Contents

Preface ................................................................................................................................. 25
Document Overview ............................................................................................................ 26
  Documentation Conventions .......................................................................................... 26
What’s New ......................................................................................................................... 28
Related Documentation ..................................................................................................... 30
Customer Care ................................................................................................................ 31
  User Accounts ................................................................................................................ 31
  Software Upgrades ........................................................................................................ 31
  Technical Support .......................................................................................................... 31

Part 1 Appliance GUI

Chapter 1 Infoblox Grid Manager .................................................................................... 35
  Management System Requirements ............................................................................... 37
    Supported Browsers ..................................................................................................... 37
    Browser Limitations ..................................................................................................... 38
  About Grid Manager ....................................................................................................... 39
    Admin Permissions for Grid Manager ........................................................................... 39
    Logging in to the GUI .................................................................................................. 39
  Setting Login Options .................................................................................................... 40
    Specifying the Grid Name and Hostname .................................................................. 40
    Creating a Login Banner ............................................................................................... 40
    Changing the Password and Email Address ............................................................... 41
    Specifying the Table Size ............................................................................................ 41
    Selecting Your Home Page ............................................................................................ 42
    Setting the Browser Time Zone .................................................................................... 42
  SSL (Secure Sockets Layer) Protocol ............................................................................ 43
  Managing Certificates .................................................................................................... 44
    About HTTPS Certificates ............................................................................................ 44
    About Client Certificates ............................................................................................... 47
  About the Grid Manager Interface ................................................................................. 48
    System Messages ........................................................................................................ 48
    Breadcrumbs Navigation ............................................................................................... 49
    Global Search ............................................................................................................... 49
    Finder Panel .................................................................................................................. 49
    Toolbar Panel ............................................................................................................... 49
    Help Panel .................................................................................................................... 49
    Wizards and Editors ..................................................................................................... 49
    Tooltips ......................................................................................................................... 49
    Customizing Tables ...................................................................................................... 50
    Selecting Objects in Tables .......................................................................................... 50
    Modifying Data in Tables ............................................................................................. 52
  Finding and Restoring Data ............................................................................................. 53
    Using Bookmarks ......................................................................................................... 53
    Using the Recycle Bin ................................................................................................... 54
    Managing Third Party URL Links ................................................................................. 56
Using Filters ................................................................. 57
Using Quick Filters ....................................................... 57
Using Global Search ..................................................... 60
Using the Go To Function ............................................... 61
About Long Running Tasks ............................................. 62
Running Tasks in the Background ................................... 63
Monitoring Long Running Tasks ..................................... 63
About CSV Import ......................................................... 64
CSV Import Limitations ................................................ 64
Creating a Data File for Import ....................................... 65
Exporting Data to Files ................................................ 65
Configuring Import Options .......................................... 65
Starting a CSV Import .................................................. 66
Exporting Displayed Data .............................................. 67
Printing from Grid Manager .......................................... 67
Multilingual Support ..................................................... 68
UTF-8 Supported Fields ................................................ 68
UTF-8 Support Limitations ............................................ 68

Chapter 2 Dashboards .................................................... 69
About Dashboards ......................................................... 70
The Tasks Dashboard ..................................................... 70
About Task Packs ........................................................ 70
The IPAM Task Pack ...................................................... 71
The Automation Task Pack ............................................ 78
Automation Task Options .............................................. 78
Network Provisioning Automation Task ......................... 78
Using the Port Activation Automation Task .................... 81
VLAN Reassignment ..................................................... 82
Provision Bare Metal Device ......................................... 83
Rogue DHCP Server Remediation .................................. 83
Using the Task Viewer to View Job Logs and Approve Jobs .................................................................................. 83
Registering NetMRI with NIOS ........................................ 84
About Dashboard Templates .......................................... 85
Adding Dashboard Templates ......................................... 85
Resetting Dashboard Templates ...................................... 86
Modifying Dashboard Templates .................................... 86
Deleting Dashboard Templates ...................................... 86
Assigning Dashboard Templates ..................................... 86
The Status Dashboard ..................................................... 87
Grid Status ...................................................................... 88
Grid Upgrade Status ...................................................... 89
Member Status (System Status) ....................................... 89
DNS Statistics ............................................................... 90
Ranges Over Threshold .................................................. 91
IPv4 Fallback Association Status ................................... 91
DHCP Statistics ............................................................ 91
Network Statistics ......................................................... 93
IPv4 Networks Over Threshold ...................................... 94
Discovery Status .......................................................... 94
My Commands .............................................................. 95
DDNS Statistics ............................................................. 95
System Activity Monitor ............................................... 95
Chapter 3 Smart Folders ................................................................. 99
About Smart Folders ..................................................................... 100
  Global Smart Folders ................................................................ 101
  My Smart Folders .................................................................... 101
Creating Smart Folders ............................................................... 102
Viewing and Modifying Data in Smart Folders......................... 103
Modifying Smart Folders ............................................................ 104
Deleting Smart Folders ............................................................... 104
Saving a Copy of a Smart Folder ............................................... 104
Printing and Exporting Data in Smart Folders ......................... 105
Part 2 Appliance Administration

Chapter 4 Managing Administrators ........................................... 109
About Admin Accounts ............................................................... 111
About Admin Groups ................................................................. 113
  Creating Superuser Admin Groups ........................................ 114
  Creating Limited-Access Admin Groups ............................... 114
About Admin Roles .................................................................... 116
  Creating Admin Roles ............................................................ 116
Managing Admin Groups and Admin Roles ............................... 117
  Modifying Admin Groups and Roles ...................................... 117
  Deleting Admin Groups and Roles ......................................... 118
  Viewing Admin Groups .......................................................... 118
  Viewing Admin Roles ............................................................ 118
  Viewing Admin Group Assignments ..................................... 119
About Administrative Permissions ............................................ 120
  Defining Global Permissions ................................................ 121
  Defining Object Permissions ................................................ 121
  Defining DNS and DHCP Permissions on Grid Members .... 124
  Applying Permissions and Managing Overlaps ..................... 126
  Managing Permissions ............................................................ 128
Authenticating Administrators ............................................... 130
Creating Local Admins ............................................................. 130
  Managing Passwords ............................................................ 131
  Modifying and Deleting Admin Accounts ............................ 131
About Remote Admins ............................................................... 133
Authenticating Admins Using RADIUS .................................... 135
  Authentication Protocols ........................................................ 135
  Accounting Activities Using RADIUS ..................................... 136
Configuring Remote RADIUS Servers .................................... 136
Configuring RADIUS Authentication ...................................... 136
Configuring a RADIUS Authentication Server Group ............ 137
Authenticating Admins Using Active Directory ....................... 139
  Configuring an Active Directory Authentication Service Group .. 140
Chapter 7 Enabling DNS Services

- Adding an HA Member
- Configuration Example: Configuring a Grid
- Cable All Appliances to the Network and Turn On Power
- Create the Grid Master
- Define Members on the Grid Master
- Join Appliances to the Grid
- Import DHCP Data
- Import DNS Data
- Using the Wizard
- After Using the Wizard
- Managing a Grid
- Changing Grid Properties
- Setting the MTU for VPN Tunnels
- Removing a Grid Member
- Promoting a Master Candidate

About the Master Grid

Chapter 6 Deploying Independent Appliances

- Independent Deployment Overview
- System Manager GUI
- Deploying a Single Independent Appliance
  - Method 1 – Using the LCD
  - Method 2 – Using the CLI
- Configuration Example: Deploying a NIOS Appliance as a Primary DNS Server
  - Cabling the Appliance to the Network and Turning On Power
  - Specifying Initial Network Settings
  - Specifying Appliance Settings
  - Defining a NAT Address
  - Enabling Zone Transfers on the Legacy Name Server
  - Importing Zone Data on an Independent Appliance
  - Designating the New Primary on the Secondary Name Server (at the ISP Site)
  - Configuring NAT and Policies on the Firewall
- Deploying an Independent HA Pair
  - Using the Infoblox NIOS Startup Wizard to Configure an HA Pair
- Configuration Example: Configuring an HA Pair for Internal DNS and DHCP Services
  - Cabling Appliances to the Network and Turning On Power
  - Specifying Initial Network Settings
  - Specifying Appliance Settings
  - Enabling Zone Transfers
  - Importing Zone Data
  - Defining Networks, Reverse-Mapping Zones, DHCP Ranges, and Infoblox Hosts
  - Defining Multiple Forwarders
  - Enabling Recursion on External DNS Servers
  - Modifying the Firewall and Router Configurations
  - Enabling DHCP and Switching Service to the NIOS Appliance
  - Managing and Monitoring
- Verifying the Deployment
  - Single Independent Appliance
  - Independent HA Pair
- Infoblox Tools for Migrating Bulk Data
Chapter 7 Managing Appliance Operations ............................................................. 241

Managing Time Settings ......................................................................................... 243
  Changing Time and Date Settings ........................................................................ 243
  Changing Time Zone Settings .............................................................................. 243
  Monitoring Time Services .................................................................................... 244

Using NTP for Time Settings .................................................................................. 245
  Authenticating NTP .............................................................................................. 246
  NIOS Appliance as NTP Client ............................................................................ 248
  Configuring a Grid to Use NTP ........................................................................... 249
  Configuring Grid Members to Use NTP ................................................................. 251
  NIOS Appliance as NTP Server ........................................................................... 252
  Configuring a NIOS Appliance as an NTP Server .............................................. 253
  Monitoring NTP .................................................................................................... 255

Scheduling Tasks ...................................................................................................... 256
  Scheduling Additions and Modifications ............................................................. 257
  Scheduling Appliance Operations ........................................................................ 257
  Scheduling Deletions ............................................................................................ 257
  Viewing Scheduled Tasks ..................................................................................... 258
  Rescheduling Tasks .............................................................................................. 260
  Guidelines for Upgrading, Backing Up, and Restoring the Database ................. 261

About Extensible Attributes ..................................................................................... 262
  Configuring Extensible Attributes ...................................................................... 263
  Using Extensible Attributes ................................................................................ 265

Managing Security Operations ................................................................................ 268
  Enabling Support Access .................................................................................... 268
  Enabling Remote Console Access ...................................................................... 268
  Permanently Disabling Remote Console and Support Access ............................ 268
  Restricting GUI/API Access ............................................................................... 268
  Enabling HTTP Redirection .............................................................................. 268
  Modifying the Session Timeout Setting ............................................................... 269
  Disabling the LCD Input Buttons ........................................................................ 269
  Configuring Security Features ............................................................................ 269

Ethernet Port Usage ................................................................................................. 271
  Modifying Ethernet Port Settings ....................................................................... 276

Using the LAN2 Port ................................................................................................. 277
  About NIC Redundancy ...................................................................................... 278
  Configuring the LAN2 Port .................................................................................. 279
  Enabling DHCP on LAN2 .................................................................................... 280
  Enabling DNS on LAN2 ....................................................................................... 281

Using the MGMT Port ............................................................................................... 282
  Appliance Management ....................................................................................... 283
  Grid Communications ......................................................................................... 285
  DNS Services ....................................................................................................... 287

Setting Static Routes ................................................................................................ 289

Enabling DNS Resolution ...................................................................................... 293

Managing Licenses .................................................................................................. 294
  Obtaining and Adding Licenses .......................................................................... 294
  Obtaining Temporary Licenses ........................................................................... 295
  Viewing Licenses .................................................................................................. 295
  Backing Up Licenses ............................................................................................ 296
  Removing Licenses ............................................................................................... 296
<table>
<thead>
<tr>
<th>Chapter 8 File Distribution Services</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About File Distribution</td>
<td>307</td>
</tr>
<tr>
<td>Configuring the TFTP Service</td>
<td>308</td>
</tr>
<tr>
<td>Configuring the FTP Service</td>
<td>309</td>
</tr>
<tr>
<td>Configuring the HTTP Service</td>
<td>310</td>
</tr>
<tr>
<td>Configuring Access Control Lists</td>
<td>310</td>
</tr>
<tr>
<td>Modifying Access Control Lists</td>
<td>311</td>
</tr>
<tr>
<td>Managing File Distribution Services</td>
<td>312</td>
</tr>
<tr>
<td>Starting and Stopping File Distribution Services</td>
<td>312</td>
</tr>
<tr>
<td>Monitoring File Distribution Services</td>
<td>312</td>
</tr>
<tr>
<td>Managing Files and Directories</td>
<td>313</td>
</tr>
<tr>
<td>Configuring File Distribution Storage Settings</td>
<td>313</td>
</tr>
<tr>
<td>Adding Directories</td>
<td>313</td>
</tr>
<tr>
<td>Modifying Directories</td>
<td>313</td>
</tr>
<tr>
<td>Uploading Files</td>
<td>314</td>
</tr>
<tr>
<td>Viewing Directories</td>
<td>314</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 9 Managing NIOS Software and Configuration Files</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Upgrades</td>
<td>315</td>
</tr>
<tr>
<td>Lite Upgrades</td>
<td>316</td>
</tr>
<tr>
<td>Full Upgrades</td>
<td>316</td>
</tr>
<tr>
<td>Managing Upgrade Groups</td>
<td>317</td>
</tr>
<tr>
<td>Adding Upgrade Groups</td>
<td>317</td>
</tr>
<tr>
<td>Modifying Upgrade Groups</td>
<td>318</td>
</tr>
<tr>
<td>Viewing Upgrade Groups</td>
<td>318</td>
</tr>
<tr>
<td>Deleting Upgrade Groups</td>
<td>319</td>
</tr>
<tr>
<td>Viewing Software Versions</td>
<td>320</td>
</tr>
<tr>
<td>Upgrading NIOS Software</td>
<td>320</td>
</tr>
<tr>
<td>Uploading NIOS Software</td>
<td>321</td>
</tr>
<tr>
<td>Distributing Software Upgrade Files</td>
<td>321</td>
</tr>
<tr>
<td>Managing Distributions</td>
<td>322</td>
</tr>
<tr>
<td>Testing Software Upgrades</td>
<td>324</td>
</tr>
<tr>
<td>Performing Software Upgrades</td>
<td>325</td>
</tr>
<tr>
<td>Managing Upgrades</td>
<td>329</td>
</tr>
<tr>
<td>Monitoring Distribution and Upgrade Status</td>
<td>330</td>
</tr>
<tr>
<td>Downgrading Software</td>
<td>331</td>
</tr>
<tr>
<td>Reverting to the Previously Running Software Version</td>
<td>332</td>
</tr>
<tr>
<td>Shutting Down, Rebooting, and Resetting a NIOS Appliance</td>
<td>297</td>
</tr>
<tr>
<td>Rebooting a NIOS Appliance</td>
<td>297</td>
</tr>
<tr>
<td>Shutting Down a NIOS Appliance</td>
<td>297</td>
</tr>
<tr>
<td>Resetting a NIOS Appliance</td>
<td>297</td>
</tr>
<tr>
<td>Managing the Disk Subsystem on the Infoblox-2000-A and -4010</td>
<td>299</td>
</tr>
<tr>
<td>About RAID 10</td>
<td>299</td>
</tr>
<tr>
<td>Evaluating the Status of the Disk Subsystem</td>
<td>300</td>
</tr>
<tr>
<td>Disk Drive Front Panel LEDs</td>
<td>301</td>
</tr>
<tr>
<td>Replacing a Failed Disk Drive</td>
<td>302</td>
</tr>
<tr>
<td>Disk Array Guidelines</td>
<td>303</td>
</tr>
<tr>
<td>Restoring Services</td>
<td>304</td>
</tr>
<tr>
<td>Canceling a Scheduled Restart</td>
<td>306</td>
</tr>
<tr>
<td>Monitoring Distribution and Upgrade Status</td>
<td>330</td>
</tr>
<tr>
<td>Managing Upgrades</td>
<td>329</td>
</tr>
<tr>
<td>Performing Software Upgrades</td>
<td>325</td>
</tr>
<tr>
<td>Full Upgrades</td>
<td>316</td>
</tr>
<tr>
<td>Lite Upgrades</td>
<td>316</td>
</tr>
<tr>
<td>About RAID 10</td>
<td>299</td>
</tr>
<tr>
<td>Configuring File Distribution Storage Settings</td>
<td>313</td>
</tr>
<tr>
<td>Adding Directories</td>
<td>313</td>
</tr>
<tr>
<td>Modifying Directories</td>
<td>313</td>
</tr>
<tr>
<td>Uploading Files</td>
<td>314</td>
</tr>
<tr>
<td>Viewing Directories</td>
<td>314</td>
</tr>
</tbody>
</table>
### Chapter 13 Configuring DNS Zones

- About Authoritative Zones
  - Configuring Authoritative Zones
  - Creating an Authoritative Forward-Mapping Zone
  - Creating an Authoritative Reverse-Mapping Zone
  - Creating a Root Zone
  - Adding an Authoritative Subzone
  - Locking and Unlocking Zones
  - Enabling and Disabling Zones
- About Domains and Zones
- Assigning Zone Authority to Name Servers
  - Specifying a Primary Server
  - Specifying a Secondary Server
- Using Name Server Groups
  - Adding Name Server Groups
  - Viewing Name Server Groups
  - Applying Name Server Groups
- Importing Zone Data
  - About Importing Data into a New Zone
  - About Importing Data into an Existing Zone
  - Importing Data into Zones
- Configuring Authoritative Zone Properties
- Removing Zones
- Restoring Zone Data
- Configuring Delegated, Forward, and Stub Zones
  - Configuring a Delegation
  - Configuring a Forward Zone
  - Configuring Stub Zones
- Viewing Zones

### Chapter 14 DNS Resource Records

- About Bulk Hosts
  - Specifying Bulk Host Name Formats
  - Before Defining Bulk Host Name Formats
  - Adding Bulk Hosts
- Managing Resource Records
  - Managing A Records
  - Managing NS Records
  - Managing AAAA Records
  - Managing PTR Records
  - Managing MX Records
  - Managing SRV Records
  - Managing TXT Records
  - Managing CNAME Records
  - Managing DNAME Records
  - Managing NAPTR Records
  - Modifying, Disabling, and Deleting Host and Resource Records
- About Shared Record Groups
  - Shared Records Guidelines
  - Configuring Shared Record Groups
  - Managing Shared Resource Records
# Chapter 15 Configuring DNS Services

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About DNS64</td>
<td>473</td>
</tr>
<tr>
<td>Specifying Hostname Policies</td>
<td>470</td>
</tr>
<tr>
<td>Configuring a DNS Blackhole List</td>
<td>468</td>
</tr>
<tr>
<td>Specifying Hostname Policies</td>
<td>470</td>
</tr>
<tr>
<td>Configuring DNS64</td>
<td>473</td>
</tr>
<tr>
<td>About Synthesis Groups</td>
<td>474</td>
</tr>
<tr>
<td>Controlling DNS Queries</td>
<td>450</td>
</tr>
<tr>
<td>Specifying Queriers</td>
<td>450</td>
</tr>
<tr>
<td>Enabling Recursive Queries</td>
<td>451</td>
</tr>
<tr>
<td>Restricting Recursive Clients</td>
<td>452</td>
</tr>
<tr>
<td>About NXDOMAIN Redirection</td>
<td>453</td>
</tr>
<tr>
<td>About NXDOMAIN Rulesets</td>
<td>454</td>
</tr>
<tr>
<td>Examples</td>
<td>455</td>
</tr>
<tr>
<td>NXDOMAIN Redirection Guidelines</td>
<td>456</td>
</tr>
<tr>
<td>Configuring NXDOMAIN Redirection</td>
<td>457</td>
</tr>
<tr>
<td>Creating Rulesets</td>
<td>457</td>
</tr>
<tr>
<td>Enabling NXDOMAIN Redirection</td>
<td>458</td>
</tr>
<tr>
<td>About Blacklists</td>
<td>459</td>
</tr>
<tr>
<td>About Blacklist Rulesets</td>
<td>460</td>
</tr>
<tr>
<td>Blacklist Guidelines</td>
<td>461</td>
</tr>
<tr>
<td>Configuring the Blacklist Feature</td>
<td>461</td>
</tr>
<tr>
<td>Enabling Blacklisting</td>
<td>462</td>
</tr>
<tr>
<td>Enabling Zone Transfers</td>
<td>463</td>
</tr>
<tr>
<td>Configure Zone Transfers</td>
<td>463</td>
</tr>
<tr>
<td>About Root Name Servers</td>
<td>465</td>
</tr>
<tr>
<td>Specifying Root Name Servers</td>
<td>465</td>
</tr>
<tr>
<td>About Sort Lists</td>
<td>466</td>
</tr>
<tr>
<td>Defining a Sort List</td>
<td>466</td>
</tr>
<tr>
<td>Configuring a DNS Blackhole List</td>
<td>468</td>
</tr>
<tr>
<td>Defining a DNS Blackhole List</td>
<td>469</td>
</tr>
<tr>
<td>Specifying Hostname Policies</td>
<td>470</td>
</tr>
<tr>
<td>Defining Grid Hostname Policies</td>
<td>470</td>
</tr>
<tr>
<td>Defining Hostname Restrictions</td>
<td>471</td>
</tr>
<tr>
<td>Obtaining a List of Invalid Record Names</td>
<td>471</td>
</tr>
<tr>
<td>About DNS64</td>
<td>472</td>
</tr>
<tr>
<td>Configuring DNS64</td>
<td>473</td>
</tr>
<tr>
<td>About Synthesis Groups</td>
<td>474</td>
</tr>
<tr>
<td>Managing Associated Zones</td>
<td>438</td>
</tr>
<tr>
<td>Configuration Example: Configuring Shared Records</td>
<td>439</td>
</tr>
</tbody>
</table>

**Contents**

- Managing Associated Zones
- Configuration Example: Configuring Shared Records
- Chapter 15 Configuring DNS Services
- Configuring DNS Service Properties
  - About Time To Live Settings
  - Adding an Email Address to the SOA Record
  - Notifying External Secondary Servers
  - Enabling the Configuration of RRset Orders
  - Specifying Port Settings for DNS
  - Specifying Minimal Responses
  - Starting and Stopping the DNS Service
- Using Forwarders
  - Specifying Forwarders
- Controlling DNS Queries
  - Specifying Queriers
- Enabling Recursive Queries
  - Enabling Recursion
  - Restricting Recursive Clients
- About NXDOMAIN Redirection
  - About NXDOMAIN Rulesets
  - Examples
  - NXDOMAIN Redirection Guidelines
  - Configuring NXDOMAIN Redirection
  - Creating Rulesets
  - Enabling NXDOMAIN Redirection
- About Blacklists
  - About Blacklist Rulesets
  - Blacklist Guidelines
  - Configuring the Blacklist Feature
  - Enabling Blacklisting
- Enabling Zone Transfers
  - Configure Zone Transfers
- About Root Name Servers
  - Specifying Root Name Servers
- About Sort Lists
  - Defining a Sort List
- Configuring a DNS Blackhole List
  - Defining a DNS Blackhole List
- Specifying Hostname Policies
  - Defining Grid Hostname Policies
  - Defining Hostname Restrictions
  - Obtaining a List of Invalid Record Names
- About DNS64
  - Configuring DNS64
Chapter 16 Configuring DDNS Updates from DHCP ........................................ 477

Understanding DDNS Updates from DHCP ........................................ 479
Configuring DHCP for DDNS .................................................................. 483
Enabling DDNS for IPv4 and IPv6 DHCP Clients .................................... 484
Sending Updates to DNS Servers ......................................................... 485
Configuring DDNS Features .................................................................. 487
Resending DDNS Updates ................................................................. 487
Generating Host Names for DDNS Updates ........................................ 487
Updating DNS for IPv4 Clients with Fixed Addresses ......................... 487
Configuring DDNS Features ............................................................... 488
About the Client FQDN Option ......................................................... 489
Enabling FQDN Option Support ....................................................... 490
Sending Updates for DHCP Clients Using the FQDN Option ................ 491
Configuring DDNS Update Verification ............................................. 492
Configuring DNS Servers for DDNS .................................................. 495
Enabling a DNS Server to Accept DDNS Updates ............................. 495
Forwarding Updates ......................................................................... 496
Supporting Active Directory .............................................................. 498
Sending DDNS Updates to a DNS Server ........................................... 498
About GSS-TSIG ............................................................................. 499
Sending Secure DDNS Updates to a DNS Server in the Same Domain .... 500
Configuring DHCP to Send GSS-TSIG Updates in the Same Domain .... 502
Sending Secure DDNS Updates to a DNS Server in Another Domain .... 509
Configuring DHCP to Send GSS-TSIG Updates to Another Domain .... 510
Sending GSS-TSIG Updates to a DNS Server in Another Forest .......... 512
Accepting DDNS Updates from DHCP Clients .................................... 513
Supporting Active Directory and Unauthenticated DDNS Updates ........ 513
Accepting GSS-TSIG-Authenticated Updates ....................................... 515
Configuring DNS to Receive GSS-TSIG Updates .............................. 517

Chapter 17 DNSSEC ........................................................................... 523

About DNSSEC ................................................................................ 524
DNSSEC Resource Records ............................................................... 525
DNSKEY Resource Records ............................................................... 525
RRSIG Resource Records ................................................................. 527
NSEC/NSEC3 Resource Records ....................................................... 528
NSEC3PARAM Resource Records .................................................... 529
DS Resource Records ................................................................. 530
Configuring DNSSEC on a Grid .......................................................... 531
Grid Master as Primary Server .......................................................... 531
Enabling DNSSEC ........................................................................ 533
Setting DNSSEC Parameters ............................................................. 534
About the DNSKEY Algorithm ......................................................... 534
About Key Rollovers ....................................................................... 534
RRSIG Signatures ......................................................................... 535
Configuring DNSSEC Parameters ..................................................... 536
Signing a Zone .............................................................................. 537
## Contents

### Managing Signed Zones
- Importing a Keyset ................................................. 539
- Exporting Trust Anchors ........................................ 539
- Checking Key-Signing Keys ..................................... 540
- Rolling Key-Signing Keys ........................................ 540
- Unsigning a Zone .................................................. 541
- Deleting and Restoring Signed Zones ......................... 541

### About HSM Signing ......................................................... 542
- Configuring a SafeNet HSM Device ............................. 543
- Monitoring the HSM Group ....................................... 544
- Enabling HSM Signing ............................................. 545
- Testing the HSM Group ............................................ 546
- Synchronizing the HSM Group .................................. 546

### Configuring Grid Members to Support DNSSEC as Secondary Servers ......................................................... 548
### Configuring Recursion and Validation for Signed Zones ......................................................... 549
- Enabling Recursion and Validation for Signed Zones .... 549
- Enabling DNSSEC Validation ................................. 550

### Chapter 18 Configuring IP Routing Options ...................... 551

#### Using the Loopback Interface ........................................ 552
#### Configuring IP Addresses on the Loopback Interface ............ 553
- Advertising Loopback Addresses to the Network .............. 554
#### About Anycast Addressing for DNS ............................. 555
- Configuring Anycast Addresses .............................. 556

### IP Routing Options ......................................................... 557
- About OSPF ......................................................... 558
- Configuring OSPF .................................................. 559
- About BGP .......................................................... 561
- Configuring BGP .................................................... 563

### Part 4 DHCP

### Chapter 19 Infoblox DHCP Services ................................. 567

#### About Infoblox DHCP Services ........................................ 568
#### IPv4 DHCP Protocol Overview ....................................... 569
#### IPv6 DHCP Protocol Overview ...................................... 570
#### IPv6 Address Structure ............................................... 571

#### Configuring DHCP Overview ........................................ 572

#### Managing DHCP Data .................................................... 574
- About Networks ....................................................... 574
- About Shared Networks .......................................... 574
- About DHCP Ranges ............................................... 574
- About Fixed Addresses .......................................... 575
- About Hosts .......................................................... 575
- DHCP Configuration Checklists ....................................... 576

#### About DHCP Inheritance ................................................ 578
- Overriding DHCP Properties ....................................... 579
- Viewing Inherited Values ......................................... 579
Chapter 21 Managing DHCP Templates .................................................. 623
  About DHCP Templates ........................................................................ 624
  About IPv4 DHCP Templates ................................................................ 625
  About IPv6 DHCP Templates ................................................................ 623
    About IPv4 Range Templates ............................................................... 625
    About IPv4 Fixed Address/Reservation Templates .............................. 625
    About IPv4 Network Templates .......................................................... 627
    Configuration Example: Creating an IPv4 Network Using a Template .... 628
  About IPv6 DHCP Templates ................................................................ 631
    About IPv6 Range Templates ............................................................... 633
    About IPv6 Fixed Address Templates ................................................. 633
    About IPv6 Network Templates .......................................................... 634
  Viewing Templates .................................................................................. 638
  Deleting Templates ................................................................................ 638

Chapter 22 Managing IPv4 DHCP Data .................................................... 639
  Configuring DHCP for IPv4 ................................................................. 641
  About the Next Available Network or IP Address ................................. 642
    Obtaining the Next Available ............................................................. 642
    Guidelines for the Next Available Network and IP Address ................ 642
  Configuring IPv4 Networks ................................................................... 643
    Adding IPv4 Networks ....................................................................... 643
    Viewing Networks .............................................................................. 645
    Modifying IPv4 Networks ................................................................... 646
    Deleting IPv4 Networks ..................................................................... 647
  Configuring IPv4 Shared Networks ....................................................... 648
    Adding IPv4 Shared Networks ............................................................ 648
    Viewing Shared Networks ................................................................... 648
    Modifying IPv4 Shared Networks ...................................................... 649
    Deleting IPv4 Shared Networks ......................................................... 649
  Configuring IPv4 Address Ranges ........................................................ 650
    Adding IPv4 Address Ranges .............................................................. 650
    Modifying IPv4 Address Ranges ......................................................... 651
    Controlling Lease Assignments .......................................................... 652
    Deleting IPv4 Address Ranges ............................................................. 652
  Configuring IPv4 Fixed Addresses ....................................................... 653
    Adding IPv4 Fixed Addresses ............................................................. 654
    Modifying IPv4 Fixed Addresses ......................................................... 655
    Deleting Fixed Addresses .................................................................. 655
  Configuring IPv4 Reservations ............................................................. 656
    Adding IPv4 Reservations ................................................................ 656
    Modifying Reservations ................................................................... 657
  Viewing IPv4 DHCP Objects ................................................................... 658
  About Roaming Hosts ........................................................................... 659
    Configuring Roaming Hosts ............................................................... 659
    Enabling Support for Roaming Hosts .................................................. 659
    Adding IPv4 Roaming Hosts ............................................................... 660
    Adding IPv6 Roaming Hosts ............................................................... 661
    Adding IPv4/IPv6 Roaming Hosts ....................................................... 661
    Viewing Roaming Hosts ..................................................................... 662
    Setting Properties for Roaming Hosts .................................................. 663
    Deleting Roaming Hosts ...................................................................... 664
## Contents

Using the Captive Portal Wizard ....................................................... 715  
Adding and Modifying the Filters and Associations ................................ 717  
Monitoring DHCP Authentication ...................................................... 717  
  Viewing DHCP Ranges and Filters .................................................. 717  
Configuration Example: Configuring Authenticated DHCP ................................ 718  
NAC Integration ................................................................................. 724  
Configuring NAC with Sophos NAC Advanced Servers ......................... 725  
About Authentication Servers ............................................................ 726  
  Adding a Server Group ................................................................... 726  
  Associating a Server Group with a Member ...................................... 727  
  Managing Server Groups ................................................................. 727  
  Clearing the Authentication Cache ................................................... 728  
Configuring DHCP Ranges .................................................................. 729  
  Listing DHCP Ranges ..................................................................... 729  
About NAC Filters ............................................................................. 730  
  Defining a NAC Filter ..................................................................... 731  

### Chapter 26 Managing IPv6 DHCP Data .................................................. 733  
Configuring IPv6 Networks .................................................................... 734  
Defining Global IPv6 Prefixes ............................................................... 734  
Managing IPv6 Networks ....................................................................... 735  
  Adding IPv6 Networks ................................................................... 735  
  Modifying IPv6 Networks ................................................................. 736  
  Deleting IPv6 Networks .................................................................. 737  
About IPv6 Shared Networks ................................................................ 737  
  Adding IPv6 Shared Networks .......................................................... 738  
  Modifying IPv6 Shared Networks ...................................................... 738  
  Deleting IPv6 Shared Networks ........................................................ 739  
Configuring IPv6 Address Ranges .......................................................... 739  
  Adding IPv6 Address Ranges ............................................................. 739  
  Setting the Priority of IPv6 Address Ranges ..................................... 740  
  Modifying IPv6 Address Ranges ......................................................... 740  
  Deleting IPv6 Address Ranges ......................................................... 741  
Configuring IPv6 Fixed Addresses ........................................................ 741  
  Adding IPv6 Fixed Addresses ........................................................... 741  
  Modifying IPv6 Fixed Addresses ....................................................... 742  
  Deleting IPv6 Fixed Addresses ........................................................ 743  
Viewing IPv6 DHCP Objects ................................................................ 743  

### Chapter 27 Managing Leases ............................................................... 745  
About DHCP Leases .......................................................................... 746  
Viewing Current Leases ..................................................................... 746  
Viewing Detailed Lease Information ..................................................... 748  
Viewing Lease History ....................................................................... 749  
Viewing Lease Event Detailed Information .......................................... 749  
Exporting Lease Records .................................................................... 750  
Clearing Leases .................................................................................. 750
# Part 5 Managing Microsoft Windows Servers

## Chapter 28 Managing Microsoft Windows Servers

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Managing Microsoft Servers</td>
<td>754</td>
</tr>
<tr>
<td>Requirements</td>
<td>755</td>
</tr>
<tr>
<td>Deployment Guidelines</td>
<td>756</td>
</tr>
<tr>
<td>Configuring Members to Manage Microsoft Servers</td>
<td>757</td>
</tr>
<tr>
<td>Setting Microsoft Server Credentials</td>
<td>757</td>
</tr>
<tr>
<td>Configuring a Managing Member</td>
<td>758</td>
</tr>
<tr>
<td>Managing Microsoft Servers</td>
<td>761</td>
</tr>
<tr>
<td>Setting Microsoft Server Properties</td>
<td>761</td>
</tr>
<tr>
<td>Changing the Managing Member or Management Mode</td>
<td>762</td>
</tr>
<tr>
<td>Backing Up Synchronized Data</td>
<td>762</td>
</tr>
<tr>
<td>Disabling Synchronization</td>
<td>762</td>
</tr>
<tr>
<td>Removing a Managed Microsoft Server</td>
<td>763</td>
</tr>
<tr>
<td>Monitoring Managed Microsoft Servers</td>
<td>763</td>
</tr>
<tr>
<td>Viewing the Status of Servers</td>
<td>763</td>
</tr>
<tr>
<td>Viewing Detailed Status Information</td>
<td>765</td>
</tr>
<tr>
<td>Viewing Synchronization Logs</td>
<td>765</td>
</tr>
<tr>
<td>Disabling Synchronization</td>
<td>762</td>
</tr>
<tr>
<td>Backing Up Synchronized Data</td>
<td>762</td>
</tr>
<tr>
<td>Setting Microsoft Server Properties</td>
<td>761</td>
</tr>
<tr>
<td>Adding Zones to Microsoft Servers</td>
<td>771</td>
</tr>
<tr>
<td>Setting Zone Properties</td>
<td>772</td>
</tr>
<tr>
<td>Deleting and Restoring Synchronized Zones</td>
<td>773</td>
</tr>
<tr>
<td>Managing Resource Records in Synchronized Zones</td>
<td>774</td>
</tr>
<tr>
<td>Synchronizing Updates</td>
<td>776</td>
</tr>
<tr>
<td>Synchronizing Delegations</td>
<td>779</td>
</tr>
<tr>
<td>Synchronizing AD-Integrated Zones</td>
<td>782</td>
</tr>
<tr>
<td>Resolving Conflicts</td>
<td>782</td>
</tr>
<tr>
<td>Viewing Members and Managed Servers</td>
<td>783</td>
</tr>
<tr>
<td>Specifying Forwarders for Microsoft Servers</td>
<td>783</td>
</tr>
<tr>
<td>Disabling and Removing Microsoft DNS Servers</td>
<td>784</td>
</tr>
<tr>
<td>Requirements</td>
<td>755</td>
</tr>
</tbody>
</table>

## Chapter 29 Managing Microsoft DNS Services

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing Microsoft DNS Servers</td>
<td>768</td>
</tr>
<tr>
<td>Synchronizing DNS Data</td>
<td>768</td>
</tr>
<tr>
<td>Synchronizing with Multiple Servers</td>
<td>769</td>
</tr>
<tr>
<td>Managing Synchronized DNS Data</td>
<td>770</td>
</tr>
<tr>
<td>Adding Zones to Microsoft Servers</td>
<td>771</td>
</tr>
<tr>
<td>Setting Zone Properties</td>
<td>772</td>
</tr>
<tr>
<td>Deleting and Restoring Synchronized Zones</td>
<td>773</td>
</tr>
<tr>
<td>Managing Resource Records in Synchronized Zones</td>
<td>774</td>
</tr>
<tr>
<td>Synchronizing Updates</td>
<td>776</td>
</tr>
<tr>
<td>Synchronizing Delegations</td>
<td>779</td>
</tr>
<tr>
<td>Synchronizing AD-Integrated Zones</td>
<td>782</td>
</tr>
<tr>
<td>Resolving Conflicts</td>
<td>782</td>
</tr>
<tr>
<td>Viewing Members and Managed Servers</td>
<td>783</td>
</tr>
<tr>
<td>Specifying Forwarders for Microsoft Servers</td>
<td>783</td>
</tr>
<tr>
<td>Disabling and Removing Microsoft DNS Servers</td>
<td>784</td>
</tr>
</tbody>
</table>

## Chapter 30 Managing Microsoft DHCP Services

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Microsoft DHCP Management</td>
<td>786</td>
</tr>
<tr>
<td>Synchronizing DHCP Data from Microsoft Servers</td>
<td>787</td>
</tr>
<tr>
<td>Viewing Synchronized Leases</td>
<td>789</td>
</tr>
<tr>
<td>Managing Synchronized DHCP Data</td>
<td>790</td>
</tr>
<tr>
<td>Adding and Managing Scopes</td>
<td>790</td>
</tr>
<tr>
<td>Viewing Scopes</td>
<td>797</td>
</tr>
<tr>
<td>Adding Fixed Addresses/Microsoft Reservations</td>
<td>798</td>
</tr>
<tr>
<td>About Superscopes</td>
<td>800</td>
</tr>
<tr>
<td>Synchronizing Updates</td>
<td>802</td>
</tr>
<tr>
<td>Managing Microsoft DHCP Servers</td>
<td>803</td>
</tr>
<tr>
<td>Viewing Members and Managed DHCP Servers</td>
<td>803</td>
</tr>
</tbody>
</table>
Configuring SNMPv3 Users ................................................................. 896
About User-Based Security Model in SNMPv3 ........................................ 895
Configuring DNS Alert Thresholds ....................................................... 890
Monitoring DNS Transactions ............................................................. 887
Using the Phone Home Feature ......................................................... 886
Using the Capacity Report ................................................................. 885
Using the Traffic Capture Tool ............................................................ 884
Using the Capacity Report ................................................................. 885
Using the Phone Home Feature ......................................................... 886
Monitoring DNS Transactions ............................................................. 887
Viewing DNS Alert Indicator Status .................................................... 889
Configuring DNS Alert Thresholds ....................................................... 890

Part 7 Monitoring and Reporting

Chapter 33 Monitoring the Appliance .................................................... 867
Viewing Status ....................................................................................... 868
Grid Status ............................................................................................ 868
Member Status ....................................................................................... 868
Viewing the Grid Node Tree ................................................................. 873
Viewing Hardware Status ...................................................................... 874
Monitoring Services ................................................................................ 875
Service Status ........................................................................................ 875
Monitoring Grid Services ....................................................................... 875
Monitoring Member Services ............................................................... 876
Using a Syslog Server ........................................................................... 877
Specifying Syslog Servers ..................................................................... 877
Configuring Syslog for Grid Members .................................................... 878
Setting DNS Logging Categories ............................................................ 879
Viewing the Syslog ................................................................................ 880
Searching in the Syslog .......................................................................... 880
Downloading the Syslog File .................................................................. 880
Monitoring Tools ................................................................................... 881
Using the Audit Log ............................................................................... 881
Viewing the Replication Status .............................................................. 883
Using the Traffic Capture Tool .............................................................. 884
Using the Capacity Report .................................................................... 885
Using the Phone Home Feature ............................................................ 886
Monitoring DNS Transactions ............................................................. 887
Viewing DNS Alert Indicator Status ..................................................... 889
Configuring DNS Alert Thresholds ....................................................... 890

Chapter 34 Monitoring with SNMP ....................................................... 893
Understanding SNMP .......................................................................... 894
About SNMPv1 and SNMPv2 ............................................................... 895
About User-Based Security Model in SNMPv3 ....................................... 895
Configuring SNMP ............................................................................... 895
Configuring SNMPv3 Users ................................................................. 896
<table>
<thead>
<tr>
<th>RFC Compliance</th>
<th>1023</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP RFC Compliance</td>
<td>1021</td>
</tr>
<tr>
<td>DNS RFC Compliance</td>
<td>1021</td>
</tr>
<tr>
<td>DHCP RFC Compliance</td>
<td>1023</td>
</tr>
</tbody>
</table>

**Part 8 Reference**

<table>
<thead>
<tr>
<th>Appendix A Glossary of Terms</th>
<th>999</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix B Grid Manager Icons</td>
<td>1007</td>
</tr>
<tr>
<td>Appendix C Regular Expressions</td>
<td>1013</td>
</tr>
<tr>
<td>Supported Expressions for Search Parameters</td>
<td>1013</td>
</tr>
<tr>
<td>Appendix D vNIOS Appliance Limitations</td>
<td>1015</td>
</tr>
<tr>
<td>vNIOS for Riverbed</td>
<td>1016</td>
</tr>
<tr>
<td>vNIOS for VMware</td>
<td>1016</td>
</tr>
<tr>
<td>Appendix E Product Compliance</td>
<td>1017</td>
</tr>
<tr>
<td>Power Safety Information</td>
<td>1018</td>
</tr>
<tr>
<td>AC</td>
<td>1018</td>
</tr>
<tr>
<td>DC</td>
<td>1018</td>
</tr>
<tr>
<td>Agency Compliance</td>
<td>1019</td>
</tr>
<tr>
<td>FCC</td>
<td>1019</td>
</tr>
<tr>
<td>Canadian Compliance</td>
<td>1019</td>
</tr>
<tr>
<td>VCCI</td>
<td>1020</td>
</tr>
<tr>
<td>RFC Compliance</td>
<td>1021</td>
</tr>
<tr>
<td>DNS RFC Compliance</td>
<td>1021</td>
</tr>
<tr>
<td>DHCP RFC Compliance</td>
<td>1023</td>
</tr>
</tbody>
</table>
Appendix F Open Source Copyright and License Statements .................... 1025

GNU General Public License ........................................................... 1027
GNU Lesser General Public License ............................................... 1030
Apache Software License, Version 2.0 .............................................. 1036
perl Artistic License ................................................................. 1041
ISC BIND Copyright ................................................................. 1042
ISC DHCP Copyright ................................................................. 1043
Julian Seward Copyright ............................................................ 1044
Carnegie Mellon University Copyright ......................................... 1044
Thai Open Source Software Center Copyright .................................. 1045
Ian F. Darwin Copyright ............................................................ 1046
Lawrence Berkeley Copyright ...................................................... 1047
MIT Kerberos Copyright .............................................................. 1047
BSD License ............................................................................... 1048
David L. Mills Copyright .............................................................. 1049
OpenLDAP License ..................................................................... 1049
OpenSSL License ....................................................................... 1050
VIM License ............................................................................. 1051
ZLIB License ............................................................................. 1053
Wietse Venema Copyright ............................................................ 1053
ECLIPSE SOFTWARE .................................................................. 1054
Eclipse Public License - v 1.0 ....................................................... 1054
AOP Alliance (Java/J2EE AOP standards) ...................................... 1058
ASM ....................................................................................... 1058
Distributed Computing Laboratory, Emory University ...................... 1059
COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) .... 1059
The FreeType Project LICENSE ..................................................... 1063
The Independent JPEG Group's JPEG software ................................ 1067
Net-SNMP ............................................................................... 1069
The PHP License, version 3.01 ...................................................... 1075
INFO-ZIP ............................................................................... 1076
MIT License ............................................................................... 1078
Ehcache ................................................................................... 1078

Index ...................................................................................... 1079
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 26
  — **Documentation Conventions** on page 26
• **What’s New** on page 28
• **Related Documentation** on page 30
• **Customer Care** on page 31
  — **User Accounts** on page 31
  — **Software Upgrades** on page 31
  — **Technical Support** on page 31
Document Overview

This guide describes how to configure and manage NIOS appliances using NIOS 6.3. It was last updated on February 1, 2012. 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>
</table>
| **bold**  | • Indicates anything that you input in the user interface, by clicking, choosing, selecting, typing, or by pressing on the keyboard.  
            • Indicates the field names in the user interface.             |
| **input** | Signifies command line entries that you type.                        |
| **variable** | Signifies variables typed into the user interface that you need to modify specifically for your configuration. These can be command line variables, file names, and keyboard characters. Indicates the names of the wizards, editors, and dialog boxes in Grid Manager, such as the Add Network wizard or the DHCP Network editor. |

Variables

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>a_record</code></td>
<td>A record</td>
</tr>
<tr>
<td><code>aaaa_record</code></td>
<td>AAAA record</td>
</tr>
<tr>
<td><code>admin_group</code></td>
<td>Name of a group of administrators</td>
</tr>
<tr>
<td><code>admin_name</code></td>
<td>Name of the appliance administrator</td>
</tr>
<tr>
<td><code>addr_range</code></td>
<td>IP address range</td>
</tr>
<tr>
<td><code>dhcp_template</code></td>
<td>DHCP template</td>
</tr>
<tr>
<td><code>domain_name</code></td>
<td>Domain name</td>
</tr>
<tr>
<td><code>directory</code></td>
<td>Directory name</td>
</tr>
<tr>
<td><code>failover_association</code></td>
<td>Failover association</td>
</tr>
<tr>
<td><code>filter_name</code></td>
<td>Name of a DHCP filter</td>
</tr>
<tr>
<td><code>fixed_address</code></td>
<td>Fixed address</td>
</tr>
<tr>
<td><code>fixed_address_template</code></td>
<td>Fixed address template</td>
</tr>
<tr>
<td><code>Grid</code></td>
<td>Grid name</td>
</tr>
<tr>
<td><code>Grid_master</code></td>
<td>Grid Master</td>
</tr>
<tr>
<td><code>Grid_member</code></td>
<td>Grid Member</td>
</tr>
<tr>
<td><code>hostname</code></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:

• **Dashboard Templates and Tasks Dashboard Only Restriction**: As part of the Task Automation features, superusers can now specify the tasks an admin group can perform from the Tasks Dashboard by creating a dashboard template and assigning it to the admin group. When you create a dashboard template, you define the tasks users in an admin group can perform and specify whether the users can configure their own dashboards when they log in to Grid Manager. When you assign a dashboard template to an admin group, all users in this group can see and perform only the tasks you define in the template, provided that the users also have the correct permissions to the objects related to the tasks.

Superusers can also restrict limited-access users to access only the Tasks Dashboard when they log in to Grid Manager. These users cannot manage other core network services through Grid Manager. They can only see the Tasks Dashboard tab and access only the tasks defined in the dashboard template, if applicable. This feature is useful when you want to define different levels of admin users and restrict them to specific tasks based on their organizational functions. For more information, see Chapter 2, Dashboards, on page 69.

• **TAE (Trinzic Automation Engine) Support**: You can now leverage NetMRI appliances to perform automated network tasks, through the Automation task pack in the Tasks Dashboard. The task pack provides the following tasks:
  — **Port Activation** – enables users to set interfaces on switches and routers to administratively Up or administratively Down;
  — **VLAN Reassignment** – enables users to reassign VLANS to different switch interfaces from any device and device group;
  — **Network Provisioning** – Enables users to provision IPv4 or IPv4/IPv6 networks with netmask, gateway router IP offset values, extensible attributes for network identification, and support for NIOS network views. Simple and Complex provisioning models are provided. IPv6 configuration supports parent networks. Interface hostnames are also supported.
  — **Rogue DHCP Server** – This task is triggered by an automated DHCP server discovery service within the automation engine. The system will detect any DHCP services that are not managed by Infoblox or contained in an approved exceptions list, and will raise an event in the Task Viewer. Automated remediation and notification can be configured. To fully utilize this feature, you must also go to Settings icon –> Setup –> Collectors and Groups –> Global tab –> Network Polling side tab and enable the Fingerprinting checkbox, which is disabled by default.
  — **Bare Metal Provisioning** – This task is triggered by the network infrastructure discovery service within the Trinzic Automation Engine. Provisioning templates and parameters configured to allow specific network configuration for new network infrastructure devices.

You can select custom scripts for execution by tasks. The scripts are developed using the Job Scripting features in NetMRI. For information about the Automation task pack, see The Automation Task Pack on page 78. For information about how to register a NetMRI appliance so you can view and perform tasks in the Automation task pack, see Registering NetMRI with NIOS on page 84.

• **Next Available Networks**: When you add networks, you can now obtain the next available IPv4 or IPv6 network from a specific network container. The next available network address is the first unused network address in the network container to which you have administrative permissions. This feature automates the allocation of networks so you can manage your network space more efficiently. For more information, see About the Next Available Network or IP Address on page 642.

• **Reserved Ranges**: When you define an address range, you can now reserve the IP addresses in the range for static hosts, provided that you do not assign a member or failover association to it. The addresses in a reserved range cannot be served as dynamic addresses. You can use this feature to organize network devices. For example, you can create a reserved range called “Printer Range” to reserve static IP addresses for printers in your network. When you allocate IP addresses for printers, you can have the appliance search for the next available IP address within “Printer Range,” and then allocate the address to a new printer. For more information, see Adding IPv4 Range Templates on page 625 and Configuring IPv4 Address Ranges on page 650.
• **Trinzic Reporting:** Infoblox provides tools that support reporting of core network services in an Infoblox Grid. You can now add an Infoblox reporting appliance as a member to the Grid and configure it as a dedicated reporting appliance. The reporting appliance collects data from Infoblox members, stores the data in the database, and generates reports that provide statistical data about IPAM, DNS, DHCP, and system activities and performance. Infoblox provides a collection of predefined reports and searches. You can also create custom report dashboards and searches based on your organizational needs. For more information, see Chapter 35, *Infoblox Reporting Solution,* on page 967.

The new Trinzic Reporting platforms are the Trinzic Reporting 1400, 4000, and 2000 appliances, and the Trinzic Reporting VM-800 appliance (virtual appliance). For information about these appliances, refer to their respective installation guides.

• **Query Redirection License:** You can install a Query Redirection license on a recursive DNS member to control its response to queries for A records of non-existent domain names and other domain names that you specify. After the license is installed, Grid Manager displays the NXDOMAIN Rulesets tab where you can create rules that specify how a DNS member responds to queries for A records for certain domain names and non-existent domain names. Each rule contains a domain name specification, and the action of the DNS member when the domain name in the query matches that in the rule. After you create the rules, you then enable the NXDOMAIN redirection feature and list the IP addresses that are included in the synthesized responses. For more information, see About NXDOMAIN Redirection on page 453.

• **IPv6 Network Map:** Just like the IPv4 Net Map, the IPv6 Net Map provides a high-level view of the network address space. You can use the IPv6 Net Map to design and plan your network infrastructure, and to configure and manage individual networks. For more information, see IPv6 Network Map on page 832.

• **IPv6 Discovery:** The appliance now supports the import of IPv6 discovery information from a NetMRI appliance. Users can then convert those discovered objects into managed IPAM data. For more information, see Integrating Discovered Data From Trinzic NetMRI on page 857.

• **DHCP Hardware Operator:** You can define the Hardware Operator option and add it as a match rule to an option filter. This option enables the appliance to match the hardware type and MAC address of the DHCP client, which it derives from the htype (hardware type), hlen (hardware length) and chaddr (client hardware address) fields of the client’s DHCP Discover and Renew packets. For more information, see DHCP Hardware Operator on page 686.

• **Scheduling Full Upgrades:** You can schedule a full upgrade that allows for member-to-master data replication. A full upgrade occurs when there are database schema changes between the existing and upgrade software versions. Scheduling an upgrade for a grid can minimize network and operational outages, especially when you have grid members that are in different time zones. Depending on the configuration of your grid and the software version that is currently running in the grid, you can schedule your upgrades for different members or upgrade groups over a period of nine days. For more information, see Scheduling Upgrades on page 325.

• **SafeNet HSM:** You can now integrate SafeNet Hardware Security Modules (HSMs) for secure private key storage and generation, and zone-signing off-loading. When using a network-attached HSM, you can provide tight physical access control, allowing only selected security personnel to physically access the HSM that stores the DNSSEC keys. When you enable this feature, the HSM performs DNSSEC zone signing, key generation, and key safe keeping. For more information, see Configuring a SafeNet HSM Device on page 543.

• **Security Enhancements:** This release contains the following security enhancements:
  — DNS TSIG keys now support the SHA256 algorithm in addition to MD5.
  — It is now possible to specify password complexity and password expiration policies.

• **SNMP Enhancements:** A number of new traps have been added as well as new statistical information to poll for. You are now able to configure thresholds for member information such as CPU, memory and LAN interface. The DHCP thresholding capability has been enhanced to now have a high-water trigger/reset as well as a low-water trigger/reset. In addition, the administrator can now select which traps to enable for forwarding to a SNMP trap receiver and/or email address. Infoblox recommends that you install the latest MIBs on your system. For more information, see Defining Thresholds for Traps on page 899 and Setting SNMP and Email Notifications on page 900.
• **Member DNS/DHCP Permissions**: You can now separate DNS and DHCP administration on different grid members by applying specific DNS and DHCP permissions to admin groups and roles. For example, you can create an admin group or role that can only create, modify, and delete DHCP ranges in a specific network on a specific member in the Grid. This admin group or role is restricted to the specified tasks on the selected Grid member. It cannot perform other DNS or DHCP tasks on this member, and it cannot perform the specified tasks on other grid members. You can also control whether admins can modify member DNS and DHCP properties. For more information, see *Defining DNS and DHCP Permissions on Grid Members* on page 124.

• **LAN2 Failover in HA**: This NIOS release supports NIC redundancy between LAN1 and LAN2 for HA configurations. For more information, see *About NIC Redundancy* on page 278.

---

### Related Documentation

Other Infoblox appliance documentation:
- *Infoblox CLI Guide*
- *Infoblox API Documentation*
- *Infoblox CSV Import Reference*
- *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 NetMRI-1102-A 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*
- *Infoblox Installation Guide for the Infoblox-4010 Appliance*
- *Quick Start Guide for Installing vNIOS Software on Riverbed Services Platforms*
- *Quick Start Guide for Installing vNIOS Software on Cisco Application eXtension Platforms*
- *Infoblox Installation Guide for Installing vNIOS on VMware*
- *Quick Start Guide for Installing vIBOS Software on VMware Platforms*
- *Infoblox Safety Guide*

To provide feedback on any of the Infoblox technical documents, please e-mail techpubs@infoblox.com.
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 109.

Software Upgrades

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

Technical Support

Part 1 Appliance GUI

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

- Chapter 1, Infoblox Grid Manager, on page 35
- Chapter 2, Dashboards, on page 69
- Chapter 3, Smart Folders, on page 99
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 37
  - **Supported Browsers** on page 37
  - **Browser Limitations** on page 38
- **About Grid Manager** on page 39
  - **Admin Permissions for Grid Manager** on page 39
  - **Logging in to the GUI** on page 39
- **Setting Login Options** on page 40
  - **Specifying the Grid Name and Hostname** on page 40
  - **Creating a Login Banner** on page 40
  - **Changing the Password and Email Address** on page 41
  - **Specifying the Table Size** on page 41
  - **Selecting Your Home Page** on page 42
  - **Setting the Browser Time Zone** on page 42
- **SSL (Secure Sockets Layer) Protocol** on page 43
- **Managing Certificates** on page 44
  - **About HTTPS Certificates** on page 44
  - **About Client Certificates** on page 47
- **About the Grid Manager Interface** on page 48
  - **System Messages** on page 48
  - **Breadcrumbs Navigation** on page 49
  - **Global Search** on page 49
  - **Finder Panel** on page 49
  - **Toolbar Panel** on page 49
  - **Help Panel** on page 49
  - **Wizards and Editors** on page 49
  - **Tooltips** on page 49
  - **Customizing Tables** on page 50
  - **Selecting Objects in Tables** on page 50
  - **Modifying Data in Tables** on page 52
• Finding and Restoring Data on page 53
  — Using Bookmarks on page 53
  — Using the Recycle Bin on page 54
  — Managing Third Party URL Links on page 56
  — Using Filters on page 57
  — Using Quick Filters on page 57
  — Using Global Search on page 60
  — Using the Go To Function on page 61
• About Long Running Tasks on page 62
  — Running Tasks in the Background on page 63
  — Monitoring Long Running Tasks on page 63
• About CSV Import on page 64
  — CSV Import Limitations on page 64
  — Creating a Data File for Import on page 65
  — Exporting Data to Files on page 65
  — Configuring Import Options on page 65
  — Starting a CSV Import on page 66
• Exporting Displayed Data on page 67
• Printing from Grid Manager on page 67
• Multilingual Support on page 68
  — UTF-8 Supported Fields on page 68
  — UTF-8 Support Limitations on page 68
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 37 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>• Secure Socket Shell (SSH) client that supports SSHv2</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>• Terminal emulation program, such as minicom or Hilgraeve Hyperterminal®</td>
<td>• Monitor Resolution: 1024 x 768 (minimum) 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 and 9.x Mozilla Firefox 5.x, 7.x and 8.x Google Chrome 10.x and 15.x</td>
</tr>
<tr>
<td>Microsoft Windows XP® (SP2+)</td>
<td>Microsoft Internet Explorer 7.x and 8.x Mozilla Firefox 3.6.x, 5.x and 7.x Google Chrome 10.x and 15.x</td>
</tr>
<tr>
<td>Red Hat® Enterprise Linux® 6.x</td>
<td>Mozilla Firefox 5.x and 7.x Google Chrome 7.x and 10.x</td>
</tr>
<tr>
<td>Red Hat® Enterprise Linux 5.x</td>
<td>Mozilla Firefox 5.x and 7.x Google Chrome 7.x and 10.x</td>
</tr>
<tr>
<td>Apple® Mac OS X 10.7.x</td>
<td>Safari 5.x Mozilla Firefox 5.x and 7.x Google Chrome 10.x and 15.x</td>
</tr>
<tr>
<td>Apple® Mac OS X 10.6.x</td>
<td>Safari 5.x Mozilla Firefox 5.x and 7.x Google Chrome 10.x and 15.x</td>
</tr>
</tbody>
</table>
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 99.
- The network and IP address maps and lists provide views of your networks and IP addresses, so you can quickly evaluate IP address usage and understand how your network resources are being utilized. You can quickly determine which IP addresses are in use, when they were allocated, and to which devices they were assigned. For information, see Chapter 31, IP Address Management, on page 809.
- Customize the Dashboard to monitor your Grid and networks. The Dashboard also provides access to frequently-used commands and the network discovery feature. You can run network discoveries to identify IP address conflicts and troubleshoot network issues. For information, see Dashboards on page 69.
- Tools such as the Finder panel, filters, and global search help you quickly find the information you need. For information, see About the Grid Manager Interface on page 48.
- 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 49.

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 37.

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 109.

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 37.
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.
   Note that if your password expired or was reset by a superuser, you may be required to enter a new password.
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 Dashboards on page 69.
Setting Login Options

Grid Manager provides several options that you can set to facilitate the login process. Additionally, you can manage CA (Certificate Authority) and server certificates on the NIOS appliance. You can import certificates, select and view their details, or remove them. To manage certificates, see *Managing Certificates* on page 44.

Specifying the Grid Name and Hostname

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

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

Creating a Login Banner

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

To create a login banner:

1. From the Grid tab, select the Grid Manager tab, and then click Grid Properties -> Edit from the Toolbar.
2. In the Grid Properties editor, select the Security tab, and then select Enable Login Banner. In the text field, enter the text that you want displayed on the login screen.
3. Save the configuration and click Restart when it displays at the top of the screen.
Changing the Password and Email Address

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

Note that when multiple users log in to Grid Manager using the same admin account, they share the same user profile and preference settings, such as the widget, table size and column settings, independent of their browser settings. Instead of using the same admin account for multiple users, you can add multiple users to the same admin group so they can share the same permissions. For information about configuring admin accounts and admin groups, see Managing Administrators on page 109.

If you can access only the Tasks Dashboard, you may not see or configure certain fields in the User Profile editor.

To change your password and email address:
1. 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.
   — Password: You can set a new password according to the requirements that are displayed.
     — Set Password: If you are a local user, select this check box to set a new password for your account. If you are a remote user, this field does not appear.
     — Old Password: Enter your current password.
     — New Password: Enter the new password, and then re-enter it in the Retype Password field.
   — Email Address: Enter your email address. Note that this address simply provides contact information. By default, this field is blank.
3. Save the configuration and click Restart if it displays at the top of the screen.

Specifying the Table Size

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

To specify table size:
1. 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. Save the configuration and click Restart if it displays at the top of the screen.
Selecting Your Home Page

When you first log in to Grid Manager, the Tasks Dashboard is your home page. You can change your home page for subsequent logins.

To change your home page:
1. Select any tab in Grid Manager, and then click User Profile from the Toolbar.
2. In the User Profile editor, complete the following:
   — Default Dashboard: Select Status or Task from the drop-down list.
3. Save the configuration and click Restart if it displays at the top of the screen.
   Grid Manager displays the selected dashboard as your home page when you log in the next time.

Setting the Browser Time Zone

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

To manually set the time zone of your browser:
1. 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. Save the configuration and click Restart if it displays at the top of the screen.
SSL (Secure Sockets Layer) Protocol

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

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

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

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

Figure 1.2 SSL Handshake
Managing Certificates

About HTTPS Certificates

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

Because the default certificate is self-signed, your browser does not have a trusted CA certificate or a cached NIOS appliance server certificate (saved from an earlier connection) to authenticate the NIOS appliance certificate. Also, the hostname in the default certificate is www.infoblox.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 45.
- When you receive the certificate from the CA, import it to the appliance, as described in Uploading Certificates on page 45.
- Download the certificate from a trusted CA, as described in Downloading Certificates on page 46.

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.
Managing Certificates

— **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 45.

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.

**Downloading Certificates**

You can download the current certificate or a self-signed certificate, as described in *Generating Self-Signed Certificates* on page 44.

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.
Managing Certificates

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

Generating a Client Certificate
To generate a client certificate:
1. Grid: From the Grid tab, select the Grid Manager tab.
   Grid Master Candidate: From the Grid tab, select the Grid Manager tab -> Members tab -> member check box.
2. From the Toolbar, click Client Cert -> Generate Client Certificate, and select either RSASHA1 or RSASHA256.
   — If you are generating a certificate for an HSM group with SafeNet Luna SA 4 devices, you must select RSASHA1; and if the certificate is for an HSM group with SafeNet Luna SA 5 devices, select RSASHA256.

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

Viewing Client Certificates
To view the client certificates that were generated:
1. Grid: From the Grid tab, select the Grid Manager tab.
   Grid Master Candidate: From the Grid tab, select the Grid Manager tab -> Members tab -> member check box.
2. From the Toolbar, click Client Cert -> View Client Certificate, and select either RSASHA1 or RSASHA256.

   The appliance displays the selected certificate.

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

![Grid Manager Interface Diagram](image)

**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 60.

Finder Panel

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

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

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

Toolbar Panel

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

Help Panel

The Help panel provides the following types of Help:

• Help: Expand this section to view information about the window currently displayed.
• Documentation: Expand this section to download the latest versions of the Infoblox Administrator Guide and Infoblox API Documentation.
• Support: Expand this section to view links to the Infoblox web site and Technical Support site.
• About: Expand this section to view information about the NIOS software version.

You can resize, collapse, and expand the Help panel. In addition, each dialog box also provides a Help panel that contains information specific to the dialog box. You can expand and collapse the Help panel in dialog boxes as well.

Wizards and Editors

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

Note that all required fields are denoted by asterisks.

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

ToolTips

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

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

To resize columns in a table:

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

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

1. In the table, mouse over to a header title and click the down arrow key.
2. Select Sort Ascending or Sort Descending.

To edit columns:

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 check box to select all rows on this page only.

Click this link to select all rows on all pages.

Use these navigational buttons to page through the display.
Modifying Data in Tables

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

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

To modify data in a table:

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

Figure 1.5 Inline Editing
Finding and Restoring Data

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

- **Smart Folders**: Contains a hierarchical list of smart folders that are available in My Smart Folders. For information, see [My Smart Folders](#) on page 101.
- **Bookmarks**: Contains bookmarked objects, such as networks and IP addresses. For information, see [Using Bookmarks](#).
- **Recycle Bin**: Contains deleted objects that can be restored or permanently removed. For information, see [Using the Recycle Bin](#) on page 54.
- **URL Links**: Contains a list of third party URLs that you previously added. You can add more URL links, and modify and delete existing URL links. For information, see [Managing Third Party URL Links](#) on page 56.

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

In addition, Grid Manager also provides the following:

- **Filters** to customize data displays. For more information, see [Using Filters](#) on page 57 and [Using Quick Filters](#) on page 57.
- **Global Search** to search the NIOS database for objects that match your criteria. For more information, see [Using Global Search](#) on page 60.
- **Go To function** to quickly locate an object. For more information, see [Using the Go To Function](#) on page 61.

Using Bookmarks

The Bookmarks section displays objects for which you have created bookmarks. You can create bookmarks for objects such as networks, DNS zones, and admin groups. To bookmark an object, navigate to its page and click the Bookmark icon at the top of the page. If you have more than one network view, Grid Manager displays the name of the bookmark with the network view to which the object belongs. For example, when you bookmark IP address 10.128.0.10 in the default network view, Grid Manager displays the bookmark as `default > 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.
Using the Recycle Bin

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

You must enable the Recycle Bin in Grid Manager to store and restore deleted objects. For information about how to enable and disable the Recycle Bin, see 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. Save the configuration and click Restart if it displays at the top of the screen.

Viewing Objects in the Recycle Bin

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

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

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

On the appliance, only superusers have permissions to fully manage the URL links. Superusers can create URL links and make them globally available to all users. If you have limited-access permissions, you can only add URL links for your own use. You cannot share the links with other users.

You can do the following in the URL Links section:

- Add new URL links, as described in Adding URL Links.
- Modify URL links, as described in Modifying URL Links.
- Delete URL links, as described in Deleting URL Links.

Adding URL Links

1. In the Finder panel, expand URL Links.
2. Click Add.
3. In the URL Configuration dialog box, complete the following:
   - URL: Enter the URL of the destination page you want to add. The appliance supports valid URL entries that contain up to 2000 characters. When you enter the URL, the appliance validates the entry. You cannot save the entry if the URL is not in a valid format.
   - Name: Enter a name that represents the portal or site of the URL.
   - Set as global parameter: This field appears only if you log in as a superuser. Select this check box to make the URL link globally available to all users.
   - Logo: Click Upload to add a logo to the URL. The appliance displays the logo in 16x16 pixels. Click Reset to Default to use the default logo.
4. Save the configuration.

Modifying URL Links

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

Deleting URL Links

To permanently delete an URL link:
1. In the Finder panel, expand URL Links.
2. Hover your mouse over the URL you want to delete, and then click the Delete icon.
3. In the Delete URL Link dialog box, click Yes.
Finding and Restoring Data

Using Filters

You can control the amount and the kind of data displayed in a specific panel by adding filter criteria. When you add filter criteria, the appliance screens the data based on your filter rules and displays only the information that matches the rules. To narrow your search for specific information, you can add up to 10 filter rules. In some panels, such as the DHCP Networks tab, you can switch between viewing information with and without the filter criteria by toggling the filter on and off. You can save filter criteria as quick filters so you can reuse the same filter rules to obtain updated information without redefining them each time you log in to the appliance. For information about quick filters, see Using Quick Filters on page 57.

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 266. For example, after you modify the extensible attribute “Building” with new value “West”, you can find the objects that are not updated by defining a filter with “Building” “does not equal” “West”.

To use a filter:

1. In a panel, click Show Filter to enable the function.
2. In the filter section, complete the following:
   - In the first drop-down list, select a field such as an object name, comment, or an extensible attribute (fields with a gray background) as the filter criterion. Grid Manager displays only the supported fields.
   - In the operator drop-down list, select an operator for the filter criterion. Depending on what you select in the first filter field, this list displays the relevant operators for the selection.
   - 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.
- Click Toggle Filter Off to have the appliance list all data without applying filter criteria.

Using Quick Filters

A quick filter saves filter rules that you define in a specific panel. You can reuse a quick filter to find updated information in a panel without specifying the same rules each time. Superusers can define quick filters and share them with local users. Limited-access users can only create quick filters for their own use. You can create up to 10 global and 10 local quick filters in each panel that supports filters. For information about filters, see Using Filters on page 57.

The appliance supports the following quick filters:

- System quick filters: These are predefined filters. You cannot modify the criteria of these filters. System quick filters are prefixed with [S] in the quick filter list. Infoblox currently supports the following system quick filters in the DNS data panels:
  - All Forward Mapping Zones: This quick filter displays all forward mapping zones in lexicographical order.
  - All Reverse Mapping Zones: This quick filter displays all IPv4 and IPv6 reverse mapping zones in numerical order. The appliance displays IPv4 zones before IPv6 zones.
  - All IPv4 Reverse Mapping Zones: This quick filter displays only the IPv4 reverse mapping zones in numerical order.
— **All IPv6 Reverse Mapping Zones**: This quick filter displays only the IPv6 reverse mapping zones in numerical order.

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

- Global quick filters: Only superusers can define global quick filters. You can make global filters available to all users. Limited-access users can use global quick filters, but they cannot modify them. Global filters are prefixed with [G] in the filter list.
- Local quick filters: Limited-access users can create local quick filters for their own use. You cannot share local quick filters with other users in the Grid. Local filters are prefixed with [L] in the filter list.

**Adding Quick Filters**

1. In a panel that supports filters, click **Show Filters**.
2. In the filter section, define filter criteria for the quick filter, as described in **Using Filters** on page 57.
3. Click **Save**.
4. In the **Save Quick Filter** dialog box, complete the following:
   - **Name**: Enter a name for the quick filter. The name must be 20 characters or longer. Ensure that you use a unique name for each quick filter in a particular filter category. For example, you can use the same filter name for both a global and local filter, but you cannot do so for two local filters.
   - **Set as a global quick filter**: This displays only if you log in as a superuser. Select this check box to make the quick filter globally available to all users.
5. Save the configuration.

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

**Modifying Quick Filters**

1. In a panel that supports filters, click **Show Filters**, and then select the quick filter you want to modify from the **Quick Filter** drop-down list.
2. In the filter section, click the **Edit** icon next to the filter name.
3. Modify the filter criteria, as described in **Using Filters** on page 57.
4. Click **Save**.
5. In the **Save Quick Filter** dialog box, you can click **Save** to save the modified filter criteria under the same quick filter name. You can also modify the quick filter name, as described in **Adding Quick Filters**, and save the entry as a new quick filter.
6. Save the configuration.

**Applying Quick Filters**

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

Turning Off Quick Filters
You can do one of the following to turn off a quick filter:
• Select None from the quick filter drop-down list.
• Click Toggle Filter Off or Reset in the filter section.
• Delete a quick filter, as described in Deleting Quick Filters.

Deleting Quick Filters
1. In a panel that supports filters, click Show Filters, and then select the quick filter you want to delete from the Quick Filter drop-down list.
2. In the filter section, click the Delete icon next to the filter name.
3. In the Delete Quick Filter dialog box, click Yes to permanently delete the quick filter.
Using Global Search

You can use the global search function to search the entire NIOS database for data that matches a specific value and filter criteria. You can enter a search value and define filter criteria to refine the search. 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 1013.
   - In the Type drop-down list, select an object type, comment, or an extensible attribute (fields with a gray background) as the filter criterion. Grid Manager displays all the supported fields in the drop-down list. The default is Type. Grid Manager searches all objects when you use the default. You can narrow down the search and improve the search performance by selecting an object type.
   - In the operator drop-down list, select an operator for the filter criterion. Depending on what you select in the first filter field, this list displays the relevant operators for the selection.
   - In the value field, enter or select the attribute value for the first filter field. Depending on what you select for the first two filter fields, you can either enter a value or select an attribute from a drop-down list. For example, if you select an extensible attribute in the first filter field, you can enter the attribute value here. If you use the default Type in the first filter field, you can select an object or record type from the drop-down list. The default is ALL. Grid Manager searches all object types when you use the default.
3. Optionally, click the + icon to add another filter. You can add up to 10 filter rules.
4. After you finish defining filters, click Apply or press Enter.

In the Results table, 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 Using the Recycle Bin on page 54.

You can print search results. You can also export search results in CSV (comma separated value) format. For information, see About CSV Import on page 64 and Exporting Displayed Data on page 67.

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

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

You can run the following tasks in the background:

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

To run a task in the background:

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

You can view the progress of the task by clicking the progress bar at the top of the interface. For information, see Monitoring Long Running Tasks on page 63.

Monitoring Long Running Tasks

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

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

The CSV import feature allows you to import DNS, DHCP, and IPAM data through Grid Manager. You can use this feature to do the following:

- Migrate or add new data
- Overwrite existing data
- Merge new data with existing data

To import new data, you must first prepare a data file, include all the required fields and follow the proper syntax, and then start an import through Grid Manager. Alternatively, you can export existing data to a data file, modify the data, and then use the import feature to import the modified data in to the database. The appliance allows you to either overwrite existing data with the modified data or merge new data with the existing data. For information, see Configuring Import Options on page 65.

The appliance supports CSV import for most record types. For the list of supported record types, refer to the Infoblox CSV Import Reference. For each supported record type, you must include all required fields in the header row of the dataset that you want to import. For specific guidelines for creating a data file, refer to the Infoblox CSV Import Reference. After each import, the Restart icon is enabled even when restarting services is not required for the imported data to take effect.

CSV Import Limitations

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

- Only superusers can perform CSV import operations.
- You can import only one CSV file at a time.
- When you stop an import, the appliance completes the import of the data row it is currently processing before it stops the import. You cannot resume the import from where it stopped.
- You cannot roll back to previous data.
- The following data cannot be imported: Microsoft management, DNSSEC, and GSS-TSIG data.
- CSV import does not support DNSSEC zones, though resource records added for a signed zone are supported.
- Only editable data can be imported. Discovered data cannot be imported or manipulated.
- When you promote a new Grid Master during an import, the import stops; and it does not restart on the new Grid Master. When a failover occurs during an import, the import stops on the old active node, and it does not restart on the new active node.
- It may take longer than expected to import a large number of DHCP ranges that are associated with a single MAC address filter.
- When a CSV import starts, the appliance validates the first 100,000 rows of data in the CSV file. If the file contains more than 100,000 rows of data, the appliance validates the rest of the data as the import progresses.
- The appliance supports up to one million rows of data in each CSV import.

You must complete the following to import a data file:

1. If you do not already have a data file, create one following the guidelines for the supported objects to ensure that you include all the required fields in the file. For information, refer to the Infoblox CSV Import Reference. Alternatively, you can export existing data and update the file for re-import. For information, see Exporting Data to Files on page 65.
2. Configure import options. For information, see Configuring Import Options on page 65.
3. Start a data import. For information, see Starting a CSV Import on page 66.
About CSV Import

Creating a Data File for Import

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

Exporting Data to Files

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

To export all data to a CSV file:

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

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

You can also export only the displayed fields in a panel. For information, see Exporting Displayed Data on page 67.

Configuring Import Options

Before you import a data file, configure the import options, as follows:

1. From the Data Management tab, click CSV Import from the Toolbar.
2. In the Import Manager editor, select the Options tab, and then complete the following:
   - Add - Create a new object from each row in the uploaded file: Select this to add new information to the database.
   - Edit - Modify existing object: Select one of the following to update the existing data:
     - Overwrite - Values from the uploaded file replace existing values: When you select this option, the appliance overwrites the existing data with the data from the uploaded file. If you want to overwrite values in the required fields, you must include the required fields and the corresponding _NEW_XXXX fields in the data file.
     - Merge - Update missing values with values from the uploaded file: When you select this option, the appliance adds only the data that is not currently in the database. It does not overwrite the existing data, even if the data file contains new values for certain fields. If you want to overwrite values in the required fields, you must include the required fields and the corresponding _NEW_XXXX fields in the data file.
   - On error: Select one of the following to tell the appliance what to do when it encounters an error during an import:
     - Stop importing: The appliance stops the data import once it encounters an error in the uploaded file.
     - Skip to the next row and continue: The appliance skips over errors and continues the data import. You can download an error report to identify the erroneous data. For information, see Starting a CSV Import on page 66.
Starting a CSV Import

After you configure the import options, you can select a data file and start an import.

1. From the **Data Management** tab, select the **IPAM**, **DNS**, or **DHCP** tab.
2. Click **CSV Import** from the Toolbar.
3. In the **Import Manager** editor, select the **File Selection** tab, and then complete the following:
   - **File**: Click **Select**. In the **Upload** dialog box, click **Select** to navigate to the file you want to import, and then click **Upload**.
   - **Separator**: From the drop-down list, select the separator you use in the data file. The default is **Comma**.

In the File Preview table, Grid Manager displays the header row, the first six rows, and up to 15 columns of the imported data. Field names with asterisks (*) indicate required fields. Note that you must define these fields in the imported file. If any of the required fields are missing, the appliance generates an error during the import.

Grid Manager also displays the following information:
   - **Current Status**: If an import is in progress, this field displays its current status. Otherwise, it displays the date and time of the last import.
   - **Last Action**: Displays the last operation and the admin who initiated it.
   - **Rows Completed**: The number of rows of data the import has processed. Depending on the import options, Grid Manager displays either the row number at which it stops an import when it encounters an error or the total number of rows it has processed by skipping over the erroneous data. For example, if there are 100 rows of data and you select “On error: Stop importing,” and there is an error in row 90, Grid Manager displays 90 of 100 here. If you select “On error: Skip to the next row and continue,” Grid Manager displays 100 of 100 here and displays 1 in **Rows with Errors**.
   - **Rows with Errors**: The number of rows of data the import has detected errors. Click **Download Errors** to download the CSV file that contains the fields and the rows of erroneous data. You can use this report as a reference to update the data file before you import the file again.

**Note**: You can also start and stop an import, and review the import status from the **CSV Import Status** widget on the Dashboard. For information, see **CSV Import Status** on page 98.
### Exporting Displayed Data

You can export visible information, such as global search results and the syslog file, in CSV format from panels and pages that support the Export function, and then easily convert the file to PDF and other file formats. You can also export all data in a specific panel. For information, see [Exporting Data to Files](#) on page 65.

To export displayed data:

1. From Grid Manager, navigate to the panel that contains the data you want to export. For example, if you want to export data for DNS zones, select the **Data Management** tab -> **DNS** tab -> **Zones** tab.
2. In the panel, select **Export visible data** from the Export drop-down menu.
3. In the **Export** dialog box, click **Start**. Grid Manager displays a message about the time required to export data could be long depending on the amount of data.
4. Click **Download** when the export is finished.
5. Depending on your browser and operating system, you may need to do one of the following in the **Opening .csv** dialog box:
   - **Open with**: Select a program with which you want to open the .csv file.
   - **Save to Disk**: Select this if you want to save the .csv file to your local computer.
   - **Do this automatically for files like this from now on**: Select this check box if you want Grid Manager to use the same method for future exports. When you select this check box, Grid Manager does not display the Opening .csv dialog box in the future.
6. Click **OK**.
   - Depending on the selected option, Grid Manager opens the file using the program you select, or saves the file to your local computer.

### Printing from Grid Manager

In Grid Manager, you can print information from panels and pages that support the Print function. Grid Manager prints data one page at a time. The amount of data that is displayed in a specific panel depends on the table size configuration that you set in your user profile. For information, see [Specifying the Table Size](#) on page 41.

To print:

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

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

- Hostnames for Microsoft Windows clients that support Microsoft Windows code pages. For information, see Configuring UTF-8 Encoding for Hostnames on page 610.
- 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  Dashboards

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

- **About Dashboards** on page 70
- **The Tasks Dashboard** on page 70
  - **About Task Packs** on page 70
  - **The IPAM Task Pack** on page 71
  - **The Automation Task Pack** on page 78
- **About Dashboard Templates** on page 85
  - **Adding Dashboard Templates** on page 85
  - **Modifying Dashboard Templates** on page 86
  - **Deleting Dashboard Templates** on page 86
  - **Assigning Dashboard Templates** on page 86
- **The Status Dashboard** on page 87
  - **Grid Status** on page 88
  - **Grid Upgrade Status** on page 89
  - **Member Status (System Status)** on page 89
  - **DNS Statistics** on page 90
  - **Ranges Over Threshold** on page 91
  - **IPv4 Failover Associations Status** on page 91
  - **DHCP Statistics** on page 91
  - **Network Statistics** on page 93
  - **IPv4 Networks Over Threshold** on page 94
  - **Discovery Status** on page 94
  - **My Commands** on page 95
  - **DDNS Statistics** on page 95
  - **System Activity Monitor** on page 95
  - **File Distribution Statistics** on page 96
  - **Active WebUI Users** on page 96
  - **Microsoft Servers Status Widget** on page 97
  - **CSV Import Status** on page 98
About Dashboards

The Dashboard is your home page on Grid Manager. It provides easy access to tasks and a quick view to the status of your Grid and core network services. Grid Manager provides the following dashboards:

- **Tasks**: The Tasks Dashboard contains task packs that provide easy access to commonly performed tasks. A task pack is a collection of tasks that belong to a specific service or function, such as IPAM or Automation. For information, see The Tasks Dashboard on page 70.
- **Status**: The Status Dashboard provides various widgets for viewing and managing DNS, DHCP, and IPAM status and data. For information, see The Status Dashboard on page 87.

When you first log in to Grid Manager, the Tasks Dashboard is your home page. You can change your home page for subsequent logins.

To change your home page:

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

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

The Tasks Dashboard

The Tasks Dashboard provides easy access to commonly performed tasks, such as adding networks and adding host records. Tasks are grouped by service-specific task packs. You must install valid licenses on the appliance to see and perform specific tasks on the Tasks Dashboard. For information about the required licenses for IPAM tasks, see Table 2.1 on page 71.

You must also have at least read-only permission to a task-related object to add or hide the task in its task pack. To execute a task, you must have the appropriate permissions to the member and objects that are related to the tasks. For example, to add a host record from the Tasks Dashboard, you must have at least read-only permission to the host records task and read/write permission to the zone and network in which the host records are created. For information about permissions, see Administrative Permissions for Dashboard Tasks on page 170.

About Task Packs

Grid Manager displays task packs, such as the IPAM and Automation task packs, based on valid licenses installed on the appliance. To access the IPAM task pack, you must have valid DNS or DHCP license installed on the NIOS appliance. To access the Automation task pack, you must first set up a Trinzic NetMRI appliance, install the Trinzic Automation license on the NIOS appliance, and register as a user. For information about how to activate the Automation task pack, refer to the Trinzic NetMRI Administrator Guide.

Each task in a task pack opens a workflow dialog in which you can create task-related objects without navigating through other tabs and editors in Grid Manager. Depending on the task you perform, Grid Manager displays task results in the Result page from which you can access newly created objects, such as networks and host records. Note that when a task takes longer than usual to complete, it becomes a long running task. For information about long running tasks, see About Long Running Tasks on page 62.

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

- **The IPAM Task Pack** on page 71
- **The Automation Task Pack** on page 78
The IPAM Task Pack

The IPAM task pack contains the following tasks:

- Add Networks
- Add Hosts
- Add Fixed Addresses
- Add CNAME Record
- Add TXT Record
- Add MX Record

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

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

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

Required Licenses for IPAM Tasks

Table 2.1 lists the required licenses for viewing and performing IPAM tasks on the Tasks Dashboard.

Table 2.1: Required Licenses for IPAM Tasks

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

For information about how to install licenses, see Managing Licenses on page 294.

Add Networks

You can create IPv4 and IPv6 networks from the Tasks Dashboard (either from scratch or from a network template that contains predefined properties). You can also create networks from the Data Management tab. For more information about IPv4 and IPv6 networks, see Configuring IPv4 Networks on page 643 and Configuring IPv6 Networks on page 734.

To add networks from the Tasks Dashboard:
1. Click Add Networks in the IPAM task pack and complete the following in the Add Networks wizard:
   - Network View: This appears only when you have multiple network views. From the drop-down list, select the network view in which you want to create the network.
   - Mask: Enter the netmask or use the netmask slider to select the appropriate number of subnet mask bits for the network.
— **Template**: Click **Select Template** to select a network template. When you use a template to create a network, the configuration of the template applies to the new network. If the template specifies a fixed netmask, you cannot edit the netmask in this dialog. You can click **Clear** to remove the template. For information about templates, see *About IPv4 Network Templates* on page 628 and *About IPv6 Network Templates* on page 636.

— **Networks**: Do one of the following to add new networks:

  - **Click** the Add icon to create a new network.
    - **For IPv4 networks**: Grid Manager adds a row to the table. Enter the network address in the **Network** field. You can also select a network and click the **Delete** icon to delete it.
    - **For IPv6 networks**: If you are adding a network for a previously defined global IPv6 prefix, you can select the prefix from the **IPv6 Prefix** drop-down list. The default is **None**, which means that you are not creating an IPv6 network for a previously defined subnet route. If you have defined a global prefix at the Grid level, the default is the global prefix value. Click **Add** and Grid Manager adds a row to the table. Enter the network address in the **Network** field. When you enter an IPv6 address, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2001:0db8:0000:0000:0000:0000:0102:0304 can be shortened to 2001:db8::0102:0304. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The appliance displays an IPv6 address in its shortened form, regardless of its form when it was entered. Click **Add** again to add another network. You can also select a network and click the **Delete** icon to delete it.

  or

  Click the Next Available icon to have the appliance search for the next available network. For more information about the next available network, see *About the Next Available Network or IP Address* on page 642. Complete the following in the Next Available Networks section:

  - **Create new network(s) under**: Enter the network container in which you want to create the new network. When you enter a network that does not exist, the appliance adds it as a network container. When you enter a network that is part of a parent network, the parent network is converted into a network container if it does not have a member assignment or does not contain address ranges, fixed addresses, reservations, shared networks, and host records that are served by DHCP. When you enter a network that has a lower CIDR than an existing network, the appliance creates the network as a parent network and displays a message indicating that the newly created network overlaps an existing network. You can also click **Select Network** to select a specific network in the **Network Selector** dialog box. For information about how the appliance searches for the next available network, see *Obtaining the Next Available* on page 642.

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

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

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

— **Extensible Attributes**: Click the Add icon to enter extensible attributes. Grid Manager adds a row to the table each time you click the Add icon. Select the row and the attribute name from the drop-down list, enter the value, and select whether the attribute is required. For more information about extensible attributes, see *Using Extensible Attributes* on page 265.
The Tasks Dashboard

2. Save the configuration.

or

Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, click Later and enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.

The appliance saves the networks you just created, and Grid Manager displays them in the Result page. When you click a newly created network on this page, Grid Manager displays the IP Map panel from which you can view detailed information about the network. For information about the IP Map panel, see IP Map on page 825.

You can also add and modify other information about the networks you just created. For information about modifying network information, see Managing IPv4 DHCP Data on page 639 and Managing IPv6 DHCP Data on page 733.

Add Hosts

Host records provide a unique approach to the management of DNS, DHCP, and IPAM data. By using host records, you can manage multiple DNS records and DHCP and IPAM data collectively, as one object on the appliance. You can add IPv4 and IPv6 addresses to host records from the Tasks Dashboard or the Data Management tab. Note that when you add a host record from the Tasks Dashboard, they are configured only for DNS. For more information about Infoblox host records, see About Host Records on page 811.

To add host records from the Tasks Dashboard:

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

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

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

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

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

     Click the Add icon and the appliance adds a row to the table. Complete the following in the table to add a new host record:

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

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

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

     or

     Click the Next Available icon to have the appliance search for the next available IP address for the host record. For information about the next available IP address, see About the Next Available Network or IP Address on page 642. Complete the following in the Next Available IP section:

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

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

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

     — **Extensible Attributes** table: Click the Add icon to enter extensible attributes. The appliance adds a row to the table each time you click the Add icon. Select the row and the attribute name from the drop-down list, enter the value, and select whether the attribute is required. For more information about extensible attributes, see Using Extensible Attributes on page 265.
2. Save the configuration.

   or

   Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, click **Later** and enter a date, time, and time zone. For information, see **Scheduling Tasks** on page 256.

   The appliance saves the host records you just created, and Grid Manager displays them in the Result page. When you click a newly created host on this page, Grid Manager displays the **Data Management -> DNS -> Zones** tab from which you can view information about the host record.

   You can also add and modify other information about the host records. For information about modifying host information, see **About Host Records** on page 811.

### Add Fixed Addresses

You can add IPv4 and IPv6 fixed addresses from the Tasks Dashboard or from the **Data Management** tab. For more information about fixed addresses, see **Configuring IPv4 Fixed Addresses** on page 653 and **Configuring IPv6 Fixed Addresses** on page 741.

To add fixed addresses from the Tasks Dashboard:

1. Click **Add Fixed Addresses** in the IPAM task pack and complete the following in the **Add Fixed Addresses** wizard:
   - **Network View**: This appears only when you have multiple network views. From the drop-down list, select the network view in which you want to create the fixed address.
   - **Protocol**: Select **IPv4** to add IPv4 addresses and **IPv6** to add IPv6 addresses.
   - **Template**:
     - Click **Select Template** to select a fixed address template. When you use a template to create a fixed address, the configuration of the template applies to the new fixed address. You can also click **Clear** to remove the template. For information about templates, see **About DHCP Templates** on page 624.
     - **Addresses**:
       - Do one of the following to add fixed addresses:
         - For IPv4 fixed addresses: Enter the IPv4 address and MAC address. Click the Add icon to add another fixed address.
         - For IPv6 fixed addresses: Enter the IPv6 address and DUID. Click the Add icon again to add another fixed address.
       - or
       - Click the Next Available icon to have the appliance search for the next available address. Complete the following:
         - **Create new fixed addresses under**: Click **Select** to select the network or address range in the **Network/Range Selector** dialog box from which you want the appliance to search for the next available IP address for this fixed address.
         - **Number of new fixed addresses**: Enter the number of fixed addresses you want to add to the selected network or address range. Note that if there is not enough space in the selected network or address range to create the number of fixed addresses specified here, Grid Manager displays an error message. The maximum number is 20 at a time. Note that when you have existing fixed addresses in the table and you select one, the number you enter here includes the selected fixed address.
         - **Add Next**: Click **Add Next** to add the fixed addresses. The appliance lists the fixed addresses to the table. Ensure that you enter the MAC address or DUID for each fixed address.
         - **Extensible Attributes** table: Click the Add icon to enter extensible attributes. The appliance adds a row to the table each time you click the Add icon. Select the row and the attribute name from the drop-down list, enter the value, and select whether the attribute is required. For more information about extensible attributes, see **Using Extensible Attributes** on page 265.
2. Save the configuration.
   or
   Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, click Later
   and enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.
   The appliance saves the fixed addresses you just created, and Grid Manager displays them in the Result page.
   When you click a newly created fixed address on this page, Grid Manager displays the Data Management -> IPAM
   -> IP Map or List tab from which you can view information about the fixed address.
   You can also add and modify other information about the fixed addresses you just created. For more information
   about modifying fixed address information, see Managing IPv4 DHCP Data on page 639 and Managing IPv6 DHCP
   Data on page 733.

Add CNAME Record

A CNAME record maps an alias to a canonical name. You can use CNAME records in both IPv4 forward- and IPv4
reverse-mapping zones to serve two different purposes. (At this time, you cannot use CNAME records with IPv6
reverse-mapping zones.) For more information about CNAME records, see Managing CNAME Records on page 421.
To add a CNAME record from the Tasks Dashboard:
1. Click Add CNAME Record in the IPAM task pack and complete the following in the Add CNAME Record wizard:
   — Network View: This appears only when you have multiple network views. From the drop-down list, select the
     network view in which you want to create the CNAME record.
   — Alias: Click Select Zone to select a DNS zone from the Zone Selector dialog box. If you have only one zone,
     Grid Manager displays the zone name here when you click Select Zone. Enter the alias for the canonical
     name. For an IPv4 reverse-mapping zone, enter the host portion of an IP address. For example, if the full IP
     address is 10.1.1.1 in a network with a 25-bit netmask, enter 1. (The 10.1.1.0/25 network contains host
     addresses from 10.1.1.1 to 10.1.1.126. The network address is 10.1.1.0, and the broadcast address is
     10.1.1.127.)
   — 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.
     To add a CNAME record to a forward-mapping zone, enter the complete canonical (or official) name of the
     host. To add a CNAME record to a reverse-mapping zone, enter host_ip_addr.prefix.network.in-addr.arpa
     (host IP address + 2317 prefix + network IP address + in-addr.arpa). For example, enter
     1.0.25.1.1.10.in-addr.arpa. This IP address must match the address defined in the PTR record in the
     delegated child zone.
   — Comments: Enter useful information about this record.
   — Disable: Select the check box to disable the record without deleting its configuration. Clear the check box to
     enable the record.
2. Save the configuration, or click Next to define extensible attributes. For information, see Using Extensible
   Attributes on page 265.
   or
   Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, click Later
   and enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.
3. Click Restart if it appears at the top of the screen.
   You can also add and modify other information about the CNAME record you just created. For more information about
   modifying the CNAME record, see Modifying, Disabling, and Deleting Host and Resource Records on page 431.

Add TXT Record

A TXT (text record) record contains supplemental information for a host. For example, if you have a sales server that
serves only North America, you can create a text record stating this fact. You can create more than one text record for
a domain name. You can add a TXT record from the Tasks Dashboard or the Data Management tab. For more
information about TXT records, see Managing TXT Records on page 420.
To add TXT records from the Tasks Dashboard:

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

2. Save the configuration, or click **Next** to define extensible attributes. For information, see **Using Extensible Attributes** on page 265.

   or

   Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, click **Later** and enter a date, time, and time zone. For information, see **Scheduling Tasks** on page 256.

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

### Add MX Record

An MX (mail exchanger) record maps a domain name to a mail exchanger. A mail exchanger is a server that either delivers or forwards mail. You can specify one or more mail exchangers for a zone, as well as the preference for using each mail exchanger. A standard MX record applies to a particular domain or subdomain. You can add an MX record from the Tasks Dashboard or the **Data Management** tab. For more information about MX records, see **Managing MX Records** on page 418.

To add MX records from the Tasks Dashboard:

1. Click **Add MX Record** in the IPAM task pack and complete the following in the **Add TXT Record** wizard:
   - **Network View**: This appears only when you have multiple network views. From the drop-down list, select the network view in which you want to create the MX record.
   - **Mail Destination**: If Grid Manager displays a zone name, enter the mail destination here. If no zone name is displayed or if you want to specify a different zone, click **Select Zone**. When there are multiple zones, Grid Manager displays the **Zone Selector** dialog box. Click a zone name in the dialog box, and then enter the mail destination. If you want to define an MX record for a domain whose name matches the zone you selected, leave this field blank. Grid Manager automatically adds the domain name (the same as the zone name) to the MX record. For example, if you want to create an MX record for a mail exchanger serving the **corp100.com** domain and you selected the **corp100.com** zone, and leave this field empty.
If you want to define an MX record for a subdomain, enter the subdomain name. The appliance prefixes the name you enter to the domain name of the selected zone. For example, if you want to create an MX record for a mail exchanger serving site1.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.

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

— **Shared Record Group**: This field appears only when you are creating a shared record. Click Select Shared Record Group. If you have only one shared record group, the appliance displays the name of the shared record group here. If you have multiple shared record groups, select the shared record group in the Shared Record Group Selector dialog box. You can use filters or the Go to function to narrow down the list.

— **Host Name Policy**: Displays the hostname policy of the selected zone. Ensure that the hostname you enter complies with the hostname restriction policy defined for the zone.

— **Mail Exchanger**: Enter the fully qualified domain name of the mail exchanger.

— **Preference**: Select an integer from 10 to 100, or enter a value from 0 to 65535. The preference determines the order in which a client attempts to contact the target mail exchanger.

— **Comment**: Enter useful information about this record.

— **Disable**: Select the check box to disable the record without deleting its configuration. Clear the check box to enable the record.

2. Save the configuration, or click **Next** to define extensible attributes. For information, see Using Extensible Attributes on page 265.

   or

   Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, click **Later** and enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.

3. Click **Restart** if it appears at the top of the screen.
The Automation Task Pack

The Automation task pack requires the configuration, licensing and connection of a Trinzic NetMRI appliance to support automation tasks. The appliance models that support task pack operation include the following:

- Trinzic NetMRI 1102-A
- Trinzic Automation 4000

You install the Trinzic NetMRI appliance into the managed network, ensuring the appliance is reachable by the NIOS Grid Master.

The Automation task pack contains the following tasks:

- Network Provisioning Automation Task
- Using the Port Activation Automation Task
- Specifying a Port Activation Script
- Assigning a New Script to the VLAN Reassignments Task
- Rogue DHCP Server Remediation

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

To hide tasks in a task pack:

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

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

Required Licenses for Automation Tasks

To view results, configure features and perform automation tasks on the Tasks Dashboard, you install the TAE license into the NIOS system. A specific license must also be installed on the Trinzic NetMRI appliance supporting the TAE feature set.

For information about how to install licenses, see Managing Licenses on page 294.

Automation Task Options

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

- Network Provisioning Automation Task
- Using the Port Activation Automation Task
- Specifying a Port Activation Script

Network Provisioning Automation Task

The Network Provisioning task runs in two modes: a basic mode with a much shorter list of configuration options, and a more complex mode that provides detailed configuration for provisioning a network, including the use of NIOS network views, extensible attributes and network templates.

New networks can be provisioned on routed networks and on switched networks. In the latter case, you can specify the new VLAN number and VLAN name for provisioning, along with the Device Group Device and Interface. the Device Group values are taken from the Device Groups defined on the Trinzic Automation Engine from which NIOS obtains its data.
Network Provisioning supports two types of networks: IPv4, in which the new network is IPv4 only, and IPv4 and IPv6, in which the new network runs both protocol stacks.

Simple vs. Complex Provisioning

Use of a Network View determines whether you use the simple or detailed views of provisioning a network. A network view is a single routing domain with its own networks and shared networks. In NIOS, all networks must belong to a network view. You can manage networks in one network view independently of other network views. Because network views are mutually exclusive, the networks in each view can have overlapping address spaces with multiple duplicate IP addresses without impacting network integrity.

Also, the same network segment can be present in multiple network views. When you create a new network, you select one view in which to place it, and preserve those values to apply to another view.

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

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

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

Applying Extensible Attributes

Extensible attributes are associated with a specific network view, and are referenced by the Network Provisioning task. Should you configure a new network using a network view, you may need to consider the application of extensible attributes to the new network (they are not automatically applied, but will appear in the Network Provisioning dialog if those attributes are defined in the chosen Network View). Extensible attributes are generally defined for descriptive and tracking purposes in the network. A network view may have attributes such as Building, Country, Region, Site, State or VLAN, for example. Attributes are defined for network views in NIOS but are not defined by the Trinzic Automation Engine.

If the NIOS system supports only a single network view, no View selections are made for the purposes of network provisioning.

Required settings for provisioning a new network will show a red asterisk (*) by the option name.

To perform an automatic network provisioning task:

1. From the Dashboards tab, select the Tasks tab -> Network Provisioning.
2. Select the network Type for provisioning: IPv4 or IPv4 and IPv6.
3. To configure IPv4 provisioning:
   a. Enter the Parent Network value (or click Select Network to choose the parent network from a list if using a Network View).
   b. Choose the Network Template from the drop-down list if one is provided by the chosen Network View. The Network template is otherwise optional.
   c. Drag the Netmask slider to the required CIDR mask bit depth (1-32).
   d. In the New Network field, enter the IP prefix for the new network.
   e. In the Router Address field, enter the IP address for the router interface.
   f. Select any Extensible Attributes in the list if they are provided; otherwise, you can create new ones by clicking Add and choosing the Attribute Name, Value and the Required setting.
4. To configure IPv6 provisioning:
   a. Enter the Parent Network value (or click Select Network to choose the parent network from a list if using a Network View).
   b. Choose the Network Template from the drop-down list if one is provided by the chosen Network View. The Network template is otherwise optional.

The Provision Network task provides subnetting tools.
c. Drag the Netmask slider to the required CIDR mask bit depth (1-32).

d. In the New Network field, enter the IP prefix for the new network.

e. In the Router Address field, enter the IP address for the router interface.

f. Select any Extensible Attributes in the list if they are provided; otherwise, you can create new ones by clicking Add and choosing the Attribute Name, Value and the Required setting.

5. Enter the required name value in the Interface Hostname field. (Examples include “eth0” and “serial0.”)

6. Select the DNS Zone under which the hostname operates.

7. Choose a device group from the Device Group drop-down list.

8. From the Device drop-down list, choose the switch or router on which the network will originate.

9. If the selected device is a router, the VLAN Number and VLAN Name fields will be disabled.

10. From the Interface list, choose the interface to which the network will be reassigned. The drop-down list contains all the interfaces from the chosen network device, and also shows the ports’ respective states (up/down, up/up and so on).

   If an interface shows Routed or Switched, it cannot be selected for provisioning as it is already being used as part of an active network.

11. If the chosen device is a switch, enter the new VLAN Number on which the new network segment runs.

12. If the chosen device is a switch, enter the new VLAN Name on which the new network segment runs.

13. Click Provision Network to commit settings.

The system sends the configuration request to the Trinzic Automation Engine and displays the task configuration sequence.

You can start NetMRI from the registered Trinzic Automation Engine to check job execution.

1. In the Automation Tasks pane, click the down arrow gadget and select Launch TAE.

NetMRI will launch in a new browser tab. To check on script executions, go to Configuration Management –> Job Management side tab –> Job History and view details about provisioning jobs and other jobs that execute as a result of NIOS-based automation tasks.

**Defining Options for the Network Provisioning Task**

The Network Provisioning task provides several configuration options that affect how the task operates. Hostname provisioning for interfaces is useful for troubleshooting purposes in the network, usually to ensure that an admin knows which router interface they are connecting through to communicate with the device. The hostname value is actually provisioned from within the Network Provisioning task. Enabling the Hostname Required? check box sets the Trinzic Automation Engine to provision the network with hostnames applied to the router interfaces for easier identification.

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

The same principles also apply for IPv6 networks, except that the IPv6 value is entered manually in hexadecimal instead of being selected from a drop-down list. Most provisioned IPv6 networks will use a /64 network address. You can also select a different script from the default for the Network Provisioning task.
To define settings for the Network Provisioning automated task:

1. From the Dashboards tab, select the Tasks tab. Under the Network Provisioning task, click the settings icon on the top right.

2. If the provisioning process requires a hostname, enable the Hostname Required? check box. (The network interface hostname ("eth0," "serial0") and the Zone that it belongs to are defined in the Network Provisioning task.)

3. Choose a gateway offset value from the IPv4 Gateway Address Offset drop-down list. If no value is selected, the offset value defaults to 1 for the provisioned network address.

4. If an IPv6 offset is required for provisioning an IPv6 network or for provisioning a network that supports both IPv4 and IPv6 addressing, enter the IPv6 Gateway Address Offset value in hexadecimal. If no value is entered, the offset value defaults to 0000.0000.0000.0001 for the provisioned network address, indicating an offset value of 1 for the gateway IP address.

5. In the Script Name dropdown, choose the script that you wish to run for the Port Activation task. The scripts are located on the Trinzic Automation 4000 appliance, and referenced for use by NIOS. By default, the bundled Port Activation script is selected.

6. Click Save to commit settings.

7. Click Cancel to close the dialog.

The system sends the request to the Trinzic Automation Engine and displays a Provisioning Network Config updated notification message.

Using the Port Activation Automation Task

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

1. From the Dashboards tab, select the Tasks tab -> Port Activation.

2. Choose the Device Group from the drop-down list.

3. From the Device drop-down list, choose the network device on which port activation will be executed.

   The Interfaces table lists all interfaces on the current device. The VLAN and VLAN Name columns list the VLAN assigned to each port (VLAN 1/Default resides on all ports without an explicit VLAN assignment). The OP Status column will show the current state of each interface.

4. Scroll down the table to locate the interface(s) you want to activate.

5. From the Admin Status column, select Up (or Down) from the drop-down list for the chosen interface.

6. Set any other interfaces on the current device based on your assigned task.

7. Click Apply to commit settings.

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

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

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

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

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

The system sends the request to the Trinzic Automation Engine and displays a notification message.

VLAN Reassignment

VLANs can be reassigned to new interfaces on individual L2/L3 switches in the managed network. A VLAN can have a path across several switches; when you make changes on a given switch, make sure that the path is maintained. To ensure end-to-end connectivity, you may need to change VLAN port assignments on more than one switch in the path. This feature operates with the VLAN Trunking Protocol (VTP). VLAN switching is changed across one port per switch at a time. Should you need to change VLAN assignments across more than one switch in the path, plan accordingly.

VLANs must already be configured on the switch(es) being changed, and be detected by the Trinzic Automation Engine.

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

   Note: You can reassign a VLAN to a port that is operationally or administratively Down.

   The Current VLAN value will show the VLAN to which the selected interface is currently assigned.

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

   The system sends the configuration request to the Trinzic Automation Engine and displays the task configuration sequence.

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

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

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

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

The system sends the request to the Trinzic Automation Engine and displays a notification message. The VLAN Reassignment task will also write the full running configuration to the device’s memory, making it the saved configuration. If the user made a change to the running configuration, in parallel with the port activation change, and did not save it, those changes will also be saved.

Provision Bare Metal Device

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

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

Rogue DHCP Server Remediation

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

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

Using the Task Viewer to View Job Logs and Approve Jobs

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

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

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

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

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

4. Click Close to close the Task Viewer.

In the Trinzic Automation Engine, you can also check Configuration Management –> Job Management side tab –> Job History and view details about any jobs that execute as a result of NIOS-based automation tasks.

### Registering NetMRI with NIOS

You must register a NetMRI/Trinzic Automation 4000 system with NIOS to support driving the Trinzic Automation Tasks. This registration is done directly in the NIOS system. You need the admin account and password for the Trinzic Automation Engine system (a NetMRI 1102-A appliance or a Trinzic Automation 4000 system) and its hostname or IP address.

1. From the **Dashboards** tab, select the **Tasks** tab.

2. In the Automation Tasks pane, click the down arrow gadget and select **TAE Registration**.

3. Under TAE Settings, do the following:
   a. Enter the IP address or resolved host name of the Trinzic Automation Engine system supporting the Automation task pack.
   b. Enter the **TAE Admin Password**.

   This information is specific to the Trinzic NetMRI or Trinzic Automation 4000 system supporting the Automation tasks in NIOS.

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

After registration, the TAE Registration menu item changes to read **TAE Deregistration** to support disconnecting from the Trinzic Automation Engine appliance.

You can also start NetMRI from the registered Trinzic Automation Engine.

1. From the **Dashboard** tab, select the **Tasks** tab.

2. In the Automation Tasks pane, click the down arrow gadget and select **Launch TAE**.

NetMRI will launch in a new browser tab. To check on script executions, go to Configuration Management –> Job Management side tab –> Scripts and check the Last Run column.

The NIOS Task Viewer (see **Using the Task Viewer to View Job Logs and Approve Jobs**) also provides the log history of automated jobs.
About Dashboard Templates

Superusers can specify the tasks an admin group can perform from the Tasks Dashboard tab by creating a dashboard template and assigning it to the admin group. When you create a dashboard template, you define the tasks users in an admin group can perform and specify whether the users can configure their own dashboards when they log in to Grid Manager. When you assign a dashboard template to an admin group, all users in this group can see and perform the tasks you define in the template, provided that the users also have the correct permissions to the objects related to the tasks. For information about administrative permissions, see Administrative Permissions for Dashboard Tasks on page 170. If the assigned template is unlocked, users can configure tasks on their dashboard. If you lock the dashboard template, users cannot configure task packs on their own dashboards.

Superusers can also restrict limited-access users to access only the Tasks Dashboard tab when they log in to Grid Manager. These users cannot manage other core network services through Grid Manager. They can only see the Tasks Dashboard tab and access only the tasks defined in the dashboard template, if applicable. This feature is useful when you want to define different levels of admin users and restrict them to specific tasks based on their organizational functions. For information about how to set this restriction, see Creating Limited-Access Admin Groups on page 114.

To configure and apply dashboard templates, complete the following:
1. Configure dashboard templates, as described in Adding Dashboard Templates on page 85.
2. Assign dashboard templates to admin groups, as described in About Admin Groups on page 113.

Adding Dashboard Templates

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

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

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

To reset a dashboard template:
1. Select the Dashboards -> Tasks tab.
2. For superusers: At the top right corner of the Tasks Dashboard panel, click the Configure icon -> Reset. Note that the Configure icon appears only if you are a superuser.
   For limited-access users: At the top right corner of the Tasks Dashboard panel, click Reset.
   The appliance reset your dashboard to the original dashboard template that was assigned to your admin group.

Modifying Dashboard Templates

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

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

Deleting Dashboard Templates

Only superusers can delete dashboard templates. To delete a dashboard template that is currently assigned to an admin group, you must first unassign the template from the admin group. For more information, see Creating Limited-Access Admin Groups on page 114.

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

Assigning Dashboard Templates

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

To assign a dashboard template to an admin group, see About Admin Groups on page 113.
The Status Dashboard

The Status Dashboard contains various widgets for viewing and managing data. Widgets are the building blocks of your Status 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 Status Dashboard depends on whether you are managing a Grid, an independent appliance, or an Infoblox Orchestration server:

- Grid Status
- Grid Upgrade Status
- Member Status (System Status)
- DNS Statistics
- Ranges Over Threshold
- IPv4 Failover Associations Status
- DHCP Statistics
- Network Statistics
- IPv4 Networks Over Threshold
- Discovery Status
- My Commands
- DDNS Statistics
- System Activity Monitor
- File Distribution Statistics
- Active WebUI Users
- Microsoft Servers Status Widget
- CSV Import Status

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. Use the scroll bar on the right to scroll through the 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, Captive Portal, and Reporting 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 868.
Grid Upgrade Status

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

The Grid Upgrade Status widget displays the following information:

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

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

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

Member Status (System Status)

The Member Status widget provides status information about the system resources and services of a Grid member, including the reporting server. 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. When you select the reporting server, the widget displays reporting related information, such as reporting usage and reporting warning count.
- **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. The widget also displays the upgrade status if the member is currently in the process of an upgrade. If the member is scheduled for an upgrade, the **Scheduled for upgrade** link appears. You can click this link to access the Grid tab -> Upgrade tab to view more details about the date and time of the scheduled upgrade.

The widget also displays the service status of the following: FTP, TFTP, HTTP (File Distribution), DNS, DHCP, NTP, bloxTools, Captive Portal, IF-MAP (for IF-MAP server only), and Reporting in the Services section. The service status can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><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 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><img src="image" alt="Gray" /></td>
<td>Gray</td>
<td>The service is not configured or is disabled.</td>
</tr>
</tbody>
</table>

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

When you select the reporting server, you can also see the following information:

- **Reporting Usage**: Displays the percentage of the reporting capacity that is currently in use.
- **Reporting Warning Count**: When the data usage on the reporting server approaches or reaches the daily maximum limit, the appliance sends an SNMP trap and email notification, if configured. When you receive five (5) violation notifications in a rolling period of 30 days, you cannot view reports or configure reporting related functions. You must then contact Infoblox Technical Support to resolve the issue.

For more information about reporting, see **Infoblox Reporting Solution** on page 967.

**DNS Statistics**

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

You can add a **DNS Statistics** widget to your Dashboard for each zone or member DNS server on the Grid.

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

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

  or

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

The widget displays only the option that you selected on your subsequent logins. For example, if you clicked **Select Member**, the widget displays the **Select Member** option only, and not the **Select Zone** option, when you log in again.
- **Graph Configuration**: Select which DNS messages you want to track in the **Responses per Second** graph.
  - **Success**: The number of successful queries.
  - **NXDOMAIN**: The number of queries for domain names that did not exist in the database.
  - **Referral**: The number of queries that became referrals.
  - **NXRRSET**: The number of queries for domain names that did not have the requested records.
  - **Failure**: The number of queries that failed due to reasons other than nonexistent domain names or records in a domain.
  - **Recursion**: The number of recursive queries for which the name server sent queries to other name servers.

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

**Ranges Over Threshold**

The **Ranges Over Threshold** widget enables you to monitor IPv4 DHCP range usage from your Dashboard. It lists the IPv4 ranges that are allocated above a specified threshold and thus may warrant your attention. The default threshold is 75%. For information, see **Configuring Thresholds for DHCP Ranges** on page 603. Note that the appliance highlights disabled IPv4 ranges in gray.

The widget displays the IPv4 ranges with utilization percentages that surpass the threshold.

To configure the **Ranges Over Threshold** widget, click the Configure icon and do the following:
- **Network View**: Select a network view in which you want to monitor the IPv4 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 IPv4 ranges that surpass the threshold to a file in CSV format.
- Click the Refresh button to refresh the data in the list.

**IPv4 Failover Associations Status**

The **IPv4 Failover Associations Status** widget enables you to monitor the status of the failover associations from your Dashboard. It lists all the failover associations in the Grid and displays their names and status. The widget also displays the primary and secondary servers in the association. When you click a failover association link or a status link, Grid Manager displays the Failover Association section where you can get detailed information about the failover association. For information, see **Monitoring Failover Associations** on page 671.

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:
Dashboard

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

Select which IPv6 messages you want to track in the *Messages per Second* graph.
  - **Declines:** The number of Decline messages that the Grid member received. A DHCP client sends a Decline message to a DHCP server when it discovers that the IP address offered by a DHCP server is already in use.
  - **Renews:** The number of Renew messages that the Grid member received. A DHCP client sends a Renew message to a DHCP server to extend the lifetimes on the leases granted by the DHCP server and to update other properties.
  - **Information Requests:** The number of Information-Request messages that the Grid member received. A client sends an Information-Request message to retrieve configuration parameters, such as the IP addresses of DNS servers in the network.
  - **Solicits:** The number of Solicit messages that the Grid member received, including Solicit messages embedded in Relay-Forward messages. A DHCP client sends a Solicit message to locate DHCP servers.
  - **Requests:** The number of Request messages that the Grid member received. A DHCP client sends a Request message to request one or more IP addresses and configuration parameters from a DHCP server.
  - **Rebinds:** The number of Rebind messages that the Grid member received. A DHCP client sends a Rebind message to extend the lifetime of its lease and to update configuration parameters.
  - **Releases:** The number of Release messages that the Grid member received. A DHCP client sends a Release message when it terminates its lease and releases its IP address.
  - **Advertisements:** The number of Advertise messages that the Grid member sent. When a DHCP server receives a Solicit message, it can respond with an Advertise message to indicate that the server is available for DHCP service.
  - **Replies:** The number of Reply messages that the Grid member sent. A DHCP server sends a Reply message that includes IP addresses and configuration parameters when it responds to Solicit, Request, Renew or Rebind message. It sends a Reply message with configuration parameters only when it responds to an Information-Request message.
The widget displays the following information:

- **DHCP Messages** tab: Displays a pie chart and the totals for each type of DHCP message. It also displays the number of Deferred Updates, which are DDNS update requests 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 an IPv4 network. You can monitor several networks simultaneously to view the distribution of address resources. Such information can indicate if there is a sufficient number of available addresses in each network. It can also provide information about the distribution of address resources, indicating if there are too many unused addresses in one network while all the addresses in another are in use.

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

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

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

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

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

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

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

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

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

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

- **Conflicts**: The number of IP addresses that have either a MAC address conflict or a DHCP range conflict. To obtain this data, you must run a discovery process on the network first. A discovered host has a MAC address conflict when its MAC address is different from that specified in its fixed address, DHCP lease, or host record. A discovered host has a DHCP range conflict when it is part of a DHCP range, but it does not have a matching fixed address or DHCP lease, and it is not part of an exclusion range.
IPv4 Networks Over Threshold

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

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

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 IPv4 DHCP Utilization. For information, see *Managing IPv4 DHCP Data* on page 639.

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 32, *Network Discovery*, on page 843.

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.
- **IPv4 Discovery**: Displays the total number of IPv4 networks and the IPv4 network and IP address range on which the IP discovery is currently running. You can click 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.
  - **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><img src="icon-green.png" alt="Green" /></td>
<td>Green</td>
<td>The DNS service is functioning properly.</td>
</tr>
<tr>
<td><img src="icon-red.png" alt="Red" /></td>
<td>Red</td>
<td>The DNS service is stopped.</td>
</tr>
<tr>
<td><img src="icon-yellow.png" alt="Yellow" /></td>
<td>Yellow</td>
<td>The DNS service is starting or stopping.</td>
</tr>
<tr>
<td><img src="icon-gray.png" alt="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><img src="icon-green.png" alt="Green" /></td>
<td>Green</td>
<td>The DHCP service is functioning properly.</td>
</tr>
<tr>
<td><img src="icon-red.png" alt="Red" /></td>
<td>Red</td>
<td>The DHCP service is stopped.</td>
</tr>
<tr>
<td><img src="icon-yellow.png" alt="Yellow" /></td>
<td>Yellow</td>
<td>The DHCP service is starting or stopping.</td>
</tr>
<tr>
<td><img src="icon-gray.png" alt="Gray" /></td>
<td>Gray</td>
<td>Management of the Microsoft DHCP server is disabled.</td>
</tr>
</tbody>
</table>
CSV Import Status

You can start a file import from the Import Manager editor and control and monitor it from the CSV Import Status widget.

- Click the Start button to start the import.
- Click the Stop button to stop the import.

After you start a file import, the CSV Import Status widget displays a status bar that indicates the import is in progress. It also tracks the number of rows of imported data and the number of rows of data with errors. You can click the Refresh icon or configure auto refresh to update the status.

The widget displays the following information about the import:

- **Current Status**: If an import is in progress, this field displays its current status. Otherwise, it displays the date and time of the last import.
- **Last Action**: Displays the last operation and the admin who initiated it.
- **CSV File**: The name of the imported file.
- **Rows Completed**: The number of rows of data the import has processed. Depending on the import options, Grid Manager displays the row number at which it stops the import when it encounters an error, or the total number of rows it has processed by skipping over the erroneous data. For example, if there are 100 rows of data and you select “On error: Stop importing,” and there is an error in row 90, the appliance displays 90 of 100 here. If you select “On error: Skip to the next row and continue,” the appliance displays 100 of 100 here and displays 1 in **Rows with Errors**.
- **Rows with Errors**: The number of rows of data the import has detected errors. Click Download Errors to download the CSV file that contains the header row and the rows of erroneous data. You can use this report as a reference for updating the data file before you import the file again.
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 100
  —  Global Smart Folders  on page 101
  —  My Smart Folders  on page 101
•   Creating Smart Folders  on page 102
•   Viewing and Modifying Data in Smart Folders  on page 103
•   Modifying Smart Folders  on page 104
•   Deleting Smart Folders  on page 104
•   Saving a Copy of a Smart Folder  on page 104
•   Printing and Exporting Data in Smart Folders  on page 105
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 103. 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. You can also decide whether you want to include objects that do not contain attribute values when you use the Group By criteria to group filtered data by extensible attributes. For information, see Creating Smart Folders on page 102. 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 101. 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 101.

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 262.

   **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 102.

### 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 104.

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 104. 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 The Finder panel, which appears on all pages in Grid Manager, provides tools for organizing your data. The Finder panel provides easy access to the following: on page 53.

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. You can also set Group By rules to group the filtered data by extensible attributes. Grid Manager displays a hierarchical view of the data using the Group By rules you define. By default, the appliance does not include objects that do not contain any attribute values. If you select to include objects that do not contain attribute values, the appliance may take longer to process the request. If you upgrade from a previous NIOS release, the appliance continues to include objects that do not contain attribute values in the Group By criteria. You must configure the smart folder not to include these objects by clearing the Include objects with no values for the Group By attributes check box.

To create a smart folder:

1. Click the Smart Folders tab.

2. Click the My Smart Folders tab to create a personal smart folder.

   or

   If you logged in with a superuser account, click the Global Smart Folders tab to create a global smart folder.

3. Click Create.

4. In the Smart Folder data panel, complete the following:

   — Name: Enter the name of the smart folder.

   — Comment: Optionally, enter additional information about the smart folder.

   — Include objects with no values for the Group By attributes: Select this to include objects that do not contain values in the selected attributes when you group your smart folder results using the Group By rules. The appliance may take longer to include these objects in the results table when you select this option. To achieve better performance, clear this check box.

   — In the first drop-down list, select a field as the filter. You can select a network view 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.

   Note: When you select “IF-MAP publishing equals Yes” as the filter, only networks and ranges that have IF-MAP publishing explicitly enabled appear in the results table. When you select “IF-MAP publishing equals No,” only networks and ranges that have IF-MAP publishing explicitly disabled appear in the results table.

   — Optionally, click + to add another filter. You can also click Apply to view the filtered data in the results table.

   — Optionally, select the Group Results check box to organize the filtered data. You can also disable a Group By filter by deselecting the check box.

   — From the Group by drop-down list, select an extensible attribute by which you want to group the filtered data. For example, if you want to group the filtered data by building number, you can select Building from the drop-down list. To add additional Group By rules, click the + icon, and then select a field from the drop-down list. You can apply up to 10 Group By rules. You can also delete a rule by selecting the rule and clicking the - icon.
— After you add all filter criteria and Group By rules, click **Apply**. Grid Manager displays the filtered data in the results table. Note that in the **Name** field, the appliance highlights disabled DHCP objects in gray. A DHCP object can be a DHCP range, fixed address, reservation, host configured for DHCP, or roaming host with an allocated IP address. If you select to include objects with no attribute values in the Group By rules, the appliance may take longer to process the results.

5. Click **Save** to save the smart folder.

### Viewing and Modifying Data in Smart Folders

After you set up a smart folder, the appliance searches for matching objects based on the filter criteria you specified for the folder. Grid Manager also groups the objects by the Group By rules you specify. If you select to include objects with no attribute values, the appliance may take longer to process the results. Each smart folder you create can contain up to 2,000 objects. When the number of objects exceeds 2,000, Grid Manager sorts and displays the first 2,000 objects and a message at the top of the panel. In this case, you may want to redefine your filter criteria to further refine the filtered data in your smart folders.

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

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

In the smart folder list panel, however, Grid Manager displays all the smart folders in a flat list. You can modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see *Modifying Data in Tables* on page 52.

In the smart folder data panel, Grid Manager displays the first hierarchical level of the smart folder based on your Group By rules. If you do not configure any Group By rule, Grid Manager displays all the objects in the results table. If you select to include objects with no attribute values, Grid Manager also includes these objects in the hierarchical view. Depending on your Group By rules, you can view detailed information about the objects by clicking the object link and drilling down to the lowest hierarchical level, and then opening an object. To go back to a previous hierarchical view, click the link of the corresponding level in the breadcrumb.

To view detailed information about an object:

1. In the Smart Folder data panel, click the object link until you drill down to the last hierarchical level of the folder.

2. Grid Manager displays the following information:
   - **Name**: The name or IP address of the object. 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 35.
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 102.

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 62 and *Exporting Data to 
Files* on page 65.
Part 2 Appliance Administration

This section provides information about configuring admin groups, roles, and accounts, and defining the appropriate permissions. It explains how to configure and manage a Grid or an independent appliance, and set operational parameters. It also describes the file distribution services (TFTP, FTP, and HTTP) and the bloxTools environment. It includes the following chapters:

- Chapter 4, Managing Administrators, on page 109
- Chapter 5, Deploying a Grid, on page 171
- Chapter 6, Deploying Independent Appliances, on page 211
- Chapter 7, Managing Appliance Operations, on page 241
- Chapter 8, File Distribution Services, on page 307
- Chapter 9, Managing NIOS Software and Configuration Files, on page 315
- Chapter 10, bloxTools Environment, on page 339
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 111
- **About Admin Groups** on page 113
  - Creating Superuser Admin Groups on page 114
  - Creating Limited-Access Admin Groups on page 114
- **About Admin Roles** on page 116
  - Creating Admin Roles on page 116
- **Managing Admin Groups and Admin Roles** on page 117
  - Modifying Admin Groups and Roles on page 117
  - Deleting Admin Groups and Roles on page 118
  - Viewing Admin Groups on page 118
  - Viewing Admin Roles on page 118
  - Viewing Admin Group Assignments on page 119
- **About Administrative Permissions** on page 120
  - Defining Global Permissions on page 121
  - Defining Object Permissions on page 121
  - Defining DNS and DHCP Permissions on Grid Members on page 124
  - Applying Permissions and Managing Overlaps on page 126
  - Managing Permissions on page 128
- **Authenticating Administrators** on page 130
- **Creating Local Admins** on page 130
  - Managing Passwords on page 131
  - Modifying and Deleting Admin Accounts on page 131
- **About Remote Admins** on page 133
- **Authenticating Admins Using RADIUS** on page 135
  - Authentication Protocols on page 135
  - Accounting Activities Using RADIUS on page 136
  - Configuring Remote RADIUS Servers on page 136
  - Configuring RADIUS Authentication on page 136
  - Configuring a RADIUS Authentication Server Group on page 137
• Authenticating Admins Using Active Directory on page 139
  — Configuring an Active Directory Authentication Service Group on page 140
• Authenticating Admin Accounts Using TACACS+ on page 141
  — TACACS+ Accounting on page 142
  — Configuring TACACS+ on page 142
  — Configuring a TACACS+ Authentication Server Group on page 142
• Defining the Authentication Policy on page 144
  — Configuring a List of Authentication Server Groups on page 144
  — Configuring a List of Remote Admin Groups on page 144
• Changing Password Length Requirements on page 145
• Notifying Administrators on page 146
• Administrative Permissions for Common Tasks on page 147
• Administrative Permission for the Grid on page 149
  — Administrative Permissions for Grid Members on page 149
  — Administrative Permissions for Network Discovery on page 150
  — Administrative Permissions for Scheduling Tasks on page 150
  — Administrative Permissions for Microsoft Servers on page 151
• Administrative Permissions for IPAM Resources on page 153
  — Administrative Permissions for IPv4 and IPv6 Networks on page 153
  — Administrative Permissions for Hosts on page 153
• Administrative Permissions for DNS Resources on page 154
  — Administrative Permissions for DNS Views on page 155
  — Administrative Permissions for Zones on page 156
  — Administrative Permissions for Resource Records on page 157
  — Administrative Permissions for Shared Record Groups on page 158
  — Administrative Permissions for DNS64 Synthesis Groups on page 159
• Administrative Permissions for DHCP Resources on page 160
  — Administrative Permissions for Network Views on page 161
  — Administrative Permissions for IPv4 nd IPv6 Networks and Shared Networks on page 162
  — Administrative Permissions for IPv4 or IPv6 Fixed Addresses and IPv4 Reservations on page 164
  — Administrative Permissions for IPv4 and IPv6 DHCP Ranges on page 165
  — Administrative Permissions for IPv4 or IPv6 DHCP Templates on page 166
  — Administrative Permissions for MAC Address Filters on page 167
  — Administrative Permissions for the IPv4 and IPv6 DHCP Lease Histories on page 168
• Administrative Permissions for File Distribution Services on page 168
• Administrative Permissions for Dashboard Tasks on page 170
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 113.

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

The NIOS appliance can authenticate users that are stored on its local database as well as users stored remotely on an Active Directory domain controller, a RADIUS server, or a TACACS+ 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/AD Domain Controller/TACAS+ Server</th>
</tr>
</thead>
</table>
| **To store admin accounts locally** | • Use the default admin group (“admin-group”) or define a new group  
• Set the privileges and properties for the group  
• Add admin accounts to the group | • Configure communication settings with the NIOS appliance  
If you use admin groups:  
• Import Infoblox VSAs (vendor-specific attributes) (if RADIUS)  
• Define an admin group with the same name as that on the NIOS appliance  
• Define admin accounts and link them to an admin group  
If you do not use admin groups:  
• Define admin accounts |
| **To store admin accounts remotely** | • Configure communication settings with a RADIUS server, an Active Directory domain controller, or TACACS+ server  
If you use admin groups on the RADIUS server, Active Directory domain controller, or TACACS+ server:  
• Configure admin groups that match the remote admin groups  
• Set the privileges and properties for the groups  
If you do not use admin groups on the RADIUS server, Active Directory domain controller, or TACACS+ server:  
• Assign an admin group as the default | |

The admin policy defines how the appliance authenticates the admin: with the local database, RADIUS, Active Directory, or TACACS+. You must add RADIUS, Active Directory, or TACACS+ as one of the authentication methods in the admin policy to enable that authentication method for admins. See Defining the Authentication Policy on page 144 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 113.
2. Define the administrative permissions of the admin group. See About Administrative Permissions on page 120.
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 130.
   - To configure the appliance to authenticate the admin account stored remotely, see About Remote Admins on page 133.
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. You can assign a dashboard template to an admin group. A dashboard template specifies the tasks an admin group can access through the Tasks Dashboard tab when they log in to Grid Manager. For information about dashboard templates, see About Dashboard Templates on page 85. You can also restrict certain user groups to manage specific tasks in the Tasks Dashboard tab only. These users cannot manage other core network services through Grid Manager. For information about how to apply this restriction, see Creating Limited-Access Admin Groups on page 114.

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 114.
2. Assign permissions to the admin group, as described in About Administrative Permissions on page 120.

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

1. Create an admin role, as described in About Admin Roles on page 116.
2. Define permissions for the newly created admin role, as described in Creating Admin Roles on page 116.
3. Create an admin group and assign the role to the group, as described in Creating Limited-Access Admin Groups on page 114.

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 130.
- For remote admins, see About Remote Admins on page 133.
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, AD domain controllers, or TACACS+ servers.

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. Click Next and complete the following to define the dashboard template:
   - Dashboard Template: From the drop-down list, select the dashboard template you want to assign to this superuser group. When you apply a dashboard template to an admin group, the template applies to all users in the group. The default is None, which means that users in this group can access all licensed tasks in the Tasks Dashboard tab if they have the correct permissions to the task-related objects. Note that if you want to delete a template, you must first unassign the template from an admin group, or select None, before you can delete it. For more information about dashboard templates, see About Dashboard Templates on page 85.
5. Optionally, click Next to add extensible attributes to the admin group. For information, see About Extensible Attributes on page 262.
6. Save the configuration and click Restart if it displays at the top of the screen.

You can do one of the following after you create a superuser admin group:
- Add local admins to the superuser group. For information, see Creating Local Admins on page 130.
- Assign the superuser group to remote admins. For information, see About RemoteAdmins on page 133.

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.
About Admin Groups

— **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. Click **Next** and complete the following to define the dashboard template:

— **Dashboard Template**: From the drop-down list, select the dashboard template you want to assign to this superuser group. When you assign a dashboard template to an admin group, the template applies to all users in the group. The default is **None**, which means that users in this group can perform all licensed tasks in the **Tasks Dashboard** tab if they have the correct permissions to the task-related objects. Note that if you want to delete a template, you must first unassign the template from an admin group, or select **None**, before you can delete it. For more information about dashboard templates, see *About Dashboard Templates* on page 85.

— **Display Taskflow Dashboards Only**: Select this check box if you want to restrict this admin group to access only the Tasks Dashboard in Grid Manager. Note that when you select this check box, users in this admin group have access to the tasks you specified in the selected dashboard template, if applicable. They cannot perform any other tasks or manage any core network services in Grid Manager the next time they log in to the system.

5. Optionally, click **Next** to add or delete extensible attributes for this admin group. For information, see *About Extensible Attributes* on page 262.

6. Save the configuration and click **Restart** if it displays at the top of the screen.
About Admin Roles

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

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

You can assign these system-defined roles to admin groups and create additional roles based on the job functions in your organization. If you are creating a role that has similar permissions to an existing role, you can copy the role and then make the necessary modifications to the new role. Thus you do not have to create each new role from scratch.

You can assign up to 21 roles to an admin group, and you can assign a role to more than one admin group. When you make a change to a role, the appliance automatically applies the change to that role in all admin groups to which the role is assigned.

Creating Admin Roles

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

To create a new role from scratch:

1. From the Administration tab, select the Administrators tab -> Roles tab, and then click the Add icon.
2. In the Add Role wizard, complete the following:
   - **Name**: Enter a name for the role.
   - **Comment**: Enter useful information about the role. For example, if you are creating a role for IT personnel, you can put the information here.
   - **Disable**: Select this to retain an inactivated profile for this admin role in the configuration.
3. Optionally, click Next to add extensible attributes to this role. For information, see About Extensible Attributes on page 262.
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 120.
   - **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 Admin Groups and Admin Roles

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 120.

• Assign roles to admin groups, as described in Creating Limited-Access Admin Groups on page 114.

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 114.
   — 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. Save the configuration and click Restart if it displays at the top of the screen.

Managing Admin Groups and Admin Roles

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

To copy an existing role:

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

2. The Copy Role editor provides the following tabs from which you can modify data for the new role:
   — General: Enter the name and information about the new role. You can also disable the role in this tab.
   — Admin Groups: Displays a list of admin groups that are currently using this role. You cannot modify the list.
   — Extensible Attributes: Add and delete extensible attributes that are associated with the admin role. You can also modify the values of the extensible attributes. For information, see About Extensible Attributes on page 262.

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

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 120.

• Assign roles to admin groups, as described in Creating Limited-Access Admin Groups on page 114.
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 do the following:
• Sort the data in ascending or descending order by column.
• Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
• Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 57.
• Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables on page 52.
• Print or export the data.

Viewing Admin Roles

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

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

You can select the additional fields, Disabled and Site, for display. You can also do the following:
• Sort the data in ascending or descending order by column.
• Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
• Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 57.
Managing Admin Groups and Admin Roles

- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables on page 52.
- Print or export the data.

Viewing Admin Group Assignments

After you define permissions for an admin role, you can assign it to multiple admin groups. You can view the list of admin groups to which an admin role is assigned, as follows:

1. From the Administration tab, select the Administrators tab -> Roles tab -> admin_group check box, and then click the Edit icon.
2. In the Role editor, select the Admin Groups tab.
   Grid Manager displays the list of admin groups to which the role is assigned.
About Administrative Permissions

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

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

By default, the superuser group (admin-group) has full access to all resources on the appliance. Superusers can create limited-access admin groups and grant them permissions to resources at the global and object levels. Limited-access admin groups must have either read-only or read/write permissions assigned in order to view information or perform tasks on any supported objects.

When you assign permissions at the global level, the permissions apply to all objects that belong to the specified resource. For example, when you define a read/write permission to all DHCP networks, the permission applies to all DHCP ranges and fixed addresses in the networks. For information about global permissions, see "Defining Global Permissions" on page 121.

You can also define permissions at a more granular level, such as for a specific grid member, DNS zone, network, and even an individual database object, such as a resource record or fixed address. When you define a permission at the object level, admins with this permission can only manage the specified object and its associated objects. For information about object permissions, see "Defining Object Permissions" on page 121.

You can use global and object permissions to restrict admins to specific DNS and DHCP resources on specific grid members by assigning the appropriate permissions. You can use this feature to separate DNS and DHCP administration on selected grid members. For more information, see "Defining DNS and DHCP Permissions on Grid Members" on page 124.

You can configure global permissions, object permissions, and member DNS and DHCP permissions for default and custom admin groups and roles. You cannot however define permissions for the factory default roles, such as DHCP Admin.

The appliance supports the following resource groups:

- **Grid resources:** Includes grid DNS properties, grid DHCP properties, all grid members, Microsoft servers that are managed by the grid, network discovery, task scheduling, and all dashboard tasks.
- **IPAM resources:** Includes network views, IPv4 and IPv6 networks, and host records.
- **DHCP resources:** Includes grid DHCP properties, 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 grid DNS properties, 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.

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 147.
- **Permissions for the Grid and Grid members,** as described in "Administrative Permission for the Grid" on page 149.
• Permissions for IPAM resources, such as IPv6 networks, as described in Administrative Permissions for IPAM Resources on page 153.

• Permissions for DNS resources, such as DNS views and A records, as described in Administrative Permissions for DNS Resources on page 154.

• Permissions for DHCP resources, such as network views and fixed addresses, as described in Administrative Permissions for DHCP Resources on page 160.

• Permissions for file distribution services, as described in Administrative Permissions for File Distribution Services on page 168.

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 126.

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

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.
You select five forward-mapping authoritative DNS zones that have resource records such as A records, Hosts, and CNAME records. 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.

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

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

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

2. Grid Manager displays the Create Object Permissions wizard. For an admin group, the appliance displays the selected group in the Group 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. Save the configuration and click Restart if it displays at the top of the screen.

Grid Manager displays a warning message when the permissions you define here overlap with other permissions in the system. Click See Conflicts to view the overlapping permissions in the Permissions Conflict dialog box. For information, see Applying Permissions and Managing Overlaps on page 126.
You can also set permissions for specific objects from the objects themselves. For example, to define permissions for a particular Grid member, navigate to that Grid member and define its permissions.

To define the permissions of a specific object:

1. Navigate to the object. For example, to define permissions for a particular network, from the Data Management tab, select the IPAM tab -> network check box, and then click the Edit icon.
2. In the editor, select the Permissions tab, and then do one of the following:
   - Click the Add icon to add permission to the object. In the Admin Group/Role Selector dialog box, select an admin group or role to which you want to assign the permission, and then click the Select icon.
   - Modify the permission and resource type of a selected admin group or role.
   - Select an admin group or role and click the Delete icon to delete it.
3. Save the configuration and click Restart if it displays at the top of the screen.

**Defining DNS and DHCP Permissions on Grid Members**

You can restrict certain admin groups or roles to perform specific DNS and DHCP tasks on specific grid members by assigning the correct global and object permissions. You can use this feature to separate the DNS and DHCP administration on different grid members. For example, you can create an admin group or role that can only create, modify, and delete DHCP ranges in a specific network on a specific member in the grid. This admin group or role is restricted to the specified tasks on the selected grid member. It cannot perform other DNS or DHCP tasks on this member, and it cannot perform the specified tasks on other grid members.

For example, you can define permissions that allow admins to create, modify, and delete DHCP ranges in network 10.0.0.0/8 on grid member “sales.infoblox.com” by granting read/write object permissions to all DHCP ranges, network 10.0.0.0/8, and member DHCP on sales.infoblox.com. Admins with these permissions can only add, modify, and delete DHCP ranges in network 10.0.0.0/8 on grid member sales.infoblox.com. They cannot perform other DHCP or DNS tasks on the member, and they cannot perform these tasks on other grid members.

For information about required permissions for specific DNS and DHCP tasks, see Administrative Permissions for Common Tasks on page 147.

You can define the following DNS and DHCP permissions for an admin group or role:

- **Grid DNS or Grid DHCP**: Admins with read/write permissions can manage any DNS or DHCP resources on any grid members. They can also modify grid DNS or grid DHCP properties and any member DNS and member DHCP properties. Admins with read-only permissions can only view DNS or DHCP resources. They cannot modify any DNS or DHCP resources or restart related services.
- **Member DNS or Member DHCP**: Admins with read/write permissions can perform the defined DNS or DHCP tasks only on the specified grid member, not any other members. They can also modify DNS or DHCP properties on the specified member. Admins with read-only permission cannot assign the grid member to any DNS or DHCP resources.
- **Restart DNS or Restart DHCP on member**: Admins with read/write permissions can restart the DNS or DHCP service on the specified grid member, not any other members. However, they cannot modify DNS or DHCP properties on the member. They can assign the specified grid member to any DNS or DHCP resources, but they cannot assign any other grid members to DNS or DHCP resources.

To specify member DNS and DHCP permissions, define DNS or DHCP permissions at the global or object level for an admin group or admin role, as described in Defining Global Permissions on page 121 and Defining Object Permissions on page 121. Ensure that you include the grid member object to which you want to restrict DNS or DHCP administration.

You can also control whether the admins can modify DNS or DHCP properties on a member, as described in Modifying Permissions on a Grid Member on page 125.
**Modifying Permissions on a Grid Member**

Admins can perform different tasks on a grid member based on the permissions they have. *Table 4.2* outlines the permissions and the tasks admins can perform on a grid member:

*Table 4.2 Member Permissions and Tasks*

<table>
<thead>
<tr>
<th>Grid Member</th>
<th>Member DNS or DHCP Properties</th>
<th>Restart DNS or DHCP on Grid Member</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Read/ Write</strong></td>
<td>- Modify member properties</td>
<td>- Modify member DNS or DHCP properties</td>
</tr>
<tr>
<td></td>
<td>- Restart, reboot, and shutdown member</td>
<td>- Restart member DNS or DHCP service</td>
</tr>
<tr>
<td></td>
<td>- Modify member DNS and DHCP properties</td>
<td>- Assign and un-assign member to DNS or DHCP objects</td>
</tr>
<tr>
<td></td>
<td>- Restart member DNS and DHCP services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Assign and un-assign member to DNS and DHCP objects</td>
<td></td>
</tr>
<tr>
<td><strong>Read-only</strong></td>
<td>- View member DNS and DHCP properties</td>
<td>- View member DNS or DHCP properties</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- N/A (You cannot define a read-only permission)</td>
</tr>
<tr>
<td><strong>Deny</strong></td>
<td>- Cannot modify member, DNS, and DHCP properties</td>
<td>- Cannot modify member, DNS, and DHCP properties</td>
</tr>
<tr>
<td></td>
<td>- Cannot restart related services</td>
<td>- Cannot restart related services</td>
</tr>
<tr>
<td></td>
<td>- Cannot assign member to DNS and DHCP objects</td>
<td>- Cannot assign member to DNS and DHCP objects</td>
</tr>
</tbody>
</table>

After you add permissions to an admin group or role for a specific grid member, you can modify the member permissions and resources. Note that when you modify the member permissions and resources, the appliance updates the permissions of the admin group or role accordingly.

To modify grid member permissions:

1. From the **Data Management** tab, select the **DHCP** or **DNS** tab -> **Members** tab -> **grid_member**, and then click the **Edit** icon.
2. In the **Member DHCP Properties** or **Member DNS Properties** editor, select the **Permissions** tab.
3. Click a permission in the Permissions table, select a different permission from the **Permissions** drop-down list or select a different resource from the **Resources** drop-down list. Note that when you select **Restart DNS** or **Restart DHCP**, the admins with this permission can only restart the DNS or DHCP service on the selected member. They cannot modify DNS or DHCP properties of this member.
4. Save the configuration. Note that the appliance automatically updates the permissions of the corresponding admin group or role in the **Administration** tab.
Applying Permissions and Managing Overlaps

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

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

For example, an admin from the DNS1 admin group tries to access the a1.test.com A record in the test.com zone in the Infoblox default view. The appliance first checks if the DNS1 admin group has a permission defined for the a1.test.com A record. If there is none, then the appliance checks the roles assigned to DNS1. If there is no permission defined for the a1.test.com A record, the appliance continues checking for permissions in the order listed in Table 4.3. The appliance uses the first permission it finds.

Table 4.3 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 4.4, 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 4.4 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>Effective permissions</td>
<td>Deny to the test.com zone Read/Write to all A records in test.com zone Deny to all other resource records in test.com zone</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 4.5, 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 4.5 Multiple Roles

| Role 1 permission                          | Read-only to all A records in the test.com zone |
| Role 2 permission                          | Read/Write to all A records in test.com zone    |
|                                            | Read/Write to all MX records in test.com zone  |
| Effective permissions                      | Deny to the test.com zone                       |
|                                            | Read-only to all A records in the test.com zone |
|                                            | Read/Write to all MX records in test.com zone  |

You can check for overlapped permissions when you add permissions to roles and to admin groups, and when you assign roles to an admin group. When you create a permission that overlaps with existing permissions, Grid Manager displays a warning message and the See Conflicts link on which you click to view the overlapped permissions. For information, see Viewing Overlapping Permissions on page 127. 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 114.

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 128.
- Modify the permissions, as described in Modifying Permissions on page 129.
- Delete the permission, as described in Deleting Permissions on page 129.

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 Mange Global Permissions or Create Object permissions editor, select the new permission: Read/Write, Read-Only or Deny for the resource.
5. Save the configuration and click Restart if it displays at the top of the screen.

Deleting Permissions

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

To delete a permission:

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

**Authenticating Administrators**

The NIOS appliance supports the following authentication methods: local database, RADIUS, Active Directory, and TACACS+. The appliance can use any combination of these authentication methods. It authenticates admins against its local database by default. Therefore, if you want to use local authentication only, you must configure the admin groups and add the local admin accounts, as described in *Creating Local Admins* on page 130.

If you want to authenticate admins using RADIUS, Active Directory, or TACACS+ 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 133.

**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 *About Extensible Attributes* on page 262.
5. Save the configuration and click **Restart** if it displays at the top of the screen.
Managing Passwords

Superusers can define requirements for the passwords of local admins according to your organization's policies. In addition to specifying the minimum password length, you can define rules that specify the character types that are allowed in the password. You can also specify whether passwords expire, their duration, and when reminders are sent to the users. Additionally, you can require admins to change their passwords when they first log in or after their passwords are reset.

You set the requirements at the Grid level, so they apply to all local admins who log in to the Grid. The requirements that you define appear in the User Profile of all local admins and when users are required to change their password.

To define the password requirements for local admins:

1. From the Grid tab, select the Grid Manager tab.
2. Expand the Toolbar and select Grid Properties.
3. In the Grid Properties editor, select the Password tab and complete the following:
   - **Minimum Password Length**: Specify the minimum number of characters that are required in a password.
   - **Password Complexity**: Specify the following password requirements:
     - the minimum number of lowercase characters
     - the minimum number of uppercase characters
     - the minimum number of numeric characters
     - the minimum number of symbol characters. The allowed characters are: ! @ # $ % ^ & * ( )
     You must also specify how many characters an admin must change when revising a password.
   - **Password must expire**: Select this check box to enable passwords to expire after a specified period. Specify the duration of each password and the number of days before the expiration that the appliance sends a reminder.
   - **Force password change at next login**: Select this check box to force all new users to change their passwords when they first log in and to force existing users whose passwords were just reset to change their passwords.
4. Click Save & Close.

Modifying and Deleting Admin Accounts

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

To modify an admin account:

1. From the Administration tab, select the Administrators tab -> Admins tab -> admin_account check box, and then click the Edit icon.
   
or
   
   From the Administration tab, select the Administrators tab -> Groups tab -> admin_group -> admin_account check box, and then click the Edit icon.
2. The Administrator editor provides the following tabs from which you can modify data:
   - **General**: In the General Basic tab, modify data of the admin account as described in Creating Local Admins on page 130.
     
     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.
Managing Administrators

- **Extensible Attributes**: Add and delete extensible attributes that are associated with the admin account. You can also modify the values of the extensible attributes. For information, see *About Extensible Attributes* on page 262.

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

To delete an admin account:

1. From the *Administration* tab, select the *Administrators* tab -> *Admins* tab -> *admin_account* check box, and then click the Delete icon.

   or

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

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

NIOS can authenticate admins whose user credentials are stored remotely on RADIUS servers, AD domain controllers, or TACACS+ servers. You can configure authentication server groups for each type of server to which NIOS sends authentication requests. For example, you can create a server group for RADIUS servers and another server group for AD domain controllers. Then in the admin authentication policy, you can list which authentication server groups to use and in what order.

In addition, if admin groups are configured on the remote authentication server, you can configure admin groups with the same names on the NIOS appliance and list them in the authentication policy as well. Then if the remote authentication server provides the admin group name while authenticating an admin, NIOS can automatically assign the admin to the matching admin group specified in the authentication policy. You can also create a default admin group for all admins that are authenticated through a remote authentication service.

Figure 4.4 illustrates the authentication and authorization process for remote admins. In the example, two authentication server groups are configured—a RADIUS server group and an AD server group. When an admin logs in with a user name and password, the appliance uses the first service listed in the admin policy to authenticate the admin. If authentication fails, the appliance tries the next service listed, and so on. It tries each service on the list until it is successful or all services fail. If all services fail, then the appliance denies access and generates an error message in syslog.

If authentication succeeds, the NIOS appliance tries to match the admin group names in the admin policy to any groups received from the remote server. If it finds a match, the NIOS appliance applies the privileges of that group to the admin and allows access. If the appliance does not find a match, then it applies the privileges of the default group. If no default group is defined, then the appliance denies access.

Figure 4.4 Authenticating Remote Admins

1. An admin enters his user name and password to log in to the appliance.
2. The appliance first checks the local admin policy, and then the admin policy for the authentication service, which can be a RADIUS, AD, or TACACS+ service. 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 service on the list, which is an Active Directory (AD) service. 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 group.
Only superusers can perform the following tasks to configure NIOS to authenticate admins using remote authentication servers:

- Configure the authentication server groups. You can create multiple RADIUS and AD server groups, but only one TACACS+ server group.
  - For information about RADIUS authentication, see *Authenticating Admins Using RADIUS*.
  - For information about AD authentication, see *Authenticating Admins Using Active Directory* on page 139.
  - For information about TACACS+ authentication, see *Authenticating Admin Accounts Using TACACS+* on page 141.
- Configure admin groups with names that match those on the remote server. For information about admin groups, see *About Admin Groups* on page 113.
- Configure the admin policy, as described in *Defining the Authentication Policy* on page 144.

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

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

When NIOS authenticates administrators against RADIUS servers, NIOS acts similarly to a network access server (NAS), which is a RADIUS client that sends authentication and accounting requests to a RADIUS server. Figure 4.5 illustrates the RADIUS authentication process.

**Figure 4.5 Authentication using a RADIUS server**

Authentication Protocols

When you configure the NIOS appliance to authenticate admins against a RADIUS server group, you must specify the authentication protocol of each RADIUS server, which can be either PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol).

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

With CHAP, when the client tries to log in, it sends its user name and password to the NIOS appliance. The appliance then creates an MD5 hash of the password together with a random number that the appliance generates. It then sends the random number, user name, and hash to the RADIUS server in an Access-Request packet. 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.
Accounting Activities Using RADIUS

You can enable the accounting feature on the RADIUS server to track whether an administrator has initiated a session. After an administrator successfully logs in, the appliance sends an Accounting-Start packet to the RADIUS server.

Configuring Remote RADIUS Servers

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

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

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

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

Configuring Admin Groups on the Remote RADIUS Server

Infoblox supports admin accounts on one or more RADIUS servers.

On the remote RADIUS server, do the following to set up admins and associate them with an admin group:

- Import Infoblox VSAs (vendor-specific attributes) to the dictionary file on the RADIUS server
- For third-party RADIUS servers, import the Infoblox vendor file (the Infoblox vendor ID is 7779)
- Define the admin group
- Associate one or more remote admin accounts with the admin group
- Add and activate a policy for the admin accounts, but do not associate the policy with a policy group that contains an infoblox-group-info attribute.

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

Configuring RADIUS Authentication

To configure NIOS to use one or more RADIUS server groups to authenticate administrators, you must do the following:

- Configure at least one RADIUS authentication server group. For more information, see Configuring a RADIUS Authentication Server Group on page 137.
- Define admin groups for the admins that are authenticated by the RADIUS servers and specify their privileges and settings. The group names in NIOS must match the admin group names on the RADIUS server. See About Admin Groups on page 113 for information about defining admin groups.
- In the authentication policy, add the RADIUS server groups and the admin groups that match those on the RADIUS server. You can also designate an admin group as the default group for remote admins. NIOS assigns admins to this group when it does not find a matching group for a remote admin. See Defining the Authentication Policy on page 144 for more information about configuring the policy.
Configuring a RADIUS Authentication Server Group

You can add multiple RADIUS servers to the group for redundancy. When you do, the appliance tries to connect to the first RADIUS server on the list and if the server does not respond within the maximum retransmission limit, then it tries the next RADIUS server on the list. NIOS tries to connect to each RADIUS server in the order the servers are listed. If it does not receive a response within the configured timeout period and has tried to connect the specified retry value, then it tries the next RADIUS server on the list. It logs an error to syslog when it fails to connect to any of the servers in the group.

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

To configure a RADIUS authentication server group:

1. From the Administration tab, click the Authentication Server Groups tab.
2. Click the Add icon in the RADIUS Services subtab.
3. In the Add RADIUS Authentication Service wizard, complete the following:
   - **Name**: Enter the name of the server group.
   - **RADIUS Servers**: Click the Add icon and enter the following:
     - **Server Name or IP Address**: Enter the FQDN or the IP address of the RADIUS server that is used for authentication.
     - **Comment**: Enter additional information about the RADIUS server.
     - **Authentication Port**: The destination port on the RADIUS server. The default is 1812. This field is required only if you do not enable accounting on the RADIUS server. This field is not required if you enable accounting to configure an accounting-only RADIUS server.
     - **Authentication Type**: Select either PAP or CHAP from the drop-down list. The default is PAP.
     - **Shared Secret**: Enter the shared secret that the NIOS appliance and the RADIUS server use to encrypt and decrypt their messages. This shared secret is a value that is known only to the NIOS appliance and the RADIUS server.
     - **Enable Accounting**: Select this to enable RADIUS accounting for the server so you can track an administrator's activities during a session. When you enable accounting, you must enter a valid port number in the Accounting Port field.
     - **Accounting Port**: The destination port on the RADIUS server. The default is 1813.
     - **Connect through Management Interface**: Select this so that the NIOS appliance uses the MGMT port for administrator authentication communications with just this RADIUS server.
     - **Disable server**: Select this to disable the RADIUS server if, for example, the connection to the server is down and you want to stop the NIOS appliance from trying to connect to this server.
     - **Click Test** to test the configuration. If the NIOS appliance connects to the RADIUS server using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the RADIUS server, the appliance displays a message indicating an error in the configuration.
   - **Click Add** to add the server to the list.

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

You can also delete a RADIUS server by selecting it and clicking the Delete icon.
   - **Authentication**: Optionally, modify the authentication settings. These settings apply to all RADIUS servers that you configure on the NIOS appliance.
   - **Timeout(s)**: Specify the number of seconds that the appliance waits for a response from the RADIUS server.
**Retries:** Specify how many times the appliance attempts to contact an authentication RADIUS server. The default is 5.

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

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

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

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

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

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

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

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

Note that the following fields in the wizard do not apply to this feature: Enable NAC Filter, Cache Time to Live, and Recovery Interval. They are used with the NAC Integration feature described in Chapter 25, Authenticated DHCP, on page 701.
Authenticating Admins Using Active Directory

Active Directory™ (AD) is a distributed directory service that is a repository for user information. The NIOS appliance can authenticate admin accounts by verifying user names and passwords against Active Directory. In addition, the NIOS appliance queries the AD domain controller for the group membership information of the admin. The appliance matches the group names from the domain controller with the admin groups on its local database. It then authorizes services and grants the admin privileges, based upon the matching admin group on the appliance.

Figure 4.6 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 authentication policy to determine which authentication service to use. The authentication policy specifies an AD authentication service.

3. The appliance sends an authentication request to the first domain controller in the AD server group. The appliance also requests the group membership information of the admin.

4a. Authentication is successful. The domain controller successfully authenticates the admin user. The group membership information for the administrator is sent to the appliance. The first group in the list that matches the groups returned by the domain controller is assigned to the admin, along with the associated permissions after that admin logs in.

4b. Authentication is unsuccessful. The domain controller sends back a deny access result to the appliance. No group membership information is sent.

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

- Configure one or more AD authentication server group on the appliance and add AD domain controllers to the group. For information about configuring an AD authentication service group for admins, see Configuring an Active Directory Authentication Service Group.
Managing Administrators

- If you configured admin groups on the AD controller, you must create those same groups on the NIOS appliance and specify their privileges and settings. Note that the admin group names must match those on the AD domain controller. You can specify a default group as well. The NIOS appliance assigns admins to the default group if none of the admin groups on the NIOS appliance match the admin groups on the AD domain controller or if there are no other admin groups configured. For information about configuring group permissions and privileges, see About Admin Groups on page 113.
- Add the newly configured Active Directory service to the list of authentication services in the admin policy, and add the admin group names as well. See Defining the Authentication Policy on page 144 for more information about configuring an admin policy.

Configuring an Active Directory Authentication Service Group

You can add multiple domain controllers to an AD authentication server group for redundancy. The NIOS appliance tries to connect with the first domain controller on the list. If it is unable to connect, it tries the next domain controller on the list, and so on.

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

1. From the Administration tab, click the Authentication Server Groups tab.
2. Click the Active Directory Services subtab and click the Add icon.
3. In the Add Active Directory Authentication Service wizard, complete the following:
   - Name: Enter a name for the service.
   - Active Directory Domain: Enter the AD domain name.
   - Domain Controllers: Click the Add icon and complete the following to add an AD domain controller:
     - Server Name or IP Address: Enter the FQDN or the IP address of the AD server that is used for authentication.
     - Comment: Enter additional information about the AD server.
     - Authentication Port: Enter the port number on the domain controller to which the appliance sends authentication requests. The default is 389.
     - Encryption: Select SSL from the drop-down list to transmit through an SSL (Secure Sockets Layer) tunnel. When you select SSL, the appliance automatically updates the authentication port to 636. Infoblox strongly recommends that you select this option to ensure the security of all communications between the NIOS appliance and the AD server. If you select this option, you must upload a CA certificate from the AD server. Click CA Certificates to upload the certificate. In the CA Certificates dialog box, click the Add icon, and then navigate to the certificate to upload it.
     - Connect through Management Interface: Select this so that the NIOS appliance uses the MGMT port for administrator authentication communications with just this AD server.
     - Disable server: Select this to disable an AD server if, for example, the connection to the server is down and you want to stop the NIOS appliance from trying to connect to this server.
     - Click Test to test the configuration. If the NIOS appliance connects to the domain controller using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the server, the appliance displays a message indicating an error in the configuration.
     - Click Add to add the domain controller to the group.
   - When you add multiple domain controllers, the appliance lists the servers in the order you added them. This list also determines the order in which the NIOS appliance attempts to contact a domain controller. You can move a server up or down the list by selecting it and clicking the up or down arrow.
   - You can also delete a domain controller by selecting it and clicking the Delete icon.
   - Timeout(s): The number of seconds that the NIOS appliance waits for a response from the specified authentication server. The default is 5.
   - Comment: Enter additional information about the service.
   - Disable: Select this to retain an inactive AD authentication service profile.
4. Save the configuration and click Restart if it displays at the top of the screen.
Authenticating Admin Accounts Using TACACS+

You can configure NIOS to authenticate admins against TACACS+ (Terminal Access Controller Access-Control System Plus) servers. TACACS+ provides separate authentication, authorization, and accounting services. To ensure reliable delivery, it uses TCP as its transport protocol, and to ensure confidentiality, all protocol exchanges between the TACACS+ server and its clients are encrypted. For detailed information about TACACS+, refer to the Internet draft http://tools.ietf.org/html/draft-grant-tacacs-02.

In addition, you can configure a custom service, infoblox, on the TACACS+ server, and then define a user group and specify the group name in the custom attribute infoblox-admin-group. Ensure that you apply the user group to the custom service infoblox. On NIOS, you define a group with the same name and add it to the authentication policy. Then when the TACACS+ server responds to an authentication and authorization request and includes the infoblox-admin-group attribute, NIOS can match the group name with the group in the authentication policy and automatically assign the admin to that group.

*Figure 4.7* illustrates the TACACS+ authentication and authorization process when PAP/CHAP authentication is used.

<table>
<thead>
<tr>
<th></th>
<th>Administrator</th>
<th>NIOS Appliance</th>
<th>TACACS+ Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A user makes an HTTPS connection to the NIOS appliance and sends an account name and password.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>The appliance checks the authentication policy, which specifies the TACACS+ authentication server group.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>The appliance sends an AUTHENTICATION START message with the user’s credentials.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>The TACACS+ server sends an AUTHENTICATION REPLY indicating the admin was successfully authenticated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>The appliance sends an AUTHORIZATION REQUEST with the attribute-value string for the “infoblox” service.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6a</td>
<td>NIOS allows the user to log in and assigns it to the admin group in the authentication policy that matches the group in the custom attribute. If NIOS does not find a matching group in the authentication policy, it assigns the user to the default admin group.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6b</td>
<td>The TACACS+ server sends an AUTHORIZATION RESPONSE indicating authorization succeeded and includes the custom attribute “infoblox-admin-group”.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The appliance does not allow the user to log in.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The TACACS+ server sends a REPLY message indicating authentication and/or authorization is unsuccessful.</td>
<td></td>
</tr>
</tbody>
</table>
Managing Administrators

TACACS+ Accounting

When you enable TACACS+ accounting, NIOS sends the TACACS+ accounting server a TACACS+ accounting event with the same information that it sends to the Audit Log for any user command/event. NIOS sends an accounting start packet when a user first logs in successfully using TACACS+ authentication, and it sends an accounting STOP packet when a user logs out of the GUI or CLI or when a GUI or CLI session times out. If a product restarts or software failure occurs, NIOS drops any outstanding accounting packets. Note that audit log entries that are greater than 3,600 characters are truncated in accounting events sent to TACAS+ servers.

Configuring TACACS+

Complete the following tasks to enable NIOS and the TACACS+ servers to communicate.

On each TACACS+ server that you are adding to the authentication server group:

- For Windows TACACS+ servers, add the NIOS appliance as an AAA client. This step is not required for LINUX TACACS+ servers.
- Determine which user group on the TACACS+ server is used to match the admin group in NIOS, and then configure the following settings for the user group:
  - Add “infoblox” as a custom service.
  - Define the custom attribute for the group, in the format: `infoblox-admin-group=group_name`. For example, `infoblox-admin-group=remoteadmins1`. The group name can have a maximum of 64 characters.

On the NIOS appliance:

- Create a TACACS+ authentication server group. You can create only one TACACS+ server group. For more information, see Configuring a TACACS+ Authentication Server Group.
- Create the local admin group in NIOS that matches the user group on the TACACS+ server. Note that the NIOS admin group name must match the group name specified in the TACACS+ server and in the custom attribute. For example, if the custom attribute is `infoblox-admin-group=remoteadmins1`, then the admin group name must be `remoteadmins1`. In addition, you can designate a default admin group for remote admins. For information about configuring group permissions and privileges, see About Admin Groups on page 113.
- In the authentication policy, add the newly configured TACACS+ server group and the TACACS+ admin group name. See Defining the Authentication Policy on page 144 for more information about configuring an admin policy.

Configuring a TACACS+ Authentication Server Group

You can add multiple TACACS+ servers to the TACACS+ authentication server group. NIOS sends authentication requests to the TACACS+ servers in the order they are listed. NIOS sends authentication requests to the first server on the list. If that server is unreachable or generates an error, then NIOS sends the request to the next server in the list that has not been previously queried, and so on. NIOS logs an error message in syslog if all servers have been queried and they all generate errors or are unreachable.

To configure a TACACS+ authentication server group:

1. From the Administration tab, click the Authentication Server Groups tab.
2. Click the TACACS+ Services subtab and click the Add icon.
3. In the Add TACACS+ Service wizard, complete the following:
   - **Name**: Enter a name for the server group.
   - **TACACS+ Servers**: Click the Add icon and complete the following:
     - **Server Name or IP address**: The name or IP address of the TACACS+ server.
     - **Comment**: You can enter additional information about the server.
     - **Port**: The TCP destination port for TACACS+ communication. This port is used for authentication, accounting and authorization packets. The default is port 49.
     - **Authentication Type**: Select ASCII, PAP or CHAP. The default is CHAP.
— **Shared Secret:** The shared key that the NIOS appliance and the TACACS+ server use to encrypt and decrypt messages.

— **Enable Accounting:** Select this to enable NIOS to send accounting information to the TACACS+ server.

— Connect through Management Interface: Select this check box to enable the appliance to use the MGMT port to communicate with the TACACS+ server. Ensure that the MGMT port is configured. Otherwise, the appliance will use the LAN interface

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

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

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

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

— **Timeout(s):** Specify the number of seconds or milliseconds that the appliance waits for a response from the TACACS+ server before it tries to contact it again. The amount of time before the server is retried. The default and minimum is 5000, and the maximum is 60000.

— **Retries:** Specify how many times NIOS attempts to contact a TACACS+ server and fails before it tries to contact the next server on the list. The default is 0. The maximum is 5.

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

— **Timeout(s):** Specify the number of seconds or milliseconds that the appliance waits for a response from the TACACS+ server. The amount of time before the server is retried. The default and minimum is 1000, and the maximum is 30000.

— **Retries:** Specify how many times the appliance attempts to contact an accounting TACACS+ server and fails before it tries to contact the next accounting server on the list. The default is 0. The maximum is 5.

— **Comment:** Enter additional information about the service.

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

4. Save the configuration.
Managing Administrators

### Defining the Authentication Policy

The authentication policy defines which authentication server groups the appliance uses to authenticate admins and lists the local admin groups that map to the remote admin groups.

By default, the appliance provides the “Local Admin” service for authenticating users against the local database. You cannot modify or delete this default service.

### Configuring a List of Authentication Server Groups

To enable NIOS to use multiple authentication server groups, define a prioritized list as follows:

1. From the Administration tab, select the Administrators tab -> Authentication Policy tab.
2. From the Authenticate users against these services in this order section, click the Add icon to add an authentication server group.
3. Select one of the following in the Add Authentication Service section:
   - **Active Directory**: Select this to add an AD authentication server group, and then select a group from the drop-down list.
   - **RADIUS**: Select this to add a RADIUS authentication server group, and then select a group from the drop-down list.
   - **TACACS+**: Select this to add the TACACS+ authentication server group, and then select a group from the drop-down list.
4. Click Add.

   You can reorder the list by selecting an authentication server group and moving it up or down the list using the arrow keys.

### Configuring a List of Remote Admin Groups

In order for NIOS to assign a remote admin to the correct group, you must list the admin groups in the local database that match the remote admin groups. You can also define a default admin group to which NIOS assigns remote users with no admin groups listed.

The appliance matches a remote admin to a group in the order the groups are listed. When the appliance receives information that an admin belongs to one or more groups, the appliance assigns the user to the first group in the list that matches. It assigns the admin to the default group, if specified, if no groups are returned by the authentication server, or if the appliance does not find a group in the local database that matches the group returned by the authentication server.

To configure the remote admin group list:

1. From the Administration tab, select the Administrators tab -> Authentication Policy tab.
2. From the Map the remote admin group to the local group in this order section, click the Add icon.
3. In the Admin Group Selector dialog box, select an admin group, and then click the Select icon. Use Shift+click and Ctrl+click to select multiple admin groups.

   You can reorder the list by selecting an admin group and using the arrow keys to move it up or down the list.

To assign a user to a specific admin group if the remote admin group is not found, select Assign User to this Group if Remote Admin Group cannot be found, and then click Select. In the Admin Group Selector dialog box, select an admin group, and then click the Select icon.
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. Save the configuration and click Restart if it displays at the top of the screen.
Notifying Administrators

You can notify individual administrators about system status through email, or notify a group of people using an alias email address. If you have configured DNS resolution on your network, the E-mail relay configuration function is not required. If you did not configure the settings on the DNS Resolver section, you must enter a static IP address of the target system in the Relay Name/IP Address field. The appliance sends e-mail to administrators when certain events occur. 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 904

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

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

Grid Level

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

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

Member Level

To define email settings for a member:

1. From the Grid tab, select the Grid Manager tab -> member check box, and then select the Edit icon.
2. In the Grid Member Properties editor, select the Email tab, and then click Override to override Grid-level settings.
3. Complete the email configuration as described in Grid Level on page 146.
# Administrative Permissions for Common Tasks

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

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

### Table 4.6 Permissions for Common Tasks

<table>
<thead>
<tr>
<th>Tasks</th>
<th>All Grid Members</th>
<th>Grid DNS Properties</th>
<th>Specific Grid Member(s)</th>
<th>Member DNS Properties</th>
<th>Member DHCP Properties</th>
<th>All DNS Views</th>
<th>All DNS Zones</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>
<td></td>
<td></td>
</tr>
<tr>
<td>Restart services for the 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>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure grid DNS properties, configure member DNS properties, assign members to DNS objects, and restart DNS service on 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>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure grid DHCP properties, configure member DHCP properties, assign members to DHCP objects, and restart DHCP service on 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>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure 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>
<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>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure member DNS properties, assign member to DNS objects, and restart DNS service on 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>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure member DHCP properties, assign member to DHCP objects, and restart DHCP service on 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>
<td></td>
<td></td>
</tr>
<tr>
<td>Restart member DNS service</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>
<td></td>
<td></td>
</tr>
<tr>
<td>Restart member DHCP service</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>
<td></td>
<td></td>
</tr>
<tr>
<td>Initiate and control network discovery on all networks</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>
<td></td>
<td></td>
</tr>
<tr>
<td>Scheduling tasks for all supported objects</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>
<td></td>
<td></td>
</tr>
<tr>
<td>Tasks</td>
<td>All Grid Members</td>
<td>Grid DHCP Properties</td>
<td>Specific Grid Member(s)</td>
<td>Member DNS Properties</td>
<td>Member DHCP Properties</td>
<td>Restart Member DNS</td>
<td>Restart Member DHCP</td>
<td>All DNS Views</td>
<td>All DNS Zones</td>
<td>All Shared Record Groups</td>
<td>All Resource Records</td>
<td>All Network Views</td>
<td>All Networks</td>
<td>Specific Network(s)</td>
<td>DHCP Range(s)</td>
</tr>
<tr>
<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>--------------</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>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete DNS views</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>
<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>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete DNS zones with assigned members</td>
<td>RW</td>
<td></td>
<td></td>
<td></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></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 all resource records</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>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for all resource records</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>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign member to DNS objects</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>
<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>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete network views and their associated 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>
<td></td>
<td></td>
</tr>
<tr>
<td>View network properties and statistics</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>
<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>
<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>
<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></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 fixed addresses in a specific network 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>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign member to DHCP objects</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>
<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 126.

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 149
- Administrative Permissions for Network Discovery on page 150
- Administrative Permissions for Scheduling Tasks on page 150
- Administrative Permissions for Microsoft Servers on page 151

Administrative Permissions for Grid Members

Table 4.7 lists the tasks admins can perform and the required permissions for Grid members.

Table 4.7  rid Member Permissions

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid Member(s)</th>
<th>Member DNS Properties</th>
<th>Member DHCP Properties</th>
<th>Restart Member DNS</th>
<th>Restart Member DHCP</th>
<th>DNS Views</th>
<th>DNS Zones</th>
<th>Networks</th>
<th>DHCP Ranges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign member to DNS zones</td>
<td></td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign member to networks</td>
<td></td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign member to DHCP ranges</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure member properties</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add a member to a Match Members list of a DNS view</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete a view with members in a Match Members list</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View DNS and DHCP member properties</td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
<td></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>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View DNS and DHCP configuration file</td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
<td></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>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restart DNS service on the member</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restart DHCP service on the member</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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 121. The following table lists the tasks admins can perform and the required permissions for network discovery.

Table 4.8  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>RO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add unmanaged data to existing hosts, and resolve conflicting IP addresses</td>
<td>RW</td>
<td></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 256. 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 121. 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 4.9  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 149.
- DNS resources—See *Administrative Permissions for DNS Resources* on page 154.
- DHCP resources—See *Administrative Permissions for DHCP Resources* on page 160.

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 4.10 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>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove a Microsoft server as the primary or secondary server of a zone</td>
<td>RW</td>
<td></td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove a zone from a Microsoft server</td>
<td>RW</td>
<td></td>
<td></td>
<td>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></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 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>RW</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 161
- Administrative Permissions for IPv4 and IPv6 Networks on page 153
- Administrative Permissions for Hosts on page 153

Administrative Permissions for IPv4 and IPv6 Networks

Limited-access admin groups can access IPv4 and IPv6 networks only if their administrative permissions are defined. Permissions for a network apply to all its DNS and DHCP resources, if configured. To override network-level permissions, you must define permissions for specific objects within the networks. You can also define permissions for specific DHCP objects and grid member to restrict admins to perform only the specified DHCP tasks on the specified member. For more information, see Defining DNS and DHCP Permissions on Grid Members on page 124.

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

- All IPv4 or IPv6 networks—Global permission that applies to all networks in the database.
- A specific network—Network permissions apply to all objects in the network. This overrides global permissions.
- A specific network on a specific member—Network permissions apply to all objects in the network and member permissions apply to the specific member. For information about member permissions, see Modifying Permissions on a Grid Member on page 125.

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
- DNS64 synthesis groups

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 126.

You can also define permissions for specific DNS objects and grid member to restrict admins to perform only the specified DNS tasks on the specified member. For more information, see "Defining DNS and DHCP Permissions on Grid Members" on page 124.

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

- Administrative Permissions for DNS Views on page 155
- Administrative Permissions for Zones on page 156
- Administrative Permissions for Resource Records on page 157
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 126.

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

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

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

For example, you can grant an admin group the following permissions:
- Read-only to a zone and to all its A, AAAA, and PTR records
- Read/Write permission to all MX and SRV records in the zone
- Deny to all the other resource records—CNAME, DNAME, TXT, host, and bulk host

You can grant read-only or read/write permission, or deny access to zones as follows:
- All zones — Global permission that applies to all zones in all views.
- All zones in a view—Permissions at this level override the global permissions.
- A specific zone—Applies to the zone properties and resource records, if you do not define permissions for its resource records. This overrides global and view-level permissions. If you delete a zone and reparent its subzone, the subzone inherits the permissions of the new parent zone.
- 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 126.

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

Table 4.12 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></td>
<td></td>
<td>RW</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></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RD</td>
</tr>
<tr>
<td>Search for zones, subzones, and resource records in a specific DNS view</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RO</td>
</tr>
<tr>
<td>Copy resource records from one zone to another: Source zone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RO</td>
</tr>
<tr>
<td>Copy resource records from one zone to another: Destination Zone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RO</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 126. The following table lists the tasks admins can perform and the required permissions for resource records.

<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></td>
</tr>
<tr>
<td>View resource records for a specified type only</td>
<td>RO</td>
<td></td>
</tr>
<tr>
<td>Search for records of a specified type</td>
<td>RO</td>
<td></td>
</tr>
<tr>
<td>View a specific resource record</td>
<td>RO</td>
<td></td>
</tr>
<tr>
<td>View, modify, and delete a specific resource record</td>
<td>RW</td>
<td></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 126. The following table lists the tasks admins can perform and the required permissions for shared record groups.

Table 4.14 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></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View a specific shared record</td>
<td></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>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Administrative Permissions for DNS64 Synthesis Groups

By default, only superusers can add, edit, and delete DNS64 synthesis groups. Limited-access admin groups can access synthesis groups, only if their administrative permissions are defined.

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

- All synthesis groups—Global permission that applies to all shared record groups in the database.
- A specific synthesis group—Overrides global permissions.

For information on setting permissions for synthesis groups, see *Applying Permissions and Managing Overlaps* on page 126. The following table lists the tasks admins can perform and the required permissions for synthesis groups.

**Table 4.15 Permissions for DNS64 Synthesis Groups**

<table>
<thead>
<tr>
<th>Tasks</th>
<th>All Shared Record Groups</th>
<th>Specific Shared Record Group</th>
<th>Shared Record Type</th>
<th>Specific DNS Zone</th>
<th>Specific Shared Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the DNS zones associated with a shared record</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete zones with a shared record group assigned. Before you delete a shared record group, you must remove all zones associated with it.</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete synthesis groups</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify and delete a specific synthesis group</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View a synthesis group</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apply a synthesis group to the Grid</td>
<td>RO</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apply a synthesis group to a member</td>
<td>RO</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apply a synthesis group to a DNS view</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
</tr>
</tbody>
</table>
Administrative Permissions for DHCP Resources

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

- Network views
- IPv4 networks
- Hosts
- IPv4 DHCP ranges
- IPv4 DHCP fixed addresses
- IPv4 DHCP reservations
- MAC address filters
- IPv4 shared networks
- IPv4 network templates
- IPv4 DHCP range templates
- IPv4 fixed address templates
- IPv4 DHCP lease history
- Roaming hosts
- IPv6 networks
- IPv6 DHCP ranges
- IPv6 DHCP fixed addresses
- IPv6 shared networks
- IPv6 network templates
- IPv6 DHCP range templates
- IPv6 fixed address templates
- IPv6 DHCP lease history

You can grant an admin group broad permissions to DHCP resources, such as read/write permission to all IPv4 or IPv6 networks and shared networks in the database. In addition, you can grant permission to specific resources, such as a specific IPv4 or IPv6 network or DHCP range, or an individual address in an IPv4 or IPv6 network. Permissions at more specific levels override global permissions.

You can also define permissions for specific DHCP objects and grid member to restrict admins to perform only the specified DHCP tasks on the specified member. For more information, see Defining DNS and DHCP Permissions on Grid Members on page 124.

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

- Administrative Permissions for Network Views on page 161
- Administrative Permissions for IPv4 and IPv6 Networks and Shared Networks on page 162
- Administrative Permissions for IPv4 or IPv6 Fixed Addresses and IPv4 Reservations on page 164
- Administrative Permissions for IPv4 and IPv6 DHCP Ranges on page 165
- Administrative Permissions for IPv4 or IPv6 DHCP Templates on page 166
- Administrative Permissions for MAC Address Filters on page 167
- Administrative Permissions for the IPv4 and IPv6 DHCP Lease Histories on page 168
Administrative Permissions for Network Views

Limited-access admin groups can access network views, including the default network view, only if they have read-only or read/write permission to a specific network view or to all network views. Permissions granted to a network view apply to all its IPv4 and IPv6 networks, shared networks, DHCP ranges and fixed addresses. You can grant admin groups read-only or read/write permission, or deny access to network views as follows:

- All network views—Global permission that applies to all network views in the database.
- A specific network view—Permission to a specific network view applies to the properties you set in the Network View editor, and to all the IPv4 and IPv6 networks and shared networks in the network view. This overrides the global permission to all network views. When you configure permissions for a network view, you can also set permissions for the following:
  - All IPv4 and IPv6 networks in the selected network view—If you do not define permissions for IPv4 or IPv6 networks, they inherit the permissions of their network view.
  - All IPv4 and IPv6 shared networks in a specific network view—If you do not define permissions for IPv4 or IPv6 shared networks, they inherit the permissions of their network view.

Note that you can grant an admin group read-only or read/write permission to specific IPv4 or IPv6 networks in a network view, without granting them permission to that network view. For information, see Administrative Permissions for IPv4 and IPv6 Networks and Shared Networks on page 162.

For information on how to define permissions for network views, see Applying Permissions and Managing Overlaps on page 126.

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

Table 4.16 Network View Permissions

<table>
<thead>
<tr>
<th>Tasks</th>
<th>All DNS View</th>
<th>Specific DNS View</th>
<th>All Network Views</th>
<th>Specific Network View</th>
<th>All IPv4 or IPv6 Networks</th>
<th>All IPv4 or IPv6 Shared Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create and delete network views and their associated DNS views</td>
<td>RW</td>
<td>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 IPv4 and IPv6 networks and shared networks in all network views</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete IPv4 and IPv6 networks and shared networks in a network view</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View the properties of all network views</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View network statistics of all network views</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for all IPv4 and IPv6 networks and shared networks</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View the properties of a network view</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for IPv4 and IPv6 networks and shared networks in a network view</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expand and join IPv4 and IPv6 networks</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expand and join IPv4 and IPv6 networks in a specific network view</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete IPv4 and IPv6 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>
</tbody>
</table>
Administrative Permissions for IPv4 and IPv6 Networks and Shared Networks

Limited-access admin groups can access IPv4 and IPv6 networks, including shared networks, only if their administrative permissions are defined. Permissions for a network apply to all its DHCP ranges and fixed addresses. To override network-level permissions, you must define permissions for specific DHCP ranges and fixed addresses. For example, you can grant an admin group read-only permission to a network, read/write permission to its DHCP ranges, and read-only permission to its fixed addresses.

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

- **All IPv4 or IPv6 networks**—Global permission that applies to all IPv4 or all IPv6 networks in the database.
- **All IPv4 or IPv6 shared networks**—Global permission that applies to all IPv4 or all IPv6 shared networks in the database.
- **A specific IPv4 or IPv6 network**—Network permissions apply to its properties and to all DHCP ranges, fixed addresses and hosts in the network, if they do not have permissions defined. This overrides global permissions.
- **All IPv4 or IPv6 DHCP ranges in a network**—If you do not define permissions for DHCP ranges, they inherit the permissions of the network in which they reside.
- **All IPv4 or IPv6 fixed addresses in a network**—If you do not define permissions for fixed addresses, they inherit the permissions of the network in which they reside.

To define permissions for a specific IPv4 or IPv6 network and its DHCP ranges and fixed addresses, see *Applying Permissions and Managing Overlaps* on page 126.

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

<table>
<thead>
<tr>
<th>Tasks</th>
<th>All DNS View</th>
<th>Specific DNS View</th>
<th>All Network View</th>
<th>Specific Network View</th>
<th>All IPv4 or IPv6 Networks</th>
<th>All IPv4 or IPv6 Shared Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>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>
<tr>
<td>Search for IPv4 and IPv6 networks in a network view</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete all IPv4 or IPv6 shared networks</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View the properties of all IPv4 or IPv6 shared networks</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for IPv4 and IPv6 shared networks in a network view</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restart services from the DHCP tab</td>
<td>RO</td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 4.17 Network Permissions

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid Member(s)</th>
<th>All IPv4 or IPv6 Networks</th>
<th>Specific IPv4 or IPv6 Network</th>
<th>Specific IPv4 or IPv6 DNS Zone</th>
<th>All IPv4 or IPv6 DHCP Ranges</th>
<th>All IPv4 or IPv6 Fixed Addresses</th>
<th>IPv4 or IPv6 Network Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete IPv4 or IPv6 networks, DHCP ranges, and fixed addresses without assigned Grid members</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete IPv4 or IPv6 networks, DHCP ranges, and fixed addresses with assigned Grid members</td>
<td>RW RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign a Grid member to a specific IPv4 or IPv6 network and its DHCP ranges</td>
<td>RW RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expand and join IPv4 or IPv6 networks</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create IPv4 or IPv6 networks from templates</td>
<td>RW RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete an IPv4 or IPv6 network</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View IPv4 or IPv6 network properties and statistics, and search for DHCP ranges and fixed addresses in a specific network</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete IPv4 or IPv6 DHCP ranges and fixed addresses in a specific network</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create and split an IPv4 or IPv6 network and automatically create a reverse DNS zone</td>
<td>RW RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete IPv4 or IPv6 shared networks</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View IPv4 or IPv6 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 IPv4 or IPv6 DHCP ranges with an assigned member in a specific network</td>
<td>RW RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete IPv4 or IPv6 DHCP ranges</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for IPv4 or IPv6 DHCP ranges in a specific network</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete IPv4 or IPv6 fixed addresses</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for IPv4 or IPv6 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 IPv4 or IPv6 Fixed Addresses and IPv4 Reservations

IPv4 and IPv6 fixed addresses and IPv4 reservations inherit the permissions of the networks in which they reside. You can override network-level permissions by defining permissions for fixed addresses.

You can grant read-only or read-write permission, or deny access to fixed addresses, as follows:
- All IPv4 fixed addresses/reservations—Global permission that applies to all IPv4 fixed addresses and reservations in the database.
- All IPv6 fixed addresses—Global permission that applies to all IPv6 fixed addresses in the database.
- All IPv4 fixed addresses/reservations in a network—Permissions at this level override global permissions. If you do not define permissions for fixed addresses and reservations, they inherit the permissions of the network in which they reside.
- All IPv6 fixed addresses in a network—Permissions at this level override global permissions. If you do not define permissions for IPv6 fixed addresses, they inherit the permissions of the network in which they reside.
- A single IPv4 fixed address/reservation—Overrides global and network-level permissions.
- A single IPv6 fixed address—Overrides global and network-level permissions.

For information on setting permissions for fixed addresses, see Applying Permissions and Managing Overlaps on page 126.

The following table lists the tasks admins can perform and the required permissions for IPv4 and IPv6 fixed addresses.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Specific IPv4 or IPv6 Network</th>
<th>All IPv4 or IPv6 fixed Addresses/IPv4 Reservations</th>
<th>Specific IPv4 or IPv6 Fixed Address/IPv4 Reservation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete IPv4 fixed addresses/reservations or IPv6 fixed addresses</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete IPv4 fixed addresses/reservations or IPv6 fixed addresses in a specific network</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify and delete an IPv4 fixed address/reservation or IPv6 fixed address</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for all IPv4 fixed addresses/reservations or IPv6 fixed addresses</td>
<td>RO</td>
<td></td>
<td>RO</td>
</tr>
<tr>
<td>View and search for IPv4 fixed addresses/reservations or IPv6 fixed addresses in a network</td>
<td>RO</td>
<td></td>
<td>RO</td>
</tr>
<tr>
<td>View and search for an IPv4 fixed address/reservation or IPv6 fixed address</td>
<td>RO</td>
<td></td>
<td>RO</td>
</tr>
</tbody>
</table>
Administrative Permissions for IPv4 and IPv6 DHCP Ranges

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

- All IPv4 or IPv6 DHCP ranges—Global permission that applies to all IPv4 or IPv6 DHCP ranges in the database.
- All IPv4 or IPv6 DHCP ranges in a network—Permissions at this level override global permissions. If you do not define permissions for DHCP ranges, they inherit the permissions of the network in which they reside.
- A single IPv4 or IPv6 DHCP range—Overrides global and network-level permissions.

For information on setting permissions for DHCP ranges, see Applying Permissions and Managing Overlaps on page 126. The following table lists the tasks admin can perform and the required permissions for DHCP ranges.

Table 4.19 DHCP Ranges

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid Member(s)</th>
<th>Specific IPv4 or IPv6 Network</th>
<th>All DHCP IPv4 or IPv6 Ranges</th>
<th>Specific IPv4 or IPv6 DHCP Range</th>
<th>MAC Address Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete IPv4 or IPv6 DHCP ranges with an assigned member or a failover association</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete IPv4 or IPv6 DHCP ranges in a network with assigned members</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify and delete an IPv4 or IPv6 DHCP range with an assigned member</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for all IPv4 or IPv6 DHCP ranges with an assigned member</td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for IPv4 or IPv6 DHCP ranges in a network with assigned members</td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for an IPv4 or IPv6 DHCP range with an assigned member</td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for an IPv4 or IPv6 DHCP range without an assigned member</td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apply relay agent and option filters to an IPv4 DHCP range</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apply a MAC address filter to an IPv4 DHCP range</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Administrative Permissions for IPv4 or IPv6 DHCP Templates

There are three types of DHCP templates for IPv4 and IPv6 objects—network, DHCP range, and fixed address/reservation templates. To access any of these templates, a limited-access admin group must have read-only permission to the template. Limited-access admin groups cannot have read/write permission to the templates. Only superusers can create, modify and delete network, DHCP range, and fixed address templates. An admin group with read-only permission to the DHCP templates can view them and use them to create networks, DHCP ranges and fixed addresses, as long as they have read/write permissions to those DHCP resources as well.

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

For information on setting permissions, see Applying Permissions and Managing Overlaps on page 126. The following table lists the tasks admins can perform and the required permissions for DHCP templates.

Table 4.20 Permissions for DHCP Templates

<table>
<thead>
<tr>
<th>Tasks</th>
<th>IPv4 or IPv6 DHCP Templates</th>
<th>All IPv4 or IPv6 Networks</th>
<th>All IPv4 or IPv6 DHCP Ranges</th>
<th>All IPv4 or IPv6 Fixed Addresses/IPv4 Reservations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create IPv4 or IPv6 networks from templates</td>
<td>RO</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create IPv4 or IPv6 DHCP ranges from templates</td>
<td>RO</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create IPv4 fixed addresses/reservations or IPv6 fixed addresses from templates</td>
<td>RO</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View templates</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note the following additional guidelines:

- DHCP range templates and fixed address templates do not inherit their permissions from network templates. You must set permissions for each type of template.
- An admin group can create a network using a network template that includes a DHCP range template and a fixed address template, even if it has no permission to access the DHCP range and fixed address templates.
Administrative Permissions for 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 126. The following table lists the tasks admins can perform and the required permissions for MAC address filters.

Table 4.21 Permissions for MAC Filters

<table>
<thead>
<tr>
<th>Tasks</th>
<th>All MAC Address Filters</th>
<th>Specific MAC Address Filter</th>
<th>Specific IPv4 DHCP Ranges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete MAC address filters</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete MAC address entries for a MAC address filter</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify and delete a MAC address filter</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apply a MAC address filter to an IPv4 DHCP range</td>
<td>RO</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>Delete a MAC address filter from an IPv4 DHCP range</td>
<td>RO</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>View MAC address filters and their MAC address entries</td>
<td>RO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View a MAC address filter and its MAC address entries</td>
<td>RO</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Administrative Permissions for the IPv4 and IPv6 DHCP Lease Histories

A limited-access admin group can view and export the IPv4 and IPv6 DHCP lease histories if it has read-only permission to the IPv4 and IPv6 DHCP lease history. Permissions to the IPv4 and IPv6 DHCP lease histories are different from the network permissions. Therefore, an admin group can access the IPv4 and IPv6 DHCP lease histories, regardless of its network permissions. Note that only superusers can import a DHCP lease history file.

To define permissions for the IPv4 and IPv6 DHCP lease histories:

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

or

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

2. Complete the following in the Manage Global Permissions dialog box:
   — Permission Type: Select DHCP Permissions from the drop-down list.
   — In the table, select Read/Write, Read-only, or Deny for All IPv4 DHCP Lease History and All IPv6 DHCP Lease History.

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

Administrative Permissions for File Distribution Services

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

You can grant read-only or read/write permission, or deny access to the following resources:

- Grid File Distribution Properties—Applies to the Grid and its members, directories, and files. You can set this from the Administrators perspective only.
- Member File Distribution Properties—Applies to the Grid member properties only.
- A specific directory—Applies to the directory and its files.

For information on setting permissions, see Applying Permissions and Managing Overlaps on page 126. The following table lists the tasks admins can perform and the required permissions for file distribution services.
Table 4.22 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>
Administrative Permissions for Dashboard Tasks

Limited-access admin groups can configure IPAM tasks on the Tasks Dashboard only if their administrative permissions are defined. The appliance denies access to IPAM tasks for which an admin group does not have defined permissions.

You can grant read-only or read/write permission, or deny access to IPAM tasks as follows:
- All IPAM tasks on the Tasks Dashboard
- A specific IPAM task

When you deny access to an IPAM task for an admin group, users cannot configure the task on their dashboards. Users must have at least read-only permission to a specific task to see it in the task pack. To perform a specific task, users must also have read/write permission to the objects associated with the task. For information about specific permissions for IPAM, DNS, and DHCP objects, see Administrative Permissions for IPAM Resources on page 153, Administrative Permissions for DNS Resources on page 154, and Administrative Permissions for DHCP Resources on page 160.

For information about setting permissions, see Applying Permissions and Managing Overlaps on page 126. The following table lists the tasks admins can perform and the required permissions for configuring IPAM tasks on the Tasks Dashboard.

Table 4.23 Permissions for IPAM Tasks

<table>
<thead>
<tr>
<th>Tasks</th>
<th>All Dashboard Tasks</th>
<th>Add Networks</th>
<th>Add Hosts</th>
<th>Add Fixed Addresses</th>
<th>Add CNAME Record</th>
<th>Add TXT Record</th>
<th>Add MX Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure all tasks in the IPAM task pack</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the Add Networks task</td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the Add Hosts task</td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the Add Fixed Addresses task</td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the Add CNAME Record task</td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the Add TXT Record task</td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the Add MX Record task</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></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 173
  — Grid Communications  on page 174
  — NAT Groups  on page 175
  — Automatic Software Version Coordination  on page 178
  — Grid Bandwidth Considerations  on page 180
• About HA Pairs  on page 182
  — Planning for an HA Pair  on page 182
  — About HA Failover  on page 183
  — VRRP Advertisements  on page 184
• Creating a Grid Master  on page 185
  — Port Numbers for Grid Communication  on page 187
  — Grid Setup Wizard  on page 187
  — Creating an HA Grid Master  on page 187
  — Creating a Single Grid Master  on page 190
• Adding Grid Members  on page 192
  — Adding a Single Member  on page 192
  — Adding an HA Member  on page 193
  — Joining Appliances to a Grid  on page 194
• Configuration Example: Configuring a Grid  on page 195
  — Cable All Appliances to the Network and Turn On Power  on page 197
  — Create the Grid Master  on page 197
  — Define Members on the Grid Master  on page 199
  — Join Appliances to the Grid  on page 200
  — Import DHCP Data  on page 202
  — Import DNS Data  on page 203
  — Using the Wizard  on page 204
  — After Using the Wizard  on page 206
Deploying a Grid

- Managing a Grid on page 207
  - Changing Grid Properties on page 208
  - Setting the MTU for VPN Tunnels on page 209
  - Removing a Grid Member on page 209
  - Promoting a Master Candidate on page 209
- About the Master Grid on page 210
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 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 the other vNIOS appliances as Grid members only. For information, see Supported vNIOS Appliance Configurations on page 1015.

You can also add any of the supported Trinzic Reporting platforms as a logging and reporting device in your Grid. Infoblox provides a few Infoblox platforms that you can use as the logging and reporting device. For information about the supported appliances, see Supported Platforms for Reporting on page 970. The reporting appliance collects data from members in the Grid and stores the data in the database. It then uses the data to generate predefined and user-defined reports that you can access through Grid Manager. These reports provide useful information about the IPAM, DNS, DHCP, and system activities and usage in your Grid. For more information about reporting, see Infoblox Reporting Solution on page 967.

Figure 5.1 shows the basic concept of a Grid, database distribution (or “replication”), and reporting.

Figure 5.1 Grid and Partitioned Database Replication

- The administrator makes a secure connection to the Grid Master to configure and manage all Grid members.
- The Grid Master replicates the section of the database that applies to each member … and it replicates the entire database to the master candidate.
- The reporting member collects data from Grid members, stores the data in the reporting database, and ... the Grid Master.
- The reporting member polls data from members.

**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 1015.

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 D, "vNIOS Appliance Limitations", on page 1015. For additional information specific to each platform, refer to the Quick Start Guide for Installing vNIOS Software on Riverbed Services Platforms and the Quick Start Guide for Installing vNIOS Software on VMware Platforms.

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 282.

**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 177.
**Deploying a Grid**

**Figure 5.4 NAT without NAT Groups**

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 282.

**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 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**

Members 1 – 5 use the addresses in **black bold** for Grid communications. Members 1 and 6 use their interface addresses in **underlined blue bold**. If Member 4 became master, it would use its interface address in **double underlined green bold** to communicate with Member 5, and its NAT address to communicate with all other members.

Members 3 and 4 are master candidates. Because Member 3 is alone behind a NAT appliance, it does not need to be in a NAT group. It always uses its NAT address for Grid communications. However, Member 4 is behind the same NAT appliance as Member 5, so they are put in the same NAT group. If Member 4 ever became the Grid Master, it would use its interface address to communicate with Member 5 and its NAT address to communicate with all other members.

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, it became necessary to create NAT Group 2 and add Members 4 and 5 to it. Similarly, if you add another member behind the NAT appliance in front of Member 3, then you must create a new NAT group and add Member 3 and the new member to it. Always using NAT groups can simplify such changes to the Grid and ensure that NAT appliances never interrupt Grid communications.

To create a NAT group:

1. From the **Grid** tab, select the **Grid Manager** tab.
2. Expand the Toolbar and select **Grid Properties -> Edit**.
3. In the **Grid Properties** editor, select the **NAT Groups** tab.
4. Click the Add icon, and enter a name in the **Name** field and optionally, a comment in the Comment field.
5. Save the configuration and click **Restart** if it displays at the top of the screen.
To add members to the NAT group:

1. From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab.
2. Select a Grid member and click the Edit icon.
3. In the **Grid Member Properties** editor, select the **Network** -> **Advanced** tab and complete the following:
   - **Enable NAT compatibility**: 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. Save the configuration and click **Restart** if it displays at the top of the screen.

**Automatic Software Version Coordination**

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

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

---

**Note**: The Grid Master checks the software version every time an appliance or HA pair joins the Grid. The software version check occurs during the initial join operation and when a member goes offline and then rejoins the Grid.
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 on the active node automatically restarts. This causes an HA failover.
5. The new active node (which was previously the passive node) attempts to join the Grid, repeating steps 1 - 4.
6. When the NIOS application on the currently active node restarts, there is another failover, and the currently passive node becomes active again.
7. The active node again contacts the Grid Master and step 1 is repeated. Because the software versions now match, it can complete its attempt to join the Grid.
Grid Bandwidth Considerations

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

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

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

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

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

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

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

At a minimum, there must be 256 Kbps (kilobits per second) bandwidth between the Grid Master and each member, with a maximum round-trip delay of 500 milliseconds. For ongoing database updates, the amount of data sent or received is 15 Kb for every DDNS update, and 10 Kb for every DHCP lease offer/renew. The baseline amount for heartbeat and other maintenance traffic for each member is 2 Kbps. Measure the peak DNS and DHCP traffic you see in your network to determine the bandwidth needed between the Grid Master and its members for this activity. For example, you might decide to place your Grid members in the locations shown in Figure 5.6 on page 177.
In this example, the Grid Master is optimally placed in the Data Center West. There are a total of seven members: the HA Grid Master, three HA members, and three single members. If all the members are master candidates, the Grid Master replicates all changes to the other six members. Assuming that the master receives 20 dynamic updates per minute and 40 DHCP lease renewals per minute, the calculation for Grid bandwidth is:

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

Another component is the upgrade process. See *Upgrading NIOS Software* on page 320 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 183.
- **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 184.

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 226. To deploy an HA Grid Master, see Creating a Grid Master on page 185.

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 182, 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

![Diagram of HA Failover]

The clients always make service requests to—and receive replies from—the VIP and virtual MAC address. After an HA failover occurs, Node 2 becomes the active node. Because Node 2 is now active, it now owns the VIP address and virtual MAC address.
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).

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 182. 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-A and appliances with a 50 GB disk, support configuration as a Grid Master or Grid Master candidate. For information about which vNIOS appliance supports configuration as a Grid Master, see Supported vNIOS Appliance Configurations on page 1015.

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.

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 186.
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.

Note: If you enable the MGMT port, you can only make an HTTPS connection to the IP address of the active node. If you try to connect to the IP address of the passive node, the appliance redirects your browser to the IP address of the active node. SSHv2, however, behaves differently from HTTPS. If you enable the MGMT port and define its network settings for both nodes in the HA pair, you can make an SSHv2 connection to the IP addresses of the LAN and MGMT ports on both the active and passive nodes.
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*

---

**Port Numbers for Grid Communication**

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

To configure the VPN port number:

1. From the Grid tab, select the Grid Manager tab.
2. Expand the Toolbar and click Grid Properties -> Edit.
3. In the General tab of the Grid Properties editor, type a new port number in the VPN Port field.
4. Save the configuration.
5. When Grid Manager displays a warning indicating that a product restart is required, click Yes to continue.
   The product automatically restarts.

A member and master first perform a handshake to authenticate each other and exchange encryption keys. Then they
build an encrypted VPN tunnel between themselves. The member typically initiates both of these connections. The
master only initiates a key exchange if you manually promote a member to the role of master (see *Promoting a Master
Candidate* on page 209). *Figure 5.13* on page 186 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 1015.
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 276 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-A, 550-A, 1050-A, 1550-A, 1552-A, 1852-A, 2000-A, and 4010 appliances are autosensing, so you can use either a straight-through or cross-over Ethernet cable for these connections.
3. Use the LCD on one appliance or make a console connection to it, and configure the network settings of its LAN1 port so that it is on the local subnet and you can reach it on the network.
   
   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 39.
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 1015.

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 216.
- Console port – Method 2 – Using the CLI on page 216.

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.

   Note: The Ethernet ports on the Infoblox-250-A, 550-A, 1050-A, 1550-A, 1552-A, 1852-A, 2000-A, and 4010 appliances are autosensing, so you can use either a straight-through or cross-over Ethernet cable for this connection.

3. If you have not changed the default IP address (192.168.1.2/24) of the LAN1 port through the LCD or CLI—and the subnet to which you connect the appliance does not happen to be 192.168.1.0/24—put your management system in the 192.168.1.0/24 subnet and connect an Ethernet cable between your management system and the NIOS appliance.
4. Open a web browser and make an HTTPS connection to the IP address of the LAN1 port. To reach the default IP address, enter: https://192.168.1.2.

   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 Creating a Login Banner on page 40.

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 276.

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.
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 1015.

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 209.

   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 175.

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 194.

   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* and the *Quick Start Guide for Installing vNIOS Software on VMware Platforms*.

Configuring a Single Member on the Grid Master

1. From the Grid tab, select the Grid Manager tab -> Members tab.

2. Expand the Toolbar and click Add -> Add Grid Member.

3. In the Add Grid Member wizard, enter the following and click Next:

   — **Member Type**: Specify the appliance type of the Grid member. If the member is an Infoblox appliance, select Infoblox, which is the default. For a vNIOS appliance, select Riverbed, or Virtual NIOS for 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 1015.
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 276.

5. Optionally, define extensible attributes. For information, see *About Extensible Attributes* on page 262.

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 194.

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 285.

**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 1015.

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**
Deploying a Grid

1. Ensure that the gateway for the subnet on which the interfaces are set has the IP address of the gateway for the subnet on which the interfaces are set. This is the same for all interfaces.
2. 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 276.
3. Optionally, define extensible attributes. For information, see *Using Extensible Attributes* on page 265.
4. 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 187.

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 285), 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 197.
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 199.
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 200.

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 202 and *Import DNS Data* on page 203.

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 207.
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.

   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.

6. 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 into 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>
</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. Save the configuration and click Restart if it displays at the top of the screen.
6. Log out from the Grid Master.

Join Appliances to the Grid

To complete the process of adding appliances to the Grid, log in to and configure each individual appliance so that it can contact the Grid Master.

HQ Site – HA Grid Member (Node 1)

Make a console connection to the appliance that you want to make Node 1 in the HA pair, and enter the following:

```
Infoblox > set network
NOTICE: All HA configuration is performed from the GUI. This interface is used only to configure a standalone node or to join a Grid.
Enter IP address: 10.0.2.6
Enter netmask [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. Save the configuration and click Restart if it displays at the top of the screen.
12. To check the imported DHCP configuration file, from the Data Management tab, select the DHCP tab, ->Members tab →10.0.2.10 -check box. Expand the Toolbar and click View DHCP Configuration.
13. In the DHCP configuration file, check that all the imported subnets are present, and navigate to the beginning of the file and check that you see the 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 204: 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 206: 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. Save the configuration and click Restart if it displays at the top of the screen.

Note: When all DNS servers are members in the same Grid, the members use database replication to synchronize all their data—including DNS zone data. You can change the default behavior so that Grid members use zone transfers instead. In this example, Grid members use database replication.

Infoblox Grid Master – Name Server Groups

1. From the Data Management tab, select the DNS tab -> Name Server Groups tab.

2. Click the Add icon to open the Add Name Server Group wizard.

3. Enter the following:
   — Name Server Group Name: HQ-Group

4. Click the Add icon and add the following:
   — Grid Primary: ns1.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 203 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 209
- *Removing a Grid Member* on page 209
- *Promoting a Master Candidate* on page 209
Changing Grid Properties

You can change a Grid name, its shared secret, and the port number of the VPN tunnels that the Grid uses for communications. Note that changing the VPN port number, time zone, date or time requires a product restart.

To modify the properties of a Grid:

1. From the Grid tab, select the Grid Manager tab.
2. Expand the Toolbar and select Grid Properties -> Edit.
3. In the Grid Properties editor, select the General tab, 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. For more information, see Port Numbers for Grid Communication on page 187.
   - Enable Recycle Bin: Select the check box to enable the Recycle Bin. The Recycle Bin stores deleted items when the user deletes Grid, DNS, or DHCP configuration items. Enabling the Recycle Bin allows you to undo deletions and to restore the items on the appliance at a later time. If you do not enable this feature, deleted items from the GUI are permanently removed from the database.
   - Audit Logging: Select one of the following:
     - Detailed: This is the default type. It is automatically selected. It provides detailed information on all administrative changes such as the date and time stamp of the change, administrator name, changed object name, and the new values of all properties.
     - Brief: Provides information on administrative changes such as the date and time stamp of the change, administrator name, and the changed object name. It does not show the new value of the object.
4. Save the configuration.

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

You can configure the VPN MTU (maximum transmission unit) for any appliance with a network link that does not support the default MTU size (1500 bytes) and that cannot join a Grid because of this limitation. If an appliance on such a link attempts to establish a VPN tunnel with a Grid Master to join a Grid, the appliance receives a PATH-MTU error, indicating that the path MTU discovery process has failed. For information about the MTU discovery process, see RFC 1191, Path MTU Discovery.

To avoid this problem, you can set a VPN MTU value on the Grid Master for any appliance that cannot link to it using a 1500-byte MTU. When the appliance contacts the master during the key exchange handshake that occurs during the Grid-joining operation, the master sends the appliance the MTU setting to use.

To set the VPN MTU for a Grid member:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box -> Edit icon.
2. Select the Network -> Advanced tab of the Grid Member Properties editor.
3. In the VPN MTU field, enter a value between 600 and 1500.
4. Save the configuration and click Restart if it displays at the top of the screen.

Removing a Grid Member

You might want or need to remove a member from a Grid, perhaps to disable it or to make it an independent appliance or an independent HA pair. Before you remove a member, make sure that it is not assigned to serve any zones or networks.

To remove a Grid member, from the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and click the Delete icon.

Promoting a Master Candidate

To 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 174.

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 216.
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:
   ```plaintext
   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 CLI of those members to investigate.

---

**About the Master Grid**

A Master Grid provides centralized management of multiple Grids. When a Grid is managed by a Master Grid, the Master Grid icon appears on the left side of the top panel of Multi-Grid Manager. Assuming you have permission, you can click this icon to access Multi-Grid Manager. In addition, the Toolbar provides several functions for joining the Master Grid, editing its properties and leaving the Master Grid. For more information about the Master Grid and these functions, refer to the *Multi-Grid Manager Administrator Guide*. 
Chapter 6  Deploying Independent Appliances

This chapter explains how to deploy single independent appliances and independent HA pairs. Independent appliances run NIOS without the Grid upgrade and are deployed independently from a Grid. This chapter includes the following sections:

- **Independent Deployment Overview** on page 213
  - System Manager GUI on page 214
- **Deploying a Single Independent Appliance** on page 215
  - Method 1 - Using the LCD on page 216
  - Method 2 - Using the CLI on page 216
  - Method 3 - Using the Infoblox NIOS Startup Wizard on page 217
- **Configuration Example: Deploying a NIOS Appliance as a Primary DNS Server** on page 219
  - Cabling the Appliance to the Network and Turning On Power on page 220
  - Specifying Initial Network Settings on page 220
  - Specifying Appliance Settings on page 220
  - Defining a NAT Address on page 221
  - Enabling Zone Transfers on the Legacy Name Server on page 222
  - Importing Zone Data on an Independent Appliance on page 222
  - Designating the New Primary on the Secondary Name Server (at the ISP Site) on page 225
  - Configuring NAT and Policies on the Firewall on page 225
- **Deploying an Independent HA Pair** on page 226
  - Using the Infoblox NIOS Startup Wizard to Configure an HA Pair on page 226
- **Configuration Example: Configuring an HA Pair for Internal DNS and DHCP Services** on page 229
  - Cabling Appliances to the Network and Turning On Power on page 230
  - Specifying Initial Network Settings on page 231
  - Specifying Appliance Settings on page 231
  - Enabling Zone Transfers on page 233
  - Importing Zone Data on page 233
  - Defining Networks, Reverse-Mapping Zones, DHCP Ranges, and Infoblox Hosts on page 233
  - Defining Multiple Forwarders on page 236
  - Enabling Recursion on External DNS Servers on page 236
  - Modifying the Firewall and Router Configurations on page 237
Deploying Independent Appliances

- Enabling DHCP and Switching Service to the NIOS Appliance on page 238
- Managing and Monitoring on page 238
- Verifying the Deployment on page 239
  - Single Independent Appliance on page 239
  - Independent HA Pair on page 239
- Infoblox Tools for Migrating Bulk Data on page 240
**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 182.

*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 268.
  - Advantage: You do not need to change the IP address of the management system to connect to the NIOS appliance.

- **Method 3 – Using the Infoblox NIOS Startup Wizard**
  - Requirements: An HTTPS connection from your management system to the LAN1 port on the NIOS appliance.
  - Advantage: The wizard provides step-by-step guidance for changing not only the IP settings for the LAN1 port, but also changing the appliance host name and admin password, setting the system clock, and—if using NTP (Network Time Protocol)—enabling the NIOS appliance to be an NTP client.

Note that you can configure network settings using the Startup wizard any time after you have configured the appliance. To start the wizard, from System Manager, select the System tab, and then click System Properties -> Startup Wizard from the Toolbar.

After you configure the network settings on a single independent appliance, you can migrate data from legacy DNS and DHCP servers to the NIOS appliance. Several tools and methods are available for migrating data and configuration settings. For a list of the available options, see Infoblox Tools for Migrating Bulk Data on page 240.
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.

   ```plaintext
   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. For information about installing and cabling the appliance, refer to the user guide or installation guide that was shipped with the product.

**Method 3 – Using the Infoblox NIOS Startup Wizard**

When you first make an HTTPS connection to a NIOS appliance, the Infoblox NIOS Startup Wizard guides you through the deployment options and basic network settings. You can also change the password of the superuser (admin) and set up the system clock.

Note that you can configure network settings using the Startup wizard any time after you have configured the appliance. To start the wizard, from Grid Manager, select the System tab, and then click System Properties -> Startup Wizard from the Toolbar.

To make an HTTPS 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 37. 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 44.
3. Enter the default username and password (admin and infoblox) on the Grid Manager login page, and then click Login or press Enter. For information, see Logging in to the GUI on page 39.

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 226.

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 Creating a Login Banner on page 40.

3. Enter the default username and password (admin and infoblox) on the Grid Manager login page, and then click Login or press Enter. For information, see Logging in to the GUI on page 39.

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

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. Save the configuration and click **Restart** if it displays at the top of the screen.
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.
**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/](http://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. Save the configuration and click **Restart** if it displays at the top of the screen.

**Creating a Forward-Mapping Zone**

**Note:** To import zone data, you must first create a zone and save it.

1. To create an authoritative zone, from the Data Management tab, select the DNS tab -> Zones tab, and then click the Add icon -> Authoritative Zone.
2. In the Add Authoritative Zone wizard, select Add an authoritative forward-mapping zone.
3. Click Next and complete the following:
   - **Name:** Enter `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. Save the configuration and click **Restart** if it displays at the top of the screen.
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:

```plaintext
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:

```plaintext
set address dmz nsl 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 nsl any dns permit
set policy from untrust to dmz any mip(1.1.1.2) dns permit
set policy from dmz to untrust nsl ntp_server ntp permit
```

At this point, the new DNS server can take over DNS service from the legacy server. You can remove the legacy server and unset any firewall policies permitting traffic to and from 10.1.5.3.
Deploying an Independent HA Pair

To deploy an independent HA pair, you cable the HA and LAN1 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 182.

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 276 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 215 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 37.

   Several certificate warnings may appear during the login process because the preloaded certificate is self-signed and has the hostname www.infoblox.com, which may not match the destination IP address you entered in step 1. To stop the warning messages from occurring each time you log in to Grid Manager, you can generate a new self-signed certificate or import a third-party certificate with a common name that matches the FQDN (fully qualified domain name) of the appliance. For information, see `Creating a Login Banner` on page 40.

2. Enter the default username and password (admin and infoblox) on the Grid Manager login page, and then click `Login` or press Enter. For information, see `Logging in to the GUI` on page 39.

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.
Deploying Independent Appliances

— Select No to specify a date and time.
— Date: Enter the data in YYYY-MM-DD format. You can also click the calendar icon to select a date from the calendar widget.
— Time: Enter the time in HH:MM:SS AM/PM format. You can also click the clock icon to select a time from the drop-down list.

9. Click Next to view the summary of the configuration. Review the information and verify that it is correct. You can change the information you entered by clicking Previous to go back to a previous step.

10. Click Finish.

Configuring Node 2

1. Open an Internet browser window and enter https://<the IP address of the appliance> to make an HTTPS connection to the second node. For information about supported browsers, see Supported Browsers on page 37.
   Several certificate warnings may appear during the login process because the preloaded certificate is self-signed and has the hostname www.infoblox.com, which may not match the destination IP address you entered in step 1. To stop the warning messages from occurring each time you log in to Grid Manager, you can generate a new self-signed certificate or import a third-party certificate with a common name that matches the FQDN (fully qualified domain name) of the appliance. For information, see Creating a Login Banner on page 40.

2. Enter the default username and password (admin and infoblox) on the Grid Manager login screen, and then click Login or press Enter. For information, see Logging in to the GUI on page 39.

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>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP 10.1.4.10 (the address that the active node of the HA pair uses)</td>
<td></td>
</tr>
<tr>
<td>Node 1</td>
<td>Node 2</td>
</tr>
<tr>
<td>• LAN1 10.1.4.6</td>
<td>• LAN1 10.1.4.8</td>
</tr>
<tr>
<td>• HA 10.1.4.7</td>
<td>• HA 10.1.4.9</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 Creating a Login Banner on page 40.
3. Enter the default username and password (admin and infoblox) on the Grid Manager login page, and then click Login or press Enter. For information, see Logging in to the GUI on page 39.
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 222.
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 222.

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 222. 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 IPv4 Networks on page 643.

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, click the MAC Address field, and then enter the following:
   - MAC Address: 00:00:00:aa:aa:aa
4. Click Save & Close.
5. Follow steps 1 – 4 to modify hosts with the following information:
   - printer2
     - IP Address: 10.1.2.2
     - MAC Address: 00:00:00:bb:bb:bb
   - storage1
     - IP Address: 10.1.4.2
     - MAC Address: 00:00:00:dd:dd:dd
   - storage2
     - IP Address: 10.1.4.3
     - MAC Address: 00:00:00:ee:ee:ee
   - proxymail
     - IP Address: 10.1.4.4
     - MAC Address: 00:00:00:ff:ff:ff
   - proxyweb
     - IP Address: 10.1.4.5
     - MAC Address: 00:00:00:11:11:11
   - www
     - IP Address: 10.1.5.5
     - MAC Address: 00:00:00:55:55:55
   - mail
     - IP Address: 10.1.5.6
     - MAC Address: 00:00:00:66:66:66
   - ftp
     - IP Address: 10.1.5.7
     - MAC Address: 00:00:00:77:77:77
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. Save the configuration and click Restart if it displays at the top of the screen.

Each of the forwarders is assigned a random response time. The appliance sends the initial outbound query to the forwarder that has the lowest response time. If the first forwarder does not reply, the appliance tries the one with the next lowest random response time. The appliance adjusts and keeps track of the response times of the forwarders, and uses the quicker one for future queries. If the quicker forwarder does not respond, the appliance then uses another one.

Enabling Recursion on External DNS Servers

Because the HA pair forwards outbound queries to the two external DNS servers ns1.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. Save the configuration and click Restart if it displays at the top of the screen.

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.
Logs

The following are some useful information:

- Logs, as described in Monitoring the Appliance on page 867.
  - Audit Log – Contains administrator-initiated events.
  - System Log – Contains events related to hardware and software operations.
- DNS statistics, as described in Configuring DNS Services on page 441.
  - DNS Configuration – Contains DNS server settings for the Infoblox DNS server.
  - Zone Statistics – Contains the results of all DNS queries per zone.
- DHCP information, as described in Configuring DHCP Properties on page 587.
  - DHCP Configuration – Contains DHCP server settings and network, DHCP range, and host settings for the Infoblox DHCP server.
  - DHCP Leases – Contains a real-time record of DHCP leases.
  - DHCP Lease History - Contains an historical record of DHCP leases.
  - DHCP Statistics – Contains the number of currently assigned static and dynamic addresses, and the high and low watermarks per network.
  - Network Statistics – Contains the number of static hosts, dynamic hosts, and available hosts per network.

Verifying the Deployment

After you deploy a single independent appliance or HA pair, you can make an HTTPS connection to it, log in, and check its status.

Single Independent Appliance

From the Dashboard, check the appliance status in the System Status widget. For information, see Member Status (System Status) on page 89.

- 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 89.
   - 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 Bulk Data

Typically, the next step after cabling a single independent appliance to a network and configuring its network settings—or cabling two independent appliances to a network and configuring them as an HA pair—is to import data from legacy DNS, DHCP, and TFTP servers. Infoblox provides several tools to accomplish this:

- The CSV import feature allows you to import DNS, DHCP, and IPAM data through Grid Manager. You can add, overwrite, or merge data using this feature. The appliance updates the database based on import settings and the data you specify in the data files. From the Data Management tab of Grid Manager, you can access the Import Manager editor from which you start a data import. You can also export existing data to a CSV file. You can use this file to modify data, and then re-import the data into the database using the CSV import feature. For information, see About CSV Import on page 64.

- The Infoblox Data Import Wizard is a useful tool that simplifies the importation of DNS, DHCP and IPAM, and TFTP settings and data into a NIOS appliance. For large data sets, this option is an efficient approach. To download the Data Import Wizard, visit www.infoblox.com/import/.

- 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 385).
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 243
  - Changing Time and Date Settings on page 243
  - Changing Time Zone Settings on page 243
  - Monitoring Time Services on page 244
- Using NTP for Time Settings on page 245
  - Authenticating NTP on page 246
  - NIOS Appliance as NTP Client on page 248
  - Configuring a Grid to Use NTP on page 249
  - Configuring Grid Members to Use NTP on page 251
  - NIOS Appliance as NTP Server on page 252
  - Configuring a NIOS Appliance as an NTP Server on page 253
  - Monitoring NTP on page 255
- Scheduling Tasks on page 256
  - Scheduling Additions and Modifications on page 257
  - Scheduling Appliance Operations on page 257
  - Scheduling Deletions on page 257
  - Viewing Scheduled Tasks on page 258
  - Rescheduling Tasks on page 260
  - Guidelines for Upgrading, Backing Up, and Restoring the Database on page 261
- About Extensible Attributes on page 262
  - Configuring Extensible Attributes on page 263
  - Using Extensible Attributes on page 265
- Managing Security Operations on page 268
  - Enabling Support Access on page 268
  - Enabling Remote Console Access on page 268
  - Permanently Disabling Remote Console and Support Access on page 268
  - Restricting GUI/API Access on page 268
  - Enabling HTTP Redirection on page 268
  - Modifying the Session Timeout Setting on page 269
Managing Appliance Operations

- Disabling the LCD Input Buttons on page 269
- Configuring Security Features on page 269

- Ethernet Port Usage on page 271
  - Modifying Ethernet Port Settings on page 276

- Using the LAN2 Port on page 277
  - About NIC Redundancy on page 278
  - Configuring the LAN2 Port on page 280
  - Enabling DHCP on LAN2 on page 280
  - Enabling DNS on LAN2 on page 281

- Using the MGMT Port on page 282
  - Appliance Management on page 283
  - Grid Communications on page 285
  - DNS Services on page 287

- Setting Static Routes on page 289

- Enabling DNS Resolution on page 293

- Managing Licenses on page 294
  - Obtaining and Adding Licenses on page 294
  - Obtaining Temporary Licenses on page 295
  - Viewing Licenses on page 295
  - Backing Up Licenses on page 296
  - Removing Licenses on page 296

- Shutting Down, Rebooting, and Resetting a NIOS Appliance on page 297
  - Rebooting a NIOS Appliance on page 297
  - Shutting Down a NIOS Appliance on page 297
  - Resetting a NIOS Appliance on page 297

- Managing the Disk Subsystem on the Infoblox-2000-A and -4010 on page 299
  - About RAID 10 on page 299
  - Evaluating the Status of the Disk Subsystem on page 300
  - Disk Drive Front Panel LEDs on page 301
  - Replacing a Failed Disk Drive on page 302
  - Disk Array Guidelines on page 303

- Restarting Services on page 304
  - Canceling a Scheduled Restart on page 306
Managing Time Settings

You can define the date and time settings for your NIOS appliance using the Infoblox Appliance Startup Wizard. Alternatively, you can set the date and time of the appliance anytime after you first configure it if you did not do so using the startup wizard or if you need to change it if, for example, you move an appliance from a location in one time zone to a location in a different time zone. To set the date and time of the appliance, you can either manually enter the values or configure the appliance to synchronize its time with a public NTP server.

Changing Time and Date Settings

If you do not use the NTP service, you can set the date and time for a Grid.

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

To set the time and date for a Grid using the Grid Properties editor:

1. From the Grid tab, select the Grid Manager tab, expand the Toolbar and click Grid Properties -> Edit.
2. In the General tab of the Grid Properties editor, complete the following:
   - **Date:** Click the calendar icon to select a date or enter the date in YYYY-MM-DD format.
   - **Time:** Click the clock icon to select a time or enter the time in HH:MM:SS format. For afternoon and evening hours, use the integers 13-24.
3. Save the configuration and click Restart if it displays at the top of the screen.

**Note:** Changing the date and time resets the application and terminates the management session.

Changing Time Zone Settings

Whether you enable NTP (Network Time Protocol) or manually configure the date and time, you must always set the time zone manually. You can set the time zone for a Grid, which then applies to all members. If different members are in different time zones, you can choose the time zone that applies to most members at the Grid level, and then override the setting for the remaining members.

**Note:** Changing the time zone does not reset the application nor does it terminate the management session.

To set the time zone for a Grid or member:

1. **Grid:** From the Grid tab, select the Grid Manager tab, expand the Toolbar and click Grid Properties -> Edit.
   - **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. Save the configuration and click Restart if it displays at the top of the screen.
Monitoring Time Services

In a Grid, the Grid Master and its members use an internal NTP daemon to synchronize their time. It is not user-configurable and functions regardless of how you set the time on the Grid Master. The Detailed Status panel contains an NTP Synchronization icon so you can monitor the internal NTP daemon that runs within a Grid to ensure the time among its members is synchronized.

To display the Detailed Status panel, from the Grid tab, select the Grid Manager tab -> Members tab -> Grid member check box, and then click the Detailed Status icon in the table toolbar of the Members panel.

The following are descriptions of the NTP status icons in the Detailed Status panel:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="green.png" alt="Green" /></td>
<td>Green</td>
<td>The NTP service is running properly.</td>
</tr>
<tr>
<td><img src="yellow.png" alt="Yellow" /></td>
<td>Yellow</td>
<td>The appliance is synchronizing its time.</td>
</tr>
<tr>
<td><img src="red.png" 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 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.
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.

Authenticate 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.
Using NTP for Time Settings

- A: The key is a DES key written as a 1-8 character ASCII string.
- N: The key is a 64-bit hexadecimal number in NTP format. It is the same as the S format, but the bits in each octet have been rotated one bit right so the parity bit is in the high order bit of the octet. You must specify leading zeros and odd parity must be maintained.

- Key String: The key data used to calculate the MAC. The format depends on the Key Type you select.

When the NTP client initiates a request for time services to the NTP server, it creates the MAC by using the agreed upon algorithm to compress the message and then encrypts the compressed message (which is also called a message digest) with the secret key. The client appends the MAC to the message it sends to the NTP server. When the NTP server receives the message from the client, it performs the same procedure on the message — it compresses the message it received, encrypts it with the secret key and generates the MAC. It then compares the MAC it created with the MAC it received. If they match, the server continues to process and respond to the message. If the MACs do not match, the receiver drops the message.

Figure 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 246.

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

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 250.

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.

2. Click the Add icon in the NTP Keys section and enter the following information.

   — Key Number: A positive integer that identifies a key.

   — Type: Specifies the key format and the algorithm used to calculate the MAC (message authentication code) of a message.

      — MD5 in ASCII format (M): The key is a 1-31 character ASCII string using MD5 (Message Digest).

      — DES in hex format (S): The key is a 64-bit hexadecimal number in DES (Data Encryption Standard) format. The high order 7 bits of each octet form the 56-bit key, and the low order bit of each octet is given a value so that the octet maintains odd parity. You must specify leading zeros so the key is exactly 16 hexadecimal digits long and maintains odd parity.

      — DES in ASCII format (A): The key is a DES key written as a 1-8 character ASCII string.

      — DES in NTP format (N): The key is a 64-bit hexadecimal number in NTP format. It is the same as the S format, but the bits in each octet have been rotated one bit right so the parity bit is in the high order bit of the octet. You must specify leading zeros and odd parity must be maintained.

   — String: The key data used to calculate the MAC. The format depends on the Key Type you select.

3. Click Save to save the entry and keep the editor open so you can enable the 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 293.
   - **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 249.
5. Save the configuration and click Restart if it displays at the top of the screen.
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 293.
   — 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).
   — Authentication Key: Select a key that you previously entered, and then click OK. For information, see Adding NTP Authentication Keys on page 249.
6. Save the configuration and click Restart if it displays at the top of the screen.

Managing External NTP Servers

You can specify multiple NTP servers for failover purposes. The NIOS appliance attempts to connect to the NTP servers in the order they are listed. A Grid member uses the Grid Master as the NTP server when it cannot reach any of its external NTP servers.

You can change the order of the list by selecting an NTP server and dragging it to its new location or by clicking the up and down arrows. You can add and delete servers and modify their information as well.
NIOS 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.

Figure 7.4 Grid Members as NTP Servers

To configure a NIOS appliance as an NTP server, perform the following tasks:

- Enable the appliance as an NTP server.
- Enable authentication between the appliance and its NTP clients.
- Optionally, specify which clients can access the NTP service of the appliance.
- Optionally, specify which clients can use ntpq to query the appliance.
Configuring a NIOS Appliance as an NTP Server

You can configure a Grid member—including the Grid Master—or an independent appliance or HA pair to function as an NTP server. When you enable a NIOS appliance to function as an NTP server, you can enable authentication between a NIOS appliance functioning as an NTP server and its NTP clients. When you enable authentication, you must specify the keys that the appliance and its clients must use for authentication. In a Grid, you can enter NTP authentication keys at the Grid level so that all the members can use them to authenticate their clients. You can also enter keys at the member level, if you want that member to use different keys from those set at the Grid level. After you enter the keys, you can download the key file and distribute the file to the NTP clients.

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 253.
- Optionally, define NTP access control. For information, see Defining NTP Access Control on page 254.

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 249.
5. Save the configuration and click Restart if it displays at the top of the screen.

After you enter the authentication keys, you can download the key file (usually called ntp.keys) and distribute it to NTP clients as follows:

1. Grid: From the Grid tab, select the Grid Manager tab.
   - Member: From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box.
2. Expand the Toolbar and click NTP -> Download NTP Keys.
3. In the Opening ntp.keys dialog box, save the file, and then click OK.
4. Distribute this to the NTP clients using a secure transport.
Defining NTP Access Control

The NTP access control list specifies which clients can use a NIOS appliance as an NTP server. If you do not 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. Save the configuration and click Restart if it displays at the top of the screen.
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 34, Monitoring with SNMP, on page 893.

<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 150.
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. Save the configuration and click Restart if it displays at the top of the screen.

Scheduling Appliance Operations

The appliance supports the scheduling of the following operations:

- Network discoveries—For information, see Chapter 32, Network Discovery, on page 843.
- Service restarts—For information, see Restarting Services on page 304.

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 259.

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 258.

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 260.

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 260.

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 258. 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 261.
- 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. Save the configuration and click Restart if it displays at the top of the screen.
To reschedule a task in an editor:
1. Navigate to the object with a scheduled task that you want to reschedule.
2. Click the scheduled task icon next to the object.
3. **For modification:** In the editor, click the Schedule icon at the top of the editor. In the Schedule Change panel, modify the date, time, and time zone. You can also select **Now** to execute the task upon saving the entry. **For deletion:** In the Schedule Deletion dialog box, modify the date, time, and time zone. You can also select **Delete Now** to delete the object upon clicking **Delete Now**. The appliance puts the deleted object in the Recycle Bin, if enabled.
4. Save the configuration and click **Restart** if it displays at the top of the screen.

### 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. Save the configuration and click **Restart** if it displays at the top of the screen.

### 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 create attributes such as Device Type, Location, Owner, and Manufacturer, and associate them with hosts. Each attribute tracks specific information about the device. These details provide valuable information for network, asset, and service management.

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 50.

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 265.

You can also create your own attributes, as described in Adding Extensible Attributes on page 263.

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 881.

5. Save the configuration and click **Restart** if it displays at the top of the screen.

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.
You can do the following in this panel:

- Sort the displayed data in ascending or descending order by column.
- Use filters and the **Go to** function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the **Go to** field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see **Using Quick Filters** on page 57.
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see **Modifying Data in Tables** on page 52.
- Add or delete extensible attributes.
- Print or export the data.

**Modifying Extensible Attributes**

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

To modify an extensible attribute:

1. 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 263.
5. Save the configuration and click **Restart** if it displays at the top of the screen.

**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.

To delete all attributes:
1. Click the Attribute Name check box.
2. Click the Delete icon.

Note: You can delete only attributes that are not required. If you have one or more required attributes, you cannot use the delete all function.

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

Editing Multiple Extensible Attribute Values

You can also manage the extensible attributes of multiple objects at the same time. For example, you can select several zones, and view and modify their extensible attributes all at once.

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 50.
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 62.
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,

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 Redirection

You can enable the NIOS appliance to redirect administrative connection requests using HTTP to the secure HTTPS protocol. When you disable redirection, the NIOS appliance ignores any administrative connection requests not using HTTPS. By default, the NIOS appliance does not redirect HTTP connection requests to HTTPS. When you change this setting, the application restarts and your management session terminates.
Modifying the Session Timeout Setting

You can set the length of idle time before an administrative session to the Infoblox GUI times out. The default timeout value is 600 seconds (10 minutes).

If a user does not interact with the application for the specified time, the appliance displays a message that a timeout has occurred. Click OK to restart the GUI session.

**Note:** If you change the session timeout value, the new setting takes effect only after you log out and log back in.

Disabling the LCD Input Buttons

By default, the LCD input function is enabled, which allows you to use the LCD buttons on the front panel of a NIOS appliance to change the 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. Save the configuration and click **Restart** if it displays at the top of the screen.
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-A, 550-A, -1050-A, -1550-A, -1552-A, -1852-A, -2000-A, and -4010 appliances. For information about how to use the LAN2 port, see *Using the LAN2 Port* on page 277.
- **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 273 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 273.

**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>LAN1</td>
<td>LAN1</td>
<td>LAN1</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>LAN1</td>
<td>LAN1</td>
<td>LAN1</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>LAN1 or MGMT</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>Yes</td>
<td>Active</td>
<td>Enabled</td>
<td>VIP on HA</td>
<td>VIP on HA</td>
<td>MGMT</td>
<td>MGMT</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>Yes</td>
<td>Passive</td>
<td>Enabled</td>
<td>LAN1</td>
<td>–</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>Single Independent</td>
<td>No</td>
<td>–</td>
<td>Enabled</td>
<td>–</td>
<td>LAN1 or MGMT</td>
<td>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>VIP on HA</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>Indicates 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 DDNS 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</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>DNS Queries</td>
<td>Client</td>
<td>LAN1, LAN2, VIP, or broadcast on NIOS appliance</td>
<td>6 TCP</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>
<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>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></td>
<td>1814</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 client</td>
<td>1 ICMP Type 0</td>
<td>-</td>
<td>-</td>
<td>Required for response from ICMP echo request (ping).</td>
</tr>
<tr>
<td>ICMP Echo Request</td>
<td>VIP, LAN1, LAN2, or MGMT, or client</td>
<td>VIP, LAN1, LAN2, or MGMT, or client</td>
<td>1 ICMP Type 8</td>
<td>-</td>
<td>-</td>
<td>Required to send pings and respond to the Windows-based traceroute tool.</td>
</tr>
<tr>
<td>ICMP TTL Exceeded</td>
<td>Gateway device (router or firewall)</td>
<td>Windows client</td>
<td>1 ICMP Type 11</td>
<td>-</td>
<td>-</td>
<td>Gateway sends an ICMP TTL exceeded message to a Windows client, which then records router hops along a data path.</td>
</tr>
<tr>
<td>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 -&gt; 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 -&gt; 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>17 UDP</td>
<td>1024 -&gt; 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>17 UDP</td>
<td>1024 -&gt; 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>6 TCP</td>
<td>1024 -&gt; 65535</td>
<td>22</td>
<td>Administrators can make an SSHv2 connection to the LAN1, LAN2, VIP, or MGMT port Optional for management</td>
</tr>
<tr>
<td>Syslog</td>
<td>LAN1, LAN2, or MGMT of NIOS appliance</td>
<td>syslog server</td>
<td>17 UDP</td>
<td>1024 -&gt; 65535</td>
<td>514</td>
<td>Required for remote syslog logging</td>
</tr>
<tr>
<td>Traceroute</td>
<td>LAN1, LAN2, or UNIX-based appliance</td>
<td>VIP, LAN1, LAN2, or MGMT, or client</td>
<td>17 UDP</td>
<td>1024 -&gt; 65535</td>
<td>33000 -&gt; 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>17 UDP</td>
<td>1024 -&gt; 65535</td>
<td>69, then 1024 -&gt; 63999</td>
<td>For contacting a TFTP server during database and configuration backup and restore operations</td>
</tr>
<tr>
<td>VRRP</td>
<td>HA IP on the active node of HA pair</td>
<td>Multicast address 224.0.0.18</td>
<td>112 VRRP</td>
<td>802</td>
<td></td>
<td>For periodic announcements of the availability of the HA node that is linked to the VIP. The nodes in the HA pair must be in the same subnet.</td>
</tr>
<tr>
<td>HTTP</td>
<td>Management System</td>
<td>VIP, LAN1, or MGMT</td>
<td>6 TCP</td>
<td>1024 -&gt; 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>6 TCP</td>
<td>1024 -&gt; 65535</td>
<td>443</td>
<td>Required for administration through the GUI</td>
</tr>
</tbody>
</table>
Managing Appliance Operations

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 282.

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

   **Note:** The port settings on the connecting switch must be identical to those you set on the NIOS appliance.
Using the LAN2 Port

Note: This feature is not supported on vNIOS Grid members for Riverbed.

The LAN2 port is a 10/100/1000Base-T Ethernet connector on the front panel of Infoblox-250-A, -550-A, -1050-A, -1550-A, -1552-A, -1852-A, -2000-A, and -4010 appliances. By default, the LAN2 port is disabled and the appliance uses the LAN1 port (and HA port when deployed in an HA pair). Before you can enable and configure the LAN2 port on a Grid member, you must first configure the member and join it to the Grid. You must also have read/write permission to the Grid member on which you want to enable the port. When you enable the LAN2 port and SNMP, the appliance sends traps from this port for LAN2 related events.

You can configure the LAN2 port in different ways. You can enable the 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. Alternatively, you can configure the LAN2 port on a different IP network than LAN1, and enable the LAN2 port to provide DNS and DHCP services. For information about these features, see the following sections:

- For information about the LAN2 failover feature, see About NIC Redundancy on page 278.
- For information about configuring the LAN2 port, see Configuring the LAN2 Port on page 280.
- For information about enabling the LAN2 port to provide DHCP services, see Enabling DHCP on LAN2 on page 280.
- For information about enabling the LAN2 port to provide DNS services, see Enabling DNS on LAN2 on page 281.

Note that you cannot use the LAN2 port to access the GUI and the API, or to connect to the Grid. This can impact the ability of other appliances, such as the NetMRI and PortIQ appliances, to communicate with the Grid Master.
Managing Appliance Operations

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 single or HA independent appliances and Grid members.

Figure 7.8 Using the LAN2 Failover Feature

![Diagram showing the connections between Grid Master, LAN1, MGMT, LAN2, Private Network, and Public Network. LAN1 and LAN2 share the LAN1 IP address, and clients send service requests and replies to the LAN1 IP address. Failover is active for IPv4 or IPv6 addresses.]
Before you enable NIC redundancy, ensure that both LAN1 and LAN2 are enabled. 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 **LAN (Failover)**.
   
   Grid Manager adds the **LAN (Failover)** entry to the table. The **Address** field is blank and 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 displays at the top of the screen.
   
   The **Detailed Status** panel displays the status of both the LAN1 and LAN2 ports. In an HA pair, both nodes display the port information when NIC redundancy is enabled.
Managing Appliance Operations

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 LAN2 port.
   - Port Settings: Choose the connection speed that you want the port to use. You can also choose the duplex setting. Choose Full for concurrent bidirectional data transmission or Half for data transmission in one direction at a time. Select Automatic to instruct the 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. Save the configuration and click Restart if it displays at the top of the screen.

The Detailed Status panel displays the status of the LAN2 port. In an HA pair, only the active node displays the LAN2 information.

Enabling DHCP on LAN2

You can configure an appliance to provide DHCP 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. Save the configuration and click Restart if it displays at the top of the screen.
Enabling DNS on LAN2

If you enable DNS on an appliance, it always serves DNS on the LAN1 port. Optionally, you can configure the appliance to provide DNS services through the LAN2 port as well. For example, the appliance can provide DNS services through the LAN1 port for internal clients on a private network, and DNS services through the LAN2 port for external clients on a public network.

After you configure the LAN2 port, you can enable DNS services on the LAN2 port as follows:

1. From the Data Management tab, select the DNS tab -> Members tab -> Grid_member check box, and then click the Edit icon.
2. In the General -> Basic tab of the Member DNS Configuration editor, do the following:
   - 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. Save the configuration and click Restart if it displays at the top of the screen.
5. Click Restart to restart services.
Managing Appliance Operations

Using the MGMT Port

**Note:** This feature is not supported on vNIOS Grid members for Riverbed.

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

- **Appliance Management** on page 283
- **Grid Communications** on page 285
- **DNS Services** on page 287

For information about what types of traffic qualify as appliance management, Grid communications, and DNS services, see *Table 7.3* on page 273.

**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.

*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.

<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>

* 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.

*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). Figure 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.

3. 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.

4. In the **Network** -> **Advanced** tab, make sure that the **Enable VPN on MGMT Port** check box is not selected.

5. Save the configuration and click **Restart** if it displays at the top of the screen.

6. Log out of Grid Manager.

7. Cable the MGMT port to your management system or to a switch or router to which your management system can also connect.

8. 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.

9. Open an Internet browser window and enter the IP address of the MGMT port as follows: `https://<IP address of MGMT port>`

10. Log in to Grid Manager.

11. 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.

*Figure 7.10 Grid Communications*

---

The private network (10.1.1.0/24) is reserved for Grid communications between the Grid Master and all Grid members, and for appliance management between the management system and the Grid Master.

The Grid Master and master candidate connect to the private network using a VIP on their HA ports.

The common Grid members connect to the public network through their MGMT ports*. They connect to the public network through their LAN and HA ports (using a VIP).

The common Grid members use the public network (1.1.1.0/24) for DNS and DHCP services.

* 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 282.

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. Save the configuration and click Restart if it displays at the top of the screen.
   The master communicates the new port settings to the member, which immediately begins using them. The member stops using its LAN port for Grid communications and begins using the MGMT port.
9. To confirm that the member still has Grid connectivity, check that the status icons for that member are green on the Detailed Status and Grid panels.
DNS Services

You can configure a single independent appliance or single Grid member to provide DNS services through the MGMT port in addition to the LAN port. For example, the appliance can provide DNS services through the MGMT port for internal clients on a private network, and DNS services through the LAN port for external clients on a public network. While providing DNS services on the MGMT port, you can still use that port simultaneously for appliance management. Figure 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 282.

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

To see that the appliance now also serves DNS on the MGMT port:

1. From the **Data Management** tab, select the **DNS** tab -> **Members** tab -> Grid_member check box.
2. Expand the Toolbar and click **View** -> **View DNS Configuration**.
3. Check that the IP address of the MGMT port appears in the address match list in the listen-on substatement.
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 289, the appliance is in the DMZ behind a firewall and connects to the rest of the network through the DMZ interface on the firewall. For example, when hosts send DNS queries from the Internet and the internal network to the appliance and when the appliance replies to those hosts, the firewall takes care of all the routing.

Note: This feature is not supported on vNIOS Grid members for Riverbed.

Figure 7.12 Single Default Route

The default route points all traffic from the LAN or LAN1 port on the NIOS appliance to the DMZ interface (1.2.2.1) on the firewall.

The appliance responds to all queries from the Internet and internal network by sending its responses to the DMZ interface (1.2.2.1) on the firewall.

The appliance only needs a single default route to the firewall. The firewall then routes the traffic where it needs to go.

When the 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 290, 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.

**Figure 7.14 Properly Routed DNS Replies**

The default route points all traffic from the NIOS appliance to the DMZ interface (1.2.2.1) on firewall-1.

**Default route:**
- **Network:** 0.0.0.0
- **Netmask:** 0.0.0.0
- **Gateway:** 1.2.2.1

DNS queries from the Internet reach the appliance through firewall-1, and the appliance sends its replies back through firewall-1.

DNS queries from the internal network reach the appliance through firewall-2, but because there is only one default route, the appliance erroneously sends DNS replies to the DMZ interface (1.2.2.1) on firewall-1.

A second route on the appliance points traffic destined for 10.1.1.0/24 to the DMZ interface (1.2.2.2) on firewall-2.
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

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.

Route Tables on the NIOS appliance

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
10.1.2.0/24 dev eth0  proto kernel  scope link  src 10.1.2.5
default via 1.2.2.1 dev eth1
```

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.

The two static routes direct traffic from the NIOS appliance:

- From the LAN port (eth1, 1.2.2.5) through the gateway at 1.2.2.2 to the 10.1.1.0/24 subnet.
- From the MGMT port (eth0, 10.1.2.5) through the gateway at 10.1.2.1 to the 10.1.3.0/24 subnet.
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. Save the configuration and click Restart if it displays at the top of the screen.
Enabling DNS Resolution

You can specify a network server to perform domain name queries and specify up to two name servers for resolving a DNS name. You can specify the IP address of a preferred name server and that of an alternate name server, plus use a search list for performing partial name resolution.

To enable DNS resolution for 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. Save the configuration and click **Restart** if it displays at the top of the screen.
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 with the Grid license, you must contact Infoblox Technical Support and follow the procedures in Viewing Licenses on page 295.

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. For more information, refer to the Infoblox Installation Guide for vNIOS Software on 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. Note that the DNS and DHCP services are disabled by default. Once you have obtained licenses for these services, start the services after you complete the configuration.

- **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 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)**.

   The appliance validates the license and adds it to the table. Close the browser window and log in to the Infoblox GUI. If you are activating licenses for an HA pair, you must follow this procedure for both nodes.

**Note:** To transfer licenses between vNIOS on VMware appliances, refer to the Infoblox Installation Guide for vNIOS Software on VMware.
Managing Licenses

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.

In this panel, you can use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches. You can also create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 57.

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.
   - **Address**: The IP address of the appliance.
   - **Hardware ID**: The unique hardware ID of the appliance. The ID is highlighted in red if the license on the appliance was removed.
   - **Type**: The type of license installed.
   - **Type Context**: Depending on the license type, this field displays the attribute, such as Model and Connector, that the license controls. For example, when you purchase an IF-MAP Federation license with a limited number of federation connectors, this field displays Connector. This field is blank if the license does not control any attribute type. This field can display one of the following:
     - **Model**: Indicates that this vNIOS license supports a specific vNIOS virtual appliance model. This includes the supported virtual appliance for the IF-MAP Starter Kit. The model supported is displayed in the Type Details field.
     - **Connector**: Indicates that this IF-MAP Federation license supports a specific number of IF-MAP federation connectors. The number of federation connectors supported is displayed in the Type Details field.
   - **Type Details**: Information about the attribute type that the license monitors. This field can display the following information for each attribute:
     - **Model**: The model of the vNIOS virtual appliance, such as IB-VM-550 or IB-VM-1050.
     - **Connector**: The number of federation connectors that the IF-MAP Federation license supports.
     - **Expiration**: The expiration date of the license.
     - **Replaced Hardware ID**: The hardware ID of the appliance whose license was removed.
Managing Appliance Operations

Back up Licenses

You can back up the licenses installed on the appliance, in case you need to re-install them at a later time. Infoblox recommends backing up the licenses before removing any of them.

When you back up the licenses, 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 re-install them at a future time.

This should be used with great caution as it can render an appliance unusable if the wrong license is removed.

To remove a license:

1. From the Grid tab, select the Licenses tab.
2. Select the license and click the Delete icon.
   - Check the license that you are about to remove. Note that removing the wrong license can render an appliance unusable.
3. Click Yes when the confirmation dialog appears.
4. Close the browser window and log in to the Infoblox GUI.
Shutting Down, Rebooting, and Resetting 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 298
- Resetting a NIOS Appliance to Factory Settings on page 298
- Resetting the NIOS Appliance to Factory Settings and Removing Licenses on page 298
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`
Among its many features, the Infoblox-2000-A and Infoblox-4010 use a RAID (Redundant Array of Independent Disks) 10 array to provide the optimum mix of high database performance and redundant data storage with recovery features in the event of disk failures. The disk array is completely self managed. There are no maintenance or special procedures required to service the disk subsystem.

Caution: Never remove more than one disk at a time from the array. Removing two or more disks at once can cause an array failure and result in an unrecoverable condition. You should replace only one disk at a time, using a replacement disk from Infoblox. For information, see Replacing a Failed Disk Drive on page 302.

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-A or -4010, it is best to think of the disk subsystem as a single, integrated unit with four components, rather than four independent disk drives. For information, see Evaluating the Status of the Disk Subsystem on page 300.
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-A or 4010 using the command:

```
Infoblox > show hardware_status
POWER:    Power OK
Fan1:     7258 RPM
Fan2:     6887 RPM
Fan3:     7258 RPM
CPU1_TEMP: +20.0 C
CPU2_TEMP: +24.0 C
SYS_TEMP:    +35 C
RAID_ARRAY: OPTIMAL
RAID_BATTERY: OK READY Yes 103 HOURS
```

The **Detailed Status** panel provides a detailed status report on the appliance and service operations. To see a detailed status report:

- From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box -> Detailed Status icon in the table toolbar.

After displaying the **Detailed Status** panel, you can view the status of the selected Grid member. For more information on the **Detailed Status** panel, see [Viewing Status](#) on page 868.

The RAID icons indicate the status of the RAID array on the Infoblox-2000-A and 4010.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green" /></td>
<td>Green</td>
<td>The RAID array is in an optimal state.</td>
</tr>
<tr>
<td><img src="image" alt="Yellow" /></td>
<td>Yellow</td>
<td>A new disk was inserted and the RAID array is rebuilding.</td>
</tr>
<tr>
<td><img src="image" alt="Red" /></td>
<td>Red</td>
<td>The RAID array is degraded. At least one disk is not functioning properly. The GUI lists the disks that are online. Replace only the disks that are offline.</td>
</tr>
</tbody>
</table>

The appliance also displays the type of each disk. In the event of a disk failure, you must replace the failed disk with one that is qualified and shipped from Infoblox and has the same disk type as the rest of the disks in the array. The disk type of the Infoblox-2000-A can be one of the following:

- IB-Type 1: Infoblox supported disk type
- IB-Type 2: Infoblox supported disk type
- Unk: Unknown disk type that Infoblox does not support

Infoblox-4010 uses only the IB-Type 3 disk type. All disk drives in the array must have the same disk type for the array to function properly. You can have either IB-Type 1, IB-Type 2, or IB-Type 3, but you cannot mix both in the array. When you have a mismatched disk in the array, you must promptly replace the disk with a replacement disk from Infoblox to avoid operational issues.
Disk Drive Front Panel LEDs

The disk drives of the Infoblox-2000-A are located on the right side of the appliance front panel. To the right of each drive, there is an LED that displays the status of each drive. The front panel LCD scrolls and displays the disk array status every 20 seconds. Table 7.5 lists the disk drive LEDs.

Table 7.5 Infoblox-2000-A Disk Drive LEDs

<table>
<thead>
<tr>
<th>LED Color</th>
<th>Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Disk operating normally</td>
<td>None</td>
</tr>
<tr>
<td>Yellow</td>
<td>Disk read/write activity</td>
<td>Disk is functioning normally or is synchronizing if recently inserted.</td>
</tr>
<tr>
<td>Dark</td>
<td>Disk has failed or not inserted</td>
<td>Verify the failure in the GUI or CLI. Remove the disk and replace with a functional disk drive. Note that the drive rebuilds with its twin.</td>
</tr>
</tbody>
</table>

The disk drives of the Infoblox-4010 are located on the appliance front panel. To the right of each drive, two LEDs display connection and activity status. Table 7.6 lists the disk drive LED combinations and the states they represent.

Table 7.6 Infoblox-4010 Disk Drive LED Combinations

<table>
<thead>
<tr>
<th>Online/Activity LED (Green)</th>
<th>Fault/UID LED (Amber/Blue)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On, off, or blinking</td>
<td>Alternating amber and blue</td>
<td>The drive has failed, or it has received a predictive failure alert; it also has been selected by a management application.</td>
</tr>
<tr>
<td>On, off, or blinking</td>
<td>Steadily blue</td>
<td>The drive is operating normally.</td>
</tr>
<tr>
<td>On</td>
<td>Amber, blinking regularly (1 Hz)</td>
<td>The drive has received a predictive failure alert. Replace the drive as soon as possible.</td>
</tr>
<tr>
<td>On</td>
<td>Off</td>
<td>The drive is online but it is not currently active.</td>
</tr>
<tr>
<td>Blinking regularly (1Hz)</td>
<td>Off</td>
<td>Do not remove the drive. The drive is rebuilding. Removing the drive may terminate the current operation and cause data loss.</td>
</tr>
<tr>
<td>Blinking irregularly</td>
<td>Amber, blinking regularly (1 Hz)</td>
<td>The drive is active, but it has received a predictive failure alert. Replace the drive as soon as possible.</td>
</tr>
<tr>
<td>Blinking irregularly</td>
<td>Off</td>
<td>The drive is active and operating normally.</td>
</tr>
<tr>
<td>Off</td>
<td>Steadily amber</td>
<td>A critical fault condition has been identified for this drive, and the controller has placed it offline. Replace the drive as soon as possible.</td>
</tr>
<tr>
<td>Off</td>
<td>Amber, blinking regularly (1 Hz)</td>
<td>The drive has received a predictive failure alert. Replace the drive as soon as possible.</td>
</tr>
<tr>
<td>Off</td>
<td>Off</td>
<td>The drive is offline, a spare, or not configured as part of an array.</td>
</tr>
</tbody>
</table>
Replacing a Failed Disk Drive

The Infoblox-2000-A and -4010 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. Make sure you have identified the correct drive.

   **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 304
- Restarting Member Services on page 305

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 881.

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.

   **Impacted 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 258.

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 261.
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 308
  - Configuring the TFTP Service on page 309
  - Configuring the FTP Service on page 309
  - Configuring the HTTP Service on page 310
  - Configuring Access Control Lists on page 310
  - Modifying Access Control Lists on page 311

- **Monitoring File Distribution Services** on page 312
  - Starting and Stopping File Distribution Services on page 312
  - Monitoring File Distribution Services on page 312

- **Managing Files and Directories** on page 313
  - Configuring File Distribution Storage Settings on page 313
  - Adding Directories on page 313
  - Modifying Directories on page 313
  - Uploading Files on page 314
  - Viewing Directories on page 314
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 or a 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 312.
- Modify storage space for file distribution, as described in Configuring File Distribution Storage Settings on page 313.
- Upload files to the appliance, as described in Uploading Files on page 314.
- View current files, as described in Viewing Directories on page 314.
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 310.

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

After you configure the TFTP service, you must enable the service to allow file distribution access. For information, see Starting and Stopping File Distribution Services on page 312.

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 310.

3. Save the configuration and click Restart if it displays at the top of the screen.
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 Redirection on page 268. For information on how to specify the MGMT port for HTTP, see Using the MGMT Port on page 282.

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 310.
3. Save the configuration and click Restart if it displays at the top of the screen.

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

**Modifying Access Control Lists**

1. From the **Data Management** tab, select the **File Distribution** tab ->**Members** tab ->**member** check box, and then click the Edit icon.

2. In the **Member File Distribution Properties** editor, select the tab of the service to which the list belongs.

3. In the **Allow file transfers from** section, modify the fields as described in *Configuring Access Control Lists* on page 310.

You can also do the following:

- Add a new permission. For information, see *Configuring Access Control Lists* on page 310.
- 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 312.
- Monitor the current status of the services, as described in Monitoring File Distribution Services on page 312.

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 313.
- Create a directory structure for file distribution, as described in Adding Directories on page 313.
- Upload files to the appliance, as described in Uploading Files on page 314.
- View the uploaded files, as described in Viewing Directories on page 314.

Configuring File Distribution Storage Settings

The maximum storage space for distributed files is five gigabytes on a Grid with NIOS appliances 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. Save the configuration and click Restart if it displays at the top of the screen.

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 313.

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 120.
4. Save the configuration and click Restart if it displays at the top of the screen.
You can also select a directory and click the Delete icon to delete it.

Note: When you delete a directory, the appliance automatically removes all its contents 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 313.

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 168.

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.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 57.
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables on page 52.
- Print and export the information in this panel.
- Add a directory or a file. For information, see Adding Directories on page 313 and Uploading Files on page 314.
- Open and edit a directory. For information, see Modifying Directories on page 313.
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:

- **About Upgrades** on page 316
  - Adding Upgrade Groups on page 317
  - Modifying Upgrade Groups on page 318
  - Viewing Upgrade Groups on page 318
  - Deleting Upgrade Groups on page 319
- **Viewing Software Versions** on page 320
- **Upgrading NIOS Software** on page 320
  - Uploading NIOS Software on page 321
  - Uploading NIOS Software on page 321
  - Distributing Software Upgrade Files on page 321
  - Managing Distributions on page 323
  - Testing Software Upgrades on page 324
  - Performing Software Upgrades on page 325
  - Monitoring Distribution and Upgrade Status on page 330
- **Downgrading Software** on page 331
- **Reverting to the Previously Running Software Version** on page 332
- **Backing Up and Restoring Configuration Files** on page 332
  - Backing Up Files on page 332
  - Automatically Backing Up Data Files on page 333
  - Manually Backing Up Data Files on page 335
  - Downloading Backup Files on page 335
  - Restoring Backup Files on page 336
  - Downloading Backup Files from a Different Appliance on page 337
- **Downloading Support Bundles** on page 338
About Upgrades

Infoblox frequently releases updated NIOS software. Contact Infoblox Technical Support to learn which file name to use when downloading a new upgrade file, or watch your email for periodic notifications that a new software upgrade is available. To get the latest upgrade, your local network must be capable of downloading a file from the Internet. For information about how to upgrade, see Upgrading NIOS Software on page 320.

You can upgrade an appliance to a specific release if the current release on your appliance supports the upgrade path. For information about the upgrade and revert paths of a specific release, refer to the latest release notes at http://www.infoblox.com/en/support/support-center-login.html. Depending on whether there are database schema changes between the existing and upgrade releases, the appliance can perform either a lite or full upgrade. For information, see Lite Upgrades and Full Upgrades.

You can schedule certain upgrades for a grid. Scheduling an upgrade can minimize network and operational outages, especially when grid members are spanned across different time zones. You can also arrange the upgrade to happen during non-peak hours for specific members to avoid overloading the network traffic. When you schedule an upgrade, you can schedule to update all grid members at the same time or at different times. Depending on the configuration of your grid and the software version that is currently running in the grid, you can also schedule your upgrades for different members over a period of time. For information about scheduling an upgrade, see Scheduling Upgrades on page 325.

Based on your network requirements and topology, you can organize your members into upgrade groups so these members can be upgraded at the same time. For information about upgrade groups, see About Upgrades on page 316.

Lite Upgrades

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. Whenever possible, the appliance uses the lite upgrade mode to speed up the upgrade process. You can schedule a lite upgrade. Note that the appliance disables the testing function for lite upgrades because you do not need to test a lite upgrade for any database translation. For information about scheduling an upgrade, see Scheduling Upgrades on page 325.

Full Upgrades

A full upgrade occurs when there are database schema changes between the existing and upgrade versions. In general, when you upgrade to a major release, you are performing a full upgrade. Depending on the upgrade and revert paths that your existing release supports, you may or may not be able to schedule a full upgrade. Infoblox supports the following full upgrades:

- **Full upgrades that can be scheduled**: This upgrade allows for member-to-master replication of data. In this type of full upgrade, dynamic DNS or DHCP updates that occur on the member are forwarded to the grid master. Any configuration changes made through the grid master are forwarded to the member after the upgrade process is completed. You can schedule this type of full upgrade, with some limitations. For information about the limitations, see Guidelines for Scheduling Full Upgrades on page 326.

- **Full upgrades that cannot be scheduled**: This upgrade does not allow for replication of data between the grid master and members. You cannot schedule this type of full upgrade. All members in the grid must be upgraded at the same time.

When you schedule a full upgrade, you can arrange for different members and upgrade groups to be upgraded at different times over a period of nine days. For information about scheduling an upgrade, see Scheduling Upgrades on page 325.
Managing Upgrade Groups

To minimize the impact of grid upgrades on your system operations, you can organize members into upgrade groups and schedule their software distributions. This is useful, for example, in a large grid spanning multiple time zones where there are fluctuating network and downtime considerations at various locations. Note that you can also schedule their upgrades, depending on the existing releases and their upgrade paths. For information about the different upgrade methods, see About Upgrades on page 316.

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 318.

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 318.
- View upgrade group information, as described in Viewing Upgrade Groups on page 318.
- Delete an upgrade group, as described in Deleting Upgrade Groups on page 319.

Adding Upgrade Groups

When you create an upgrade group, you select the Grid members for that group, and specify whether the software distribution and upgrade occur on all group members at the same time, or successively in the order they are listed in the group members list. A Grid member can belong to only one upgrade group.

**Note:** The appliance displays a warning message when you create an upgrade group that includes the two peers of a DHCP failover association. Infoblox recommends that you assign DHCP failover peers to separate upgrade groups to minimize the risk of a loss in DHCP services. For example, if DHCP failover peers are in the same upgrade group and its members upgrade simultaneously, the upgrade causes a loss in DHCP services.

Note the following recommendations when you create an upgrade group:

- Put the following members in the first upgrade group after the grid master upgrade: all grid master candidates, DNS primaries, and the DHCP logging member.
- To minimize the risk of a loss in DNS services, put the name servers for a zone in different upgrade groups, and assign the primary and secondary servers to separate upgrade groups.

To add an upgrade group:

1. From the **Grid** tab, select the **Upgrade** tab.
2. Click **Toggle Group List View** to display the list of upgrade groups, and then click the Add icon.
3. In the **Add Upgrade Group** wizard, complete the following:
   - **Name**: Enter a name for the upgrade group. The name can contain alphanumeric characters, spaces, underscores, hyphens, and dashes.
   - **Distribute to Members**: Select one of the following to specify how the Grid Master distributes software to the members in the group.
     - **Simultaneously**: Select this to distribute software upgrade files to all group members at the same time.
     - **Sequentially**: Select this to distribute software upgrade files to group members in the order they are listed in the group members list.
Managing NIOS Software and Configuration Files

— **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 243.)

5. Save the configuration and click **Restart** if it displays at the top of the screen.

**Modifying Upgrade Groups**

You can modify an existing upgrade group to change the group name or how the distribution and upgrade are performed. You can also add and delete members.

To modify an upgrade group:
1. From the **Grid** tab, select the **Upgrade** tab, and then click **Toggle Group List View**.
2. Select an **upgrade_group** check box, and then click the Edit icon in the row. You can also click the Edit icon directly without selecting the check box.
3. The **Upgrade Group** editor provides the following tabs from which you can modify data:
   — **General:** Modify the fields as described in **Adding Upgrade Groups** on page 317.
   — **Member Assignment:** Add or delete members as described in **Adding Upgrade Groups** on page 317.

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

**Viewing Upgrade Groups**

In the **Upgrade** tab, Grid Manager lists the Grid Master group, the Default group, and other upgrade groups you have configured. You cannot modify or delete the Grid Master group. You can modify the Default group, but you cannot delete it. To view the members in a specific upgrade group, click the arrow next to the group name to expand the group. All groups are collapsed by default.

Before a distribution or upgrade starts, you can move members from one group to another, reorder the members, or remove a member from an upgrade group. The member you remove automatically joins the Default group. (For information, see **Managing Distributions** on page 323.) 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 323.
To view the upgrade groups in a Grid:

1. From the **Grid** tab, select the **Upgrade** tab, and then click **Toggle Group List View**.
   Grid Manager displays the Grid Master at the top of the list. All other upgrade groups are listed alphabetically after the Grid Master. You can click the arrow next to a group to view members in the group.

2. Grid Manager displays the following:
   - **Group**: The name of an upgrade group to which the member belongs.
   - **Member**: The name of the member.
   - **Status**: Displays the overall status of an upgrade group at the group level and individual status for each member when you expand the upgrade group. At the group level, this displays the most severe status among the members. For example, when there are three out of five members are offline, the overall status shows **3 of 5 members** in red, which means offline.
   - **IP Address**: The IP address of the member.
   - **Running Version**: The NIOS software version that is currently running on the member.
   - **Distribution Status**: The distribution status of the group.
   - **Timestamp**: The date, time, and time zone when a distribution or upgrade is complete.

You can hide some of the default columns, but you cannot sort the information in this table. You can use filters and the **Go to** function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the **Go to** field and select the object from the possible matches. You can also create a quick filter to save frequently used filter criteria. For information, see *Using Quick Filters* on page 57.

### Deleting Upgrade Groups

When you delete an upgrade group, members in the upgrade group that you want to delete will be moved to the Default group. Grid Manager displays a warning before deleting an upgrade group.

To delete an upgrade group:

1. From the **Grid** tab, select the **Upgrade** tab, and then click **Toggle Group List View**.
2. Select an **upgrade-group** check box, and then click the **Delete** icon.
3. In the **Delete Confirmation** dialog box, click **Yes**.
Viewing Software Versions

Before you upgrade, downgrade, or revert to a different NIOS software version, you can view the current software version that is running on the Grid, the NIOS image you have uploaded, and the available version to which you can revert. Grid Manager displays the software information in the Upgrade tab.

To view software information:

1. From the Grid tab, select the Upgrade tab.
2. Grid Manager displays the following in the Grid Version Information section:
   - Running: The NIOS software version that is currently running on the grid.
   - Uploaded: The latest NIOS image file you have uploaded and is available for distribution.
   - Distribution: The NIOS software version used for distribution or is available for distribution.
   - Revert: The NIOS software version to which the appliance can revert.
   - Distribution Schedule: Displays the date and time of the next scheduled distribution.
   - Upgrade Schedule: Displays the date and time of the next scheduled upgrade.

Note: Grid Manager leaves a field empty when there is no available software for the specific function.

Grid Manager automatically refreshes the Upgrade tab with the latest information and displays the timestamp in the Last Updated field below the Grid Version Information section.

Upgrading NIOS Software

Infoblox frequently releases updated NIOS software. Contact Infoblox Technical Support to learn which file name to use when downloading a new upgrade file, or watch your email for periodic notifications that a new software upgrade is available. To get the latest upgrade, your local network must be capable of downloading a file from the Internet.

After you download and store the new upgrade file on your local network, complete the following tasks to upgrade an Infoblox independent appliance or a Grid.

• 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 321.
• Optionally, test the upgrade, as described in Testing Software Upgrades on page 324.
• Perform the software upgrade, as described in Performing Software Upgrades on page 325.

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.
Upgrading 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 321), 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 323.

Note that starting a manual distribution cancels a scheduled distribution.

Scheduling Distributions

When you schedule a distribution, you schedule the distribution of the Grid Master as well as the upgrade groups, including the Default group. The Grid Master distribution must always occur before the distribution of the upgrade groups.

To schedule a software distribution:

1. From the Grid tab, select the Upgrade tab, and then click Distribute -> Schedule Distribution from the Toolbar.
2. In the Schedule Distribution editor, complete the following:
   - **Activate Distribution Schedule:** Select this to enable the distribution schedule. Clear this if you are creating a distribution schedule you plan to activate at a later date. You can configure and save information in this editor even when you deactivate a scheduled distribution.
   - **Grid Master Distribution Start Information:** Enter a Grid Master distribution date, time, and time zone. The distribution date and time must be before those of the upgrade groups.
— **Date**: Enter a start date of the Grid Master distribution in YYYY-MM-DD (year-month-day) format. You can click the calendar icon to select a date from the calendar widget.

— **Time**: Enter a start time of the Grid Master distribution in hh:mm:ss AM/PM (hour:minute:second in AM or PM) format. You can also select a time from the drop-down list.

— **Time Zone**: Select a time zone that applies to the start time you enter. If this time zone is different from the Grid time zone, the appliance converts the time you enter here based on the Grid time zone, after you save this schedule. When you display this schedule again, it displays the converted time. Selecting the time zone here does not affect any time zone settings in the Grid. (For information about selecting the Grid and member time zones, see [Managing Time Settings](#) on page 243.)

— **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 130.

— 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 243.) 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 317.

— **Admin Local Time**: Displays the start date and time in the time zone of the administrator, as explained in [Creating Local Admins](#) on page 130.

— **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 318.

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

Grid Manager confirms that the schedule is saved and indicates whether the distribution schedule is active. You can click the Refresh icon to refresh the information in this panel.

Note that the appliance does not save the schedule and displays an error message if the schedule contains the following:

— Circular dependencies between upgrade groups. For example, the distribution of Group A is scheduled after Group B, and the distribution of Group B is scheduled after Group A.

— The distribution time is in the past.

### Software Distribution Process

The following series of events occur after a Grid distribution starts:

- The appliance checks if a NIOS software upgrade was uploaded.
  - If the upgrade files are not uploaded, the distribution stops. The appliance displays an error message and if the distribution is scheduled, the appliance deactivates the distribution schedule.
If the upgrade files are uploaded, the distribution proceeds.

- A single Grid Master uploads the file to a backup partition and unpacks the contents, which overwrites any existing backup software that might have been there. For an HA Grid Master, it is the active node that uploads the file to a backup partition and unpacks the contents.
  - The Grid Master (or active node of the HA Grid Master) sends a command to all nodes that are online to copy their database and software to a backup software partition.
  - For an HA Grid Master, the active node sends the command to the passive node as well.
  - The nodes perform resynchronization on their backup partition, retrieving only the changed files from the Grid Master.
  - After the active node of an HA member receives the software, it then distributes it to the passive node.

When the distribution successfully completes, the appliance updates the distribution status and sets the schedule, if configured, to inactive. The new software is now staged on all member appliances and is ready for use. Grid Manager displays the software version in the Distribution field in the Grid Version Information section.

### Managing Distributions

After you start a distribution, you can pause, resume, or stop it. For information, see Pausing and Resuming Distributions on page 323 and Stopping Distributions on page 323. Grid Manager displays the status of the overall distribution as well as the status of individual members. You can view this information in the Upgrade tab.

### Pausing and Resuming Distributions

The following are some operational guidelines for performing a distribution:

- You cannot create new upgrade groups, add members to a group, or remove members from a group after a distribution starts.
- You can skip a member that is currently offline from a distribution. When both nodes of an HA pair are online, the skip member function is not available.

To pause a distribution:

1. From the Grid Distribution Status bar, click the Pause icon.
2. When the appliance displays a confirmation dialog box, click Yes to pause the distribution.

The Grid Distribution Status bar indicates the distribution is paused. For information about the distribution status of each member, see Monitoring Distribution and Upgrade Status on page 330.

To skip a member from a distribution:

1. From the Grid tab, click the Upgrade tab, and then click Toggle Member List View.
2. Select a member check box, and then click Skip Member from the Toolbar. Grid Manager automatically skips the distribution of software to the members that are offline.

To resume a distribution:

1. From the Grid Distribution Status bar, click the Resume icon.
2. When the appliance displays a dialog box confirming that you want to resume the distribution, click Yes to continue.

Members that have not completed or started distributions that were scheduled at an earlier time resume the distribution.

### Stopping Distributions

You can stop a distribution immediately, for example, if there are offline members and you do not want to wait for them to come back online, or if you realize that you have uploaded the wrong software version. When you stop a distribution, you can do the following:

- If the Grid Master has completed its distribution, you can upgrade the Grid immediately. This forces members that do not have a complete distribution to synchronize their releases with the Grid Master.
• If the Grid Master does not have a valid distribution, you can restart the distribution.
• Upload another software upgrade.

Ending a distribution does not affect the upgrade schedule, if configured. The Grid upgrade starts as scheduled, as long as the Grid Master completes its distribution.

To stop a distribution:
1. From the Grid Distribution Status bar, click the Stop icon.
2. When the appliance displays a dialog box confirming that you want to stop the distribution, click Yes to continue.

Testing Software Upgrades

After you successfully distribute a software upgrade to the Grid Master, you can test an upgrade on the Grid Master before actually implementing it. This allows you to resolve potential data migration issues before the actual upgrade. The length of time the upgrade test takes depends on the amount of data and the difference between the current NIOS version and the software upgrade. The test does not affect NIOS services and you can perform other administrative tasks during the upgrade test.

To start an upgrade test:
• From the Grid tab, select the Upgrade tab, and then click Test Upgrade from the Toolbar. Test upgrade is enabled only for a major upgrade (not an Upgrade Lite compatible upgrade).

After you start an upgrade test, you can view its status in the status bar. You can also stop it at anytime.

To stop an upgrade test:
• From the Grid Upgrade Test Status bar, click the Stop icon.

Note that if an admin restarts the Grid services or reboots the Grid Master, or if an HA failover occurs on the Grid Master during the upgrade test, the appliance automatically stops the test. The appliance always resets the status of the Grid to “Distributed” when it stops the upgrade test.

If the appliance encounters an error during the test, it stops the test and displays a message in the Upgrade Status panel indicating that the upgrade test failed and the reason for the failure, such as a data translation error or data import error. You can review the syslog for specific error messages before downloading the Support Bundle and contacting Infoblox Technical Support.

After the test successfully finishes, the appliance displays a message confirming that the test upgrade is complete. You can then perform the actual upgrade as described in Performing Software Upgrades on page 325.
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 332.

When upgrading to software releases that are Upgrade Lite compatible, you can schedule the Grid upgrade as described in Scheduling Upgrades on page 325.

Upgrading Immediately

For unschedulable full upgrades, all the grid members in the grid must upgrade at the same time. For lite upgrades and schedulable full upgrades, you can schedule the upgrades as described in Scheduling Upgrades on page 325, or you can upgrade all the grid members at the same time.

To upgrade a grid immediately:

- From the Grid tab, select the Upgrade tab, and then click Upgrade -> Upgrade Now from the Toolbar.

**Note:** The grid upgrades immediately and if there is an active upgrade schedule, it becomes inactive.

Scheduling Upgrades

You can schedule a lite upgrade and full upgrades of some NIOS versions. For limitations on scheduling a full upgrade, see Guidelines for Scheduling Full Upgrades on page 326. When you schedule an upgrade, you schedule the upgrade for the grid master and the upgrade groups, including the Default group. The grid master must always upgrade before the upgrade groups. When you schedule a full upgrade, you can schedule the upgrade for the grid master and upgrade groups at different times over a period of nine days. If you schedule an upgrade that takes more than nine days, the appliance displays a warning.

To schedule an upgrade:

1. From the Grid tab, select the Upgrade tab, and then click Upgrade -> Schedule Upgrade from the Toolbar.
2. In the Upgrade Schedule editor, complete the following:
   - **Activate Upgrade Schedule:** Select this to enable the upgrade schedule. Clear it if you are creating an upgrade schedule that you plan to activate at a later date. You can configure and save information in this editor even when you deactivate a distribution.
   - **Grid Master Upgrade Start Information:** Enter a Grid Master upgrade date, time, and time zone. The date and time must be before those of the upgrade groups.
     - **Date:** Enter a start date of the Grid Master upgrade in YYYY-MM-DD (year-month-day) format. You can click the calendar icon to select a date from the calendar widget.
     - **Time:** Enter a start time of the Grid Master upgrade in hh:mm:ss AM/PM (hour:minute:second in AM or PM) format. You can select a time from the drop-down list.
     - **Time Zone:** Select a time zone that applies to the start time you enter. If this time zone is different from the Grid time zone, the appliance converts the time you enter here based on the Grid time zone, after you save this schedule. When you display this schedule again, it displays the converted time. Selecting the time zone here does not affect any time zone settings in the Grid. (For information about setting the Grid and member time zones, see Managing Time Settings on page 243.)
     - **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 130.
   - In the upgrade member table, specify the following by clicking the corresponding field in each row:
     - **Group:** The name of the upgrade group. You can assign a different upgrade group by selecting the group from the drop-down list.
— **Group Members**: When you expand an upgrade group, this field displays the group members.

— **Warning**: This field turns yellow when there is a conflict among the upgrade groups. Hover your mouse over the field and the tooltip displays the member that contains the conflict. It also displays recommended upgrade groups in the **Group** column so you can change the group assignment to resolve the conflict. The tooltip can display one of the following: **GMC, DNS Primary, DHCP Logging Member**, or **DHCP Failover**. For information about how to resolve a conflict, see **Resolving Upgrade Warnings** on page 327. Select an upgrade group from the drop-down list in the **Group** column to assign a different upgrade group. Click **Validate and Refresh** to validate the new group assignment.

— **Start Upgrade**: Specify when the upgrade occurs. Select one of the following from the drop-down list:
  - **Date/Time**: Select this to configure the upgrade start date, time, and time zone.
  - **After <group>**: Select **After Grid Master** to start the distribution immediately after the completion of the grid master distribution. Select an upgrade group that must complete its distribution before the group you are configuring. If you select this option, you cannot enter a date, time, and time zone.

  **Date, Time, and Time Zone** are enabled only when you select **Date/Time** for **Start Upgrade**.

— **Date**: Enter an upgrade start date in **YYYY-MM-DD** (year-month-day) format. You can click the calendar icon to select a date from the calendar widget.

— **Time**: Enter an upgrade start time in **hh:mm:ss AM/PM** (hour:minute:second in AM or PM) format. You can select a time from the drop-down list.

— **Time Zone**: By default, the appliance displays the time zone of the first grid member in the Upgrade Group. You can change this time zone, if you want to enter the time using a different time zone. After you save the schedule though, the appliance converts the time you entered to the time zone of the upgrade group, if it is different. (For information about setting the grid and member time zones, see **Managing Time Settings** on page 207.) 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 317.

— **Admin Local Time**: Displays the data and time in the time zone of the administrator, as explained in **Creating Local Admins** on page 97.

— **Upgrade Members**: Indicates whether the upgrade within the group occurs simultaneously or sequentially. You cannot edit this field here. You define this when you create the upgrade group. To change this setting, see **Modifying Upgrade Groups** on page 318.

3. Save the configuration.

The appliance does not save the schedule and displays an error message if the schedule contains the following:
  - Circular dependencies between upgrade groups; for example, the upgrade of Group A is scheduled after Group B, and the upgrade of Group B is scheduled after Group A.
  - The upgrade time is in the past.

The appliance also does not save the schedule and displays a warning when there is a group assignment conflict. For information about how to resolve these conflicts, see **Resolving Upgrade Warnings**. Otherwise, the appliance confirms that the schedule is saved and indicates whether the upgrade schedule is active.

**Guidelines for Scheduling Full Upgrades**

Ensure that you review the following before you schedule a full upgrade:

- Only the following objects (if changed on a member) are replicated to the grid master during the upgrade process: DNS updates, leases, PTR records, A records, TXT records, SOA, DS records, NAPTR records, AAAA records, CNAME records, DNAME records, MX records, NS records, SRV records, and host records.
- During an upgrade, all discovery processes are stopped on the members performing the discoveries, except for PortIQ discoveries. You cannot start a new discovery on the specified members until after the upgrade is completed.
- On a member that synchronizes data with Microsoft DNS and DHCP servers, the following functions are deactivated during an upgrade:
Upgrading NIOS Software

— Synchronization of Microsoft DNS and DHCP data
— Rotation of Microsoft logs
— Start and stop of Microsoft servers
— Releases of DHCP leases from a Microsoft DHCP server

**Note:** Note that the deactivation of these functions does not affect any data on the Microsoft servers. After the upgrade, the member automatically restarts the synchronization of Microsoft data.

• During an upgrade, the grid replication of data between the DNS primary and secondary is switched to DNS zone transfer. The primary zone configuration is also temporarily changed to allow for transfers from the DNS secondary server. These activities are recorded in the syslog file.

**Note:** Ensure that UPD port 53 and TCP port 53 between the grid primary and grid secondary members are open when the scheduled upgrade starts.

• You cannot restart services through Grid Manager during an upgrade. You can however use the CLI command `restart service` to restart services on a member if needed.

• DHCP logging is temporarily disabled during an upgrade. DHCP events are synchronized after the upgrade is completed. Since the size of the queue is limited, some DHCP events could be lost if the upgrade takes too long to complete.

• If a grid is not configured to use NTP, you cannot change the date and time on any members in the grid during a distribution or an upgrade, whether the process is in progress or paused.

• You cannot do the following to a DHCP failover association until all members in the association complete the upgrade:
  — Update the DHCP failover association if it is associated with a DHCP range
  — Add, modify, or delete a DHCP range that is associated with the failover association
  — Reorder DHCP ranges in a network if any of these ranges is associated with the failover association

**Resolving Upgrade Warnings**

The appliance can generate the following warnings when you schedule an upgrade:

• **GMC:** To resolve this warning, put all grid master candidates in the first upgrade group.

• **DNS Primary:** To resolve this warning, put all the members that are serving as DNS primaries in the first upgrade group.

• **DHCP Logging Member:** To resolve this warning, put the DHCP logging member in the first upgrade group.

• **DHCP Failover:** To resolve this warning, place the peers of a DHCP failover association in separate upgrade groups. Ensure that you schedule upgrades of the failover peers close to each other to minimize configuration restrictions. NIOS does not allow DHCP configuration changes that affect the communication between the peers until both peers are upgraded.

**Upgrading Groups Immediately**

After you schedule an upgrade with multiple upgrade groups, you can choose to immediately upgrade an upgrade group that has not been upgraded yet. This function is available only for scheduled upgrades.

To upgrade an upgrade group now:

1. From the Grid tab, select the Upgrade tab, and then click **Toggle Group List View.**
2. In the Group List view, click the Upgrade Group Now icon in the upgrade group row.

Grid Manager immediately upgrades the selected group.
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 329 (for a single Grid Master).

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.

Managing Upgrades

During an upgrade, Grid Manager displays a system message at the top of the screen indicating the grid is being upgraded. After you start an upgrade, you can pause or resume it. For information, see Pausing and Resuming Upgrades and Monitoring Distribution and Upgrade Status on page 330.

Pausing and Resuming Upgrades

The following are some operational guidelines for performing an upgrade:

- You may not be able to perform certain administrative tasks during an upgrade.
- The Grid Manager session terminates when an HA grid master fails over from Node 1 to Node 2, or when a single grid master reboots and goes offline. You can log back in to the appliance after the upgrade.
- When you pause an upgrade, you can do the following
  - Change the sequence of the upgrade groups
  - Change the scheduled upgrade time for an upgrade group

To pause an upgrade, from the Grid Upgrade Status bar, click the Pause icon. When you pause an upgrade, Grid Manager displays a system message at the top of the screen indicating the upgrade is paused, until you resume the upgrade. For information about the upgrade status of each member, see Monitoring Distribution and Upgrade Status on page 330.
To resume an upgrade:
1. From the Grid Upgrade Status bar, click the Resume icon.
2. When the appliance displays a dialog box confirming that you want to resume the upgrade, click Yes to continue.
   Members that have not completed or started upgrades that were scheduled at an earlier time resume the upgrade.

Monitoring Distribution and Upgrade Status

During a distribution or an upgrade, Grid Manager displays the status of the distribution or upgrade in the status bar. It also displays the process status for each member. You can view the status in either the Member List view or Group List view from the Grid tab -> Upgrade tab.

When you perform a distribution or an upgrade, the status bar displays the overall Grid distribution status with a progress bar that describes the process being performed. The status bar also displays the number of members that have completed the distribution or upgrade.

A difference between a distribution and an upgrade process is that during an upgrade, the Grid Manager session terminates when an HA Grid Master fails over from Node 1 to Node 2, or when a single Grid Master reboots and goes offline. You can log back in to the appliance after the upgrade.

Grid and Member Status

You can view the distribution and upgrade process status at the Grid and member level. To view the process status, from the Grid tab, select the Upgrade tab, and then click Toggle Member List View.

The status bar displays the status of the overall Grid process. It contains a progress bar that indicates the percentage of completion. It also shows the number of members that have completed the process.

Grid Manager displays the following information for each member:
- **Member**: The name of the Grid member.
- **Group**: The upgrade group to which the member belongs.
- **HA**: Indicates whether the member is an HA pair or not.
- **Status**: The current distribution or upgrade status. This can be Running (green) or Offline (red).
- **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. You can also select the member IP address for display.

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).
Downgrading Software

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 333
- **Manually Backing Up Data Files** on page 335
- **Restoring Backup Files** on page 336
- **Downloading Backup Files from a Different Appliance** on page 337

**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 336. 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. Save the configuration and click **Restart** if it displays at the top of the screen.
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.
Managing NIOS Software and 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 337.

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.
— **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 336.

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 336.

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.
Managing NIOS Software and Configuration Files

Downloading Support Bundles

When you need assistance troubleshooting a NIOS appliance, you can log in to the appliance as a superuser, download the support bundle of the appliance, and then send it to Infoblox Technical Support for analysis. A support bundle is a tar.gz file that contains configuration files and the appliance system files. You can download a support bundle for an independent appliance and for each member in a Grid. When you download a support bundle for an HA pair, it includes the files of both nodes in the HA pair.

By default, the appliance includes the following files in the support bundle: core files, current logs, and rotated logs. Because core files can be quite large and take a significant amount of time to download, Infoblox recommends that you include core files in the support bundle only when requested by Infoblox Technical Support.

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  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 340
  - System Requirements on page 341
- Using the bloxTools Environment on page 341
  - Configuring the Service on page 341
  - Allocating Memory on page 342
  - Uploading Files on page 342
  - Scheduling Tasks on page 343
  - Moving the bloxTools Service on page 343
- Monitoring the Service on page 344
  - Viewing the Logs on page 344
  - Viewing Detailed Status on page 344
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. Note that no direct external remote user (telnet and ssh, for example) or shell access is available in this environment.

The bloxTools environment “borrows” resources such as CPU, memory, disk space, and networking from the host Infoblox appliance, but is logically separated from the NIOS. The logical separation ensures that any failure in the bloxTools service does not affect the other services running on the appliance.

The bloxTools environment can only be configured to run on an independent appliance or a Grid member. You cannot run the bloxTools service on a Grid Master, a Grid Master candidate, or a virtual appliance, such as vNIOs for Riverbed, or VMware.

**Note:** In previous NIOS releases, you could run the bloxTools service only on a Grid Master. If bloxTools has been configured to run on a Grid Master before an upgrade, the bloxTools service continues to run on the Grid Master after an upgrade. This configuration is preserved mainly for migration purposes only. Infoblox strongly recommends that you move the bloxTools service to a Grid member after the upgrade. For information, see *Moving the bloxTools Service* on page 343.

In a Grid, you can run the bloxTools service only on one Grid member at a time, and you cannot configure this member as a Grid Master candidate. However, you can move the bloxTools service from one member to another. For information, see *Moving the bloxTools Service* on page 343.

On an HA member, the bloxTools service runs on the active node. If there is an HA failover, the bloxTools service is automatically launched after the passive node becomes active. For information, see *About HA Pairs* on page 182.

**Note:** When you run the bloxTools service on an independent appliance or a Grid member, the performance of other services running on the appliance may be affected. Infoblox recommends that you run the bloxTools environment on a member that does not host critical services.

After you enable the bloxTools service and configure its built-in file transfer services, you can upload content to the bloxTools portal using either an FTP (File Transfer Protocol) or SFTP (SSH File Transfer Protocol) client. The uploaded content is included in system backups and you can restore it from the backups.

For more information about the bloxTools environment and to access free applications, visit [https://www.bloxtools.com](https://www.bloxtools.com).

**Note:** The bloxTools environment is not supported on vNIOs appliances on Riverbed, Cisco, and VMware.
Using the bloxTools Environment

Complete the following tasks to upload custom applications to the bloxTools environment:

1. Log in to the appliance as a superuser and configure the bloxTools service, as described in Configuring the Service.
2. Use an FTP or a SFTP client to upload content to the bloxTools environment.

In addition, you can schedule tasks as described in Scheduling Tasks on page 343, and monitor the bloxTools service as described in Monitoring the Service on page 344.

**WARNING:** Resetting the Grid member using either the *reset all* or *reset database* CLI commands permanently deletes the content you uploaded to the bloxTools environment. Infoblox recommends that you backup the appliance before using any of these commands.

### Configuring the Service

When you configure the bloxTools service, you can enable FTP, SFTP, and HTTPS, and set their operational parameters. FTP and SFTP are the services you use to upload data. You can disable these services when they are not in use. HTTPS must remain enabled to allow the web based bloxTools applications to run. Note that the bloxTools service uses the same SSL certificate as the host Infoblox appliance. (For information on certificates, see *Managing Certificates* on page 44.)

To configure the bloxTools service:

1. Log in as a superuser.
2. From the Grid tab, select the Grid Manager tab, and then click *bloxTools*. In the Services tab, click Edit -> Grid bloxTools Properties from the Toolbar.
3. In the Grid bloxTools Properties editor, complete the following:
   - **Enable Web Service:** Select HTTPS Port to enable users to access the applications through an HTTPS connection. The default port is 444. You can change the 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.

---

### Table 10.1 Memory and Disk Space Requirements

<table>
<thead>
<tr>
<th>Supported Infoblox Appliance</th>
<th>Memory Requirement</th>
<th>Allocated Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infoblox-250-A</td>
<td>Feature not supported</td>
<td></td>
</tr>
<tr>
<td>Infoblox-550-A</td>
<td>128 MB to 1024 MB (configurable)</td>
<td>Up to four gigabytes</td>
</tr>
<tr>
<td>Infoblox-1050-A</td>
<td>The default is 256 MB</td>
<td></td>
</tr>
<tr>
<td>Infoblox-1550-A</td>
<td>128 MB to 2048 MB (configurable)</td>
<td>Up to four gigabytes</td>
</tr>
<tr>
<td>Infoblox-1552-A</td>
<td>The default is 256 MB</td>
<td></td>
</tr>
<tr>
<td>Infoblox-1852-A</td>
<td>128 MB to 4096 MB (configurable)</td>
<td>Up to four gigabytes</td>
</tr>
<tr>
<td>Infoblox-2000-A</td>
<td>The default is 256 MB</td>
<td></td>
</tr>
</tbody>
</table>
Enable SFTP Service: Select SFTP Port to enable the SFTP service for secure file transfer. The default port is 28. You can change the port to a number between 1024 and 63999, provided that the port is not currently used for another purpose.

Login: Enter the username for the FTP and SFTP services. The username can contain lower case letters, numbers, underscores (_), and dollar signs ($), and it must begin with a letter, not a number.

Set Password: Enter the password for the FTP and SFTP services in this field.

Retype Password: Enter the same password.

Note: The password is sent as clear text when you use the FTP service. To maintain security on the Infoblox appliance, this password should be different from the password set for the Infoblox appliance.

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

When you configure the bloxTools service on an independent appliance, you can configure the allocated memory in the System bloxTools Properties editor. For information, see Allocating Memory on page 342.

Allocating Memory

You can configure the memory you want to allocate to the bloxTools service. You must configure this at the member level. If you run the bloxTools service on an independent appliance, you can configure the allocated memory in the System bloxTools Properties editor.

To configure the allocated memory:

1. Log in as a superuser.

2. From the Grid tab, select the Grid Manager tab, and then click bloxTools. In the Services tab, click Edit -> Member bloxTools Properties from the Toolbar.

3. In the Member 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 256 MB. You can change this allocation, depending on the appliance platform. See System Requirements on page 341 for the requirements and allowed values of each appliance.

Uploading Files

Use an FTP or a SFTP client to upload content, such as Perl modules, JavaScript files, PHP files, CGI files, and image files, to the bloxTools environment. You can upload a maximum of 4 GB of data. After you have uploaded content to your bloxTools environment, you should disable the FTP and SFTP services to prevent unauthorized or accidental changes.

To upload files using the FTP service:

1. Open an Internet browser window and log in to the FTP service by entering:

   ftp://Grid_member_ip_addr:ftp_port

   For example, if the IP address of the Grid member is 10.1.1.1 and the FTP port number is 26, enter:

   ftp://10.1.1.1:26

2. In the Authentication Required dialog box, enter the username and password. This is the username and password you entered for the FTP service in the bloxTools Environment editor on the appliance.

3. Follow the instructions provided by your FTP client to upload the files.
To upload files using the SFTP service:

1. Open a terminal window and log in to the SFTP service by entering:

   ```
   sftp -oPort=sftp_port sftp_user@Grid_member_ip_addr
   ```
   
   For example, if the IP address of the Grid member is 10.1.1.1, the login username for the SFTP service is jdoe, and the SFTP port number is 28, enter:

   ```
   sftp -oPort=28 jdoe@10.1.1.1
   ```

2. Enter the password. This is the password you entered for the SFTP service in the bloxTools Environment editor on the appliance.

3. Follow the instructions provided by your SFTP client to upload the files.

Note: On a computer running Microsoft Windows, you can use WinSCP as the FTP or SFTP client for uploading files.

The bloxTools environment stores the uploaded data in the /portal directory.

## Scheduling Tasks

bloxTools includes support for the Perl module `Config::Crontab` so you can manage scheduler services. You can use the scheduler to execute commands in the future. You can also schedule recurring commands. For example, you can schedule the creation of a host record or schedule recurring reports. The scheduler allows default “user level” crontab access and you can use the user account ‘nobody’ to submit commands. The Grid Master replicates the crontab data to the master candidates.

## Moving the bloxTools Service

In a Grid, you can move the bloxTools service from one Grid member to another. When you move the bloxTools service, the source member synchronizes data with the Grid Master, and the Grid Master synchronizes data with the destination member. The time to resynchronize the bloxTools data on to the destination member depends on the amount of data to synchronize and the Grid configuration. If the migration takes longer than two minutes, it becomes a long running task. This allows the move of the bloxTools service to run in the background while you perform other tasks. For information, see About Long Running Tasks on page 62. Note that on an independent appliance, you cannot move the bloxTools service to another member.

After an upgrade from previous NIOS releases, Grid Manager displays a warning message in the system message panel if you have previously configured to run the bloxTools service on the Grid Master. You can click Move in this panel to launch the Move bloxTools dialog box to move the bloxTools service to a Grid member.

To move the bloxTools Service:

1. From the Grid tab, select the Grid Manager tab ->Members tab, and then click bloxTools ->Move from the Toolbar.
2. In the Move bloxTools dialog box, complete the following:
   - **Source Member**: Displays the name of the Grid member that is currently running the bloxTools service. You cannot modify this field.
   - **Destination Member**: Click Select. In the Member Selector dialog box, select the member to which you want to move the bloxTools service. Grid Manager displays the name of the selected member here.
3. Click Move.

The appliance synchronizes data with the Grid Master, and the Grid Master synchronizes data with the destination member. This may take a while to complete depending on your Grid configuration and the amount of data.
Monitoring the Service

Infoblox provides several tools for monitoring the bloxTools Environment. The bloxTools Environment has its own syslog service which you can access to view logs generated by the bloxTools service and its processes. The Detailed Status panel also displays the status of the bloxTools Environment.

Viewing the Logs

The bloxTools Environment generates the following logs:

- access.log: The Apache access log
- error.log: The Apache error log
- syslog.log: The bloxTools Environment system log

These log files are included in the support bundle. You can download the log files using FTP. You can also connect to the CLI of the member running the bloxTools environment and use the following commands to view the logs:

- Use the `show file` command to view the list of log files.
- Use the `show bloxtools` command to view the status of the bloxTools Environment.
- Use the `show file bloxtools portal_access` command to view the web portal access log.
- Use the `show file bloxtools portal_error` command to view the web portal error log.
- Use the `show file bloxtools portal_log` command to view the web portal system log.

Viewing Detailed Status

You can view the status of the bloxTools Environment from the Services tab of the Grid Manager tab. To display the bloxTools service status, from the Grid tab, select the Grid Manager tab -> Services tab, and then click bloxTools. Grid Manager displays all Grid members that can host the bloxTools service. The name of the Grid Master is displayed only if you have completed an upgrade and previously configured the bloxTools service to run on the Grid Master. Though you can continue to run the bloxTools service on the Grid Master, Infoblox strongly recommends that you move the bloxTools service to a Grid member. For information, see Moving the bloxTools Service on page 343.

Grid Manager displays the following information about all Grid members:

- **Name**: The Grid member name.
- **Service Status**: Indicates the current operational status of the bloxTools service running on the member. This can include the migration status if you are moving the bloxTools service to another member.
- **IP Address**: The IP address of the member.
- **Comment**: Information about the bloxTools Environment.
- **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>-</td>
<td>The bloxTools Environment is disabled or offline.</td>
</tr>
<tr>
<td>Green</td>
<td>-</td>
<td>The CPU, memory, and disk usage is below 80%.</td>
</tr>
<tr>
<td>Yellow</td>
<td>-</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>
</tr>
<tr>
<td>Red</td>
<td>-</td>
<td>The bloxTools Environment is down, or an essential service within the bloxTools Environment has failed.</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 11, Infoblox DNS Service, on page 347
- Chapter 12, DNS Views, on page 355
- Chapter 13, Configuring DNS Zones, on page 369
- Chapter 14, DNS Resource Records, on page 407
- Chapter 15, Configuring DNS Services, on page 441
- Chapter 16, Configuring DDNS Updates from DHCP, on page 477
- Chapter 17, DNSSEC, on page 523
- Chapter 18, “Configuring IP Routing Options”, on page 551
Chapter 11 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 1021).

This chapter provides an overview of the DNS configuration tasks. It includes the following sections:

- Configuring DNS Overview on page 348
  - DNS Configuration Checklist on page 349
- About Inheriting DNS Properties on page 350
  - Overriding DNS Properties on page 351
- Understanding DNS for IPv6 on page 352
  - Configuring IPv6 on a Grid Member on page 353
  - Configuring DNS for IPv6 Addressing on page 354
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.
- Do you want to configure member DNS properties?
  - Yes: Configure member DNS properties.
  - No: 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.
  - - Add resource records.
  - - Import zone data.
- Authoritative zone
  - - Choose the primary member or specify the external primary.
  - - Choose Grid secondaries or specify external secondaries.
- Delegated zone
  - Specify the IP address and FQDN of the authoritative name server for the zone.
- Stub zone
  - Specify the IP address of the master server, and select the Grid member that hosts the zone.
- Do you want to add more zones?
  - Yes: Configure member DNS properties.
  - No: Start DNS service on the member.

Initial DNS configuration is complete.
DNS Configuration Checklist

The following checklist includes the major steps for configuring DNS:

Table 11.1  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 11, Infoblox DNS Service</em>, on page 347</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 12, DNS Views</em>, on page 355</td>
</tr>
<tr>
<td>Decide which type of DNS zone you want to configure</td>
<td>• <em>Chapter 13, Configuring DNS Zones</em>, on page 369</td>
</tr>
<tr>
<td>Add hosts and resource records</td>
<td>• <em>Chapter 14, DNS Resource Records</em>, on page 407</td>
</tr>
<tr>
<td>Import zone data</td>
<td>• <em>Importing Zone Data</em> on page 385</td>
</tr>
<tr>
<td>Enable DNS service on the member</td>
<td>• <em>Starting and Stopping the DNS Service</em> on page 448</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 &lt;object&gt;</td>
<td>the DNS property has a definite value from an inheritance source.</td>
</tr>
<tr>
<td>Inherited From Upper Level</td>
<td>the appliance cannot yet determine the inherited value or inheritance source for the DNS property.</td>
</tr>
<tr>
<td>Inherited From Multiple</td>
<td>the DNS property has the same value that it inherits from multiple sources.</td>
</tr>
<tr>
<td>Settings Inherited from Multiple Ancestors, View Multiple Inheritance Scenarios</td>
<td>the DNS property has different values that it inherits from multiple sources, and you can view the values and their corresponding sources by clicking the View Multiple Inheritance Scenarios link.</td>
</tr>
</tbody>
</table>

Based on the information provided, you can then decide whether to override or keep the inherited values. You must have read/write permissions to the DNS resources to override inherited values. You can only view inherited values and paths if you have at least read-only permissions.

In the example in Figure 11.1, the DNS zone is served by members with different query settings.

*Figure 11.1  DNS Zone with Different Inherited Settings*
The Multiple Inheritance Viewer indicates that the two servers have different query ACLs, as shown in *Figure 11.2*. 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 11.2 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 813.
- **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 11.3 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. Save the configuration and click Restart if it displays at the top of the screen.
Configuring DNS for IPv6 Addressing

Configuring the appliance to manage DNS services for IPv6 connections is similar to configuring DNS services for IPv4 connections. For simplicity, the IPv6 procedures are located in the same location as the corresponding procedures for IPv4 in this chapter. In most cases, the key difference within the procedure involves selecting an IPv6 mapping zone instead of an IPv4 mapping zone. You can configure the following tasks:

Table 11.2  IPv6 DNS Configuration Checklist

<table>
<thead>
<tr>
<th>Step</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create primary or secondary name servers and specify an IPv6 root server.</td>
<td>• About Authoritative Zones on page 370</td>
</tr>
<tr>
<td></td>
<td>• Specifying a Primary Server on page 377</td>
</tr>
<tr>
<td></td>
<td>• Specifying a Secondary Server on page 380</td>
</tr>
<tr>
<td></td>
<td>• Creating a Root Zone on page 374</td>
</tr>
<tr>
<td>Configure the IPv6 zones.</td>
<td>• Creating an Authoritative Forward-Mapping Zone on page 371</td>
</tr>
<tr>
<td></td>
<td>• Creating an Authoritative Reverse-Mapping Zone on page 372</td>
</tr>
<tr>
<td>Configure IPv6 resource records</td>
<td>• Managing AAAA Records on page 416</td>
</tr>
<tr>
<td></td>
<td>• Managing PTR Records on page 417</td>
</tr>
</tbody>
</table>
Chapter 12 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 356
  - About DNS Views and Network Views on page 358
- **Configuring DNS Views** on page 358
  - Adding a DNS View on page 359
  - Defining a Match Clients List on page 360
  - Defining a Match Destinations List on page 361
  - Managing the DNS Views of a Grid Member on page 362
  - Managing Recursive DNS Views on page 363
  - Managing the Order of DNS Views on page 364
  - Managing DNS Views on page 365
- **Configuration Example: Configuring a DNS View** on page 366
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 12.1, 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 12.1 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 441.

You can provide multiple views of a given zone with a different set of records in each DNS view. In Figure 12.2, 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 12.2 Zone Data in Each DNS View

<table>
<thead>
<tr>
<th>Internal DNS View</th>
<th>corp100.com</th>
<th>sales.corp100.com</th>
<th>finance.corp100.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>MX</td>
<td>mx.corp100.com</td>
<td>serv1.sales.corp100.com</td>
<td>server.finance.corp100.com</td>
</tr>
<tr>
<td>NS</td>
<td>dns.corp100.com</td>
<td>serv2.sales.corp100.com</td>
<td>printer.finance.corp100.com</td>
</tr>
<tr>
<td>A</td>
<td>host1.corp100.com</td>
<td>serv3.sales.corp100.com</td>
<td>fin1.finance.corp100.com</td>
</tr>
<tr>
<td>A</td>
<td>host2.corp100.com</td>
<td>printer.sales.corp100.com</td>
<td>fin2.finance.corp100.com</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>External DNS View</th>
<th>corp100.com</th>
<th>sales.corp100.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>MX</td>
<td>email.corp100.com</td>
<td>web3.sales.corp100.com</td>
</tr>
<tr>
<td>A</td>
<td>web1.corp100.com</td>
<td>ftp.sales.corp100.com</td>
</tr>
<tr>
<td>A</td>
<td>web2.corp100.com</td>
<td>serv1.sales.corp100.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>serv2.sales.corp100.com</td>
</tr>
</tbody>
</table>
You can control which clients access a DNS view through the use of a match list specifying IP addresses and/or TSIG (transaction signature) keys. When the NIOS appliance receives a request from a client, it tries to match the source IP address and/or TSIG key with its match list when determining which DNS view, if any, the client can access. After the appliance determines that a client can access a DNS view, it checks the zone level settings to determine if it can provide the service that the client is requesting.

For information on TSIG keys or defining zone transfer settings, see **Enabling Zone Transfers** on page 463. For more information on match lists, see **Defining a Match Clients List** on page 360. For information on defining query settings, refer to **Controlling DNS Queries** on page 450.

**Figure 12.3** 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 12.3 Query Resolution**

When you create more than one DNS view, as shown in **Figure 12.3**, the order of the views is important. View order determines the order in which the NIOS appliance checks the match lists. In **Figure 12.3**, 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 362.

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 377.
About DNS Views and Network Views

The NIOS appliance provides one default DNS view, which is always associated with the default network view. You can create additional network and DNS views. A network view is a single routing domain with its own networks. For information about network views, see Configuring DHCP for IPv4 on page 641.

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 498.

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 359.
2. Add zones to the DNS view. You can add authoritative forward-mapping and reverse-mapping zones, as well as delegated, forward, and stub zones. For information about configuring each type of zone, see Configuring Authoritative Zones on page 370 and Configuring Delegated, Forward, and Stub Zones on page 393.

You can optionally do the following:

1. Define a Match Clients list and a Match Destination list to restrict access to the DNS view. For more information, see Defining a Match Clients List on page 360 and Defining a Match Destinations List on page 361
2. Copy resource records from one zone to another. This is useful when different DNS views have the same zone and have multiple resource records in common. For information, see Managing DNS Views on page 365.
3. Create resource records in a group and share the group among multiple zones. For information, see About Shared Record Groups on page 432.
4. Specify which interface IP address is published in the glue A record of the DNS view. For information, see Changing the Interface IP Address on page 363.
5. Manage recursive views. For information, see Managing Recursive DNS Views on page 363.
6. Manage the order of the DNS views, as this determines the order in which the NIOS appliance checks the Match Clients list. For information, see Managing the Order of DNS Views on page 364.
7. Configure forwarders for a DNS view. For more information, see Using Forwarders on page 449.
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 a Match Clients List on page 360.
- 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 366

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. Save the configuration and click Restart if it displays at the top of the screen, or click Next to define a Match Clients list. For information, see Defining a Match Clients List on page 360.
   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 256.
Defining a Match Clients List

When you configure a DNS view, you can create a Match Clients list to identify source IP addresses and TSIG keys that are allowed or denied access to the DNS view. The NIOS appliance determines which hosts can access a DNS view by matching the source IP address or TSIG key with its Match Clients list. After the appliance determines that a host can access a DNS view, it checks the zone level settings to determine whether it can provide the service that the host is requesting for that zone.

If you do not configure a Match Clients list, then all devices are allowed access to the DNS view. However, if you configure a Match Clients list, then only those devices in the list with “Allow” permission can access the DNS view. All other devices are denied access, including grid members. Therefore, to allow a primary server of a zone to receive dynamic DNS updates from member DHCP servers, you must add the members to the Match Clients list as well. Note that if you “Deny” permission to certain IP addresses or networks, you must add the “Allow Any” permission at the end of the Match Clients list to ensure that all other IP addresses and networks that are not in the “Deny” list are allowed access to the DNS view.

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 359. To define a Match Clients list for an existing DNS view:

1. From the Data Management tab, click the DNS tab -> Zones tab -> dns_view check box -> Edit icon. Or, if there is only one DNS view, for example the predefined default view, you can just click the Edit icon beside it.
2. 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 Algorithm: Select either HMAC-MD5 or HMAC-SHA256.
     - Key Data: To use an existing TSIG key, type or paste the key in the Key Data field. Alternatively, you can select the key algorithm, select the key length from the Generate Key Data drop down list, and then click Generate Key Data to create a new key.
     - 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. Save the configuration and click **Restart** if it displays at the top of the screen, or click **Next** to define extensible attributes. For information, see **Using Extensible Attributes** on page 265. You can also click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see **Scheduling Tasks** on page 256.

**Defining a Match Destinations List**

You can define a Match Destinations list that identifies destination addresses and TSIG keys that are allowed access to a DNS view. When the NIOS appliance receives a DNS request from a client, it tries to match the destination address or TSIG key in the incoming message with its Match Destination list to determine which DNS view, if any, the client can access. After the appliance determines that a host can access a DNS view, it checks the zone level settings to determine whether it can provide the service that the host is requesting for that zone.

You can define a Match Destination list when you edit an existing DNS view as follows:

1. From the **Data Management** tab, click the **DNS** tab -> **Zones** tab -> **dns_view check box** -> **Edit icon.** Or, if there is only one DNS view, for example the predefined default view, you can just click the Edit icon beside it.

2. Click the **Match Destinations** tab, and then click the Add icon and select the item to add. Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding:
   - **IPv4 Address:** In the **Name** field of the new row, enter the destination IP address. 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 Destinations 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 destination IPv6 address. 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 Destinations 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 Destinations list:
     - **Key Name:** Enter a meaningful name for the key. This name must match the name of the same TSIG key on other name servers.
     - **Key Algorithm:** Select either **HMAC-MD5** or **HMAC-SHA256**.
     - **Key Data:** To use an existing TSIG key, type or paste the key in the **Key Data** field. Alternatively, you can select the key algorithm, select the key length from the **Generate Key Data** drop down list, and then click **Generate Key Data** to create a new key.
     - **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.

3. Save the configuration.
Copy 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 363.
- You can assign an empty recursive view to a member, as described in **Managing Recursive DNS Views** on page 363.
- You can control the list of DNS views as described in **Changing the Order of DNS Views** on page 364.
Changing the Interface IP Address

By default, a Grid member publishes its LAN address in glue A records in the DNS view. You can change this default for each DNS view associated with a member. You can specify the NAT IP address or another IP address.

To specify the interface IP address for glue A records in a view:

1. From the Data Management tab, click the DNS tab -> Members tab -> member check box, and then click the Edit icon.
2. In the Member DNS Configuration editor, click Toggle Expert Mode if the editor is in basic mode, and then select the DNS Views tab.
   The Address Of Member Used in DNS Views table lists the default DNS view and DNS views with zones that are served by the member.
3. To change the address, click the entry in the Interface column of a DNS view, and select one of the following:
   — NAT IP Address 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. Save the configuration and click Restart if it displays at the top of the screen.

Managing Recursive DNS Views

When you add a DNS view that has recursion enabled, the appliance resolves recursive queries from hosts on the Match Clients list of that view. If the DNS view contains zones and you delete those zones, the appliance retains the view in its configuration file, as long as recursion is enabled in the view. Such a view is called an empty recursive DNS view because it does not contain any zones. It enables the appliance to respond to 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 Expert Mode if the editor is in basic mode, and then select the DNS Views tab.
3. The Recursive Views Assigned to this Member section lists the empty recursive DNS views. Move a DNS view to the Selected column to explicitly assign the view to the Grid member and include it in the DNS configuration file of the member. Move a DNS view to the Available column to remove it from the configuration file of the member.
   Empty recursive DNS views that you retain in the configuration file are automatically listed at the bottom of the list of DNS views. You can move them up on the list when you manually change the order of the DNS views, as described in Managing the DNS Views of a Grid Member on page 362.
4. Save the configuration and click Restart if it displays at the top of the screen.
Managing the Order of DNS Views

When a member receives a query from a DNS client, it checks the Match Client lists in the order the DNS views are listed in the *Order of DNS Views* table of the DNS Views tab in the DNS Member editor. The NIOS appliance can order DNS views automatically, or you can order the DNS views manually. If you choose to have the appliance automatically update the order of the DNS views, it does so after each of the following events:

- Adding a DNS view to a member.
- Removing a DNS view from a member.
- Changing the address match list of a DNS view hosted by the member.

About IP Addresses and the Order of DNS Views

NIOS appliances with both IPv4 and IPv6 enabled can contain both types of addresses in the Match Clients list. When you enable IPv6 on the appliance, the order of DNS views in the GUI may be affected. Views are ordered and sorted automatically based on Match Clients lists. Views with IPv6 enabled are sorted as follows:

- If the Match Clients lists of all views contain IPv4 addresses only—The appliance orders views based on IPv4 addresses.
- If the Match Clients lists of all views contain IPv6 addresses only—The appliance orders views based on IPv6 addresses.
- If the Match Clients list of one DNS view has 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 Expert Mode* if the editor is in basic mode, and then select the DNS Views tab.
3. In the Order of DNS Views section, select one of the following:
   - *Order DNS Views Automatically:* Click this to automatically order views after adding a new DNS view, removing a DNS view, or changing the match client list.
   - *Order DNS Views Manually:* This able lists the DNS views that have zones assigned to the Grid member and the empty recursive views associated with the member. Select a DNS view, then click an arrow to move it up or down in the list.
4. Save the configuration and click *Restart* if it displays at the top of the screen.
Managing DNS Views

You can list the DNS views, and then modify, disable, or remove any custom DNS view. You can modify and disable the default DNS view; however, under no circumstances can it be removed.

Listing DNS Views

After you configure additional DNS views, you can list all DNS views by navigating to the Data Management tab -> DNS tab -> Zones panel. This panel lists DNS views only after you modify the default DNS view or add a DNS view. If you never added DNS views or modified the default DNS view, this panel does not display the default DNS view. Instead, it lists the zones in the default DNS view. To display the properties of the default DNS view and edit it, use the Global Search function to locate and edit it.

Note that if you have not used Grid Manager to add a new DNS view, and you import DNS views through the Data Import Wizard or the API, you must log out and log back in to Grid Manager to display the newly imported DNS views.

For each DNS view, this panel displays the following by default:

- **Comment**: Comments that were entered for the DNS view.
- **Site**: Values that were entered for this pre-defined attribute.

You can also display the following column:

- **Disabled**: Indicates if the DNS view is enabled or disabled. Disabled DNS views are excluded from the named.conf file.

From this list, you can do the following:

- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 57.
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only.
- List the zones in a DNS view by clicking a DNS view name.
- Edit information about a DNS view, as described in the next section.
- Delete a DNS view, as described in Deleting DNS Views on page 366.

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 358.
   - In the Match Clients tab, you can define or update a Match Clients list, as described in Defining a Match Clients List on page 360.
   - In the DNSSEC tab, you can specify parameters for DNSSEC as described in Configuring DNSSEC on a Grid on page 531.
   - In the Root Name Servers tab, you can configure root name servers, as described in About Root Name Servers on page 465.
   - In the Extensible Attributes tab, you can modify the attributes. For information, see Using Extensible Attributes on page 265.
   - The Permissions tab displays if you logged in as a superuser. For information, see About Administrative Permissions on page 120.
3. Save the configuration and click **Restart** if it displays at the top of the screen.
   or
   Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 256.

**Deleting DNS Views**

You can delete a DNS view if it is not the only view associated with a network view and if it is not selected for dynamic DNS updates. You cannot remove the system-defined default DNS view. When you remove a DNS view, the NIOS appliance removes the forward and reverse mappings of all the zones defined in the DNS view.

To delete a DNS view:

- From the **Data Management** tab, select the *->DNS* tab-*Zones* tab-*dns_view* check box.

  To delete the DNS view immediately, click the Delete icon, and then click **Yes** to confirm the delete request. To schedule the deletion, click **Schedule Deletion** and in the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 256.

  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 12.4*, 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 12.4  Configuring a DNS View*

```plaintext
Master

Member-A 10.0.0.1
Primary Name Server for corp100.com

Infoblox-B 192.168.10.1
External Secondary Name Server for corp100.com
```

```bash
View "internal" {
  match-clients {192.168.10.1; 10.2.2.0/24;};
  zone "corp100.com" {
    type master;
    allow-query {10.2.2.0/24;};
    allow-transfer {11.0.0.1; } //auto added
  };
};
```
**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 **Address** field.
   - The **Permission** field displays **Allow** by default. Leave it as is.
   - Click **Add**.
   
   You will have 255 allowed client addresses in the **Match Clients** list when you are done.
5. Save the configuration and click **Restart** if it displays at the top of the screen.

**Adding a Zone to a DNS View**

1. Expand the Toolbar and click **Add -> Zone -> Add Auth Zone**.
2. In the **Add Auth Zone** wizard, click **Add an authoritative forward-mapping zone** and click **Next**.
3. Specify the following, and then click **Next**:
   - **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 **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. Save the configuration and click **Restart** if it displays at the top of the screen.

**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. Save the configuration and click **Restart** if it displays at the top of the screen.
   
   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 13 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 370
  - Configuring Authoritative Zones on page 370
  - Creating an Authoritative Forward-Mapping Zone on page 371
  - Creating an Authoritative Reverse-Mapping Zone on page 372
  - Creating a Root Zone on page 374
  - Adding an Authoritative Subzone on page 374
  - Locking and Unlocking Zones on page 375
  - Enabling and Disabling Zones on page 375
- **About Domains and Zones** on page 376
- **Assigning Zone Authority to Name Servers** on page 377
  - Specifying a Primary Server on page 377
  - Specifying a Secondary Server on page 380
- **Using Name Server Groups** on page 383
  - Adding Name Server Groups on page 383
  - Viewing Name Server Groups on page 384
  - Applying Name Server Groups on page 384
- **Importing Zone Data** on page 385
  - About Importing Data into a New Zone on page 386
  - About Importing Data into an Existing Zone on page 386
  - Importing Data into Zones on page 386
- **Configuring Authoritative Zone Properties** on page 387
- **Removing Zones** on page 389
- **Restoring Zone Data** on page 391
- **Configuring Delegated, Forward, and Stub Zones** on page 393
  - Configuring a Delegation on page 393
  - Configuring a Forward Zone on page 395
  - Configuring Stub Zones on page 398
- **Viewing Zones** on page 406
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 371
   — Creating an Authoritative Reverse-Mapping Zone on page 372
   — Creating a Root Zone on page 374
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 377.
3. Import resource records or add resource records manually. The following provides information about resource records:
   — Managing Resource Records on page 413
   — Importing Zone Data on page 385
4. Configure additional parameters. For information, see Configuring Authoritative Zone Properties on page 387.
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 611.
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 375.
   - **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 375.
4. Save the configuration, or click **Next** to continue to the next steps in the wizard as follows:
   - Define the name servers for the zone. 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 377.
     - For information on specifying name server groups, see **Using Name Server Groups** on page 383.
   - Define extensible attributes. For information, see **Using Extensible Attributes** on page 265.
   - 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 256.
5. Click **Restart** if it displays at the top of the screen.
Creating an Authoritative Reverse-Mapping Zone

An authoritative reverse-mapping zone is an area of network space for which one or more name servers—primary and secondary—have the responsibility to respond to address-to-name queries. Infoblox supports reverse-mapping zones for both IPv4 and IPv6 addresses.

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.

In addition to IPv4 reverse-mapping zones, you can also configure IPv4 reverse-mapping delegation zones that have an RFC2317 prefix. For more information about configuring a delegation for a reverse-mapping zone, see Configuring a Delegation on page 393.

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:
   - Enter one of the following to identify the zone:
     - 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 372.
     - 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.
About Authoritative Zones

— **Disable this zone:** Select this option to temporarily disable this zone. For information, see *Enabling and Disabling Zones* on page 375.

— **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 375.

4. Save the configuration, or click **Next** to continue to the next steps in the wizard as follows:

— Define the name servers for the zone. 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 377.
  — For information on specifying name server groups, see *Using Name Server Groups* on page 383.
  — Define extensible attributes. For information, see *Using Extensible Attributes* on page 265.

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 256.

5. Click **Restart** if it displays at the top of the screen.

**Adding an IPv6 Reverse-Mapping Zone**

To add an IPv6 reverse-mapping zone:

1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Add -> Zone -> Add Auth Zone**.

2. In the **Add Authoritative Zone** wizard, click **Add an authoritative IPv6 reverse-mapping zone** and click **Next**.

3. Enter the following zone information:

   — Enter one of the following to identify the zone:
     — **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 375.
     — **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 375.

4. Save the configuration, or click **Next** to continue to the next steps in the wizard as follows:

— Define the name servers for the zone. 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 377.
  — For information on specifying name server groups, see *Using Name Server Groups* on page 383.
  — Define extensible attributes. For information, see *Using Extensible Attributes* on page 265.

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 256.
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 465.

To create a root zone, create an authoritative forward-mapping zone as described in Creating an Authoritative Forward-Mapping Zone on page 371 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 393.

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 13.1 on page 375 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.
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 370.

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.
**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 13.1 on page 375 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 13.2 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 383.

**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 28, Managing Microsoft Windows Servers*, on page 753.

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 370. 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 378.
   - 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 379.
   - 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 379.
5. Save the configuration and click Restart if it displays at the top of the screen.
   or
   Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.

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. Save the configuration and click Restart if it displays at the top of the screen.
   or
   Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.
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 28, Managing Microsoft Windows Servers, on page 753.

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.
- **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.
- **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 370. 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 381.
   - **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 381.
   - **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 382.
5. Save the configuration and click Restart if it displays at the top of the screen. 
   or
   Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.
Assigning Zone Authority to Name Servers

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**: This setting applies only if the primary server is a Grid member or Microsoft server. Select this to hide the NS record for the secondary name server from DNS queries. The NIOS appliance does not create an NS record for this name server in the zone data. Select the check box again to display the NS record for the secondary name server in responses to queries. A secondary server in stealth mode is also known as a “hidden secondary”.

  For example, you can configure a hidden secondary when a secondary server is at a branch office with a slow connection to the rest of corporate network. Configure local hosts at the branch office to send DNS queries to the secondary server, but keep it hidden from other name servers on the rest of the network so that they do not send it queries. Instead, they use a server located in a different part of the network that has faster connection speeds.

- **Lead Secondary**: This option becomes available only after you specify the primary name server as external. When a primary server is external to a Grid whose members are secondary servers, you can select this check box to designate one member as a lead secondary. The primary server sends zone transfers to the lead secondary, which distributes the zone data to the other secondary servers in the Grid using zone transfers (not the Grid data replication mechanism). After you designate a Grid member as a lead secondary for a zone, you do not have to configure members to use the lead secondary server. All other Grid members acting as secondary servers for the zone automatically use the lead secondary to get zone data. Using a lead secondary simplifies the addition, modification, and removal of other secondary servers in the Grid. As long as the lead secondary remains unchanged, you need not update intervening firewall policies or the external primary server whenever you make changes to non-lead secondary Grid members. This approach also reduces the amount of traffic between primary and secondary servers.

- **Update Zones Using**: This option becomes available only after you specify a Grid member as the primary server.
  - **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 28, Managing Microsoft Windows Servers*, on page 753.

Since Microsoft servers cannot replicate data from the Grid, when a DNS zone is defined as a secondary on a Microsoft server, the Microsoft server obtains the content of the zone only through DNS zone transfers.

- In the Add Microsoft Secondary panel, do the following:
  - If no server is displayed, click **Select Server** to specify a Microsoft server. When there are multiple servers, Grid Manager displays the Server Selector dialog box from which you can select a Microsoft server. Grid Manager lists Microsoft servers that are managed in read/write mode. It does not include Microsoft servers managed in read-only mode.
  - **Information to create NS record**: Grid Manager automatically creates the NS record. After you select a server, Grid Manager populates the **Name** and **IP Address** fields. Grid Manager uses this information when it creates the NS record, unless you select Stealth.
  - **Stealth**: This setting applies only if the primary server is a Grid member or a Microsoft server. Select this option to hide the NS record for the secondary name server from DNS queries. Grid Manager does not create an NS record for this name server in the zone data. Clear this option to display the NS record for the secondary name server in responses to queries.
Specifying External Secondaries

In the Add External Secondary panel, enter the following, and then click Add to add the external secondary server to the list of name servers for the zone:

- **Name**: Enter a resolvable domain name for the external secondary server.
- **Address**: Enter the IP address of the external secondary server.
- **Stealth**: This setting applies only if the primary server is a Grid member or a Microsoft server. Click this check box to hide the NS record for the secondary name server from DNS queries. The NIOS appliance does not create an NS record for the secondary name server in the zone data. Select the check box again to display the NS record for the secondary name server in 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 378.
     - Grid Secondary: Choose this option to select a Grid member as a secondary server for the zone. See Adding Grid Secondaries on page 381.
     - 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 379.
     - 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 382.
   - Default NS Group: Select this to specify this name server group as the default.
   - Comment: Optionally, enter additional information about the NS group.

3. Save the configuration and click Restart if it displays at the top of the screen, or click Next to define extensible attributes. For information, see Using Extensible Attributes on page 265.

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:

- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 57.
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables on page 52.
- 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 370. 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 13.3 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 463. 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 370. 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 377.
   - **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 443.
     - Override the email settings, as described in Adding an Email Address to the SOA Record on page 444.
     - 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 378.
     - Don’t use forwarders to resolve queries in subzones: If the DNS members are configured to use forwarders to resolve queries that they cannot resolve locally, you can select this check box to disable the use of forwarders to resolve queries for data in the subzones.
   - **Queries**: Set restrictions for queries as described in Controlling DNS Queries on page 450.
   - **Zone Transfers**: Specify to which servers zone transfers are allowed as described in Enabling Zone Transfers on page 463.
   - **Updates**: Set dynamic DNS update properties as described in Configuring DNS Servers for DDNS on page 495.
   - **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 498.
   - **Extensible Attributes**: Define extensible attributes. For information, see Using Extensible Attributes on page 265.
   - **Permissions**: Define administrative permissions. For information, see About Administrative Permissions on page 120.
3. Click Toggle Expert 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 611.
     - **Host Naming**: Set restrictions for host names. For information, see Specifying Hostname Policies on page 470.
— **Shared Record Groups:** Add shared record groups to a zone. For information, see *About Shared Record Groups* on page 432.

— **DNSSEC:** Configure DNSSEC properties. For information, see *Chapter 17, DNSSEC,* on page 523.

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

   or

   Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 256.
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 13.4.

Figure 13.4 Removing or Reparenting Subzones

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, domainDNSzones, 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 13.5.
Configuring DNS Zones

Figure 13.5 Changed Admin Access Settings after Reparenting Subzones

If you remove Zone B and … … reparent its subzones …

Zone A
Read/Write

Zone B
Deny

Subzone C
Inherits “Deny”

Zone A
Read/Write

Subzone C
Inherits “Read/Write”

… the admin access settings for subzone C change because the privileges for its new parent zone (zone A) are different from those of its previous parent zone (zone B).

Before you remove zone B, subzone C inherits a “Deny” admin access setting from zone B. After the removal, subzone C inherits “Read/Write” access from its new parent zone, zone A.

Note that if you set a specific “Deny” admin access privilege for subzone C before removing its parent zone (zone B), subzone C retains its specified “Deny” setting.

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.

You can also schedule the deletion for a later time. Click Schedule Deletion and in the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.

Note: Instead of removing a zone, you can also disable it. For more information, refer to Enabling and Disabling Zones on page 375.
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 391. 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 392.

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 389.
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 13.6:

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 13.6 Restoring Zones After a Zone Import
Restoring Zone Data After a Zone Reimport Example

In the example shown in Figure 13.7:

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 13.7  Restoring Zones After a Zone Reimport

---

**Diagram Description**

1. You import subzones x and y into Zone B.
2. To restore Zone B after the import, delete the delegated subzones x and y under Zone B and then remove Zone B by selecting the **Remove Zone only** option.
3. Restore Zone B and subzones x and y from the Recycle Bin. The appliance reparents its subzones B1 and B2 back to Zone A.
Configuring Delegated, Forward, and Stub Zones

In addition to authoritative zones, the NIOS appliance allows you to configure delegated, forward, and stub zones. A delegated zone is a zone managed by (delegated to) another name server who owns the authority for the zone. A forward zone is where queries are sent before being forwarded to other remote name servers. A stub zone contains records that identify the authoritative name servers in another zone. This section covers the following topics:

- Configuring a Delegation
- Configuring a Forward Zone
- Configuring Stub Zones

Configuring a Delegation

Instead of a local name server, remote name servers (which the local server knows) maintain delegated zone data. When the local name server receives a query for a delegated zone, it either responds with the NS record for the delegated zone server (if recursion is disabled on the local server) or it queries the delegated zone server on behalf of the resolver (if recursion is enabled).

For example, there is a remote office with its own name servers, and you want it to manage its own local data. On the name server at the main corporate office, define the remote office zone as delegated, and then specify the remote office name servers as authorities for the zone.

You can delegate a zone to one or more remote name servers, which are typically the authoritative primary and secondary servers for the zone. If recursion is enabled on the local name server, it queries multiple delegated name servers based on their round-trip times.

You can also 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 443.

The delegation must exist within an authoritative zone with a Grid primary server.

Configuring a Delegation for a Forward-Mapping Zone

To create a delegation for a forward-mapping zone:

1. From the Data Management tab, select the DNS tab -> Zones tab.
2. Click the parent zone to open it.
3. From the Subzones tab, click the Add icon -> Zone -> Add Delegation.
4. In the Add Delegation wizard, specify the following:
   - Name: This field displays a dot followed by the domain name of the current zone. Enter one or more labels before the dot to specify the domain name of the subzone.
   - DNS View: This field displays only when there is more than one DNS view in the network view. Displays the DNS view of the current zone.
   - Comment: Optionally, enter additional text about the zone.
   - Disable: Click this check box to temporarily disable this zone. For information, see Enabling and Disabling Zones on page 375
   - 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 375.
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. Save the configuration and click **Restart** if it displays at the top of the screen, or click **Next** to define extensible attributes as described in *Using Extensible Attributes* on page 265.

   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 256.

---

### Configuring a Delegation for a Reverse-Mapping Zone

To create a delegation for a reverse-mapping zone:

1. From the **Data Management** tab, select the **DNS** tab -> **Zones** tab.
2. Click the parent zone to open it.
   
   Grid Manager displays the **Records** and **Subzones** tabs of the zone.
3. From the **Subzones** tab, click the Add icon -> **Zone** -> **Add Delegation**.
4. In the **Add Delegation** wizard, specify the following:
   
   — **IPv4 Network**: This field displays if you are creating a delegation zone for an IPv4 reverse-mapping zone. Enter the IPv4 address for the address space for which you want to define the reverse-mapping zone and select a netmask from the Netmask drop-down list. Alternatively, you can specify the address in CIDR format, such as 192/8.
     
     To use an RFC 2317 prefix, select a netmask value that is between 25 to 31, inclusive. Grid Manager displays the following fields:
     
     **RFC 2317 Prefix**: Enter a prefix in this field. Prefixes can include alphanumeric characters. Though spaces are allowed, Grid Manager displays a warning when a prefix includes a space.
     
     **Allow manual creation of PTR records in parent zone**: Select this check box to allow users to create labels that correspond to IP addresses in the delegated address space in the parent zone.
     
     For information about RFC 2317, see *Specifying an RFC 2317 Prefix* on page 372.
   
   — **IPv6 Network Prefix**: This field displays if you are creating a delegation zone for an IPv6 reverse-mapping zone. Enter the IPv6 prefix for the address space for which you want to define the reverse-mapping zone and select the prefix length from the drop-down list.
   
   — **Name**: This field displays a dot followed by the domain name of the current zone. Enter one or more labels before the dot to specify the domain name of the subzone.
   
   — **DNS View**: This field displays only when there is more than one DNS view in the network view. Select a DNS view from the drop-down list.
   
   — **Comment**: Optionally, enter additional text about the zone.
   
   — **Disable**: Select this option to temporarily disable this zone.
   
   — **Lock**: Select this option to lock the zone so that you can make changes to it and prevent others from making conflicting changes.

5. Click **Next** to 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. Save the configuration and click **Restart** if it displays at the top of the screen, or click **Next** to define extensible attributes as described in *Using Extensible Attributes* on page 265.

   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 256.
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 449.) 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. Save the configuration and click Restart if it displays at the top of the screen, or click Next to continue to the next step where you select the appliance on which the forward zone is configured.
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. Save the configuration, or click Next to continue to the next step where you define extensible attributes as described in Using Extensible Attributes on page 265, and then optionally proceed to the next step where you define admin permissions as defined in About Administrative Permissions on page 120.
   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 256.
8. Click Restart if it displays at the top of the screen.

To configure a forward IPv4 reverse-mapping zone:

1. From the Data Management tab, select the Zones tab, expand the Toolbar and click Add --> Zone --> Add Forward Zone.
2. In the Add Forward Zone wizard, click Add a forward IPv4 reverse-mapping zone and click Next.
3. Enter the following information, and then click **Next**:
   - **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 372.
   - **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. Save the configuration, or click **Next** to continue to the next step where you select the NIOS appliance from which you want to forward queries.

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. Save the configuration, or click **Next** to continue to the next step where you define extensible attributes as described in **Using Extensible Attributes** on page 265.
   - 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 256.

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

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. Save the configuration, or click **Next** to continue to the next step where you select the NIOS appliances from which you want to forward queries.

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. Click **Next** to continue to the next step where you define extensible attributes as described in *Using Extensible Attributes* on page 265 or save the configuration and click **Restart** if it displays at the top of the screen.

   or

   Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 256.
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 13.8** and **Figure 13.9** illustrate how the NIOS appliance resolves a query for a domain name for which it is not authoritative. **Figure 13.8** illustrates how the appliance resolves a query when it does not have a stub zone. **Figure 13.9** illustrates how the appliance resolves the query with a stub zone.

In **Figure 13.8**, 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 13.8  Processing a Query without a Stub Zone*
In Figure 13.9, 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 13.9 Processing a Query with a Stub Zone**

2. The appliance has a corp200.com stub zone.
3. The appliance send a query directly to a corp200.com server...
   ... which respond with a referral to the sales.corp200.com servers.
4. The appliance send a query to a sales.corp200.com server.
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 13.10 on page 400. 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 13.10  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 13.10, 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 753.

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 447.

— 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. Click Next to continue to the next step where you define extensible attributes as described in Using Extensible Attributes on page 265.

7. Save the configuration and click Restart if it displays at the top of the screen or
   Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.

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 372.
   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 447.
   — 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. Click **Next** to continue to the next step where you define extensible attributes as described in *Using Extensible Attributes* on page 265.

7. Save the configuration and click **Restart** if it displays at the top of the screen
   or
   Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 256.

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:0000:cdef. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The NIOS appliance displays an IPv6 address in its shortened form, regardless of its form when it was entered. 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 447.
   - 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. Click **Next** to continue to the next step where you define extensible attributes as described in *Using Extensible Attributes* on page 265.
7. Save the configuration and click **Restart** if it displays at the top of the screen
   or
   Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 256.
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. Save the configuration and click Restart if it displays at the top of the screen.

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

Create the Views

Create the internal and external views. To create each view:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add DNS View.
2. In the Add DNS View wizard, enter the name of the view. In this example, enter either External or Internal.
3. Click Save & New and create the other DNS view.
Create the Zones

Create the 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. Save the configuration and click Restart if it displays at the top of the screen.

After you create the zone, you can view the NS and A records which were automatically created.

Create the stub zone, 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. Save the configuration and click Restart if it displays at the top of the screen.

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 365.)

- 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 Server:** When a zone is served by multiple Microsoft servers, this column shows which Microsoft server is actually performing the synchronization of that zone with the Grid.
- **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.
- Use filters and the **Go to** function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the **Go to** field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see [Using Quick Filters](#) on page 57.
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see [Modifying Data in Tables](#) on page 52.
- 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 14  DNS Resource Records

This chapter provides general information about Infoblox host records and DNS resource records. The topics in this chapter include:

- **About Bulk Hosts** on page 408
  - Specifying Bulk Host Name Formats on page 408
  - Before Defining Bulk Host Name Formats on page 408
  - Adding Bulk Hosts on page 411
- **Managing Resource Records** on page 413
  - Managing A Records on page 414
  - Managing NS Records on page 415
  - Managing AAAA Records on page 416
  - Managing PTR Records on page 417
  - Managing MX Records on page 418
  - Managing SRV Records on page 419
  - Managing TXT Records on page 420
  - Managing CNAME Records on page 421
  - Managing DNAME Records on page 423
  - Managing NAPTR Records on page 429
  - Modifying, Disabling, and Deleting Host and Resource Records on page 431
- **About Shared Record Groups** on page 432
  - Shared Records Guidelines on page 433
  - Configuring Shared Record Groups on page 433
  - Managing Shared Resource Records on page 435
  - Managing Associated Zones on page 438
  - Configuration Example: Configuring Shared Records on page 439
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-xx for bulk hosts. Ensure that the bulk host name does not conflict with CNAMEs, DNAMEs, or host name aliases.
- When you add a bulk host, if you enable the Automatically add reverse mapping option and there is a CNAME record in the corresponding reverse zone that conflicts with a PTR record generated by the bulk host, the bulk host insertion fails and an error message appears. For example, if there is a CNAME with the alias 15 in a reverse zone 1.168.192.in-addr.arpa and if you add a bulk host foo/192.168.1.10/192.168.1.20 with the Automatically add reverse mapping option selected, the insertion fails and an error message appears because both the bulk host and the CNAME generate a record 15.1.168.192.in-addr.arpa in the reverse zone.
- You cannot create or change a bulk host if a zone is locked by another user. If you select a different template for the Grid, it changes each record associated with the bulk host.
- You can define bulk host name formats only at the Grid level and override them at the bulk host level; not at the zone or bulk host object level.
- When you upgrade to NIOS 4.3r3 or earlier releases, the system migrates existing bulk hosts as follows:
  - If you did not customize the bulk host IP format, there is no action required. All migrated bulk hosts continue to use the Grid-level default four-octet format -$1-$2-$3-$4. See Specifying Bulk Host Name Formats on page 408.
  - 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 14.1* 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 14.1  Bulk Host Name Format Rules and Examples*

<table>
<thead>
<tr>
<th>Rule</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>The suffix format cannot have more than four octets.</td>
<td>-$4-$5 is invalid.</td>
</tr>
<tr>
<td>The octets must be in order.</td>
<td>-$2-$3-$4 is valid but -$3-$2-$4 is invalid.</td>
</tr>
<tr>
<td>Do not skip octets.</td>
<td>-$2-$3-$4 is valid but -$2-$4 is invalid.</td>
</tr>
<tr>
<td>Do not use a combination of both the $ and # symbols together as octet references; use only one of them.</td>
<td>-$2-$3-$4 is invalid.</td>
</tr>
<tr>
<td>The suffix format must contain at least the fourth octet. You must define at least one -$4 or -#4.</td>
<td>-$4 is valid but -$3 is invalid.</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 digit. You must add a non-digit prefix to each $ or # reference.</td>
<td>-$2-$3-$4</td>
</tr>
<tr>
<td>The \ character is the designated escape character for the $, # and \ characters. You cannot use the $ or # symbols as separators unless you prefix them with an escape character .</td>
<td>For the IP address 10.19.32.133, the format #-#1-#2-#3-#4 expands to #-010-019-032-133.</td>
</tr>
<tr>
<td>The bulk host name format must comply with its zone host name policy.</td>
<td>You cannot insert a bulk host name format -$?-?$4 in a zone that uses Allow Underscore as host name policy because the policy does not allow you to use the ? character in the host name.</td>
</tr>
<tr>
<td>The bulk host name must comply with the maximum label length.</td>
<td>The sum of the bulk host name prefix and suffix cannot be greater than 63 characters. When you enter a suffix format, the NIOS appliance determines the length of the longest bulk host defined, and checks that the sum of the bulk host prefix and suffix length does not exceed 63 characters; if it does, an error message appears.</td>
</tr>
<tr>
<td>The bulk host name cannot result in an FQDN with more than 255 characters.</td>
<td></td>
</tr>
<tr>
<td>The NIOS appliance computes the maximum length of the bulk host suffix by expanding the bulk host IP format using 255.255.255.255.</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.
3. Click Add to enter the name and format of a new bulk host name format.
4. Optionally, click the Default column of a format and select Default to make it the Grid default.
5. Save the configuration and click Restart if it appears at the top of the screen.

### Table 14.1 Bulk Host Name Format Rules and Examples

<table>
<thead>
<tr>
<th>Rule</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>The bulk host name must not be the same as a CNAME/DNAME.</td>
<td>If there is a CNAME record with alias foo-003-015, you cannot insert a bulk host foo/1.2.3.10/1.2.3.20 using template -#3-#4 because foo-003-015 is also one of the synthetic host names in the bulk host.</td>
</tr>
<tr>
<td>Each host name in the bulk host must be unique.</td>
<td>You cannot insert a bulk host foo/1.2.3.10/1.2.4.20 using the template -4 because the system resolves the host name foo-10 to both 1.2.3.10 and 1.2.4.10. To ensure that the bulk host name is unique, use the template -3-4.</td>
</tr>
<tr>
<td>You cannot insert a bulk host that violates the uniqueness of two bulk hosts that have the same prefix and use the same name format.</td>
<td>If there is a bulk host foo/1.2.3.10/1.2.4.20 using the template -3-4, you cannot insert another bulk host foo/1.3.4.10/1.3.5.20 using the same template because the system resolves host name foo-4-15 to both 1.2.4.15 and 1.3.4.15. Instead, use the template -2-$3-4 to ensure that the two bulk hosts are unique.</td>
</tr>
</tbody>
</table>
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.
   - DNS View: Displays the DNS view of the zone to which the bulk host records belong.
   - Host Name Policy: Displays the host name policy of the selected DNS zone.
   - Name Format: To override the default four-octet suffix format or the format set at the Grid level, and specify a different format, click Override and select a host name format from the Name Formats drop-down menu. The Name Formats drop-down menu lists the formats Four Octets, Three Octets, Two Octets, and One Octet along with any other bulk host name formats that you have defined.
   - Starting IP Address: Enter the first IP address in the range of addresses for the group.
   - End IP Address: Enter the last IP address in the range of addresses for the group.
   - Comment: Optionally, enter additional information for this record.
   - Automatically Add Reverse Mapping: Click to have the appliance automatically create a PTR record for each IP address within the bulk host range.
   - Disable: Clear the check box to enable the record. Select the check box to disable it.
3. Click Next to define extensible attributes for the bulk host record. For information, see Using Extensible Attributes on page 265.
4. Save the configuration and click Restart if it appears at the top of the screen.

To modify or delete a bulk host, see Modifying, Disabling, and Deleting Host and Resource Records on page 431.
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 414.
- **NS (Name server)**—For information, see Managing NS Records on page 415.
- **AAAA (IPv6 Address)**—For information, see Managing AAAA Records on page 416.
- **PTR (Pointer)**—For information, see Managing PTR Records on page 417.
- **MX (Mail exchanger)**—For information, see Managing MX Records on page 418.
- **SRV (Service location)**—For information, see Managing SRV Records on page 419.
- **TXT (Text)**—For information, see Managing TXT Records on page 420.
- **CNAME (Canonical name)**—For information, see Managing CNAME Records on page 421.
- **DNAME**—For information, see Managing DNAME Records on page 423.
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 611.

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.
   — Shared Record Group: This field appears only when you are creating a shared record. Click Select Shared Record Group. If you have only one shared record group, the appliance displays the name of the shared record group here. If you have multiple shared record groups, select the shared record group in the Shared Record Group Selector dialog box. You can use filters or the Go to function to narrow down the list.
   — Hostname Policy: Displays the hostname policy of the zone.
   — In the IP Addresses section, click the Add icon and do one of the following:
     — Select Add Address to enter the IPv4 address to which you want the domain name to map.
     or
     — Select Next Available IPv4 to retrieve the next available IP address in a network.
     If the A record is in a zone that has associated networks, the Network Selector dialog box lists the associated networks. If the zone has no network associations, the Network Selector dialog box lists the available networks. When you select a network, Grid Manager retrieves the next available 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. Click Next to define extensible attributes. For information, see Using Extensible Attributes on page 265.
4. Save the configuration and click Restart if it appears at the top of the screen.
Modifying A Records

When you modify an A record, you can do the following:

- In the General tab, you can change the information you previously entered through the wizard, as described in Adding A Records on page 414.
- The Discovered Data tab displays discovered data, if any, for the record. For information, see Viewing Discovered Data on page 858.

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 431.

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 About Anycast Addressing for DNS on page 555.

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. Click Next to define extensible attributes, or save the configuration and click Restart if it appears at the top of the screen.
Modifying and Deleting NS Records

When you modify an NS record, you can change the following information:

- In the **General** tab, you can change the name server name.
- In the **Addresses** tab, you can do the following:
  - Delete an address by selecting it and clicking the Delete icon.
  - Add an address by clicking the Add icon, and then entering the IP address and completing the Add PTR Record field.

Managing AAAA Records

An AAAA (quad A address) record maps a domain name to an IPv6 address. To define a specific name-to-address mapping, add an AAAA record to a previously defined authoritative forward-mapping zone. If the zone is associated with one or more networks, the IP address must belong to one of the associated networks. For example, if the AAAA record is in the 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 611.

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.
   - **Shared Record Group**: This field appears only when you are creating a shared record. Click **Select Shared Record Group**. If you have only one shared record group, the appliance displays the name of the shared record group here. If you have multiple shared record groups, select the shared record group in the **Shared Record Group Selector** dialog box. You can use filters or the **Go to** function to narrow down the list.
   - **Hostname Policy**; Displays the hostname policy of the zone.
   - **IP Address**: Enter the IPv6 address to which you want the domain name to map. When you enter an IPv6 address, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2006:0000:0000:0123:4567:89ab:0000:cdef can be shortened to 2006::123:4567:89ab:0:cdef. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The NIOS appliance displays an IPv6 address in its shortened form, regardless of its form when it was entered.
   - **Comment**: Optionally, enter additional information about this record.
   - **Disable**: Clear the check box to enable the record. Select the check box to disable it.
3. Click **Next** to define extensible attributes. For information, see *Using Extensible Attributes* on page 265.
4. Save the configuration and click **Restart** if it appears at the top of the screen.
Modifying AAAA Records

When you modify an AAAA record, you can do the following:
- In the General tab, you can change the information you previously entered through the wizard.
- In the Discovered Data tab, you can view discovered data, if any, for the record. For information, see Viewing Discovered Data on page 858.

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 431.

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. Save the configuration, or click Next to define extensible attributes. For information, see Using Extensible Attributes on page 265.
4. Click Restart if it appears at the top of the screen.

Modifying PTR Records

When you modify a PTR record, you can do the following:
- In the General tab, you can change the information you previously entered through the wizard.
- In the Discovered Data tab, you can view discovered data, if any, for the record. For information, see Viewing Discovered Data on page 858.

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 431.
### 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 14.1.*

**Figure 14.1 MX Records**

The following MX records … … direct queries for one or more domains … … to the same mail exchanger:

An MX record for the mail exchanger that answers queries for just the 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 from the Tasks Dashboard, see *Add MX Record* on page 76. You can also add MX records from the Data Management tab ->DNS tab by clicking *Add ->Record ->Add MX Record* from the Toolbar.

### Modifying and Deleting MX Records

When you modify an MX record, you can change the information you previously entered in the General tab. You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see *Modifying, Disabling, and Deleting Host and Resource Records* on page 431.
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.
   - **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.
   - **Shared Record Group**: This field appears only when you are creating a shared record. Click Select Shared Record Group. If you have only one shared record group, the appliance displays the name of the shared record group here. If you have multiple shared record groups, select the shared record group in the Shared Record Group Selector dialog box. You can use filters or the Go to function to narrow down the list.
   - **Priority**: Select or enter an integer from 0 to 65535. The priority determines the order in which a client attempts to contact the target host; the domain name host with the lowest number has the highest priority and is queried first. Target hosts with the same priority are attempted in the order defined in the Weight field.
   - **Weight**: Select or enter an integer from 0 to 65535. The weight allows you to distribute the load between target hosts. The higher the number, the more that host handles the load (compared to other target hosts). Larger weights give a target host a proportionately higher probability of being selected.
   - **Port**: Specify the appropriate port number for the service running on the target host. You can use standard or nonstandard port numbers, depending on the requirements of your network. You can select a port number from the list or enter an integer from 0 to 65535.
   - **Target**: Enter the canonical domain name of the host (not an alias); for example, www2.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. Save the configuration, or click Next to define extensible attributes. For information, see Using Extensible Attributes on page 265.

4. Click Restart if it appears at the top of the screen.

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 431.

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 an TXT record from the Tasks Dashboard, see Add TXT Record on page 75. You can also add TXT records from the Data Management tab ->DNS tab by clicking Add ->Record ->Add TXT Record from the Toolbar.

Modifying and Deleting TXT Records

When you modify a TXT record, you can change the information you previously entered in the General tab. You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records on page 431.
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 from the Tasks Dashboard, see Add CNAME Record on page 75. You can also add CNAME records from the Data Management tab ->DNS tab by clicking Add ->Record ->Add CNAME Record from the Toolbar.

CNAME Records in IPv4 Reverse-Mapping Zones

You can add CNAME records to an IPv4 reverse-mapping zone to create aliases to addresses maintained by a different name server when the reverse-mapping zone on the server is a delegated child zone with fewer than 256 addresses. This technique allows you to delegate responsibility for a reverse-mapping zone with an address space of fewer than 256 addresses to another authoritative name server. See Figure 14.2 and RFC 2317, Classless IN-ADDR.ARPA delegation.
You add CNAME records in the parent zone on your name server. The aliases defined in those CNAME records point to the addresses in PTR records in the child zone delegated to the other server.

When you define a reverse-mapping zone that has a netmask from /25 (255.255.255.128) to /31 (255.255.255.254), you must include an RFC 2317 prefix. This prefix can be anything, from the address range (examples: 0-127, 0/127) to descriptions (examples: first-network, customer1). On a NIOS appliance, creating such a reverse-mapping zone automatically generates all the necessary CNAME records. However, if you need to add them manually to a parent zone that has a child zone with fewer than 255 addresses.

**Adding CNAME Records**

To add a CNAME record to a forward-mapping or reverse-mapping zone from the Tasks Dashboard, see Add CNAME Record on page 75. You can also add CNAME records from the Data Management tab ->DNS tab by clicking Add -> Record ->Add CNAME Record from the Toolbar.

**Modifying and Deleting CNAME Records**

When you modify a CNAME record, you can change the information you previously entered in the General tab. You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records on page 431.
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>=&gt; server1.corp200.com</td>
</tr>
<tr>
<td>server2.corp100.com</td>
<td>=&gt; server2.corp200.com</td>
</tr>
<tr>
<td>server3.corp100.com</td>
<td>=&gt; server3.corp200.com</td>
</tr>
<tr>
<td>....corp100.com</td>
<td>=&gt; ....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


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 14.3 on page 424.
Corp200 buys Corp100 and wants to redirect queries for corp100.com to corp200.com; however, the multilayered 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 14.4.

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 14.4, 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.
Managing Resource Records

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 385.

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 14.5 on page 425). By doing this, you can continue to maintain resource records on the same server, potentially simplifying the continuation of DNS administration.

Figure 14.5 Making the Target Zone a Delegated Zone

The following tasks walk you through configuring the two appliances in Figure 14.5 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.

   Note: Because you can only specify the records by type, not individually, you might have to copy some records that you do not want and then delete them from the corp100.corp200.com zone.

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 393.
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. Save the configuration, or click Next to define extensible attributes. For information, see Using Extensible Attributes on page 265.
4. Click Restart if it appears at the top of the screen.

DNAME Records for Reverse-Mapping Zones

You can use DNAME records to redirect reverse lookups from one reverse-mapping zone to another. You can use DNAME records for reverse-mapping zones to simplify the management of subzones for classless address spaces larger than a class C subnet (a subnet with a 24-bit netmask).

RFC 2672, Non-Terminal DNS Name Redirection, includes an example showing the delegation of a subzone for an address space with a 22-bit netmask inside a zone for a larger space with a 16-bit netmask:

```
$ORIGIN 0.192.in-addr.arpa.
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 14.6**.

**Figure 14.6 DNAME Records to Simplify DNS for Multihomed Appliances**

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.

Note: If you specify a subdomain in the Domain Name field when configuring a DNAME record, and the subdomain is also a subzone, the DNAME record appears in the list view for the subzone, not in the list view for the parent zone that was selected when adding it.
To add a DNAME record to a reverse-mapping zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> Add DNAME Record.

2. In the Add DNAME Record wizard, complete the following fields:

   - **Alias**: If Grid Manager displays a zone name, enter the name of a subdomain here. If you are adding a DNAME record for the entire zone, leave this field empty. This field is for adding a DNAME record for a subdomain within the selected zone. The displayed zone name can either be the last selected zone or the zone from which you are adding the CNAME record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box, and then enter the name of a subdomain.

   - **Target**: Type the name of the reverse-mapping zone to which you want to map all the addresses specified in the Domain Name field.

   - **Comments**: Enter identifying text for this record, such as a meaningful note or reminder.

   - **Disable**: Clear the check box to enable the record. Select the check box to disable it.

3. Save the configuration, or click Next to define extensible attributes. For information, see Using Extensible Attributes on page 265.

4. Click Restart if it appears at the top of the screen.

**Modifying and Deleting DNAME Records**

When you modify a CNAME record, you can change the information you previously entered in the General tab. You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records on page 431.
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:

```
$ORIGIN 7.6.5.4.3.2.1.5.5.1.e164.arpa
IN NAPTR 10 100 "U" "sip + E2U" "!^.*$!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.
   - **Replacement**: This specifies the domain name for the next lookup. The default is a dot (.), which indicates
     that the regular expression in the **REGEX** field provides the replacement value. Alternatively, you can enter
     the replacement value in FQDN format.
   - **Comment**: Optionally, enter a descriptive comment for this record.
   - **Disable**: Clear the check box to enable the record. Select the check box to disable it.

3. Save the configuration, or click **Next** to define extensible attributes. For information, see Using Extensible
   Attributes on page 265.

4. Click **Restart** if it appears at the top of the screen.
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 443.
   - In the Extensible Attributes tab, you can modify the attributes. For information, see Using Extensible Attributes on page 265.
   - The Permissions tab displays if you logged in as a superuser. For information, see About Administrative Permissions on page 120.
4. Save the configuration and click Restart if it appears at the top of the screen.

When you delete host and resource records, Grid Manager moves them to the Recycle Bin. You can use the Recycle Bin to store deleted DNS configuration objects and selectively restore objects to the active configuration at a later time. You can also permanently remove the objects from the Recycle Bin.

Note: You cannot delete automatically-generated records, such as NS records and SOA records.

To delete host and resource record:
1. Perform a global search to retrieve the record you want to delete.
   or
   - From the Data Management tab, select the DNS tab, click the Zones tab -> dns_view -> zone -> host_record or resource_record.
2. Select the record and click the Delete icon.
3. 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 14.7* shows an example of how to create and use shared records.

In this example, there are two shared record groups. One group—group1—contains the A records ftp and printer1 and the MX record mx1, and the other group—group2—contains the A record web and the MX record mx2. The resource records in group1 are shared with the internal view zones sales.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 14.7 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 433.
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 435.

Creating a Shared Record Group

When you create a shared record group, the only requirement is that you give it a name. You can associate it with one or multiple zones when you first create the group or at a later time, by editing the shared record group. You can associate a shared record group with authoritative zones only. Associating the shared record group with a zone adds the shared records to the zone. The zone handles the shared records like any other resource records.

To create a shared record group:

1. From the Data Management tab, select the DNS tab -> Shared Record Groups tab, and then click the Add icon.
2. In the Shared Record Group wizard, specify the following:
   - Name: Enter the name of the shared record group. It can be up to 64 characters long and can contain any combination of printable characters. You can change the shared record group name even after you create the group. It does not impact the shared records in the group.
   - Hostname Policy: Click Override to supersede the hostname restriction policy set at the zone level or click Inherit to use the zone policy. This sets the hostname policy for the shared records in the group. See Specifying Hostname Policies on page 470.
   - Comment: Optionally, enter additional information about the shared record group.
3. Click Next to associate the shared record group with at least one zone.
4. Click the Add icon in the Associated Zones panel.
5. In the Zone Selector dialog box, select a zone by clicking the zone name. You can add multiple zones.
6. Click Next to define extensible attributes. For information, see Using Extensible Attributes on page 265.
7. Save the configuration.
Viewing Shared Record Groups

You can view the configured shared record groups by navigating to the Data Management tab -> DNS tab -> Shared Record Groups tab. Grid Manager displays the following information about each shared record group:

- **Name:** The shared record group name.
- **Comment:** Comments that were entered for the shared record group.
- **Site:** Values that were entered for this pre-defined attribute.

You can do the following:

- List the shared resource records and associated zones in a shared record group.
  - Click a shared record group name.

- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.

- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 57.

- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables on page 52.

- Edit the properties of a shared record group.
  - Click the check box beside a shared record group, and then click the Edit icon.

- Delete a shared record group.
  - Click the check box beside a shared record group, and then click the Delete icon. Note that you must remove the zone associations in a shared record group before you delete it.

- Export the list of shared record groups to a .csv file.
  - Click the Export icon.

- Print the list of shared record groups.
  - Click the Print icon.

Modifying a Shared Record Group

When you edit a shared record group, you can do the following:

1. Perform a global search to retrieve the shared record group you want to modify.
   or
   From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> shared_record_group check box, and then click the Edit icon.

2. The Shared Record Group editor contains the following tabs from which you can modify information:
   - **General:** You can change any of the information you entered when you created it, including its name. Changing the shared record group name does not impact the shared resource records in it.
   - **Extensible Attributes:** You can modify the attributes. For information, see Using Extensible Attributes on page 265.
   - **Permissions:** This tab is displayed if you logged in as a superuser. For information, see About Administrative Permissions on page 120.

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

Deleting Shared Record Groups

Before you delete a shared record group, you must remove the zone associations in the group; otherwise, an error message appears when you delete. For information, see Deleting Associated Zones on page 438.

To delete a shared record group:

1. Perform a global search to retrieve the shared record group you want to modify.
   
or
   
   From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> shared_record_group check box, and then click the Delete icon.

2. In the Delete Confirmation dialog box, click Yes.

Grid Manager moves the shared record group to the Recycle Bin, if enabled. Use the Recycle Bin feature to recover a deleted shared record group and retrieve the deleted zones. For information, see Using the Recycle Bin on page 54.

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
• Viewing Shared Records on page 436
• Modifying Shared Records on page 437
• Deleting Shared Records on page 437

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. Expand the Shared Records tab and click the Add icon.

2. Select one of the following:
   — Shared A Record
   — Shared AAAA Record
   — Shared MX Record
   — Shared SRV Record
   — Shared TXT Record

3. Enter information in the Shared Record wizard. See the online Help or the following for information about each resource record:
   — For information about A records, see Managing A Records on page 414.
   — For information about AAAA records, see Managing AAAA Records on page 416.
   — For information about MX records, see Managing MX Records on page 418.
   — For information about SRV records, see Managing SRV Records on page 419.
   — For information about TXT records, see Managing TXT Records on page 420.

4. Save the configuration, or click Next to define extensible attributes for the shared record. For information, see Using Extensible Attributes on page 265.

5. Click Restart if it appears at the top of the screen.
Viewing Shared Records

You can view the shared records in a group and in a zone. To edit the shared record properties, click the shared record name and select the Edit icon.

To view the shared records in a group:

- From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> shared_record_group -> Shared Records tab.

To view the shared records in a zone:

- From the Data Management tab, select the DNS tab -> Zones tab and select a zone.

Grid Manager lists the following information about each shared record by default:

- Name: The shared record name.
- Type: Indicates the type of resource record, such as A, AAAA, MX, SRV or TXT records. Shared records are identified as (Shared).
- Data: The data the shared resource record provides.
- Comment: Comments that were entered in the resource record.
- Site: Displays values that were entered for this pre-defined attribute.

You can display the following additional columns:

- TTL: The TTL value of the shared resource record.
- Disabled: Indicates whether the record is disabled.

You can do the following:

- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 57.
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables on page 52.
- Edit the properties of a shared resource record.
  — Select the shared resource record, and then click the Edit icon.
- Delete a shared resource record.
  — Select the shared resource record, and then click the Delete icon.
- Export the list of shared resource records to a .csv file.
  — Click the Export icon.
- Print the list of shared resource records.
  — Click the Print icon.
Modifying Shared Records

You can modify, disable, or delete any shared record. When physical repair or relocation of a network device occurs, you can disable a record instead of deleting it. This alleviates having to delete, and then add the shared record again. When the changes to the physical device are complete, you can simply enable the shared record.

To modify or disable a shared record:

1. Perform a global search to retrieve the host or resource record you want to modify.

   or

   From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> shared_record_group -> Shared Records tab.

2. Select the shared record you want to modify and click the Edit icon.

3. The Shared Records editor contains the following tabs from which you can modify information:

   — **General**: You can change most of the information, except for the read-only fields, such as the Host Name Policy. You can also select the Disable check box to disable the record.

   — **TTL**: You can modify the TTL setting. For information, see About Time To Live Settings on page 443.

   — **Extensible Attributes**: You can modify the attributes. For information, see Using Extensible Attributes on page 265.

   — **Permissions**: This tab displays if you logged in as a superuser. For information, see About Administrative Permissions on page 120.

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

Deleting Shared Records

To delete shared resource records:

1. Perform a global search to retrieve the record you want to delete.

   or

   From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> shared_record_group -> Shared Records tab.

2. Select the shared record you want to delete and click the Delete icon.

3. When the confirmation dialog box displays, select **Yes**.

   Grid Manager moves the shared records to the Recycle Bin, from which you can restore or permanently delete the records.
Managing Associated Zones

Typically, you associate a zone with a shared record group when you create the group. You can also add an associated zone to a shared record group after you create the group.

Creating Associated Zones

To associate a zone with a share record group:

1. From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> shared_record_group -> Associated Zones tab, and then click the Add icon.
2. In the Zone Selector dialog box, select a zone by clicking the zone name.

The appliance adds the zone to the Associated Zones tab.

Viewing Associated Zones

To view the associated zones in a shared record group:

• From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> shared_record_group -> Associated Zones tab.

Grid Manager lists the following information about each associated zone by default:

• **Zone**: The zone associated with the shared record group.
• **DNS View**: The DNS view to which the zones belong.
• **Network View**: The network view associated with the DNS view.
• **Comment**: Comments that were entered for the shared record group.

You can do the following:

• Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
• Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 57.
• Associate another zone with the shared record group.
  — Click the Add icon and select a zone.
• Delete an associated zone.
  — Select the zone, and then click the Delete icon.
• Export the list of associated zones to a .csv file.
  — Click the Export icon.
• Print the list of shared associated zones.
  — Click the Print icon.

Deleting Associated Zones

To delete an associated zone:

1. From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> shared_record_group -> Associated Zones tab.
2. Select the associated zone and click the Delete icon.
3. When the confirmation dialog box displays, select Yes.

Grid Manager removes the zone from the shared record group.
Configuration Example: Configuring Shared Records

The following example shows you how to configure shared records. In this example, you do the following:

• Create a shared record group: **group1**.
• Associate it with three zones: **eng.com**, **sales.com**, and **marketing.com**.
• Create an A record www and an MX record mx1.

1. Create a shared record group called **group1** and associate it with **eng.com**, **sales.com**, and **marketing.com**.
   a. From the Data Management tab, select the DNS tab -> Shared Record Groups tab, and then click the Add icon.
   b. In the first step of the Shared Record Group wizard, specify the following
      Name: Enter **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. Save the configuration and click **Restart** if it appears at the top of the screen.

2. Add an A record **www** to **group1**.
   a. Expand the Toolbar and click Add -> Shared Record > Shared A Record.
   b. In the Shared A Record wizard, specify the following:
      Name: Enter **www**.
      Shared Record Group: Select **group1** from the drop-down list.
      IP Address: Enter the IP address 10.9.1.1.
   c. Save the configuration and click **Restart** if it appears at the top of the screen.

3. Add an MX record **mx1** into **group1**.
   a. Expand the Toolbar and click Add -> Shared Record > Shared MX Record.
   b. In the Shared MX Record wizard, specify the following:
      Mail Destination: Enter **mx1**.
      Shared Record Group: Select **group1** from the drop-down list.
      Mail Exchanger: Enter **www.infoblox.com**.
      Preference: Enter **10**.
      Comment: Enter **mail exchanger record for shared record group1**.
   c. Save the configuration and click **Restart** if it appears at the top of the screen.
Chapter 15 Configuring DNS Services

This chapter provides general information about DNS service properties. The topics in this chapter include:

- **Configuring DNS Service Properties** on page 443
  - *About Time To Live Settings* on page 443
  - *Adding an Email Address to the SOA Record* on page 444
  - *Notifying External Secondary Servers* on page 445
  - *Enabling the Configuration of RRset Orders* on page 445
  - *Specifying Port Settings for DNS* on page 446
  - *Specifying Minimal Responses* on page 447
  - *Starting and Stopping the DNS Service* on page 448
- **Using Forwarders** on page 449
  - *Specifying Forwarders* on page 449
- **Controlling DNS Queries** on page 450
  - *Specifying Queriers* on page 450
- **Enabling Recursive Queries** on page 451
  - *Enabling Recursion* on page 451
  - *Restricting Recursive Clients* on page 452
- **About NXDOMAIN Redirection** on page 453
  - *About NXDOMAIN Rulesets* on page 454
  - *NXDOMAIN Redirection Guidelines* on page 456
  - *Configuring NXDOMAIN Redirection* on page 457
  - *Creating Rulesets* on page 457
  - *Enabling NXDOMAIN Redirection* on page 458
- **About Blacklists** on page 459
  - *About Blacklist Rulesets* on page 460
  - *Blacklist Guidelines* on page 461
  - *Configuring the Blacklist Feature* on page 461
  - *Enabling Blacklisting* on page 462
- **Enabling Zone Transfers** on page 463
  - *Configure Zone Transfers* on page 463
- **About Root Name Servers** on page 465
  - *Specifying Root Name Servers* on page 465
• About Sort Lists on page 466
  — Defining a Sort List on page 466
• Configuring a DNS Blackhole List on page 468
  — Defining a DNS Blackhole List on page 469
• Specifying Hostname Policies on page 470
  — Defining Grid Hostname Policies on page 470
  — Defining Hostname Restrictions on page 471
  — Obtaining a List of Invalid Record Names on page 471
• About DNS64 on page 472
  — Configuring DNS64 on page 473
  — About Synthesis Groups on page 474
Configuring DNS Service Properties

The DNS service is enabled by default on NIOS appliances. You can configure general DNS service properties and change some default values. This section describes the DNS service properties that you can set:

- **About Time To Live Settings**
- **Adding an Email Address to the SOA Record** on page 444
- **Notifying External Secondary Servers** on page 445
- **Specifying Port Settings for DNS** on page 446
- **Specifying Minimal Responses** on page 447
- **Starting and Stopping the DNS Service** on page 448

### 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. Save the configuration and click Restart if it displays at the top of the screen.
Specifying TTL Settings for a Zone

To specify TTL settings for host and resource records in a zone:
1. From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view -> zone check box -> Edit icon.
2. In the Authoritative Zone editor, click Settings.
3. Click Override and complete the fields as described in the preceding section, Specifying TTL Settings for a Grid.

Specifying the TTL of a Host or Resource Record

To specify the TTL setting for an Infoblox host or resource record:
1. From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view -> zone -> resource_record.
2. The TTL tab of the resource record editor displays the TTL setting the resource record inherited from the Grid or zone. Click Override and enter a value. The setting is in hours by default. You can change it to seconds, minutes, days or weeks.
3. Save the configuration and click Restart if it displays at the top of the screen.

Adding an Email Address to the SOA Record

If the primary name server of a zone is a Grid member, you can add an administrator email address to the SOA record to help admins determine who to contact about this zone.

Adding an Email Address for SOA Records in the Grid

If all zones hosted by the Grid members have the same administrator, you can add the email address once for the Grid. The appliance then adds the email address to the RNAME field of the SOA records of the zones.
To add an email address to the SOA records at the Grid level:
1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
2. In the General -> Basic tab of the Grid DNS Properties editor, enter the email address in the E-mail Address (for SOA RNAME field) field.
3. Save the configuration and click Restart if it displays at the top of the screen.

Adding an Email Address for the Zone SOA Record

To add an email address to the SOA record of a zone:
1. From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view -> zone check box -> Edit icon.
2. In the Authoritative Zone editor, click Settings.
3. Click Override beside the Email address (for SOA RNAME field) field and enter the email address of the zone administrator.
4. Save the configuration and click Restart if it displays at the top of the screen.
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 Expert Mode**.
3. When the additional tabs appear, click the **Advanced** subtab of the **General** tab.
4. Complete the following:
   - **Enable Grid secondaries to notify external secondaries**: This option is enabled by default.
   - **Notify Delay**: Specify the number of seconds that the Grid secondary servers delays sending notification messages to the external secondaries. The default is five seconds.
5. Save the configuration and click **Restart** if it displays at the top of the screen.

For the external secondary servers to accept notify messages from the secondary name servers in the Grid and then request zone transfers from them, you must configure the external secondary servers to use the Grid secondary servers as the source of the zone transfers. This ensures that the external secondary servers continue to receive notify messages, even if the primary server is unavailable.

Enabling the Configuration of RRset Orders

You can use the Infoblox GUI to configure the order that the appliance uses to return the A and AAAA records associated with an Infoblox host. This feature is useful when you want the appliance to return the A and AAAA records of a host in a specific order. For example, if you want the management address to appear first on a list of IP addresses associated with a network device, you can configure the order of the IP addresses so the management address is always returned first on the list when you look up the name of the device. For information about using the Infoblox API to configure RRset order (resource record order) of a host, refer to the Infoblox API Documentation.

To specify an RRset order of a host record, you must first enable the feature at the Grid level. When you enable this feature and there are multiple IP addresses associated with the host record, you can specify one of the following RRset orders through the Host Record wizard and editor:

- **Fixed**: The A and AAAA records of the host are returned in the order that you specify in the IPv4 and IPv6 address tables.
- **Random**: The A and AAAA records of the host are returned in a random order.
- **Cyclic**: The A and AAAA records are returned in a round robin pattern.

For information about specifying RRset order of a host record, see *Adding Host Records* on page 813.

Note that when you configure an order type for the IP addresses associated with a host record, the order type applies to both the A and AAAA records of the host. It does not apply to any non-host A or AAAA records that may have the same owner name as the host record. By default, the appliance returns resource records in a cyclic or round robin order. The return order of non-authoritative data retrieved from a recursion is not affected by the host RRset order, and that remains cyclic.

To enable the configuration of RRset order:

1. From the **Data Management** tab -> **DNS** tab, expand the Toolbar, and then click **Grid DNS Properties**.
2. In the Grid DNS Properties editor, click **Toggle Expert Mode**.
3. When the additional tabs appear, click the **Advanced** subtab of the **General** tab.
4. Complete the following:
   — **Enable setting RRset order for hosts with multiple addresses**: Select this check box to enable the configuration of RRset order for a host record. After you enable this feature, you can configure the RRset order in the *Host Record* wizard or editor. For information, see *Adding Host Records* on page 813.
   — **Preserve host RRset order for Grid secondaries that use DNS zone transfers**: This is enabled only when you have enabled the setting of RRset order for host records. When you select this check box, the RRset order that you configure for a host record applies to the resource records of the Grid secondaries that are in the DNS transfer mode.

5. Save the configuration and click **Restart** if it displays at the top of the screen.

**Specifying Port Settings for DNS**

When requesting zone transfers from the primary server, some secondary DNS servers use the source port number (the primary server used to send the notify message) as the destination port number in the zone transfer request. If the primary server uses a random source port number when sending the notify message—that the secondary server then uses as the destination port number when requesting a zone transfer—zone transfers can fail if there is an intervening firewall blocking traffic to the destination port number.

Specifying a source port number for recursive queries ensures that a firewall allows the response. If you do not specify a source port number, the NIOS appliance sends these messages from a random port number. 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.

If you have configured anycast and non-anycast IP addresses on the loopback interface, you must enable the appliance to provide DNS services on them. You can also configure the appliance to listen for DNS queries on a specific IP address that you configure on the loopback interface, by separating the source port for DNS queries from the port for notify messages and zone transfer requests. For information about the loopback interface and anycast addressing, see *Using the Loopback Interface* on page 552.
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 ->member check box ->Edit icon.
2. In the editor, click Toggle Expert 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: Click the Add icon to add an anycast or non-anycast address you configure on the loopback interface. You must add all IP addresses you configure on the loopback interface so the appliance can provide DNS services on them. For information about adding IP addresses on the loopback interface, see Using the Loopback Interface on page 552.
   — Send queries from: If you want to improve the DNS service performance, you can separate the DNS queries from the notify messages and zone transfer requests. From the drop-down list, select the source port of the DNS queries that the Grid member sends. The appliance lists all physical interfaces and the non-anycast addresses you configure on the loopback interface. For information, see Configuring IP Addresses on the Loopback Interface on page 553.
   — Send notify messages and zone transfer requests from: From the drop-down list, select the source port of the notify messages and zone transfer requests that the Grid member sends. You can only select a physical interface, you cannot select IP addresses on the loopback interface.
   — Notify Delay: Specify the number of seconds that the Grid secondary servers delays sending notification messages to the external secondaries. The default is five seconds.
5. Save the configuration and click Restart if it displays at the top of the screen.

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.
2. Member: From the Data Management tab, select the DNS tab and click the Members tab ->member check box ->Edit icon.
3. To override an inherited property, click Override next to it and complete the appropriate fields.
4. 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 specify a source port for notify messages to ensure that the firewall allows the zone transfer request from the secondary server to the primary server. If you do not specify a source port, the appliance sends messages from a random port with a number above 1024.
5. Save the configuration and click Restart if it displays at the top of the screen.

Specifying Minimal Responses
A NIOS appliance returns a minimal amount of data in response to a query, by default. It includes records in the authority and additional data sections of its response only when required, such as in negative responses. This feature speeds up the DNS services provided by the appliance.
To disable returning minimal responses:
1. From the Data Management tab, select the DNS tab and click the Members tab ->member check box ->Edit icon.
2. In the Member DNS Configuration editor, click General ->Basic tab.
3. Clear the Return minimal responses check box
4. Save the configuration and click Restart if it displays at the top of the screen.
Starting and Stopping the DNS Service

The DNS service is disabled by default. After you complete the DNS configuration, you can start DNS service on a member. You can also disable the DNS service on any Grid member. Be aware that disabling the DNS service on a member removes the NS records from it. If you later re-enable DNS service for this member, the NS records are then restored.

To start DNS service on a member:

1. From the Data Management tab, select the DNS tab -> Members tab -> member check box.
2. Expand the Toolbar and click Start.
3. In the Start Member DNS Service dialog box, click Yes.

Grid Manager starts the DNS service on the selected member.

You can stop DNS service on a member by selecting the member check box and click Stop from the Toolbar.
Using Forwarders

A forwarder is essentially a name server to which all other name servers first send queries that they cannot resolve locally. The forwarder then sends these queries to DNS servers that are external to the network, avoiding the need for the other name servers in your network to send queries off-site. A forwarder eventually builds up a cache of information, which it uses to resolve queries. This reduces Internet traffic over the network and decreases the response time to DNS clients. This is useful in organizations that need to minimize off-site traffic, such as a remote office with a slow connection to a company’s network.

You can select any Grid member to function as a forwarder. You must configure your firewall to allow that Grid member to communicate with external DNS servers. You can also configure the NIOS appliance to send queries to one or more forwarders.

You can define a list of forwarders for the entire Grid, for each Grid member, or for each DNS view.

Specifying Forwarders

To configure forwarders for a Grid, member, or DNS view:

1. **Grid:** From the Data Management tab, select the DNS tab, expand the Toolbar and click **Grid DNS Properties**.
   **Member:** From the Data Management tab, select the **DNS** tab and click the **Members** tab -> member check box -> Edit icon.
   **DNS View:** From the Data Management tab, select the **DNS** tab -> **Zones** tab -> **dns_view** check box -> Edit icon.
   Note that if there is only one DNS view— for example, the predefined default view—you can just click the Edit icon beside it.
   To override an inherited property, click **Override** next to it and complete the appropriate fields.

2. Click the **Forwarders** tab.

3. Click the Add icon.

4. Enter an IP address in the text field.
   — To remove a forwarder, select the IP address from the Forwarders list, and then click the Delete icon.
   — To move a forwarder up or down on the list, select it and click the Up or Down arrow.

5. To use only forwarders on your network (and not root servers), select the **Use Forwarders Only** check box.

6. Save the configuration and click **Restart** if it displays at the top of the screen.
Controlling DNS Queries

By default, the NIOS appliance responds to DNS queries from any IP address. You can create a list of queriers to which the appliance is allowed to respond; restricting it to specific networks, IP addresses, and remote servers that present specified TSIG (transaction signature) keys. When using TSIG keys, it is important that the appliances and servers involved with the authentication procedure use NTP (Network Time Protocol) for their time settings (see Using NTP for Time Settings on page 245).

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 451.

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 Algorithm:** Select either HMAC-MD5 or HMAC-SHA256.
     - **Key Data:** To use an existing TSIG key, type or paste the key in the Key Data field. Alternatively, you can select the key algorithm, select the key length from the Generate Key Data drop down list, and then click Generate Key Data to create a new key.
     - **Any Address/Network:** Select to allow or disallow queries from any IP address.
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 245).

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 465.

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 358.

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 Algorithm:** Select either **HMAC-MD5** or **HMAC-SHA256**.
  
  — **Key Data:** To use an existing TSIG key, type or paste the key in the **Key Data** field. Alternatively, you can select the key algorithm, select the key length from the **Generate Key Data** drop down list, and then click **Generate Key Data** to create a new key.

  — **Any Address/Network:** Select to allow or 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. Save the configuration and click **Restart** if it displays at the top of the screen.

### 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 Expert Mode**.

3. When the additional tabs appear, click the **Advanced** subtab of the **Queries** tab.

4. Select the **Limit number of recursive clients to** option and enter a number.

5. Save the configuration and click **Restart** if it displays at the top of the screen.
About NXDOMAIN Redirection

When a DNS member with recursion enabled receives a recursive query for data for which it is not authoritative, it locates the data through queries to other servers. If the query is for a non-existent domain name, the DNS member receives an NXDOMAIN response from the authoritative name server, which the member then forwards to the DNS client. An NXDOMAIN response contains a “Name Error” RCODE, signifying that the domain name referenced in the query does not exist. (For information, you can refer to RFC 1035, Domain Names — Implementation and Specification.)

You can install a Query Redirection license on a recursive DNS member to control its response to queries for A records of non-existent domain names and other domain names that you specify. After the license is installed, Grid Manager displays the NXDOMAIN Rulesets tab where you can create rules that specify how a DNS member responds to queries for A records for certain domain names and non-existent domain names. Each rule contains a domain name specification, and the action of the DNS member when the domain name in the query matches that in the rule. After you create the rules, you then enable the NXDOMAIN redirection feature and list the IP addresses that are included in the synthesized responses.

Recursive DNS members can redirect responses to queries for A records only. DNS members resolve queries for all other records as they normally would.

In addition, you can enable DNS members to log queries that match rules with an action of “Redirect” or “Modify”. You can view the logs in the Syslog viewer. The logs include the queried domain name, source IP address, the pattern of the matched rule, and the name of the corresponding ruleset.

When DNSSEC is enabled on the Infoblox DNS server, it does not redirect DNS clients that request DNSSEC data for a non-existent domain name. Instead, it returns an authenticated negative response in the form of an NSEC or NSEC3 RR. (For information about DNSSEC, see Chapter 17, 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, member, and DNS view levels. Only recursive DNS servers can redirect DNS clients. Non-recursive DNS members do not redirect DNS clients. For information on enabling recursion on a DNS member, see Enabling Recursive Queries on page 451.

Note that if both NXDOMAIN redirection and the blacklisting feature are enabled, the DNS member applies the blacklist rulesets before the NXDOMAIN rulesets. For information about blacklisting domain names, see About Blacklists on page 459.
About NXDOMAIN Rulesets

An NXDOMAIN ruleset is a list of rules that a DNS member uses to determine its response to recursive queries for A records it does not have. Each rule consists of a domain name specification or pattern, and an associated action. Domain names can contain any printable character. You can use certain metacharacters to create domain name patterns that are used to match the domain names in DNS queries. Pattern matching is case-insensitive. Patterns support the following metacharacters:

- Use the caret character (\^) to indicate the beginning of a pattern. For example, \^foo matches foo.com but not barfoo.com. The caret character has a special meaning only if it is specified at the beginning of a pattern.

- Use the dollar sign character (\$) to indicate the end of a pattern. The dollar sign character has a special meaning, only if it is specified at the end of the pattern. For example, com\$ matches corp100.com but not corp100.com.net.

When the pattern contains a $ at the end, NIOS automatically adds a period (.) before the $. For example, if you enter com\$, NIOS saves it as com$. The period indicates that the pattern specifies a complete domain name that ends with the root label.

- Use the asterisk character (\*) as a wildcard that can match zero or more characters in one or more labels of a domain name. For example, xf*oy matches xfooy.com, but not xfoobary.

A pattern that contains a single asterisk (*) (or an equivalent expression, such as \^*\$) matches any domain name.

- Use the backslash character (\) with one of the metacharacters ($, ^, * and \) to remove their special meaning. If \ is followed by any other character, that character is taken as an ordinary character, as if \ is not present. For example, foo\.bar matches foo\.bar, and \* matches a literal asterisk in a domain name.

No other characters have any special meaning. Note in particular that the period character (\.) only matches a period used as a separator in a domain name.

The action specifies how the DNS member responds when a domain name in a query matches a pattern. The action can be one of the following: Pass, Modify or Redirect.

- Pass: The DNS member resolves the query and forwards the response to the DNS client, even if it is an NXDOMAIN response.

- Modify: The DNS member resolves the query and forwards the response to the DNS client, only if it is not an NXDOMAIN response. But if the member receives an NXDOMAIN response, it sends the client a synthesized response that includes predefined IP addresses.

- Redirect: The DNS member does not resolve the query. Instead, it sends the client a synthesized response that includes predefined IP addresses.

You can configure multiple rulesets. The DNS member applies the rulesets and their rules in the order in which they’re specified in the configuration. If multiple rulesets contain rules with duplicate patterns, the DNS member applies the first rule it encounters and ignores the other rules.
Examples

The following example illustrates how the appliance applies NXDOMAIN rulesets.

Rule set 1:

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>a1.corp100.com</td>
<td>PASS</td>
</tr>
<tr>
<td>*.corp100.com</td>
<td>REDIRECT</td>
</tr>
</tbody>
</table>

- If the DNS member receives a query for a1.corp100.com, it resolves the query and forwards the response, even if it is an NXDOMAIN response, to the client. Note that if the order of the rules was switched, the DNS client would have been redirected immediately, because the domain name a1.corp100.com matches the *.corp100.com pattern.
- If the DNS member receives a query for b1.corp100.com, the member immediately redirects the DNS client to the specified IP address because the domain name in the query matches the second rule.
- If the DNS member receives a query for b1.corp200.com, it resolves the query because the domain name does not match any rule. If the DNS member receives an A record from an authoritative server, the member forwards the response to the client. However, if the member receives an NXDOMAIN response, it redirects the DNS client to the specified IP address.

In the following example, the rules redirect queries for dotted domain names that do not have “.com” As shown in the example, an explicit PASS rule is required at the end.

Rule set 2:

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.com</td>
<td>PASS</td>
</tr>
<tr>
<td>.*.$</td>
<td>MODIFY</td>
</tr>
<tr>
<td>*</td>
<td>PASS</td>
</tr>
</tbody>
</table>

- If the DNS member receives a query for corp100.com which matches the pattern “*.com”, the member resolves the query and forwards the response, even if it is an NXDOMAIN response, to the client.
- If the DNS member receives a query for corp100.org, which matches the pattern “.*.$”, the member resolves the query. If the member receives an NXDOMAIN response, it redirects the client to the specified IP address. If the member receives a non-NXDOMAIN response, it forwards the response to the client.
- If the DNS member receives a query for corp200, the member resolves the query and forwards the response to the client.
NXDOMAIN Redirection Guidelines

The following summarizes how a DNS member responds to a query for an A record when the NXDOMAIN feature is enabled:

- If there are no rulesets configured, the DNS member queries other name servers.
  - If the DNS member receives a non-NXDOMAIN response from an authoritative server, it forwards the response to the DNS client.
  - If the DNS member receives an NXDOMAIN response from an authoritative server, it redirect the DNS client.
- If rulesets are configured, the DNS member tries to match the domain name in the query with a domain name in the rules.
  - If the DNS member finds a match, it perform the action specified in the rule.
    - If the action is “Redirect”, the DNS member redirect the DNS client.
    - If the action is “Pass”, the DNS member queries other name servers and forwards the response to the DNS client.
    - If the action is “Modify”, the DNS member queries other name servers. If it receives a non-NXDOMAIN response, it forwards the response to the DNS client; if it receives and NXDOMAIN response, it redirects the DNS client.
  - If the DNS member does not find a match, the DNS member queries other name servers.
    - If the DNS member receives a non-NXDOMAIN response, it forwards the response to the DNS client.
    - If the DNS member receives an NXDOMAIN response from an authoritative server, it redirects the DNS client.

Note that if an A record with a dotted hostname is added to an authoritative zone through a dynamic DNS update, and that A record should actually belong in an existing delegation, the appliance may not redirect a query for that A record according to the Blacklist and NXDOMAIN guidelines.
Configuring NXDOMAIN Redirection

To enable NXDOMAIN redirection and configure its properties:

1. Configure NXDOMAIN rulesets. You can create NXDOMAIN rulesets through Grid Manager, as described in Creating Rulesets. You can also specify the rulesets in a CSV file and import the file to the Grid, as described in About CSV Import on page 64.

2. Enable this feature and specify the redirection IP addresses, as described in Enabling NXDOMAIN Redirection on page 458.

Creating Rulesets

To create a ruleset:

1. From the Data Management tab -> DNS tab -> NXDOMAIN Rulesets tab, click the Add icon.

2. In the NXDOMAIN Ruleset wizard, complete the following and click Next:
   - Name: Enter a name for the ruleset.
   - Comment: You can enter additional information.
   - Disable: You can disable this ruleset for use later on. The appliance ignores disabled rulesets.

3. Click the Add icon to add a rule to the ruleset table.
   - In the Pattern column, enter a domain name or pattern, using the guidelines specified in About NXDOMAIN Rulesets.
   - In the Action column, select PASS, REDIRECT or MODIFY.
   - In the Order column, NIOS automatically displays the number of the entry in the list.
   The appliance applies the rules in the order they are listed. You can order the list as follows:
     - Use the up and down arrows to move rules up or down on the list.
     - Use the go-to-top or go-to-bottom arrow to move a rule to the top or bottom of the list.
     - Change the Order number of a rule to move it to the desired location.
     - Delete a rule by selecting it and clicking the Delete icon.

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

Managing NXDOMAIN Rulesets

To view NXDOMAIN rulesets, navigate to the Data Management tab -> DNS tab -> NXDOMAIN Rulesets tab. The panel lists the configured rulesets and their associated comments. You can also display the Disabled column which indicates which rulesets are disabled. From this panel, you can do the following:

- Add more rulesets, as described in the preceding section, Creating Rulesets.
- Edit a ruleset, by clicking its check box and clicking the Edit icon. You can set the following in the NXDOMAIN Ruleset editor:
  - In the General Basic tab, you can change entries in any of the fields.
  - In the Rules tab, you can do the following:
    - Add a rule by clicking the add icon and specifying the pattern and action.
    - Change the pattern or action of a rule, by clicking in the appropriate row.
    - Delete a rule by clicking its check box and clicking the Delete icon.
    - Move rules up and down, by using the arrows.
  - In the Permissions tab, you can set admin permissions for the ruleset. For information about admin permissions, see Chapter 4, Managing Administrators, on page 109.
- Delete a ruleset, by clicking its check box and clicking the Delete icon.
Enabling NXDOMAIN Redirection

Only DNS members with recursion enabled can support NXDOMAIN redirection. You can enable this feature at the Grid level, and override it for a member or DNS view with recursion enabled. You must specify at least one IP address as the redirection destination. You can specify different redirection IP addresses and rulesets for each Grid member or DNS view, and you can also define members that do not provide redirection. This is useful when you want to define a set of “opt out” servers for DNS clients that do not want to be redirected.

You can also enable the DNS member to log queries that match rules with an action of “Redirect” or “Modify”. The logs include the queried domain name, source IP address, the pattern of the matched rule, and the name of the corresponding ruleset. The DNS member does not log queries that matched rules with an action of “Pass”.

To enable NXDOMAIN redirection:

1. **Grid**: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
   **Member**: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
   **DNS View**: From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view check box -> Edit icon.
   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 Expert Mode.

3. Click NXDOMAIN and complete the following:
   - **Enable NXDOMAIN redirection (recursive members only)**: Select this option to enable recursive DNS members to synthesize their responses to DNS queries for A records.
   - **Redirect to**: Click the Add icon and enter the IP addresses that the DNS server includes in its synthesized response. You must specify at least one IP address. You can add up to 12 IP addresses.
   - **TTL**: Specify how long the DNS client caches the A record with the redirected IP address.
   - **Rulesets**: Click the Add icon to add an NXDOMAIN ruleset. Use the up and down arrows to move rulesets up and down in the list. The appliance applies them in the order they are listed.
   - **Log redirected queries**: Select this check box to log the redirected queries to syslog.

4. Save the configuration and click Restart if it displays at the top of the screen.
About Blacklists

Your organization can prevent customers or employees from accessing certain Internet resources, particularly websites, by prohibiting a recursive DNS member from resolving queries for domain names that you specify.

You can create blacklist rules that specify how a DNS member responds to recursive queries for data for which it is not authoritative. Each rule specifies a domain name and the action of the DNS member when the domain name in the query matches that in the rule. Instead of resolving the query, the DNS member can redirect the DNS client to predefined IP addresses or return a REFUSED response code indicating that resolution is not performed because of local policy.

When the DNS member receives a query for data for which it is not authoritative, it first tries to match the domain name in the query with a domain name in any of its rules. If it finds a match, it responds according to the action specified in the rule. If it does not find a match and the NXDOMAIN feature is enabled, the DNS member checks the NXDOMAIN rulesets for a match and responds accordingly. If the NXDOMAIN feature is not enabled, the DNS member resolves the query. (For information about the NXDOMAIN feature, see About NXDOMAIN Redirection on page 453.

Infoblox DNS members can modify their responses to queries for A records only. Therefore, if the matched query is for a record other than an A record, including a query with a type of “ANY”, the DNS member sends a REFUSED response if the matched rule has an action of “Redirect”.

In Figure 15.1, a DNS client opens a web browser and tries to access xxx.domain.com. When the DNS member receives the query for xxx.domain.com, it checks its blacklist rulesets and finds xxx.domain.com in a rule with an action of “Redirect”. The DNS client is redirected to the configured redirection destination IP address 10.1.2.3.

Figure 15.1 Blacklist

This feature supports queries for data in IPv4 and IPv6 reverse-mapping zones, as well as forward-mapping zones. Note that when a user with a Windows DNS client with IPv6 installed tries to access a domain name, the Windows client sends queries for AAAA records before queries for A records. After the DNS member sends a Refused response to the query for the AAAA record, the DNS client then sends a query for the A record. The DNS member then responds according to the blacklist rules.

When DNSSEC is enabled on the Infoblox DNS server, it does not redirect DNS clients that request DNSSEC data. (For information about DNSSEC, see Chapter 17, DNSSEC, on page 523.) If DNSSEC is not enabled and the query includes a request for DNS data, the appliance ignores the request for DNSSEC data and redirects the clients.

You can enable the blacklist feature at the Grid, member, and DNS view levels. Note that only recursive DNS servers can support this feature. For information on enabling recursion on a DNS member, see Enabling Recursive Queries on page 451.
About Blacklist Rulesets

A blacklist ruleset is a list of rules that a DNS member uses to determine its response to recursive queries for certain domain names. When you enable the blacklist feature, you must define at least one rule in a ruleset. Each rule consists of a domain name and an associated action. The DNS member matches the domain names in the rules with the entire domain name in the query, including its suffix. The domain name in the rule can contain any printable character. Domain name matching is case-insensitive. Unlike the NXDOMAIN rules, blacklist rules do not support metacharacters in domain names.

The action in a rule is either “Pass” or “Redirect”.

- **Pass**: The DNS member resolves the query and forwards the response to the DNS client.
- **Redirect**: The DNS member does not resolve the query. The DNS member redirects the client to the predefined IP addresses or sends a REFUSED response, depending on your configuration. Note that the DNS member can redirect the client only if the query is for an A record. If the query is for another resource record, the DNS member sends a REFUSED response.

You can use the Blacklist wizard, described in Adding a Blacklist Ruleset, to add blacklist rulesets, but not rules. You can only add rules by importing them in a CSV file, as described in About CSV Import on page 64. Note that if a blacklist ruleset contains duplicate domain names, the DNS member loads the first rule in the ruleset and discards the other rules.

The following example illustrates how the DNS member applies blacklist rules.

Ruleset 1:

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>a1.foo.com</td>
<td>PASS</td>
</tr>
<tr>
<td>foo.com</td>
<td>REDIRECT/BLOCK</td>
</tr>
</tbody>
</table>

- If the DNS member receives a recursive query for a1.foo.com, it resolves the query and forwards the response to the client.
- If the DNS member receives a recursive query for the A record of b1.foo.com, it redirects the DNS client to the specified IP address. If the query is for another record type, such as an MX record, the member sends a REFUSED response to the client.
Blacklist Guidelines

The following summarizes how a DNS member responds to a DNS client when the blacklist feature is enabled:

- If the domain name in the query matches a domain name in a rule, the member does the following:
  - If the query is for an A record, the member performs the action specified in the rule.
  - If the action is “Redirect”, the member performs the action specified in the Blacklist wizard.
    - If the action in the wizard is to redirect, the DNS member redirects the client to the listed IP addresses.
    - If the action in the wizard is to return a REFUSED response, the DNS member sends a REFUSED response to the DNS client.
  - If the action in the rule is “Pass”, the DNS member resolves the query and forwards the response to the DNS client.
  - If the query is for a non-A record, the member performs the action in the rule as follows:
    - If the action is “Redirect”, the DNS member returns a REFUSED response to the DNS client.
    - If the action is “Pass”, the DNS member resolves the query and forwards the response to the DNS client.
- If the domain name in the query does not match a domain name in a rule:
  - If the NXDOMAIN feature is enabled, the DNS member tries to find a match with the NXDOMAIN rules and responds accordingly.
  - If the NXDOMAIN feature is disabled, the DNS member resolves the query and forwards the response to the DNS client.

Note that if an A record with a dotted hostname is added to an authoritative zone through a dynamic DNS update, and that A record should actually belong in an existing delegation, the appliance may not redirect a query for that A record according to the Blacklist and NXDOMAIN guidelines.

Configuring the Blacklist Feature

To configure the blacklist feature:

1. Add blacklist rulesets, as described in Adding a Blacklist Ruleset on page 461.
2. Create one or more CSV files that contain the rules for each ruleset and import the files to the Grid. For information about importing CSV files, see About CSV Import on page 64.
3. Enable blacklisting, as described in Enabling Blacklisting on page 462.

Adding a Blacklist Ruleset

To add the name of a blacklist ruleset:

1. From the Data Management tab -> DNS tab -> Blacklist Rulesets tab, click the Add icon.
2. In the Blacklist wizard, complete the following:
   - Name: Enter a name for the ruleset.
   - Comment: You can enter additional information.
   - Disable: You can disable this ruleset for use later on. The appliance ignores disabled rulesets.
3. Save the configuration and click Restart if it displays at the top of the screen.

You can then use the CSV Import feature to import the rules for each ruleset.
Managing Blacklist Rulesets

To view rulesets, navigate to the Data Management tab -> DNS -> Blacklist Rulesets tab. The panel lists the configured rulesets and their associated comments. You can also display the Disabled column which indicates which rulesets are disabled. From this panel, you can do the following:

- Add more rulesets, as described in the preceding section, Adding a Blacklist Ruleset on page 461.
- Edit a ruleset, by clicking its check box and clicking the Edit icon. You can set the following in the Blacklist Ruleset editor:
  - In the General Basic tab, you can change entries in any of the fields.
  - In the Permissions tab, you can set admin permissions for the ruleset.
- Delete a ruleset, by clicking its check box and clicking the Delete icon.
- View the rules that were imported in each ruleset by selecting it. For each rule, the panel displays the following:
  - Domain name
  - The action of the recursive DNS member when the domain name in a query matches the domain name in the rule.

To delete or edit rules in a ruleset, you must delete the ruleset from this panel, edit the CSV file and re-import it.

Enabling Blacklisting

Only DNS members with recursion enabled can support this feature. You can enable this feature at the Grid level and override it for a member or DNS view with recursion enabled.

You can also enable the DNS member to log queries that matched blacklist rules. The logs include the queried domain name, source IP address, the pattern of the matched rule, and the name of the corresponding ruleset.

To enable blacklisting:

1. **Grid:** From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
   - **Member:** From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
   - **DNS View:** From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view check box -> Edit icon.
   
   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 Expert Mode.

3. Click Blacklist and complete the following:
   - **Enable Domain Name Blacklist:** Select this check box.
   - **Blacklist Rulesets:** To add a ruleset, click the Add icon. If there are multiple rulesets, select one from the Select Ruleset dialog box. Use the up and down arrows to move rulesets up and down in the list. The appliance applies rulesets in the order they are listed.
   
   For blacklisted domain names, return: Select the action of the appliance when it receives a query for a record that matches a rule with an action of Redirect/Block.
   
   If you selected This list of IP addresses, add an IP address to the Redirect to table by clicking the Add icon and entering the address. The addresses are listed in round robin fashion in the synthesized response of the DNS member. You can enter up to 12 IP addresses.
   - **Blacklist TTL:** Specify how long the DNS client caches the A record with the redirected IP address.
   - **Log queries for blacklisted domain names:** Select this option to enable the appliance to log queries for blacklisted domain names, including the source IP address of the query.

4. Save the configuration and click Restart if it displays at the top of the screen.
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 245).

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 Algorithm: Select either HMAC-MD5 or HMAC-SHA256.
     - 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. Save the configuration and click Restart if it displays at the top of the screen.

### Specifying a Zone Transfer Format

The zone transfer format determines the BIND format for a zone transfer. This provides tracking capabilities for single or multiple transfers and their associated servers.

To specify a zone transfer format:

1. **Grid**: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
   **Member**: From the Data Management tab, select the DNS tab, click the Members tab ->member check box ->Edit icon.
   To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the editor, click Toggle Expert Mode.

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

---

**About Root Name Servers**

Root name servers contain the root zone file which lists the names and IP addresses of the authoritative name servers for each top-level 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 Expert 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. Save the configuration and click **Restart** if it displays at the top of the screen.
About Sort Lists

A sort list prioritizes A and AAAA records on certain networks when those records are included in responses, sorting them to the beginning of the list in the response. For example, you can define a sort list when a server has two interfaces and you want the DNS clients to prefer one interface because it has a faster link.

When you define a sort list on the NIOS appliance, you specify the following:

- The IP address or network of the source of the query
- The IP addresses or networks that the appliance lists first in its response when it receives a query from the corresponding source address

When the NIOS appliance receives a query from the specified IP address or network and the DNS lookup produces a response with multiple addresses, the NIOS appliance sorts the addresses so that those in the sort list are at the beginning of its response.

Defining a Sort List

To define a sort list for a Grid, member, or DNS view:

1. **Grid:** From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.  
   **Member:** From the Data Management tab, select the DNS -> Members tab -> member check box -> Edit icon.  
   **DNS View:** From the Data Management tab, click the DNS tab -> Zones tab -> dns_view check box -> Edit icon.  
   To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the editor, click Toggle Expert 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 15.2.
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. Save the configuration and click **Restart** if it displays at the top of the screen.
Configuring a DNS Blackhole List

The DNS blackhole feature provides the ability to specify IP and network addresses of network devices that you do not want to use in the DNS resolution process. The DNS blackhole feature is disabled by default. When enabled, the NIOS appliance does not accept queries from IP addresses in the blackhole list and does not use them to resolve queries. For example, you can add the IP addresses of name servers that are using DNS incorrectly to prevent the NIOS appliance from accepting their queries and from using them as resolvers. You can also use this feature to fix temporary network issues. For example, you can add the IP addresses of delegated servers, configured forwarders, and DHCP servers that have temporary DNS-related issues.

You can create a DNS blackhole list for the entire Grid or create a separate list for each Grid member. For example, if one of your Grid members is behind a firewall, you might need to configure a different DNS blackhole list for this member because the clients that can access it might be mapped differently.

The appliance accepts queries from addresses and networks that are excluded from the blackhole list and uses these addresses and networks as resolvers. To add an IP address to the blackhole list, enter it and set its permission to “Include”. You can also add an IP address to the blackhole list and set its permission to “Exclude” so its not in blackhole list, effectively allowing the NIOS appliance to respond to queries from that address and to use it as a resolver.

When you add a network to a DNS blackhole list, all the IP addresses in the network are not used in the DNS resolution process. If you want to allow some IP addresses within the network, add these addresses to the list and set their permission to “Exclude.” Ensure that you list these IP addresses before the network address because the appliance applies permissions to the addresses in the order they are listed. For example, when you add the network 10.10.0.0/24 to a DNS blackhole list, all 256 IP addresses in the network are put on the blackhole list. To allow DNS traffic to the IP addresses 10.10.0.55 and 10.10.0.88, add these two addresses before the network address in the DNS blackhole list, and then set their permissions to “Exclude.”
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 Expert 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 Include by default, which adds the address to the blackhole list. To change it to Exclude, click it to display the drop-down list and select Exclude.
   - **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 Include or Exclude from the drop-down list.
   - **IPv6 Address**: In the Name field of the new row, enter an IPv6 address. The Permission column displays Include by default, which adds the address to the blackhole list. To change it to Exclude, click it to display the drop-down list and select Exclude.
   - **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 Include or Exclude from the drop-down list.
   - **Any Address/Network**: Select to include or exclude any IP address in the blackhole list.

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. Save the configuration and click **Restart** if it displays at the top of the screen.
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 ("-"'). You cannot use other special characters, such as underscore ("_"'). Note that when you select this policy, the appliance automatically applies the policy to dynamic DNS updates and zone transfers it receives.
   - 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 C, "Regular Expressions", on page 1013 for definitions of regular expressions.
   Note that Grid Manager does not validate the regular expressions that you enter. Therefore, you can inadvertently specify an invalid regular expression that might cause noncompliance errors when you create records.
6. If you select the Strict Hostname Checking policy, the Apply policy to dynamic updates and inbound zone transfers (requires Strict Hostname Checking setting) option is enabled by default. It enables the appliance to apply the policy to dynamic DNS updates and zone transfers that it receives. You can then select which action the appliance takes when it encounters names that do not conform to the policy. Select either Fail or Warn. If you select Warn, the appliance allows the dynamic DNS update or zone transfer, but logs a syslog message.
   Note: The Strict Hostname Checking policy only allows alphanumeric characters and dashes ("-"'). You cannot use other special characters, such as underscore ("_"'). Therefore, DDNS updates from Microsoft Active Directory controllers may not be accepted.
7. Save the configuration and click Restart if it appears at the top of the screen.
   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 Expert Mode.

3. When the additional tabs appear, click Host Naming.

4. Click Override.

5. From the **Host Name Policy** drop-down list, select a predefined policy or a policy that was defined at the Grid level.

6. If you select the Strict Hostname Checking policy, the Apply policy to dynamic updates and inbound zone transfers (requires Strict Hostname Checking setting) is enabled by default. It enables the appliance to apply the policy to dynamic DNS updates and zone transfers that it receives. You can then select which action the appliance takes when it encounters names that do not conform to the policy. Select either Fail or Warn. If you select Warn, the appliance allows the dynamic DNS update or zone transfer, but logs a syslog message.

   **Note:** The strict hostname checking policy only allows alphanumeric characters and dashes. It does not allow for the use of other special characters, such as underscore (“_”). Therefore, DDNS updates from Microsoft Active Directory controllers might not be accepted.

7. Save the configuration and click Restart if it displays at the top of the screen.

Obtaining a List of Invalid Record Names

You can retrieve a list of all record names that do not comply with the current hostname checking policy of a zone. These could be records that were created before the current host naming policy was set. In addition, if you selected the Strict Hostname Checking policy and allowed illegal hostnames in DDNS updates and inbound zone transfers with a warning, those records are listed in this report as well.

To display the Hostname Compliance report:

1. From the **Data Management** tab, select the DNS tab and click the Zones tab-> dns_view -> zone check box.

2. Click Hostname Compliance.

   The Hostname Compliance Report for the zone displays. It lists the record name, type, value, and comment for all records that do not comply with the hostname restriction policy of the zone.

From the report, you can select a record and do the following:

- Click the Edit icon to open the record editor.
- Click the Delete icon to move it to the Recycle Bin.
About DNS64

To support the increasing number of IPv6 and dual-stack networks, Infoblox DNS servers now support DNS64, a mechanism that synthesizes AAAA records from A records when no AAAA records exist. When you enable DNS64 on an Infoblox DNS server, it can operate with a third-party NAT64 device so IPv6-only nodes can communicate with IPv4-only nodes without any changes to either of the devices.

As illustrated in Figure 15.3, when an IPv6-only host requests the AAAA record of an IPv4-only server and none exists, a DNS64-enabled server can retrieve the A record of the IPv4 server and synthesize an AAAA record. The IPv6-only host can then use the synthesized AAAA record, which contains the IPv6 proxy address for the IPv4 address in the original A record, to initiate communication with the IPv4 host.

Figure 15.3

Following are the steps illustrated in Figure 15.3:

1. An IPv6-only host sends a recursive query for the AAAA record of the IPv4 server mail1.corp100.com.
2. The Infoblox DNS server attempts to resolve the request for the AAAA record, and determines that an AAAA record for mail1.corp100.com does not exist. The DNS server then performs a query for the A record of mail1.corp100.com.
3. The DNS server creates a synthetic AAAA resource record from the information in the A record, and returns the synthesized AAAA record to the requesting IPv6 host.
4. The host receives the synthetic AAAA record and sends a packet to the destination address specified in the synthetic AAAA record. The packet is routed to the IPv6 interface of the NAT64 device, which translates the packet from IPv6 to IPv4 and forwards it to the server, mail1.corp100.com.

Infoblox DNS servers can return synthesized AAAA records to both IPv4 and IPv6 clients when the client explicitly requests an AAAA record and none exists for the requested host. If a host has multiple A records, the DNS server synthesizes an AAAA record for each A record.
Infoblox DNS servers can also synthesize records for reverse-mapping zones. When a DNS server receives a query for a PTR record in the IP6.ARPA domain whose address matches a configured DNS64 prefix, the server synthesizes a CNAME record that contains an IPv4 address derived from the IPv6 address in the query. The server then sends a query for the PTR record so it can resolve the IPv4 address to the hostname.

For example, if a DNS server that is configured to synthesize records for the prefix 2001:db8::/96 receives a query for the PTR record of 2001:db8::0102:0304, it synthesizes a CNAME record that contains the IPv4 address 4.3.2.1.in-addr.arpa. The server then resolves the PTR record of the IPv4 address 4.3.2.1.in-addr.arpa.

If the server obtains the PTR record, then it sends the synthesized CNAME record and the PTR record to the client. If the zone exists, but there is no PTR record, then the server sends the synthesized CNAME record only. If the zone does not exist, then the server responds with a SERVFAIL with no answers.

Additionally, Infoblox DNS servers can generate synthesized records for DNSSEC secure zones, but only for non-DNSSEC clients. A DNS client or resolver includes the EDNS OPT pseudo-RR with the DO (DNSSEC OK) bit set to indicate that they are requesting DNSSEC data. DNS servers can generate synthesized AAAA records only when the request does not have the DO bit set. This ensures that DNSSEC clients receive only valid responses.

For additional information about DNS64, refer to the following Internet drafts:

Configuring DNS64

You can enable DNS64 on both authoritative and recursive DNS servers. You can configure DNS64 at the Grid, member or DNS view level.

To configure DNS64 on Infoblox DNS servers:

1. Create at least one DNS64 synthesis group. A synthesis group specifies the IPv6 prefix of the synthesized AAAA records. For more information, see Adding a DNS64 Synthesis Group on page 474.
2. Optionally, specify additional parameters for the synthesis group. For more information, see Setting Group Properties on page 475.
3. Enable the DNS64 service and assign a synthesis group to the Grid, a member or a DNS view. For more information, see Enabling DNS64 Service on page 476.

On the NAT64 device, you must specify the IPv6 prefixes that are configured on the DNS server.
About Synthesis Groups

A synthesis group specifies, among other things, the IPv6 prefix for the synthesized AAAA records. Infoblox DNS servers provide a default DNS64 synthesis group with the well-known prefix 64:ff9b::/96, which is reserved for representing IPv4 addresses in the IPv6 address space. You can keep the default group, change the prefix or delete the group. You can also add a synthesis group for a Network-Specific Prefix (NSP), which is an IPv6 prefix assigned to an organization to create IPv6 representations of IPv4 addresses.

After you create a synthesis group, you can define rules to restrict the synthesis of AAAA records to certain IPv4 addresses and networks, and specify the DNS clients and networks to which the server can send synthesized AAAA records. For more information, see Setting Group Properties on page 475.

Note that though you can control the synthesis of AAAA records, the DNS server always synthesizes CNAME records when it receives a query for an IPv6 PTR record whose address matches a prefix in a DNS64 synthesis group.

Adding a DNS64 Synthesis Group

To add a synthesis group:

1. From the Data Management tab, select the DNS tab -> DNS64 Groups tab, and then click the Add icon.
2. In the DNS64 Synthesis Group wizard, complete the following:
   - Name: Enter a name for the group.
   - Prefix: The IPv6 prefix used for the synthesized AAAA records. The default is the well-known prefix 64:FF9B::/96. The prefix length must be /32, /40, /48, /56, /64, and /96, and all bits beyond the specified length must be zero.
   - Comment: Optionally, enter additional information about the group.
   - Disabled: Select this check box if you would like to disable the group at this time. Note that you cannot disable the group if it is the only group that is used by a Grid, member or DNS view that has DNS64 enabled.
3. Click Next to define extensible attributes for the synthesis group. For information, see Using Extensible Attributes on page 265.
4. Save the configuration.

Viewing DNS64 Synthesis Groups

To view synthesis groups, from the Data Management tab, select the DNS tab -> DNS64 Groups tab. This tab displays the following information about each group:

- Name: The group name.
- Prefix: The IPv6 prefix that is assigned to the group.
- Comment: The comment that was entered for the group.
- Site: The value of this attribute, if specified.

You can display the following additional column:
- Disabled: Indicates whether the group is disabled.

You can do the following:
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables on page 52.
- Edit the properties of a synthesis group.
  - Select the synthesis group, and then click the Edit icon.
- Move a synthesis group to the Recycle Bin.
  - Select the synthesis group, and then click the Delete icon. Note that you cannot delete a synthesis group that is assigned to a Grid, member or DNS view.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
• Create a quick filter to save frequently used filter criteria. For information, see *Using Quick Filters* on page 57.
  — Click the Export icon.
• Print the list of synthesis groups.
  — Click the Print icon.

### Setting Group Properties

After you create a DNS64 synthesis group, you can specify the following:

- The DNS clients and networks to which the DNS server is allowed to send synthesized AAAA records with the specified IPv6 prefix.
- The IPv4 addresses and networks for which the DNS server can synthesize AAAA records with the specified prefix.
- IPv6 addresses or prefix ranges that cannot be used by IPv6 only hosts, such as IP addresses in the ::ffff:0:0/96 network. When the DNS server retrieves an AAAA record that contains an IPv6 address that matches an excluded address, it does not return the AAAA record. Instead, it synthesizes an AAAA record from the A record.
  
  Note that a DNS server synthesizes the AAAA record of a host that has both A and AAAA records when all the IPv6 addresses in the AAAA records match the excluded addresses. If the host has multiple AAAA records and some of them contain excluded IPv6 addresses, then the server returns the remaining AAAA records.

1. From the *Data Management* tab, select the *DNS* tab -> *DNS64 Groups* tab -> *group* check box -> *Edit* icon.
2. In the *General* tab of the *DNS64 Synthesis Groups* editor, you can do the following:
  — Modify the name, prefix or comment.
  — Select the *Disabled* check box, if you want to disable the group at this time.
  — **Perform DNS64 synthesis for these clients:** Specify IPv4 and IPv6 hosts and networks to which Infoblox DNS servers can send synthesized AAAA records. The default is to allow any IPv4 and IPv6 address and network.
    
    Click the Add icon and 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 IPv4 address of the host. 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 host. 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.
    — **Any Address/Network:** Select to allow/disallow synthesized AAAA records for any IP address.
Configuring DNS Services

— **Mapped IPv4 Addresses**: Specify IPv4 addresses and networks for which the DNS server synthesizes AAAA records. The default is to allow the DNS server to synthesize AAAA records for any IPv4 address in any network.

Click the Add icon and 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 IP address. 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 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 disallow synthesized AAAA records for any IPv4 address.

— **Exclude IPv6 addresses**: Specify IPv6 addresses of AAAA records that the appliance treats as nonexistent. The DNS server does not return the AAAA record of an address from this list. Instead, it synthesizes an AAAA record from the A record.

Click the Add icon and 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:

— **IPv6 Address**: In the Name field of the new row, enter the IPv6 address. 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.

— **Any Address/Network**: Select to allow or disallow any IPv6 address.

— **Extensible Attributes**: You can modify the attributes. For information, see Using Extensible Attributes on page 265.

— **Permissions**: This tab displays if you logged in as a superuser. For information, see About Administrative Permissions on page 120.

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

### Enabling DNS64 Service

You can enable DNS64 at the Grid, member, and DNS view level. At least one DNS64 synthesis group must be configured before you can enable DNS64.

To enable DNS64 and apply DNS64 synthesis groups:

1. **Grid**: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties. 
   **Member**: From the Data Management tab, select the DNS tab -> Members tab -> member check box -> Edit icon. 
   **DNS View**: From the Data Management tab, select the DNS tab -> Zones tab -> dns_view check box -> Edit icon. 
   To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the Grid and Member DNS Properties editor, click Toggle Expert Mode, and then click DNS64. In the View DNS Properties editor, just click DNS64.

3. Do the following in the DNS64 tab:
   — **Enable DNS64**: Select this check box.
   — **Synthesis Groups**: Click the Add icon and select a synthesis group.

4. Save the configuration and click Restart if it displays.
Chapter 16 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, DHCPv6 and DNS to support DDNS updates. It contains the following main sections:

- Understanding DDNS Updates from DHCP on page 479
- Configuring DHCP for DDNS on page 483
  - Enabling DDNS for IPv4 and IPv6 DHCP Clients on page 484
  - Sending Updates to DNS Servers on page 485
- Configuring DDNS Features on page 487
  - Resending DDNS Updates on page 487
  - Generating Host Names for DDNS Updates on page 487
  - Updating DNS for IPv4 Clients with Fixed Addresses on page 487
  - Configuring DDNS Features on page 488
- About the Client FQDN Option on page 489
  - Enabling FQDN Option Support on page 490
  - Sending Updates for DHCP Clients Using the FQDN Option on page 491
- Configuring DDNS Update Verification on page 492
- Configuring DNS Servers for DDNS on page 495
  - Enabling a DNS Server to Accept DDNS Updates on page 495
  - Forwarding Updates on page 496
- Supporting Active Directory on page 498
  - Sending DDNS Updates to a DNS Server on page 498
- About GSS-TSIG on page 499
  - Sending Secure DDNS Updates to a DNS Server in the Same Domain on page 500
  - Configuring DHCP to Send GSS-TSIG Updates in the Same Domain on page 502
  - Sending Secure DDNS Updates to a DNS Server in Another Domain on page 509
  - Configuring DHCP to Send GSS-TSIG Updates to Another Domain on page 510
  - Sending GSS-TSIG Updates to a DNS Server in Another Forest on page 512
- Accepting DDNS Updates from DHCP Clients on page 513
  - Supporting Active Directory and Unauthenticated DDNS Updates on page 513
• Accepting GSS-TSIG-Authenticated Updates on page 515
  — Configuring DNS to Receive GSS-TSIG Updates on page 517
Understanding DDNS Updates from DHCP

DHCP supports several DNS-related options (such as options 12, 15, and 81 for IPv4, and options 23, 24, and 39 for IPv6). With DDNS (Dynamic DNS) updates, a DHCP server or client can use the information in these options to inform a DNS server of dynamic domain name-to-IP address assignments.

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 16.1.

*Figure 16.1 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 16.2).

1. When an IPv4 DHCP client requests an IP address, the client sends its host name (DHCP option 12). The client also includes its MAC address in the ethernet frame header.

2. 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 463.

**Figure 16.2 DDNS Update from a DHCP Server**

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.

Note: The DHCP server asynchronously updates DNS for a particular lease and sends the DHCP ACK to the client requesting the lease. If the DNS update is unsuccessful, the DHCP client still gets its lease. The DHCP server then continues its DNS update attempts at predefined or user-defined intervals.
To enable a DHCP server to send DDNS updates to a DNS server, you must configure both servers to support the updates. First, configure the DHCP server to do the following:

- Provide what is needed to create an FQDN: add a server-generated host name to a server-provided domain name, add a server-provided domain name to a client-supplied host name, or permit the client to provide its own FQDN
- Send updates to a DNS server

Then, configure the following on the DNS server:

- Accept updates from the DHCP server, a secondary DNS server, or a DHCP client
- If the DHCP server sends updates to a secondary DNS server, configure the secondary server to forward updates to the primary DNS server
When setting up DDNS, you can determine the amount of information that DHCP clients provide to a DHCP server—and vice versa—and where the DDNS updates originate. A summary of these options for IPv4 is shown in Figure 16.3. It is similar for IPv6, except that the DHCP client and server exchange Request and Reply messages, AAAA records are updated instead of A records, and the FQDN option is option 39.

**Figure 16.3 DHCP Clients and Server Providing DNS Information and Updates**

You can configure the DHCP and DNS settings for DDNS at the Grid level, member level, and network and zone level. By applying the inheritance model in the NIOS appliance, settings made at the Grid level apply to all members in the Grid. Settings you make at the member level apply to all networks and zones configured on that member. Settings made at the network and zone level apply specifically to just that network and zone. When configuring independent appliances (that is, appliances that are not in a Grid), do not use the member-level settings. Instead, configure DDNS updates at the Grid level to apply to all zones and, if necessary, override the Grid-level settings on a per zone basis.
Configuring DHCP for DDNS

Before a DHCP server can update DNS, the DHCP server needs to have an FQDN-to-IP address mapping. When a DHCP IPv4 client requests an IP address, it typically includes its host name in option 12 of the DHCPDISCOVER packet, and an IPv6 client includes its hostname in the Request packet. You can configure the NIOS appliance to include a domain name in option 15 of the IPv4 DHCPOFFER packet or in the IPv6 Reply packet. You specify this domain name in the IPv4 DHCP Options -> Basic and IPv6 DHCP Options -> Basic tabs of the Grid DHCP Configuration editor, Member DHCP Configuration editor, and the Network editor. For IPv4 clients you can also specify a domain name in the DHCP Range and Fixed Address editors.

Then, you can enable the DHCP server to send DDNS updates for IPv4 and IPv6 clients, as described in Enabling DDNS for IPv4 and IPv6 DHCP Clients on page 484. After you enable the DHCP server to send DDNS updates, you can do the following:

- Configure the DHCP server to send DDNS updates to DNS servers in the Grid. For information, see Sending Updates to DNS Servers in the Grid on page 485.
- Configure the DHCP server to send DDNS updates to external DNS servers. For information, see Configuring DDNS Features on page 487.
- Configure certain DDNS features. For information, see Configuring DDNS Features on page 488.
- Enable support for the FQDN option for IPv4 and IPv6 clients, and configure how the DHCP server updates DNS. For information, see Enabling FQDN Option Support on page 490.

Note: Whether you deploy NIOS appliance in a Grid or independently, they send updates to UDP port 53. Grid members do not send updates through a VPN tunnel; however, Grid members do authenticate updates between each other using TSIG (transaction signatures) based on an internal TSIG key.
Enabling DDNS for IPv4 and IPv6 DHCP Clients

You can enable the DHCP server to send DDNS updates for IPv4 clients at the Grid, member, shared network, network, address range, DHCP template, fixed address, and roaming host levels, and for IPv6 clients at the Grid, member, network, shared network, network template and roaming host levels.

You can specify a different domain name that the appliance uses specifically for DDNS updates. The appliance combines the hostname from the client and the domain name you specify to create the FQDN that it uses to update DNS. For IPv4 clients, you can specify the DDNS domain name at the network, network template, range, and range template levels. For IPv6 clients, you can specify the DDNS domain name at the Grid, member, network, shared network, and network template levels. You can also use the name of a roaming host record as the name of the client for DDNS updates, as described in Setting Properties for Roaming Hosts on page 663.

To enable DDNS and specify a DDNS domain name:

1. **Grid**: From the Data Management tab, select the DHCP tab, expand the Toolbar and click Grid DHCP Properties. 
   - **Member**: From the Data Management tab, select the DHCP tab and click the Members tab -> Members -> member check box -> Edit icon.
   - **Network**: From the Data Management tab, select the DHCP tab and click the Networks tab -> Networks -> network check box -> Edit icon.
   - **Network Template**: From the Data Management tab, select the DHCP tab and click the Templates tab -> DHCP_template check box -> Edit icon.
   - **Roaming Host**: From the Data Management tab, select the DHCP tab and click the Networks tab -> Roaming Hosts -> roaming_host -> Edit icon.

   For IPv4 clients only:
   - **IPv4 Address Range**: From the Data Management tab, select the DHCP tab and click the Networks tab -> Networks -> network -> addr_range check box -> Edit icon.
   - **IPv4 Fixed Address**: From the Data Management tab, select the DHCP tab and click the Networks tab -> Networks -> network -> ip_addr check box -> Edit icon.
   - **IPv4 Address Range/Fixed Address Template**: From the Data Management tab, select the DHCP tab and click the Templates tab -> DHCP_template check box -> Edit icon.

   To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the IPv4 DDNS -> Basic tab or the IPv6 DDNS -> Basic tab, complete the following:
   - **Enable DDNS Updates**: Select this check box to enable DDNS updates. When setting properties for DHCP objects other than the Grid, you must click Override and select Enable DDNS updates for the DDNS settings to take effect.
   - **DDNS Update TTL**: You can set the TTL used for A or AAAA and PTR records updated by the DHCP server. The default is shown as zero. If you do not enter a value here, the appliance by default sets the TTL to half of the DHCP lease time with a maximum of 3600 seconds. For example, a lease time of 1800 seconds results in a TTL of 900 seconds, and a lease time of 86400 seconds results in a TTL of 3600 seconds. For information about how to set the lease time, see Defining Lease Times on page 590.
   - **DDNS domain name**: Specify the domain name of the network that the appliance uses to update DNS. For IPv4 clients, you can specify this at the network, network template, range, and range template levels. For IPv6 clients, you can specify this at the Grid, member, network, shared network, and network template levels.
   - **Update DNS on DHCP Lease Renewal**: Select this check box to enable the appliance to update DNS when a DHCP lease is renewed.

3. Save the configuration and click Restart if it displays at the top of the screen.
Sending Updates to DNS Servers

The DHCP server can send DDNS updates to DNS servers in the same Grid and to external DNS servers. When you enable the appliance to send updates to Grid members, you must specify the DNS view to be updated. If a network view has multiple DNS views, you can select only one DNS view for DDNS updates. For information about DNS views, see Using Infoblox DNS Views on page 356.

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 on page 489. 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 487.

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

The appliance sends DDNS updates to the appropriate zones in the selected DNS view. Note that you cannot delete a DNS view that has been selected for DDNS updates. By default, the DHCP server sends DDNS updates to zones using the domain name that you define for DHCP objects, such as networks and DHCP ranges.

Sending Updates for Zones on an External Name Server

The DHCP server can send dynamic updates to an external name server that you specify. For each network view, you can specify the zone to be updated and the IP address of the primary name server for that zone. You can add information for a forward and reverse zone. The DHCP server updates the A record in the forward zone and the PTR record in the reverse zone.

You can also use TSIG (transaction signatures) or GSS-TSIG to secure communications between the servers. TSIG uses the MD5 (Message Digest 5) algorithm and a shared secret key to create an HMAC (hashed message authentication code)—sometimes called a digital fingerprint—of each update. Both the DHCP server sending the update and the DNS server receiving it must share the same secret key. Also, it is important that the time stamps on the TSIG-authenticated updates and update responses be synchronized, or the participants reject them. Therefore, use an NTP server to set the time on all systems involved in TSIG authentication operations.

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 Algorithm**: Select either **HMAC-MD5** or **HMAC-SHA256**.

  **Key Data**: To use an existing TSIG key, type or paste the key in the **Key Data** field. Alternatively, you can select the key algorithm, select the key length from the **Generate Key Data** drop down list, and then click **Generate Key Data** to create a new key.

  — **GSS-TSIG**: For information about using GSS-TSIG, see *About GSS-TSIG* on page 499.

4. Save the configuration and click **Restart** if it displays at the top of the screen.
Configuring DDNS Features

You can enable the DHCP server to support certain DDNS features for IPv4 and IPv6 clients. These features affect the behavior of the DHCP server and how it handles DDNS updates. The following sections describe the different features you can set.

Resending DDNS Updates

You can enable the DHCP server to make repeated attempts to send DDNS updates to a DNS server. The DHCP server asynchronously updates DNS for a particular lease and sends the DHCP ACK to the client requesting the lease. If the update fails, the DHCP server still provides the lease and sends the DHCP ACK to the client. The DHCP server then continues to send the updates until it is successful or the lease of the client expires. You can change the default retry interval, which is five minutes.

You can enable this feature for the Grid and for individual Grid members.

Generating Host Names for DDNS Updates

Some IPv4 and IPv6 clients do not send a host name with their DHCP requests. When the DHCP server receives such a request, its default behavior is to provide a lease but not update DNS. You can configure the DHCP server to generate a host name and update DNS with this host name when it receives a DHCP request that does not include a host name. It generates a name in the following format: dhcp-ip_address, where ip_address is the IP address of the lease. For example, if this feature is enabled and the DHCP server receives a DHCP REQUEST from an IPv4 DHCP client with IP address 10.1.1.1 and no host name, the DHCP server generates the name dhcp-10-1-1-1 and appends the domain name, if specified, for the DDNS update. Likewise, if an IPv6 client with IP address 2001:db8:a23:0:0:0:0:d sends a request, the DHCP server generates the name dhcp-2001-db8-a23-0-0-0-0-d and appends the domain name, if specified, for the DDNS update.

Updating DNS for IPv4 Clients with Fixed Addresses

By default, the DHCP server does not update DNS when it allocates an IPv4 or IPv6 fixed address to a client. You can configure the DHCP server to update the A and PTR record of IPv4 clients with a fixed address. When you enable this feature and the DHCP server adds A and PTR records for a fixed address, the DHCP server never discards the records. When the lease of the client terminates, you must delete the records manually. Note that the DHCP server does not send DDNS updates for IPv6 fixed addresses and hosts.

You can define fixed address settings for the Grid, Grid members, IPv4 networks, and IPv4 shared networks.
Configuring DDNS Features

You can configure DDNS features for a Grid, its member, IPv4 and IPv6 networks and shared networks, and IPv4 DHCP address ranges. You cannot set DDNS features for IPv6 DHCP ranges.

To configure DDNS features:

1. **Grid:** From the **Data Management** tab, select the **DHCP** tab, expand the Toolbar and click **Grid DHCP 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 -> **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:** You can set this for a Grid and its members only.
     - **Retry Updates When Server Becomes Available:** Select this check box.
     - **Retry Interval (Minutes):** You can optionally set the retry interval. The default is five minutes.
   - **Generate Hostname**
     - **Generate Hostname if not Sent by Client:** Select this check box to enable the DHCP server to generate a hostname and update DNS with this hostname, when the DHCP request of a client does not include a hostname.
   - **Fixed Address Updates:** You can set this for IPv4 fixed addresses only. This option is available in the **IPv4 DDNS Advanced** tab of the **Grid DHCP Properties** and **Member DHCP Properties** editors, and in the **IPv4 DDNS Basic** tab of the **IPv4 DHCP Network** and **Shared Network** editors.
     - **Update Fixed Addresses:** Select this check box to allow the DHCP server to send updates to DNS for IPv4 fixed addresses.

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

When a lease expires, the DHCP server removes the A, AAAA, and PTR records that it updated. It does not remove any records that the client updated.
About the Client FQDN Option

When an IPv4 DHCP client sends DHCP DISCOVER and DHCP REQUEST messages, it can include option 81, the Client FQDN option. An IPv6 DHCP client can include option 39, the Client FQDN option, when it sends Solicit and Request messages.

The Client FQDN option contains 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 for IPv4 and IPv6 clients, and use the host name or FQDN that the client provides for the update. It can also allow or deny the client’s request to update DNS, according to the administrative policies of your organization. The DHCP server indicates its response in the DHCP OFFER message it sends back to an IPv4 client, and in the Reply message it sends back to an IPv6 client.

Sending Updates with the FQDN Option Enabled

When you enable the DHCP server to support the FQDN option, it uses the information provided by the IPv4 or IPv6 client to update DNS as follows:

- When an IPv4 or IPv6 DHCP client sends a DHCP request with the FQDN option, it can include either its FQDN or only its host name.
  - If the request includes the FQDN, the DHCP server uses this FQDN to update DNS. You can specify a list of forward-mapping zones to be updated for IPv4 and IPv6 clients using the FQDN option. For information, see Sending Updates for DHCP Clients Using the FQDN Option on page 491.
  - If the request includes the host name, the DHCP server provides the domain name. It combines the host name of the client and the domain name to create an FQDN for the client. It then updates DNS with the FQDN it created. (You can enter the domain name in the General page of the DHCP Properties window. For information, see Enabling DDNS for IPv4 and IPv6 DHCP Clients on page 484.)
- When a DHCP client sends a DHCP request with its hostname, the DHCP server adds the domain name you specified to create an FQDN for the client. It then updates DNS with the FQDN it created. For information about entering the domain name, see Enabling DDNS for IPv4 and IPv6 DHCP Clients on page 484.
- 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 487.
- If multiple DHCP clients specify the same FQDN or host name, the DHCP server allocates leases to the clients, but updates DNS only for the client that first sent the request. When it tries to update DNS for the succeeding clients, the update fails.

Sending Updates from DHCP Clients or a DHCP Server

When you enable the DHCP server to support the FQDN option, you must decide if you want the DHCP server to allow clients to update DNS. If you allow the client to update DNS, then the client updates its A or AAAA record only. The DHCP server always updates the PTR records. You can configure the DHCP server as follows:

- The DHCP server can allow clients to update DNS when they send the request in the FQDN option. This is useful for small sites where security is not an issue or in sites where clients move from one administrative domain to another and want to maintain the same FQDN regardless of administrative domain.
  
  If you configure the DHCP server to allow clients to perform DDNS updates, you must also configure the DNS server to accept these updates from clients. Note that multiple clients can use the same name, resulting in multiple PTR records for one client name.
  
  When a lease expires, the DHCP server does not delete the A or AAAA record, if it was added by the client.
- The DHCP server can refuse the DHCP client’s request to update DNS and always perform the updates itself.
  
  When the DHCP server updates DNS, it uses the FQDN provided by the DHCP client. Select this option if your organization requires tighter control over your network and does not allow clients to update their own records.
If you do not enable support for the FQDN option 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.

Do the following to configure support for the FQDN option for both IPv4 and IPv6 clients:

- Enable support for the option and specify who performs the DDNS update. For more information, see Enabling FQDN Option Support on page 490.
- Specify the DNS zones and DNS view for the updates. For more information, see Sending Updates for DHCP Clients Using the FQDN Option on page 491.

### Enabling FQDN Option Support

You can configure support for the FQDN option for IPv4 and IPv6 clients at the Grid, member, network and shared network levels.

To configure support for the FQDN Option (option 81) for IPv4 and (Option 39) for IPv6:

1. **Grid**: From the Data Management tab, select the DHCP tab, expand the Toolbar and click Grid DHCP Properties.
   - **Member**: From the Data Management tab, select the DHCP tab and click the Members tab -> member check box -> Edit icon.
   - **Network**: From the Data Management tab, select the DHCP tab and click the Networks tab -> Networks -> network check box -> Edit icon.
   - **Shared Network**: From the Data Management tab, select the DHCP tab and click the Networks tab -> Shared Networks -> shared_network check box -> Edit icon.
     
     To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the IPv4 DDNS -> Advanced tab for the Grid and member, or the IPv4 DDNS -> Basic tab for the network, do the following:
   - **Option 81 Support**
     - **Enable Option 81 Support**: Select this to enable the support for option 81.
     - **DHCP server always updates DNS**: Select this to allow the DHCP server to update DNS, regardless of the requests from DHCP clients.
     - **DHCP server updates DNS if requested by client**: Select this to allow the DHCP server to update DNS only when requested by DHCP clients.

3. In the IPv6 DDNS -> Advanced tab for the Grid and member, or the IPv6 DDNS -> Basic tab for the network, do the following:
   - **FQDN Support**: Select Enable FQDN Support and select one of the following to indicate whether the DHCP server or the client performs the DDNS update.
     - DHCP always updates DNS
     - DHCP always updates DNS
     - DHCP updates DNS if requested by client

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

When a lease expires, the DHCP server removes the A or AAAA records and PTR records that it updated. It does not remove any records that the client updated.
Sending Updates for DHCP Clients Using the FQDN Option

You must specify the DNS view to be updated for each network view.

To send updates to zones for DHCP IPv4 and IPv6 clients using the FQDN option:

1. If there are multiple network views in the Grid, select a network view.
2. From the Data Management tab, select the DHCP tab, and then click Configure DDNS from the Toolbar.
3. In the DDNS Properties editor, complete the following:
   - DNS View: If a network view has more than one DNS view, this field lists the associated DNS views. From the drop-down list, select the DNS view to which the DHCP server sends DDNS updates. Otherwise, the appliance uses the default DNS view.
   - Zones to Update for Hosts Using DHCP FQDN Option: In this section, you can define forward-mapping zones to which the DHCP server sends DDNS updates for IPv4 and IPv6 DHCP clients that use the FQDN option. You must first enable support for the FQDN option before the DHCP server can send DDNS updates to these zones. By default, the DHCP server sends DDNS updates to zones using the domain name that you define for DHCP objects, such as networks and DHCP ranges. For clients using this option, the DHCP server uses the domain name defined in the option.
     Click the Add icon to specify a forward-mapping zone. Note that the Forward-mapping Zone Selector dialog box displays only the DNS zones that are associated with the selected DNS view. The zones you select here are written to the dhcpd.conf file and the dhcpdv6.conf file as "zone" statements with the matching TSIG key of the DNS view, so the updates are sent to the correct DNS view.
4. Save the configuration and click Restart if it displays at the top of the screen.
Configuring DDNS Update Verification

The DHCP server can handle DDNS updates differently, depending on how stringently you configure record handling. You can configure the DHCP server to update records only after passing verification. You can adjust the way DHCP handles updates so the DHCP server updates records after passing less stringent verification requirements, or without any type of verification.

To provide a measure of protection against unintentional changes of DNS data, NIOS appliances support the generation and use of TXT records, as described in IETF draft, draft-ietf-dhc-dhcp-dns-12.txt and by the ISC (Internet Systems Consortium). When DHCP updates or deletes an A or AAAA record, the corresponding TXT record is checked first to verify the authenticity of the update. The TXT record is based on a hash of the DHCID which is unique to each client, usually based in part on the MAC address or the DUID. If the client requests an update to DNS, the DHCP server first checks the TXT record to verify that it matches the client that originally inserted the record. This process provides assurance that the updates are from the same client. These security checks are based upon inserting a cryptographic hash of the DHCID (DHCP Client Identifier) into a DNS TXT RR and then verifying that value before updating. For example, a sample client update adds the following records in DNS:

<table>
<thead>
<tr>
<th>Hostname</th>
<th>TTL</th>
<th>Type</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>oxcart.lo0.net.</td>
<td>21600</td>
<td>IN A</td>
<td>172.31.1.20</td>
</tr>
<tr>
<td>oxcart.lo0.net.</td>
<td>21600</td>
<td>IN TXT</td>
<td>&quot;313ce164780d34b91486b7c489ed7467e6&quot;</td>
</tr>
<tr>
<td>20.1.31.172.in-addr.arpa.</td>
<td>21600</td>
<td>IN PTR</td>
<td>oxcart.lo0.net.</td>
</tr>
</tbody>
</table>

However, your DNS configuration might require that the NIOS appliance handle DNS record updates differently than described in draft-ietf-dhc-dhcp-dns-12.txt. Your specific requirements might benefit from less-stringent verification of the DHCID, or might require skipping verification entirely. Verification checks might cause complications in some specific cases described below:

- **Mobility**: The TXT record is based on the DHCID unique to each client and is usually based on the MAC address or DUID of the interface. Devices such as laptops that connect to both wired and wireless networks have different MAC addresses or DUIDs and different DHCID values for each interface. In this scenario, after either one of the network interfaces inserts a DNS record, updates are allowed from that interface only. This results in a disruption of service for DDNS updates when roaming between wired and wireless networks.

- **Migration**: The second problem occurs during a migration from non-ISC based systems to ISC systems. For example, if the user is migrating from a Microsoft-based system, the clients have A or AAAA and PTR records in the DDNS updates but no TXT records. As a result, new DDNS updates fail after the migration.

- **Mixed Environments**: The final problem occurs in mixed ISC and non-ISC environments. For example, assume that both Microsoft and ISC DHCP servers update DNS records on the appliance. 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 16.4 on page 493:

**Figure 16.4  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 or AAAA, Add A or AAAA, Add PTR</td>
<td>Delete PTR</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Delete A or AAAA, TXT if TXT matches and no other A or AAAA RRs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No A or AAAA record</td>
<td>No check</td>
<td>Add A or AAAA, TXT Add PTR</td>
<td></td>
</tr>
<tr>
<td>Check TXT only</td>
<td>Exists</td>
<td>Must exist</td>
<td>Delete A or AAAA, TXT Add A or AAAA, TXT Add PTR</td>
<td>Delete PTR</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Delete A or AAAA if TXT exists and no other A or AAAA RRs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No A or AAAA record</td>
<td>No check</td>
<td>Add A or AAAA, TXT Add PTR</td>
<td></td>
</tr>
<tr>
<td>ISC Transitional</td>
<td>Exists</td>
<td>No check</td>
<td>Delete A or AAAA, TXT if exists Add A or AAAA, TXT Add PTR</td>
<td>Delete PTR</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Delete A or AAAA, TXT if TXT matches and no other A or AAAA RRs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No A or AAAA record</td>
<td>No check</td>
<td>Add A or AAAA, TXT Add PTR</td>
<td></td>
</tr>
<tr>
<td>No TXT record</td>
<td>Exists</td>
<td>No check</td>
<td>Delete A or AAAA, Add A or AAAA, Add PTR</td>
<td>Delete PTR, A or AAAA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No A or AAAA record</td>
<td>No check</td>
<td>Add A or AAAA, 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 or AAAA record.
You can enable this feature at the Grid level. To configure TXT record handling on the DHCP server:

1. From the **Data Management** tab, select the **DHCP** tab, expand the Toolbar and click **Grid DHCP Configuration**.

2. In the **IPv4 DDNS -> Advanced** tab or the **IPv6 DDNS -> Advanced** tab, select one of the following from the **TXT (DHCID) Record Handling** drop-down list:
   - **Check Only**: Select this check box to enable minimal checking of DDNS updates. Specifically, A or AAAA records are modified only if a TXT record exists. The NIOS appliance checks that a TXT record exists, but does not check its value.
   - **ISC**: Select this check box to enable standard ISC (Internet Systems Consortium) handling for DDNS updates. Specifically, A or AAAA records are modified or deleted only if the TXT records match. This option is the default setting on the appliance.
   - **ISC Transitional**: Select this check box to enable less stringent handling of DDNS updates. Specifically, the NIOS appliance enables you to add or modify A or AAAA records whether or not TXT records exist. It checks whether a TXT record exists and then processes the update. If the appliance does not find a TXT record, it adds the record.
   - **No TXT Record**: Select this check box to disable TXT record checking. Specifically, A or AAAA records are added, modified, or deleted whether or not the TXT records match. No TXT records are added, and existing TXT records are ignored.

3. Save the configuration and click **Restart** if it displays at the top of the screen.
Configuring DNS Servers for DDNS

For security reasons, an Infoblox DNS server does not accept DDNS updates by default. You must specify the sources from which you want to allow the DNS server to receive updates. You can configure the Infoblox DNS server to receive updates from specified DHCP clients, as described in Enabling a DNS Server to Accept DDNS Updates, and to accept forwarded updates from another DNS server, as described in Forwarding Updates on page 496.

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 receive updates from specified DHCP clients only. You can set this for the Grid so that the Grid members receive DDNS updates only from the specified sources. Note that you specify the IP addresses of the sources of the updates and not the actual IP addresses in the DNS records being updated.

To configure the DNS server to accept updates from the specified sources:

1. Grid: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
   Member: From the Data Management tab, select the DNS tab and click the Members tab ->member check box -> Edit icon.
   Zones: From the Data Management tab, select the DNS tab and click the Zones tab->dns_view ->zone check box ->Edit icon.
   To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the editor, click Updates.

3. In the Updates ->Basic tab, click the Add icon beside Allow updates from to specify the sources of the updates. 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.
Configuring DDNS Updates from DHCP

1. **Permission**: Select Allow or Deny from the drop-down list.

2. **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.

3. **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.

4. **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 Algorithm**: Select either HMAC-MD5 or HMAC-SHA256.
   - **Key Data**: To use an existing TSIG key, type or paste the key in the Key field. Alternatively, you can select the key algorithm, select the key length from the Generate Key Data drop down list, and then click Generate Key Data to create a new key.

5. **Any Address/Network**: Select to allow or deny updates from any IP address.

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

**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 Expert 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 Algorithm*: Select either *HMAC-MD5* or *HMAC-SHA256*.
  • *Key Data*: To use an existing TSIG key, type or paste the key in the *Key Data* field. Alternatively, you can select the key algorithm, select the key length from the *Generate Key Data* drop down list, and then click *Generate Key Data* to create a new key.

— **Any Address/Network**: Select to allow or disallow the appliance to forward updates from any IP address.

4. Save the configuration and click *Restart* if it displays at the top of the screen.
**Supporting Active Directory**

Active Directory™ (AD) is a distributed directory service that authenticates network users and—by working with DHCP and DNS—provides the location of and authorizes access to services running on devices in a Windows® network. You can integrate a NIOS appliance providing DHCP and DNS services with servers running Windows 2000 Server, Windows Server 2003, Windows Server 2008, 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 16.5*.

*Figure 16.5 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 20, Configuring DHCP Properties*, on page 587; and for information on configuring the DHCP server to send DDNS updates, see *Configuring DHCP for DDNS* on page 483.) For information about configuring a DHCP server to send GSS-TSIG authenticated updates, see *About GSS-TSIG* on page 499.
About GSS-TSIG

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 500.
  - 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 509
  - For information, see Accepting GSS-TSIG-Authenticated Updates on page 515

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 16.6. In the illustration, the Kerberos Key Distribution Center (KDC) is running on an AD domain controller, which also provides DNS service.

Figure 16.6  An Infoblox DHCP Server Sends GSS-TSIG Updates to a DNS Server

After you enable the NIOS appliance to send GSS-TSIG authenticated updates to a DNS server, the following process occurs:

1. Kerberos – Login, and TGT and Service Ticket Assignments
   a. The Infoblox appliance automatically logs in to the AD/Kerberos server.
   b. The Kerberos server sends the appliance a TGT (ticket-granting ticket).
   c. Using the TGT, the appliance requests a service ticket for the DNS server.
   d. The Kerberos server replies with a service ticket for that server.
2. **TKEY negotiations (GSS Handshake):**
   a. The appliance sends the DNS server a TKEY (transaction key) request. A Transaction Key record establishes shared secret keys for use with the TSIG resource record. For more information, see *RFC 2930, Secret Key Establishment for DNS (TKEY RR).*
   
   The request includes the service ticket. The service ticket includes the appliance’s principal and proposed TSIG (transaction signature) key, along with other items such as a ticket lifetime and a timestamp.
   b. The DNS server responds with a DNS server-signed TSIG, which is a “meta-record” that is never cached and never appears in zone data. A TSIG record is a signature of the update using an HMAC-MD5 hash that provides transaction-level authentication. For more information, see *RFC 2845, Secret Key Transaction Authentication for DNS (TSIG).*
   
   The two participants have established a security context.

When a DHCP client sends a request for an IP address to the DHCP server, the following occurs:

3. **DHCP – IP Address and Network Parameters Assignment**
   a. The DHCP client requests an IP address.
   b. The DHCP server assigns an IP address, subnet mask, gateway address, DNS server address, and a domain name.

After the appliance assigns an IP address to the DHCP client, it sends the DDNS update to the DNS server as follows:

4. **DDNS – Dynamic Update of the Client’s Resource Records**
   c. **GSS-TSIG-Authenticated DDNS Update**
      1. The appliance sends an authenticated DDNS update, which may include the following resource records:
         - A or AAAA – Address record
         - PTR – Pointer record
         - TKEY – Transaction Key record
         - TSIG – TSIG record
      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 16.7* illustrates the initial configuration tasks.

*Figure 16.7  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 503.
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 503.

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 507.
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 508.
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 507). 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
     - *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 (0xbae610f1f552c80b)
```

**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:

   ```
   ktpass -princ username@REALM -mapuser logon_name@REALM -pass password -out my.tab -ptype krb5_nt_principal -crypto encryption
   ```

   For example:

   ```
   ktpass -princ dns@CORP100.LOCAL -mapuser dns@CORP100.LOCAL -pass infoblox -out dns.tab -ptype krb5_nt_principal -crypto all
   ```

   where:

   - `princ` = Kerberos principal
     - `username`: The AD user name for the NIOS appliance. This entry must be the same on the AD domain controller and the Infoblox appliance.
     - `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` = The existing AD user account password.
     - `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. You can specify more than one encryption type or specify `-all` to indicate that all supported encryption types can be used.

You can optionally specify the following:

- `+DesOnly` = Specifies DES encryption for the account. Include this if you did not enable DES encryption for the account.
- `+setpass` = Sets a new AD user account password. This is required if the `+DesOnly` option is specified. When you use this encryption type, you must change the user’s password. Otherwise, the ticket issued for the principal becomes unusable.
  - `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:

```
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 (0xa7cbd0914c86b0a4)
keysize 45 dns@CORP100.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 2 etype 0x3 (DES-
CBC-MD5) keylength 8 (0xa7cbd0914c86b0a4)
keysize 53 dns@CORP100.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 2 etype 0x17 (RC4-
-HMAC) keylength 16 (0xe8fdd9493d114980c6369bfe56bf7fd4c4ba9b36c4bd672b4050
b073ee5023)
keysize 69 dns@CORP100.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 2 etype 0x12 (AES
256-SHA1) keylength 32 (0xe8fdd9493d114980c6369bfe56bf7fd4c4ba9b36c4bd672b4050
b073ee5023)
keysize 53 dns@CORP100.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 2 etype 0x11 (AES
128-SHA1) keylength 16 (0x2c142c8d2bf575e13b43c3703c0d0b58)
```

Note that the messages included the following warning:

```
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 **IPv4 DDNS ->Basic** tab or the **IPv6 DDNS ->Basic** tab of the editor, complete the following:
   
   — **DDNS Updates:** Select the **Enable DDNS Updates** check box.
   
   — **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 **Keytab 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 **Display** to list the external zones to which the Grid member can send secure DDNS updates.

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

Each time you export a keytab file from a Kerberos server running on Windows Server 2003, the version number of the keytab file increases incrementally. Because the version number 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.
Configuring DDNS Updates from DHCP

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.
   - dns_server_fqdn: This is the FQDN of the DNS server. You can use the “dig” command to perform a DNS lookup to obtain the FQDN of the DNS server as it appears on the SOA record.
   - ad_domain: This is the AD domain of the DNS server.
   - Click Test GSS-TSIG to list the Grid members that are allowed to send GSS-TSIG updates to the DNS server.
4. Save the configuration and click Restart if it displays at the top of the screen.

Verifying the Configuration

After you configure the AD domain controller and the Infoblox DHCP server, you can view the syslog of the Infoblox DHCP server to verify if it successfully established a security context with the AD domain controller. The DHCP server displays a series of messages similar to the following:

```
dhcpd: Enabled GSS-TSIG for zone 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.
dhcpd: Acquired 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 16.8, 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 16.8 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 503.
   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 16.8, the principal is ibdhcp/ib.child.corp100.com@CHILD.CORP100.COM. For information, see Generating the Keytab File on page 503.

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 507.
   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 16.8, the DNS principal is DNS/ns1.corp100.com@CORP100.COM. For information, see Creating an External Zone for GSS-TSIG Updates on page 508.
Configuration Example

Following are the steps to configure the example shown in Figure 16.8:

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:

   ```bash
   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. Save the configuration and click Restart if it displays at the top of the screen.
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 DDNS Properties editor, click the Add icon and complete the following fields in the Add External DDNS 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. Save the configuration and click Restart if it displays at the top of the screen.
Sending GSS-TSIG Updates to a DNS Server in Another Forest

The Infoblox DHCP server can also send secure DDNS updates to a DNS server that belongs to a domain in another forest, as long as a forest trust exists. Refer to the Microsoft Active Directory documentation for information on establishing forest trusts.

Similar to the authentication process between domains, the authentication process between forests also uses referrals. The appliance follows the referral chain until it reaches the domain controller of the domain in which the service is located. Note that forest trusts are not transitive. For example, if the DHCP server is in forest A and the DNS server is in forest C, a direct trust must exist between forest A and forest C for the DDNS updates to succeed. Having a trust between forest A and B, and between forest B and C is not sufficient.

In Figure 16.9, 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 16.9 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 510.
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 371. 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 514
- Import the zone data from the domain controller. For information, see *Importing Data into Zones* on page 386.
- 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 495.
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. Save the configuration and click Restart if it displays at the top of the screen.

To configure AD support using the Authoritative Zone editor:

1. From the Data Management tab, select the DNS tab --> Zones tab -->zone check box -->Edit icon.

2. In the Authoritative Zone editor, select the Active Directory tab and do the following:
   - Allow unsigned updates from these Domain Controllers: Select this check box and specify the AD domain controllers from which the appliance can receive DDNS updates.
   - Automatically create underscore zones: Select this check box to automatically create the subzones.

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

You can then import zone data, as described in Importing Data into Zones on page 386.
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 16.10. 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 16.10, see the section following the illustration.

Figure 16.10 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_msdcs.dom_name to the DNS server whose IP address it received through DHCP.

   b. The NIOS appliance replies with the name of the Kerberos server.

4. Kerberos – Login, and TGT and Service Ticket Assignments
   a. The client automatically logs in to the Kerberos server.

   b. The Kerberos server sends the client a TGT (ticket-granting ticket).

   c. Using the TGT, the AD member requests a service ticket for the DNS server.

   d. The Kerberos server replies with a service ticket for that server.

5. DDNS – Dynamic Update of the Client’s Resource Records
   a. Unauthenticated DDNS Update Attempt (Refused)
      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). 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.

      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).

   The two participants have established a security context.

   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 16.11.

Figure 16.11 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.
Configuring DDNS Updates from DHCP

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 518.
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 519.

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 521.
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 371.
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 372.
4. Import the zone data from the AD domain controller. For information, see Importing Zone Data on page 385.
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 521.

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 521). 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.

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 Expert Mode.
3. When the additional tabs appear, click GSS-TSIG and do the following:
   - If a principal name and version number are listed, there is a keytab file loaded on the appliance. Compare this information with that for the NIOS appliance account on the Kerberos server to make sure that they match. If there is no keytab file on the NIOS appliance or if the loaded keytab file does not match that on the Kerberos server, you must load the correct keytab file
     - Click Upload, click Browse to navigate to the keytab file, and then click Upload.
   - Enable GSS-TSIG authentication of clients: Select this check box.
4. Save the configuration and click Restart if it displays at the top of the screen.

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

You can then use the Active Directory wizard or navigate to the Active Directory tab of the Authoritative Zone editor to enable the appliance to create underscore zones for the records hosted by domain controllers and to allow GSS-TSIG signed updates to the underscore zones.

To use the Active Directory wizard:
1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Configure Active Directory.
2. In the Configure Active Directory wizard, complete the following, and then click Next:
   - Select Zone: Click this and select a zone. The name of the zone must match the name in the AD domain controller so the zone transfer from the AD domain controller to the NIOS appliance can succeed.
   - Allow GSS-TSIG-signed (secure) updates from Domain Controllers: Select this option.
Configuring DDNS Updates from DHCP

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
      forestdnzones.zone
      Note that these zones are automatically generated. You cannot edit these zones or import data into them.
   --- Allow GSS-TSIG-signed updates to underscore zones: Select this check box to allow underscore zones to
      accept GSS-TSIG signed updates.

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

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
      _tcp.zone
      _udp.zone
      domaindnzones.zone
      forestdnzones.zone
      Note that these zones are automatically generated and cannot be manually edited.
   --- Allow GSS-TSIG-signed updates to underscore zones: Select this check box to allow underscore zones to
      accept GSS-TSIG signed updates.

3. Save the configuration and click Restart if it displays at the top of the screen.
Chapter 17  DNSSEC

This chapter provides general information about DNSSEC. The topics in this chapter include:

• About DNSSEC on page 524
  — DNSSEC Resource Records on page 525
  — DNSKEY Resource Records on page 525
  — RRSIG Resource Records on page 527
  — NSEC/NSEC3 Resource Records on page 528
  — NSEC3PARAM Resource Records on page 529
  — DS Resource Records on page 530
• Configuring DNSSEC on a Grid on page 531
• Enabling DNSSEC on page 533
• Setting DNSSEC Parameters on page 534
  — About the DNSKEY Algorithm on page 534
  — About Key Rollovers on page 534
  — RRSIG Signatures on page 535
  — Configuring DNSSEC Parameters on page 536
• Signing a Zone on page 537
• Managing Signed Zones on page 539
  — Importing a Keyset on page 539
  — Exporting Trust Anchors on page 540
  — Checking Key-Signing Keys on page 540
  — Rolling Key-Signing Keys on page 540
  — Unsinging a Zone on page 541
  — Deleting and Restoring Signed Zones on page 541
• About HSM Signing on page 542
  — Configuring a SafeNet HSM Device on page 543
  — Adding and Managing a Thales HSM Group on page 544
  — Synchronizing the HSM Group on page 547
  — Monitoring the HSM Group on page 546
  — Enabling HSM Signing on page 546
• Configuring Grid Members to Support DNSSEC as Secondary Servers on page 548
• Enabling Recursion and Validation for Signed Zones on page 549
  — Enabling Recursion and Validation for Signed Zones on page 549
  — Enabling DNSSEC Validation on page 550
About DNSSEC

DNSSEC (DNS Security Extensions) provides mechanisms for authenticating the source of DNS data and ensuring its integrity. It protects DNS data from certain attacks, such as man-in-the-middle attacks and cache poisoning. A man-in-the-middle attack occurs when an attacker intercepts responses to queries and inserts false records. Cache poisoning can occur when a client accepts maliciously created data. DNSSEC helps you avoid such attacks on your networks.

DNSSEC provides changes to the DNS protocol and additional resource records (RRs) as described in the following RFCs:

- RFC 4033, DNS Security Introduction and Requirements
- RFC 4034, Resource Records for the DNS Security Extensions
- RFC 4035, DNSSEC Protocol Modifications
- RFC 4641, DNSSEC Operational Practices
- RFC 4956, DNS Security (DNSSEC) Opt-In
- RFC 4986, Requirements Related to DNS Security (DNSSEC) Trust Anchor Rollover
- RFC 5155, DNS Security (DNSSEC) Hashed Authenticated Denial of Existence
- RFC 5702, Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC

DNSSEC uses public key cryptography to authenticate the source of DNS responses and to ensure that DNS responses were not modified during transit. Public key cryptography uses an asymmetric key algorithm. With asymmetric keys, one key is used to encrypt data that was encrypted using the other key.

In DNSSEC, the primary name server of a zone generates at least one public/private key pair. It “signs” each data set in the zone by running it through a one-way hash, and then encrypting the hash value with the private key. The public key is stored in an RR type introduced by DNSSEC, the DNSKEY RR. Resolvers use the DNSKEY record to decrypt the hash value. If the hash values match, then the resolver is assured of the authenticity of the message.

In addition to the DNSKEY record, DNSSEC also introduces new RRs which DNS servers can use to authenticate the non-existence of servers, zones, or resource records. For information about the DNSSEC RRs, see DNSSEC Resource Records on page 525.

DNSSEC uses the EDNS0 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 EDNS0 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 525.
- Resource Record Signature (RRSIG) records—For information, see RRSIG Resource Records on page 527.
- Next Secure (NSEC/ NSEC3) records—For information, see NSEC/NSEC3 Resource Records on page 528.
- NSEC3PARAM records—For information, see NSEC3PARAM Resource Records on page 529.
- Delegation Signer (DS) resource records—For information, see DS Resource Records on page 530.

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 530.)

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 1296000 IN DNSKEY 257 3 5 20181231235959hiZsq1gPtqIKKeVuGBbAchPSdg4vSymSxSbgzueQM4jrrjCBsQbN7VHG95kdfcAPxhXZBwqQmGEO77xdaOeTpwqaq0vpg16EOV0ZLwWh1Imsw17XheojIarzM8nTfIPJ+4av1KrqBlIPy369J3j(ChyL8sMT0EfwS0tEAWd7Isvt2vW24cE=)
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 hiZsq1gPtqIKevuGBbAchPSdg4vSymSxSbgzueQW4jrcjCBsQbH7VH95kdfcAPxhxZBwvQmgE07dxaOeTwpqaq0vpl6EU0zLwWhIImw17XhGjIarzM8ntflFJ+44v1KrqBlIPy3693jiChyL8sMT0EfwS0tEAwD7isvt2vW24cE=)
```

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:

```
corp100.com 86400 IN NSEC a1.corp100.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:

```
u1e6lovi99jviertevoe080ta34ocu39 900 IN NSEC3 1 0 100 74ae486f6ecbbd29010047ad UL3BVITG5OAORMRFUPQV6A2197FIB 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 17.1, 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 17.1

Following is an example of the DS RR:

corp100.com 86400 IN DS 25924 5 1 49D2801B50E25DS9440F1FF1A8012B568435

The first four fields specify the owner name, TTL, class and RR type. The succeeding fields are as follows:

- Key Tag: The key tag value that is used to determine which key to use to verify signatures.
- Algorithm: Identifies the algorithm of the DNSKEY RR to which this DS RR refers. It uses the same algorithm values and types as the corresponding DNSKEY RR.
- Digest Type: Identifies the algorithm used to construct the digest. The supported algorithms are:
  - 1 = SHA-1
  - 2 = SHA-256
- Digest: If SHA-1 is the digest type, this field contains a 20 octet digest. If SHA-256 is the digest type, this field contains a 32 octet digest.
Configuring DNSSEC on a Grid

You can configure the name servers in a Grid to support DNSSEC. You can configure the Grid Master as the primary server for a signed zone and the Grid members as secondary servers. (For more information, see Configuring Grid Members to Support DNSSEC as Secondary Servers on page 548.) Note that only the Grid Master can serve as the primary server for a signed zone.

You can enable the Grid Master to sign zones and manage the DNSSEC keys, or you can configure the Grid Master as a client to a third-party, network-attached Hardware Security Module (HSM) that performs the key generation, zone signing, and key safekeeping. You must use either the Grid Master or HSM for zone signing and key management; you cannot use both. Note that each method may have different performance implications, depending on the hardware platform, number of zones and other factors. For information about using HSMs, see About HSM Signing on page 542.

Any authoritative forward-mapping or reverse-mapping zone can be signed according to the following criteria:

- The zone does not contain any bulk host records.
- DNSSEC is enabled on the Grid Master.
- The primary server of the zone must be a Grid member. If the zone is assigned to an NS group, the primary server in the group must be a Grid member that has DNSSEC enabled.

Note that you can use DNS views to separate internal and external zone data, to manage your zones more efficiently and reduce the size of the zones that require signing. For information about DNS views, see Using Infoblox DNS Views on page 356.

Grid Master as Primary Server

When you sign a zone whose primary server is a Grid member, that member becomes a secondary server and the Grid Master becomes the hidden primary server. If the zone is assigned to an NS group, the Grid Master removes the association with the NS group. The previous primary server becomes a secondary server for the zone.

If a master candidate is promoted to Grid Master and the previous Grid Master was the primary server for signed zones, the new Grid Master becomes the hidden primary server for all signed zones. The previous Grid Master, which was the primary server for the zone, becomes a secondary server for the zone.

As the primary server, the Grid Master sends zone data to the secondary servers through zone transfers; or, if the secondary servers are Grid members, the Grid Master transfers data to all Grid members through the database replication process, by default. The Grid Master transfers all records in that zone, including all NSEC/ NSEC3, RRSIG, DNSKEY and DS records with owner names that belong to that zone. The RRSIG RRs are included in zone transfers of the zone in which they are authoritative data. The Grid Master also performs incremental zone transfers to secondary servers as a result of incremental zone signings.

In addition, the Grid Master automatically performs an incremental signing of the zone data sets when their contents change. Incremental signing refers to signing just those parts of a zone that change when RRs are added, modified, or deleted. The Grid Master uses the private key of the ZSK when it incrementally signs a zone. In addition, the Grid Master adds, modifies or deletes the corresponding RRSIG records and the appropriate NSEC/ NSEC3 records.
For example, Figure 17.2 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.

Figure 17.2

1. A DNS client sends a query for data in the corp100.com zone.
2. ns1.corp200.com sends a query to ns2.corp100.com. It sets the EDNS DO bit in the query to indicate that it is requesting DNSSEC data.
3. ns2.corp100.com responds with the requested data and the appropriate DNSSEC RRs.
4. ns1.corp200.com uses the DNSKEY RR of corp100.com to validate the response. It then sends the response to the DNS client, with the AD bit set, indicating that it validated the response.

Following are the tasks to configure the Grid Master to sign zones:

1. Create the zones. For information, see Configuring Authoritative Zones on page 370.
   — 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 534.
4. Sign the zone. The appliance automatically generates the DNSSEC RRs when you sign a zone. For information, see Signing a Zone on page 537.
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 534.

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 548.

To enable DNSSEC on a Grid, member or DNS view:

1. **Grid**: From the Data Management tab, select the DNS tab. Expand the Toolbar and click Grid DNS Properties.
   
   **Member**: From the Data Management tab, select the Members tab -> `member` check box and click the Edit icon.
   
   **DNS View**: From the Data Management tab, select the Zones tab -> `dns_view` check box and click the Edit icon.

2. In the editor, click **Toggle Expert Mode**.

3. When the additional tabs appear, click **DNSSEC**.

4. In the **DNSSEC** tab, select **Enable DNSSEC**.

5. Save the configuration and click **Restart** if it appears at the top of the screen.
Setting DNSSEC Parameters

The Grid Master uses certain default parameters when it signs a zone and generates the DNSSEC RRs. You can change these defaults for the entire Grid and for individual zones, in case you want to use different parameters for certain zones. The following sections describe the different parameters that you can set:

- About the DNSKEY Algorithm
- About Key Rollovers
- RRSIG Signatures on page 535

For information on setting these parameters, see Configuring DNSSEC Parameters on page 536

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.

You can select the DNSKey algorithm for HSMs. Thales HSMs don’t support DSA. All other parameters are not used by HSMs.

About Key Rollovers

To reduce the probability of their being compromised, ZSKs and KSKs must be periodically changed. The time within which a key pair is effective is its rollover period. The rollover period starts as soon as a zone is signed. After a rollover period starts, you cannot interrupt or restart it unless you unsign the zone.

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 540.

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 540.

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 527, 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 Expert 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 or HSM uses when it generates the KSK. Note that Thales HSMs do not support DSA. 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 or HSM uses when it generates the ZSK. Note that HSMs do not support DSA. 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 1024 bits.
     - **DSA/NSEC3**: The minimum is 512 bits and maximum is 1024 bits. The default is 1024 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 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.
   - **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. Save the configuration and click **Restart** if it displays at the top of the screen.
Signing a Zone

When it signs a zone, the Grid Master generates new DNSKEY key pairs. As shown in Figure 17.3, 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 17.3 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 534.) 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 17.4**.

**Figure 17.4**

![Records](image-url)
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 539.
- 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 540.
- You must change the KSK periodically, to ensure its security. For information, see Checking Key-Signing Keys on page 540 and Rolling Key-Signing Keys on page 540.
- 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 541.
  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 541.

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 495.

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.
About HSM Signing

You can integrate a Grid with third-party, network-attached Hardware Security Modules (HSMs) for secure private key storage and generation, and zone-signing off-loading. Infoblox appliances support integration with either SafeNet HSMs or Thales HSMs. When using a network-attached HSM, you can provide tight physical access control, allowing only selected security personnel to physically access the HSM that stores the DNSSEC keys. When you enable this feature, the HSM performs DNSSEC zone signing, key generation, and key safe keeping.

Note that if you migrate from using the Grid Master to HSMs, HSM signing starts at the next key rollover.

Only a superuser can configure this feature. To configure HSM signing in a Grid, do the following:

1. Create the HSM group and add HSMs to the group. You can create either a SafeNet HSM group or a Thales HSM group. You can use only one group at a time. After you add the HSM group, the Add icon and Add button in the Toolbar are greyed out.
   - For information on adding an SafeNet HSM group, see Configuring a SafeNet HSM Device on page 543.
   - For information on adding a Thales HSM group, see Adding and Managing a Thales HSM Group on page 544.

   Note that if you delete an HSM or an HSM group, it is permanently deleted. It is not stored in the Recycle Bin.

2. Enable HSM signing. For information, see Enabling HSM Signing on page 546.

After you enable this feature, you can monitor the HSM group, as described in Monitoring the HSM Group on page 546. In addition, the Grid sends SNMP traps when zone signing succeeds or fails. For information about these traps, see Processing and Software Failure Traps on page 920.

Note that NIOS does not provide key life cycle management functions; these are handled by the HSM and must be configured via the HSM’s administrative interface to adhere to corporate policies on key management. The keys (ZSK and KSK) used for DNSSEC are stored securely on the HSM and are not deleted by NIOS when the key is no longer required by the DNSSEC function. However, references to the keys are removed from the appliance.
Configuring a SafeNet HSM Device

You can integrate a Grid with a SafeNet HSM group. The SafeNet HSM group can contain either SafeNet Luna SA 4 or SafeNet Luna SA 5 devices in standalone or HA mode; the group cannot contain a mix of both models. You must first configure each HSM device, as described in Configuring a SafeNet HSM Device; and then create the group and add the devices to the group, as described in Adding a SafeNet HSM Group.

Configuring a SafeNet HSM Device

Do the following for each SafeNet HSM device that you are adding to the group:

1. On the Grid, generate a client certificate for the Grid Master and Grid Master candidate. For information, see About Client Certificates on page 47.
2. On the SafeNet HSM, do the following:
   — Assign the Grid Master and Grid Master candidate to a partition on the HSM to avoid any service interruptions, in case the Grid Master candidate is promoted to Grid Master.
   — Upload the certificates of the Grid Master and Grid Master candidate to the HSM and register the certificates in the HSM’s list of clients. The certificates of the Grid Master and Grid Master candidate are linked to their IP addresses. Therefore, if any of their IP addresses change, you must generate a new client certificate and register it with the HSM.
   — Download the HSM certificate.
   For additional information, refer to your SafeNet HSM documentation.

Adding a SafeNet HSM Group

When you configure a SafeNet HSM group, add the SafeNet HSM devices to the group and upload their certificates to the Grid. You can add only one HSM group. To add a SafeNet HSM Group:

1. From the Grid tab, select the HSM Group tab.
2. Click the Add drop-down list and select HSM SafeNet Group.
3. In the Add HSM SafeNet Group wizard, complete the following and click Next:
   — Name: Enter a name for the HSM group.
   — Partition Password: Enter the partition password, and re-enter it in the Confirm Partition Password field.
   — Version: Select the SafeNet HSM version, which is either LUNA SA 4 or LUNA SA 5.
   — Comment: You can enter additional information about the HSM.
4. Click the Add icon to add a SafeNet HSM device, and complete the following:
   — Name or IP Address: Enter the hostname or IP address of the HSM device.
   — Partition SN: Enter the partition serial number (PSN) of the HSM. The Partition ID field automatically displays the ID after the configuration is saved and the appliance has successfully connected to the device.
   — Disabled: Select this check box to disable use of this HSM.
   — Server Certificate: Upload the certificate of the SafeNet HSM.
5. Save the configuration.

After you add the HSM group, the Add icon and Add button in the Toolbar are greyed out. Note that if the HSM is configured in FIPS 140-2 compliant mode, certain key algorithms and key sizes are disallowed. Requests for those key algorithms or key sizes result in an error. The following algorithms are FIPS 140-2 compliant: DSA, DSA/NSC3, RSA/SHA1, RSA/SHA1/NSC3, RSA/SHA-256, and RSA/SHA-512. For additional information about selecting key algorithms, see About the DNSKEY Algorithm on page 534.

You can verify whether the Grid Master candidate is properly registered with the HSM by navigating to the Grid -> Grid Manager -> Members page. Its Status icon is yellow if it is not registered with the HSM.

If DNS service is enabled, you can also verify whether the Grid Master was able to contact the SafeNet HSMs by navigating to the Data Management > DNS > Members page. If the Grid Master status is yellow, check the status of the HSMs in the Grid -> HSM Group page. (For more information, see Monitoring the HSM Group on page 546.) If the status is not green, check the configuration of the HSMs and restart the DNS service.

Adding and Managing a Thales HSM Group

On the Thales HSM, configure the Grid Master and Grid Master candidate as HSM clients. Enroll the IP addresses of both the Grid Master and Grid Master candidate to avoid any service interruptions, in case the Grid Master candidate is promoted to Grid Master. If the Grid Master and Grid Master candidates are HA pairs, you must enroll their VIPs. In addition, you must also set up client cooperation to allow both the Grid Master and Grid Master candidate access to the Remote File Server (RFS). Note that anytime you add a new Grid Master candidate, you must enroll its IP address and set up a client cooperation to allow it access to the RFS. For more information on these procedures, refer to your HSM documentation.

Note that DSA cannot be used as the DNSSEC cryptographic algorithm for Thales HSMs. Therefore, migrating to Thales HSMs is not allowed if the Grid Master uses DSA as the DNSSEC cryptographic algorithm.

You can create one Thales HSM group in the Grid, and then add HSMs to the group. The appliance tries to connect to each of the HSMs in the order that they are listed.

To add a Thales HSM group:

1. From the Grid tab, select the HSM Group tab and click the Add icon.
2. In the Add HSM Group wizard complete the following, and then click Next:
   - Name: Enter a name for the HSM group.
   - Protection: Select the level of protection that the HSM group uses for the DNSSEC key data.
     - Module: Select this if the HSM group uses a module-protected key. You do not have to enter a password phrase for this type of key.
     - Softcard: Select this if the HSM group uses a softcard-protected key. You must then specify the card name and password.
   - Card Name: Enter a name for the softcard.
   - Password Phrase: Enter the password and re-enter it in the Confirm Password Phrase field.
   - RFS IP Address: Enter the remote file server (RFS) IP address. Note that you must ensure that you enter a valid RFS IP address for the Security World. Validation is limited to IP address checking. Infoblox recommends that you use Test HSM Group to check the HSM group configuration before proceeding.
   - RFS Port: Specify the port of the RFS.
   - Comment: Optionally, enter additional information about the group.
3. To add modules to the group, click the Add icon and complete the following:
   - Remote IP: Enter the IP address of the HSM.
   - Remote Port: Specify the destination port on the HSM. The firewall must be configured to allow connection to this port.
   - Disabled: Select this check box to disable use of this HSM.
— **Keyhash**: Enter the keyhash, which is displayed on the console of the HSM. It can be obtained through an out of band mechanism from the HSM administrator. Note that the appliance validates the keyhash. If the entry is correct, the appliance displays the Electronic Serial Number (ESN) of the HSM when the editor is next launched. If the keyhash is incorrect, the appliance does not connect to the HSM.

— **ESN**: This is a read-only field that displays the ESN of the HSM after you save the configuration and relaunch the editor. Infoblox strongly recommends that you verify the ESN displayed by the appliance with the one obtained from the HSM administrator to ensure that the appliance is communicating with the correct HSM.

4. Save the configuration.
Monitoring the HSM Group

You can monitor the status of the HSM group and of individual modules in the group by navigating to the Grid tab > HSM Group panel. To view the status of each HSM, click the arrow beside the group name. This panel displays the following information:

- **Name**: The name of the HSM group or module.
- **Status**: The HSM group status displays the status for all the HSMs in the group. The status icon can be one of the following:
  - **Green**: All the HSMs in the group are functioning properly.
  - **Yellow**: At least one HSM in the group is not functioning properly.
  - **Red**: All the HSMs in the group are not functioning properly.
  - **Black**: The status of the HSM devices is unknown.
- **FIPS**: This applies to a SafeNet HSM only. It indicates if the HSM is in FIPS compliant mode.
- **Comment**: Any comments that were entered about the HSM group.

You can also do the following in this tab:

- Sort the data in ascending or descending order by column.
- Print and export the data in this tab.

Enabling HSM Signing

When you enable HSM signing, the HSM starts generating the DNSSEC keys at the next key rollover. For information about key rollovers, see About Key Rollovers on page 534. You can enable this feature at the Grid level only.

To enable HSM signing:

1. From the Data Management tab -> DNS tab, expand the Toolbar and click Grid DNS Properties.
2. In the Grid DNS Properties editor, Click **Toggle Expert Mode**, if the editor is in Basic mode, and then select the DNSSEC tab.
3. In the DNSSEC tab, select the **Enable DNSSEC** check box, if it is not selected, and then select the **HSM Signing** check box.
4. Complete the other fields described in Configuring DNSSEC Parameters on page 536. Note that Thales HSMs do not support DSA.
5. Save the configuration.
About HSM Signing

Testing the HSM Group

After you configure the HSM group, you can test the HSM signing functionality of the group. Click Test HSM Group in the Toolbar, and then click Yes when the confirmation dialog displays. The appliance then executes the command to perform a signing test. The feedback panel displays the status of the test in the Grid Manager feedback panel.

Synchronizing the HSM Group

You can click Resync HSM Group in the Toolbar to do any of the following:

- For a Thales HSM group, if the RFS security settings change use this function to have the appliance perform an RFS synchronization.
- For a SafeNet HSM group, use this function to synchronize the keys of the HSM members in the group.
Configuring Grid Members to Support DNSSEC as Secondary Servers

Any Infoblox Grid member can function as a secondary server for DNSSEC signed zones. It can receive transfers of signed zones from the Grid Master or an external primary server, and from other secondary servers. It can also respond to queries for DNS data in DNSSEC signed zones for which it is a secondary server.

Configuring a Secondary Server for Signed Zones

The following are the tasks to configure an appliance as a secondary server for signed zones:

1. Enable DNSSEC on the appliance. For information, see Enabling DNSSEC on page 533.

2. Configure the appliance as a secondary server for the zone. For information, see Specifying a Secondary Server on page 380.

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 463. 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 17.5, 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 17.5

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 533.
2. Enable validation and configure the trust anchor of each signed zone. For information, see Enabling DNSSEC Validation on page 550. You must configure at least one trusted DNSKEY RR.
3. Enable recursion on the appliance. For information, see Enabling Recursive Queries on page 451.
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 393 and Creating a Root Zone on page 374.
   - Configure global forwarders and custom root name servers, if needed. For information, see Using Forwarders on page 449 and About Root Name Servers on page 465.
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 Expert 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. Save the configuration and click **Restart** if it displays at the top of the screen.
You can configure multiple IP addresses and enable anycast addressing on the loopback interface of the NIOS appliance, allowing the appliance to function in different network deployments. Configuring non-anycast IP addresses on the loopback interface assists in server migration and network address change. Configuring anycast addresses on the appliance allows you to add redundancy and improve reliability for DNS services. You can use OSPF (Open Shortest Path First), BGP (Border Gateway Protocol), or both, as the routing protocol for anycast advertising.

This chapter contains the following sections:

- **Using the Loopback Interface** on page 552
- **Configuring IP Addresses on the Loopback Interface** on page 553
  - **Advertising Loopback Addresses to the Network** on page 554
- **About Anycast Addressing for DNS** on page 555
  - **Configuring Anycast Addresses** on page 556
- **IP Routing Options** on page 557
  - **About OSPF** on page 558
  - **Configuring OSPF** on page 559
  - **About BGP** on page 561
  - **Configuring BGP** on page 563
Using the Loopback Interface

The loopback interface is a virtual network interface on the appliance. You can do the following on the loopback interface:

- Configure IP addresses to consolidate DNS servers for migration purposes. For information, see Configuring IP Addresses on the Loopback Interface on page 553.
- Add anycast addresses to improve the reliability and performance of DNS services in multiple locations. For information, see About Anycast Addressing for DNS on page 555.
- Separate DNS traffic by assigning an IP address as the source port for DNS queries. For information, see Specifying Source Ports on page 447.

When you use the loopback interface for anycast addressing, the upstream and neighboring routers can continue to advertise anycast addresses without being affected by hardware malfunctions.

To configure non-anycast addresses on the loopback interface, complete the following:
1. Add IP addresses to the loopback interface. For information, see Configuring IP Addresses on the Loopback Interface on page 553.
2. Enable DNS services on the loopback addresses. For information, see Specifying Port Settings for DNS on page 446.

To configure DNS anycast addresses and their advertising protocols, complete the following:
1. Add anycast addresses to the loopback interface. For information, see Configuring Anycast Addresses on page 556.
2. Configure anycast addressing protocols. For information, see Configuring OSPF on page 559 and Configuring BGP on page 563.
3. Enable the DNS anycast addresses. For information, see Specifying Port Settings for DNS on page 446.

To separate DNS queries from DNS transfers and notify messages, complete the following:
1. Add an IP address of the source port for DNS queries. For information, see Configuring IP Addresses on the Loopback Interface on page 553.
2. Select the source IP for DNS queries. For information, see Specifying Source Ports on page 447.
Configuring IP Addresses on the Loopback Interface

You can configure IP addresses on the loopback interface to minimize service downtime during a server migration. As illustrated in Figure 18.1, you have two existing DNS servers (ns1.corp100.com 192.204.18.11 and ns2.corp100.com 192.204.18.12) and you want to replace these servers with a new one (ns3.corp100.com 192.204.18.88). The migration takes a few weeks and you want DNS services to be available on all three addresses during the migration. You can add all three IP addresses to the loopback interface of a NIOS appliance, and then configure the appliance to provide DNS services on all addresses. After the server migration, you can shut down the old servers and use the new one for services.

Figure 18.1 DNS Server Migration Using the Loopback Interface

You can also add an IP address that is used solely for DNS queries, to separate the DNS traffic. You first add an IP address you want to use for DNS queries on the loopback interface. You then configure the appliance to listen for DNS queries solely on this address. For information, see Specifying Source Ports on page 447.

When you configure non-anycast addresses on the loopback interface, ensure that you establish a static route between the appliance and the router so queries to these addresses are routed correctly. For information, see Advertising Loopback Addresses to the Network on page 554.

To configure an IP address on the loopback interface:

1. From the Grid tab, select the Grid Manager tab -> Grid_member check box -> Edit icon.
2. In the Grid Member Properties editor, select the Network tab -> Basic tab.
3. In the Additional Ports and Addresses table, click the Add menu and select Additional Address (loopback). The appliance adds a row to the table. Complete the following:
   - Interface: Displays Additional Address (loopback). You cannot modify this.
   - Address: Enter the IP address you want to add to the loopback interface.
### Configuring IP Routing Options

- **Subnet Mask**: You cannot change the netmask of the loopback interface. It is set to 255.255.255.255, or /32.

**Note**: You cannot configure the gateway address and port settings.

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

To add multiple IP addresses on the loopback interface, repeat the steps for each IP address.

**Note**: If you are configuring the loopback interface on a Grid Master, the Grid is temporarily disrupted upon saving the configuration and restarting services on the appliance. The Grid reconnects automatically and the appliance regains the role as Grid Master after a short delay.

### Advertising Loopback Addresses to the Network

Advertising IP addresses on the loopback interface relies on the upstream router to populate routes to the loopback interface. As illustrated in **Figure 18.2**, when a client on a different subnet queries an IP address on the loopback interface, it sends the request to the router. If the IP address on the loopback interface is not advertised to the router, the request cannot reach the appliance. Therefore, when you configure non-anycast addresses on the loopback interface, or if OSPF or BGP is not configured within your network, you must configure the upstream router to reach the NIOS appliance through a static route. Consult with your network administrator for information about configuring static routes from the router to the additional IP addresses on the loopback interface.

**Figure 18.2 Static Route for Loopback IP Addresses**

When you configure DNS anycast addresses on the loopback interface, you can select OSPF, BGP, or both, to advertise the addresses to upstream and neighboring routers, without establishing a static route. For information, see **About Anycast Addressing for DNS** on page 555.
About Anycast Addressing for DNS

Note: This feature is not supported on vNIOS appliances for Riverbed.

There are four types of communication utilized within a network:

- **Unicast** describes a one-to-one network communication between a single sender and a single recipient. The routing protocol determines the path through the network from the sender to the recipient based on the specific protocol or routing scheme. Unicast also describes the address type assigned to the recipient, 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.

The NIOS appliance provides the following support for DNS anycast addressing:

- You can configure up to 10 anycast IP addresses on the loopback interface of each Grid member.

- The appliance advertises routing information of the anycast addresses through OSPF, BGP, or both, depending on your configuration. Network routers use the configured routing protocols to determine the best path to the nearest server. The appliance advertises the route information to the upstream or neighboring router, a router that forwards data on the network link and determines the forwarding path to destinations. For information, see **IP Routing Options** on page 557.

- The appliance advertises and withdraws route information based on reachability information to DNS servers sent by the IP route advertisements.

Anycast addressing 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 router forwards the request to the next nearest server that is advertising the target address.

- **Load Distribution**: Anycast distributes the load across multiple DNS servers based on network topology.

- **Improved Performance**: The NIOS appliance uses OSPF and BGP, depending on your configuration, to advertise anycast routing information to the upstream and neighboring routers. The routers determine the best route to the nearest DNS server. Anycast enables the queries to reach the nearest server faster, as well as providing faster responses to DNS queries.

For more information about anycast addressing, refer to RFC 1546 “Host Anycasting Service”.

For more information about anycast addressing, refer to RFC 1546 “Host Anycasting Service”.
Configuring Anycast Addresses

Note: Anycast addressing is supported on the loopback interface only.

To enable and configure anycast addressing:
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 and complete the following in the Anycast Interfaces table:
   — Anycast Interface: Anycast addressing is supported on the loopback interface only.
   — Address: Enter the IP address you want to assign as the anycast address. Specify a 32-bit IPv4 address.
   — Subnet Mask: You cannot change the subnet mask of a loopback interface. The netmask is set to 255.255.255.255, or /32.
   — Gateway: You cannot modify the gateway address of the anycast address.
   — OSPF: Select this if you want the appliance to use OSPF to advertise the anycast address, and then configure the OSPF settings. For information, see Configuring OSPF on page 559.
   — BGP: Select this if you want the appliance to use BGP to advertise the anycast address, and then configure the BGP settings. For information, see Configuring BGP on page 563.
   — Comments: Enter a text string to help identify this interface and IP address.
4. Save the configuration and click Restart if it displays at the top of the screen.

The appliance displays the anycast address in the Additional Ports and Addresses table in the Network tab -> Basic tab of the Grid Member Properties editor. After you configure the anycast addresses, you must add them to the Listen on these additional IP addresses table in the Network tab -> General tab -> Advanced tab of the Grid Member Properties editor, so the appliance can provide DNS services on these addresses. For information, see Specifying Source Ports on page 447.
IP Routing Options

IP routing is a set of protocols that determine the path IP packets follow in order to travel across multiple networks from the source to the destination. When information travels through a series of routers and across multiple networks, IP routing protocols enable the routers to build up a forwarding table that correlates the final destination with the next upstream routers.

For the purpose of routing, the internet is divided into ASs (Autonomous Systems). An AS is a group of routers or IP routing prefixes managed by a single administration. Routers within an AS can exchange network routing information and share a clearly defined routing policy.

There are three types of ASs:

- **Stub AS** has a single connection to another AS. Any data sent to a destination or received from a source outside the AS must travel over this connection. For example, a small college network is a stub AS.
- **Transit AS** has multiple connections to one or more ASs. These connections allow the routing of data that is not designed for a node within the AS. For example, an ISP (internet service provider) network is a transit AS.
- **Multihomed AS** has multiple connections to one or more ASs, but it does not allow data received over one of these connections to be forwarded outside of the AS. In other words, it does not provide a transit service for other ASs. For example, a large enterprise network is multihomed AS.

In general, data can be routed within an AS using IGP (Interior Gateway Protocol) and routed across different ASs using EGP (Exterior Gateway Protocol). The NIOS appliance supports OSPF as the IGP and BGP as the EGP to advertise DNS anycast addresses. As illustrated in Figure 18.3, using OSPF and BGP, NIOS appliances can advertise DNS anycast addresses within specific ASs and across different ASs.

You can configure OSPF, BGP, or both to advertise anycast addresses configured on the loopback interface of an appliance. For information, see Configuring OSPF on page 559 and Configuring BGP on page 563.

Figure 18.3 OSPF and BGP Routing
About OSPF

OSPF is a link-state protocol based on the Dijkstra algorithm used to calculate the shortest path to a destination address within an internetwork. This protocol uses a link-state database created using routing information advertised from neighbors and peers, each with costs based on the state of that link to the destination.

OSPF network topologies consist of administrative domains called OSPF areas. An area is a logical collection of OSPF routers, servers and other network devices that have the same area identifier. A router within an area keeps an OSPF database for its OSPF area only, reducing the size of the database that is maintained.

The NIOS appliance uses the OSPF routing protocol to advertise routes for DNS anycast addresses to the upstream router. The upstream router uses the OSPF advertisement to determine the nearest server from a group of servers within the internetwork. The upstream router then forwards the query to the chosen DNS server. In practicality, the NIOS appliance relies upon OSPF to determine the best route for DNS queries to take to the nearest DNS server.

As illustrated in Figure 18.4, to enable anycast for DNS queries, you configure two or more DNS servers with the same anycast address on their loopback interfaces. When you select OSPF as the routing protocol, the upstream router determines the nearest server within the group of servers that are configured with the same anycast address. The nearest DNS server then 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 18.4 Anycast Addressing for DNS Using OSPF

OSPF determines the nearest server within an internetwork. In this example, the nearest DNS server is the Europe server, since the client is located in Europe.

DNS Query 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.

DNS anycast in this example: The desktop then connects to 10.128.1.12. 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.

You can use the CLI command show ospf to display configuration and statistical information about the OSPF protocol running on the appliance. You can also use the set ospf command to write OSPF statistical information to the syslog. After you configure the settings, you must restart the DNS services for the settings to take effect. For information, refer to the Infoblox CLI Guide. Note that when you enter any OSPF command and wait for the interface to return more information, the appliance disconnects your CLI session if you restart services or make other OSPF configuration changes through Grid Manager. You must re-enter your credentials to log back in to the CLI.
To enable the appliance to support OSPF and advertising anycast addresses, you must configure the LAN or 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.

You can also configure authentication for OSPF advertisements to ensure that the routing information received from a neighbor is authentic and the reachability information is accurate. For information, see Configuring OSPF. For more information about the OSPF routing protocol, refer to RFC 2328 “OSPFv2”.

## Configuring OSPF

You can configure the LAN or HA interface on the NIOS appliance as an OSPF advertising interface. The interface advertises the OSPF routing information to the network so that routers can determine the best server to query. On 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.

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, and then click the **Edit** icon.
2. Select the **Anycast** tab in 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:
   - **Advertising Interface**: Displays the interface that sends out OSPF routing advertisements. OSPF advertisements are supported on the LAN or HA interface only, depending on whether the appliance is an HA pair.
   - **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.
Configuring IP Routing Options

— **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. Save the configuration and click **Restart** if it displays at the top of the screen.
**About BGP**

BGP is designed to distribute routing information among ASs and exchange routing and reachability information with other BGP systems using a destination-based forwarding paradigm. Unlike OSPF, which calculates routes within a single AS, BGP is a vector routing protocol that distributes routing information among different ASs. A unique ASN (autonomous system number) is allocated to each AS to identify the individual network in BGP routing. A BGP session between two BGP peers is an eBGP (external BGP) session if the BGP peers are in different ASs. A BGP session between two BGP peers is an iBGP (internal BGP) session if the BGP peers are in the same AS.

BGP configuration enables large enterprises that use BGP as the routing protocol to provide high resilient DNS services using the Infoblox solution. While BGP is mostly used by ISPs, it is also used in some of the larger enterprise environments that must interconnect networks that span geographical and administrative boundaries. In these environments, it is required to use BGP to advertise anycast routes. Using BGP allows the appliance to advertise DNS anycast addresses to neighboring routers across multiple ASs that also use BGP as their routing protocols.

As illustrated in *Figure 18.5*, to enable anycast for DNS queries among three different networks that span different geographical regions, you can configure two DNS servers with the same DNS anycast addresses in the AS 65497 network. Since other network routers in AS 65498 and AS 65499 also use BGP as the routing protocol, the DNS anycast addresses can be advertised across these networks.

*Figure 18.5  Anycast Addressing for DNS using BGP*

![Diagram showing BGP configuration and anycast addressing for DNS services](image-url)

To enable DNS anycast addressing across different ASs, you must configure BGP as the routing protocol on the NIOS appliance. As illustrated in *Figure 18.6*, the AS 65497 network contains the Infoblox DNS anycast servers, and the AS 65499 network contains Router 1 and 2. The routers use BGP as their routing protocol and are peered with the DNS servers. You can configure anycast addressing on the loopback interface of the DNS servers and select BGP as the protocol to advertise the anycast addresses to Router 1 and 2 in AS 65499. For information, see *Configuring Anycast Addresses* on page 556. Once you have configured the DNS servers, the appliances automatically add filters on the advertising interfaces to limit the advertisements to the configured anycast IP addresses. Similarly, BGP filters are applied to ensure that the DNS servers only receive default route advertisements from the neighboring routers.
BGP uses timers to determine how often the appliance sends keepalive and update messages, and when to declare a neighboring router out of service. You can configure the time intervals for these timers. For information, see Configuring BGP on page 563.

The BGP protocol service is configured to send SNMP queries about BGP runtime data. The appliance sends SNMP traps to its neighboring routers when it encounters issues with the protocol. BGP is configured to send SNMP traps as defined in RFC4273 Definitions of Managed Objects for BGP-4. You must enable and configure the SNMP trap receiver on the Grid member for the member to send SNMP traps. For information, see SNMP MIB Hierarchy on page 901.

You can use the CLI command show bgp to diagnose problems about the BGP configuration. You can also use the set bgp command to set the verbosity levels of the BGP routing service. The appliance writes BGP statistical information to the syslog. After you configure the settings, you must restart the DNS services for the settings to take effect. For information, refer to the Infoblox CLI Guide. Note that when you enter any BGP command and wait for the interface to return more information, the appliance disconnects your CLI session if you restart services or make other BGP configuration changes through Grid Manager. You must re-enter your credentials to log back in to the CLI.

To enable the appliance to support BGP and advertising anycast addresses across multiple ASs, you must configure the LAN or HA interface as the BGP advertising interface.

**Note:** If the 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.

The appliance supports BGP version 4. For more information about BGP, refer to RFC4271, A Border Gateway Protocol 4 (BGP-4).
Configuring BGP

You can configure the LAN or HA interface on the appliance as a BGP advertising interface for anycast addresses. The interface advertises the BGP routing information to the network so routers can determine the nearest server to query. You must define the ASN of the interface and add neighboring routers that receives the BGP announcements. On an HA pair, BGP runs only on the active node. In an HA failover, the BGP service resumes on the new active node.

To configure the LAN (HA) interface to be the BGP advertising interface:

1. From the Grid tab, select the Grid Manager tab ->Grid_member check box, and then click the Edit icon.
2. In the Grid Member Properties editor, select the Anycast tab.
3. In the BGP Configuration section, complete the following:
   - **Advertising Interface**: Displays the interface that sends out BGP routing advertisements. BGP advertisements are supported on the LAN or HA interface only, depending on whether the appliance is an HA pair.
   - **ASN**: Enter the autonomous system number of the interface. Enter a number from 1 to 65535. You can configure only one ASN on each Grid member.
   - **BGP Timers**: BGP uses timers to control how often the interface sends KEEPALIVE messages and how long it waits before declaring a neighboring router out of service. The keepalive timer determines the time interval at which the interface sends KEEPALIVE messages to a neighboring router to inform the neighbor that the appliance is alive. The hold down timer determines how long the interface waits to hear a KEEPALIVE or UPDATE message before it assumes its neighbor is out of service. If a neighboring router is down, the interface terminates the BGP session and withdraws all the BGP routing information to the neighbor.
     - **Keep Alive**: Enter the time interval in seconds when the interface sends keepalive messages. You can enter a time from 1 to 21845 seconds. The default is four seconds.
     - **Hold Down**: Enter the time in seconds that the interface waits to hear a keepalive message from its neighbor before declaring the neighbor out of service. You can enter a time from 3 to 65535 seconds. The default is 16 seconds.

   Click the Add icon to add a neighboring router to receive BGP announcements. The appliance adds a row to the table. Complete the following:
   - **Neighbor Router IP**: Enter the IP address of the neighboring router that uses BGP for IP routing. The neighboring router can be within the same AS or from external ASs.
   - **Remote ASN**: Enter the ASN of the neighboring router. You can enter an ASN number from 1 to 65535.
   - **Comment**: Enter useful information about this neighboring router.

   Click the Add icon again to add another neighboring router. You can add up to 10 neighboring routers.

4. Save the configuration and click Restart if it displays at the top of the screen.
Part 4 DHCP

This section describes how to configure the Grid to provide DHCP services. It includes the following chapters:

- Chapter 19, Infoblox DHCP Services, on page 567
- Chapter 20, Configuring DHCP Properties, on page 587
- Chapter 21, Managing DHCP Templates, on page 623
- Chapter 22, Managing IPv4 DHCP Data, on page 639
- Chapter 23, DHCP Failover, on page 665
- Chapter 24, Configuring IPv4 DHCP Filters, on page 673
- Chapter 25, "Authenticated DHCP", on page 701
- Chapter 26, "Managing IPv6 DHCP Data", on page 733
- Chapter 27, Managing Leases, on page 745
Chapter 19 Infoblox DHCP Services

This chapter provides an overview of the Infoblox DHCP services for IPv4 and IPv6. It contains the following sections:

- About Infoblox DHCP Services on page 568
- IPv4 DHCP Protocol Overview on page 569
- IPv6 DHCP Protocol Overview on page 570
  - IPv6 Address Structure on page 571
- Configuring DHCP Overview on page 572
- Managing DHCP Data on page 574
  - About Networks on page 574
  - About Shared Networks on page 574
  - About DHCP Ranges on page 574
  - About Fixed Addresses on page 575
  - About Hosts on page 575
- About DHCP Inheritance on page 578
  - Overriding DHCP Properties on page 579
  - Viewing Inherited Values on page 579
- About DHCP Inheritance on page 578
  - Overriding DHCP Properties on page 579
  - Viewing Inherited Values on page 579
- About Network Views on page 583
  - Adding Network Views on page 584
  - Modifying Network Views on page 585
  - Deleting Network Views on page 585
About Infoblox DHCP Services

DHCP (Dynamic Host Configuration Protocol) is a network application protocol that automates the assignment of IP addresses and network parameters to DHCP-configured network devices (DHCP clients). When a DHCP client connects to a network, it sends a request to obtain an IP address and configuration information from the DHCP server. The DHCP server manages a pool of IP addresses and configuration information such as default gateway, domain name, and DNS server. Depending on the configuration, the DHCP server either assigns or denies an IP address to a client request. It also sends network configuration parameters to the client.

You can configure a NIOS appliance to provide DHCP service for IPv4 and IPv6. The Infoblox DHCP server complies with a number of DHCP and DHCPv6 RFCs (see Appendix A Product Compliance). Limited-access admin groups can access certain DHCP resources only if their administrative permissions are defined. For information on setting permissions for admin groups, see Chapter 3, Managing Administrators.
IPv4 DHCP Protocol Overview

As illustrated in Figure 19.1, when a DHCP client requests an IP address, it sends a DHCPDISCOVER message to the router, which can act as a relay agent. The router forwards the message to the DHCP server. When the DHCP server receives the DHCPDISCOVER message, it determines the network segment to which the client belongs and assigns an IP address. The DHCP server then sends a DHCPOFFER message that includes the IP address and other network configuration information. When the router receives the DHCPOFFER message, it broadcasts the message to the client that sent the DHCPDISCOVER message.

Figure 19.1 IP Address Allocation Process
IPv6 DHCP Protocol Overview

You can configure NIOS appliances to support DHCP for IPv6 (DHCPv6), the protocol for providing DHCP services for IPv6 networks.

The DHCPv6 client-server model is similar to that of IPv4. DHCP clients and servers use a reserved, link-scoped multicast address to exchange DHCP messages. When a DHCP client needs to send messages to a DHCP server that is not attached to the same link, a DHCP relay agent can be used to relay messages between the client and server. Each IPv6 DHCP server and client has a unique DHCP unique identifier (DUID). DHCP servers use DUIDs to identify clients when providing configuration parameters, and clients use DUIDs to identify the source of the DHCP messages from servers.

As illustrated in Figure 19.2, a DHCP client that needs an IPv6 address sends a Solicit message to the well-known multicast address. DHCPv6 servers then send Advertise messages to the client to indicate that they are available. The client sends a Request message to a specific DHCPv6 server to request IP addresses and configuration parameters. The DHCPv6 server responds with a Reply message that contains the IP addresses and configuration parameters. You can view statistics about the IPv6 messages on the Dashboard.

Figure 19.2

Infoblox DHCP servers also supports stateless configuration in which a DHCP client does not need IP addresses, but needs configuration information only. The DHCP client sends an Information-Request packet to obtain configuration information, and the server sends a Reply message with the requested information. For more information, refer to RFC 2462, IPv6 Stateless Address Autoconfiguration.
IPv6 Address Structure

An IPv6 address consists of the following:

- Global Routing Prefix—Global routing prefix is a (typically hierarchically-structured) value assigned to a site. For example, an ISP can delegate a prefix to your site, which you can then divide into subnets.
- Subnet ID—Subnet ID is an identifier of a link within the site.
- Interface ID—Interface Identifier. This portion of the address identifies the interface on the subnet. This is equivalent to the host identifier for IPv4 addresses.

Figure 19.3 IPv6 Address Structure

When you enter an IPv6 address in Grid Manager, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2006:0000:0000:0123:4567:89ab:0000:cdef can be shortened to 2006::123:4567:89ab:0:cdef. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The NIOS appliance displays an IPv6 address in its shortened form, regardless of its form when it was entered.
Configuring DHCP Overview

An overview of the complete DHCP configuration process is outlined in the following diagram (and continued on the next page), illustrating the main steps for preparing a NIOS appliance for use. Note that the process for configuring the DHCP server is the same for IPv4 and IPv6 networks, except that failover associations are not supported in IPv6 networks.

1. Specify the network address and netmask. - Select the member(s) that provide DHCP services for this network. - Specify the network address and netmask.

2. Decide how the network will be used. - Create failover associations - Configure the DHCP failover properties

* Do not start DHCP services when configuring members until the configuration is complete.

* You cannot use DHCP failover associations in IPv6 networks.
Define DHCP address ranges for this network.

Do you want to define fixed addresses for this network?

Yes

Configure the network-level DHCP properties.

No

Define DHCP address ranges for this network.

Do you want to add more ranges?

Yes

Configure the fixed addresses.

No

Do you want to add more networks?

Yes

See 1 in the previous diagram to repeat the process of adding more networks on additional members.

No

See 2 in the previous diagram to repeat the process of enabling the DHCP services on additional members.

Do you have additional members to configure for DHCP?

Yes

Initial configuration of DHCP networks is complete.

No

Start the DHCP and DHCPv6 services on members.
Managing DHCP Data

You can configure a NIOS appliance to provide DHCP service for IPv4 and IPv6, and manage both IPv4 and IPv6 objects. When you define DHCP objects, you can track specific information about a network device by defining extensible attributes. Extensible attributes are fields that you define to track properties such as network locations or device models. For more information, see About Extensible Attributes on page 262.

About Networks

You can configure DHCP IPv4 and IPv6 properties for the Grid and its members, and then define the IPv4 and IPv6 networks that they serve.

All networks, both IPv4 and IPv6, must belong to a network view. The appliance has one default network view and unless you create additional network views, all networks belong to the default view. Note that because network views are mutually exclusive, you can create networks with overlapping IP address spaces in two different network views. For more information, see About Network Views on page 583.

About Shared Networks

A shared network is a network segment to which you assign two or more subnets. When subnets in a shared network contain IP addresses that are available for dynamic allocation, the addresses are put into a common pool for allocation when client requests arise. When you create a shared network, the DHCP server can assign IP addresses to client requests from any subnet (that resides on the same network interface) in the shared network. For example, when you have networks A, B, and C on the same network interface and you assign them to a shared network, the DHCP server can allocate available IP addresses from any DHCP range within networks A, B, and C even when all the client requests originate from network A. When adding subnets to a shared network, ensure that the subnets are assigned to the same members to avoid DHCP inconsistencies.

Before creating a shared network, you must first create the subnets. For example, you must first create the IPv4 networks 10.32.1.0 and 10.30.0.0 before designating them to a shared network or create the IPv6 networks 2001:db8:1::/48 and 2001:db8:2::/48 before designating them to a shared network.

After you create a network, you can define their DHCP resources such as DHCP ranges, fixed addresses, reservations, host records, and roaming hosts. IPv4 and IPv6 support most of the same DHCP objects, except that IPv6 does not support reservations.

About DHCP Ranges

A DHCP range is a pool of IP addresses from which the appliance allocates IP addresses. You must add a DHCP address range in your network so the appliance can assign IP addresses to DHCP clients within the specified range. IPv6 DHCP ranges can also contain a range of IPv6 prefixes that it delegates to DHCP clients that request them.

You must assign a DHCP range to a Grid member. Note that you can only assign DHCP ranges to members and networks that are in the same network view. If the server is an independent appliance, you must specify this appliance as the member that serves the DHCP range. In addition, you can also assign IPv4 DHCP ranges to failover associations.

About Exclusion Ranges

You can define an exclusion range within a DHCP range. Creating an exclusion range prevents the appliance from assigning the addresses in the exclusion range to clients. IP addresses in an exclusion range are excluded from the pool of IP addresses. You can use exclusions to split a DHCP range into multiple blocks of ranges. You can also use addresses in the exclusion ranges as static IP addresses for network devices such as legacy printers that do not support DHCP. An exclusion in a range can help prevent address conflicts between statically configured devices and dynamically configured devices.
About Fixed Addresses

You can configure fixed addresses for network devices, such as routers and printers, that are not frequently moved from network to network. By creating fixed addresses for network devices, clients can reliably reach them by their domain names. Some network devices, such as web or FTP servers, can benefit from having fixed addresses for this reason. In IPv4 networks, you can also reserve an IP address that is not part of a DHCP range by defining a reservation. For information about creating reservations, see Configuring IPv4 Reservations on page 656.

About Hosts

Infoblox hosts are data objects that contain DNS, DHCP, and IPAM data of the assigned addresses. You can assign multiple IPv4 and IPv6 addresses to a host. When you create a host, you are specifying the name-to-address and address-to-name mappings for the IP addresses that you assign to the host. For information about Infoblox hosts, see About Host Records on page 811.
DHCP Configuration Checklists

After you complete the appliance configuration for each member in the Grid, as described in Chapter 7, Managing Appliance Operations, on page 241, you can configure DHCP services.

The following checklist includes the major steps for configuring DHCP service for IPv4:

Table 19.1 IPv4 DHCP Configuration Checklist

<table>
<thead>
<tr>
<th>Step</th>
<th>For more information</th>
</tr>
</thead>
</table>
| Configure DHCP properties for the Grid and members. | • Configuring IPv4 DHCP Properties on page 589  
• Chapter 16, Configuring DDNS Updates from DHCP, on page 477  
• Configuring DHCP IPv4 and IPv6 Properties on page 610  
• Configuring the Lease Logging Member on page 613 |
| Decide if you want to configure a DHCP failover association. | • Configuring Failover Associations on page 667 |
| Configure networks based on your network requirements and decide if you want to override the Grid or member DHCP configuration for the networks. | • Configuring IPv4 Networks on page 643  
• Configuring IPv4 Shared Networks on page 648 |
| Decide if you want to configure fixed addresses and reservations, and whether to override the upper level DHCP properties for the fixed addresses and reservations. | • Configuring IPv4 Fixed Addresses on page 653  
• Configuring IPv4 Reservations on page 656 |
| Define DHCP ranges and decide whether to override the upper level DHCP properties for the ranges. | • Configuring IPv4 Address Ranges on page 650 |
| Enable DHCP services on the member. | • Starting DHCP Services on a Member on page 620 |
The following checklist includes the major steps for configuring DHCP service for IPv6:

**Table 19.2 IPv6 DHCP Configuration Checklist**

<table>
<thead>
<tr>
<th>Step</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure DHCP properties for the Grid and members.</td>
<td>• Configuring DHCPv6 Properties on page 606</td>
</tr>
<tr>
<td></td>
<td>• Chapter 16, Configuring DDNS Updates from DHCP, on page 477</td>
</tr>
<tr>
<td></td>
<td>• Configuring DHCP IPv4 and IPv6 Properties on page 610</td>
</tr>
<tr>
<td></td>
<td>• Configuring the Lease Logging Member on page 613</td>
</tr>
<tr>
<td>Configure networks based on your network requirements and decide if you want to override the Grid or member DHCP configuration for the networks.</td>
<td>• Configuring IPv6 Networks on page 734</td>
</tr>
<tr>
<td></td>
<td>• About IPv6 Shared Networks on page 737</td>
</tr>
<tr>
<td>Decide if you want to configure fixed addresses and reservations, and whether to override the upper level DHCP properties for the fixed addresses and reservations.</td>
<td>• Configuring IPv6 Fixed Addresses on page 741</td>
</tr>
<tr>
<td>Define DHCP ranges and decide whether to override the upper level DHCP properties for the ranges.</td>
<td>• Configuring IPv6 Address Ranges on page 739</td>
</tr>
<tr>
<td>Enable DHCP services on the member.</td>
<td>• Starting DHCP Services on a Member on page 620</td>
</tr>
</tbody>
</table>
About DHCP Inheritance

When you configure DHCP properties for the Grid, members, networks, shared networks, DHCP ranges, fixed addresses, reservations, host addresses, and roaming hosts, the appliance applies the configured properties hierarchically. In addition, IPv4 DHCP objects inherit IPv4 specific properties and IPv6 objects inherit IPv6 specific properties. For example, when you set DHCP IPv4 properties for the Grid, all DHCP IPv4 objects inherit the properties from the Grid unless you override them at a specific level, and the same applies for IPv6 properties and objects. Properties set at the member level override Grid-level settings and apply to the objects 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 19.4 illustrates some inheritance scenarios that can occur in a Grid. As shown in the figure, the authoritative server configuration set for the Grid is inherited by the members. Since Member 1 has no overrides and Member 2 overrides the authoritative server configuration, they have different DHCP configurations. Grid Manager applies DHCP properties hierarchically from the Grid down. Therefore, a DHCP object below the member level can inherit DHCP properties with multiple values from multiple sources. In Figure 19.4, network 10.1.1.0/24 inherits multiple values (True and False) from the members for the authoritative server configuration. The shared network, which includes 10.1.1.0/24, inherits DHCP properties from both members. For DHCP range 10.1.1.11 - 10.1.1.50, since Member 1 is the assigned member, it inherits properties from Member 1 and the network. The fixed address 10.1.1.2 overrides the BOOTP settings and inherits the authoritative server configuration from both members and the network.

Figure 19.4  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.
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>Simple Inheritance.</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>Unknown Inheritance on page 580.</td>
</tr>
<tr>
<td>Inherited From Multiple</td>
<td>the DHCP property has the same value that it inherits from multiple sources.</td>
<td>Multiple Inheritance on page 581.</td>
</tr>
<tr>
<td>Settings Inherited from Multiple Ancestors, View Multiple Inheritance Scenarios</td>
<td>the DHCP property has multiple values that it inherits from multiple sources, and you can view the values and their corresponding sources by clicking the View Multiple Inheritance Scenarios link.</td>
<td>Multiple Inheritance on page 581.</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 19.5.
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 19.6, network 10.1.1.0 has unknown lease time value because it does not have any assigned member.

**Figure 19.6 Unknown Inheritance**
Multiple Inheritance

As illustrated in Figure 19.4, 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 19.7.

Figure 19.7 Multiple Inherited Paths with the Same Inherited Value

In the same Grid with the two members serving the same network, the network inherits different values for the same properties if you override the Grid configuration on one member but not on the other. For example, you can configure different PXE lease times for the members and configure a member as an authoritative DHCP server for the domain and the other not. In this case, the appliance displays Settings inherited from multiple ancestors and provides a View Multiple Inheritance Scenarios link so you can view the inherited values and paths, as shown in Figure 19.8.

Figure 19.8 Multiple Inheritance Sources with Multiple Values
For example, to view the multiple inherited values of the **Authoritative** field, click **View Multiple Inheritance Scenarios**, and the **Multiple Inheritance Viewer** displays the inherited values from the two members. Since member1.foo.net does not have a configured value for this field, the viewer displays **Not Set**, as shown in **Figure 19.9**. You can use this information to determine whether you want to keep the inherited values or configure new ones.

**Figure 19.9 Multiple Inheritance Viewer**

![Multiple Inheritance Viewer](image)

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 19.10**. You can override these options but you cannot delete them. For multiple values inherited from multiple sources, you can view the values in the **Multiple Inheritance Viewer** by clicking **View Inheritance**, as shown in **Figure 19.11**.

**Figure 19.10 DHCP Custom Options with Multiple Inheritance Sources**

![DHCP Custom Options with Multiple Inheritance Sources](image)

**Figure 19.11 Multiple Inheritance Viewers for Options**

![Multiple Inheritance Viewer](image)

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 603.
About Network Views

A network view is a single routing domain with its own networks and shared networks. A network view can contain both IPv4 and IPv6 networks. All networks must belong to a network view.

You can manage the networks in one network view independently of the other network views. Changes in one network view are not reflected in other network views. Because network views are mutually exclusive, the networks in each view can have overlapping address spaces with multiple duplicate IP addresses without impacting network integrity.

For example, two corporations, Corp 100 and Corp 200, merge. They each have their own networks and DNS domains. They also have their own private IP address spaces in the 10.0.0.0/24 network. Both corporations have DHCP and DNS servers, and use dynamic DNS updates. The DHCP servers of each corporation serve IP addresses for networks in their respective corporations. The DHCP clients in each corporation update DNS zones within their DNS domains.

They plan to migrate the networks and hosts in Corp 200 to the Corp 100 address space and the 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 19.12, you can configure network views for each corporation and manage their networks independently of the other.

Member 1 serves DNS and DHCP to Corp 100. The networks of Corp 100 are contained in the corp 100 network view, which is associated with both the internal and external DNS views of the 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 19.12 Two Network Views Managed by a Grid
A Grid member can serve one network view only, but a network view can be served by multiple Grid members. DHCP failover associations must be defined within a single network view, and both the primary and secondary peer must serve the same network view.

The NIOS appliance provides one default network view. You can rename the default view and change its settings, but you cannot delete it. There must always be at least one network view in the appliance. If you do not need to manage overlapping IP address spaces in your organization, you can use the system-defined network view for all your networks. You do not need to create additional network views. But if there are overlapping IP address spaces and you need more than one network view, you can create up to 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 19.12), but a DNS view cannot be associated with more than one network view. Each network view must be associated with a unique set of DNS views. You can initiate a network discovery in only one network view at a time. When you run a discovery task, the appliance sends updates to all DNS views associated with the network view. (For information about network discoveries, see Chapter 32, Network Discovery, on page 843.)

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 262.
4. Click Next, and then save the configuration or select:
   Configure DDNS Properties: Configure the DNS zones that are associated with the network view to receive DDNS updates. When you select this option, the Configure DDNS Properties dialog box appears. The appliance saves the network view entry before it opens the Configure DDNS Properties dialog box. For information, see Configuring DDNS Updates from DHCP on page 477.
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 262.
   - **Permissions**: This tab displays only if you belong to a superuser admin group. For information, see Administrative Permissions for DHCP Resources on page 160.

Deleting Network Views

You can delete any network view, except for the default network view. You can delete a network view that has only one DNS view associated with it. You cannot delete a network view that has more than one DNS view associated with it. When you delete a network view, the appliance deletes all the networks and records within the network view.

To delete a network view:

1. From the Administration tab, select the Network Views tab -> network_view check box, and then click the Delete icon.

2. In the Delete Confirmation dialog box, click Yes.

   The appliance removes the network view and its associated DNS views. You can restore the network view from the Recycle Bin, if enabled. If you restore a network view, the appliance restores the associated DNS views as well. For information about the Recycle Bin, see Using the Recycle Bin on page 54.
Chapter 20 Configuring DHCP Properties

This chapter explains how to configure DHCP IPv4 and IPv6 properties. It contains the following sections:

- **About DHCP Properties** on page 589
- **Configuring IPv4 DHCP Properties** on page 589
- **Configuring General IPv4 DHCP Properties** on page 590
  - Specifying Authoritative on page 590
  - Defining Lease Times on page 590
  - Scavenging Leases on page 590
- **Configuring Ping Settings** on page 592
- **Configuring IPv4 BOOTP and PXE Properties** on page 594
- **About IPv4 DHCP Options** on page 595
  - DHCP Option Data Types on page 596
  - Configuring IPv4 DHCP Options on page 597
  - Defining Basic IPv4 Options on page 597
  - Defining IPv4 Option Spaces on page 598
  - Configuring Custom DHCP Options on page 598
  - Applying DHCP Options on page 599
  - Configuration Example: Defining a Custom Option on page 600
  - Configuring Option 60 Match Rules on page 601
  - About the DHCP Relay Agent Option (Option 82) on page 602
- **Configuring Thresholds for DHCP Ranges** on page 603
- **Configuring DHCPv6 Properties** on page 606
  - Defining General IPv6 Properties on page 606
- **About DHCPv6 Options** on page 607
  - Configuring DHCPv6 Options on page 607
  - Defining IPv6 Option Spaces on page 607
  - Configuring Custom IPv6 DHCP Options on page 608
  - Applying DHCPv6 Options on page 608
- **Configuring DHCP IPv4 and IPv6 Properties** on page 610
  - Configuring UTF-8 Encoding for Hostnames on page 610
  - Associating Networks with Zones on page 611
  - Keeping Leases in Deleted IPv4 and IPv6 Networks and Ranges on page 612
  - Configuring Fixed Address Leases For Display on page 612
Configuring DHCP Properties

- **Configuring DHCP Logging** on page 613
  - Configuring the Lease Logging Member on page 613

- **About IF-MAP** on page 615
  - Configuring a Grid to Support IF-MAP on page 616
  - Validating the IF-MAP Server Certificate on page 616
  - Configuring Members as IF-MAP Clients on page 616
  - Creating IF-MAP Client Certificates on page 617
  - Overriding IF-MAP Publishing Settings on page 619
  - Deleting Data from the IF-MAP Server on page 619

- **Starting DHCP Services on a Member** on page 620

- **Viewing DHCP Member Status** on page 621
  - Viewing DHCP Configuration Files on page 622
About DHCP Properties

When you configure a NIOS appliance to function as a DHCP server, you can set DHCP properties that control how the appliance operates and enable DHCP service for IPv4 and IPv6.

You can also specify configuration information the appliance includes in its IPv4 and IPv6 DHCP messages. When a DHCP server assigns an IP address to a client, it can include information the client needs to connect to the network and communicate with other hosts and devices on the network. You can set these properties at the Grid level and override them for a member, network, shared network, DHCP range, fixed address, IPv4 reservation, host address, or roaming host.

When you configure a DHCP object that has inherited DHCP properties, you can either keep the inherited properties or override them. The appliance displays the inherited values and the levels from which the DHCP properties are inherited. For information, see About DHCP Inheritance on page 578.

Configuring IPv4 DHCP Properties

The following sections describe how to configure properties that apply to IPv4 DHCP objects only. You can configure and define the following DHCP properties:

- General properties, as described in Configuring General IPv4 DHCP Properties on page 590.
- Ping settings, as described in Configuring Ping Settings on page 592.
- BOOTP and PXE properties, as described in Configuring IPv4 BOOTP and PXE Properties on page 594.
- Custom DHCP options, as described in About IPv4 DHCP Options on page 595.
- DDNS settings, as described in Chapter 16, Configuring DDNS Updates from DHCP, on page 477.
- Thresholds for DHCP ranges, as described in Configuring Thresholds for DHCP Ranges on page 603.

For information on configuring properties that apply to IPv4 and IPv6 DHCP objects, see Configuring DHCP IPv4 and IPv6 Properties on page 610.

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 160.
Configuring General IPv4 DHCP Properties

When you configure general IPv4 DHCP properties at the Grid level, the configuration applies to the entire Grid. Though you can set DHCP properties at the Grid level, you can enable DHCP services at the member level only. Infoblox recommends that you configure the DHCP properties before you enable DHCP on the appliance. Depending on the properties, you can override some of them for the members, networks, DHCP ranges, fixed addresses, reservations, host addresses, and roaming hosts. To override an inherited DHCP property, click Override next to the property to enable the configuration.

Specifying Authoritative

Only authoritative DHCP servers can send clients DHCPNAK messages when they request invalid IP addresses. For example, a client moves to a new subnet and broadcasts a DHCPREQUEST message for its old IP address. An authoritative DHCP server responds with a DHCPNAK, causing the client to move to the INIT state and to send a DHCPDISCOVER message for a new IP address. Authoritative servers also respond to DHCPIPFORM messages from clients that receive their IP addresses from the DHCP server and require additional options after the initial leases have been granted.

Defining Lease Times

When you configure DHCP general properties, you can specify the length of time the DHCP server leases an IP address to a client. The default on the appliance is 12 hours, and you can change this default according to your network requirements. There are a number of factors to consider when setting the lease time for IP addresses, such as the types of resources and clients on the network, and impact to traffic and performance. With NIOS appliances, you can set lease times at different levels, based on these factors. You can 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.

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: 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 configure general IPv4 properties:

1. **Grid:** From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar.  
   **Member:** From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box, and then click the Edit icon.  
   **Network:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon.  
   **DHCP Range:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range check box, and then click the Edit icon.  
   **Fixed Address:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> fixed_address check box, and then click the Edit icon.  
   **Reservation:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> reservation check box, and then click the Edit icon.

2. In the DHCP Properties editor of a Grid or member, select the **General Basic** tab. For all other objects, click **Toggle Expert Mode** if the editor is in basic mode. When the additional tabs appear, select the **IPv4 DHCP Options Advanced** tab.

3. Complete the following
   - **Authoritative:** Select **DHCP server is authoritative** to set the DHCP server as authoritative for the domain. This can be set for the Grid, member, network and range.
   - **Lease Time:** Enter the lease time and select the time unit from the drop-down list. The default is 12 hours.

To set all other properties for a Grid or member, toggle to the expert mode and select the **General Advanced** tab to complete the following:

   - **DHCP Lease Scavenging:** Select **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. This can be set for the Grid, member, network and range.
   - **Ignore Optionlist:** Select **Ignore optionlist requested by client and return all defined options** if you want the appliance to ignore the requested list of options in the DHCPREQUEST messages it receives from DHCP clients, and to include all the configured options in the DHCPACK and DHCPOFFER messages it sends back to the clients.
   - **LEASEQUERY:** Select **Allow LEASEQUERY** to enable the DHCP server to respond to DHCPLEASEQUERY messages.

4. Save the configuration and click **Restart** if it displays at the top of the screen.
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 20.1 Ping Overview*

1. Client broadcasts a DHCPDISCOVER message.
2. When the NIOS appliance receives the DHCPDISCOVER message, it checks its record of IP addresses and selects an IP address for lease.
3. The appliance sends the configured number of pings to the selected IP address. The appliance receives a reply, indicating that the IP address is in use.
4. The appliance selects another IP address and sends it the configured number of pings. The appliance does not receive a response within the specified timeout, and assumes the address is not in use.
5. The appliance sends the client a DHCPOFFER message with the selected IP address.

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 -> member check box, and then click the Edit icon.

2. In the DHCP Properties editor, click **Toggle Expert Mode** if the editor is in basic mode. When the additional tabs appear, click the General tab -> Advanced tab and complete the following:
   
   - **Number of Ping Requests**: Enter the number of pings the appliance sends to an IP address to verify that it is not in use. The range is 0 to 10, inclusive. Enter 0 to disable DHCP pings.
   
   - **Ping Timeout (Seconds)**: Enter the ping timeout value. The range is 1 to 5, inclusive.

3. Save the configuration and click **Restart** if it displays at the top of the screen.
Configuring IPv4 BOOTP and PXE Properties

You can configure the DHCP server to support IPv4 clients that use BOOTP (bootstrap protocol) or that include the TFTP server name option and boot file name option in their DHCPREQUEST messages. You can specify the name or IP address of the boot server and the name of the file the host needs to boot.

In addition, you can configure the DHCP server to support hosts that use PXE (Preboot Execution Environment) to boot remotely from a server. When such a host starts up, it first requests an IP address so it can connect to a server on the network and download the file it needs to boot. After it downloads the file, the host reboots and sends another IP address request. To better manage your IP resources, set a different lease time for PXE boot requests. You can configure the DHCP server to allocate an IP address with a shorter lease time to hosts that send PXE boot requests, so IP addresses are not leased longer than necessary.

You can configure BOOTP and PXE properties at the Grid level and override them for members, IPv4 networks, DHCP ranges, fixed addresses, and reservations, host addresses, and roaming hosts. You cannot configure BOOTP and PXE properties for IPv6 DHCP objects.

To configure or override BOOTP and PXE properties:

1. **Grid Level:** From the Data Management tab, select the DHCP tab, and then click **Grid DHCP 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.

2. In the **DHCP Properties** editor, select the **BOOTP/PXE** 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.
   - **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. Save the configuration and click **Restart** if it displays at the top of the screen.
**About IPv4 DHCP Options**

DHCP options provide specific configuration and service information to DHCP clients. These options appear as variable-length fields at the end of the DHCP messages that DHCP servers and clients exchange. For example, DHCP option 3 is used to list the available routers in the network of the client and option 6 is used to list the available DNS servers.

An option space is a collection of options. ISC (Internet Systems Consortium) DHCP has five predefined option spaces: dhcp, agent, server, nwip, and fqdn. The NIOS appliance supports only the predefined DHCP option space, which contains the industry standard options as well as additional options you can configure as needed:

- **Predefined options:** These are option codes 1 to 125. They are allocated by the IANA and defined by IETF standards. The DHCP server knows these standard options, and they are predefined on the server. You cannot redefine these options or delete them from the DHCP option space.
- **Custom options:** These are option codes 126 to 254. They are not defined by IETF standards and are available for private use. You can use these option codes to provide configuration or service information that none of the predefined options provide.

You can also create option spaces to define new groups of options. For example, you can create additional option spaces to define vendor specific options, which are encapsulated in option 43. When a DHCP client requests vendor specific options, it makes a request using the vendor identifier set in option 60 and a list of requested vendor specific options (option 43). The DHCP server then responds with the list of replies for the various options encapsulated into option 43.

Note that custom options defined in the DHCP option space are included in the options section of the DHCP messages that DHCP servers and clients exchange. Custom options defined in a user-defined option space are always encapsulated in option 43 in DHCP messages.

You can apply options globally at the Grid level, or more specifically at the member, network, 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 687.

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 20.1.

Table 20.1  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:
- \(\text{aa:de:89:1b:34}\)
- \(\text{1C:8:22:A3}\) (Note that the DHCP module treats a single hexadecimal character, such as “8” as “08”.)

A few examples of incorrectly written hexadecimal strings:
- \(\text{:bb:45:d2:1f}\) - Problem: The string erroneously begins with a colon.
- \(\text{bb:45:d2:1f:}\) - Problem: The string erroneously ends with a colon.
- \(\text{bb:4 5:d2:1f}\) - Problem: The string erroneously includes a space between two characters (“4” and “5”).
- \(\text{bb:45:d2:1g}\) - Problem: The string erroneously includes a nonhexadecimal character (“g”).

The DHCP module treats incorrectly written hexadecimal strings as simple text strings, not hexadecimal strings. If the string appears in quotes, it is a text string.
Configuring IPv4 DHCP Options

To use DHCP options, you can do the following:

- Define basic DHCP options, as described in Defining Basic IPv4 Options.
- Configure one or more option spaces, as described in the next section Defining IPv4 Option Spaces.
- Define custom options in the predefined DHCP option space or add options to an option space that you configured. For more information, see Configuring Custom DHCP Options on page 598.
- 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 599.

Defining Basic IPv4 Options

You can define basic DHCP options that the DHCP server uses to provide configuration information to DHCP clients. The server includes these options in its DHCP messages.

To define DHCP options:
1. **Network:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon.

   **DHCP Range:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> DHCP_range check box, and then click the Edit icon.

   **Fixed Address:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> fixed_address check box, and then click the Edit icon.

   **Reservation:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> reservation check box, and then click the Edit icon.

   **Host Address:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> host_record check box, and then click the Edit icon. Select the host IP address, and then click the Edit icon.

   **Roaming Host:** From the Data Management tab, select the DHCP tab -> Networks tab -> Roaming Hosts -> roaming_host check box, and then click the Edit icon.

2. In the DHCP Properties editor, select the 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 16, Configuring DDNS Updates from DHCP, on page 477.
   - **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. Save the configuration and click Restart if it appears at the top of the screen.
Configuring DHCP Properties

Defining IPv4 Option Spaces

DHCP members support the DHCP option space by default. You can create additional option spaces to provide additional configuration or service information. Note that custom options defined in a user-defined option space are always encapsulated in option 43 in DHCP messages.

To add a custom option space:

1. From the Data Management tab, select the DHCP tab -> Option Spaces tab.
2. Click the Add icon -> IPv4 Option Space.
3. In the Option Space wizard, do the following:
   - Name: Enter the name of the option space.
   - Comment: Enter useful information about the option space.
   - Options: Click the Add icon to add options. For additional information, see the next section, Configuring Custom DHCP Options on page 598.
4. Save the configuration and click Restart if it displays at the top of the screen.

After you create an option space and add options to it, you can apply the options as described in Applying DHCP Options on page 599.

Configuring Custom DHCP Options

You can define custom options in the DHCP option space or in an option space that you configured, as follows:

1. From the Data Management tab, select the DHCP tab -> Option Spaces tab.
2. Select either the DHCP option space or an IPv4 option space that you configured, and then click the Edit icon.
3. In the Option Space editor, click the Add icon to add a custom option. In the new row, complete the following:
   - Name: Enter the name of the custom DHCP option.
   - Code: Select an option code from the drop-down list. Select a number between 126 and 254 if you are adding custom options to the DHCP option space. If you are adding custom options to an IPv4 option space you configured, you can enter a number between 1 and 254.
   - Type: Select the option type (such as ip-address, text, boolean, and string as described in Table 20.1). 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.
4. Save the configuration.
Applying DHCP Options

Some options may apply to all networks and some may apply to specific ranges and even hosts. When you apply an option, you select the object to which the option is applied, such as the Grid member, or network, and then specify a value for the option.

Use the following guidelines when specifying option values:

- Enter false or true for a Boolean Flag type value.
- Enter an ASCII text string, or enter a series of octets specified in hex, separated by colons.
- Separate multiple values by commas. For example, to enter multiple IP addresses for netbios-name-servers, enter a comma between each IP address.

Here are some examples of option names and correctly formatted values:

<table>
<thead>
<tr>
<th>Option name</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>option 61</td>
<td>dhcp-client-identifier</td>
<td>MyPC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Double quotes are no longer needed for string type values</td>
</tr>
<tr>
<td>dhcp-client-identifier</td>
<td>43:4c:49:54:54:2d: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 IPv4 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 596.
   - Click + to add another option, or click - to delete a previously specified option. When overriding an option, enter the new value for the selected option.
   - Note that if you created an option space as described in Defining IPv4 Option Spaces on page 598, this section displays a list of option spaces in the first drop-down menu, so you can select the option space of the option you want to define.

3. Save the configuration and click Restart if it displays at the top of the screen.
Configuration Example: Defining a Custom Option

In this example, you configure two custom options in the DHCP option space, and apply them to a DHCP range in the network 192.168.2.0/24.

Add the custom options to the DHCP options space:

1. From the Data Management tab, select the DHCP tab -> 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. Save the configuration and click Restart if it displays at the top of the screen.

The member then includes options 150 and 209 in its DHCP messages to clients that are allocated IP addresses from the DHCP range 192.168.2.10 - 100.
Defining Option 60 Match Rules

The appliance uses option 60 (vendor-class-identifier) to forward client requests to the DHCP server for services that the clients require. You can define option 60 match rules and filter on these rules. You can set these rules for the Grid and override for a member.

To define option 60 for the Grid or member:

1. **Grid**: From the Data Management tab, select the DHCP tab, and then click Grid DHCP Configuration from the Toolbar.

   **Member**: From the Data Management tab, select the DHCP tab -> Members tab -> member check box, and then click the Edit icon.

2. In the DHCP Properties editor, click **Toggle Expert 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. Save the configuration and click **Restart** if it displays at the top of the screen.
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 DHCP_OFFER 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 DHCP_OFFER message. To avoid broadcasting the DHCP_OFFER 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 683.

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 IPv4 Fixed Addresses on page 654.
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 thresholds 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 threshold might indicate network issues preventing the renewal of leases. When usage for a DHCP range crosses a threshold, the appliance makes a syslog entry and—if configured to do so—sends the administrator alerts as SNMP traps and email notifications. Figure 20.2 illustrates the relationship of allocated and available addresses to high and low watermarks in a DHCP range.

Figure 20.2 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 20.3 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 579.
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 **IPv4 Thresholds** tab and complete the following:
   
   — **DHCP Thresholds**: Select **Enable DHCP Thresholds** to enable the DHCP threshold feature.
   
     — **High**: Enter a number between 0 and 100. Enter Trigger and Reset values. If the percentage of allocated addresses in a DHCP range exceeds the Trigger value, the appliance makes a syslog entry and—if configured to do so—sends an SNMP trap and an email notification to a designated destination. When the percentage first reaches the Reset value after it hit the Trigger value, the appliance sends an SNMP trap. The default is 95.
   
     — **Low**: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range drops below the Trigger value, the appliance makes a syslog entry and—if configured to do so—sends an SNMP trap and an email notification to a designated destination. When the percentage first reaches the Reset value after it hit the Trigger value, the appliance sends an SNMP trap. The default is 0.
   
     — **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. Save the configuration and click **Restart** if it displays at the top of the screen.
Configuring DHCPv6 Properties

The following sections describe how to configure properties and options that apply to DHCPv6 objects only. You can configure and define the following DHCP properties:

- General properties, as described in the next section, *Defining General IPv6 Properties*.
- DHCP options, as described in *About DHCPv6 Options*.

Defining General IPv6 Properties

You can configure general DHCPv6 properties at the Grid level and override them at the member and lower levels.

1. **Grid**: From the *Data Management* tab, select the *DHCP* tab, and then click *Grid DHCP 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.
   - **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.

2. In the *DHCP Properties* editor, select the *IPv6 DHCP Options* tab, and complete the following:
   - **Valid Lifetime**: Specify the length of time addresses that are assigned to DHCP clients remain in the valid state. When this time expires, an address becomes invalid and can be assigned to another interface.
   - **Preferred Lifetime**: Specify the length of time that a valid address is preferred. A preferred address can be used with no restrictions. When this time expires, the address becomes deprecated.
   - **Domain Name**: Enter the name of the domain for which the Grid serves DHCP data.
   - **DNS Servers**: Click the Add icon. Grid Manager adds a row to the table. In the table, enter the IPv6 addresses of DNS recursive name servers to which the DHCP client can send name resolution requests. The DHCP server includes this information in the DNS Recursive Name Server option in Advertise, Rebind, Information-Request, and Reply messages.

3. Save the configuration.
About DHCPv6 Options

DHCPv6 options provide configuration and service information to IPv6 clients. Just like IPv4 options, IPv6 options appear as variable length fields at the end of the DHCPv6 messages.

Just as in IPv4, the NIOS appliance supports the following options in the DHCPv6 options space:

• Predefined options: These are the option codes defined in RFC 3315. You cannot redefine these options or delete them from the DHCP option space. Option codes 1-48 are reserved and cannot be used to define custom options.

• Custom options: These are option codes 49 to 254. They are not defined by IETF standards and are available for private use. You can use these option codes to provide configuration or service information that none of the predefined options provide.

You can create option spaces to define new groups of options. For example, you can create additional option spaces to define vendor specific options, which are encapsulated in DHCPv6 option 17. When an IPv6 client requests vendor specific options, it makes a request using the vendor specific options (option 17). The DHCP server then responds with the list of replies for the various options encapsulated into option 17.

Note that custom options defined in the DHCP option space are included in the options section of the DHCP messages that DHCP servers and clients exchange.

You can apply options globally at the Grid level, or more specifically at the member, network, range, host and roaming host levels.

Configuring DHCPv6 Options

To use DHCPv6 options, you can do the following:

• Configure one or more option spaces, as described in the next section Defining IPv6 Option Spaces.

• Define custom options in the predefined DHCPv6 option space or add options to an option space that you configured. For more information, see Configuring Custom IPv6 DHCP Options on page 608.

• Specify values for the options and apply them to the Grid, or to a member, network, fixed address, host, or roaming host. For more information, see Applying DHCPv6 Options on page 608.

Defining IPv6 Option Spaces

DHCP members support the DHCPv6 option space by default. You can create additional option spaces to provide additional configuration or service information.

To add a custom option space:

1. From the Data Management tab, select the DHCP tab -> Option Spaces tab.
2. Click the Add icon -> IPv6 Option Space.
3. In the IPv6 Option Space wizard, do the following:
   — Name: Enter the name of the option space.
   — Enterprise Number: Enter the vendor’s Enterprise Number that is registered with IANA.
   — Comment: Enter useful information about the option space.
   — Options: Click the Add icon to add options. For additional information, see the next section, Configuring Custom DHCP Options on page 598.
4. Save the configuration and click Restart if it displays at the top of the screen.

After you create an option space and add options to it, you can apply the options as described in Applying DHCP Options on page 599.
Configuring Custom IPv6 DHCP Options

You can define custom options in the DHCP option space or in an option space that you configured, as follows:

1. From the Data Management tab, select the DHCP tab -> Option Spaces tab.
2. Select either the DHCPv6 option space or an IPv6 option space that you configured, and then click the Edit icon.
3. In the Option Space editor, click the Add icon to add a custom option. In the new row, complete the following:
   - Name: Enter the name of the custom DHCP option.
   - Code: Select an option code from the drop-down list. Select a number between 49 and 254 if you are adding custom options to the DHCPv6 option space. If you are adding custom options to an IPv6 option space you configured, you can enter a number between 1 and 254.
   - Type: Select the option type (such as ipv6-address, text, boolean, and string as described in Table 20.1).
   
   Click the Add icon to add more options.
4. Save the configuration.

Applying DHCPv6 Options

You can apply some options at the Grid or member level, and some options to specific networks, shared networks, fixed addresses and roaming hosts. When you apply an option, you select the object to which the option is applied, such as the Grid, member, or network, and then specify a value for the option.

Use the following guidelines when specifying option values:

- Enter false or true for a Boolean Flag type value.
- Enter an ASCII text string, or enter a series of octets specified in hex, separated by colons.
- Separate multiple values by commas. For example, to enter multiple IP addresses for netbios-name-servers, enter a comma between each IP address.

DHCPv6 options support the same data types as DHCP IPv4 options. For more information about the data types, see DHCP Option Data Types on page 596.

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.
   - 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.
   - 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 **IPv6 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 596.

   Click + to add another option, or click - to delete a previously specified option. When overriding an option, enter the new value for the selected option.

   Note that if you created an option space as described in **Defining IPv4 Option Spaces** on page 598, this section displays a list of option spaces in the first drop-down menu, so you can select the option space of the option you want to define.

3. Save the configuration and click **Restart** if it displays at the top of the screen.
Configuring DHCP Properties

Configuring DHCP IPv4 and IPv6 Properties

This section describes DHCP properties that apply to both IPv4 and IPv6. It includes the following sections:

- Configuring UTF-8 Encoding for Hostnames
- Associating Networks with Zones on page 611
- Keeping Leases in Deleted IPv4 and IPv6 Networks and Ranges on page 612
- Configuring Fixed Address Leases For Display on page 612

Configuring UTF-8 Encoding for Hostnames

When you configure the appliance as a DHCP server, the appliance supports UTF-8 encoding of hostnames that are encoded with Microsoft Windows code pages. You can configure the DHCP services on the appliance to convert these client hostnames to UTF-8 characters. The appliance stores the UTF-8 encoded hostnames in the database. If you also configure the DHCP services on the appliance to perform DDNS updates, the appliance sends the UTF-8 encoded hostnames in the DDNS updates. You can configure the UTF-8 encoding of hostnames at the Grid DHCP service and member DHCP service levels. For information on UTF-8 encoding, see Printing from Grid Manager on page 67.

The appliance displays the host names in their original characters in the following:

- DHCP lease history
- DHCP lease details
- IP address management
- Syslog
- Audit log

To configure UTF-8 encoding for hostnames:

1. **Grid**: From the Data Management tab, select the DHCP tab, and then select Grid DHCP Properties from the Toolbar.
   **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 Basic tab and complete the following:
   - IPv4 Properties
     - Microsoft Clients Code Page: From the drop-down list, select the code page with which the host names are encoded when the appliance converts the Microsoft code page encoded host names to UTF-8 characters.
   - IPv6 Properties
     - Microsoft Clients Code Page: From the drop-down list, select the code page with which the host names are encoded when the appliance converts the Microsoft code page encoded host names to UTF-8 characters.

3. Save the configuration and click Restart if it displays at the top of the screen.
Associating Networks with Zones

You can associate IPv4 and IPv6 networks with DNS zones to limit the zones that admins can use when they create DNS records for IP addresses in the networks. When a network is associated with one or more zones and an admin creates a DNS record for one of its IP addresses, Grid Manager allows the admin to create the DNS record in the associated zones only. For example, if you associate the 10.1.0.0/16 network with the 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; or if you associate the 2001:db8:1::/48 network with the corp200.com zone, admins are allowed to create DNS records in the corp200.com zone only for IP addresses in the 2001:db8:1::/48 network.

This feature applies to A, AAAA and host records only. It does not apply to records in a shared record group. If you are creating a host record with multiple IP addresses in different networks, the networks must be associated with the zone of the host record.

If a network is not associated with a zone, admins can create DNS records for its IP addresses only in zones with no network associations as well.

You can associate a network with any authoritative zone whose primary server is a Grid member or a Microsoft server, or is unassigned. You cannot associate networks with zones that have external primary servers.

You can associate a network with multiple zones, and associate a zone with more than one network. You can associate IPv4 and IPv6 network containers and networks with zones. When you associate a network container with zones, its networks inherit the zone associations. You can override the zone associations at the network level.

If you split a network, the resulting subnets inherit the zone associations. If you join networks, the resulting network retains the zone associations of the network that you selected when you performed the join operation. You can override the inherited zone associations of individual networks. Subzones do not inherit the network associations of their parent zones.

When you import data into a zone that is associated with a list of networks, the imported A, AAAA and host records must have IP addresses in the associated networks. Grid Manager does not allow you to import A, AAAA and host records with IP addresses in unassociated networks.

When you associate a network with a zone, the DNS records created before the association are not affected. But if you edit an A, AAAA or host record after the association, Grid Manager does not allow you to save the record if its IP address is not in an associated network.

To associate an IPv4 or IPv6 network with a zone:
1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon.
2. In the DHCP Network editor, click Toggle Expert 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. Save the configuration or click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.

Viewing the Networks Associated with a Zone

You can view the IPv4 or IPv6 networks associated with a zone from the zone editor. The tab to display network associations in zone editors is visible only if the primary server is a Grid member, a Microsoft server, or unassigned.

To view the network associations of a zone:
1. From the Data Management tab, select the DNS tab -> Zones tab -> zone check box, and then click the Edit icon.
2. In the Authoritative Zone editor, click Toggle Expert Mode if the editor is in basic mode.
3. When the additional tabs appear, click the Advanced subtab of the General tab.

   The Network Associations table lists the networks and their corresponding comments. You cannot change the network associations in this editor. Navigate to the DHCP Network editor of the network, to change the zone associations.
Keeping Leases in Deleted IPv4 and IPv6 Networks and Ranges

You can configure the DHCP server to store leases in a deleted DHCP range for up to one week after the leases expire. When you add a new DHCP range that includes the IP addresses of these leases or assign the DHCP range to another member within the Grid, the appliance automatically restores the active leases. You can configure this feature for the Grid, and override the configuration for members, networks, and DHCP ranges.

To keep active leases in a deleted DHCP range:

1. **Grid**: From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar.
   - **Member**: From the Data Management tab, select the DHCP tab -> Members -> 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.
   - **Range**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> range check box, and then click the Edit icon.

2. In the DHCP Properties editor of the Grid or member, click **Toggle Expert Mode** if the editor is in basic mode, and then click the **Advanced** tab. In the Network editor or Range editor, click **Toggle Expert Mode** if the editor is in basic mode, and then click IPv4 DHCP Options -> Advanced or IPv6 DHCP Options -> Advanced.

   Complete the following:
   - **IPv4 Properties**
     - **Lease Deletion**: When you select Keep leases from deleted range until one week after expiration and delete a DHCP range with active leases, the appliance stores these leases for up to one week after they expire.
   - **IPv6 Properties**
     - **Lease Deletion**: When you select Keep leases from deleted range until one week after expiration and delete a DHCP range with active leases, the appliance stores these leases for up to one week after they expire.

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

Configuring Fixed Address Leases For Display

You can configure the DHCP server to capture the hostname and lease time of a fixed address when you assign an IPv4 or IPv6 fixed address to a client. The appliance displays the hostname, and the start and end time of each fixed address lease in the Current Leases panel in Grid Manager.

You can set this at the Grid level only for IPv4 and IPv6 leases.

1. From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar.

2. In the Grid DHCP Properties editor, click **Toggle Expert Mode** if the editor is in basic mode. When the additional tabs appear, click the **Advanced** tab and complete the following:

   - **IPv4 Properties**
     - **Fixed Address Lease**: Select Capture hostname and lease time when assigning Fixed Addresses. The appliance displays the host name, and the start and end time of each fixed address lease in the Current Leases panel. If there are multiple records (A, host, and lease) for the IP address, it also displays the information for the records. This option is available in the Grid Properties editor only.

   - **IPv6 Properties**
     - **Fixed Address Lease**: Select Capture hostname and lease time when assigning Fixed Addresses. The appliance displays the host name, and the start and end time of each fixed address lease in the Current Leases panel. If there are multiple records (AAAA, host, and lease) for the IP address, it also displays the information for the records. This option is available in the Grid Properties editor only.

3. Save the configuration.
Configuring DHCP Logging

If you have a syslog server operating on your network, you can specify in which facility you want the server to display the DHCP logging messages. You can also select the Grid member on which you want to store the DHCP lease history log, as described in the next section *Configuring the Lease Logging Member*. 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 -> member check box, and then click the Edit icon.

2. In the DHCP Properties editor, select the Logging Basic tab and complete the following:
   - **Syslog Facility**: From the drop-down list, select the facility that is used to tag syslog messages from the DHCP server. This facility can be used to filter messages on a central syslog server.

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

Configuring the Lease Logging Member

Logging DHCP lease events makes significant CPU demands, especially when there is heavy DHCP activity. Therefore, Infoblox strongly recommends that you designate a Grid member other than the master as a logging member whenever possible. Another way to manage the increased load that logging introduces is to log selectively per Grid member. For example, you might want to log DHCP leases for members serving critical parts of your network and not keep historical logs for members serving other parts.

*Figure 20.4 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. Save the configuration and click **Restart** if it displays at the top of the screen.

   **Note**: You cannot configure vNIOS Grid members on Riverbed as DHCP lease history logging members.

4. For information about viewing current leases, see **Viewing Current Leases** on page 746
You can configure Infoblox DHCP servers to publish DHCP data to an IF-MAP server. The IF-MAP server takes real-time information from different sources and stores it in a shared database from which clients can retrieve information about network devices, their status and activities. For details about the IF-MAP protocol, refer to http://www.trustedcomputinggroup.org. For information about the Infoblox IF-MAP server, refer to the Infoblox Administrator Guide for Infoblox Orchestration Server.

Each Infoblox DHCP server in a Grid can function as an IF-MAP client, with the ability to publish lease information to an IF-MAP server. For information about how to configure an IF-MAP client, see Configuring Members as IF-MAP Clients on page 616. You can configure the client to publish ip-mac and ip-duid (for DHCPv6 leases) metadata at the Grid and member levels. You can also configure the client to publish metadata for specific leases by overriding the Grid or member publishing settings at the network (IPv4 and IPv6) or range (IPv4 only) level. The DHCP server sends updates to the IF-MAP server using the XML format and SOAP/HTTPS bindings specified in IF-MAP v1.1r5 and v2.0r26. The DHCP server supports the IF-MAP 2.0 protocol by default. You can also enable the support for IF-MAP 1.1, as described in Configuring a Grid to Support IF-MAP.

When the DHCP server grants an IPv4 lease and sends the DHCPACK packet to the DHCP client, it updates the link in the IF-MAP server between the leased IP address and client MAC address with ip-mac metadata with the following attributes: start-time, end-time, and dhcp-server. The dhcp-server attribute contains the DHCP server hostname. The ip-mac metadata is attached to a link with:

- An ip-address identifier with the type attribute set to IPv4, a value attribute that contains the leased IP address, and the administrative-domain attribute set to the network view to which the IP address belongs.
- A mac-address identifier with a value attribute that contains the client MAC address. It does not have the administrative-domain attribute.

When the DHCP server grants an IPv6 lease and sends the Reply message to the DHCP client, it updates the link in the IF-MAP server between the leased IP address and client DHCP Unique Identifier (DUID) with ip-duid metadata that contains the following attributes: start-time, end-time, and dhcp-server. The dhcp-server attribute contains the DHCP server hostname. The ip-duid metadata is attached to a link with:

- An ip-address identifier with the type attribute set to IPv6, a value attribute that contains the leased IP address, and the administrative-domain attribute set to the network view to which the IP address belongs.
- A duid identifier with a value attribute that contains the client DUID. It does not have the administrative-domain attribute.

The Infoblox DHCP server also publishes data when an IPv4 or IPv6 lease changes. When a lease is released or when an active lease expires, the DHCP server sends a “publish delete” request to the IF-MAP server.

You can define how the IF-MAP server handles the existing ip-mac and ip-duid information before the DHCP client sends the next update. For example, you can specify the IF-MAP server to always delete existing ip-mac and ip-duid information before the next update. For information, see Deleting Existing Data Before Publishing on page 620.

Following are the tasks to enable DHCP servers in a Grid to function as IF-MAP clients:

1. Enable IF-MAP in the Grid and specify the URL and port of the IF-MAP server, as described in Configuring a Grid to Support IF-MAP on page 616.
2. Optionally, enable the validation of the IF-MAP server certificate and import the CA certificate, as described in Validating the IF-MAP Server Certificate on page 616.
3. Enable IF-MAP on each Grid member and specify an authentication method the member uses to connect to the IF-MAP server, as described in Configuring Members as IF-MAP Clients on page 616.
4. Optionally, override publishing settings at the member, network, or range level, as described in Overriding IF-MAP Publishing Settings on page 619.

You can also delete DHCP data published by a specific member, or define how the IF-MAP server deletes existing DHCP data before a client publishes an update. For information, see Deleting Data from the IF-MAP Server on page 619.
Configuring a Grid to Support IF-MAP

1. From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar.
2. In the Grid DHCP Properties editor, click Toggle Advanced Mode.
3. Click the IF-MAP tab, and then complete the following:
   - Enable IF-MAP: Select this check box to enable the IF-MAP service for the Grid. Note that you must enable the IF-MAP service in order to enable or disable publishing at the Grid, member, network, or range level.
   - IF-MAP Server URL: Enter the URL of the IF-MAP server to which the Grid members publish DHCP data. The URL must begin with 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.
   - Enable IF-MAP publishing: Select this check box to enable IF-MAP publishing for the Grid. When you select this, IF-MAP publishing is enabled for all members, networks (IPv4 and IPv6), and DHCP ranges (IPv4 only). You can override the Grid property at a specific level to control the ip-mac and ip-duid metadata you want the client to publish for specific leases. For information, see Overriding IF-MAP Publishing Settings on page 619.
   - IF-MAP Protocol Version: Select the IF-MAP protocol version you want the IF-MAP client to use to connect to the IF-MAP server. The default is IF-MAP 2.0.
4. Save the configuration and click Restart if it displays at the top of the screen.
5. You can also configure how the IF-MAP server deletes existing metadata before the IF-MAP client publishes another update. For information, see Deleting Data from the IF-MAP Server on page 619.

Validating the IF-MAP Server Certificate

You can configure the IF-MAP client to validate the IF-MAP server certificate before the client establishes a connection or performs IF-MAP transactions. To validate an IF-MAP server certificate, you must first import the certificate of the CA that signs the IF-MAP server certificate.

To configure the IF-MAP client to validate the IF-MAP server certificate:

1. From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar.
2. In the Grid DHCP Properties editor, click Toggle Advanced Mode.
3. Click the IF-MAP tab and complete the following:
   - Enable IF-MAP: Select this check box to enable the IF-MAP service for the Grid.
   - Enable IF-MAP server certificate validation: Select this check box to enable the validation of the IF-MAP server certificate, and then click Import to import the CA certificate. In the Upload dialog box, click Select to navigate to the certificate, and then click Upload. You can also copy and paste the CA certificate here.
4. Save the configuration and click Restart if it displays at the top of the screen.

Configuring Members as IF-MAP Clients

To configure a member to be an IF-MAP client, you must first enable IF-MAP on the member and then configure a client authentication method. The IF-MAP client can authenticate itself to the IF-MAP server through user name and password credentials or digital certificate. Note that each member must have unique credentials or certificates. You cannot use the same credentials or certificates on multiple members. The appliance supports only one CA-signed certificate on each member. If you want to use a roll-over certificate, you must replace the existing certificate and restart services on the member.

To enable an appliance to function as an IF-MAP client:

1. From the Data Management tab, select the DHCP tab -> Members tab -> member check box, and then click the Edit icon.
2. In the Member DHCP Properties dialog box, click Toggle Advanced Mode.
3. Click the IF-MAP tab and complete the following:
   — **Enable IF-MAP**: Select this check box to enable the IF-MAP service on the member. Note that you must enable the IF-MAP service in order to enable or disable publishing at the network and range levels.
   — **Authentication**: Select one of the following authentication methods:
     — **Certificate**: Select this to use the IF-MAP client certificate for client authentication. You must already have a certificate configured for the member before you can select and save this configuration. For information about creating a client certificate, see Creating IF-MAP Client Certificates on page 617.
     — **Basic**: Select this to use username and password credentials for IF-MAP client authentication. Complete the following:
       • **Username**: Enter the username the member uses to connect to the IF-MAP server. This username must have been configured as a valid username on the IF-MAP server. Each member must have its own username.
       • **Password**: Enter the password the member uses to connect to the IF-MAP server.
       • **Confirm Password**: Enter the password again.
   — **Enable IF-MAP publishing**: Click Override to override the Grid setting. Select this check box to enable IF-MAP publishing for all the networks that are served by this member. Ensure that you enable IF-MAP at either the Grid or member level in order to enable IF-MAP publishing for all networks.

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

**Creating IF-MAP Client Certificates**

Before you can select “Certificate” as the client authentication method, you must first create a certificate for the specified member.

You can do one of the following to generate an IF-MAP client certificate:

- Generate a self-signed certificate and save it. For information, see Generating Self-Signed Certificates.
- Request a CA (Certificate Authority) signed certificate. When you receive the certificate from the CA, upload it to the member that you configure as an IF-MAP client. For information, see Generating Certificate Signing Requests on page 618.

**Generating Self-Signed Certificates**

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

To generate a self-signed certificate:

1. From the Data Management tab, select the DHCP tab -> Members tab -> member check box, and then click IF-MAP Client Certificate -> Generate Self-signed Certificate from the Toolbar.
2. In the Generate Self-Signed Certificate dialog box, complete the following:
   — **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 member. 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.
3. Click **OK**.
4. If the appliance already has an existing client certificate, the new certificate replaces the existing one. In the *Replace IF-MAP Certificate Confirmation* dialog box, click **Yes**.

### Generating Certificate Signing Requests

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

To generate a CSR:

1. From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **member** check box, and then click **IF-MAP Client Certificate** -> **Create Signing Request** from the Toolbar.
2. In the **Create Certificate Signing Request** dialog box, enter the following:
   - **Key Size**: Select **2048** or **1024** for the length of the public/private key pair.
   - **Common Name**: Specify the domain name of the member. You can enter the FQDN of the appliance.
   - **Organization**: Enter the name of your company.
   - **Organizational Unit**: Enter the name of your department.
   - **Locality**: Enter a location, such as the city or town of your company.
   - **State or Province**: Enter the state or province.
   - **Country Code**: Enter the two-letter code that identifies the country, such as US.
   - **Admin E-mail Address**: Enter the email address of the appliance administrator.
   - **Comment**: Enter information about the certificate.
3. Click **OK**.

### Uploading Certificates

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

To import a certificate:

1. From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **member** check box, and then click **IF-MAP Client Certificate** -> **Upload Certificate** from the Toolbar.
2. Navigate to where the certificate is located and click **Open**.
3. If the appliance already has an existing IF-MAP client certificate, the new certificate replaces the existing one. In the *Replace IF-MAP Certificate Confirmation* dialog box, click **Yes**.

### Downloading Certificates

You can download the current certificate or a self-signed certificate.

To download a certificate:

1. From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **member** check box, and then click **IF-MAP Client Certificate** -> **Download Certificate** from the Toolbar.
2. Navigate to where you want to save the certificate, enter the file name, and then click **Save**.
Overriding IF-MAP Publishing Settings

When you enable IF-MAP publishing at the Grid level, all members, networks (IPv4 and IPv6), and DHCP ranges (IPv4 only) in the Grid inherit the same setting. To control which ip-mac and ip-duid metadata is published for specific leases that belong to a specific network or address range, you can override the Grid settings at a specific member, network, or range level. Note that you must first enable the IF-MAP service at the Grid and member levels in order to enable or disable IF-MAP publishing at other levels. For example, if you want the DHCP server to publish IF-MAP data for specific leases in a specific network that is served by a specific member, you must first enable the IF-MAP service at the Grid and member levels, as described in Configuring a Grid to Support IF-MAP on page 616. Then, you can enable IF-MAP publishing at the range level, as described in this section.

Though you can configure and save the settings of IF-MAP publishing any time at any level, the publishing does not actually happen unless the IF-MAP service is enabled at the Grid or member level. If a network or DHCP range is served by a specific member and you want to enable IF-MAP publishing for the network or range, you must first enable the IF-MAP service for the specified member.

To override IF-MAP publishing settings:

1. **Member**: From the Data Management tab, select the DHCP tab -> Members tab -> member check box, and then click the Edit icon.
2. **Network**: From the Data Management tab, select the DHCP tab -> Networks tab -> network check box, and then click the Edit icon.
3. **DHCP Range**: From the Data Management tab, select the DHCP tab -> Networks tab -> network -> addr_range check box, and then click the Edit icon.
4. In the editor, click **Toggle Advanced Mode**, and then click the IF-MAP tab.
5. Click **Override** and complete the following:
   - **Enable IF-MAP Publishing**: Select this check box to instruct the DHCP server to publish metadata to the IF-MAP server when the IF-MAP service is enabled for the Grid or member. Clear this check box so the DHCP server does not publish metadata to the server.

Deleting Data from the IF-MAP Server

The appliance allows you to delete IF-MAP data from the IF-MAP server. You can delete all IF-MAP data published by a specific member. You can also define how the IF-MAP server handles the deletion of existing metadata before the IF-MAP client publishes another update.

Deleting all data

You can delete all IF-MAP data published by a specified member. To delete data published by all members in a Grid, you must delete data for each member individually.

To delete IF-MAP data published by a member from the IF-MAP database:

1. From the Data Management tab, select the DHCP tab -> Members tab, and then click Clear -> IF-MAP Data from the Toolbar.
2. In the Purge IF-MAP Data dialog box, click Select Member to select a member. If there are multiple members, Grid Manager displays the Member Selector dialog box from which you can select one. Click the member name in the dialog box, and then click Purge to delete all the DHCP data published by the Grid member. You can also click Clear to clear the displayed member and select a new one.
Deleting Existing Data Before Publishing

You can define how the IF-MAP server deletes existing metadata before an IF-MAP client publishes new data. You can configure the IF-MAP client to instruct the server to always delete existing data, never delete it, or delete the data before a specified time period.

To define how the IF-MAP server deletes DHCP data before the next publish:

1. From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar.
2. In the Grid DHCP Properties editor, click Toggle Advanced Mode.
3. Click the IF-MAP tab and complete the following:
   - Enable IF-MAP: Select this check box to enable the IF-MAP service.
   - Delete existing metadata: You can define how the IF-MAP server deletes the existing metadata before the IF-MAP client publishes new data. Select one of the following:
     - Always delete: Select this to always delete existing metadata before the IF-MAP client publishes updates. This is the default.
     - Do not delete: Select this to never delete the existing metadata before the IF-MAP client publishes updates.
     - Earlier than: Select this to delete metadata that was published before a given time before the IF-MAP client publishes updates. When you select this option, enter a time value, and then select a time unit from the drop-down list.
4. Save the configuration and click Restart if it displays at the top of the screen.

Starting DHCP Services on a Member

The DHCP service is disabled by default. After you complete the DHCP configuration, you can start DHCP service on a member. To enable the member to provide DHCPv6 service as well, you must start the DHCP service and then enable the DHCPv6 service on the member. In addition, you must specify the DHCP Unique Identifier (DUID) of the member. IPv6 clients use DUIDs to identify the source of the DHCP messages from servers.

To start DHCP service on a member:

1. From the Data Management tab, select the DHCP tab -> Members tab -> member check box.
2. Expand the Toolbar and click Start.
3. In the Start Member DHCP Service dialog box, click Yes.
4. Grid Manager starts DHCP on the selected member.

You can stop DHCP service on a member by selecting the member check box and click Stop from the Toolbar.

To enable DHCPv6 service on the member:

1. From the Data Management tab, select the DHCP tab -> Members tab -> member check box.
2. In the Member DHCP Properties editor, select the General Basic tab.
3. In the IPv6 Properties section, do the following:
   - Server DUID: Enter the DUID of the member.
   - Enable DHCPv6 Service: Select this check box.
4. Save the configuration.
Viewing DHCP Member Status

You can view DHCP member status after you configure DHCP properties and start or stop DHCP services on a member.

To view member status:
1. From the Data Management tab, select the DHCP tab -> Members tab -> Members section.
2. Grid Manager displays the following information:
   - **Name**: The name of the Grid member.
   - **Status**: The status of the DHCP services on the member. This can be one of the following:
     - **Not Running**: DHCP services have not been started on the member.
     - **Running**: The DHCP services are running properly on the member.
     - **Warning**: The member is connecting or synchronizing with its Grid Master.
     - **Error**: The member is offline, is not licensed (that is, it does not have a DNSOne license with the Grid upgrade that permits Grid membership), is upgrading or downgrading, or is shutting down.
   - **Comment**: The information you entered for the member.
   - **IPv4 DHCP Utilization**: The percentage of the total IPv4 DHCP utilization of the member. This is the percentage of the total number of DHCP hosts, fixed addresses, reservations, and leases assigned to the member versus the total number of IP addresses (excluding IP addresses in the exclusion range) and all DHCP objects assigned to the member. Note that only enabled objects are included in the calculation. The appliance updates the utilization data every 15 minutes. The appliance displays the utilization data in one of the following colors:
     - Red: The DHCP resources are 100% utilized.
     - Yellow: The utilization percentage is over the effective high watermark threshold.
     - Blue: The utilization percentage is below the effective low watermark threshold.
     - Black: The utilization percentage is at any number other than 100%, or within the effective thresholds.
   - **Site**: The site to which the member belongs. This is one of the predefined extensible attributes.

You can select the following additional columns for display:
   - **Address**: The IP address of the member.
   - **Static Addresses**: The number of static IP addresses.
   - **Dynamic Addresses**: The number of dynamically assigned IP addresses.
   - **IF-MAP Connection**: The status of the IF-MAP service connection on the member. This can be one of the following:
     - **Stopped**: The DHCP or IF-MAP service on the member is stopped, or the IF-MAP service is not enabled.
     - **Running**: The IF-MAP client is connected to the IF-MAP server and the IF-MAP service is running properly.
     - **Failed**: The IF-MAP client cannot publish data to the IF-MAP server due to some errors.
     - **Warning**: Some non-fatal errors occurred. The IF-MAP client attempts to reconnect to the server.

**Note**: You can mouse over on the informational icon next to the status to view detailed information, including the status description and the timestamp when the status initially changed.

   - **IF-MAP Last Update**: The timestamp the status of the IF-MAP service was last updated. For example, if the IF-MAP connection status is **Running** and this field shows 2011-11-20 12:30:42 EST, it means that an IF-MAP operation, such as a publish, was last completed on November 20, 2011 at 12:30:42 Eastern Standard Time.
To view status information about the IF-MAP connection on an independent appliance, from the Data Management tab -> DHCP tab, click System DHCP Properties from the toolbar. The appliance displays the following:

- **IF-MAP Connection**: The status of the IF-MAP service on the independent appliance. A color icon associated with the connection status appears before the status.
- **IF-MAP Connection Information**: Detailed information about the status. On a Grid member, this information appears when you mouse over on the informational icon.
- **IF-MAP Last Update**: The timestamp when the status of the IF-MAP service last changed.

**Note**: For more information about these fields, see descriptions about Grid member status in this section.

You can view detailed information about a specific member by clicking the member link. Grid Manager displays the following information about the selected member:

- **Network**: The network assigned to the member.
- **Comment**: The information about the network.
- **IPv4 DHCP Utilization**: The percentage of the DHCP usage of the network. This is the percentage of the total number of fixed addresses, reservations, hosts, and active leases on the network over the total IP addresses in the range, excluding the number of addresses on the network. Note that only enabled objects are included in the calculation.
- **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 50.

### Viewing DHCP Configuration Files

You can view the IPv4 and IPv6 DHCP configuration of a selected member. The format of the configuration file depends on the browser you use.

To view the DHCP configuration of a selected member:

1. From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box.
2. Expand the Toolbar, select View DHCP Configuration, and then select either IPv4 or IPv6. Grid Manager displays the IPv4 or IPv6 DHCP configuration of the selected member in a new browser. You can print and save the file using the corresponding functions in your browser.
Chapter 21 Managing DHCP Templates

This chapter explains how to configure and manage IPv4 and IPv6 DHCP templates. It contains the following sections:

- About DHCP Templates on page 624
- About IPv4 DHCP Templates on page 625
  - About IPv4 Range Templates on page 625
  - About IPv4 Fixed Address/Reservation Templates on page 627
  - About IPv4 Network Templates on page 628
  - Configuration Example: Creating an IPv4 Network Using a Template on page 631
- About IPv6 DHCP Templates on page 633
  - About IPv6 Range Templates on page 634
  - About IPv6 Fixed Address Templates on page 635
  - About IPv6 Network Templates on page 636
- Viewing Templates on page 638
- Deleting Templates on page 638
About DHCP Templates

A template contains a set of predefined properties that you use to create IPv4 and IPv6 DHCP objects. It is metadata that you can modify and reuse. Using a template enables you to create objects in a quick and consistent way. You can define the object properties once in a template, and then create multiple objects that inherit their properties from the template. For example, you can create a network template that has a fixed netmask of /24 and extensible attribute “State” set to California. You can then use the template to create networks in California that contain /24 netmasks.

You can also modify and delete a template. Note that modifying or deleting a template does not affect existing objects created based on the template. You must be a superuser or have read/write permissions to add, modify, or delete a template. A superuser can set other admin group privileges on templates. For information, see Administrative Permissions for IPv4 or IPv6 DHCP Templates on page 166. You can also define extensible attributes for these templates when you create them. For information, see Using Extensible Attributes on page 265.
About IPv4 DHCP Templates

You can use templates to create DHCP IPv4 ranges, fixed addresses, reservations, roaming hosts, and networks. You can create the following IPv4 templates:

- A DHCP range template, containing DHCP range settings, such as the total number of IP addresses allocated to a range. You can add a DHCP range template to a network template. For information, see About IPv4 Range Templates on page 625.

- A fixed address/reservation template, containing information for creating fixed addresses, reservations, or roaming hosts. You can add a fixed address/reservation template to a network template. For information, see About IPv4 Network Templates on page 628.

- A network template, containing basic network properties for creating networks. It is also a container that holds your DHCP range templates and fixed address/reservation templates. When you create a network using a network template, the network inherits the properties of the range and fixed address/reservation templates. You can create a network in any network view using a network template. For information, see About IPv4 Network Templates on page 628.

Because you can potentially add DHCP range and fixed address/reservation templates to a network template, create the DHCP range and fixed address/reservation templates before you create a network template. For information, see Configuration Example: Creating an IPv4 Network Using a Template on page 631.

About IPv4 Range Templates

When you create an IPv4 range template, the start and end address fields are based on the specified offset from the network start address and the number of IP addresses in the range. After you create a DHCP range template, you can configure additional properties such as exclusion ranges and DHCP filters, as described in Modifying IPv4 Range Templates on page 626. Then when you use the template to create a DHCP range, the range inherits the properties of the template. You can also include a DHCP range template in a network template to automatically create a DHCP range when you use that network template.

Adding IPv4 Range Templates

To create an IPv4 DHCP range template:

1. From the Data Management tab, select the DHCP tab -> Templates tab, and then expand the Toolbar and click Add -> Templates -> Range -> IPv4.

2. In the Add IPv4 Range Template wizard, do the following:
   - **Name**: Enter a name that helps identify the DHCP range template. For example, enter Region 1 IT if you want to use this template to create DHCP ranges for the IT department in Region 1.
   - **Offset**: An offset in a DHCP range template determines the starting IP address of the range. The appliance adds the offset value you enter here to the start IP address of the network in which you create a DHCP range using this template. That IP address becomes the start IP address of the DHCP range. For example, 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.

3. Click **Next** and select one of the following to provide DHCP services for the range:
   - **None (Reserved Range)**: Select this if you want to reserve this address range for static hosts. Addresses in this range cannot be allocated as dynamic addresses. You can allocate the next available IP from this range to a static host. This is selected by default.
   - **Grid Member**: Click Select and choose a Grid member from the drop-down list.
   - **Failover Association**: Click Select and choose a failover association. Only failover associations that provide DHCP services in the network view of the DHCP range appear in the drop-down list.
Managing DHCP Templates

— **Microsoft DHCP Server**: Click Select and choose a Microsoft server from the drop-down list. The drop-down list displays only the servers that are associated with the network to which the DHCP range belongs.

4. Click **Next** to configure or override DHCP options as described in *Defining Basic IPv4 Options* on page 597.

5. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see *Using Extensible Attributes* on page 265.

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

Modifying IPv4 Range Templates

After you use the wizard to create an IPv4 DHCP range template, you can set additional properties for the template. Following are some guidelines:

- In the **DHCP Options** tab of a DHCP range template, the broadcast address is an address offset number rather than a broadcast IP address; network router addresses are offset numbers as well.

  An offset in a DHCP range template indicates the starting IP address of the DHCP range object created from the template. For example, you can create a network template called *test_network_template* and a DHCP range template *test_range_template* linked to this network template. If the *test_range_template* has an offset value 10, when you create a 10.0.0.0/8 network using the *test_network_template*, the appliance creates a DHCP range with the starting IP address 10.0.0.10. If you create a 20.0.0.0/8 network using the *test_network_template*, the appliance creates a DHCP range with the starting IP address 20.0.0.10.

- For the exclusion range in the template, the start and end addresses are determined by the number of offsets in the DHCP range template's start address and the number of IP addresses in the exclusion range. For more information about exclusion ranges, see *About DHCP Ranges* on page 574.

To modify and set properties for a DHCP range template:

1. From the **Data Management** tab, select the **DHCP** tab -> **Templates** tab -> **template** check box, and then click the **Edit** icon.

2. The **DHCP Range Template** editor contains the following tabs from which you can modify data:
   - **General**: Modify general information described in *Adding IPv4 Range Templates* on page 625.
   - **Member Assignment**: Change the Grid member, failover association, or Microsoft server that provides DHCP services for this template. You can also add or delete a member or failover association. For information, see *Adding IPv4 Address Ranges* on page 650.
   - **IPv4 DHCP Options**: Keep the inherited DHCP options or override them and enter unique settings for the template. For information, see *Defining Basic IPv4 Options* on page 597.
   - **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 265.
   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see *About Administrative Permissions* on page 120.

3. Optionally, you can click **Toggle Expert Mode** to display the following tabs from which you can modify data:
   - **IPv4 DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the template. For information, see *Enabling DDNS for IPv4 and IPv6 DHCP Clients* on page 484.
   - **IPv4 BOOTP/PXE**: Keep the inherited BOOTP properties or override them and enter unique settings for the template. For information, see *Configuring IPv4 BOOTP and PXE Properties* on page 594.
   - **Exclusion Ranges**: Configure a range of IP addresses that the appliance does not use for dynamic address assignments. Complete the following:
     - **Offset**: An offset for an exclusion range determines the start IP address of the exclusion range. The appliance adds the offset value you enter here to the start IP address of the DHCP range created using this template. That IP address becomes the start IP address of the exclusion range.
     - **Number of Addresses**: Enter the number of IP addresses to be included in the exclusion range.
     - **Comment**: Enter useful information about the exclusion range.
— **IPv4 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 603.

— **IPv4 Filters:** Add DHCP filters to the Class Filter List and Logic Filter List. For information, see *Applying Filters to DHCP Address Ranges* on page 692.

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

**Note:** Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

---

**About IPv4 Fixed Address/Reservation Templates**

You can use an IPv4 fixed address/reservation template to create fixed addresses, reservations and roaming hosts. When you create an IPv4 fixed address/reservation template, you can specify an offset and number of addresses. This is used when you include the template in a network template. When you include a fixed address/reservation template in a network template, the DHCP server automatically creates reservations based on the offset and number of addresses you specified in the fixed/address reservation template. It does not create fixed addresses.

After you create a fixed address/reservation template using the wizard, you can configure additional properties as described in *Modifying IPv4 Fixed Address/Reservation Templates* on page 628. Then when you use the template to create a fixed address, it inherits the properties of the template.

**Adding IPv4 Fixed Address/Reservation Templates**

To create an IPv4 fixed address/reservation template:

1. From the **Data Management** tab, select the **DHCP** tab -> **Templates** section.
2. Click the Add drop-down list and select **IPv4 Fixed Address/Reservation Template**.
3. In the **Add IPv4 Fixed Address/Reservation Template** wizard, enter the following:
   - **Name:** Enter a name that helps identify the fixed address/reservation template. For example, you can enter **HP Printer** when you create a template that contains settings for assigning fixed addresses or reservations to HP printers.
   - **Comment:** Optionally, enter additional information about the template.

   In the **Optional Settings For Range of Objects** section, do the following:
   - **Offset:** An offset in a fixed address/reservation template determines the start IP address of the object created from the template. The appliance adds the offset value you enter here to the start IP address of the network in which you create objects using this template. That IP address becomes the start IP address of the object.
   - **Number of Addresses:** Enter the number of IP addresses to be used as fixed addresses, reservations, or roaming hosts.

   **Note:** The appliance uses the offset and number of addresses only when this template is used in a network template.

4. Click **Next** to configure or override DHCP options as described in *Defining Basic IPv4 Options* on page 597.
5. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see *Using Extensible Attributes* on page 265.
6. Save the configuration and click **Restart** if it appears at the top of the screen.
Modifying IPv4 Fixed Address/Reservation Templates

To modify a fixed address/reservation template:

1. From the Data Management tab, select the DHCP tab -> Templates tab -> template check box, and then click the Edit icon.

2. The Fixed Address/Reservation Template editor contains the following tabs from which you can modify data:
   - General: Modify general information for the template as described in Adding IPv4 Fixed Address/Reservation Templates on page 627.
   - IPv4 DHCP Options: Keep the inherited DHCP options or override them and enter unique settings for the template. For information, see Defining Basic IPv4 Options on page 597.
   - 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 265.
   - Permissions: This tab appears only if you belong to a superuser admin group. For information, see About Administrative Permissions on page 120.

3. Optionally, you can click Toggle Expert Mode to display the following tabs from which you can modify data:
   - IPv4 DDNS: Keep the inherited DDNS settings or override them and enter unique settings for the template. For information, see Enabling DDNS for IPv4 and IPv6 DHCP Clients on page 484.
   - IPv4 BOOTP/PXE: Keep the inherited BOOTP properties or override them and enter unique settings for the template. For information, see Configuring IPv4 BOOTP and PXE Properties on page 594.

   Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

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

About IPv4 Network Templates

You can create IPv4 network templates to facilitate network configuration. You can use network templates to create networks in any network view. When you create a network template, you do not specify a network address. You enter the network address when you create an actual network from the template. You can specify a netmask or allow the user to define the netmask when they create the actual network.

A network template is useful for setting up a network with fixed addresses and DHCP ranges already defined. You can add DHCP range or fixed address/reservation templates to a network template. Once the fixed address and DHCP range information is set up, the network template contains a range template list and a fixed address/reservation template list.

Adding IPv4 Network Templates

To create a network template:

1. From the Data Management tab, select the DHCP tab -> Templates section.
2. Click the Add drop-down list and select IPv4 Network Template.
3. In the Add IPv4 Network Template wizard, do the following:
   - Name: Enter a name that helps identify the network template. For example, you can enter Class C if you want to configure the template for creating Class C networks.
   - Netmask: Select one of the following options:
     - Fixed: Select this and adjust the netmask slider to a fixed netmask for this network template. When you select this option, users cannot specify another netmask when they use this template to create a network. For example, if you select /24 as the fixed netmask, all networks created using this template have a /24 netmask.
     - Allow User to Specify Netmask: Select this to allow users to specify the subnet mask when creating networks using this template.
   - Comment: Optionally, enter additional information about the template.
— **Automatically Create Reverse-Mapping Zone**: This function is enabled if the fixed netmask of the template equals /8, /16, and /24, or if you select the **Allow User to Specify Netmask** option. Select this if you want the appliance to automatically create the corresponding reverse-mapping zone for the networks created using this template. A reverse-mapping zone is an area of network space for which one or more name servers have the responsibility for responding to address-to-name queries. These zones are created in the DNS view assigned to receive dynamic DNS updates at the network level.

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.

   or

   — **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 IPv4 address range and fixed address/reservation templates in the network template. Note that when you select a fixed address/reservation template, only reservations, not fixed addresses, are created for networks created using this template. You cannot add a fixed address/reservation template that does not contain an offset value or a total number of IP addresses for a range.

   a. Click the Add icon.

   b. In the **DHCP Template Selector** dialog box, choose the template that you want to include in this network template. You can choose a DHCP range or fixed address/reservation template. Use SHIFT+click and CTRL+click to select multiple templates.

   c. Click the Select icon.

   You can delete a template from the table by selecting it and clicking the Delete icon.

6. Click **Next** to configure or override DHCP options as described in **Defining Basic IPv4 Options** on page 597.

7. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see **Using Extensible Attributes** on page 265.

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

**Modifying IPv4 Network Templates**

To modify a network template:

1. From the **Data Management** tab, select the **DHCP** tab -> **Templates** tab -> template check box, and then click the **Edit** icon.

2. The **Network Template** editor contains the following tabs from which you can modify data:

   — **General**: Modify general information described in **Adding IPv4 Network Templates** on page 628.

   — **Member Assignment**: Change the Microsoft servers or Grid members that provide DHCP services for this template. For information, see **Adding IPv4 Networks** on page 643.

   — **Templates**: Add or delete DHCP range and fixed address/reservation templates. For information, see **About IPv4 Range Templates** on page 625 and **About IPv4 Fixed Address/Reservation Templates** on page 627.

   — **IPv4 DHCP Options**: Keep the inherited DHCP options or override them and enter unique settings for the template. For information, see **Defining Basic IPv4 Options** on page 597.
— **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 265.

— **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see *Managing Permissions* on page 128.

3. Optionally, you can click **Toggle Expert Mode** to display the following tabs from which you can modify data:
   — **IPv4 DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the template. For information, see *Enabling DDNS for IPv4 and IPv6 DHCP Clients* on page 484.
   — **IPv4 BootP/PXE**: Keep the inherited BOOTP properties or override them and enter unique settings for the template. For information, see *Configuring IPv4 BOOTP and PXE Properties* on page 594.
   — **IPv4 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 603.

   Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Save the configuration and click **Restart** if it appears at the top of the screen.
**Configuration Example: Creating an IPv4 Network Using a Template**

This example describes how to create a /24 network template and how to use the template to create a 192.168.2/24 network with the following configurations:

- First address 192.168.2.1 is reserved for the router
- Next 10 addresses (192.168.2.2 to 192.168.2.11) reserved for servers
- Next 10 addresses (192.168.2.12 to 192.168.2.21) reserved for printers
- Next 10 addresses (192.168.2.22 to 192.168.2.31) assigned as fixed addresses
- 100 addresses (192.168.2.32 to 192.168.2.131) reserved for workstations. The appliance assigns these dynamically.
- 10 addresses (192.168.2.42 to 192.168.2.51) are in an exclusion range. If you assigned static addresses to certain hosts in the middle of an address range template, you can exclude the addresses from the address range template so the appliance does not assign these IP addresses to clients.

*Figure 21.1* illustrates the configurations of the 192.168.2/24 network using the network template you create:

*Figure 21.1 Creating a Network Using a Template*

Use the following steps to create the sample network template (shown in *Figure 21.1*).

1. Create the following DHCP range templates. For information, see *Adding IPv4 Range Templates* on page 625.
   - **Server template** with the following values:
     - **Name**: Servers
     - **Offset**: 2
     - **Number of Addresses**: 10
     - **Comment**: Address range 2 to 11 for Servers
   - **Printer template** with the following values:
     - **Name**: Printers
     - **Offset**: 12
     - **Number of Addresses**: 10
     - **Comment**: Address range 12 to 21 for printers.
— Workstation template with the following values:
  — **Name**: Workstations
  — **Offset**: 32
  — **Number of Addresses**: 100
  — **Comment**: Address range 32 to 131 for DHCP on workstations

— Exclusion range with the following values. You must modify the *Workstations* template to add the exclusion range. For information, see *Modifying IPv4 Range Templates* on page 626.
  — **Name**: Exclusion
  — **Offset**: 42
  — **Number of Addresses**: 10
  — **Comment**: Excluding addresses 42 to 51 from the DHCP range 32 to 131.

2. Create a fixed address/reservation template with the following values. For information, see *Adding IPv4 Fixed Address/Reservation Templates* on page 627.
  — **Name**: Router
  — **Comment**: Fixed address template
  — **Offset**: 1
  — **Number of Addresses**: 1

3. Create a fixed address/reservation template with the following values. For information, see *Adding IPv4 Fixed Address/Reservation Templates* on page 627.
  — **Name**: myFixedAddress
  — **Comment**: Fixed address template
  — **Offset**: 22
  — **Number of Addresses**: 10

4. Create a network template with the following values. For information, see *Adding IPv4 Network Templates* on page 628.
  — **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 643.
  — **Address**: Enter the IP address 192.168.2.0 of the network that you want to create using the template.
  — **Select template**: Select the network template *myNetworkTemplate*.

9. To verify your configuration, from the *Data Management* tab, select the *DHCP* tab -> *Templates* tab. Select *myNetworkTemplate* and click the Edit icon. In the *Network Template* editor, click the *Templates* tab. The Grid Manager displays the DHCP range templates and fixed address templates.

10. Click *Restart* to restart services.
About IPv6 DHCP Templates

You can use templates to create DHCP IPv6 ranges, fixed addresses, roaming hosts, and networks. You can create the following IPv6 templates:

- A DHCP range template that specifies an offset and the total number of addresses in a range. You can add a DHCP range template to a network template. For more information, see About IPv6 Range Templates on page 634.

- A fixed address template, containing information for creating fixed addresses and roaming hosts. You can add a fixed address template to a network template. For information, see About IPv6 Fixed Address Templates on page 635.

- A network template, containing basic network properties for creating networks. It is also a container that holds your DHCP range templates and fixed address/reservation templates. When you create a network using a network template, the network inherits the properties of the range and fixed address/reservation templates. You can create a network in any network view using a network template. For information, see Adding IPv6 Network Templates on page 636.

Because you can potentially add DHCP range and fixed address/reservation templates to a network template, create the DHCP range and fixed address/reservation templates before you create a network template.
About IPv6 Range Templates

You can create range templates to specify an offset and the number of addresses allocated to a range. Note that you cannot create templates for prefix-delegated ranges because the start or end prefix can be outside of the subnet address boundary.

After you create a DHCP range template, you can configure additional properties such as exclusion ranges and DHCP properties, as described in Managing DHCP Templates. Then when you use the template to create a DHCP range, the range inherits the properties of the template. You can also include a DHCP range template in a network template to automatically create a DHCP range when you use that network template.

Adding IPv6 Range Templates

To create an IPv6 range template:

1. From the Data Management tab, select the DHCP tab -> Templates tab.
2. Click the Add drop-down menu and select IPv6 DHCP Range Template.
3. In the Add IPv6 Range Template wizard, complete the following:
   - **Name**: Enter a name that helps identify the IPv6 DHCP range template.
   - **Offset**: An offset in a DHCP range template determines the starting IP address of the range. The appliance adds the offset value you enter here to the start IP address of the network in which you create a DHCP range using this template. That IP address becomes the start IP address of the DHCP range. For example, you specify an offset value of 10 for the 2001:db8:1263:/48 network using the DHCP range template, the appliance creates a range with the start address 2001:db8:1263:0:0:0:0:a.
   - **Number of Addresses**: Enter the total number of IPv6 addresses to be included in the DHCP range.
   - **Comment**: Optionally, enter additional information about the template.
4. Click Next and select one of the following to provide DHCP services for the range:
   - **None (Reserved Range)**: Select this if you want to reserve this address range for static hosts. Addresses in this range cannot be allocated as dynamic addresses. You can allocate the next available IP from this range to a static host. This is selected by default.
   - **Grid Member**: Click Select and choose a Grid member from the drop-down list.
5. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes on page 265.
6. Save the configuration.

Modifying IPv6 Range Templates

You can modify the properties of a DHCP range template and define an exclusion range. For the exclusion range in the template, the start and end addresses are determined by the number of offsets in the DHCP range template’s start address and the number of IP addresses in the exclusion range. For more information about exclusion ranges, see About DHCP Ranges on page 574.

To modify a DHCP range:

1. From the Data Management tab, select the DHCP tab -> Templates tab -template check box, and then click the Edit icon.
2. The IPv6 DHCP Range Template editor contains the following tabs from which you can modify data:
   - **General**: Modify general information as described in Adding IPv6 Range Templates.
   - **Member Assignment**: Change the Grid member that provides DHCP services for ranges created from this template. For information, see Adding IPv6 Range Templates.
   - **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 265.
   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see About Administrative Permissions on page 120.
3. Optionally, you can click **Toggle Expert Mode** to display the following tabs from which you can modify data:
   - **Exclusion Ranges**: Configure a range of IP addresses that the appliance does not use for dynamic address assignments. **Exclusion Ranges**: Configure a range of IP addresses that the appliance does not use for dynamic address assignments. Complete the following:
     - **Offset**: An offset for an exclusion range determines the start IP address of the exclusion range. The appliance adds the offset value you enter here to the start IP address of the DHCP range created using this template. That IP address becomes the start IP address of the exclusion range.
     - **Number of Addresses**: Enter the number of IP addresses to be included in the exclusion range.
     - **Comment**: Enter useful information about the exclusion range.
   
   Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Save the configuration.

### About IPv6 Fixed Address Templates

A fixed address template is useful when you want to create multiple fixed addresses in a network. When you create a fixed address template, you specify the offset value and number of fixed addresses to be created. You can also specify additional properties for the fixed addresses.

Note that you can use the template to create address-based fixed addresses. You cannot specify prefixes in the template because a fixed address could use a prefix that is not part of the subnet to which the fixed address belongs. You can enter prefixes when you create the individual fixed address objects using the template.

#### Adding IPv6 Fixed Address Templates

To create an IPv6 fixed address template:

1. From the **Data Management** tab, select the **DHCP** tab -> **Templates** tab.
2. Click the Add drop-down menu and select **IPv6 Fixed Address Template**.
3. In the **Add IPv6 Fixed Address Template** wizard, enter the following:
   - **Name**: Enter a name that helps identify the IPv6 fixed address template. For example, you can enter **HP Printer** when you create a template that contains settings for assigning fixed addresses or reservations to HP printers.
   - **Comment**: Optionally, enter additional information about the template.

   In the **Optional Settings For Range of Objects** section, do the following:
   - **Offset**: An offset in a fixed address template determines the IP address of the first fixed address created from the template. The appliance adds the offset value you enter here to the start IP address of the network in which you create objects using this template, and that IP address becomes the IP address of the object. For example, you specify an offset value of 50 for the 2001:db8:1263:/48 network, when you create a fixed address using the fixed address template, the appliance assigns it the address 2001:db8:1263:0:0:0:0:32.
   - **Number of Addresses**: Enter the number of IP addresses to be used as fixed addresses or roaming hosts.

   **Note**: The appliance uses the offset and number of addresses only when this template is used in a network template.

4. Click **Next** to configure or override DHCP options as described in **Configuring DHCP Properties** on page 587.
5. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see **Using Extensible Attributes** on page 265.
6. Save the configuration.
Modifying IPv6 Fixed Address Templates

To modify a fixed address template:

1. From the Data Management tab, select the DHCP tab -> Templates tab -> template check box, and then click the Edit icon.
2. The IPv6 Fixed Address Template editor contains the following tabs from which you can modify data:
   - **General**: Modify general information for the template as described in Adding IPv6 Fixed Address Templates on page 635.
   - **IPv6 DHCP Options**: Keep the inherited DHCP options or override them and enter unique settings for the template. For information, see Defining General IPv6 Properties on page 606.
   - **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 265.
   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see About Administrative Permissions on page 120.
3. Optionally, you can click **Toggle Expert Mode** to display the following tabs from which you can modify data:
   - **IPv6 DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the template. For information, see Enabling DDNS for IPv4 and IPv6 DHCP Clients on page 484.

   Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.
4. Save the configuration.

**About IPv6 Network Templates**

You can create IPv6 network templates to facilitate network configuration. You can use network templates to create networks in any network view. When you create a network template, you do not specify a network address. You enter the network address when you create an actual network from the template. You can specify a netmask or allow the user to define the netmask when they create the actual network.

A network template is useful for setting up a network with fixed addresses and DHCP ranges already defined. You can add DHCP range or fixed address templates to a network template.

**Adding IPv6 Network Templates**

To create a network template:

1. From the Data Management tab, select the DHCP tab -> Templates tab.
2. Click the Add drop-down menu and select IPv6 Network Template.
3. In the Add IPv6 Network Template wizard, do the following:
   - **IPv6 Prefix**: If you are adding a template for a previously defined global IPv6 prefix, you can select it from the list.
   - **Name**: Enter a name that helps identify the network template.
   - **Netmask**: Select one of the following options:
     - **Fixed**: Select this and adjust the netmask slider to a fixed netmask for this network template. When you select this option, users cannot specify another netmask when they use this template to create a network. For example, if you select /24 as the fixed netmask, all networks created using this template have a /24 netmask.
     - **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.
About IPv6 DHCP Templates

— **Automatically create a reverse-mapping zone:** This function is enabled if the fixed netmask of the template is a multiple of 4 (4, 8, 24, and so on), or if you select the *Allow User to Specify Netmask* option. Select this if you want the appliance to automatically create the corresponding reverse-mapping zone for the networks created using this template. These zones are created in the DNS view assigned to receive dynamic DNS updates at the network level.

4. Click **Next** to assign Grid members to this network template. Ensure that you include members that are associated with other templates that you plan to add to this network template. You can assign one or multiple members to this template. However, you cannot assign a combination of NIOS Grid members and vNIOS Grid members to the template.

— Click the Add icon to add a Grid member as a DHCP server for the networks created using this template. Select the Grid member from the *Member Selector* dialog box. Keep in mind, DHCP properties for the network are inherited from this member. Networks created using this template can be served by multiple members, but a member can serve networks in one network view only.

5. Click **Next**, and then click the Add icon to include DHCP range and fixed address templates in the network template. Choose the template that you want to include in this network template. Use SHIFT+click and CTRL+click to select multiple templates.

You can remove a template from the list by selecting the template and clicking the Delete icon.

6. Click **Next** to configure or override DHCP options as described in *Defining General IPv6 Properties* on page 606.

7. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see *Using Extensible Attributes* on page 265.

8. Save the configuration.

Modifying IPv6 Network Templates

To modify and set the properties of a network template:

1. From the **Data Management** tab, select the **DHCP** tab -> **Templates** tab -> *template* check box, and then click the **Edit** icon.

2. The **Network Template** editor contains the following tabs from which you can modify data:

   — **General:** Modify general information described in *Adding IPv6 Network Templates* on page 636.

   — **Member Assignment:** Change the Grid members that provide DHCP services for networks created from this template. For information, see *Adding IPv6 Networks* on page 735.

   — **Templates:** Add or delete DHCP range and fixed address templates. For information, see *Adding IPv6 Range Templates* on page 634 and *Adding IPv6 Fixed Address Templates* on page 635

   — **IPv6 DHCP Options:** Keep the inherited DHCP options or override them and enter unique settings for the template. For information, see *Defining General IPv6 Properties* on page 606.

   — **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 265.

   — **Permissions:** This tab appears only if you belong to a superuser admin group. For information, see *Managing Permissions* on page 128.

3. Optionally, you can click **Toggle Expert Mode** to display the following tabs from which you can modify data:

   — **IPv6 DDNS:** Keep the inherited DDNS settings or override them and enter unique settings for the template. For information, see *Enabling DDNS for IPv4 and IPv6 DHCP Clients* on page 484.

   Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Save the configuration.
Viewing Templates

To view a list of all IPv4 and IPv6 DHCP templates:
1. From the Data Management tab, select the DHCP tab -> Templates tab.
2. Grid Manager displays the following information:
   - Name: The name of the template.
   - Type: The template type, such as IPv4 Network Template or IPv6 Network Template.
   - Comment: The information you entered about the template.
   - Site: The site to which the template belongs. This is one of the predefined extensible attributes.

You can select predefined and user defined extensible attributes for display.

You can also do the following in this panel:
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables on page 52.
- Sort the displayed data in ascending or descending order by column.
- Delete a selected template or multiple templates. For information, see Deleting Templates.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 57.
- Select an object and edit its information.
- Print or export the data in the panel.

Deleting Templates

To delete a template:
1. From the Data Management tab, select the DHCP tab -> Templates tab -> template check box, and then click the Delete icon.
2. In the Delete Confirmation dialog box, click Yes.
Chapter 22  Managing IPv4 DHCP Data

This chapter explains how to configure and manage IPv4 DHCP data. It contains the following sections:

- Configuring DHCP for IPv4  on page 641
- About the Next Available Network or IP Address  on page 642
- Configuring IPv4 Networks  on page 643  
  — Adding IPv4 Networks  on page 643  
  — Viewing Networks  on page 645  
  — Modifying IPv4 Networks  on page 646  
  — Deleting IPv4 Networks  on page 647
- Configuring IPv4 Shared Networks  on page 648  
  — Adding IPv4 Shared Networks  on page 648  
  — Viewing Shared Networks  on page 648  
  — Modifying IPv4 Shared Networks  on page 649  
  — Deleting IPv4 Shared Networks  on page 649
- Configuring IPv4 Address Ranges  on page 650  
  — Adding IPv4 Address Ranges  on page 650  
  — Modifying IPv4 Address Ranges  on page 651  
  — Controlling Lease Assignments  on page 652  
  — Deleting IPv4 Address Ranges  on page 652
- Configuring IPv4 Fixed Addresses  on page 653  
  — Adding IPv4 Fixed Addresses  on page 654  
  — Adding IPv4 Fixed Addresses  on page 654  
  — Modifying IPv4 Fixed Addresses  on page 655  
  — Deleting Fixed Addresses  on page 655
- Configuring IPv4 Reservations  on page 656  
  — Adding IPv4 Reservations  on page 656  
  — Modifying Reservations  on page 657
- Viewing IPv4 DHCP Objects  on page 658
- About Roaming Hosts  on page 659  
  — Configuring Roaming Hosts  on page 659  
  — Enabling Support for Roaming Hosts  on page 659  
  — Adding IPv4 Roaming Hosts  on page 660  
  — Adding IPv6 Roaming Hosts  on page 661
— Adding IPv4/IPv6 Roaming Hosts on page 661
— Viewing Roaming Hosts on page 662
— Setting Properties for Roaming Hosts on page 663
— Deleting Roaming Hosts on page 664
Configuring DHCP for IPv4

To configure DHCP service for an IPv4 network and the resources in the network, perform the following tasks:

1. Create a network and assign it to Grid members or Microsoft DHCP servers. For information, see Adding IPv4 Networks and Modifying IPv4 Networks on page 646.
2. Configure DHCP properties for the network. You can override properties set at the Grid or member level and enter unique values for the network. For information, see Configuring General IPv4 DHCP Properties on page 590 and Configuring DHCP IPv4 and IPv6 Properties on page 610.
3. Optionally, assign zones to a network. For information, see Associating Networks with Zones on page 611.
4. Add a DHCP range to the network and assign it to a member, a failover association, or a Microsoft DHCP server. For information, see Adding IPv4 Address Ranges on page 650 and Modifying IPv4 Address Ranges on page 651.
5. Optionally, add exclusions to the DHCP range for addresses that are not used for dynamic allocation. For information, see Configuring IPv4 Fixed Addresses on page 653.
6. Optionally, configure DHCP properties for the address range. You can override properties set at an upper level and enter unique values for the address range. For information, see Modifying IPv4 Address Ranges on page 651.
7. Optionally, define filters for precise address assignments and apply them to the DHCP range. For information, see About IPv4 DHCP Filters on page 674.
8. Optionally, add fixed addresses and reservations to the network and configure DHCP properties for them. For information, see Configuring IPv4 Fixed Addresses on page 653 and Configuring IPv4 Reservations on page 656.
About the Next Available Network or IP Address

When you create certain objects through Grid Manager, the appliance can obtain the next available IPv4 or IPv6 network from a specific network container. It can also obtain the next available IP address from a specific network or address range. This feature automates the allocation of networks and IP addresses so you can manage your network space more efficiently. You can also use this feature to organize network devices. For example, you can create a reserved range called "Printer Range" to reserve static IP addresses for printers in your network. When you allocate IP addresses for printers, you can have the appliance search for the next available IP address within "Printer Range," and then allocate the next available address to a new printer.

When you create a new network, the appliance can look up the next available network address within a specific network container. The next available network address is the first unused network address in the network container to which you have administrative permissions. For information about creating IPv4 and IPv6 networks using the next available feature, see Adding IPv4 Networks on page 643 and Adding IPv6 Networks on page 735.

You can also obtain the next available IP address when you define a fixed address, reservation, or host record. The next available IP address is the first unused IP address in a specified network, DHCP range, or reserved range to which you have administrative permissions. For information about creating fixed addresses, reservations, and host records using the next available feature, see Configuring IPv4 Fixed Addresses on page 653, Configuring IPv4 Reservations on page 656, and Adding Host Records on page 813.

Obtaining the Next Available

The appliance searches for the next available network or IP address based on the context you define when you create an object. For example, when you create a network within a specific network container, the appliance searches for the next available network within the specified container. Similarly, when you drill down to an address range and create an object from there, the appliance looks up the next available IP address within that address range. If you are not within a specific network or address range when you create an object, Grid Manager displays a selector from which you can select the network or address range for the next available network or IP address.

For information about how the appliance select the next available network and IP address, see Guidelines for the Next Available Network and IP Address.

Guidelines for the Next Available Network and IP Address

The appliance follows certain rules when searching for the next available network and IP address in the specified wizard, network container, and address range.

In a wizard where you can obtain the next available network or IP address, the following applies:

• In a wizard, if you add a network or IP address and then delete it, the appliance excludes it from the next available. When you try to obtain the next available network or IP address in the same wizard, the appliance does not return the deleted network or IP address until you exit the wizard.

In a network, the appliance searches for the next IP address that meets all of the following criteria:

• It does not match any DNS resource record, such as an A or PTR record, that is associated with an IP address.
• It is not assigned to a DHCP fixed address or host address record.
• 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 any reserved 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 256.

In a DHCP range, the appliance searches for the next IP address that meets all of the following criteria:
### Configuring IPv4 Networks

When you create an IPv4 network, you can do so from scratch or from a network template that contains predefined properties. When you use a template to create a network, the properties of the template apply to the new network. For information about network templates, see [About IPv4 Network Templates](#) on page 628. You can also create an IPv4 network from the Tasks Dashboard, as described in [The Tasks Dashboard](#) on page 70.

After you create IPv4 networks, you can combine them into shared networks or create ranges and fixed addresses.

### Adding IPv4 Networks

When you configure an IPv4 network, you must assign either Grid members or Microsoft servers to the network. A network cannot be served by a mix of Microsoft and Infoblox DHCP servers. Multiple servers can serve a network, but Grid members and Microsoft servers cannot serve the same network.

A Grid member can serve only one network view. Similarly, a Microsoft server can serve only one network view. Therefore when you assign Grid members to networks, you must assign the members to networks in the same network view. For information, see [Configuring DHCP for IPv4](#) on page 641.

To add an IPv4 network:

1. Select the **Data Management** tab.
2. If you have more than one network view in the system, select the network view in which you want to add the network.
3. Select the **DHCP** tab -> **Networks** tab.
4. In the **Networks** section, select **IPv4 Network** from the Add drop-down menu.
5. In the **Add Network** wizard, select one of the following and click **Next**:
   - **Add Network**: Click this to add a network from scratch.
   - **Add Network using Template**: To use a template, click this, and then click **Select Template** and select a network template. For information, see [About IPv4 Range Templates](#) on page 625. The appliance populates the template properties in the wizard when you click **Next**. You can then edit the pre-populated properties, except for **Netmask**.
6. Complete the following and click **Next**:

- It is not assigned to a fixed address or host 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.

In a reserved range, the appliance searches for the next IP address that meets all of the following criteria:

- It is not assigned to a fixed address or host record.
- It does not match any unmanaged IP address.
- It is not part of a scheduled task that involves a fixed address.

**Note:** The appliance does not search for deleted leases in the Recycle Bin.

When multiple users simultaneously request for the next available network or IP address, the appliance returns the same unused network or IP address to all users. The user who first saves the task gets the next available network or IP address. In some cases, other users get an error message telling them that the network or IP address is not available when they save their tasks. They can then request another unused network or IP address or enter a new one.
— **Mask**: 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.

— **Networks**: Do one of the following to add new networks:

  1. Click the Add icon to enter a new network. Grid Manager adds a row to the table. Enter the network address in the **Network** field. Click the Add icon again to add another network.
  2. or
  3. Click the Next Available icon to have the appliance search for the next available network. Complete the following in the **Next Available Networks** section:

    — **Create new network(s) under**: Enter the network container in which you want to create the new network. When you enter a network that is part of a parent network, the parent network is converted into a network container if it does not have a member assignment or does not contain address ranges, fixed addresses, reservations, shared networks, and host records that are served by DHCP. When you enter a network that has a lower CIDR than an existing network, the appliance creates the network as a parent network and displays a message indicating that the newly created network overlaps an existing network. You can also click **Select Network** to select a specific network in the **Network Selector** dialog box. For information about how the appliance searches for the next available network, see [Obtaining the Next Available](#) on page 642.

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

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

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

— **Comment**: Enter useful information about the network, such as the name of the organization it serves.

— **Automatically Create Reverse-Mapping Zone**: This function is enabled if the netmask of the network equals /8, /16, or /24. Select this to have the appliance automatically create reverse-mapping zones for the network. A reverse-mapping zone is an area of network space for which one or more name servers have the responsibility for responding to address-to-name queries. These zones are created in the DNS view assigned to receive dynamic DNS updates at the network view level.

— **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.

7. 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:

      1. **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.
8. Click **Next** to override DHCP properties as described in *About DHCP Properties* on page 589. This only applies if you are adding a network that is served by an Infoblox Grid member.

9. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see *About Extensible Attributes* on page 262.

10. Save the configuration.

or

— Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 256.

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 822.
- 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 823. You can also create a shared network for subnets that are on the same network segment.

Networks served by Microsoft servers do not support the split and join functions.

**Viewing Networks**

You can view IPv4 networks in the Net Map and List panels in the IPAM tab. The Net Map panel provides a graphical view of your networks and the List panel displays the networks in table format. For more information, see *IPv4 Network Map* on page 818 and *Network List* on page 821.

You can view a list of IPv4 and IPv6 networks in the **DHCP tab -> Networks tab -> Networks** panel. This panel displays all IPv4 and IPv6 networks.

In the *Networks* panel, you can use filters or the **Go to** function to navigate to a specific network. You can also create a quick filter to save frequently used filter criteria. For information, see *Using Quick Filters* on page 57. You can add, delete, or edit a network. You can also monitor the DHCP utilization of a selected network.

To view IPv4 and IPv6 networks, from the Data Management tab, select the **DHCP tab -> Networks tab -> Networks**. Grid Manager displays the following information:

- **Network**: The network address.
- **Comment**: The information you entered about the network.
- **DHCP Utilization**: This information is available for IPv4 networks only. It displays the percentage of the total DHCP usage of the IPv4 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.

You can select the following additional columns for display:

- **Protocol**: Displays whether the network is an IPv4 or IPv6 network.
- **Disabled**: Indicates if the network is disabled.
Managing IPv4 DHCP Data

- IPAM Utilization: This information is available for IPv4 networks only. It displays the percentage based on the IP addresses in use divided by the total addresses in the network. For example, in a /24 network, if there are 25 static IP addresses defined and a DHCP range that includes 100 addresses, the total number of IP addresses in use is 125. Of the possible 256 addresses in the network, the IPAM utilization is about 50% for this network.

In this panel, you can sort the list of networks in ascending or descending order by columns. For information about customizing tables in Grid Manager, see Customizing Tables on page 50.

You can also modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables on page 52.

Viewing Network Details

You can view detailed information about a specific network by clicking the network link. Grid Manager displays the objects in the network, including DHCP ranges, hosts, fixed addresses and roaming hosts. It displays the following information about the network:

- 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.
- IPv4 DHCP Utilization: The percentage of the total DHCP usage of a DHCP range. This is the percentage of the total number of fixed addresses, reservations, hosts, and active leases in the DHCP range divided by the total IP addresses in the range, excluding the number of addresses in the exclusion ranges. Note that only enabled objects are included in the calculation.
- Site: The site to which the DHCP object belongs. This is one of the predefined extensible attributes.

You can select the following additional columns for display:

- Static Addresses: Indicates whether the IP address is a static address.
- Dynamic Addresses: Indicates whether the IP address is a dynamically assigned address.
- Disabled: Indicates whether the object is disabled.
- Priority: Displays the priority of a DHCP range when NAC filters are applied.
- Available extensible attributes.

You can also do the following in this panel:

- Sort the displayed data in ascending or descending order by column.
- Click Go to IPAM View to view information about the object in the IPAM tab.
- Add new objects, such as DHCP ranges, to the network.
- Delete or schedule the deletion of a selected object or multiple objects.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 57.
- Print or export the data.

Modifying IPv4 Networks

You can modify existing network settings and override the Grid or member DHCP properties, with the exception of the network address and netmask.

To modify an IPv4 network:
1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** section -> **network** check box, and then click the **Edit** icon.

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 643.
   - **IPv4 DHCP Options**: Keep the inherited DHCP properties or override them and enter unique settings for the network. For information, see **Defining Basic IPv4 Options** on page 597.
   - **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 262.
   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see **Managing Permissions** on page 20.

3. Optionally, click **Toggle Advanced Mode** to display the following tabs from which you can modify advanced data.
   - **General Advanced**: You can associate zones with a network. For information, see **Associating Networks with Zones** on page 611.
   - **IPv4 DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the network. Note that you must click **Override** and select **Enable DDNS updates** for the DDNS settings you configure in this tab to take effect. For information, see **Enabling DDNS for IPv4 and IPv6 DHCP Clients** on page 484.
   - **IPv4 BOOTP/PXE**: Keep the inherited BOOTP properties or override them and enter unique settings for the network. For information, see **Configuring IPv4 BOOTP and PXE Properties** on page 594.
   - **IPv4 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 603.

4. Save the configuration or click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see **Scheduling Tasks** on page 256.

### 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 646.

To delete a network:

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** section -> **network** check box, and then select **Delete** or **Schedule Delete** from the Delete drop-down menu.

2. To delete the network now, in the **Delete Confirmation** dialog box, click **Yes**. To schedule the deletion, see **Scheduling Tasks** on page 256.

   The appliance puts the deleted network in the Recycle Bin, if enabled.
Configuring IPv4 Shared Networks

You can combine individual contiguous networks into a shared network to allow the DHCP server to assign IP addresses from any subnet (that resides on the same network interface) in the shared network.

Before creating a shared network, you must first create the subnets. For example, you must first create the networks 10.32.1.0 and 10.30.0.0 before designating them to a shared network. For more information, see About Shared Networks on page 574.

Adding IPv4 Shared Networks

To add a shared network:

1. Select the Data Management tab.
2. If you have more than one network view in the system, select the network view in which you want to add the network.
3. Select the DHCP tab -> Networks tab.
4. In the Shared Networks section, select IPv4 Shared Network from the Add drop-down menu.
5. In the Add IPv4 Shared Network wizard, complete the following and click Next:
   - Name: Enter the name of the shared network.
   - Comment: Enter information about the shared network.
   - Disabled: Select this if you want to enable the shared network at a later time. You can disable and enable existing networks instead of removing them from the database. This feature is especially helpful when you have to move or repair the server for a particular network.
6. Do the following to add networks:
   a. Click the Add icon.
   b. In the Select Network dialog box, select the networks that you want to include in the shared network. Ensure that the networks are served by the same Grid members to avoid DHCP inconsistencies.
7. Click Next to configure or override DHCP options as described in Defining Basic IPv4 Options on page 597.
8. Click Next to enter values for required extensible attributes or add optional extensible attributes for the shared network. For information, see Using Extensible Attributes on page 265.
9. Save the configuration or click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.

Viewing Shared Networks

To view IPv4 and IPv6 shared networks:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Shared Networks.
2. Grid Manager displays the following information:
   - Name: The name of the shared network.
   - Protocol: Displays whether the network is an IPv4 or IPv6 network.
   - Comment: The information you entered about the shared network.
   - IPv4 DHCP Utilization: The percentage of the DHCP utilization of the networks that belong to the shared network. This is the percentage of the total number of available IP addresses from all the networks that belong to the shared network versus the total number of all IP addresses in all of the networks in the shared network.
   - Site: The site to which the shared network belongs. This is one of the predefined extensible attributes.

You can select Disabled or available extensible attributes for display. You also can view detailed information about a network in a shared network by clicking the network link.
In this panel, you can use filters or the Go to function to navigate to a specific network. You can also create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 57.

You can sort the list of networks in ascending or descending order by columns. For information about customizing tables in Grid Manager, see Customizing Tables on page 50.

You can also modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables on page 52.

### Modifying IPv4 Shared Networks

You can modify existing network settings and override the Grid or member DHCP properties:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Shared Networks section -> shared_network check box, and then click the Edit icon.

2. The Shared Network editor contains the following tabs from which you can modify data:
   - **General**: Modify the fields Name, Comments, and Disabled as described in Adding IPv4 Shared Networks on page 648.
   - **Networks**: Displays the networks that are currently assigned to the shared network. You can add or delete a network. To add a network, click the Add icon. In the Select Network dialog box, select the network you want to add. To delete an existing network, select the network check box, and then click the Delete icon.
   - **Extensible Attributes**: Add and delete extensible attributes that are associated with a specific network. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes on page 265.
   - **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.
   - **IPv4 DHCP Options**: Keep the inherited DHCP properties or override them and enter unique settings for the shared network. For information, see Defining Basic IPv4 Options on page 597.
   - **IPv4 DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the shared network. Note that you must click Override and select Enable DDNS updates for the DDNS settings you configure in this tab to take effect. For information, see Enabling DDNS for IPv4 and IPv6 DHCP Clients on page 484.
   - **IPv4 BOOTP/PXE**: Keep the inherited BOOTP properties or override them and enter unique settings for the shared network. For information, see Configuring IPv4 BOOTP and PXE Properties on page 594.

Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

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

   or

   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.

### Deleting IPv4 Shared Networks

Though you can delete the networks in a shared network, a shared network must have at least one network in it. To delete a shared network:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Shared Networks section -> shared_network check box, and then select Delete or Schedule Delete from the drop-down menu.

2. To delete the shared network now, in the Delete Confirmation dialog box, click Yes. To schedule the deletion, see Scheduling Tasks on page 256.

The appliance puts the deleted shared network in the Recycle Bin, if enabled.
Configuring IPv4 Address Ranges

In a network, you define address ranges from which the DHCP server or failover association assigns IP addresses to client requests. When a DHCP client requests an IP address, the appliance allocates an address within a defined DHCP range. The DHCP client can use the assigned IP address until the lease expires.

When you do not assign a DHCP server or failover association to an address range, the range becomes a reserved range. A reserved range contains IP addresses that are reserved for static hosts, not for dynamic assignments. You can allocate the next available IP from a reserved range.

You can also apply filters to DHCP ranges to control how the DHCP server allocates IP addresses. For information about DHCP filters, see About IPv4 DHCP Filters on page 674.

Adding IPv4 Address Ranges

To add an IPv4 address range:

1. Navigate to the IPv4 network to which you want to add an address range, and then select Range from the Add drop down menu.
   
or
   From any panel in the DHCP tab, expand the Toolbar and click Add -> Range -> IPv4.

2. In the Add IPv4 Range wizard, select one of the following and click Next:
   — Add Range: Select this to add an address range from scratch.
   
or
   — Add Range Using Template: Click Select Template and select the template that you want to use. Note that when you use a template to create an address range, the configurations of the template apply to the new range. The appliance automatically populates the range properties in the wizard. You can then edit the pre-populated properties.

3. Complete the following:
   — Network: Click Select Network. Grid Manager displays the network address here if you have only one network configured. When there are multiple networks, Grid Manager displays the Select Network dialog box from which you can select one.
   
   — Start: Enter the first available IP address in the range.
   
   — End: Enter the last available IP address in the range.
   
   — Name: Optionally, enter a name for the range.
   
   — Comment: Enter additional information about the address range.
   
   — Disabled: Select this if you want to save the configuration for the address range but do not want to activate the address range yet. You can clear this check box when you are ready to allocate addresses from this range.

4. Click Next and select one of the following:
   — None (Reserved Range): Select this if you want to reserve this address range for static hosts. Addresses in this range cannot be allocated as dynamic addresses. You can allocate the next available IP from this range to a static host. This is selected by default.
   
   — Grid Member: Select this if you want a Grid member to serve DHCP for this address range. Select a Grid member from the drop-down list. The drop-down list displays only the Grid members that are associated with the network to which the DHCP range belongs.
   
   — Failover Association: Select this if you want a failover association to serve DHCP for this address range. Click Select Association. In the DHCP Failover Association Selector dialog box, choose a failover association, and then click the Select icon. The appliance lists failover associations that serve DHCP in the network view of the DHCP range. For information, see Chapter 23, DHCP Failover, on page 665.

5. Click Next to configure or override DHCP options as described in Defining Basic IPv4 Options on page 597.
6. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see *Using Extensible Attributes* on page 265.

7. Save the configuration and click **Restart** if it appears at the top of the screen.
   or
   — Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 256.

For information on viewing address ranges in a network, see *Viewing IPv4 DHCP Objects* on page 658

### Modifying IPv4 Address Ranges

You can modify settings for the DHCP range. You can also define an exclusion range to prevent the appliance from assigning the addresses in the exclusion range to clients. IP addresses in an exclusion range are excluded from the pool of IP addresses. For more information, see *About Exclusion Ranges* on page 574.

To modify an IPv4 address range:

1. From the *Data Management* tab, select the DHCP tab -> *Networks* tab -> *Networks* section -> *network-*addr_range check box, and then click the Edit icon.

2. The *DHCP Range* editor contains the following basic tabs from which you can modify data:
   — **General**: Modify the fields, except the network address, as described in *Adding IPv4 Address Ranges* on page 650.
   — **Member Assignment**: Modify the Grid member or failover association that provides DHCP services for the DHCP range as described in *Adding IPv4 Address Ranges* on page 650.
   — **IPv4 DHCP Options**: Keep the inherited DHCP options or override them and enter unique settings for the DHCP range. For information, see *Defining Basic IPv4 Options* on page 597.
   — **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 265.
   — **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.
   — **IPv4 DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the DHCP range. Note that you must click **Override** and select **Enable DDNS updates** for the DDNS settings you configure in this tab to take effect. For information, see *Enabling DDNS for IPv4 and IPv6 DHCP Clients* on page 484.
   — **IPv4 BOOTP/PXE**: Keep the inherited BOOTP properties or override them and enter unique settings for the DHCP range. For information, see *Configuring IPv4 BOOTP and PXE Properties* on page 594.
   — **Exclusion Ranges**: Configure a range of IP addresses that the appliance does not use to assign to clients. You can use these exclusion addresses as static IP addresses. Enter the start and end addresses of the exclusion range, and optionally, enter information about this exclusion range.
   — **IPv4 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 603.
   — **Filters**: You can add or delete DHCP filters to the range. For information, see *Applying Filters to DHCP Address Ranges* on page 692.

Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Save the configuration and click **Restart** if it displays at the top of the screen.
   or
   — Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 256.
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. Save the configuration and click **Restart** if it displays at the top of the screen.

Deleting IPv4 Address Ranges

To delete a DHCP range:

- From the Data Management tab, select the DHCP tab -> Networks tab -> Networks section -> network -> addr_range check box, and then click the Delete icon.
Configuring IPv4 Fixed Addresses

A fixed address represents a persistent link between an IP address and one of the following:

- MAC address
- Client identifier
- Circuit ID or remote ID in the DHCP relay agent option (option 82)

You can create fixed addresses as described in Adding IPv4 Fixed Addresses or from the Tasks Dashboard. For information about the Tasks Dashboard, see The Tasks Dashboard on page 70. 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 813 and Converting DHCP Leases on page 838.

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 (.)
- aabbc-ddeeff — Two groups of six hexadecimal digits separated by a hyphen (-)
- aabbc-ddeeff — 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 602. 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 General IPv4 DHCP Properties on page 590.
Adding IPv4 Fixed Addresses

To add an IPv4 fixed address:

1. Navigate to the network to which you want to add a fixed address, and then select Fixed Address from the Add drop-down menu.
   or
   From any panel in the DHCP tab, expand the Toolbar and click Add -> Fixed Address -> IPv4.

2. In the Add IPv4 Fixed Address wizard, select one of the following and click Next:
   — Add Fixed Address
   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.

3. Complete the following:
   — 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 About the Next Available Network or IP Address on page 642.
   — 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 IPv4 Fixed Addresses on page 653.
     — 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 602. 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 596. 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 798.
   — 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.

4. Click Next to configure or override DHCP options as described in About IPv4 DHCP Options on page 595.

Note: You cannot use the same circuit ID or remote ID for different fixed addresses if the addresses are in the same network or the same shared network.
5. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see *Using Extensible Attributes* on page 265.

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

   or

   — Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 256.

For information on viewing fixed addresses and other DHCP objects, see *Viewing IPv4 DHCP Objects* on page 658.

### Modifying IPv4 Fixed Addresses

To modify the settings of a fixed address:

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** section -> **network** -> fixed_address check box, and then click the Edit icon.

2. The **Fixed Address** editor contains the following basic tabs from which you can modify data:

   — **General**: You can modify the fields, except the network address, as described in *Adding IPv4 Fixed Addresses* on page 654.

   — **IPv4 DHCP Options**: You can keep the inherited DHCP options or override them and enter unique settings for the fixed address. For information, see *Defining Basic IPv4 Options* on page 597.

   — **Discovered Data**: Displays the discovered data of the fixed address. For information, see *Viewing Discovered Data* on page 858.

   — **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 265.

   — **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.

   — **IPv4 DDNS**: You can keep the inherited DDNS settings or override them and enter unique settings for the fixed address. Note that you must click **Override** and select **Enable DDNS updates** for the DDNS settings you configure in this tab to take effect. For information, see *Enabling DDNS for IPv4 and IPv6 DHCP Clients* on page 484.

   — **IPv4 BOOTP/PXE**: You can keep the inherited BOOTP properties or override them and enter unique settings for the fixed address. For information, see *Configuring IPv4 BOOTP and PXE Properties* on page 594.

   Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

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

   or

   — Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 256.

### Deleting Fixed Addresses

To delete a fixed address, from the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** section -> **network** -> fixed_address check box, and then click the Delete icon.
Configuring IPv4 Reservations

You can create a reservation as a static IP address for future use. A reservation is a pre-provisioned fixed address that is associated with a MAC address of 00:00:00:00:00:00. Since 00:00:00:00:00:00 is not a real MAC address, no client can receive this IP address from the address pool. You can reserve this static IP address and assign it to a client in the future.

To create a reservation, you can do one of the following:

- Add a reservation. For information, see Adding IPv4 Reservations.
- Convert a fixed address or a dynamic address with an active lease to a reservation. For information, see Converting Objects Associated with IP Addresses on page 838.
- Define a fixed address with an IP address. For information, see Adding IPv4 Fixed Addresses on page 654.

Adding IPv4 Reservations

To create a reservation:

1. Navigate to the network to which you want to add a reservation, and then select Reservation from the Add drop down menu.
   or
   From any panel in the DHCP tab, expand the Toolbar and click Add ->IPv4 Reservation.

2. In the Add Reservation wizard, select one of the following and click Next:
   - Add Reservation
   or
   - Add Reservation using Template
     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.

3. Complete the following:
   - Network: The displayed network address can either be the last selected network or the network from which you are adding the DHCP range. If no network address is displayed or if you want to specify a different network, click Select Network. When there are multiple networks, Grid Manager displays the Select Network dialog box from which you can select one.
   - IP Address: Enter the IP address that you want to reserve for manual assignment, or click Next Available IP to obtain the next available IP address. For information about obtaining the next available IP address, see Adding IPv4 Fixed Addresses on page 654.
   - Name: Optionally, enter a name for the reservation.
   - Comment: Optionally, enter additional information about the reservation.
   - Disabled: Select this if you do not want the DHCP server to use this reservation at this time.

4. Click Next to configure or override DHCP options as described in Defining Basic IPv4 Options on page 597.
5. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes on page 265.
6. Save the configuration and click Restart if it appears at the top of the screen.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.
Modifying Reservations

To modify a reservation:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks section -> network -> reservation check box, and then click the Edit icon.

2. The Reservation Address editor contains the following tabs from which you can modify data:
   - **General**: Modify the fields, except the network address, as described in Adding IPv4 Reservations on page 656.
   - **IPv4 DHCP Options**: Keep the inherited DHCP options or override them and enter unique settings for the reservation. For information, see Defining Basic IPv4 Options on page 597.
   - **Discovered Data**: Displays the discovered data of the reservation. For information, see Viewing Discovered Data on page 858.
   - **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 265.
   - **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.
   - **IPv4 DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the reservation. Note that you must click **Override** and select **Enable DDNS updates** for the DDNS settings you configure in this tab to take effect. For information, see Enabling DDNS for IPv4 and IPv6 DHCP Clients on page 484.
   - **IPv4 BOOTP/PXE**: You can keep the inherited BOOTP properties or override them and enter unique settings for the reservation. For information, see Configuring IPv4 BOOTP and PXE Properties on page 594.
   Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Save the configuration and click **Restart** if it displays at the top of the screen.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.
Viewing IPv4 DHCP Objects

To view the address ranges, fixed addresses and reservations in a network:

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **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 and the **Go to** function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the **Go to** field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see *Using Quick Filters* on page 57.
- Select an object and view detailed information.
- Print or export the data.
About Roaming Hosts

A roaming host is a host with a dynamically assigned IP address and a specific set of properties and DHCP options. When you create a roaming host for a network device, the device can receive any dynamically assigned address from the network to which it belongs. You can create roaming hosts for devices, such as laptop computers and mobile phones, that require different IP addresses each time they are moved from one network to another and require a unique set of DHCP options.

You can configure IPv4 addresses, IPv6 addresses, or IPv4 and IPv6 addresses for roaming hosts that require both types of addresses. When you configure IPv4 addresses for a roaming host, you must specify the host MAC address or a DHCP client identifier that the appliance uses to match the host, and specify DHCP options for the host. The appliance assigns an IP address from the DHCP range associated with the network from which the address request originates. You can configure an IPv6 prefix or address for a DHCP client. When you do, you must specify the DUID of the host so the appliance can use the DUID to match the host.

A roaming host also receives DHCP options from the Grid, member, network, or shared network with which it associates.

When you configure a roaming host, you must configure it in a specific network view. If you have multiple network views, you must specify the network view to which the requesting hosts belong so the appliance can assign addresses to the hosts from the networks within the same network view.

After you enable support for roaming hosts at the Grid level, you can add a roaming host that supports IPv4, IPv6, or both protocols. You can also convert an IPv4 roaming host to an IPv6 roaming host and vice versa, or convert an IPv4 or IPv6 roaming host to one that supports both IPv4 and IPv6.

Configuring Roaming Hosts

To configure a roaming host, perform the following tasks:
1. Enable support for roaming hosts at the Grid level. For information, see, Adding IPv4 Roaming Hosts.
2. Add a roaming host.
   - To add an IPv4 roaming host, see Adding IPv4 Roaming Hosts
   - To add an IPv6 roaming host, see Adding IPv6 Roaming Hosts
   - To add a dual stack roaming host, see Adding IPv4/IPv6 Roaming Hosts
3. Optionally, configure DHCP properties for the roaming host. You can override properties set for the upper levels and enter unique values for the roaming hosts. For information, see Defining Basic IPv4 Options on page 597

You can do the following after you configure roaming hosts:
4. View the configured roaming hosts. For information, see Viewing Roaming Hosts
5. Modify existing roaming hosts. For information, see Setting Properties for Roaming Hosts on page 663.
6. Delete roaming hosts that are not currently in use. For information, see Deleting Roaming Hosts on page 664.

Enabling Support for Roaming Hosts

You must first enable support for roaming hosts before adding them. After you enable this feature, you can disable it only after you delete all the existing roaming hosts.

To enable support for roaming hosts:
1. From the Data Management tab, select the DHCP tab.
2. Expand the Toolbar and click Grid DHCP Configuration.
3. In the General Advanced tab, select Enable support for roaming host.
4. Save the configuration and click Restart if it appears at the top of the screen.
Adding IPv4 Roaming Hosts

To add an IPv4 roaming host:

1. From the Data Management tab, select the DHCP tab.
2. Select a network view from the drop-down list.
3. Expand the Toolbar and click Add -> Roaming Host -> IPv4.
4. In the Add Roaming Host wizard, select one of the following and click Next:
   - Add Roaming Host
   or
   - Add Roaming Host using Template
     Click Select Template to create a roaming host using a fixed address/reservation template. In the DHCP Template Selector dialog box, select the template that you want to use. Note that when you use a template to create a roaming host, the configurations of the template apply to the new host. The appliance automatically populates the host properties in the wizard. You can then edit the pre-populated properties.
5. Complete the following:
   - Name: Enter the name of the roaming host. The name must be unique for each roaming host in a given network view.
   - Assign IPv4 Address by: Select one of the following criteria on which the appliance matches when assigning an IP address to the host.
     - MAC Address: Select this to assign a dynamic IP address to a host, provided that the MAC address of the requesting host matches the MAC address that you specify here.
     - DHCP Client Identifier: Select this to assign a dynamic IP address to a host with the same DHCP client identifier that you specify here. When you select this, the Match null (\0) at beginning of DHCP client identifier check box is displayed. Select this when a DHCP client sends a \000 prefix to the DHCP client identifier. \0 is the null character. Some DHCP clients (for example, Microsoft) send the client identifier in a \000foo format (with the null character prefix instead of just foo). The client identifier for the requesting host and the client identifier stored in the appliance must match.
   - Comment: Enter useful information about the roaming host.
   - Disabled: Select this if you do not want the DHCP server to use this roaming host definition. When you disable a roaming host, the host gets an IP address without the defined DHCP options.
6. Click Next to configure the DHCP options for the roaming host, as described in Defining Basic IPv4 Options on page 597.
7. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes on page 265.
8. Save the configuration and click Restart if it displays at the top of the screen.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.
Adding IPv6 Roaming Hosts

To add an IPv6 roaming host:

1. From the Data Management tab, select the DHCP tab.
2. Select a network view from the drop-down list.
3. Expand the Toolbar and click Add -> Roaming Host -> IPv6.
4. In the Add Roaming Host wizard, select one of the following and click Next:
   - Add IPv6 Roaming Host
   or
   - Add Roaming Host Using IPv6 Template
     Click Select IPv6 Template to create a roaming host using an IPv6 fixed address template. In the DHCP Template Selector dialog box, select the template that you want to use. Note that when you use a template to create a roaming host, the configurations of the template apply to the new host. The appliance automatically populates the host properties in the wizard. You can then edit the pre-populated properties.
5. Complete the following:
   - Name: Enter the name of the roaming host. The name must be unique for each roaming host in a given network view.
   - DUID: Enter the DHCP unique identifier of the host.
   - Comment: Optionally, enter additional information about the roaming host.
   - Disabled: Select this if you do not want the DHCP server to use this roaming host definition. When you disable a roaming host, the host gets an IP address without the defined DHCP options.
6. Click Next to configure the DHCP options for the roaming host, as described in Defining General IPv6 Properties on page 606.
7. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes on page 265.
8. Save the configuration and click Restart if it displays at the top of the screen.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.

Adding IPv4/IPv6 Roaming Hosts

To add an IPv4/IPv6 roaming host:

1. From the Data Management tab, select the DHCP tab.
2. Select a network view from the drop-down list.
3. Expand the Toolbar and click Add -> Roaming Host -> Both.
4. In the Add Roaming Host wizard, select one of the following and click Next:
   - Add Roaming Host
   or
   - Add Roaming Host using Both IPv4 and IPv6 Templates
     When you use both templates to create a roaming host, the appliance applies the IPv4 template and then the IPv6 template. Therefore, the comments and extensible attributes from the IPv6 template override those from the IPv4 template.
5. Complete the following:
   - **Name:** Enter the name of the roaming host. The name must be unique for each roaming host in a given network view.
   - **Assign IP Address by:** Select one of the following criteria on which the appliance matches when assigning an IP address to the host.
     - **MAC Address:** Select this to assign a dynamic IP address to a host, provided that the MAC address of the requesting host matches the MAC address that you specify here.
     - **DHCP Client Identifier:** Select this to assign a dynamic IP address to a host with the same DHCP client identifier that you specify here. When you select this, the **Match null (\0) at beginning of DHCP client identifier** check box is displayed. Select this when a DHCP client sends a \000 prefixed to the DHCP client identifier. \0 is the null character. Some DHCP clients (for example, Microsoft) send the client identifier in a \000foo format (with the null character prefix instead of just foo). The client identifier for the requesting host and the client identifier stored in the appliance must match.
     - **DUID:** Specify the DHCP unique identifier of the host.
   - **Comment:** If both IPv4 and IPv6 templates were used to create the host, this field displays the comment from the IPv6 template. You can change or add information.
   - **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 IPv4 DHCP options for the roaming host, as described in *Defining Basic IPv4 Options* on page 597.
7. Click **Next** to configure IPv6 properties described in *Defining General IPv6 Properties* on page 606.
8. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. If both IPv4 and IPv6 templates were used to create the host, this panel displays the attributes from the IPv6 template. You can change or add information. For information, see *Using Extensible Attributes* on page 265.
9. Save the configuration and click **Restart** if it displays at the top of the screen.

   or

   - Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 256.

**Viewing Roaming Hosts**

To view a list of roaming hosts in a specific network view:

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Roaming Hosts**.
2. From the **Network View** drop-down list, select the network view to which the roaming hosts belong.
3. The Grid Manager displays the following for each roaming host:
   - **Name:** The name of the roaming host.
   - **Address:** The IP address of the roaming host.
   - **Comment:** The information that you entered for the roaming host.
   - **Site:** The site to which the template belongs. This is one of the predefined extensible attributes.

You can select **Disabled** and available extensible attributes for display.

You can also do the following:

- Sort the displayed data in ascending or descending order by column.
- Use filters and the **Go to** function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the **Go to** field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see *Using Quick Filters* on page 57.
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see *Modifying Data in Tables* on page 52.
Setting Properties for Roaming Hosts

You can modify an existing roaming host to add, modify or delete IPv4 or IPv6 addresses, and to set IPv4 and IPv6 DHCP properties.

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Roaming Hosts section -> roaming_host check box, and then click the Edit icon.

2. The Roaming Host editor contains the following tabs from which you can modify data:
   - General: Edit the fields as described in Adding IPv4 Roaming Hosts on page 660, except for the Templates field.
   - IPv4 DHCP Options: Keep the inherited DHCP options or override them and enter unique settings for the roaming host. For information, see Defining Basic IPv4 Options on page 597.
   - IPv6 DHCP Options: Keep the inherited IPv6 DHCP properties or override them. For more information, see Defining General IPv6 Properties on page 606.
   - 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 265.
   - 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.
   - IPv4 DDNS: Click Override and select Enable DDNS updates for the DDNS settings you configure in this tab to take effect. You can specify the following:
     - DDNS Domain Name: Specify the domain name that the appliance uses to update DNS.
     - DDNS Hostname: Select the Replace the host name dynamically provided by the client/member with the roaming host name check box to use the name of the roaming host record as the name of the client for DDNS updates.
   
4. Save the configuration and click Restart if it appears at the top of the screen.

   or

   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.
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 256.

   The Grid Manager puts the deleted roaming host in the Recycle Bin, if enabled.
Chapter 23  DHCP Failover

This chapter explains how to configure DHCP failover associations. It contains the following sections:

- **About DHCP Failover** on page 666
  - **Failover Association Operations** on page 666
- **Configuring Failover Associations** on page 667
  - **Adding Failover Associations** on page 668
- **Managing Failover Associations** on page 670
  - **Modifying Failover Associations** on page 670
  - **Monitoring Failover Associations** on page 671
  - **Deleting Failover Associations** on page 672
  - **Setting a Peer in the Partner-Down State** on page 672
  - **Performing a Force Recovery** on page 672
About DHCP Failover

You can create a failover association between two DHCP servers (a primary server and a secondary) and assign the failover association to serve an IPv4 DHCP range. When you set up a failover association, you greatly reduce DHCP service downtime if one of your DHCP servers is out of service. You can better manage IP address requests by making two servers available for DHCP services. You can also configure one of the servers to assume full DHCP services when you know the other server may go out of service for a period of time.

You can configure two NIOS appliances, or one appliance and one external server, to form a failover association. The pairing of a primary and secondary server is called a peer association. The failover peers establish a TCP connection for their communication. They share a pool of IP addresses that they allocate to hosts on their networks based on load balancing. Load balancing is a technique to split the address allocation workload evenly across the two DHCP servers. You can assign a DHCP failover association to serve DHCP ranges in a network. A DHCP failover association can serve DHCP ranges that belong to one network view only. It cannot serve ranges in different network views.

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 23.1, when a host broadcasts a DHCPDISCOVER message, both the primary and secondary servers receive the message. They perform a hash operation on the MAC address in the DHCPDISCOVER message, and the result is 250. Since the load balancing split is 50% and the hash result is 250, the secondary server responds to the host with a DHCPOFFER message. The secondary peer allocates an IP address from its assigned pool of IP addresses. It then sends a lease update message to the primary server so that the primary server knows how the address is assigned and can properly take over if the secondary server fails.

Figure 23.1 Load Balancing and IP Addresses Allocation

1. When a host broadcasts a DHCPDISCOVER message, it includes its MAC address.
2. Both servers receive the DHCPDISCOVER message. Each server performs a hash on the MAC address, and the result is 250.
3. The load balancing split is 128. Since the hash result is between 128 and 255, the secondary server responds to the host and allocates the IP address to the host.
Configuring Failover Associations

1. Grid: From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar. Click Toggle Expert Mode if the editor is in basic mode. When the additional tabs appear, select the General Advanced tab to complete the following:
   - Failover Port: You can modify the port number that members use for failover associations. You can use any available port from 1 to 63999. The default is 647 for a new installation and 519 for an upgrade.

The following are tasks and guidelines for configuring a DHCP failover:

1. Identify the primary and secondary DHCP servers and ensure that the appliances are set up correctly for the failover association, using the following guidelines:
   - Configure a failover association using two NIOS appliances, or a NIOS appliance and an ISC DHCP compliant server.
   - One of the DHCP servers must be an independent appliance or in an Infoblox Grid.
   - The DHCP servers do not have to be in the same geographic location.
   - The clocks on both servers must be synchronized. This happens automatically when both servers are on the same Grid.
   - Both servers must use the same version of the DHCP configuration file. This happens automatically when both servers are on the same Grid.
   - If you use firewalls on your networks, ensure that the firewalls allow TCP port 519 between the servers, and that TCP port 7911 is open for partner down operations.
   - Each pair of DHCP servers can participate in only one failover association. An appliance can participate in more than one failover association, as long as it is with a different peer.

Configure the same DHCP properties on the primary and secondary servers, as described in Configuring General IPv4 DHCP Properties on page 590.
   - 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 668.
   - 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 IPv4 networks and DHCP ranges in the same network view. Failover associations can serve only IPv4 DHCP ranges. For information, see Configuring IPv4 Address Ranges on page 650.
   - 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 670.

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 -> Members tab -> IPv4 Failover Associations section, and then click the Add icon.
   or
   Expand the Toolbar and click Add -> IPv4 Failover Association.

2. In the Add Failover Association wizard, complete the following:
   - Name: Enter a unique name for the failover association. The failover association name is case sensitive. Enter the same name on both the primary and secondary servers. The appliance validates the names on both servers. The names must be exactly the same. If they do not match, the failover association goes into disconnect mode.
   - DHCP Failover Primary: Select one of the following. The default is Grid Member.
     - Grid Member: Click Select member. In the Select Member dialog box, select the primary server and click the Select icon.
     - 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.
   - Comment: Enter useful information about the failover association.

3. Click Next and do the following to control the IP address allocation between the peers and how they switch from one to the other based on the configuration:
   - 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 responds to all IP address requests, and the secondary server does not respond to any. The opposite applies when you move the slider all the way to the right. Infoblox recommends that you use the default (50/50) to enable the primary and secondary servers to respond to IP address requests on an equal basis.
— **Lease Deletion**: Select the following to override settings at the Grid and member levels.
  
  — **Keep leases from deleted ranges until one week after expiration**: When you select this and delete a DHCP range with active leases, the appliance stores these leases up to one week after they expire. When you add a new DHCP range that includes the IP addresses of these active leases, the appliance automatically restores the leases.

4. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see *Using Extensible Attributes* on page 265.

5. Save the configuration and click **Restart** if it displays at the top of the screen.
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 671
- Deleting Failover Associations on page 672

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 672
- Performing a Force Recovery on page 672

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 668. 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 in the Basic tab, see Adding Failover Associations on page 668. The following are the triggers in the Advanced tab:
     - **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.
Managing Failover Associations

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 265.

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.

In this panel, you can also modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables on page 52.

To monitor the failover association status:

1. From the Data Management tab, select the DHCP tab -> Members tab -> IPv4 Failover Associations section. Grid Manager displays the list of failover associations and their overall status.
2. To view detailed information about a failover association, select the failover_association check box, and then click the Show Status icon.
3. In the Failover Association Status dialog box, Grid Manager displays the overall status of the failover association and the status of both the primary and secondary servers.

The failover association can be in one of the following states:

- **OK** (green): The failover association is functioning properly.
- **DEGRADED** (yellow): The failover association is degraded when one of the peers is giving out limited addresses.
- **FAILURE** (red): The failover association is not functioning. 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 peer responds to DHCP clients.
- **PAUSED**: This state allows a peer to inform the other peer that it is going out of service for a short period of time so the other peer can immediately transition to the COMMUNICATIONS-INTERRUPTED state and start providing DHCP service to DHCP clients.
- **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.
- **POSSIBLE-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.
- **SHUTDOWN**: This state allows a peer to inform the other peer that it is going out of service for a long period of time so the other peer can immediately transition to the PARTNER-DOWN state and completely assume control of the DHCP service.
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 all 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 24  Configuring IPv4 DHCP Filters

This chapter explains how to configure IPv4 DHCP filters. It contains the following sections:

- **About IPv4 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 683
  - *Defining Relay Agent Filters* on page 684
- **About Option Filters** on page 685
  - *Defining Option Filters* on page 687
  - *Configuring User Class Filters* on page 690
  - *Configuration Example: Using Option Filters* on page 691
- **Applying Filters to DHCP Address Ranges** on page 692
  - *Adding Filters to the Class Filter List* on page 692
  - *Adding Filters to the Logic Filter List* on page 692
  - *Configuration Example: Using the Class and Logic Filter Lists* on page 694
- **Managing DHCP Filters** on page 697
  - *Modifying DHCP Filters* on page 697
  - *Viewing DHCP Filters* on page 698
  - *Deleting Filters* on page 699
About IPv4 DHCP Filters

To control how the appliance allocates IPv4 addresses, you can define DHCP filters and apply them to address ranges and range templates. Depending on your configuration, DHCP filters screen requesting clients by matching MAC addresses, relay agent identifiers, or DHCP options you define in the filters. If you configure DHCP servers in the Grid to send authentication requests to a RADIUS authentication server group, you can also filter requests by matching the authentication results. (For information about this feature, see Chapter 25, Authenticated DHCP, on page 701.) When you define DHCP filters, you classify DHCP clients based on the information provided by the clients or by the RADIUS server. When you apply filters to an address range, the appliance responds to your address requests based on your configuration. The appliance also decides which DHCP options to return to the matching clients based on how you apply the filters. For more information, see Applying Filters to DHCP Address Ranges on page 692.

You can use filters to control address allocation based on your network requirements. For example, you can use DHCP filters to screen unmanaged hosts on a network by denying their address and option requests. If you have multiple DHCP address ranges on the same network and you want to assign IP addresses from specific address ranges to specific clients, you can use filters to screen the address assignments. For information, see IP Address Allocation.

The appliance supports the following filters:

- MAC address filters 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 683.
- 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 685.
- 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 25, Authenticated DHCP, on page 701.

You can use MAC, option, and NAC filters to define DHCP options that matching clients can receive. Depending on how you apply a filter to an address range, all DHCP clients with matching criteria can receive all or some of the DHCP options defined in the filter. DHCP options defined for a matching filter supersede those defined at the Grid, member, network, and DHCP range levels. Options defined for a filter that is in the Class Filter List of an address range supersede those defined in the Logic Filter List. For more information about how the appliance returns options and how to apply DHCP filters, see Applying Filters to DHCP Address Ranges on page 692.

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 24.1, 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 24.2 on page 676.
Configuring IPv4 DHCP Filters

The addressing scheme depicted in *Figure 24.1* on page 675 and *Figure 24.2* 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 24.3* 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.
IP Address Allocation Using Filters

To control the assignment of addresses from specific address ranges to specific hosts, the NIOS appliance provides the following filters:

- A MAC address filter to which you add MAC addresses as filter criteria. For information, see About MAC Address Filters on page 680.
- A relay agent filter with configured circuit ID and remote ID as specified by the relay agent (DHCP option 82). For information, see About Relay Agent Filters on page 683.
- An option filter in which you specify DHCP options and matching values. For information, see About Option Filters on page 685.
- A NAC filter in which you specify authentication results from a RADIUS authentication server group as filter criteria. For information, see About NAC Filters on page 730.

When the appliance receives an address request, it checks if the request matches a filter. If it does not, the appliance assigns an address from the address range with the highest available IP address. If the request matches at least one class filter for a range, the appliance applies the following rules:

- If there are grant address filters applied to that range, the request must match one of the class filters or the appliance does not grant an address from that range.
- If there are deny address filters applied to that range, the request must not match any of the filters. If the request matches a deny filter, the appliance does not grant an address from that range.
- If an address range has a combination of grant and deny filters, the request must:
  - Match a grant filter
  - Not match a deny filter

If more hosts request addresses, the appliance continues to assign them from address range 2—the 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.
Two rules govern the behavior of the appliance in relation to DHCP filters:

1. Depending on your filter configuration, the appliance checks if any data in an address request (such as the MAC address of the client, DHCP options 77 and 82, etc.) matches any filters applied to an address range.

2. The appliance checks for available addresses in the address ranges containing the highest addresses first. (“Highest” means closest to 255.255.255.255, and “lowest” means closest to 0.0.0.0.)

These two rules can work in coordination. For example, when the appliance receives an address request, it first checks if the request matches any filter. If it matches more than one filter assigned to different address ranges, the appliance first applies the filter that belongs to the range with the highest IP addresses. If that address does not grant an address lease (because the filter action is Deny or all address leases in that range are already in use), the appliance then applies the matching filter for the range with the next higher set of IP addresses. If the appliance still has not granted a lease from the address ranges whose filters match data in the request and there are unfiltered address ranges, the appliance attempts to assign an address from one of these ranges, again beginning with the range having the highest IP addresses. Figure 24.4 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 24.4 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</td>
</tr>
<tr>
<td>address range,</td>
<td>is deny or the action is grant but all addresses in that range are in use), the appliance then checks if it can assign an</td>
</tr>
<tr>
<td></td>
<td>address from an unfiltered address range (if there are any), starting with the range with the highest addresses first, as shown</td>
</tr>
<tr>
<td></td>
<td>in Figure 24.3 on page 677.</td>
</tr>
<tr>
<td>the same filter applies to multiple address ranges and the</td>
<td>it checks the address range with the highest IP addresses matching that filter. If the appliance does not assign an address</td>
</tr>
<tr>
<td>appliance receives an address request matching that filter,</td>
<td>from that range, it checks the filtered address range with the next highest IP addresses, and so on. If it still has not</td>
</tr>
<tr>
<td></td>
<td>assigned an address, the appliance starts checking unfiltered address ranges (if there are any), again beginning with the</td>
</tr>
<tr>
<td></td>
<td>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 requesting client matches both a MAC address filter (granting</td>
</tr>
<tr>
<td>other (one filter grants a lease and another denies it) and a</td>
<td>a lease) and a user class filter (denying a lease) for the same address range, the appliance denies the lease. When faced</td>
</tr>
<tr>
<td>requesting client matches both filters,</td>
<td>with a choice to either allow or deny a lease based on equal but contradictory filters, the appliance takes the more secure</td>
</tr>
<tr>
<td></td>
<td>stance of denying it.</td>
</tr>
</tbody>
</table>
About MAC Address Filters

The appliance can filter an address request by the MAC address of a requesting host. Depending on how you apply the MAC filter, the appliance can grant or deny the address request if the requesting host matches the filter criteria. You can also define DHCP options that you want to return to the matching client if the options are so configured. The client can also request specific options to be returned through DHCP option 55. The appliance returns DHCP options to matching clients based on how you apply the filters. For information, see Applying Filters to DHCP Address Ranges on page 692.

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 or range template, and specify that if the MAC address of a requesting host matches the filter definition, the appliance either grants or denies the address assignment. For information, see Applying Filters to DHCP Address Ranges on page 692.

Defining MAC Address Filters

To define a MAC address filter:
1. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab, and then expand the Toolbar and click Add -> IPv4 MAC Address Filter.
   or
   From any panel in the DHCP tab, expand the Toolbar and click Add -> IPv4 MAC Address Filter.
2. In the Add IPv4 MAC Filter wizard, complete the following:
   — Name: Enter a meaningful name for the filter. For example, if you want to filter address requests by department, you can name one filter “Marketing”, another “Finance”, and so on. The name must be unique within a specific network. If you want to specify option settings in the filter, the filter name must be unique among all MAC filters.
   — Comment: Enter useful information about the filter.
3. Click Next and complete the following to define the DHCP options to return to the matching client:
   — Option Space: Select an option space from the drop-down list. This field is displayed only when you have custom option spaces. The appliance uses the DHCP option space as the default.
   — Lease Time: Enter the value of the lease time in the field and select the time unit from the drop-down list. The lease time applies to hosts that meet the filter criteria.

Options to Merge with Object Options
Click the Add icon. Grid Manager adds a new row to the table with the default DHCP option space and option name displayed. Complete the following:
   — Option Space: Click the down arrow and select an option space from the drop-down list. The selected option space contains the corresponding DHCP options.
   — Option Name: Click the down arrow and from the drop-down list, select the DHCP option you want to return to the requesting host.
   — Value: Enter the value that you want the filter to return for the selected DHCP option. For example, enter the value 255.255.255.0 for the subnet-mask option.
To add more options to the filter, click the Add icon and repeat the steps.
4. Click **Next** and complete the following to configure the expiration setting:

   — **Default MAC Address Expiration**
     Select one of the following to configure the expiration setting for the filter:
     - **Never Expires**: Select this if you want the MAC address filter to never expire. This is selected by default.
     - **Automatically Expires in**: Select this if you want the filter to expire after a specific time frame. You can specify the time in seconds, minutes, hours, or days.

     The filter expiration time you configure here affects how long the DHCP server grants a lease to a client. It has an upper limit of 15 minutes on the lease time you configure for the Grid. For example, if both the filter expiration time and the lease time are less than 15 minutes, the appliance uses the lease time. If both 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.

   — **Enforce Expiration Times**: Select this to enable the expiration setting.
   — **Enabled**: The filter is enabled by default. Clear the check box to disable this filter.

5. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see *Using Extensible Attributes* on page 265.

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

### Adding MAC Address Filter Items

To add a MAC address to a MAC address filter:

1. From the **Data Management** tab, select the **DHCP** tab ->**IPv4 Filters** tab, and then expand the Toolbar and click **Add** ->**IPv4 MAC Address Filter Item**.

   or

   From any panel in the **DHCP** tab, expand the Toolbar and click **Add** ->**IPv4 MAC Address Filter Item**.

2. In the **Add IPv4 MAC Address Filter Item** wizard, complete the following:

   — **MAC Address 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.
3. Click **Next** and select one of the following to configure user registration (optional):
   - **Register as User**: Select this and enter a username in the field.
   - **Register as Guest**: Select this and enter the first name, middle name, last name, email address, and phone number of the guest user.
   
   The appliance displays the information you enter here in the lease viewers.

4. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes on page 265.

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

After you define a MAC address filter and add MAC addresses to it, you can assign the filter to a DHCP range. The appliance filters IP address requests based on the filter criteria. For information, see Applying Filters to DHCP Address Ranges on page 692.
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 602. 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 24.5*. 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 24.5 Relay Agent Filtering*

To apply a relay agent filter to an address range:

1. Define a relay agent filter. For information, see *Defining Relay Agent Filters*.
2. Apply the filter to a DHCP address range or range template, and specify that if the circuit ID or remote ID of a requesting host matches the filter definition, the appliance either grants or denies the address assignment. For information, see *Applying Filters to DHCP Address Ranges* on page 692.
3. Define the access privileges of limited-access admin group for relay agent filters. For information, see *Managing Administrators* on page 109.
Defining Relay Agent Filters

To define a relay agent filter:

1. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab, and then expand the Toolbar and click Add -> IPv4 Relay Agent Filter.

   or

   From any panel in the DHCP tab, expand the Toolbar and click Add -> IPv4 Relay Agent Filter.

2. In the Add IPv4 Relay Agent Filter wizard, complete the following:
   - **Name**: Enter a meaningful name for the filter. For example, you can enter the IP address or the name of the router acting as the relay agent. The name must be unique within a specific network.
   - **Comment**: Enter useful information about the filter.

3. Click **Next** to define the relay agent ID type. If you apply both ID types, the relay agent must provide both identifiers when submitting a DHCP address request.
   - Select one of the following for both Circuit ID and Remote ID:
     - **Any**: Select this and the filter matches any of the circuit identifiers for remote hosts. You cannot select this for both circuit ID and remote ID at the same time.
     - **Not Set**: Select this and no circuit identifier is set for remote hosts.
     - **Matches Values**: Select this and enter the circuit ID or remote ID. You can enter the ID in hexadecimal format, such as 1f:cd, ab, or ef:23:56, or in string format, such as abcd or aa:gg. The appliance matches the value you enter here with the value sent by the DHCP client in counted octet sequence format.

4. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes on page 265.

5. Save the configuration and click **Restart** if it displays at the top of the screen.

   After you define a relay agent filter, you can assign it to a DHCP range. The appliance responds to address requests based on the filter criteria. For information, see Applying Filters to DHCP Address Ranges on page 692.
About Option Filters

You can use option filters to classify DHCP clients and decide which DHCP options each group of clients can receive. By default, regardless of the networks in which the DHCP clients reside and whether an option filter is applied to a DHCP range or range template, all DHCP clients that match the filter criteria receive the DHCP options and values you define in the filter. You can change this configuration so the appliance does not use the filter to classify DHCP clients. For information about how to configure this, see Defining Option Filters on page 687.

You can add DHCP options and the Hardware Operator option to an option filter. (For information about the Hardware Operator option, see DHCP Hardware Operator.) Depending on whether the options you add to the filter are also defined at the Grid, member, network, and DHCP range levels, and whether you add the filter to the Class Filter List or Logic Filter List of a range or range template, the appliance either appends them to the existing options or overwrites the option values before returning them to the matching clients. For more information about how the appliance returns DHCP options, see Adding Filters to the Logic Filter List on page 692.

The appliance can filter an address request by the options (such as root-server-ip-address or user-class) of the requesting host. Depending on how you apply an option filter, the appliance can grant or deny an address request if the requesting host matches the filter criteria. You can also create complex match rules that use the AND and OR logic to further define the filter criteria. When you select match rules in Grid Manager, you can preview the rules before committing them to the filter. Grid Manager provides an expression builder that automatically builds the rules after you define them. For information, see Defining Option Filters on page 687.

To define an option filter and apply it to an address range:

1. Define an option filter based on either the predefined or custom DHCP options. For information, see Defining Option Filters.

2. Apply the filter to a DHCP address range or range template in the Class Filter List or Logic Filter List. For information, see Applying Filters to DHCP Address Ranges on page 692.

After you define an option space and add options to it, you can set up option filters and define option values. For example, to handle two different client classes, you can define two option filters (vendor-class_1 and vendor-class_2) and send different option values to different clients based on the vendor-class-identifier options that you obtain from the clients.
DHCP Hardware Operator

You can define the Hardware Operator option and add it as a match rule to an option filter. This option enables the appliance to match the hardware type and MAC address of the DHCP client, which it derives from the htype (hardware type), hlen (hardware length) and chaddr (client hardware address) fields of the client’s DHCP Discover and Renew packets.

To add Hardware Operator to an option filter, fill in the fields as follows:

- In the first drop-down list, select **Hardware Operator**. Note that because it is not a DHCP Option, it does not have an actual option number.
- In the second drop-down list, select one of the following operators: **equals**, **does not equal**, **substring equals** and **substring does not equal**.
  
  If the operator is **substring equals** or **substring does not equal**, specify the offset and length.
- In the text field, enter the string that represents the hardware type and MAC address to match. For example, the htype value is 1 for the Ethernet hardware type. The hardware types (htype) are defined in RFC 1700, Assigned Numbers.

This filter rule assumes that the values exist in the DHCP packets.

The following table provides examples of rules that include the Hardware Operator option. The entry in the first drop-down list for all rules is **Hardware Operator**.

<table>
<thead>
<tr>
<th>Rule Description</th>
<th>Second Drop-Down List (operator)</th>
<th>Text Field (string)</th>
<th>Offset</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match a hardware type and MAC address.</td>
<td>equals</td>
<td>01:00:C0:B0:AA:BB:CC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Match hardware type only.</td>
<td>substring equals</td>
<td>01</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Match the vendor MAC prefix (first three bytes of MAC address).</td>
<td>substring equals</td>
<td>00:C0:B0</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>
Defining Option Filters

To define an option filter:

1. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab, and then expand the Toolbar and click Add -> IPv4 Option Filter.

   or

   From any panel in the DHCP tab, expand the Toolbar and click Add -> IPv4 Option Filter.

2. In the Add IPv4 Option Filter wizard, complete the following:
   - **Name**: Enter a meaningful name for the option filter. For example, you can enter Linux if you plan to use this option filter to screen Linux systems. The name must be unique within a specific network. If you want to specify option settings in the filter, the filter name must be unique among all option filters.
   - **Comment**: Enter useful information about the filter.
   - **Apply this filter as a global DHCP class**: This check box is selected by default. When you select this check box, the appliance defines a global class statement in the dhcpd configuration file for members that have DHCP enabled, regardless of whether the filter is applied to a DHCP range or range template. All DHCP clients that belong to this class receive the DHCP options and values you define in the filter. When you clear this check box, you cannot apply this filter to the Class Filter List of a range or range template. You cannot clear this check box if the filter is currently applied to a range or range template. The appliance displays an error message when you try to save this configuration.

3. Click Next and complete the following to add match rules:
   - In the first drop-down list, select a DHCP option. For example, select user-class (77) for a specific user class, such as mobile users.
   - In the second drop-down list, select an operator. If you select equals or does not equal, enter the value of the selected option you want the filter to match in the field.
   - If your operator and match value include a substring of an option value, enter the offset and length of the substring based on the following definitions:
     - **Offset**: Enter the number of characters at which the match value substring starts in the option data. Enter 0 to start at the beginning of the option data, enter 1 for the second position, and so on. For example, when you enter 2 and have a match value of MSFT, the appliance matches the value MSFT starting at the third character of the option data.
     - **Length**: Enter the length of the match value. For example, if the match value is MSFT, the length is 4.
   
   You can do the following and repeat the filter selection steps to add another rule:
   - Click + to add another rule at the same level.
   - Click [<<] to add an all (logical AND) or any (logical OR) operator line and a parenthetical rule that is indented one level and above the first rule.
   - Click [>>] to add an all (logical AND) or any (logical OR) operator line and a parenthetical rule that is indented one level.

   After you add all the match rules, you can click Preview to view the rules that are written to the dhcpd configuration file or click Reset to remove the previously configured rules and start again. For information about how to use match rules, see Using Match Rules in Option Filters on page 689.

4. Click Next and complete the following to define which DHCP options to return to the matching client:
   - **Option Space**: Select an option space from the drop-down list. This field is not displayed if you do not have custom option spaces. The appliance uses the DHCP option space as the default.
   - **Lease Time**: Enter the value of the lease time in the field and select the time unit from the drop-down list. The lease time applies to hosts that meet the filter criteria.

   **Options to Merge with Object Options**

   Click the Add icon. Grid Manager adds a new row to the table with the default DHCP option space and option name displayed. Complete the following:
— **Option Space**: Click the down arrow and select an option space from the drop-down list. The selected option space contains the corresponding DHCP options that you can use as filter criteria.

— **Option Name**: Click the down arrow and from the drop-down list, select the DHCP option you want to use as filter criteria.

— **Value**: Enter the match value that you want the filter to use for the selected DHCP option.

To add more options to the filter, click the Add icon and repeat the steps.

5. Click **Next** to define extensible attributes. For information, see *Using Extensible Attributes* on page 265.

6. Save the configuration and click **Restart** if it appears at the top of the screen.
Using Match Rules in Option Filters

Each match rule you define in an option filter further defines the filter criteria of a matching client. You can add multiple match rules to an option filter. The appliance writes these rules to the dhcpd configuration file. You can also create complex match rules that use the AND and OR logic to further define the filter criteria. After you define the match rules, you can preview the rules before committing them to the filters.

For example, you can define the following rules in an option filter:

**DHCP option = vendor-class-identifier**

Substring offset = 0 (the match value starts at the beginning of the option data received from the client)
Substring length = 4 (the length of the match value MSFT)
Match value = MSFT

The appliance generates the following rules in the dhcpd configuration file:

```
class "microsoft-other" {  
  match if (option vendor-class-identifier,  
            0, 4) = "MSFT";  
  vendor-option-space MSFT;  
}
```

You can also define more complex rules using the AND and OR logic as follows:

**DHCP option = vendor-class-identifier**

Match value = infoblox2000a

**OR**

**DHCP option = vendor-encapsulated-options**

Substring offset = 0 (the match value starts at the first character of the option data received from the client)
Substring length = 8 (the length of the match value infoblox)
Match value = infoblox

**AND**

**DHCP option = vendor-encapsulated-options**

Substring offset = 10 (the match value starts at the ninth character of the option data received from the client)
Substring length = 5, the length of the match value 2000a
Match value = 2000a

The appliance generates the following rules in the dhcpd configuration file:

```
class "infoblox" {  
  match if (option vendor-class-identifier=infoblox2000a;) or  
         ((substring(option vendor-encapsulated-options,0,8)="infoblox") and  
          (substring(option vendor-encapsulated-options,10,5)="2000a"));  
  vendor-option-space DHCP  
}
```
Configuring User Class Filters

The NIOS appliance can filter DHCP address requests by user class filters. A user class indicates a category of user, application, or device of which the DHCP client is a member. User class identifiers are configured on DHCP clients and are sent during a DHCP address request operation. The client includes the user class identifier in DHCP option 77 when sending DHCPDISCOVER and DHCPREQUEST messages.

By using user class identifiers, a DHCP server can screen address requests and assign addresses from select address ranges based on the different user class identifiers it receives. For example, if you assign a user class filter named mobile to a range of addresses from 10.1.1.31–10.1.1.80, the appliance selects an address from that range if it receives an address request that includes the user class name mobile and there are still addresses available in that range. You might want mobile users to receive these addresses because you have given them shorter lease times than other, more stationary DHCP clients. See Figure 24.6.

Figure 24.6 Applying User Class Filtering

The user class for laptop A is mobile. When it sends DHCPDISCOVER and DHCPREQUEST messages, it includes its user class in the DHCP option 77 field.

The NIOS appliance has a filter that screens address requests by user class. If the user class for a DHCP client is mobile, the appliance assigns it an address from address range 2.

Note: The leases for addresses in address range 2 are shorter than those for more stationary computers. The intended use for address range 2 is to provide IP addresses for mobile users who log in to the network for relatively short periods of time and, therefore, do not require longer leases.

If the NIOS appliance receives address requests with the user class mobile and there are no available addresses in address range 2 but there are available addresses in ranges 1 and 3, the appliance begins assigning addresses from address range 3 (because its addresses are higher than those in range 1). Then, if all addresses in range 3 are in use, the appliance begins assigning addresses from address range 1. If you want the appliance to assign addresses to mobile users (that is, those identified with the user class mobile) exclusively from address range 2, then you must apply user class filters for “mobile” to address ranges 1 and 3 that deny lease requests matching that user class.
### Configuration Example: Using Option Filters

The following example shows you how to create an option space, add custom options to it, create an option filter, and a match rule to filter the options so that the NIOS appliance can filter an address request by the vendor options of the requesting hosts. It can grant or deny an address request if the requesting host matches the filter.

1. Add an option space called MSFT, and then add the following options to it. For information, see Applying DHCP Options on page 599.

<table>
<thead>
<tr>
<th>Option name</th>
<th>Code</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>root-mount-options</td>
<td>1</td>
<td>Text</td>
</tr>
<tr>
<td>root-server-ip-address</td>
<td>2</td>
<td>IP address</td>
</tr>
<tr>
<td>root-server-host-name</td>
<td>3</td>
<td>Text</td>
</tr>
<tr>
<td>root-server-path-name</td>
<td>4</td>
<td>Text</td>
</tr>
<tr>
<td>swap-server-ip-address</td>
<td>5</td>
<td>IP address</td>
</tr>
<tr>
<td>swap-file-path-name</td>
<td>6</td>
<td>Text</td>
</tr>
<tr>
<td>boot-file-path-name</td>
<td>7</td>
<td>Text</td>
</tr>
<tr>
<td>posix-timezone-string</td>
<td>8</td>
<td>String</td>
</tr>
<tr>
<td>boot-read-size</td>
<td>9</td>
<td>16-Bit unsigned integer</td>
</tr>
</tbody>
</table>

2. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab and click the Add icon.
3. In the Add IPv4 Filter wizard, enter the filter name i86pc, and then select Options as the filter type.
4. Select MSFT as the option space, select an option, specify a value for it, and then add it to the i86pc option filter. You can select multiple options. Add the following options to the i86pc option filter:

<table>
<thead>
<tr>
<th>Option name</th>
<th>Code</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>root-server-ip-address</td>
<td>2</td>
<td>IP address</td>
</tr>
<tr>
<td>root-server-host-name</td>
<td>3</td>
<td>Text</td>
</tr>
<tr>
<td>root-server-path-name</td>
<td>4</td>
<td>Text</td>
</tr>
<tr>
<td>boot-file-path-name</td>
<td>7</td>
<td>Text</td>
</tr>
</tbody>
</table>

5. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab -> filter_name, and then click the Add icon.
6. In the Add IPv4 Match Rule wizard, select i86pc as the option filter, select vendor-class-identifier (60) as the matching option, and then enter MSFT as the matching value.
7. Add a DHCP range to the network. For information, see Configuring IPv4 Address Ranges on page 650.
8. Apply the i86pc option filter to the DHCP address range. For information, see Applying Filters to DHCP Address Ranges on page 692.
9. Click Restart to restart services.
Applying Filters to DHCP Address Ranges

To further control how the appliance allocates IPv4 addresses to DHCP client requests, you can apply DHCP filters to an address range or range template so the appliance can determine the following:

- The class statements
- The address ranges from which it assigns leases
- When to grant or deny leases to the matching clients
- Which DHCP options to return to the matching clients

Adding Filters to the Class Filter List

You can apply any DHCP filter to the Class Filter List of a DHCP range or range template. The appliance uses the matching rules of these filters to select the address range from which it assigns a lease. You can define permissions for these filters to instruct the appliance whether to grant or deny a lease to the matching client. When you add a filter with a grant permission, the client must match the filter criteria to receive a lease. When you define a filter with a deny permission, clients that do not match the filter criteria still receive leases. Only the client that matches the filter criteria is denied a lease.

Filters in the Class Filter List correspond to the class statement generated in the dhcpd configuration file, which is a classification of the client packet. All DHCP clients that match the option filter and relay agent filter criteria become members of the same class and are eligible to receive DHCP options for that class, regardless of the networks in which the clients reside. However, a client can only become a member of the MAC or NAC filter class when it is granted a lease from the DHCP range based on the filter criteria. Whether a client receives specific options and option values depends on the hierarchy of the options and how you apply the filters. For information about how the appliance returns DHCP options, see Adding Filters to the Logic Filter List.

Adding Filters to the Logic Filter List

The filters you add to the Logic Filter List correspond to the match rules that are written to the dhcpd configuration file. The appliance uses these filters to identify DHCP options and values to return to the matching clients. You can apply option, MAC, and NAC filters to the Logic Filter List. Note that a DHCP client is eligible to receive DHCP options defined in a filter if it matches the filter criteria. Whether the client receives specific options and their corresponding values depends on the hierarchy of the options and the list of options requested by the client through DHCP option 55. You can configure the appliance to ignore the option list requested by a matching client and return all the options that the client is eligible to receive. For information about how to ignore the option list requested by a client, see Configuring General IPv4 DHCP Properties on page 590.

The appliance decides which options and values to return to a client based on the following:

- If you have different DHCP options defined in a range and any DHCP filters in the Class Filter and Logic Filter lists, and these options do not overlap, the appliance merges and returns all options to the matching client. For example, a DHCP client obtains a lease from a DHCP address range (R) through an option filter in the Class Filter List (CF), which contains an option statement (O1) with a value of (S1). The appliance then matches a filter in the Logic Filter List (LF) that contains an option statement (O2) with a value of (S2). In this case, option statements O1 and O2 and their values S1 and S2 are merged and returned to the matching client.

- If there are overlapping DHCP options in a range and any DHCP filters in the Class Filter and Logic Filter lists, the values defined in the Class Filter List filters take precedence over those defined in the range and filters in the Logic Filter List. The appliance returns the option value defined in the class filters to the matching client. For example, a DHCP client obtains a lease from a DHCP address range (R) through an option filter in the Class Filter List (CF), which contains an option statement (O1) with a value of (S1). The appliance then matches a filter in the Logic Filter List (LF) that contains the same option statement (O1) with a value of (S2). In this case, the option value S1 defined in the option filter in the Class Filter List takes precedence and is returned to the DHCP client.
Applying Filters to DHCP Address Ranges

- When you apply option, MAC, and NAC filters to the Logic Filter List, the appliance translates their match rules into a DHCP if/elseif/else statement using the match rules of the first filter on the list as the “if” expression in the statement. Match rules in subsequent filters are translated into the “elseif” statements, and the last filter that does not contain any match rules is translated into the “else” statement. Note that a filter without any match rules can only be added as the last filter in the Logic Filter List.

For more information on how the appliance grants and denies leases to requesting clients and determines which DHCP options to return to the matching clients, see *Configuration Example: Using the Class and Logic Filter Lists* on page 694.

To apply filters to a DHCP address range:

1. From the Data Management tab, select the DHCP tab ->Networks tab ->Networks ->network ->addr_range check box, and then click the Edit icon.
2. In the DHCP Range editor, click Toggle Advanced Mode.
3. Click the IPv4 Filters tab.
4. Class Filter List: Click the Add icon to add a filter to identify the class of a matching client, and to grant or deny a lease to a client. For more information, see *Adding Filters to the Logic Filter List* on page 692. If you have only one configured DHCP filter, the appliance displays the filter in the table. Otherwise, in the DHCP Filter Selector dialog box, click the filter you want to add. Use SHIFT+click and CTRL+click to select multiple filters.

For each filter you add, click the Action column and select one of the following from the drop-down list:

- **Grant lease:**
  - For MAC address filters: Select this to assign an IP address from the address range to a requesting host whose MAC address matches the MAC address in the filter.
  - For relay agent filters: Select this to assign an IP address from the address range when one or both of the relay agent identifiers of the requesting host match the filter criteria.
  - For option filters: Select this to assign an IP address from the address range to a requesting host whose DHCP options match the DHCP options and match rules defined in the filter.
  - For NAC filters: Select this to assign an IP address from the address range to a requesting host based on the authentication results from a RADIUS authentication server group.

- **Deny lease:**
  - For MAC address filters: Select this to deny an address request from a host whose MAC address matches a MAC address in the filter.
  - For relay agent filters: Select this to deny an address request when one or both relay agent identifiers match the filter criteria in the filter.
  - For option filters: Select this to deny an address request from a host whose DHCP options match the options and match rules in the filter.
  - For NAC filters: Select this to deny an address request from a host based on the authentication results from a RADIUS authentication server group.

5. Logic Filter List: Click the Add icon to add a filter to match a client based on the match rules defined in the filter. The appliance uses filters in both the Class Filter and Logic Filter lists to determine the DHCP options and values it returns to the matching clients. For more information, see *Adding Filters to the Logic Filter List* on page 692. If you have only one configured DHCP filter, the appliance displays the filter in the table. Otherwise, in the DHCP Filter Selector dialog box, click the filter you want to add. Use SHIFT+click and CTRL+click to select multiple filters.

**Note:** You can only add a filter that does not contain any match rules as the last filter in the Logic Filter List.

6. Save the configuration and click Restart if it appears at the top of the screen.
Configuration Example: Using the Class and Logic Filter Lists

The following example shows you how to define DHCP filters and apply them to the class and logic filter lists. It also shows you the DHCP configuration file that is generated based on the configuration.

In this example, you first define a MAC filter, two option filters (one without match rules), and a NAC filter, and then apply the MAC filter to the Class Filter List and the other filters to the Logic Filter List of the address range 10.34.34.6 - 10.34.34.55.

1. Configure and save a MAC filter as follows. For more information, see Defining MAC Address Filters on page 680.
   a. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab, and then expand the Toolbar and click Add -> IPv4 MAC Address Filter.
   b. In the Add IPv4 MAC Filter wizard, complete the following:
      — Name: Enter MAC1.
   c. Click Next and complete the following to define the DHCP options to return to the matching client:
      — Lease Time: Enter 1234 and select seconds from the drop-down list.
      Options to Merge with Object Options: Click the Add icon. Grid Manager adds a new row to the table with the default DHCP option space and option name displayed. Complete the following:
      — Option Name: Click the down arrow and select log-server(7) from the drop-down list.
      — Value: Enter 10.34.34.3 as the value for the log-server option that is sent to the client in the OFFER/ACK message.
   d. Save the configuration.

2. Add a MAC address filter item as follows. For more information, see Adding MAC Address Filter Items on page 681.
   a. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab, and then expand the Toolbar and click Add -> IPv4 MAC Address Filter Item.
   b. In the Add IPv4 MAC Address Filter Item wizard, complete the following:
      — MAC Address Filter: Click Select Filter. In the DHCP Filter Selector dialog box, click MAC1.
      — MAC Address: Enter AB:DE:CC:DD:EE:01 as the MAC address.
   c. Save the configuration.

3. Configure and save an option filter with match rules as follows. For more information, see Defining Option Filters on page 687.
   a. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab, and then expand the Toolbar and click Add -> IPv4 Option Filter.
   b. In the Add IPv4 Option Filter wizard, complete the following:
      — Name: Enter Option1.
   c. Click Next and complete the following to add match rules:
      — In the first drop-down list, select vendor-class-identifier.
      — In the second drop-down list, select substring equals, and then enter the following:
        • Offset: Enter 0 to match the value starting at the first character of the option data.
        • Length: Enter 4.
        • Enter MSFT as the matching value.
      Click Preview and the appliance displays the expression: (vendor-class-identifier,0,4="MSFT").
Applying Filters to DHCP Address Ranges

4. Configure and save another option filter without match rules as follows:
   a. In the Add IPv4 Option Filter wizard, complete the following:
      — Name: Enter Option2.
   b. Click Next. Do not define any match rules.
   c. Click Next again and complete the following to define the DHCP options to return to the matching client:
      Options to Merge with Object Options: Click the Add icon. Grid Manager adds a new row to the table with
      the default DHCP option space and option name displayed. Complete the following:
      — Option Name: Click the down arrow and from the drop-down list, select domain-name(6).
   d. Save the configuration.

5. Configure and save a NAC filter as follows. For more information, see Defining a NAC Filter on page 731.
   a. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab, and then expand the Toolbar and
      click Add -> IPv4 NAC Filter.
   b. In the Add Filter Wizard, complete the following and click Next:
      — Name: Enter NAC1.
   c. Create a rule as follows:
      — In the first drop-down list, select Compliance State.
      — In the second drop-down list, select equals.
      — In the third drop-down list, select Compliant.
      Click Preview and the appliance displays the expression: (Sophos.ComplianceState="Compliant").
   d. Click Next and complete the following to define DHCP options:
      — Lease Time: Enter 1000 and select seconds from the drop-down list.
      Options to Merge with Object Options: Click the Add icon. Grid Manager adds a new row to the table with
      the default DHCP option space and option name displayed. Complete the following:
      — Option Name: Click the down arrow and from the drop-down list, select cookies-servers(8).
      — Value: Enter 10.34.34.5.
   e. Save the configuration.

6. Apply the filters to the address range as follows. For more information, see Applying Filters to DHCP Address
   Ranges on page 692.
   a. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> 10.34.34.6-10.34.34.55
      check box, and then click the Edit icon.
   b. In the DHCP Range editor, click Toggle Advanced Mode.
   c. Click the IPv4 Filters tab and complete the following:
      Class Filter List: Click the Add icon and add MAC1 as a class filter. Click the Action column and select Grant
      lease from the drop-down list.
      Logic Filter List: Click the Add icon and add Option1, NAC1, and Option2 respectively as logic filters.
   d. Save the configuration.
The appliance generates the following information in the DHCP configuration file based on the filter configuration in this example:

```
# MAC filter "MAC1"
class "MAC1" {
    default-lease-time 1234;
    min-lease-time 1234;
    max-lease-time 1234;
    option log-servers 10.34.34.3;
}
# NAC filter "NAC1"
{option sophos.compliance
    state="compliant"
}
subnet 10.34.34.0 netmask 255.255.255.0 {
    pool {
        infoblox-range 10.34.34.6 10.34.34.55;
        range 10.34.34.6 10.34.34.55;
        option routers 10.34.34.1;
        # INFOBLOXMACFILTERDEBUGINFO: allow members of "MAC1";
        if (substring(option vendor-class-identifier,0,4)="MSFT") {
            # Option filter "Option1"
            option time-servers 10.34.34.2;
        }
        elsif (option Sophos.ComplianceState="Compliant") {
            # NAC filter "NAC1"
            default-lease-time 1000;
            min-lease-time 1000;
            max-lease-time 1000;
            option cookie-servers 10.34.34.5;
        }
        else {
            # Option filter "Option2"
            default-lease-time 2500;
            min-lease-time 2500;
            max-lease-time 2500;
            option domain-name "www.infoblox.com";
        }
    }
}
```

Depending on client requests and the matching criteria, the following scenarios can happen in this example:

If the requesting client matches the MAC1 and Option1 filters, the appliance returns the following:

- Lease time = 1234 seconds (from the MAC filter)
- Returned options:
  - Router(3) with a value of 10.34.34.1 (from the address range)
  - Log-server(7) with a value of 10.34.34.3 (from the MAC filter MAC1)
  - Time-server(4) with a value of 10.34.34.2 (from the option filter Option1)

If the requesting client matches the MAC1 and NAC1 filters, the appliance returns the following:

- Lease time = 1234 seconds (from the MAC filter MAC1)
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 698.
- Delete filters that are not in use. For information, see Deleting Filters on page 699.

Modifying DHCP Filters

To modify a filter:

1. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab -> filter_name check box, and then click the Edit icon.

2. For a MAC address filter:
   - The DHCP MAC Filter editor contains the following tabs from which you can edit data:
     - General: Modify the fields as described in Defining MAC Address Filters on page 680.
     - DHCP Options: Add or delete DHCP options. For information, see 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 265.
     - Permissions: This tab appears only if you belong to a superuser admin group. For information, see About Administrative Permissions on page 120.

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 684.
     - 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 265.

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 687.
     - Rules: Modify the match rules as described in Defining Option Filters on page 687.
Configuring IPv4 DHCP Filters

- **DHCP Options**: Modify option spaces and DHCP options in the Basic tab as described in *Defining Option Filters* on page 687. You must define the PXE Lease Time in the Advanced tab.

- **BOOTP**: Modify BOOTP settings as described in *Configuring IPv4 BOOTP and PXE Properties* on page 594.

- **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 265.

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 731.
  - **DHCP Options**: Add or delete DHCP options. For information, see *Defining a NAC Filter* on page 731.
  - **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 265.

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

You can modify the MAC address filter items and match rules for corresponding MAC address filters and option filters. For information, see *Modifying MAC Address Filter Items* on page 698 and *Viewing DHCP Filters* on page 698.

**Modifying MAC Address Filter Items**

To modify a MAC address filter item:

1. From the **Data Management** tab, select the **DHCP** tab -> **IPv4 Filters** tab -> *filter_name* -> mac_filter check box, and then click the Edit icon.

2. The **MAC Address Filter Item** editor contains the following tabs from which you can edit data:
   - **General**: Modify the fields as described in *Adding MAC Address Filter Items* 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 265.

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

**Viewing DHCP Filters**

To view DHCP filters:

1. From the **Data Management** tab, select the **DHCP** tab -> **IPv4 Filters** tab.

2. Grid Manager displays the following for each filter:
   - **Name**: The name of the filter.
   - **Filter Type**: The filter type.
   - **Comment**: The information about the filter.
   - **Site**: The location to which the filter belongs. This is one of the predefined extensible attributes.
Viewing MAC Address Filter Items

To view a list of MAC addresses in a specific MAC address filter:

1. From the **Data Management** tab, select the **DHCP** tab -> **IPv4 Filters** tab -> **filter_name**.
2. Grid Manager displays the following:
   - **MAC Address**: The 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.

Deleting Filters

You can delete a filter that is not currently assigned to a DHCP range. You can also remove a filter from a DHCP range, and then delete the filter if it is not in use.

To delete a filter:

1. From the **Data Management** tab, select the **DHCP** tab -> **IPv4 Filters** tab -> **filter_name**, and then click the Delete icon.
2. In the **Delete Confirmation** dialog box, click **Yes**.
   - The appliance puts the deleted filters in the Recycle Bin, if enabled.
Chapter 25  Authenticated DHCP

This chapter includes the following sections:

• About Authenticated DHCP on page 702
  — DHCP Authentication Process on page 703
• Configuring DHCP Authentication on page 706
• About Authentication Server Groups on page 707
  — Configuring a RADIUS Authentication Server Group on page 707
  — Configuring an Active Directory Authentication Server Group on page 708
• About the Captive Portal on page 709
  — Configuring Captive Portal Properties on page 710
  — Customizing the Captive Portal Interface on page 711
  — Managing Captive Portal Certificates on page 712
  — Starting the Captive Portal Service on page 713
• Defining the IPv4 Network and DHCP Ranges on page 714
• Defining MAC Address Filters on page 715
• Using the Captive Portal Wizard on page 715
• Adding and Modifying the Filters and Associations on page 717
• Monitoring DHCP Authentication on page 717
  — Viewing DHCP Ranges and Filters on page 717
• Configuration Example: Configuring Authenticated DHCP on page 718
• NAC Integration on page 724
• Configuring NAC with Sophos NAC Advanced Servers on page 725
• About Authentication Servers on page 726
  — Adding a Server Group on page 726
  — Associating a Server Group with a Member on page 727
  — Managing Server Groups on page 727
  — Clearing the Authentication Cache on page 728
• Configuring DHCP Ranges on page 729
  — Listing DHCP Ranges on page 729
• About NAC Filters on page 730
  — Defining a NAC Filter on page 731
About Authenticated DHCP

This feature provides the ability to control access to your IPv4 networks. (This feature does not support IPv6 networks.) You can divide a network into segments for unauthenticated, authenticated and guest users, and the DHCP server assigns clients to the appropriate segment based on their MAC addresses and authentication credentials.

For example, you can divide a network into one or more production segments for valid employees and systems, a guest segment with access only to the Internet and/or limited public servers, and a quarantine segment with access to a captive portal only. A captive portal is a web page that can provide an option to register as an authenticated user or as a guest.

On a member DHCP server, configure DHCP ranges for each access level—quarantine, authenticated, and guest—and create MAC address filters for the DHCP ranges. You can use DHCP options and Access Control Lists (ACLs) on your routers and firewall policies to define the appropriate services for each access level. On another Grid member, configure the captive portal and specify the authentication server group that authenticates the users. You can configure an authentication server group for external servers running RADIUS or Active Directory (AD).

When a DHCP client first sends a request for an IP address, the DHCP server offers an IP address from the quarantine range and directs the client to the captive portal, where the user can register either as an authenticated user or as a guest. When users sign in as guests or are successfully authenticated, the member automatically adds their MAC addresses to the appropriate MAC address filters and assigns addresses out of the appropriate address range.
About Authenticated DHCP

This section illustrates the DHCP authentication process. As illustrated in Figure 25.1, 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.

Figure 25.1 Stage 1: Quarantining an Unauthenticated DHCP Client

Note that the quarantine range in Figure 25.1 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 25.2*, the member authenticates the user with the authentication service that you configured, which can be either RADIUS or AD.

*Figure 25.2 Stage 2a: Authenticating the User*

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 25.3, the user can fill in the guest registration page provided by the captive portal.

Figure 25.3 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 707.
   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 710.

3. Optionally, customize the captive portal interface and guest registration page, as described in Customizing the Captive Portal Interface on page 711. Additionally, if you enabled SSL encryption, upload the required certificates, as described in Managing Captive Portal Certificates on page 712.

4. Enable the captive portal, as described in Starting the Captive Portal Service on page 713.

5. Configure the network and a DHCP range for quarantine DHCP clients. Configure DHCP ranges for authenticated and guest DHCP clients, depending on whether you are allowing either one or both types of users to access your network. For information about configuring these DHCP ranges, see Defining the IPv4 Network and DHCP Ranges on page 714.

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 715. Alternatively, you can perform these tasks separately or modify the configured properties, as described in Adding and Modifying the Filters and Associations on page 717.

7. Enable the DHCP service. For more information, see Starting DHCP Services on a Member on page 620.
   For information about monitoring the captive portal and the DHCP service, see Monitoring DHCP Authentication on page 717.
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 708

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

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

---

### 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 448.

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 714. 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 710.
2. Optionally, customize the captive portal and registration page. For information about these tasks, see *Customizing the Captive Portal Interface* on page 711.
3. If you enabled SSL, generate the CA certificate, as described in *Managing Captive Portal Certificates* on page 712.
4. Start the captive portal, as described in *Starting the Captive Portal Service* on page 713.
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 553. For information on the LAN2 port, see Using the LAN2 Port on page 277.

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 707.
   — 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 712.
   — 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. Save the configuration and click Restart if it displays at the top of the screen.
**Customizing the Captive Portal Interface**

You can customize the captive portal, and if configured, the guest registration page as well. You can upload image files to the appliance and display your own logo, header and footer. In addition, you can upload the acceptable use policies that are displayed on the captive portal and guest registration page.

Following are guidelines for each item you can customize:

- **Logo Image**: The maximum size is 200 pixels wide by 55 pixels high, and the images can be in JPEG, GIF, or PNG format. It displays on top of the header image.

- **Header Image**: The optimal size is 600 pixels wide by 137 pixels high. The image can be in JPEG, GIF, or PNG format. The header displays at the top of the page.

- **Footer Image**: The optimal size is 600 pixels wide by 20 pixels high. The image can be in JPEG, GIF, or PNG format. The footer displays at the bottom of the page.

- **Acceptable Use Policy**: The policy must be saved as a UTF-8 encoded file. It appears below the welcome message in the captive portal. Users can scroll through the policy when they review it. This is used in the captive portal and guest registration page. 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. Save the configuration and click **Restart** if it displays at the top of the screen.
Managing Captive Portal Certificates

When you enable support for encrypted web traffic sent over SSL/TLS, you can do any of the following:

- Generate a self-signed certificate and save it to the certificate store of your browser.
- Request a CA-signed certificate. When you receive the certificate from the CA, upload it on the member running the captive portal.

Generating Self-Signed Certificates

You can generate a self-signed certificate for the captive portal. When you generate a self-signed certificate, you can specify the hostname and change the public/private key size, enter valid dates and specify additional information specific to the captive portal. If you have multiple captive portals, you can generate a certificate for each captive portal with the appropriate hostname.

To generate a self-signed certificate:

1. From the Grid tab, select the Grid Manager tab.
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 713.

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.
— **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 IPv4 Network and DHCP Ranges

First define the IPv4 network that uses DHCP authentication, and then define the DHCP ranges and services for each access level that you want to provide on the network:

- Quarantine
- Authenticated
- Guest

For information about configuring DHCP IPv4 networks, ranges and services, see Chapter 22, Managing IPv4 DHCP Data, on page 639 and Chapter 20, Configuring DHCP Properties, on page 587.

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 715. Alternatively, you can set the lease time and the DNS server IP address in the DHCP tab of the DHCP Range editor. For information about the DHCP Range editor, see Configuring IPv4 Address Ranges on page 650.

To ensure that clients can reach the captive portal, you must specify a route to the captive portal. On a network where all systems can reach each other without going through a router, that is, all IP addresses are on the same subnet, you must configure Option 33 for the quarantine DHCP range. This option specifies a list of static routes that the client should install in its routing cache. The routes consist of a list of IP address pairs. For clients to reach the captive portal, specify the portal IP address first (destination address), and the LAN address of the NIOS appliance second. When the appliance assigns an IP address from the quarantine DHCP range, it also includes the static route that you specified in option 33. For information about configuring DHCP options, see Configuring IPv4 DHCP Options on page 597. 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 711.
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 710. For example, if you indicated that the captive portal is used for authenticated users only, then the wizard allows you to create a MAC filter for the authenticated DHCP range only.
  - If the captive portal is used to register users for authentication, the wizard allows you to create a MAC address filter for the authenticated range. The wizard then automatically adds the filter to the authenticated DHCP range with an action of Allow. It also adds the filter to the quarantine range with an action of Deny. This ensures that the member does not allocate an address from the quarantine range to a host whose MAC address matches an entry in the MAC filter.
  - If the captive portal is used to register guest users, the wizard allows you to create a MAC address filter for the guest range. The wizard then automatically adds the filter to the guest DHCP range with an action of Allow. It also adds the filter to the quarantine range with an action of Deny. This ensures that the member does not allocate an address from the quarantine range to a host whose MAC address matches an entry in the MAC filter.
- Add the captive portal IP address as the DNS server for the quarantine address range.
- Set the lease time of the quarantine range to 30 seconds.

To use the Captive Portal wizard to complete the tasks for the DHCP authentication feature:

1. From the Data Management tab, select the DHCP tab, or from the Grid tab, select the Grid Manager tab.
2. Expand the Toolbar and click Configure Captive Portal.
3. In the Captive Portal wizard, complete the following and click Next:
   - Member DHCP: Select the member DHCP server that uses this captive portal to authenticate users.
   - Captive Portal: Select the member that runs the captive portal. Note that the member that runs the captive portal cannot run any other service, such as DHCP or DNS, and cannot be the Grid Master or Grid Master candidate.
4. This panel allows you to create MAC filters for the authenticated and guest DHCP ranges. The MAC filters you can create depend on your entry in the Captive Portal properties of the Grid member. For example, if you indicated that the captive portal is used for authenticated users only, then this panel allows you to create a MAC filter for the authenticated DHCP range only.

You can also specify existing MAC filters, if you want to apply them to the authenticated and guest DHCP ranges. Complete the following and click **Next**:

- **Authenticated MAC Filter**: Specify a name for the MAC filter that is used for authenticated users.
- **Expiration Time**: Specify how long a MAC address is stored in the MAC address filter for authenticated users.
  - **Never**: Select this option to store MAC addresses in the MAC address filter until they are manually removed.
  - **Expires in**: Select this option to store MAC addresses in the MAC address filter for the specified period of time.

- **Guest MAC Filter**: Specify a name for the MAC filter that is used for guest users.
- **Expiration Time**: Specify how long a MAC address is stored in the MAC address filter for guest users.
  - **Never**: Select this option to store MAC addresses in the MAC address filter until they are manually removed.
  - **Expires in**: Select this option to store MAC addresses in the MAC address filter for the specified period of time.

5. In this panel, you specify the network and address ranges, so the wizard can apply the MAC address filters to the appropriate ranges. Complete the following:

- **Network**: Select the network that uses DHCP authentication.
- **Authenticated Range**: Select the IP address range that the appliance uses for authenticated users. The wizard applies the authenticated MAC address filter you specified in the preceding step to this DHCP range with an action of Allow. This effectively allows the member to assign an IP address from the address range to a requesting host whose MAC address matches the MAC address in the filter.

- **Guest Range**: Select the IP address range that the appliance uses for guest users. The wizard applies the guest MAC address filter you specified in the preceding step to this DHCP range with an action of Allow. This effectively allows the member to assign an IP address from the address range to a requesting host whose MAC address matches the MAC address in the filter.

- **Quarantine Range**: Select the IP address range that the appliance uses for quarantined addresses. The wizard applies the authenticated and guest MAC address filters to the quarantine DHCP range with an action of Deny. This effectively denies an address request from a host whose MAC address matches an entry in the MAC filters for the authenticated and guest DHCP ranges.

6. Save the configuration and click **Restart** if it appears at the top of the screen.
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 692.
- To specify the DNS server IP address for the quarantine range and set the lease time to 30 seconds, see *Configuring General IPv4 DHCP Properties* on page 590.
- 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 IPv4 Authenticated DHCP tab and complete the following:
     - Use this Captive Portal for Infoblox Authenticated DHCP: Select this check box and select the captive portal that you want to associate with the member.
     - Authenticated User MAC Filter: Select the MAC filter used for authenticated users. To change your section, click Clear and click Select again.
     - Guest User MAC Filter: Select the MAC filter for guest users. To change you selection, click Clear and click Select again.
  3. Save the configuration and click Restart if it displays at the top of the screen.

Monitoring DHCP Authentication

You can monitor the status of the captive portal service, as described in *Monitoring Services* on page 875. You can check its status in the Grid Status widget and the Member Status widget on the Dashboard. For information about these widgets, see Chapter 2, Dashboards, on page 69.

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 699.

Viewing DHCP Ranges and Filters

To view the newly created MAC address filters:

1. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab.
   Grid Manager lists all the configured filters.
2. You can select a filter and view or configure its properties, such as extensible attributes.
   For more information about the filters and editing their properties, see *Managing DHCP Filters* on page 697.

To view the DHCP ranges and the newly added filters:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks section -> network.
2. Select the DHCP range you want to view and click the Edit icon.
3. If the editor is in Basic mode, click Toggle Expert Mode.
4. Click the Filters tab to view the filters.

To verify that the captive portal is the DNS server in the quarantine range:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks section -> network.
2. Select the quarantine DHCP range and click the Edit icon.
3. In the DHCP Range editor, click the DHCP tab.
   The captive portal IP address is listed in the DNS Servers table.
**Configuration Example: Configuring Authenticated DHCP**

In this example, a school (school.edu) has two locations, its main campus, campus1.school.edu, and a satellite campus, campus2.school.edu. It has a captive portal server in each location. In the main campus, the Grid Master also functions as a DHCP server and uses a captive portal server to register DHCP clients. In the satellite campus, two members serve DHCP and use the same captive portal server. The captive portal servers use the same RADIUS authentication server group to authenticate users.

*Figure 25.4*

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:
Configuration Example: Configuring Authenticated DHCP

— **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 -> Networks tab -> Networks section.
2. Click the Add drop-down list and select IPv4 Network.
3. In the Add IPv4 Network wizard, select one of the following and click Next:
   — **Add Network**: Click this.
4. Complete the following and click Next:
   — **Address**: Enter 10.2.1.0/24.
5. Complete the following to assign the network to the Grid Master:
   — **Add Infoblox Member**: Select gm.campus1.school.edu.
6. Click **Save & Close**.

Configure the ranges on the Grid Master.

To create the authenticated range:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks section.
2. Click the 10.2.1.0/24 network link, and then click the Add drop-down list and select DHCP Range.
3. In the Add IPv4 Range wizard, select Add DHCP Range and click Next:
4. Complete the following:
   — **Network**: Click Select Network and select 10.2.1.0/24.
   — **Start**: Enter 10.2.1.50.
   — **End**: Enter 10.2.1.150.
   — **Name**: Enter authenticated range.
5. Click Next and complete the following:
   — **Grid Member**: Select this option and select gm.campus1.school.edu.
6. Click **Save & Close**.

To create the guest range:

1. Click the 10.2.1.0/24 network link, and then click the Add drop-down list and select DHCP Range.
2. In the Add IPv4 Range wizard, select Add DHCP Range and click Next:
3. Complete the following:
   — **Network**: Click Select Network and select 10.2.1.0/24.
   — **Start**: Enter 10.2.1.151.
   — **End**: Enter 10.2.1.170.
   — **Name**: Enter guest range.
4. Click **Next** and complete the following:
   - **Grid Member**: Select this option and select `gm.campus1.school.edu`.

5. Click **Save & Close**.

To create the quarantine range:
1. Click the `10.2.1.0/24` network link, and then click the Add drop-down list and select **DHCP Range**.
2. In the **Add IPv4 Range** wizard, select **Add DHCP Range** and click **Next**:
3. Complete the following:
   - **Network**: Click Select Network and select `10.2.1.0/24`.
   - **Start**: Enter `10.2.1.225`.
   - **End**: Enter `10.2.1.254`.
   - **Name**: Enter `quarantine range`.
4. Click **Next** and complete the following:
   - **Grid Member**: Select this option and select `gm.campus1.school.edu`.
5. Click **Save & Close**.

Create the network and DHCP ranges for the DHCP servers `ds1.campus1.school.edu` and `ds2.campus2.school.edu`.

**Run the Captive Portal Wizard**

Run the **Captive Portal** wizard to associate the Grid Master with its captive portal, and to configure the MAC address filters:
1. From the **Data Management** tab, select the **DHCP** tab, or from the **Grid** tab, select the **Grid Manager** tab.
2. Expand the Toolbar and click **Configure Captive Portal**.
3. In the **Captive Portal** wizard, complete the following and click **Next**:
   - **Member DHCP**: Select the Grid Master, `gm.campus1.school.edu`.
   - **Captive Portal**: Select `cp1.campus1.school.edu`.
4. Complete the following and click **Next**:
   - **Authenticated MAC Filter**: Enter `Auth_MAC_Filter`.
   - **Expiration Time**: Select **Never**.
   - **Guest MAC Filter**: Enter `Guest_MAC_Filter`.
   - **Expiration Time**: Select **Never**.
5. Complete the following:
   - **Network**: Select `10.2.1.0/24`.
   - **Authenticated Range**: Select `10.2.1.50 - 10.2.1.150`.
   - **Guest Range**: Select `10.2.1.151 - 10.2.1.170`.
   - **Quarantine Range**: Select `10.2.1.225 - 10.2.1.254`.
6. Click **Save & Close**.

Run the **Captive Portal** wizard to associate `ds1.campus2.school.edu` with the captive portal server `cp2.campus2.school.edu`, and then run it again to associate `ds2.campus2.school.edu` with the same captive portal server.
Start the DHCP Service

To start the DHCP service on the Grid Master:

1. From the Data Management tab, select the DHCP tab -> Members tab.
2. Select the Grid Master gm.campus1.school.edu, and the two members, ds1.campus2.school.edu and ds2.campus2.school.edu.
3. Expand the Toolbar and click Start.
4. In the Start Member DHCP Service dialog box, click Yes.
5. Grid Manager starts DHCP services on the Grid Master and on the selected members.
NAC Integration

You can configure member DHCP servers to send authentication requests to RADIUS servers and to allocate addresses based on the authentication results. This allows you to place DHCP clients into separate network segments.

You can divide your network into different segments by configuring address ranges and applying NAC filters to them. NAC filters use authentication results from RADIUS servers as matching criteria for granting or denying address requests.

When a DHCP client requests a lease, the member DHCP server can query 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 25.5* 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 25.5*

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 DHCP OFFER that contains an IP address from the corresponding DHCP range. The server also provides the configuration and options associated with that range.
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 726.

2. Associate the authentication server group with the Grid member. For information, see Associating a Server Group with a Member on page 727.

3. Configure the network and the DHCP ranges. For information, see Configuring DHCP Ranges on page 729.

4. Configure the NAC filters, as described in About NAC Filters on page 730

5. Apply the NAC filters to the DHCP ranges, as described in Applying Filters to DHCP Address Ranges on page 692.

6. Enable the DHCP service. For information, see Starting DHCP Services on a Member on page 620.

Optionally, you can do the following:

- Manage the authentication cache, as described in Clearing the Authentication Cache on page 728.
Authenticated DHCP

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.
   - **Server Name or IP Address**: Enter the Sophos NAC Advanced server FQDN or IP address.
   - **Comment**: You can enter additional information about the server.
   - **Authentication Port**: The destination port on the Sophos NAC Advanced server. The default is 1812.
   - **Authentication Type**: Select the authentication method of the RADIUS server from the drop-down list. You can specify either PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol). The default is PAP.
   - **Shared Secret**: Enter the shared secret that the member DHCP server and the Sophos NAC Advanced server use to encrypt and decrypt their messages. This shared secret must match the one you entered on the Sophos NAC Advanced server.
   - **Enable Accounting**: Leave this blank. RADIUS accounting is not supported.
   - **Connect through Management Interface**: Select this so that the NIOS appliance uses the MGMT port for communications with just this server.
   - **Disable server**: Select this to disable the Sophos NAC Advanced server if, for example, the connection to the server is down and you want to stop the DHCP server from trying to connect to this server.
   - **Click Test** to validate the configuration and check that the Grid Master can connect to the Sophos NAC Advanced server. Before you can test the configuration though, you must specify the authentication and accounting timeout values.
     - If the Grid Master connects to the Sophos NAC Advanced server using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the Sophos NAC Advanced server, the appliance displays a message indicating an error in the configuration.
   - **Click Add** to add the Sophos NAC Advanced server to the server group.

When you add multiple Sophos NAC Advanced servers to the list, you can use the up and down arrows to change the position of the servers on the list. The member DHCP server connects to the Sophos NAC Advanced servers in the order they are listed.

- **Authentication Timeout**: The time that the member DHCP server waits for a response from a Sophos NAC Advanced server before considering it unreachable. You can enter the time in milliseconds or seconds.
— **Retries**: The number of times the member DHCP server retries connecting to a Sophos NAC Advanced server before it considers the server unreachable. The default is five.

— **Mode**: Specifies how the member DHCP server selects the first Sophos NAC Advanced server to contact.
  
  — **Ordered List**: The member DHCP server always selects the first Sophos NAC Advanced server in the list when it sends an authentication request. It queries the next server only when the first server is considered down. This is the default.
  
  — **Round Robin**: The member DHCP server selects the first Sophos NAC Advanced server for the first request, the second server for the next request, and so on. If the last server is reached, then the DHCP server starts with the first server 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 728.

— **Cache Time to Live**: Specifies the duration of time an authentication result is stored. The default is one hour. The maximum is 259200 seconds (3 days).

— **Recovery Interval**: Specifies the duration of time a Sophos NAC Advanced server stays inactive after being down, before becoming eligible to have RADIUS requests sent to it. The recovery interval starts when a Sophos RADIUS server is first discovered to be down.

— **Comment**: You can enter additional information about the server group.

— **Disable**: Select this to disable the authentication server group.

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

### Associating a Server Group with a Member

To associate an authentication server group with a member DHCP server:

1. From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **member** check box, and click the **Edit** icon.

2. If the **Member DHCP Properties** editor is in Basic mode, click **Toggle Expert Mode**.

3. Select the **IPv4 Authenticated DHCP** tab.

4. Click the **Use this Authentication Server Group for Sophos/RAIDIUS Authenticated DHCP** check box, and then select a group from the drop-down list.

5. **Save the configuration and click Restart** if it displays at the top of the screen.

### Managing Server Groups

To view the list of authentication server groups, from the **Administration** tab, click the **Authentication Server Groups** tab and expand the **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 IPv4 network and DHCP ranges as described in Chapter 22, Managing IPv4 DHCP Data, on page 639. 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 by navigating to the DHCP tab -> Networks tab -> Networks panel, and then clicking the network link. You can select the Priority column for display to view the order of the DHCP ranges. For information about editing the columns, see Customizing Tables on page 50.
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 or range template and indicate whether the DHCP server grants or denies a lease when the authentication result matches the filter. You can apply NAC filters to any DHCP range and DHCP range template.

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 729.

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 24, Configuring IPv4 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 -> IPv4 Filters tab, and then expand the Toolbar and click Add -> IPv4 NAC Filter.
   or
   From any panel in the DHCP tab, expand the Toolbar and click Add -> IPv4 NAC Filter.
2. In the Add Filter Wizard, complete the following and click Next:
   — Name: Enter a name for the filter. You can enter a maximum of 255 characters. The name must be unique within a specific network. If you want to specify option settings in the filter, the name must be unique among all NAC filters.
   — Comment: Optionally, enter additional information about the NAC filter.
3. Create a rule as follows:
   — In the first drop-down list, select one of the following criterion: Compliance State, Server Error, Server Response, Server State or User Class.
   — In the second drop-down list, select an operator: equals or does not equal.
   — The selections in the third drop-down list depend on the criterion you selected:
     Compliance State: Select one of the following compliance states: Unknown, Non-compliant, Compliant or Partially Compliant.
     Server Error: The Infoblox DHCP server expects certain 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 another rule at the same level.
     — Click |< to add an all (logical AND) or any (logical OR) operator line and a parenthetical rule that is indented one level and above the first rule.
     — Click ->| to add an all (logical AND) or any (logical OR) operator line and a parenthetical rule that is indented one level.
   After you add all the match rules, you can click Preview to view the rules or click Reset to remove the previously configured rules and start again.
4. Click Next and complete the following to define DHCP options:
   — Option Space: Select an option space from the drop-down list. This field is not displayed if you do not have custom option spaces. The appliance uses the DHCP option space as the default.
Authenticated DHCP

— **Lease Time**: Enter the value of the lease time in the field and select the time unit from the drop-down list. The lease time applies to hosts that meet the filter criteria.

**Options to Merge with Object Options**

Click the Add icon. Grid Manager adds a new row to the table with the default DHCP option space and option name displayed. Complete the following:

— **Option Space**: Click the down arrow and select an option space from the drop-down list. The selected option space contains the corresponding DHCP options.

— **Option Name**: Click the down arrow and from the drop-down list, select the DHCP option you want to return to the matching client.

— **Value**: Enter the match value that you want the filter to use for the selected DHCP option. For example, enter the value 172.124.3.0 for the SUNW.SrootIP4 option.

To add more options to the filter, click the Add icon and repeat the steps.

5. Click **Next** to define extensible attributes. For information, see *Using Extensible Attributes* on page 265.

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

After you add NAC filters, you must then apply them to DHCP ranges, as described in *Applying Filters to DHCP Address Ranges* on page 692. You can also list, modify or delete NAC filters, as described in *Managing DHCP Filters* on page 697.
Chapter 26 Managing IPv6 DHCP Data

This chapter explains how to configure and manage IPv6 DHCP data. It contains the following sections:

• Configuring IPv6 Networks on page 734
• Defining Global IPv6 Prefixes on page 734
• Managing IPv6 Networks on page 735
  — Adding IPv6 Networks on page 735
  — Modifying IPv6 Networks on page 736
  — Deleting IPv6 Networks on page 737
• About IPv6 Shared Networks on page 737
  — Adding IPv6 Shared Networks on page 738
  — Modifying IPv6 Shared Networks on page 738
  — Deleting IPv6 Shared Networks on page 739
• Configuring IPv6 Address Ranges on page 739
  — Adding IPv6 Address Ranges on page 739
  — Setting the Priority of IPv6 Address Ranges on page 740
  — Modifying IPv6 Address Ranges on page 740
  — Deleting IPv6 Address Ranges on page 741
• Configuring IPv6 Fixed Addresses on page 741
  — Adding IPv6 Fixed Addresses on page 741
  — Modifying IPv6 Fixed Addresses on page 742
  — Deleting IPv6 Fixed Addresses on page 743
• Viewing IPv6 DHCP Objects on page 743
Configuring IPv6 Networks

To configure DHCP services for an IPv6 network and the resources in the network, perform the following tasks:

1. To facilitate network creation, you can specify the IPv6 global prefixes for the Grid. For more information, see Defining Global IPv6 Prefixes.
2. Create a network and assign it to Grid members. For information, see Managing IPv6 Networks on page 735 and About IPv6 Shared Networks on page 737.
3. Optionally, configure DHCP properties for the network. You can override properties set at the Grid or member level and enter unique values for the network and fixed addresses. For information, see Configuring DHCPv6 Properties on page 606 and Configuring DHCP IPv4 and IPv6 Properties on page 610.
4. Optionally, assign zones to a network. For information, see Associating Networks with Zones on page 737.
5. Add a DHCP range to the network and assign it to a member. For information, see Configuring IPv6 Address Ranges on page 739.
6. Optionally, add exclusions to the DHCP range for addresses that are not used for dynamic allocation. For information, see Modifying IPv6 Address Ranges on page 740.
7. Optionally, configure DHCP properties for the address range. You can override properties set at an upper level and enter unique values for the address range. For information, see Modifying IPv6 Address Ranges on page 740.
8. Optionally, add fixed addresses to the network and configure DHCP properties for them. For information, see Configuring IPv6 Fixed Addresses on page 741.
9. Start the DHCP service and the IPv6 DHCP service. For more information, see Starting DHCP Services on a Member on page 620.

Defining Global IPv6 Prefixes

To simplify network creation, you can define IPv6 prefixes that are used for networks served by the Grid members. If your organization is assigned IPv6 prefixes, you can enter them globally at the Grid level, and then just select the appropriate IPv6 prefix when you define the networks.

To add global IPv6 prefixes:

1. From the Data Management tab, select the DHCP tab.
2. Expand the Toolbar and click Grid DHCP Properties.
3. In the Grid DHCP Properties editor, select the IPv6 Global Prefixes tab.
4. Click the Add icon and enter a name for the prefix and the prefix. Select the Default check box if you’d like to specify a default IPv6 prefix for the Grid.
5. Save the configuration.
Managing IPv6 Networks

You can create an IPv6 network from scratch or create a network template and then use that template to create one or more networks. Using a network template facilitates creating multiple IPv6 networks with similar properties. You can also create an IPv6 network from the Tasks Dashboard. For information about the Tasks Dashboard, see The Tasks Dashboard on page 70.

An IPv6 network inherits its DHCP options & DDNS settings from its shared network, if it is part of a shared network, or from the member to which it is assigned.

Adding IPv6 Networks

To add an IPv6 network:
1. Select the Data Management tab.
2. If you have more than one network view in the system, select the network view in which you want to add the network.
3. Select the DHCP tab -> Networks tab.
4. In the Networks section, click the Add drop-down list and select IPv6 Network.
5. In the Add IPv6 Network wizard, select one of the following and click Next:
   - Add IPv6 Network: Click this to add an IPv6 network from scratch.
   - Add IPv6 Network using Template: To use a template, click this, and then click Select Template and select an IPv6 network template. For information about network templates, see About IPv6 Network Templates on page 636. When you use a template to create a network, the configurations of the template apply to the new network. The appliance populates the template properties in the wizard when you click Next. You can then edit the pre-populated properties. If the template specified a fixed netmask, you cannot edit the netmask.
6. Complete the following and click Next:
   - Mask: Use the netmask slider to select the appropriate number of subnet mask bits for the network.
   - Networks: Do one of the following to add new networks:
     - Create new network(s) under: Enter the network container in which you want to create the new network. When you enter a network that does not exist, the appliance adds it as a network container. When you enter a network that is part of a parent network, the parent network is converted into a network container if it does not have a member assignment or does not contain fixed addresses and host records that are served by DHCP. You can also click Select Network to select a specific network in the Network Selector dialog box. For information about how the appliance searches for the next available network, see Obtaining the Next Available on page 642.
— **Number of new networks**: Enter the number of networks you want to add to the selected network container. Note that if there is not enough network space in the selected network to create the number of networks specified here, Grid Manager displays an error message. The maximum number is 20 at a time. Note that when you have existing networks in the table and you select one, the number you enter here includes the selected network.

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

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

— **Comment**: Enter additional information about the network, such as the name of the organization it serves.

— **Automatically create reverse-mapping zone**: This function is enabled if the netmask of the network is a multiple of four, such as 4, 8, 12 or 16. Select this to have the appliance automatically create reverse-mapping zones for the network. A reverse-mapping zone is an area of network space for which one or more name servers have the responsibility for responding to address-to-name queries. These zones are created in the DNS view assigned to receive dynamic DNS updates at the network view level.

— **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.

7. Click **Next** and add one or more Grid members as DHCP servers for the network.

— click the Add icon and select a Grid member from the **Member Selector** dialog box. Keep in mind, some DHCP properties for the network are inherited from this member. The network can be served by multiple members, but a member can serve networks in one network view only.

8. Click **Next** to override the DHCP properties described in *Defining General IPv6 Properties* on page 606.

9. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see *About Extensible Attributes* on page 262.

10. Save the configuration.

or

— Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 256.

After you create a network, you can do the following:

• Add it to a shared network. For more information, see *Adding IPv6 Shared Networks* on page 738.

• Use the split network feature to create subnets for the network. For information, see *Splitting IPv6 Networks into Subnets* on page 836.

• Use the join networks feature to create a parent network that encompasses multiple subnets into a larger network. For information, see *Joining IPv6 Networks* on page 836. You can also create a shared network for subnets that are on the same network segment.

• View a list of networks. For more information, see *Viewing Networks* on page 645.

**Modifying IPv6 Networks**

You can modify existing network settings and override the Grid or member DHCP properties, with the exception of the network address and netmask.

To modify an IPv6 network:

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** -> **network** check box, and then click the Edit icon.

2. The **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.
  — **IPv6 DHCP Options**: Keep the inherited DHCP properties or override them and enter unique settings for the network. For information, see *Defining General IPv6 Properties* on page 606.
  — **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 262.
  — **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 611.
   — **IPv6 DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the network. Note that you must click **Override** and select **Enable DDNS updates** for the DDNS settings you configure in this tab to take effect. For information, see *Enabling DDNS for IPv4 and IPv6 DHCP Clients* on page 484.
     Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Save the configuration or click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 256.

### Deleting IPv6 Networks

When you delete a network, all of its data, including all DHCP records, subnets, and records in its subnets, is deleted from the database. Because of the potentially large loss of data that can occur when you delete a network, the appliance stores the deleted network in the Recycle Bin. You can restore a deleted network from the Recycle Bin, if enabled. You can also disable a network instead of deleting it. For information, see *Modifying IPv6 Networks* on page 736.

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 256.
   The appliance puts the deleted network in the Recycle Bin, if enabled.

### About IPv6 Shared Networks

You can combine two or more contiguous IPv6 networks into a shared network. When you do, the DHCP server allocates IP addresses from both subnets. To create a shared network, create the individual subnets, and then create the shared network and add the subnets to it. For more information about shared networks, see *About Shared Networks* on page 574.
**Adding IPv6 Shared Networks**

To add an IPv6 shared network:
1. Select the **Data Management** tab.
2. If you have more than one network view in the system, select the network view in which you want to add the network.
3. Select the **DHCP** tab -> **Networks** tab.
4. In the **Shared Networks** section, select **IPv6 Shared Network** from the Add drop-down menu.
5. In the **Add IPv6 Shared Network** wizard, do the following:
   - **Name**: Enter the name of the shared network.
   - **Comment**: Enter information about the shared network.
   - **Disabled**: Select this if you want to enable the shared network at a later time. You can disable and enable existing networks instead of removing them from the database. This feature is especially helpful when you have to move or repair the server for a particular network.
6. Click **Next** and do the following to add networks:
   a. Click the Add icon.
   b. In the **Network Selector**, select the networks that you want to include in the shared network. Ensure that the networks are served by the same Grid members to avoid DHCP inconsistencies.
7. Click **Next** to configure DHCP properties described in **Defining General IPv6 Properties** on page 606.
8. Click **Next** to enter values for required extensible attributes or add optional extensible attributes for the shared network. For information, see **Using Extensible Attributes** on page 265.
9. Save the configuration or click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see **Scheduling Tasks** on page 256.

For information on viewing shared networks, see **Viewing Shared Networks** on page 648.

**Modifying IPv6 Shared Networks**

To modify a shared network:
1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Shared Networks** section -> **shared_network** check box, and then click the Edit icon.
2. The **IPv6 Shared Network** editor contains the following tabs from which you can modify data:
   - **General**: Modify the fields **Name**, **Comments**, and **Disabled** as described in **Adding IPv6 Shared Networks** on page 738.
   - **Networks**: Displays the networks that are currently assigned to the shared network. You can add or delete a network. To add a network, click the Add icon. To delete a network, select the **network** check box, and then click the Delete icon.
   - **IPv6 DHCP Options**: Keep the inherited DHCP properties or override them and enter unique settings for the shared network. For information, see **Defining General IPv6 Properties** on page 606.
   - **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 265.
   - **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.
Configuring IPv6 Address Ranges

— IPv6 DDNS: Keep the inherited DDNS settings or override them and enter unique settings for the shared network. Note that you must click Override and select Enable DDNS updates for the DDNS settings you configure in this tab to take effect. For information, see Enabling DDNS for IPv4 and IPv6 DHCP Clients on page 484.

Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

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

or

— Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.

Deleting IPv6 Shared Networks

Though you can delete the networks in a shared network, a shared network must have at least one network in it.

To delete a shared network:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Shared Networks section -> shared_network check box, and then select Delete or Schedule Delete from the drop-down menu.

2. To delete the shared network now, in the Delete Confirmation dialog box, click Yes. To schedule the deletion, see Scheduling Tasks on page 256.

   The appliance puts the deleted shared network in the Recycle Bin, if enabled.

Configuring IPv6 Address Ranges

You can configure IPv6 ranges that are used to delegate IPv6 prefixes only, to assign IPv6 addresses only, or to delegate IPv6 prefixes and assign IPv6 addresses. When you define a DHCP range to delegate prefixes, the prefixes can be outside of the network where they are being defined. IPv6 ranges inherit their properties from their network, so each range in a subnet provides the same set of options to their DHCP clients.

Note that when an Infoblox DHCP server grants IPv4 leases, it starts from the last IP address in the range to the first. When the server grants IPv6 leases, it uses an algorithm based on the DUID of the client.

Adding IPv6 Address Ranges

To add a IPv6 address range:

1. Navigate to the IPv6 network to which you want to add an address range, and then select Range from the Add drop down menu.

   or

   From any panel in the DHCP tab, expand the Toolbar and click Add -> Range -> IPv6.

2. In the Add IPv6 Range wizard, select one of the following and click Next:

   — Add IPv6 Range: Select this to add an address range from scratch.

   or

   — Add IPv6 Range Using Template

      Click Select Template and select the template that you want to use. Note that when you use a template to create a DHCP range, the configurations of the template apply to the new range. The appliance automatically populates the address range properties in the wizard. You can then edit the pre-populated properties. For more information, see About IPv6 Range Templates on page 634

3. Complete the following:

   — Network: Click Select Network. Grid Manager displays the network address here if you have only one network configured. When there are multiple networks, Grid Manager displays the Select Network dialog box from which you can select one.
Specify one of the following:

- **Address**: Select this if the address range is used to allocate IPv6 addresses only to DHCP clients, and then enter the start and end addresses in the range.
- **Prefix Delegated**: Select this if the DHCP server uses this address range to delegate IPv6 prefixes only to DHCP clients. Enter the start and end prefixes, and the prefix length.
- **Both**: Select this if the DHCP server delegates IPv6 prefixes and allocates IPv6 addresses from this range. Enter the start and end addresses in the range, and the start and end prefixes, and the prefix length.

Complete the following:

- **Name**: Enter a name for the address range.
- **Comment**: Enter additional information about the address range.
- **Disabled**: Select this if you want to save the configuration for the address range but do not want to activate the address range yet. You can clear this check box when you are ready to allocate addresses from this range.

4. Click **Next** and select one of the following to provide DHCP services for the DHCP range:

- **None (Reserved Range)**: Select this if you want to reserve this address range for static hosts. Addresses in this range cannot be allocated as dynamic addresses. You can allocate the next available IP from this range to a static host. This is selected by default.
- **Grid Member**: Select this if you want a Grid member to serve DHCP for this DHCP range. Select a Grid member from the drop-down list. The drop-down list displays only the Grid members that are associated with the network to which the DHCP range belongs.

5. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see **Using Extensible Attributes** on page 265.

6. Save the configuration and click **Restart** if it displays at the top of the screen.

   or

   - Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see **Scheduling Tasks** on page 256.

### Setting the Priority of IPv6 Address Ranges

The DHCP server allocates IP addresses from the configured DHCP ranges according to the order in which the ranges are listed. By default, ranges are listed according to their start addresses. You can move the ranges up and down in the list to change their order. For information about viewing DHCP ranges and other objects in a network, see **Viewing IPv6 DHCP Objects** on page 743.

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**.

### Modifying IPv6 Address Ranges

To modify an IPv6 address range:

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Network** -> **addr_range** check box, and then click the **Edit** icon.
2. The **DHCP Range** editor contains the following basic tabs from which you can modify data:
   - **General**: Modify the fields, except the network address, as described in **Adding IPv6 Address Ranges** on page 739.
Configuring IPv6 Fixed Addresses

You can configure IPv6 fixed addresses with either an IPv6 address or prefix. You can assign prefix-based fixed addresses to routers so they can advertise the prefixes associated with a link. DHCP hosts, in turn, use these prefixes to generate IP addresses using the stateless autoconfiguration mechanism defined in RFC 2462, IPv6 Stateless Autoconfiguration. You can also create IPv6 fixed addresses from the Tasks Dashboard. For information about the Tasks Dashboard, see The Tasks Dashboard on page 70.

Note that dynamic DNS updates for IPv6 fixed addresses are not supported.

Adding IPv6 Fixed Addresses

To add an IPv6 fixed address:

1. Navigate to the network to which you want to add a fixed address, and then select Fixed Address from the Add drop down menu.
   or
   From any panel in the DHCP tab, expand the Toolbar and click Add ->Fixed Address ->IPv6.
2. In the Add Fixed Address wizard, select one of the following and click Next:
   — Add IPv6 Fixed Address
   or
   — Add IPv6 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.

3. In this panel, the displayed network address can either be the last selected network or the network from which you are adding the fixed address. If no network address is displayed or if you want to specify a different network, click Select Network. When there are multiple networks, Grid Manager displays the Select Network dialog box. Specify one of the following:
   — Select Address to assign an IPv6 address to a fixed address. You can either enter an IPv6 address or select Next Available IP to obtain the next available IP address.
   — Select Prefix Delegated to assign an IPv6 prefix. Enter the prefix and prefix length.
   — Select Both to assign an IPv6 prefix and address. Enter the IPv6 address, prefix, and prefix length.
Complete the following:
   — DUID: Specify the DHCP Unique Identifier (DUID) of the DHCP client assigned to this fixed address.
   — Name: Enter a name for the fixed address.
   — Comment: Optionally, enter additional information.
   — Disabled: Select this if you do not want the DHCP server to allocate this IP address at this time.

4. Click Next to configure or override DHCP options as described in Defining General IPv6 Properties on page 606.
5. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes on page 265.
6. Save the configuration and click Restart if it displays at the top of the screen.
   or
   — Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.

For information on viewing IPv6 fixed addresses in a network, see Viewing IPv6 DHCP Objects on page 743.

### Modifying IPv6 Fixed Addresses

To modify a fixed address:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks section -> network -> fixed_address check box, and then click the Edit icon.
2. The Fixed Address editor contains the following basic tabs from which you can modify data:
   — General: You can modify all the fields you filled out in the first step of the wizard described in Adding IPv6 Fixed Addresses on page 741.
   — IPv6 DHCP Options: You can keep the inherited DHCP options or override them and enter unique settings for the fixed address. For information, see Defining General IPv6 Properties on page 606.
   — Discovered Data: You can view discovered data of this address, if any, in this tab. For information, see Viewing Discovered Data on page 858.
   — 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 265.
   — Permissions: This tab appears only if you belong to a superuser admin group. For information, see Managing Permissions on page 20.
3. Save the configuration and click Restart if it displays at the top of the screen.
   or
   — Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.
Deleting IPv6 Fixed Addresses

To delete a fixed address, from the **Data Management** tab, select the **DHCP** tab -> Networks tab -> Networks section -> network -> fixed_address check box, and then click the Delete icon.

Viewing IPv6 DHCP Objects

You can view the DHCP objects in an IPv6 network by navigating to the **DHCP** tab -> Networks tab -> Networks panel, and then clicking the network link. This panel displays the following information about DHCP objects in the selected IPv6 network:

- **IP Address**: The IPv6 address of a DHCP object, such as a DHCP range, fixed address, or host configured for DHCP, or roaming host with an allocated IP address. For a DHCP range, this field displays the start and end addresses of the range. For a host that has multiple 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 IPv6 DHCP Range or IPv6 Fixed Address.
- **Name**: The object name. For example, if the IP address belongs to a host record, this field displays the hostname.
- **Comment**: The information you entered for the object.
- **Site**: The site to which the DHCP object belongs. This is one of the predefined extensible attributes.

You can select the following additional columns for display:

- **Priority**: Displays the priority of the DHCP range.
- **Disabled**: Indicates whether the network is disabled.

You can also do the following in this panel:

- Modify some of the data in the table. Double click a row, and either modify the data in the field or select an item from a drop-down list. Click **Save** to save the changes. Note that some fields are read only.
- Sort the data in ascending or descending order by column.
- Create a bookmark for the object.
- Click **Go to IPAM View** to view information about the object in the IPAM tab.
- Delete or schedule the deletion of a selected object or multiple objects.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 57.
- Print or export the data.
Chapter 27  Managing Leases

This chapter explains how to manage IPv4 and IPv6 leases. It contains the following sections:

- About DHCP Leases  on page 746
- Viewing Current Leases  on page 746
- Viewing Detailed Lease Information  on page 748
- Viewing Lease History  on page 749
- Viewing Lease Event Detailed Information  on page 749
- Exporting Lease Records  on page 750
- Clearing Leases  on page 750
**About DHCP Leases**

Historical DHCP lease records complement the real-time DHCP lease viewer by allowing the appliance to store and correlate DHCP lease information over the lifetime of a lease. You can see critical information such as when the appliance issued or freed an IPv4 or IPv6 address, the MAC address or DUID and host name of the device that received the IP address, the Grid member that supplied the lease, and the start and end dates of the lease.

You can view current leases and lease history in the Data Management -> DHCP -> Leases tab in Grid Manager. To view lease history, you must first enable lease logging at the Grid level. For information, see Configuring DHCP Logging on page 613 and Configuring the Lease Logging Member on page 613. 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 746.
- View detailed information about a specific lease. For information, see Viewing Detailed Lease Information on page 748.
- View historical lease records. For information, Viewing Lease History on page 749.
- View detailed information about a lease event. For information, see Viewing Lease Event Detailed Information on page 749.
- Export current leases and lease history logs. For information, see Exporting Lease Records on page 750.
- Clear leases. For information, see Clearing Leases on page 750.

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.

**Viewing Current Leases**

To view current IPv4 and IPv6 leases:

1. From the Data Management tab, select the DHCP tab -> Leases tab -> Current Leases.
2. Grid Manager displays the following information:
   - **IP Address**: The IPv4 address or IPv6 prefix or address that the appliance assigned to a DHCP client for this lease.
   - **Protocol**: Indicates whether the lease is for an IPv4 or IPv6 address.
   - **Members/Servers**: The Grid member or Microsoft server (for IPv4 leases only) that granted the lease.
   - **MAC address**: The MAC address of the IPv4 DHCP client that received the lease for an IPv4 address.
   - **DUID**: The DHCP Unique Identifier (DUID) of the IPv6 DHCP client that received the lease for an IPv6 address.
   - **Host Name**: The hostname that the DHCP client sent with its DHCP request. For IPv4 leases, this field displays the hostname of the DHCP client. For IPv6 leases, this field typically displays the FQDN.
   - **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 state of the lease ends.
   - **Start**: The day, date, and time when the state of 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 an IPv4 lease. The client sends the client identifier as option 61 in the DHCP DISCOVER and REQUEST packets, as described in RFC2132, DHCP Options and BOOTP Vendor Extensions. The client identifier is either the MAC address of the network interface card requesting the address or any string uniquely identifying the client. This field is not displayed by default.

**Note**: The dates and timestamps in the **Leases** tab are determined by the time zone setting of the admin account that you use to log in to the appliance.

You can display the following discovered data for IPv4 leases:

— **Last Discovered**: The timestamp when the IP address was last discovered. This data is read-only.
— **OS**: The operating system of the 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.
— **NetBIOS Name**: The name returned in the NetBIOS reply or the name you manually register for the discovered host.
— **Discovered Name**: The name of the network device associated with the discovered IP address.
— **Discoverer**: Specifies whether the IP address was discovered by a PortIQ or NIOS discovery process.

You can do the following in this tab:

- Sort the data in ascending or descending order by column.
- View the lease detailed information of a current lease by selecting the check box of the lease, and then clicking the Open icon.
- Change a current lease state to **Free** by selecting the check box of a current lease, and then clicking the Delete icon.
- Use filters and the **Go to** function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the **Go to** field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see **Using Quick Filters** on page 57.
- Print and export the data in this tab.
Viewing Detailed Lease Information

You can view detailed information about a specific lease.

To view detailed information of a specific lease:

1. From the Data Management tab, select DHCP tab -> Leases -> Current Leases -> lease check box, and then click the Lease Details icon.
   
   or

   From the Data Management tab, select the IPAM tab, drill down to the IP Map, IP List, or IP address panel, and then click Lease Details from the Toolbar.

2. In the Lease Detailed Information viewer, Grid Manager displays the following for each type of lease:

   For IPv4 leases, it displays the fields Member, MAC address, Host, Start, End, Binding State, Username, Binding State, as described in Viewing Current Leases on page 746, 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.
     
   For IPv6 leases, it displays most of the same fields as IPv4 leases, plus the following information:
     
   — DUID: The DUID of the IPv6 DHCP client that received the lease for an IPv6 address.
     
   — Prefix Bits: The prefix length.
     
   — Preferred Lifetime: The length of time that a valid address is preferred. A preferred address can be used with no restrictions. When this time expires, the address becomes deprecated.
Viewing Lease History

To view historical IPv4 or IPv6 lease records:
• From the Data Management tab, select the DHCP tab -> Leases tab -> Lease History.

Grid Manager displays a table of historical leases that have been archived in the system. You can export the information in the lease history table. You can also search by the IP address or MAC address of the lease. Grid Manager displays the following read-only information:
• Lease Issue: The date and time when the lease was issued.
• Protocol: Indicates whether the lease is for an IPv4 or IPv6 address.
• IP Address: The IPv4 address or IPv6 prefix or address of the lease.
• MAC Address: The MAC address of the IPv4 lease.
• DUID: The DUID of the DHCP client that received the lease for an IPv6 address.
• Host Name: The host name that the DHCP client sent to the appliance.
• Action: This can be one of the following: Issued, Renewed, Freed, or Abandoned.
• User Name: The name of the user who received the lease for the IP address.
• Start: The start date of the lease.
• Stop: The end date of the lease.
• Member/Server: The DHCP member or Microsoft server that granted the lease.
• Member IP Address: The IP address of the DHCP member that granted the lease.

You can do the following in this section:
• View the lease event detailed information of a historical lease by selecting the check box of a lease, and then clicking the Open icon.
• Print or export the information in this section.

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 748.

You can also export and print the information in this panel. For information, see Exporting Lease Records on page 750.
Exporting Lease Records

The DHCP lease history log holds a maximum of 100,000 entries. After that maximum is reached, the appliance begins deleting entries, starting with the oldest. To archive DHCP lease history logs, you can export them and save them as CSV (comma separated variables) files. You do not need to export the entire log. You can selectively export a section of the log, such as the lease events for a single day.

As a conservative approach to archiving DHCP lease data, Infoblox recommends exporting the log on a daily basis, perhaps through API (application programming interface) scripting. By exporting the daily log entries every day over a certain period of time and then opening the exported files with a spreadsheet program, you can see the number of entries for each day. You can then estimate how often you need to export the log to ensure that you save all of the entries before the log fills up (at 100,000 entries). As a result, you might discover that you need to export the log more or less frequently than once a day to archive all the records.

A limited-access admin group can view and export the DHCP lease history if it has read-only permission to the DHCP lease history. For information on setting permissions for the DHCP lease history, see Administrative Permissions for the IPv4 and IPv6 DHCP Lease Histories on page 168.

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

You can clear active leases for which you have read/write permission. When you clear an active lease, its IP address becomes available and its status changes to “Free”. To clear an active lease:
1. From the Data Management tab, select the DHCP tab -> Leases tab -> Current Leases.
2. Click the check boxes beside the IP addresses of the leases you want to clear, and then click the Clear Lease icon.

Grid Manager clears the selected leases. You can view information about a cleared lease, by selecting it in the Lease History panel and clicking the Edit icon.
Part 5 Managing Microsoft Windows Servers

This section describes how you can centrally manage Microsoft Windows® DNS and DHCP servers from Grid Manager. You can synchronize your DNS and DHCP data from the Microsoft servers to the Grid, and then use IPAM tools to facilitate DHCP and DNS configuration and data management. This section includes the following chapters:

- Chapter 28, "Managing Microsoft Windows Servers", on page 753
- Chapter 29, "Managing Microsoft DNS Services", on page 767
- Chapter 30, "Managing Microsoft DHCP Services", on page 785
Chapter 28 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 754
  - **Requirements** on page 755
  - **Deployment Guidelines** on page 756
- **Configuring Members to Manage Microsoft Servers** on page 757
  - **Setting Microsoft Server Credentials** on page 757
  - **Configuring a Managing Member** on page 758
- **Managing Microsoft Servers** on page 761
  - **Setting Microsoft Server Properties** on page 761
  - **Changing the Managing Member or Management Mode** on page 762
  - **Backing Up Synchronized Data** on page 762
  - **Disabling Synchronization** on page 762
  - **Removing a Managed Microsoft Server** on page 763
- **Monitoring Managed Microsoft Servers** on page 763
  - **Viewing the Status of Servers** on page 763
  - **Viewing Detailed Status Information** on page 765
  - **Viewing Synchronization Logs** on page 765
### About Managing Microsoft Servers

You can configure Grid members to manage Microsoft Windows DNS and DHCP servers, and synchronize their DNS and DHCP data to the Grid database, so you can view and optionally, manage the data from Grid Manager. After the data is synchronized, you can use the IPAM tools of Grid Manager to simplify DNS and DHCP configuration and troubleshooting. You can use Smart Folders to organize your data, and monitor your networks and Microsoft servers from the Dashboard. In addition, you can control the DNS and DHCP services of the Microsoft servers from Grid Manager and configure server properties as well.

*Figure 28.1* 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 28.1 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.
About Managing Microsoft Servers

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</td>
<td>SP2</td>
<td>32 bits</td>
</tr>
<tr>
<td>Standard and Enterprise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows 2003 R2</td>
<td>Initial Release</td>
<td>32 bits, 64 bits</td>
</tr>
<tr>
<td>Standard and Enterprise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows 2008</td>
<td>SP2</td>
<td>32 bits, 64 bits</td>
</tr>
<tr>
<td>Standard and Enterprise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows 2008 R2</td>
<td>Initial Release</td>
<td>64 bits</td>
</tr>
<tr>
<td>Standard 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 151.

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 154 and Administrative Permissions for DHCP Resources on page 160.

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 ports 135 and 445 must be open on the Microsoft server, in addition to the dynamic port range. Ports 135 and 445 are used by the port mapper interface, which is a service on the Microsoft server that provides information to clients on which port to use to connect to a specific service, such as the service that allows the management of the DNS service.

- The capacity of the managing member must be greater than or equal to the sum of all its assigned Microsoft servers.

- The capacity of the Grid Master must be greater than or equal to the sum of all managed Microsoft servers.

- A Microsoft server can synchronize its data to only one network view, and for DNS data, only one DNS view.

- Multiple Microsoft servers can synchronize their data into the same network view and DNS view, unless there is a conflict in their data. For example, two Microsoft servers in different locations could serve the same private IP address space, such as 10.1.0.0/16, or serve reverse-mapping zones with the same name, such as 10.in-addr.arpa. Synchronizing their data to the same network view and DNS view would cause conflicts which result in the Grid member synchronizing the data of only one Microsoft server and logging an error for the other Microsoft server. In such situations, Infoblox recommends that you synchronize each Microsoft server to a different network view and DNS view to ensure that data from both servers are synchronized.
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 Builtin, 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 the section DNS Server Service Permissions at http://technet.microsoft.com/en-us/library/gg638675.aspx. To find additional information, you can also search for "Least Privilege Setup" on the Microsoft sites.
  2. Grant permissions to the DNS and/or DHCP service on each managed server by doing one of the following:
     - Use the sc command line utility to remotely configure each managed DNS or DHCP server. Note that you need to know the SID of the user account and its current permissions. You can retrieve the SID of the user account by using the dsquery and dsget commands.
     - Use the Domain Controller Policy editor to define a global policy that applies to all DNS or DHCP services running in a domain or on domain controllers. For additional information, refer to http://support.microsoft.com/kb/324802.

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 759.
- 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 759.

For the steps on configuring the managing member, see Assigning Grid Members to Microsoft Servers on page 759.
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 151.

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 Configuring DHCP for IPv4 on page 641. For information about DNS views, see Chapter 12, DNS Views, on page 355.

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 763.

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. In order for the member to resolve the FQDN of a Microsoft server, you must define a DNS resolver for the Grid member in the DNS Resolver tab of the Member Properties editor. Note that if the IP address of the Microsoft server is specified, then the DNS resolver must resolve it when the member and Microsoft server synchronize DHCP data only.

— **DNS**: 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 and test their connection the Grid member.

— Click the Add icon to add another Microsoft server.

— Select a Microsoft server and click the Test Microsoft Server icon to verify whether the appliance can successfully connect to the Microsoft server. The appliance displays the test results in the Test Microsoft Server Results dialog box.

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

or

Click **Next**: Continue to the next step and define extensible attributes for the Microsoft servers. For information, see *Using Extensible Attributes* on page 265.

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 763. 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 406. To view DHCP data, navigate to the **Networks** tab of the network view that you specified. For information, see *Managing IPv4 DHCP Data* on page 639.

  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 99.

- Update the synchronized data. For information, see *Chapter 29, Managing Microsoft DNS Services*, on page 767 and *Chapter 30, Managing Microsoft DHCP Services*, on page 785.

You can also use Global Search to search for synchronized data, such as zones and IP addresses. For information, see *Global Search* on page 49.
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 762.
- Back up the synchronized data, as described in Backing Up Synchronized Data on page 762.
- Disable synchronization with a Microsoft server, as described in Disabling Synchronization on page 762.
- Remove a Microsoft server, as described in Removing a Managed Microsoft Server on page 763.

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 -> 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 759.
   - 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 765 for a description of each level.
   - Extensible Attributes: Define extensible attributes for the server. For information, see Using Extensible Attributes on page 265.
   - Permissions: Define administrative permissions that apply to the server. For information see About Administrative Permissions on page 120.
3. Save the configuration and click Restart if it displays at the top of the screen.

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

Backing Up Synchronized Data

When you back up the Grid, it includes all managed Microsoft data. If you restore a backup, the data is restored on the Grid only. It is not synchronized to the Microsoft servers. When the Grid member synchronizes the data after the restore operation, it overrides the data on the Grid with the data from the Microsoft servers. For information about backing up and restoring data, see Chapter 9, Managing NIOS Software and Configuration Files, on page 315.

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. Save the configuration and click Restart if it displays at the top of the screen.
Removing a Managed Microsoft Server

When you remove a Microsoft server from the Grid, the managing member stops any 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 784 and Disabling and Removing Microsoft DHCP Servers on page 805.

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 97.
- You can view the status of Microsoft servers. For information, see Viewing the Status of Servers on page 763.
- You can view the logs of the Microsoft servers. For information, see Viewing Synchronization Logs on page 765.

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><img src="image" alt="Green" /></td>
<td>Green</td>
<td>The DNS service is functioning properly.</td>
</tr>
<tr>
<td><img src="image" alt="Red" /></td>
<td>Red</td>
<td>The DNS service is stopped.</td>
</tr>
<tr>
<td><img src="image" alt="Yellow" /></td>
<td>Yellow</td>
<td>The DNS service is starting or stopping.</td>
</tr>
<tr>
<td><img src="image" alt="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 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 DHCP service is functioning properly.</td>
</tr>
<tr>
<td><img src="image" alt="Red" /></td>
<td>Red</td>
<td>The DHCP service is stopped.</td>
</tr>
<tr>
<td><img src="image" alt="Yellow" /></td>
<td>Yellow</td>
<td>The DHCP service is starting or stopping.</td>
</tr>
<tr>
<td><img src="image" alt="Gray" /></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 761.

• **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 763.
• 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 804. For information about setting DNS server properties, see Specifying Forwarders for Microsoft Servers on page 783.
• View detailed server status information, as described in Viewing Detailed Status Information on page 765.
• Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
• Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 57.
• 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 763.
• **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 763.
• **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 761.

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.
- Use filters and the *Go to* function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the *Go to* field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see *Using Quick Filters* on page 57.
- Export or print the content of the log.
Chapter 29 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 755.

The topics in this chapter include:

- Managing Microsoft DNS Servers on page 768
  - Synchronizing DNS Data on page 768
  - Synchronizing with Multiple Servers on page 769
- Managing Synchronized DNS Data on page 770
  - Adding Zones to Microsoft Servers on page 771
  - Setting Zone Properties on page 772
  - Deleting and Restoring Synchronized Zones on page 773
  - Managing Resource Records in Synchronized Zones on page 774
- Synchronizing Updates on page 776
  - Synchronizing Delegations on page 779
  - Synchronizing AD-Integrated Zones on page 782
  - Resolving Conflicts on page 782
- Viewing Members and Managed Servers on page 783
- Specifying Forwarders for Microsoft Servers on page 783
- Disabling and Removing Microsoft DNS Servers on page 784
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 Server column of the Zones tab shows which Microsoft server is actually performing the synchronization of that zone with the Grid.
Managing Synchronized DNS Data

When Grid members are configured to manage Microsoft servers in read/write mode, you can use Grid Manager to view, edit and delete the DNS data of those servers. You can add new zones and assign them to a Microsoft server. You can modify the properties of zones synchronized from the Microsoft server and edit their resource records as well. All updates are synchronized to the Microsoft servers at regular intervals.

The following sections provide guidelines for managing the zones and resource records served by Microsoft servers:

- Adding Zones to Microsoft Servers on page 771
- Setting Zone Properties on page 772
- Deleting and Restoring Synchronized Zones on page 773
- Managing Resource Records in Synchronized Zones on page 774

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 385.
- You can copy records to and from zones synchronized with Microsoft servers. When copying records to a Microsoft zone, you can copy only those records that are supported by Microsoft servers. For information about copying records, see Defining a Match Destinations List on page 361.
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 370.
- Forward- and reverse-mapping stub zones—For information, see Configuring Stub Zones on page 398.
- Delegations—For information, see Configuring a Delegation on page 393.

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 on page 772.
- You can set certain zone properties that are not supported and synchronized to the Microsoft server. For example, you can define extensible attributes and administrative permissions. When you set these properties, they apply to the zones only when they are managed from Grid Manager.
- Infoblox does not support all the zone properties of a Microsoft DNS server. When a Grid member synchronizes zones that were created on Grid Manager to the Microsoft server, the zones contain default values for all unsupported properties.
- If you set the Disable option, the zone status is set to “Paused” on the Microsoft server. A zone in a “Paused” status is not served to DNS clients, nor is it available for zone updates.
- Setting the Disable option does not stop synchronization. Grid members synchronize disabled zones.
- The member learns the Windows version of the Microsoft server after its first successful synchronization. Certain zones and resource records are dependent on a specific Windows version. You cannot assign these zones to Microsoft servers whose versions are unknown or insufficient.
- If the member is a secondary server for a zone with a Microsoft primary server, the member obtains the zone data through DNS zone transfers from the Microsoft primary server, not through synchronizations. This ensures that the zone data is always current on the Infoblox secondary server, as it does not have to wait for synchronizations to update its data.
Setting Zone Properties

When the primary server of a zone is a Microsoft server, it does not inherit its properties from the Grid. Zones that are synchronized from a Microsoft server retain their original properties. Zones that Grid Manager admins create assume the Infoblox-defined default values.

To modify the properties of a synchronized zone:

1. From the Data Management tab, select the DNS tab -> Zones tab -> DNS_view -> zone check box and click the Edit icon.

2. In the Authoritative Zone editor, you can do the following in each tab:
   - **General**: You can add or edit comments, and set the Disable and Lock options. Setting the Disable option sets the status of the zone to “Paused” on the Microsoft server. Grid members synchronize disabled zones to Microsoft servers.
   - **Name Servers**: You can modify the name servers assigned to the zone. For information, see Assigning Zone Authority to Name Servers on page 377.
   - **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 443.
   - **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 463. 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 463.
       - **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 both the primary and secondary servers are Microsoft servers, the dialog box displays the Zone Transfer Settings for Microsoft Servers table only.
     - If no Microsoft servers are primary or secondary servers, then the dialog box displays the Zone Transfer Settings for Infoblox Members table only.
   - **Updates**: In this tab, you specify whether the zone can accept dynamic DNS updates. For information about dynamic DNS updates, see Chapter 16, Configuring DDNS Updates from DHCP, on page 477. 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.
Managing Synchronized DNS Data

— **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
  - domain dns zones . zone
  - forest dns zones . 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 265.

- **Permissions:** These permissions apply to Infoblox Grid Manager administrators only. For information, see *About Administrative Permissions* on page 120.

### 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 389.

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 391.
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 413. 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 31, IP Address Management, on page 809.

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 470. 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 443.

• Grid Manager and Microsoft DNS servers display TXT records differently. On Grid Manager, you enter the text string of TXT records as defined in RFC 1035. You can enter the following:
  — A contiguous set of characters without spaces. If you enclose the characters in double quotes, Grid Manager displays the character string without the double quotes. For example, if you enter "abcdef", Grid Manager displays abcd
def.
  — 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 29.1

<table>
<thead>
<tr>
<th>Grid Manager Admin...</th>
<th>Microsoft Server Admin...</th>
<th>After Synchronization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deletes the 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 29.1**, 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 29.1**

![Diagram of Synchronizing Updates](image)

• 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 29.2**, 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 29.2**

![Diagram of Synchronizing Updates](image)
• 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](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 372.

• Grid members synchronize DNS records that contain values that Infoblox does not support. Grid Manager admins can view these records, but they cannot edit or restore such records. For example, if a member synchronizes a NAPTR record that contains an unsupported value in the Service field, admins can view this record but they cannot edit or restore it, as long as it contains an unsupported value.

• When a Grid member synchronizes a zone from a Microsoft server to the appliance and that zone contains UTF-8 characters in the "Responsible Person" field, Grid Manager displays the "Responsible Person" value in the RNAME field of the SOA record of the zone. Note though that you cannot edit the SOA record if the RNAME field contains unsupported UTF-8 characters.

• Synchronizing a new zone from the Microsoft server to the Grid is a two-step process. First the zone name is synchronized, and then its properties and records are synchronized. The zone synchronization from the Microsoft server is not considered complete until both steps are done. NIOS drops any records that are created on the appliance for the synchronized zone before it is completely synchronized.

For example, the corp100.com zone is created on a Microsoft server and then synchronized to the NIOS appliance. If a NIOS admin creates a record, such as an A record, in the corp100.com zone before it is fully synchronized, the record is removed from the corp100.com zone. Ensure that both the zone and its contents are completely synchronized before you add a record to a zone on the NIOS appliance.

• When a Microsoft admin deletes a zone whose primary and secondary servers are Microsoft servers, the zone is deleted from the Grid after a synchronization. If the secondary Microsoft servers are managed by the member in Read-Write mode, the zone is removed from the secondary servers as well. But if some of the secondary Microsoft servers are managed by the member in Read-Only mode, then at the next synchronization the zone is recreated on the Grid with the Microsoft servers as the secondary servers and the masters defined for the zone as external primary servers.

• If you add Grid members or other Microsoft servers as secondary servers to a zone on the Microsoft server, NIOS does not automatically add them as Grid Secondary or Microsoft Secondary servers in the Name Servers tab of the zone after the synchronization. Instead, NIOS creates NS records for them in the zone.
Synchronizing Delegations

When a parent zone delegates a subdomain to one or more name servers, Infoblox DNS servers require the delegation name servers to also be authoritative for the subzone. Microsoft servers do not; they allow the delegation servers of a subzone to be different from its authoritative servers. Infoblox DNS servers support this configuration only if the primary server of the parent zone is a Microsoft server. This configuration is retained when delegations are synchronized from Microsoft servers to the Grid.

For example, as shown in Figure 29.3, on a Microsoft server, corp100.com delegates sales.corp100.com to the name server ns1.corp100.com; but the authoritative server of sales.corp100.com is 2k3r264-2.infoblox.com.

Figure 29.3  Delegation Server and Authoritative Server for corp100.com

The delegation server for sales.corp100.com is different from its authoritative server.

Figure 29.4 shows that after corp100.com and its subzone are synchronized to the Grid, corp100.com contains an NS record for sales.corp100.com and an A record for the delegation name server ns1.corp100.com. The MS Delegation Addresses column displays the IP address of the delegation server of the subzone sales.corp100.com.

Figure 29.4  corp100.com Synchronized to the Grid
After the synchronization, you can add name servers for the delegation as follows:

1. Select the zone by navigating to the Data Management tab ->DNS ->Zones ->parent_zone.
2. Click the Add icon and select Record ->NS Record.
3. Complete the following and click Next:
   - **Name Server**: Enter the hostname you want to configure as the name server for the zone.
   - **Name**: Specify the name of the subzone. Note that you cannot change this name when you edit the record.
4. Enter the IP address of the name server.
5. Save the configuration.

NIOS adds an NS record for the new delegation server and synchronizes this update to the Microsoft server. In Figure 29.5, a new delegation server, ns2.corp100.com, was added.

*Figure 29.5  NS Record for ns2.corp100.com*

corp100.com  Zone  

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
<th>NS Delegation Addresses</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SOA Record</td>
<td>Serial 11</td>
<td></td>
<td>Auto-created by Add Zone</td>
</tr>
<tr>
<td></td>
<td>DNS</td>
<td>NAME 2k8r264-2.infoblox</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS</td>
<td>Name servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ns1</td>
<td>A Record</td>
<td>10.2.3.4</td>
<td></td>
<td>Auto-created by Add Zone</td>
</tr>
<tr>
<td>ns2</td>
<td>A Record</td>
<td>10.1.2.3</td>
<td></td>
<td>Auto-created by Add Zone</td>
</tr>
<tr>
<td>sales1</td>
<td>NS Record</td>
<td>ns1.corp100.com</td>
<td>10.2.3.4</td>
<td>Auto-created by Add NS</td>
</tr>
<tr>
<td>sales2</td>
<td>NS Record</td>
<td>ns2.corp100.com</td>
<td>10.1.2.3</td>
<td>Auto-created by Add NS</td>
</tr>
</tbody>
</table>

When you navigate to the Name Servers tab of sales.corp100.com to view the authoritative name servers for the subzone, note that as shown in Figure 29.6, the table displays 2k8r264-2.infoblox.com as the authoritative server for the subzone. The Parent Delegation column indicates if the FQDN and IP address of the authoritative name server for the zone matches the FQDN and IP address in the delegation zone’s NS record. In the example, the authoritative name server 2k8r264-2.infoblox.com is different from the delegation name servers (ns1.corp100.com and ns2.corp100.com), so the column displays No.

*Figure 29.6 Authoritative Name Server of sales.corp100.com*
Note though that because Infoblox DNS servers require the delegation servers to also be authoritative for the subzone, if you add another authoritative name server to the subzone from Grid Manager, NIOS also adds it as a delegation server in the parent zone. For example, as shown in *Figure 29.7*, when an admin adds the name server ns-100.corp100.com as an external secondary server for sales.corp100.com, NIOS automatically adds it as a delegation server by adding an NS record for it in the parent zone.

*Figure 29.7 Adding Another Authoritative Server from Grid Manager*
Synchronizing AD-Integrated Zones

An AD-integrated zone can be served by multiple domain controllers, and a Grid member can manage more than one of the domain controllers. If the domain controllers are configured to synchronize their DNS data to different DNS views, the Grid member synchronizes DNS data with each domain controller. If the domain controllers are configured to synchronize their DNS data to the same DNS view, the member selects a principal server for synchronization purposes and synchronizes data with that principal server only. The selection of the principal server is logged, as well as when it changes. The Grid member selects a principal server as follows:

- The first domain controller that is assigned as the primary server is designated principal server.
- If a domain controller fails three successive synchronizations, it loses its principal status. The Grid Master then checks the date that each domain controller last became a principal server and selects the one that has not been the designated principal the longest.
- If the domain controllers are managed in read-only and read/write modes, the Grid member always selects the domain controller that is managed in read/write mode.

When a zone is served by multiple Microsoft servers, the MS Sync Server column of the Zones tab shows which Microsoft server is actually performing the synchronization of that zone with the Grid.

The Grid member periodically checks if each zone has one principal server. If it does not find a principal server for a zone, the Grid member selects one among the name servers assigned to the zone. It gives priority to the server that was not the designated principal server the longest.

Following are additional guidelines when synchronizing AD-integrated zones:

- You can create an AD-integrated zone on Grid Manager and assign one domain controller as its primary server. If a domain controller admin adds more primary servers to the zone, they are added to the zone on Grid Manager when the zone is synchronized. If you want to delete the primary servers, you must delete all the primary servers at once. You cannot delete only a subset of the servers.
- A situation could arise where two domain controllers in different AD domains are primary servers for zones with the same name. For example, two reverse-mapping zones could be named 1.1.10.in-addr-arpa in two domain controllers managed by the same member. If the two domain controllers are synchronized to different DNS views, the Grid member synchronizes each one separately. If the domain controllers are synchronized to the same DNS view, then the Grid member synchronizes the zone with the first domain controller. During the synchronization with the second domain controller, the Grid member logs an error and does not synchronize the zone.
- If a Grid Manager admin deletes a CNAME record that has a blank canonical name from an AD-integrated zone, this CNAME record is not deleted from the Microsoft server after the synchronization if the AD-integrated zone is hosted on a Microsoft server running Windows 2008 R2.
- When a Microsoft server is the primary server of a zone that contains an _msdcs zone, it appends the parent zone name to the server name in the NS record of the _msdcs zone. But when an Infoblox grid member is the primary server of a zone that contains an _msdcs zone, it specifies the server name only in the NS record. For example, the _msdcs zone is in the corp100.com zone and the name server is nameserver100.com. When a Microsoft server is the primary server of corp100.com, the server name on the NS record of the _msdcs zone is nameserver100.com.corp100.com. When a Grid member is the primary server, the server name on the NS record of the _msdcs zone is nameserver100.com.

Resolving Conflicts

Some conflicts require intervention from an admin. For example, a Grid member cannot synchronize a zone when its primary server on the Microsoft server is different from its primary server on the Grid. When a Grid member is unable to synchronize data due to such conflicts, it logs an error, skips the object with the error and continues synchronizing the rest of the data. You can then view the Microsoft logs to check which objects were not synchronized. If you resolve the problem, the Grid member synchronizes the object on its next attempt. For information about the logs, see Viewing Synchronization Logs on page 765.
**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 443. To edit the DNS properties of a Microsoft server, see Specifying Forwarders for Microsoft Servers.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 57.
- Export the list of Grid members and Microsoft servers to a .csv file.
  - Click the Export icon.
- Print the list of Grid members and Microsoft servers.
  - Click the Print icon.

**Specifying Forwarders for Microsoft Servers**

A forwarder is a name server to which all other name servers first send queries that they cannot resolve locally. The forwarder then sends these queries to DNS servers that are external to the network, avoiding the need for the other name servers in your network to send queries off-site. You can define a list of forwarders for each managed Microsoft server as follows:

1. From the Data Management tab, select the DNS tab -> Members/Servers tab -> ms_server check box -> Edit icon.
2. Click the Add icon and enter the IP address of the forwarder in the text field.
3. Save the configuration and click Restart if it displays at the top of the screen.
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 762.

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 30 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 755.

The topics in this chapter include:

- About Microsoft DHCP Management on page 786
  - Synchronizing DHCP Data from Microsoft Servers on page 787
  - Viewing Synchronized Leases on page 789
- Managing Synchronized DHCP Data on page 790
  - Adding and Managing Scopes on page 790
  - Adding Fixed Addresses/Microsoft Reservations on page 798
  - About Superscopes on page 800
- Synchronizing Updates on page 802
- Managing Microsoft DHCP Servers on page 803
  - Viewing Members and Managed DHCP Servers on page 803
  - Setting Microsoft DHCP Server Properties on page 804
  - Controlling the DHCP Service of a Microsoft Server on page 805
  - Disabling and Removing Microsoft DHCP Servers on page 805
  - Modifying DHCP Server Assignments on page 805
About Microsoft DHCP Management

Grid Manager enables you to centrally manage the DHCP data of multiple Microsoft DHCP servers from a single interface. Once the DHCP data is synchronized, you can use the Dashboard on Grid Manager to monitor DHCP and server operations, or organize DHCP data into Smart Folders. Through IPAM tools, such as network maps and IP maps, you can track and manage IP address usage in your networks and monitor DHCP range utilization. You can also run a network discovery to retrieve IP allocation for both managed and unmanaged devices—including virtualized resources. For information about the IPAM features, see Chapter 31, IP Address Management, on page 809.

Figure 30.1 Managing Microsoft DHCP Servers from Grid Manager

An admin logs into Grid Manager and uses its tools, such as the Dashboard an IP Map, to manage and monitor multiple DHCP servers.
Synchronizing DHCP Data from Microsoft Servers

After you configure a member to manage the DHCP service of a Microsoft server, the Grid member connects to the server and starts synchronizing IPv4 DHCP data from the Microsoft server to the Grid database. It synchronizes the Microsoft server properties, leases, scopes and reservations.

The synchronization time varies, depending on different factors, such as the number of managed Microsoft servers and the amount of data being synchronized.

**Note:** Synchronizing IPv6 data is not supported.

As shown in Table 30.1, Microsoft servers and Infoblox DHCP servers represent DHCP data differently. Scopes on Microsoft servers are DHCP ranges on Infoblox DHCP servers. Additionally, Microsoft servers support split-scopes, which is a scope assigned to two Microsoft servers. Each scope has an exclusion range on opposite ends to specify the pool of IP addresses that the other Microsoft server allocates. On an Infoblox DHCP server, each scope in the split-scope is represented as a DHCP range with an exclusion range. Note that NIOS also synchronizes scopes assigned to more than two Microsoft servers, but they are not synchronized as split-scopes.

Fixed addresses on Infoblox DHCP servers are the same as reservations on Microsoft servers. Infoblox reservations, which are IP addresses that are excluded from DHCP, are not supported on Microsoft servers. Microsoft superscopes, which are used to group scopes, are represented as superscopes and can be managed from Infoblox DHCP servers.

<table>
<thead>
<tr>
<th>DHCP Data</th>
<th>Microsoft DHCP Servers</th>
<th>Infoblox DHCP Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address pool from which the server allocates addresses</td>
<td>Scope</td>
<td>DHCP Address Range in a Network</td>
</tr>
<tr>
<td>An IP address that is always assigned to the same device</td>
<td>Reservation</td>
<td>Fixed Address</td>
</tr>
<tr>
<td>An IP address that is excluded from DHCP because a user intends to configure it manually on a network device</td>
<td>Not supported</td>
<td>Reservation</td>
</tr>
<tr>
<td>Administrative group of scopes</td>
<td>Superscope</td>
<td>Microsoft superscope</td>
</tr>
</tbody>
</table>

**Note:** In this chapter, reservations always refer to Microsoft reservations (Infoblox fixed addresses), unless otherwise specified.
When the member synchronizes a scope to the Grid, it converts the scope to a DHCP range and network. For example, it converts the Microsoft scope 10.1.1.1-10.1.1.200 with a netmask of /24 to the network 10.1.1.0/24 and DHCP range 10.1.1.1-10.1.1.200 on Grid Manager. The member associates the DHCP properties of the scope, including its DHCP and Microsoft vendor options, with the DHCP range. It synchronizes the leases within the range and if configured, the exclusion range as well.

NIOS synchronizes two scopes as split-scopes if the following conditions are met:

- Two scopes have the same address range.
- The scopes are assigned to two different Microsoft servers.
- Each scope has an exclusion range and the exclusion ranges are at opposite ends of the scope, so they complement each other. For example, the scope 10.1.1.1-10.1.1.200 on Microsoft server A has an exclusion range of 10.1.1.100-10.1.1.200 and the same scope on Microsoft server B has an exclusion range of 10.1.1.1-10.1.1.99.

When the appliance synchronizes a split-scope, it sets a split-scope flag on each scope to indicate that it is part of a split-scope. For more information, see Viewing Scopes on page 797. It synchronizes any reservations that are configured in each scope as well.

When the member synchronizes a Microsoft reservation to the Grid, it converts the reservation to a fixed address and static lease on Grid Manager. It associates the DHCP properties and DHCP and Microsoft vendor options of the reservation with the fixed address record.

The Grid member synchronizes superscopes to the Grid as well. The Grid supports Microsoft superscopes, when an MS management license is installed. For information about adding and managing superscopes in Infoblox DHCP servers, see About Superscopes on page 800.

Following are some guidelines on how a Grid member synchronizes DHCP data from Microsoft servers to the Grid:

- If two superscopes have the same name, but are served by different servers, the member creates two different superscopes on the Grid, each appended with the Microsoft server FQDN.
- The member synchronizes all active and inactive scopes from a managed Microsoft server as long as the scopes do not conflict or include any networks currently served by a Grid member. The member does not synchronize a scope if its network already exists in the Grid and is served by a Grid member. It can synchronize a scope if its network is included in an existing network, only if the network is not served by DHCP.
- Synchronizing scopes that are larger than /12 is not supported.
- NIOS synchronizes all scopes except for those with serving ranges that overlap the serving ranges of existing DHCP ranges.
- If the appliance manages multiple Microsoft servers and synchronizes identical scopes from more than two Microsoft servers, it does not flag the scopes as split-scopes.
- If the appliance synchronizes one or more scopes from Microsoft servers that are identical to an existing split-scope, it removes the split-scope flag from the existing split-scope.
- NIOS does not synchronize partially overlapping scopes inside a single network from different Microsoft servers. It synchronizes only ranges that completely overlap.
- More than two scopes are not synchronized as split-scopes, even if they are identical and have exclusion ranges that complement each other.
- Scopes that have more than one exclusion range are not synchronized as split-scopes, even if the exclusion ranges complement each other. In addition, if a split-scope is synchronized from a Microsoft server and one of the scopes is split again on the Microsoft server, NIOS synchronizes the third scope, but does not set a split-scope flag. In addition, it removes the split-scope flag from the original split-scopes.

You can view the synchronized data as follows:

- To view the networks of the scopes, select the Data Management tab -> DHCP tab -> Networks tab -> Networks panel. This panel displays all IPv4 networks. For information about this panel, see Modifying IPv4 Networks on page 646.
- To view the corresponding DHCP ranges and reservations, select the Data Management tab -> DHCP tab -> Networks tab, and click a network link. For information about this panel, see Viewing Scopes on page 797.

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 31, IP Address Management, on page 809.
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 746. 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 748.
- Clear a lease, by selecting it and clicking the Clear Lease icon. Note that Grid Manager clears the lease immediately. It does not wait for the next synchronization.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 57.

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 613 and Viewing Lease History on page 749.
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*
- *Adding Fixed Addresses/Microsoft Reservations* on page 798
- *About Superscopes* on page 800

Adding and Managing Scopes

To add a scope from Grid Manager, you must create an IPv4 network and a DHCP range, and then assign the Microsoft server to the network and range. To add a split-scope from Grid Manager, you must create an IPv4 network and a DHCP range, and then assign two Microsoft server to the network and range.

To edit a scope synchronized from a Microsoft server, you must edit the properties of its corresponding DHCP range. The following sections describe how to add, edit, and remove scopes using Grid Manager.

**Note:** Microsoft servers do not support Infoblox hosts and reservations. You cannot add them to networks and DHCP ranges served by Microsoft servers.

Adding Networks for Scopes

Following are guidelines for adding a network for Microsoft scopes:

- The network must be served by Microsoft servers. It cannot be served by a mix of Microsoft and Infoblox DHCP servers.
- If you are adding a split-scope, you must assign the network to two Microsoft servers that serve the split-scope. A split-scope cannot be served by a mix of Microsoft and Infoblox DHCP servers.
- The network can contain only one DHCP range per Microsoft server. It can contain multiple DHCP ranges as long as they do not overlap and are each served by a different Microsoft server.
- You can set DHCP properties at the DHCP range level only, not the network level.

You can run discoveries on networks served by Microsoft servers. For information about network discoveries, see *Network Discovery* on page 843.

**Note:** Networks served by Microsoft DHCP servers do not support the split, join, and expand functions.
You can create a network from scratch or use a network template. For information about creating network templates, see *Adding IPv4 Network Templates* on page 628. To add an IPv4 network for a scope:

1. From the **Data Management** tab, select the **DHCP** tab.
2. If you have more than one network view in the system, select the network view in which you want to add the network. It must be the same network view to which the Microsoft server is assigned.
3. Expand the Toolbar and click **Add -> Network**.
4. In the **Add Network wizard**, select one of the following and click **Next**:
   - **Add Network**
   - **Add Network using Template**: Click **Select Template** and select a network template. For more information, see *About IPv4 Network Templates* on page 628. 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. For a split-scope, you must assign two Microsoft servers to the network.
7. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see *About Extensible Attributes* on page 262.
8. Save the configuration and click **Restart** if it displays at the top of the screen.
   - Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 256.
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 643. 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 262.
   - 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 Expert Mode to display the following tabs from which you can modify advanced data.
   - General Advanced: You can associate zones with a network. For information, see Associating Networks with Zones on page 611.
   - Thresholds: These watermarks represent thresholds above or below which address usage is unexpected and might warrant your attention. Thresholds are inherited from the Grid.
     - High-water Mark: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range exceeds this number, the appliance makes a syslog entry. The default is 95.
     - Low-water Mark: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range drops below this number, the appliance makes a syslog entry. The default is 0. Address usage must initially exceed the low-water mark threshold and then dip below it before the appliance considers low address usage an event requiring an alert.

4. Save the configuration and click Restart if it displays at the top of the screen.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.

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 647. For information about restoring data, see Using the Recycle Bin on page 54.
Adding a DHCP Range/Scope

After you add a network for a scope, you must then define its DHCP range. You can create the DHCP range from scratch or use a DHCP Range template. For information about DHCP templates, see About IPv4 Range Templates on page 625. You can add multiple ranges to the same network, as long as each range is served by a different Microsoft server and the ranges do not overlap.

When you add a split-scope, you must specify the Microsoft servers that serve the scopes and their exclusion ranges. Each scope inherits its options from its respective Microsoft server. Note that the enabled/disabled setting of the first range automatically applies to the second range. Therefore, if the first range is initially disabled, then the second range is initially disabled as well.

To add a DHCP range for a scope:

1. From the Data Management tab, select the DHCP tab.
2. Navigate to the network to which you want to add a DHCP range, and then click Add -> DHCP Range from the Toolbar. You can also add a DHCP range from any panel in the DHCP tab.
3. In the Add Range wizard, select one of the following and click Next:
   - Add DHCP Range
   - Add DHCP Range using Template
     * Click Select Template and select the template that you want to use. Note that when you use a template to create a DHCP range, the configurations of the template apply to the new range. The appliance automatically populates the DHCP range properties in the wizard. You can then edit the pre-populated properties.
4. Complete the following:
   - Network: Click Select Network to select the network to which you want to add the DHCP range. The network must be served by a Microsoft server. If you are adding a DHCP range while viewing the contents of a specific network, the appliance displays the network address here. You can still select a different network by clicking Select Network.
   - Start: Enter the first IP address in the range.
   - End: Enter the last IP address in the range.
   - Name: You can enter a name for the DHCP range.
   - Comment: You can enter additional information. After the range is synchronized to the Microsoft server as a scope, this text appears in the Description field of the scope on the Microsoft server.
   - 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.
   - Microsoft Split-Scope: Select this to create a split-scope, and then complete the following:
     - Microsoft Server #1: Read-only field that displays the Microsoft server that you specified in the preceding step.
     - Microsoft Server #2: Select the Microsoft server that will serve the split-scope.
   - Split Percentage: Specify the percentage of IP addresses in the scope that is allocated to the exclusion range of each Microsoft server. The default is 50%. You can either move the slider or enter the percentages in the text fields. When you use the slider, you are specifying the percentage of addresses in the exclusion range of the first server. A tooltip window displays the percentage as you adjust the slider. When you set the slider, the Split Percentage, Exclusion Starting Address, and Exclusion Ending Address fields are updated accordingly.
— **Exclusion Starting Address**: When you set the split percentages, these fields automatically display the starting address of the exclusion range of each Microsoft server. Alternatively, you can enter the starting address of the exclusion range of the first Microsoft server, and the **Split Percentage** and **Exclusion Ending Address** values adjust accordingly.

— **Exclusion Ending Range**: When you set the split percentage, these fields automatically display the ending address of the exclusion range of each Microsoft server. Alternatively, you can enter the ending address of the exclusion range of the second Microsoft server, and the **Split Percentage** and **Exclusion Starting Address** values adjust accordingly.

6. Click **Next**, and optionally set operational parameters for the scope. Otherwise, the scope inherits its parameters from the first Microsoft DHCP server.

   • **Lease Time**: Specify the lease time. The default is 8 days. When the range is served by a Microsoft server and you enter a lease time of 1000 days or more, Grid Manager automatically grays out this field and checks the Unlimited Lease Time option after you save your entries.

   — **Unlimited Lease Time**: Select this option to set an infinite lease time for the IP addresses leased from this range.

   — **Routers**: In the table, enter the IP address of the router that is connected to the same network as the DHCP clients. Click the Add icon to add more routers.

   — **Domain Name**: Enter the name of the domain for which the Microsoft server serves DHCP data. The DHCP server includes this domain name in Option 15 when it responds with a DHCPOFFER packet to a 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 265.

8. Save the configuration and click **Restart** if it displays at the top of the screen.

   or

   — Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see **Scheduling Tasks** on page 256.
Setting DHCP Range/Scope Properties

A Microsoft scope inherits its properties from its Microsoft server. In Grid Manager, you can override the inherited values or set other properties by editing the DHCP range. You can also configure an exclusion range within the scope and set thresholds, to enable the appliance to make a syslog entry when address usage goes above or below the thresholds.

You can modify a scope’s properties, including its start and end addresses, servers, and exclusion ranges. If you edit the properties of a split-scope and it results in gaps or overlapping exclusion ranges so that the ranges are no longer identical, Grid Manager displays a warning indicating that continuing with the operation automatically removes the split-scope flag. Grid Manager also removes the flag when the start or end address of a scope changes, so its range is no longer the same.

To set DHCP range properties:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range check box, and then click the Edit icon.

2. The DHCP Range editor contains the following basic tabs from which you can modify data:
   - **General**: Modify the fields, including the start and end addresses, as described in Adding a DHCP Range/Scope.
   - **Server Assignment**: Switch to None or select a different Microsoft server for the DHCP range.
   - **IPv4 DHCP Options**: Keep the DHCP properties or override them and enter unique settings for the DHCP range. For information about the fields, see Adding a DHCP Range/Scope on page 793.
     This tab displays DHCP and Microsoft vendor options that were synchronized from the Microsoft server. You can edit any of the options. When you select a different User Class or Vendor Class from the drop-down menus, Grid Manager automatically updates the option definitions in the drop-down list.
     To configure additional DHCP options, click + and select a User Class and Vendor Class from the drop-down menus. Select an option from the drop-down list, and enter a value in the field beside it. You can click - to remove an option.
   - **Extensible Attributes**: You can add and delete extensible attributes that are associated with a specific DHCP range. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes on page 265.
   - **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 Expert Mode** to display the following tabs from which you can modify advanced data.
   - **DDNS**: Complete the following to set DDNS parameters for the range:
     - **Enable DDNS Updates**: Click the check box to enable the Microsoft DHCP server to send dynamic DNS updates or clear the check box to disable this function.
     - **Option 81 Support**
       - **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 Configuring IPv4 Fixed Addresses on page 653. In a split-scope, the exclusion range identifies the range of IP addresses that the other Microsoft server serves. If you edit the exclusion range of either of the scopes in a split-scope and the exclusion ranges no longer complement each other, NIOS removes the split-scope flag from both scopes.
   - **Thresholds**: Thresholds are inherited from the Grid. These watermarks represent thresholds above or below which address usage is unexpected and might warrant your attention.
     - **High-water Mark**: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range exceeds this number, the appliance makes a syslog entry. The default is 95.
— **Low-water Mark**: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range drops below this number, the appliance makes a syslog entry. The default is 0. Address usage must initially exceed the low-water mark threshold and then dip below it before the appliance considers low address usage an event requiring an alert.

4. Save the configuration and click **Restart** if it displays at the top of the screen.
   or
   — Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks* on page 256.

**Deleting and Restoring a DHCP Range/Scope**

When you delete a DHCP range, Grid Manager moves it and its exclusion range and fixed addresses to the Recycle Bin, and permanently deletes its leases. At the next synchronization, the member deletes the scope, its exclusion range and reservations from the Microsoft server. If you restore a DHCP range on Grid Manager, then the Grid member adds its corresponding scope, exclusion range and reservations to the Microsoft server at the next synchronization. For information about deleting DHCP ranges, see *Deleting IPv4 Address Ranges* on page 652. For information about restoring data, see *Using the Recycle Bin* on page 54.

If you delete a scope that is part of a split-scope, Grid Manager automatically removes the split-scope flag from the remaining scope.
Viewing Scopes

To view the scopes in a network, navigate to DHCP -> Networks -> network. The panel displays the objects in the network, including the scopes and split-scopes. For split-scopes, the panel displays both scopes with the same start and end address. It displays the following information about each object:

- **IP Address**: The IP address of the DHCP object. For a scope, this field displays the start and end addresses of the scope. Note that the appliance highlights all disabled DHCP objects in gray.
- **Split-Scope**: Displays Yes if the scope is a split-scope.
- **MS Server**: Displays the Microsoft server that is serving the scope.
- **Type**: The DHCP object type, such as DHCP Range or Fixed Address.
- **Name**: The object name. For example, if the IP address belongs to a host record, this field displays the hostname.
- **Comment**: The information you entered for the object.
- **IPv4 DHCP Utilization**: The percentage of the total DHCP usage of a DHCP range. This is the percentage of the total number of fixed addresses, reservations, hosts, and active leases in the DHCP range divided by the total IP addresses in the range, excluding the number of addresses in the exclusion ranges. Note that only enabled objects are included in the calculation.
- **Site**: The site to which the DHCP object belongs. This is one of the predefined extensible attributes.

You can select the following additional columns for display:

- **Static Addresses**: Indicates whether the IP address is a static address.
- **Dynamic Addresses**: Indicates whether the IP address is a dynamically assigned address.
- **Disabled**: Indicates whether the object is disabled.
- **Priority**: Displays the priority of a DHCP range when NAC filters are applied.
- **Available extensible attributes.

You can also do the following in this panel:

- Sort the displayed data in ascending or descending order by column.
- Click **Go to IPAM View** to view information about the object in the IPAM tab.
- Add new objects, such as DHCP ranges, to the network.
- Delete or schedule the deletion of a selected object or multiple objects.
- Use filters and the **Go to** function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the **Go to** field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see **Using Quick Filters** on page 57.
- **Print** or export the data.

You can also view the scopes in the IP Map.
Adding Fixed Addresses/Microsoft Reservations

To add a reservation from Grid Manager, add a fixed address and Grid Manager synchronizes it to the Microsoft server as a reservation. You can create fixed addresses from scratch or use fixed address templates. For information about fixed address templates, see Adding IPv4 Fixed Address/Reservation Templates on page 627.

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 265.
7. Save the configuration and click Restart if it displays at the top of the screen.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.
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 -> 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 798.
   - IPv4 DHCP Options: Keep the inherited properties, or override them and enter unique settings.
     This section displays DHCP and Microsoft vendor options that were synchronized from the Microsoft server. You can edit any of the options. When you select a different User Class or Vendor Class from the drop-down menus, Grid Manager automatically updates the option definitions in the drop-down list.
     To configure additional DHCP options, click + and select a User Class and Vendor Class from the drop-down menus. Select an option from the drop-down list, and enter a value in the field beside it. You can click - to remove an option.
   - Discovered Data: If you ran a discovery on the network, Grid Manager displays the discovered data of the fixed address. For information, see Viewing Discovered Data on page 858. 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 861.
   - 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 265.
   - Permissions: This tab appears only if you belong to a superuser admin group. For information, see Managing Permissions on page 128.

3. Optionally, you can click Toggle Expert Mode to display the DDNS tab. To set DDNS parameters for the fixed address, complete the following:
   - Enable DDNS Updates: Click the check box to enable the Microsoft DHCP server to send dynamic DNS updates or clear the check box to disable this function.
   - Option 81 Support
     - DHCP Server Updates DNS If Requested by Client: The DHCP server updates DNS only if it is requested by the client. Otherwise, the client updates DNS.
     - DHCP Server Always Updates DNS: The DHCP server always updates DNS, regardless of any client request.

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

or

- Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.

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 655. For information about restoring data, see Using the Recycle Bin on page 54.
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 262.
7. Save the configuration and click Restart if it displays at the top of the screen.

or
   — Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks on page 256.

Viewing Superscopes

To view superscopes, navigate to the Data Management tab -> DHCP tab -> Networks tab -> Microsoft Superscopes. Grid Manager displays the following information about each superscope that is displayed:

- Name: The name of the superscope. Grid Manager appends the FQDN of its associated Microsoft server so you can identify which superscope belongs to which server.
- Comment: The comment that was entered for the superscope.
- DHCP Utilization: The percentage of the total DHCP usage of the ranges in the superscope. Fixed addresses and reservations that are outside of a range are excluded from the calculation.
- Site: The site of the superscope. This is one of the predefined extensible attributes.

You can add the following columns for viewing:

- Static Addresses: The number of static addresses.
- Dynamic Addresses: The number of dynamic addresses.
- Disabled: Indicates whether the superscope is enabled.
You can do the following in this section:

- Click the link of a superscope to list its address ranges.
- Add a superscope.
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see **Modifying Data in Tables** on page 52.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see **Using Quick Filters** on page 57.
- 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 265.
   - **Permissions**: Define administrative permissions that apply to the superscope when it is managed in Grid Manager. For information see **About Administrative Permissions** on page 120.
3. Save the configuration and click **Restart** if it displays at the top of the screen.

### Deleting Superscopes

When you delete a superscope in Grid Manager, it is permanently deleted from the database. The superscope is deleted from the Microsoft server at the next synchronization. Note that deleting a superscope does not delete the DHCP ranges in the superscope. These are retained in the database.

To delete a superscope:

1. From the **Data Management** tab, select the **DHCP** tab -> **Network** tab -> **Microsoft Superscopes** -> **ms_superscope** check box, and then click the Delete icon.
2. Click **Yes** when the confirmation dialog appears.
Synchronizing Updates

A Grid member synchronizes DHCP data with each of its managed Microsoft server at regular intervals. During each synchronization, updates from Grid Manager are applied to the Microsoft server and updates from the Microsoft server are applied to the Grid as well.

Because admins can update DHCP data from both the Microsoft server and from Grid Manager, conflicts can occur during synchronization. The following guidelines describe how the Grid member resolves conflicts and handles any differences when DHCP data is synchronized between a Microsoft server and the Grid.

- If a Microsoft server admin modifies an object that has a pending scheduled task in Grid Manager and synchronization occurs before the scheduled task, the object is modified in both the Microsoft server and the Grid member. When the scheduled task executes at its scheduled time, it fails and an error message is logged in the audit log.
- When a Microsoft server admin and a Grid Manager admin change the same object, the Grid member retains the version that exists on the Microsoft server. Following are some examples:

  **Table 30.2**

<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>

- 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 765.

  Note that a Grid member can synchronize scopes with overlapping reservations because they are served by different Microsoft servers.

- When a Grid member synchronizes a split-scope to its respective Microsoft servers, the scopes use the default value for the DHCP Offer Delay value, since this property is not supported by NIOS.

- If you create a split-scope on a NIOS appliance, synchronization fails if there is an existing scope in the same network on one of the Microsoft servers. Only one scope is allowed in a network, per Microsoft server.

- If a Microsoft admin adds a DHCP range and a NIOS admin is in the process of adding the same range when a synchronization occurs, the NIOS admin will not be able to save the range after the synchronization. Grid Manager will display an error message indicating that the range already exists.

- If both a NIOS admin and a Microsoft admin create a scope or split-scope and conflicts occur, the Microsoft server always takes precedence. All conflicts are logged to the Microsoft log. Following are some examples:
  - If the NIOS admin creates a scope and a Microsoft server admin creates a split-scope for the same DHCP range, the split-scope is synchronized to Grid Manager.
  - If the NIOS admin creates a split-scope on Microsoft servers 1 and 2, and a Microsoft admin creates the same split-scope on Microsoft servers 1 and 3 but with different exclusion ranges, the scope created by the NIOS admin on Microsoft server 1 is dropped upon synchronization.
  - If the NIOS admin creates a split-scope on Microsoft servers 1 and 2, and a Microsoft admin creates the same split-scope on the same Microsoft servers but with different exclusion ranges, the split-scope created by the Microsoft admin is synchronized to NIOS and retained. The split-scope created by the NIOS admin is dropped.
Managing Microsoft DHCP Servers

You can control the DHCP services of managed Microsoft servers and set certain properties as well. This section includes the following topics:

- Viewing Members and Managed DHCP Servers
- Setting Microsoft DHCP Server Properties on page 804
- Controlling the DHCP Service of a Microsoft Server on page 805
- Disabling and Removing Microsoft DHCP Servers on page 805
- Modifying DHCP Server Assignments on page 805

Viewing Members and Managed DHCP Servers

You can view Infoblox and Microsoft DHCP servers by navigating to the Data Management tab -> DHCP tab, and then selecting the Members/Servers tab. The panel displays the following information about each DHCP server:

- **Name:** The hostname of the Grid member or Microsoft server.
- **Status:** The status of the DHCP service on the Grid member or Microsoft server.
- **Comment:** Comments that were entered for the Grid member or Microsoft server.
- **DHCP Utilization:** The percentage of the total DHCP utilization of the member or Microsoft server. This is the percentage of the total number of DHCP hosts, fixed addresses, reservations, and leases assigned to the member or Microsoft server versus the total number of IP addresses (excluding IP addresses in the exclusion range) and all DHCP objects assigned to the member or DHCP server. Note that only enabled objects are included in the calculation. The appliance updates the utilization data every 15 minutes. The appliance displays the utilization data in one of the following colors:
  - Red: The DHCP resources are 100% utilized.
  - Yellow: The utilization percentage is over the effective high watermark threshold.
  - Blue: The utilization percentage is below the effective low watermark threshold.
  - Black: The utilization percentage is at any number other than 100%, or within the effective thresholds.
- **Site:** Values that were entered for this pre-defined attribute.

You can select the following additional columns for display:

- **Address:** The IP address of the member or Microsoft server.
- **Static Addresses:** The number of static IP addresses.
- **Dynamic Addresses:** The number of dynamically assigned IP addresses.

You can do the following:

- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 57.
- 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 and the logging.

To set properties for a Microsoft DHCP server:

1. From the Data Management tab, select the DHCP tab -> Members/Servers tab -> Members/Servers -> ms_server check box, and then click the Edit icon.

2. In the Microsoft Server DHCP Properties editor, you can configure DHCP properties in each tab as follows:
   - IPv4 DHCP Options tab: Complete the following to configure basic DHCP options for the server:
     - Routers: Click the Add icon and enter the IP address of the router that is connected to the same network as the DHCP clients.
     - Domain Name: Enter the name of the domain for which the server serves DHCP data. The DHCP server includes this domain name in Option 15 when it responds with a DHCPOFFER packet to a DHCPDISCOVER packet from a client. If DDNS is enabled on the DHCP server, it combines the host name from the client and this domain name to create the FQDN (fully-qualified domain name) that it uses to update DNS.
     - DNS Servers: Click the Add icon and enter the IP address of the DNS server to which the DHCP client sends name resolution requests. The DHCP server includes this information in the DHCPOFFER and DHCPACK messages.
     - Broadcast Address: Enter the broadcast IP address of the network to which the DHCP server is attached.
     - Custom DHCP Options: This section displays DHCP and Microsoft vendor options that were synchronized from the Microsoft server. You can edit any of the options. When you select a different User Class or Vendor Class from the drop-down menus, Grid Manager automatically updates the option definitions in the drop-down list.
       To configure additional DHCP options, click + and select a User Class and Vendor Class from the drop-down menus. Select an option from the drop-down list, and enter a value in the field beside it. You can click - to remove an option.
   - DDNS tab: You can enable or disable dynamic DNS updates and set certain properties.
     - Enable DDNS Updates: Click the check box to enable the Microsoft DHCP server to send dynamic DNS updates or clear the check box to disable this function.
     - Option 81 Support
       - DHCP Server Updates DNS If Requested by Client: The DHCP server updates DNS only if it is requested by the client. Otherwise, the client updates DNS.
       - DHCP Server Always Updates DNS: The DHCP server always updates DNS, regardless of any client request.
   - Thresholds tab: Thresholds are inherited from the Grid. These watermarks represent thresholds above or below which address usage is unexpected and might warrant your attention.
     - Enable DHCP Thresholds: Select this check box to enable the feature.
       - High-water Mark: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range exceeds this number, the DHCP server makes a syslog entry. The default is 95.
       - Low-water Mark: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range drops below this number, the DHCP server makes a syslog entry. The default is 0. Address usage must initially exceed the low-water mark threshold and then dip below it before the appliance considers low address usage an event requiring an alert.

3. Optionally, you can click Toggle Expert Mode to display the Logging tab, where you can enable the managing member to log the lease events of the Microsoft server. This setting is inherited from the Grid. You can override that setting by clicking Override, and then selecting or clearing the Log Lease Events from DHCP server check box.

4. Save the configuration and click Restart if it displays at the top of the screen.
Controlling the DHCP Service of a Microsoft Server

You can start and stop the DHCP service of a managed Microsoft server from Grid Manager as follows:

1. From the Data Management tab, select the DHCP tab -> Members/Servers tab -> Members/Servers -> ms_server check box.
2. Expand the Toolbar and click Start or Stop.
3. Click Yes when the confirmation dialog appears.

Disabling and Removing Microsoft DHCP Servers

If you remove a Microsoft server as a managed server, Grid Manager deletes all the DHCP ranges, leases, and fixed addresses associated with the server. It also deletes networks that were assigned only to the Microsoft server. It does not delete a network if it was assigned to other Microsoft servers as well.

When you disable a Microsoft server, the managing Grid member terminates any on-going synchronization and restarts synchronization only when the server is re-enabled. The DHCP data associated with that server is preserved in the same state until synchronization resumes.

For information on removing and disabling Microsoft servers, see Disabling Synchronization on page 762 and Removing a Managed Microsoft Server on page 763.

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 IP Address Management

IPAM (IP Address Management) is the allocation, administration, reporting, and tracking of IP addresses, network devices, and their associated data. This section provides information about IPAM and how to use the Infoblox tools to perform IPAM tasks and manage your entire IP network. It includes the following chapters:

- Chapter 31, IP Address Management, on page 809
- Chapter 32, Network Discovery, on page 843
Chapter 31 IP Address Management

This chapter describes how to manage your networks and IP addresses through the Infoblox IPAM (IP Address Management) implementation. It contains the following sections:

- **About IP Address Management** on page 810
- **About Host Records** on page 811
  - Assigning Multiple IP Addresses to a Host on page 812
  - Adding Host Records on page 813
  - Modifying Host Records on page 814
- **About Network Containers** on page 815
  - Adding IPv4 and IPv6 Network Containers and Networks on page 816
  - Modifying IPv4 and IPv6 Network Containers and Networks on page 816
  - Deleting Network Containers on page 817
- **Managing IPv4 Networks** on page 817
  - IPv4 Network Map on page 818
  - Network List on page 821
  - Resizing IPv4 Networks on page 822
  - Splitting IPv4 Networks into Subnets on page 822
  - Joining IPv4 Networks on page 823
  - Deleting Networks on page 824
- **Viewing and Managing IPv4 Addresses** on page 825
  - IP Map on page 825
  - IP Address List on page 827
  - Managing IPv4 Addresses on page 829
- **Managing IPv6 Networks** on page 831
  - IPv6 Network Map on page 832
  - IPv6 Network List on page 835
  - Splitting IPv6 Networks into Subnets on page 836
  - Joining IPv6 Networks on page 836
- **Viewing IPv6 Data** on page 837
- **Managing IPv4 and IPv6 Addresses** on page 838
  - Converting Objects Associated with IP Addresses on page 838
  - Reclaiming Objects Associated with IPv4 and IPv6 Addresses on page 841
  - Pinging IP Addresses on page 841
  - Clearing Active DHCP Leases on page 841
About IP Address Management

IPAM is the allocation, administration, reporting, and tracking of public and private IP spaces, network devices, and their associated data. It comprises the deployment of DNS and DHCP services and the monitoring of network devices and performance to ensure data integrity and security of your networks.

The Infoblox IPAM implementation is a feature-rich and easy-to-use solution that encompasses support for IPv4, IPv6, network discovery, and automated monitoring.

Infoblox IPAM provides tools that integrate the allocation, administration, reporting, and tracking of your entire network space. *Figure 31.1* highlights the Infoblox IPAM implementation.

*Figure 31.1 Infoblox IPAM Features*

You can do the following:

- Create host records. Host records integrate the DNS records and DHCP data of a network device. You can use a host record to manage a network device from one central point. For more information, see *About Host Records* on page 811.
- Create IPv4 and IPv6 network containers and networks. For information, see *About Network Containers* on page 815.
- View your IPv4 network and address utilization in a graphical mode. For information, see *IPv4 Network Map* on page 818 and *IP Map* on page 825.
- Manage IPv4 and IPv6 address data. For information, see *Viewing and Managing IPv4 Addresses* on page 825, *Viewing IPv6 Data* on page 837, and *Managing IPv4 and IPv6 Addresses* on page 838.
- Add and manage A, AAAA, and PTR records associated with IP addresses. You can add these records from the Toolbar in the *IPAM* tab and the *DNS* tab. For information, see *Chapter 14, DNS Resource Records*, on page 407.
About Host Records

Host records provide a unique approach to the management of DNS, DHCP, and IPAM data. By using host records, you can manage multiple DNS records and DHCP and IPAM data collectively, as one object on the appliance.

When you create a host record, you are specifying the name-to-address and address-to-name mappings for the IP address that you assign to the host. The Infoblox DNS server then uses this data to respond to DNS queries for the host. When the server receives a name-to-address query, it responds with an A record for an IPv4 host or an AAAA record for an IPv6 host that contains the data from the host record. Likewise, when it receives an address-to-name query for the host, the appliance responds with a PTR record that contains data from the host record. Additionally, if you specify an alias in the host record, the appliance uses this data as a CNAME record to respond to queries with the alias. It maps the alias to the canonical name and sends back a response with the canonical name and IP address of the host. Thus, a single host record is equivalent to creating A, PTR, and CNAME resource records for an IPv4 address and AAAA and PTR records for an IPv6 address.

Hosts also support prefix delegation for IPv6. For example, you can specify an IPv6 prefix in the host record of a router. The router then advertises this prefix on one of its interfaces, so hosts that connect to the interface can generate their IP addresses, using the stateless autoconfiguration mechanism defined in RFC 2462, IPv6 Stateless Autoconfiguration.

In addition, if the Infoblox DHCP server manages the IP address assigned to the host, the server uses it as a fixed address record as well. The DHCP server assigns the IP address to the host when it receives a DHCP request with the matching MAC address or DUID. Its response includes configuration information, and any DHCP options and options filters defined for the host or inherited from the network to which the fixed address belongs. You can also assign multiple IPv4 and IPv6 addresses to a host, as described in Assigning Multiple IP Addresses to a Host on page 812.

Note that you can modify the host record of an IPv4 and make it a reservation, as well. For information, see Configuring IPv4 Reservations on page 656.

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 262.

Figure 31.2 illustrates how the appliance uses the host record for both DHCP and DNS.

Figure 31.2 Using the Host Record for DHCP and DNS

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.

DNS and DHCP server

A resolver sends a query for the IP address of ftp.corp.100.com.

DNS Resolver

ftp.corp100.com

1. A resolver sends a query for the IP address of ftp.corp.100.com.
2. 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 611.
Assigning Multiple IP Addresses to a Host

You can assign multiple IPv4 and IPv6 addresses to a host depending on the function of the device. For example, you can create a host record for a router that supports three network interfaces in two different networks, and assign IP addresses to each interface, as illustrated in Figure 31.3. When the DNS server responds to DNS queries for the host, it includes an A or AAAA record for each IP address.

In addition, if the IP addresses belong to different networks, they can have different DHCP configurations and options. As shown in Figure 31.3, the configuration information and DHCP options of the interface with the IPv6 address 2001:db8:1::2 may be different from the other two interfaces, 10.31.209.5 and 10.31.209.7, because it is in a different network.

Figure 31.3 Assigning Multiple IP Addresses to one Host Record

You create a host record for the router and assign three IP addresses to it.
Adding Host Records

You can add host records from the Toolbar of the IPAM, DHCP and DNS tabs of the Data Management tab and from the Tasks Dashboard. For information about the Tasks Dashboard, see The Tasks Dashboard on page 70.

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 from the Data Management tab:

1. From the IPAM, DHCP or DNS tab of the Data Management tab, expand the Toolbar.
2. Click Add and select the option to add a host 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 is 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.

   — **RRset Order**: Select one of the following RRset orders that the appliance uses to return A and AAAA records of the host. This check box appears only when you have enabled the configuration of RRset order for the Grid and there are multiple IP addresses in this host record. For information about how to enable this feature, see Enabling the Configuration of RRset Orders on page 445.

     — **Cyclic**: The records are returned in a round robin pattern. This is the default.

     — **Fixed**: The records are returned in the order you specify in this host record. When you select this check box, the appliance displays up and down arrows next to the IPv4 and IPv6 address tables. You can use these arrows to reorder the address list. The appliance returns the A and AAAA records of this host based on the order you define in the address tables.

     — **Random**: The records are returned in a random order.

   Note that when you specify Fixed as the RRset order, the appliance places the resource records as follows:

   • A and AAAA records of the host in the fixed order you specify in the address tables. Note that the order of the returned A and AAAA records is independent of each other.

   • Other A and AAAA records in an undefined order.

   • Other record types in the default cyclic order.

   For more information about RRset order, see Enabling the Configuration of RRset Orders on page 445.

   — In the IPv4 Addresses and IPv6 Addresses sections, specify the IP addresses of the host record. Click the Add icon do one of the following:

     — Select Next Available IP Address to retrieve the next available IP address in a network. Infoblox recommends this option to ensure that you assign an IP address from the appropriate network.

     If the host record is in a zone that has one associated network, Grid Manager retrieves the next available IP address in that network.

     If the host record is in 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 352.

Optionally, you can delete an IP address from the host by selecting an IP address in the table and clicking the Delete icon.

or

— Select Add Address to enter an IPv4 or IPv6 address. You can also enter an IPv6 prefix. Note that when you use this option, you could specify an IP address from a network that has not yet been defined. To avoid this, use the Next Available IP Address option instead.

— MAC Address: For an IPv4 address, enter the MAC address of the network device associated with this host IP address. Note that you must enter a MAC address if DHCP is enabled for the host IP address.

or

— DUID: For an IPv6 address, enter the DHCP Unique Identifier (DUID) of the network device associated with this host IP address. Note that you must enter a DUID if DHCP is enabled for an IPv6 host address.

— DHCP: Select this to enable the DHCP services to manage the host IP address. If you do not select this option, the host IP address is not managed by the DHCP server.

— Comment: Optionally, enter additional information about the host record.

— Disable: Select this option to temporarily disable the host record. For example, you might want to disable a host when you need to update the network device.

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

or

Click Next to define extensible attributes. For information, see Using Extensible Attributes on page 265.

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 813.

   — TTL: This tab displays the default TTL settings the record inherited from the Grid or the DNS zone, if you enabled override TTL settings at the zone level. You can keep the default settings or override them. To override the inherited value, click Override to enable the configuration. Specify how long the record is cached. Select the time period in seconds, minutes, hours, days, or weeks from the drop-down list. To enable the record to inherit the Grid or zone TTL settings, click Inherit.

   — Aliases: Click the Add icon. Grid Manager displays a new row in the table. Enter a fully qualified domain name (a CNAME record for the host) in the Aliases column. You can delete an alias by selecting the alias check box and clicking the Delete icon.

   — IPv4 Discovered Data: Displays the discovered data of the IPv4 addresses, if any, of the host record. For information, see Viewing Discovered Data on page 858.

   — IPv6 Discovered Data: Displays the discovered data of the IPv6 addresses, if any, of the host record. For information, see Viewing Discovered Data on page 858.

   — 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 265.
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 31.4 illustrates the IPv4 20.0.0.0/8 network, which is a network container with two network containers, 20.8.0.0/13 and 20.72.0.0/13. The 20.8.0.0/13 network has two leaf networks, 20.8.0.0/16 and 20.9.0.0/16. The 20.72.0.0/13 network has one leaf network, 20.72.0.0/16.

Figure 31.4 IPv4 Network Container

From Grid Manager, you can click the link of the network container 20.0.0.0/8 in the IP List panel and drill down to the two network containers, 20.8.0.0/13 and 20.7.0.0/13, as shown in Figure 31.5. You can click the network container links to drill down further to the leaf networks.
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 822 and Splitting IPv6 Networks into Subnets on page 836.

Adding IPv4 and IPv6 Network Containers and Networks

To add an IPv4 or IPv6 network container or network:
1. From the Data Management tab, select the IPAM tab.
2. Click the Add icon and select either IPv4 Network or IPv6 Network.
3. In the Add Network wizard, create a network as described in Adding IPv4 Networks on page 643 or Adding IPv6 Networks on page 735.

Modifying IPv4 and IPv6 Network Containers and Networks

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

To modify an IPv4 or IPv6 network container or network:
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 646 or Modifying IPv6 Networks on page 736.
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 Using the Recycle Bin on page 54.

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

In Grid Manager, you use the Net Map (network map) and List panels to manage your IPv4 network infrastructure. After you select a network container from the IPAM tab, Grid Manager displays it in the Net Map panel, by default. The Net Map panel provides a graphical view of your networks and has a number of features that simplify network management. The List panel displays the networks in table format.

You can always switch your view of a network container between the Net Map and List panels. Grid Manager keeps track of which panel you last used. 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 IPv4 Network Map on page 818 and Network List on page 821.

Use the IP Map and List panels to manage the IP addresses in leaf networks. For information, see Viewing and Managing IPv4 Addresses on page 825.

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:

- Resize a network. For information, see Resizing IPv4 Networks on page 822.
- Split a network into subnets. For information, see Splitting IPv4 Networks into Subnets on page 822.
- Join a network. For information, see Joining IPv4 Networks on page 823.
IPv4 Network Map

After you select an IPv4 network container from the IPAM tab, Grid Manager displays it in the Net Map (network map) panel, by default. Net Map provides a high-level view of your IPv4 network address space. You can use Net Map to design and plan your network infrastructure, configure and manage individual networks, and evaluate their utilization. Its unique display of the IPv4 network address space across multiple rows is similar to a road map that starts with the first IP address in the network and ends with the last address. Net Map displays the network address space across a maximum of eight rows, depending on the size of the network. It automatically scales the map so that it displays the entire address space of a network container.

The Net Map panel presents a complete view of the network space, including the different types of networks that are in it and its unused address space. IP addresses that belong to a network are blocked off. Each color-coded block represents a network container, a leaf network, or a block of networks that are too small to be displayed individually in the map. For example, in a /8 or /16 network, networks smaller than /20 or /28 respectively and that are beside each other are represented as a multiple network block. In addition, the fill pattern of the blocks indicates their utilization. Therefore, you can quickly evaluate how many and what type of networks are in a network container, their relative sizes, utilization, and how much space you have left.

As you mouse over areas of the map, it displays IP information about the area. Net Map also has a zoom feature that allows you to enlarge or reduce your view of a particular area.

Figure 31.6 displays the network map of a 20.0.0.0/8 network, which is a network container that has network containers and leaf networks.

Figure 31.6 20.0.0.0/8 Network Map
Displaying IP Information

As shown in Figure 31.6, as you mouse over the map, Net Map displays IP information about the area. When you mouse over an unused area, Net Map displays the following information:

- The start and end IP address
- The number of IP addresses that can fit in that space
- The largest possible network
- The number of /16 and /24 networks that can fit in that space

When you mouse over a network, Net Map displays the following information:

- Network address and netmask
- Utilization of the network. For a leaf network, Net Map reports the percentage of used IP addresses, except the broadcast and network addresses. For a network container, Net Map reports the percentage of the IP address space that has been allocated to either network containers or leaf networks.
- The first and last IP address of the network
- The total number of IP addresses in the network

When you mouse over a block of multiple networks, Net Map displays the following information:

- The start and end IP address of that block of networks
- The total number of IP addresses in that block of networks
- The number of networks in that block

Zooming In and Out

Use the zoom function to enlarge and reduce your view of a selected area. You can zoom in on any area in your network. You can zoom in on an area until it displays 128 addresses per row, for a total of 1024 addresses for the map. When you reach the last possible zoom level, the Zoom In icon in the Net Map task bar and the menu item are disabled.

After you zoom in on an area, you can click the Zoom Controller icon to track where you zoomed in. The Zoom Controller lists all the areas that you zoomed in and updates its list dynamically. You can click an item on the list to view that area again. Click the Zoom Controller again to close it.

To select an area and zoom in:

1. Right-click and select **Zoom In**, or click the Zoom In icon in the Net Map task bar.
   The pointer changes to the zoom in selector.
2. Select a starting point and drag to the end point. The starting point can be anywhere in the map. It does not have to be at the beginning of a network.
   Net Map displays a magnified view of the selected area after you release the mouse button. As you mouse over the zoomed in area, Net Map displays IP information about it.
3. You can do the following:
   - Select an area and zoom in again.
   - Add a network. If you zoom in on an area and click Add without selecting an open area first, Net Map selects the area where it can create the biggest possible network in that magnified area.
   - Select a network and perform any of the following operations:
     - Split the network.
     - Join it to another network.
     - Resize the network.
     - Edit its properties.
     - Open it to display its network or IP map.
   - Right-click and select **Zoom Out**, or click the Zoom Out icon in the Net Map task bar. Each time you click **Zoom Out**, Net Map zooms out one level and the Zoom Controller is updated accordingly.
Net Map Tasks
From Net Map, you can create IPv4 networks, and evaluate and manage your network resources according to the needs of your organization. You can do the following:

- Zoom in on specific areas, as described in Zooming In and Out on page 819.
- 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 821.
- Select a network and edit its properties, as described in Modifying IPv4 and IPv6 Network Containers and Networks on page 816.
- Split a network, as described in Splitting IPv4 Networks into Subnets on page 822.
- Join networks, as described in Joining IPv4 Networks on page 823.
- Resize a network, as described in Resizing IPv4 Networks on page 822.
- Delete one or multiple networks, as described in Deleting Networks on page 824.
- Switch to the List view of the network. For information, see Network List on page 821.
  - 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 643.) You cannot change the network address and netmask.
6. Save the configuration and click Restart if it displays at the top of the screen.
Managing IPv4 Networks

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 panel shows all the networks of a selected network view in table format. A network list displays only the first-level subnets. It does not show further descendant or child subnets. You can open a subnet to view its child subnets. Subnets that contain child subnets are displayed as network containers. If the number of subnets in a network exceeds the maximum page size of the table, the network list displays the subnets on multiple pages. You can use the page navigation buttons at the bottom of the table to navigate through the pages of subnets.

The IPAM home panel displays the following:

- **Network**: The network address.
- **Comment**: Information you entered about the network.
- **IPAM Utilization**: For a network, this is the percentage based on the IP addresses in use divided by the total addresses in the network. 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 sort the list of subnets in ascending or descending order by columns. For information about customizing tables in Grid Manager, see [Customizing Tables](#) on page 50.

You can also modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see [Modifying Data in Tables](#) on page 52.
Tip: If you select a network from the list and switch to the Net Map panel, the network is also selected in the network map.

Filtering the Network List
You can filter the network list, so it displays only the networks you need. You can filter the list based on certain parameters, such as network addresses, comments and extensible attributes. When you expand the list of available fields you can use for the filter, note that the extensible attributes are those with a gray background.

Resizing IPv4 Networks
You can resize a network to increase or decrease the network size and the number of IP addresses in the network. When you resize a network to a smaller netmask, you increase the number of IP addresses within that network. You can change the size of an IPv4 network when the operation does not affect existing objects in the network. You can resize an existing network only if the resized network does not exceed the upper network limit or create orphan objects, such as hosts and DHCP ranges. When a network has a parent network or subnets, the upper limit of the network size is marked in red in the resize network slider, and you cannot resize beyond this limit. For example, if a network has a /16 parent network, you cannot resize the network to a network that is larger than /16.

To resize a network:
1. From the Net Map or List panel, select a network, and then click *Resize* from the Toolbar.
2. In the *Resize Network* editor, do the following:
   - **Address**: Displays the network address. You cannot modify this field.
   - **Netmask**: Displays the netmask of the network as you resize the network. You cannot modify this field.
   - **Resize slider**: Use the resize network slider to specify the appropriate subnet masks for the subnets. When you move the slider, Grid Manager displays the number of subnets and IP addresses within that subnet.
   - **Automatically create reverse-mapping zone**: This is enabled only when you resize a /8, /16, or /24 network. Select this check box to have the appliance automatically create reverse-mapping zones for the subnet. The appliance automatically creates reverse-mapping zones only for /8, /16, and /24 netmasks.
3. Click *OK*.

Splitting IPv4 Networks into Subnets
You can create smaller subnets simultaneously within a network by splitting it. You do not have to configure each subnet individually. You can create smaller subnets with larger netmasks. A larger netmask defines more networks with a smaller number of IP addresses.

These subnets inherit the address properties of the parent network, such as member assignments. The exceptions are the default router and broadcast address configuration. The default router and broadcast address configuration for address ranges and fixed address are disabled by default after splitting a network. You can enable these properties for each subnet after splitting the parent network.

Note that you cannot split a network that is part of a shared network.

To split a network:
1. From the Net Map or List panel, select 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.
Managing IPv4 Networks

1. 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. This 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**.
Deleting Networks

From the IPAM tab, you can delete multiple IPv4 and IPv6 networks. When you delete a network, all of its data, including all of its DHCP records, subnets, and records in its subnets, is deleted from the database and goes to the Recycle Bin, if enabled. Because of the potentially large loss of data that can occur when you delete a network, Grid Manager requires a confirmation to move the data to the Recycle Bin.

To delete IPv4 or IPv6 networks:

1. From the Data Management tab, select the IPAM tab -> network check box. You can select multiple check boxes for multiple networks.
2. Select Delete or Schedule Delete from the Delete drop-down menu.
3. To delete the network now, in the Delete Confirmation dialog box, click Yes. To schedule a deletion, see Scheduling Tasks on page 256.

The appliance puts the deleted network in the Recycle Bin, if enabled.
Viewing and Managing IPv4 Addresses

You can view and manage IPv4 address data in the IP Map and IP List panels. Grid Manager displays the IP Map and List panels for a specific network after you navigate through the network hierarchy, or when the selected network does not have subnets under it.

IP Map

The IPv4 Map panel provides a graphical representation of all IPv4 addresses in a given subnet. IP Map displays cells that represent IPv4 addresses. Each cell in the map represents an IPv4 address, and its color indicates its status as described in the legend section. You can run a network discovery on the selected network, and the status of each IP address is updated accordingly. For information, see Chapter 32, Network Discovery, on page 843.

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.
- **Reserved Range**: A range of IP addresses that are reserved for statically configured hosts. They are not served as dynamic addresses. You can allocate the next available IP from the reserved range when you create a static host.

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 do the following in the IP Map panel:

- Click **Go to DHCP View** to view DHCP properties of a selected network.
- Select an address range by clicking once on a start address and then use SHIFT+click on the end address. Click Add - >Range from the Toolbar to add the selected range as an IPv4 or IPv6 DHCP range or reserved range.
- Click the Resolve Conflict icon to resolve IP address conflicts. For information, see Resolving Conflicting Addresses on page 861.
• Click the Ping icon to ping a selected IP address. For information, see Pinging IP Addresses on page 841.
• Click the Reclaim icon to reclaim an IP address. For information, see Reclaiming Objects Associated with IPv4 and IPv6 Addresses on page 841.
• Click the Clear icon to clear an active lease. For information, see Clearing Active DHCP Leases on page 841.

You can also select an IP address from the IP Map panel and view the following information:
• General information, as described in IP Address Header Panel on page 828.
• Data retrieved through a network discovery or integrated from a PortIQ appliance and Trinzic NetMRI. For information, see Viewing Discovered Data on page 858.
• The records associated with the IP address, as described in Related Objects on page 837.
• The audit history, as described in Audit History on page 837.
• Detailed lease information, as described in Viewing Detailed Lease Information on page 748.
• Click DHCP View to view DHCP properties of the selected network. For information, see Modifying IPv4 Networks on page 646.
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 an DHCP address 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 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 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 timestamp when the IP address was last discovered. This data is read-only.
- **OS**: The operating system of the discovered host. The OS value can be one of the following:
  - *Microsoft* for all discovered hosts that have a non-null value in the MAC addresses using the NetBIOS discovery method.
  - A value that a TCP discovery returns.
  - The OS of a virtual entity on a vSphere server.
  
  Note that this field sometimes displays the percentage of certainty about the discovered OS.
- **NetBIOS Name**: The returned NetBIOS name from the last discovery.
- **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 or Trinzic NetMRI appliances. For information about the PortIQ data, see *Integrating Data from PortIQ Appliances* on page 856. For information about integrating discovered data from Trinzic NetMRI, see *Integrating Discovered Data From Trinzic NetMRI* on page 857.

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 828.
- Data retrieved through a network discovery or integrated from a PortIQ appliance, as described in *Viewing Discovered Data* on page 858.
- The records associated with the IP address, as described in *Related Objects* on page 837.
- Audit history, as described in *Audit History* on page 837.
- Detailed lease information, as described in *Viewing Detailed Lease Information* on page 748.

You can also do the following from the IP List panel:
• Click **Go to DHCP View** to view DHCP properties of a selected network. For information, see *Modifying IPv4 Networks* on page 646.

• Click the Ping icon to ping a selected IP address. For information, see *Pinging IP Addresses* on page 841.

### Filtering the IP Address List

You can filter the IP address list, so it displays only the IP addresses you need. You can filter the list based on any combination of extensible attributes and the parameters displayed in the IP address list, such as usage and type. When you expand the list of available fields you can add to the filter, note that the extensible attributes are those with the gray background.

### IP Address Header Panel

When you select an IP address from the IP Map or List panel, Grid Manager displays information about the highest priority object associated with the IP address. Depending on the object type, Grid Manager displays all or some of the following information. For example, if the highest priority object is a fixed address, Grid Manager displays only the object type, MAC address, lease state, and comment of the object.

- **Type**: The object or record type, such as A record, PTR record, or host record.
- **Name**: The name of the object. For example, if the IP address belongs to a host record, this field displays the hostname. The appliance highlights disabled DHCP objects in gray. A DHCP object can be a DHCP address range, fixed address, reservation, host configured for DHCP, or roaming host with an allocated IP address.
- **MAC**: The MAC address of the network device associated with the IP address.
- **Lease State**: The current status of the DHCP lease.
- **Comment**: Comments about the IP address.

### Discovered Data

The **Discovered Data** tab displays discovered data through a network discovery or integrated from PortIQ and Trinzic NetMRI appliances. For information about viewing discovered data, see *Viewing Discovered Data* on page 858.

### Related Objects

The Related Objects tab displays the following information about the records associated with the IP address:

- **Name**: The name of the object. For example, if the IP address belongs to a host record, this field displays the hostname. The appliance highlights disabled DHCP objects in gray. A DHCP object can be a DHCP range, fixed address, reservation, host configured for DHCP, or roaming host with an allocated IP address.
- **Type**: The object type, such as DHCP lease, host, A record, and bulk host.
- **Comment**: Information about the object.

You can also select the following for display:

- **DNS view**: The DNS view to which the object belongs.

You can do the following in this tab:

- **Add a resource record.** You can select the following from the drop-down list:
  - Host Record—For information, see *Adding Host Records* on page 813.
  - Range—For information, see *Adding IPv4 Address Ranges* on page 650.
  - Fixed Address—For information, see *Adding IPv4 Fixed Addresses* on page 654.
  - Reservation—For information, see *Adding IPv4 Reservations* on page 656.
  - A Record—For information, see *Adding A Records* on page 414.
  - PTR Record—For information, see *Adding PTR Records* on page 417.

- **Edit the properties of the selected object.** Depending on the type of object, Grid Manager displays the corresponding editor for the object. For example, if the selected object is a fixed address, Grid Manager displays the fixed address editor. When you select a lease object, Grid Manager displays the lease viewer.
• You can also modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables on page 52. 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 748.
• 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.

Managing IPv4 Addresses
You can do the following from the IP Map and List panels:
• Add IP addresses to existing hosts. For information, see Adding IP Addresses to Existing Host Records on page 829.
• Clean unmanaged IP addresses. For information, see Clearing Unmanaged Data on page 830.
• Convert objects to other object types. For information, see Converting Objects Associated with IP Addresses on page 838.
• Reclaim IP addresses. For information, see Reclaiming Objects Associated with IPv4 and IPv6 Addresses on page 841.
• Ping IP addresses. For information, see Pinging IP Addresses on page 841.
• Configure and run a network discovery. For information, see Network Discovery on page 843.
• Resolve discovery conflicts. For information, see Resolving Conflicting Addresses on page 861.
• Clear discovered data. For information, see Clearing Discovered Data on page 863.

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 57 and Using the Go To Function on page 61.
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 814.
4. Save the configuration and click Restart if it displays at the top of the screen.
   To close the editor without saving the changes, click the Close icon.

Clearing Unmanaged Data

You can clear the status of unmanaged data at the network and IP address levels. When you clear an unmanaged address, the status of the IP address changes to Unused. An unmanaged address is an IP address with a discovered host, is not previously known to the appliance, and does not have an A record, PTR record, fixed address, host address, lease, or is not within a DHCP range. You can change an unmanaged address to a host, a DHCP fixed address, an A record, or a PTR record. You can also clear the unmanaged data associated with the address.

To clear unmanaged data:
1. From the IP Map or List panel, select the IP address for which you want to clear unmanaged data, and then click Clear -> Clear Unmanaged Data from the Toolbar. You can select multiple IP addresses.
2. In the Clear Unmanaged data dialog box, click Yes.
Managing IPv6 Networks

In Grid Manager, you can use the IPv6 Net Map (network map) and List panels to manage your IPv6 network infrastructure. After you select a network container from the IPAM tab, Grid Manager displays it in the Net Map panel, by default. The Net Map panel provides a graphical view of your networks and has a number of features that simplify network management. The List panel displays the networks in table format.

You can always switch your view of a network container between the Net Map and List panels. Grid Manager keeps track of which panel you last 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 IPv4 Network Map on page 818 and Network List on page 821.

You can use Grid Manager to manage IPv6 networks and their AAAA, PTR and host resource records. You can configure IPv6 networks and track IP address usage in those networks. You can also split and join IPv6 networks, when necessary.
IPv6 Network Map

After you select an IPv6 network container from the IPAM tab, Grid Manager displays it in the IPv6 Net Map (network map) panel, by default. Just like the IPv4 Net Map, the IPv6 Net Map provides a high-level view of the network address space. You can use Net Map to design and plan your network infrastructure, and to configure and manage individual networks.

The Net Map panel presents a complete view of the network space, including the different types of networks that are in it and its unused address space. IP addresses that belong to a network are blocked off. Each color-coded block represents a network container, a leaf network, or a block of networks that are too small to be displayed individually in the map. For example, in an /64 or /96 network, networks smaller than /76 or /108 respectively and that are beside each other are represented as a multiple network block. In addition, the fill pattern of the blocks indicates their utilization. Therefore, you can quickly evaluate how many networks are in a network container, their relative sizes, utilization, and how much space you have left.

As you mouse over areas of the map, it displays IP information about the area. Net Map also has a zoom feature that allows you to enlarge or reduce your view of a particular area.

Figure 31.7 displays the network map of a 1111::/16 network, which is a network container that has network containers and leaf networks.

Figure 31.7 IPv6 Network Map
Displaying Network Information

As shown in Figure 31.7, as you mouse over the map, Net Map displays IP information about the area. When you mouse over an unused area, Net Map displays the following information:

- The start and end IP address
- The largest possible network
- The number of /64 networks that can fit in that space

When you mouse over a network container, Net Map displays the following information:

- Network address and netmask
- The first and last IP address of the network
- The number of networks in that block
- IPAM utilization

When you mouse over a network, Net Map displays the following information:

- Network address and netmask
- The first and last IP address of the network

When you mouse over a block of multiple networks, Net Map displays the following information:

- The start and end IP address of that block of networks
- The number of networks in that block

Zooming In and Out

Use the zoom function to enlarge and reduce your view of a selected area. You can zoom in on any area in your network. You can zoom in on an area until it displays 128 addresses per row, for a total of 1024 addresses for the map. When you reach the last possible zoom level, the Zoom In icon in the Net Map task bar and the menu item are disabled.

After you zoom in on an area, you can click the Zoom Controller icon to track where you zoomed in. The Zoom Controller lists all the areas that you zoomed in and updates its list dynamically. You can click an item on the list to view that area again. Click the Zoom Controller again to close it.

To select an area and zoom in:

1. Right-click and select **Zoom In**, or click the Zoom In icon in the Net Map task bar.
   The pointer changes to the zoom in selector.

2. Select a starting point and drag to the end point. The starting point can be anywhere in the map. It does not have to be at the beginning of a network.
   Net Map displays a magnified view of the selected area after you release the mouse button. As you mouse over the zoomed in area, Net Map displays IP information about it.

3. You can do the following:
   - Select an area and zoom in again.
   - Add a network. If you zoom in on an area and click Add without selecting an open area first, Net Map selects the area where it can create the biggest possible network in that magnified area.
   - Select a network and perform any of the following operations:
     - Edit its properties.
     - Open it to display its IP List.
     - Delete it immediately, or schedule its deletion.
   - Right-click and select **Zoom Out**, or click the Zoom Out icon in the Net Map task bar. Each time you click **Zoom Out**, Net Map zooms out one level and the Zoom Controller is updated accordingly.
Net Map Tasks

From Net Map, you can create IPv6 networks, and evaluate and manage your network resources according to the needs of your organization. You can do the following:

- Zoom in on specific areas, as described in Zooming In and Out on page 819.
- Use the Go to function to find a network in the current zoom level of Net Map.
- Add a network, as described in Adding a Network from Net Map.
- Select a network and view IP address list, as described in Viewing IPv6 Data on page 837.
- Select a network and edit its properties, as described in Modifying IPv4 and IPv6 Network Containers and Networks on page 816.
- Split a network, as described in Splitting IPv6 Networks into Subnets on page 836.
- Join networks, as described in Joining IPv6 Networks on page 836.
- Delete one or multiple networks, as described in Deleting Networks on page 824.
- Switch to the List view of the network. For information, see IPv6 Network List on page 835.
  - When you select one or more networks in Net Map and then switch to the List view, the list displays the page with the first selected network.
  - If you select one or more networks in the List view and then switch to the Net Map view, the first network is also selected in Net Map. Although, if you select a network in the List view that is part of a Multiple Networks block in Net Map, it is not selected when you switch to the Net Map view.

Adding a Network from Net Map

When you create networks from Net Map, you can view the address space to which you are adding a network, so you can determine how much space is available and which IP addresses are not in use. When you mouse over an open area, Net Map displays useful information, such as the largest possible network that fits in that area. In addition, you can create networks without having to calculate anything. When you add a network, Net Map displays a netmask slider so you can determine the appropriate netmask for the size of the network that you need. As you move the slider, it displays network information, including the total number of addresses. After you select the netmask, you can even move the new network around the open area to select another valid start address.

To add a network from the Net Map panel:

1. Do one of the following:
   - Click the Add icon.
     Net Map displays the netmask slider and outlines the open area that can accommodate the largest network.
   - Select an open area, and then click the Add icon.
     Net Map displays the netmask slider and outlines the largest network that you can create in the open area that you selected.

2. Move the slider to the desired netmask. You can move the slider to the netmask of the largest network that can be created in the open area. You can also move the slider to the smallest network that can be placed in the current zoom level of Net Map.

   As you move the slider, Net Map displays the netmask. The outline in the network map also adjusts as you move the slider. When you mouse over the outline, it displays the start and end address of the network.

3. After you set the slider to the desired netmask, you can drag the new network block around the open area to select a new valid starting address. You cannot move the block to a starting address that is invalid.

4. Click Launch Wizard to create the network.
   The Add Network wizard displays the selected network address and netmask.

5. You can add comments, automatically create reverse mapping zones, and edit the extensible attributes. (For information, see Adding IPv6 Networks on page 735.)

6. Save the configuration and click Restart if it displays at the top of the screen.

   Grid Manager updates Net Map with the newly created network.
Viewing Network Details

From Net Map, you can focus on a specific network or area and view additional information about it. If you have a network hierarchy of networks within network containers, you can drill down to individual leaf networks and view their IP address usage.

1. Select a network or area.
2. Click the Open icon.
   - If you selected a network container, Grid Manager displays it in the Net Map panel. You can drill down further by selecting a network or open area and clicking the Open icon again.
   - If you selected a block of multiple networks, Grid Manager displays the individual networks in the Net Map panel. You can then select a network or open area for viewing.
   - If you selected a leaf network, Grid Manager displays it in the Network List panel.
   - If you selected an open area, Grid Manager displays an enlarged view of that area in the Net Map panel. This is useful when you are creating small networks in an open area.

IPv6 Network List

The Network list panel is an alternative view of an IPv6 network hierarchy. For a given network, the panel shows all the networks of a selected network view in table format. A network list displays only the first-level subnets. It does not show further descendant or child subnets. You can open a subnet to view its child subnets. Subnets that contain child subnets are displayed as network containers. If the number of subnets in a network exceeds the maximum page size of the table, the network list displays the subnets on multiple pages. You can use the page navigation buttons at the bottom of the table to navigate through the pages of subnets.

The IPAM home panel displays the following:

- **Network**: The network address.
- **Comment**: Information you entered about the network.
- **IPAM Utilization**: For a network, this is the percentage based on the IP addresses in use divided by the total addresses in the network. You can use this information to verify if there is a sufficient number of available addresses in a network. The IPAM utilization is calculated approximately every 15 minutes.
- **Site**: The site to which the IP address belongs. This is a predefined extensible attribute.

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 sort the list of subnets in ascending or descending order by columns. For information about customizing tables in Grid Manager, see *Customizing Tables* on page 50.

You can also modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see *Modifying Data in Tables* on page 52.

**Tip**: If you select a network from the list and switch to the Net Map panel, the network is also selected in the network map.

Filtering the Network List

You can filter the network list, so it displays only the networks you need. You can filter the list based on certain parameters, such as network addresses, comments and extensible attributes. When you expand the list of available fields you can use for the filter, note that the extensible attributes are those with a gray background.
Splitting IPv6 Networks into Subnets

You can create smaller subnets simultaneously within a network by splitting it. You do not have to configure each subnet individually. You can create smaller subnets with larger netmasks. A larger netmask defines a larger number of network addresses and a smaller number of IP addresses.

Note that you cannot split a network that is part of a shared network.

To split an IPv6 network:

1. From the Data Management tab, select the IPAM tab -> network check box, and then click Split from the Toolbar.
2. In the Split Network editor, do the following:
   - **Address**: Displays the network address. You cannot modify this field.
   - **Netmask**: Specify the appropriate netmask for each subnet.
   - **IPv6 Prefix Collector Network**: If you split a network with prefix delegations that are not tied to specific addresses, specify the network in which all prefix delegations are assigned. If you leave this field blank, the server assigns all prefix delegations that are not tied to specific addresses to the first network.
   - **Immediately create**: Select one of the following
     - **Only networks with ranges and fixed addresses**: Adds only the networks that have DHCP ranges and fixed addresses.
     - **All possible networks**: Adds all networks that are within the selected netmasks. You can select this option only when you increase the CIDR by 8 bits.
     - **Automatically create reverse-mapping zone**: Select this check box to have the appliance automatically create reverse-mapping zones for the subnets. This function is enabled if the netmask of the network is a multiple of four, such as 4, 12 or 16.
3. Click OK.

Joining IPv6 Networks

Joining multiple networks into a larger network is the opposite of splitting a network. You can select a network and expand it into a larger network with a smaller netmask. A smaller netmask defines fewer networks while accommodating a larger number of IP addresses. Joining or expanding a network allows you to consolidate all of the adjacent networks into the expanded network. Adjacent networks are all networks that fall under the netmask of the newly-expanded network.

To join or expand a network:

1. From the Data Management tab, select the IPAM tab -> network check box, and then click Join from the Toolbar.
2. In the Join Network editor, do the following:
   - **Address**: Displays the network address. You cannot modify this field.
   - **Netmask**: Enter the netmask of the expanded network.
   - **Automatically create reverse-mapping zone**: Select this check box to configure the expanded network to support reverse-mapping zones. The appliance automatically creates reverse-mapping zones only if the netmask is between /4 through /128, in increments of 4 (that is, /4, /8, /12, and so on until /128).
3. Click OK.
Viewing IPv6 Data

To the configured IP addresses in an IPv6 network:

by selecting an IPv6 leaf network from the Network List panel

- For a leaf network that is not in a network container, from the Data Management tab, select the IPAM tab, and then click the IPv6 network you want to view.
- For a leaf network that is in a network container, from the Data Management tab, select the IPAM tab -> network_container -> network.

Grid Manager lists the configured IPv6 addresses. You can export and print the list. It displays the following information about each IP address:

- **IP Address**: The name of the IPv6 DHCP object, which can be a DHCP range, fixed address, host configured for DHCP, or a roaming host with an allocated IP address.
- **Name**: The name of the record associated with the IP address.
- **DUID**: The DHCP Unique Identifier (DUID) of the device that was assigned the IP address.
- **Status**: The status of the IPv6 object, such as Used or Unused.
- **Type**: The object type associated with the IP address, such as AAAA record, IPv6 Fixed Address, or Unmanaged.
- **Usage**: Indicates whether the IPv6 address is configured for DNS or DHCP.
- **Lease State**: The lease state of the record, such as Active.
- **Comment**: Displays comments about the record.

You can display all available extensible attributes. You can also sort the list of IP addresses in ascending or descending order by IP Address only.

You can drill down further and view the records associated with an IP address. To view the associated records of an IP address, select it and Grid Manager displays information about the IP address in the Related Objects and Audit History tabs.

**Related Objects**

Grid Manager displays the following information about the records associated with the IP address:

- **Name**: The record name. For example, if the IP address belongs to a host record, this field displays the hostname.
- **Type**: The object type. For example, AAAA Record, PTR Record, Host Record, IPv6 Fixed Address.
- **Comment**: Additional information that was entered in the record about the IP address.

**Audit History**

Grid Manager displays the following information about the last five actions performed on the selected IP:

- **Timestamp**: The day, date, and time of the operation.
- **Action**: The type of operation that was performed by the administrator.
- **Object Type**: The object type of the entry.
- **Admin Name**: The name of the administrator that performed the operation.
- **Message**: Description of the administrative activity.

**Filtering the IP Address List**

You can filter the IP address list, so it displays only the IP 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.
Managing IPv4 and IPv6 Addresses

Grid Manager uses IP addresses as the entry point to the data set containing Infoblox host, DNS, DHCP, and other information related to that address. You can view the data, modify it, assign extensible attributes to the objects associated with the address, and convert DHCP lease types, such as changing a currently active dynamic lease to a fixed address or host record.

You can view and manage IPv4 address data in the IP Map panel, and view and manage IPv4 and IPv6 data in the IP List panel. You can do the following for IPv4 and IPv6 data from the IP List panel:

- Convert objects to other object types. For information, see Converting Objects Associated with IP Addresses on page 838.
- Reclaim IP addresses. For information, see Reclaiming Objects Associated with IPv4 and IPv6 Addresses on page 841.
- Ping IP addresses. For information, see Pinging IP Addresses on page 841.
- Clear DHCP leases. For information, see Clearing Active DHCP Leases on page 841.

You can also print and export in CSV format the information displayed in any panel that supports these functions.

Converting Objects Associated with IP Addresses

The NIOS appliance provides a simple mechanism for converting unmanaged IP addresses to resource records, such as host records and A or AAAA records. You can also convert the active lease of a dynamically assigned IPv4 or IPv6 address to a fixed address or host, and convert an IPv4 lease to an IPv4 reservation. Using the conversion mechanism, you can keep the existing information of a network device during the conversion.

The appliance supports the following conversions for IPv4 objects:

- DHCP leases to fixed addresses, reservations, or host records
- Fixed addresses to reservations or host records
- Unmanaged addresses to host records, A records, PTR records, or fixed addresses
- A records to host records
- PTR records to host records

The appliance supports the following conversions for IPv6 objects:

- DHCP leases to fixed addresses or host records
- Fixed addresses to host records
- AAAA records to host records
- IPv6 PTR records to host records

Note: You cannot convert unmanaged IP addresses or leases served by Microsoft DHCP servers to host records.

Converting DHCP Leases

To create a fixed address, you bind an IPv4 address to a MAC address or an IPv6 address to a DUID. You can make that binding by converting an active dynamically leased address to a fixed address. The lease conversion transforms the temporary binding between the IPv4 address and MAC address or the IPv6 address and DUID in the dynamic lease to a persistent one. The lease must be active so that the NIOS appliance has an IPv4-to-MAC address or IPv6-to-DUID binding to convert into a fixed address.

The appliance uses the following rules when converting a DHCP lease:

- If an IPv4 DHCP lease is converted to a fixed address, the appliance copies the client identifier to the fixed address, based on information in the lease. If the appliance finds the client identifier in the lease information, the appliance includes it when it creates the host. If it finds the MAC address, the appliance includes it when it creates the host. If it finds both, the appliance includes only the MAC address (default) when it creates the host.
- If an IPv6 DHCP lease is converted to a fixed address, the appliance copies the DUID to the fixed address.
• If you try to convert an IPv4 DHCP lease or a fixed address with a client identifier, not a MAC address, to a host, the appliance displays an error message in the host editor. This ensures that you do not attempt this operation and lose the data.

• You cannot create two IPv4 fixed addresses with the same client identifier or MAC address in the same network. You cannot create two IPv6 fixed addresses with the same DUID in the same network.

• If the appliance receives a second IPv4 DHCP request with the same client identifier, it provides the same fixed IP address if the lease is still binding.

*Figure 31.8* illustrates converting a dynamic IPv4 lease to a fixed lease.

*Figure 31.8*  *Converting a Dynamic IPv4 Lease to a Fixed Lease*

---

An advantage of converting an active dynamic lease is that you do not need to learn the MAC address or DUID of the device to which you want to assign an IP address and manually enter it in the fixed address configuration.

An IPv4 reservation is an address that you exclude from DHCP use because you intend to configure that address manually on a device, such as a firewall, router, or printer. You can also convert an IPv4 fixed address or a dynamic address with an active lease to a reservation.

When you convert an address in a DHCP range to a reservation, you reduce the total number of dynamically assignable addresses in that range by one. Correspondingly, this reduces the number of allocated addresses needed to exceed a high or low watermark threshold for that range.

**Note:** To return an IP address to its place in a DHCP range after converting it from an active dynamic lease to a fixed address, reservation, or Infoblox host, delete the fixed address, reservation, or host to which you previously converted the IP address. The IP address then becomes part of the DHCP range to which it first belonged.
You can convert IPv4 fixed addresses to reservations, as shown in Figure 31.9.

**Figure 31.9 Converting an IPv4 Dynamic Lease or Fixed Address to a Reservation**

To convert an object:
1. From the IP Map, select an IPv4 address or from the IP List panel, select an IPv4 or IPv6 address.
2. In the Related Objects tab, select the check box of the object, and then click **Convert** from the Toolbar or navigation bar.
3. Select the object type to which you want to convert the object. Grid Manager displays the corresponding editor for the object type.
4. For all IPv4 conversions, Grid Manager populates the discovered information in the corresponding editor. Depending on the type of conversion, do one of the following:
   - For host record conversions, see **Modifying Host Records** on page 814.
   - For IPv4 reservation conversions, see **Modifying Reservations** on page 657.
   - For fixed address conversions, see **Modifying IPv4 Fixed Addresses** on page 655.
   - For A record conversions, see **Modifying A Records** on page 415.
   - For PTR record conversions, see **Modifying PTR Records** on page 417.

**Note:** When you select an object for conversion, Grid Manager displays only the available conversion types for the object. You must save the changes in the editor for the conversion to take place.
Reclaiming Objects Associated with IPv4 and IPv6 Addresses

You can use the reclaim IP function to delete all objects, except the active DHCP lease, that are associated with a selected IP address. To delete a DHCP lease, use the clear lease function as described in Clearing Active DHCP Leases. When you reclaim an IP address, Grid Manager deletes the associated objects and puts them in the Recycle Bin, if enabled. You can reclaim any used and unmanaged IP addresses. You can also select multiple IP addresses for this function. After you reclaim an IP address, the address status changes to Unused. You can then 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 IPv4 or IPv6 address:

• From the IP Map or IP List panel, select the IP address that you want to ping, and then click Ping from the Toolbar.

To ping all IPv4 addresses:

• From the IP Map panel, click Multi-ping from the Toolbar. Grid Manager pings all IP addresses displayed in the IP Map panel and displays the ping status in the panel.

When the ping or multi-ping is complete, the status bar displays the number of active IP addresses detected through the ping. To close the ping status bar, click the Close icon.

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.
Chapter 32 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 discovered data from Infoblox PortIQ and Trinzic NetMRI appliances. This chapter includes the following sections:

- **About Network Discovery** on page 844
  - Administrative Permissions on page 845
  - IP Discovery Process on page 846
  - Supported IP Discovery Methods on page 847
  - VM Discovery Process on page 849
- **About Configuring a Discovery** on page 850
  - Considerations Before Starting a Discovery on page 851
  - Selecting a Grid Member on page 852
  - Enabling or Disabling the Merging of Discovered Data on page 852
  - Updating Discovered Data for Managed Objects on page 853
  - Configuring IP Discovery on page 853
  - Configuring VM Discovery on page 854
  - Starting a Discovery on page 855
  - Scheduling a Discovery on page 855
  - Managing a Discovery on page 855
  - Monitoring Discovery Status on page 855
- **Integrating Data from PortIQ Appliances** on page 856
- **Integrating Discovered Data From Trinzic NetMRI** on page 857
- **Viewing Discovered Data** on page 858
- **Managing Discovered Data** on page 859
  - Managing Unmanaged Data on page 859
  - Resolving Conflicting Addresses on page 861
  - Clearing Discovered Data on page 863
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 847.

- **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 849.

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 851.

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 850.

After a discovery is complete, you can view and manage the discovered data. For information, see *Viewing Discovered Data* on page 858 and *Managing Discovered Data* on page 859. 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 102. The appliance records all discovery operations in the audit log.
**About Network Discovery**

*Figure 32.1* shows a high-level perspective of the discovery process.

**Figure 32.1 High-Level Discovery Process**

1. A user configures a discovery.
2. The Grid Master sends a discovery request to the Grid member that runs the discovery.
3. The Grid member scans the network and the vSphere servers.
4. In the IP discovery, active hosts respond to the discovery. In the VM discovery, information about virtual entities is retrieved.
5. The Grid member returns information about detected active hosts and virtual entities.
6. The Grid Master updates the database with discovered data.

**Administrative Permissions**

You can initiate a discovery and manage discovered data based on your administrative permissions. For information, see *Managing Administrators* on page 109.

You must have read/write permission to discover 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 855.

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 32.2 illustrates how an IP discovery works.

*Figure 32.2 IP Discovery Process*

The Grid member scans networks using a splitting mechanism. Each IP chunk in a network contains 64 contiguous IP addresses. The Grid member reports the discovery status and discovered data. Grid Manager displays the discovery status in the Discovery Manager widget and updates the database with the discovered data.

The Grid member probes each IP address in each chunk, reports the detected information, updates the progress report, and then moves on to the next chunk until it hits the last IP chunk in the last discovered network.
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 on page 848.
- Full—For information, see Full on page 848.

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</td>
<td>NetBIOS query and reply</td>
</tr>
<tr>
<td></td>
<td>• MAC address</td>
<td>non-Microsoft networks that run some NetBIOS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OS</td>
<td>services</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</td>
<td>The appliance communicates with the vSphere servers to collect discovered</td>
</tr>
<tr>
<td></td>
<td>• MAC address</td>
<td>VM discovery</td>
<td>data</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>
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 852.
- 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 852.
- Configure an IP discovery. For information, see Updating Discovered Data for Managed Objects on page 853. You must first define the networks on which you want to run an IP discovery. For information, see Configuring DHCP for IPv4 on page 641.
- Add the vSphere servers on which you want to run a VM discovery. For information, see Configuring VM Discovery on page 854.

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 855 and Scheduling a Discovery on page 855. After you start a discovery, you can pause or stop it. For information, see Managing a Discovery on page 855. 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 Dashboards on page 69.
- View the discovered data. For information, see Viewing Discovered Data on page 858.
- Manage the discovered data. For information, see Managing Discovered Data on page 859.
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 861.
  - 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 57 and Using the Go To Function on page 61.

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 853.
• Configure a VM discovery, as described in Configuring VM Discovery on page 854.

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 853.
• Configure a VM discovery, as described in Configuring VM Discovery on page 854.
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 854.

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 847. 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 57 and Using the Go To Function on page 61.

   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 848.
   — 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 855. You can also schedule the discovery to run at a later date, as described in *Scheduling a Discovery* on page 855.

### 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 855. You can also schedule the discovery to run at a later date, as described in *Scheduling a Discovery* on page 855.
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 63.

**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 94.
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.
- **Attached Device**: Identifies the switch that is 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 Discovered Data on page 858 and Managing Discovered Data on page 859.
   - In the IP List panel, you can add data fields. For information, see Managing Discovered Data on page 859.
Integrating Discovered Data From Trinzic NetMRI

Trinzic NetMRI appliances discover and track IPv4 and IPv6 network devices and provide information about the discovered IP addresses. You can integrate IPv4 and IPv6 discovered data into the NIOS appliance database, and then view the data in the IP List panel of Grid Manager as well as in the Discovered Data tab of certain DNS and DHCP object editors. For information about Trinzic NetMRI network discovery and how to import discovered data from a Trinzic NetMRI appliance to the NIOS appliance, refer to the Trinzic NetMRI Administrator Guide.

Note: The NIOS appliance does not import IPv6 leases that contain prefixes and link-local IPv6 addresses. This data is discarded during an import.

The appliance can import the following IPv4 and IPv6 data that NetMRI discovers:

- **IP Address**: The discovered IPv4 or IPv6 address.
- **Discovered MAC Address**: The MAC address of the discovered host.
- **Last Discovered**: The date and time the IP address was last discovered.
- **NetBIOS Name**: The name returned in the NetBIOS reply or the name you manually register for the discovered host.
- **OS**: The operating system of the detected host.
- **First Discovered**: The date and time the IP address was first discovered.
- **Discoverer**: Specifies whether the IP address was discovered by a NetMRI discovery process.
- **Discovered Name**: The name of the network device associated with the discovered IP address.
- **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 Name**: The name of the switch port connected to the end device.
- **Attached Device Port**: The number of the switch port connected to the end device.
- **Attached Device**: Identifies the switch that is 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 Name**: The name of the VLAN of the switch port.
- **VLAN**: The ID of the VLAN of the switch port.
Viewing Discovered Data

After a discovery or after integrating data from PortIQ and Trinzic NetMRI appliances, you can view the discovered data in the following:

- IP Map panel for IPv4 addresses, as described in IP Map on page 825.
- IP List panel, as described in IP Address List on page 827.
- Discovered Data tab in certain DNS and DHCP object editors, as described below.

To specify the data fields to display in the Discovered Data tab of the IP Map and IP List panels:

1. Expand the Discovered Data tab.
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.

The Discovered Data section displays the fields you specified. A discovery creates only Unmanaged and Conflict data. Depending on the source of the discovered data, when you modify certain DNS and DHCP objects, Grid Manager can display the following IPv4 and IPv6 discovered data (if any) in the Discovered Data tab:

- **NetBIOS Name**: The name returned in the NetBIOS reply or the name you manually register for the discovered host.
- **OS**: The operating system of the detected host 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.
- **Discovered 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.
- **Discovered DUID**: For IPv6 address only. The DHCP unique identifier of the discovered host. This is an optional field, and data might not be included.
- **Last Discovered**: The date and time the IP address was last discovered.
- **First Discovered**: The date and time the IP address was first discovered.
- **Discoverer**: Specifies whether the IP address was discovered by a NetMRI or NIOS discovery process.
- **Discovered Name**: The name of the network device associated with the discovered IP address.

If you imported data from Infoblox PortIQ or Trinzic NetMRI appliances, Grid Manager may display the following information, if available. You can also select all or some of this data for display in the Discovered Data tab of the IP Map and IP List panels. For information about the data imported from PortIQ and Trinzic NetMRI appliances, see Integrating Data from PortIQ Appliances on page 856 and Integrating Discovered Data From Trinzic NetMRI on page 857.

- **Attached Device Description**: A textual description of the switch that is connected to the end device.
- **Attached Device Address**: The IPv4 or IPv6 address of the switch that is connected to the end device.
- **Attached Device Name**: If a reverse lookup was successful for the IP address associated with this switch, the host name is displayed here.
- **Attached Device Port Description**: A textual description of the switch port that is connected to the end device.
- **Attached Device Port Name**: 
- **Attached Device Port**: The number of the switch port connected to the end device.
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 859.
- Resolve conflicting addresses. For information, see Resolving Conflicting Addresses on page 861.
- Clear discovered data. For information, see Clearing Discovered Data on page 863.

Managing Unmanaged Data

You can manage unused and unmanaged addresses by doing one of the following:

- Add to an existing host, as described in Adding to an Existing Host on page 859.
- Convert to a fixed address, host, A record, or PTR record, as described in Converting Unmanaged Data on page 860.
- Clear the unmanaged status, as described in Clearing Unmanaged Data on page 860.

Note: You cannot convert unmanaged IP addresses served by Microsoft DHCP servers to host records.

Adding to an Existing Host

You can add an unmanaged address, including all its information, to an existing host. You can select the desired host to which you want to add the unmanaged address.

To add an unmanaged address to an existing host:

1. From the IP Map or List panel, select an unmanaged address you want to add to a host, and then click Add -> Add to Existing Host from the Toolbar.
2. In the Select Host dialog box, select a host from the table. You can also search for a host using filters or the Go to function. For information, see Using Filters on page 57 and Using the Go To Function on page 61. Click the Select icon to select the desired host.

**Note:** Depending on the page size configuration, the search results are limited to the page size that you set. If the search results exceed the page size limit, the appliance displays an error message to inform you to refine your search criteria or to change the page size limit. In the Host Record editor, complete the information as described in Modifying Host Records on page 814.

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

### 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. For IPv4 addresses, you can select **To Host**, **To A Record**, **To PTR Record**, or **To Fixed Address**. For IPv6 addresses, you can select **To Host**, **To AAAA**, **To PTR Record**, or **To IPv6 Fixed Address**.

   Depending on the record type you select, Grid Manager displays the corresponding editor. It also populates the attributes of the unmanaged address in the editor. Enter the appropriate information in the editor.

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

**Note:** After the conversion, the status of the unmanaged address changes to **Used**.

The following are some conditions for a conversion:

- **A and AAAA records**: You must select a DNS zone when converting an unmanaged address to an A or AAAA record.
- **PTR record**: You must select a DNS zone when converting an unmanaged address to a PTR record.
- **IPv4 and IPv6 Fixed Address**: Grid Manager displays a confirmation dialog box to ensure that you want to create a fixed address for the unmanaged address.
- **IPv4 and IPv6 Host record**: You can use the unmanaged address to enable a host record for DNS or DHCP.

### Clearing Unmanaged Data

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 the click **Clear** -> Clear Unmanaged Data from the Toolbar.

   or

   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.

2. In the Clear Unmanaged Data confirmation dialog box, click **Yes**.

**Note:** When you clear unmanaged addresses in a given network view, all unmanaged IPv4 and IPv6 addresses of all networks in the network view are cleared. When you select an entire network or a specific network in the 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**.
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 862.
- 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 862.
- 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 862.

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.
   - Keep the existing and ignore this conflict: Keeps the current DHCP lease for the address and ignores the lease conflict.
2. Click OK.
Resolving Fixed Address Conflicts

When the discovered MAC address of an IPv4 address does not match its existing MAC address, or when the DUID of an IPv6 address does not match its existing DUID, the IP address has a fixed address conflict.

To resolve a fixed address conflict:
1. In the Resolve Conflict 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. Note that you cannot convert an IPv6 address to a reservation.
   - Clear discovered data: Clears the discovered data and no object is created for the IP address.
2. Click OK.

Resolving Host Conflicts

When the MAC address of an IPv4 address that belongs to a host record a does not match its existing MAC address, or when the DUID of an IPv6 address that belongs to a host record does not match its existing DUID, the IP address has a host conflict.

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 IPv4 or IPv6 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**.

**Note:** When you clear all discovered data in a given network view, all imported discovered data for managed addresses in all IPv4 and IPv6 networks in the network view are cleared.
Part 7 Monitoring and Reporting

This section explains how to use the different monitoring and reporting tools, including SNMP. It includes the following chapters:

- Chapter 33, "Monitoring the Appliance", on page 867
- Chapter 34, "Monitoring with SNMP", on page 893
- Chapter 35, "Infoblox Reporting Solution", on page 967
Chapter 33 Monitoring the Appliance

This chapter describes the status icons that indicate the state of appliances, services, database capacity, Ethernet ports, HA, and Grid replication. It also explains how to use the various logs and the traffic capture tool to monitor a NIOS appliance.

This chapter contains the following sections:

- **Viewing Status** on page 868
  - Grid Status on page 868
  - Member Status on page 868
  - Viewing Hardware Status on page 874
- **Monitoring Services** on page 875
  - Service Status on page 875
  - Monitoring Grid Services on page 875
  - Monitoring Member Services on page 876
- **Using a Syslog Server** on page 877
  - Specifying Syslog Servers on page 877
  - Configuring Syslog for Grid Members on page 878
  - Setting DNS Logging Categories on page 879
  - Viewing the Syslog on page 880
  - Searching in the Syslog on page 880
  - Downloading the Syslog File on page 880
- **Monitoring Tools** on page 881
  - Using the Audit Log on page 881
  - Viewing the Replication Status on page 883
  - Using the Traffic Capture Tool on page 884
  - Using the Capacity Report on page 885
  - Using the Phone Home Feature on page 886
  - Monitoring DNS Transactions on page 887
  - Viewing DNS Alert Indicator Status on page 889
  - Configuring DNS Alert Thresholds on page 890
**Viewing Status**

Grid Manager provides tools for monitoring the status of the Grid, members, and services. You can monitor overall Grid and member status from the Dashboard, which provides a high-level view of your Grid, members and IP address data, and easy access to tasks. For information, see Grid Manager on page 59.

Grid Manager also displays status icons to indicate the state of appliances, services, database capacity, Ethernet ports, HA, and Grid replication. For the Infoblox-1852-A and -2000-A, and -4010, Grid Manager displays status icons for the power supplies. For the Infoblox -2000-A and -4010, 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 893.

**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 88.

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 Manger 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 875. 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 89.

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 875.
- **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="green.png" alt="Green" /></td>
<td>Green</td>
<td>The appliance is operating normally in a “Running” state.</td>
</tr>
<tr>
<td><img src="yellow.png" alt="Yellow" /></td>
<td>Yellow</td>
<td>The appliance is connecting or synchronizing with its Grid Master.</td>
</tr>
<tr>
<td><img src="red.png" 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="green.png" alt="Green" /></td>
<td>Green</td>
<td>Under 85% of the capacity is currently in use.</td>
</tr>
<tr>
<td><img src="yellow.png" alt="Yellow" /></td>
<td>Yellow</td>
<td>Between 85% and 95% of the capacity in use.</td>
</tr>
<tr>
<td><img src="red.png" 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 885. 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="green.png" alt="Green" /></td>
<td>Green</td>
<td>Under 85% of the database capacity is currently in use.</td>
</tr>
<tr>
<td><img src="yellow.png" 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="green" 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="red" alt="Red" /></td>
<td>Red</td>
<td>The port is not able to make a network connection.</td>
</tr>
<tr>
<td><img src="gray" 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="green" alt="Green" /></td>
<td>Green</td>
<td>The LCD is functioning properly.</td>
</tr>
<tr>
<td><img src="yellow" 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="green" alt="Green" /></td>
<td>Green</td>
<td>Under 90% capacity.</td>
</tr>
<tr>
<td><img src="yellow" alt="Yellow" /></td>
<td>Yellow</td>
<td>Between 90% and 95% capacity.</td>
</tr>
<tr>
<td><img src="red" 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 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="green" alt="Green" /></td>
<td>Green</td>
<td>The fan is functioning properly.</td>
</tr>
<tr>
<td><img src="red" alt="Red" /></td>
<td>Red</td>
<td>The fan is not running.</td>
</tr>
</tbody>
</table>
Power Supply
The Infoblox-1552-A, -1852-A, -2000-A, and -4010 have redundant power supplies. The power supply icon indicates the operational status of the power supplies.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Green]</td>
<td>Green</td>
<td>The power supplies are functioning properly.</td>
</tr>
<tr>
<td>![Red]</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>![Green]</td>
<td>Green</td>
<td>The NTP service is enabled and running properly.</td>
</tr>
<tr>
<td>![Yellow]</td>
<td>Yellow</td>
<td>The NTP service is enabled, and the appliance is synchronizing its time.</td>
</tr>
<tr>
<td>![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>![Gray]</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 VMware do not monitor or report the CPU temperature.

System Temperature
This icon is always green. The description reports the system temperature.

Note: vNIOS appliances on VMware do not monitor or report the system temperature.

CPU Usage
Grid Manager displays the current percentage of the CPU usage on the selected Grid member. The maximum is 100%. The status icon can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Green]</td>
<td>Green</td>
<td>Under 90% capacity</td>
</tr>
<tr>
<td>![Yellow]</td>
<td>Yellow</td>
<td>Between 90% and 95% capacity</td>
</tr>
<tr>
<td>![Red]</td>
<td>Red</td>
<td>Over 95% capacity</td>
</tr>
</tbody>
</table>
RAID

For the Infoblox-2000-A and -4010, Grid Manager displays one of the following icons to indicate the status of each disk in the RAID array. Next to the status icon is a summary that includes the disk number, the operational status of the disk, and the disk type. Grid Manager also displays a RAID summary with an overall array status icon and the percentage at which the array is currently operating.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Green]</td>
<td>Green</td>
<td>The RAID array or the disk is functioning properly.</td>
</tr>
<tr>
<td>![Yellow]</td>
<td>Yellow</td>
<td>A new disk has been inserted and the RAID array is rebuilding.</td>
</tr>
<tr>
<td>![Red]</td>
<td>Red</td>
<td>The RAID array or the disk is degraded. At least one disk in the array is not functioning properly. Grid Manager lists the disks that are online. Replace only the disks that are offline.</td>
</tr>
</tbody>
</table>

In the event of a disk failure, you must replace the failed disk with one that is qualified and shipped from Infoblox and has the same disk type as the rest of the disks in the array. The appliance displays information about mismatched disks. The disk type of the Infoblox-2000-A can be one of the following:

- IB-Type 1: Infoblox supported disk type
- IB-Type 2: Infoblox supported disk type
- Unk: Unknown disk type that Infoblox does not support

Infoblox-4010 uses only the IB-Type 3 disk type. All disk drives in the array must have the same disk type for the array to function properly. You can have either IB-Type 1, IB-Type 2, or IB-Type 3, but you cannot mix both in the array. When you have a mismatched disk in the array, you must promptly replace the disk with a replacement disk from Infoblox to avoid operational issues.

RAID Battery

The icon indicates the status of the disk controller backup battery on the Infoblox-2000-A or -4010.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Green]</td>
<td>Green</td>
<td>The battery is charged. The description indicates the estimated number of hours of charge remaining on the battery.</td>
</tr>
<tr>
<td>![Yellow]</td>
<td>Yellow</td>
<td>The battery is charging.</td>
</tr>
<tr>
<td>![Red]</td>
<td>Red</td>
<td>The battery is not charged.</td>
</tr>
</tbody>
</table>
Viewing the Grid Node Tree

Navigate to the Grid -> Grid Manager -> Visualization tab to view a graphical representation of the Grid, with its members represented as nodes in the tree. Each member is labeled with its hostname. You can click Display Node Labels on the left panel to display or hide the labels.

By default, the Grid Master is the root node at the center of the tree. It is represented by a color-coded icon connected to its members. You can then click a member to re-center the tree on that node. The left panel displays information about the member that is at the center of the node tree.

In the node tree, the shape of the icons indicate the role of the member in the Grid:
- Circle: Grid Master
- Ellipse: Grid Members

The colors of the icons indicate the status of the member:
- Green: The member is online and functioning properly.
- Grey: The member has not joined the Grid.
- Red: The member has operational problems.

The connectors indicate the connection status between the Grid Master and the member:
- Blue Line: Connects the Grid Master with online Grid members
- Thick White Line: Connects the Grid Master with Grid Master Candidates
- Dashed Line Connector: Connects the Grid Master with offline Grid members

The node tree includes zooming and panning capabilities to enable quick navigation and selection among multiple nodes. You can also hover your mouse over a node to view node information. It displays the same information as that displayed on the left panel, when a node is at the center of the tree.

For the Grid Master:
- Grid name
- Standalone or HA
- Number of members in the Grid
- Status of each protocol running on the Grid
- Grid status

For a Member:
- Member name
- Standalone or HA
- HA Status if HA pair
- Status of each protocol running on that member
Viewing Hardware Status

You can view the link activity and connection speed of an Ethernet port by looking at its Link/Act and Speed LEDs on the appliance. The status the LEDs convey through their color and illumination (steady glow or blinking) are presented in the following tables.

For Infoblox-2000-A Appliances

<table>
<thead>
<tr>
<th>MGMT and HA Ports</th>
<th>Label</th>
<th>Color</th>
<th>Port Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link/Act</td>
<td>Steady Orange</td>
<td>Link is up but inactive</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Blinking Orange</td>
<td>Link is up and active</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dark</td>
<td>Link is down</td>
<td></td>
</tr>
</tbody>
</table>

MGMT, HA, and LAN Ports

<table>
<thead>
<tr>
<th>Label</th>
<th>Color</th>
<th>Port Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>Steady Amber</td>
<td>1000 Mbps</td>
</tr>
<tr>
<td></td>
<td>Steady Green</td>
<td>100 Mbps</td>
</tr>
<tr>
<td></td>
<td>Dark</td>
<td>10 Mbps</td>
</tr>
</tbody>
</table>

For Infoblox-1050-A, -1550-A, -1552-A, and -1852-A Appliances

<table>
<thead>
<tr>
<th>Label</th>
<th>Color</th>
<th>Port Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link/Act</td>
<td>Steady Green</td>
<td>Link is up but inactive</td>
</tr>
<tr>
<td></td>
<td>Blinking Green</td>
<td>Link is up and active</td>
</tr>
<tr>
<td></td>
<td>Dark</td>
<td>Link is down</td>
</tr>
<tr>
<td>Speed</td>
<td>Steady Amber</td>
<td>1000 Mbps</td>
</tr>
<tr>
<td></td>
<td>Steady Green</td>
<td>100 Mbps</td>
</tr>
<tr>
<td></td>
<td>Dark</td>
<td>10 Mbps</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. NIOS appliances include syslog messages generated by the bloxTools service. You can also include audit log messages and specific BIND messages among the messages the appliance sends to the syslog server.

In addition to saving system messages to a remote syslog server, a NIOS appliance also stores the system messages locally. When the syslog file reaches its maximum size, which is 300 MB for Infoblox appliances and VMware virtual appliances, and 20 MB for Riverbed virtual appliances, the appliance automatically writes the file into a new file by adding a .0 extension to the first file and incrementing subsequent file extensions by 1.

Files are compressed during the rotation process, adding 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 877
- Configuring Syslog for Grid Members on page 878
- Setting DNS Logging Categories on page 879
- Viewing the Syslog on page 880
- Searching in the Syslog on page 880
- Downloading the Audit Log on page 883

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
     - 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.
Monitoring the Appliance

— **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. Save the configuration and click **Restart** if it displays at the top of the screen.

**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 877.
   In addition to storing the system log on a Grid member, you can configure a member to send the log to a syslog server.
3. Select the **Advanced** tab and complete the following:
   — **Enable syslog proxy:** Select this to enable the appliance to receive syslog messages from other devices, such as syslog servers and routers, and then forward these messages to an external syslog server.
   — **Enable listening on TCP:** Select this if the appliance uses TCP to receive messages from other devices. Enter the number of the port through which the appliance receives syslog messages from other devices.
— **Enable listening on UDP**: Select this if the appliance uses UDP to receive messages from other devices. Enter the number of the port through which the appliance receives syslog messages from other devices.

— **Proxy Access Control**: 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. Save the configuration and click **Restart** if it displays at the top of the screen.

### 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 877.

To specify logging categories:

1. From the **Data Management** tab, select the **DNS** tab, and then click **Grid DNS Properties** from the Toolbar.
   or
   From the **Data Management** tab, select the **DNS** tab -> **Members** tab -> **Grid_member** check box, and then click the **Edit** icon.

2. In the **Grid DNS Properties** or **Member DNS Properties** editor, click **Toggle Expert Mode** if the editor is in the basic mode, select the **Logging** tab, and then complete the following:
   — **Logging Facility**: Select a facility from the drop-down list. This is the location on the syslog server to which you want to sort the DNS logging messages.
   — **Logging Category**: Select one or more of these log categories:
     — **general**: Records the BIND messages that are not specifically classified.
     — **client**: 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. Save the configuration and click **Restart** if it displays at the top of the screen.
Viewing the Syslog

1. From the Administration tab, select the Logs tab -> Syslog tab.
2. From the drop-down list at the upper right corner, select the Grid member on which you want to view the syslog.
3. Optionally, use the filters to narrow down the system messages you want to view. Click Show Filters to enable the filters. Configure the filter criteria, and then click Apply.

Based on your filter criteria (if any), Grid Manager displays the following in the Syslog viewer:

- **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.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 57.
- 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 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 883
- Using the Traffic Capture Tool on page 884
- Using the Capacity Report on page 885
- Using the Phone Home Feature on page 886
- Monitoring DNS Transactions on page 887
- Viewing DNS Alert Indicator Status on page 889
- Configuring DNS Alert Thresholds on page 886

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 765.

Using the Audit Log

The audit log contains a record of all Infoblox administrative activities. It provides the following detailed information:

- Timestamp of the change. If you have different admin accounts with different time zone settings, the appliance uses the time zone of the admin account that you use to log in to the appliance to display the date and timestamp.
- Administrator name
- Changed object name
- New value of the object. If you change multiple properties of an object, the audit log lists all changes in a comma-separated log entry. You can also search the audit log to find the new value of an object.

The appliance logs the following successful operations:

- Logins to Grid Manager and the API.
- Logout events, including when users log out by clicking the Logout button, when the Grid Manager GUI times out, and when users are logged out due to an error.
- Write operations such as the addition, modification, and deletion of objects.
- System management operations such as service restarts and appliance reboots.
- Scheduled tasks such as adding an A record or modifying a fixed address.

Enabling Audit Log Rolling

When the audit log reaches its maximum size, which is 100 MB, the appliance automatically writes the file into a new file by adding a .0 extension to the first file and incrementing subsequent file extensions by 1. Files are compressed during the rotation process, adding a .gz extension following the numerical increment (file.1.gz). The sequential incrementation goes from zero through nine. When the eleventh file is started, the tenth log file (file.10.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.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters on page 57.
- Export or print the content of the log.
Searching in the Audit Log

Instead of paging through the audit log file to locate messages, you can have the appliance search for messages with certain text strings.

To search for specific messages:

- Enter a search value in the search field below the filters, and then click the Search icon.
  
  The appliance searches through the audit log file and highlights the search value in the viewer. You can use the arrow keys next to the Search icon to locate the previous or next message that contains the search value.

Downloading the Audit Log

You can download the audit log file to a specified directory, if you want to analyze it later.

To download an audit log file:

1. From the Administration tab, select the Logs tab -> Audit Log tab, and then click the Download icon.
2. Navigate to a directory where you want to save the file, optionally change the file name (the default name is auditLog.tar.gz), and then click OK. If you want to download multiple audit log files to the same location, rename each downloaded file before downloading the next.

Note: If your browser has a pop-up blocker enabled, you must turn off the pop-up blocker or configure your browser to allow pop-ups for downloading files.

Viewing the Replication Status

The Replication Status panel reports the status of the database replication between Grid members and Grid Master, and between the two nodes in an independent HA pair. You can use this information to check the health of the Grid and HA pair activity.

To view the current replication status, from the Grid tab, select the Grid Manager tab -> Members tab, and then click Toggle Replication Status View.

Grid Manager can display the following replication information for each member:

- **Name**: The FQDN (fully qualified domain name) of the appliance.
- **Send Queue**: The size of the queue from the Grid Master to the Grid member.
- **Last Send**: The timestamp of the last replication information sent by the Grid Master.
- **Receive Queue**: The size of the queue from the Grid member to the Grid Master.
- **Last Receive**: The timestamp of the last replication information sent received by the Grid Master.
- **Member Replication Status**: The replication status between the member and the Grid Master. Grid Manager displays the status in green when the status is fine or red when the member is offline.
- **HA Replication Status**: The HA replication status between the active and passive nodes. The status is at the member level, not at the node level. Grid Manager displays the status in red when one of the nodes is offline.
- **Status**: The current operational status of the appliance. The status can be one of the following:
  - **Green**: The appliance is operating normally in a “Running” state.
  - **Yellow**: The appliance is connecting or synchronizing with its Grid Master.
  - **Red**: The Grid member is offline, is not licensed (that is, it does not have a DNSOne license with the Grid upgrade that permits Grid membership), is upgrading or downgrading, or is shutting down.
- **IP Address**: The IP address of the appliance.
- **DHCP, DNS, TFTP, HTTP, FTP, NTP, bloxTools, Captive Portal**: The current status of the service. The status can be one of the following:
  - **Green**: The service is enabled and running properly.
  - **Yellow**: The service is enabled, but there may be some issues that require attention.
— **Red**: The service is enabled, but it is not running properly. A red status icon can also appear temporarily when a service is enabled and begins running, but the monitoring mechanism has not yet notified the Infoblox GUI.

— **Gray**: The service is not configured or it is disabled.

- **Hardware Type**: The hardware type of the appliance, such as IB-1550-A.
- **Serial Number**: The serial number of the appliance.
- **DB Utilization**: The percentage of the database that is currently in use.
- **Comment**: Information about the appliance.
- **Site**: The location to which the member belongs. This is one of the predefined extensible attributes.
- **HA**: Indicates whether the member is an HA pair. If the member is an HA pair, Grid Manager displays the status of the HA pair.
- **Hardware Model**: The hardware model of the appliance.

You can do the following:

- Use filters and the **Go to** function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the **Go to** field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see *Using Quick Filters* on page 57.
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see *Modifying Data in Tables* on page 52.
- Edit the properties of a member.
  — Click the check box beside a member, and then click the **Edit** icon.
- Delete a member.
  — Click the check box beside a member, and then click the **Delete** icon.
- Export or print the list.

### Using the Traffic Capture Tool

You can capture the traffic on one or all of the ports on 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 278.)
— **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.

**Note**: Riverbed virtual appliances support capturing traffic only on the LAN port.

— **Seconds to run**: Specify the number of seconds you want the traffic capture tool to run.

3. **Capture Control**: Click the Start icon to start the capture. A warning message appears indicating that this report will overwrite the existing file. Click Yes. You can click the Stop icon to stop the capture after you start it.

4. **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 146, 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. Save the configuration and click Restart if it displays at the top of the screen.
Monitoring DNS Transactions

The NIOS appliance provides tools for monitoring DNS transactions and mitigating cache poisoning. Cache poisoning can occur when a DNS server accepts maliciously created unauthentic data. The DNS server ends up locally caching the incorrect entries and serving them to users that make the same DNS requests. In a maliciously created situation, the attacker can redirect Internet traffic from the legitimate host to another host that the attacker controls.

You can configure the appliance to track invalid DNS responses for recursive DNS queries. The appliance tracks DNS responses that arrive on invalid ports or have invalid TXIDs (DNS transaction IDs). Both invalid ports and invalid TXIDs could be indicators of cache poisoning. An invalid port is a DNS response that arrives from UDP (User Datagram Protocol) port 53 with either one of the following conditions:

- There are no outstanding DNS requests from the port on which the response arrives.
- The TXID of the DNS response matches the TXID of an outstanding request. However, the request was sent from a port other than the port on which the response arrives.

An invalid TXID is a DNS response that arrives from UDP port 53, and the TXID does not match the TXID of an outstanding DNS request. 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 888.
2. Configure the thresholds for DNS alert indicators. For information, seeConfiguring DNS Alert Thresholds on page 890.
3. Enable SNMP traps and e-mail notifications. For information, see Configuring SNMP on page 895.
4. Review the DNS alert status. For information, see Viewing DNS Alert Indicator Status on page 889.
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, seeThreshold Crossing Traps on page 926.

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, seeEnabling and Disabling Rate Limiting from External Sources on page 891.
• Configure rate limit traffic rules from specific sources. For information, see Configuring Rate Limiting Rules on page 891.

You can verify the rate limiting rules after you configure them. For information, seeViewing Rate Limiting Rules on page 892.

Enabling and Disabling DNS Alert Monitoring

The appliance monitors only UDP traffic on port 53 for recursive queries, and then reports invalid DNS responses. DNS alert monitoring is disabled by default. For an HA pair, you must enable DNS alert monitoring on both the active and passive nodes.

To enable DNS network monitoring and DNS alert monitoring:
1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:
   ```
   set monitor dns on
   ```
   The appliance displays the following:
   ```
   Turning on DNS Network Monitoring...
   ```
3. Enter the following command:
   ```
   set monitor dns alert on
   ```
   When you enable DNS alert monitoring and DNS network monitoring is disabled, the appliance automatically enables DNS network monitoring and displays the following:
   ```
   DNS Network Monitoring is disabled. It must be enabled for alerting to function.
   Enable DNS Monitoring now? (y or n):
   ```
   You can also disable DNS network monitoring and DNS alert monitoring using the following commands:
   ```
   set monitor dns off
   set monitor dns alert off
   ```

**Note:** When you restart DNS network monitoring, you also reset the SNMP counters for DNS alerts.

You can then view the alert status to identify the primary source of invalid DNS responses. For information, see Viewing DNS Alert Indicator Status on page 889.
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 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 895.

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 external sources.

To enable rate limiting from sources:

1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:
   ```bash
   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 891.

   You can also disable rate limiting by entering the following command:
   ```bash
   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 external sources. 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:
   ```bash
   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:
     ```bash
     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:
     ```bash
     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:
     ```bash
     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:
     ```bash
     set ip_rate_limit add source all limit 5000/m
     ```
Removing Rate Limiting Rules
You can remove the existing rate limiting rules.
To remove all the existing rules:
1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:
   — To remove the rate limiting rule that limits traffic from all sources, enter:
     ```
     set ip_rate_limit remove source all
     ```
   or
   — To remove all of the rate limiting rules from all sources, enter:
     ```
     set ip_rate_limit remove all
     ```
To remove one of the existing rules for an existing host:
1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:
   ```
   set ip_rate_limit remove source ip-address[/mask]
   ```

Viewing Rate Limiting Rules
You can view the existing rate limiting rules 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:

<table>
<thead>
<tr>
<th>Source</th>
<th>Limit</th>
<th>Burst</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.1.1</td>
<td>0 packets/minute</td>
<td>0 packets</td>
</tr>
<tr>
<td>10.10.1.2</td>
<td>5 packets/minute</td>
<td>5 packets</td>
</tr>
<tr>
<td>10.10.2.1/24</td>
<td>5 packets/minute</td>
<td>10 packets</td>
</tr>
<tr>
<td>all</td>
<td>5000 packets/minute</td>
<td>5000 packets</td>
</tr>
</tbody>
</table>
Chapter 34 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 894
  — About SNMPv1 and SNMPv2 on page 895
  — About User-Based Security Model in SNMPv3 on page 895

• **Configuring SNMP** on page 895
  — Configuring SNMPv3 Users on page 896
  — Modifying SNMPv3 Users on page 897
  — Deleting SNMPv3 Users on page 897
  — Accepting Queries on page 897
  — Adding Trap Receivers on page 898
  — Defining Thresholds for Traps on page 899
  — Setting SNMP and Email Notifications on page 900
  — Setting SNMP System Information on page 899
  — Testing the SNMP Configuration on page 900

• **SNMP MIB Hierarchy** on page 901
  — MIB Objects on page 902
  — System Object IDs on page 902

• **Infoblox MIBs** on page 904
  — Loading the Infoblox MIBs on page 904
  — ibTrap MIB on page 906
  — ibPlatformOne MIB on page 936
  — ibDHCPOne MIB on page 953
  — ibDNSOne MIB on page 961
  — IB-DNSSERV-MIB on page 965
  — IB-DHCPserv-MIB on page 965
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.

The NIOS appliance supports SNMPv1, SNMPv2, and SNMPv3. It also adheres to the following RFCs:

- RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413, Simple Network Management Protocol (SNMP) Applications
- RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP)
- RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
- RFC 1155, Structure and identification of Management information for TCP/IP-based internets
- RFC 1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II
- RFC 2578, Structure of Management Information Version 2 (SMIV2)
About SNMPv1 and SNMPv2

SNMPv1 is the initial implementation of SNMP. It operates over protocols such as UDP (User Datagram Protocol) and IP (Internet Protocol). SNMPv2 includes improvements in performance and security. It adds new protocol operations such as GetBulk and Inform, which allow the management system to request larger blocks of data from the agent. Both SNMPv1 and SNMPv2 use common strings that are sent in clear text to authenticate clients.

The NIOS appliance supports SNMPv1 and SNMPv2 in which the SNMPv2 agent acts as a proxy agent for the SNMPv1 management systems. When an SNMPv1 management system sends a query to the appliance, the SNMPv2 proxy agent forwards the request to the SNMPv1 agent. The proxy agent maps the SNMPv1 trap messages to the SNMPv2 trap messages, and then forward the messages to the management system.

You can enable the appliance to receive queries from SNMPv1 and SNMPv2 management systems. You can also add SNMPv1 and SNMPv2 management systems to receive traps from the appliance. For information about how to configure SNMPv1 and SNMPv2 on the appliance, see Configuring SNMP on page 895.

About User-Based Security Model in SNMPv3

SNMPv3 adds security and remote configuration enhancements to SNMPv1 and SNMPv2. The NIOS appliance supports the USM (User-based Security Model) in SNMPv3 for the authentication, encryption, and decryption of SNMP data. SNMPv3 uses the same MIB objects as those supported in SNMPv1 and SNMPv2.

SNMPv3 provides the following security measures:

- Data integrity: Ensure that SNMP data is not maliciously modified by unauthorized entities during its transmission through the network. This protects against unauthorized management operations, such as falsifying the value of a MIB object.
- Authentication: Verify the identities of the origin of the SNMP data to protect against masquerade threats that may temper the identity of users who have the appropriate authorization to send and receive SNMP data.
- Confidentiality: Ensure that unauthorized users cannot eavesdrop on any data exchanges between SNMP agents and management systems, depending on local policies of the systems.
- Timeliness: Ensure that the SNMP data is received in a timely manner to prevent malicious reordering of data by unauthorized entities.

To enable SNMPv3 on the NIOS appliance to provide user-based security, you must first configure SNMPv3 users on the appliance to enable access by SNMP management systems. The appliance supports HMAC-MD5-96 and HMAC-SHA-96 hash functions as the authentication protocols, and DES (Data Encryption Standard) and AES (Advanced Encryptions Standard) as the encryption methods for SNMPv3 users. For information, see Configuring SNMP on page 895.

Configuring SNMP

You can configure the appliance to receive SNMP queries from specific management systems and send SNMP traps to specific trap receivers. The appliance supports SNMPv1, SNMPv2, and SNMPv3. You can set up either SNMPv1/SNMPv2 or SNMPv3, or all of them for the Grid. You can also override the Grid settings at a member level.

To configure SNMPv1 and SNMPv2 on the appliance, do the following:

- Enable the NIOS appliance to accept queries, as described in Accepting Queries on page 897.
- Specify the management systems to which the appliance sends traps, as described in Adding Trap Receivers on page 898.
- Specify system information using managed objects in MIB-II, the standard MIB defined in RFC 1213. For information, see Setting SNMP System Information on page 899.
To configure SNMPv3 on the appliance, do the following:

- Add an SNMPv3 user and set up authentication and privacy protocols. For information, see Configuring SNMPv3 Users on page 896. After you set up an SNMPv3 user, you can modify and delete it. For information, see Modifying SNMPv3 Users on page 897 and Deleting SNMPv3 Users on page 897.
- Enable the NIOS appliance to accept queries, as described in Accepting Queries on page 897.
- Specify the management systems to which the appliance sends traps, as described in see Adding Trap Receivers.
- Specify system information using managed objects in MIB-II, the standard MIB defined in RFC 1213. For information, see Setting SNMP System Information on page 899.

### Configuring SNMPv3 Users

To enable SNMPv3, you must first configure SNMPv3 users on the appliance. For information about SNMPv3, see About User-Based Security Model in SNMPv3 on page 895.

To configure an SNMPv3 user:

1. From the Administration tab, select the SNMPv3 Users tab, and then click the Add icon.
2. In the Add SNMPv3 User wizard, complete the following:
   - **Name**: Enter a user name for the SNMPv3 management system.
   - **Authentication Protocol**: Select one of the following:
     - **MD5**: Select this to use the HMAC-MD5-96 authentication protocol to authenticate the SNMPv3 user. This protocol uses the MD5 (Message-Digest algorithm 5) hash function in HMAC (Hash-based Message Authentication Code) and truncates the output to 96 bits. The output is included as part of the SNMP message sent to the receiver. For detailed information about the protocol, refer to RFC1321, The MD5 Message-Digest Algorithm.
     - **SHA**: Select this to use the HMAC-SHA-96 authentication protocol to authenticate the SNMPv3 user. This protocol uses the SHA (Secure Hash Algorithm) hash function and truncates the output to 96 bits. The output is included as part of the SNMP message sent to the receiver.
     - **None**: Select this to decline using any authentication protocol for this SNMPv3 user. When you select this option, you are not required to enter a password.
   - **Password**: Enter a password for the selected authentication protocol.
   - **Confirm Password**: Enter the same password.
   - **Privacy Protocol**: Select one of the following:
     - **DES**: Select this to use DES for data encryption. DES is a block cipher that employs a 56-bit key size and 64-bit block size in the encryption.
     - **AES**: Select this to use AES for data encryption. AES is a symmetric-key encryption standard that comprises three block ciphers, AES-128, AES-192, and AES-256. Each of these ciphers has a 128-bit block size and a key size of 128, 192, and 256 bits, respectively.
     - **None**: Select this to decline using any privacy protocol for this SNMPv3 user. When you select this option, you are not required to enter a password.
   - **Password**: Enter a password for the privacy protocol.
   - **Confirm Password**: Enter the same password.
   - **Comment**: Enter useful information about the SNMP user, such as location or department.
   - **Disable**: Select this check box to retain an inactive profile for this SNMP user in the configuration. You can clear this check box to activate the profile.

   **Note**: If an SNMPv3 user is configured to send SNMP queries, you cannot delete the user.

3. Click **Next** to define extensible attributes. For information, see Using Extensible Attributes on page 265.
4. Save the configuration.
Modifying SNMPv3 Users

1. From the Administration tab, select the SNMPv3 Users tab -> snmpv3user, and then click the Edit icon.
2. The SNMPv3 User editor provides the following tabs from which you can edit data:
   - General: Modify the data as described in Configuring SNMPv3 Users on page 896.
   - Extensible Attributes: Add and delete extensible attributes that are associated with the SNMPv3 user account. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes on page 265.
3. Save the configuration.

Deleting SNMPv3 Users

When you delete an SNMPv3 user that is configured to send queries or receive traps, a warning message states that the SNMPv3 is associated with the corresponding function. You can then decide whether you want to delete the user or not.

To delete an SNMPv3 user:

1. From the Administration tab, select the SNMPv3 Users tab -> snmpv3user, and then click the Delete icon.
2. In the Delete confirmation dialog box, click Yes.

   Note: You cannot schedule the deletion of an SNMPv3 user.

Accepting Queries

You can allow specific management systems to send SNMP queries to a NIOS appliance. For SNMPv1 and SNMPv2, you must specify a community string. The appliance accepts queries only from management systems that provide the correct community string. You can also specify SNMPv3 users to send queries. For information about configuring SNMPv3 users, see Configuring SNMPv3 Users on page 896.

To configure an appliance to accept SNMP queries:

1. From the Grid tab, select the Grid Manager tab, and then select Grid Properties -> Edit from the Toolbar.
   or
   From the Grid tab, select the Grid Manager -> Members tab -> member, and then click the Edit icon.
2. In the Grid Properties or Grid Member Properties editor, select the SNMP tab. To override Grid settings, click Override in the Grid Member Properties editor.
3. Complete the following in the SNMP section.
   - Enable SNMPv1/SNMPv2 Queries: Select this to accept SNMPv1 and SNMPv2 queries from management systems.
     - Community String: Enter a text string that the management system must send together with its queries to the appliance. A community string is similar to a password in that the appliance accepts queries only from management systems that send the correct community string. Note that this community string must match exactly what you enter in the management system.
     - Engine ID: Displays the engine ID of the appliance that manages the SNMP agent. The management system needs this ID to send traps to the appliance. If the appliance is an HA pair, this field displays the engine IDs for both the active and passive nodes.
   - Enable SNMPv3 Queries: Select this to enable queries from SNMPv3 management systems. Click the Add icon to add SNMPv3 users that you have configured on the appliance. In the SNMPv3 User Selector dialog box, click the SNMPv3 user you want to add. The appliance displays the selected SNMPv3 users in the table. You can add comments in the table. You can also select an SNMPv3 user and click the Delete icon to remove it from the table. Note that a disabled SNMPv3 user cannot send queries to the appliance.
4. Save the configuration.
Adding Trap Receivers

You can enable the NIOS appliance to send traps to specific management systems using either SNMPv1/SNMPv2 or SNMPv3, or all versions of SNMP. You can then add management systems that are allowed to receive traps from the appliance. Note that you cannot enable both SNMPv1/SNMPv2 and SNMPv3 on the same trap receiver. The appliance sends traps when certain events occur. You can enable SNMP traps and add trap receivers to the Grid. You can also override the Grid settings at the member level.

To enable the appliance to send traps and to add trap receivers, do the following:

1. From the Grid tab, select the Grid Manager tab, and then select Grid Properties -> Edit from the Toolbar.
   or
   From the Grid tab, select the Grid Manager -> Members tab -> member, and then click the Edit icon.
2. In the Grid Properties or Grid Member Properties editor, select the SNMP tab. To override Grid settings, click Override in the Grid Member Properties editor.
3. Complete the following in the SNMP tab:
   — Enable SNMPv1/SNMPv2 Traps: Select this to enable the appliance to send traps to specified management systems.
     — Community String: Enter a text string that the NIOS appliance sends to the management system together with its traps. Note that this community string must match exactly what you enter in the management system.
   — Enable SNMPv3 Traps: Select this to enable the appliance to send traps to specified SNMPv3 users.
4. Click the Add icon and select one of the following from the drop-down menu to add an SNMP trap receiver:
   — SNMPv1/SNMPv2: Select this to add an SNMPv1 or SNMPv2 management system as a trap receiver. Grid Manager adds a row to the table. In the Address field, enter the IP address of the SNMP management system to which you want the SNMP agent on the appliance to send traps. You can enter more than one trap receiver. To remove a trap receiver from the list, select the address, and then click the Delete icon.
   — SNMPv3: Select this to add an SNMPv3 management system as a trap receiver. Grid Manager displays the SNMPv3 User Selector dialog box. Click the name of the SNMPv3 user in the dialog box. Grid Manager adds the user to the table. In the Address field, enter the IP address of the SNMP management system to which you want the SNMP agent on the appliance to send traps. You can add more than one trap receiver. To remove a trap receiver from the list, select the address, and then click the Delete icon.

In the Trap Receiver table, Grid Manager displays the following information about the trap receivers:
   — Address: The IPv4 or IPv6 address of the trap receiver. Note that when an SNMPv3 user is disabled, SNMPv1/SNMPv2 traps are disabled. You can modify the IP address of the trap receiver even when the following are disabled: SNMPv3 users, SNMPv1/SNMPv2 traps, and SNMPv3 traps.
   — SNMPv3 User: The user name of the SNMPv3 trap receiver. This is for SNMPv3 only.
   — Comment: Information you entered about the management system.
5. Save the configuration.
Setting SNMP System Information

You can enter values for certain managed objects in MIB-II, the standard MIB defined in RFC 1213. Management systems that are allowed to send queries to the appliance can query these values. You can enter these values for the Grid and specific members. You can also override the Grid values at a member level.

To enter system information:
1. From the Grid tab, select the Grid Manager tab, and then select Grid Properties -> Edit from the Toolbar.
   or
   From the Grid tab, select the Grid Manager -> Members tab -> member, and then click the Edit icon.
2. In the Grid Properties or Grid Member Properties editor, select the SNMP tab. To override Grid settings, click Override in the Grid Member Properties editor.
3. Complete the following in the SNMP tab. For an HA member, click Override Node 2 settings to enter information for node 2 of the HA pair.
   — sysContact: Enter the name of the contact person for the appliance.
   — sysLocation: Enter the physical location of the appliance.
   — sysName: Enter the fully qualified domain name of the appliance.
   — sysDescr: Enter useful information about the appliance, such as the software version it is running.
4. Save the configuration and click Restart if it displays at the top of the screen.

Defining Thresholds for Traps

Threshold events for appliance performance are configurable. For each event, you can set a value that triggers the appliance to send a trap and another value at which the appliance sends a CLEAR trap. The appliance sends a CLEAR trap the first time the event value reaches the reset value after it reached the trigger value.

To define the threshold values:
1. From the Grid tab, select the Grid Manager tab, and then select Grid Properties -> Edit from the Toolbar.
   or
   From the Grid tab, select the Grid Manager -> Members tab -> member, and then click the Edit icon.
2. In the Grid Properties or Grid Member Properties editor, click Toggle Advanced Mode, and then select the SNMP Threshold tab. To override Grid settings, click Override in the Grid Member Properties editor.
3. Complete the following in the SNMP Threshold tab. Each of the following event types have default Trigger and Reset values. You can change the values for any of them.
   — CPU Usage: The percentage of the CPU that is in use. The default Trigger value is 81, and the default Reset value is 70.
   — DBObjects: The percentage of the appliance’s database capacity that is in use. The default Trigger value is 80, and the default Reset value is 70.
   — Disk: The percentage of the appliance’s primary hard disk that is in use. The default Trigger value is 85, and the default Reset value is 70.
   — Memory: The percentage of the appliance’s memory that is in use. The default Trigger value is 90, and the default Reset value is 80.
   — Network Capacity: When the Grid is part of a Master Grid, this is the percentage of the Master Grid’s network capacity that is used by the Grid’s networks. The default Trigger value is 85, and the default Reset value is 75.
   — Reporting Volume: The percentage of data transmissions to the reporting server. The default Trigger value is 80, and the default Reset value is 71.
   — Rootfs: The percentage of the appliance’s root file system (“/”) that is in use. The default Trigger value is 85, and the default Reset value is 70.
4. Save the configuration and click Restart if it displays at the top of the screen.
Setting SNMP and Email Notifications

You can specify the event types that trigger trap and email notifications.

To set SNMP trap and email notifications:

1. From the Grid tab, select the Grid Manager tab, and then select Grid Properties -> Edit from the Toolbar.
   or
   From the Grid tab, select the Grid Manager -> Members tab -> member, and then click the Edit icon.

2. In the Grid Properties or Grid Member Properties editor, click Toggle Advanced Mode, and then select the Notification tab. To override Grid settings, click Override in the Grid Member Properties editor.

3. Complete the following:
   - **Enable All SNMP Notifications**: Select this check box if you want the appliance to send SNMP notifications (traps) for all events to the configured trap receivers. This is selected by default.
     For information on configuring trap receivers, see Adding Trap Receivers on page 898.
   - **Enable All Email Notifications**: Select this check box if you want the appliance to send email notifications (traps) for all events to the configured email recipients.
     For information on enabling email notifications and specifying recipients, see Notifying Administrators on page 146.
   - Alternatively, you can select specific event types from the table, and specify whether you want the appliance to send SNMP Notifications and Email notifications for each type of event.

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

Testing the SNMP Configuration

After you configure SNMP on the appliance, you can do the following to test your SNMP configuration:

- From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and then select Test SNMP from the Toolbar.

The appliance sends a “test trap” string to the trap receiver and displays a confirmation message at the top of the screen if your SNMP configuration is properly set up. If your SNMP configuration is not complete or if it is invalid, the appliance displays an error message. You can check your configuration and try again.

The following is a sample test trap that the trap receiver can get:

```
2011-04-04 17:37:14 10.32.2.80 [UDP: [10.32.2.80]:49244->[10.32.2.80]]:
SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-MIB::snmpTrapOID
SNMPv2-MIB::sysName.0 = STRING: 'Test trap'
```
in addition to implementing its own enterprise MIBs, Infoblox supports the standard MIBs defined in RFC-1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II.

The Infoblox MIBs are part of a universal hierarchical structure, usually referred to as the MIB tree. The MIB tree has an unlabeled root with three subtrees. Figure 34.2 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 34.2, Infoblox is a branch of the Enterprise subtree. IANA (Internet Assigned Numbers Authority) administers the Enterprise subtree, which is designated specifically for vendors who define their own MIBs. The IANA-assigned enterprise number of Infoblox is 7779; therefore, the OIDs of all Infoblox MIB objects begin with the prefix .1.3.6.1.4.1.7779. In addition, IB-DNSSERV and IB-DHCPSErv are branches of the Enterprise subtree as well. The Infoblox SNMP subtree branches down through two levels, ibProduct and ibOne, to the Infoblox MIBs: ibTrap, ibPlatformOne, ibDNSOne, and ibDHCPOne. The ibTrap MIB defines the traps that NIOS appliances send, and the ibPlatformOne, ibDNSOne, and ibDHCPOne MIBs provide information about the appliance. For detailed information about these MIBs, see Infoblox MIBs on page 904.

Figure 34.2 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>OBJECT-TYPE</th>
<th><code>sysObjectID</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>SYNTAX</td>
<td>Object Identifier</td>
</tr>
<tr>
<td>MAX-ACCESS</td>
<td>read-only</td>
</tr>
<tr>
<td>STATUS</td>
<td>current</td>
</tr>
</tbody>
</table>
| DESCRIPTION       | "The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining `what kind of box' is being managed. For example, if vendor 'Flintstones,Inc.' was assigned the subtree 1.3.6.1.4.1.424242, it could assign the identifier 1.3.6.1.4.1.424242.1.1 to its `Fred Router`."

```
Table 34.1 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 34.1 `sysObjectID` for Infoblox Hardware

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>ibDefault</td>
<td>Default environments, such as chroot</td>
</tr>
<tr>
<td>1001</td>
<td>ibRsp2</td>
<td>vNIOS appliances on Riverbed Services Platforms</td>
</tr>
<tr>
<td>1003</td>
<td>ibvm</td>
<td>vNIOS appliances on VMware ESX or ESXi servers</td>
</tr>
<tr>
<td>1004</td>
<td>ibvnios</td>
<td>Virtual NIOS</td>
</tr>
<tr>
<td>1101</td>
<td>ib1000</td>
<td>Infoblox-1000 appliances</td>
</tr>
<tr>
<td>1102</td>
<td>ib1200</td>
<td>Infoblox-1200 appliances</td>
</tr>
<tr>
<td>1103</td>
<td>ib500</td>
<td>Infoblox-500 appliances</td>
</tr>
<tr>
<td>1201</td>
<td>ib550</td>
<td>Infoblox-550 appliances</td>
</tr>
<tr>
<td>1202</td>
<td>ib1050</td>
<td>Infoblox-1050 appliances</td>
</tr>
<tr>
<td>1203</td>
<td>ib1550</td>
<td>Infoblox-1550 appliances</td>
</tr>
<tr>
<td>1204</td>
<td>ib1552</td>
<td>Infoblox-1552 appliances</td>
</tr>
<tr>
<td>1205</td>
<td>ib2000</td>
<td>Infoblox-2000 appliances</td>
</tr>
<tr>
<td>1206</td>
<td>ib250</td>
<td>Infoblox-250 appliances</td>
</tr>
<tr>
<td>1207</td>
<td>ib1220</td>
<td>Infoblox-1220 appliances</td>
</tr>
<tr>
<td>1301</td>
<td>ib550a</td>
<td>Infoblox-550-A appliances</td>
</tr>
<tr>
<td>1302</td>
<td>ib1050a</td>
<td>Infoblox-1050-A appliances</td>
</tr>
<tr>
<td>1303</td>
<td>ib1550a</td>
<td>Infoblox-1550-A appliances</td>
</tr>
<tr>
<td>1304</td>
<td>ib1552a</td>
<td>Infoblox-1552-A appliances</td>
</tr>
<tr>
<td>1305</td>
<td>ib1852a</td>
<td>Infoblox-1852-A appliances</td>
</tr>
<tr>
<td>1306</td>
<td>ib250a</td>
<td>Infoblox-250-A appliances</td>
</tr>
<tr>
<td>1307</td>
<td>ib2000a</td>
<td>Infoblox-2000-A appliances</td>
</tr>
<tr>
<td>1421</td>
<td>ib4010</td>
<td>Infoblox-4010 appliances</td>
</tr>
</tbody>
</table>
Infoblox MIBs

You can configure a NIOS appliance as an SNMP-managed device so that an SNMP management station can send queries to the appliance and retrieve information from its MIBs. Perform the following tasks to access the Infoblox MIBs:

1. Configure a NIOS appliance to accept queries, as described in Configuring SNMPv3 Users on page 896.
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
6. IB-DNSSERV-MIB.txt
7. IB-DHCPSERV-MIB.txt
8. IB-DHCPV6ONE-MIB.txt

In addition, if the SNMP manager toolkit you use requires a different MIB file naming convention, you can rename the MIB files accordingly.

NET-SNMP MIBs

NIOS appliances support NET-SNMP (formerly UCD-SNMP), a collection of applications used to implement the SNMP protocol. The NET-SNMP MIBs provide the top-level infrastructure for the SNMP MIB tree. They define, among other things, the objects in the SNMP traps that the agent sends when the SNMP engine starts and stops. For information about NET-SNMP and the MIB files distributed with NET-SNMP, refer to [http://net-snmp.sourceforge.net/](http://net-snmp.sourceforge.net/).

For SNMP traps to function properly, you must download the following NET-SNMP MIBs directly from [http://net-snmp.sourceforge.net/docs/mibs/](http://net-snmp.sourceforge.net/docs/mibs/):

- NET-SNMP-MIB
- UCD-SNMP-MIB

**Note:** Ensure that you save the MIBs as text files in the directory to which you save all the other MIB files.
BGP4 MIB

Infoblox supports BGP4 (Border Gateway Protocol) for DNS anycast addressing. BGP is configured to send SNMP traps to neighboring routers, as defined in RFC4273 Definitions of Managed Objects for BGP-4. You must enable and configure the SNMP trap receiver on the Grid member for the member to send SNMP traps. For information, see SNMP MIB Hierarchy on page 901.

The BGP protocol service is configured to send SNMP queries about BGP runtime data. The information is returned using the following OIDs and definitions:

<table>
<thead>
<tr>
<th>OID</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.2.1.15.900.1.1</td>
<td>Number of peers</td>
</tr>
<tr>
<td>1.3.6.1.2.1.15.900.1.2</td>
<td>Number of active peers</td>
</tr>
<tr>
<td>1.3.6.1.2.1.15.900.1.3</td>
<td>Number of AS path entries</td>
</tr>
<tr>
<td>1.3.6.1.2.1.15.900.1.4</td>
<td>Number of BGP community entries</td>
</tr>
<tr>
<td>1.3.6.1.2.1.15.900.1.5</td>
<td>Total number of prefixes</td>
</tr>
</tbody>
</table>

For each configured BGP peer (a, b, c, d), the information is returned using the following OIDs and definitions:

<table>
<thead>
<tr>
<th>OID</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.2.1.15.900.1.9.a.b.c.d.1</td>
<td>IP address: same as a.b.c.d</td>
</tr>
<tr>
<td>1.3.6.1.2.1.15.900.1.9.a.b.c.d.2</td>
<td>State: 0=down, 1=up</td>
</tr>
<tr>
<td>1.3.6.1.2.1.15.900.1.9.a.b.c.d.3</td>
<td>ASN</td>
</tr>
<tr>
<td>1.3.6.1.2.1.15.900.1.9.a.b.c.d.4</td>
<td>Prefixes</td>
</tr>
<tr>
<td>1.3.6.1.2.1.15.900.1.9.a.b.c.d.5</td>
<td>Up/Down time</td>
</tr>
</tbody>
</table>
ibTrap MIB

NIOS appliances send SNMP traps when events, internal process failures, or critical service failures occur. The ibTrap MIB defines the types of traps that a NIOS appliance sends and the value that each MIB object represents. The Infoblox SNMP traps report objects which the ibTrap MIB defines. Figure 34.3 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 34.3 ibTrapOne MIB Structure
Interpreting Infoblox SNMP Traps

Depending on the SNMP management application your management system uses, the SNMP traps you receive may list the OIDs for all relevant MIB objects from both the ibTrapOneModule and ibNotificationVarBind trees. For OIDs that have string values, the trap lists the text. For OIDs that contain integers, you can use the tables in this section to find out the values. Some SNMP management applications list only the object names and their corresponding values in the SNMP traps. Whether or not your SNMP management application lists OIDs, you can use the tables in this section to find out the corresponding value and definition for each MIB object.

The following is a sample trap 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 919.

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"`
    
    tells you the IP address of the appliance on which the trap occurred.

- **ibObjectName (OID 7779.3.1.1.1.2.3.0)**
  - The statement 
    
    `7779.3.1.1.1.2.3.0 = STRING: "ntp_sync"`
    
    tells you the MIB object ibObjectName, which is the name of the object for which the trap was generated, has a value of “ntp_sync” that indicates NTP synchronization issues.

- **ibPreviousState (OID 7779.3.1.1.1.2.9.0)**
  - The statement 
    
    `7779.3.1.1.1.2.9.0 = INTEGER: 15`
    
    tells you the MIB object ibPreviousState, which indicates the previous state of the appliance, has a value of 15. Using the `ibPreviousState and ibCurrentState Values` table, you know that 15 represents “ntp-sync-up”, which means the NTP server was up and running.

- **ibCurrentState (OID 7779.3.1.1.1.2.10.0)**
  - The statement 
    
    `7779.3.1.1.1.2.10.0 = INTEGER: 16`
    
    tells you the MIB object ibCurrentState, which indicates the current state of the appliance, has a value of 16. Using the `ibPreviousState and ibCurrentState Values` table, you know that 16 represents “ntp-sync-down”, which means the NTP server is now out of sync.

- **ibTrapDesc (OID 7779.3.1.1.1.2.11.0)**
  - The last statement 
    
    `7779.3.1.1.1.2.11.0 = STRING: "The NTP service is out of synchronization."`
    
    states the description of the trap. Using the `Object State Change Traps` table for ibTrapDesc, you can find out the trap description and recommended actions for this problem.
Types of Traps (OID 3.1.1.1.1)

ibTrapOneModule defines the types of traps that the NIOS appliance can send. There are five types of SNMP traps. Table 34.2 describe the types of traps and their objects in the ibTrapOneModule tree.

Table 34.2 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</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>• <code>ibNodeName</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <code>ibTrapSeverity</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <code>ibObjectName</code> (equipment name)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <code>ibProbableCause</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <code>ibTrapDesc</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For a list of trap descriptions, see Equipment Failure Traps on page 919.</td>
</tr>
<tr>
<td>3.1.1.1.2</td>
<td>Processing and Software Failure</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></td>
<td></td>
<td>• <code>ibNodeName</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <code>ibTrapSeverity</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <code>ibSubsystemName</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <code>ibProbableCause</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <code>ibTrapDesc</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For a list of trap descriptions, see Processing and Software Failure Traps on page 920.</td>
</tr>
</tbody>
</table>
### Threshold Crossing

**ibThresholdCrossingEvent** The NIOS appliance generates this trap when any of the following events occur:
- System memory or disk usage exceeds 90%.
- CPU usage exceeds the trigger value for 15 seconds.
- A problem occurs when the Grid Master replicates its database to its Grid members.
- DHCP address usage crosses a watermark threshold. For more information about tracking IP address usage, see *Threshold Crossing Traps* on page 926.
- The number or percentage of the DNS security alerts exceeds the thresholds of the DNS security alert triggers.

This trap includes the following objects:
- `ibNodeName`
- `ibTrapSeverity`
- `ibObjectName` (threshold name)
- `ibCurThresholdvalue`
- `ibThresholdHigh`
- `ibThresholdLow`
- `ibTrapDesc`

For a list of trap descriptions, see *Threshold Crossing Traps* on page 926.

### Object State Change

**ibStateChangeEvent** The NIOS appliance generates this trap when there is a change in its state, such as:
- The link to one of the configured ports goes down, and then goes back up again.
- A failover occurs in an HA (high availability) pair configuration.
- A member connects to the Grid Master.
- An appliance in a Grid goes offline.

This trap includes the following objects:
- `ibNodeName`
- `ibTrapSeverity`
- `ibObjectName`
- `ibPreviousState`
- `ibCurrentState`
- `ibTrapDesc`

For a list of possible trap descriptions, see *Object State Change Traps* on page 932.
### Monitoring with SNMP

When 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 timeout 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 934.

### ibRevokedLicenseTrap

The NIOS appliance generates this trap when a license is revoked.

This trap includes the following objects:
- `ibNodeName`
- `ibTrapSeverity`
- `ibSubsystemName`
- `ibTrapDesc`

<table>
<thead>
<tr>
<th>OID</th>
<th>Trap Type</th>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
</table>
| 3.1.1.1.5    | Process Started and Stopped | ibProcStartStopTrap | 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 timeout 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 934. |
| 3.1.1.1.6    | ibRevokedLicenseTrap       |                     | The NIOS appliance generates this trap when a license is revoked.  
This trap includes the following objects:  
- `ibNodeName`
- `ibTrapSeverity`
- `ibSubsystemName`
- `ibTrapDesc` |
### 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 34.3 describes the objects in the `ibNotificationVarBind` module.

#### Table 34.3 `ibNotificationVarBind` (OID 3.1.1.1.2)

<table>
<thead>
<tr>
<th>OID</th>
<th>MIB Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1.1.2.1.0</td>
<td>ibNodeName (DisplayString)</td>
<td>The IP address of the appliance on which the trap occurs. This may or may not be the same as the appliance that sends the trap. This object is used in all types of traps.</td>
</tr>
<tr>
<td>3.1.1.1.2.2.0</td>
<td>ibTrapSeverity (Integer)</td>
<td>The severity of the trap. There are five levels of severity. See Trap Severity (OID 3.1.1.1.2.2.0) on page 912 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 913 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 915 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) | This object is used in Threshold Crossing traps. For CPU usage, this is the trigger value of the SNMP trap. For DHCP address usage, this is the value of the high watermark. This only applies when the appliance sends a trap to indicate that DHCP address usage is above the configured high watermark value for a DHCP address range. For more information, see Threshold Crossing Traps on page 926. |
| 3.1.1.1.2.8.0 | ibThresholdLow (Integer) | This object is used in Threshold Crossing traps. For CPU usage, this is the reset value of the SNMP trap. For DHCP address usage, this is the value for the low watermark. This only applies when the appliance sends a trap to indicate that DHCP address usage went below the configured low watermark value for a DHCP address range. For more information, see Threshold Crossing Traps on page 926. |
| 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 917 for definitions of each value. |

**Note:** The OIDs shown in the following table do not include the prefix “.1.3.6.1.4.1.7779.”.
Monitoring with SNMP

<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>ibCurrentState (Integer)</td>
<td>The current state of the appliance. This object is used in the Object State Change traps. See <em>ibPreviousState (OID 3.1.1.1.2.9.0)</em> and <em>ibCurrentState (OID 3.1.1.1.2.10.0)</em> on page 917 for the definition of each value.</td>
</tr>
<tr>
<td>3.1.1.1.2.11.0</td>
<td>ibTrapDesc (DisplayString)</td>
<td>The description of the trap. This object is used in all types of traps. See <em>ibTrapDesc (OID 3.1.1.1.2.11.0)</em> on page 919 for the description, possible cause, and recommended actions for each Infoblox SNMP trap.</td>
</tr>
</tbody>
</table>

**Trap Severity (OID 3.1.1.1.2.2.0)**

The object `ibTrapSeverity` defines the severity level for each Infoblox SNMP trap. There are five levels of severity.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Undetermined</td>
</tr>
<tr>
<td>2</td>
<td>Informational: Event that requires no further action.</td>
</tr>
<tr>
<td>3</td>
<td>Minor: Event that does not require user intervention.</td>
</tr>
<tr>
<td>4</td>
<td>Major: Event that requires user intervention and assistance from Infoblox Technical Support.</td>
</tr>
<tr>
<td>5</td>
<td>Critical: Problem that affects services and system operations, and requires assistance from Infoblox Technical Support.</td>
</tr>
</tbody>
</table>
**ibProbableCause Values (OID 3.1.1.2.4.0)**

*Table 34.5* 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 34.4  *ibProbableCause Values

<table>
<thead>
<tr>
<th>Value</th>
<th>OID 3.1.1.2.4.0  ibProbableCause</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>ibClear</td>
</tr>
<tr>
<td>1</td>
<td>ibUnknown</td>
</tr>
<tr>
<td>2</td>
<td>ibPrimaryDiskFailure</td>
</tr>
<tr>
<td>3</td>
<td>ibFanFailure-old</td>
</tr>
<tr>
<td>4</td>
<td>ibPowerSupplyFailure</td>
</tr>
<tr>
<td>5</td>
<td>ibDBFailure</td>
</tr>
<tr>
<td>6</td>
<td>ibApacheSoftwareFailure</td>
</tr>
<tr>
<td>7</td>
<td>ibSerialConsoleFailure</td>
</tr>
<tr>
<td>11</td>
<td>ibControldSoftwareFailure</td>
</tr>
<tr>
<td>12</td>
<td>ibUpgradeFailure</td>
</tr>
<tr>
<td>13</td>
<td>ibSNMPDFailure</td>
</tr>
<tr>
<td>15</td>
<td>ibSSHDSoftwareFailure</td>
</tr>
<tr>
<td>16</td>
<td>ibNTPDSoftwareFailure</td>
</tr>
<tr>
<td>17</td>
<td>ibClusterdSoftwareFailure</td>
</tr>
<tr>
<td>18</td>
<td>ibLCDSoftwareFailure</td>
</tr>
<tr>
<td>19</td>
<td>ibDHCPdSoftwareFailure</td>
</tr>
<tr>
<td>20</td>
<td>ibNamedSoftwareFailure</td>
</tr>
<tr>
<td>21</td>
<td>ibAuthServerGroupDown</td>
</tr>
<tr>
<td>22</td>
<td>ibAuthServerGroupUp</td>
</tr>
<tr>
<td>24</td>
<td>ibNTLMSoftwareFailure</td>
</tr>
<tr>
<td>25</td>
<td>ibNetBIOSDaemonFailure</td>
</tr>
<tr>
<td>26</td>
<td>ibWindowBindDaemonFailure</td>
</tr>
<tr>
<td>27</td>
<td>ibTFTPDSoftwareFailure</td>
</tr>
<tr>
<td>29</td>
<td>ibBackupSoftwareFailure</td>
</tr>
<tr>
<td>30</td>
<td>ibBackupDatabaseSoftwareFailure</td>
</tr>
<tr>
<td>31</td>
<td>ibBackupModuleSoftwareFailure</td>
</tr>
<tr>
<td>32</td>
<td>ibBackupSizeSoftwareFailure</td>
</tr>
<tr>
<td>33</td>
<td>ibBackupLockSoftwareFailure</td>
</tr>
<tr>
<td>34</td>
<td>ibHTTPFileDistSoftwareFailure</td>
</tr>
<tr>
<td>Value</td>
<td>OID 3.1.1.2.4.0</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------</td>
</tr>
<tr>
<td>35</td>
<td>ibOSPFSoftwareFailure</td>
</tr>
<tr>
<td>36</td>
<td>ibAuthDHCPTenantSoftwareFailure</td>
</tr>
<tr>
<td>37</td>
<td>ibFan1Failure</td>
</tr>
<tr>
<td>38</td>
<td>ibFan2Failure</td>
</tr>
<tr>
<td>39</td>
<td>ibFan3Failure</td>
</tr>
<tr>
<td>40</td>
<td>ibFan1OK</td>
</tr>
<tr>
<td>41</td>
<td>ibFan2OK</td>
</tr>
<tr>
<td>42</td>
<td>ibFan3OK</td>
</tr>
<tr>
<td>44</td>
<td>ibFTPSsoftwareFailure</td>
</tr>
<tr>
<td>46</td>
<td>ibPowerSupplyOK</td>
</tr>
<tr>
<td>47</td>
<td>ibWebUISoftwareFailure</td>
</tr>
<tr>
<td>49</td>
<td>ibADAgentSyncFailure</td>
</tr>
<tr>
<td>50</td>
<td>ibIFMAPSoftwareFailure</td>
</tr>
<tr>
<td>51</td>
<td>ibCaptivePortalSoftwareFailure</td>
</tr>
<tr>
<td>52</td>
<td>ibDuplicateIPAddressFailure</td>
</tr>
<tr>
<td>53</td>
<td>ibBGPSoftwareFailure</td>
</tr>
<tr>
<td>54</td>
<td>ibRevokedLicense</td>
</tr>
<tr>
<td>58</td>
<td>ibGUILoginFailure</td>
</tr>
<tr>
<td>59</td>
<td>ibSerialConsoleLoginFailure</td>
</tr>
<tr>
<td>60</td>
<td>ibSystemReboot</td>
</tr>
<tr>
<td>61</td>
<td>ibSystemRestart</td>
</tr>
<tr>
<td>62</td>
<td>ibZoneTransferFailure</td>
</tr>
<tr>
<td>63</td>
<td>ibDHCPLeaseConflict</td>
</tr>
<tr>
<td>64</td>
<td>ibDHCPAddressConflict</td>
</tr>
<tr>
<td>65</td>
<td>ibDHCPRangeConflict</td>
</tr>
<tr>
<td>66</td>
<td>ibDHCPHostConflict</td>
</tr>
<tr>
<td>67</td>
<td>ibSyslogFailure</td>
</tr>
<tr>
<td>2029</td>
<td>ibHSMGroupFailure</td>
</tr>
<tr>
<td>2030</td>
<td>ibHSMGroupOK</td>
</tr>
<tr>
<td>2035</td>
<td>ibHAStateActiveActive</td>
</tr>
<tr>
<td>3001</td>
<td>ibRAIDIsOptimal</td>
</tr>
<tr>
<td>3002</td>
<td>ibRAIDIsDegraded</td>
</tr>
<tr>
<td>3003</td>
<td>ibRAIDIsRebuilding</td>
</tr>
</tbody>
</table>
### ibSubsystemName Values (OID 3.1.1.1.2.9.0)

*Table 34.5* 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 3.1.1.1.2.9.0 ibSubsystemName</th>
</tr>
</thead>
<tbody>
<tr>
<td>3004</td>
<td>ibRAIDStatusUnknown</td>
</tr>
<tr>
<td>3005</td>
<td>ibRAIDBatteryIsOK</td>
</tr>
<tr>
<td>3006</td>
<td>ibRAIDBatteryFailed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Value</th>
<th>OID 3.1.1.1.2.9.0 ibSubsystemName</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Uses the original ibObjectName and ibSubsystemName when the trap is cleared. The process failure trap is appended to the CLEAR trap descriptions.</td>
</tr>
<tr>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>2</td>
<td>N/A</td>
</tr>
<tr>
<td>3</td>
<td>N/A</td>
</tr>
<tr>
<td>4</td>
<td>N/A</td>
</tr>
<tr>
<td>5</td>
<td>Db_jnld</td>
</tr>
<tr>
<td>6</td>
<td>httpd</td>
</tr>
<tr>
<td>7</td>
<td>serial_console</td>
</tr>
<tr>
<td>11</td>
<td>controld</td>
</tr>
<tr>
<td>12</td>
<td>N/A</td>
</tr>
<tr>
<td>13</td>
<td>Snmpd</td>
</tr>
<tr>
<td>15</td>
<td>Sshd</td>
</tr>
<tr>
<td>16</td>
<td>Ntpd</td>
</tr>
<tr>
<td>17</td>
<td>Clusterd</td>
</tr>
<tr>
<td>18</td>
<td>Lcd</td>
</tr>
<tr>
<td>19</td>
<td>Dhcpd</td>
</tr>
<tr>
<td>20</td>
<td>Named</td>
</tr>
<tr>
<td>24</td>
<td>NTLM</td>
</tr>
<tr>
<td>25</td>
<td>Netbiosd</td>
</tr>
<tr>
<td>26</td>
<td>Winbinddd</td>
</tr>
<tr>
<td>27</td>
<td>Tftpd</td>
</tr>
<tr>
<td>Value</td>
<td>OID 3.1.1.1.2.9.0 ibSubsystemName</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>29</td>
<td>N/A</td>
</tr>
<tr>
<td>30</td>
<td>N/A</td>
</tr>
<tr>
<td>31</td>
<td>N/A</td>
</tr>
<tr>
<td>32</td>
<td>N/A</td>
</tr>
<tr>
<td>33</td>
<td>N/A</td>
</tr>
<tr>
<td>34</td>
<td>HTTPd</td>
</tr>
<tr>
<td>35</td>
<td>OSPF</td>
</tr>
</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 34.6* shows the message and description for each state.

*Table 34.6  ibPreviousState and ibCurrentState Values*

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>None</td>
<td>No previous state.</td>
</tr>
<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>
<tr>
<td>17</td>
<td>ms-server-up</td>
<td>Microsoft server is active</td>
</tr>
<tr>
<td>18</td>
<td>ms-server-down</td>
<td>Microsoft server is inactive</td>
</tr>
<tr>
<td>19</td>
<td>ms-service-up</td>
<td>Microsoft service connection is up</td>
</tr>
<tr>
<td>20</td>
<td>ms-service-down</td>
<td>Microsoft service connection is down</td>
</tr>
<tr>
<td>21</td>
<td>nac-server-group-down</td>
<td>NAC Authentication server group is down</td>
</tr>
<tr>
<td>22</td>
<td>nac-server-group-up</td>
<td>NAC Authentication server group is up</td>
</tr>
<tr>
<td>2029</td>
<td>hsm-group-failure</td>
<td>HSM operation failed</td>
</tr>
<tr>
<td>2030</td>
<td>hsm-group-up</td>
<td>HSM operation succeeded</td>
</tr>
<tr>
<td>23</td>
<td>mgm-service-up</td>
<td>MGM service is active</td>
</tr>
<tr>
<td>24</td>
<td>mgm-service-down</td>
<td>MGM service is inactive</td>
</tr>
<tr>
<td>25</td>
<td>ha-active-active</td>
<td>HA Pair in Dual Active</td>
</tr>
<tr>
<td>26</td>
<td>ftp-service-working</td>
<td>FTP service is working</td>
</tr>
<tr>
<td>27</td>
<td>ftp-service-failed</td>
<td>FTP service failed</td>
</tr>
<tr>
<td>Value</td>
<td>Description</td>
<td>Definition</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>28</td>
<td>ftp-service-inactive</td>
<td>FTP service is inactive</td>
</tr>
<tr>
<td>29</td>
<td>tftp-service-working</td>
<td>TFTP service is working</td>
</tr>
<tr>
<td>30</td>
<td>tftp-service-failed</td>
<td>TFTP service failed</td>
</tr>
<tr>
<td>31</td>
<td>tftp-service-inactive</td>
<td>TFTP service is inactive</td>
</tr>
<tr>
<td>32</td>
<td>dns-service-working</td>
<td>DNS service is working</td>
</tr>
<tr>
<td>33</td>
<td>dns-service-failed</td>
<td>DNS service failed</td>
</tr>
<tr>
<td>34</td>
<td>dns-service-inactive</td>
<td>DNS service is inactive</td>
</tr>
<tr>
<td>35</td>
<td>ntp-service-working</td>
<td>NTP service is working</td>
</tr>
<tr>
<td>36</td>
<td>ntp-service-failed</td>
<td>NTP service failed</td>
</tr>
<tr>
<td>37</td>
<td>ntp-service-inactive</td>
<td>NTP service is inactive</td>
</tr>
<tr>
<td>38</td>
<td>http-file-dist-service-working</td>
<td>HTTP File Dist service is working</td>
</tr>
<tr>
<td>39</td>
<td>http-file-dist-service-failed</td>
<td>HTTP File Dist service failed</td>
</tr>
<tr>
<td>40</td>
<td>http-file-dist-service-inactive</td>
<td>HTTP File Dist service is inactive</td>
</tr>
<tr>
<td>41</td>
<td>bloxtools-service-working</td>
<td>bloxTools service is working</td>
</tr>
<tr>
<td>42</td>
<td>bloxtools-service-warnin</td>
<td>bloxTools service is in warning state</td>
</tr>
<tr>
<td>43</td>
<td>bloxtools-service-failed</td>
<td>bloxTools service failed</td>
</tr>
<tr>
<td>44</td>
<td>bloxtools-service-inactive</td>
<td>bloxTools service is inactive</td>
</tr>
<tr>
<td>45</td>
<td>dhcp-service-working</td>
<td>DHCP service is working</td>
</tr>
<tr>
<td>46</td>
<td>dhcp-service-warning</td>
<td>DHCP service is in warning state</td>
</tr>
<tr>
<td>47</td>
<td>dhcp-service-failed</td>
<td>DHCP service failed</td>
</tr>
<tr>
<td>48</td>
<td>dhcp-service-inactive</td>
<td>DHCP service is inactive</td>
</tr>
</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>ibTrapServerity 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>
</tbody>
</table>

**Fan Monitoring**

| Fan <n>failure has occurred. | Minor | The specified fan failed. The fan number <n> can be 1, 2, or 3. | Inspect the specified fan for mechanical or electrical problems. |
| Fan <n>is OK.                | Informational | The specified fan is functioning properly. The fan number <n> can be 1, 2, or 3. | No action is required. |

**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><code>ibTrapDesc OID 3.1.1.1.2.11.0</code></th>
<th><code>ibTrapServerity OID 3.1.1.1.2.2</code></th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>A RAID battery failure has occurred.</td>
<td>Major</td>
<td>The system RAID battery failed. The alert light is red.</td>
<td>Inspect the battery for the possible cause of the failure.</td>
</tr>
<tr>
<td>The system’s RAID battery is OK.</td>
<td>Informational</td>
<td>The system RAID battery is charging and functioning properly. The alert light changed from red to green.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Unable to retrieve RAID array state!</td>
<td>Undetermined</td>
<td>The appliance failed to retrieve the RAID array state. The alert light is red.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>The system’s RAID array is now running in an optimal state.</td>
<td>Informational</td>
<td>The RAID system is functioning at an optimal state.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>The system’s RAID array is in a degraded state.</td>
<td>Major</td>
<td>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.</td>
<td>Minor</td>
<td>The RAID system is rebuilding.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

### Processing and Software Failure Traps

<table>
<thead>
<tr>
<th><code>ibTrapDesc OID 3.1.1.1.2.11.0</code></th>
<th><code>ibTrapServerity OID 3.1.1.1.2.2</code></th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Named Daemon Failure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A named daemon monitoring failure has occurred.</td>
<td>Critical</td>
<td>The named process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>DHCP Daemon Failure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A DHCP daemon monitoring failure has occurred.</td>
<td>Critical</td>
<td>The dhcpd process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>SSH Daemon Failure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>An SSH daemon failure has occurred.</td>
<td>Major</td>
<td>The sshd process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>NTP Daemon Failure, monitored every 10 minutes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>An NTP daemon failure has occurred.</td>
<td>Major</td>
<td>The ntpd process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Trap Description</td>
<td>Trap Severity</td>
<td>Description/Cause</td>
<td>Recommended Actions</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------</td>
<td>------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Cluster Daemon Failure</td>
<td>Critical</td>
<td>The clusterd process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>LCD Daemon Failure</td>
<td>Major</td>
<td>The LCD process failed. The alert light is yellow.</td>
<td>1. Inspect the LCD panel for the possible cause of this problem. 2. Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Apache Software httpd failure, monitored every 2 minutes</td>
<td>Critical</td>
<td>The request to monitor the Apache server failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Serial Console Failure</td>
<td>Major</td>
<td>The Infoblox serial console failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Controld Software Failure</td>
<td>Critical</td>
<td>The controld process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>SNMP Sub-agent Failure</td>
<td>Major</td>
<td>The one-subagent process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>TFTPD and FTPD Failure</td>
<td>Critical</td>
<td>The tftpd process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>HTTP File Distribution, monitored at 10 second intervals</td>
<td>Critical</td>
<td>The HTTP file distribution process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>auth_named Process Failure</td>
<td>Critical</td>
<td>The auth_named server failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>DNS ONE quagga Processes (zebra &amp; ospfd)</td>
<td>Critical</td>
<td>Either the zebra process or the ospfd process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>
| **ibTrapDesc**  
| OID 3.1.1.1.2.11.0 | **ibTrapServertity**  
| OID 3.1.1.1.2.2 | **Description/Cause** | **Recommended Actions** |
|---------------------|---------------------|---------------------|---------------------|
| **Backup Failure** | **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** | **Module backup failed.** | **Not implemented** | **The backup of product-specific files failed.**  
| | | | **Review the syslog file to identify the possible cause of this problem.** |
| **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.**  
<p>| | | | <strong>Wait until the backup or restore is complete before starting another backup.</strong> |</p>
<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.2.11.0</th>
<th>ibTrapServerity OID 3.1.1.1.2</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Watchdog Process Monitoring</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| WATCHDOG: <registered client name> failed on <server IP address> | Critical | The watchdog process detected a registered client failure on a specific server. The <registered client name> could be one of the following:  
• Clusterd _timeout  
• DB_Sentinel  
• Process_Manager  
• Clusterd_monitor  
• Disk_monitor | Review the syslog file to identify the possible cause of this problem. |
<p>| <strong>Microsoft Server</strong> |                               |                   |                     |
| Microsoft server hostname has failed. | Major | The Microsoft server could not be reached. | Check that the Microsoft server is connected to the network and configured properly. |
| Microsoft server hostname is OK. | Informational | The Microsoft server can be reached and is functioning properly | No action is required. |
| <strong>Microsoft DNS/DHCP Service</strong> |                               |                   |                     |
| Service connection to Microsoft DNS server hostname has failed. | Major | The Microsoft DNS service is not responding. | Check that the DNS service is configured and running on the Microsoft server. |
| Service connection to Microsoft DHCP server hostname has failed. | Major | The Microsoft DHCP service is not responding. | Check that the DHCP service is configured and running on the Microsoft server. |
| Service connection to Microsoft DNS server hostname is OK. | Informational | The Microsoft DNS service is responding. | No action is required. |
| Service connection to Microsoft DHCP server hostname is OK. | Informational | The Microsoft DHCP service is responding. | No action is required. |</p>
<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.2.11.0</th>
<th>ibTrapServery OID 3.1.1.1.2.2</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAC Authentication Server Group</td>
<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>
</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>

**GUI Login**

| Major | An admin failed to log in to the GUI. | An admin failed to log in to the GUI. | Check the credentials of the admin. |

**Serial Console Login**

| Major | An admin failed to log in through the serial console. | Check the credentials and permissions, and check that the serial console is enabled. |

**Reboot**

| Major | A system reboot was initiated. | A system reboot command was sent. | No action is required. |

**DHCP Lease Conflict**

| Major | The discovery process found a DHCP lease conflict. | In the IP Map or List panel, select a conflicting address, and then click Resolve Conflict. For more information, see Resolving DHCP Lease Conflicts on page 861 |

**DHCP Fixed Address Conflict**

| Major | The discovery process found a fixed address conflict. | In the IP Map or List panel, select a conflicting address, and then click Resolve Conflict. For more information, see Resolving Fixed Address Conflicts on page 862 |

**DHCP Range Conflict**

| Major | The discovery process found a conflict with an existing range. | In the IP Map or List panel, select a conflicting address, and then click Resolve Conflict. For more information, see Resolving DHCP Range Conflicts on page 862 |

**DHCP Host Conflict**

<p>| Major | The discovery process found a conflict with an existing host address. | In the IP Map or List panel, select a conflicting address, and then click Resolve Conflict. For more information, see Resolving Host Conflicts on page 862 |</p>
<table>
<thead>
<tr>
<th>ibTrapDesc</th>
<th>ibTrapSeverity</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID 3.1.1.1.2.11.0</td>
<td>OID 3.1.1.1.2.2</td>
<td>Syslog Daemon Failure</td>
<td>A syslog daemon failure occurred. Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Process Stop/Start</td>
<td>Major</td>
<td>The system stopped and started a process.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Zone Transfer Failed</td>
<td>Major</td>
<td>A zone transfer failure occurred.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>
## Threshold Crossing Traps

<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.2.11.0</th>
<th>ibTrapSeverity</th>
<th>ibObjectName OID 3.1.1.1.2.3.0</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Memory Usage</td>
<td>Major</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></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></td>
<td>• The total physical memory was less than the total free memory.</td>
<td></td>
</tr>
<tr>
<td></td>
<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></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></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></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</th>
<th>ibTrapSeverity</th>
<th>ibObjectName OID</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
</table>
| 3.1.1.1.2.11.0 | Minor          | memory           | The memory usage on the appliance exceeded the configured Trigger value. For more information, see [*Defining Thresholds for Traps*](#) on page 899. 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 usage is over the configured Trigger value. | Minor | memory | The memory usage on the system is at or below the Reset value after it went above the Trigger value. | No action is required. |
Primary Hard Drive Usage (monitored every 30 seconds)

<table>
<thead>
<tr>
<th>Description/Cause</th>
<th>ibTrapSeverity</th>
<th>ibObjectName OID</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>System primary hard disk usage is over the configured Trigger value. The default value is 85.</td>
<td>Minor</td>
<td>disk usage</td>
<td>The appliance sends this trap when primary hard disk usage first exceeds the configured Trigger value. The alert light is yellow. For more information, see <strong>Defining Thresholds for Traps</strong> on page 899.</td>
</tr>
<tr>
<td>Primary drive is full.</td>
<td>Major</td>
<td>disk usage</td>
<td>The primary hard disk usage exceeded 95%. The alert light is red.</td>
</tr>
<tr>
<td>Primary drive usage is OK.</td>
<td>Minor</td>
<td>disk usage</td>
<td>The appliance sends this trap when the primary hard disk usage first moves at or below the configured Reset value after it exceeded the Trigger value. The default is 70. The alert light is green.</td>
</tr>
</tbody>
</table>

**CPU Usage**

<table>
<thead>
<tr>
<th>Description/Cause</th>
<th>ibTrapSeverity</th>
<th>ibObjectName OID</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU usage above threshold value.</td>
<td>Major</td>
<td>cpu usage</td>
<td>CPU usage exceeded the trigger value for 15 seconds. For more information, see <strong>Defining Thresholds for Traps</strong> on page 899.</td>
</tr>
<tr>
<td>CPU usage OK.</td>
<td>Minor</td>
<td>cpu usage</td>
<td>CPU usage dipped below the reset value after the “CPU usage above threshold value” trap was sent.</td>
</tr>
</tbody>
</table>

**Note:** Use the CLI command `set thresholdtrap` to enable the CPU usage trap and configure the trigger and reset values. For information, refer to the **Infoblox CLI Guide**.

Replication Statistics Monitoring

<table>
<thead>
<tr>
<th>Description/Cause</th>
<th>ibObjectName OID</th>
<th>Recommended Actions</th>
</tr>
</thead>
</table>
| Grid queue replication problem. | | The system encountered this problem when all of the following conditions occurred:  
• The node was online.  
• The number of the replication queue being sent from the master column was greater than 0, or the number of the queue received was greater than 0.  
• It was more than 10 minutes since the last replication queue was sent and monitored. | Review the syslog file to identify the possible cause of this problem. |
<table>
<thead>
<tr>
<th>ibTrapDesc OID</th>
<th>ibTrapSeverity</th>
<th>ibObjectName OID</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1.1.2.11.0</td>
<td>N/A</td>
<td>3.1.1.1.2.3.0</td>
<td>Threshold</td>
<td></td>
</tr>
</tbody>
</table>

**DHCP Range Threshold Crossing**

- **Member:** `<DHCP server node VIP>`
- **Network:** `<network> / <network view>`
- **Range:** `<DHCP range> / <network view>`
- **High:** `<high percentage>` (95% by default)
- **Low:** `<low percentage>` (0% by default)
- **Current Usage:** `<current usage percentage>`
- **Active Leases:** `<number of active leases>`
- **Available Leases:** `<number of available leases>`
- **Total Addresses:** `<total addresses>`

- The system encountered this problem when one of the following conditions occurred:
  - The address usage in the DHCP range is greater than the configured High Trigger value and when it first dips below the Reset value after it hit the Trigger value.
  - The address usage in the DHCP range goes below the Low Trigger value and when it first goes above the Reset value after it hit the Trigger value.

- Review the syslog file to identify the possible cause of this problem.

**DHCP DDNS Updates Deferred**

- **Retried at least once:** `<number of retries>`
- **Maximum number of deferred updates since start of problem episode (or restart):** `<max number>`

- **Threshold**
- The DNS updates were deferred because of DDNS update errors.

- Review the syslog file to identify the possible cause of this problem.
### Database Capacity Usage

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minor</td>
<td>Over 85% database capacity used.</td>
<td>Increase the database capacity.</td>
</tr>
<tr>
<td>Minor</td>
<td>Database capacity used is OK.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

### DNS Monitor

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
</table>
| Major    | For invalid ports: "dns_security_port" For invalid TXIDs: "dns_security_txid" | DNS security alert. There were actual DNS responses to {invalid ports with invalid TXID} in the last minute, comprising percent% of all responses. Primary sources: ip_address sent count, ip_address sent count. where  
  - actual is the total number of DNS responses arrive on invalid ports or have invalid TXIDs.  
  - percent% is the percentage of invalid DNS responses over the total number of DNS responses.  
  - ip_address is the IP address of the primary source that generated the invalid DNS responses.  
  - count is the number of invalid responses generated by the specified IP address.  
  Example: DNS security alert. There were 1072 DNS responses to invalid ports in the last minute, comprising 92% of all responses. Primary sources: 10.0.0.0 sent 1058, 2.2.2.2 sent 14. | 1. Review the following:  
  - DNS alert status  
  - syslog file  
  2. Limit access or block connections from the primary sources. For information, see Configuring Rate Limiting Rules on page 891. |
<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.2.11.0</th>
<th>ibTrapSeverity</th>
<th>ibObjectName OID 3.1.1.1.2.3.0</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RootFS Partition Monitor</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Root file system is full.</td>
<td>Major</td>
<td>Root filesystem</td>
<td>The Root filesystem usage exceeded the maximum.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Root file system disk usage is over the configured Trigger value.</td>
<td>Minor</td>
<td>Root filesystem</td>
<td>The appliance sends this trap when the Root filesystem usage first exceeds the configured Trigger value.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Root file system disk usage is OK.</td>
<td>Minor</td>
<td>Root filesystem</td>
<td>The appliance sends this trap when the Root filesystem disk usage first moves at or below the configured Reset value after it exceeded the Trigger value. For information on setting the Trigger and Reset values, see Defining Thresholds for Traps on page 899.</td>
<td>No action</td>
</tr>
<tr>
<td><strong>Reporting</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reporting drive is full.</td>
<td>Major</td>
<td>Reporting</td>
<td>Reporting drive reached the maximum capacity.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Reporting drive usage is over the configured Trigger value.</td>
<td>Minor</td>
<td>Reporting</td>
<td>The appliance sends this trap when the Reporting volume first exceeds the configured Trigger value. The default Trigger value is 80.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Reporting drive usage is OK.</td>
<td>Minor</td>
<td>Reporting</td>
<td>The appliance sends this trap when the Reporting volume first moves at or below the configured Reset value after it exceeded the Trigger value. The default Reset value is 71. For information on setting the Trigger and Reset values, see Defining Thresholds for Traps on page 899.</td>
<td>No action</td>
</tr>
</tbody>
</table>
## Object State Change Traps

<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.2.11.0</th>
<th>ibTrapSeverity</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Shutdown</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shutting down services due to database snapshot.</td>
<td>Major</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>Major</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>
<td></td>
</tr>
<tr>
<td>LAN port link is down. Please check the connection.</td>
<td>Major</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>Major</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>Major</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>Major</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>Major</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>Major</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>
<td></td>
</tr>
<tr>
<td>The node has become ACTIVE.</td>
<td>Informational</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>
<td></td>
</tr>
<tr>
<td>The node has become ACTIVE.</td>
<td>Informational</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 to Active-Active</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The node is in an ACTIVE-ACTIVE state.</td>
<td>Informational</td>
<td>The node is in the active state.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><strong>HA State Change from Initial to Passive</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ibTrapDesc OID 3.1.1.1.2.11.0</td>
<td>ibTrapSeverity</td>
<td>Description/Cause</td>
<td>Recommended Actions</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------</td>
<td>-------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>The node has become PASSIVE.</td>
<td>Informational</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>
<tr>
<td>Node Connected to Grid</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Grid member is connected to the Grid Master.</td>
<td>Informational</td>
<td>The Grid member joined the Grid, and it is not a Grid Master candidate.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Node Disconnected from Grid</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Grid member is not connected to the Grid Master.</td>
<td>Informational</td>
<td>The Grid member lost its connection to the Grid Master.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Replication State Monitoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ha-replication-online (13)</td>
<td>Informational</td>
<td>The HA replication is online.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>ha-replication-offline (14)</td>
<td>Informational</td>
<td>The HA replication is offline.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>NTP is out of sync, monitored every 30 seconds</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The NTP server is out of synchronization.</td>
<td>Major</td>
<td>The Infoblox NTP server and the external NTP server are not synchronized.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>DHCP service state change</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP service returned to working state.</td>
<td>Informational</td>
<td>The DHCP service started working again.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>DHCP service is in a warning state</td>
<td>Informational</td>
<td>The DHCP service is in a warning state.</td>
<td>Review the syslog file</td>
</tr>
<tr>
<td>DHCP service became inactive.</td>
<td>Informational</td>
<td>The DHCP service became inactive.</td>
<td>Check if an admin disabled the service.</td>
</tr>
<tr>
<td>DNS service state change</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS service returned to working state.</td>
<td>Informational</td>
<td>The DNS service started working again.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>DNS service is in a warning state</td>
<td>Informational</td>
<td>The DNS service is in a warning state.</td>
<td>Review the syslog file</td>
</tr>
<tr>
<td>DNS service became inactive.</td>
<td>Informational</td>
<td>The DNS service became inactive.</td>
<td>Check if an admin disabled the service.</td>
</tr>
<tr>
<td>NTP service state change</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP service returned to working state.</td>
<td>Informational</td>
<td>The NTP service started working again.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>
Monitoring with SNMP

<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.2.11.0</th>
<th>ibTrapSeverity</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP service became inactive.</td>
<td>Informational</td>
<td>The NTP service became inactive.</td>
<td>Check if an admin disabled the service.</td>
</tr>
</tbody>
</table>

**TFTP service state change**

| TFTP service returned to working state. | Informational | The TFTP service started working again. | No action is required. |
| TFTP service became inactive. | Informational | The TFTP service became inactive. | Check if an admin disabled the service. |

**FTP service state change**

| FTP service returned to working state. | Informational | The FTP service started working again. | No action is required. |
| FTP service became inactive. | Informational | The FTP service became inactive. | Check if an admin disabled the service. |

**HTTP service state change**

| HTTP service returned to working state. | Informational | The HTTP service started working again. | No action is required. |

**bloxTools service state change**

| bloxTools service returned to working state. | Informational | The bloxTools service started working again. | No action is required. |
| bloxTools service is in a warning state | Informational | The bloxTools service is in a warning state. | Review the syslog file |
| bloxTools service became inactive. | Informational | The bloxTools service became inactive. | Check if an admin disabled the service. |
| bloxTools service failed. | Critical | The bloxTools daemon failed | Review the syslog file |

**Process Started and Stopped Traps**

<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.2.11.0</th>
<th>ibTrapSeverity</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Httpd Start</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The process started normally.</td>
<td>Informational</td>
<td>The httpd process started.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Httpd Stop</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The process stopped normally.</td>
<td>Informational</td>
<td>The httpd process stopped.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Process Stop/Start</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system stopped and started a process.</td>
<td>Major</td>
<td>The system restarted a process.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Zone Transfer Failed</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Revoked License Trap

<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.2.11.0</th>
<th>ibTrapSeverity</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>This trap is generated when a license is revoked</td>
<td>Critical</td>
<td>A license was revoked</td>
<td>Obtain and install new license</td>
</tr>
</tbody>
</table>

| A zone transfer failure occurred. | Critical | A zone transfer failed. | Review the syslog file       |

**Description/Cause**

Revoked License Trap
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 34.4 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 938.
- ibNetworkMonitor provides information about the average latency of authoritative and nonauthoritative replies to DNS queries for different time intervals. It also provides information about invalid DNS responses that arrive on invalid ports or have invalid DNS transaction IDs. For information, see ibNetwork Monitor on page 939.
- ibHardwareType (IbString) provides information about the hardware platform. For an Infoblox appliance, it provides the model number of the Infoblox hardware platform. For vNIOS appliances, it identifies whether the hardware platform is Riverbed or VMware.
- ibHardwareId (IbString) provides the hardware ID of the NIOS appliance.
- ibSerialNumber (IbString) provides the serial number of the Infoblox hardware platform.
- ibNiosVersion (IbString) provides the version of the NIOS software.
- ibSystemMonitor provides information about the CPU and memory utilization of the appliance. For information, see ibSystemMonitor on page 945.
- ibGridStatus provides information about an appliance. It indicates whether the appliance is a Grid Master, member, or an independent appliance.
- ibHASStatus provides information about the HA status of a member. It indicates if the member is part of an HA configuration, and if it is the active or passive node.
- ibGridMasterCandStatus indicates if a member is a Grid Master candidate.
- ibGridMasterVIP provides the Grid Master virtual IP address.
- ibGridReplicationState provides information about the replication status.

The ibPlatformOne MIB also contains the following tables that provide status of the Infoblox services as well as system and hardware services on the appliance you query:

- ibMemberServiceStatusTable provides status of the Infoblox services, such as the DNS and DHCP services, on a queried appliance. For information, see ibMemberServiceStatusTable on page 945.
- ibMemberNode1ServiceStatusTable provides status of the system and hardware services on a queried appliance. For information, see ibMemberNode1ServiceStatusTable on page 948.
- 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 950.
Figure 34.4  *ibPlatformOne MIB Structure*

(3.1.1.2) *ibPlatformOne MIB*  

(3.1.1.2.1) *ibPlatformOneModule*  

(3.1.1.2.1.1)  

*ibCPUTemperature*  

(3.1.1.2.1.2)  

*ibClusterReplicationStatusTable*  

*ibClusterReplicationStatusTable Objects* on page 938

(3.1.1.2.1.3)  

*ibNetworkMonitor*  

*ibNetworkMonitor Objects* on page 939

(3.1.1.2.1.4)  

*ibHardwareType*  

(3.1.1.2.1.5)  

*ibHardwareId*  

(3.1.1.2.1.6)  

*ibSerialNumber*  

(3.1.1.2.1.7)  

*ibNiosVersion*  

(3.1.1.2.1.8)  

*ibSystemMonitor*  

*ibSystemMonitor Objects3* on page 945

(3.1.1.2.1.9)  

*ibMemberServiceStatusTable*  

*ibMemberServiceStatusTable Objects* on page 946

(3.1.1.2.1.10)  

*ibMemberNode1ServiceStatusTable*  

*ibMemberNode1ServiceStatusTable Objects* on page 948

(3.1.1.2.1.11)  

*ibMemberNode2ServiceStatusTable*  

*ibMemberNode2ServiceStatusTable Objects* on page 950

(3.1.1.2.1.12)  

*ibGridStatus*  

(3.1.1.2.1.13)  

*ibHAStatus*  

(3.1.1.2.1.14)  

*ibGridMasterCandStatus*  

(3.1.1.2.1.15)  

*ibGridMasterVIP*  

(3.1.1.2.1.16)  

*ibGridReplicationState*
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 919.

*Figure 34.5* shows the sub branches of ibClusterReplicationStatusTable.

*Figure 34.5  ibClusterReplicationStatusTable Objects*

![Diagram of ibClusterReplicationStatusTable objects]

Table 34.7 provides information about the ibClusterReplicationStatusTable objects.

Table 34.7  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 34.6*, 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 941.

- `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 942.

- `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`
  - `ibNetworkMonitorDNSSecurityInvalidPortOnly` (Counter)
    - `ibNetworkMonitorDNSSecurityInvalidPortCount` (Counter)
  - `ibNetworkMonitorDNSSecurityInvalidTxidOnly` (Counter)
  - `ibNetworkMonitorDNSSecurityInvalidTxidAndPort` (Counter)

For information, see *Table 34.10* on page 943.

*Figure 34.6 ibNetworkMonitor Objects*
Figure 34.7 *ibNetworkMonitorDNSNonAA and ibNetworkMonitorDNSAA Subtrees*
Table 34.8 describes the objects in `ibNetworkMonitorDNSNonAA`. You can send queries to retrieve values for these objects.

### Table 34.8 `ibNetworkMonitorDNSNonAA` Objects

<table>
<thead>
<tr>
<th>Object Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ibNetworkMonitorDNSNonAAT1</code></td>
<td>File that contains the objects for monitoring the average latency of nonauthoritative replies to queries in the last minute.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSNonAAT1AvgLatency</code> (Integer)</td>
<td>Indicates the average latency in microseconds of nonauthoritative replies to queries in the last minute.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSNonAAT1Count</code> (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><code>ibNetworkMonitorDNSNonAAT5</code></td>
<td>File that contains the objects for monitoring the average latency of nonauthoritative replies to queries in the last five minutes.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSNonAAT5AvgLatency</code> (Integer)</td>
<td>Indicates the average latency in microseconds of nonauthoritative replies to queries in the last five minutes.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSNonAAT5Count</code> (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><code>ibNetworkMonitorDNSNonAAT15</code></td>
<td>File that contains the objects for monitoring the average latency of nonauthoritative replies to queries in the last 15 minutes.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSNonAAT15AvgLatency</code> (Integer)</td>
<td>Indicates the average latency in microseconds of nonauthoritative replies to queries in the last 15 minutes.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSNonAAT15Count</code> (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><code>ibNetworkMonitorDNSNonAAT60</code></td>
<td>File that contains the objects for monitoring the average latency of nonauthoritative replies to queries in the last 60 minutes.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSNonAAT60AvgLatency</code> (Integer)</td>
<td>Indicates the average latency in microseconds of nonauthoritative replies to queries in the last 60 minutes.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSNonAAT60Count</code> (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><code>ibNetworkMonitorDNSNonAAT1440</code></td>
<td>File that contains the objects for monitoring the average latency of nonauthoritative replies to queries in the last 24 hours.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSNonAAT1440AvgLatency</code> (Integer)</td>
<td>Indicates the average latency in microseconds of nonauthoritative replies to queries in the last 24 hours.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSNonAAT1440Count</code> (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 34.9 describes the objects in ibNetworkMonitorDNSAA. You can send queries to retrieve values for these objects.

### Table 34.9 ibNetworkMonitorDNSAA Objects

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibNetworkMonitorDNSAAT1</td>
<td>File that contains the objects for monitoring the average latency of authoritative replies to queries in the last minute.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT1AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of authoritative replies to queries in the last minute.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT1Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of authoritative replies in the last minute.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT5</td>
<td>File that contains the objects for monitoring the average latency of authoritative replies to queries in the last five minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT5AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of authoritative replies to queries in the last five minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT5Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of authoritative replies in the last five minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT15</td>
<td>File that contains the objects for monitoring the average latency of authoritative replies to queries in the last 15 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT15AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of authoritative replies to queries in the last 15 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT15Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of authoritative replies in the last 15 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT60</td>
<td>File that contains the objects for monitoring the average latency of authoritative replies to queries in the last 60 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT60AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of authoritative replies to queries in the last 60 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT60Count (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>ibNetworkMonitorDNSAAT1440</td>
<td>File that contains the objects for monitoring the average latency of authoritative replies to queries in the last 24 hours.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT1440AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of authoritative replies to queries in the last 24 hours.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT1440Count (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 34.10 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 34.10  *ibNetworkMonitorDNSSecurity Objects*

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
</table>
| ibNetworkMonitorDNSSecurityInvalidPort             | Tracks the number of invalid DNS responses that arrive on invalid ports. For information about invalid ports, see *Monitoring DNS Transactions* on page 887.  
This object contains a subtree with six objects that track invalid ports within a certain time interval. For information, see Table 34.11. |
| ibNetworkMonitorDNSSecurityInvalidTxid             | Tracks the number of invalid TXIDs (DNS transaction IDs). For information about invalid TXIDs, see *Monitoring DNS Transactions* on page 887.  
This object contains a subtree with six objects that track invalid TXIDs within a certain time interval. For information, see Table 34.12. |
| ibNetworkMonitorDNSSecurityInvalidPortOnly (Counter) | Tracks the number of DNS responses with both of the following conditions:  
• Arrive on invalid ports  
• Have valid TXIDs                                                                 |
| ibNetworkMonitorDNSSecurityInvalidTxidOnly (Counter) | Tracks the number of DNS responses with both of the following conditions:  
• Arrive on valid ports  
• Have invalid TXIDs                                                                 |
| ibNetworkMonitorDNSSecurityInvalidPortCount (Counter) | Tracks the total number of invalid DNS responses that arrive on invalid ports.                                                              |
| ibNetworkMonitorDNSSecurityInvalidTxidCount (Counter) | Tracks the total number of DNS responses that have invalid DNS transaction IDs.                                                            |
| ibNetworkMonitorDNSSecurityInvalidTxidAndPort (Counter) | Tracks the number of DNS responses with both of the following conditions:  
• Arrive on invalid ports  
• Have invalid TXIDs                                                                 |
**Table 34.11** describes the objects in `ibNetworkMonitorDNSSecurityInvalidPort`.

**Table 34.11  `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 34.12** describes the objects in `ibNetworkMonitorDNSSecurityInvalidTxid`.

**Table 34.12  `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 34.4, 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 34.8 ibSystemMonitor Objects

ibMemberServiceStatusTable

As shown in Figure 34.9, 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 947.
- 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 948 and ibMemberNode2ServiceStatusTable on page 950.
**Infoblox Services for ibMemberServiceStatusTable**

*Table 34.13* lists the values and descriptions of the Infoblox services that appear in *ibMemberServiceStatusTable*.

*Table 34.13  ibServiceName Values for ibMemberServiceStatusTable*

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>dhcp</td>
<td>DHCP service</td>
</tr>
<tr>
<td>2</td>
<td>dns</td>
<td>DNS service</td>
</tr>
<tr>
<td>3</td>
<td>ntp</td>
<td>NTP service</td>
</tr>
<tr>
<td>4</td>
<td>tftp</td>
<td>File distribution using the TFTP service</td>
</tr>
<tr>
<td>5</td>
<td>http-file-dist</td>
<td>File distribution using the HTTP service</td>
</tr>
<tr>
<td>6</td>
<td>ftp</td>
<td>File distribution using the FTP service</td>
</tr>
<tr>
<td>7</td>
<td>bloxtools-move</td>
<td>Moving the bloxTools service</td>
</tr>
<tr>
<td>8</td>
<td>bloxtools</td>
<td>The bloxTools environment</td>
</tr>
<tr>
<td>9</td>
<td>node-status</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>disk-usage</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>enet-lan</td>
<td>LAN port</td>
</tr>
<tr>
<td>12</td>
<td>enet-lan2</td>
<td>LAN2 port</td>
</tr>
<tr>
<td>13</td>
<td>enet-ha</td>
<td>HA port</td>
</tr>
<tr>
<td>14</td>
<td>enet-mgmt</td>
<td>MGMT port</td>
</tr>
<tr>
<td>15</td>
<td>lcd</td>
<td>LCD</td>
</tr>
<tr>
<td>16</td>
<td>memory</td>
<td>Memory</td>
</tr>
<tr>
<td>17</td>
<td>replication</td>
<td>Replication service</td>
</tr>
<tr>
<td>18</td>
<td>db-object</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>raid-summary</td>
<td>RAID array</td>
</tr>
<tr>
<td>20</td>
<td>raid-disk1</td>
<td>RAID Disk 1</td>
</tr>
</tbody>
</table>
When you query the service status on an appliance, the response includes the status of the services. Table 34.14 shows the values and descriptions of the status. Note that for internal Grid operations, the NTP service is always in the “working” state even if it has been disabled through the Infoblox GUI.

### Table 34.14 ibServiceStates Values

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>working</td>
<td>The service is functioning properly.</td>
</tr>
<tr>
<td>2</td>
<td>warning</td>
<td>The service is having some issues. Check the service or hardware function and the syslog to identify the problem.</td>
</tr>
<tr>
<td>3</td>
<td>failed</td>
<td>The service failed. Review the syslog to identify the problem.</td>
</tr>
<tr>
<td>4</td>
<td>inactive</td>
<td>The service is disabled or out of service.</td>
</tr>
<tr>
<td>5</td>
<td>unknown</td>
<td>The appliance cannot detect the current status of the service.</td>
</tr>
</tbody>
</table>
ibMemberNode1ServiceStatusTable

As shown in Figure 34.10, 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 949.
- ibMemberNode1ServiceStatus (Integer) reports the status of the services. For a list of service status, see Service Status on page 947.
- 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 950.

Note: For an independent appliance and the passive node of an HA pair, no information is returned when you query ibMemberNode2ServiceStatusTable.

Figure 34.10 ibMemberNode1ServiceStatusTable Objects
System and Hardware Services for ibMemberNode1ServiceStatusTable

Table 34.15 lists the values and descriptions of the system and hardware services that appear in ibMemberNode1ServiceStatusTable.

**Table 34.15 ibServiceNames Values for ibMemberNode1ServiceStatusTable**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>dhcp</td>
<td>DHCP service</td>
</tr>
<tr>
<td>2</td>
<td>dns</td>
<td>DNS service</td>
</tr>
<tr>
<td>3</td>
<td>ntp</td>
<td>NTP service</td>
</tr>
<tr>
<td>4</td>
<td>tftp</td>
<td>TFTP file distribution</td>
</tr>
<tr>
<td>5</td>
<td>http-file-dist</td>
<td>HTTP file distribution</td>
</tr>
<tr>
<td>6</td>
<td>ftp</td>
<td>FTP file distribution</td>
</tr>
<tr>
<td>7</td>
<td>bloxtools-move</td>
<td>Moving the bloxTools service</td>
</tr>
<tr>
<td>8</td>
<td>bloxtools</td>
<td>The bloxTools service</td>
</tr>
<tr>
<td>9</td>
<td>node-status</td>
<td>Node status</td>
</tr>
<tr>
<td>10</td>
<td>disk-usage</td>
<td>Disk usage</td>
</tr>
<tr>
<td>11</td>
<td>enet-lan</td>
<td>LAN 1 port</td>
</tr>
<tr>
<td>12</td>
<td>enet-lan2</td>
<td>LAN 2 port</td>
</tr>
<tr>
<td>13</td>
<td>enet-ha</td>
<td>HA port</td>
</tr>
<tr>
<td>14</td>
<td>enet-mgmt</td>
<td>MGMT port</td>
</tr>
<tr>
<td>15</td>
<td>lcd</td>
<td>LCD</td>
</tr>
<tr>
<td>16</td>
<td>memory</td>
<td>Virtual memory</td>
</tr>
<tr>
<td>17</td>
<td>replication</td>
<td>Replication process</td>
</tr>
<tr>
<td>18</td>
<td>db-object</td>
<td>Database usage</td>
</tr>
<tr>
<td>19</td>
<td>raid-summary</td>
<td>Summary of the RAID array</td>
</tr>
<tr>
<td>20</td>
<td>raid-disk1</td>
<td>Disk 1 of the RAID array (for Infoblox-2000, -2000-A, and -4010)</td>
</tr>
<tr>
<td>21</td>
<td>raid-disk2</td>
<td>Disk 2 of the RAID array (for Infoblox-2000, -2000-A, and -4010)</td>
</tr>
<tr>
<td>22</td>
<td>raid-disk3</td>
<td>Disk 3 of the RAID array (for Infoblox-2000, -2000-A, and -4010)</td>
</tr>
<tr>
<td>23</td>
<td>raid-disk4</td>
<td>Disk 4 of the RAID array (for Infoblox-2000, -2000-A, and -4010)</td>
</tr>
<tr>
<td>24</td>
<td>fan1</td>
<td>FAN 1 status</td>
</tr>
<tr>
<td>25</td>
<td>fan2</td>
<td>FAN 2 status</td>
</tr>
<tr>
<td>26</td>
<td>fan3</td>
<td>FAN 3 status</td>
</tr>
<tr>
<td>27</td>
<td>power-supply</td>
<td>Power supply</td>
</tr>
<tr>
<td>28</td>
<td>ntp-sync</td>
<td>NTP service synchronization</td>
</tr>
<tr>
<td>29</td>
<td>cpu1-temp</td>
<td>CPU 1 temperature</td>
</tr>
<tr>
<td>30</td>
<td>cpu2-temp</td>
<td>CPU 2 temperature</td>
</tr>
</tbody>
</table>
As shown in Figure 34.11, `ibMemberNode2ServiceStatusTable` (object ID 3.1.1.2.1.2.11) 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 947.
- `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 34.11 ibMemberNode2ServiceStatusTable Objects**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>sys-temp</td>
<td>System temperature</td>
</tr>
<tr>
<td>32</td>
<td>raid-battery</td>
<td>RAID battery</td>
</tr>
<tr>
<td>33</td>
<td>cpu-usage</td>
<td>CPU usage</td>
</tr>
<tr>
<td>34</td>
<td>ospf</td>
<td>Anycast using OSPF</td>
</tr>
<tr>
<td>35</td>
<td>bgp</td>
<td>Anycast using BGP</td>
</tr>
</tbody>
</table>
System and Hardware Services for `ibMemberNode2ServiceStatusTable`

`Table 34.16` lists the values and descriptions of the system and hardware services that appear in `ibMemberNode2ServiceStatusTable`.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>dhcp</td>
<td>DHCP service</td>
</tr>
<tr>
<td>2</td>
<td>dns</td>
<td>DNS service</td>
</tr>
<tr>
<td>3</td>
<td>ntp</td>
<td>NTP service</td>
</tr>
<tr>
<td>4</td>
<td>tftp</td>
<td>TFTP file distribution</td>
</tr>
<tr>
<td>5</td>
<td>http-file-dist</td>
<td>HTTP file distribution</td>
</tr>
<tr>
<td>6</td>
<td>ftp</td>
<td>FTP file distribution</td>
</tr>
<tr>
<td>7</td>
<td>bloxtools-move</td>
<td>Moving the bloxTools service</td>
</tr>
<tr>
<td>8</td>
<td>bloxtools</td>
<td>The bloxTools service</td>
</tr>
<tr>
<td>9</td>
<td>node-status</td>
<td>Node status</td>
</tr>
<tr>
<td>10</td>
<td>disk-usage</td>
<td>Disk usage</td>
</tr>
<tr>
<td>11</td>
<td>enet-lan</td>
<td>LAN 1 port</td>
</tr>
<tr>
<td>12</td>
<td>enet-lan2</td>
<td>LAN 2 port</td>
</tr>
<tr>
<td>13</td>
<td>enet-ha</td>
<td>HA port</td>
</tr>
<tr>
<td>14</td>
<td>enet-mgmt</td>
<td>MGMT port</td>
</tr>
<tr>
<td>15</td>
<td>lcd</td>
<td>LCD</td>
</tr>
<tr>
<td>16</td>
<td>memory</td>
<td>Virtual memory</td>
</tr>
<tr>
<td>17</td>
<td>replication</td>
<td>Replication process</td>
</tr>
<tr>
<td>18</td>
<td>db-object</td>
<td>Database usage</td>
</tr>
<tr>
<td>19</td>
<td>raid-summary</td>
<td>Summary of the RAID array</td>
</tr>
<tr>
<td>20</td>
<td>raid-disk1</td>
<td>Disk 1 of the RAID array (for Infoblox-2000, -2000-A, and -4010)</td>
</tr>
<tr>
<td>21</td>
<td>raid-disk2</td>
<td>Disk 2 of the RAID array (for Infoblox-2000, -2000-A, and -4010)</td>
</tr>
<tr>
<td>22</td>
<td>raid-disk3</td>
<td>Disk 3 of the RAID array (for Infoblox-2000, -2000-A, and -4010)</td>
</tr>
<tr>
<td>23</td>
<td>raid-disk4</td>
<td>Disk 4 of the RAID array (for Infoblox-2000, -2000-A, and -4010)</td>
</tr>
<tr>
<td>24</td>
<td>fan1</td>
<td>FAN 1 status</td>
</tr>
<tr>
<td>25</td>
<td>fan2</td>
<td>FAN 2 status</td>
</tr>
<tr>
<td>26</td>
<td>fan3</td>
<td>FAN 3 status</td>
</tr>
<tr>
<td>27</td>
<td>power-supply</td>
<td>Power supply</td>
</tr>
<tr>
<td>28</td>
<td>ntp-sync</td>
<td>NTP service synchronization</td>
</tr>
<tr>
<td>29</td>
<td>cpu1-temp</td>
<td>CPU 1 temperature</td>
</tr>
<tr>
<td>30</td>
<td>cpu2-temp</td>
<td>CPU 2 temperature</td>
</tr>
<tr>
<td>Value</td>
<td>Description</td>
<td>Definition</td>
</tr>
<tr>
<td>-------</td>
<td>--------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>31</td>
<td>sys-temp</td>
<td>System temperature</td>
</tr>
<tr>
<td>32</td>
<td>raid-battery</td>
<td>RAID battery</td>
</tr>
<tr>
<td>33</td>
<td>cpu-usage</td>
<td>CPU usage</td>
</tr>
<tr>
<td>34</td>
<td>ospf</td>
<td>Anycast using OSPF</td>
</tr>
<tr>
<td>35</td>
<td>bgp</td>
<td>Anycast using BGP</td>
</tr>
</tbody>
</table>
ibDHCPOne MIB

The ibDHCPOne MIB provides information about address usage within a subnet, DHCP lease statistics, and DHCP packet counts. It includes two modules, ibDHCPModule for IPv4 data and ibDHCPv6Module for IPv6 data.

ibDHCPModule

*Figure 34.12* illustrates the structure of the ibDHCPModule. (Note that the OIDs shown in the illustration do not include the prefix .1.3.6.1.4.1.7779.) ibDHCPModule contains the following objects:

- ibDHCPSubnetTable provides statistical data about the DHCP operations of the appliance. For information, see *ibDHCPSubnetTable* on page 954.
- ibDHCPStatistics maintains counters for different types of packets. For information, see *ibDHCPStatistics* on page 955.
- ibDHCPDeferredQueuesize tracks the total number of deferred DDNS updates that are currently in the queue to be retried. When DDNS updates are deferred due to timeout or server issues, the DHCP server puts these updates in this queue.
- ibDHCPDDNSStats monitors the average latency for the DDNS updates in microseconds and the number of timeouts during different time intervals. For information, see *ibDHCPDDNSStats* on page 956.

*Figure 34.12  ibDHCPModule*
ibDHCPSubnetTable

ibDHCPSubnetTable provides statistical data about the DHCP operations of the appliance. It contains the following objects:

Table 34.17  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 (IbpAddr)</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 (IbpAddr)</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 34.13  MIB Browser View 1

<table>
<thead>
<tr>
<th>ibDHCPSubnetNetworkAddress</th>
<th>ibDHCPSubnetNetworkMask</th>
<th>ibDHCPSubnetPercentUsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 0.0.0</td>
<td>255.0.0.0</td>
<td>0.0000</td>
</tr>
<tr>
<td>20 0.0.0</td>
<td>255.255.255.0</td>
<td>0.0000</td>
</tr>
<tr>
<td>20 0.1.0</td>
<td>255.255.255.0</td>
<td>0.0000</td>
</tr>
<tr>
<td>20 0.2.0</td>
<td>255.255.255.0</td>
<td>0.0000</td>
</tr>
<tr>
<td>20 0.3.0</td>
<td>255.255.255.0</td>
<td>0.0000</td>
</tr>
<tr>
<td>20 0.4.0</td>
<td>255.255.255.0</td>
<td>0.0000</td>
</tr>
<tr>
<td>20 0.5.0</td>
<td>255.255.255.0</td>
<td>0.0000</td>
</tr>
<tr>
<td>20 0.6.0</td>
<td>255.255.255.0</td>
<td>0.0000</td>
</tr>
<tr>
<td>20 0.7.0</td>
<td>255.255.255.0</td>
<td>0.0000</td>
</tr>
<tr>
<td>20 0.8.0</td>
<td>255.255.255.0</td>
<td>0.0000</td>
</tr>
</tbody>
</table>
ibDHCPStatistics

ibDHCPStatistics maintains counters for different types of packets. The counters always start with zero when the DHCP service is restarted. Therefore, the numbers reflect the total number of packets received since the DHCP service was last restarted on the appliance. The ibDHCPStatistics module contains the following objects:

<table>
<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>
ibDHCPDDNSStats

ibDHCPDDNSStats monitors the average latency for the DHCP DDNS updates in microseconds and the number of timeouts during different time intervals. The ibDHCPDDNSStats module contains the following objects:

Table 34.19  ibDHCPStatistics

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibDHCPDDNSAvgLatency5 (Integer)</td>
<td>Indicates the average latency in microseconds of the DHCP DDNS updates in the last five minutes.</td>
</tr>
<tr>
<td>ibDHCPDDNSAvgLatency15 (Integer)</td>
<td>Indicates the average latency in microseconds of the DHCP DDNS updates in the last 15 minutes.</td>
</tr>
<tr>
<td>ibDHCPDDNSAvgLatency60 (Integer)</td>
<td>Indicates the average latency in microseconds of the DHCP DDNS updates in the last 60 minutes.</td>
</tr>
<tr>
<td>ibDHCPDDNSAvgLatency1440 (Integer)</td>
<td>Indicates the average latency in microseconds of the DHCP DDNS updates in the last 24 hours.</td>
</tr>
<tr>
<td>ibDHCPDDNSTimeoutCount5 (Integer)</td>
<td>The number of timeouts for the DHCP DDNS updates in the last five minutes.</td>
</tr>
<tr>
<td>ibDHCPDDNSTimeoutCount15 (Integer)</td>
<td>The number of timeouts for the DHCP DDNS updates in the last 15 minutes.</td>
</tr>
<tr>
<td>ibDHCPDDNSTimeoutCount60 (Integer)</td>
<td>The number of timeouts for the DHCP DDNS updates in the last 60 minutes.</td>
</tr>
<tr>
<td>ibDHCPDDNSTimeoutCount1440 (Integer)</td>
<td>The number of timeouts for the DHCP DDNS updates in the last 24 hours.</td>
</tr>
</tbody>
</table>
**ibDHCPv6Module**

*Figure 34.14* illustrates the structure of the ibDHCPv6Module, which contains the following objects:

- **ibDHCPv6SubnetTable** provides statistical data about the DHCPv6 operations of the appliance. For information, see *ibDHCPv6SubnetTable* on page 958.
- **ibDHCPv6Statistics** maintains counters for different types of packets. For information, see *ibDHCPv6Statistics* on page 959.
- **ibDHCPv6DeferredQueuesize** tracks the total number of deferred DDNS updates that are currently in the queue to be retried. When DDNS updates are deferred due to timeout or server issues, the DHCP server puts these updates in this queue.
- **ibDHCPv6DDNSStats** monitors the average latency for the DDNS updates in microseconds and the number of timeouts during different time intervals. For information, see *ibDHCPv6DDNSStats* on page 960.

*Figure 34.14  ibDHCPv6Module*
ibDHCPv6SubnetTable

ibDHCPv6SubnetTable provides statistical data about the DHCPv6 operations of the appliance. It contains the following objects:

Table 34.20 ibDHCPv6SubnetTable

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibDHCPv6Subnet Entry</td>
<td>File that contains the objects for monitoring DHCPv6 operations on the appliance.</td>
</tr>
<tr>
<td>ibDHCPv6SubnetNetworkAddress (IbIpAddr)</td>
<td>The subnetworks, in IPv6 address format, that have IPv6 addresses for lease. A subnetwork may have many address ranges for lease.</td>
</tr>
<tr>
<td>ibDHCPv6SubnetNetworkMask (IbIpAddr)</td>
<td>The subnet mask in CIDR notation format.</td>
</tr>
</tbody>
</table>
### ibDHCPv6Statistics

ibDHCPv6Statistics maintains counters for different types of packets. The counters always start with zero when the DHCP service is restarted. Therefore, the numbers reflect the total number of packets received since the DHCP service was last restarted on the appliance. The `ibDHCPv6Statistics` module contains the following objects:

Table 34.21  `ibDHCPv6Statistics`

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ibDhcpv6TotalNoOfSolicits</code> (Counter)</td>
<td>The number of Solicit messages that the Grid member received, including Solicit messages embedded in Relay-Forward messages. A DHCP client sends a Solicit message to locate DHCP servers.</td>
</tr>
<tr>
<td><code>ibDhcpv6TotalNoOfRequests</code> (Counter)</td>
<td>The number of Request messages that the Grid member received. A DHCP client sends a Request message to request one or more IP addresses and configuration parameters from a DHCP server.</td>
</tr>
<tr>
<td><code>ibDhcpv6TotalNoOfReleases</code> (Counter)</td>
<td>The number of Release messages that the Grid member received. A DHCP client sends a Release message when it terminates its lease and releases its IP address.</td>
</tr>
<tr>
<td><code>ibDhcpv6TotalNoOfAdvertises</code> (Counter)</td>
<td>The number of Advertise messages that the Grid member sent. When a DHCP server receives a Solicit message, it can respond with an Advertise message to indicate that the server is available for DHCP service.</td>
</tr>
<tr>
<td><code>ibDhcpv6TotalNoOfReplies</code> (Counter)</td>
<td>The number of Reply messages that the Grid member sent. A DHCP server sends a Reply message that includes IP addresses and configuration parameters when it responds to Solicit, Request, Renew or Rebind message. It sends a Reply message with configuration parameters only when it responds to an Information-Request message.</td>
</tr>
<tr>
<td><code>ibDhcpv6TotalNoOfRenews</code> (Counter)</td>
<td>The number of Renew messages that the Grid member received. A DHCP client sends a Renew message to a DHCP server to extend the lifetimes on the leases granted by the DHCP server and to update other properties.</td>
</tr>
<tr>
<td><code>ibDhcpv6TotalNoOfRebinds</code> (Counter)</td>
<td>The number of Rebind messages that the Grid member received. A DHCP client sends a Rebind message to extend the lifetime of its lease and to update configuration parameters.</td>
</tr>
<tr>
<td><code>ibDhcpv6TotalNoOfDeclines</code> (Counter)</td>
<td>The number of Decline messages that the Grid member received. A DHCP client sends a Decline message to a DHCP server when it discovers that the IP address offered by a DHCP server is already in use.</td>
</tr>
<tr>
<td><code>ibDhcpv6TotalNoOfInformationRequests</code> (Counter)</td>
<td>The number of Information-Request messages that the Grid member received. A client sends an Information-Request message to retrieve configuration parameters, such as the IP addresses of DNS servers in the network.</td>
</tr>
<tr>
<td><code>ibDhcpv6TotalNoOfOthers</code> (Counter)</td>
<td>The total number of DHCP messages other than those used in negotiation.</td>
</tr>
</tbody>
</table>
Monitoring with SNMP

ibDHCPv6DDNSStats

ibDHCPv6DDNSStats monitors the average latency for the DHCPv6 DDNS updates in microseconds and the number of timeouts during different time intervals. The ibDHCPv6DDNSStats module contains the following objects:

Table 34.22  ibDHCPStatistics

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibDHCPv6DDNSAvgLatency5 (Integer)</td>
<td>Indicates the average latency in microseconds of the DHCPv6 DDNS updates in the last five minutes.</td>
</tr>
<tr>
<td>ibDHCPv6DDNSAvgLatency15 (Integer)</td>
<td>Indicates the average latency in microseconds of the DHCPv6 DDNS updates in the last 15 minutes.</td>
</tr>
<tr>
<td>ibDHCPv6DDNSAvgLatency60 (Integer)</td>
<td>Indicates the average latency in microseconds of the DHCPv6 DDNS updates in the last 60 minutes.</td>
</tr>
<tr>
<td>ibDHCPv6DDNSAvgLatency1440 (Integer)</td>
<td>Indicates the average latency in microseconds of the DHCPv6 DDNS updates in the last 24 hours.</td>
</tr>
<tr>
<td>ibDHCPv6DDNSTimeoutCount5 (Integer)</td>
<td>The number of timeouts for the DHCPv6 DDNS updates in the last five minutes.</td>
</tr>
<tr>
<td>ibDHCPv6DDNSTimeoutCount15 (Integer)</td>
<td>The number of timeouts for the DHCPv6 DDNS updates in the last 15 minutes.</td>
</tr>
<tr>
<td>ibDHCPv6DDNSTimeoutCount60 (Integer)</td>
<td>The number of timeouts for the DHCPv6 DDNS updates in the last 60 minutes.</td>
</tr>
<tr>
<td>ibDHCPv6DDNSTimeoutCount1440 (Integer)</td>
<td>The number of timeouts for the DHCPv6 DDNS updates in the last 24 hours.</td>
</tr>
</tbody>
</table>
**ibDNSOne MIB**

The ibDNSOne MIB provides DNS statistics about all zones in all views. *Figure 34.15* illustrates the structure of the ibDNSOne MIB. (Note that the OIDs shown in the illustration do not include the prefix 1.3.6.1.4.1.7779.) The ibDNSOne MIB contains four subtrees: ibZoneStatisticsTable (Counter64), ibZonePlusViewStatisticsTable (Counter64), ibDDNSUpdateStatistics (Counter64), and ibBindZoneTransferCount (Counter64).

*Figure 34.15  ibDNSOne MIB*
Using the DNS Zone Statistics Tables

ibZoneStatisticsTable and ibZonePlusViewStatisticsTable provide DNS statistics for all zones in all DNS views, including the default and all user-defined DNS views. You can use the information in these tables to calculate the total number of recursive queries on the DNS server. Depending on whether your DNS server is an authoritative or a caching-only server, you calculate the total number of recursive queries differently. For information, see Calculating Recursive DNS Queries on page 964.

ibZoneStatisticsTable

ibZoneStatisticsTable contains DNS statistics of all zones in the default DNS view. DNS statistics of user-defined DNS views are captured in ibZonePlusViewStatisticsTable. For information, see ibZonePlusViewStatisticsTable on page 963.

ibZoneStatisticsTable includes a “summary” zone that provides global statistics for the DNS server, including statistics for all zones in the default and user-defined DNS views.

The syntax of the objects in ibZoneStatisticsTable uses a Counter64 format. In some cases, the counter format may not be compatible with SNMP toolkits that use a 32-bit counter. Ensure that you reconfigure or update these tools to use the Counter64 format. ibZoneStatisticsTable contains the following objects:

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibBindZoneName (IbString)</td>
<td>DNS zone name. The index name for global statistics is “summary.”</td>
</tr>
<tr>
<td>ibBindZoneSuccess (Counter64)</td>
<td>The number of successful responses since the DNS process started.</td>
</tr>
<tr>
<td>ibBindZoneReferral (Counter64)</td>
<td>The number of DNS referrals since the DNS process started.</td>
</tr>
<tr>
<td>ibBindZoneNxRRset (Counter64)</td>
<td>The number of DNS queries received for non-existent records.</td>
</tr>
<tr>
<td>ibBindZoneNxDomain (Counter64)</td>
<td>The number of DNS queries received for non-existent domains.</td>
</tr>
<tr>
<td>ibBindZoneRecursion (Counter64)</td>
<td>The number recursive queries received since the DNS process started.</td>
</tr>
<tr>
<td>ibBindZoneFailure (Counter64)</td>
<td>The number of failed queries since the DNS process started.</td>
</tr>
</tbody>
</table>

Following is an example of the table as viewed through a MIB browser:
ibZonePlusViewStatisticsTable provides DNS statistics about all zones in user-defined DNS views. DNS statistics about zones in the default view are captured in ibZoneStatisticsTable. Note that information in ibZonePlusViewStatisticsTable is rolled up to the “summary” zone in ibZoneStatisticsTable. For information, see ibZoneStatisticsTable on page 962.

The syntax of the objects in ibZonePlusViewStatisticsTable uses a Counter64 format. In some cases, the counter format may not be compatible with SNMP toolkits that use a 32-bit counter. Ensure that you reconfigure or update these tools to use the Counter64 format. ibZonePlusViewStatisticsTable contains the following objects:

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibBindZonePlusViewName (IbString)</td>
<td>The zone name.</td>
</tr>
<tr>
<td>ibBindZonePlusViewSuccess (Counter64)</td>
<td>The number of successful responses since the DNS process started.</td>
</tr>
<tr>
<td>ibBindZonePlusViewReferral (Counter64)</td>
<td>The number of DNS referrals since the DNS process started.</td>
</tr>
<tr>
<td>ibBindZonePlusViewNxRRset (Counter64)</td>
<td>The number of DNS queries received for non-existent records.</td>
</tr>
<tr>
<td>ibBindZonePlusViewNxDomain (Counter64)</td>
<td>The number of DNS queries received for non-existent domains.</td>
</tr>
<tr>
<td>ibBindZonePlusViewRecursion (Counter64)</td>
<td>The number of recursive queries received since the DNS process started.</td>
</tr>
</tbody>
</table>
Calculating Recursive DNS Queries

You can use the information in `ibZoneStatisticsTable` and `ibZonePlusViewStatisticsTable` to calculate the total number of recursive queries.

Following is an example of `ibZoneStatisticsTable` indexed by zone names in the default view:

```
index  ibBindZoneName  ibBindZoneSuccess  ibBindZoneReferral  ibBindZoneNxRRset  ibBindZoneNxDomain  ibBindZoneRecursion  ibBindZoneFailure
"abc.com"  abc.com  0  0  0  0  0  0
"summary"  summary  5  0  0  0  0  0
"internal.com"  internal.com  1  0  0  0  0  0
```

Following is an example of `ibZonePlusViewStatisticsTable` indexed by zone names in all user-defined views:

```
index  ibBindZonePlusViewName  ibBindZonePlusViewSuccess  ibBindZonePlusViewReferral  ibBindZonePlusViewNxRRset  ibBindZonePlusViewNxDomain  ibBindZonePlusViewRecursion  ibBindZonePlusViewFailure  ibBindViewName
"ext1.com"  ext1.com  1  0  0  0  0  0  DNS1
"ext2.com"  ext2.com  2  0  0  0  0  0  DNS1
"ext3.com"  ext3.com  0  0  0  0  0  0  DNS2
```

Use the `ibBindZoneSuccess` object in both tables to determine the total number of recursive queries. If your DNS server is a caching-only server, the total number of recursive queries is the number indicated in the `ibBindZoneSuccess` object of the “summary” zone. In this example, for a caching-only server, the total number of recursive queries is 5.

If your DNS server is an authoritative server, add all the numbers in `ibBindZoneSuccess` for all zones in both tables, excluding the “summary” zone. In this example, the total is 4. You then subtract this number from the number in `ibBindZoneSuccess` of the “summary” zone. In this case, the total number of recursive queries is 1 for an authoritative DNS server.
**ibDDNSUpdateStatistics**

`ibDDNSUpdateStatistics` provides statistical data about DDNS updates. The counters always start with zero when the DNS service is restarted. They report the total numbers since the DNS service was last restarted.

`ibDDNSUpdateStatistics` contains the following objects:

<table>
<thead>
<tr>
<th>Object</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).

**IB-DNSSERV-MIB**

The IB-DNSSERV-MIB contains one object, `ibDnsServConfig`, which reports the DNS BIND version implemented by the NIOS software.

**IB-DHCPSERV-MIB**

The IB-DHCPSERV-MIB contains one object, `ibDhcpv4ServerSystemDescr`, which provides the DHCP server name and its DHCP version.
Chapter 35 Infoblox Reporting Solution

This chapter describes the Infoblox reporting solution and its features. It explains how to view predefined reports and create user-defined reports and searches. It also provides best practices for customizing searches. It contains the following sections:

- **Infoblox Reporting Solution** on page 969
  - **Supported Platforms for Reporting** on page 970
- **Configuring Grid Reporting Properties** on page 971
  - **Configuring General Reporting Properties** on page 971
  - **Setting Network Port for Reporting** on page 972
  - **Setting Email Properties** on page 972
  - **Defining PDF Settings** on page 973
- **Overriding Member Reporting Properties** on page 973
  - **Starting and Overriding Reporting Service on Members** on page 973
  - **Overriding Report Categories** on page 973
- **Scheduling Report Deliveries** on page 974
- **About Reports** on page 974
  - **Adding New Reports** on page 975
  - **Adding New Panels to Reports** on page 976
  - **Cloning Predefined Reports** on page 976
  - **Modifying User-defined Reports** on page 976
  - **Deleting User-defined Reports** on page 977
- **About Searches** on page 977
  - **Guidelines for Customizing Searches** on page 977
  - **Reporting Indexes and Update Time Intervals** on page 978
  - **Modifying Searches** on page 980
  - **Scheduling Searches** on page 981
  - **Exporting Searches** on page 982
  - **Scheduling Exports of Search Results** on page 982
- **Managing Reports** on page 993
  - **Adding New Reports** on page 975
  - **Modifying User-defined Reports** on page 976
  - **Deleting User-defined Reports** on page 977
• Managing Reports on page 993
  — Printing Reports on page 993
  — Backing Up Reporting Data on page 993
  — Scheduling the Backup of the Reporting Database on page 994
  — Restoring the Reporting Database on page 995
Infoblox Reporting Solution

Infoblox provides tools that support reporting of core network services in an Infoblox Grid. You can add any of the supported Trinzic Reporting platforms as a member to the Grid and configure it as a reporting appliance. The reporting appliance collects data from Infoblox members, stores the data in the database, and generates reports that provide statistical data about IPAM, DNS, DHCP, and system activities and performance. The Infoblox reporting solution automates the collection, analysis, and presentation of core network service data that assists you in planning and mitigating network outage risks so you can manage your networks more efficiently. For information about how an Infoblox reporting appliance works with your Grid, see Introduction to Grids on page 173. For information about Infoblox platforms that support reporting, see Supported Platforms for Reporting.

You can set up a reporting appliance solely for reporting purposes. You cannot add licenses to run other services, such as DNS and DHCP, on a reporting appliance. When you set up a reporting appliance with valid licenses in the Grid, the reporting server acts as an indexer that receives data from Grid members while the members are forwards that transmit information to the reporting server. Depending on your needs, you can enable certain Grid members as forwards and disable others so the reporting server receives only the information you need from specific members. Note that the reporting service is disabled by default. You must complete the following before you can view and manage reports in the Grid:

• Configure Grid reporting properties, as described in Configuring Grid Reporting Properties on page 971.
• Enable or disable specific members to forward data to the reporting server, as described in Overriding Member Reporting Properties on page 973.

When you enable the Grid reporting service, all members transmit data to the reporting server. You can disable data transmission from specific members to the reporting server.

After you set up and configure the reporting server and enable reporting service on specific members, you can view and manage reports through the Reporting tab of Grid Manager. Infoblox provides predefined reports and searches that capture useful information about the activities and performance of core network services (IPAM, DNS, DHCP, and system) in your Grid. You can also create your own reports and searches based on your organization’s needs.

Note: You must enable reporting service on the Grid or members before you can use the reporting functions. For information about how to enable the reporting service, see Configuring General Reporting Properties on page 971 and Starting and Overiding Reporting Service on Members on page 973.

You can do the following in the Reporting tab:

• Configure Grid reporting settings, as described in Configuring Grid Reporting Properties on page 971.
• Schedule the delivery of reports in PDF format to specified email addresses, as described in Scheduling Report Deliveries on page 974.
• Create new reports, as described in Adding New Reports on page 975.
• Create, modify, and delete user-defined searches, as described in About Searches on page 977.
• View predefined reports, as described in About Predefined Reports on page 984.
• Create user defined reports, as described in Managing Reports on page 993.
• Print a list of reports, as described in Printing Reports on page 993.
• Back up and restore the reporting database, as described in Backing Up Reporting Data on page 993 and Restoring the Reporting Database on page 995.
Supported Platforms for Reporting

Infoblox provides a few reporting appliances that address your organization needs. Table 35.1 lists the supported Trinzic Reporting platforms based on IP capacities and average DHCP leases and DNS queries per second:

Table 35.1 Trinzic Reporting Platforms

<table>
<thead>
<tr>
<th>Enterprise Model</th>
<th>Supported Infoblox Appliance</th>
<th>Daily Maximum Data Consumption*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Large enterprises</td>
<td>Trinzic Reporting 4000 Appliance</td>
<td>20 GB</td>
</tr>
<tr>
<td>Service providers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Large enterprises</td>
<td>Trinzic Reporting 2000 Appliance</td>
<td>10 GB</td>
</tr>
<tr>
<td>Mid-size enterprises</td>
<td>Trinzic Reporting 1400 Appliance</td>
<td>5 GB</td>
</tr>
<tr>
<td>Mid-size enterprises</td>
<td>Trinzic Reporting VM-800 (virtual appliance)</td>
<td>1 GB</td>
</tr>
</tbody>
</table>

Note: * The daily maximum data consumption includes all DNS, DDNS, IPAM, DHCP, and system traffic or events from all members with data transmission enabled within your Grid. When data traffic exceeds the daily maximum, the reporting server sends an SNMP trap and email notification, if configured. After five (5) daily maximum warnings in a rolling period of 30 days, you cannot view reports or perform any report related functions. For information about how to avoid this problem, see Guidelines for Customizing Searches on page 977. Note that the reporting server continues to process incoming data during the violation state. However, you cannot view any reports or manage any reporting related functions until you fix the violation issue.

For information about the Trinzic Reporting platforms, their specifications, and how to install them as reporting appliances, refer to the following:

- Infoblox Installation Guide for the Trinzic Reporting 4000 Appliance
- Infoblox Installation Guide for the Trinzic Reporting 2000 Appliance
- Infoblox Installation Guide for the Trinzic Reporting 1400 Appliance
- Infoblox Installation Guide for the Trinzic Reporting VM-800 Appliance
Configuring Grid Reporting Properties

After you set up a dedicated reporting appliance in your Grid, you can configure Grid settings to communicate with the reporting appliance and retrieve report data through the Grid Master. You can select specific report categories and configure report settings. You must be a superuser to view and configure Grid reporting properties. Complete the following to set up your reporting solution:

- Configure general reporting properties, including the selection of report categories, as described in Configuring General Reporting Properties on page 971.
- Specify the network port for reporting, as described in Setting Network Port for Reporting on page 972.
- Define email properties for messages related to reporting, as described in Setting Email Properties on page 972.
- Configure the PDF settings of the reports that you schedule for delivery, as described in Defining PDF Settings on page 973.

Configuring General Reporting Properties

To configure general Grid reporting properties:

1. From the Reporting tab, click Grid Reporting Properties form the Toolbar.
2. In the Grid Reporting Properties editor, select the General -> Basic tab and complete the following:
   - **Reporting Server**: Grid Manager displays the name of the reporting server here.
   - **Enable Data Indexing**: Select this check box to enable data transmissions to the reporting server from all members in the Grid. Data transmission is disabled by default. When you select this check box, all Grid members transmit data to the reporting appliance. You can override this setting at the member level. Note that enabling data transmissions for all members can affect the overall data consumption on the reporting server. For information about the daily maximum data consumption per day for your reporting appliance, see Supported Platforms for Reporting on page 970.
   - **Report Category**: Select the reports you want the reporting server to generate. For information about report categories and their corresponding reports, see Table 35.2 on page 971. The reporting server automatically configures data sources and configurations required to generate the reports you select here. The required data is stored in the reporting server database. No report categories are selected by default. You can also override the report categories at a member level. For information, see Overriding Report Categories on page 973.

   **Report Settings**:
   - **Total Custom Reports per user**: Displays the total number of user-defined reports each user can create. The maximum number per superuser is 300 and per limited-access user is 5.
   - **Total Custom Reports for Grid**: Displays the total number of user-defined reports that are allowed in the Grid. The maximum number is 300. You cannot modify this field.
3. Save the configuration.

Report Categories and Corresponding Reports

*Table 35.2* lists the report categories and their corresponding reports.

*Table 35.2* Report Categories

<table>
<thead>
<tr>
<th>Report Category</th>
<th>Corresponding Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDNS</td>
<td><strong>DDNS Update Rate Trend</strong></td>
</tr>
<tr>
<td>DHCP Lease</td>
<td><strong>DHCP Lease History</strong></td>
</tr>
</tbody>
</table>
Setting Network Port for Reporting

All Grid members use port 9997 for reporting service by default. This port is used for data transmissions between the reporting member and other members. Ensure that you configure your firewall rules to allow traffic on this port. You can designate another network port for reporting purposes. To set the network port for reporting:

1. From the Reporting tab, click Grid Reporting Properties form the Toolbar.
2. In the Grid Reporting Properties editor, select the General ->Advanced tab and complete the following:
   — Port: Enter the port number you want to use for reporting purposes. The default port is 9997.
3. Save the configuration.

Setting Email Properties

You can enable and configure the settings of email messages that the appliance sends when there are changes to the link status of the network port and when certain events that affect the reporting feature arise.

To configure email properties:
1. From the Reporting tab, click Grid Reporting Properties form the Toolbar.
2. In the Grid Reporting Properties editor, select the Email tab and complete the following:
   — Email As: Enter the name of the admin or organization that sends the message.
   — Email Subject Prefix: Enter the subject prefix for the email messages.
   — Email Format: From the drop-down list, select the format for the email messages. The default is HTML.
3. Save the configuration.

<table>
<thead>
<tr>
<th>Report Category</th>
<th>Corresponding Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Performance</td>
<td>DHCPv4 Usage Statistics</td>
</tr>
<tr>
<td></td>
<td>DHCPv4 Range Utilization Trend</td>
</tr>
<tr>
<td></td>
<td>DHCPv4 Usage Trend</td>
</tr>
<tr>
<td></td>
<td>DHCP Message Rate Trend</td>
</tr>
<tr>
<td>DNS Performance</td>
<td>DNS Query Rate by Query Type</td>
</tr>
<tr>
<td></td>
<td>DNS Query Rate by Server</td>
</tr>
<tr>
<td></td>
<td>DNS Response Latency Trend</td>
</tr>
<tr>
<td>DNS Query</td>
<td>DNS Top Requested Domain Names</td>
</tr>
<tr>
<td></td>
<td>DNS Cache Hit Rate Trend</td>
</tr>
<tr>
<td></td>
<td>DNS Top Clients</td>
</tr>
<tr>
<td></td>
<td>DNS Replies Trend</td>
</tr>
<tr>
<td>IPAMv4 Utilization</td>
<td>IPAMv4 Network Usage Statistics</td>
</tr>
<tr>
<td></td>
<td>DNS Zone Statistics Per DNS View</td>
</tr>
<tr>
<td></td>
<td>IPAMv4 Top Utilized Networks</td>
</tr>
<tr>
<td></td>
<td>DHCPv4 Top Utilized Networks</td>
</tr>
<tr>
<td>System</td>
<td>CPU Utilization Trend</td>
</tr>
<tr>
<td></td>
<td>Memory Utilization Trend</td>
</tr>
<tr>
<td></td>
<td>Traffic Rate</td>
</tr>
</tbody>
</table>
Defining PDF Settings

You can schedule to send reports in PDF format to email addresses that you define. For information about scheduling the delivery of reports, see *Scheduling Report Deliveries*.

To define the PDF settings for the reports:

1. From the **Reporting** tab, click **Grid Reporting Properties** from the Toolbar.
2. In the **Grid Reporting Properties** editor, select the **PDF** tab and complete the following:
   - **Paper Size**: From the drop-down list, select the paper size.
   - **Report Orientation**: From the drop-down list, select the page orientation for the report.
3. Save the configuration.

Overriding Member Reporting Properties

You can override the following reporting properties at a member level:

- Reporting service, as described in *Starting and Overriding Reporting Service on Members*.
- Report categories, as described in *Overriding Report Categories* on page 973.

Starting and Overriding Reporting Service on Members

The reporting service is disabled by default. You must enable the service for the Grid or on each member so that data is transmitted to the reporting server. When you enable reporting service for the Grid, the service is enabled for all members. You can override this setting at the member level.

To start reporting service on a member:

1. From the **Grid** tab, select the **Grid Manager -> Services** tab -> **member** check box.
2. Select the **Reporting** service on top of the panel.
3. Expand the Toolbar and click **Start**.
4. In the **Start Member Reporting Service** dialog box, click **Start**. Grid Manager starts the reporting service on the selected member.

You can stop the reporting service on a member by selecting the member check box and click **Stop** from the Toolbar. When you stop the reporting service on a member, the member does not transmit data to the reporting server.

To override the reporting service setting on a member:

1. From the **Grid** tab, select the **Grid Manager -> Services** tab -> **member** check box.
2. Click the **Edit** icon, and complete the following in the **Reporting Member Properties** dialog box:
   - **Reporting Settings**: Click **Override**.
   - **Enable data forwarding to the indexer on this member**: Select or deselect this check box.
3. Save the configuration.

Overriding Report Categories

1. From the **Grid** tab, select the **Grid Manager -> Services** tab -> **member** check box.
2. Click the **Edit** icon, and complete the following in the **Reporting Member Properties** dialog box:
   - **Select the data categories to forward**: Click **Override** next to the report category you want to modify and then select or deselect the check box.
3. Save the configuration.
**Scheduling Report Deliveries**

1. From the **Reporting** tab -> Reports tab, select a report dashboard.
2. Click **Schedule** from the Toolbar.
3. In the **Schedule Report Settings** editor, complete the following:
   - **Schedule Report Settings**: Select this check box to enable report delivery.
   - **Run Report Every**: From the drop-down list, select **Hour**, **Day**, **Week**, or **Month**. Depending on your selection, complete the following to define the day and time when the appliance runs the report:
     - **Minutes Past Hour**: When you select **Hour**, enter the number of minutes past the hour.
     - **Time**: When you select **Day**, enter the time of the day.
     - **Time** and **Weekday**: When you select **Week**, enter the time of the day in hh:mm:ss format and select the day of the week from the drop-down list.
     - **Day of Month** and **Time**: When you select **Month**, enter the day of the month and the time in hh:mm:ss format.
   - **Report Format**: All reports are sent in PDF format. You cannot modify this field.
   - **Send to owner**: Select this to send the report to the report owner. This is displayed only for custom reports.
   - **Email List**: Click the Add icon to add an email address to which the report is delivered. Grid Manager adds a row to the table. Select the row and enter the email address. Click the Add icon again to add another email address. You can also select an email address and click the Delete icon to delete it.
4. Click **OK** to save the configuration.

**About Reports**

Infoblox provides predefined reports that are categorized by core network service functions, such as DNS query and system utilization. Predefined reports contain predefined search criteria that retrieve specific data from the reporting database. Each predefined report is associated with a search. You cannot modify predefined searches. For information about searches, see **About Searches** on page 977.

Predefined reports provide summary views for most of the data and trends in your Grid. They are tailored for optimal performance so your reporting server can run them in a reasonable speed under normal circumstances. Though you cannot modify the search criteria for these reports, you can define filters to further refine the report data. For more information about predefined reports, see **About Predefined Reports**. When you select a predefined report from the Reporting -> Reports tab, Grid Manager displays it as a single-panel report.

**Note:** Ensure that you have Flash plug-in installed to view reports.

You can also create a user-defined report by cloning a predefined report and its search or by adding a new report. You can then modify the search criteria for the new report and add new panels to the report. A user-defined report may contain more than one panel, and each panel contains a search, which generates a corresponding report. For example, you can add a report called “DHCP Activities,” and then add DHCP searches, such as DHCP Top Lease Clients and DHCP Lease History, to the new panels. When you save the “DHCP Activities” report, the reporting server saves all the searches in the panels and displays reports with updated data in the “DHCP Activities” report. User-defined reports can provide you with a single point of access when you want to review multiple reports that are relevant to the activities you want to monitor.

Each report comes with a set of available filters that you can use to further refine the report data. Note that filters of different type use the AND logic and filters of the same type use the OR logic. For example, the appliance uses the AND logic when you apply both the “Time” and “A record” filters. It uses the OR logic when you apply the “Member equals marketing.corp100.com” and “Member equals hr.corp100.com” filters.
You can also use quick filters to narrow down the list of reports displayed in the Reports tab. Grid Manager provides the following quick filters: Local Reports, Global Reports, and System Reports. For information about how to use quick filters, see Using Quick Filters on page 57.

You can do the following in reports:

- Use available filters to refine the report data. Each report comes with a set of available filters.
- Change the report format, as described in Changing Report Formats..
- Click Reports to go back to the Reports tab.
- In reports that are in table format, you can sort data based on the following:
  - You can only sort by certain columns, such as Timestamp
  - If all data in a column are numeric, you can sort numerically
  - If data in a column are in string format, the appliance sort by string
- Use the navigation buttons to page through reports that contain multiple pages
- You can mouse over a graph to display the coordinates of any point in the graph.

**Note:** All timestamps displayed in reports and all start and end times you select for a report are based on the time zone you configure on the reporting server, not the Grid Master.

You can do the following to create a user-defined report:

1. Add a new report, as described in Adding New Reports on page 975.
2. Add new panels and searches to the dashboard, as described in Adding New Panels to Reports on page 976.

or

1. Clone an existing predefined report, as described in Adding New Reports on page 975.
2. Modify the search of the new report, if you have cloned the search, as described in Modifying Searches on page 980.

**Adding New Reports**

When you add a new report, Grid Manager displays it in the Reports tab. You can add multiple panels and searches to the new report. For information, see Adding New Panels to Reports on page 976.

To add a new report:

1. From the Reporting tab -> Reports tab, click Add from the Toolbar.
2. In the Reporting Dashboard wizard, complete the following:
   - **Name:** Enter the name of the new report. Use ASCII characters.
   - **Description:** A brief description about this report. You cannot modify this field.
   - **Scope:** Select the Set as Global Report check box if you want to make this report globally available to all users. Only superusers can see this field when creating a new report. Limited-access users cannot see this field. They can only create personal reports.
   - **Comment:** Enter useful information about this dashboard.
3. Click Next to enter extensible attributes
   or
   Save the configuration.

Grid Manager saves the new report and displays it in the Reports tab.
Adding New Panels to Reports

You can add panels to a user-defined report, and then add a search to the newly created panel. When you add a search to the panel, Grid Manager generates the corresponding report in the panel. When you save the report, Grid Manager updates the searches in each panel.

To add a new panel to a new report:

1. From the Reporting tab -> Reports tab, select a user-defined report.
2. In the Reporting Dashboard, click the Add Panel icon.
3. In the Reporting Search Selector dialog box, select a search that you want to place in the panel.
4. Grid Manager displays the following in the new panel:
   - **Panel Title**: Enter the report title here.
   - **Search Name**: Displays the search you have selected. You can click Select to select a new search.
   - **Search Type**: Displays the search type. You cannot modify this.
   - **Search Category**: Displays the search category. You cannot modify this.
   - **Panel Type**: Select the report type from the drop-down list. Depending on the search category, you can select different types of format, such as Table, Line Chart, or Stacked Area.
5. Click Save.

Grid Manager places the panel in the new report.

Note: You can rearrange panels by dragging and dropping them to their desired locations within the report.

Cloning Predefined Reports

To create a user-defined report:

1. From the Reporting tab -> Reports tab, select a report.
2. Click Clone from the Toolbar.
3. From the Clone a Report wizard, complete the following:
   - **Clone Report**: Display the name of the selected report.
   - **Name**: Enter the name of the new report. Use ASCII characters only.
   - **Set as Global Report**: Select the check box to make the new report globally available to all users. Only superusers can see this field when cloning a report. Limited-access users cannot see this field. They can only create personal reports.
   - **Clone Reporting Searches as well**: Select this to clone the search criteria of the report. If you do not select this, the appliance does not clone the search, and you cannot modify the search criteria for the report or add the search to a report panel.
   - The new report contains the same data as the original report. You can modify the search criteria for the new report if you clone its search.
4. Click OK.

Modifying User-defined Reports

1. From the Reporting tab -> Reports tab, select a user-defined report.
2. Click the Edit icon.
3. The Clone a Report editor provides the following tabs from which you can modify data:
   - **General** tab: This tab displays the report name, its description and scope. You cannot modify these fields. You can only modify the comments you entered.
About Searches

— **Delivery Schedule** tab: Modify the delivery schedule of the report. For information, see *Scheduling Report Deliveries* on page 974.
— **Extensible Attribute** tab: Add or modify extensible attributes. For information, see *Using Extensible Attributes* on page 265.
— **Permissions** tab: Add and modify administrative permissions. For information, see *About Administrative Permissions* on page 120.

4. Save the configuration.

Deleting User-defined Reports

1. From the **Reporting** tab -> **Reports** tab, select a user-defined report.
2. Click the Delete icon.
3. The **Delete Confirmation** dialog box, click **Yes**.

About Searches

Searches are criteria the reporting server uses to generate reports. Each predefined report has an associated search. You cannot modify or delete searches for predefined reports. You can however clone a predefined search when you clone its corresponding report. You can also create a new search by cloning an existing search, and then modify the search criteria. When you modify search criteria for a report, ensure that you follow some best practices so you can optimize the performance of your reporting server. For example, define specific and restrictive search criteria for a new report so the reporting server can generate the report in a reasonable speed. Reports with search criteria that involve a large amount of data take longer to generate. Infoblox recommends that you follow some guidelines when modifying searches for new reports. For information about best practices for custom searches, see *Guidelines for Customizing Searches* on page 977.

Note that you can use the same search in multiple reports. You can also use quick filters to narrow down the list of searches displayed in the **Searches** tab. Grid Manager provides the following quick filters: Local Searches, Global Searches, System Searches, and Scheduled Searches. For information about how to use quick filters, see *Using Quick Filters* on page 57.

To create a new search, complete the following:

1. Clone an existing search, as described in *Cloning Searches* on page 980.
2. Modify the settings of the new search, as described in *Modifying Searches* on page 980.
3. Schedule how often the reporting server runs the search. By default, the reporting server runs a predefined search only when you open a report. For DHCP Lease History report however, the search is scheduled hourly by default. For information about scheduling a search, see *Scheduling Searches* on page 981.

You can also do the following in the **Searches** tab:

- Export search data in XML or CSV format, as described in *Exporting Searches* on page 982.
- Schedule the export of search data, as described in *Scheduling Exports of Search Results* on page 982.

Guidelines for Customizing Searches

When you follow some best practices for searching, you can optimize the performance of your reporting server and be able to view and manage your reports more efficiently. Depending on the type of search and the data you want to search for, Infoblox highly recommends that you use the following guidelines:

- Specify shorter start and end times when running detailed reports. When you define a long duration of time, more data is included in the search, and the server takes longer to process the data.
- Be specific about the fields that you want to include in the search. The more specific and restrictive you define your search criteria, the faster the search is. For example, if you want to view DHCP lease history for a specific member, modify the search criteria to include only that member.
When you define how often the reporting server runs a search, be aware of other searches that the server is running as well. For example, when you schedule the server to run many searches at the same time, the server performance can be negatively affected. Try to stagger your searches whenever possible.

Scheduling a search can minimize the workload on the reporting server. When you schedule a search, Grid Manager displays pre-existing report data, and this can reduce the workload on the reporting server. Though you can open a report each time you want to see up-to-date report data, on-demand searches can put more workload on the reporting server and may affect other searches and system performance.

Create custom searches or detailed searches only when necessary. Infoblox provides predefined summary reports for most of the data and trends in your Grid. These reports are tailored for optimal performance so your reporting server can run them in a reasonable speed under normal circumstances. Summary reports collect events that have happened during a certain time period, and then summarizes the data before an update occurs. Since there are less raw data involved in a summary report than in a detailed report, summary reports take less time to generate. Though you cannot see identical results between a summary report and a detailed report, creating too many detailed searches or reports may affect your system performance. Note that the reporting server categorizes each detailed and summary report by indexes; and each index updates its data at different time intervals. You can use this information to determine the best way to obtain information you need without overloading the reporting server. For information about update frequencies for each report, see Reporting Indexes and Update Time Intervals on page 978.

Take into consideration the daily maximum data consumption for your reporting server. Ensure that you select only the reports that you need from each Grid member so the reporting server is not overloaded with traffic. You can disable the reporting service on specific members to avoid unnecessary data transmissions. For information about daily maximum data consumption, see Supported Platforms for Reporting on page 970.

Review the daily data usage to avoid license violation. You can view the data usage from the Member Status widget in the Status Dashboard. When the data usage on the reporting server approaches or reaches the daily maximum, the appliance sends an SNMP trap and email notification, if configured. When you receive five (5) violation notifications in a rolling period of 30 days, you cannot view reports or configure report related functions. You must then contact Infoblox Technical Support to resolve the issue.

**Note:** The reporting server continues to process incoming data during the violation state. However, you cannot view any reports or manage any report related functions until you fix the violation issue.

### Reporting Indexes and Update Time Intervals

*Table 35.3* lists the search indexes that the reporting server uses to generate reports. It contains information about the frequency of summary report updates for each report. Use this information to plan your reporting strategy for the Grid so you can optimize the performance of the reporting server.

Each summary report or search has its own update frequency. For example, the DNS Top Requested Domain report updates its data every 30 minutes, starting at the 4th minute of the hour. It collects report data during the first 30 minutes of the previous 60 minutes. For example, if the report starts an update at 6:04 a.m., the data it collects is from 5:04 a.m. to 5:34 a.m.

*Table 35.3 Reporting Indexes*

<table>
<thead>
<tr>
<th>Indexes</th>
<th>Reports</th>
<th>Report Data Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Lease History</td>
<td>DHCP Lease History</td>
<td>Every 30 minutes, starting at the 16th minute of</td>
</tr>
<tr>
<td>(Summary)</td>
<td></td>
<td>the hour. Data covers the first 30 minutes of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the previous 60 minutes.</td>
</tr>
<tr>
<td></td>
<td>DHCP Top Lease Clients</td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>DDNS Update Rate Trend</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Replies Trend</td>
<td></td>
</tr>
<tr>
<td><strong>Indexes</strong></td>
<td><strong>Reports</strong></td>
<td><strong>Report Data Updates</strong></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>DNS Response Latency Trend</td>
<td>DNS Top Clients</td>
<td>Every 30 minutes, starting at the 2nd minute of the hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
</tr>
<tr>
<td>DNS Top Clients</td>
<td>DNS Top Requested Domain Names</td>
<td>Every 30 minutes, starting at the 4th minute of the hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
</tr>
<tr>
<td>DNS Top Requested Domain Names</td>
<td>DDNS Update Rate Trend (Summary)</td>
<td>Every 30 minutes, starting at the 6th minute of the hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
</tr>
<tr>
<td>DNS Query Rate by Query Type</td>
<td>DNS Cache Hit Rate Trend (Summary)</td>
<td>Every 30 minutes, starting at the 8th minute of the hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
</tr>
<tr>
<td>DNS Query Rate by Server</td>
<td>DNS Query Rate by Query Type (Summary)</td>
<td>Every 30 minutes, starting at the 10th minute of the hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
</tr>
<tr>
<td>DNS Summary</td>
<td>DNS Query Rate by Server (Summary)</td>
<td>Every 30 minutes, starting at the 12th minute of the hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
</tr>
<tr>
<td></td>
<td>DNS Replies Trend (Summary)</td>
<td>Every 30 minutes, starting at the 18th minute of the hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
</tr>
<tr>
<td></td>
<td>DNS Response Latency Trend (Summary)</td>
<td>Every 30 minutes, starting at the 20th minute of the hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
</tr>
<tr>
<td>DHCP</td>
<td>DHCP Message Rate Trend</td>
<td>Every 30 minutes, starting at the 14th minute of the hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
</tr>
<tr>
<td></td>
<td>DHCPv4 Usage Statistics</td>
<td>Every 8 hours, starting at the 22th minute of the hour. Data covers the first 8 hours of the previous 8.25 hours.</td>
</tr>
<tr>
<td></td>
<td>DHCPv4 Top Utilized Networks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DHCPv4 Usage Trend</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DHCPv4 Range Utilization Trend</td>
<td></td>
</tr>
<tr>
<td>DHCP Summary</td>
<td>DHCP Message Rate Trend (Summary)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DHCPv4 Usage Trend (Summary)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DHCPv4 Range Utilization Trend (Summary)</td>
<td></td>
</tr>
<tr>
<td>IPAMv4</td>
<td>IPAM Network Usage</td>
<td></td>
</tr>
</tbody>
</table>
Cloning Searches

You can select an existing search and clone it. When you clone a search, you can give it a different name and make it globally available to other users.

To clone a search:

1. From the Reporting tab -> Searches tab, select a search you want to clone.
2. Click the Clone icon.
3. In the Clone a Search dialog box, complete the following:
   — **Clone Search**: Display the name of the original search.
   — **Name**: Enter a name for the new search. You can enter up to 255 ASCII characters.
   — **Set as Global Search**: Select this check box if you want to make this search globally available to all users.

The new search contains the same search criteria as the original search. You can modify the search criteria for the new search. For information, see Modifying Searches.

Modifying Searches

1. From the Reporting tab -> Searches tab, select the search you want to modify.
2. Click the Edit icon.
3. The Searches editor provides the following tabs from which you can modify data:
   — **General** tab: This tab displays the search name, its description, category, and scope. You cannot modify these fields. You can however modify the report type and comments.

   **Note:** When you change the report type, the appliance removes all the query items from the current search.

   — **Settings** tab: You can redefine the filter settings for the search in this tab, as follows:
     — In the first drop-down list, select a field as the filter.
— 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.
— Optionally, click + to add another filter. You can also click - to delete a filter.

**Note:** Filters of different type use the AND logic and filters of the same type use the OR logic. For example, the
appliance uses the AND logic when you apply both the “Time” and “A record” filters. It uses the OR logic
when you apply the “Member equals marketing.corp100.com” and “Member equals hr.corp100.com”
filters. Be specific and restrictive when you define the search criteria. For information about best practices
for searches, see *Guidelines for Customizing Searches* on page 977.

— **Schedule** tab: Modify the search schedule, as described in *Scheduling Searches*.
— **Extensible Attribute** tab: Add or modify extensible attributes. For information, see *Using Extensible
Attributes* on page 265.
— **Permissions** tab: Add and modify administrative permissions for this search object. For information, see
*About Administrative Permissions* on page 120.

4. Save the configuration.

### Scheduling Searches

When you schedule a search, the appliance runs the search based on your configuration. The appliance also
overrides the scheduled search if you open a report before the first scheduled search of the report. This also applies
to the predefined *DHCP Lease History* report. Though you can only schedule searches for user-defined reports, you
can run a search for a predefined report each time you open the report.

To schedule a search:

1. From the Reporting tab -> Searches tab, select a user-defined search.
2. Click the Edit icon.
3. In the Searches editor, select the Schedule tab and complete the following:
   — **Run search each time report dashboard loads:** When you select this, the appliance updates the report
dashboard each time you open the report, based on the search criteria.
   — **Run search once:** When you select this, the appliance runs the search based on your settings:
     — **Day of Month:** Enter the day of the month you want to run the search.
     — **Time:** Enter a time in hh:mm AM/PM format or select a time from the wizard.
   — **Recurrence:** When you select this, the appliance updates the report dashboard based on the frequency you
define here.
     — **Run search every:** Enter a frequency and then from the drop-down list, select Months, Weeks, Days,
or Hours. Note that the frequency you enter and select here may affect the overall performance of your
reporting server. For more information about how to optimize your searches, see *Guidelines for
Customizing Searches* on page 977.
4. Save the configuration.
Exporting Searches

You can export the data in the selected search in CSV (comma separated value) or XML format. This may take a long time depending on the amount of data you want to export.

To export data in a selected search:
1. From the Reporting tab -> Searches tab, select the search that you want to export.
2. Select the Export icon -> Export Search Results.
3. In the Export Search Results editor, complete the following:
   — **File name**: Enter the file name. You can enter up to 255 ASCII characters. Note that when you export a search, the appliance includes the file extension of .csv and .xml in the total number of characters. If you have a file name that contains 252 characters, the appliance cannot export the file because the file name exceeds the maximum number of characters.
   — **Format**: Select a format from the drop-down list.
   — **Max # of results to export**: Define the maximum number of data lines you want to export. The default is 10,000.

Scheduling Exports of Search Results

You can schedule the export of search data.

To schedule the export of search data:
1. From the Reporting tab -> Searches tab, select the search that you want to export.
2. Select the Export icon -> Schedule Export Search Results.
3. In the Schedule Export editor, complete the following:
   — **Reporting Search**: Click Select and select a user-defined report from the Reporting Search Selector. Note that you can only select user-defined searches.
   — **Disable Schedule**: Select this check box to disable the scheduling at this time. You can still save the configuration of this task.
   — **Format**: Select a format from the drop-down list.
   — **Export to**: Select the type of server to which you plan to export the data from the drop-down list.
     — **FTP**: Export the search results to an FTP server. This is the default.
       • **IP Address of FTP Server**: The IP address of the FTP server.
       • **Directory Path**: Enter the directory path and the file name of the export file. For example, you can enter /export/Infoblox_2009_10_20_15_30 on a Linux server, or c:\export\Infoblox_2009_10_20_15_30 on a Microsoft Windows server.
       • **Username**: Enter the username of your FTP account.
       • **Password**: Enter the password of your FTP account.
     — **SCP**: Export the search results to a SCP server.
       • **IP Address of SCP Server**: The IP address of the SCP server.
       • **Directory Path**: Enter the directory path and the file name of the export file. For example, you can enter /export/Infoblox_2009_10_20_15_30 on a Linux server, or c:\export\Infoblox_2009_10_20_15_30 on a Microsoft Windows server.
       • **Username**: Enter the username of your SCP account.
       • **Password**: Enter the password of your SCP account.
     — **TFTP**: Export the search results to a TFTP server.
       • **IP Address of FTP Server**: The IP address of the TFTP server.
       • **Directory Path**: Enter the directory path and the file name of the export file. For example, you can enter /export/Infoblox_2009_10_20_15_30 on a Linux server, or c:\export\Infoblox_2009_10_20_15_30 on a Microsoft Windows server.
— **Recurrence**: Select *Once* or *Repeat* from the drop-down list, and then complete the following accordingly:
— **Frequency**: For *Repeat* only. From the drop-down list, select DAILY, HOURLY, WEEKLY, or MONTHLY.
— **Day of Month**: Enter the day of month you want to run the search.
— **Time**: Enter a time in hh:mm:ss AM/PM format or select a time from the wizard.
About Predefined Reports

To view all available reports, from the Reporting tab, select the Reports tab. Grid Manager displays a list of predefined reports that you have selected when you set up your Grid or member reporting properties. You cannot modify or delete predefined reports or the search criteria of predefined reports. You can however modify user-defined reports. For information about how to create user-defined reports, see Managing Reports on page 993.

Predefined reports are classified in the following categories: DDNS, DHCP Lease, DHCP Performance, DNS Query, DNS Performance, IPAM Utilization, and System. You can select the categories of report data you want the members to forward to the reporting server. For information about selecting report categories, see Configuring General Reporting Properties on page 971. No report categories are selected by default.

Changing Report Formats

All predefined reports are displayed in default formats, such as line graphs or tables. You can change the presentation of certain reports by selecting an available format.

To change the report format:
1. From the Reporting tab -> Reports tab, select a report.
2. In the Reporting Dashboard, click the Configure icon.
3. In the Configuration panel, complete the following:
   — Panel Type: Select the report type from the drop-down list. Depending on the search category, you can select different types of format, such as table, line chart, or stacked area.
   
   Grid Manager displays the report in the selected format.

You can view the following report dashboards in the Reports tab:

DDNS Query
   DDNS Update Rate Trend

DHCP Lease
   DHCP Lease History
   DHCP Top Lease Clients

DHCP Performance
   DHCPv4 Usage Statistics
   DHCPv4 Range Utilization Trend
   DHCPv4 Usage Trend
   DHCP Message Rate Trend

DNS Performance
   DNS Query Rate by Query Type
   DNS Query Rate by Server
   DNS Response Latency Trend

DNS Query
   DNS Top Requested Domain Names
   DNS Cache Hit Rate Trend
   DNS Top Clients
   DNS Replies Trend
About Predefined Reports

IPAM Reports
- IPAMv4 Network Usage Statistics
- DNS Zone Statistics Per DNS View
- IPAMv4 Top Utilized Networks
- DHCPv4 Top Utilized Networks

System Reports
- CPU Utilization Trend
- Memory Utilization Trend
- Traffic Rate

DDNS Update Rate Trend

The DDNS Update Rate Trend report provides information about the dynamic DNS (DDNS) updates that occur on the DNS service. The default report shows a line graph that tracks the rate of DDNS updates (counts per second) by query type in the given time frame.

This report displays DDNS updates per second by the following query type: Success, Failure, Reject, and Prerequisite Reject. The time is displayed according to the time zone specified on the reporting server in UTC format. You can mouse over the graph to display the coordinates of any point in the graph.

You can also use filters to get specific information in this report. This report provides the following filters:
- **Time**: Filter by last day, last week, last month, or last year.
- **Start Time**: Specify a start time.
- **End Time**: Specify an end time.
- **Members**: Filter by a specific member.
- **Response Type**: Filter by Success, Failure, Reject, or Prerequisite Reject.
- **Source IP Address**: Specify an IP address of the requesting source.
- **DNS Zone**: Filter by a specific DNS zone.

DHCP Lease History

The DHCP Lease History report provides DHCP lease history in a given time frame. The search of the DHCP Lease History report is scheduled hourly by default.

**Note:** When you join a new member to the Grid and do not start reporting service on the member, lease history for this member is not captured in the DHCP Lease History report. You can view lease history for this member in the Data Management tab -> DHCP tab -> Leases tab.

The default report displays the following information in table format:
- **Time**: Filter by last minute, last day, last week, last month, or last year.
- **Start Time**: Specify a start time.
- **End Time**: Specify an end time.
- **Members**: The DHCP member that granted the lease.
- **Member IP**: The IP address of the DHCP member that granted the lease.
- **Lease IP**: The IP address of the lease.
- **Protocol**: Indicates whether the lease is for an IPv4 or IPv6 address.
- **Action**: The status of the lease. This can be one of the following: Issued, Renewed, Freed, or Abandoned.
- **Hostname**: The host name that the DHCP client sent to the appliance using DHCP option 12.
- **MAC/DUID**: For an IPv4 address, this is the MAC address of the lease. For an IPv6 address, this is the DUID (DHCP Unique Identifier) of the DHCP client that received the lease.
• **Lease Start**: The timestamp when the lease started.
• **Lease End**: The timestamp when the lease ended.

You can use any of the displayed fields, plus the start time and end time, as filters to get specific information in this report.

**DHCP Top Lease Clients**

The *DHCP Top Lease Clients* report provides information about the DHCP clients that have issued, renewed, and freed within a certain time frame.

This report shows the following information:
• **MAC/DUID**: The MAC address or DUID of the DHCP client.
• **Issued**: The total number of DHCP lease issued.
• **Renewed**: The number of DHCP lease renewals.
• **Freed**: The number of leases that were released.
• **MAC/DUID Total**: The total number of DHCP leases that were being requested, renewed, and released.

You can use filters to get specific information in the report. This report provides the following filters:
• **Time**: Filter by last day, last week, last month, or last year.
• **Start Time**: Specify a start time.
• **End Time**: Specify an end time.
• **Members**: Filter by a specific member.
• **TopN**: The number of DHCP clients that have requested the most leases.
• **Report On**: Filter by leases that were issued, renewed, or freed.

**DHCPv4 Usage Statistics**

The *DHCPv4 Usage Statistics* report provides the overall DHCPv4 usage in a given time frame. The default report includes all network views, all members, all subnets, all IPv4 addresses, and all DHCP ranges, and the default time frame is the last hour. The table is sorted by DHCP utilization rate.

This report displays the following information in table format:
• **Timestamps**: The date and time of the event.
• **Network View**: Filter by a specific network view.
• **Network**: The network address.
• **CIDR**: The subnet mask in CIDR format.
• **DHCPv4 Utilization**: The percentage of DHCP address in use over the total number of DHCP addresses provisioned.
• **Ranges**: The total number of IP address ranges in the network.
• **Provisioned**: The total number of DHCP addresses configured.
• **Dynamic**: The number of dynamic DHCP leases issued.
• **Static**: The number of static DHCP addresses configured.
• **Free**: The number of free DHCP addresses.
• **Used**: The total number of DHCP addresses in use.

You can use filters to get specific information in the report. This report provides the following filters:
• **Time**: Filter by last day, last week, last month, or last year.
• **Start Time**: Specify a start time.
• **End Time**: Specify an end time.
• **Members**: Filter by a specific member.
• **Network View**: Filter by a specific network view.
• Network: Filter by a specific network.
• CIDR: Filter by the subnet mask in CIDR format.
• Utilization Rate: Filter by the percentage of DHCP address in use over the total number of DHCP addresses provisioned.

**DHCPv4 Range Utilization Trend**

The *DHCPv4 Range Utilization Trend* report provides DHCP usage trends for the top five most utilized address ranges in a given time frame. The default report includes the top five most utilized DHCP ranges among all network views, all members, all subnets, and all IPv4 addresses.

The default report displays line graphs for the top five most utilized address ranges and shows their DHCPv4 usage trends over the last 24 hours. Each of the five address ranges is represented with a different color line graph.

You can use filters to get specific information in the report. This report provides the following filters:

- Time: Filter by last day, last week, last month, or last year.
- Start Time: Specify a start time.
- End Time: Specify an end time.
- Members: Filter by all members or a specific member.
- Network: Filter by IPv4 addresses.
- DHCP Ranges: Filter by a specific DHCP range. The default is the top five most utilized address ranges.

**DHCPv4 Usage Trend**

The *DHCPv4 Usage Trend* report provides the overall DHCP usage trend for all members in a given time frame. The default report includes information about all DHCP ranges in all network views, all members, all subnets, and all IPv4 addresses. It displays line graphs for the dynamic, static, and free DHCPv4 leases and shows their DHCPv4 usage trends over the last 24 hours. Each of the DHCPv4 leases is represented with a different color line graph.

You can also select to display this report in table format with the following information:

- Time: The timestamp of the event.
- Dynamic: The number of dynamic DHCP leases issued.
- Static: The number of static DHCP addresses configured.
- Free: The number of free DHCP addresses.

Each of the line graphs is represented with a different color.

You can use filters to get specific information in the report. This report provides the following filters:

- Time: Filter by last day, last week, last month, or last year.
- Start Time: Specify a start time.
- End Time: Specify an end time.
- Members: Filter by all members or a specific member.
- DHCP Ranges: Filter by a specific DHCP range.

When you select more than one member as the filter criteria, the report displays line graphs for each of the following data: Dynamic, Static, and Free, for each selected member.
DHCP Message Rate Trend

The DHCP Message Rate Trend report provides the overall DHCP message rate trends for DHCP message types in a given time frame. The default report displays the actual, maximum, average, and minimum rate trends in the last 24 hours for the following message types: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, and DHCPACK.

You can also select to display this report in table format with the following information:

- **Time**: The timestamp of the event.
- **DHCPDISCOVER**: The actual rate trend of the DHCPDISCOVER messages.
- **DHCPOFFER**: The actual rate trend of the DHCPOFFER messages.
- **DHCPREQUEST**: The actual rate trend of the DHCPREQUEST messages.
- **DHCPACK**: The actual rate trend of the DHCPACK messages.

Each of the line graphs is represented with a different color.

You can use filters to get specific information in the report. This report provides the following filters:

- **Time**: Filter by last day, last week, last month, or last year.
- **Start Time**: Specify a start time.
- **End Time**: Specify an end time.
- **DHCP Message Type**: Filter by a specific DHCP message type. The default includes all message types.
- **Member**: Filter by all members or a specific member.
- **Protocol**: Filter by IPv4 or IPv6 addresses.
- **Statistics**: Filter by minimum, average, or maximum rate. The default is None, which means the report displays only the actual rate trend.

DNS Query Rate by Query Type

The DNS Query Rate by Query Type report shows the trend of DNS queries per second by DNS record type. This report displays line graphs of DNS query trends for selected DNS record types over a given time frame.

You can also use filters to get specific information in this report. This report provides the following filters:

- **Time**: Filter by last day, last week, last month, or last year.
- **Start Time**: Specify a start time.
- **End Time**: Specify an end time.
- **Member**: Filter by all members or a specific member.
- **Record Type**: Filter by a specific record type.

DNS Query Rate by Server

The DNS Query Rate by Server report shows the trend of DNS queries for selected members. This report displays line graphs of DNS query trends for the selected members over a given time frame.

You can also use filters to get specific information in this report. This report provides the following filters:

- **Time**: Filter by last day, last week, last month, or last year.
- **Start Time**: Specify a start time.
- **End Time**: Specify an end time.
- **Members**: Filter by all members or a specific member.
DNS Response Latency Trend

The *DNS Response Latency Trend* report provides DNS latency response times for all or selected cache servers. This report shows line graphs of DNS latency response times for each server.

You can use filters to get specific information in the report. This report provides the following filters:

- **Time**: Filter by last day, last week, last month, or last year.
- **Start Time**: Specify a start time.
- **End Time**: Specify an end time.
- **Members**: Filter by specific members.

DNS Top Requested Domain Names

The *DNS Top Requested Domain Names* report lists the top most requested domain names, their counts and the percentage of request over a given time frame. The report shows horizontal bar charts that list the total counts and request percentage for the top most requested domain names. The default report displays the top 10 domain names within the last 24 hours.

You can use filters to get specific information in this report. This report provides the following filters:

- **TopN**: Filter by the number of the top most requested domain names.
- **Time**: Filter by last day, last week, last month, or last year.
- **Start Time**: Specify a start time.
- **End Time**: Specify an end time.
- **Members**: Filter by all members or a specific member.
- **TLD**: Filter by the top-level domain, such as .com, .edu, or .org.

DNS Cache Hit Rate Trend

The *DNS Cache Hit Rate Trend* report provides information about the cache hit ratio of selected Grid members. The report shows line graphs that track cache hit rates over a given time frame. Note that if you have one member with two DNS views with requests sent to only one DNS view, the maximum hit rate is 50%, not 100%, for the member because one of the DNS view has 100% hit rate and the other has 0, and the average is 50%.

You can also use filters to get specific information in this report. This report provides the following filters:

- **Time**: Filter by last day, last week, last month, or last year.
- **Start Time**: Specify a start time.
- **End Time**: Specify an end time.
- **Members**: Filter by all members or a specific member.

DNS Top Clients

The *DNS Top Clients* report lists clients that have the most DNS queries. The report shows horizontal bar charts that list clients that have the most total counts of DNS requests and their percentages over a given time frame. The default report displays the top 10 clients within the last 24 hours.

You can use filters to get specific information in this report. This report provides the following filters:

- **TopN**: Filter by the number of clients that have the top most DNS queries.
- **Time**: Filter by last day, last week, last month, or last year.
- **Start Time**: Specify a start time.
- **End Time**: Specify an end time.
- **Member**: Filter by all members or a specific member.
DNS Replies Trend

The DNS Replies Trend report provides information about DNS query trends by message types. The report shows line graphs that track DNS query replies by message type over a given time frame.

This report displays line graphs of DNS query replies by the following query type: Failure, NXDomain, NXRRset, Referral, Success, Refused, and Other.

You can also use filters to get specific information in this report. This report provides the following filters:

- Time: Filter by last day, last week, last month, or last year.
- Start Time: Specify a start time.
- End Time: Specify an end time.
- Member: Filter by all members or a specific member.
- Response Type: Filter by NXDomain, NXRRset, Referral, Success, and Refused.

IPAMv4 Network Usage Statistics

The IPAMv4 Network Usage Statistics report provides usage statistics for each network in a given time frame. This report displays the following information in table format:

- Timestamp: The timestamp when the network container was created.
- Network View: The network view.
- CIDR: The subnet mask in CIDR format.
- DHCPv4 Utilization %: The percentage of DHCP addresses in use over the total number of DHCP addresses provisioned.
- CIDR: The subnet mask in CIDR format.
- Total: The total number of IPAM addresses in the network.
- Allocated: The number of allocated IP addresses in the network.
- Reserved: The number of reserved IP addresses in the network.
- Assigned: The number of assigned IP addresses in the network.
- Utilization %: The percentage of IP address in use over the total number of IP addresses in the network.
- Unmanaged: The number of discovered IP addresses that do not have corresponding records on the appliance, such as A records, PTR records, fixed address records, host records, or leases.

You can also use filters to get specific information you want in this report. This report provides the following filters:

- Time: Filter by last day, last week, last month, or last year.
- Start Time: Specify a start time.
- End Time: Specify an end time.
- Network View: Filter by a specific network views.
- Utilization Rate: Filter by the utilization percentage.

DNS Zone Statistics Per DNS View

The DNS Zone Statistics Per DNS View report provides DNS zone statistics for each DNS view in a given time frame. The default report includes information for all network views, all members, all IPv4 and IPv6 reverse-mapping zones, all forward-mapping zones, and all DNS records by record type.

This report displays the following information in table format:

- Timestamp: The date and time of the event.
- View: The DNS view.
- Members: The FQDN of the member that is associated with the DNS view.
• Forward-Mapping Zone: The number of forward-mapping zones.
• IPv4 Reverse-Mapping Zone: The number of IPv4 reverse-mapping zones.
• IPv6 Reverse-Mapping Zone: The number of IPv6 reverse-mapping zones.
• Signed Zone: The number of signed zones.
• Host: The number of host records.
• Total Records: The total number of DNS resource records.

Grid Manager also displays the number of each relevant DNS resource records.

You can also use filters to get specific information in this report. This report provides the following filters:
• Time: Filter by last day, last week, last month, or last year.
• Start Time: Specify a start time.
• End Time: Specify an end time.
• Member: Filter by specific members.
• DNS View: Filter by specific DNS views.

### IPAMv4 Top Utilized Networks

The *IPAMv4 Top Utilized Networks* report provides statistics about the top most utilized IPv4 networks. The default report includes the top 10 most utilized networks within the last hour.

This report displays the following information in table format:
• Timestamp: The date and time of the recorded utilization.
• Network View: The network view.
• Network: The network address.
• CIDR: The subnet mask in CIDR format.
• DHCPv4 Utilization %: The percentage of IP address in use over the total number of IP addresses in the network.
• Total: The total number of IP addresses in the network.
• Assigned: The total number of IP addresses assigned in the network.
• Reserved: The total number of reserved IP addresses in the network.
• Unmanaged: The number of discovered IP addresses that do not have corresponding records on the appliance, such as A records, PTR records, fixed address records, host records, or leases.

You can use filters to get specific information in this report. This report provides the following filters:
• Time: Filter by last day, last week, last month, or last year.
• Start Time: Specify a start time.
• End Time: Specify an end time.
• Member: Filter by all members or a specific member.
• TopN: The number of the top most utilized networks. The default is 10.

### DHCPv4 Top Utilized Networks

The *DHCPv4 Top Utilized Ranges* report provides statistics about the top most utilized DHCPv4 networks. The default report includes the top 10 most utilized DHCPv4 networks within the last 24 hours.

This report displays the following information in table format:
• Timestamp: The date and time of the recorded utilization.
• Network View: The network view.
• Network: The network address.
• CIDR: The subnet mask in CIDR format.
• DHCPv4 Utilization %: The percentage of DHCP addresses in use over the total number of DHCP addresses provisioned.
- **Ranges**: The number of DHCP address ranges in the network.
- **Provisioned**: The total number of IP addresses in the range.
- **Dynamic**: The number of dynamic IP addresses in the range.
- **Static**: The number of static IP addresses in the range.
- **Free**: The number of free DHCP addresses.
- **Used**: The total number of IP addresses in use.

You can use filters to get specific information in this report. This report provides the following filters:
- **Time**: Filter by last day, last week, last month, or last year.
- **Start Time**: Specify a start time.
- **End Time**: Specify an end time.
- **Member**: Filter by all members or a specific member.
- **TopN**: The number of the top most utilized networks. The default is 10.

### CPU Utilization Trend

The *CPU Utilization Trend* report provides CPU usage trends over a given time frame. The default report displays line graphs that show CPU usage trends for all members in the Grid over the last 24 hours. Each of the members is represented with a different color line graph.

You can use filters to get specific information in the report. This report provides the following filters:
- **Members**: Filter by specific members.
- **Time**: Filter by last day, last week, last month, or last year.
- **Start Time**: Specify a start time.
- **End Time**: Specify an end time.

### Memory Utilization Trend

The *Memory Utilization Trend* report provides memory usage trends over a given time frame. The default report displays line graphs that show memory usage trends for all members in the Grid over the last 24 hours. Each of the members is represented with a different color line graph.

You can use filters to get specific information in the report. This report provides the following filters:
- **Members**: Filter by specific members.
- **Time**: Filter by last day, last week, last month, or last year.
- **Start Time**: Specify a start time.
- **End Time**: Specify an end time.

### Traffic Rate

The *Traffic Rate* report provides inbound and outbound traffic over a given time frame. The report displays line graphs that show traffic rate for members with reporting service enabled within the last 24 hours. Grid Manager uses different color line graphs to distinguish inbound and outbound traffic for different members.

You can use filters to get specific information in the report. This report provides the following filters:
- **Members**: Filter by all members or specific members.
- **Time**: Filter by the last day, last week, last month, or last year.
- **Start Time**: Specify a start time.
- **End Time**: Specify an end time.
Managing Reports

You can do the following to manage predefined and user-defined reports in the Reporting tab:

- Print predefined and user-defined reports, as described in Printing Reports.
- Back up the reporting database manually, as described in Backing Up Reporting Data.
- Schedule the backup of the reporting database, as described in Scheduling the Backup of the Reporting Database on page 994.
- Restore the reporting database on the reporting server, as described in Restoring the Reporting Database on page 995.

Printing Reports

1. From the Reporting tab -> Reports tab, click a report name.
2. In the Reporting Dashboard, click the Print icon.
   Grid Manager displays the list of reports in another window.
3. Click Print.

Backing Up Reporting Data

Before you back up the reporting database, ensure that the reporting service is enabled on the reporting server. You cannot perform or schedule a backup if the reporting service is disabled on the reporting server. If you want to upgrade your reporting server, back up all the data before you power down the server.

Note that reporting data backups are incremental backups, which means that backup files are copied to the designated file server only when there are new events generated since the last backup.

You can manually back up the reporting database or schedule a backup, but you cannot perform both at the same time.

You can perform the following reporting data backups:

- Manual backups, as described in Backing Up the Reporting Database Manually.
- Scheduled backups, as described in Scheduling the Backup of the Reporting Database on page 994.

Backing Up the Reporting Database Manually

1. From the Grid tab, select Backup -> Reporting Backup -> Manual Backup from the Toolbar.
2. In the Manual Reporting Backup editor, complete the following:
   - **Status**: Displays the status of the backup process, if in progress.
   - **Backup to**: Select the destination of the backup file from the drop-down list:
     - **FTP**: Back up the reporting database to an FTP server.
       - **Filepath**: Enter the directory path. For example, you can enter `/archive/backups/Infoblox/` on a Linux server, or `c:\archive\backups\Infoblox\` 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 the reporting database to an SSH server that supports SCP.
       - **Filepath**: Enter the directory path. For example, you can enter `/archive/backups/Infoblox/` on a Linux server, or `c:\archive\backups\Infoblox\` 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.

Scheduling the Backup of the Reporting Database

1. From the Grid tab, select Backup -> Reporting Backup -> Schedule Backup from the Toolbar.
2. In the Schedule Reporting Backup editor, complete the following:
   - Status: Displays the status of the backup process, if in progress.
   - Select the destination of the backup file from the Backup to drop-down list:
     - FTP: Back up the reporting database files to an FTP server.
       - IP Address of FTP Server: The IP address of the FTP server.
       - Directory Path: Enter the directory path. 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 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.
       - 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 the reporting database 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 FTP 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.
Restoring the Reporting Database

Restoring the reporting database may take a long time to perform, and the reporting service is unavailable during a restore. Ensure that you must restore the reporting database before you perform the operation.

Note the following during a restore:

- The reporting service is unavailable.
- Existing reporting data is removed from the reporting server.
- Backup data is restored up to the amount the reporting server can accommodate.

1. From the Grid tab, select **Restore -> Restore Reporting** from the Toolbar.
2. In the Restore dialog box, complete the following:
   - **Status**: Displays the status of the restore process, if in progress.
   - **Restore from**: Select the destination of the backup file.
     - **FTP**: Restore the reporting backup files from a FTP server.
       - **Filepath**: Enter the directory path. For example, you can enter `/archive/backups/Infoblox/` on a Linux server, or `c:\archive\backups\Infoblox\` 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**: Restore the reporting backup files from a SCP server.
       - **Filepath**: Enter the directory path. For example, you can enter `/archive/backups/Infoblox/` on a Linux server, or `c:\archive\backups\Infoblox\` 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.
3. Click **Restore**.
Part 8 Reference

This section provides reference information in the following appendices:

- Appendix A, "Glossary of Terms", on page 999
- Appendix B, "Grid Manager Icons", on page 1007
- Appendix C, "Regular Expressions", on page 1013
- Appendix D, "vNIOS Appliance Limitations", on page 1015
- Appendix E, "Product Compliance", on page 1017
- Appendix F, "Open Source Copyright and License Statements", on page 1025
Appendix A Glossary of Terms

The following table provides descriptions of some key terminology used in the Infoblox products. Some terms, such as Grids and high availability, are used in different ways by other networking product vendors. The alphabetically arranged table can help you understand the terms and concepts as Infoblox uses them and as they are used in this guide.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Node</strong></td>
<td>The NIOS appliance in an HA (high availability) pair that receives, processes, and responds to all service requests. When an HA failover occurs, the active node becomes the passive node in the HA pair.</td>
</tr>
<tr>
<td><strong>API (Application Programming Interface)</strong></td>
<td>A set of rules and specifications that software programs follow to communicate with each other. It serves as an interface between different software programs and facilitates their interaction. Infoblox provides a Perl API to help facilitate the integration of Infoblox NIOS appliances into network environments. It is an alternate method to the GUI (graphical user interface) in which you use a mouse pointer to click and select options and items to perform tasks.</td>
</tr>
<tr>
<td><strong>Authenticated DHCP</strong></td>
<td>The process of authenticating a network device before a DHCP server assigns a lease. On Infoblox appliances, you can divide a network into segments for unauthenticated, authenticated, and guest users. The Infoblox DHCP server assigns clients to the appropriate segment based on their MAC addresses and authentication credentials.</td>
</tr>
<tr>
<td><strong>BIND (Berkeley Internet Name Domain)</strong></td>
<td>The most commonly used DNS server on the Internet. It allows for a standard way of naming objects and resource records in distributed UNIX environments. It also provides operations for storing and retrieving information about these objects and records.</td>
</tr>
<tr>
<td><strong>bloxSYNC</strong></td>
<td>An Infoblox proprietary mechanism for secure, real-time synchronization of the database that maintains the data, system configuration, and protocol service configuration between the active and passive nodes of an HA pair. With bloxSYNC, the nodes continuously synchronize changes of their configurations and states. When a failover occurs, the passive node can quickly take over services from the active node.</td>
</tr>
<tr>
<td><strong>bloxTools</strong></td>
<td>An Infoblox pre-installed environment that provides tools for creating custom applications that facilitate administrative tasks for an organization.</td>
</tr>
<tr>
<td><strong>Bulk Host</strong></td>
<td>If you need to add a large number of A and PTR records, you can have the NIOS appliance add them as a group and automatically assign host names based on a range of IP addresses and the host name format you specify. Such a group of records is called a bulk host, which the appliance manages and displays as a single bulk host record.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>Captive Portal</td>
<td>An Infoblox service that you enable on Grid members to register users, guest users, or both types of users for authentication purposes on network segments that you define using the authenticated DHCP feature.</td>
</tr>
<tr>
<td>CIDR (Classless Inter-Domain Routing) Notation</td>
<td>A compact specification of an IPv4 or IPv6 address and its associated routing prefix. For example, the CIDR notation of 192.168.100.1/24 represents the IPv4 address of 192.168.100.1 and its routing prefix of 192.168.100.0, or its subnet mask of 255.255.255.0. The CIDR notation of 2001:DB8::/48 represents the IPv6 addresses from 2001:DB8::0 to 2001:DB8::FFFF:FFFF:FFFF:FFFF.</td>
</tr>
<tr>
<td>CLI (Command-line Interface)</td>
<td>A way to interact with Infoblox products by typing text-only commands to perform specific tasks.</td>
</tr>
<tr>
<td>Dashboard</td>
<td>Your home page on Infoblox Multi-Grid Manager, Grid Manager, and System Manager. It provides easy access to tasks and to the status of your Grids and networks. It also provides various widgets for viewing and managing data.</td>
</tr>
<tr>
<td>DDNS (Dynamic DNS)</td>
<td>The automatic updating of real-time DNS configuration changes and other information on a DNS server when a network device is assigned a new IP address.</td>
</tr>
<tr>
<td>DHCP (Dynamic Host Configuration Protocol)</td>
<td>A configuration protocol that provides address assignments to network devices within a network. It keeps track of network configuration for each network device.</td>
</tr>
<tr>
<td>DHCP Failover Association</td>
<td>The pairing of two DHCP servers that establish a TCP connection for their communications. The servers form a pair of DHCP failover peers and provide DHCP protocol redundancy to minimize DHCP service outages.</td>
</tr>
<tr>
<td>DHCP Filter</td>
<td>A set of criteria and rules used to screen requesting hosts by matching MAC addresses, relay agent identifiers, DHCP options, or RADIUS authentication results.</td>
</tr>
<tr>
<td>DHCP Template</td>
<td>A set of predefined properties that you use to create IPv4 and IPv6 DHCP objects, such as networks and DHCP ranges, on the Infoblox appliance.</td>
</tr>
<tr>
<td>DIW (Data Import Wizard)</td>
<td>An Infoblox software tool that facilitates the import of DNS, DHCP, and TFTP data from legacy servers to Infoblox NIOS appliances. DIW supports DNS data import in the following formats: BIND 9, BIND 8, BIND 4, Microsoft DNS, Lucent VitalQIP, and Nortel NetID. It supports DHCP data import in the following formats: ISC DHCP, Microsoft DHCP, Lucent VitalQIP, and Nortel NetID.</td>
</tr>
<tr>
<td>DNS (Domain Name System)</td>
<td>A hierarchical naming system that translates domain names of any network devices into IP addresses for the purpose of locating and addressing these devices worldwide.</td>
</tr>
<tr>
<td>DNS View</td>
<td>On Infoblox appliances, a DNS view provides the ability to serve one version of DNS data to one set of clients and another version to another set of clients. With DNS views, the Infoblox appliance can provide a different answer to the same DNS query, depending on the source and match destinations of the query.</td>
</tr>
<tr>
<td>DNSSEC (Domain Name System Security Extensions)</td>
<td>A suite of IETF (Internet Engineering Task Force) specifications for securing certain kinds of information provided by DNS for use on IP networks. It is a set of extensions to DNS, which provide DNS resolvers with the original authentication of DNS data, authenticated denial of existence, and data integrity.</td>
</tr>
<tr>
<td>DNSone™</td>
<td>The software package that enables Infoblox appliances to provide DNS, DHCP and TFTP services. You can add the Grid upgrade to Infoblox appliances running DNSone.</td>
</tr>
<tr>
<td>Endpoint</td>
<td>An IP device such as a personal computer, laptop, or mobile handheld device. This term is often used in a security context.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Extensible Attribute</td>
<td>Metadata you define to capture additional information about an object managed by the Infoblox NIOS appliance. You can use predefined attributes or create your own. You can also specify required attributes and restrict the values that users can enter for each attribute.</td>
</tr>
<tr>
<td>Filters</td>
<td>Criteria the Infoblox NIOS appliance uses to request specific information in the database. You can use filters to control the amount and the kind of data displayed in a panel or table in Infoblox Multi-Grid Manager, Grid Manager, and System Manager.</td>
</tr>
<tr>
<td>FQDN (fully qualified domain name)</td>
<td>A complete domain name that specifies its exact location in the hierarchy of the DNS. It specifies all the domain levels, including the top-level domain and the root domain.</td>
</tr>
<tr>
<td>FTP (File Transfer Protocol)</td>
<td>A standard network protocol used to transfer files from one network device to another over a TCP-based network, such as the Internet. FTP is built on a client-server architecture and utilizes separate control and data connections between the client and server.</td>
</tr>
<tr>
<td>Gateway</td>
<td>The default router for the immediate network segment of an interface.</td>
</tr>
<tr>
<td>Grid™ Technology</td>
<td>Infoblox’s unique and patented high availability Grid technology ensures network reliability. The Infoblox Grid provides resilient network services, failover, recovery, and seamless maintenance for an Infoblox deployment inside a single building, across a networked campus, or between remote locations. The Infoblox Grid establishes a distributed relationship between individual or paired appliances to remove single points of failure and other operational risks inherent in legacy DNS, DHCP, and IP address management infrastructure.</td>
</tr>
<tr>
<td>Grid Manager</td>
<td>The NIOS web interface that provides access to your Grid for performing IPAM, DNS, and DHCP management and other administration tasks.</td>
</tr>
<tr>
<td>Grid Master</td>
<td>The Grid member in an Infoblox Grid that maintains the NIOS database that is distributed among all members of the Grid. You connect to the Grid Master to configure and monitor the entire Grid.</td>
</tr>
<tr>
<td>Grid Member</td>
<td>Any single Infoblox NIOS appliance or HA pair that belongs to a Grid. Each member can use the data and services of the Grid. You can also modify settings so that a Grid member can use unique data and member-specific services.</td>
</tr>
<tr>
<td>HA Pair</td>
<td>Two physical Infoblox NIOS appliances that are linked to perform as a single virtual appliance in an HA (high availability) configuration. The HA configuration provides hardware redundancy to minimize service outages. In this configuration, one appliance is the active node and the other is the passive node.</td>
</tr>
<tr>
<td>Host Record</td>
<td>On Infoblox appliances, host records provide a unique approach that enables you to manage multiple DNS records and DHCP and IPAM data collectively, as one object on the appliance.</td>
</tr>
<tr>
<td>IBOS (Infoblox Orchestration Server)</td>
<td>IBOS is the Infoblox IF-MAP (Interface to Metadata Access Points) server that contains a searchable database for storing state information about network resources. It is the central point with which IF-MAP clients communicate to send and retrieve real-time information defined in the IF-MAP data format.</td>
</tr>
<tr>
<td>IF-MAP (Interface for Metadata Access Points)</td>
<td>An open standard client-server protocol developed by the Trusted Computing Group as one of the core protocols of the TNC (Trusted Network Connect) open architecture. IF-MAP allows network resources to share real-time information.</td>
</tr>
<tr>
<td>IP Map</td>
<td>In Infoblox Grid Manager or System Manager, this is a graphical representation of all IPv4 addresses in a given subnet.</td>
</tr>
</tbody>
</table>
### Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPAM (IP Address Management)</td>
<td>Infoblox IPAM provides a means of planning, tracking, and managing IP address space in a network. It glues DNS and DHCP services together so that each service is aware of changes in the other. The Infoblox IPAM implementation offers an IP address-centric approach so you can manage your networks and IP addresses through a centralized GUI.</td>
</tr>
<tr>
<td>Leaf Network</td>
<td>On Infoblox appliances, a network that does not contain any subnets.</td>
</tr>
<tr>
<td>Lease Logging Member</td>
<td>An Infoblox Grid member that is designated to collect DHCP lease events.</td>
</tr>
<tr>
<td>Limited-Access User</td>
<td>An admin user account that has specific roles and permissions assigned. Limited-access users have restricted access to Infoblox Multi-Grid Manager, Grid Manager, and System Manager, and can only perform certain tasks based on their assigned roles and permissions.</td>
</tr>
<tr>
<td>Lite Upgrade</td>
<td>On Infoblox appliances, a lite upgrade occurs when there are incremental changes to the NIOS software that do not require any change to the database. The appliance can perform a lite upgrade only if the format of the database between the existing NIOS version and the upgrade version is the same. In general, when you upgrade from a major release to a patch release or a patch release to another patch release, you are performing a lite upgrade.</td>
</tr>
<tr>
<td>Loopback Interface</td>
<td>On Infoblox appliances, the virtual network interface on which you can consolidate DNS servers for migration purposes, add anycast addresses to improve the performance of the DNS service, and separate DNS traffic.</td>
</tr>
<tr>
<td>Managing Member</td>
<td>An Infoblox Grid member that is configured to manage Microsoft DNS and DHCP servers.</td>
</tr>
<tr>
<td>Master Candidate</td>
<td>An Infoblox Grid member that is designated to assume the role of the Grid Master as a disaster recovery measure.</td>
</tr>
<tr>
<td>Master Grid</td>
<td>A group of Infoblox appliances that are connected to provide a single point of administration for multiple Grids and network management of these Grids.</td>
</tr>
<tr>
<td>Master Grid Member</td>
<td>Any single Infoblox appliance or HA pair that belongs to the Master Grid. All Master Grid members serve as Master Candidates.</td>
</tr>
<tr>
<td>Multi-Grid Manager</td>
<td>The NIOS web interface that provides access to the Master Grid, from which you can manage multiple Grids and their networks.</td>
</tr>
<tr>
<td>Multi-Grid Master</td>
<td>The Infoblox Master Grid member that maintains the NIOS database that is distributed among all Master Grid members. You connect to Multi-Grid Manager to configure and monitor the Master Grid.</td>
</tr>
<tr>
<td>Multi-Grid Master Candidate</td>
<td>An Infoblox Master Grid member that is designated to assume the role of the Multi-Grid Master as a disaster recovery measure.</td>
</tr>
<tr>
<td>Name Server Group</td>
<td>On Infoblox appliances, a server group that contains one primary DNS server and/or one or more secondary DNS servers. Specifying a single name server group can simplify DNS zone creation.</td>
</tr>
<tr>
<td>NAT (Network Address Translation) Group</td>
<td>A group of Infoblox Grid members that are configured on the same side of a NAT appliance. In a Grid configuration where the Grid Master is configured behind a NAT appliance and there are Grid members on both sides of the NAT appliance, it is necessary to create a NAT group to ensure that the Grid Master and Grid members use the correct NAT and interface addresses for Grid communications.</td>
</tr>
<tr>
<td>Network Block</td>
<td>On Infoblox appliances, an IP address space that is defined in the Master Grid. A network block can consist of other network blocks, network containers, and leaf networks.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network Container</td>
<td>On Infoblox appliances, an automatically created container of multiple networks that are subnets of the IP address space configured for the network container. A network container cannot be assigned to a Grid member or be directly created.</td>
</tr>
<tr>
<td>Network Discovery</td>
<td>A set of tools provided by the Infoblox NIOS appliance for detecting active hosts on specified networks and specified VMware vSphere servers.</td>
</tr>
<tr>
<td>Network Map</td>
<td>In Infoblox Grid Manager and System Manager, Network Map presents a complete view of your network space, including the different types of networks that are in it and its unused address space. You can use Network Map to design and plan your network infrastructure, configure and manage individual networks, and evaluate their utilization.</td>
</tr>
<tr>
<td>Network Mask or Netmask</td>
<td>A numeric representation of the bits that are used to split an IP address into the network portion and the host portion. In Infoblox products, this is represented by either quad-dotted decimal representation or CIDR notation for IPv4 network masks, or by CIDR notation for IPv6 network masks.</td>
</tr>
<tr>
<td>Network View</td>
<td>On Infoblox appliances, a single routing domain with its own networks and shared networks. A network view can contain both IPv4 and IPv6 networks. All networks must belong to a network view on the Infoblox appliance.</td>
</tr>
<tr>
<td>NIOS</td>
<td>An Infoblox proprietary system that powers Infoblox solutions with an embedded processor that delivers core network services. It is the operating system that runs on the NIOS appliances—a security-hardened, real-time set of appliances built to ensure the non-stop operation of network infrastructure. NIOS automates the error-prone and time-consuming manual tasks associated with deploying and managing IPAM, DNS, and DHCP required for continuous IP network availability and business uptime.</td>
</tr>
<tr>
<td>NIOS Virtual Appliance</td>
<td>Any Infoblox supported platform, such as the Riverbed Steelhead appliances or VMWare appliances, that runs the vNIOS software. These appliances are also known as the vNIOS appliances.</td>
</tr>
<tr>
<td>Node</td>
<td>A single Infoblox appliance of an HA (high availability) pair. An HA pair consists of an active node and a passive node.</td>
</tr>
<tr>
<td>NTP (Network Time Protocol)</td>
<td>A protocol for synchronizing the clocks of computer systems over packet-switched, variable latency data networks; it essentially keeps network devices on a common clock by resisting the effects of variable latency by means of a jitter buffer.</td>
</tr>
<tr>
<td>Passive Node</td>
<td>The Infoblox NIOS appliance in an HA pair that constantly keeps its database synchronized with that of the active node, so it can take over core network services when an HA failover occurs. When an HA failover occurs, the passive node becomes the active node in the HA pair.</td>
</tr>
<tr>
<td>PortIQ</td>
<td>An Infoblox switch port appliance that enables quick discovery of the Ethernet switch ports. PortIQ identifies ports that are not fully utilized and those that exceed their capacity. You can use PortIQ to troubleshoot LAN environments.</td>
</tr>
<tr>
<td>Quick Filter</td>
<td>A filter that stores specific filter criteria for requesting information displayed in a specific panel in Infoblox Multi-Grid Manager, Grid Manager, and System Manager. For more information, see “Filter.”</td>
</tr>
<tr>
<td>Overlapping Network</td>
<td>On Infoblox appliances, a network that exists in multiple locations, which can be multiple Grids in the Master Grid or within various network views in a Grid.</td>
</tr>
<tr>
<td>Replication</td>
<td>Database distribution among the Infoblox Grid Master and Grid members as well as among the Multi-Grid Master and Master Grid members.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reservation</td>
<td>On Infoblox appliances, a static IP address that you create for future use. A reservation is a pre-provisioned fixed address. You can reserve this static IP address on the NIOS appliance and assign it to a client in the future.</td>
</tr>
<tr>
<td>Resource Records</td>
<td>A collection of data in the DNS server database. Each resource record specifies information about a DNS object. For example, an A (address mapping) record maps a host name to an IP address, and a PTR (reverse-lookup pointer) record maps an IP address to a host name. The DNS server uses these records to answer queries.</td>
</tr>
<tr>
<td>Roaming Host</td>
<td>On Infoblox appliances, a host with a dynamically assigned IP address and a specific set of properties and DHCP options. When you create a roaming host for a network device, the device can receive any dynamically assigned address from the network to which it belongs.</td>
</tr>
<tr>
<td>Scope</td>
<td>A DHCP address range on a Microsoft server. Microsoft scope information is converted to equivalent DHCP range information after Microsoft data is synchronized with the NIOS appliance.</td>
</tr>
<tr>
<td>Shared Network</td>
<td>On Infoblox appliances, a network segment to which you assign two or more subnets. When subnets in a shared network contain IP addresses that are available for dynamic allocation, the addresses are put into a common pool for allocation when client requests arise.</td>
</tr>
<tr>
<td>Shared Record Group</td>
<td>On Infoblox appliances, a set of resource records that you add to multiple DNS zones. You can create resource records in a group and share the group among multiple zones. The zones handle the shared resource records as any other resource record.</td>
</tr>
<tr>
<td>SSO (Single Sign On)</td>
<td>An Infoblox feature that allows you to automatically sign in to selected Grids from the Master Grid, without having to log in to each individual Grid each time you sign on.</td>
</tr>
<tr>
<td>Smart Folder</td>
<td>On Infoblox appliances, a virtual folder in which you place the results of filter criteria that you select to request specific data in the NIOS database. Once you set up a smart folder, the appliance displays up-to-date information based on your filter and grouping criteria each time you access the folder.</td>
</tr>
<tr>
<td>Subnet (or network)</td>
<td>A logical division of an IP network. A subnet of network may also be called a network. For example, 10.1.0.0/16 is a subnet of 10.0.0.0/8, and fc80:8:8:16::/64 is a subnet of fc80:8:8::/48.</td>
</tr>
<tr>
<td>Superscope</td>
<td>On a Microsoft server, superscope comprises multiple scopes or DHCP address ranges created on a single physical network segment. Microsoft superscope information is converted to equivalent network information after Microsoft data is synchronized with the NIOS appliance.</td>
</tr>
<tr>
<td>Superuser</td>
<td>An admin user account that has unrestricted access to Infoblox Multi-Grid Manager, Grid Manager, or System Manager.</td>
</tr>
<tr>
<td>Support Bundle</td>
<td>A tar.gz file that contains configuration files and system files of the Infoblox NIOS appliance. You can download a support bundle for an independent appliance and for each member in a Grid.</td>
</tr>
<tr>
<td>System Manager</td>
<td>The NIOS web interface that provides access to an independent appliance (single or HA) for performing IPAM, DNS, and DHCP management and other administration tasks.</td>
</tr>
<tr>
<td>TFTP (Trivial File Transfer Protocol)</td>
<td>A data transfer service that provides devices—such as phones, RFID readers, IP cameras, and other devices—with up-to-date software and configuration data.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Traffic Capture</td>
<td>An Infoblox tools that captures the traffic on one or all of the ports on a NIOS appliance. The NIOS appliance saves all captured traffic in a .cap file and compresses it into a .tar.gz file.</td>
</tr>
<tr>
<td>Upgrade Group</td>
<td>On Infoblox appliances, a group of Grid members that you put together so you can perform software distribution and upgrade at the same time.</td>
</tr>
<tr>
<td>VIP (Virtual IP)</td>
<td>On Infoblox appliances, the shared IP address of an HA pair. A VIP address links to the HA port on the active node of an HA pair.</td>
</tr>
<tr>
<td>VRID (Virtual Router ID)</td>
<td>VRID identifies the VRRP (Virtual Router Redundancy Protocol) HA pair to which the Infoblox appliance belongs. Through VRID, two HA nodes identify each other as belonging to the same HA pair, and they obtain a virtual MAC address to share with a VIP. A VRID can be any number between 1 and 255, and it must be unique on the local LAN so that it does not conflict with any other Infoblox appliances using VRRP on the same subnet.</td>
</tr>
<tr>
<td>vNIOS</td>
<td>The virtual version of NIOS. You can install Infoblox vNIOS software on any supported virtual platform and configure the system as a vNIOS virtual appliance.</td>
</tr>
<tr>
<td>VRRP (Virtual Router Redundancy Protocol)</td>
<td>An industry standard MAC address level HA failover mechanism.</td>
</tr>
</tbody>
</table>
Appendix B Grid Manager Icons

This appendix contains the following information about icons used in Grid Manager, System Manager, and Orchestration Server Manager:

- **Icon**: The graphical display of an icon.
- **Icon Name**: The icon name.
- **Description**: The task that Grid Manager performs after you click the icon.
- **Tab/Table/Panel**: Lists the tab, table, or panel in which the icon appears.

The following are common icons that appear in most of the tabs, tables, and panels, and in the Toolbar:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Add Icon" /></td>
<td>Add</td>
<td>Adds an object</td>
</tr>
<tr>
<td><img src="image" alt="Add Bookmark Icon" /></td>
<td>Add Bookmark</td>
<td>Adds a bookmark for an object and displays it in the Bookmarks panel</td>
</tr>
<tr>
<td><img src="image" alt="Arrow (Down) Icon" /></td>
<td>Arrow (Down)</td>
<td>Moves an object down in a list</td>
</tr>
<tr>
<td><img src="image" alt="Arrow (Up) Icon" /></td>
<td>Arrow (Up)</td>
<td>Moves an object up in a list</td>
</tr>
<tr>
<td><img src="image" alt="Clear Icon" /></td>
<td>Clear</td>
<td>Clears the status of an object</td>
</tr>
<tr>
<td><img src="image" alt="Clock Icon" /></td>
<td>Clock</td>
<td>Displays a drop-down list for time</td>
</tr>
<tr>
<td><img src="image" alt="Delete Icon" /></td>
<td>Delete</td>
<td>Deletes an object</td>
</tr>
<tr>
<td><img src="image" alt="Disabled Icon" /></td>
<td>Disabled</td>
<td>Indicates a disabled object</td>
</tr>
<tr>
<td><img src="image" alt="Download Icon" /></td>
<td>Download</td>
<td>Downloads a file or data</td>
</tr>
<tr>
<td><img src="image" alt="Edit Icon" /></td>
<td>Edit</td>
<td>Displays the corresponding editor for modifying object configurations</td>
</tr>
<tr>
<td><img src="image" alt="Edit Icon" /></td>
<td>Edit</td>
<td>Displays the corresponding editor for modifying object configurations</td>
</tr>
<tr>
<td><img src="image" alt="Execute Now Icon" /></td>
<td>Execute Now</td>
<td>Executes a scheduled task immediately</td>
</tr>
<tr>
<td>Icon</td>
<td>Icon Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><img src="image" alt="Export Icon" /></td>
<td>Export</td>
<td>Exports data in the current panel</td>
</tr>
<tr>
<td><img src="image" alt="Extensible Attribute Icon" /></td>
<td>Extensible Attribute</td>
<td>Configures extensible attributes for the selected object</td>
</tr>
<tr>
<td><img src="image" alt="Flat View Icon" /></td>
<td>Flat View</td>
<td>Displays a list of objects in a flat view</td>
</tr>
<tr>
<td><img src="image" alt="Help Icon" /></td>
<td>Help</td>
<td>Displays information about an object</td>
</tr>
<tr>
<td><img src="image" alt="Hierarchy Icon" /></td>
<td>Hierarchy</td>
<td>Displays objects in a hierarchical view</td>
</tr>
<tr>
<td><img src="image" alt="Import Icon" /></td>
<td>Import</td>
<td>Imports a file or data</td>
</tr>
<tr>
<td><img src="image" alt="Information Icon" /></td>
<td>Information</td>
<td>Displays informational data about an object</td>
</tr>
<tr>
<td><img src="image" alt="Locked Icon" /></td>
<td>Locked</td>
<td>Indicates a locked object</td>
</tr>
<tr>
<td><img src="image" alt="Microsoft Server Icon" /></td>
<td>Microsoft Server</td>
<td>Indicates a Microsoft server</td>
</tr>
<tr>
<td><img src="image" alt="Pause Icon" /></td>
<td>Pause</td>
<td>Pauses a function</td>
</tr>
<tr>
<td><img src="image" alt="Print Icon" /></td>
<td>Print</td>
<td>Prints the information in the current panel</td>
</tr>
<tr>
<td><img src="image" alt="Refresh Icon" /></td>
<td>Refresh</td>
<td>Refreshes the current page or table</td>
</tr>
<tr>
<td><img src="image" alt="Report Icon" /></td>
<td>Report</td>
<td>Displays a report, such as the capacity report</td>
</tr>
<tr>
<td><img src="image" alt="Search Icon" /></td>
<td>Search</td>
<td>Searches for specific objects</td>
</tr>
<tr>
<td><img src="image" alt="Selected object Icon" /></td>
<td>Selected object</td>
<td>Selects an object in a table for a specific function</td>
</tr>
<tr>
<td><img src="image" alt="Start Icon" /></td>
<td>Start</td>
<td>Starts a process</td>
</tr>
<tr>
<td><img src="image" alt="Stop Icon" /></td>
<td>Stop</td>
<td>Stops a process</td>
</tr>
<tr>
<td><img src="image" alt="Unlocked Icon" /></td>
<td>Unlocked</td>
<td>Indicates an unlocked object</td>
</tr>
<tr>
<td><img src="image" alt="User Profile Icon" /></td>
<td>User Profile</td>
<td>Configures a user profile</td>
</tr>
<tr>
<td><img src="image" alt="View 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>
| ![icon] | 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 |
<p>| ![icon] | Conflict                | Indicates an IP address conflict                                             | <strong>Data Management</strong> tab -&gt;<strong>IPAM</strong> tab -&gt;<strong>Net Map</strong> |
| ![icon] | Convert                 | Converts an object                                                           | <strong>Data Management</strong> tab -&gt;<strong>IPAM</strong> tab -&gt;<strong>network</strong> -&gt;<strong>IP Map</strong> -&gt;<strong>Toolbar</strong> |
| ![icon] | Discovery               | Performs a network discovery                                                 | <strong>Data Management</strong> tab -&gt;<strong>IPAM</strong> tab -&gt; <strong>Toolbar</strong> |
| ![icon] | Force HA Failover       | Forces an HA failover                                                        | <strong>Data Management</strong> tab -&gt;<strong>DHCP</strong> tab -&gt; <strong>Toolbar</strong> |
| ![icon] | Force Recovery          | Forces a recovery                                                            | <strong>Data Management</strong> tab -&gt;<strong>DHCP</strong> tab -&gt;<strong>Members</strong> tab -&gt;<strong>Failover Associations</strong> tab -&gt;<strong>Toolbar</strong> |
| ![icon] | Grid Manager            | Indicates the Grid Master                                                    | <strong>Data Management</strong> tab -&gt;<strong>DHCP</strong> tab -&gt;<strong>Members</strong> tab -&gt; <strong>Data Management</strong> tab -&gt;<strong>IPAM</strong> tab |
| ![icon] | Grid Manager Candidate  | Indicates the Grid Master candidate                                          | <strong>Data Management</strong> tab -&gt;<strong>DHCP</strong> tab -&gt;<strong>Members</strong> tab -&gt; <strong>Data Management</strong> tab -&gt;<strong>IPAM</strong> tab |
| ![icon] | Grid Member             | Indicates the Grid member                                                    | <strong>Data Management</strong> tab -&gt;<strong>DHCP</strong> tab -&gt;<strong>Members</strong> tab -&gt; <strong>Data Management</strong> tab -&gt;<strong>IPAM</strong> tab |
| ![icon] | Join                    | Joins networks                                                               | <strong>Data Management</strong> tab -&gt;<strong>IPAM</strong> tab -&gt;<strong>network</strong> -&gt;<strong>Toolbar</strong> |
| ![icon] | Key-signing Key Rollover| Indicates the key-signing key that is due to rollover                        | <strong>Data Management</strong> tab -&gt;<strong>DNS</strong> tab |
| ![icon] | Leaf Network            | Indicates a leaf network                                                     | <strong>Data Management</strong> tab -&gt;<strong>IPAM</strong> tab or <strong>DHCP</strong> tab |
| ![icon] | Disabled Leaf Network   | Indicates a disabled leaf network                                            | <strong>Data Management</strong> tab -&gt;<strong>IPAM</strong> tab or <strong>DHCP</strong> tab |
| ![icon] | Microsoft Server        | Indicates a Microsoft server                                                 | <strong>Data Management</strong> tab -&gt;<strong>DHCP</strong> tab -&gt;<strong>Members</strong> tab -&gt; <strong>Data Management</strong> tab -&gt;<strong>IPAM</strong> tab |
| ![icon] | Multi-Ping              | Pings all the addresses in a network                                         | <strong>Data Management</strong> tab -&gt;<strong>IPAM</strong> tab -&gt;<strong>IP Map</strong> -&gt;<strong>Toolbar</strong> |</p>
<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon Name</th>
<th>Description</th>
<th>Tab/Table/Panel</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Network" /></td>
<td>Network</td>
<td>Indicates a network</td>
<td>Data Management tab -&gt; IPAM tab or DHCP tab</td>
</tr>
<tr>
<td><img src="image" alt="Network Container" /></td>
<td>Network Container</td>
<td>Indicates a network container</td>
<td>Data Management tab -&gt; IPAM tab or DHCP tab</td>
</tr>
<tr>
<td><img src="image" alt="Network (Disabled)" /></td>
<td>Network (Disabled)</td>
<td>Indicates a disabled network</td>
<td>Data Management tab -&gt; IPAM tab or DHCP tab</td>
</tr>
<tr>
<td><img src="image" alt="Microsoft Network" /></td>
<td>Microsoft Network</td>
<td>Indicates a network with Microsoft servers</td>
<td>Data Management tab -&gt; IPAM tab or DHCP tab</td>
</tr>
<tr>
<td><img src="image" alt="Infoblox Network" /></td>
<td>Infoblox Network</td>
<td>Indicates a network with Infoblox appliances</td>
<td>Data Management tab -&gt; IPAM tab or DHCP tab</td>
</tr>
<tr>
<td><img src="image" alt="Ping" /></td>
<td>Ping</td>
<td>Pings an IP address</td>
<td>Data Management tab -&gt; IPAM tab -&gt; IP Map -&gt; Toolbar</td>
</tr>
<tr>
<td><img src="image" alt="Properties" /></td>
<td>Properties</td>
<td>Configures Grid DNS properties</td>
<td>Data Management tab -&gt; DNS tab -&gt; Toolbar</td>
</tr>
<tr>
<td><img src="image" alt="Reclaim" /></td>
<td>Reclaim</td>
<td>Reclaims an IP address</td>
<td>Data Management tab -&gt; IPAM tab -&gt; IP Map -&gt; Toolbar</td>
</tr>
<tr>
<td><img src="image" alt="Resize" /></td>
<td>Resize</td>
<td>Resizes a network</td>
<td>Data Management tab -&gt; IPAM tab -&gt; network -&gt; Toolbar</td>
</tr>
<tr>
<td><img src="image" alt="Resolve Conflict" /></td>
<td>Resolve Conflict</td>
<td>Resolves an IP address conflict</td>
<td>Data Management tab -&gt; IPAM tab -&gt; IP Map -&gt; Toolbar</td>
</tr>
<tr>
<td><img src="image" alt="Set Partner Down" /></td>
<td>Set Partner Down</td>
<td>Sets partner down</td>
<td>Data Management tab -&gt; DHCP tab -&gt; Members tab -&gt; Failover Associations tab -&gt; Toolbar</td>
</tr>
<tr>
<td><img src="image" alt="Split Network" /></td>
<td>Split Network</td>
<td>Splits a network</td>
<td>Data Management tab -&gt; IPAM tab -&gt; network -&gt; Toolbar</td>
</tr>
<tr>
<td><img src="image" alt="DNSSEC status" /></td>
<td>DNSSEC status</td>
<td>Displays status for DNSSEC</td>
<td>Data Management tab -&gt; DNS tab -&gt; Toolbar</td>
</tr>
<tr>
<td><img src="image" alt="Secondary Zone Status" /></td>
<td>Secondary Zone Status</td>
<td>Displays status for the secondary zone</td>
<td>Data Management tab -&gt; DNS tab</td>
</tr>
<tr>
<td><img src="image" alt="Zoom In" /></td>
<td>Zoom In</td>
<td>Zooms in to the selected network</td>
<td>Data Management tab -&gt; IPAM tab -&gt; Net Map</td>
</tr>
<tr>
<td><img src="image" alt="Zoom Out" /></td>
<td>Zoom Out</td>
<td>Zooms out from the selected network</td>
<td>Data Management tab -&gt; IPAM tab -&gt; Net Map</td>
</tr>
<tr>
<td><img src="image" alt="Directory" /></td>
<td>Directory</td>
<td>Indicates a directory</td>
<td>Data Management tab -&gt; 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><img src="image" alt="Icon" /></td>
<td>Smart Folder</td>
<td>Lists a smart folder</td>
<td>Smart Folders tab</td>
</tr>
<tr>
<td><img src="image" alt="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><img src="image" alt="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><img src="image" alt="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><img src="image" alt="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><img src="image" alt="Icon" /></td>
<td>bloxTools</td>
<td>Performs bloxTools services</td>
<td>Grid tab -&gt; Grid Manager tab -&gt; Toolbar</td>
</tr>
<tr>
<td><img src="image" alt="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><img src="image" alt="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><img src="image" alt="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><img src="image" alt="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><img src="image" alt="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><img src="image" alt="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><img src="image" alt="Icon" /></td>
<td>Overlap</td>
<td>Shows overlapping permissions</td>
<td>Administration tab -&gt; Permissions tab</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Reschedule</td>
<td>Reschedules a task</td>
<td>Administration tab -&gt; Scheduling tab -&gt; Toolbar</td>
</tr>
<tr>
<td><img src="image" alt="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>
<tr>
<td>🌐</td>
<td>URL Links</td>
<td>Adds URL links</td>
</tr>
</tbody>
</table>
## Appendix C 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] [abcd] [15a-d]</td>
<td>Matches “0” or “3”. Matches “a”, “b”, “c”, or “d”. 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-n]</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 D vNIOS Appliance Limitations

vNIOS appliances support most of the features of the Infoblox NIOS software, with some limitations. This appendix describes these limitations. *Table D.1* summarizes the supported Grid configurations on vNIOS appliances for Riverbed and VMware.

Table D.1  Supported vNIOS Appliance Configurations

<table>
<thead>
<tr>
<th>vNIOS Appliance</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>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Grid Master</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Grid Master Candidate</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>HA Grid Member</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Single Grid Member</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

For detailed information about the limitations on each vNIOS appliance, see the following:

-  *vNIOS for Riverbed*
-  *vNIOS for VMware*
vNIOS Appliance Limitations

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

The Infoblox vNIOS for VMware can also run on Cisco SRE-V (Services Ready Engine Virtualization), which is part of the Cisco UCS (Unified Computing System) Express. For more information about vNIOS for VMware, refer to the Infoblox Installation Guide for vNIOS Software on 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 is supported on Cisco SRE-V and can function as a Grid member only. It does not support configuration as an independent appliance, an HA pair, a Grid Master, or a Grid Master candidate. It also does not support access to the Infoblox GUI.
- The IB-VM-250 virtual appliance supports all the services provided by 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-1050 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 E 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 1018
  - **AC** on page 1018
  - **DC** on page 1018

- **Agency Compliance** on page 1019
  - **FCC** on page 1019
  - **Canadian Compliance** on page 1019
  - **VCCI** on page 1020

- **RFC Compliance** on page 1021
  - **DNS RFC Compliance** on page 1021
  - **DHCP RFC Compliance** on page 1023
Power Safety Information

The main external power connector for the Infoblox appliance is located on the back of the system. Ensure power to the system is off before connecting the power cord into the power connector. Please read the following power safety statements for your AC- or DC-powered appliance:

**AC**

**English**

WARNING: This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120VAC, 15A U.S. (240VAC, 10A international) is used on the phase conductors (all current-carrying conductors).

**French**

WARNING: Pour ce qui est de la protection contre les courts-circuits (surtension), ce produit dépend de l'installation électrique du local. Vérifier qu'un fusible ou qu'un disjoncteur de 120V alt., 15A U.S. maximum (240V alt., 10A international) est utilisé sur les conducteurs de phase (conducteurs de charge).

**German**


**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 E.1 Agency Regulation Compliance

<table>
<thead>
<tr>
<th>Standard</th>
<th>Agency</th>
<th>Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCC Part 15</td>
<td>FCC</td>
<td>FCC</td>
</tr>
<tr>
<td>EN55022, EN55024, EN61000-3-2, EN61000-3-3</td>
<td>TUV</td>
<td>CE</td>
</tr>
<tr>
<td>UL60950/CSA60950</td>
<td>UL</td>
<td>cULus</td>
</tr>
<tr>
<td>EN60950</td>
<td>TUV</td>
<td>GS</td>
</tr>
<tr>
<td>CB Scheme</td>
<td>IECEE</td>
<td>Report and Certificate IEC 60950-1:2001</td>
</tr>
<tr>
<td>VCCI-A</td>
<td>VCCI</td>
<td>VCCI</td>
</tr>
<tr>
<td>AS/NZS 3548</td>
<td>ACMA</td>
<td>C-Tick</td>
</tr>
</tbody>
</table>

FCC

The FCC label on the back of the system indicates this network appliance is compliant with limits for a Class A digital device in accordance with Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when this equipment is operated in a commercial environment. Operation is subject to the following two conditions:

- This device might not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This device generates, uses, and can radiate radio frequency energy if not installed and used in accordance with the instructions in this manual. Operating this equipment in a residential area is likely to cause harmful interference, and the customer will be required to rectify the interference at his or her own expense. This product requires the use of external shielded cables to maintain compliance pursuant to Part 15 of the FCC Rules.

Canadian Compliance

English

This Class A digital apparatus complies with Canadian ICES-003.

French

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.
VCCI

The Infoblox appliance complies with this VCCI regulation (compliance statement follow by its translation):

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

This is a Class A product based on the Technical Requirements of the Voluntary Control Council for Interference Technology (VCCI). In a domestic environment this product may cause radio interference, in which case the user may be required to take corrective action.

Caution: Lithium battery included with this board. Do not puncture, mutilate, or dispose of battery in fire. Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by manufacturer. Dispose of used battery according to manufacturer instructions and in accordance with your local regulations.
RFC Compliance

The NIOS appliance is compliant with the following:

- Qualys and Nessus security requirements
- Joint Interoperability Test Command (JITC) certification for Internet Protocol version 6 capability
- RFCs (Request for Comments):
  - *DNS RFC Compliance* on page 1021
  - *DHCP RFC Compliance* on page 1023

DNS RFC Compliance

The NIOS appliance complies with the following DNS RFCs:

*Table E.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>
</tbody>
</table>
**RFC Compliance**

The appliance complies with the following DHCP RFCs:

Table E.3  *RFCs for DHCP*

<table>
<thead>
<tr>
<th>RFC Number</th>
<th>RFC Title</th>
</tr>
</thead>
<tbody>
<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 E.3  *RFCs for DHCP*

<table>
<thead>
<tr>
<th>RFC Number</th>
<th>RFC Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1531</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>1534</td>
<td>Interoperation Between DHCP and BOOTP</td>
</tr>
<tr>
<td>1542</td>
<td>Clarifications and Extensions for the Bootstrap Protocol</td>
</tr>
<tr>
<td>2131</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>2132</td>
<td>DHCP Options and BOOTP Vendor Extensions</td>
</tr>
<tr>
<td>3046</td>
<td>DHCP Relay Agent Information Option</td>
</tr>
<tr>
<td>3315</td>
<td>Dynamic Host Configuration Protocol for IPv6 (DHCPv6)</td>
</tr>
<tr>
<td>3925</td>
<td>Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)</td>
</tr>
<tr>
<td>4388</td>
<td>Dynamic Host Configuration Protocol (DHCP) Leasequery</td>
</tr>
</tbody>
</table>
Appendix F  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 1027
- GNU Lesser General Public License on page 1030
- Apache Software License, Version 2.0 on page 1036
- ISC BIND Copyright on page 1042
- ISC DHCP Copyright on page 1043
- Julian Seward Copyright on page 1044
- Carnegie Mellon University Copyright on page 1044
- Thai Open Source Software Center Copyright on page 1045
- Ian F. Darwin Copyright on page 1046
- Lawrence Berkeley Copyright on page 1047
- MIT Kerberos Copyright on page 1047
- BSD License on page 1048
- David L. Mills Copyright on page 1049
- OpenLDAP License on page 1049
- OpenSSL License on page 1050
- VIM License on page 1051
- ZLIB License on page 1053
- Wietse Venema Copyright on page 1053
- ECLIPSE SOFTWARE on page 1054
- Eclipse Public License - v 1.0 on page 1054
- AOP Alliance (Java/j2EE AOP standards) on page 1058
- ASM on page 1058
- Distributed Computing Laboratory, Emory University on page 1059
- COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) on page 1059
- The FreeType Project LICENSE on page 1063
- The Independent JPEG Group's JPEG software on page 1067
- Net-SNMP on page 1069
- The PHP License, version 3.01 on page 1075
- INFO-ZIP on page 1076
- MIT License on page 1078
- Ehcache on page 1078
GNU General Public License

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundations software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each authors protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyones free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".
Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Programs source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

   In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be 11 distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.
8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

GNU Lesser General Public License

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999
Copyright (C) 1991, 1999 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.
This license, the Lesser General Public License, applies to some specially designated software packages—typically libraries—of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can 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 Librarys complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at nocharge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an appropriate program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.
(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can 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 definition 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
textual 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,
your Contribution intentionally submitted for inclusion in the Work
by You to the Licensor shall be under the terms and conditions of
this License, without any additional terms or conditions.
Notwithstanding the above, nothing herein shall supersede or modify
the terms of any separate license agreement you may have executed
with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade
names, trademarks, service marks, or product names of the Licensor,
except as required for reasonable and customary use in describing the
origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
agreed to in writing, Licensor provides the Work (and each
Contributor provides its Contributions) on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
implied, including, without limitation, any warranties or conditions
of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
PARTICULAR PURPOSE. You are solely responsible for determining the
appropriateness of using or redistributing the Work and assume any
risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
whether in tort (including negligence), contract, or otherwise,
unless required by applicable law (such as deliberate and grossly
negligent acts) or agreed to in writing, shall any Contributor be
liable to You for damages, including any direct, indirect, special,
incidental, or consequential damages of any character arising as a
result of this License or out of the use or inability to use the
Work (including but not limited to damages for loss of goodwill,
work stoppage, computer failure or malfunction, or any and all
other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.
perl Artistic License

The "Artistic License"

Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions:

"Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.

"Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder as specified below.

"Copyright Holder" is whoever is named in the copyright or copyrights for the package.

"You" is you, if you're thinking about copying or distributing this Package.

"Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)

"Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.

2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:

   a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

   b) use the modified Package only within your corporation or organization.

   c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.

   d) make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

   a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

   b) accompany the distribution with the machine-readable source of the Package with your modifications.

   c) give non-standard executables non-standard names, and clearly document the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.

   d) make other distribution arrangements with the Copyright Holder.
5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own. You may embed this Package's interpreter within an executable of yours (by linking); this shall be construed as a mere form of aggregation, provided that the complete Standard Version of the interpreter is so embedded.

6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whoever generated them, and may be sold commercially, and may be aggregated with this Package. If such scripts or library files are aggregated with this Package via the so-called "undump" or "unexec" methods of producing a binary executable image, then distribution of such an image shall neither be construed as a distribution of this Package nor shall it fall under the restrictions of Paragraphs 3 and 4, provided that you do not represent such an executable image as a Standard Version of this Package.

7. C subroutines (or comparably compiled subroutines in other languages) supplied by you and linked into this Package in order to emulate subroutines and variables of the language defined by this Package shall not be considered part of this Package, but are the equivalent of input as in Paragraph 6, provided these subroutines do not change the language in any way that would cause it to fail the regression tests for the language.

8. Aggregation of this Package with a commercial distribution is always permitted provided that the use of this Package is embedded; that is, when no overt attempt is made to make this Package's interfaces visible to the end user of the commercial distribution. Such use shall not be construed as a distribution of this Package.

9. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

10. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The End

ISC BIND Copyright

Copyright (C) 1996-2002 Internet Software Consortium.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright (C) 1996-2001 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 NOMIMUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL NOMIMUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR
ISC DHCP Copyright

Copyright (c) 1995, 1996, 1997, 1998, 1999 Internet Software Consortium -DHCP. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of Internet Software Consortium - DHCP nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY INTERNET SOFTWARE CONSORTIUM AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Julian Seward Copyright

This program, "bzip2" and associated library "libbzip2", are copyright (C) 1996-2002 Julian R Seward. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, Cambridge, UK.
jsward@acm.org
bzip2/libbzip2 version 1.0.2 of 30 December 2001

Carnegie Mellon University Copyright

/*
 * Copyright (c) 2001 Carnegie Mellon University. All rights reserved.
 * 
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are met:
 * 
 * 1. Redistributions of source code must retain the above copyright
 * notice, this list of conditions and the following disclaimer.
 * 
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in
 * the documentation and/or other materials provided with the
 * distribution.
 * 
 * 3. The name "Carnegie Mellon University" must not be used to
 * endorse or promote products derived from this software without
 * prior written permission. For permission or any other legal
 * details, please contact
 */
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


This software is not subject to any export provision of the United States Department of Commerce, and may be exported to any country or planet.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice immediately at the beginning of the file, without modification, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Ian F. Darwin and others.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Lawrence Berkeley Copyright

Copyright (c) 1990 The Regents of the University of California.
All rights reserved.
This code is derived from software contributed to Berkeley by Vern Paxson.
The United States Government has rights in this work pursuant to contract no.
DE-AC03-76SF00098 between the United States Department of Energy and the University of California.
Redistribution and use in source and binary forms with or without modification are permitted provided that: (1) source distributions retain this entire copyright notice and comment, and (2) distributions including binaries display the following acknowledgement: "This product includes software developed by the University of California, Berkeley and its contributors" in the documentation or other materials provided with the distribution and in all advertising materials mentioning features or use of this software. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

MIT Kerberos Copyright

Copyright Notice and Legal Administrivia
-----------------------------------------
Copyright (C) 1985-2002 by the Massachusetts Institute of Technology.
All rights reserved.
Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.
WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Furthermore if you modify this software you must label your software as modified software and not distribute it in such a fashion that it might be confused with the original MIT software.
M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.
THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
Individual source code files are copyright MIT, Cygnus Support, OpenVision, Oracle, Sun Soft, FundsXpress, and others.
Project Athena, Athena, Athena MUSE, Discuss, Hesiod, Kerberos, Moira, and Zephyr are trademarks of the Massachusetts Institute of Technology (MIT). No commercial use of these trademarks may be made without prior written permission of MIT.
"Commercial use" means use of a name in a product or other for-profit manner. It does
NOT prevent a commercial firm from referring to the MIT trademarks in order to convey
information (although in doing so, recognition of their trademark status should be
given).

The following copyright and permission notice applies to the OpenVision Kerberos
Administration system located in kadmin/create, kadmin/dbutil, kadmin/passwd,
kadmin/server, lib/kadm5, and portions of lib/rpc:

Copyright, OpenVision Technologies, Inc., 1996, All Rights Reserved

WARNING: Retrieving the OpenVision Kerberos Administration system source code, as
described below, indicates your acceptance of the following terms. If you do not agree
to the following terms, do not retrieve the OpenVision Kerberos administration system.

You may freely use and distribute the Source Code and Object Code compiled from it, with
or without modification, but this Source Code is provided to you "AS IS" EXCLUSIVE OF
ANY WARRANTY, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS
FOR A PARTICULAR PURPOSE, OR ANY OTHER WARRANTY, WHETHER EXPRESS OR IMPLIED. IN NO EVENT
WILL OPENVISION HAVE ANY LIABILITY FOR ANY LOST PROFITS, LOSS OF DATA OR COSTS OF
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR
CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, THOSE
RESULTING FROM THE USE OF THE SOURCE CODE, OR THE FAILURE OF THE SOURCE CODE TO PERFORM,
OR FOR ANY OTHER REASON.

OpenVision retains all copyrights in the donated Source Code. OpenVision also retains
copyright to derivative works of the Source Code, whether created by OpenVision or by a
third party. The OpenVision copyright notice must be preserved if derivative works are
made based on the donated Source Code.

OpenVision Technologies, Inc. has donated this Kerberos Administration system to MIT for
inclusion in the standard Kerberos 5 distribution. This donation underscores our
commitment to continuing Kerberos technology development and our gratitude for the
valuable work which has been performed by MIT and the Kerberos community.

Portions contributed by Matt Crawford <crawdad@fnal.gov> were work performed at Fermi
National Accelerator Laboratory, which is operated by Universities Research Association,
Inc., under contract DE-AC02-76CH03000 with the U.S. Department of Energy.

BSD License

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of
   conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list
   of conditions and the following disclaimer in the documentation and/or other materials
   provided with the distribution.

3. The names of the authors may not be used to endorse or promote products derived from
   this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES,
INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE.
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:
a) If you make changes to Vim yourself, you must clearly describe in the distribution how to contact you. When the maintainer asks you (in any way) for a copy of the modified Vim you distributed, you must make your changes, including source code, available to the maintainer without fee. The maintainer reserves the right to include your changes in the official version of Vim. What the maintainer will do with your changes and under what license they will be distributed is negotiable. If there has been no negotiation then this license, or a later version, also applies to your changes. The current maintainer is Bram Moolenaar <Bram@vim.org>. If this changes it will be announced in appropriate places (most likely vim.sf.net, www.vim.org and/or comp.editors). When it is completely impossible to contact the maintainer, the obligation to send him your changes ceases. Once the maintainer has confirmed that he has received your changes they will not have to be sent again.

b) If you have received a modified Vim that was distributed as mentioned under a) you are allowed to further distribute it unmodified, as mentioned at 1). If you make additional changes the text under a) applies to those changes.

c) Provide all the changes, including source code, with every copy of the modified Vim you distribute. This may be done in the form of a context diff. You can choose what license to use for new code you add. The changes and their license must not restrict others from making their own changes to the official version of Vim.

d) When you have a modified Vim which includes changes as mentioned under c), you can distribute it without the source code for the changes if the following three conditions are met:

- The license that applies to the changes permits you to distribute the changes to the Vim maintainer without fee or restriction, and permits the Vim maintainer to include the changes in the official version of Vim without fee or restriction.
- You keep the changes for at least three years after last distributing the corresponding modified Vim. When the maintainer or someone who you distributed the modified Vim to asks you (in any way) for the changes within this period, you must make them available to him.
- You clearly describe in the distribution how to contact you. This contact information must remain valid for at least three years after last distributing the corresponding modified Vim, or as long as possible.

e) When the GNU General Public License (GPL) applies to the changes, you can distribute the modified Vim under the GNU GPL version 2 or any later version.

3) A message must be added, at least in the output of the ":version" command and in the intro screen, such that the user of the modified Vim is able to see that it was modified. When distributing as mentioned under 2)e) adding the message is only required for as far as this does not conflict with the license used for the changes.

4) The contact information as required under 2)a) and 2)d) must not be removed or changed, except that the person himself can make corrections.

If you distribute a modified version of Vim, you are encouraged to use the Vim license for your changes and make them available to the maintainer, including the source code. The preferred way to do this is by e-mail or by uploading the files to a server and e-mailing the URL. If the number of changes is small (e.g., a modified Makefile) e-mailing a context diff will do. The e-mail address to be used is <maintainer@vim.org>

It is not allowed to remove this license from the distribution of the Vim sources, parts of it or from a modified version. You may use this license for previous Vim releases instead of the license that they came with, at your option.

=== end of license ===
ZLIB License

(C) 1995-2002 Jean-loup Gailly and Mark Adler

This software is provided as-is, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

This notice may not be removed or altered from any source distribution.

Jean-loup Gailly Mark Adler
jloup@gzip.org madler@alumni.caltech.edu

If you use the zlib library in a product, we would appreciate *not* receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes.

Wietse Venema Copyright

/****************************************************************************
 * Copyright 1995 by Wietse Venema. All rights reserved. Some individual * files may be covered by other copyrights. *
 * This material was originally written and compiled by Wietse Venema at * Eindhoven University of Technology, The Netherlands, in 1990, 1991, * 1992, 1993, 1994 and 1995. * * Redistribution and use in source and binary forms are permitted * provided that this entire copyright notice is duplicated in all such * copies. * * This software is provided "as is" and without any expressed or implied * warranties, including, without limitation, the implied warranties of * merchantability and fitness for any particular purpose. *
****************************************************************************/

}
ECLIPSE SOFTWARE

The product includes Eclipse software (the "Eclipse Program") provided by the Eclipse Foundation and licensed to Infoblox Inc. under the Eclipse Public License v1.0.

EXCEPT AS EXPRESSLY SET FORTH IN THE ECLIPSE PUBLIC LICENSE, THE ECLIPSE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

EXCEPT AS EXPRESSLY SET FORTH IN THE ECLIPSE PUBLIC LICENSE, NEITHER THE ECLIPSE FOUNDATION NOR ANY CONTRIBUTORS TO THE ECLIPSE PROGRAM SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE ECLIPSE PROGRAM, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any provisions provided by Infoblox relating to the Eclipse Program which differ from the above terms or the Eclipse Public License are offered by Infoblox alone and not by any other party.

The source code for the Eclipse Program is available from Infoblox as described in the open source introduction.

Eclipse Public License - v 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS ECLIPSE PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.
"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient’s responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;
ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must:

a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor’s responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.
5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient’s patent(s), then such Recipient’s rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient’s rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient’s rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient’s obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. The Eclipse Foundation is the initial Agreement Steward. The Eclipse Foundation may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses
to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

Related Links
* EPL in plain HTML
* The EPL on OSI’s site
* CPL to EPL conversion

---

**AOP Alliance (Java/J2EE AOP standards)**

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
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 dateInitial
Developer first distributes or otherwise makes the Original Software available to a
third party under the terms of this License.

(d) Notwithstanding Section 2.1(b) above, no patent license is granted: (1) for code
that You delete from the Original Software, or (2) for infringements caused by: (i)
the modification of the Original Software, or (ii) the combination of the Original
Software with other software or devices.

2.2. Contributor Grant.
Conditioned upon Your compliance with Section 3.1 below and subject to third party
intellectual property claims, each Contributor hereby grants You a world-wide,
royalty-free, non-exclusive license:

(a) under intellectual property rights (other than patent or trademark) Licensable by
Contributor to use, reproduce, modify, display, perform, sublicense and distribute the
Modifications created by such Contributor (or portions thereof), either on an unmodified
basis, with other Modifications, as Covered Software and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using, or selling of Modifications made
by that Contributor either alone and/or in combination with its Contributor Version (or
portions of such combination), to make, use, sell, offer for sale, have made, and/or
otherwise dispose of: (1) Modifications made by that Contributor (or portions thereof); and
(2) the combination of Modifications made by that Contributor with its Contributor
Version (or portions of such combination).

(c) The licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date
Contributor first distributes or otherwise makes the Modifications available to a third
party.

(d) Notwithstanding Section 2.2(b) above, no patent license is granted: (1) for any code
that Contributor has deleted from the Contributor Version; (2) for infringements caused by:
(i) third party modifications of Contributor Version, or (ii) the combination of
Modifications made by that Contributor with other software (except as part of the
Contributor Version) or other devices; or (3) under Patent Claims infringed by Covered
Software in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Availability of Source Code.

Any Covered Software that You distribute or otherwise make available in Executable form
must also be made available in Source Code form and that Source Code form must be
distributed only under the terms of this License.
You must include a copy of this License with every copy of the Source Code form of the Covered Software You distribute or otherwise make available. You must inform recipients of any such Covered Software in Executable form as to how they can obtain such Covered Software in Source Code form in a reasonable manner on or through a medium customarily used for software exchange.

3.2. Modifications.
The Modifications that You create or to which You contribute are governed by the terms of this License. You represent that You believe Your Modifications are Your original creation(s) and/or You have sufficient rights to grant the rights conveyed by this License.

3.3. Required Notices.
You must include a notice in each of Your Modifications that identifies You as the Contributor of the Modification. You may not remove or alter any copyright, patent or trademark notices contained within the Covered Software, or any notices of licensing or any descriptive text giving attribution to any Contributor or the Initial Developer.

3.4. Application of Additional Terms.
You may not offer or impose any terms on any Covered Software in Source Code form that alters or restricts the applicable version of this License or the recipients rights hereunder. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, you may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear that any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.5. Distribution of Executable Versions.
You may distribute the Executable form of the Covered Software under the terms of this License or under the terms of a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable form does not attempt to limit or alter the recipients rights in the Source Code form from the rights set forth in this License. If You distribute the Covered Software in Executable form under a different license, You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

You may create a Larger Work by combining Covered Software with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Software.

4. Versions of the License.

4.1. New Versions.
Sun Microsystems, Inc. is the initial license steward and may publish revised and/or new versions of this License from time to time. Each version will be given a distinguishing version number. Except as provided in Section 4.3, no one other than the license steward has the right to modify this License.

4.2. Effect of New Versions.
You may always continue to use, distribute or otherwise make the Covered Software available under the terms of the version of the License under which You originally received the Covered Software. If the Initial Developer includes a notice in the Original Software prohibiting it from being distributed or otherwise made available under any
subsequent version of the License, You must distribute and make the Covered Software available under the terms of the version of the License under which You originally received the Covered Software. Otherwise, You may also choose to use, distribute or otherwise make the Covered Software available under the terms of any subsequent version of the License published by the license steward.

4.3. Modified Versions.
When You are an Initial Developer and You want to create a new license for Your Original Software, You may create and use a modified version of this License if You: (a) rename the license and remove any references to the name of the license steward (except to note that the license differs from this License); and (b) otherwise make it clear that the license contains terms which differ from this License.

5. DISCLAIMER OF WARRANTY.

COVERED SOFTWARE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED SOFTWARE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-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.
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

1. We don't promise that this software works. (But if you find any bugs, please let us know!)
2. You can use this software for whatever you want. You don't have to pay us.
3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-1998, Thomas G. Lane. All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice.
unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software. (Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.)
So far as we are aware, there are no patent restrictions on the remaining code.
The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that
"The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts. Up until 2001, the project was based at UC Davis, and the first part covers all code written during this time. From 2001 onwards, the project has been based at SourceForge, and Networks Associates Technology, Inc hold the copyright on behalf of the wider Net-SNMP community, covering all derivative work done since then. An additional copyright section has been added as Part 3 below also under a BSD license for the work contributed by Cambridge Broadband Ltd. to the project since 2001. An additional copyright section has been added as Part 4 below also under a BSD license for the work contributed by Sun Microsystems, Inc. to the project since 2003.

Code has been contributed to this project by many people over the years it has been in development, and a full list of contributors can be found in the README file under the THANKS section.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----
Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) ----- 

Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER `AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.
This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS `AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2005, Sparta, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) ------

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003
oss@fabasoft.com
Author: Bernhard Penz <bernhard.penz@fabasoft.com>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
The PHP License, version 3.01

Copyright (c) 1999 - 2006 The PHP Group. All rights reserved.
Redistribution and use in source and binary forms, with or without
modification, is permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in
   the documentation and/or other materials provided with the
   distribution.

3. The name "PHP" must not be used to endorse or promote products
   derived from this software without prior written permission. For
   written permission, please contact group@php.net.

4. Products derived from this software may not be called "PHP", nor
   may "PHP" appear in their name, without prior written permission
   from group@php.net. You may indicate that your software works in
   conjunction with PHP by saying "Foo for PHP" instead of calling
   it "PHP Foo" or "phpfoo"

5. The PHP Group may publish revised and/or new versions of the
   license from time to time. Each version will be given a
   distinguishing version number.
   Once covered code has been published under a particular version
   of the license, you may always continue to use it under the terms
   of that version. You may also choose to use such covered code
   under the terms of any subsequent version of the license
   published by the PHP Group. No one other than the PHP Group has
   the right to modify the terms applicable to covered code created
   under this License.

6. Redistributions of any form whatsoever must retain the following
   acknowledgment:
   "This product includes PHP software, freely available from
   <http://www.php.net/software/>".

   THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM `AS IS'
   AND
   ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
   TO,
   THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

--------------------------------------------------------------------

This software consists of voluntary contributions made by many individuals on behalf of the PHP Group.

The PHP Group can be contacted via Email at group@php.net.

For more information on the PHP Group and the PHP project, please see <http://www.php.net>.


INFO-ZIP


Copyright (c) 1990-2007 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

MIT License

Copyright (c) 2010 Paul T. McGuire

Permission is hereby granted, free of charge, to any person obtaining a copy of this
software and associated documentation files (the "Software"), to deal in the Software
without restriction, including without limitation the rights to use, copy, modify, merge,
publish, distribute, sublicense, and/or sell copies of the Software, and to permit
persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or
substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR
PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE
FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR
OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER
DEALINGS IN THE SOFTWARE.

Ehcache

The open source Ehcache project is licensed under the Apache 2.0 License. The text of
the license is available below:

/**
 * Copyright 2003-2010 Terracotta, Inc.
 *
 * Licensed under the Apache License, Version 2.0 (the "License");
 * you may not use this file except in compliance with the License.
 * You may obtain a copy of the License at
 *
 * http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
# Index

## A

- **A records**
  - adding to shared record groups 429, 432
  - bulk hosts 402
  - DDNS updates 486
  - host records 803
  - sort lists 460

- **AAAA records**
  - adding 410
  - adding to shared record groups 429, 432
  - sort lists 460

- **access control lists**
  - for TFTP, HTTP, FTP services 304

- **Active Directory**
  - authenticating admins 133
  - configuring support for 492

- **admin groups** 107
  - ALL USERS group 107
  - configuring on remote RADIUS server 130
  - defining permissions 114
  - limited-access 107
  - managing 111
  - superusers 107

- **admin roles** 110

- **admins**
  - authenticating 124
  - authenticating using RADIUS 129
  - defining admin policy 138
  - defining user profiles 41
  - managing 103
  - notifying 139, 140
  - password length 139
  - using Active Directory to authenticate 133

- **anycast** 547

- **API**
  - migrating data 234

- **appliance status**
  - viewing 861, 866

- **audit history**
  - IP addresses 821

- **audit log**
  - configuring 873
  - selecting type 202
  - sending to syslog 870

## B

- **backing up**
  - guidelines for scheduled tasks 255

- **backup files**
  - creating and restoring 326

- **BGP** 553

- **blackhole list**
  - configuring for DNS 462

- **Blacklists** 453

- **bloxTools environment** 333

- **bookmarks** 52

- **BOOTP**
  - specifying parameters 586

## browsers

- limitations 38
- setting time zone 42

## bulk host records 402

## admin permissions 151

## C

- **capacity report** 877

- **capture traffic** 876

- **certificates**
  - generating a certificate signing request 45
  - generating a certificate signing request for a captive portal 704
  - generating self-signed 44
  - generating self-signed for captive portal 704
  - importing 45
  - importing for Captive Portal 705

- **CLI**
  - defining network settings 210

- **CNAME records**
  - adding 415

- **code pages**
  - Microsoft Windows 67

- **columns**
  - editing 49

- **CPU temperature status** 863

- **CPU usage status** 863

- **CSV Import**
  - blacklist rules 454

- **CSV import** 63

## D

- **Dashboard** 39

- **Data Import Wizard**
  - migrating data 234

- **database replication**
  - bandwidth considerations 174

- **database status** 861

- **DDNS** 471–516
  - configuring DHCP 477–488
  - configuring DNS 489–491

- **delegated zones** 387

- **detailed status** 860

- **DHCP**
  - bloxTools Environment 338
  - NTP status icons 238
  - viewing 860, 960

- **DHCP configuration checklist** 568

- **defining admin permissions** 154

- **dynamic DNS updates** 473

- **enabling LAN2 port** 273

- **general properties** 581

- **inheriting properties** 570

- **NAC Foundation module** 695

- **starting and stopping service** 612

- **viewing status** 867
DHCP failover
   configuring 658–664
   Dashboard 84
DHCP filters 666
DHCP lease history
   defining admin permissions 162
   enabling 605
DHCP leases
   clearing active 833
   converting 830
   scavenging 582
DHCP option filters 677
DHCP options
   option 12 478
   option 15 478
   option 60 593
   option 81 483
DHCP ranges
   applying MAC address filters 684
   configuring 642, 731
   Dashboard 84
   defining admin permissions 147, 156, 159
   permission to create from template 160
   using templates 617
DHCP templates
   configuring 616–624
   defining admin permissions 160
DHCPv6 options 599
disk usage status 861
DNAME records
   adding 417
DNS
   configuration checklist 343
   defining admin permissions 148
   enabling LAN2 port 274
   IPv6 346
   logging categories 871
   root name servers 459
   specifying DNS resolvers 286
   starting and stopping service 442
   updates for a zone 479, 485
   using MGMT port 280
   viewing status 867
DNS anycast
   BGP 553
   OSPF 550
DNS monitoring 879
DNS statistics
   Dashboard 83
DNS views 350–362
   defining admin permissions 149
   read-only permission 147, 156
DNS64 466
DNSKEY resource record 519
DNSSEC 518
documentation
   related technical documents 29
downgrading NIOS software 325
DS resource record 524
dynamic DNS
   See DDNS

E
Ethernet ports 265
exporting data 64, 66
   capacity report 877
   from smart folders 99
   lease records 742
extensible attributes
   256–260
   in wizards and editors 259
   smart folders 94
   UTF-8 encoding 67

F
fan status 862
file distribution services
   status 90
   TFTP, HTTP, FTP 302
filters
   DHCP 666
   in global search 59
   search criteria 56
   using for smart folders 94
   viewing permissions list 122
Finder panel 39, 48
fixed addresses
   configuring 645, 733
   defining admin permissions 147, 156, 159
   displaying lease information 604
   DNS updates 481
   host records 803
   permission to create from template 160
   using templates 619
force restore 331
forward zones 389
forwarders 443
FTP
   backup files 326
   configuring 303
   defining admin permissions 162
   uploading files 308
   UTF-8 encoding for file names 67
   viewing status 867

G
global search 59
exporting results 66
grid
   configuring 165–204
   configuring NTP 243
   configuring syslog 869
   configuring upgrade groups 311
   DNS updates for DHCP 479
downgrading 325
monitoring services 867
NAT groups 169
promoting master candidate 203
removing a member 203
restarting services 297
restricting access 262
setting date, time, time zone 237
Grid Manager
overview 39
grid master 167
configuring 179
promoting candidate 203
scheduled tasks after promoting 255
grid members
adding to grid 186
configuring NTP 245
configuring syslog 870
defining admin permissions 143
distribution and upgrade status 324
logging DHCP leases 606
monitoring services 868
permissions 150
read-only permission 147, 156
restarting services 298
setting date, time, time zone 237
grid status
distribution and upgrade 324
viewing detailed 860, 964
widget in Dashboard 81
GSS-TSIG
authenticating DDNS updates 493

H
hardware and software requirements 37
hardware status 866
Help panel 48
high availability (HA) pair
configuring grid master 181
deploying independent 220
grid members 187
rebooting 290
VRRP advertisements 178
host records
adding IP addresses 821
admin permissions 151
bulk 402
configuring 803
hostname restrictions 464
Hostname Compliance Report 465
admin permissions 151
hostnames
for DNS updates 481
restrictions 464
HSM signing 536
HTTP
configuring 304
defining admin permissions 162
redirecting to HTTPS 262
restricting access to appliance 262
uploading files 308
viewing status 867
HTTPS
defined 43

I
ICMP
network discovery 839
ICMP echo requests
ping 584
IF-MAP
Infoblox DHCP server 608
importing CSV files 63
importing zone data 379
independent appliances 205
Infoblox-1552, -1552-A
power supply status 863
Infoblox-1852-A
power supply status 863
Infoblox-2000, -2000-A
power supply status 863
RAID status 864
IP Address Management panel
admin permissions 147, 156
IP addresses
converting associated objects 830
reclaiming associated objects 833
selecting next available 634
viewing IP Map 817
IP Map 39, 817
IPv6
adding AAAA records 410
adding PTR records 411
configuring DNS 346
configuring for host records 806
configuring forward reverse-mapping zone 390
DNS views 358
managing networks and addresses 823
reverse-mapping zone 367
stub reverse-mapping zone 397

J
joining networks 815

L
LAN2 ports
configuring 271
viewing status 862
languages
supporting multiple 67
LCD
configure network settings 210
disabling 263
viewing status 862
licenses
activating 287
managing 287
removing 289, 291
lite upgrades 310
local admins 124
logging
configuring member 605
logging in
creating a banner 40
login options 40
steps 39
login banner 40
UTF-8 encoding 67
logs
audit log 873
DHCP 605
DHCP and DNS data 233
DHCP logs 605
DNS logging 871
Microsoft 757
replication 875
syslog 869
traffic capture 876
loopback interface
captive portal IP address 702

M
MAC address filters 672–674
defining admin permissions 161, 164
using in NAC Foundation module 695
MAC addresses
formats 645
master candidate 203
member status
Dashboard 81, 82
viewing detailed 860, 972
memory usage status 862
MGMT port
static routes 284
using 275
viewing status 862
MIBs
SNMP 893
Microsoft servers
configuring managing members 749
supported Windows versions 747
synchronizing DHCP data 777
synchronizing DNS data 759
Microsoft superscopes 792
MTU
for VPN tunnels 203
multi-ping 833
MX records
adding 412
adding to shared record groups 429, 432

N
name server groups 377–378
NAT
configuration example 215
NAT groups 169
NetBIOS
network discovery 839
network discovery
835–847
Dashboard 88
defining permissions 144, 837
managing discovered data 851
PortIQ appliances 848
viewing discovered data 850
network list 813, 827
network map 39, 810
network statistics
Dashboard 87
network views
configuring 575
displayed in bookmarks 52
DNS views 352
networks
adding from Net Map 812, 826
configuring and managing 345, 633
Dashboard 87
defining admin permissions 156
joining 815
permission to create from template 160
resizing 814
splitting 814
using templates 620
NIOS appliance
managing licenses 287
rebooting 290
resetting 290
restricting HTTP access 262
shutting down 290
NIOS GUI
setting timeout 263
NIOS software
downgrading 325
reverting 326
upgrading 314
NIOS version
upgrading and downgrading 172
viewing 314
NS records 409
NSEC resource record 522
NSEC3 resource record 522
NSEC3PARAM resource record 523
NTP
adding an authentication key 243
appliance as client 242
appliance as NTP server 246
authenticating 240
independent appliance 221
monitoring status 81, 238
using for appliances 239
viewing status 863
NXDOMAIN redirection 447

O
OSPF 550

P
passwords
length for admins 139
setting in user profile 41
permissions
applying 120
Dashboard widgets 71, 80
defining for admin groups 114
defining for DHCP 154
defining for DNS 148
defining for objects 115
defining for IFTP, HTTP, and FTP services 162
defining global 115, 118
for common tasks 141
for grid members 143
for network discovery 144
overview 114
phone home 878
ping
configuring settings 584
IP addresses 833
multi-ping 833
PortIQ appliances 848
ports
configuring VPN 202
DNS settings 440
Ethernet and service ports 265–269
for grid communications 181
   LAN2 271
   MGMT 275
source for DNS messages 274
viewing status 862
primary servers
   configuring 371
   name server groups 377
   stealth 372
printing data 66
   capacity report 877
   in smart folders 99
PTR records
   adding 411
   bulk hosts 402
   host records 803

Q queries
   controlling 444
   recursive 445

R RADIUS
   authenticating admins 129
   authenticating DHCP clients 716
RAID
   monitoring status 864
rebooting 290
recursion
   configuring 445
DNS views 353
   DNSSEC 541
recycle bin 52, 53
   enabling 202
   restoring zone data 385
relay agent filters 675–676
remote admins
   authenticating 127
   authenticating using Active Directory 133
   authenticating using RADIUS 129
   creating admin groups for 138
remote console access
   enabling and disabling 262
replication status
   viewing 875
reservations
   configuring 648
   defining admin permissions 158
   using templates 619
resetting NIOS appliances 290
resizing networks 814
resource records
   adding 407
   adding to shared record groups 429, 432
   bulk host records 402
   defining permissions 150, 151
DNSSEC 519
   specifying TTL 437
restarting services 297
restoring
   backup files 330
   using Recycle Bin 53
restoring database
   guidelines for scheduled tasks 255
reverting 326
   guidelines for scheduled tasks 255
RFC 2317 366
Riverbed Steelhead appliances
   vNIOS appliances 167
roaming hosts 651
root name servers 459
root zone 368
RRset Orders 439
RRSIG resource record 521
Rulesets
   blacklist 454
   NXDOMAIN 448

S scavenging leases 582
scheduling tasks
   canceling scheduled restart 299
   distributions 315
   network discovery 847
   upgrades 319
search
   global 59
   setting filters 56
secondary servers
   configuring 374
   forwarding updates 490
   name server groups 377
   notifying external 439
service status 867
shared networks
   defining admin permissions 156
   shared record groups 426
   admin permissions 152
shutting down 290
smart folders 93–99
   Finder panel 52
SNMP 885
   enable threshold crossing event trap 597
Infoblox MIBs 893
SOA records
   adding email address 438
   stub zone 398
   zone settings 372
software and hardware requirements 37
software distribution 315
   monitoring 324
Sophos NAC Advanced server 716
sort lists
   DNS 460
   sorting data 49
SPF records 414
splitting networks 814
SRV records
   adding 413
   adding to shared record groups 429, 432
SSH
   remote console access 262
   restrict access to MGMT port 279
SSL
   certificates 43–45
   overview 43
standalone configuring 207
Startup Wizard
  independent appliance 211
  independent HA pair 220
  single grid master 184
static routes configuring 282
stub zones 392
subzones 368
superusers
  configuring admin groups 108
  configuring extensible attributes 256
  defining global smart folders 95
  empty recycle bin 54
  name server groups 377
  scheduling grid restart 297
support bundles downloading 332
syslog 869–872
  exporting 66
system status
  Dashboard 82
system temperature status 863
system time
  monitoring 238
  setting date and time 237
  using NTP 239
T
tables
  customizing 49
  printing data 66
  selecting objects 49
  setting size 41
TACACS+
  authenticating admins 135
tasks
  monitoring background 62
TCP
  network discovery 840
technical support
  download support bundle 332
  enabling and disabling access 262
  restrict access to MGMT port 279
testing upgrades 318
TFTP
  backup files 326
  configuring 303
  defining admin permissions 162
  uploading files 308
  UTF-8 encoding for file names 67
  viewing status 867
time zone
  setting for grid 202
  setting for grid and members 237
  setting for independent appliances 221
  setting in user profiles 42
  upgrade schedule 319
timeout, setting 263
toolbar 48
tooltips 48
traffic capture tool 876
TTL
  DNSSEC key rollovers 529
  setting for resource records 437
TXT records
  adding 414
  adding to shared record groups 429, 432
  DDNS updates 486
U
upgrade groups 311
upgrade test 318
upgrading 314
  configuring upgrade groups 311
  guidelines for scheduled tasks 255
uploading NIOS software 315
user class filters 682
user names
  setting in user profile 41
  user profiles 41
UTF-8 encoding
  multilingual support 67
V
views
  See DNS views
  See network views
virtual appliances 167
virtual router ID
  in VRRP advertisements 178
  independent HA pair 221
VMware
  vNIOS appliances 167
  vNIOS appliances 167
  VRRP advertisements 178
W
widgets
  Dashboard 71
Z
zones
  applying name server groups 378
  configuring authoritative 364
  configuring properties 381
  copying records 356
  defining admin permissions 149, 150
  delegation 387
  enabling and disabling 369
  enabling transfers 457
  forward 389
  importing data 216, 379
  locking and unlocking 369
  removing 383
  restoring data 385
  root 368
  stub 392
  subzones 368