Applying Filters to DHCP Address Ranges** on page 687.
### About Option Filters

You can use option filters to classify DHCP clients and decide which DHCP options each group of clients can receive. Note that regardless of the networks in which the DHCP clients reside and whether an option filter is applied to a DHCP range or not, all DHCP clients that match the filter criteria receive the DHCP options and values you define in the filter. The DHCP options defined for the option filter supersede those defined at the member, network, and DHCP range levels. When you define additional DHCP options in an option filter, the appliance appends them to the existing options and returns them to the clients that have matching filter criteria.

The NIOS appliance can filter an address request by the DHCP options (such as root-server-ip-address or user-class) of the requesting host. The filter instructs the appliance to either grant or deny an address request if the requesting host matches the filter.

To define an option filter and apply it to an address range:

1. Define an option filter based on either the predefined or custom DHCP options. For information, see Defining Option Filters.
2. Add match rules to the filter. For information, see Adding Match Rules on page 685.
3. Apply the filter to a DHCP address range, and specify that if the DHCP options of a requesting host match the filter definition, the appliance either grants or denies the address assignment. For information, see Applying Filters to DHCP AddressRanges on page 687.

After you define an option space and add options to it, you can set up option filters and define option values. For example, to handle two different client classes such as SUNW.Ultra-5_10 and SUNW.i86pc, you can define two option filters (vendor-class_1 and vendor-class_2) and send different option values to different clients based on the vendor-class-identifier options that you obtain from the clients.

### Defining Option Filters

To define an option filter:

1. From the Data Management tab, select the DHCP tab.
2. Expand the Toolbar and click Add -> Filter.
3. In the Add Filter wizard, complete the following:
   - **Name**: Enter a meaningful name for the option filter. For example, you can enter Sun-Blade-1000 if you plan to use this option filter to screen Sun Blade 1000 systems.
   - **Comment**: Enter useful information about the filter.
   - **Filter Type**: Select Options from the drop-down list.
4. Click Next and complete the following:
   - **Option Space**: Select an option space from the drop-down list. This field is not displayed if you do not have custom option spaces. The appliance uses the DHCP option space as the default.
   - **Lease Time**: Enter the value of the lease time in the field and select the time unit from the drop-down list. The lease time applies to hosts that meet the filter criteria.

### Options to Merge with Object Options

Click the Add icon. Grid Manager adds a new row to the table with the default DHCP option space and option name displayed. Complete the following:

- **Option Space**: Click the down arrow and select an option space from the drop-down list. The selected option space contains the corresponding DHCP options that you can use as filter criteria.
- **Option Name**: Click the down arrow and from the drop-down list, select the DHCP option you want to use as filter criteria.
- **Value**: Enter the match value that you want the filter to use for the selected DHCP option. For example, enter the value 172.124.3.0 for the SUNW.SrootIP4 option.

To add more options to the filter, click the Add icon and repeat the steps.
5. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see *Using Extensible Attributes* on page 225.

6. Select one of the following:
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and continue to edit.
   - **Save & New**: Save the entry and open a new wizard.

After you define an option filter, you can add match rules to it. The appliance responds to address requests based on the match rules in the filter. For information, see *Adding Match Rules* on page 685.

### Adding Match Rules

Each match rule in an option filter can filter a specific DHCP option. You can add multiple match rules to an option filter. When the DHCP server receives a client packet that contains the option and the matching option value, it either grants or denies the address request based on your configuration.

To add a match rule to an option filter:
1. From the **Data Management** tab, select the **DHCP** tab.
2. Expand the Toolbar and click **Add -> Match Rule**.
3. In the **Add Match Rule** wizard, complete the following:
   - **Match Rule Filter**: Click **Select Filter**. In the **DHCP Filter Selector** dialog box, select the option filter to which you want to apply a match rule, and then click the Select icon.
   - **Match Option**: Select a DHCP option from the drop-down list. For example, select user-class (77) for a specific user class, such as mobile users.
   - **Match Value**: Enter a value for the selected option.
   - **Value is a substring**: Select this if your match value is a substring of an option value. Complete the following:
     - **Substring Offset**: Enter the number of characters at which the match value substring starts in the option data. Enter 0 to start at the beginning of the option data, enter 1 for the second position, and so on. For example, when you enter 2 and have a match value of RAS, the appliance matches the value RAS starting at the third character of the option data.
     - **Substring length**: Enter the length of the match value. For example, if the match value is SUNW, the length is 4.
   - **Comment**: Enter useful information about the match rule.
4. Select one of the following:
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and continue to edit.
   - **Save & New**: Save the entry and open a new wizard.

**Note:** When the DHCP server receives a client packet that contains the option and the matching option value, it returns the DHCP options in the option filter to the client. Regardless of the networks in which the DHCP clients reside and whether the option filter is applied to a DHCP range or not, all DHCP clients that match the filter criteria receive the DHCP options and values you define in the filter.

In the following example, the **match if** statement is generated from the data in the match rule object. In the match statement:

- **Match option** is "vendor-class-identifier".
- **Match value** is "SUNW".
- **Substring offset** is "0" (the match value starts at the beginning of the option data received from the client).
Configuring DHCP Filters

The NIOS appliance can filter DHCP address requests by user class filters. A user class indicates a category of user, application, or device of which the DHCP client is a member. User class identifiers are configured on DHCP clients and are sent during a DHCP address request operation. The client includes the user class identifier in DHCP option 77 when sending DHCPDISCOVER and DHCPREQUEST messages.

By using user class identifiers, a DHCP server can screen address requests and assign addresses from select address ranges based on the different user class identifiers it receives. For example, if you assign a user class filter named mobile to a range of addresses from 10.1.1.31–10.1.1.80, the appliance selects an address from that range if it receives an address request that includes the user class name mobile and there are still addresses available in that range. You might want mobile users to receive these addresses because you have given them shorter lease times than other, more stationary DHCP clients. See Figure 27.6.

Figure 27.6 Applying User Class Filtering

The user class for laptop A is mobile. When it sends DHCPDISCOVER and DHCPREQUEST messages, it includes its user class in the DHCP option 77 field.

The NIOS appliance has a filter that screens address requests by user class. If the user class for a DHCP client is mobile, the appliance assigns it an address from address range 2.

Note: The leases for addresses in address range 2 are shorter than those for more stationary computers. The intended use for address range 2 is to provide IP addresses for mobile users who log in to the network for relatively short periods of time and, therefore, do not require longer leases.
If the NIOS appliance receives address requests with the user class mobile and there are no available addresses in address range 2 but there are available addresses in ranges 1 and 3, the appliance begins assigning addresses from address range 3 (because its addresses are higher than those in range 1). Then, if all addresses in range 3 are in use, the appliance begins assigning addresses from address range 1. If you want the appliance to assign addresses to mobile users (that is, those identified with the user class mobile) exclusively from address range 2, then you must apply user class filters for “mobile” to address ranges 1 and 3 that deny lease requests matching that user class.

### Applying Filters to DHCP Address Ranges

To apply a filter to a DHCP address range:

1. From the **Data Management** tab, select the **DHCP tab -> Networks tab -> Networks -> addr_range** check box, and then click the **Edit icon**.
2. In the **DHCP Range editor**, select the **Filters tab**, and then click the **Add icon**.
3. In the **DHCP Filter Selector dialog box**, select the filter to which you want to assign this DHCP range, and then click the **Select icon**. Use **SHIFT+click and CTRL+click** to select multiple filters.
4. For each filter, click the **Action** column and select one of the following from the drop-down list:
   - **Grant lease**:
     - For MAC address filters: Select this to assign an IP address from the address range to a requesting host whose MAC address matches the MAC address in the filter.
     - For relay agent filters: Select this to assign an IP address from the address range when one or both of the relay agent identifiers of the requesting host match the filter criteria.
     - For option filters: Select this to assign an IP address from the address range to a requesting host whose DHCP options match the DHCP options and match rules defined in the filter.
     - For NAC filters: Select this to assign an IP address from the address range to a requesting host based on the authentication results from a RADIUS authentication server group.
   - **Deny lease**:
     - For MAC address filters: Select this to deny an address request from a host whose MAC address matches an entry in the filter.
     - For relay agent filters: Select this to deny an address request when one or both relay agent identifiers match the filter criteria in the filter.
     - For option filters: Select this to deny an address request from a host whose DHCP options match the options and match rules in the filter.
     - For NAC filters: Select this to deny an address request from a host based on the authentication results from a RADIUS authentication server group.
     Select one of the following:
     - **Save & Close**: Save the entry and close the editor.
     - **Save**: Save the entry and continue to edit.
MANAGING DHCP FILTERS

You can do the following to manage DHCP filters:

- Modify filter settings. For information, see Modifying DHCP Filters.
- View a complete list of filters, MAC address items, and match rules. For information, see Viewing DHCP Filters on page 689.
- Delete filters that are not in use. For information, see Deleting Filters on page 690.

Modifying DHCP Filters

To modify a filter:
1. From the Data Management tab, select the DHCP tab -> Filters/Option Spaces tab -> Filters -> filter_name check box, and then click the Edit icon.
2. For a MAC address filter:
   - The DHCP MAC Filter editor contains the following tabs from which you can edit data:
     - General: Modify the fields as described in Defining MAC Address Filters on page 680.
     - Extensible Attributes: Add or delete extensible attributes that are associated with a specific DHCP range. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes on page 225.
     - Permissions: This tab appears only if you belong to a superuser admin group. For information, see About Administrative Permissions on page 87.

   For a relay agent filter:
   - The Relay Agent Filter editor contains the following tabs from which you can edit data:
     - General: Modify the fields as described in Defining Relay Agent Filters on page 683.
     - Extensible Attributes: Add and delete extensible attributes that are associated with a specific DHCP range. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes on page 225.

   For an option filter:
   - The Option Filter editor contains the following tabs from which you can edit data:
     - General: Modify the fields as described in Defining Option Filters on page 684.
     - DHCP: Modify option spaces and DHCP options in the Basic tab as described in Defining Option Filters on page 684. You must define the PXE Lease Time in the Advanced tab.
     - BOOTP: Modify BOOTP settings as described in Configuring BOOTP Properties on page 625.
     - Extensible Attributes: Add or delete extensible attributes that are associated with a specific DHCP range. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes on page 225.

   For a NAC filter:
   - The NAC Filter editor contains the following tabs from which you can edit data:
     - General: Modify the name and comment.
     - Rules: Modify the rules as described in Defining a NAC Filter on page 724.
     - Extensible Attributes: Add and delete extensible attributes that are associated with a specific DHCP range. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes on page 225.
Managing DHCP Filters

3. Select one of the following:
   — **Save & Close**: Save the entry and close the editor.
   — **Save**: Save the entry and continue to edit.

You can modify the MAC address filter items and match rules for corresponding MAC address filters and option filters. For information, see *Modifying MAC Address Filter Items* on page 689 and *Modifying Match Rules* on page 689.

### Modifying MAC Address Filter Items

To modify a MAC address filter item:

1. From the **Data Management** tab, select the **DHCP** tab -> **Filters/Option Spaces** tab -> **Filters** -> `filter_name` -> `mac_filter` check box, and then click the Edit icon.

2. The **MAC Address Filter Item** editor contains the following tabs from which you can edit data:
   — **General**: Modify the fields as described in *Adding MAC Address Filter Items* on page 681.
   — **Registration**: Modify registration settings as described in *Adding MAC Address Filter Items* on page 681.
   — **Extensible Attributes**: Add or delete extensible attributes that are associated with a specific DHCP range. You can also modify the values of extensible attributes. For information, see *Using Extensible Attributes* on page 225.

3. Select one of the following:
   — **Save & Close**: Save the entry and close the editor.
   — **Save**: Save the entry and continue to edit.

### Modifying Match Rules

To modify a match rule:

1. From the **Data Management** tab, select the **DHCP** tab -> **Filters/Option Spaces** tab -> **Filters** -> `filter_name` -> `match_rule` check box, and then click the Edit icon.

2. The **Match Rule** editor contains the following tab from which you can edit data:
   — **General**: Modify the fields as described in *Adding Match Rules* on page 685.

3. Select one of the following:
   — **Save & Close**: Save the entry and close the editor.
   — **Save**: Save the entry and continue to edit.

### Viewing DHCP Filters

To view DHCP filters:

1. From the **Data Management** tab, select the **DHCP** tab -> **Filters/Option Spaces** tab -> **Filters**.

2. Grid Manager displays the following for each filter:
   — **Name**: The name of the filter.
   — **Filter Type**: The filter type.
   — **Comment**: The information about the filter.
   — **Site**: The location to which the filter belongs. This is one of the predefined extensible attributes.
Viewing MAC Address Filter Items

To view a list of MAC addresses in a specific MAC address filter:

1. From the Data Management tab, select the DHCP tab -> Filters/Option Spaces tab -> Filters -> filter_name.
2. Grid Manager displays the following:
   - MAC Address: The MAC address assigned to the filter.
   - Username: Grid Manager displays the username to which the MAC address belongs in the lease viewers.
   - Comment: The information you entered about the filter item.
   - Expiration Time: The expiration time you configured for the MAC address.
   - Site: The location to which the filter belongs. This is one of the predefined extensible attributes.

Viewing Match Rules

To view match rules:

1. From the Data Management tab, select the DHCP tab -> Filters/Option Spaces tab -> Filters -> filter_name.
2. Grid Manager displays the following:
   - Match Option: The DHCP option you selected for the match rule.
   - Match Value: The value you entered for the matching option.
   - Comment: The information you entered about the match rule.

Deleting Filters

You can delete a filter that is not currently assigned to a DHCP range. You can also remove a filter from a DHCP range, and then delete the filter if it is not in use.

To delete a filter:

1. From the Data Management tab, select the DHCP tab -> Filters/Option Spaces tab -> Filters -> filter_name, and then click the Delete icon.
2. In the Delete Confirmation dialog box, click Yes.
   The appliance puts the deleted filters in the Recycle Bin, if enabled.
**Configuration Example: Using Option Filters**

The following example shows you how to create an option space, add custom options to it, create an option filter, and a match rule to filter the options so that the NIOS appliance can filter an address request by the vendor options of the requesting hosts. It can grant or deny an address request if the requesting host matches the filter.

1. Add an option space called SUNW, and then add the following options to it. For information, see *Applying DHCP Options* on page 629.

<table>
<thead>
<tr>
<th>Option name</th>
<th>Code</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>root-mount-options</td>
<td>1</td>
<td>Text</td>
</tr>
<tr>
<td>root-server-ip-address</td>
<td>2</td>
<td>IP address</td>
</tr>
<tr>
<td>root-server-host-name</td>
<td>3</td>
<td>Text</td>
</tr>
<tr>
<td>root-server-path-name</td>
<td>4</td>
<td>Text</td>
</tr>
<tr>
<td>swap-server-ip-address</td>
<td>5</td>
<td>IP address</td>
</tr>
<tr>
<td>swap-file-path-name</td>
<td>6</td>
<td>Text</td>
</tr>
<tr>
<td>boot-file-path-name</td>
<td>7</td>
<td>Text</td>
</tr>
<tr>
<td>posix-timezone-string</td>
<td>8</td>
<td>String</td>
</tr>
<tr>
<td>boot-read-size</td>
<td>9</td>
<td>16-Bit unsigned integer</td>
</tr>
</tbody>
</table>

2. From the Data Management tab, select the DHCP tab, and then click Add -> Filters from the Toolbar.
3. In the Add Filter wizard, enter the filter name i86pc, and then select Options as the filter type.
4. Select SUNW as the option space, select an option, specify a value for it, and then add it to the i86pc option filter. You can select multiple options. Add the following options to the i86pc option filter:

<table>
<thead>
<tr>
<th>Option name</th>
<th>Code</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>root-server-ip-address</td>
<td>2</td>
<td>IP address</td>
</tr>
<tr>
<td>root-server-host-name</td>
<td>3</td>
<td>Text</td>
</tr>
<tr>
<td>root-server-path-name</td>
<td>4</td>
<td>Text</td>
</tr>
<tr>
<td>boot-file-path-name</td>
<td>7</td>
<td>Text</td>
</tr>
</tbody>
</table>

5. From the Toolbar, click Add -> Match Rule.
6. In the Add Match Rule wizard, select i86pc as the option filter, select vendor-class-identifier (60) as the matching option, and then enter SUNW as the matching value.
7. Add a DHCP range to the network. For information, see *Configuring DHCP Address Ranges* on page 604.
8. Apply the i86pc option filter to the DHCP address range. For information, see *Applying Filters to DHCP Address Ranges* on page 687.
9. Click Restart to restart services.
Chapter 28  Authenticated DHCP

This chapter includes the following sections:

- About Authenticated DHCP on page 694
  - DHCP Authentication Process on page 694
- Configuring DHCP Authentication on page 698
- About Authentication Server Groups on page 699
  - Configuring a RADIUS Authentication Server Group on page 699
  - Configuring an Active Directory Authentication Server Group on page 700
- About the Captive Portal on page 702
  - Configuring Captive Portal Properties on page 703
  - Customizing the Captive Portal Interface on page 704
  - Managing Captive Portal Certificates on page 705
  - Starting the Captive Portal Service on page 706
- Defining the Network and DHCP Ranges on page 707
- Defining MAC Address Filters on page 708
- Using the Captive Portal Wizard on page 708
- Adding and Modifying the Filters and Associations on page 710
- Monitoring DHCP Authentication on page 710
  - Viewing DHCP Ranges and Filters on page 710
- Configuration Example: Configuring Authenticated DHCP on page 711
- NAC Integration on page 717
- Configuring NAC with Sophos NAC Advanced Servers on page 718
- About Authentication Servers on page 719
  - Adding a Server Group on page 719
  - Associating a Server Group with a Member on page 721
  - Managing Server Groups on page 721
  - Clearing the Authentication Cache on page 721
- Configuring DHCP Ranges on page 722
  - Listing DHCP Ranges on page 722
- About NAC Filters on page 723
  - Defining a NAC Filter on page 724
About Authenticated DHCP

This feature provides the ability to control access to your networks. You can divide a network into segments for unauthenticated, authenticated and guest users, and the DHCP server assigns clients to the appropriate segment based on their MAC addresses and authentication credentials.

For example, you can divide a network into one or more production segments for valid employees and systems, a guest segment with access only to the Internet and/or limited public servers, and a quarantine segment with access to a captive portal only. A captive portal is a web page that can provide an option to register as an authenticated user or as a guest.

On a member DHCP server, configure DHCP ranges for each access level—quarantine, authenticated, and guest—and create MAC address filters for the DHCP ranges. You can use DHCP options and Access Control Lists (ACLs) on your routers and firewall policies to define the appropriate services for each access level. On another grid member, configure the captive portal and specify the authentication server group that authenticates the users. You can configure an authentication server group for external servers running RADIUS or Active Directory (AD). Note that you cannot configure an independent appliance as a DHCP server and as the captive portal server. These must be on separate members in a grid.

When a DHCP client first sends a request for an IP address, the DHCP server offers an IP address from the quarantine range and directs the client to the captive portal, where the user can register either as an authenticated user or as a guest. When users sign in as guests or are successfully authenticated, the member automatically adds their MAC addresses to the appropriate MAC address filters and assigns addresses out of the appropriate address range.

DHCP Authentication Process

This section illustrates the DHCP authentication process. As illustrated in Figure 28.1, the DHCP authentication process begins when a DHCP client attempts to connect to the network. The member DHCP server checks if the MAC address of the DHCP client matches a MAC address in the guest or authenticated MAC address filters. If the member does not find a match, it assigns an IP address from the quarantine range to the DHCP client. When the client tries to access a web site, it is redirected to the captive portal page.
Note that the quarantine range in Figure 28.1 contains MAC address filters to deny leases in the quarantine range to DHCP clients with MAC addresses that match those in the Guest and Authenticated MAC address filters.

When the client connects to the captive portal IP address through its web browser, the user can register and continue the authentication process to obtain an IP address from the authenticated DHCP range, or register as a guest and obtain an IP address from the guest DHCP range.

If the user chooses to continue the authentication process, as shown in Figure 28.2, the member authenticates the user with the authentication service that you configured, which can be either RADIUS or AD.
After the client successfully passes the authentication stage, the appliance stores the MAC address of the client in the MAC address filter for the authenticated range. When the client tries to renew its IP address, it receives a new IP address from the authenticated DHCP range.

Note that if the MAC address filter has an expiration period, the member automatically deletes expired MAC addresses from the filter. Therefore, if a DHCP client tries to renew its IP address after the expiration period, the client is redirected to the captive portal because its MAC address is no longer in the MAC address filter. For more information, see Defining MAC Address Filters on page 680.
If the user chooses to sign in as a guest, as shown in Figure 28.3, the user can fill in the guest registration page provided by the captive portal.

Figure 28.3  Stage 2b: Registering as a Guest

After the user signs in as a guest, the appliance stores the MAC address of the client in the MAC address filter for the guest range. When the DHCP client tries to renew its IP address, it receives a new IP address from the guest DHCP range, unless the MAC address of the client expired and was removed from the filter. In this case, the DHCP client is redirected to the captive portal.
Configuring DHCP Authentication

Following are the tasks to configure the DHCP Authentication feature:

1. Configure the authentication server group which the captive portal uses to authenticate DHCP clients. For more information, see About Authentication Server Groups on page 699.
   If the captive portal is used to register guest users and does not authenticate users, then you do not have to configure an authentication server group.

2. Configure the captive portal properties and associate the captive portal with the authentication server group. For more information, see Configuring Captive Portal Properties on page 703.

3. Optionally, customize the captive portal interface and guest registration page, as described in Customizing the Captive Portal Interface on page 704. Additionally, if you enabled SSL encryption, upload the required certificates, as described in Managing Captive Portal Certificates on page 705.

4. Enable the captive portal, as described in Starting the Captive Portal Service on page 706.

5. Configure the network and a DHCP range for quarantine DHCP clients. Configure DHCP ranges for authenticated and guest DHCP clients, depending on whether you are allowing either one or both types of users to access your network. For information about configuring these DHCP ranges, see Defining the Network and DHCP Ranges on page 707.

6. Run the Captive Portal wizard to create MAC address filters for the quarantine range and for the authenticated, and guest DHCP ranges, if configured; and to associate the captive portal server with the member that serves the DHCP ranges. To accomplish these tasks and set other properties, see Using the Captive Portal Wizard on page 708. Alternatively, you can perform these tasks separately or modify the configured properties, as described in Adding and Modifying the Filters and Associations on page 710.

7. Enable the DHCP service. For more information, see Starting DHCP Services on a Member on page 639.
   For information about monitoring the captive portal and the DHCP service, see Monitoring DHCP Authentication on page 710.
**About Authentication Server Groups**

Create an authentication server group if you want the captive portal server to authenticate users when they register. You can create an authentication server group with either RADIUS servers or Active Directory servers, and then associate the group with the member that runs the captive portal and sends the authentication requests. You can associate an authentication server group with multiple captive portals, but you can associate a captive portal with only one authentication server group.

The following sections provide instructions for creating a RADIUS authentication server group and an AD authentication server group:

- Configuring a RADIUS Authentication Server Group
- Configuring an Active Directory Authentication Server Group on page 700

**Configuring a RADIUS Authentication Server Group**

You can add multiple RADIUS servers to an authentication server group and prioritize them. When the member sends an authentication request, it always selects the first RADIUS server in the list. It only sends authentication requests to the next server on the list if the first server goes down.

To configure the RADIUS authentication server group to which a captive portal server sends authentication requests:

1. From the **Administration** tab, click the **Authentication Server Groups** tab.
2. Expand the Toolbar and click **Add -> RADIUS Service**.
3. In the **Add RADIUS Authentication Service** wizard, complete the following:
   - **Name**: Enter the name of the server group.
   - **RADIUS Servers**: Click the Add icon and enter the following:
     - **Server Name or IP Address**: Enter the RADIUS server FQDN or IP address.
     - **Comment**: You can enter additional information about the server.
     - **Authentication Port**: The destination port on the RADIUS server. The default is 1812.
     - **Authentication Type**: Select the authentication method of the RADIUS server from the drop-down list. You can specify either PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol). The default is PAP.
     - **Shared Secret**: Enter the shared secret that the member DHCP server and the RADIUS server use to encrypt and decrypt their messages. This shared secret must match the one you entered on the RADIUS server.
     - **Connect through Management Interface**: Select this to enable the member to use its MGMT port to communicate with just this server.
     - **Disable server**: Select this to disable the RADIUS server if, for example, the connection to the server is down and you want to stop the DHCP server from trying to connect to this server.
     - **Click Test** to validate the configuration and check that the grid master can connect to the RADIUS server. Before you can test the configuration though, you must specify the authentication and accounting timeout and retry values.
       - If the grid master connects to the RADIUS server using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the RADIUS server, the appliance displays a message indicating an error in the configuration.
     - **Click Add** to add the RADIUS server to the group.

When you add multiple RADIUS servers to the list, you can use the up and down arrows to change the position of the servers on the list. The member DHCP server connects to the RADIUS servers in the order they are listed.

- **Authentication**
- **Timeout**: The time that the member DHCP server waits for a response from a RADIUS server before considering it unreachable. You can enter the time in milliseconds or seconds. The maximum is 10 seconds.
— **Retries:** The number of times the member DHCP server retries connecting to a RADIUS server before it considers the server unreachable. The default is five.

— **Accounting**

— **Timeout:** The time that the member DHCP server waits for a response from a RADIUS server before considering it unreachable. You can enter the time in milliseconds or seconds. The maximum is 10 seconds.

— **Retries:** The number of times the member DHCP server retries connecting to a RADIUS server before it considers the server unreachable. The default is five.

— **Recovery Interval:** Specifies the duration of time a RADIUS server stays inactive after being down, before becoming eligible to have RADIUS requests sent to it. The recovery interval starts when a RADIUS server is first discovered to be down.

— **Comment:** You can enter additional information about the server group.

— **Disable:** Select this to disable the authentication server group.

4. Select one of the following:
   — **Save & Close:** Save the entry and close the wizard.
   — **Save & Edit:** Save the entry and continue to edit.
   — **Save & New:** Save the entry and open a new wizard.

### Configuring an Active Directory Authentication Server Group

You can add multiple Active Directory servers running Windows Server 2003 or Windows Server 2008 to an authentication server group and prioritize the servers. When the member sends an authentication request, it always selects the first AD server in the list. It only sends authentication requests to the next server on the list if the first server goes down.

To configure an Active Directory authentication server group for a captive portal server:

1. From the **Administration** tab, click the **Authentication Server Groups** tab.
2. Click the **Active Directory Services** subtab and click the **Add** icon.
3. In the **Add Active Directory Authentication Service** wizard, complete the following:

   — **Name:** Enter a name for the service.

   — **Active Directory Domain:** Enter the AD domain name.

   — **Domain Controllers:** Click the **Add** icon and complete the following to add an AD domain controller:

     — **Server Name or IP Address:** Enter the FQDN or the IP address of the AD server that is used for authentication.

     — **Comment:** Enter additional information about the AD server.

     — **Authentication Port:** Enter the port number on the domain controller to which the member sends authentication requests. The default is 389.

     — **Encryption:** Select **SSL** from the drop-down list to transmit through an SSL (Secure Sockets Layer) tunnel. When you select SSL, the appliance automatically updates the authentication port to 636. Infoblox strongly recommends that you select this option to ensure the security of all communications between the member and the AD server. If you select this option, you must upload a CA certificate from the AD server. Click **CA Certificates** to upload the certificate. In the **CA Certificates** dialog box, click the **Add** icon, and then navigate to the certificate to upload it.

     — **Connect through Management Interface:** Select this so that the member uses the MGMT port for administrator authentication communications with just this AD server.

     — **Disable server:** Select this to disable an AD server if, for example, the connection to the server is down and you want to stop the grid member from trying to connect to this server.

     — **Click Test** to test the configuration. If the grid member connects to the domain controller using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the server, the appliance displays a message indicating an error in the configuration.

     — **Click Add** to add the domain controller to the group.
— **Timeout(s):** The number of seconds that the grid member waits for a response from the specified authentication server. The default is 5.
— **Comment:** Enter additional information about the service.
— **Disable:** Select this to retain an inactive AD authentication service profile.

4. Select one of the following:
— **Save & Close:** Save the entry and close the wizard.
— **Save & Edit:** Save the entry and continue to edit.
— **Save & New:** Save the entry and open a new wizard.
ABOUT THE CAPTIVE PORTAL

The captive portal can be used to register users for authentication, guest users, or both types of users. When a DHCP client attempts to connect to the network and its MAC address is not in any of the configured MAC filters, the member DHCP server assigns it an IP address in the quarantine range. When the quarantined client tries to reach any web site, it is redirected to the captive portal. The captive portal runs a limited DNS server that is used solely to redirect queries to the captive portal web interface.

You can enable the captive portal as a service on any grid member, except the grid master or grid master candidate. The grid member that runs the captive portal cannot run any other service, such as DHCP and DNS. Note that the limited DNS service that the captive portal runs is different from the full-scale DNS service that is enabled by default on an Infoblox appliance. The full-scale DNS service must be explicitly disabled on the member that runs the captive portal. For information on disabling DNS service, see Starting and Stopping the DNS Service on page 484.

You can configure one or more captive portals in the grid. You can also configure one or more member DHCP servers to use a captive portal to register users. For example, if your organization has two sites, you can configure a captive portal for each site and configure the DHCP servers in each site to use their respective captive portals to authenticate users.

In order for clients to reach the captive portal, you must specify a route to the captive portal. In a network where all IP addresses are on the same subnet, you can configure Option 33 for the quarantine DHCP range. For additional information, see Quarantine DHCP Range on page 707. On a routed network, you must configure a default route on the router for the subnet.

Following are the tasks to configure a captive portal:

1. Select the grid member that runs the captive portal and configure its properties, as described in Configuring Captive Portal Properties on page 703.
2. Optionally, customize the captive portal and registration page. For information about these tasks, see Customizing the Captive Portal Interface on page 704.
3. If you enabled SSL, generate the CA certificate, as described in Managing Captive Portal Certificates on page 705.
4. Start the captive portal, as described in Starting the Captive Portal Service on page 706.
Configuring Captive Portal Properties

When you configure the captive portal properties of a member, you specify if it is used to register users for authentication, guests, or both. If it is used to register guests only, then do not associate it with an authentication server group.

You can specify the VIP address of the grid member or configure an additional IP address on the loopback interface as the captive portal IP address. Alternatively, if the grid member supports the LAN2 port and it is enabled, but the NIC failover feature is disabled, you can use the IP address of the LAN2 port as the captive portal IP address. To configure an IP address on the loopback interface, see Configuring IP Addresses on the Loopback Interface on page 490. For information on the LAN2 port, see Using the LAN2 Port on page 147.

In addition, you can configure the port on which the appliance listens for authentication requests redirected from the captive portal. When a user logs in to the captive portal, the member sends an authentication request to its associated authentication server group. The member determines future DHCP replies to client requests based on the authentication result.

To configure the properties of the captive portal:

1. From the Grid tab, select the Grid Manager tab.
2. Click the Captive Portal tab -> Services tab.
   Grid Manager lists all the members, except for the grid master and grid master candidate.
3. Select the member that runs the captive portal and click the Edit icon.
4. In the General Basic tab of the Member Captive Portal Properties editor, complete the following:
   - Use This Authentication Server Group for Authenticating Captive Portal Users: Select the authentication server group that authenticates users for this captive portal. For information about authentication server groups, see About Authentication Server Groups on page 699.
   - Captive Portal User Types: Specify whether the captive portal is used to register Authenticated users only, Guest users only, or Both.
   - Portal IP Address: Select the IP address of the captive portal server. The appliance lists the VIP address and the IP addresses of the loopback interface and the LAN2 port, if enabled. You can select any of these addresses as the portal IP address.
   - Enable SSL on Portal: Select this to support encrypted web traffic through SSL/TLS. If you select this option, you must upload a certificate or generate a self-signed certificate. For information about creating and uploading a certificate for the captive portal, see Managing Captive Portal Certificates on page 705.
   - Network View: This field displays if there are multiple network views configured. Select the network view in which the authenticated, quarantine, and guest DHCP ranges belong.
   - Log Registration Success: Select to enable the member to log successful registrations in syslog, and then select the logging level from the drop-down list.
   - Log Registration Failure: Select to enable the member to log failed registrations in syslog, and then select the logging level from the drop-down list.
5. In the General Advanced tab of the editor, you can specify the port on which the member listens for authentication requests redirected from the captive portal. The default port is 4433. Depending on your firewall and network policies, you can configure an unused port greater than 1 and less than 63999.
6. Click Save & Close.
Customizing the Captive Portal Interface

You can customize the captive portal, and if configured, the guest registration page as well. You can upload image files to the appliance and display your own logo, header and footer. In addition, you can upload the acceptable use policies that are displayed on the captive portal and guest registration page.

Following are guidelines for each item you can customize:

• **Logo Image:** The maximum size is 200 pixels wide by 55 pixels high, and the images can be in JPEG, GIF, or PNG format. It displays on top of the header image.

• **Header Image:** The optimal size is 600 pixels wide by 137 pixels high. The image can be in JPEG, GIF, or PNG format. The header displays at the top of the page.

• **Footer Image:** The optimal size is 600 pixels wide by 20 pixels high. The image can be in JPEG, GIF, or PNG format. The footer displays at the bottom of the page.

• **Acceptable Use Policy:** The policy must be saved as a UTF-8 encoded file. It appears below the welcome message in the captive portal. Users can scroll through the policy when they review it. This is used in the captive portal and guest registration page. It must be a .txt file with a maximum of 8000 characters, including white space.

If any of the customizable fields are not configured, then the factory defaults are displayed.

To customize the captive portal:

1. From the Grid tab, select the Grid Manager tab.
2. Click the Captive Portal tab→ Services tab.
3. Select the member that is running the captive portal and click the Edit icon.
4. Select the Customization tab of the Member Captive Portal Properties editor.
5. In the General Captive Portal Customization section, complete the following:
   - **Company Name:** Enter the name of your company. The company name displays on the title bar of the browser. You can enter a maximum of 256 characters.
   - **Welcome Message:** Type the message that displays on the captive portal. The message can contain a maximum of 300 characters.
   - **Help Desk Message:** Type a message that provides Helpdesk information, such as contact information for technical assistance. The message can contain a maximum of 300 characters.
   - **Logo Image, Header Image, Footer Image, Acceptable Use Policy:** To display the image files and the acceptable use policy on the captive portal, click Select beside the item you want to upload. In the Upload dialog box, click Select File and navigate to the image or text file. Select the file you want to display and click Upload. Note that these files have size requirements, as listed earlier in this section.
6. In the Guest Users Web Page Customization section, complete the following:
   - The appliance displays certain fields on the guest registration page. Select the check boxes of the fields that users are required to complete: Require First Name, Require Middle Name, Require Last Name, Require Email, and Require Phone.
   - **Custom Field 1 — Custom Field 4:** You can display up to four additional fields on the guest registration page. To add a field to the guest registration page, enter a label for that field. The label can have a maximum of 32 characters. Select Require to require users to complete the field.

Users can enter a maximum of 128 characters in each of the fields in the captive portal login page and the guest registration page.

7. Click Save & Close.
Managing Captive Portal Certificates

When you enable support for encrypted web traffic sent over SSL/TLS, you can do any of the following:

- Generate a self-signed certificate and save it to the certificate store of your browser.
- Request a CA-signed certificate. When you receive the certificate from the CA, upload it on the member running the captive portal.

Generating Self-Signed Certificates

You can generate a self-signed certificate for the captive portal. When you generate a self-signed certificate, you can specify the hostname and change the public/private key size, enter valid dates and specify additional information specific to the captive portal. If you have multiple captive portals, you can generate a certificate for each captive portal with the appropriate hostname.

To generate a self-signed certificate:

1. From the Grid tab, select the Grid Manager tab.
2. Click the Captive Portal tab -> Services tab.
3. Select the member that is running the captive portal, and then click HTTPS Cert -> Generate Self-signed Certificate from the Toolbar.
4. In the Generate Self-signed Certificate dialog box, complete the following:
   - **Key Size**: Select either 2048 or 1024 for the length of the public key.
   - **Days Valid**: Specify the validity period of the certificate.
   - **Common Name**: Specify the domain name of the captive portal.
   - **Organization**: Enter the name of your company.
   - **Organizational Unit**: Enter the name of your department.
   - **Locality**: Enter a location, such as the city or town of your company.
   - **State or Province**: Enter the state or province.
   - **Country Code**: Enter the two-letter code that identifies the country, such as US.
   - **Admin E-mail Address**: Enter the email address of the captive portal administrator.
   - **Comment**: Enter additional information about the certificate.
5. Click OK.

Generating Certificate Signing Requests

You can generate a CSR (certificate signing request) that you can use to obtain a signed certificate from your own trusted CA. Once you receive the signed certificate, you can import it in to the grid member that runs the captive portal, as described in Uploading Certificates on page 706.

To generate a CSR:

1. From the Grid tab, select the Grid Manager tab.
2. Click the Captive Portal tab -> Services tab.
3. Select the member that is running the Captive Portal, and then click HTTPS Cert -> Create Signing Request from the Toolbar.
4. In the Create Signing Request dialog box, enter the following:
   - **Key Size**: Select either 2048 or 1024 for the length of the public/private key pair.
   - **Common Name**: Specify the domain name of the captive portal.
   - **Organization**: Enter the name of your company.
   - **Organizational Unit**: Enter the name of your department.
   - **Locality**: Enter a location, such as the city or town of your company.
   - **State or Province**: Enter the state or province.
Authenticated DHCP

- **Country Code**: Enter the two-letter code that identifies the country, such as US.
- **Admin E-mail Address**: Enter the email address of the captive portal administrator.
- **Comment**: Enter information about the certificate.

5. Click OK.

**Uploading Certificates**

When you upload a certificate, the NIOS appliance finds the matching CSR and takes the private key associated with the CSR and associates it with the newly uploaded certificate. The appliance then automatically deletes the CSR.

If the CA sends an intermediate certificate that must be installed along with the server certificate, you can upload both certificates to the appliance. The appliance supports the use of intermediate certificates to complete the chain of trust from the server certificate to a trusted root CA.

To upload a certificate:

1. From the Grid tab, select the Grid Manager tab.
2. Click the Captive Portal tab → Services tab.
3. Select the member that is running the captive portal, and then click HTTPS Cert → Upload Certificate from the Toolbar.
4. In the Upload dialog box, click Select File, navigate to the certificate location, and click Open.
   
   The appliance imports the certificate. When you log in to the appliance again, it uses the certificate you imported.

**Downloading Certificates**

You can download the current certificate or a self-signed certificate so users can install it in their browsers.

To download a certificate:

1. From the Grid tab, select the Grid Manager tab.
2. Click the Captive Portal tab → Services tab.
3. Select the member that is running the captive portal, and then click HTTPS Cert → Download Certificate from the Toolbar.
4. Navigate to where you want to save the certificate and save it.

**Starting the Captive Portal Service**

Before you start the captive portal service, ensure that the member is not running any other service.

To start the captive portal service:

1. From the Grid tab, select the Grid Manager tab.
2. Click the Captive Portal tab → Services tab.
3. Select the member that is configured to run the captive portal service and click the Start icon.
Defining the Network and DHCP Ranges

First define the network that uses DHCP authentication, and then define the DHCP ranges and services for each access level that you want to provide on the network:

- Quarantine
- Authenticated
- Guest

For information about configuring DHCP networks, ranges and services, see Chapter 14, Managing DHCP Data, on page 499 and Chapter 15, Configuring DHCP Services, on page 529.

Quarantine DHCP Range

You must configure a DHCP range for the quarantine level so the member DHCP server can assign IP addresses within that range to unauthenticated DHCP clients. An unauthenticated client is allowed to access the captive portal only and must successfully pass the authentication process before it can receive an IP address from the authenticated range.

Infoblox recommends 30-second leases for addresses in the quarantine DHCP range. This provides enough time for the user authentication process, so when the client attempts to renew the lease at the midpoint of its lease time, the member can then assign the client a new IP address, depending on the result of the authentication process.

When you configure the quarantine DHCP range, you must specify the captive portal IP address as the DNS server for the address range. The captive portal runs a limited DNS server that resolves all queries with the IP address assigned to the web interface on the captive portal.

Note that you can run the Captive Portal wizard to automatically set the lease time of the quarantine range to 30 seconds and to add the captive portal IP address as the DNS server. For information about the Captive Portal wizard, see Using the Captive Portal Wizard on page 708. Alternatively, you can set the lease time and the DNS server IP address in the DHCP tab of the DHCP Range editor. For information about the DHCP Range editor, see Configuring DHCP Address Ranges on page 604.

To ensure that clients can reach the captive portal, you must specify a route to the captive portal. On a network where all systems can reach each other without going through a router, that is, all IP addresses are on the same subnet, you must configure Option 33 for the quarantine DHCP range. This option specifies a list of static routes that the client should install in its routing cache. The routes consist of a list of IP address pairs. For clients to reach the captive portal, specify the portal IP address first (destination address), and the LAN address of the NIOS appliance second. When the appliance assigns an IP address from the quarantine DHCP range, it also includes the static route that you specified in option 33. For information about configuring DHCP options, see Specifying Custom DHCP Options on page 542. On a routed network, you must configure a default route via the router on the subnet.

Authenticated DHCP Range

Configure a DHCP range for authenticated users if you want the grid member to assign IP addresses within that range to authenticated DHCP clients. Users that receive an IP address in this range typically are allowed full access to the network.

When a client successfully passes authentication, the member automatically stores its MAC address in the corresponding MAC address filter. When the client attempts to renew the lease at the midpoint of its lease time, the member matches the source MAC address in the request with a MAC address in the filter for the authenticated DHCP address range. The member then assigns the client a new IP address from the authenticated DHCP range.

Guest DHCP Range

Configure a guest DHCP range if you want to provide guest access privileges. You can configure and customize a guest registration page when you configure the captive portal. For information about this feature, see Customizing the Captive Portal Interface on page 704.
**Defining MAC Address Filters**

After you configure the network and DHCP ranges, you must then configure the MAC address filters and add them to the appropriate DHCP ranges. If you configured DHCP ranges for authenticated and guest users, you must configure MAC address filters for each range with an action of Allow. You must also add those filters to the quarantine range with an action of Deny, to ensure that the member does not allocate an address from the quarantine range to a host whose MAC address matches an entry in the MAC filters for the authenticated and guest DHCP ranges.

When you create the filters, you also specify whether the MAC address entries expire. The member automatically deletes expired MAC address entries from the filter. If a client that registered earlier attempts to renew its IP address or to register after its MAC address has expired, it is redirected to the captive portal because its MAC address is no longer in the filter.

You can run the Captive Portal wizard to automatically create the MAC address filters, as described in the next section, *Using the Captive Portal Wizard*, or you can configure each filter as described in *Defining MAC Address Filters* on page 680.

**Using the Captive Portal Wizard**

After you configure the captive portal and the DHCP ranges for each access level, you can use the Captive Portal wizard to accomplish the following tasks:

- Associate the captive portal member with the member that serves the DHCP ranges you configured.
- Create MAC address filters and add them to the appropriate DHCP ranges. The wizard allows you to create MAC address filters for the quarantine DHCP range, and for the authenticated and guest DHCP ranges, depending on whether the captive portal is used to register users for authentication, guests, or both. This was specified when you configured the captive portal properties, described in *Configuring Captive Portal Properties* on page 703.

For example, if you indicated that the captive portal is used for authenticated users only, then the wizard allows you to create a MAC filter for the authenticated DHCP range only.

- If the captive portal is used to register users for authentication, the wizard allows you to create a MAC address filter for the authenticated range. The wizard then automatically adds the filter to the authenticated DHCP range with an action of Allow. It also adds the filter to the quarantine range with an action of Deny. This ensures that the member does not allocate an address from the quarantine range to a host whose MAC address matches an entry in the MAC filter.

- If the captive portal is used to register guest users, the wizard allows you to create a MAC address filter for the guest range. The wizard then automatically adds the filter to the guest DHCP range with an action of Allow. It also adds the filter to the quarantine range with an action of Deny. This ensures that the member does not allocate an address from the quarantine range to a host whose MAC address matches an entry in the MAC filter.

- Add the captive portal IP address as the DNS server for the quarantine address range.
- Set the lease time of the quarantine range to 30 seconds.

To use the Captive Portal wizard to complete the tasks for the DHCP authentication feature:

1. From the Data Management tab, select the DHCP tab, or from the Grid tab, select the Grid Manager tab.
2. Expand the Toolbar and click Configure Captive Portal.
3. In the Captive Portal wizard, complete the following and click Next:

   - **Member DHCP**: Select the member DHCP server that uses this captive portal to authenticate users.
   - **Captive Portal**: Select the member that runs the captive portal. Note that the member that runs the captive portal cannot run any other service, such as DHCP or DNS, and cannot be the grid master or grid master candidate.
4. This panel allows you to create MAC filters for the authenticated and guest DHCP ranges. The MAC filters you can create depend on your entry in the Captive Portal properties of the grid member. For example, if you indicated that the captive portal is used for authenticated users only, then this panel allows you to create a MAC filter for the authenticated DHCP range only.

You can also specify existing MAC filters, if you want to apply them to the authenticated and guest DHCP ranges. Complete the following and click **Next**:

- **Authenticated MAC Filter**: Specify a name for the MAC filter that is used for authenticated users.
- **Expiration Time**: Specify how long a MAC address is stored in the MAC address filter for authenticated users.
  - **Never**: Select this option to store MAC addresses in the MAC address filter until they are manually removed.
  - **Expires in**: Select this option to store MAC addresses in the MAC address filter for the specified period of time.

- **Guest MAC Filter**: Specify a name for the MAC filter that is used for guest users.
- **Expiration Time**: Specify how long a MAC address is stored in the MAC address filter for guest users.
  - **Never**: Select this option to store MAC addresses in the MAC address filter until they are manually removed.
  - **Expires in**: Select this option to store MAC addresses in the MAC address filter for the specified period of time.

5. In this panel, you specify the network and address ranges, so the wizard can apply the MAC address filters to the appropriate ranges. Complete the following:

- **Network**: Select the network that uses DHCP authentication.
- **Authenticated Range**: Select the IP address range that the appliance uses for authenticated users. The wizard applies the authenticated MAC address filter you specified in the preceding step to this DHCP range with an action of Allow. This effectively allows the member to assign an IP address from the address range to a requesting host whose MAC address matches the MAC address in the filter.

- **Guest Range**: Select the IP address range that the appliance uses for guest users. The wizard applies the guest MAC address filter you specified in the preceding step to this DHCP range with an action of Allow. This effectively allows the member to assign an IP address from the address range to a requesting host whose MAC address matches the MAC address in the filter.

- **Quarantine Range**: Select the IP address range that the appliance uses for quarantined addresses. The wizard applies the authenticated and guest MAC address filters to the quarantine DHCP range with an action of Deny. This effectively denies an address request from a host whose MAC address matches an entry in the MAC filters for the authenticated and guest DHCP ranges.

6. Click **Save & Close**.
Adding and Modifying the Filters and Associations

The Captive Portal wizard simplified the configuration process by accomplishing a number of tasks simultaneously. To accomplish each task separately, or to modify the filters or associations after you have run the wizard:

- To define the MAC address filters for each range, see Defining MAC Address Filters on page 680.
- To bind each filter to the appropriate DHCP range, see Applying Filters to DHCP Address Ranges on page 687.
- To specify the DNS server IP address for the quarantine range and set the lease time to 30 seconds, see Configuring General DHCP Properties on page 619 and Configuring DHCP Lease Times on page 621.
- To associate a member DHCP server with a captive portal and specify the MAC filters for the authenticated and guest DHCP ranges:
  1. From the Data Management tab, select the DHCP tab -> Members tab -> member check box -> Edit icon.
  2. In the Member DHCP Properties editor, click the Authenticated DHCP tab and complete the following:
     - Use this Captive Portal for Infoblox Authenticated DHCP: Select this check box and select the captive portal that you want to associate with the member.
     - Authenticated User MAC Filter: Select the MAC filter used for authenticated users. To change your section, click Clear and click Select again.
     - Guest User MAC Filter: Select the MAC filter for guest users. To change your selection, click Clear and click Select again.
  3. Click Save & Close.

Monitoring DHCP Authentication

You can monitor the status of the captive portal service, as described in Monitoring Services on page 304. You can check its status in the Grid Status widget and the Member Status widget on the Dashboard. For information about these widgets, see Chapter 2, The Dashboard, on page 55.

You can also view the MAC addresses that were added to each MAC address filter, as described in Viewing MAC Address Filter Items on page 690.

Viewing DHCP Ranges and Filters

To view the newly created MAC address filters:

1. From the Data Management tab, select the DHCP tab -> Filters/Option Spaces tab -> Filters.
   Grid Manager lists all the configured filters.
2. You can select a filter and view or configure its properties, such as extensible attributes.
   For more information about the filters and editing their properties, see Managing DHCP Filters on page 688.

To view the DHCP ranges and the newly added filters:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network.
2. Select the DHCP range you want to view and click the Edit icon.
3. If the editor is in Basic mode, click Toggle Advanced Mode.
4. Click the Filters tab to view the filters.

To verify that the captive portal is the DNS server in the quarantine range:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network.
2. Select the quarantine DHCP range and click the Edit icon.
3. In the DHCP Range editor, click the DHCP tab.
   The captive portal IP address is listed in the DNS Servers table.
**Configuration Example: Configuring Authenticated DHCP**

In this example, a school (school.edu) has two locations, its main campus, campus1.school.edu, and a satellite campus, campus2.school.edu. It has a captive portal server in each location. In the main campus, the grid master also functions as a DHCP server and uses a captive portal server to register DHCP clients. In the satellite campus, two members serve DHCP and use the same captive portal server. The captive portal servers use the same RADIUS authentication server group to authenticate users.

*Figure 28.4*

Create the RADIUS Authentication Server Group

Create the RADIUS authentication server group and add two RADIUS servers to the group.

1. From the **Administration** tab, click the **Authentication Server Groups** tab.
2. Expand the Toolbar and click **Add -> RADIUS Service**.
3. In the **Add RADIUS Authentication Service** wizard, complete the following:
   - **Name**: Enter **RADIUS ASG**.
   - **RADIUS Servers**: Click the Add icon and enter the following:
     - authenticated: 10.2.1.50 - 10.2.1.150
     - guest: 10.2.1.151 - 10.2.1.170
     - quarantine: 10.2.1.225 - 10.2.1.254
     - authenticated: 10.1.1.50 - 10.1.1.150
     - guest: 10.1.1.151 - 10.1.1.170
     - quarantine: 10.1.1.225 - 10.1.1.254
     - guest: 10.1.2.151 - 10.1.2.170
     - quarantine: 10.1.2.225 - 10.1.2.254
— **Server Name or IP Address:** Enter the RADIUS server FQDN, which is `rs1.school.edu`.
— **Authentication Port:** Accept the default port (1812).
— **Authentication Type:** Select the PAP authentication method.
— **Shared Secret:** Enter `no1nose`.

— **Authentication**
  — **Timeout:** Enter 5 seconds.
  — **Retries:** Accept the default, which is five.

— **Accounting**
  — **Timeout:** Enter 5 seconds.
  — **Retries:** Accept the default, which is five.
  — **Click Test** to validate the configuration and check that the grid master can connect to the RADIUS server.

  Grid Manager displays a message confirming the configuration is valid.

Click **Add** to add another RADIUS server to the group, and then enter the following:

— **Server Name or IP Address:** Enter the RADIUS server FQDN, which is `rs2.school.edu`.
— **Authentication Port:** Accept the default port (1812).
— **Authentication Type:** Select the PAP authentication method.
— **Shared Secret:** Enter `no1nose`.

— **Authentication**
  — **Timeout:** Enter 5 seconds.
  — **Retries:** Accept the default, which is five.

— **Accounting**
  — **Timeout:** Enter 5 seconds.
  — **Retries:** Accept the default, which is five.
  — **Click Test** to validate the configuration and check that the grid master can connect to the RADIUS server.

  Grid Manager displays a message confirming the configuration is valid.

4. Click **Save & Close**.

### Configure the Captive Portal Properties

Configure the captive portal properties of `cp1.campus1.school.edu`.

1. From the **Grid** tab, select the **Grid Manager** tab.
2. Click the **Captive Portal** tab -> **Services** tab.
3. Select the member `cp1.campus1.school.edu` and click the **Edit** icon.
4. In the **General Basic** tab of the **Member Captive Portal Properties** editor, complete the following:
   — **Use This Authentication Server Group for Authenticating Captive Portal Users:** Select RADIUS ASG.
   — **Captive Portal User Types:** Select Both.
   — **Portal IP Address:** Select `10.2.2.10`.
   — **Enable SSL on Portal:** Select this option.
   — **Log Registration Success:** Select Informational.
   — **Log Registration Failure:** Select Informational.
5. Click **Save & Close**.

Configure the captive portal properties of `cp2.campus2.school.edu`.

1. From the **Grid** tab, select the **Grid Manager** tab.
2. Click the **Captive Portal** tab -> **Services** tab.
3. Select the member cp2.campus2.school.edu and click the Edit icon.

4. In the **General Basic** tab of the *Member Captive Portal Properties* editor, complete the following:
   - **Use This Authentication Server Group for Authenticating Captive Portal Users**: Select RADIUS ASG.
   - **Captive Portal User Types**: Select Both.
   - **Portal IP Address**: Select 10.1.3.10.
   - **Enable SSL on Portal**: Select this option.
   - **Log Registration Success**: Select Informational.
   - **Log Registration Failure**: Select Informational.

5. Click **Save & Close**.

### Customize the Captive Portals

Customize the captive portal cp1.campus1.school.edu.

1. From the Grid tab, select the Grid Manager tab.
2. Click the Captive Portal tab→ Services tab.
3. Select cp1.campus1.school.edu and click the Edit icon.
4. Select the Customization tab of the *Member Captive Portal Properties* editor.
5. In the **General Captive Portal Customization** section, complete the following:
   - **Company Name**: Enter School.
   - **Welcome Message**: Type the following: Welcome to School. Please sign in.
   - **Help Desk Message**: Type: To reach the Helpdesk, call (408) 111-2222 or email helpdesk@school.edu.
   - **Logo Image**: Click Select beside the logo file and upload it.
6. In the **Guest Users Web Page Customization** section, complete the following:
   - Select the check boxes beside **Require First Name**, **Require Last Name**, **Require Email**.
7. Click **Save & Close**.

Select the other captive portal server, cp2.campus2.school.edu, and enter the same information.

### Generate a Self-Signed Certificate and Upload It

To generate a self-signed certificate for cp1.campus1.school.edu:

1. From the Grid tab, select the Grid Manager tab.
2. Click the Captive Portal tab→ Services tab.
3. Select cp1.campus1.school.edu, and then click HTTPS Cert → Generate Self-signed Certificate from the Toolbar.
4. In the *Generate Self-signed Certificate* dialog box, complete the following:
   - **Key Size**: Select 1024 for the length of the public key.
   - **Days Valid**: Enter 60 days.
   - **Common Name**: Enter cp1.campus1.school.edu.
5. Click OK.
6. Click **Save & Close**.

To generate a self-signed certificate for the captive portal cp2.campus2.school.edu:

1. From the Grid tab, select the Grid Manager tab.
2. Click the Captive Portal tab→ Services tab.
3. Select cp2.campus2.school.edu, and then click HTTPS Cert → Generate Self-signed Certificate from the Toolbar.
4. In the *Generate Self-signed Certificate* dialog box, complete the following:
   - **Key Size:** Select 1024 for the length of the public key.
   - **Days Valid:** Enter 60 days.
   - **Common Name:** Enter cp2.campus2.school.edu.

5. Click **OK**.

6. Click **Save & Close**.

**Start the Captive Portal Service**

1. From the Grid tab, select the Grid Manager tab.
2. Click the Captive Portal tab → Services tab.
3. Select cp1.campus1.school.edu and cp2.campus2.school.edu, and then click the Start icon.

**Configure the Networks and DHCP Ranges**

Configure the network on the grid master.

1. From the Data Management tab, select the DHCP tab.
2. Expand the Toolbar and click **Add → Network**.
3. In the *Add Network* wizard, select one of the following and click **Next**:
   - **Add Network:** Click this.
4. Complete the following and click **Next**:
   - **Address:** Enter 10.2.1.0/24.
5. Complete the following to assign the network to the grid master:
   - **Add Infoblox Member:** Select gm.campus1.school.edu.
6. Click **Save & Close**.

Configure the ranges on the grid master.

To create the authenticated range:

1. From the Data Management tab, select the DHCP tab.
2. Select the 10.2.1.0/24 network, and then click **Add → DHCP Range** from the Toolbar.
3. In the *Add Range* wizard, select Add DHCP Range and click **Next**:
4. Complete the following:
   - **Network:** Click **Select Network** and select 10.2.1.0/24.
   - **Start:** Enter 10.2.1.50.
   - **End:** Enter 10.2.1.150.
   - **Name:** Enter authenticated range.
5. Click **Next** and complete the following:
   - **Grid Member:** Select this option and select gm.campus1.school.edu.
6. Click **Save & Close**.

To create the guest range:

1. Select the 10.2.1.0/24 network, and then click **Add → DHCP Range** from the Toolbar.
2. In the *Add Range* wizard, select Add DHCP Range and click **Next**:
3. Complete the following:
   - **Network:** Click **Select Network** and select 10.2.1.0/24.
   - **Start:** Enter 10.2.1.151.
   - **End:** Enter 10.2.1.170.
   - **Name:** Enter guest range.
4. Click **Next** and complete the following:
   - **Grid Member**: Select this option and select gm.campus1.school.edu.

5. Click **Save & Close**.

To create the quarantine range:

1. Select the 10.2.1.0/24 network, and then click **Add -> DHCP Range** from the Toolbar.

2. In the **Add Range** wizard, select **Add DHCP Range** and click **Next**:

3. Complete the following:
   - **Network**: Click **Select Network** and select 10.2.1.0/24.
   - **Start**: Enter 10.2.1.225.
   - **End**: Enter 10.2.1.254.
   - **Name**: Enter quarantine range.

4. Click **Next** and complete the following:
   - **Grid Member**: Select this option and select gm.campus1.school.edu.

5. Click **Save & Close**.

Create the network and DHCP ranges for the DHCP servers ds1.campus1.school.edu and ds2.campus2.school.edu.

**Run the Captive Portal Wizard**

Run the Captive Portal wizard to associate the grid master with its captive portal, and to configure the MAC address filters:

1. From the Data Management tab, select the DHCP tab, or from the Grid tab, select the Grid Manager tab.

2. Expand the Toolbar and click Configure Captive Portal.

3. In the Captive Portal wizard, complete the following and click **Next**:
   - **Member DHCP**: Select the grid master, gm.campus1.school.edu.
   - **Captive Portal**: Select cp1.campus1.school.edu.

4. Complete the following and click **Next**:
   - **Authenticated MAC Filter**: Enter Auth_MAC_Filter.
   - **Expiration Time**: Select Never.
   - **Guest MAC filter**: Enter Guest_MAC_Filter.
   - **Expiration Time**: Select Never.

5. Complete the following:
   - **Network**: Select 10.2.1.0/24.
   - **Authenticated Range**: Select 10.2.1.50 - 10.2.1.150.
   - **Guest Range**: Select 10.2.1.151 - 10.2.1.170.
   - **Quarantine Range**: Select 10.2.1.225 - 10.2.1.254.

6. Click **Save & Close**.

Run the Captive Portal wizard to associate ds1.campus2.school.edu with the captive portal server cp2.campus2.school.edu, and then run it again to associate ds2.campus2.school.edu with the same captive portal server.
**Start the DHCP Service**

To start the DHCP service on the grid master:

1. From the **Data Management** tab, select the **DHCP tab -> Members tab**.
2. Select the grid master gm.campus1.school.edu, and the two members, ds1.campus2.school.edu and ds2.campus2.school.edu.
3. Expand the Toolbar and click **Start**.
4. In the **Start Member DHCP Service** dialog box, click **Yes**.
5. Grid Manager starts DHCP services on the grid master and on the selected members.
NAC INTEGRATION

You can configure member DHCP servers to send authentication requests to RADIUS servers and to allocate addresses based on the authentication results. This allows you to place DHCP clients into separate network segments.

You can divide your network into different segments by configuring address ranges and applying NAC filters to them. NAC filters use authentication results from RADIUS servers as matching criteria for granting or denying address requests.

When a DHCP client requests a lease, the member DHCP server can query the RADIUS server that runs on a Sophos NAC Advanced server to determine if the DHCP client is authorized to access the network. A Sophos NAC Advanced server is an access-control and compliance server that supports the RADIUS protocol. For information about Sophos NAC Advanced servers, refer to the Sophos documentation.

The Sophos NAC Advanced server then checks its database and provides the Sophos compliance state and user class, if configured, of the DHCP client. The member DHCP server matches the response with the configured NAC filters, and grants a lease to the appropriate network segment.

Figure 28.5 presents an example illustrating the authentication process and how a member DHCP server matches the response with NAC filters to determine whether to grant or deny a lease. In the example, there are two DHCP ranges configured, each with a NAC filter that specifies the Sophos compliance state of DHCP clients allowed in each range.

Figure 28.5

The following steps relate to Figure 28.5.

1. A DHCP client sends a DHCPDISCOVER, DHCPREQUEST, or DHCPINFORM to the Infoblox DHCP server.
2. The DHCP server sends the Sophos NAC Advanced server a RADIUS Access-Request packet that includes Sophos VSAs (Vendor Specific Attributes) with the MAC address and DHCP transaction ID of the DHCP client.
3. When the Sophos NAC Advanced server receives the Access-Request packet, it does the following:
   a. It looks up the MAC address in its database to retrieve the associated compliance state and user class.
   b. The Sophos NAC Advanced server sends back a RADIUS Access-Accept packet that includes Sophos VSAs with the compliance status and user class.
4. The DHCP server receives the Access-Accept packet and tries to match the response with a NAC filter.
5. The DHCP server matches the response with the NAC filter for compliant DHCP clients and sends the DHCP client a DHCPOFFER that contains an IP address from the corresponding DHCP range. The server also provides the configuration and options associated with that range.

Figure 28.5

<table>
<thead>
<tr>
<th>DHCP Client</th>
<th>Infoblox DHCP Server</th>
<th>Sophos NAC Advanced Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAC Filters</td>
<td>DHPC Ranges</td>
<td>RADIUS Server</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Non-Compliant

192.168.1.50-192.168.1.150

Compliant

192.168.1.151-192.168.1.200
**CONFIGURING NAC WITH SOPHOS NAC ADVANCED SERVERS**

Complete the following tasks to configure the Sophos NAC Advanced server and the member DHCP server.

On an already functioning Sophos NAC Advanced server:

- Add the member DHCP server as a RADIUS client. Make sure that the shared secret you enter on the Sophos NAC Advanced server matches the shared secret that you specify when you add the server to the authentication server group in Grid Manager.
  
  Note that on Grid Manager, you can enter only one shared secret for each Sophos NAC Advanced server. Therefore, on a Sophos NAC Advanced server, you must define the same shared secret for all grid members that connect to it.
  
  For information about adding RADIUS clients, refer to the Sophos NAC Advanced documentation.

- Add the Infoblox grid master as a RADIUS client, even if it is not going to perform NAC authentication. This enables you to test the connection to the Sophos NAC Advanced server.

On the member DHCP server:

1. Configure the authentication server group for the Sophos NAC Advanced servers. For information, see *Adding a Server Group* on page 719.

2. Associate the authentication server group with the grid member. For information, see *Associating a Server Group with a Member* on page 721.

3. Configure the network and the DHCP ranges. For information, see *Configuring DHCP Ranges* on page 722.

4. Configure the NAC filters, as described in *About NAC Filters* on page 723.

5. Apply the NAC filters to the DHCP ranges, as described in *Applying Filters to DHCP Address Ranges* on page 687.

6. Enable the DHCP service. For information, see *Member Level* on page 536.

Optionally, you can do the following:

- Manage the authentication cache, as described in *Clearing the Authentication Cache* on page 721.
About Authentication Servers

You can create a RADIUS authentication server group for Sophos NAC Advanced servers, and then associate the group with the member DHCP server that sends authentication requests. The member DHCP server tries to connect to each Sophos NAC Advanced server in the group using one of the following methods: Ordered List or Round Robin.

In the Ordered List method, the member DHCP server always selects the first Sophos NAC Advanced server in the list when it sends an authentication request. It only sends authentication requests to the next server on the list if the first server goes down.

In the Round Robin method, the member DHCP server selects the first Sophos NAC Advanced server for the first request, the second server for the next request, and so on until it selects the last server in the list. Then it starts with the first server in the list and continues the same selection process.

Each member DHCP server can have only one RADIUS server group assigned, but a RADIUS server group can be assigned to multiple member DHCP servers.

Adding a Server Group

To create a RADIUS authentication server group for Sophos NAC Advanced servers:

1. From the Administration tab, click the Authentication Server Groups tab.
2. Expand the Toolbar and click Add -> RADIUS Service.
3. In the Add RADIUS Authentication Service wizard, complete the following:
   - Name: Enter the name of the server group.
   - RADIUS Servers: Click the Add icon and enter the following:
     - Server Name or IP Address: Enter the Sophos NAC Advanced server FQDN or IP address.
     - Comment: You can enter additional information about the server.
     - Authentication Port: The destination port on the Sophos NAC Advanced server. The default is 1812.
     - Authentication Type: Select the authentication method of the RADIUS server from the drop-down list. You can specify either PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol). The default is PAP.
     - Shared Secret: Enter the shared secret that the member DHCP server and the Sophos NAC Advanced server use to encrypt and decrypt their messages. This shared secret must match the one you entered on the Sophos NAC Advanced server.
     - Enable Accounting: Leave this blank. RADIUS accounting is not supported.
     - Connect through Management Interface: Select this so that the NIOS appliance uses the MGMT port for communications with just this server.
     - Disable server: Select this to disable the Sophos NAC Advanced server if, for example, the connection to the server is down and you want to stop the DHCP server from trying to connect to this server.
     - Click Test to validate the configuration and check that the grid master can connect to the Sophos NAC Advanced server. Before you can test the configuration though, you must specify the authentication and accounting timeout values.
     - If the grid master connects to the Sophos NAC Advanced server using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the Sophos NAC Advanced server, the appliance displays a message indicating an error in the configuration.
     - Click Add to add the Sophos NAC Advanced server to the server group.

When you add multiple Sophos NAC Advanced servers to the list, you can use the up and down arrows to change the position of the servers on the list. The member DHCP server connects to the Sophos NAC Advanced servers in the order they are listed.

- Authentication
  - Timeout: The time that the member DHCP server waits for a response from a Sophos NAC Advanced server before considering it unreachable. You can enter the time in milliseconds or seconds.
Authenticated DHCP

— **Retries**: The number of times the member DHCP server retries connecting to a Sophos NAC Advanced server before it considers the server unreachable. The default is five.

— **Mode**: Specifies how the member DHCP server selects the first Sophos NAC Advanced server to contact.
  - **Ordered List**: The member DHCP server always selects the first Sophos NAC Advanced server in the list when it sends an authentication request. It queries the next server only when the first server is considered down. This is the default.
  - **Round Robin**: The member DHCP server selects the first Sophos NAC Advanced server for the first request, the second server for the next request, and so on. If the last server is reached, then the DHCP server starts with the first server in the list, and so on.

— **Enable Authentication Cache**: The member DHCP server automatically caches authentication results for 120 seconds. When you enable this option, you can override this default in the **Cache Time to Live** field. You must enable this option to clear the cache, as described in *Clearing the Authentication Cache* on page 721.

— **Cache Time to Live**: Specifies the duration of time an authentication result is stored. The default is one hour. The maximum is 259200 seconds (3 days).

— **Recovery Interval**: Specifies the duration of time a Sophos NAC Advanced server stays inactive after being down, before becoming eligible to have RADIUS requests sent to it. The recovery interval starts when a Sophos RADIUS server is first discovered to be down.

— **Comment**: You can enter additional information about the server group.

— **Disable**: Select this to disable the authentication server group.

4. Select one of the following:
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and continue to edit.
   - **Save & New**: Save the entry and open a new wizard.
Associating a Server Group with a Member

To associate an authentication server group with a member DHCP server:
1. From the Data Management tab, select the DHCP tab -> Members tab -> member check box, and click the Edit icon.
2. If the Member DHCP Properties editor is in Basic mode, click Toggle Advanced Mode.
3. Select the Sophos NAC tab.
4. Click the Use this authentication server group check box and select a group from the drop-down list.
5. Click Save & Close.

Managing Server Groups

To view the list of authentication server groups, from the Administration tab, click the Authentication Server Groups tab and expand the RADIUS Service subtab. For each server group, you can view the server group name, comments, and whether the group is available or disabled. You can then select a server group to modify or delete it.
To modify a server group, select it and click the Edit icon. You can modify any of its properties, and add or delete servers from the group. When you delete a Sophos NAC Advanced server from a group, the appliance permanently deletes it.
To delete a server group, select it and click the Delete icon. When you delete an authentication server group, the appliance permanently deletes it.

Clearing the Authentication Cache

The authentication cache can store authentication results for up to 20,000 DHCP clients. When the cache reaches its limit, the DHCP member logs a message in syslog. To clear the entire cache or the cache entry of a specific MAC address, you must enable the authentication cache in the RADIUS Service wizard or editor.
To clear the entire authentication cache:
1. From the Data Management tab, select the DHCP tab -> Members tab -> member check box.
2. Expand the Toolbar and select Clear -> Authentication Cache.
3. When the Clear Authentication Cache confirmation dialog appears, click Purge.
To delete a specific entry:
1. From the Data Management tab, select the DHCP tab -> Members tab -> member check box.
2. Expand the Toolbar and select Clear -> Authentication Record.
3. In the Clear Authentication Record dialog box, enter the DHCP client MAC address, and then click Purge.
Configuring DHCP Ranges

Create the network and DHCP ranges as described in Chapter 14, Managing DHCP Data, on page 499. You can create multiple DHCP ranges and apply one or more NAC filters to each of them.

Listing DHCP Ranges

By default, DHCP ranges are listed according to their start addresses. You can reorder them according to the order in which you want the member DHCP server to evaluate the ranges.

Consider the following sample DHCP ranges:
- 10.20.30.100-10.20.30.199 (NAC filter that allows leases for compliant DHCP clients)
- 10.20.30.0-10.20.30.99 (No filters)

If the DHCP range with the NAC filter is listed before the range with no filters, then the DHCP server consults the Sophos NAC Advanced server and applies the NAC filter before it grants a lease. It grants leases from the range with no filters only if no NAC filters matched or after all leases from the first range are exhausted. If the first range is the production range and the second range is for the quarantine group, then the server applies the NAC filters for the production range, before it grants leases to the quarantine range.

To change the order of DHCP ranges in a network:
1. From the Data Management tab, select the DHCP tab -> Networks tab -> network.
2. Expand the Toolbar and click Order DHCP Ranges.
3. In the Order DHCP Ranges dialog box, click the up and down arrows to move ranges up or down on the list. The Priority value changes accordingly.
4. Click OK.

You can view the DHCP objects in a network, including its DHCP ranges by navigating to the DHCP tab -> Networks tab -> Networks panel, and then clicking the network link. For information about this panel, see Viewing Network Details on page 596. You can select the Priority column for display to view the order of the DHCP ranges. For information about editing the columns, see Customizing Tables on page 44.
About NAC Filters

You can define NAC filters that specify authentication results from the Sophos NAC Advanced servers. You can then apply each filter to a DHCP range and indicate whether the DHCP server grants or denies a lease when the authentication result matches the filter. You can apply NAC filters to any DHCP range and DHCP range template.

In a NAC filter, you can define rules that specify the following:

- The status of the RADIUS authentication server group:
  - Success: At least one of the servers in the RADIUS authentication server group is up.
  - Fail: The MAC address in the DHCP request is not in the authentication cache and all servers in the server group are down.
  - Disabled: The RADIUS authentication server group is disabled, all the servers in the group are disabled, or the member is not assigned a server group.

- The response from the RADIUS server:
  - Accept: The response is an Access-Accept packet.
  - Reject: The response is an Access-Reject packet.

- Whether the Access-Accept packet contains an error. The Infoblox DHCP server expects certain Sophos VSAs in the Access-Accept packet. An error occurs when any of the Sophos VSAs are missing. For information about the Access-Accept packet and the Sophos VSAs, refer to the Sophos documentation.
  - Yes: The Access-Accept packet does not include one or more Sophos VSAs.
  - No: There are no errors in the Access-Accept packet.

- A Sophos compliance state: unknown, non-compliant, compliant or partially compliant

- A Sophos user class

When the member DHCP server receives an address request, it checks the DHCP ranges in their priority order. For information about the order of DHCP ranges, see Listing DHCP Ranges on page 722.

For each DHCP range, it checks if the request matches any MAC filters, relay agent filters, or DHCP option filters that apply to the range. (For information about these filters, see Chapter 27, Configuring DHCP Filters, on page 673.) If any of those filters match, then the member either grants or denies a lease to the DHCP client, based on the filter. If none of those filters match and there are NAC filters defined, then the member tries to send an authentication request to a server in the RADIUS authentication server group.

If you want the member DHCP server to grant leases to specific DHCP ranges in case the RADIUS authentication server group is considered disabled (server state = disabled) or if all RADIUS servers are down (server state = failure), create a NAC filter for each situation and apply it to the appropriate range.

Note that when you create a NAC filter, you do not have to include rules that specify prerequisite conditions. For example, when you create a filter that specifies a Sophos compliance state or user class, you do not have to include rules that specify the following: server state = success, server response = accept, and server error = no.
Defining a NAC Filter

To define a NAC filter:
1. From the Data Management tab, select the DHCP tab -> Filters/Option Spaces tab.
2. Click the Add icon.
3. In the Add Filter Wizard, complete the following and click Next:
   - Name: Enter a name for the filter. You can enter a maximum of 255 characters.
   - Comment: Optionally, enter additional information about the NAC filter.
   - Filter Type: Select NAC from the drop-down list.
4. Create a rule as follows:
   - In the first drop-down list, select one of the following criterion: Compliance State, Server Error, Server Response, Server State or User Class.
   - In the second drop-down list, select an operator: equals or does not equal.
   - The selections in the third drop-down list depend on the criterion you selected:
     - Compliance State: Select one of the following compliance states: Unknown, Non-compliant, Compliant or Partially Compliant.
     - Server Error: The Infoblox DHCP server expects certain Sophos VSAs in the Access-Accept packet. When any of the VSAs are missing, then the DHCP server considers this an error. For information about the Access-Accept packet and the VSAs, refer to the Sophos documentation. Select one of the following:
       - Yes: Create a rule that matches when the RADIUS server sends an Access-Accept packet with a missing VSA.
       - No: Create a rule that matches when the RADIUS server sends an Access-Accept packet with no errors.
     - Server Response: Select one of the following:
       - Accept: Create a rule that matches when the server sends back an Access-Accept packet.
       - Reject: Create a rule that matches when the server sends back an Access-Reject packet.
     - Server State: Select one of the following:
       - Success: Create a rule that matches when at least one RADIUS server in the group is up.
       - Fail: Create a rule that matches when the MAC address of the DHCP client is not in the cache and all RADIUS servers in the server group are down.
       - Disable: Create a rule that matches when the RADIUS authentication server group is disabled, all servers in the group are disable, or the member was not assigned a server group.
     - User Class: Enter the Sophos user class value, for example, NACDeny. The member DHCP server does not validate the entry. Therefore, you must make sure that the user class you enter matches the user class name on the Sophos NAC Advanced server.
   - To add another rule:
     - Click |<- to add a parenthetical rule above the first line that is indented one level.
     - Click - to delete a rule.
     - Click + to add another rule at the same level.
     - Click ->| to add an ALL (logical AND) or ANY (logical OR) operator line, and a parenthetical rule that is indented one level.
   - You can click Preview to view the authentication clause or click Reset to remove the previously configured rules and start again.
5. Click Next to define extensible attributes. For information, see Using Extensible Attributes on page 225.
6. Click Save & Close.
   After you add NAC filters, you must then apply them to DHCP ranges, as described in Applying Filters to DHCP Address Ranges on page 687. You can also list, modify or delete NAC filters, as described in Managing DHCP Filters on page 688.
PART 5 MANAGING MICROSOFT WINDOWS SERVERS

This section describes how to manage Microsoft Windows® servers from the grid. It includes the following chapters:

- Chapter 29, "Managing Microsoft Windows Servers", on page 727
- Chapter 30, "Managing Microsoft DNS Services", on page 741
- Chapter 31, "Managing Microsoft DHCP Services", on page 757
Chapter 29 Managing Microsoft Windows Servers

This chapter explains how to configure grid members to manage Microsoft Windows DNS and DHCP servers from Grid Manager. It includes the following sections:

- **About Managing Microsoft Servers** on page 728
  - Requirements on page 729
  - Deployment Guidelines on page 730
- **Configuring Members to Manage Microsoft Servers** on page 731
  - Setting Microsoft Server Credentials on page 731
  - Configuring a Managing Member on page 732
- **Managing Microsoft Servers** on page 735
  - Setting Microsoft Server Properties on page 735
  - Changing the Managing Member or Management Mode on page 736
  - Backing Up Synchronized Data on page 736
  - Disabling Synchronization on page 736
  - Removing a Managed Microsoft Server on page 737
- **Monitoring Managed Microsoft Servers** on page 737
  - Viewing the Status of Servers on page 737
  - Viewing Detailed Status Information on page 739
  - Viewing Synchronization Logs on page 739

**Note:** vNIOS grid members do not support this feature.
About Managing Microsoft Servers

You can configure grid members to manage Microsoft Windows DNS and DHCP servers and synchronize the Microsoft data to the grid database, so you can view and optionally, manage the data from Grid Manager. In addition, you can control the DNS and DHCP services of the Microsoft servers from Grid Manager and configure server properties as well.

Figure 29.1 illustrates a grid that includes a member that provides DNS and DHCP services, and two other members that manage multiple Microsoft DNS and DHCP servers. Assuming the admin has the appropriate permissions, the admin can centrally manage five Microsoft DNS and DHCP servers and one Infoblox DNS and DHCP server from a single interface, Grid Manager.

Figure 29.1 Managing Microsoft and Infoblox DNS and DHCP Servers from the Grid Master

You do not have to configure or install any application on the Microsoft servers for the grid members to communicate with the servers. Infoblox uses MS-RPC (Microsoft Remote Procedure Calls) to manage Microsoft servers.

A grid member can manage a Microsoft server in either of two modes, read-only or read/write. In read-only mode, the grid member synchronizes data from the Microsoft server to the grid so admins can use Grid Manager to view the synchronized data, but not update it. Read/Write mode allows admins to update the synchronized data as well. Updates from Grid Manager are then synchronized to the Microsoft server, and updates from the Microsoft server are synchronized to the grid.

Configuration changes and data synchronized from the grid to the Microsoft server apply immediately after the synchronization. You do not have to restart the Microsoft server or for DNS, reload the zones.
Requirements

A grid member must have a Microsoft Management license installed to manage a Microsoft server. The license allows the member to synchronize data with Microsoft servers. It also activates the tabs, dialog boxes and other elements in Grid Manager that you need to manage a Microsoft server.

Note that if you do not see the Microsoft Servers tab after you add a member that has a Microsoft Management license, you might have to restart the grid master to view the tab and to manage Microsoft DNS and DHCP servers in the grid.

Supported Windows Versions

Infoblox grid members can manage Microsoft servers that support the following Windows versions:

<table>
<thead>
<tr>
<th>OS</th>
<th>Levels</th>
<th>Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 2003 Standard</td>
<td>SP2</td>
<td>32 bits</td>
</tr>
<tr>
<td>and Enterprise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows 2003 R2 Standard</td>
<td>Initial Release</td>
<td>32 bits, 64 bits</td>
</tr>
<tr>
<td>and Enterprise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows 2008 Standard</td>
<td>SP2</td>
<td>32 bits, 64 bits</td>
</tr>
<tr>
<td>and Enterprise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows 2008 R2 Standard</td>
<td>Initial Release</td>
<td>64 bits</td>
</tr>
<tr>
<td>and Enterprise</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Grid members check the Windows version of the Microsoft servers before each synchronization. If a Microsoft server reports an unsupported version before a synchronization, the member logs an error and the synchronization fails.

Note that some Windows versions require certain updates and hotfixes installed, so the Microsoft server can synchronize with the grid member. Following are the current requirements:

- Windows Server 2003, Enterprise x64 Edition requires the installation of security update 935966.
- Windows Server 2008 R2 requires the hotfix referenced in the Knowledge Base article 981776.
- Windows Server 2008-based DNS servers might not display delegations for reverse lookup zones. For information about this issue, including the available hotfix, refer to Knowledge Base article 958190.

For information about the updates, enter their IDs in the Search field of the Microsoft Support website at http://support.microsoft.com.

Administrative Permissions

By default, only superusers can configure grid members to manage Microsoft servers. Superusers can give limited-access users read-only or read/write permission to Microsoft servers. Read-only permission allows admins to view the properties and data of a Microsoft server from Grid Manager. Write permission is required to configure grid members to manage Microsoft servers, edit their properties, and start or stop their DNS and DHCP services. For additional information, see Administrative Permissions for Microsoft Servers on page 114.

Note that to view and manage the DNS and DHCP data synchronized from Microsoft servers, admins must have permissions to the applicable DNS and DHCP resources. For example, to view DNS zones synchronized from Microsoft servers, admins must have read-only permission to zones, and to edit the zones, admins need read/write permission to them. Similarly, to view DHCP ranges synchronized from Microsoft servers, admins must have read-only permission to DHCP ranges, and to edit the DHCP ranges, admins need read/write permission to the DHCP ranges. For information, see Administrative Permissions for DNS Resources on page 116 and Administrative Permissions for DHCP Resources on page 121.

The administrative permissions on the grid are different from those on the Microsoft server. These permissions are independent of each other and are not synchronized.
Deployment Guidelines

Following are some recommendations and considerations when configuring grid members to manage Microsoft servers:

- Infoblox recommends that you schedule the initial synchronization at a time when your network is less busy, especially if you are synchronizing a large amount of data. In addition, if a Microsoft server reconnects after being disconnected for a long period of time, it could synchronize a significant amount of data and this could impact the grid master performance.

- vNIOS grid members and grid members running on Infoblox-250 and Infoblox-250-A appliances do not support being configured as managing members.

- The managing member must be close, in terms of network hops, latency and bandwidth, to the Microsoft servers that it manages. This will help reduce the synchronization time and potential retries due to network delays.

- Although a grid member that manages Microsoft servers can run other protocols and services, to optimize performance, Infoblox recommends that you configure one or more members solely for managing Microsoft servers.

  If you are considering running other protocols and services on a managing member, consider using a member that is running on a platform other than the Infoblox-550-A.

- Grid members connect to Microsoft servers using RPC calls over TCP/IP. You must adjust your firewall policies to allow traffic between the managing grid member and its assigned Microsoft servers. Grid members use the VIP as their source port. In Windows Server 2003, RPC uses the dynamic port range 1025-5000, by default. In Windows Server 2008, RPC uses the dynamic port range 49152-65535, by default. You can reduce the number of available ports as follows:

  - In Windows Server 2003, use the rpccfg.exe tool. For information, refer to http://support.microsoft.com/kb/908472.
  - In Windows Server 2008 and later, use the netsh tool. For information, refer to http://support.microsoft.com/kb/929851.

  The minimum number of ports required in the range is 255.

  Note that TCP port 445 must be open on the Microsoft server, in addition to the dynamic port range. Port 445 is used by the port mapper interface, which is a service on the Microsoft server that provides information to clients on which port to use to connect to a specific service, such as the service that allows the management of the DNS service.

- The capacity of the managing member must be greater than or equal to the sum of all its assigned Microsoft servers.

- The capacity of the grid master must be greater than or equal to the sum of all managed Microsoft servers.

- A Microsoft server can synchronize its data to only one network view, and for DNS data, only one DNS view.

- Multiple Microsoft servers can synchronize their data into the same network view and DNS view, unless there is a conflict in their data. For example, two Microsoft servers in different locations could serve the same private IP address space, such as 10.1.0.0/16, or serve reverse-mapping zones with the same name, such as 10.in-addr.arpa. Synchronizing their data to the same network view and DNS view would cause conflicts which result in the grid member synchronizing the data of only one Microsoft server and logging an error for the other Microsoft server. In such situations, Infoblox recommends that you synchronize each Microsoft server to a different network view and DNS view to ensure that data from both servers are synchronized.
Configuring Members to Manage Microsoft Servers

Any grid member, including the grid master and grid master candidate, can manage Microsoft DNS and DHCP servers. If the grid master and grid master candidate both manage Microsoft servers and the master candidate is promoted to grid master, the Microsoft server assignments remain the same. Microsoft servers that were assigned to the demoted grid master remain assigned to the demoted grid master. Microsoft servers that were assigned to the promoted grid master remain assigned to the promoted grid master.

When an HA pair manages Microsoft servers, the active node handles synchronization. If an HA failover occurs during a synchronization, the failing node immediately aborts the synchronization. The new active node resumes the next synchronization. Changes that occurred on the grid since the end of the last synchronization are lost.

Complete the following tasks to configure a grid member to manage a Microsoft server:

1. On the Microsoft server, create a user account for the grid member. For information, see Setting Microsoft Server Credentials.
2. On the grid master, configure the managing member, as described in Configuring a Managing Member.

Setting Microsoft Server Credentials

To enable a grid member to synchronize data with a Microsoft server and control DNS and DHCP services, you must do the following on the Microsoft server:

1. Create a user account for the grid member.
2. Grant the user account the necessary permissions.
   - You can either add the user account to the Administrators Group or add the user account to specific groups and explicitly set only the permissions necessary to access the DHCP and DNS services of the Microsoft server. The following sections provide general instruction on each method. For more detailed information, refer to the Microsoft documentation or contact Microsoft Technical Support.

Adding the User Account to the Administrators Group

Adding the user account of the grid member to the Administrators Group provides total control over the AD domain. Do one of the following:

- If the managed Microsoft server is a standalone server or a member server in a domain, open Computer Management, click Groups, and add the user account to the Administrators Group.
- If the managed Microsoft server is a domain controller, open Active Directory Users and Computers, select the domain name, click Built-in, and add the user account to the Administrators Group.
Setting Specific Group Memberships and Permissions

If your security policy precludes adding user accounts to the Administrators group, you can add the user account to individual groups and grant only the required permissions. For guidelines and more information, see the following:

http://support.microsoft.com/kb/325349
http://support.microsoft.com/kb/914392

To add the user account of the grid member to individual groups and grant specific permissions:

- To enable the member to synchronize DNS data with the Microsoft server, add its user account to the DnsAdmins Group.
- To enable the member to synchronize DHCP data with the Microsoft server, add its user account to the Dhcp Administrators Group.
- To enable the grid member to monitor, start, and stop the DNS and DHCP services, grant the user account permissions on the Service Control Manager (SCM), as follows:
  1. Grant permissions to the SCM on each managed Microsoft server. For more information, refer to http://support.microsoft.com/kb/907460.
  2. Grant permissions to the DNS and/or DHCP service on each managed server by doing one of the following:
     - Use the sc command line utility to remotely configure each managed DNS or DHCP server. For additional information, refer to http://technet.microsoft.com/en-us/library/dd187143.aspx
       Note that you need to know the SID of the user account and its current permissions. You can retrieve the SID of the user account by using the dsquery and dsget commands.
     - Use the Domain Controller Policy editor to define a global policy that applies to all DNS or DHCP services running in a domain or on domain controllers. For additional information, refer to http://support.microsoft.com/kb/324802.

Configuring a Managing Member

When you configure a member to manage Microsoft servers, you must specify the following:

- The management mode of the Microsoft server. For information, see Setting the Management Mode on page 733.
- A network view, if there is more than one in the grid, and a DNS view, if there is more than one in the network view. For information, see Synchronizing to a Network View and DNS View on page 733.

For the steps on configuring the managing member, see Assigning Grid Members to Microsoft Servers on page 733.
Configuring Members to Manage Microsoft Servers

Setting the Management Mode

A grid member can manage a Microsoft server in read-only mode, which is the default, or in read-write mode. In read-only mode, the grid member copies the DNS and DHCP data from the Microsoft server to the grid so Grid Manager admins can view the synchronized data. They cannot update the data, control the DNS and DHCP service of the Microsoft server, or configure any properties.

In read/write mode, Grid Manager admins are allowed to update the data of the Microsoft server. Therefore during each synchronization, the grid member applies changes from the grid to the Microsoft server and vice versa. Read/Write mode also allows admins to control DNS and DHCP services of the Microsoft server and configure some of their properties.

Note that the management mode of a Microsoft server is separate from the admin permissions that the appliance requires to access the Microsoft servers and DNS and DHCP resources. An admin must still have the applicable permissions to the Microsoft servers and DNS and DHCP resources they want to access. For information on admin permissions, see Administrative Permissions for Microsoft Servers on page 114.

Synchronizing to a Network View and DNS View

A grid has one system-defined default network view, which contains a system-defined default DNS view. A network view is a single routing domain with its own networks and shared networks. A DNS view contains a version of DNS data that it can serve to specified clients. Admins can create additional network views and DNS views, according to their business needs. For information about network views, see About Network Views on page 591. For information about DNS views, see Chapter 14, DNS Views, on page 391.

A Microsoft server can synchronize its data to only one network view and one DNS view. If a grid contains the default network view and DNS view only, Grid Manager automatically assigns Microsoft servers to these default views. If a grid has more than one network view, you must select one for the Microsoft server to synchronize its data; and if there are multiple DNS views, you must select one as well. You cannot modify the assigned network view or DNS view of a Microsoft server after its data has been synchronized. Instead, you must remove the Microsoft server and then add it again. For information about removing a server, see Removing a Managed Microsoft Server on page 737.

Microsoft servers do not support network views and DNS views. Therefore, network view and DNS view properties have no effect on the DNS and DHCP data synchronized from Microsoft servers.

Assigning Grid Members to Microsoft Servers

To configure a grid member to manage one or more Microsoft servers:

1. From the Grid tab -> Microsoft Servers tab, click the Add icon.
2. In the Add Microsoft Server(s) wizard, complete the following and click Next:
   - **Managing Member**: Click Select Member and select the grid member that manages the Microsoft servers. The default is the grid master.
   - **Synchronization Interval**: The default synchronization interval is two minutes. This is the time between the completion of one synchronization and the start of a new one. Synchronizing large data sets could take longer than the synchronization interval, causing a delay in the start of the next synchronization. For example, if the synchronization interval is two minutes but a synchronization takes five minutes, the time between the start of the first synchronization and the start of the next one is approximately seven minutes.
   - **Credentials to Connect to the Microsoft Server(s)**: Enter the login name and password that the appliance uses to connect to the Microsoft servers. These must be the same as those you specified when you created the user account for the grid member on the Microsoft servers. Note that you might have to specify the domain name and the user name in the following format: domain_name\user_name
   - **Manage Server(s) in**: Select the management mode, which is either Read-only or Read/Write.
   - **Synchronize Data into Network View**: This field appears only when there is more than one network view in the grid. Specify to which network view the data from the Microsoft servers is synchronized.
   - **Synchronize DNS Data into DNS View**: This field appears only when there is more than one DNS view in the network view. Specify to which DNS view the data from the Microsoft servers is synchronized.
   - **Comment**: You can enter additional information about the servers.
— **Disable**: Select this to disable the Microsoft servers. This allows you to preprovision the Microsoft servers and then enable them at a later time.

3. Do the following in the Managed Servers table:
   — **Name or IP Address**: Enter either the FQDN or IP address of the Microsoft server. If you enter an FQDN, the member first resolves the FQDN to the IP address and uses the resolved IP address to connect to the Microsoft server. The member resolves the FQDN by sending a DNS query to the DNS resolver specified in the DNS Resolver tab of the Member Properties editor.
   
   — **DNS**: Select this option to enable the grid member to manage the DNS service and synchronize DNS data with this server. Clearing this check box disables DNS service management and data synchronization. This allows you to preprovision specific Microsoft servers and then enable them at a later time.
   
   — **DHCP**: Select this option to manage the DHCP service of the Microsoft server and synchronize DHCP data with this server. Clearing this check box disables DHCP service management and data synchronization. This allows you to preprovision specific Microsoft servers and then enable them at a later time.

You can assign multiple Microsoft servers to a grid member. Click the Add icon to add another Microsoft server.

4. Select one of the following:
   — **Next**: Continue to the next step and define extensible attributes for the Microsoft servers. For information, see *Using Extensible Attributes* on page 225.
   
   — **Save & Close**: Save the entry and close the wizard.
   
   — **Save & New**: Save the entry and configure another grid member to manage Microsoft servers.

After you configure a grid member to manage a Microsoft server, the member automatically connects to the Microsoft server and starts synchronizing data. You can then do the following:

- View the status of the servers in the **Microsoft Servers** panel, as described in *Monitoring Managed Microsoft Servers* on page 737. Newly added servers first display a status of **Connecting** as the grid member contacts the Microsoft servers. The status changes to **OK** after the grid member successfully connects to the Microsoft server.

- View the data synchronized from the Microsoft servers. To view DNS data, navigate to the DNS view you specified. For information, see *Viewing Zones* on page 440. To view DHCP data, navigate to the **Networks** tab of the network view that you specified. For information, see *Managing DHCP Data* on page 589. Network conditions and the amount of data can affect the synchronization time. Therefore, you might not be able to view all of the synchronized data immediately.

- Use Smart Folders to organize the Microsoft servers and their data. For example, you can create a folder for DNS zones and another folder for DHCP scopes synchronized from a Microsoft server. For information about Smart Folders, see *Chapter 3, Smart Folders,* on page 67.

- Update the synchronized data. For information, see *Chapter 30, Managing Microsoft DNS Services,* on page 741 and *Chapter 31, Managing Microsoft DHCP Services,* on page 757.

You can also use Global Search to search for synchronized data, such as zones and IP addresses. For information, see *Global Search* on page 43.
MANAGING MICROSOFT SERVERS

After you configure grid members to manage Microsoft servers, you can set certain properties and manage the servers as follows:

- Set server properties, as described in Setting Microsoft Server Properties.
- Change the managing member or the management mode, as described in Changing the Managing Member or Management Mode on page 736.
- Back up the synchronized data, as described in Backing Up Synchronized Data on page 736.
- Disable synchronization with a Microsoft server, as described in Disabling Synchronization on page 736.
- Remove a Microsoft server, as described in Removing a Managed Microsoft Server on page 737.

Setting Microsoft Server Properties

You can modify any of the Microsoft server properties you previously configured, except for the network view and DNS view. You can also set certain properties, including the logging level, extensible attributes, and administrative permissions. Extensible attributes and permissions apply to the data only when they are managed from Grid Manager. Extensible attributes and permissions are not synchronized to the Microsoft server.

To set the properties of a Microsoft server:

1. From the Grid tab, select the Microsoft Servers tab \textarrow{} ms_server check box, and click the Edit icon.
2. In the Microsoft Server Properties editor, you can set properties in the following tabs:
   - General: Modify the settings described in Assigning Grid Members to Microsoft Servers on page 733.
   - Logging: Select a logging level for the Microsoft server log.
     - Low: Logs only error messages.
     - Normal: Logs warning and error messages.
     - High: Logs warning, error and information messages.
     - Debug: Logs messages about all events associated with synchronization.
     See Viewing Synchronization Logs on page 739 for a description of each level.
   - Extensible Attributes: Define extensible attributes for the server. For information, see Using Extensible Attributes on page 225.
   - Permissions: Define administrative permissions that apply to the server. For information see About Administrative Permissions on page 87.
3. Click Save & Close.

You can edit the General and Logging properties of multiple Microsoft servers at the same time by selecting the Microsoft servers and clicking the Edit icon. When Grid Manager displays the Microsoft Server Properties editor, it displays the values that the Microsoft servers have in common. If a property has multiple values, it indicates this. You can then change any of the values and when you click Save, Grid Manager applies your changes to all the selected Microsoft servers.
Changing the Managing Member or Management Mode

You can change the managing member and the management mode of a Microsoft server.

If you change the managing member, the previous member aborts any ongoing synchronization, and the newly assigned member resumes the synchronization process.

If you change the management mode of a Microsoft server from read/write to read-only, the grid member reverts any changes that were made from Grid Manager since the last synchronization. For example, an admin adds a network and DHCP range for a scope. If another admin changes the management mode of the Microsoft server to read-only before the next synchronization, the grid member deletes the network and DHCP range at the next synchronization.

To change the member or management mode:
1. From the Grid tab, select the Microsoft Servers tab -> ms_server check box, and click the Edit icon.
2. In the Microsoft Server Properties editor, select the General tab and do any of the following:
   — Managing Member: Click Select Member and select another grid member.
   — Manage Server(s) in: Select either Read-only or Read/Write.
3. Click Save & Close.

Backing Up Synchronized Data

When you back up the grid, it includes all managed Microsoft data. If you restore a backup, the data is restored on the grid only. It is not synchronized to the Microsoft servers. When the grid member synchronizes the data after the restore operation, it overrides the data on the grid with the data from the Microsoft servers. For information about backing up and restoring data, see Chapter 9, Managing NIOS Software and Configuration Files, on page 273.

Disabling Synchronization

When you set the disable option, the grid member completes any on-going synchronization and does not start a new one. Setting this option only affects data synchronization and does not affect the operations of the Microsoft server. Synchronization resumes when the Microsoft server is re-enabled.

To disable a Microsoft server:
1. From the Grid tab, select the Microsoft Servers tab -> ms_server check box, and click the Edit icon.
2. In the General tab, select the Disable option.
3. Click Save & Close.
Removing a Managed Microsoft Server

When you remove a Microsoft server from the grid, the managing member stops any on-going synchronization and does not start a new one. If the Microsoft server served DNS, the synchronized DNS data remains unchanged in the grid. If the Microsoft server served DHCP, then Grid Manager deletes all the DHCP ranges, leases, and fixed addresses associated with the server. It also deletes networks that were assigned only to the Microsoft server. It does not delete a network if it was assigned to other Microsoft servers as well.

Removing a managed Microsoft server from the grid does not affect the operations of the Microsoft server.

To remove a managed server:
1. From the Grid tab, select the Microsoft Servers tab → ms_server check box, and click the Delete icon.
2. When the Delete Confirmation dialog box appears, click Yes.

For information about how removing a Microsoft server affects the synchronized DNS and DHCP data, see Disabling and Removing Microsoft DNS Servers on page 755 and Disabling and Removing Microsoft DHCP Servers on page 773.

Monitoring Managed Microsoft Servers

You can monitor the status of managed Microsoft servers from the Dashboard and from various panels in the Grid tab. Grid Manager also maintains a log for each managed Microsoft server. You can monitor Microsoft servers and their services as follows:

- You can view the Microsoft Servers Status widget on the Dashboard. For information, see Microsoft Servers Status Widget on page 65.
- You can view the status of Microsoft servers. For information, see Viewing the Status of Servers on page 737.
- You can view the logs of the Microsoft servers. For information, see Viewing Synchronization Logs on page 739.

Viewing the Status of Servers

You can view details about the managed Microsoft servers by navigating to the Grid tab → Microsoft Servers tab. For each Microsoft server, the panel displays the following by default:

- **Name**: The FQDN of the Microsoft server
- **Status**: The connection status, which can be one of the following:
  - **Running**: The grid member is connected to the Microsoft server.
  - **Connecting**: The grid member is connecting to the Microsoft server.
  - **Error**: The grid member failed to connect to the Microsoft server. Check the Microsoft log for any messages to determine the reason for the failure.
  - **Unknown**: The Microsoft server is disabled. The grid member does not try to connect to disabled servers.
- **IP Address**: The IP address of the Microsoft server
• **DNS**: The status of the DNS service on the Microsoft server. The status icon can be one of the following:

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

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

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

• **Comment**: Displays any comments that were entered for the Microsoft server.
• **Site**: Displays any values that were entered for this pre-defined attribute.

You can add the following columns for display:
• **Version**: The Windows version of the managed server.
• **Managing Member**: The hostname of the grid member that manages the server.

You can click **Toggle Synchronization Status View** to display the synchronization status of each managed server. The **Status** column changes to **Synchronization Status** and there is an additional column, **Last Seen**.

• **Synchronization Status**: Displays the synchronization status as follows:
  — **Running**: The Microsoft server is synchronizing data with the grid member.
  — **Connecting**: The grid member is trying to connect to the server.
  — **Error**: Synchronization failed between the member and server. You can check the messages in the Microsoft server log to determine the reason for the failure.

• **Last Seen**: The time of the last synchronization.

You can also do the following:
• Add Microsoft servers.
  — Click the Add icon.
• Edit the properties of a Microsoft server.
  — Click the check box beside a server, and then click the Edit icon. For information, see *Setting Microsoft Server Properties* on page 735.
• Delete a Microsoft server.
  — Click the check box beside a server, and then click the Delete icon. For information, see *Removing a Managed Microsoft Server* on page 737.
• Manage DNS and DHCP services of a Microsoft server.
  — Click the check box beside a server, and then click the Manage Server Services icon to view the service status. You can mouse over the DNS and DHCP service icons and click the Start/Stop service icon to start or stop a service, or click the Edit Service icon to edit the service properties. For information about setting DHCP server properties, see Setting Microsoft DHCP Server Properties on page 772. For information about setting DNS server properties, see Specifying Forwarders for Microsoft Servers on page 754.
• View detailed server status information, as described in Viewing Detailed Status Information on page 739.
• Export the list of Microsoft servers to a .csv file.
  — Click the Export icon.
• Print the list of Microsoft servers.
  — Click the Print icon.

Viewing Detailed Status Information

You can view more status information by selecting a server from the Microsoft Servers panel and clicking the Detailed Status icon. The Detailed Status panel displays the following Information:

• **Synchronization Status**: The status icon indicates the synchronization status as follows:
  — Green: The Microsoft server is synchronizing data with the grid member.
  — Red: Synchronization failed between the member and server. You can check the messages in the Microsoft server log to determine the reason for the failure.
• **Last Seen**: The time of the last synchronization.
• **DNS Service Status**: For information about the status icons, see Viewing the Status of Servers on page 737.
• **DNS Service Last Changed**: The date and time of the last DNS status update.
• **DHCP Service Status**: For information about the status icons, see Viewing the Status of Servers on page 737.
• **DHCP Service Last Changed**: The date and time of the last DHCP status update.

Viewing Synchronization Logs

Grid Manager maintains a synchronization log file for each Microsoft server managed by a grid member. It logs events related to the synchronization process, depending on the logging level that you configured in the Logging tab of the Microsoft Server Properties editor described in Setting Microsoft Server Properties on page 735.

The log files are rotated and compressed once they reach 40MB.

To view the log file of managed Microsoft server:

1. From the Administration tab, select the Logs tab -> Microsoft Logs tab.
2. If there is more than one managed server in the grid, you can select the Microsoft server whose logs you want to view.
3. The log file contains information related to the synchronization of the Microsoft DNS and DHCP data, as follows:
   • **Timestamp**: The date and time of the log message. The time zone is the time zone configured in the User Profile.
   • **Source**: Identifies the event that generated the message, such as a server synchronization or zone synchronization.
   • **Level**: Indicates the severity of the message, which can be one of the following:
     — **Debug**: Provides information about all events associated with synchronization.
     — **Information**: The grid member is synchronizing with the Microsoft server and these messages provide normal status information.
— **Warning:** The grid member synchronized the data, but there was an issue, which is detailed in the Message section.

If the grid member encounters an error during the synchronization, it skips the object with the error, logs the error in the Microsoft log, and continues to synchronize the rest of the data. The grid member logs the error at each synchronization until you resolve the issue and it can synchronize the object successfully.

— **Error:** The grid member failed to synchronize an object, such as a DNS zone or DHCP scope, due to the error described in the Message section.

- **Object Type:** The type of object that corresponds to the entry, such as FQDN or ADDRESS.
- **Object Name:** The name of the object that corresponds to the entry
- **Message:** Detailed information about the event.

You can also do the following in the log viewer:

- Toggle between the single line view and the multi-line view.
- Navigate to the next or last page of the file using the paging buttons.
- Refresh the view.
- Click the Follow icon to have the appliance automatically refresh the log every five seconds.
- Download the log.
- Clear the contents of the log.
- Export or print the content of the log.
Chapter 30 Managing Microsoft DNS Services

This chapter provides guidelines for using Grid Manager to manage Microsoft DNS servers and for synchronizing DNS data between Microsoft servers and the grid. It discusses some features of the Microsoft DNS servers only as they relate to the synchronization of data. Please review the Microsoft documentation for complete information about Microsoft DNS servers and their features.

In addition, if you encounter technical issues with your Microsoft DNS servers, contact Microsoft Technical Support or consult the Microsoft Support site at http://support.microsoft.com/. Some Windows versions require certain updates and hotfixes installed, so the Microsoft server can synchronize with the grid member. For information about these requirements, see Requirements on page 729.

The topics in this chapter include:

- Managing Microsoft DNS Servers on page 742
  - Synchronizing DNS Data on page 742
  - Synchronizing with Multiple Servers on page 743
- Managing Synchronized DNS Data on page 744
  - Adding Zones to Microsoft Servers on page 745
  - Setting Zone Properties on page 746
  - Deleting and Restoring Synchronized Zones on page 747
  - Managing Resource Records in Synchronized Zones on page 748
- Synchronizing Updates on page 750
  - Synchronizing AD-Integrated Zones on page 753
  - Resolving Conflicts on page 753
- Viewing Members and Managed Servers on page 754
- Specifying Forwarders for Microsoft Servers on page 754
- Disabling and Removing Microsoft DNS Servers on page 755
Managing Microsoft DNS Servers

After you configure a grid member to manage a Microsoft DNS server, the grid member connects to the Microsoft server and starts synchronizing DNS data from the Microsoft server to its database. First, it synchronizes the Microsoft server properties and its list of zones. Then it synchronizes each zone individually, including its properties and resource records.

The synchronization time varies, depending on different factors, such as the number of managed Microsoft servers and the amount of data being synchronized. The synchronized data is then replicated to the grid master through the grid replication process.

If the server is managed in read/write mode, admins can update the synchronized DNS data, control the DNS service of the server and specify forwarders for it as well.

Synchronizing DNS Data

Grid members synchronize the properties and resource records of the following types of DNS zones:

- Authoritative forward-mapping zones
- IPv4 and IPv6 reverse-mapping zones
- Stub zones
- Delegations
- Active Directory-integrated zones

Grid members synchronize most of the resource records supported by Microsoft servers, except for WINS, WINSR, and ATMA records. They synchronize all the resource records supported by Infoblox DNS servers, as well as unsupported records, such as ISDN and X25 records. You can view the unsupported records in Grid Manager and delete them, but you cannot edit them. Note that Grid Manager and Microsoft DNS servers display some resource records, such as SIG records, in a different format.

Grid members do not synchronize the following DNS zones supported by Microsoft servers:

- Forwarding zones
- Cached zones
- Root zone
- 0.in-addr.arpa
- 127.in-addr.arpa
- 255.in-addr.arpa
- TrustAnchors

You cannot use Grid Manager to create the unsupported zones and assign them to a Microsoft server. Any zone on the grid that has the same name as a forwarding, cached or root zone on the Microsoft server is not synchronized. In addition, grid members do not synchronize the contents of a zone if the Microsoft server is a secondary server.

Subdomains defined within a Microsoft DNS zone are not synchronized unless they contain at least one resource record. For example, in the corp100.com zone, any resource record defined in a subdomain of the corp100.com zone is synchronized. If the subdomain sub.corp100.com zone has no resource record, it is not synchronized.

The following zones and resource records are supported on Microsoft servers running Windows Server 2008 only. Therefore, grid members can only synchronize these DNS zones and resource records with Microsoft servers running Windows Server 2008.

- IPv6 reverse-mapping zones
- Global Names zones
- DNAME records
- NAPTR records
- DNSSEC records
Synchronizing with Multiple Servers

Because a grid member can manage multiple Microsoft servers, it could potentially manage multiple servers assigned to the same zone. For example, a grid member could manage a Microsoft server that is the primary server of a zone and one or more Microsoft servers that are secondary servers of the same zone. It could also manage multiple Microsoft servers that are secondary servers for the same zone.

If a grid member manages the primary server and at least one secondary server of a zone, the grid member always synchronizes DNS data with the primary server only. It never synchronizes data with the secondary server, even if the primary server fails.

If a grid member manages several Microsoft servers that are secondary servers of the same zone, it synchronizes DNS data as follows:

- If each Microsoft server is assigned to a different DNS view, the grid member synchronizes data with each one.
- If the Microsoft servers are synchronized to the same DNS view, the grid member selects a principal server for synchronization purposes, as follows:
  - The first Microsoft server that is assigned as the DNS secondary server is designated principal server.
  - If the secondary servers are managed in read-only and read/write modes, the grid member always selects a server that is managed in read/write mode.
  - If a Microsoft server fails three successive synchronizations, it loses its principal server status. The grid master checks the date that each server last became a principal server and selects the server that has not been the designated principal server the longest.

Note that a grid member could fail to synchronize with a Microsoft server due to errors, such as a disabled account or an expired password. In these situations, the failure count is reset and is not increased. This prevents the Microsoft server from losing its master status to another Microsoft server that could experience the same errors.

When a zone is served by multiple Microsoft servers, the MS Sync Master column of the Zones tab shows which Microsoft server is actually performing the synchronization of that zone with the grid.
Managing Synchronized DNS Data

When grid members are configured to manage Microsoft servers in read/write mode, you can use Grid Manager to view, edit and delete the DNS data of those servers. You can add new zones and assign them to a Microsoft server. You can modify the properties of zones synchronized from the Microsoft server and edit their resource records as well. All updates are synchronized to the Microsoft servers at regular intervals.

The following sections provide guidelines for managing the zones and resource records served by Microsoft servers:

- Adding Zones to Microsoft Servers on page 745
- Setting Zone Properties on page 746
- Deleting and Restoring Synchronized Zones on page 747
- Managing Resource Records in Synchronized Zones on page 748

Synchronized zones also support the following features:

- You can import data to zones synchronized with Microsoft servers. Note that the import fails if you try to import unsupported records to a Microsoft zone. For information about importing records, see Importing Zone Data on page 419.
- You can copy records to and from zones synchronized with Microsoft servers. When copying records to a Microsoft zone, you can copy only those records that are supported by Microsoft servers. For information about copying records, see Copying Zone Records on page 397.
Adding Zones to Microsoft Servers

From Grid Manager, you can create zones and assign Microsoft servers as their primary or secondary servers. The managing grid member then synchronize these zones to the appropriate Microsoft servers.

From Grid Manager, you can add the following types of zones to Microsoft servers:

- Authoritative forward- and reverse-mapping zones—For information, see Configuring Authoritative Zones on page 404.
- Forward- and reverse-mapping stub zones—For information, see Configuring Stub Zones on page 432.
- Delegations—For information, see Configuring a Delegation on page 427.

Note that you cannot add a zone on a Microsoft server and configure it to be served by an Infoblox grid member. For example, on the Microsoft server, you cannot add a zone and assign a grid member as its primary server and the Microsoft server as the secondary server. You must add such a zone from Grid Manager.

Following are guidelines for adding zones to a Microsoft server:

- The primary or secondary server of the zone must be a Microsoft server.
- If the primary server is a domain controller, you can enable the option to store the zone in Active Directory, making it an AD-integrated zone. Note that you can enable Active Directory integration only after the Microsoft server has been synchronized at least once because its AD ability is not known before the synchronization.
- You do not have to assign a grid member as the primary or a secondary server of the zone. For example, a zone can have a Microsoft server as its primary server and an external secondary server.
- The zone must be in the same DNS view to which the DNS data of the Microsoft server was synchronized. You cannot add a zone served by the Microsoft server to a different DNS view.
- The zone does not inherit the properties from the grid or from the DNS view. It uses the Infoblox-defined defaults. You can change the property values, as described in Setting Zone Properties.
- You can set certain zone properties that are not supported and synchronized to the Microsoft server. For example, you can define extensible attributes and administrative permissions. When you set these properties, they apply to the zones only when they are managed from Grid Manager.
- Infoblox does not support all the zone properties of a Microsoft DNS server. When a grid member synchronizes zones that were created on Grid Manager to the Microsoft server, the zones contain default values for all unsupported properties.
- If you set the Disable option, the zone status is set to “Paused” on the Microsoft server. A zone in a “Paused” status is not served to DNS clients, nor is it available for zone updates.
- Setting the Disable option does not stop synchronization. Grid members synchronize disabled zones.
- The member learns the Windows version of the Microsoft server after its first successful synchronization. Certain zones and resource records are dependent on a specific Windows version. You cannot assign these zones to Microsoft servers whose versions are unknown or insufficient.
- If the member is a secondary server for a zone with a Microsoft primary server, the member obtains the zone data through DNS zone transfers from the Microsoft primary server; not through synchronizations. This ensures that the zone data is always current on the Infoblox secondary server, as it does not have to wait for synchronizations to update its data.

In addition, superusers can add managed Microsoft DNS servers to name server groups. A name server group is a collection of one primary server and one or more secondary servers which you can assign to serve authoritative forward-mapping and reverse-mapping zones. For information about name server groups, see Using Name Server Groups on page 417.
Setting Zone Properties

When the primary server of a zone is a Microsoft server, it does not inherit its properties from the grid. Zones that are synchronized from a Microsoft server retain their original properties. Zones that Grid Manager admins create assume the Infoblox-defined default values.

To modify the properties of a synchronized zone:

1. From the Data Management tab, select the DNS tab -> Zones tab -> DNS_view-> zone check box and click the Edit icon.
2. In the Authoritative Zone editor, you can do the following in each tab:
   - General: You can add or edit comments, and set the Disable and Lock options. Setting the Disable option sets the status of the zone to “Paused” on the Microsoft server. Grid members synchronize disabled zones to Microsoft servers.
   - Name Servers: You can modify the name servers assigned to the zone. For information, see Assigning Zone Authority to Name Servers on page 411.
   - Settings: If the zone was synchronized from a Microsoft server, this tab displays the original settings from the Microsoft server. If the zone was created using Grid Manager, then it inherits the TTL values from the grid. Note that these values might be different from those on the Microsoft server. To change any of these values, see Configuring DNS Service Properties on page 480.
   - Zone Transfers: In this tab, you specify the servers to which zone transfers are allowed. For information about zone transfers, see Enabling Zone Transfers on page 491. Set the following parameters, depending on whether the primary or secondary servers of the zone are Infoblox or Microsoft DNS servers:
     - If the primary server is an Infoblox, Microsoft or external primary and the secondary servers are both Infoblox and Microsoft DNS servers, this tab displays two separate tables where you can specify zone transfer settings for the Infoblox DNS servers and the Microsoft DNS servers.
     - Zone Transfer Settings for Infoblox Members: Specify the settings as described in Configure Zone Transfers on page 491.
     - Zone Transfer Settings for Microsoft Servers: You can set zone transfers to one of the following:
       - None: Does not allow zone transfers to any name server.
       - Any: Allows zone transfers to any IP address.
       - Any Name Server: Allows zone transfers to any name server in the Name Servers table.
       - Address: Allows zone transfers to the IP address that you specify.
     - If the primary server is an Infoblox, Microsoft or external primary and the secondary servers are both Infoblox and Microsoft DNS servers, this tab displays two separate tables where you can specify zone transfer settings for the Infoblox DNS servers and the Microsoft DNS servers.
     - Zone Transfer Settings for Infoblox Members: Specify the settings as described in Configure Zone Transfers on page 491.
     - Zone Transfer Settings for Microsoft Servers: You can set zone transfers to one of the following:
       - None: Does not allow zone transfers to any name server.
       - Secure Only: This appears only if the zone is AD-integrated. The zone accepts GSS-TSIG-signed updates only.
       - Nonsecure and Secure: The zone accepts both nonsecure and GSS-TSIG-signed updates.
   - Updates: In this tab, you specify whether the zone can accept dynamic DNS updates. For information about dynamic DNS updates, see Chapter 18, Configuring DDNS Updates from DHCP, on page 501. If the primary server is a Microsoft server, regardless of the secondary servers, the Updates tab displays the following:
     - Dynamic Updates: Select one of the following:
       - None: The zone does not accept dynamic updates.
       - Secure Only: This appears only if the zone is AD-integrated. The zone accepts GSS-TSIG-signed updates only.
       - Nonsecure and Secure: The zone accepts both nonsecure and GSS-TSIG-signed updates.
— **Active Directory:**
  
  — **Automatically create underscore zones:** This option allows the appliance to create the following subzones that the DNS server must have to answer AD-related DNS queries:
    
    `_msdcs.zone`
    `_sites.zone`
    `_tcp.zone`
    `_udp.zone`
    `domaindnszones.zone`
    `forestdnszones.zone`

    Note that these zones are automatically generated. You cannot edit these zones or import data into them. They cannot be modified, thus providing protection against forged updates.

  • **Extensible Attributes:** Extensible attributes apply to the zones only when they are managed from Grid Manager. For information, see *Using Extensible Attributes* on page 225.

  • **Permissions:** These permissions apply to Infoblox Grid Manager administrators only. For information, see *About Administrative Permissions* on page 87.

### Deleting and Restoring Synchronized Zones

When you delete a synchronized zone from the grid, Grid Manager moves the zone and its resource records to the Recycle Bin. It deletes the zone and its resource records from the Microsoft server at the next synchronization.

Note that if you delete a zone on Grid Manager and plan to add it back to the database with different properties or resource records, ensure that you wait until after the deletion is synchronized to the Microsoft server to add the new zone. Otherwise, if you delete a zone and add a new zone with the same name within a synchronization interval, Grid Manager will synchronize the zone properties and resource records from the Microsoft server to the newly added zone on Grid Manager.

If a zone has subzones, you can choose to remove them and their resource records or “reparent” them to the parent zone of the one you are removing. For information, see *Removing Zones* on page 423.

If you restore deleted zones from the Recycle Bin, the grid member restores it on the Microsoft server as well. For information, see *Restoring Zone Data* on page 425.
Managing Resource Records in Synchronized Zones

From Grid Manager, you can add and edit resource records in zones served by Microsoft servers. For information about adding and managing resource records, see Managing Resource Records on page 451. You can also use IP Map and the IP List to track A, AAAA and PTR records that are synchronized from Microsoft servers. For information, see Chapter 32, IP Address Management, on page 777.

Microsoft DNS servers support all the resource records supported by Infoblox DNS servers, except for hosts, bulk hosts and shared record groups. You cannot add these records to zones served by Microsoft servers or assign zones with these records to Microsoft servers.

Following are guidelines for adding and managing resource records in synchronized zones:

- Infoblox DNS servers support defining a naming policy for the hostnames of A, AAAA, MX, and NS records based on user-defined or default patterns. For information, see Specifying Hostname Policies on page 499. The hostname policy applies only when records are created from Grid Manager. Resource records that originate from the Microsoft server are synchronized to the grid member even if they do not comply with the hostname policy of the grid member. The policy is enforced only if you edit the resource record from Grid manager.

- When you create an A or AAAA resource record on the NIOS appliance with the option to automatically create the corresponding PTR record, Grid Manager uses the deepest reverse zone that can hold the record. For example, a grid has the following reverse zones: 10.in-addr.arpa, 0.10.in-addr.arpa, and 0.0.10.in-addr.arpa. When you create the A record www A with the IP address 10.0.0.1, Grid Manager creates a PTR record in the zone 0.0.10.in-addr.arpa. If the deepest zone does not allow the creation of the PTR record, Grid Manager creates the A record, but not the PTR record, and displays a warning.

- You can add and edit DNAME records in a DNS zone assigned to a Microsoft server running Windows 2008. You cannot add or edit DNAME records in zones assigned to Microsoft servers running earlier Windows versions.

- You can disable synchronized resource records from Grid Manager. When you disable a resource record, it is removed from the Microsoft server at the next synchronization.

- If you add a resource record with invalid data from Grid Manager, such as a DNAME record with an alias name that has special characters, the invalid resource record is not synchronized to the Microsoft server and is eventually deleted from the grid. The error is logged in the Microsoft log.

- If the zone of the resource record was created using Grid Manager, then it and all its resource records inherit their TTL values from the grid. Note that these values might be different from those on the Microsoft server. You can change these values to match those on the Microsoft server. For information on changing these values, see Configuring DNS Service Properties on page 480.

- Grid Manager and Microsoft DNS servers display TXT records differently.
  
  On Grid Manager, you enter the text string of TXT records as defined in RFC 1035. You can enter the following:
  
  - A contiguous set of characters without spaces. If you enclose the characters in double quotes, Grid Manager displays the character string without the double quotes. For example, if you enter "abcdef", Grid Manager displays abcdef.
  
  - A string that contains any character, including spaces, enclosed in quotes.
    
    - If the string contains a quote ("), you must precede it with a backslash.
    
    - If you enter a text string with multiple spaces between each word and the string is not enclosed in double quotes, Grid Manager displays the text string with a single space between each word. For example, if you enter text string, the GUI displays text string. To preserve multiple spaces, enclose the string in double quotes.

  Unlike on Microsoft DNS servers, you cannot enter a text string on multiple lines in Grid Manager. However, each contiguous set of characters or quoted string entered on Grid Manager is equivalent to a separate line entered on a Microsoft DNS server.
On a Microsoft DNS server, you can enter text without quotes and with each line on a separate line. Microsoft DNS servers then display the text in a brief format where the lines are separated by a comma and a space. For example, if you enter the following in the Text field of the TXT Record wizard or editor on Grid Manager:

"this is a line""with another line""and a third one"

It is served by the Microsoft and Infoblox DNS servers as:

"this is a line""with another line""and a third one"

But it is displayed in the Microsoft DNS server as:

this is a line, with another line, and a third one
Synchronizing Updates

A grid member synchronizes DNS data with each managed Microsoft server at regular intervals. Grid Manager admins with the applicable permissions can then update the synchronized DNS zones and resource records. During each synchronization, updates from Grid Manager are applied to the Microsoft server and updates from the Microsoft server are applied to the grid as well. Note that the resource records are synchronized only if there is a change to the SOA record on either the Microsoft server or the grid.

The following examples illustrate how grid members synchronize DNS data:

- If a Microsoft server admin adds the finance.corp100.com zone, it is also added to the grid after a synchronization.
- If a Grid Manager admin changes the A record of admin.corp100.com from 10.2.1.5 to 10.2.1.6, the IP address of its corresponding A record on the Microsoft server is updated to 10.2.1.6
- If a Grid Manager admin deletes a DNS zone that is assigned to a Microsoft server, the corresponding zone on the Microsoft server is deleted as well in the next synchronization.

Because admins can update DNS data from the Microsoft server and from Grid Manager, conflicts can occur during synchronization. In addition, Microsoft servers and Infoblox DNS servers have some differences in the features they support and the way they handle certain zones and resource records.

The following guidelines describe how the grid member resolves conflicts and handles any differences when DNS data is synchronized between a Microsoft server and the grid.

- On Microsoft servers, users can enter FQDNs and labels using a mix of upper and lower case characters. The servers preserve the original case when they store the data. When the grid member synchronizes data with the Microsoft server, it displays the data in lower case in Grid Manager and the Infoblox API. The case of the data is preserved as long as no change is made to the DNS zone or resource record. If a Grid Manager admin modifies a DNS zone or resource record, the next synchronization converts the object name to lower case on the Microsoft server.

- If a Microsoft server admin modifies an object that has a pending scheduled task and synchronization occurs before the scheduled task, the object is modified in both the Microsoft server and the grid member. When the scheduled task executes at its scheduled time, it fails and an error message is logged in the audit log.

- A situation could arise where two Microsoft servers in different domains are primary servers for zones with the same name. For example, two reverse-mapping zones could be named 1.1.10.in-addr-arpa in two Microsoft servers managed by the same member. If the two Microsoft servers are synchronized to different DNS views, the grid member synchronizes each one separately. If the Microsoft servers are synchronized to the same DNS view, then the grid member synchronizes the zone with the first Microsoft server. During the synchronization with the second Microsoft server, the grid member logs an error and does not synchronize the zone.

- The grid member does not synchronize the naming policy configured on Microsoft servers. Zones and resource records that fail the policy check on Microsoft servers are reported in the synchronization log file.

- When you remove a Microsoft server that is assigned to a zone, the succeeding synchronization removes the zone from the Microsoft server.

- When a Microsoft server admin and a Grid Manager admin change the same object, the grid member retains the version that exists on the Microsoft server. Following are some examples:

<table>
<thead>
<tr>
<th>Grid Manager Admin...</th>
<th>Microsoft Server Admin...</th>
<th>After Synchronization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deletes the corp100.com zone</td>
<td>Updates the corp100.com zone</td>
<td>The corp100.com zone is created on the grid with the updates and is assigned to the Microsoft server.</td>
</tr>
<tr>
<td>Changes the zone transfer settings of the sales.corp100.com zone.</td>
<td>Deletes the sales.corp100.com zone.</td>
<td>The sales.corp100.com is deleted from the grid as well.</td>
</tr>
</tbody>
</table>
• Changing the name or IP address of a resource record on the Microsoft server effectively deletes the original resource record and creates a new record with the current information. During the synchronization, the grid member also deletes the original record, including its associated properties, such as its extensible attributes and administrative permissions, and creates a new record.

For example, as shown in Figure 30.1, the A record for printer1.corp100.com is on both the Microsoft and Infoblox grid member. On the grid, the A record has extensible attributes and a comment. A Microsoft server admin changes the IP address of the A1 resource record from 10.1.1.2 to 10.1.1.3. On the Microsoft server, this is equivalent to deleting the A1 resource record with the IP address 10.1.1.2 and then adding a new A1 resource record with the IP address 10.1.1.3. When the data is synchronized, the grid member deletes the original record with its extensible attributes and comments and creates a new A record with IP address 10.1.1.3.

Figure 30.1

• If a Microsoft server admin changes the IP address of a resource record and a Grid Manager admin changes the IP address of the same resource record, they are effectively deleting the record and each creating a new one.

For example, as shown in Figure 30.2, a Microsoft server admin changes the IP address of the A resource record for printer1.corp100.com from 10.1.1.2 to 10.1.1.3, and a Grid Manager admin changes the IP address of the same resource record to 10.1.1.4. When the data is synchronized, the grid member deletes the A1 resource record with IP address 10.1.1.2 and creates an A resource record with IP address 10.1.1.3 and another A1 resource record with IP address 10.1.1.4.

Figure 30.2
• Grid members can synchronize classless IPv4 reverse-mapping zones from the Microsoft server to the grid only if the zone prefix is in one of the following formats: `<subnet>/subnet mask bit count>` or `<subnet>-<subnet mask bit count>`. For example, 128/26.2.0.192.in-addr.arpa. If the zone prefix is not in the specified format, the grid member skips the zone and logs an error message. For information, see http://technet.microsoft.com/en-us/library/cc961414.aspx.

Likewise, Grid Manager admins can add a classless IPv4 reverse-mapping authoritative or stub zone to a Microsoft server only if its prefix is in the specified format. For information about configuring classless IPv4 reverse-mapping zones in Grid Manager, see Specifying an RFC 2317 Prefix on page 406.

• Grid members synchronize DNS records that contain values that Infoblox does not support. Grid Manager admins can view these records, but they cannot edit or restore such records. For example, if a member synchronizes a NAPTR record that contains an unsupported value in the Service field, admins can view this record but they cannot edit or restore it, as long as it contains an unsupported value.

• When you configure a grid member to manage a Microsoft server that is a secondary server for a zone, and that zone is already assigned to a name server group on the grid, the name server group association is removed from the zone and its servers are explicitly defined at the zone as name servers. Therefore, after the synchronization, the DNS servers that were in the name server group are each assigned as the primary or secondary server for the zone. Additionally, the managed Microsoft server remains assigned as a secondary server for the zone.
Synchronizing AD-Integrated Zones

An AD-integrated zone can be served by multiple domain controllers, and a grid member can manage more than one of the domain controllers. If the domain controllers are configured to synchronize their DNS data to different DNS views, the grid member synchronizes DNS data with each domain controller. If the domain controllers are configured to synchronize their DNS data to the same DNS view, the member selects a principal server for synchronization purposes and synchronizes data with that principal server only. The selection of the principal server is logged, as well as when it changes. The grid member selects a principal server as follows:

- The first domain controller that is assigned as the primary server is designated principal server.
- If a domain controller fails three successive synchronizations, it loses its principal status. The grid master then checks the date that each domain controller last became a principal server and selects the one that has not been the designated principal the longest.
- If the domain controllers are managed in read-only and read/write modes, the grid member always selects the domain controller that is managed in read/write mode.

When a zone is served by multiple Microsoft servers, the MS Sync Master column of the Zones tab shows which Microsoft server is actually performing the synchronization of that zone with the grid.

The grid member periodically checks if each zone has one principal server. If it does not find a principal server for a zone, the grid member selects one among the name servers assigned to the zone. It gives priority to the server that was not the designated principal server the longest.

You can create an AD-integrated zone on Grid Manager and assign one domain controller as its primary server. If a domain controller admin adds more primary servers to the zone, they are added to the zone on Grid Manager when the zone is synchronized. If you want to delete the primary servers, you must delete all the primary servers at once. You cannot delete only a subset of the servers.

A situation could arise where two domain controllers in different AD domains are primary servers for zones with the same name. For example, two reverse-mapping zones could be named 1.1.10.in-addr-arpa in two domain controllers managed by the same member. If the two domain controllers are synchronized to different DNS views, the grid member synchronizes each one separately. If the domain controllers are synchronized to the same DNS view, then the grid member synchronizes the zone with the first domain controller. During the synchronization with the second domain controller, the grid member logs an error and does not synchronize the zone.

Resolving Conflicts

Some conflicts require intervention from an admin. For example, a grid member cannot synchronize a zone when its primary server on the Microsoft server is different from its primary server on the grid. When a grid member is unable to synchronize data due to such conflicts, it logs an error, skips the object with the error and continues synchronizing the rest of the data. You can then view the Microsoft logs to check which objects were not synchronized. If you resolve the problem, the grid member synchronizes the object on its next attempt. For information about the logs, see Viewing Synchronization Logs on page 739.
**VIEWING MEMBERS AND MANAGED SERVERS**

You can view Infoblox and Microsoft DNS servers by navigating to the Data Management tab -> DNS tab, and then selecting the Members/Servers tab. The panel displays the following information about each DNS server:

- **Name:** The hostname of the grid member or Microsoft server.
- **Status:** The status of the DNS service on the grid member or Microsoft server.
- **Comment:** Comments that were entered for the grid member or Microsoft server.
- **Site:** Values that were entered for this pre-defined attribute.
- **Address:** The IP address of the grid member or Microsoft server.

You can do the following:

- List the DNS views or zones served by the member or Microsoft server.
  - Click a grid member or Microsoft server name.
- Edit the properties of a grid member or Microsoft server.
  - Click the check box beside a grid member or Microsoft server, and then click the Edit icon. To edit the DNS properties of a grid member, see *Configuring DNS Service Properties* on page 480. To edit the DNS properties of a Microsoft server, see *Specifying Forwarders for Microsoft Servers*.
- Export the list of grid members and Microsoft servers to a .csv file.
  - Click the Export icon.
- Print the list of grid members and Microsoft servers.
  - Click the Print icon.

**SPECIFYING FORWARDERS FOR MICROSOFT SERVERS**

A forwarder is a name server to which all other name servers first send queries that they cannot resolve locally. The forwarder then sends these queries to DNS servers that are external to the network, avoiding the need for the other name servers in your network to send queries off-site. You can define a list of forwarders for each managed Microsoft server as follows:

1. From the Data Management tab, select the DNS tab -> Members/Servers tab -> ms_server check box -> Edit icon.
2. Click the Add icon and enter the IP address of the forwarder in the text field.
3. Click Save & Close.
Disabling and Removing Microsoft DNS Servers

When you disable synchronization with a Microsoft server, the managing grid member terminates any ongoing synchronization and restarts it when the Microsoft server is re-enabled. The synchronized DNS data stays in the same state until synchronization resumes. For information, see Disabling Synchronization on page 736.

When you remove a managed Microsoft server from the grid, the managing grid member terminates any ongoing synchronization and does not start a new one. Zones and their content on the Microsoft server remain in the state that existed the moment the Microsoft server was removed. The grid retains the zones that were assigned to the Microsoft server that was removed, but deletes the Microsoft server from its assigned zones as follows:

- If the Microsoft server is the only primary server and there are no other assigned servers or if the secondary server is an external secondary server, Grid Manager deletes all the server assignments.
- If the Microsoft server is the only primary server and there are grid secondary servers, an external primary is created with the FQDN and IP address of the removed Microsoft server.
- If the Microsoft server is a secondary server and there is a grid primary, an external secondary is created with the FQDN and IP address of the removed Microsoft server.
- If the Microsoft server is a server for a stub zone, the server is removed.

To remove a Microsoft DNS server:

1. From the Data Management tab, select the DNS tab -> Members/Servers tab -> ms_server check box.
2. Expand the Toolbar and click Delete.
3. Click Yes when the confirmation dialog box appears.
Chapter 31 Managing Microsoft DHCP Services

This chapter provides guidelines for using Grid Manager to manage Microsoft DHCP servers and for synchronizing DHCP data between Microsoft servers and the grid. It discusses some features of the Microsoft DHCP servers only as they relate to the synchronization of data. Please review the Microsoft documentation for complete information about Microsoft DHCP servers and their features.

In addition, if you encounter technical issues with your Microsoft DHCP servers, contact Microsoft Technical Support or consult the Microsoft Support site at http://support.microsoft.com/. Some Windows versions require certain updates and hotfixes installed, so the Microsoft server can synchronize with the grid member. For information about these requirements, see Requirements on page 729.

The topics in this chapter include:

- **Managing Microsoft DHCP Servers** on page 758
  - Synchronizing DHCP Data on page 758
  - Viewing Synchronized Leases on page 759
- **Managing Synchronized DHCP Data** on page 760
  - Adding and Managing Scopes on page 760
  - Adding Fixed Addresses/Microsoft Reservations on page 766
  - About Superscopes on page 768
- **Synchronizing Updates** on page 770
- **Managing Microsoft DHCP Servers** on page 771
  - Viewing Members and Managed DHCP Servers on page 771
  - Setting Microsoft DHCP Server Properties on page 772
  - Controlling the DHCP Service of a Microsoft Server on page 773
  - Disabling and Removing Microsoft DHCP Servers on page 773
  - Modifying DHCP Server Assignments on page 773
Managing Microsoft DHCP Servers

When you use Grid Manager to manage Microsoft DHCP servers, you can manage the DHCP data of several servers all at once. You can also use the IP address management (IPAM) tools of Grid Manager to track and manage IP address usage in your networks. For information about the IPAM features, see Chapter 32, IP Address Management, on page 777.

As shown in Table 31.1, Microsoft servers and Infoblox DHCP servers represent DHCP data differently. DHCP ranges on Infoblox DHCP servers are scopes on Microsoft servers. Fixed addresses on Infoblox DHCP servers are the same as reservations on Microsoft servers. Infoblox reservations, which are IP addresses that are excluded from DHCP, are not supported on Microsoft servers. Microsoft superscopes, which are used to group scopes, can be managed from Infoblox DHCP servers.

Table 31.1 DHCP Data in Microsoft and Infoblox DHCP Servers

<table>
<thead>
<tr>
<th>DHCP Data</th>
<th>Microsoft DHCP Servers</th>
<th>Infoblox DHCP Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address pool from which the server allocates addresses</td>
<td>Scope</td>
<td>DHCP Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range in a Network</td>
</tr>
<tr>
<td>An IP address that is always assigned to the same device</td>
<td>Reservation</td>
<td>Fixed Address</td>
</tr>
<tr>
<td>An IP address that is excluded from DHCP because a user intends to</td>
<td>Not supported</td>
<td>Reservation</td>
</tr>
<tr>
<td>configure it manually on a network device</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrative group of scopes</td>
<td>Superscope</td>
<td>Microsoft superscope</td>
</tr>
</tbody>
</table>

Note: In this chapter, reservations always refer to Microsoft reservations (Infoblox fixed addresses), unless otherwise specified.

Synchronizing DHCP Data

After you configure a member to manage the DHCP service of a Microsoft server, the grid member connects to the server and starts synchronizing IPv4 DHCP data from the Microsoft server to the grid database. It synchronizes the Microsoft server properties, leases, scopes and reservations.

The synchronization time varies, depending on different factors, such as the number of managed Microsoft servers and the amount of data being synchronized.

Note: Synchronizing IPv6 data is not supported.

When the member synchronizes a scope to the grid, it converts the scope to a DHCP range and network. For example, it converts the Microsoft scope 10.1.1.1·10.1.1.200 with a netmask of /24 to the network 10.1.1.0/24 and DHCP range 10.1.1.1·10.1.1.200 on Grid Manager. The member associates the DHCP properties of the scope, including its DHCP and Microsoft vendor options, with the DHCP range. It synchronizes the leases within the range and if configured, the exclusion range as well.
When the member synchronizes a Microsoft reservation to the grid, it converts the reservation to a fixed address and static lease on Grid Manager. It associates the DHCP properties and DHCP and Microsoft vendor options of the reservation with the fixed address record.

The grid member synchronizes superscopes to the grid as well. The grid supports Microsoft superscopes, when an MS management license is installed. For information about adding and managing superscopes in Infoblox DHCP servers, see About Superscopes on page 768.

Following are some guidelines on how a grid member synchronizes DHCP data from Microsoft servers to the grid:

- If two superscopes have the same name, but are served by different servers, the member creates two different superscopes on the grid, each appended with the Microsoft server FQDN.
- The member synchronizes all active and inactive scopes from a managed Microsoft server as long as the scopes do not conflict or include any networks currently served by a grid member. The member does not synchronize a scope if its network already exists in the grid and is served by a grid member. It can synchronize a scope if its network is included in an existing network, only if the network is not served by DHCP.
- Synchronizing scopes that are larger than /12 is not supported.
- If a grid member manages multiple Microsoft servers, it can synchronize scopes to the same network as long as they are served by different Microsoft servers and they do not overlap. If the Microsoft servers have scopes that overlap, the grid member synchronizes only one of the scopes, including its reservations. It does not synchronize the other scopes and logs an error message for each scope that is not synchronized. For information about the Microsoft logs, see Viewing Synchronization Logs on page 739.

Note that a grid member can synchronize scopes with overlapping reservations because they are served by different Microsoft servers.

You can view the synchronized data as follows:

- To view the networks of the scopes, select the Data Management tab -> DHCP tab -> Networks tab -> Networks panel. This panel displays all IPv4 networks. For information about this panel, see Viewing IPv4 Networks on page 596.
- To view the corresponding DHCP ranges and reservations, select the Data Management tab -> DHCP tab -> Networks tab, and click a network link. For information about this panel, see Viewing Network Details on page 596.

You can also use the features in the IPAM tab, such as the Net Map and IP Map, to view and manage the Microsoft DHCP data. For information, see Chapter 32, IP Address Management, on page 777.

### Viewing Synchronized Leases

A grid member synchronizes all leases from its managed Microsoft server to the grid. Microsoft servers automatically generate a static lease for each reservation. These static leases are synchronized to the grid as well. You can view the synchronized leases by navigating to the Data Management -> DHCP -> Leases tab. For information about viewing current leases, see Viewing Current Leases on page 668. You can do the following:

- View lease details, by selecting a lease and clicking the Lease Details icon. For additional information, see Viewing Detailed Lease Information on page 669.
- Clear a lease, by selecting it and clicking the Clear Lease icon. Note that Grid Manager clears the lease immediately. It does not wait for the next synchronization.

Additionally, you can enable a grid member to log lease related operations, so you can view these events in the Lease History panel. For information, see Configuring the Lease Logging Member on page 665 and Viewing Lease History on page 670.
Managing Synchronized DHCP Data

When grid members are configured to manage Microsoft DHCP servers in read/write mode, you can use Grid Manager to view, edit and delete the DHCP data of those servers. You can add and manage networks and DHCP ranges that are synchronized as scopes to the Microsoft server, and add and manage reservations and superscopes. All updates are synchronized to the Microsoft servers at regular intervals.

Grid Manager also allows you to set admin permissions, extensible attributes, and thresholds. These apply only when the DHCP data is managed on Grid Manager. These properties are not synchronized to Microsoft servers.

The following sections provide guidelines for managing Microsoft DHCP data from Grid Manager:

- Adding and Managing Scopes on page 760
- Adding Fixed Addresses/Microsoft Reservations on page 766
- About Superscopes on page 768

Adding and Managing Scopes

To add a scope from Grid Manager, you must create an IPv4 network and a DHCP range, and then assign the Microsoft server to the network and range. To edit a scope synchronized from a Microsoft server, you must edit the properties of its corresponding DHCP range. The following sections describe how to add, edit and remove scopes using Grid Manager.

Note: Microsoft servers do not support Infoblox hosts and reservations. You cannot add them to networks and DHCP ranges served by Microsoft servers.

Adding Networks for Scopes

Following are guidelines for adding a network for Microsoft scopes:

- The network must be served by Microsoft servers. It cannot be served by a mix of Microsoft and Infoblox DHCP servers.
- The network can contain only one DHCP range per Microsoft server. It can contain multiple DHCP ranges as long as they do not overlap and are each served by a different Microsoft server.
- You can set DHCP properties at the DHCP range level only, not the network level.

You can run discoveries on networks served by Microsoft servers. For information about network discoveries, see Network Discovery on page 805.

Note: Networks served by Microsoft DHCP servers do not support the split, join, and expand functions.
You can create a network from scratch or use a network template. For information about creating network templates, see Adding Network Templates on page 649. To add an IPv4 network for a scope:

1. From the Data Management tab, select the DHCP tab.
2. If you have more than one network view in the system, select the network view in which you want to add the network. It must be the same network view to which the Microsoft server is assigned.
3. Expand the Toolbar and click Add Network.
4. In the Add Network wizard, select one of the following and click Next:
   - Add Network
   or
   - Add Network using Template: Click Select Template and select a network template. For information, see About DHCP Templates on page 644. In the DHCP Network Template Selector dialog box, select the template you want to use and click the Select icon. Note that when you use a template to create a network, the configurations of the template apply to the new network. The appliance populates the template properties in the wizard when you click Next. You can then edit the pre-populated properties, except for Netmask.
5. Complete the following and click Next:
   - Address: Enter the IP address of the network. You can enter the IP address with a CIDR block. For example, enter 10.0.0.0/24, and the netmask slider adjusts the netmask to /24. You can also enter partial IP address with a CIDR block. When you are done, Grid Manager displays the complete IP address with the CIDR block. For example, when you enter 15/24, Grid Manager displays 15.0.0.0/24 and the netmask slider adjusts the netmask to /24. Note that Microsoft DHCP servers do not support /32 subnets.
   - Netmask: Use the netmask slider to select the appropriate number of subnet mask bits for the network. Microsoft servers support /1 to /31 netmasks. Note that when you use a template that contains a fixed netmask, you cannot adjust the netmask for this network.
   - Comment: Enter additional information about the network, such as the name of the organization it serves.
   - Automatically create reverse-mapping zone in view: This function is enabled if the netmask of the network equals /8, /16, or /24. Select this to have the appliance automatically create reverse-mapping zones for the network. A reverse-mapping zone is an area of network space for which one or more name servers have the responsibility for responding to address-to-name queries. These zones are created in the DNS view assigned to receive dynamic DNS updates at the network view level.
   - Disabled: This option does not apply to networks assigned to Microsoft servers. The member ignores this field when the network is assigned to Microsoft servers. You can disable DHCP ranges assigned to Microsoft servers, but not networks.
6. Click Next to add Microsoft servers as DHCP servers for the network. Click the Add icon and select the following:
   - Add Microsoft Server: Select the Microsoft server from the Microsoft Server Selector dialog box. You can add multiple Microsoft servers, if you are adding multiple DHCP ranges served by different Microsoft servers.
7. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see About Extensible Attributes on page 222.
8. Select one of the following:
   - Save & Close: Save the entry and close the wizard.
   - Save & Edit: Save the entry and continue to edit.
   - Save & New: Save the entry and open a new wizard.
   or
   Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 25.
Managing Microsoft DHCP Services

Setting Network Properties

You can change the Microsoft servers assigned to the network, and define extensible attributes and admin permissions to the network. You can also set thresholds for the network, to enable the appliance to make a syslog entry when address usage goes above or below the thresholds.

To set network properties:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon.

2. The Network editor contains the following basic tabs from which you can modify data:
   - General Basic: You can enter or modify comments.
   - Member Assignment: Add or delete Microsoft servers. For information, see Adding IPv4 Networks on page 594. If the network contains multiple DHCP ranges each managed by a different Microsoft server, then you can add those Microsoft servers here.
   - Extensible Attributes: Add and delete extensible attributes that are associated with a specific network. You can also modify the values of the extensible attributes. For information, see About Extensible Attributes on page 222.
   - Permissions: This tab appears only if you belong to a superuser admin group. For information, see Managing Permissions on page 20.

3. Optionally, you can click Toggle Advanced Mode to display the following tabs from which you can modify advanced data.
   - General Advanced: You can associate zones with a network. For information, see Associating Networks with Zones on page 598.
   - Thresholds: These watermarks represent thresholds above or below which address usage is unexpected and might warrant your attention. Thresholds are inherited from the grid.
     - High-water Mark: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range exceeds this number, the appliance makes a syslog entry. The default is 95.
     - Low-water Mark: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range drops below this number, the appliance makes a syslog entry. The default is 0. Address usage must initially exceed the low-water mark threshold and then dip below it before the appliance considers low address usage an event requiring an alert.

4. Select one of the following:
   - Save & Close: Save the entry and close the editor.
   - Save: Save the entry and continue to edit.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 25.

Deleting and Restoring a Network

When you delete a network, Grid Manager moves it and its DHCP ranges and fixed addresses to the Recycle Bin, and permanently deletes its leases. The corresponding scopes and reservations are deleted from the Microsoft server at the next synchronization. If you restore the network on Grid Manager, its DHCP ranges and fixed addresses are restored as well. The grid member then adds the corresponding scopes and reservations to the Microsoft server on the next synchronization. For information about deleting networks, see Deleting IPv4 Networks on page 599. For information about restoring data, see Recycle Bin on page 47.
Adding a DHCP Range/Scope

After you add a network for a scope, you must then define its DHCP range. You can create the DHCP range from scratch or use a DHCP Range template. For information about DHCP templates, see About DHCP Range Templates on page 645.

You can add multiple ranges to the same network, as long as each range is served by a different Microsoft server and the ranges do not overlap.

To add a DHCP range for a scope:
1. From the Data Management tab, select the DHCP tab.
2. Navigate to the network to which you want to add a DHCP range, and then click Add -> DHCP Range from the Toolbar. You can also add a DHCP range from any panel in the DHCP tab.
3. In the Add Range wizard, select one of the following and click Next:
   - Add DHCP Range
   or
   - Add DHCP Range using Template
     Click Select Template and select the template that you want to use. Note that when you use a template to create a DHCP range, the configurations of the template apply to the new range. The appliance automatically populates the DHCP range properties in the wizard. You can then edit the pre-populated properties.
4. Complete the following:
   - Network: Click Select Network to select the network to which you want to add the DHCP range. The network must be served by a Microsoft server. If you are adding a DHCP range while viewing the contents of a specific network, the appliance displays the network address here. You can still select a different network by clicking Select Network.
   - Start: Enter the first IP address in the range.
   - End: Enter the last IP address in the range.
   - Name: You can enter a name for the DHCP range.
   - Comment: You can enter additional information. After the range is synchronized to the Microsoft server as a scope, this text appears in the Description field of the scope on the Microsoft server.
   - Disabled: Select this if you do not want the DHCP server to allocate IP addresses from this DHCP range at this time. If you select this, the grid member synchronizes the range to the Microsoft server as an inactive scope.
5. Click Next and select one of the following to provide DHCP services for the DHCP range:
   - None: Select this if you do not want to synchronize this range to the Microsoft DHCP server.
   - Microsoft Server: This field displays the Microsoft server that you selected for the network. If several servers were assigned to the network, you can select one from the list.
6. Click Next, and optionally set operational parameters for the scope. Otherwise, the scope inherits its parameters from the Microsoft DHCP server.
   - Lease Time: Specify the lease time. The default is 8 days. When the range is served by a Microsoft server and you enter a lease time of 1000 days or more, Grid Manager automatically grays out this field and checks the Unlimited Lease Time option after you save your entries.
     - Unlimited Lease Time: Select this option to set an infinite lease time for the IP addresses leased from this range.
     - Routers: In the table, enter the IP address of the router that is connected to the same network as the DHCP clients. Click the Add icon to add more routers.
     - Domain Name: Enter the name of the domain for which the Microsoft server serves DHCP data. The DHCP server includes this domain name in Option 15 when it responds with a DHCPOFFER packet to a DHCPDISCOVER packet from a client.
— **DNS Servers:** In the table, enter the IP address of the DNS server to which the DHCP clients send name resolution requests. The DHCP server includes this information in the DHCPOFFER and DHCPACK messages.

— **Broadcast Address:** Enter the broadcast IP address of the network to which the DHCP server is attached.

7. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see *Using Extensible Attributes* on page 225.

8. Select one of the following:
   — **Save & Close:** Save the entry and close the wizard.
   — **Save & Edit:** Save the entry and continue to edit.
   — **Save & New:** Save the entry and open a new wizard.
   or
   — Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 25.

### Setting DHCP Range/Scope Properties

A Microsoft scope inherits its properties from its Microsoft server. In Grid Manager, you can override the inherited values or set other properties by editing the DHCP range. You can also configure an exclusion range within the scope and set thresholds, to enable the appliance to make a syslog entry when address usage goes above or below the thresholds.

To set DHCP range properties:

1. From the *Data Management* tab, select the *DHCP* tab -> *Networks* tab -> *Networks* -> *addr_range* check box, and then click the Edit icon.

2. The *DHCP Range* editor contains the following basic tabs from which you can modify data:
   — **General:** Modify the fields, including the start and end addresses, as described in *Adding a DHCP Range/Scope*.
   — **Server Assignment:** Switch to **None** or select a different Microsoft server for the DHCP range.
   — **DHCP:** Keep the DHCP properties or override them and enter unique settings for the DHCP range. For information about the fields, see *Adding a DHCP Range/Scope* on page 763.

   This tab displays DHCP and Microsoft vendor options that were synchronized from the Microsoft server. You can edit only the DHCP standard options defined for the default user class. All other options are displayed as read-only.

   To configure additional DHCP options, click +, select an option from the drop-down list, and enter a value in the field beside it. You can click - to remove an option.

   — **Extensible Attributes:** You can add and delete extensible attributes that are associated with a specific DHCP range. You can also modify the values of extensible attributes. For information, see *Using Extensible Attributes* on page 225.

   — **Permissions:** This tab appears only if you belong to a superuser admin group. For information, see *Managing Permissions* on page 20.

3. Optionally, you can click **Toggle Advanced Mode** to display the following tabs from which you can modify advanced data.

   — **DDNS:** Complete the following to set DDNS parameters for the range:
     — **Enable DDNS Updates:** Click the check box to enable the Microsoft DHCP server to send dynamic DNS updates or clear the check box to disable this function.
     — **Option 81 Support**
       — **DHCP Server Updates DNS If Requested by Client:** The DHCP server updates DNS only if it is requested by the client. Otherwise, the client updates DNS.
       — **DHCP Server Always Updates DNS:** The DHCP server always updates DNS, regardless of any client request.
— **Exclusion Ranges**: Configure a range of IP addresses that the server does not use to assign to clients. You can use these exclusion addresses as static IP addresses. For information, see *Excluding Addresses from DHCP Ranges and Templates* on page 607.

— **Thresholds**: Thresholds are inherited from the grid. These watermarks represent thresholds above or below which address usage is unexpected and might warrant your attention.
  
  — **High-water Mark**: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range exceeds this number, the appliance makes a syslog entry. The default is 95.
  
  — **Low-water Mark**: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range drops below this number, the appliance makes a syslog entry. The default is 0. Address usage must initially exceed the low-water mark threshold and then dip below it before the appliance considers low address usage an event requiring an alert.

4. Select one of the following:
  
  — **Save & Close**: Save the entry and close the editor.
  
  — **Save**: Save the entry and continue to edit.
  
  or
  
  — Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 25.

### Deleting and Restoring a DHCP Range/Scope

When you delete a DHCP range, Grid Manager moves it and its exclusion range and fixed addresses to the Recycle Bin, and permanently deletes its leases. At the next synchronization, the member deletes the scope, its exclusion range and reservations from the Microsoft server. If you restore a DHCP range on Grid Manager, then the grid member adds its corresponding scope, exclusion range and reservations to the Microsoft server at the next synchronization. For information about deleting DHCP ranges, see *Deleting DHCP Ranges* on page 607. For information about restoring data, see *Recycle Bin* on page 47.
Adding Fixed Addresses/Microsoft Reservations

To add a reservation from Grid Manager, add a fixed address and Grid Manager synchronizes it to the Microsoft server as a reservation. You can create fixed addresses from scratch or use fixed address templates. For information about fixed address templates, see Adding Fixed Address/Reservation Templates on page 647.

To add a fixed address:

1. From the Data Management tab, select the DHCP tab.
2. Expand the Toolbar and click Add -> Fixed Address.
3. In the Add Fixed Address wizard, select one of the following and click Next:
   - Add Fixed Address
   or
   - Add Fixed Address using Template
     Click Select Template and select the template that you want to use.

4. Complete the following:
   - **Network**: Click Select Network to select the network to which you want to add the fixed address. If you are adding the fixed address from a specific network, the appliance displays the network address here. You can still select a different network by clicking Select Network.
   - **IP Address**: Enter the IPv4 address for the fixed address, or click Next Available IP to obtain the next available IP address.
   - **MAC Address**: Enter the MAC address of the host.
   - **Name**: Enter a name for the fixed address. This is required for reservations on Microsoft servers.
   - **Configure On**:
     - **None**: Select this if you do not want this synchronized to the Microsoft server.
     - **Microsoft Server**: Select the Microsoft server that serves this fixed address.
   - **Comment**: Optionally, enter additional information. The text in this field appears in the Description field of the Microsoft reservation after the fixed address is synchronized.

5. Click Next, and optionally set operational parameters for the fixed address. Otherwise, the fixed address inherits its parameters from its scope.
   - **Routers**: In the table, enter the IP address of the router that is connected to the same network as the DHCP client. Click the Add icon to add more routers.
   - **Domain Name**: Enter the name of the domain for which the Microsoft DHCP serves DHCP data. The DHCP server includes this domain name in Option 15 when it responds with a DHCPOFFER packet to a DHCPDISCOVER packet from a client.
   - **DNS Servers**: In the table, enter the IP address of the DNS server to which the DHCP client sends name resolution requests. The DHCP server includes this information in the DHCPOFFER and DHCPACK messages.
   - **Broadcast Address**: Enter the broadcast IP address of the network to which the DHCP server is attached.

6. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes on page 225.

7. Select one of the following:
   - **Save & Close**: Save the entry and close the wizard.
   - **Save & Edit**: Save the entry and continue to edit.
   - **Save & New**: Save the entry and open a new wizard.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 25.
Managing Synchronized DHCP Data

Setting Fixed Address/Reservation Properties

Microsoft reservations inherit their properties from their scopes. In Grid Manager, you can override the inherited values or set other properties of a Microsoft reservation, by editing its fixed address.

To modify a fixed address:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> fixed_address check box, and then click the Edit icon.

2. The Fixed Address editor contains the following basic tabs from which you can enter data:
   - General: You can modify the fields described in Adding Fixed Addresses/Microsoft Reservations on page 766.
   - DHCP: Keep the inherited properties, or override them and enter unique settings. This tab displays DHCP and Microsoft vendor options that were synchronized from the Microsoft server. You can edit only the DHCP standard options defined for the default user class. All other options are displayed as read-only.
     To configure additional DHCP options, click +, select an option from the drop-down list, and enter a value in the field beside it. You can click - to remove an option.
   - Discovered Data: If you ran a discovery on the network, Grid Manager displays the discovered data of the fixed address. For information, see Viewing Data in the Discovered Data Section on page 820. Note that conflicts can occur when discovered data does not match the existing IP address data. For information about resolving these conflicts, see Resolving Conflicting Addresses on page 823.
   - Extensible Attributes: Add and delete extensible attributes that are associated with a specific network. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes on page 225.
   - Permissions: This tab appears only if you belong to a superuser admin group. For information, see Managing Permissions on page 20.

3. Optionally, you can click Toggle Advanced Mode to display the DDNS tab. To set DDNS parameters for the fixed address, complete the following:
   - Enable DDNS Updates: Click the check box to enable the Microsoft DHCP server to send dynamic DNS updates or clear the check box to disable this function.
   - Option 81 Support
   - DHCP Server Updates DNS If Requested by Client: The DHCP server updates DNS only if it is requested by the client. Otherwise, the client updates DNS.
   - DHCP Server Always Updates DNS: The DHCP server always updates DNS, regardless of any client request.

4. Select one of the following:
   - Save & Close: Save the entry and close the editor.
   - Save: Save the entry and continue to edit.
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 25.

Deleting and Restoring a Fixed Address/Reservation

When you delete a fixed address, Grid Manager moves it to the Recycle Bin. At the next synchronization, the grid member deletes its corresponding reservation from the Microsoft server. If you restore fixed address, then the grid member adds its corresponding reservation to the Microsoft server at the next synchronization. For information about deleting fixed addresses, see Deleting Fixed Addresses on page 610. For information about restoring data, see Recycle Bin on page 47.
About Superscopes

In Grid Manager, you can group DHCP ranges served by Microsoft servers into a superscope. You can add multiple DHCP ranges to a superscope, as long as the ranges are all served by the same Microsoft DHCP server. The grid member then synchronizes the superscope and its associated DHCP ranges as superscopes and scopes to the Microsoft DHCP server.

You can also associate extensible attributes with superscopes in Grid Manager. Extensible attributes are not synchronized to the Microsoft DHCP server.

Only admins with read/write permission to superscopes can add and manage superscopes.

Adding Superscopes

Before you add a superscope, you must first create at least one DHCP range to include in the superscope.

To add a superscope:

1. From the Data Management tab, select the DHCP tab.
2. If you have more than one network view in the system, select the network view in which you want to add the superscope. The network view must be the same one that is assigned to the Microsoft server.
3. Expand the Toolbar and click Add -> Superscope.
4. In the Add Superscope wizard, complete the following and click Next:
   - Name: Enter a name for the superscope.
   - Comment: Optionally, enter additional information about the superscope.
   - Disabled: Select this to disable the DHCP ranges in the superscope. They are then synchronized as inactive scopes on the Microsoft server.
5. Click the Add icon and select a range from the Select Range dialog box. This dialog box lists only the address ranges that are served by a Microsoft server.
6. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see About Extensible Attributes on page 222.
7. Select one of the following:
   - Save & Close: Save the entry and close the wizard.
   - Save & Edit: Save the entry and continue to edit.
   - Save & New: Save the entry and open a new wizard.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 25.

Viewing Superscopes

To view superscopes, navigate to the Data Management tab -> DHCP tab -> Network tab -> Microsoft Superscopes. Grid Manager displays the following information about each superscope that is displayed:

- Name: The name of the superscope. Grid Manager appends the FQDN of its associated Microsoft server so you can identify which superscope belongs to which server.
- Comment: The comment that was entered for the superscope.
- DHCP Utilization: The percentage of the total DHCP usage of the ranges in the superscope. Fixed addresses and reservations that are outside of a range are excluded from the calculation.
- Site: The site of the superscope. This is one of the predefined extensible attributes.

You can add the following columns for viewing:

- Static Addresses: The number of static addresses.
- Dynamic Addresses: The number of dynamic addresses.
- Disabled: Indicates whether the superscope is enabled.
You can do the following in this section:

- Click the link of a superscope to list its address ranges.
- Add a superscope.
- Print or export the information in this section.
- Delete a superscope.

**Modifying Superscopes**

To modify a superscope:

1. From the **Data Management** tab, select the **DHCP tab -> Network tab -> Microsoft Superscopes -> ms_superscope** check box, and then click the **Edit icon**.

2. The **Superscopes** editor contains the following tabs from which you can modify data:
   - **General**: You can modify the name and comment, and enable or disable the superscope. You can also add and delete address ranges from the superscope. Note that when you delete the last DHCP range in a superscope, Grid Manager automatically deletes the superscope as well.
   - **Extensible Attributes**: Define extensible attributes for the superscope. These apply only when the superscope is managed in Grid Manager. For information, see [Using Extensible Attributes](#) on page 225.
   - **Permissions**: Define administrative permissions that apply to the superscope when it is managed in Grid Manager. For information see [About Administrative Permissions](#) on page 87.

3. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and continue editing.

**Deleting Superscopes**

When you delete a superscope in Grid Manager, it is permanently deleted from the database. The superscope is deleted from the Microsoft server at the next synchronization. Note that deleting a superscope does not delete the DHCP ranges in the superscope. These are retained in the database.

To delete a superscope:

1. From the **Data Management** tab, select the **DHCP tab -> Network tab -> Microsoft Superscopes -> ms_superscope** check box, and then click the **Delete icon**.

2. Click **Yes** when the confirmation dialog appears.
SYNCHRONIZING UPDATES

Each grid member synchronizes DHCP data with each of its managed Microsoft server at regular intervals. During each synchronization, updates from Grid Manager are applied to the Microsoft server and updates from the Microsoft server are applied to the grid as well.

Because admins can update DHCP data from the Microsoft server and from Grid Manager, conflicts can occur during synchronization. The following guidelines describe how the grid member resolves conflicts and handles any differences when DHCP data is synchronized between a Microsoft server and the grid.

- If a Microsoft server admin modifies an object that has a pending scheduled task in Grid Manager and synchronization occurs before the scheduled task, the object is modified in both the Microsoft server and the grid member. When the scheduled task executes at its scheduled time, it fails and an error message is logged in the audit log.
- When a Microsoft server admin and a Grid Manager admin change the same object, the grid member retains the version that exists on the Microsoft server. Following are some examples:

Table 31.2

<table>
<thead>
<tr>
<th>Grid Manager Admin...</th>
<th>Microsoft Server Admin...</th>
<th>After Synchronization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deletes the 10.1.1.0/24 network which has two DHCP ranges</td>
<td>Adds a scope that is within the 10.1.1.0/24 network</td>
<td>The 10.1.1.0/24 network is created on the grid with the updates and is assigned to the Microsoft server.</td>
</tr>
<tr>
<td>Changes the DHCP options of a scope</td>
<td>Deletes the scope.</td>
<td>The scope is deleted from the grid as well.</td>
</tr>
</tbody>
</table>
Managing Microsoft DHCP Servers

You can control the DHCP services of managed Microsoft servers and set certain properties as well. This section includes the following topics:

- *Viewing Members and Managed DHCP Servers*
- *Setting Microsoft DHCP Server Properties* on page 772
- *Controlling the DHCP Service of a Microsoft Server* on page 773
- *Disabling and Removing Microsoft DHCP Servers* on page 773
- *Modifying DHCP Server Assignments* on page 773

Viewing Members and Managed DHCP Servers

You can view Infoblox and Microsoft DHCP servers by navigating to the Data Management tab -> DHCP tab, and then selecting the Members/Servers tab. The panel displays the following information about each DHCP server:

- **Name:** The hostname of the grid member or Microsoft server.
- **Status:** The status of the DHCP service on the grid member or Microsoft server.
- **Comment:** Comments that were entered for the grid member or Microsoft server.
- **DHCP Utilization:** The percentage of the total DHCP utilization of the member or Microsoft server. This is the percentage of the total number of DHCP hosts, fixed addresses, reservations, and leases assigned to the member or Microsoft server versus the total number of IP addresses (excluding IP addresses in the exclusion range) and all DHCP objects assigned to the member or DHCP server. Note that only enabled objects are included in the calculation. The appliance updates the utilization data every 15 minutes. The appliance displays the utilization data in one of the following colors:
  - Red: The DHCP resources are 100% utilized.
  - Yellow: The utilization percentage is over the effective high watermark threshold.
  - Blue: The utilization percentage is below the effective low watermark threshold.
  - Black: The utilization percentage is at any number other than 100%, or within the effective thresholds.
- **Site:** Values that were entered for this pre-defined attribute.

You can select the following additional columns for display:

- **Address:** The IP address of the member or Microsoft server.
- **Static Addresses:** The number of static IP addresses.
- **Dynamic Addresses:** The number of dynamically assigned IP addresses.

You can do the following:

- Edit the properties of a grid member or Microsoft server.
  - Click the check box beside a grid member or Microsoft server, and then click the Edit icon.
- Export the list of grid members and Microsoft servers to a .csv file.
  - Click the Export icon.
- Print the list of grid members and Microsoft servers.
  - Click the Print icon.
Setting Microsoft DHCP Server Properties

From Grid Manager, you can set DHCP properties supported by a Microsoft server. These are applied to the server at the next synchronization. You can also set other properties that apply to Grid Manager only, such as thresholds and the logging.

To set properties for a Microsoft DHCP server:

1. From the Data Management tab, select the DHCP tab -> Members/Servers tab -> Members/Servers -> ms_server check box, and then click the Edit icon.

2. In the Microsoft Server DHCP Properties editor, you can configure DHCP properties in each tab as follows:
   - **DHCP Options tab**: Complete the following to configure basic DHCP options for the server:
     - **Routers**: Click the Add icon and enter the IP address of the router that is connected to the same network as the DHCP clients.
     - **Domain Name**: Enter the name of the domain for which the server serves DHCP data. The DHCP server includes this domain name in Option 15 when it responds with a DHCPOFFER packet to a DHCPDISCOVER packet from a client. If DDNS is enabled on the DHCP server, it combines the host name from the client and this domain name to create the FQDN (fully-qualified domain name) that it uses to update DNS.
     - **DNS Servers**: Click the Add icon and enter the IP address of the DNS server to which the DHCP client sends name resolution requests. The DHCP server includes this information in the DHCPOFFER and DHCPACK messages.
     - **Broadcast Address**: Enter the broadcast IP address of the network to which the DHCP server is attached.
     - **Custom DHCP Options**: This section displays DHCP and Microsoft vendor options that were synchronized from the Microsoft server. You can edit only the DHCP standard options defined for the default user class. All other options are displayed as read-only.

   To configure additional DHCP options, click +, select an option from the drop-down list, and enter a value in the field beside it. You can click - to remove an option.
   - **DDNS tab**: You can enable or disable dynamic DNS updates and set certain properties.
     - **Enable DDNS Updates**: Click the check box to enable the Microsoft DHCP server to send dynamic DNS updates or clear the check box to disable this function.
     - **Option 81 Support**
       - **DHCP Server Updates DNS If Requested by Client**: The DHCP server updates DNS only if it is requested by the client. Otherwise, the client updates DNS.
       - **DHCP Server Always Updates DNS**: The DHCP server always updates DNS, regardless of any client request.
   - **Thresholds tab**: Thresholds are inherited from the grid. These watermarks represent thresholds above or below which address usage is unexpected and might warrant your attention.
     - **Enable DHCP Thresholds**: Select this check box to enable the feature.
     - **High-water Mark**: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range exceeds this number, the DHCP server makes a syslog entry. The default is 95.
     - **Low-water Mark**: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range drops below this number, the DHCP server makes a syslog entry. The default is 0. Address usage must initially exceed the low-water mark threshold and then dip below it before the appliance considers low address usage an event requiring an alert.

3. Optionally, you can click **Toggle Advanced Mode** to display the **Logging** tab, where you can enable the managing member to log the lease events of the Microsoft server. This setting is inherited from the grid. You can override that setting by clicking **Override**, and then selecting or clearing the **Log Lease Events from DHCP server** check box.

4. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry and continue editing.
Controlling the DHCP Service of a Microsoft Server

You can start and stop the DHCP service of a managed Microsoft server from Grid Manager as follows:

1. From the Data Management tab, select the DHCP tab -> Members/Servers tab -> Members/Servers -> ms_server check box.
2. Expand the Toolbar and click Start or Stop.
3. Click Yes when the confirmation dialog appears.

Disabling and Removing Microsoft DHCP Servers

If you remove a Microsoft server as a managed server, Grid Manager deletes all the DHCP ranges, leases, and fixed addresses associated with the server. It also deletes networks that were assigned only to the Microsoft server. It does not delete a network if it was assigned to other Microsoft servers as well.

When you disable a Microsoft server, the managing grid member terminates any on-going synchronization and restarts synchronization only when the server is re-enabled. The DHCP data associated with that server is preserved in the same state until synchronization resumes.

For information on removing and disabling Microsoft servers, see Disabling Synchronization on page 736 and Removing a Managed Microsoft Server on page 737.

Modifying DHCP Server Assignments

If you disable a Microsoft DHCP server or take it offline for maintenance purposes, for example, you can assign its scopes to a member DHCP server.

Following are the tasks to reassign scopes from a Microsoft server to a member DHCP server:

1. Set the server assignments of all fixed addresses in the scope to “None”.
   - From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> fixed_address check box, and then click the Edit icon. You can change the server assignment in the General tab of the Fixed Address editor.
2. Set the server assignments of all address ranges served by the Microsoft server to “None”.
   - From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range check box, and then click the Edit icon. You can change the server assignment in the General tab of the DHCP Range editor.
3. Change the server assignments of the networks by deleting the Microsoft server and replacing it with a member DHCP server.
   - From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon. You can change the server assignment in the Member Assignment tab of the Network editor.
4. Modify the server assignments of all address ranges and specify the member DHCP server.
   - From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range check box, and then click the Edit icon. You can change the server assignment in the General tab of the DHCP Range editor.
5. Restart services.

The member DHCP server starts granting lease requests after the restart. Note that you do not need to clear the leases that were active on the Microsoft server, because the member automatically clears them when you change the DHCP server assignment.
PART 6 IPAM MANAGEMENT

This section provides information about managing your IP data. It includes the following chapters:

- Chapter 32, *IP Address Management*, on page 777
- Chapter 33, *Network Discovery*, on page 805
Chapter 32 IP Address Management

This chapter describes how to manage your networks and IP addresses. It contains the following sections:

- **IP Address Management** on page 779
  - **About Network Containers** on page 780
    - **Deleting Network Containers** on page 781
  - **Managing IPv4 Networks** on page 782
    - **Network Map** on page 783
    - **Network List** on page 787
    - **Adding IPv4 Networks** on page 787
    - **Modifying IPv4 Networks** on page 787
    - **Deleting IPv4 Networks** on page 788
    - **Resizing IPv4 Networks** on page 788
    - **Splitting IPv4 Networks into Subnets** on page 788
    - **Joining IPv4 Networks** on page 789
  - **Managing IPv4 Addresses** on page 790
    - **IP Map** on page 791
    - **IP Address List** on page 792
    - **Adding IP Addresses to Existing Host Records** on page 794
    - **Converting Objects Associated with IP Addresses** on page 794
    - **Reclaiming Objects Associated with IP Addresses** on page 797
    - **Pinging IP Addresses** on page 797
    - **Clearing Active DHCP Leases** on page 797
    - **Clearing Unmanaged Data** on page 798
  - **Managing IPv6 Networks and IP Addresses** on page 798
    - **Adding IPv6 Networks** on page 798
    - **Modifying IPv6 Networks** on page 799
    - **Splitting IPv6 Networks into Subnets** on page 799
    - **Joining IPv6 Networks** on page 800
    - **Deleting IPv6 Networks** on page 800
    - **Managing IPv6 Addresses** on page 800
• Managing IP Address Data on page 801
  — Fixed Addresses on page 801
  — Reservations on page 802

• Managing Resource Records on page 803
  — A Records on page 803
  — AAAA Records on page 803
  — PTR Records on page 804
  — Host Records on page 804
IP ADDRESS MANAGEMENT

With the increasing number of network devices, the various types of network access (wired, wireless, VPNs), and the shifting network boundaries needed to accommodate mobile remote users, network management and security have become increasingly complex. The Infoblox IPAM (IP address management) implementation offers an IP address-centric approach to network management so you can face these challenges.

Grid Manager provides the tools that you need to track and manage IP address usage in your networks. You can configure IPv4 and IPv6 networks, allocate IP addresses, and manage IP address usage within these networks. IPAM integrates IP address management with IP address services, so you can access DNS and DHCP data for each IP address. You can do the following:

- Configure and manage IPv4 networks and addresses. For information, see Managing IPv4 Networks on page 782 and Managing IPv4 Addresses on page 790.
- Configure and manage IPv6 networks and addresses. For information, see Managing IPv6 Networks and IP Addresses on page 798.
- When necessary, resize, join, or split networks. For information, see Resizing IPv4 Networks on page 788, Splitting IPv4 Networks into Subnets on page 788, Joining IPv4 Networks on page 789, Splitting IPv6 Networks into Subnets on page 799, and Joining IPv6 Networks on page 800.
- View your network and address utilization in a graphical mode. For information, see Network Map on page 783 and IP Map on page 791.
- Manage IP address data. For information, see Managing IP Address Data on page 801 and Managing Resource Records on page 803.
- Configure and run network discoveries. For information, see Network Discovery on page 805.
About Network Containers

Grid Manager uses network containers to group IPv4 and IPv6 networks. A network container is a parent network that contains other network containers and leaf networks. A leaf network is a network that does not contain other networks. For example, Figure 32.1 illustrates the IPv4 20.0.0.0/8 network, which is a network container with two network containers, 20.8.0.0/13 and 20.72.0.0/13. The 20.8.0.0/13 network has two leaf networks, 20.8.0.0/16 and 20.9.0.0/16. The 20.72.0.0/13 network has one leaf network, 20.72.0.0/16.

Figure 32.1  IPv4 Network Container

From Grid Manager, you can click the link of the network container 20.0.0.0/8 in the IP List panel and drill down to the two network containers, 20.8.0.0/13 and 20.7.0.0/13, as shown in Figure 32.2. You can click the network container links to drill down further to the leaf networks.

Figure 32.2  IP List View of Network Containers
In the IPAM tab, when you create an IPv4 or IPv6 network that belongs to a larger network, the appliance automatically creates a network container and puts the leaf network in the container. The appliance also creates network containers when you split IPv4 or IPv6 networks into smaller networks. For information, see Splitting IPv4 Networks into Subnets on page 788 and Splitting IPv6 Networks into Subnets on page 799.

Deleting Network Containers

When you remove a network container, you can choose to keep its contents or delete them. Contents in a network container can include other network containers, leaf networks, and associated objects, such as host records. When you delete a network container only, the appliance reparents the other network containers and leaf networks in the IPAM tab.

The appliance moves a deleted network container and its contents to the Recycle Bin, if enabled. When you restore the network container from the Recycle Bin, all its contents, if any, are reparented to the restored network container. For information, see Recycle Bin on page 47.

To delete a network container:

1. From the Data Management tab, select the IPAM tab -> network_container check box. You can select multiple network containers for deletion.
2. Click the Delete icon.
3. In the Delete Confirmation dialog box, select one of the following:
   - Delete only the network container and re-parent the subnets
   - Delete the network and all objects under it (subnets, hosts, etc.)

The appliance puts the deleted network container in the Recycle Bin, if enabled.
Managing IPv4 Networks

With Grid Manager, you can configure and manage your IPv4 networks. Depending on the needs of your organization, you can configure a single network, multiple networks, or multiple levels of networks within networks. Grid Manager uses network containers to group IPv4 networks. For information, see About Network Containers on page 780.

In Grid Manager, you use the Net Map (network map) and List panels to manage your network infrastructure. After you select a network container from the IPAM tab, Grid Manager displays it in the Net Map panel, by default. The Net Map panel provides a graphical view of your networks and has a number of features that simplify network management. The List panel displays the networks in table format.

You can always switch your view of a network container between the Net Map and List panels. Grid Manager keeps track of which panel you last used. When you select a network container, Grid Manager displays it in the Net Map or List panel, depending on which one you last used. For information about each panel, see Network Map on page 783 and Network List on page 787.

Use the IP Map and List panels to manage the IP addresses in leaf networks. For information, see Managing IPv4 Addresses on page 790.

After you create an IPv4 network, you can modify its properties, resize it, use the split network feature to create subnets, or join it to another network to create a larger network that encompasses adjacent subnets. You can do the following from both the Net Map and List panels:

- Add IPv4 networks. For information, see Adding IPv4 Networks on page 787.
- Delete IPv4 networks. For information, see Deleting IPv4 Networks on page 788.
- Modify network properties. For information, see Modifying IPv4 Networks on page 787.
- Resize a network. For information, see Resizing IPv4 Networks on page 788.
- Split a network into subnets. For information, see Splitting IPv4 Networks into Subnets on page 788.
- Join a network. For information, see Joining IPv4 Networks on page 789.
Network Map

After you select a network container from the IPAM tab, Grid Manager displays it in the Net Map (network map) panel, by default. Net Map provides a high-level view of the network address space. You can use Net Map to design and plan your network infrastructure, configure and manage individual networks, and evaluate their utilization. Its unique display of the network address space across multiple rows is similar to a road map that starts with the first IP address in the network and ends with the last address. Net Map displays the network address space across a maximum of eight rows, depending on the size of the network. It automatically scales the map so that it displays the entire address space of a network container.

The Net Map panel presents a complete view of the network space, including the different types of networks that are in it and its unused address space. IP addresses that belong to a network are blocked off. Each color-coded block represents a network container, a leaf network, or a block of networks that are too small to be displayed individually in the map. For example, in a /8 or /16 network, networks smaller than /20 or /28 respectively and that are beside each other are represented as a multiple network block. In addition, the fill pattern of the blocks indicates their utilization. Therefore, you can quickly evaluate how many and what type of networks are in a network container, their relative sizes, utilization, and how much space you have left.

As you mouse over areas of the map, it displays IP information about the area. Net Map also has a zoom feature that allows you to enlarge or reduce your view of a particular area. 

Figure 32.3 displays the network map of a 20.0.0.0/8 network, which is a network container that has network containers and leaf networks.

Figure 32.3  20.0.0.0/8 Network Map
Displaying IP Information

As shown in Figure 32.3, as you mouse over the map, Net Map displays IP information about the area. When you mouse over an unused area, Net Map displays the following information:

- The start and end IP address
- The number of IP addresses that can fit in that space
- The largest possible network
- The number of /16 and /24 networks that can fit in that space

When you mouse over a network, Net Map displays the following information:

- Network address and netmask
- Utilization of the network. For a leaf network, Net Map reports the percentage of used IP addresses, except the broadcast and network addresses. For a network container, Net Map reports the percentage of the IP address space that has been allocated to either network containers or leaf networks.
- The first and last IP address of the network
- The total number of IP addresses in the network

When you mouse over a block of multiple networks, Net Map displays the following information:

- The start and end IP address of that block of networks
- The total number of IP addresses in that block of networks
- The number of networks in that block

Zooming In and Out

Use the zoom function to enlarge and reduce your view of a selected area. You can zoom in on any area in your network. You can zoom in on an area until it displays 128 addresses per row, for a total of 1024 addresses for the map. When you reach the last possible zoom level, the Zoom In icon in the Net Map task bar and the menu item are disabled.

After you zoom in on an area, you can click the Zoom Controller icon to track where you zoomed in. The Zoom Controller lists all the areas that you zoomed in and updates its list dynamically. You can click an item on the list to view that area again. Click the Zoom Controller again to close it.

To select an area and zoom in:

1. Right-click and select **Zoom In**, or click the Zoom In icon in the Net Map task bar.
   - The pointer changes to the zoom in selector.

2. Select a starting point and drag to the end point. The starting point can be anywhere in the map. It does not have to be at the beginning of a network.
   - Net Map displays a magnified view of the selected area after you release the mouse button. As you mouse over the zoomed in area, Net Map displays IP information about it.

3. You can do the following:
   - Select an area and zoom in again.
   - Add a network. If you zoom in on an area and click Add without selecting an open area first, Net Map selects the area where it can create the biggest possible network in that magnified area.
   - Select a network and perform any of the following operations:
     - Split the network.
     - Join it to another network.
     - Resize the network.
     - Edit its properties.
     - Open it to display its network or IP map.
   - Right-click and select **Zoom Out**, or click the Zoom Out icon in the Net Map task bar. Each time you click **Zoom Out**, Net Map zooms out one level and the Zoom Controller is updated accordingly.
Net Map Tasks

From Net Map, you can create IPv4 networks, and evaluate and manage your network resources according to the needs of your organization. You can do the following:

- Zoom in on specific areas, as described in Zooming In and Out on page 784.
- Add a network, as described in Adding a Network from Net Map.
- Select a network and view either its network or IP map, as described in Viewing Network Details on page 786.
- Select a network and edit its properties, as described in Modifying IPv4 Networks on page 787.
- Split a network, as described in Splitting IPv4 Networks into Subnets on page 788.
- Join networks, as described in Joining IPv4 Networks on page 789.
- Resize a network, as described in Resizing IPv4 Networks on page 788.
- Delete one or multiple networks, as described in Deleting IPv4 Networks on page 788.
- Switch to the List view of the network. For information, see Network List on page 787.
  - When you select one or more networks in Net Map and then switch to the List view, the list displays the page with the first selected network.
  - If you select one or more networks in the List view and then switch to the Net Map view, the first network is also selected in Net Map. Although, if you select a network in the List view that is part of a Multiple Networks block in Net Map, it is not selected when you switch to the Net Map view.

Adding a Network from Net Map

When you create networks from Net Map, you can evaluate your network infrastructure and add networks accordingly. You can view the address space to which you are adding a network, so you can determine how much space is available and which IP addresses are not in use. When you mouse over an open area, Net Map displays useful information, such as the largest possible network that fits in that area and the total number of IP addresses. In addition, you can create networks without having to calculate anything. When you add a network, Net Map displays a netmask slider so you can determine the appropriate netmask for the size of the network that you need. As you move the slider, it displays network information, including the total number of addresses. After you select the netmask, you can even move the new network around the open area to select another valid start address.

To add a network from the Net Map panel:

1. Do one of the following:
   - Click the Add icon.
     Net Map displays the netmask slider and outlines the open area that can accommodate the largest network.
   - Select an open area, and then click the Add icon.
     Net Map displays the netmask slider and outlines the largest network that you can create in the open area that you selected.

2. Move the slider to the desired netmask. You can move the slider to the netmask of the largest network that can be created in the open area.
   As you move the slider, Net Map displays the netmask and its corresponding number of IP addresses. The outline in the network map also adjusts as you move the slider. When you mouse over the outline, it displays the start and end address of the network.

3. After you set the slider to the desired netmask, you can drag the new network block around the open area to select a new valid starting address. You cannot move the block to a starting address that is invalid.

4. Click Launch Wizard to create the network.
   The Add Network wizard displays the selected network address and netmask.

5. You can add comments, automatically create reverse mapping zones, and edit the extensible attributes. (For information, see Adding IPv4 Networks on page 787.) You cannot change the network address and netmask.
6. Select one of the following:
   — **Save & Close**: Save the entry and close the wizard.
   — **Save & Edit**: Save the entry, and Grid Manager displays the editor for additional configurations.
   — **Save & New**: Save the entry and display a new wizard.

   Grid Manager updates Net Map with the newly created network.

**Viewing Network Details**

From the Net Map panel, you can focus on a specific network or area and view additional information about it. If you have a network hierarchy of networks within network containers, you can drill down to individual leaf networks and view their IP address usage.

1. Select a network or area.
2. Click the Open icon.
   — If you selected a network container, Grid Manager displays it in the Net Map panel. You can drill down further by selecting a network or open area and clicking the Open icon again.
   — If you selected a block of multiple networks, Grid Manager displays the individual networks in the Net Map panel. You can then select a network or open area for viewing.
   — If you selected a leaf network, Grid Manager displays it in the IP Map panel.
   — If you selected an open area, Grid Manager displays an enlarged view of that area in the Net Map panel. This is useful when you are creating small networks in an open area.
Network List

The network List panel is an alternative view of an IPv4 network hierarchy. For a given network, the List panel shows all the subnets of a selected network in table format. A network list displays only the first-level subnets. It does not show further descendant or child subnets. You can open a subnet to view its child subnets. Subnets that contain child subnets are displayed as network containers. If the number of subnets in a network exceeds the maximum page size of the table, the network list displays the subnets on multiple pages. You can use the page navigation buttons at the bottom of the table to navigate through the pages of subnets.

The network List panel displays the following:

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

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

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

- **Site**: The site to which the IP address belongs. This is a predefined extensible attribute.

You can select the following columns for display:

- **Disabled**: Indicates whether the network is disabled.
- **Leaf Network**: Indicates whether the network is a leaf network or not.
- **Other available extensible attributes**

You can also sort the list of subnets in ascending or descending order by columns. For information on customizing tables in Grid Manager, see [Customizing Tables](#) on page 44.

Tip: If you select a network from the list and switch to the Net Map panel, the network is also selected in the network map.

Filtering the Network List

You can filter the network list, so it displays only the networks you need. You can filter the list based on certain parameters, such as network addresses, comments and extensible attributes. When you expand the list of available fields you can use for the filter, note that the extensible attributes are those with a gray background.

Adding IPv4 Networks

To add an IPv4 network:

1. From the **Data Management** tab, select the **IPAM** tab, and then click **Add -> Add IPv4 Networks** from the Toolbar.
2. In the **Add Network** wizard, create a network as described in **Adding IPv4 Networks** on page 594.

Modifying IPv4 Networks

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

To modify an IPv4 network:

1. From the **Data Management** tab, select the **IPAM** tab -> **network** check box, and then click the Edit icon.
2. In the **DHCP Network** editor, modify the network settings as described in **Modifying IPv4 Networks** on page 597.
Deleting IPv4 Networks

You can delete multiple IPv4 networks from the Net Map and List panels. When you delete a network, all of its data, including all of its DHCP records, subnets, and records in its subnets, is deleted from the database and goes to the Recycle Bin, if enabled. Because of the potentially large loss of data that can occur when you delete a network, Grid Manager requires a confirmation to move the data to the Recycle Bin.

To delete an IPv4 network from the IPAM tab:

1. From the Data Management tab, select the IPAM tab -> network check box. You can select multiple check boxes for multiple networks.
2. Select Delete or Schedule Delete from the Delete drop-down menu.
3. To delete the network now, in the Delete Confirmation dialog box, click Yes. To schedule a deletion, see Scheduling Tasks on page 25.
   The appliance puts the deleted network in the Recycle Bin, if enabled.

Resizing IPv4 Networks

You can resize a network to increase or decrease the network size and the number of IP addresses in the network. When you resize a network to a smaller netmask, you increase the number of IP addresses within that network. You can change the size of an IPv4 network when the operation does not affect existing objects in the network. You can resize an existing network only if the resized network does not exceed the upper network limit or create orphan objects, such as hosts and DHCP ranges. When a network has a parent network or subnets, the upper limit of the network size is marked in red in the resize network slider, and you cannot resize beyond this limit. For example, if a network has a /16 parent network, you cannot resize the network to a network that is larger than /16.

To resize a network:

1. From the Net Map or List panel, select a network, and then click Resize from the Toolbar.
2. In the Resize Network editor, do the following:
   - Address: Displays the network address. You cannot modify this field.
   - Netmask: Displays the netmask of the network as you resize the network. You cannot modify this field.
   - Resize slider: Use the resize network slider to specify the appropriate subnet masks for the subnets. When you move the slider, Grid Manager displays the number of subnets and IP addresses within that subnet.
   - Automatically create reverse-mapping zone: This is enabled only when you resize a /8, /16, or /24 network. Select this check box to have the appliance automatically create reverse-mapping zones for the subnet. The appliance automatically creates reverse-mapping zones only for /8, /16, and /24 netmasks.
3. Click OK.

Splitting IPv4 Networks into Subnets

You can create smaller subnets simultaneously within a network by splitting it. You do not have to configure each subnet individually. You can create smaller subnets with larger netmasks. A larger netmask defines more networks with a smaller number of IP addresses.

These subnets inherit the address properties of the parent network, such as member assignments. The exceptions are the default router and broadcast address configuration. The default router and broadcast address configuration for address ranges and fixed address are disabled by default after splitting a network. You can enable these properties for each subnet after splitting the parent network.

To split a network:

1. From the Net Map or List panel, select the check box of a network, and then click Split from the Toolbar.
2. In the Split Network editor, do the following:
   - Address: Displays the network address. You cannot modify this field.
   - Netmask: Displays the netmask of the network. You cannot modify this field.
   - Subnetworks: Displays the number of subnets and IP addresses for each subnet.
— **Split network slider:** Use the split network slider to specify the appropriate subnet masks for each subnet. When you move the slider, Grid Manager displays the number of subnets and the IP address range within that subnet.

— **Immediately Add:** Select one of the following options.
  — **Only networks with ranges and fixed addresses and unmanaged:** Adds only the networks that have DHCP ranges, fixed addresses, and unmanaged addresses.
  — **All possible networks:** Adds all networks that are within the selected netmasks. The is enabled only when you split the /8 networks to /9 or /16 networks.

Note that when you add a large number of networks, it could take a little longer for Grid Manager to display the networks.

— **Automatically create reverse-mapping zone:** Select this check box to have the appliance automatically create reverse-mapping zones for the subnets.

3. **Click OK.**

### Joining IPv4 Networks

Joining multiple networks into a larger network is the opposite of splitting a network. You can select a network and expand it into a larger network with a smaller netmask. A smaller netmask defines fewer networks while accommodating a larger number of IP addresses. Joining or expanding a network allows you to consolidate all of the adjacent networks into the expanded network. Adjacent networks are all networks falling under the netmask of the newly-expanded network.

Each of the adjacent networks join the expanded network and inherit the DHCP member configuration options of the selected network. The expanded network does not inherit the default router and broadcast address configurations of the adjacent networks. Those configurations are disabled by default.

**Note:** The member assignment for the expanded network combines all member assignments of the joining networks.

To join or expand a network:

1. From the Net Map or List panel, select a network, and then click **Join** from the Toolbar.

2. In the **Join Network** editor, do the following:
   — **Address:** Displays the network address. You cannot modify this field.
   — **Netmask:** Displays the netmask of the network as you expand the network.
   — **Join Network slider:** Use the join network slider to specify the available subnet masks for the newly expanded network. Select a smaller netmask value, based on your requirements of the newly-expanded network. When you move the slider, a dialog box displays the total number of IP addresses and the IP address range of a selected subnet mask.

   — **Automatically create reverse-mapping zone:** Select this check box to configure the expanded network to support reverse-mapping zones.

3. **Click OK.**
MANAGING IPv4 ADDRESSES

Grid Manager uses IP addresses as the entry point to the data set containing Infoblox host, DNS, DHCP, and other information related to that address. You can view the data, modify it, assign extensible attributes to the objects associated with the address, and convert DHCP lease types, such as changing a currently active dynamic lease to a fixed address, reservation, or host record.

You can view and manage IPv4 address data in the IP Map and List panels. Grid Manager displays the IP Map and List panels for a specific network after you navigate through the network hierarchy, or when the selected network does not have subnets under it. For information about network map and network list, see Managing IPv4 Networks on page 782.

You can do the following from the IP Map and List panels:

- View IP address usage and details. For information, see IP Map on page 791 and IP Address List on page 792.
- Add IP addresses to existing hosts. For information, see Adding IP Addresses to Existing Host Records on page 794.
- Add fixed addresses and reservations. For information, see Adding Fixed Addresses on page 801 and Modifying Reservations on page 802.
- Add resource records. For information, see Managing Resource Records on page 803.
- Convert objects to other object types. For information, see Converting Objects Associated with IP Addresses on page 794.
- Reclaim IP addresses. For information, see Reclaiming Objects Associated with IP Addresses on page 797.
- Ping IP addresses. For information, see Pinging IP Addresses on page 797.
- Clear DHCP leases. For information, see Clearing Active DHCP Leases on page 797.
- Clear unmanaged IP addresses. For information, see Clearing Unmanaged Data on page 798.
- Configure and run a network discovery. For information, see Network Discovery on page 805.
- Resolve discovery conflicts. For information, see Resolving Conflicting Addresses on page 823.
- Clear discovered data. For information, see Clearing Discovered Data on page 824.

You can also print and export in csv format the information displayed in any panel that supports these functions.
IP Map

The IP Map panel provides a graphical representation of all IPv4 addresses in a given subnet. IP Map displays cells that represent IPv4 addresses. Each cell in the map represents an IPv4 address, and its color indicates its status as described in the legend section. You can run a network discovery on the selected network, and the status of each IP address is updated accordingly. For information, see Chapter 33, Network Discovery, on page 805.

Each IP Map panel can accommodate up to 256 cells with each cell representing an IP address. If a given network has more than 256 addresses, additional IP addresses are displayed by paging to the next page. You can use the page navigation buttons to page through the IP addresses. To go to a specific IP address, you can enter the IP address in the Go to field or click a specific cell in IP Map.

IP Map has a basic and an advanced view. You can toggle between these views by clicking Toggle Basic View or Toggle Advanced View.

In the basic view, the IP Map panel displays the following IP address status:

- **Unused**: An IP address that has not been detected and is not associated with any network device or active host on the network.
- **Conflict**: An IP address that has either a MAC address conflict or a DHCP lease conflict detected through a network discovery.
- **Used**: An IP address that is associated with an active host on the network. It can be a resource record, fixed address, reservation, DHCP lease, or host record.
- **Selected IP**: The IP address that you selected.
- **DHCP Range**: The IP addresses within a DHCP range in the network.

In the advanced view, the IP Map panel displays additional status as follows:

- **Unmanaged**: An IP address that has a discovered host, is not previously known to the appliance, and does not have an A record, PTR record, fixed address, host address, lease, or is not within a DHCP range. You can change an unmanaged address to a host, DHCP fixed address, A record, or PTR record. You can also clear an unmanaged address. All existing administrator permissions apply to the unmanaged addresses.
- **Fixed Address/Reservation**: A host that is either a fixed address or reservation.
- **DNS Object**: An object that is configured for DNS usage.
- **Host Not in DNS/DHCP**: An IP address that is associated with a host record, but is not configured for DHCP or DNS services.
- **Active Lease**: An IP Address that has an active DHCP lease.
- **DHCP Exclusion Range**: A range of IP addresses within a DHCP range. The appliance cannot assign addresses in the exclusion range to a client. You can use these addresses as static IP addresses. This prevents address conflicts between statically configured devices and dynamically configured devices.

You can select an IP address from the IP Map panel and view the following information:

- General information, as described in IP Address Header Panel on page 793.
- Data retrieved through a network discovery or integrated from a PortIQ appliance. For information, see Viewing Discovered Data on page 819.
- The records associated with the IP address, as described in Related Objects on page 801.
- The audit history, as described in Audit History on page 801.
- Detailed lease information, as described in Viewing Detailed Lease Information on page 669.
- Click DHCP View to view DHCP properties of the selected network. For information, see Viewing IPv4 Networks on page 596.
IP Address List

The IP address List panel displays all IPv4 addresses of a selected subnet in table format. The list provides information about the IP addresses in a hierarchy view. You can use this list to view detailed information about each IP address and its related objects in a selected network. This list provides information such as address status, object type, and usage.

You can configure filter criteria to display only IP addresses that you want to see in the table. For example, you can enter "MAC Address begins with 00" as the filter criteria to view only IP addresses that have associated MAC addresses that begin with 00. You can also enter a specific IP address in the Go to field to view information about the address.

By default, Grid Manager displays the following information for the IP addresses, except for Disabled.

- **IP Address**: The IP address of the corresponding record. The appliance highlights disabled DHCP objects in gray. A DHCP object can be a DHCP range, fixed address, reservation, host configured for DHCP, or roaming host with an allocated IP address.
- **Name**: The record name. For example, if the IP address belongs to a host record, this field displays the hostname.
- **MAC Address**: The MAC address of the related record.
- **Status**: The current status of the corresponding record, such as Used, Unmanaged, Conflict, or Unused.
- **Type**: The object type, such as A Record, Fixed Address, or Host Record.
- **Usage**: Indicates whether the IP address is configured for DNS or DHCP.
- **Lease State**: The lease state of the record, such as Active.
- **User Name**: The name of the user who created or modified the record.
- **Comment**: Additional information about the record.
- **Last Discovered**: The time the object was last discovered through discovery.
- **OS**: The operating system of the detected host through a discovery.
- **NetBIOS Name**: The returned NetBIOS name from the last discovery.
- **Site**: The site to which the IP address belongs. This is a predefined extensible attribute.
- **Disabled (hidden)**: Indicates whether the DHCP or DNS record is disabled.

You can display all available extensible attributes. You can also sort the list of IP addresses in ascending or descending order by IP Address only. If you enabled the IP Discovery feature, you can configure the IP List panel to display discovered data and fields imported from PortIQ appliances. For information about the PortIQ data, see *Integrating Data from PortIQ Appliances* on page 818. For information about customizing the tables in Grid Manager, see *Customizing Tables* on page 44.

You can select an IP address from the List panel and view the following information about it:

- General information, as described in *IP Address Header Panel* on page 793.
- Data retrieved through a network discovery or integrated from a PortIQ appliance, as described in *Viewing Discovered Data* on page 819.
- The records associated with the IP address, as described in *Related Objects* on page 801.
- Audit history, as described in *Audit History* on page 801.
- Detailed lease information, as described in *Viewing Detailed Lease Information* on page 669.

You can also do the following from the IP List panel:

- Click *Go to DHCP View* to view DHCP properties of a selected network. For information, see *Viewing IPv4 Networks* on page 596.
- Click the Ping icon to ping a selected IP address. For information, see *Pinging IP Addresses* on page 797.
Filtering the IP Address List

You can filter the IP address list, so it displays only the IP addressees you need. You can filter the list based on any combination of extensible attributes and the parameters displayed in the IP address list, such as usage and type. When you expand the list of available fields you can add to the filter, note that the extensible attributes are those with the gray background.

IP Address Header Panel

When you select an IP address from the IP Map or List panel, Grid Manager displays information about the highest priority object associated with the IP address. Depending on the object type, Grid Manager displays all or some of the following information. For example, if the highest priority object is a fixed address, Grid Manager displays only the object type, MAC address, lease state, and comment of the object.

• **Type**: The object or record type, such as A record, PTR record, or host record.
• **Name**: The name of the object. For example, if the IP address belongs to a host record, this field displays the hostname. The appliance highlights disabled DHCP objects in gray. A DHCP object can be a DHCP range, fixed address, reservation, host configured for DHCP, or roaming host with an allocated IP address.
• **MAC**: The MAC address of the network device associated with the IP address.
• **Lease State**: The current status of the DHCP lease.
• **Comment**: Comments about the IP address.

Related Objects

The Related Objects tab displays the following information about the records associated with the IP address:

• **Name**: The name of the object. For example, if the IP address belongs to a host record, this field displays the hostname. The appliance highlights disabled DHCP objects in gray. A DHCP object can be a DHCP range, fixed address, reservation, host configured for DHCP, or roaming host with an allocated IP address.
• **Type**: The object type, such as DHCP lease, host, A record, and bulk host.
• **Comment**: Information about the object.

You can also select the following for display:

• **DNS view**: The DNS view to which the object belongs.

You can do the following in this tab:

• Add a resource record. You can select the following from the drop-down list:
  — Add Host Record, as described in *Adding Host Records* on page 804.
  — Add Fixed Address, as described in *Adding Fixed Addresses* on page 801.
  — Add Reservation, as described in *Adding Reservations* on page 802.
  — Add A Record, as described in *Adding A records* on page 803.
  — Add PTR Record, as described in *Adding PTR Records* on page 804.
• Edit the properties of the selected object. Depending on the type of object, Grid Manager displays the corresponding editor for the object. For example, if the selected object is a fixed address, Grid Manager displays the fixed address editor. When you select a lease object, Grid Manager displays the lease viewer.
• Delete a selected object or multiple objects.
• When you select a lease object and click the Show Details icon, you can view the lease start and end dates.
• Depending on the object type, you can convert a selected object to one of the following:
  — Reservation
  — Host
  — Fixed Address
• View detailed lease information about the IP address, as described in *Viewing Detailed Lease Information* on page 669.
• Print and export the information in the Related Objects table.
Audit History

By default, the Audit History tab displays the following information about the last five actions performed on the selected IP:

- **Timestamp**: The day, date, and time of the operation.
- **Action**: The type of operation that was performed by the administrator.
- **Object Type**: The object type of the entry.
- **Object Name**: The name of the object.
- **Admin Name**: The name of the administrator who performed the operation.
- **Message**: The description of the administrative activity.

Adding IP Addresses to Existing Host Records

You can add unused and unmanaged addresses, including all their information, to existing host records. When you add an unmanaged address to a host record, the appliance adds the discovered data to the host record. You can select the desired host to which you want to add the unmanaged address.

To add an unmanaged IP address to an existing host record:

1. From the IP Map or List panel, select an IP address, and then click Add -> Add to Existing Host from the Toolbar.
2. In the Select Host dialog box, do the following:
   - In the table, select the host to which you want to add the selected IP address. You can also use the filters or the Go To field to narrow down the host list. For information, see Using Filters on page 49 and Using the Go To Function on page 51.
   - Click the Select icon.
Grid Manager displays the Host Record editor.
3. In the Host Record editor, update the host properties as described in Modifying Host Records on page 804.
4. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save the entry, and Grid Manager displays the Host Record editor for additional configurations.
   To close the editor without saving the changes, click the Close icon.

Converting Objects Associated with IP Addresses

The NIOS appliance provides a simple mechanism for converting unmanaged IP addresses to resource records, such as host records and A records. You can also convert the active lease of a dynamically assigned IP address to a fixed address, reservation, or Infoblox host record. Using the conversion mechanism, you can keep the existing information of a network device during the conversion.

The appliance supports the following conversions:

- DHCP leases to fixed addresses, reservations, or host records
- Fixed addresses to reservations or host records
- Unmanaged addresses to host records, A records, PTR records, or fixed addresses
- A records to host records
- PTR records to host records

**Note:** You cannot convert unmanaged IP addresses or leases served by Microsoft DHCP servers to host records.
Converting DHCP Leases

To create a fixed address, you bind an IP address to a MAC address. You can make that binding by converting an active dynamically leased address to a fixed address. The lease conversion transforms the temporary binding between the IP address and MAC address in the dynamic lease to a persistent one. The lease must be active so that the NIOS appliance has an IP-to-MAC address binding to convert into a fixed address.

The appliance uses the following rules when converting a DHCP lease:

- If a DHCP lease is converted to a fixed address, the appliance copies the client identifier to the fixed address, based on information in the lease. If the appliance finds the client identifier in the lease information, the appliance includes it when it creates the host. If it finds the MAC address, the appliance includes it when it creates the host. If it finds both, the appliance includes only the MAC address (default) when it creates the host.
- If you try to convert a DHCP lease or a fixed address with a client identifier, not a MAC address, to a host, the appliance displays an error message in the host editor. This ensures that you do not attempt this operation and lose the data.
- You cannot create two fixed addresses with the same client identifier or MAC address in the same network.
- If the appliance receives a second DHCP request with the same client identifier, it provides the same fixed IP address if the lease is still binding.

Figure 32.4  Converting a Dynamic Lease to a Fixed Lease

An advantage of converting an active dynamic lease is that you do not need to learn the MAC address of the device to which you want to assign an IP address and manually enter it in the fixed address configuration.

A reservation is an address that you exclude from DHCP use because you intend to configure that address manually on a device, such as a firewall, router, or printer. You can also convert a fixed address or a dynamic address with an active lease to a reservation.

When you convert an address in a DHCP range to a reservation, you reduce the total number of dynamically assignable addresses in that range by one. Correspondingly, this reduces the number of allocated addresses needed to exceed a high or low watermark threshold for that range.
Note: To return an IP address to its place in a DHCP range after converting it from an active dynamic lease to a fixed address, reservation, or Infoblox host, delete the fixed address, reservation, or host to which you previously converted the IP address. The IP address then becomes part of the DHCP range to which it first belonged.

You can convert fixed addresses to reservations, as shown in Figure 32.5.

Figure 32.5 Converting a Dynamic Lease or Fixed Address to a Reservation

To convert an object:
1. From the IP Map or List panel, select an IP address.
2. In the Related Objects tab, select the check box of the object, and then click Convert from the Toolbar or navigation bar.
3. Select the object type to which you want to convert the object. Grid Manager displays the corresponding editor for the object type.
4. For all conversions, Grid Manager populates the discovered information in the corresponding editor. Depending on the type of conversion, do one of the following:
   - For host record conversions, see Modifying Host Records on page 804.
   - For reservation conversions, see Modifying Reservations on page 802.
   - For fixed address conversions, see Modifying Fixed Addresses on page 802.
   - For A record conversions, see Modifying A records on page 803.
   - For PTR record conversions, see Modifying PTR Records on page 804.

Note: When you select an object for conversion, Grid Manager displays only the available conversion types for the object. You must save the changes in the editor for the conversion to take place.
Reclaiming Objects Associated with IP Addresses

You can use the reclaim IP function to delete all the objects that are associated with a selected IP address. When you reclaim an IP address, Grid Manager deletes the associated objects and puts them in the Recycle Bin, if enabled. You can reclaim any used and unmanaged IP addresses. You can also select multiple IP addresses for this function. After you reclaim an IP address, the address status changes to Unused. You can then reassign the IP address to other objects. For example, when you reclaim a fixed address, Grid Manager deletes the fixed address object and puts it in the Recycle Bin. When you reclaim an IP address that is associated with a host record and the address is the only address in the host, Grid Manager deletes the host record.

Grid Manager deletes all the objects that are associated with the selected IP addresses and puts them in the recycle bin, with the following exceptions:

- When you reclaim IP addresses that are in a DHCP range, all the objects that are associated with the IP addresses are deleted and the IP addresses remain in the DHCP range.
- When you select an IP address that is part of a host record, only the selected IP address is deleted from the host. However, if the selected address is the only address in the host, Grid Manager deletes the host record.

Grid Manager does not reclaim the following:

- Unused IP addresses
- Bulk hosts

To reclaim an IP address:

1. From the IP Map or List panel, select the IP address you want to reclaim, and then click Reclaim from the Toolbar. You can select multiple IP addresses.
2. In the Delete Confirmation dialog box, click Yes. Grid Manager puts the deleted objects in the Recycle Bin, if enabled.

Pinging IP Addresses

You can find out whether an IP address is accessible and active by pinging the address. Grid Manager sends a packet to the selected IP address and waits for a reply when you ping the address. You can ping individual IP addresses from the IP Map and IP List panels. You can ping all IP addresses from the IP Map panel only.

To ping an IP address:

- From the IP Map or IP List panel, select the IP address that you want to ping, and then click Ping from the Toolbar.

To ping all IP addresses:

- From the IP Map panel, click Multi-ping from the Toolbar. Grid Manager pings all IP addresses displayed in the IP Map panel and displays the ping status in the panel.

When the ping or multi-ping is complete, the status bar displays the number of active IP addresses detected through the ping. To close the ping status bar, click the Close icon.

Clearing Active DHCP Leases

A DHCP lease specifies the amount of time that the DHCP server grants to a network device the permission to use a particular IP address. You may sometimes need to terminate an active lease. The following are some of the reasons for clearing active DHCP leases:

- When a network device is moved to another network.
- Reset a DHCP lease to fix other problems.

In Grid Manager, you can select multiple IP addresses and clear their active DHCP leases.

To clear an active lease:

1. From the IP Map or List panel, select the IP address for which you want to clear a DHCP lease, and then click Clear -> Clear Lease from the Toolbar. You can select multiple IP addresses.
2. In the Clear DHCP Lease Confirmation dialog box, click Yes.
Clearing Unmanaged Data

You can clear the status of unmanaged data at the network and IP address levels. When you clear an unmanaged address, the status of the IP address changes to Unused. An unmanaged address is an IP address with a discovered host, is not previously known to the appliance, and does not have an A record, PTR record, fixed address, host address, lease, or is not within a DHCP range. You can change an unmanaged address to a host, a DHCP fixed address, an A record, or a PTR record. You can also clear the unmanaged data associated with the address.

To clear unmanaged data:
1. From the IP Map or List panel, select the IP address for which you want to clear unmanaged data, and then click Clear -> Clear Unmanaged Data from the Toolbar. You can select multiple IP addresses.
2. In the Clear Unmanaged data dialog box, click Yes.

Managing IPv6 Networks and IP Addresses

You can use Grid Manager to manage IPv6 networks and their AAAA, PTR and host resource records. You can configure IPv6 networks and track IP address usage in those networks. You can also split and join IPv6 networks, when necessary. Note that the Infoblox appliance does not currently serve DHCP to IPv6 networks.

Grid Manager uses network containers to group IPv6 networks. For information, see About Network Containers on page 780.

Adding IPv6 Networks

To add an IPv6 network:
1. From the Data Management tab, select the IPAM tab, and then click Add -> Add IPv6 Network from the Toolbar.
2. In the Add IPv6 Network wizard, complete the following:
   - Address: Enter the IPv6 network address. When you enter an IPv6 address, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2006:0000:0000:0123:4567:89ab:0000:cdef can be shortened to 2006::123:4567:89ab:0:cdef. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The NIOS appliance displays an IPv6 address in its shortened form, regardless of its form when it was entered.
   - Netmask: Enter the appropriate netmask between 3 and 128.
   - Comment: Optionally, enter information about the network.
   - Automatically create a reverse-mapping zone: Select this check box if you want the appliance to automatically create the corresponding reverse-mapping zone for the network. If you select this check box, you can view the reverse zone in the Grid Manager GUI. The appliance automatically creates reverse-mapping zones only if the netmask is between /4 through /128, in increments of 4 (that is, /4, /8, /12, and so on until /128).
3. Click Next to enter values for extensible attributes for the network. For information, see Using Extensible Attributes on page 225
4. Select one of the following:
   - Save & Edit: Save the entry and configure additional parameters.
   - Save & New: Save the entry and create a new network.
   - Save & Close: Save the entry and close the wizard.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a data, time, and time zone. For information, see Scheduling Tasks on page 25.
Modifying IPv6 Networks

After you add an IPv6 network through the wizard, you can modify some of its parameters.

To modify the parameters of an IPv6 network:

1. Click the check box beside the IPv6 network, and then click the Edit icon.

2. The IPv6 Network editor provides the following tabs from which you can modify data:
   - **General**: You can modify the Comment field for a network.
   - **Extensible Attributes**: You can add, change, and delete extensible attributes that are associated with a specific network. For information about extensible attributes, refer to Using Extensible Attributes on page 225.
   - **Permission**: This tab displays only if you have superuser admin account. For information, see About Administrative Permissions on page 87.

3. Select one of the following:
   - **Save & Close**: Save the entry and close the editor.
   - **Save**: Save your changes and leave the editor open.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a data, time, and time zone. For information, see Scheduling Tasks on page 25.

Splitting IPv6 Networks into Subnets

You can create smaller subnets simultaneously within a network by splitting it. You do not have to configure each subnet individually. You can create smaller subnets with larger netmasks. A larger netmask defines a larger number of network addresses and a smaller number of IP addresses.

To split an IPv6 network:

1. From the Data Management tab, select the IPAM tab -> network check box, and then click Split from the Toolbar.

2. In the Split Network editor, do the following:
   - **Address**: Displays the network address. You cannot modify this field.
   - **Netmask**: Specify the appropriate netmask for each subnet.
   - **Immediately add all possible networks**: Select this check box if you want Grid Manager to create all the subnets that result from splitting the network. Clear the check box to create a network container.
     Note that when you add a large number of networks, it could take a little longer for Grid Manager to display the networks.
   - **Automatically create reverse-mapping zone**: Select this check box to have the appliance automatically create reverse-mapping zones for the subnets. The appliance automatically creates reverse-mapping zones only if the netmask is between /4 through /128, in increments of 4 (that is, /4, /8, /12, and so on until /128).

3. Click **OK**.
Joining IPv6 Networks

Joining multiple networks into a larger network is the opposite of splitting a network. You can select a network and expand it into a larger network with a smaller netmask. A smaller netmask defines fewer networks while accommodating a larger number of IP addresses. Joining or expanding a network allows you to consolidate all of the adjacent networks into the expanded network. Adjacent networks are all networks that fall under the netmask of the newly-expanded network.

To join or expand a network:
1. From the Data Management tab, select the IPAM tab -> network check box, and then click Join from the Toolbar.
2. In the Join Network editor, do the following:
   - Address: Displays the network address. You cannot modify this field.
   - Netmask: Enter the netmask of the expanded network.
   - Automatically create reverse-mapping zone: Select this check box to configure the expanded network to support reverse-mapping zones. The appliance automatically creates reverse-mapping zones only if the netmask is between /4 through /128, in increments of 4 (that is, /4, /8, /12, and so on until /128).
3. Click OK.

Deleting IPv6 Networks

To delete an IPv6 network:
1. From the Data Management tab, select the IPAM tab -> network check box. You can select multiple check boxes for multiple networks.
2. Select Delete or Schedule Delete from the Delete drop-down menu.
3. To delete the network now, in the Delete Confirmation dialog box, click Yes. To schedule a deletion, see Scheduling Tasks on page 25.
   The appliance puts the deleted network in the Recycle Bin, if enabled.

Managing IPv6 Addresses

You can assign IPv6 addresses to AAAA, PTR, and host records. When you select an IPv6 network, you can list the configured IP addresses in that network. You can then drill down and view the records associated with that IP address.

To list the configured IP addresses in an IPv6 network:
- From the Data Management tab, select the IPAM tab, and then click the IPv6 network you want to view.
Grid Manager lists the configured IPv6 addresses. You can export and print the list. It displays the following information about each IP address:
- Name: The name of the record associated with the IP address.
- MAC Address: The MAC address of the device that was assigned the IP address.
- Status: The status of the IP address.
- Type: The resource record types associated with the IP address. For IPv6 addresses, these are AAAA, host and PTR records.
- Usage: Indicates that the IPv6 address is used for DNS.
- Comment: Displays comments about the record.
From the list, you can select an IP address and do the following:
- Reclaim it
- View its associated records
You can drill down further and view the records associated with an IP address. To view the associated records of an IP address, select it and Grid Manager displays information about the IP address in the Related Objects and Audit History tabs.
Related Objects

Grid Manager displays the following information about the records associated with the IP address:

- **Name**: The record name. For example, if the IP address belongs to a host record, this field displays the hostname.
- **Type**: The object type. For example, AAAA Record, PTR Record, or Host Record.
- **Comment**: Additional information that was entered in the record about the IP address.

Audit History

Grid Manager displays the following information about the last five actions performed on the selected IP:

- **Timestamp**: The day, date, and time of the operation.
- **Action**: The type of operation that was performed by the administrator.
- **Object Type**: The object type of the entry.
- **Admin Name**: The name of the administrator that performed the operation.
- **Message**: Description of the administrative activity.

Filtering the IP Address List

You can filter the IP address list, so it displays only the IP addresses you need. You can filter the list based on any combination of extensible attributes and the parameters displayed in the IP address list, such as usage and type. When you expand the list of available fields you can add to the filter, note that the extensible attributes are those with the gray background.

Managing IP Address Data

You can manage and track the allocation of IP addresses. You can assign fixed address to network devices and create reservations as described in the following sections:

- **Fixed Addresses**
- **Reservations** on page 802

Fixed Addresses

A fixed address represents a persistent link between an IP address and a MAC address or a client identifier, so that every time the DHCP client with that MAC address or identifier requests an IP address, the DHCP server assigns it the same address. For information, see *Configuring Fixed Addresses* on page 608.

You can also convert an active dynamically leased address to a fixed address. The lease conversion transforms the temporary binding between the IP address and MAC address in the dynamic lease to a persistent one. For information, see *Converting DHCP Leases* on page 795.

Adding Fixed Addresses

You can add fixed addresses from the following panels in the IPAM tab:

- **IPAM Home**
- **Net Map and List panels**
- **IP Map and List panels**

To add a fixed address:

1. From the **Data Management** tab, select the **IPAM** tab, and then click **Add -> Add Fixed Address** from the Toolbar.
2. In the **Add Fixed Address** wizard, complete the fields as described in *Adding Fixed Addresses* on page 609.
Modifying Fixed Addresses

To modify a fixed address:
1. From the Data Management tab, select the IPAM tab -> network -> fixed_address check box, and then click the Edit icon.
2. In the Fixed Address editor, modify information as described in Modifying Fixed Addresses on page 610.

Reservations

A reservation is an IP address that you exclude from DHCP use because you intend to configure the address manually on a network device. For information, see Configuring Reservations on page 611.

You can add a reservation or convert a fixed address or a dynamic address with an active lease to a reservation. For information, see Converting Objects Associated with IP Addresses on page 794.

Adding Reservations

You can add reservations from the following panels in the IPAM tab:

- IPAM Home
- Net Map and List panels
- IP Map and List panels

To add a reservation:
1. From the Data Management tab, select the IPAM tab, and then click Add -> Add Reservation from the Toolbar.
2. In the Add Reservation wizard, complete the fields as described in Adding Reservations on page 611.

Modifying Reservations

To modify a reservation:
1. From the Data Management tab, select the IPAM tab -> network -> reservation check box, and then click the Edit icon.
2. In the Reservation editor, modify information as described in Modifying Reservations on page 612.
Managing Resource Records

In the IPAM tab, you can manage the following resource records that are associated with IP addresses:

- **A Records**
- **AAAA Records**
- **PTR Records**
- **Host Records**

### A Records

An A (address) record is a DNS resource record that maps a domain name to an IPv4 address. To define a specific name-to-address mapping, you can add an A record to a previously defined authoritative forward-mapping zone. In Grid Manager, you can add, modify, and delete A records. For information, see Managing A Records on page 452.

#### Adding A records

You can add A records from the following panels in the IPAM tab:

- IPAM Home
- Net Map and List panels
- IP Map and List panels

To add an A record:

1. From the Data Management tab, select the IPAM tab, and then click Add -> Add A Record from the Toolbar.
2. In the Add A Record wizard, complete the fields as described in Adding A records on page 803.

#### Modifying A records

To modify an A record:

1. From the Data Management tab, select the IPAM tab -> network -> ip_addr -> a_record check box in the Related Objects tab, and then click the Edit icon.
2. In the A Record editor, modify information as described in Modifying A records on page 803.

### AAAA Records

An AAAA (quad A address) record maps a domain name to an IPv6 address. To define a specific name-to-address mapping, add an AAAA record to a previously defined authoritative forward-mapping zone. You can also select an AAAA record and create a Host and PTR record for the same IP address. For information, see Managing AAAA Records on page 454.

#### Adding AAAA Records

To add an AAAA record:

1. From the Data Management tab, select the IPAM tab, and then click Add -> Add AAAA Record from the Toolbar.
2. In the Add AAAA Record wizard, complete the fields as described in Adding AAAA Records on page 454.

#### Modifying AAAA Records

To modify an AAAA record:

1. From the Data Management tab, select the IPAM tab -> network -> ip-addr -> aaaa_record check box in the Related Objects tab, and then click the Edit icon.
2. In the AAAA Record editor, modify information as described in Modifying AAAA Records on page 455.
**PTR Records**

A PTR (pointer) record is a DNS resource record that maps an IP address to a hostname, and can only be added for a reverse mapping zone. You must first create a reverse mapping zone before adding a PTR record for the zone. To create a PTR record, you need to specify a domain name and a hostname. For information, see *Managing PTR Records* on page 455.

**Note:** You must configure PTR records manually for IPv6 addresses.

**Adding PTR Records**

To add a PTR record:

1. From the Data Management tab, select the IPAM tab, and then click Add -> Add PTR Record from the Toolbar.
2. In the Add PTR Record wizard, complete the fields as described in *Adding PTR Records* on page 455.

**Modifying PTR Records**

To modify a PTR record:

1. From the Data Management tab, select the IPAM tab -> network -> ip_addr-> ptr_record check box, and then click the Edit icon.
2. In the PTR Record editor, modify information as described in *Modifying PTR Records* on page 455.

**Host Records**

Infoblox host records are data objects that contain DNS and DHCP information, network discovery data, and information for network devices. For information, see *About Host Records* on page 442.

You can choose to manually add individual host records or bulk hosts. For information, see *About Bulk Hosts* on page 446.

**Adding Host Records**

You can add host records from the following panels in the IPAM tab:

- IPAM Home
- Net Map and List panels
- IP Map and List panels

To add a host record:

1. From the Data Management tab, select the IPAM tab, and then click Add -> Add Host Record from the Toolbar.
2. In the Add Host Record wizard, complete the fields as described in *Adding Host Records* on page 444.

**Modifying Host Records**

To modify a host record:

1. From the Data Management tab, select the IPAM tab -> network -> ip_addr-> host_record check box in the Related Objects tab, and then click the Edit icon.
2. In the Host Record editor, modify information as described in *Modifying Host Records* on page 445.
Chapter 33  Network Discovery

This chapter provides information about the Infoblox discovery process, and how you can use the discovery feature to gather and manage information about predefined networks as well as virtual entities on VMware vSphere servers. It also explains how to integrate and view data from Infoblox PortIQ appliances. This chapter includes the following sections:

- **About Network Discovery** on page 806
  - Administrative Permissions on page 807
  - IP Discovery Process on page 808
  - Supported IP Discovery Methods on page 809
  - VM Discovery Process on page 811
- **About Configuring a Discovery** on page 812
  - Considerations Before Starting a Discovery on page 813
  - Selecting a Grid Member on page 814
  - Enabling or Disabling the Merging of Discovered Data on page 814
  - Updating Discovered Data for Managed Objects on page 815
  - Configuring IP Discovery on page 815
  - Configuring VM Discovery on page 816
  - Starting a Discovery on page 817
  - Scheduling a Discovery on page 817
  - Managing a Discovery on page 817
  - Monitoring Discovery Status on page 817
- **Integrating Data from PortIQ Appliances** on page 818
- **Viewing Discovered Data** on page 819
  - Viewing Data in IP Map on page 819
  - Viewing Data in IP List on page 820
  - Viewing Data in the Discovered Data Section on page 820
- **Managing Discovered Data** on page 821
  - Managing Unmanaged Data on page 821
  - Resolving Conflicting Addresses on page 823
  - Clearing Discovered Data on page 824
ABOUT NETWORK DISCOVERY

The appliance provides discovery tools for detecting active hosts on predefined networks and on specified VMware vSphere servers. You can use the discovery feature to obtain and manage information about your network hosts. Depending on which discovery method you use, the appliance returns information, such as IP addresses, MAC addresses, and operating systems, about the detected hosts and virtual entities.

You can include one or both of the following in a discovery task:

- **IP discovery**: The appliance detects active hosts on specified networks in a network view. You can perform an IP discovery using the following protocols: ICMP (Internet Control Message Protocol), NetBIOS (Network Basic Input/Output System), and TCP (Transmission Control Protocol). For information, see Supported IP Discovery Methods on page 809.

- **VM discovery**: The appliance detects active hosts on specified VMware vSphere servers. It also collects vSphere-specific data about the virtual entities on the specified vSphere servers. For information, see VM Discovery Process on page 811.

After a discovery, the appliance updates the database with the discovered data. It can either merge the newly discovered data or update only the unmanaged data. Unmanaged data is information that is not configured for DNS or DHCP before the discovery. For information about the guidelines the appliance uses to update the database, see Considerations Before Starting a Discovery on page 813.

You can configure and initiate a discovery from the Discovery Manager wizard. You must first select a grid member to run the discovery. You can run an IP discovery on a set of networks and a VM discovery on a set of VMware vSphere servers. After you configure a discovery task, the grid master sends a discovery request to the selected grid member. The discovery request contains information, such as the target network view, networks, and discovery method. Depending on your configuration, the selected grid member runs an IP discovery on the predefined networks. When VM discovery is configured, it also collects information about virtual entities from the specified vSphere servers. The grid member then reports the discovered results to the grid master. For information, see About Configuring a Discovery on page 812.

After a discovery is complete, you can view and manage the discovered data. For information, see Viewing Discovered Data on page 819 and Managing Discovered Data on page 821. You can also use the discovered data, such as unmanaged data, last discovered timestamps, and virtual machine data, as filters for Smart Folders. For information, see Creating Smart Folders on page 70. The appliance records all discovery operations in the audit log.
**Administrative Permissions**

You can initiate a discovery and manage discovered data based on your administrative permissions. For information, see *Managing Administrators* on page 77.

You must have read/write permission to discovery to initiate and control a discovery. The following are permission guidelines for initiating and controlling a discovery:

- Superusers can initiate and control a discovery on all networks.
- Administrators with read/write permission to discovery can initiate and control an IP discovery on networks to which they have read/write or read-only permission. They can also initiate a VM discovery. Only the objects with IP addresses to which the administrators have read/write permission are updated to include the vSphere discovered data.

After a discovery is complete, the following permission guidelines apply to viewing and managing discovered data:

- Superusers can view and manage all discovered data.
- Administrators with read/write permission to networks can view all discovered data. They can also add unmanaged data to existing hosts, and resolve IP address conflicts.
- Only administrators with read/write permission to a DNS zone or specific record type can convert unmanaged data to a host, fixed address, reservation, A record, or PTR record.
- Administrators with read-only permission to networks can only view discovered data. They cannot change any discovered data.
IP Discovery Process

Once an IP discovery starts, the grid member reports the discovery status, such as Completed, Running, Paused, Stopped, or Error, in the Discovery Manager wizard and the Discovery Status widget on the Dashboard. In the Discovery Status widget, Grid Manager reports the time when the discovery status was last updated and the numbers of each type of discovered data. For information, see Monitoring Discovery Status on page 817.

When an IP discovery starts, the appliance divides the IP addresses in a network into chunks, with each chunk containing 64 contiguous IP addresses. The discovery process probes each IP address in parallel and in ascending order, reports the detected information, updates the progress report, and then moves on to the next chunk until it hits the last chunk of IP addresses. The appliance then updates the database with the discovered data.

An IP discovery scans the selected networks in the order the networks appear in the Discover Manager wizard. Figure 33.2 illustrates how an IP discovery works.

Figure 33.2 IP Discovery Process
Supported IP Discovery Methods

When you perform an IP discovery, you can choose one of the following discovery methods:

- **ICMP**—For information, see [ICMP](#).
- **NetBIOS**—For information, see [NetBIOS](#).
- **TCP**—For information, see [TCP](#).
- **Full**—For information, see [Full](#).

These methods actively scan predefined networks and probe IP addresses. The grid member listens for responses from the IP addresses as proof of activities. The IP discovery scans through the specified network ranges and probes IP addresses in each network, except for the /31 and /32 subnets as well as the network, broadcast, and multicast address types.

**ICMP**

This method detects active hosts on a network by sending ICMP echo request packets (also referred to as pings) and listening for ICMP echo responses. The ICMP discovery is a simple and fast discovery that detects whether an IP address exists or not. It returns only the IP address and MAC address (only if the grid member running the discovery is on the same discovered network) of a detected host. The ICMP discovery might miss some active hosts on the network due to security measures that are put in place to block ICMP attacks.

You configure the timeout value and the number of attempts in the [Discovery Manager](#) wizard. The ICMP discovery method returns the following information for each detected host:

- **IP address**: The IP address of the host.
- **MAC address**: The discovery returns the MAC address only if the grid member running the discovery is on the same discovered network.

To use the ICMP discovery method, the ICMP protocol between the grid member performing the discovery and the target networks must be unfiltered.

**NetBIOS**

The NetBIOS method queries IP addresses for an existing NetBIOS service. This method detects active hosts by sending NetBIOS queries and listening for NetBIOS replies. It is a fast discovery that focuses on Microsoft hosts or non-Microsoft hosts that run NetBIOS services.

You configure the timeout value and the number of attempts in the [Discovery Manager](#) wizard. This method returns the following information for each detected host:

- **IP address**: The IP address of the host.
- **MAC address**: Only if the discovered host is running Microsoft.
- **OS**: This value is set to [Microsoft](#) for an active host that has a MAC address in the NetBIOS reply.
- **NetBIOS name**: This value is set to the name returned in the NetBIOS reply.

To use the NetBIOS discovery method, ports 137 (UDP/TCP) and 139 (UDP/TCP) between the grid member performing the discovery and the target networks must be unfiltered.
TCP

The TCP discovery probes each active host on a list of TCP ports using TCP SYN packets. This method detects all active hosts that generate SYN ACK responses to at least one TCP SYN. The discovery can determine the OS on a host by analyzing how the host reacts to the requests on opened and closed ports. It then uses the TCP fingerprints to guess the OS. To obtain a TCP fingerprint, IP discovery provides two scanning techniques, SYN and CONNECT.

When you use the SYN technique, the discovery sends a TCP SYN packet to establish a connection on a TCP port. If the port is open, the host replies with a SYN ACK response. The discovery does not close the port connection.

The CONNECT technique is a three-way TCP handshake. The discovery starts with the same process as the SYN technique by sending the TCP SYN packet. If the host replies with a SYN ACK response, the discovery then sends a RST packet to close the connection. If the response contains a RST flag, it indicates that the port is closed. If there is no reply, the port is considered as filtered. The TCP discovery is a deliberate and accurate discovery method. It can basically detect all active hosts on a network provided that there are no firewalls implemented on the network.

You can select the TCP ports, the TCP scanning technique, and configure the timeout value and the number of attempts in the Discovery Manager wizard. This method returns the following information for each detected host:

- IP address: The IP address of the host.
- MAC address: The discovery returns the MAC address only if the grid member running the discovery is on the same discovered network.
- OS: This is set to the highest probable OS reported in the response.

To use the TCP discovery method, the TCP port and a specific set of ports between the grid member and the discovered networks must be unfiltered. The default set of ports is defined by the factory settings.

Full

The full discovery method is a combination of an ICMP discovery, a NetBIOS discovery, a TCP discovery, and a UDP scan. This method starts by sending an ICMP echo request. If no IP address on the network responds to the ICMP request, the discovery ends. If there is at least one response to the ICMP echo request, a NetBIOS discovery starts. A TCP discovery then follows by skipping through the active hosts that the NetBIOS discovery detects. The TCP discovery also handles the NetBIOS-detected hosts that have no MAC addresses. This method also performs a UDP scan to determine which UDP ports are open.

You configure the timeout value and the number of attempts in the Discovery Manager wizard. The full discovery method returns the following information for each detected host:

- IP address
- MAC address
- OS
- NetBIOS name

To use the full discovery, all the filter and firewall requirements in the ICMP, NetBIOS, and TCP discovery methods apply.
The following is a summary of the supported IP discovery methods:

<table>
<thead>
<tr>
<th>Discovery Type</th>
<th>Returned Data</th>
<th>Guideline</th>
<th>Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP</td>
<td>• IP address</td>
<td>Use ICMP for a rough and fast discovery</td>
<td>ICMP echo request and reply</td>
</tr>
<tr>
<td></td>
<td>• MAC address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetBIOS</td>
<td>• IP address</td>
<td>Use NetBIOS for discovering Microsoft networks or non-Microsoft networks that run some NetBIOS services</td>
<td>NetBIOS query and reply</td>
</tr>
<tr>
<td></td>
<td>• MAC address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NetBIOS name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>• IP address</td>
<td>Use TCP for an accurate but slow discovery</td>
<td>TCP SYN packet and SYN ACK packet</td>
</tr>
<tr>
<td></td>
<td>• MAC address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full</td>
<td>• IP address</td>
<td>Use Full for a general and comprehensive discovery</td>
<td>1. ICMP echo request and reply</td>
</tr>
<tr>
<td></td>
<td>• MAC address</td>
<td></td>
<td>2. NetBIOS query and reply</td>
</tr>
<tr>
<td></td>
<td>• OS</td>
<td></td>
<td>3. TCP SYN packet and SYN ACK packet</td>
</tr>
<tr>
<td></td>
<td>• NetBIOS name</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The method you select to run an IP discovery determines the kind of information the discovery returns and the time it takes to complete an IP discovery. If time is a concern, the following are factors you may consider when configuring an IP discovery:

- The timeout value
- The number of attempts
- The number of ports the discovery scans
- The size of network you want to discover

**VM Discovery Process**

When you perform a VM discovery, the appliance communicates with the specified vSphere servers to collect vSphere-specific data. Unlike IP discovery, VM discovery processes all the IP addresses on the specified vSphere servers. Therefore, VM discovery can discover IP addresses in all the networks within the selected network view.

The following is a summary of the VM discovery:

<table>
<thead>
<tr>
<th>Discovery Type</th>
<th>Returned Data</th>
<th>Guideline</th>
<th>Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM discovery</td>
<td>• IP address</td>
<td>Add the VMware vSphere servers on which you want to perform the VM discovery</td>
<td>The appliance communicates with the vSphere servers to collect discovered data</td>
</tr>
<tr>
<td></td>
<td>• MAC address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Discovered name</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Virtual entity type</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Virtual entity name</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Virtual cluster</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Virtual datacenter</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Virtual switch</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Virtual host</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Virtual host adapter</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Network Discovery

About Configuring a Discovery

You can configure and control a discovery from the Discovery Manager wizard, which is accessible from the Discovery Status widget on the Dashboard or from the Data Management tab -> IPAM tab. In a grid, only one member can run a discovery at a time. Multiple members cannot run discoveries simultaneously.

The following are guidelines for configuring a discovery task:

- You must have read/write permission to the discovery process to initiate a discovery.
- After you start a discovery, you cannot change the configuration of the discovery.

You can perform the following tasks from the Discovery Manager wizard:

- Select the grid member from which you want to run the discovery. For an IP discovery, the grid member does not need to be assigned to the discovered network or within a DHCP range. For information, see Selecting a Grid Member on page 814.
- Optionally, enable or disable the merging of discovered data with existing data. This function is enabled by default. For information, see Enabling or Disabling the Merging of Discovered Data on page 814.
- Configure an IP discovery. For information, see Updating Discovered Data for Managed Objects on page 815. You must first define the networks on which you want to run an IP discovery. For information, see About DHCP Networks on page 594.
- Add the vSphere servers on which you want to run a VM discovery. For information, see Configuring VM Discovery on page 816.

You can include both the IP discovery and VM discovery in a discovery task. Note that the IP discovery and VM discovery are enabled by default for a new NIOS installation. For an upgrade, the IP discovery is enabled and the VM discovery is disabled.

After you configure a discovery, you can start the discovery immediately or schedule the start of the discovery task for a later date. For information, see Starting a Discovery on page 817 and Scheduling a Discovery on page 817. After you start a discovery, you can pause or stop it. For information, see Managing a Discovery on page 817. The appliance saves the configuration of the last discovery.

You can do the following after a discovery is complete:

- View the discovery status. You can view the current discovery status in the Discovery Status widget on the Dashboard. For information, see The Dashboard on page 55.
- View the discovered data. For information, see Viewing Discovered Data on page 819.
- Manage the discovered data. For information, see Managing Discovered Data on page 821.
Considerations Before Starting a Discovery

The following are some guidelines for consideration before you start a discovery.

Database updates

After the grid master receives discovery data from the grid member, it integrates the data based on the following rules:

- For a discovered host with a new IP address, the appliance marks the IP address “unmanaged”.
- For a discovered host associated with one of the following, the appliance updates the data of the associated object:
  - A fixed address reservation or host address reservation
  - A host address not configured for DHCP services
  - A fixed address or host address with the same MAC address as that of the discovered host
  - An A or PTR record
  - A DHCP lease with the same MAC address as that of the discovered host
- For a DHCP lease that does not have any associated object, such as a fixed address or host record, the appliance updates the IP address with the discovered data. When the lease expires and the IP address has no associated objects, the appliance marks the IP address “unmanaged”. When the lease expires and the IP address is associated with the same MAC address, the appliance preserves the discovered data.
- For a discovered host associated with one of the following, the appliance updates all data except the MAC address and marks the IP address as a conflict. For information, see Resolving Conflicting Addresses on page 823.
  - A fixed address with a different MAC address than that of the discovered host
  - A DHCP lease with associated objects and with a different MAC address than that of the discovered host
  - An Infoblox host address configured for DHCP services and with a different MAC address than that of the discovered host
- For a discovered host that is part of a DHCP range but does not have a fixed or leased address or is not within an exclusion range, the appliance assigns a DHCP range conflict to the IP address.
- For a discovered host through a VM discovery, the appliance adds the discovered data to the database. The data is displayed in the IP Map and IP List panels, the Discovered Data tab of an object editor, and the Discovered Data section of the IP Address panel.
- The OS of an IP address obtained by an IP discovery supersedes that obtained by a VM discovery, and the newly discovered name of a host supersedes the last discovered data.
- When a VM discovery cannot obtain the IP address of a virtual entity, it does not return any discovered data for the entity.
- Only the objects with IP addresses to which the administrators have read/write permission are updated to include the VM discovery data.

Database Capacity

When the grid master database reaches its maximum capacity (the maximum capacity varies based on the appliance model), the grid master stops updating the database and requests that the grid member stop the discovery. When the discovering grid member database reaches its capacity, the grid member pauses the discovery. The appliance displays a dialog to inform you that the discovery pauses. The grid member resumes the discovery once the database falls below its capacity. When a discovery pauses because of capacity issues, you cannot resume the discovery or start a new discovery. You can check the capacity of your appliance database before starting a discovery.
HA Failover

In an HA pair, if the grid master fails over to the passive node, the passive node takes over and continues with the discovery from the last known state. If an independent appliance fails, the appliance stops the discovery process and keeps the discovery in a paused state. The appliance resumes the discovery once it starts up again.

Selecting a Grid Member

You must select a grid member from which you want to run a discovery.

1. From the Data Management tab, select the IPAM tab, and then click Discovery from the Toolbar.
   or
   From the Discovery Status widget, click Discovery Manager.
2. In the Discovery Manager wizard, click the General tab and complete the following:
   — Current Status: Displays the last discovery status and timestamp. This data is read-only.
   — Member Name: Click Select Member. In the Member Selector dialog box, select the grid member from which you want to run the discovery. You can also use filters or the Go to function to find a specific member. For information, see Using Filters on page 49 and Using the Go To Function on page 51.

After you select a grid member, you can do the following:

- Enable or disable the merging of discovered data, as described in Enabling or Disabling the Merging of Discovered Data.
- Configure an IP discovery, as described in Configuring IP Discovery on page 815.
- Configure a VM discovery, as described in Configuring VM Discovery on page 816.

Enabling or Disabling the Merging of Discovered Data

You can decide whether to merge the newly discovered data with the current data in the database. This function is enabled by default.

To enable or disable the merging of discovered data:

1. From the Data Management tab, select the IPAM tab, and then click Discovery from the Toolbar.
   or
   From the Discovery Status widget, click Discovery Manager.
2. In the Discovery Manager wizard, click the General tab and complete the following:
   — Merge the discovered data with existing data: When you select this check box, the appliance merges the discovered data with the existing data. It appends newly discovered data to existing data and preserves the existing data when there is no newly discovered data.
   When you clear this check box, the appliance replaces the existing data with the newly discovered data.
   When there are no newly discovered values for some fields, the appliance removes the existing values for these fields. This check box is selected by default.

You can do the following:

- Configure an IP discovery, as described in Configuring IP Discovery on page 815.
- Configure a VM discovery, as described in Configuring VM Discovery on page 816.
Updating Discovered Data for Managed Objects

You can decide whether you want the appliance to update the data of existing A records, PTR records, host records, and fixed addresses.

To update discovered data for managed objects:

1. From the **Data Management** tab, select the **IPAM** tab, and then click **Discovery** from the Toolbar.
   or
   From the **Discovery Status** widget, click **Discovery Manager**.

2. In the **Discovery Manager** wizard, click the **General** tab and complete the following:
   - **Update discovered data for managed objects**: Select this check box if you want the appliance to update the data of existing A records, PTR records, host records, and fixed addresses. If you do not select this check box, the appliance updates only the unmanaged objects.

You can do the following:
- Configure an IP discovery, as described in *Configuring IP Discovery*.
- Configure a VM discovery, as described in *Configuring VM Discovery* on page 816.

### Configuring IP Discovery

When you start an IP discovery from the IPAM Home, Net Map or network List panel, you can select the networks on which you want the discovery to run. When you start an IP discovery from the IP Map or IP List panel, the discovered network is the one to which the IP addresses belong. You can include additional networks when you configure the IP discovery from the **Discovery Manager** wizard. You can run an IP discovery on multiple networks in one network view.

1. From the **Data Management** tab, select the **IPAM** tab, and then click **Discovery** from the Toolbar.
   or
   From the **Discovery Status** widget, click **Discovery Manager**.

2. In the **Discovery Manager** wizard, click the **IP Discovery** tab, and then complete the following in the **Basic** tab:
   - **Mode**: Select the IP discovery method you want to use. For information, see *Supported IP Discovery Methods* on page 809. If you select **TCP** or **FULL**, ensure that you configure the TCP ports in the **Advanced** tab. The default is **Full**.
   - Click the **Add** icon to add networks. In the **Network Selector** dialog box, select the network view and networks. Use **SHIFT+click** and **CTRL+click** to select multiple networks. You can also use filters or the **Go to** function to find a specific network. For information, see *Using Filters* on page 49 and *Using the Go To Function* on page 51.

   You can do the following in the table:
   - Click the **Add** icon again to add more networks.
   - Select a network or multiple networks in the network table and click **Delete** to delete them.
   - Click the **Export** icon to export the data in CSV format.
   - Click the **Print** icon to print the data.
   - **Disable**: Select this to exclude IP discovery from the discovery task and to run a VM discovery only. IP discovery is enabled by default. You can configure a VM discovery in the same discovery task. You cannot start a discovery if you disable both IP discovery and VM discovery.

3. If you select **TCP** or **FULL** in **Mode**, click the **Advanced** tab and complete the following:
   - **TCP Scan Technique**: Select the TCP technique you want to use for the discovery. The default is **SYN**. For information, see *TCP* on page 810.

   In the port table, select the check box of the port you want to configure. You can select all ports by clicking the check box in the header.
Optionally, you can click the Add icon and complete the following to add a new service to the list.

— **Port**: Enter the port number you want to add to the list. You must enter a number between 1 and 65535.
— **Service**: Enter the name of the service.

You can also delete a specific TCP port in the list. You can select multiple ports for deletion.

— **Timeout (ms)**: Enter the timeout value in milliseconds for the discovery. The timeout value determines how long the discovery waits for a response from an IP address after probing it. The minimum is 5 and the maximum is 4000. The default is 1000.
— **Attempts**: Enter the number of times you want the discovery to probe an IP address when scanning a network. The minimum is 1 and the maximum is 5. The default is 2.

4. Start the discovery or save the configuration, as described in *Starting a Discovery* on page 817. You can also schedule the discovery to run at a later date, as described in *Scheduling a Discovery* on page 817.

### Configuring VM Discovery

A VM discovery retrieves information about vSphere servers and the virtual entities running on the servers. You can add more than one vSphere server to the discovery. When you disable specific servers, the appliance excludes them from the VM discovery.

1. From the **Data Management** tab, select the **IPAM** tab, and then click **Discovery** from the Toolbar.
   or
   From the **Discovery Status** widget, click **Discovery Manager**.
2. In the **Discovery Manager** wizard, click the **VM Discovery** tab, and then complete the following:
   - **Network View**: Select the network view in which you want to perform the VM discovery. This appears only when there are multiple network views. Otherwise, the VM discovery is performed in the default network view.
   Click the Add icon and complete the following in the Add vSphere Server section:
   — **Server**: Enter the FQDN or IP address of the vSphere server.
   — **Protocol**: Select the protocol that is used to connect to the vSphere server. The default is HTTPS.
   — **Port Number**: Enter the number of the port the appliance uses to communicate with the vSphere server. The default is 443.
   — **Username**: Enter the username the appliance uses to log in to the vSphere server. The user account on the vSphere server should have at least read-only permission.
   — **Password**: Enter the password of the vSphere server account.
3. Click **Test** to test the settings before adding them to the table.
4. Click **Add** to add the vSphere server to the table. You can also do the following in the table:
   — Click the Add icon again to add more vSphere servers.
   — Select the **Disable** check box in the table to exclude a specific vSphere server from the VM discovery. The appliance keeps the server configuration when you disable the server. All servers in the list are included in the VM discovery by default.
   — Select a server and click the **Edit** icon to modify its configuration.
   — Select a server and click the **Delete** icon to delete the server.
   — Click the Export icon to export the data in CSV format.
5. Optionally, select the **Disable** check box to exclude VM discovery from the discovery task. VM discovery is enabled by default. The appliance keeps the server configurations when you disable VM discovery.
6. Start the discovery or save the configuration, as described in *Starting a Discovery* on page 817. You can also schedule the discovery to run at a later date, as described in *Scheduling a Discovery* on page 817.
Starting a Discovery

After you configure a discovery task, you can select one of the following:

- **Restore to Defaults**: Restores the discovery configuration using the default values.
- **Start**: Starts the discovery.
- **Save**: Saves the discovery configuration.
- **Close**: Cancels the configuration. If you have started a discovery, the discovery runs in the background when you click Close. For information, see Running Tasks in the Background on page 52.

**Note**: Once you start a discovery, you cannot change the discovery configuration. After you click Start, the button changes to Pause. You can click Pause to pause a discovery. When the discovery is paused, the button changes to Resume. You can click Resume to continue the paused discovery.

Scheduling a Discovery

After you configure a discovery, you can schedule to run it at a later date and time. Note that you can only schedule the start of a discovery, you cannot schedule it to pause, stop, or resume. After a scheduled discovery starts, you can then pause, stop, or resume it.

To schedule a discovery, click the Schedule icon at the top of the wizard. In the Schedule Change panel, click Later, and then specify a date, time, and time zone. Click Schedule Start to schedule the discovery. If applicable, you can select Click here to view/manage the scheduled items to reschedule a discovery or view all scheduled discoveries. You can schedule multiple discoveries to start at different times using the same configuration. When you schedule two discoveries to start at the same time, only the one submitted first get executed. Once you schedule a discovery, you cannot change the configuration until the task is cancelled or executed.

Managing a Discovery

You can do the following after you start a discovery:

- **Pause**: The appliance pauses the discovery at the current chunk of IP addresses.
- **Resume**: The appliance continues the discovery from the last Pause state. It resumes the discovery at the beginning of the first unprocessed chunk of IP addresses on the network.
- **Stop**: The appliance stops and terminates the discovery. It marks the operation as complete. You cannot resume this discovery. All discovered data remains intact in the database.

Monitoring Discovery Status

You can monitor the discovery status through the Discovery Status widget on the Dashboard. You can also start, pause, resume, and stop a discovery from the widget. For information, see Discovery Status on page 62.
INTEGRATING DATA FROM PORTIQ APPLIANCES

Infoblox PortIQ appliances discover and track where devices connect to your network switches, and provide information about the switch ports to which the devices connect. You can integrate the data discovered by PortIQ appliances into the NIOS appliance database, and then view the data in the IP Map and List panels of Grid Manager. For information about PortIQ appliances, refer to the Infoblox Administrator Guide for PortIQ Appliances.

You can import the following data about the IP addresses that PortIQ appliances discover:

- **Discovered Name**: The name of the network device associated with the discovered IP address.
- **Discoverer**: Specifies whether the IP address was discovered by a PortIQ or NIOS discovery process.
- **First Seen**: The date and time the IP address was first seen.
- **Attached Device Description**: A textual description of the switch that is connected to the end device.
- **Attached Device Address**: The IP address of the switch that is connected to the end device.
- **Attached Device Name**: If a reverse lookup was successful for the IP address associated with this switch, the host name is displayed here.
- **Attached Device Port Description**: A textual description of the switch port that is connected to the end device.
- **Attached Device Port**: The number of the switch port connected to the end device.
- **Port Duplex**: The negotiated or operational duplex setting of the switch port connected to the end device.
- **Port Link**: The link status of the switch port connected to the end device. Indicates whether it is connected.
- **Port Speed**: The interface speed, in Mbps, of the switch port.
- **Port Status**: The operational status of the switch port. Indicates whether the port is up or down.
- **VLAN Description**: The description of the VLAN of the switch port that is connected to the end device.
- **VLAN Name**: The name of the VLAN of the switch port.
- **VLAN**: The ID of the VLAN of the switch port.

Do the following to integrate data from PortIQ appliances into the NIOS appliance:

1. Configure the PortIQ appliance to synchronize its data with the NIOS appliance. In a grid, PortIQ appliances must synchronize their data with the grid master. For information, refer to the Infoblox PortIQ Appliance User Guide.

2. Specify the data to be displayed in the IP Map and IP List panels.
   - When you select an IP address from the IP Map or IP List panel, this information can be displayed in the Discovered Data section. For information, see Viewing Data in IP Map on page 819 and Viewing Data in IP List on page 820.
   - In the IP List panel, you can add data fields. For information, see Viewing Data in IP List on page 820.
Viewing Discovered Data

After a discovery or after integrating data from PortIQ appliances, you can view the discovered data in the IP Map and IP List panels.

To view discovered data:
1. From the Data Management tab, select the IPAM tab.
2. Select and open the network you want to view.
   Grid Manager displays the IP address data in both the IP Map and List panels.

In the IP Map panel, Grid Manager displays the different types of discovered data in distinctive colors. For information, see Viewing Data in IP Map. In the List panel, Grid Manager displays the attributes of the discovered data. For information, see Viewing Data in IP List.

Viewing Data in IP Map

After you run an IP discovery, a VM discovery, or integrate data from PortIQ appliances, you can view the updated status of IP addresses in the IP Map panel. The default Basic view displays the status of the discovered IP addresses as follows:

- **Unused** (in white): An IP address that has not been detected and is not associated with any network device or active host on the network.
- **Conflict** (in red): When a discovery detects an IP address that has conflicting data, it assigns a “Conflict” status to the address. The IP address can have one of the following conflicts: DHCP lease, fixed address, DHCP range, and host. For information, see Resolving Conflicting Addresses on page 823.
- **Used** (in black): An IP address that is known to the appliance, and has an A record, PTR record, fixed address record, host record, lease, or is within a DHCP range.

You can click **Toggle Advanced View** to view additional status of the discovered IP addresses as follows:

- **Unmanaged** (in yellow): An IP address that does not have an A record, PTR record, fixed address, host record, lease, or is not within a DHCP range. It can also be an IP address with an expired DHCP lease and does not have any associated objects. Unmanaged data is classified as Unused data in the Basic view.

  You can convert an unmanaged address to a host, a DHCP fixed address, an A record, or a PTR record. You can also delete an unmanaged address. For information, see Managing Unmanaged Data on page 821. All existing administrator permissions apply to the unmanaged addresses.

- **Fixed Address/Reservation** (in magenta): A host that is either a fixed address or a reservation.
- **DNS Object** (in purple): An object that is configured for DNS.
- **Host not in DNS/DHCP** (in orange): An IP address that is associated with a host record, but is not configured for DNS or DHCP.
- **Active Lease** (in black diamond): An IP address that has an active lease.
- **DHCP Exclusion Range**: A range of IP addresses within a DHCP range. The appliance cannot assign addresses in the exclusion range to a client. You can use these addresses as static IP addresses. This prevents address conflicts between statically configured devices and dynamically configured devices.

**Note:** A discovery creates only the Unmanaged and Conflict data.

You can select an IP address from the IP Map panel and view discovered data about the IP address, as described in Viewing Data in the Discovered Data Section on page 820.
Viewing Data in IP List

In the IP List panel, Grid Manager displays the following information for each discovered record:

- **Name**: The domain name of the IP address.
- **MAC Address**: The discovered MAC address of the host. This is the unique identifier of a network device. The discovery acquires the MAC address for hosts that are located on the same network as the grid member that is running the discovery. This can also be the MAC address of a virtual entity on a specified vSphere server.
- **Status**: The type of discovered data. For information about the data types, see Viewing Data in IP Map on page 819.
- **Type**: The type of record that the IP address represents, such as A record or fixed address.
- **Usage**: Shows whether the IP address is configured for DNS or DHCP.
- **NetBIOS**: The NetBIOS name that was discovered. The discovery returns the NetBIOS Name if you run a NetBIOS or Full discovery. For more information, see Supported IP Discovery Methods on page 809.
- **OS**: The operating system of the detected host. The OS value can be one of the following:
  - Microsoft for all discovered hosts that have a non-null value in the MAC addresses using the NetBIOS discovery method.
  - A value that a TCP discovery returns.
  - The OS of a virtual entity on a vSphere server.
  Note that this field sometimes displays the percentage of certainty about the discovered OS.
- **Last Discovered**: The timestamp when the IP address was last discovered. This data is read-only.

In addition, you can view data integrated from Infoblox PortIQ appliances by editing the columns in the IP List panel as described in Integrating Data from PortIQ Appliances on page 818.

You can select an IP address from the List panel and view discovered data about the IP address, as described in Viewing Data in the Discovered Data Section.

Viewing Data in the Discovered Data Section

When you modify certain Infoblox objects, such as fixed addresses and reservations, or when you select an IP address from the IP Map and IP List panels, Grid Manager displays the following discovered data (if any) in the Discovered Data tab and the Discovered Data section of the corresponding editors and panels:

- **NetBIOS**: The name returned in the NetBIOS reply or the name you manually register for the discovered host.
- **OS**: The operating system of the detected host or virtual entity. The OS can be one of the following:
  - Microsoft for all discovered hosts that have a non-null value in the MAC addresses using the NetBIOS discovery method.
  - A value that a TCP discovery returns.
  - The OS of a virtual entity on a vSphere server.
- **MAC Address**: The discovered MAC address for the host. This is the unique identifier of a network device. The discovery acquires the MAC address for hosts that are located on the same network as the grid member that is running the discovery. This can also be the MAC address of a virtual entity on a specified vSphere server.
- **Last Discovered**: The timestamp when the IP address was last discovered.
- **First Discovered**: The timestamp when the IP address was first discovered.

For IP addresses discovered through a VM discovery, Grid Manager displays the following additional information in the Discovered Data tab of an editor. You can also select this information for display in the Discovered Data section of the IP Map and IP List panels:

- **Discovered Name**: The domain name of the virtual entity.
- **Virtual Entity Type**: The virtual entity type. This can be blank or one of the following: Virtual Machine, Virtual Host, or Virtual Center. Virtual Center represents a VMware vCenter server.
- **Virtual Entity Name**: The name of the virtual entity.
- **Virtual Cluster**: The name of the VMware cluster to which the virtual entity belongs.
Managing Discovered Data

- **Virtual Datacenter**: The name of the vSphere datacenter or container to which the virtual entity belongs.
- **Virtual Switch**: The name of the switch to which the virtual entity is connected.
- **Virtual Host**: The name of the VMware server on which the virtual entity was discovered.
- **Virtual Host Adapter**: The name of the physical network adapter through which the virtual entity is connected to the appliance.

If you imported data from Infoblox PortIQ appliances, Grid Manager displays available information in the **Discovered Data** tab. You can also select all or some of this data for display in the Discovered Data section of the IP Map and IP List panels. For information about the data imported from PortIQ appliances, see **Integrating Data from PortIQ Appliances** on page 818.

To specify the data fields to display in the Discovered Data section of the IP Map and IP List panels:
1. Click the **Toggle icon** to expand the Discovered Data section.
2. Click the **Configure icon**.
3. Select a field from the **Available list** and click the > arrow to move it to the **Selected list**. You can always move the fields between the two lists. Use SHIFT-click and CTRL-click to select multiple fields.
4. You can also change the order in which the fields are displayed by moving the fields up and down in the **Selected list**. To move a field up in the list, select it and click the Up arrow. To move a field down, select it and click the Down arrow.
5. You can click the **Configure icon** to hide the editing options.

The Discovered Data section displays the fields you specified.

---

**MANAGING DISCOVERED DATA**

In addition to viewing the discovered data, you can do the following to manage the data:
- Manage an unmanaged address by adding it to a host, converting it to managed data, or clearing its unmanaged status. For information, see **Managing Unmanaged Data** on page 821.
- Resolve conflicting addresses. For information, see **Resolving Conflicting Addresses** on page 823.
- Clear discovered data. For information, see **Clearing Discovered Data** on page 824.

**Managing Unmanaged Data**

You can manage unused and unmanaged addresses by doing one of the following:
- Add to an existing host
- Convert to a fixed address, host, A record, or PTR record
- Clear the unmanaged status

*Note*: You cannot convert unmanaged IP addresses served by Microsoft DHCP servers to host records.

**Adding to an Existing Host**

You can add an unmanaged address, including all its information, to an existing host. You can select the desired host to which you want to add the unmanaged address.

To add an unmanaged address to an existing host:
1. From the **IP Map or List** panel, select an unmanaged address you want to add to a host, and then click **Add** to **Add to Existing Host** from the Toolbar.
2. In the **Select Host** dialog box, select a host from the table. You can also search for a host using filters or the Go to function. For information, see **Using Filters** on page 49 and **Using the Go To Function** on page 51. Click the Select icon to select the desired host.
Network Discovery

**Note:** Depending on the page size configuration, the search results are limited to the page size that you set. If the search results exceed the page size limit, the appliance displays an error message to inform you to refine your search criteria or to change the page size limit. In the Host Record editor, complete the information as described in *Modifying Host Records* on page 445.

3. Select one of the following:
   - **Save & Close**: Save the entry and close the wizard.
   - **Save**: Save the entry and continue editing.

### Converting Unmanaged Data

You can convert an unmanaged address to a host, an A record, a PTR record, or a fixed address.

**To convert an unmanaged address:**

1. In the *IP Map or List* panel, select an unmanaged address you want to convert, and then select **Convert** from the Toolbar.

2. In the drop-down list, select the type of address to which you want to convert the unmanaged address. You can select **To Host**, **To A Record**, **To PTR Record**, or **To Fixed Address**.

   Depending on the record type you select, Grid Manager displays the corresponding editor. It also populates the attributes of the unmanaged address in the editor. Enter the appropriate information in the editor.

3. Select one of the following:
   - **Save & Close**: Save the entry and close the wizard.
   - **Save**: Save the entry and continue editing.

**Note:** After the conversion, the status of the unmanaged address changes to **Used**.

The following are some conditions for a conversion:

- **A record**: You must select a DNS zone when converting an unmanaged address to an A record.
- **PTR record**: You must select a DNS zone when converting an unmanaged address to a PTR record.
- **Fixed Address**: Grid Manager displays a confirmation dialog box to ensure that you want to create a fixed address for the unmanaged address.
- **Host record**: You can use the unmanaged address to enable a host record for DNS or DHCP.

### Clearing Unmanaged Data

You can clear the status of unmanaged data. When you clear an unmanaged address, the status of the IP address changes to **Unused**. You can clear individual and multiple unmanaged addresses in the *IP Map or List* panel. You can also clear all the unmanaged data within a network in the *Net Map and List* panels.

**To clear an unmanaged address:**

1. In the *IP Map or List* panel, select an unmanaged address, and then click **Clear -> Clear Unmanaged Data** from the Toolbar.

2. or

3. In the *Net Map or List* panel, select a network or networks, and then click **Clear -> Clear All Unmanaged Data** from the Toolbar to clear all unmanaged addresses in the networks.

4. In the **Clear Unmanaged Data** confirmation dialog box, click **Yes**.

**Note:** When you select an entire network or a specific network in the *Net Map or List* panel, all the unmanaged addresses in the network are cleared. After you clear the unmanaged data, the status of the IP addresses changes to **Unused**.
Managing Discovered Data

Resolving Conflicting Addresses

Conflicts happen when discovered data does not match the existing IP address data. The IP Map panel displays conflicting addresses in red. The List panel displays Conflict as the status for all conflicting addresses. Depending on the conflict, you can do one of the following to resolve it:

- For a DHCP lease conflict, you can clear the existing lease and create either a fixed address or a reservation for the IP address. You can also keep the existing data and clear the discovered data. For information, see Resolving DHCP Lease Conflicts.

- For a fixed address conflict, you can either keep the existing fixed address data or update the existing data with the discovered data. For information, see Resolving Fixed Address Conflicts on page 824.

- For a DHCP range conflict, you can create a fixed address, create a reservation, or clear the discovered data. For information, see Resolving DHCP Range Conflicts on page 824.

- For a host conflict, you can either keep the existing host record data or update the existing data with the discovered data. For information, see Resolving Host Conflicts on page 824.

You must resolve conflicting addresses individually. You cannot resolve multiple conflicts at the same time.

Note: Once the conflict is resolved, the status of the IP address changes depending on how you resolved the conflict.

To resolve a conflict:

1. In the IP Map or List panel, select a conflicting address, and then click Resolve Conflict from the Toolbar.
2. The Resolve Conflict dialog box displays the reason of the conflict and lists the existing information and discovered information of the address in the Description field. Depending on the type of conflict, the appliance displays the corresponding resolution options. You can compare the existing and discovered data and decide how you want to resolve the conflict.

Resolving DHCP Lease Conflicts

When an IP address has a DHCP lease and the discovered MAC address is in conflict with the existing MAC address, the IP address has a DHCP lease conflict.

To resolve a DHCP lease conflict:

1. In the Resolve Conflict dialog box, select one of the following:
   - Clear lease and create fixed address from discovered data: Clears the existing DHCP lease and creates a fixed address with the discovered data. The Fixed Address editor appears with the discovered data populated.
   - Clear lease and create a reservation from discovered data: Clears the existing DHCP lease and creates a new reservation using the discovered data. The Reservation editor appears with the discovered data populated. This option does not apply to leases served by Microsoft DHCP servers because they do not support Infoblox reservations. For information about managing DHCP data served by Microsoft servers, see Chapter 31, Managing Microsoft DHCP Services, on page 757.
   - Keep lease and clear discovered data: Keeps the current DHCP lease for the address and clears the discovered data.
2. Click OK.
Resolving Fixed Address Conflicts

When an IP address has a fixed address and the discovered MAC address does not match the existing MAC address, the IP address has a fixed address conflict.

To resolve a fixed address conflict:

1. In the Resolve Conflict dialog box, select one of the following:
   - Keep fixed address and clear discovered data: Keeps the existing fixed address and clears the discovered data.
   - Update fixed address with discovered data: Updates the existing fixed address data with the discovered data.
2. Click OK.

Resolving DHCP Range Conflicts

When an IP address is in a DHCP range and does not match an existing DHCP lease, fixed address, or exclusion range and it shows an active state during a discovery, the IP address has a DHCP range conflict.

To resolve a DHCP range conflict:

1. In the Resolve Conflict dialog box, select one of the following:
   - Create a fixed address: Creates a fixed address with the discovered data.
     If the fixed address is served by a Microsoft server, but is outside of a scope, you must then navigate to the Fixed Address editor and assign the fixed address to the appropriate Microsoft server.
   - Create a reservation: Creates a reservation with the discovered data. This creates an Infoblox reservation and therefore cannot be used for IP addresses served by Microsoft servers.
   - Clear discovered data: Clears the discovered data and no object is created for the IP address.
2. Click OK.

Resolving Host Conflicts

When an IP address belongs to a host record and the discovered MAC address does not match the existing MAC address, the IP address has a host conflict.

To resolve a host conflict:

1. In the Resolve Conflict dialog box, select one of the following:
   - Keep host record and clear discovered data: Keeps the existing data and clears the discovered data.
   - Update host record with discovered data: Updates the existing host record data with the discovered data.
2. Click OK.

Clearing Discovered Data

You can clear discovered data on selected networks. This is useful, for example, if the network topology has changed since the last time you ran a discovery on the network.

To clear discovered data:

1. In the Net Map or List panel, select a network, and then click Clear → Clear Discovered Data from the Toolbar.
2. In the Clear Discovered Data dialog box, click Yes.

You can also clear discovered data on all networks in a network view as follows:

1. In the Net Map or List panel, select a network, and then click Clear → Clear All Discovered Data from the Toolbar.
2. In the Clear All Discovered Data dialog box, click Yes.
PART 7 REFERENCE

This section provides reference information in the following appendices:

- Appendix A, "Grid Manager Icons", on page 827
- Appendix B, "Regular Expressions", on page 833
- Appendix C, "vNIOS Appliance Limitations", on page 835
- Appendix D, "Product Compliance", on page 839
- Appendix E, "Open Source Copyright and License Statements", on page 847
Appendix A Grid Manager Icons

This appendix contains the following information about icons used in Grid Manager, System Manager, and Orchestration Server Manager:

- **Icon**: The graphical display of an icon.
- **Icon Name**: The icon name.
- **Description**: The task that Grid Manager performs after you click the icon.
- **Tab/Table/Panel**: Lists the the tab, table, or panel in which the icon appears.

The following are common icons that appear in most of the tabs, tables, and panels, and in the Toolbar:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Add" /></td>
<td>Add</td>
<td>Adds an object</td>
</tr>
<tr>
<td><img src="image" alt="Add Bookmark" /></td>
<td>Add Bookmark</td>
<td>Adds a bookmark for an object and displays it in the Bookmarks panel</td>
</tr>
<tr>
<td><img src="image" alt="Arrow (Down)" /></td>
<td>Arrow (Down)</td>
<td>Moves an object down in a list</td>
</tr>
<tr>
<td><img src="image" alt="Arrow (Up)" /></td>
<td>Arrow (Up)</td>
<td>Moves an object up in a list</td>
</tr>
<tr>
<td><img src="image" alt="Clear" /></td>
<td>Clear</td>
<td>Clears the status of an object</td>
</tr>
<tr>
<td><img src="image" alt="Clock" /></td>
<td>Clock</td>
<td>Displays a drop-down list for time</td>
</tr>
<tr>
<td><img src="image" alt="Delete" /></td>
<td>Delete</td>
<td>Deletes an object</td>
</tr>
<tr>
<td><img src="image" alt="Disabled" /></td>
<td>Disabled</td>
<td>Indicates a disabled object</td>
</tr>
<tr>
<td><img src="image" alt="Download" /></td>
<td>Download</td>
<td>Downloads a file or data</td>
</tr>
<tr>
<td><img src="image" alt="Edit" /></td>
<td>Edit</td>
<td>Displays the corresponding editor for modifying object configurations</td>
</tr>
<tr>
<td><img src="image" alt="Edit" /></td>
<td>Edit</td>
<td>Displays the corresponding editor for modifying object configurations</td>
</tr>
<tr>
<td><img src="image" alt="Execute Now" /></td>
<td>Execute Now</td>
<td>Executes a scheduled task immediately</td>
</tr>
<tr>
<td>Icon</td>
<td>Icon Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------</td>
<td>--------------------------------------------------------------------</td>
</tr>
<tr>
<td><img src="image1.png" alt="Icon" /></td>
<td>Export</td>
<td>Exports data in the current panel</td>
</tr>
<tr>
<td><img src="image2.png" alt="Icon" /></td>
<td>Extensible Attribute</td>
<td>Configures extensible attributes for the selected object</td>
</tr>
<tr>
<td><img src="image3.png" alt="Icon" /></td>
<td>Flat View</td>
<td>Displays a list of objects in a flat view</td>
</tr>
<tr>
<td><img src="image4.png" alt="Icon" /></td>
<td>Help</td>
<td>Displays information about an object</td>
</tr>
<tr>
<td><img src="image5.png" alt="Icon" /></td>
<td>Hierarchy</td>
<td>Displays objects in a hierarchical view</td>
</tr>
<tr>
<td><img src="image6.png" alt="Icon" /></td>
<td>Import</td>
<td>Imports a file or data</td>
</tr>
<tr>
<td><img src="image7.png" alt="Icon" /></td>
<td>Information</td>
<td>Displays informational data about an object</td>
</tr>
<tr>
<td><img src="image8.png" alt="Icon" /></td>
<td>Locked</td>
<td>Indicates a locked object</td>
</tr>
<tr>
<td><img src="image9.png" alt="Icon" /></td>
<td>Microsoft Server</td>
<td>Indicates a Microsoft server</td>
</tr>
<tr>
<td><img src="image10.png" alt="Icon" /></td>
<td>Pause</td>
<td>Pauses a function</td>
</tr>
<tr>
<td><img src="image11.png" alt="Icon" /></td>
<td>Print</td>
<td>Prints the information in the current panel</td>
</tr>
<tr>
<td><img src="image12.png" alt="Icon" /></td>
<td>Refresh</td>
<td>Refreshes the current page or table</td>
</tr>
<tr>
<td><img src="image13.png" alt="Icon" /></td>
<td>Report</td>
<td>Displays a report, such as the capacity report</td>
</tr>
<tr>
<td><img src="image14.png" alt="Icon" /></td>
<td>Search</td>
<td>Searches for specific objects</td>
</tr>
<tr>
<td><img src="image15.png" alt="Icon" /></td>
<td>Selected object</td>
<td>Selects an object in a table for a specific function</td>
</tr>
<tr>
<td><img src="image16.png" alt="Icon" /></td>
<td>Start</td>
<td>Starts a process</td>
</tr>
<tr>
<td><img src="image17.png" alt="Icon" /></td>
<td>Stop</td>
<td>Stops a process</td>
</tr>
<tr>
<td><img src="image18.png" alt="Icon" /></td>
<td>Unlocked</td>
<td>Indicates an unlocked object</td>
</tr>
<tr>
<td><img src="image19.png" alt="Icon" /></td>
<td>User Profile</td>
<td>Configures a user profile</td>
</tr>
<tr>
<td><img src="image20.png" alt="Icon" /></td>
<td>View</td>
<td>Lists data in the current panel or lists detailed status about an object</td>
</tr>
</tbody>
</table>
The following icons appear in the **Data Management** tab:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon Name</th>
<th>Description</th>
<th>Tab/Table/Panel</th>
</tr>
</thead>
</table>
| ![Configure Icon](image) | Configure | • Configures DHCP properties  
• Configures File Distribution properties  
• Configures Licenses | Data Management tab → DHCP tab  
→ Toolbar  
Data Management tab → DHCP tab  
→ Toolbar  
Grid tab → Grid Manager tab → Toolbar |
| ![Conflict Icon](image) | Conflict | Indicates an IP address conflict | Data Management tab → IPAM tab → Net Map |
| ![Convert Icon](image) | Convert | Converts an object | Data Management tab → IPAM tab → network → IP Map → Toolbar |
| ![Discovery Icon](image) | Discovery | Performs a network discovery | Data Management tab → IPAM tab → Toolbar |
| ![Force HA Failover Icon](image) | Force HA Failover | Forces an HA failover | Data Management tab → DHCP tab → Toolbar |
| ![Force Recovery Icon](image) | Force Recovery | Forces a recovery | Data Management tab → DHCP tab → Members tab → Failover Associations tab → Toolbar |
| ![Grid Manager Icon](image) | Grid Manager | Indicates the grid master | Data Management tab → DHCP tab → Members tab →  
Data Management tab → IPAM tab |
| ![Grid Manager Candidate Icon](image) | Grid Manager Candidate | Indicates the grid master candidate | Data Management tab → DHCP tab → Members tab →  
Data Management tab → IPAM tab |
| ![Grid Member Icon](image) | Grid Member | Indicates the grid member | Data Management tab → DHCP tab → Members tab →  
Data Management tab → IPAM tab |
| ![Join Icon](image) | Join | Joins networks | Data Management tab → IPAM tab → network → Toolbar |
| ![Key-signing Key Rollover Icon](image) | Key-signing Key Rollover | Indicates the key-signing key that is due to rollover | Data Management tab → DNS tab |
| ![Leaf Network Icon](image) | Leaf Network | Indicates a leaf network | Data Management tab → IPAM tab or DHCP tab |
| ![Disabled Leaf Network Icon](image) | Disabled Leaf Network | Indicates a disabled leaf network | Data Management tab → IPAM tab or DHCP tab |
| ![Microsoft Server Icon](image) | Microsoft Server | Indicates a Microsoft server | Data Management tab → DHCP tab → Members tab →  
Data Management tab → IPAM tab |
<p>| <img src="image" alt="Multi-Ping Icon" /> | Multi-Ping | Pings all the addresses in a network | Data Management tab → IPAM tab → IP Map → Toolbar |</p>
<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon Name</th>
<th>Description</th>
<th>Tab/Table/Panel</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Network]</td>
<td>Network</td>
<td>Indicates a network</td>
<td>Data Management tab → IPAM tab or DHCP tab</td>
</tr>
<tr>
<td>![Network Container]</td>
<td>Network Container</td>
<td>Indicates a network container</td>
<td>Data Management tab → IPAM tab or DHCP tab</td>
</tr>
<tr>
<td>![Network (Disabled)]</td>
<td>Network (Disabled)</td>
<td>Indicates a disabled network</td>
<td>Data Management tab → IPAM tab or DHCP tab</td>
</tr>
<tr>
<td>![Microsoft Network]</td>
<td>Microsoft Network</td>
<td>Indicates a network with Microsoft servers</td>
<td>Data Management tab → IPAM tab or DHCP tab</td>
</tr>
<tr>
<td>![Infoblox Network]</td>
<td>Infoblox Network</td>
<td>Indicates a network with Infoblox appliances</td>
<td>Data Management tab → IPAM tab or DHCP tab</td>
</tr>
<tr>
<td>![Ping]</td>
<td>Ping</td>
<td>Pings an IP address</td>
<td>Data Management tab → IPAM tab → IP Map → Toolbar</td>
</tr>
<tr>
<td>![Properties]</td>
<td>Properties</td>
<td>Configures Grid DNS properties</td>
<td>Data Management tab → DNS tab → Toolbar</td>
</tr>
<tr>
<td>![Reclaim]</td>
<td>Reclaim</td>
<td>Reclaims an IP address</td>
<td>Data Management tab → IPAM tab → IP Map → Toolbar</td>
</tr>
<tr>
<td>![Resize]</td>
<td>Resize</td>
<td>Resizes a network</td>
<td>Data Management tab → IPAM tab → network → Toolbar</td>
</tr>
<tr>
<td>![Resolve Conflict]</td>
<td>Resolve Conflict</td>
<td>Resolves an IP address conflict</td>
<td>Data Management tab → IPAM tab → IP Map → Toolbar</td>
</tr>
<tr>
<td>![Set Partner Down]</td>
<td>Set Partner Down</td>
<td>Sets partner down</td>
<td>Data Management tab → DHCP tab → Members tab → Failover Associations tab → Toolbar</td>
</tr>
<tr>
<td>![Split Network]</td>
<td>Split Network</td>
<td>Splits a network</td>
<td>Data Management tab → IPAM tab → network → Toolbar</td>
</tr>
<tr>
<td>![DNSSEC status]</td>
<td>DNSSEC status</td>
<td>Displays status for DNSSEC</td>
<td>Data Management tab → DNS tab → Toolbar</td>
</tr>
<tr>
<td>![Secondary Zone Status]</td>
<td>Secondary Zone Status</td>
<td>Displays status for the secondary zone</td>
<td>Data Management tab → DNS tab</td>
</tr>
<tr>
<td>![Zoom In]</td>
<td>Zoom In</td>
<td>Zooms in to the selected network</td>
<td>Data Management tab → IPAM tab → Net Map</td>
</tr>
<tr>
<td>![Zoom Out]</td>
<td>Zoom Out</td>
<td>Zooms out from the selected network</td>
<td>Data Management tab → IPAM tab → Net Map</td>
</tr>
<tr>
<td>![Directory]</td>
<td>Directory</td>
<td>Indicates a directory</td>
<td>Data Management tab → File Distribution tab</td>
</tr>
</tbody>
</table>
The following icons appear in the **Smart Folders** tab:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon Name</th>
<th>Description</th>
<th>Tab/Table/Panel</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>Smart Folder</td>
<td>Lists a smart folder</td>
<td>Smart Folders tab</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Smart Folder (Group By)</td>
<td>Lists smart folders in a group-by list</td>
<td>Smart Folders tab</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Smart Folder (Link)</td>
<td>Indicates a link to the smart folder</td>
<td>Smart Folders tab and other selectors</td>
</tr>
</tbody>
</table>

The following icons appear in the **Grid** tab:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon Name</th>
<th>Description</th>
<th>Tab/Table/Panel</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>Backup</td>
<td>Backs up the configuration file and database</td>
<td>Grid tab -&gt; Grid Manager tab -&gt; Toolbar</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Restore</td>
<td>Restores the configuration file and database</td>
<td>Grid tab -&gt; Grid Manager tab -&gt; Toolbar</td>
</tr>
<tr>
<td>![Icon]</td>
<td>bloxTools</td>
<td>Performs bloxTools services</td>
<td>Grid tab -&gt; Grid Manager tab -&gt; Toolbar</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Certificate</td>
<td>Creates, generates, uploads, or downloads an HTTPS certificate</td>
<td>Grid tab -&gt; Grid Manager tab -&gt; Toolbar</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Control</td>
<td>Restarts, reboots, or shuts down a member</td>
<td>Grid tab -&gt; Grid Manager tab -&gt; Members tab -&gt; member -&gt; Toolbar</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Manage Services</td>
<td>Manages member services</td>
<td>Grid tab -&gt; Grid Manager tab -&gt; Members tab -&gt; member</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Syslog</td>
<td>Displays the syslog file</td>
<td>Grid tab -&gt; Grid Manager tab -&gt; Members tab -&gt; member -&gt; Toolbar</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Traffic Capture</td>
<td>Captures the traffic report on a member</td>
<td>Grid tab -&gt; Grid Manager tab -&gt; Members tab -&gt; member -&gt; Toolbar</td>
</tr>
</tbody>
</table>

The following icons appear in the **Administration** tab:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon Name</th>
<th>Description</th>
<th>Tab/Table/Panel</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>Execute Now</td>
<td>Executes a scheduled task immediately</td>
<td>Administration tab -&gt; Scheduling tab -&gt; Toolbar</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Overlap</td>
<td>Shows overlapping permissions</td>
<td>Administration tab -&gt; Permissions tab</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Reschedule</td>
<td>Reschedules a task</td>
<td>Administration tab -&gt; Scheduling tab -&gt; Toolbar</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Schedule Delete</td>
<td>Schedules a deletion for a task</td>
<td>Administration tab -&gt; Scheduling tab -&gt; Toolbar</td>
</tr>
</tbody>
</table>
The following icons appear in the **Finder** panel:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🌟</td>
<td>Bookmarks</td>
<td>Lists all bookmarked objects</td>
</tr>
<tr>
<td>🗑️</td>
<td>Recycle Bin</td>
<td>Lists all deleted objects</td>
</tr>
<tr>
<td>📦</td>
<td>Smart Folders</td>
<td>Lists all smart folders</td>
</tr>
</tbody>
</table>
# Appendix B Regular Expressions

## Supported Expressions for Search Parameters

Regular expressions are text strings that you use to describe search patterns. You can use the following special characters to define regular expressions for search parameters.

<table>
<thead>
<tr>
<th>Special character</th>
<th>Purpose</th>
<th>Example</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>()</td>
<td>Defines the scope and precedence of the operator</td>
<td>gr(a</td>
<td>e)y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Matches either the regular expression before or after the vertical bar</td>
<td>a</td>
</tr>
<tr>
<td>.</td>
<td>Matches any single character</td>
<td>.at</td>
<td>Matches any text string ending with “at”, such as “hat”, “cat”, and “bat”.</td>
</tr>
<tr>
<td>*</td>
<td>Matches the previous regular expression zero or more times</td>
<td>a*bc</td>
<td>Matches zero or multiple occurrences of “a” followed by “bc”, such as “bc”, “abc”, “aabc”, “aaabc”, and so on.</td>
</tr>
<tr>
<td>+</td>
<td>Matches the previous regular expression one or more times</td>
<td>a+bc</td>
<td>Matches one or more occurrences of “a”, followed by “bc”, such as “abc”, “aabc”, “aaabc”, and so on.</td>
</tr>
<tr>
<td>?</td>
<td>Matches the previous regular expression zero or one time</td>
<td>a?bc</td>
<td>Matches zero or one occurrence of “a”, followed by “bc”, such as “bc” or “abc”.</td>
</tr>
<tr>
<td>^</td>
<td>Matches the beginning of a text string</td>
<td>^c</td>
<td>Matches any string beginning with “c”, such as “cat”.</td>
</tr>
<tr>
<td>$</td>
<td>Matches the end of a text string</td>
<td>com$</td>
<td>Matches any string ending with “com”, such as “Infoblox.com”.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Matches any character specified in the brackets</td>
<td>[03]</td>
<td>Matches “0” or “3”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[abcd]</td>
<td>Matches “a”, “b”, “c”, or “d”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[15a-d]</td>
<td>Matches “1”, “5”, “a”, “b”, “c”, or “d”.</td>
</tr>
</tbody>
</table>
Note: You can change a special character—such as the period (.), asterisk (*), plus sign (+), or question mark (?)—into a literal character by prefixing it with a backslash (\). For example, to specify a literal period, asterisk, plus sign, or question mark, use the characters within the following parentheses: (\.), (\*), (\+), (\?), (\^), (\$).

<table>
<thead>
<tr>
<th>Special character</th>
<th>Purpose</th>
<th>Example</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>[n-m]</td>
<td>Matches single characters contained in the specified range, including the start and end points</td>
<td>[0-3] [a-f]</td>
<td>Matches 0, 1, 2, and 3. Matches a, b, c, d, e, and f.</td>
</tr>
<tr>
<td>{m,n}</td>
<td>Matches the preceding expression at least m but not more than n times.</td>
<td>a{3,5}</td>
<td>Matches “aaa”, “aaaa”, and “aaaaa”.</td>
</tr>
</tbody>
</table>
Appendix C vNIOS Appliance Limitations

vNIOS appliances support most of the features of the Infoblox NIOS software, with some limitations. This appendix describes these limitations. *Table C.1* summarizes the supported grid configurations on vNIOS appliances for Cisco, Riverbed, and VMware.

*Table C.1  Supported vNIOS Appliance Configurations*

<table>
<thead>
<tr>
<th>vNIOS Appliance</th>
<th>vNIOS for Cisco</th>
<th>vNIOS for Riverbed</th>
<th>vNIOS for VMware (All IB-VM models)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Independent Appliance</td>
<td>✖</td>
<td>✖</td>
<td>✓</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>✖</td>
<td>✖</td>
<td>✓</td>
</tr>
<tr>
<td>Grid Master</td>
<td>✖</td>
<td>✖</td>
<td>✓</td>
</tr>
<tr>
<td>Grid Master Candidate</td>
<td>✖</td>
<td>✖</td>
<td>✓</td>
</tr>
<tr>
<td>HA Grid Member</td>
<td>✖</td>
<td>✖</td>
<td>✓</td>
</tr>
<tr>
<td>Single Grid Member</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

For detailed information about the limitations on each vNIOS appliance, see the following:

- *vNIOS for Cisco*
- *vNIOS for Riverbed*
- *vNIOS for VMware*
vNIOS for Cisco

vNIOS appliances on Cisco have the following limitations:

- They can function as grid members only. You cannot configure them as HA (high availability) pairs, grid masters, grid master candidates, or independent appliances.
- The Cisco AXP service module has an internal and external interface. The vNIOS software package uses the internal interface only. You cannot configure the speed and transmission type (full or half duplex) of the network interface.
- You can use the traffic capture tool of the vNIOS software package to capture traffic only on the LAN port of the vNIOS appliance.
- vNIOS appliances on Cisco provide SSH access on port 2222, instead of port 22.
- vNIOS appliances on Cisco do not support monitoring the following: CPU temperature, fan speed, and system temperature.
- vNIOS appliances on Cisco do not automatically synchronize their time with the grid master. You must configure the Cisco AXP service module to synchronize its time with the the same NTP server as the grid master. Alternatively, if the grid master is configured as an NTP server, you can configure the Cisco AXP service module to use the grid master as its NTP server.
- vNIOS appliances on Cisco do not support the following features:
  - IP address configuration through the vNIOS console and the GUI
  - Anycast addressing
  - Configuration as a DHCP lease history logging member
  - Dedicated MGMT port
  - NTP service
  - Static routes
  - IPv6
  - bloxTools environment
  - Configuration for managing Microsoft® Windows DNS servers
  - IF-MAP service
vNIOS for Riverbed

vNIOS appliances on Riverbed have the following limitations:

- They can function as grid members only. You cannot configure them as HA (high availability) pairs, grid masters, grid master candidates, or independent appliances.
- On a grid with a vNIOS appliance on Riverbed as a grid member, the maximum storage space for HTTP, FTP and TFTP is 1 GB (a grid with only Infoblox appliances provides a maximum of 5 GB for these services), core files are 100 MB each, and syslog and inflobox.log files are 20 MB each. Scheduled backup file is 100 MB.
- The LAN interface is the only network interface available on the vNIOS appliance. You cannot configure the speed and transmission type (full or half duplex) of the network interface.
- You can use the traffic capture tool of the vNIOS software package to capture traffic only on the LAN port of the vNIOS appliance.
- vNIOS appliances on Riverbed do not support the following features:
  - Anycast addressing
  - Configuration as a DHCP lease history logging member
  - Dedicated MGMT port
  - NTP service
  - bloxTools environment
  - Configuration for managing Microsoft® Windows DNS servers
  - IF-MAP service

vNIOS for VMware

vNIOS for VMware appliances support most of the features of the Infoblox NIOS appliances, with the following limitations:

- You must have a vNIOS license installed on the appliance before you can access the Infoblox GUI.
- vNIOS appliances do not support the following features:
  - Configuration of port settings for MGMT, LAN, LAN2, and HA ports
  - The bloxTools environment
- The IB-BOB virtual appliance can function as a grid member only. It does not support configuration as an independent appliance, an HA pair, a grid master, or a grid master candidate. It also does not support access to the Infoblox GUI.
- The IB-VM-250 virtual appliance supports all the services provided by vNIOS virtual appliances, but it is not recommended as a grid master or grid master candidate.
- The Captive Portal is supported only on IB-VM-250 virtual appliances.
- When you configure an HA pair, both nodes in the HA pair must be vNIOS instances. You cannot configure a physical NIOS appliance and a vNIOS instance in an HA pair.
- vNIOS appliances run on virtual hardware. They do not have sensors to monitor the physical CPU temperature, fan speed, and system temperature.
- Changing the vNIOS appliance settings through the VMware vSphere or vCenter console may violate the terms of the vNIOS licensing and support models. The vNIOS appliance may not join the grid or function properly.
Appendix D Product Compliance

This appendix describes the hardware components, requirements, and specifications, plus agency and RFC (Request for Comments) compliance for the Infoblox appliance. Topics in this appendix include:

- **Power Safety Information** on page 840
  - **AC** on page 840
  - **DC** on page 840

- **Agency Compliance** on page 841
  - **FCC** on page 841
  - **Canadian Compliance** on page 841
  - **VCCI** on page 842

- **RFC Compliance** on page 843
  - **DNS RFC Compliance** on page 843
  - **DHCP RFC Compliance** on page 845
POWER SAFETY INFORMATION

The main external power connector for the Infoblox appliance is located on the back of the system. Ensure power to the system is off before connecting the power cord into the power connector. Please read the following power safety statements for your AC- or DC-powered appliance:

AC

English

WARNING: This product relies on the building’s installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120VAC, 15A U.S. (240VAC, 10A international) is used on the phase conductors (all current-carrying conductors).

French

WARNING: Pour ce qui est de la protection contre les courts-circuits (surtension), ce produit dépend de l’installation électrique du local. Vérifier qu’un fusible ou un disjoncteur de 120V alt., 15A U.S. maximum (240V alt., 10A international) est utilisé sur les conducteurs de phase (conducteurs de charge).

German


DC

English

WARNING: When stranded wiring is required, use approved wiring terminations, such as closed-loop or spade-type with upturned lugs. These terminations should be the appropriate size for the wires and should clamp both the insulation and conductor.
Agency Compliance

The Infoblox appliance is compliant with these EMI and safety agency regulations:

Table D.1 Agency Regulation Compliance

<table>
<thead>
<tr>
<th>Standard</th>
<th>Agency</th>
<th>Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCC Part 15</td>
<td>FCC</td>
<td>FCC</td>
</tr>
<tr>
<td>EN55022, EN55024, EN61000-3-2, EN61000-3-3</td>
<td>TUV</td>
<td>CE</td>
</tr>
<tr>
<td>UL60950/CSA60950</td>
<td>UL</td>
<td>cULus</td>
</tr>
<tr>
<td>EN60950</td>
<td>TUV</td>
<td>GS</td>
</tr>
<tr>
<td>CB Scheme</td>
<td>IECEE</td>
<td>Report and Certificate IEC 60950-1:2001</td>
</tr>
<tr>
<td>VCCI-A</td>
<td>VCCI</td>
<td>VCCI</td>
</tr>
<tr>
<td>AS/NZS 3548</td>
<td>ACMA</td>
<td>C-Tick</td>
</tr>
</tbody>
</table>

FCC

The FCC label on the back of the system indicates this network appliance is compliant with limits for a Class A digital device in accordance with Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when this equipment is operated in a commercial environment. Operation is subject to the following two conditions:

- This device might not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This device generates, uses, and can radiate radio frequency energy if not installed and used in accordance with the instructions in this manual. Operating this equipment in a residential area is likely to cause harmful interference, and the customer will be required to rectify the interference at his or her own expense. This product requires the use of external shielded cables to maintain compliance pursuant to Part 15 of the FCC Rules.

Canadian Compliance

English

This Class A digital apparatus complies with Canadian ICES-003.

French

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.
VCCI

The Infoblox appliance complies with this VCCI regulation (compliance statement follow by its translation):

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求することがあります。

This is a Class A product based on the Technical Requirements of the Voluntary Control Council for Interference Technology (VCCI). In a domestic environment this product may cause radio interference, in which case the user may be required to take corrective action.

Caution: Lithium battery included with this board. Do not puncture, mutilate, or dispose of battery in fire. Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by manufacturer. Dispose of used battery according to manufacturer instructions and in accordance with your local regulations.
RFC Compliance

The NIOS appliance is compliant with the following:

- Qualys and Nessus security requirements
- Joint Interoperability Test Command (JITC) certification for Internet Protocol version 6 capability
- RFCs (Request for Comments):
  - DNS RFC Compliance on page 843
  - DHCP RFC Compliance on page 845

DNS RFC Compliance

The NIOS appliance complies with the following DNS RFCs:

Table D.2 RFCs for DNS

<table>
<thead>
<tr>
<th>RFC Number</th>
<th>RFC Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>805</td>
<td>Computer Mail Meeting Notes</td>
</tr>
<tr>
<td>811</td>
<td>Hostnames Server</td>
</tr>
<tr>
<td>819</td>
<td>The Domain Naming Convention for Internet User Applications</td>
</tr>
<tr>
<td>881</td>
<td>The Domain Names Plan and Schedule</td>
</tr>
<tr>
<td>882</td>
<td>Domain Names: Concepts and Facilities</td>
</tr>
<tr>
<td>883</td>
<td>Domain Names: Implementation Specification</td>
</tr>
<tr>
<td>897</td>
<td>Domain Name System Implementation Schedule</td>
</tr>
<tr>
<td>920</td>
<td>Domain Requirements</td>
</tr>
<tr>
<td>921</td>
<td>Domain Name System Implementation Schedule – Revised</td>
</tr>
<tr>
<td>973</td>
<td>Domain System Changes and Observations</td>
</tr>
<tr>
<td>974</td>
<td>Mail Routing and the Domain System</td>
</tr>
<tr>
<td>1032</td>
<td>Domain Administrators Guide</td>
</tr>
<tr>
<td>1033</td>
<td>Domain Administrators Operations Guide</td>
</tr>
<tr>
<td>1034</td>
<td>Domain Names – Concepts and Facilities</td>
</tr>
<tr>
<td>1035</td>
<td>Domain Names – Implementation and Specification</td>
</tr>
<tr>
<td>1101</td>
<td>DNS Encoding of Network Names and Other Types</td>
</tr>
<tr>
<td>1122</td>
<td>Requirements for Internet Hosts – Communication Layers</td>
</tr>
<tr>
<td>1123</td>
<td>Requirements for Internet Hosts – Application and Support</td>
</tr>
<tr>
<td>1178</td>
<td>Choosing a Name for Your Computer</td>
</tr>
<tr>
<td>1348</td>
<td>DNS NSAP RRs</td>
</tr>
<tr>
<td>1386</td>
<td>The US Domain</td>
</tr>
<tr>
<td>1464</td>
<td>Using the Domain Name System to Store Arbitrary String Attributes</td>
</tr>
<tr>
<td>1535</td>
<td>A Security Problem and Proposed Correction with Widely Deployed DNS Software</td>
</tr>
<tr>
<td>RFC Number</td>
<td>RFC Title</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
</tr>
<tr>
<td>1536</td>
<td>Common DNS Implementation Errors and Suggested Fixes</td>
</tr>
<tr>
<td>1537</td>
<td>Common DNS Data File Configuration Errors</td>
</tr>
<tr>
<td>1591</td>
<td>Domain Name System Structure and Delegation</td>
</tr>
<tr>
<td>1611</td>
<td>DNS Server MIB Extensions</td>
</tr>
<tr>
<td>1612</td>
<td>DNS Resolver MIB Extensions</td>
</tr>
<tr>
<td>1637</td>
<td>DNS NSAP Resource Records</td>
</tr>
<tr>
<td>1664</td>
<td>Using the Internet DNS to Distribute RFC 1327 Mail Address Mapping Tables</td>
</tr>
<tr>
<td>1713</td>
<td>Tools for DNS debugging</td>
</tr>
<tr>
<td>1794</td>
<td>DNS Support for Load Balancing</td>
</tr>
<tr>
<td>1811</td>
<td>U.S. Government Internet Domain Names</td>
</tr>
<tr>
<td>1816</td>
<td>U.S. Government Internet Domain Names</td>
</tr>
<tr>
<td>1912</td>
<td>Common DNS Operational and Configuration Errors</td>
</tr>
<tr>
<td>1956</td>
<td>Registration in the MIL Domain</td>
</tr>
<tr>
<td>1982</td>
<td>Serial Number Arithmetic</td>
</tr>
<tr>
<td>1995</td>
<td>Incremental Zone Transfer in DNS</td>
</tr>
<tr>
<td>1996</td>
<td>A Mechanism for Prompt Notification of Zone Changes</td>
</tr>
<tr>
<td>2010</td>
<td>Operational Criteria for Root Name Servers</td>
</tr>
<tr>
<td>2052</td>
<td>A DNS RR for specifying the location of services (DNS SRV)</td>
</tr>
<tr>
<td>2053</td>
<td>The AM (Armenia) Domain</td>
</tr>
<tr>
<td>2136</td>
<td>Dynamic Updates in the Domain Name System (DNS UPDATE)</td>
</tr>
<tr>
<td>2142</td>
<td>Mailbox Names for Common Services, Roles and Functions</td>
</tr>
<tr>
<td>2146</td>
<td>U.S. Government Internet Domain Names</td>
</tr>
<tr>
<td>2168</td>
<td>Resolution of Uniform Resource Identifiers using the Domain Name System</td>
</tr>
<tr>
<td>2181</td>
<td>Clarifications to the DNS Specification</td>
</tr>
<tr>
<td>2182</td>
<td>Selection and Operation of Secondary DNS Servers</td>
</tr>
<tr>
<td>2219</td>
<td>Use of DNS Aliases for Network Services</td>
</tr>
<tr>
<td>2240</td>
<td>A Legal Basis for Domain Name Allocation</td>
</tr>
<tr>
<td>2308</td>
<td>Negative Caching of DNS Queries (DNS NCACHE)</td>
</tr>
<tr>
<td>2317</td>
<td>Classless IN-ADDR.ARPA Delegation</td>
</tr>
<tr>
<td>2352</td>
<td>A Convention for Using Legal Names as Domain Names</td>
</tr>
<tr>
<td>2537</td>
<td>RSA/MD5 KEYS and SIGs in the Domain Name System (DNS)</td>
</tr>
<tr>
<td>2606</td>
<td>Reserved Top Level DNS Names</td>
</tr>
<tr>
<td>2671</td>
<td>Extension Mechanisms for DNS (EDNS0)</td>
</tr>
<tr>
<td>2782</td>
<td>A DNS RR for Specifying the Location of Services (DNS SRV)</td>
</tr>
<tr>
<td>RFC Number</td>
<td>RFC Title</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
</tr>
<tr>
<td>2845</td>
<td>Secret Key Transaction Authentication for DNS (TSIG)</td>
</tr>
<tr>
<td>2915</td>
<td>The Naming Authority Pointer (NAPTR) DNS Resource Record</td>
</tr>
<tr>
<td>3596</td>
<td>DNS Extensions to Support IP Version 6</td>
</tr>
<tr>
<td>3768</td>
<td>Virtual Router Redundancy Protocol (VRRP)</td>
</tr>
<tr>
<td>4033</td>
<td>DNS Security Introduction and Requirements</td>
</tr>
<tr>
<td>4034</td>
<td>Resource Records for the DNS Security Extensions</td>
</tr>
<tr>
<td>4035</td>
<td>Protocol Modifications for the DNS Security Extensions</td>
</tr>
<tr>
<td>4641</td>
<td>DNSSEC Operational Practices</td>
</tr>
<tr>
<td>4956</td>
<td>DNS Security (DNSSEC) Opt-In</td>
</tr>
<tr>
<td>4986</td>
<td>Requirements Related to DNS Security (DNSSEC) Trust Anchor Rollover</td>
</tr>
<tr>
<td>5155</td>
<td>DNSSEC Hashed Authenticated Denial of Existence</td>
</tr>
<tr>
<td>5702</td>
<td>Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC</td>
</tr>
</tbody>
</table>

**DHCP RFC Compliance**

The appliance complies with the following DHCP RFCs:

*Table D.3 RFCs for DHCP*

<table>
<thead>
<tr>
<th>RFC Number</th>
<th>RFC Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1531</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>1534</td>
<td>Interoperation Between DHCP and BOOTP</td>
</tr>
<tr>
<td>1542</td>
<td>Clarifications and Extensions for the Bootstrap Protocol</td>
</tr>
<tr>
<td>2131</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>2132</td>
<td>DHCP Options and BOOTP Vendor Extensions</td>
</tr>
<tr>
<td>3046</td>
<td>DHCP Relay Agent Information Option</td>
</tr>
<tr>
<td>3925</td>
<td>Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)</td>
</tr>
<tr>
<td>4388</td>
<td>Dynamic Host Configuration Protocol (DHCP) Leasequery</td>
</tr>
</tbody>
</table>
Appendix E  Open Source Copyright and License Statements

Infoblox has made every attempt to adhere to the guidelines for use and contribution to the open source community. Please report back to Infoblox any suspected violations of the copyrights, use of open source contributions via the distribution of binaries and/or source from Infoblox. It is the intent of Infoblox to comply with the open source rules of use, and comply with the various copyrights found in the distribution of the products from Infoblox.

This appendix contains the copyright notices for the binary-only distribution from Infoblox. Source changes are contributed back to the open source community when the copyright holder states this is desired. As stated by the enclosed copyrights, a copy of open source files used in our binary-only distribution is available from Infoblox. There is a nominal cost to obtain a CD containing the source files, to cover our costs of duplication and distribution. To obtain a copy of the source, contact us via e-mail at info@infoblox.com, or call us at 1.408.625.4200. The sections in this appendix include:

- GNU General Public License on page 849
- GNU Lesser General Public License on page 852
- Apache Software License, Version 2.0 on page 858
- ISC BIND Copyright on page 864
- ISC DHCP Copyright on page 865
- Julian Seward Copyright on page 866
- Carnegie Mellon University Copyright on page 866
- Thai Open Source Software Center Copyright on page 867
- Ian F. Darwin Copyright on page 868
- Lawrence Berkeley Copyright on page 869
- MIT Kerberos Copyright on page 869
- BSD License on page 870
- David L. Mills Copyright on page 871
- OpenLDAP License on page 871
- OpenSSL License on page 872
- VIM License on page 873
- ZLIB License on page 875
- Wietse Venema Copyright on page 875
- ECLIPSE SOFTWARE on page 876
- Eclipse Public License - v 1.0 on page 876
- AOP Alliance (Java/J2EE AOP standards) on page 880
- ASM on page 880
• **Distributed Computing Laboratory, Emory University** on page 881
• **COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL)** on page 881
• **The FreeType Project LICENSE** on page 885
• **The Independent JPEG Group’s JPEG software** on page 889
• **Net-SNMP** on page 891
• **The PHP License, version 3.01** on page 897
• **INFO-ZIP** on page 898
• **MIT License** on page 900
• **Ehcache** on page 900
GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundations software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each authors protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyones free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".
Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Programs source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.
You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
   
   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be 11 distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.
8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

END OF TERMS AND CONDITIONS

GNU LESSER GENERAL PUBLIC LICENSE

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.
This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original authors reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License.

We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the users freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.
In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
   a) The modified work must itself be a software library.
   b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
   c) You must cause the whole of the work to be licensed at nocharge to all third parties under the terms of this License.
   d) If a facility in the modified Library refers to a function or a table of data to be supplied by an appropriate program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.
(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)
Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.
8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.
14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Apache Software License, Version 2.0

Copyright (c) 2004 The Apache Software Foundation. All rights reserved.

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications,
including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.
3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and
do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NONINFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all
other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.
PERL ARTISTIC LICENSE

The "Artistic License"

Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions:

"Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.

"Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder as specified below.

"Copyright Holder" is whoever is named in the copyright or copyrights for the package.

"You" is you, if you're thinking about copying or distributing this Package.

"Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)

"Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.

2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:

   a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

   b) use the modified Package only within your corporation or organization.

   c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.

   d) make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

   a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

   b) accompany the distribution with the machine-readable source of the Package with your modifications.

   c) give non-standard executables non-standard names, and clearly document the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.

   d) make other distribution arrangements with the Copyright Holder.
5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own. You may embed this Packages interpreter within an executable of yours (by linking); this shall be construed as a mere form of aggregation, provided that the complete Standard Version of the interpreter is so embedded.

6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whoever generated them, and may be sold commercially, and may be aggregated with this Package. If such scripts or library files are aggregated with this Package via the so-called "undump" or "unexec" methods of producing a binary executable image, then distribution of such an image shall neither be construed as a distribution of this Package nor shall it fall under the restrictions of Paragraphs 3 and 4, provided that you do not represent such an executable image as a Standard Version of this Package.

7. C subroutines (or comparably compiled subroutines in other languages) supplied by you and linked into this Package in order to emulate subroutines and variables of the language defined by this Package shall not be considered part of this Package, but are the equivalent of input as in Paragraph 6, provided these subroutines do not change the language in any way that would cause it to fail the regression tests for the language.

8. Aggregation of this Package with a commercial distribution is always permitted provided that the use of this Package is embedded; that is, when no overt attempt is made to make this Packages interfaces visible to the end user of the commercial distribution. Such use shall not be construed as a distribution of this Package.

9. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

10. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The End

ISC BIND Copyright

Copyright (C) 1996-2002 Internet Software Consortium.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright (C) 1996-2001 Nomimum, Inc.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NOMINUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL NOMINUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR
ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION
OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH
THE USE OR PERFORMANCE OF THIS SOFTWARE.

ISC DHCP COPYRIGHT

Copyright (c) 1995, 1996, 1997, 1998, 1999 Internet Software Consortium - DHCP. All rights
reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of
   conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list
   of conditions and the following disclaimer in the documentation and/or other materials
   provided with the distribution.
3. Neither the name of Internet Software Consortium - DHCP nor the names of its
   contributors may be used to endorse or promote products derived from this software without
   specific prior written permission. THIS SOFTWARE IS PROVIDED BY INTERNET SOFTWARE
   CONSORTIUM AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING,
   BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
   PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM OR CONTRIBUTORS
   BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
   DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS
   OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
   LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
   OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
   POSSIBILITY OF SUCH DAMAGE.
**Julian Seward Copyright**

This program, "bzip2" and associated library "libbz2", are copyright (C) 1996-2002 Julian R Seward. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, Cambridge, UK.
jseward@acm.org

bzip2/libbz2 version 1.0.2 of 30 December 2001

---

**Carnegie Mellon University Copyright**

/*
 * Copyright (c) 2001 Carnegie Mellon University. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. The name "Carnegie Mellon University" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For permission or any other legal
 *    details, please contact
4. Redistributions of any form whatsoever must retain the following
   acknowledgment:
   "This product includes software developed by Computing Services
   at Carnegie Mellon University (http://www.cmu.edu/computing/)."

Carnegie Mellon University disclaims all warranties with regard to
this software, including all implied warranties of merchantability
and fitness, in no event shall Carnegie Mellon University be liable
for any special, indirect or consequential damages or any damages
whatsoever resulting from loss of use, data or profits, whether in
an action of contract, negligence or other tortious action, arising
out of or in connection with the use or performance of this software.

Thai Open Source Software Center Copyright

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd
and Clark Cooper

Copyright (c) 2001, 2002 Expat maintainers.

Permission is hereby granted, free of charge, to any person obtaining a copy of this
software and associated documentation files (the "Software"), to deal in the Software
without restriction, including without limitation the rights to use, copy, modify, merge,
publish, distribute, sublicense, and/or sell copies of the Software, and to permit
persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or
substantial portions of the Software.

The Software is provided "as is", without warranty of any kind, express or implied,
including but not limited to the warranties of merchantability, fitness for a particular
purpose and noninfringement. In no event shall the authors or copyright holders be liable
for any claim, damages or other liability, whether in an action of contract, tort or
otherwise, arising from, out of or in connection with the software or the use or other
dealings in the software.
IAN F. DARWIN COPYRIGHT

Software written by Ian F. Darwin and others;

This software is not subject to any export provision of the United States Department of
Commerce, and may be exported to any country or planet.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice immediately at
the beginning of the file, without modification, this list of conditions, and the
following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

3. All advertising materials mentioning features or use of this software must display
the following acknowledgement:
This product includes software developed by Ian F. Darwin and others.

4. The name of the author may not be used to endorse or promote products derived from
this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR
TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
**Lawrence Berkeley Copyright**

Copyright (c) 1990 The Regents of the University of California.  
All rights reserved.  
This code is derived from software contributed to Berkeley by Vern Paxson.  
The United States Government has rights in this work pursuant to contract no.  
DE-AC03-76SF00098 between the United States Department of Energy and the University of California.  
Redistribution and use in source and binary forms with or without modification are permitted provided that: (1) source distributions retain this entire copyright notice and comment, and (2) distributions including binaries display the following acknowledgement: “This product includes software developed by the University of California, Berkeley and its contributors” in the documentation or other materials provided with the distribution and in all advertising materials mentioning features or use of this software. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.  
THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

**MIT Kerberos Copyright**

Copyright Notice and Legal Administrivia  
------------------------------------------  
Copyright (C) 1985-2002 by the Massachusetts Institute of Technology.  
All rights reserved.  
Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.  
WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Furthermore if you modify this software you must label your software as modified software and not distribute it in such a fashion that it might be confused with the original MIT software.  
M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.  
THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.  
Individual source code files are copyright MIT, Cygnus Support, OpenVision, Oracle, SunSoft, FundsXpress, and others.  
Project Athena, Athena, Athena MUSE, Discuss, Hesiod, Kerberos, Moira, and Zephyr are trademarks of the Massachusetts Institute of Technology (MIT). No commercial use of these trademarks may be made without prior written permission of MIT.
"Commercial use" means use of a name in a product or other for-profit manner. It does not prevent a commercial firm from referring to the MIT trademarks in order to convey information (although in doing so, recognition of their trademark status should be given).

The following copyright and permission notice applies to the OpenVision Kerberos Administration system located in kadmin/create, kadmin/dbutil, kadmin/passwd, kadmin/server, lib/kadm5, and portions of lib/rpc:

Copyright, OpenVision Technologies, Inc., 1996, All Rights Reserved

WARNING: Retrieving the OpenVision Kerberos Administration system source code, as described below, indicates your acceptance of the following terms. If you do not agree to the following terms, do not retrieve the OpenVision Kerberos administration system.

You may freely use and distribute the Source Code and Object Code compiled from it, with or without modification, but this Source Code is provided to you "AS IS" EXCLUSIVE OF ANY WARRANTY, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY OTHER WARRANTY, WHETHER EXPRESS OR IMPLIED. IN NO EVENT WILL OPENVISION HAVE ANY LIABILITY FOR ANY LOST PROFITS, LOSS OF DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, THOSE RESULTING FROM THE USE OF THE SOURCE CODE, OR THE FAILURE OF THE SOURCE CODE TO PERFORM, OR FOR ANY OTHER REASON.

OpenVision retains all copyrights in the donated Source Code. OpenVision also retains copyright to derivative works of the Source Code, whether created by OpenVision or by a third party. The OpenVision copyright notice must be preserved if derivative works are made based on the donated Source Code.

OpenVision Technologies, Inc. has donated this Kerberos Administration system to MIT for inclusion in the standard Kerberos 5 distribution. This donation underscores our commitment to continuing Kerberos technology development and our gratitude for the valuable work which has been performed by MIT and the Kerberos community.

Portions contributed by Matt Crawford <crawdad@fnal.gov> were work performed at Fermi National Accelerator Laboratory, which is operated by Universities Research Association, Inc., under contract DE-AC02-76CH03000 with the U.S. Department of Energy.

**BSD License**

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
DAVID L. MILLS COPYRIGHT

**************************************************************************
** Copyright (c) David L. Mills 1992-2003 **
** Permission to use, copy, modify, and distribute this software and **
** its documentation for any purpose and without fee is hereby **
** granted, provided that the above copyright notice appears in all **
** copies and that both the copyright notice and this permission **
** notice appear in supporting documentation, and that the name **
** University of Delaware not be used in advertising or publicity **
** pertaining to distribution of the software without specific, **
** written prior permission. The University of Delaware makes no **
** representations about the suitability this software for any **
** purpose. It is provided "as is" without express or implied **
** warranty. **
****************************************************************************

OPENLDAP LICENSE

The OpenLDAP Public License
Version 2.8, 17 August 2003
Redistribution and use of this software and associated documentation ("Software"), with
or without modification, are permitted provided that the following conditions are met:
1. Redistributions in source form must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and
notices, this list of conditions, and the following disclaimer in the documentation
and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.
The OpenLDAP Foundation may revise this license from time to time. Each revision is
distinguished by a version number. You may use this Software under terms of this license
revision or under the terms of any subsequent revision of the license.
THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS "AS IS" AND
ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO
EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF
THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON
ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
 ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
The names of the authors and copyright holders must not be used in advertising or
otherwise to promote the sale, use or other dealing in this Software without specific,
written prior permission. Title to copyright in this Software shall at all times remain
with copyright holders.
OpenLDAP is a registered trademark of the OpenLDAP Foundation.
Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights
Reserved. Permission to copy and distribute verbatim copies of this document is granted.
OpenSSL License

/* ====================================================================
 * Copyright (c) 1998-2003 The OpenSSL Project. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com). This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 */
COPYING

Vim is Charityware. You can use and copy it as much as you like, but you are encouraged to make a donation to orphans in Uganda. Please read the file "runtime/doc/uganda.txt" for details.

There are no restrictions on distributing an unmodified copy of Vim. Parts of Vim may also be distributed, but this text must always be included. You are allowed to include executables that you made from the unmodified Vim sources, your own usage examples and Vim scripts.

If you distribute a modified version of Vim, you are encouraged to send the maintainer a copy, including the source code. Or make it available to the maintainer through ftp; let him know where it can be found. If the number of changes is small (e.g., a modified Makefile) e-mailing the diffs will do. When the maintainer asks for it (in any way) you must make your changes, including source code, available to him.

The maintainer reserves the right to include any changes in the official version of Vim. This is negotiable. You are not allowed to distribute a modified version of Vim when you are not willing to make the source code available to the maintainer.

The current maintainer is Bram Moolenaar <Bram@vim.org>. If this changes, it will be announced in appropriate places (most likely www.vim.org and comp.editors). When it is completely impossible to contact the maintainer, the obligation to send him modified source code ceases.

It is not allowed to remove these restrictions from the distribution of the Vim sources or parts of it. These restrictions may also be used for previous Vim releases instead of the text that was included with it.

Vim is Charityware. You can use and copy it as much as you like, but you are encouraged to make a donation for needy children in Uganda. Please see |kcc| below or visit the ICCF web site, available at these mirrors:

http://iccf-holland.org/
http://www.vim.org/iccf/
http://www.iccf.nl/

The Open Publication License applies to the Vim documentation, see |manual-copyright|.

=== begin of license ===

VIM LICENSE

There are no restrictions on distributing unmodified copies of Vim except that they must include this license text. You can also distribute unmodified parts of Vim, likewise unrestricted except that they must include this license text. You are also allowed to include executables that you made from the unmodified Vim sources, plus your own usage examples and Vim scripts.

It is allowed to distribute a modified (or extended) version of Vim, including executables and/or source code, when the following four conditions are met:
1) This license text must be included unmodified.
2) The modified Vim must be distributed in one of the following five ways:
Open Source Copyright and License Statements

a) If you make changes to Vim yourself, you must clearly describe in the distribution how to contact you. When the maintainer asks you (in any way) for a copy of the modified Vim you distributed, you must make your changes, including source code, available to the maintainer without fee. The maintainer reserves the right to include your changes in the official version of Vim. What the maintainer will do with your changes and under what license they will be distributed is negotiable. If there has been no negotiation then this license, or a later version, also applies to your changes. The current maintainer is Bram Moolenaar <Bram@vim.org>. If this changes it will be announced in appropriate places (most likely vim.sf.net, www.vim.org and/or comp.editors). When it is completely impossible to contact the maintainer, the obligation to send him your changes ceases. Once the maintainer has confirmed that he has received your changes they will not have to be sent again.

b) If you have received a modified Vim that was distributed as mentioned under a) you are allowed to further distribute it unmodified, as mentioned at i). If you make additional changes the text under a) applies to those changes.

c) Provide all the changes, including source code, with every copy of the modified Vim you distribute. This may be done in the form of a context diff. You can choose what license to use for new code you add. The changes and their license must not restrict others from making their own changes to the official version of Vim.

d) When you have a modified Vim which includes changes as mentioned under c), you can distribute it without the source code for the changes if the following three conditions are met:

- The license that applies to the changes permits you to distribute the changes to the Vim maintainer without fee or restriction, and permits the Vim maintainer to include the changes in the official version of Vim without fee or restriction.
- You keep the changes for at least three years after last distributing the corresponding modified Vim. When the maintainer or someone who you distributed the modified Vim to asks you (in any way) for the changes within this period, you must make them available to him.
- You clearly describe in the distribution how to contact you. This contact information must remain valid for at least three years after last distributing the corresponding modified Vim, or as long as possible.

e) When the GNU General Public License (GPL) applies to the changes, you can distribute the modified Vim under the GNU GPL version 2 or any later version.

3) A message must be added, at least in the output of the ":version" command and in the intro screen, such that the user of the modified Vim is able to see that it was modified. When distributing as mentioned under 2)e) adding the message is only required for as far as this does not conflict with the license used for the changes.

4) The contact information as required under 2)a) and 2)d) must not be removed or changed, except that the person himself can make corrections.

If you distribute a modified version of Vim, you are encouraged to use the Vim license for your changes and make them available to the maintainer, including the source code. The preferred way to do this is by e-mail or by uploading the files to a server and e-mailing the URL. If the number of changes is small (e.g., a modified Makefile) e-mailing a context diff will do. The e-mail address to be used is <maintainer@vim.org>

It is not allowed to remove this license from the distribution of the Vim sources, parts of it or from a modified version. You may use this license for previous Vim releases instead of the license that they came with, at your option.

=== end of license ===
ZLIB LICENSE

(C) 1995-2002 Jean-loup Gailly and Mark Adler

This software is provided as-is, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

This notice may not be removed or altered from any source distribution.

Jean-loup Gailly Mark Adler
jloup@gzip.org madler@alumni.caltech.edu

If you use the zlib library in a product, we would appreciate *not* receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes.

WIELSE VENEMA COPYRIGHT

/******************************* Copyright 1995 by Wietse Venema. All rights reserved. Some individual * files may be covered by other copyrights. * This material was originally written and compiled by Wietse Venema at * Eindhoven University of Technology, The Netherlands, in 1990, 1991, * 1992, 1993, * 1994 and 1995. * Redistribution and use in source and binary forms are permitted * provided that this entire copyright notice is duplicated in all such * copies. * This software is provided "as is" and without any expressed or implied * warranties, including, without limitation, the implied warranties of * merchantability and fitness for any particular purpose. */
ECLIPSE SOFTWARE

The product includes Eclipse software (the "Eclipse Program") provided by the Eclipse Foundation and licensed to Infoblox Inc. under the Eclipse Public License v1.0.

EXCEPT AS EXPRESSLY SET FORTH IN THE ECLIPSE PUBLIC LICENSE, THE ECLIPSE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

EXCEPT AS EXPRESSLY SET FORTH IN THE ECLIPSE PUBLIC LICENSE, NEITHER THE ECLIPSE FOUNDATION NOR ANY CONTRIBUTORS TO THE ECLIPSE PROGRAM SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE ECLIPSE PROGRAM, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any provisions provided by Infoblox relating to the Eclipse Program which differ from the above terms or the Eclipse Public License are offered by Infoblox alone and not by any other party.

The source code for the Eclipse Program is available from Infoblox as described in the open source introduction.

ECLIPSE PUBLIC LICENSE - v 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS ECLIPSE PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPipient’S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

  b) in the case of each subsequent Contributor:

    i) changes to the Program, and

    ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.
"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient’s responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;
ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must:

a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor’s responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.
5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient’s patent(s), then such Recipient’s rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient’s rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient’s rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient’s obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. The Eclipse Foundation is the initial Agreement Steward. The Eclipse Foundation may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses
to the intellectual property of any Contributor under this Agreement, whether expressly, 
by implication, estoppel or otherwise. All rights in the Program not expressly granted 
under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual 
property laws of the United States of America. No party to this Agreement will bring a 
legal action under this Agreement more than one year after the cause of action arose. 
Each party waives its rights to a jury trial in any resulting litigation.

Related Links
* EPL in plain HTML
* The EPL on OSI’s site
* CPL to EPL conversion

**AOP ALLIANCE (JAVA/J2EE AOP STANDARDS)**

LICENCE: all the source code provided by AOP Alliance is Public Domain.

**ASM**

Copyright (c) 2000-2005 INRIA, France Telecom

All rights reserved.

Redistribution and use in source and binary forms, with or without 
modification, are permitted provided that the following conditions 
are met:

1. Redistributions of source code must retain the above copyright 
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright 
   notice, this list of conditions and the following disclaimer in the 
documentation and/or other materials provided with the distribution.
3. Neither the name of the copyright holders nor the names of its 
   contributors may be used to endorse or promote products derived from 
   this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" 
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE 
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE 
ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE 
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR 
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF 
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Distributed Computing Laboratory, Emory University

This software is released to the public domain, in the spirit of the original code written by Doug Lea. The code can be used for any purpose, modified, and redistributed without acknowledgment. No warranty is provided, either express or implied.

COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL)

Version 1.0

1. Definitions.

1.1. Contributor means each individual or entity that creates or contributes to the creation of Modifications.

1.2. Contributor Version means the combination of the Original Software, prior Modifications used by a Contributor (if any), and the Modifications made by that particular Contributor.

1.3. Covered Software means (a) the Original Software, or (b) Modifications, or (c) the combination of files containing Original Software with files containing Modifications, in each case including portions thereof.

1.4. Executable means the Covered Software in any form other than Source Code.

1.5. Initial Developer means the individual or entity that first makes Original Software available under this License.

1.6. Larger Work means a work which combines Covered Software or portions thereof with code not governed by the terms of this License.

1.7. License means this document.

1.8. Licensable means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. Modifications means the Source Code and Executable form of any of the following:

A. Any file that results from an addition to, deletion from or modification of the contents of a file containing Original Software or previous Modifications;

B. Any new file that contains any part of the Original Software or previous Modification; or

C. Any new file that is contributed or otherwise made available under the terms of this License.

1.10. Original Software means the Source Code and Executable form of computer software code that is originally released under this License.

1.11. Patent Claims means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.
1.12. **Source Code** means (a) the common form of computer software code in which 1.13. You (or Your) means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License. For legal entities, You includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, control means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. License Grants.

2.1. **The Initial Developer Grant.**

Conditioned upon Your compliance with Section 3.1 below and subject to third party intellectual property claims, the Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license:

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer, to use, reproduce, modify, display, perform, sublicense and distribute the Original Software (or portions thereof), with or without Modifications, and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using or selling of Original Software, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Software (or portions thereof).

(c) The licenses granted in Sections 2.1(a) and (b) are effective on the date Initial Developer first distributes or otherwise makes the Original Software available to a third party under the terms of this License.

(d) Notwithstanding Section 2.1(b) above, no patent license is granted: (1) for code that You delete from the Original Software, or (2) for infringements caused by: (i) the modification of the Original Software, or (ii) the combination of the Original Software with other software or devices.

2.2. **Contributor Grant.**

Conditioned upon Your compliance with Section 3.1 below and subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof), either on an unmodified basis, with other Modifications, as Covered Software and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: (1) Modifications made by that Contributor (or portions thereof); and (2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

(c) The licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date Contributor first distributes or otherwise makes the Modifications available to a third party.

(d) Notwithstanding Section 2.2(b) above, no patent license is granted: (1) for any code that Contributor has deleted from the Contributor Version; (2) for infringements caused by: (i) third party modifications of Contributor Version, or (ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or (3) under Patent Claims infringed by Covered Software in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. **Availability of Source Code.**

Any Covered Software that You distribute or otherwise make available in Executable form must also be made available in Source Code form and that Source Code form must be distributed only under the terms of this License.
You must include a copy of this License with every copy of the Source Code form of the Covered Software You distribute or otherwise make available. You must inform recipients of any such Covered Software in Executable form as to how they can obtain such Covered Software in Source Code form in a reasonable manner on or through a medium customarily used for software exchange.

3.2. Modifications.
The Modifications that You create or to which You contribute are governed by the terms of this License. You represent that You believe Your Modifications are Your original creation(s) and/or You have sufficient rights to grant the rights conveyed by this License.

3.3. Required Notices.
You must include a notice in each of Your Modifications that identifies You as the Contributor of the Modification. You may not remove or alter any copyright, patent or trademark notices contained within the Covered Software, or any notices of licensing or any descriptive text giving attribution to any Contributor or the Initial Developer.

3.4. Application of Additional Terms.
You may not offer or impose any terms on any Covered Software in Source Code form that alters or restricts the applicable version of this License or the recipients rights hereunder. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, you may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear that any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.5. Distribution of Executable Versions.
You may distribute the Executable form of the Covered Software under the terms of this License or under the terms of a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable form does not attempt to limit or alter the recipients rights in the Source Code form from the rights set forth in this License. If You distribute the Covered Software in Executable form under a different license, You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

You may create a Larger Work by combining Covered Software with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Software.

4. Versions of the License.
4.1. New Versions.
Sun Microsystems, Inc. is the initial license steward and may publish revised and/or new versions of this License from time to time. Each version will be given a distinguishing version number. Except as provided in Section 4.3, no one other than the license steward has the right to modify this License.

4.2. Effect of New Versions.
You may always continue to use, distribute or otherwise make the Covered Software available under the terms of the version of the License under which You originally received the Covered Software. If the Initial Developer includes a notice in the Original Software prohibiting it from being distributed or otherwise made available under any
Open Source Copyright and License Statements

subsequent version of the License, You must distribute and make the Covered Software available under the terms of the version of the License under which You originally received the Covered Software. Otherwise, You may also choose to use, distribute or otherwise make the Covered Software available under the terms of any subsequent version of the License published by the license steward.

4.3. Modified Versions.
When You are an Initial Developer and You want to create a new license for Your Original Software, You may create and use a modified version of this License if You: (a) rename the license and remove any references to the name of the license steward (except to note that the license differs from this License); and (b) otherwise make it clear that the license contains terms which differ from this License.

5. DISCLAIMER OF WARRANTY.
COVERED SOFTWARE IS PROVIDED UNDER THIS LICENSE ON AN AS IS BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED SOFTWARE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED SOFTWARE IS WITH YOU. SHOULD ANY COVERED SOFTWARE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED SOFTWARE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

6. TERMINATION.
6.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

6.2. If You assert a patent infringement claim (excluding declaratory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You assert such claim is referred to as Participant) alleging that the Participant Software (meaning the Contributor Version where the Participant is a Contributor or the Original Software where the Participant is the Initial Developer) directly or indirectly infringes any patent, then any and all rights granted directly or indirectly to You by such Participant, the Initial Developer (if the Initial Developer is not the Participant) and all Contributors under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively and automatically at the expiration of such 60 day notice period, unless if within such 60 day period You withdraw Your claim with respect to the Participant Software against such Participant either unilaterally or pursuant to a written agreement with Participant.

6.3. In the event of termination under Sections 6.1 or 6.2 above, all end user licenses that have been validly granted by You or any distributor hereunder prior to termination (excluding licenses granted to You by any distributor) shall survive termination.

7. LIMITATION OF LIABILITY.
UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED SOFTWARE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

8. U.S. GOVERNMENT END USERS.
The Covered Software is a commercial item, as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of commercial computer software (as that term is defined at 48 C.F.R. 252.227-7014(a)(1)) and commercial computer software documentation as such terms
are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Software with only those rights set forth herein. This U.S. Government Rights clause is in lieu of, and supersedes, any other FAR, DFAR, or other clause or provision that addresses Government rights in computer software under this License.

9. MISCELLANEOUS.

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by the law of the jurisdiction specified in a notice contained within the Original Software (except to the extent applicable law, if any, provides otherwise), excluding such jurisdictions conflict-of-law provisions. Any litigation relating to this License shall be subject to the jurisdiction of the courts located in the jurisdiction and venue specified in a notice contained within the Original Software, with the losing party responsible for costs, including, without limitation, court costs and reasonable attorneys fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License. You agree that You alone are responsible for compliance with the United States export administration regulations (and the export control laws and regulation of any other countries) when You use, distribute or otherwise make available any Covered Software.

10. RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

---

**The FreeType Project LICENSE**

2002-Apr-11

Copyright 1996-2002 by

David Turner, Robert Wilhelm, and Werner Lemberg

Introduction

==========

The FreeType Project is distributed in several archive packages; some of them may contain, in addition to the FreeType font engine, various tools and contributions which rely on, or relate to, the FreeType Project.

This license applies to all files found in such packages, and which do not fall under their own explicit license. The license
affects thus the FreeType font engine, the test programs, documentation and makefiles, at the very least.

This license was inspired by the BSD, Artistic, and IJG (Independent JPEG Group) licenses, which all encourage inclusion and use of free software in commercial and freeware products alike. As a consequence, its main points are that:

- We don't promise that this software works. However, we will be interested in any kind of bug reports. (`as is' distribution)

- You can use this software for whatever you want, in parts or full form, without having to pay us. (`royalty-free' usage)

- You may not pretend that you wrote this software. If you use it, or only parts of it, in a program, you must acknowledge somewhere in your documentation that you have used the FreeType code. (`credits')

We specifically permit and encourage the inclusion of this software, with or without modifications, in commercial products. We disclaim all warranties covering The FreeType Project and assume no liability related to The FreeType Project.

Finally, many people asked us for a preferred form for a credit/disclaimer to use in compliance with this license. We thus encourage you to use the following text:


Portions of this software are copyright © 1996-2002 The FreeType Project (www.freetype.org). All rights reserved.

Legal Terms

0. Definitions

Throughout this license, the terms 'package', 'FreeType Project', and 'FreeType archive' refer to the set of files originally distributed by the authors (David Turner, Robert Wilhelm, and Werner Lemberg) as the 'FreeType Project', be they named as alpha,
beta or final release.

`You' refers to the licensee, or person using the project, where 'using' is a generic term including compiling the project's source code as well as linking it to form a 'program' or 'executable'. This program is referred to as 'a program using the FreeType engine'.

This license applies to all files distributed in the original FreeType Project, including all source code, binaries and documentation, unless otherwise stated in the file in its original, unmodified form as distributed in the original archive. If you are unsure whether or not a particular file is covered by this license, you must contact us to verify this.

The FreeType Project is copyright (C) 1996-2000 by David Turner, Robert Wilhelm, and Werner Lemberg. All rights reserved except as specified below.

1. No Warranty
---------------

THE FREETYPE PROJECT IS PROVIDED 'AS IS' WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL ANY OF THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY DAMAGES CAUSED BY THE USE OR THE INABILITY TO USE, OF THE FREETYPE PROJECT.

2. Redistribution
-----------------

This license grants a worldwide, royalty-free, perpetual and irrevocable right and license to use, execute, perform, compile, display, copy, create derivative works of, distribute and sublicense the FreeType Project (in both source and object code forms) and derivative works thereof for any purpose; and to authorize others to exercise some or all of the rights granted herein, subject to the following conditions:

- Redistribution of source code must retain this license file ('FTL.TXT') unaltered; any additions, deletions or changes to the original files must be clearly indicated in accompanying documentation. The copyright notices of the unaltered, original files must be preserved in all copies of source
files.

- Redistribution in binary form must provide a disclaimer that states that the software is based in part of the work of the FreeType Team, in the distribution documentation. We also encourage you to put an URL to the FreeType web page in your documentation, though this isn't mandatory.

These conditions apply to any software derived from or based on the FreeType Project, not just the unmodified files. If you use our work, you must acknowledge us. However, no fee need be paid to us.

3. Advertising
-------------

Neither the FreeType authors and contributors nor you shall use the name of the other for commercial, advertising, or promotional purposes without specific prior written permission.

We suggest, but do not require, that you use one or more of the following phrases to refer to this software in your documentation or advertising materials: `FreeType Project', `FreeType Engine', `FreeType library', or `FreeType Distribution'.

As you have not signed this license, you are not required to accept it. However, as the FreeType Project is copyrighted material, only this license, or another one contracted with the authors, grants you the right to use, distribute, and modify it. Therefore, by using, distributing, or modifying the FreeType Project, you indicate that you understand and accept all the terms of this license.

4. Contacts
-----------

There are two mailing lists related to FreeType:

- freetype@freetype.org

  Discusses general use and applications of FreeType, as well as future and wanted additions to the library and distribution. If you are looking for support, start in this list if you haven't found anything to help you in the documentation.
The Independent JPEG Group's JPEG software

- devel@freetype.org
  Discusses bugs, as well as engine internals, design issues, specific licenses, porting, etc.

- http://www.freetype.org
  Holds the current FreeType web page, which will allow you to download our latest development version and read online documentation.

You can also contact us individually at:

David Turner <david.turner@freetype.org>
Robert Wilhelm <robert.wilhelm@freetype.org>
Werner Lemberg <werner.lemberg@freetype.org>

THE INDEPENDENT JPEG GROUP'S JPEG SOFTWARE

In plain English:

1. We don't promise that this software works. (But if you find any bugs, please let us know!)  
2. You can use this software for whatever you want. You don't have to pay us.  
3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-1998, Thomas G. Lane. All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice.

NIOS 5.1r4
NIOS Administrator Guide (Rev. A) ||| 889
unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software. (Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining code.
The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that

"The Graphics Interchange Format(c) is the Copyright property of
CompuServe Incorporated. GIF(sm) is a Service Mark property of
CompuServe Incorporated."

--- Part 1: CMU/UCD copyright notice: (BSD like) -----


Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved
Permission to use, copy, modify and distribute this software and its
documentation for any purpose and without fee is hereby granted,
provided that the above copyright notice appears in all copies and
that both that copyright notice and this permission notice appear in
supporting documentation, and that the name of CMU and The Regents of
the University of California not be used in advertising or publicity
pertaining to distribution of the software without specific written
permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL
WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR
THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL,
INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING
FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF
CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN
CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the
  names of its contributors may be used to endorse or promote
  products derived from this software without specific prior written
  permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS `AS
IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) ------

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) ------

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.
This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS `AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2005, Sparta, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the
documentatio

Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS `AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS `AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) ----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003
oss@fabasoft.com
Author: Bernhard Penz <bernhard.penz@fabasoft.com>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
THE PHP LICENSE, VERSION 3.01

Copyright (c) 1999 - 2006 The PHP Group. All rights reserved.
Redistribution and use in source and binary forms, with or without
modification, is permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in
   the documentation and/or other materials provided with the
   distribution.

3. The name "PHP" must not be used to endorse or promote products
   derived from this software without prior written permission. For
   written permission, please contact group@php.net.

4. Products derived from this software may not be called "PHP", nor
   may "PHP" appear in their name, without prior written permission
   from group@php.net. You may indicate that your software works in
   conjunction with PHP by saying "Foo for PHP" instead of calling
   it "PHP Foo" or "phpfoo"

5. The PHP Group may publish revised and/or new versions of the
   license from time to time. Each version will be given a
   distinguishing version number.
   Once covered code has been published under a particular version
   of the license, you may always continue to use it under the terms
   of that version. You may also choose to use such covered code
   under the terms of any subsequent version of the license
   published by the PHP Group. No one other than the PHP Group has
   the right to modify the terms applicable to covered code created
   under this License.

6. Redistributions of any form whatsoever must retain the following
   acknowledgment:
   "This product includes PHP software, freely available from
   <http://www.php.net/software/>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM `AS IS' AND
ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP
DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT,
INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
OF THE POSSIBILITY OF SUCH DAMAGE.

--------------------------------------------------------------------

This software consists of voluntary contributions made by many
individuals on behalf of the PHP Group.

The PHP Group can be contacted via Email at group@php.net.

For more information on the PHP Group and the PHP project,
please see <http://www.php.net>.

PHP includes the Zend Engine, freely available at

INFO-ZIP

This is version 2007-Mar-4 of the Info-ZIP license.
The definitive version of this document should be available at
ftp://ftp.info-zip.org/pub/infozip/license.html indefinitely and

Copyright (c) 1990-2007 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as
the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois,
Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth,
Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz,
David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko,
Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs,
Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda,
Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren,
Rich Wales, Mike White.
This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

MIT License

Copyright (c) 2010 Paul T. McGuire

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Ehcache

The open source Ehcache project is licensed under the Apache 2.0 License. The text of the license is available below:

/**
 * Copyright 2003-2010 Terracotta, Inc.
 *
 * Licensed under the Apache License, Version 2.0 (the "License");
 * you may not use this file except in compliance with the License.
 * You may obtain a copy of the License at
 *
 * http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
Index

A
A records
  adding to shared record groups 475
  bulk hosts 446
DDNS updates 512
host records 442
managing in IPAM 803
sort lists 495
AAAA records
  adding 454
  adding to shared record groups 475
  managing in IPAM 803
  sort lists 495
access control lists
  for TFTP, HTTP, FTP services 268
Active Directory
  authenticating admins 104
  configuring support for 518
admin groups 81
  ALL USERS group 81
  configuring on remote RADIUS server 103
  defining permissions 87
  limited-access 81
  managing 85
  superusers 81
admin roles 84
admins
  authenticating 95
  authenticating using RADIUS 99
  defining admin policy 107
  defining user profiles 36
  managing 77–130
  notifying 108, 109
  password length 108
  using Active Directory to authenticate 104
anycast 570
API
  migrating data 200
appliance status
  viewing 299, 303
audit history
  IP addresses 794
audit log
  configuring 310
  selecting type 168
  sending to syslog 307
B
backing up
  guidelines for scheduled tasks 221
backup files
  creating and restoring 289
blackhole list
  configuring for DNS 497
bloxTools environment 375
  viewing status 304
bookmarks 46
BOOTP
  specifying parameters 625
  browsers
    limitations 34
    setting time zone 37
    supported 33
bulk host records 446
  admin permissions 119
C
capacity report 313
capture traffic 312
certificates
  generating a certificate signing request 40
  generating a certificate signing request for a captive portal 705
  generating self-signed 39
  generating self-signed for captive portal 705
  importing 40
  importing for Captive Portal 706
  manage during login 36
Cisco Integrated Service Routers
  vNIOS appliances 133
CLI
  defining network settings 176
CNAME records
  adding 460
  host records 442
code pages
  Microsoft Windows 54
  columns
    editing 44
CPU temperature status 301
CPU usage status 301
D
Dashboard 35, 55–64
Data Import Wizard
  migrating data 200
database replication
  bandwidth considerations 140
database status 299
DDNS 501–542
  configuring DHCP 505–514
  configuring DNS 515–517
delegated zones 427
detailed status 298
dhcp
  bloxTools Environment 379
  NTP status icons 204
  viewing 298
DHCP configuration checklist 581
  defining admin permissions 121
dynamic DNS updates 502
  enabling LAN2 port 238
general properties 587, 618
  inheriting properties 582
  lease times 621
  NAC Foundation module 694
  starting and stopping service 639
viewing status 304
DHCP failover
configuring 656–661
Dashboard 60
DHCP filters 674
DHCP lease history
defining admin permissions 129
enabling 637
DHCP leases
clearing active 797
converting 795
scavenging 672
DHCP option filters 684
DHCP options
option 12 506
option 15 506
option 60 632
option 81 509
DHCP ranges
applying MAC address filters 687
configuring 604
Dashboard 60
defining admin permissions 115, 123, 126
permission to create from template 127
using templates 645
DHCP templates
configuring 644–653
defining admin permissions 127
disk usage status 299
DNAME records
adding 462
DNS
configuration checklist 385
defining admin permissions 116
enabling LAN2 port 239
IPv6 388
logging categories 308
root name servers 494
specifying DNS resolvers 251
starting and stopping service 484
updates for a zone 507, 508
using MGMT port 245
viewing status 304
DNS monitoring 315
DNS statistics
Dashboard 59
DNS views 392–402
defining admin permissions 117
read-only permission 115, 123
DNSKEY resource record 546
DNSSEC 544–565
documentation
related technical documents 27
downgrading NIOS software 288
dS resource record 551
dynamic DNS
See DDNS
E
Ethernet ports 230
excluding addresses
DHCP ranges and templates 607
exporting data 53
capacity report 313
from smart folders 73
lease records 671
extensible attributes
222–226
in wizards and editors 225
smart folders 68
UTF-8 encoding 54
F
fan status 300
file distribution services
status 64
TFTP, HTTP, FTP 266
filters
DHCP 674
in global search 49
search criteria 49
using for smart folders 68
viewing permissions list 93
Finder panel 35, 43, 46
fixed addresses
configuring 608
defining admin permissions 115, 123, 126
displaying lease information 667
DNS updates 509
host records 442
managing in IPAM 801
permission to create from template 127
using templates 647
force restore 294
forward zones 428
forwarders 485
FTP
backup files 289
configuring 267
defining admin permissions 130
uploading files 272
UTF-8 encoding for file names 54
viewing status 304
G
global search 49
exporting results 53
grid
configuring 131–169
configuring NTP 209
configuring syslog 306
configuring upgrade groups 274
DNS updates for DHCP 507
downgrading 288
monitoring services 304
NAT groups 135
promoting master candidate 168
removing a member 168
restarting services 261
restricting access 227
setting date, time, time zone 203
Grid Manager
overview 35
grid master 133
  configuring 145
  promoting candidate 168
  scheduled tasks after promoting 221
grid members
  adding to grid 152
  configuring NTP 211
  configuring syslog 307
  defining admin permissions 111
  distribution and upgrade status 287
  logging DHCP leases 665
  monitoring services 305
  permissions 118
  read-only permission 115, 123
  restarting services 262
  setting date, time, time zone 203
grid status
  distribution and upgrade 287
  viewing detailed 298
  widget in Dashboard 57
GSS-TSIG
  authenticating DDNS updates 519

H
  hardware and software requirements 33
  hardware status 303
  Help panel 43
  high availability (HA) pair
    configuring grid master 147
    deploying independent 186
    grid members 153
    rebooting 255
    VRRP advertisements 144
host records
  adding IP addresses 794
  admin permissions 119
  bulk 446
  configuring 442
  hostname restrictions 499
  managing in IPAM 804
  roaming 613
Hostname Compliance Report 500
  admin permissions 119
hostname
  for DNS updates 509
  restrictions 499
HTTP
  configuring 268
  defining admin permissions 130
  redirecting to HTTPS 227
  restricting access to appliance 227
  uploading files 272
  viewing status 304
HTTPS
  defined 38

I
  ICMP
    network discovery 809
  ICMP echo requests
    ping 623
  IF-MAP
    Infoblox DHCP server 638
  importing zone data 419
  independent appliances 171
  Infoblox-1552, -1552-A
    power supply status 301
  Infoblox-1852-A
    power supply status 301
  Infoblox-2000, -2000-A 257
    power supply status 301
    RAID status 302
  IP Address Management panel
    admin permissions 115, 123
  IP addresses
    converting associated objects 794
    reclaiming associated objects 797
    selecting next available 603
    viewing IP Map 791
  IP Map 35, 791
    viewing discovery data 819
  IPv6
    adding AAAA records 454
    adding PTR records 455
    configuring DNS 388
    configuring for host records 444
    configuring forward reverse-mapping zone 430
    DNS views 399
    managing networks and addresses 798
    reverse-mapping zone 407
    stub reverse-mapping zone 437

J
  joining networks 789

L
  LAN2 ports
    configuring 236
    viewing status 300
  languages
    supporting multiple 54
  LCD
    configure network settings 176
    disabling 228
    viewing status 300
  licenses
    activating 252
    managing 252
    removing 254, 256
  lite upgrades 278
  local admins 95
  logging
    configuring member 665
    in
      creating a banner 36
      login options 36
      steps 35
    login banner 36
    UTF-8 encoding 54
  logs
    audit log 310
    DHCP 665
    DHCP and DNS data 199
    DHCP logs 637
    DNS logging 308
    Microsoft 739
    replication 312
    syslog 306
### Traffic Capture
- 312

### Loopback Interface
- 568

### Captive Portal IP Address
- 703

### MAC Address Filters
- 680–681
- 128
- 694

### MAC Addresses
- Formats 608
- Master Candidate 168
- Member Status
  - Dashboard 57, 58
  - Viewing Detailed 298
- Memory Usage Status 300
- MGMT Port
  - Static Routes 249
  - Using 240
  - Viewing Status 300
- MIBs
  - SNMP 323

### Microsoft Servers
- Configuring Managing Members 731
- Supported Windows Versions 729
- Synchronizing DHCP Data 757
- Synchronizing DNS Data 741

### Microsoft Superscopes
- 768

### MTU
- For VPN Tunnels 168
- Multi-ping 797

### MX Records
- Adding 456
- Adding to Shared Record Groups 475

### Name Server Groups
- 417–418

### NAT
- Configuration Example 181
- Groups 135

### NetBIOS
- Network Discovery 809
- Network Containers 782

### Network Discovery
- 805–817
- Dashboard 62
- Defining Permissions 112, 807
- Managing Discovered Data 821
- PortIQ Appliances 818
- Viewing Discovered Data 819

### Network List
- 787

### Network Map
- 35, 783

### Network Statistics
- Dashboard 61

### Network Views
- Configuring 591
- Displayed in Bookmarks 46
- DNS Views 394

### Networks
- Adding from Net Map 785
- Configuring and Managing 387, 594
- Dashboard 62
- Defining Admin Permissions 123
- Joining 789
- Permission to Create from Template 127

### Resizing
- 788

### Shared
- 600

### Splitting
- 788

### Using in NAC Foundation Module 649

### NIOS Appliance
- Managing Licenses 252
- Rebooting 255
- Resetting 255
- Restricting HTTP Access 227
- Shutting Down 255

### NIOS GUI
- Setting Timeout 228

### NIOS Software
- Downgrading 288
- Reverting 289
- Upgrading 278

### NIOS Version
- Upgrading and Downgrading 138
- Viewing 277

### NS Records
- 453

### NSEC Resource Record 549

### NSEC3 Resource Record 549

### NSEC3PARAM Resource Record 550

### NTP
- Adding an Authentication Key 209
- Appliance as Client 208
- Appliance as NTP Server 212
- Authenticating 206
- Independent Appliance 187
- Monitoring Status 57, 204
- Using for Appliances 205
- Viewing Status 301

### OSF
- 572

### Passwords
- Length for Admins 108
- Setting in User Profile 36

### Permissions
- Applying 91
- Dashboard Widgets 56
- Defining for Admin Groups 87
- Defining for DHCP 121
- Defining for DNS 116
- Defining for Objects 88
- Defining for TFTP, HTTP, and FTP Services 130
- Defining Global 88
  - For Common Tasks 110
  - For Grid Members 110
  - For Network Discovery 112
  - Overview 87

### Phone Home
- 314

### Ping
- Configuring Settings 623
- IP Addresses 797
- Multi-ping 797

### PortIQ Appliances 818

### Ports
- Configuring VPN 167
- DNS Settings 482
- Ethernet and Service Ports 230–234
- For Grid Communications 147
LAN 236
MGMT 240
source for DNS messages 239
viewing status 300
primary servers
configuring 411
name server groups 417
stealth 412
printing data 53
capacity report 313
in smart folders 73
PTR records
adding 455
bulk hosts 446
host records 442
managing in IPAM 804

Q
queries
controlling 486
recursive 488

R
RADIUS
authenticating admins 99
authenticating DHCP clients 717
RAID
Infoblox-2000, Infoblox-2000-A 257
monitoring status 302
rebooting 255
recursion
driving 488
DNS views 395
DNSSEC 564
recycle bin 46, 47
enabling 167
restoring zone data 425
relay agent filters 682–683
remote admins
authenticating 97
authenticating using Active Directory 104
authenticating using RADIUS 99
creating admin groups for 107
remote console access
enabling and disabling 227
replication status
viewing 312
reservations
configuring 611
defining admin permissions 125
managing in IPAM 802
using templates 647
resetting NIOS appliances 255
resizing networks 788
resource records
adding 451
adding to shared record groups 475
bulk host records 446
defining permissions 118, 119
DNSSEC 545
managing in IPAM 803
specifying TTL 480
restarting services 261
restoring
backup files 293
using Recycle Bin 47
restoring database
guidelines for scheduled tasks 221
reverting 289
guidelines for scheduled tasks 221
RFC 2317 406
Riverbed Steelhead appliances
vNIOS appliances 133
roaming hosts 613
root name servers 494
root zone 408
RRSIG resource record 548

S
scavenging leases 672
scheduling tasks 216
canceling scheduled restart 263
distributions 279
network discovery 817
upgrades 817
search
global 49
setting filters 49
secondary servers
configuring 414
forwarding updates 516
name server groups 417
notifying external 482
service status 304
shared networks 600
defining admin permissions 123
shared record groups 472
admin permissions 120
shutting down 255
smart folders 67–73
Finder panel 46
SNMP 321–374
configuring 373
enable threshold crossing event trap 636
Infoblox MIBs 323
SOA records
adding email address 481
stub zone 438
zone settings 412
software and hardware requirements 33
software distribution 279
monitoring 287
Sophos NAC Advanced server 717
sort lists
DNS 495
sorting data 44
SPF records 459
splitting networks 788
SRV records
adding 457
adding to shared record groups 475
SSH
remote console access 227
restrict access to MGMT port 244
SSL
certificates 38–40
overview 38
standalone
configuring 173
Startup Wizard
  independent appliance 177
  independent HA pair 186
  single grid master 150
static routes
  configuring 247
stub zones 432
subzones 408
superusers
  configuring admin groups 82
  configuring extensible attributes 222
  defining global smart folders 69
  empty recycle bin 48
  name server groups 417
  scheduling grid restart 261
support bundles
  downloading 295
syslog 306–309
  exporting 53
system status
  Dashboard 58
system temperature status 301
system time
  monitoring 204
  setting date and time 203
  using NTP 205
T
tables
  customizing 44
  printing data 53
  selecting objects 44
  setting size 37
tasks
  monitoring background 53
  scheduling 216
TCP
  network discovery 810
technical support
  downloading support bundle 295
  enabling and disabling access 227
  restricting access to MGMT port 244
testing upgrades 282
TFTP
  backup files 289
  configuring 267
  defining admin permissions 130
  uploading files 272
  UTF-8 encoding for file names 54
  viewing status 304
time zone
  setting for grid 167
  setting for grid and members 203
  setting for independent appliances 187
  setting in user profiles 37
  upgrade schedule 283
timeout, setting 228
toolbar 43
tooltips 43
traffic capture tool 312
TTL
  DNSSEC key rollovers 556
  setting for resource records 480
TXT records
  adding 459
  adding to shared record groups 475
  DDNS updates 512
U
  upgrade groups 274
  upgrade test 282
  upgrading 278
    configuring upgrade groups 274
    guidelines for scheduled tasks 221
  uploading NIOS software 221
user class filters 686
user names
  setting in user profile 36
user profiles 36
UTF-8 encoding
  DHCP 587
  multilingual support 54
V
  views
    See DNS views
    See network views
virtual appliances 133
virtual router ID
  in VRRP advertisements 144
  independent HA pair 187
VMware
  vNIOS appliances 133
vNIOS appliances 133
VRRP advertisements 144
W
  widgets
    Dashboard 56
Z
  zones
    applying name server groups 418
    configuring authoritative 404
    configuring properties 421
    copying records 397
    defining admin permissions 117, 118
    delegation 427
    enabling and disabling 409
    enabling transfers 491
    forward 428
    importing data 182, 419
    locking and unlocking 409
    removing 423
    restoring data 425
    root 408
    stub 432
    subzones 408