

INTRODUCTION

Infoblox NIOS™ 4.2r5-3 software, coupled with Infoblox appliance platforms, enables customers to deploy large, robust, manageable and cost effective Infoblox grids. The next-generation solution enables distributed delivery of core network services – including DNS, DHCP, IPAM, RADIUS, TFTP, and FTP – with the nonstop availability and real-time service management required for today's 24x7 advanced IP networks and applications.

In addition, Infoblox NIOS 4.2r5-3 software supports the Infoblox IPAM WinConnect system, which provides powerful IP management capabilities for Microsoft® DNS and DHCP services. You can download the WinConnect software components and documentation from the Infoblox support site.

For the most current version of these release notes, visit <http://www.infoblox.com/support>.

CHANGES TO DEFAULT BEHAVIOR IN NIOS 4.2r5-3

- In previous releases, because of the fix for CERT VU#800113, the maximum number of concurrent clients from which the appliance could receive recursive queries was limited to 800. In this release, that limit has increased to 20,000 due to the implementation of the ISC 9.3.5-P2 patch.

CHANGES TO DEFAULT BEHAVIOR IN NIOS 4.2r5-1

The fix for Vulnerability Note VU#800113 (see #24190 in the Resolved Issues section) resulted in the following changes to how BIND serves recursive queries:

- BIND uses random ports to serve recursive queries. Because of this change, Infoblox strongly recommends that firewall administrators set policies to allow the DNS service to use the entire range of ports; otherwise, the DNS service will be adversely affected.
- BIND uses a new socket (and hence file descriptor) for each recursive query. A large number of recursive queries could cause BIND to run out of file descriptors, affecting DNS service.

Therefore, the maximum number of concurrent clients from which the appliance can receive recursive queries is now limited to 800, when you enable the appliance to accept recursive queries and do not specify a static source port. Note that you can lower this value, but not increase it, in the Queries section of the Member DNS Properties editor.

NIOS 4.2r5 FEATURE

NIOS Virtual Appliance for Riverbed – You can now install the Infoblox NIOS software on Riverbed Steelhead appliances (models 520, 1020, 1520, and 2020) running the Riverbed RIOS Services Platform (RSP), and configure them as NIOS virtual appliances. NIOS virtual appliances are virtual grid members that include a full suite of core network services—DNS, DHCP, IPAM, RADIUS, FTP, TFTP, HTTP, and NTP. This combined solution allows you to configure a serverless branch office and, at the same time, deliver reliable local services to end users. Distributed organizations obtain the cost benefits of consolidation and the simplicity of centrally managed Infoblox NIOS virtual appliances.

The joint Infoblox-Riverbed solution supports hybrid environments that include a mix of physical Infoblox appliances and NIOS virtual appliances depending on branch office requirements. Each NIOS virtual appliance appears to the grid as a grid member, with all of the benefits of distributed services and centralized management. This includes centralized backup and restoration of user data, DHCP failover capabilities, one-touch software upgrades, local RADIUS authentication, DNS without latency, and many other benefits of the Infoblox solution.

For information on supported features and how to install the NIOS software on the RSP, refer to the *Quick Start Guide for Installing NIOS Software on Riverbed Services Platforms*.

NIOS 4.2r4 FEATURES

Authorization Model — Infoblox now provides additional fine-grained control over most DNS and DHCP objects in the Infoblox database. By default, Infoblox devices deny non-superusers access to grid members and certain DNS and DHCP objects if their administrative permissions are not defined. You can define permissions at a global level, for example, read-only permission to all DNS views or all DHCP networks in the database, as well as more granular permissions, such as read-write permission to a specific zone or network. You can even define permissions for a single record, such as an A record or a single fixed address. In addition, you can view and search for object permissions.

Staged Upgrades — To minimize the impact of grid upgrades to your operations, you can organize grid members into upgrade groups and define how and when their software distribution occurs. You can schedule their upgrade as well, when upgrading to an Upgrade Lite compatible maintenance release. You can define distribution and upgrade schedules to accommodate bandwidth and other constraints.

RADIUS Policies — You can define RADIUS policies that provide configuration information to hosts based on attributes the device receives in Access-Request packets. In addition, you can also define RADIUS policies that provide configuration information, such as VLAN assignments, to replicated users and users authenticated against an LDAP server based on their group membership.

IPAM Audit Fields — You can classify devices in your network and identify attributes you want to track in the audit log. The Infoblox device includes a set of predefined device types, such as routers and firewalls. You can create your own device types in addition to the predefined set. Each device type, whether predefined or user-defined, provides labels where users can enter specific information about a device, such as location, owner and manufacturer. There are also custom labels that you can define to meet the unique needs of your organization; for example, asset tag, building number, and floor number. These entries and the administrator who entered or changed them can be tracked in the audit log. Administrators can choose which device types and data labels are tracked in the audit log.

CSV Export — You can easily extract critical data from the Infoblox device and export it to a CSV (Comma Separated Values) file. You can move, hide, and display columns in the NIOS GUI to export data in the format you want.

Installable Grid Manager — You can install the Infoblox Grid Manager on a computer running any of the following Windows operating systems: Microsoft Windows XP with Service Pack 2 and Microsoft Windows Vista. The Grid Manager installs the Infoblox NIOS JRE files in a container within a Java sandbox on your computer. The files in the sandbox are used only by the Grid Manager and do not affect any other Java application on your system.

NIOS Cache — You can now manage the number of cached NIOS versions on your computer. By default, the Infoblox device caches 10 NIOS versions on your computer. You can change this default at any time. When the system meets the predefined maximum number of cache files, it deletes the first (oldest) and then adds the new version to the cache file.

Ranges and Fixed Address Templates — You can create DHCP range and fixed address templates to enforce organization standards for IP configuration. Users can then create DHCP ranges and fixed addresses based on the pre-defined templates. You are no longer required to add the DHCP range and fixed address templates to a network template before you can use them.

IPv6 Configuration Support — A device can now acquire the IP address of the default gateway and the link MTU from router advertisements.

DHCP 3.1 — NIOS now supports DHCP 3.1, which has enhancements that improve system stability and fault tolerance. Due to incompatibilities in the DHCP failover protocol in DHCP 3.1 and 3.0, DHCP failover does not work between two peers that are not from the same grid and that run a different DHCP version. For example, one peer runs NIOS 4.2r2 which supports DHCP 3.0.x and the other peer runs 4.2r4, which supports DHCP 3.1.x. In this case, Infoblox recommends that you upgrade both peers within a minimal amount of time. Note that when upgrading DHCP failover peers, the peers may work in a communications-interrupted state, and lease durations may be less than the configured default.

Host Information for Fixed Addresses — Syslog and the Name column of the IP Address Management panel now display the DHCP client hostname for fixed addresses as well as dynamic addresses.

DHCP Lease Details — When a DHCP failover peer allocates a lease, the Dynamic Lease Details panel now displays the DHCP server that allocated the lease and whether it is the primary or secondary peer in the DHCP failover association.

API Enhancements — This release includes following enhancements to the API:

- You can search for a specific Bulk Host object using zones with regular expressions. You can also filter the search by entering a start and end address.
- You can add, get, update, delete and search for IPAM device types.
- You can search for a host using the fields in the IPAM panel, such as name, device type and location, as well as the Custom1 through Custom20 fields. Regular expressions are supported.
- You can now search for DHCP templates using comments or name; both support regular expression.
- When you start a session and there is a version mismatch, the API returns a message reporting the version mismatch. You must then upgrade the Infoblox Perl module to the correct version.

CHANGES TO DEFAULT BEHAVIOR IN NIOS 4.2r4

- The required administrative permissions for some tasks have changed as follows:
 - Assigning a grid member to a zone requires read/write permission to the grid member.
 - Deleting a zone requires read/write permission to the grid member serving the zone.
 - Adding a match member to a view requires read-writer permission to the member.
 - Adding a view requires read/write permission to all views.
- After upgrading to 4.2r4, permissions set for “all zones” are converted to permissions for “all views”.
- The maximum Java heap size increased from 64 MB to 256 MB. Therefore, the Infoblox NIOS application may consume more memory on the administrator’s management station.
- The IB-TRAPONE-MIB was renamed to IB-TRAP_MIB. A “0” was also added to the OIDs of notifications.
- In previous releases, the DHCP process only validated the failover association name for peers that were members of the same grid. Starting with this release, the DHCP process also validates the DHCP failover association name for failover peers that are not members of the same grid. If the failover association names specified on the peers do not match, the failover association goes into disconnect mode.
- VitalQIP: After a VitalQIP push, the “named” service on the Infoblox device automatically restarted. The automatic restart could cause a routing recalculation if Anycast was configured. Starting with this release, the “named” service automatically reloads after an update push. However, you must restart

the “named” service after a configuration and data push. You can restart the “named” service through a user exit, or by using the QIP_CLI commands in the VitalQIP chroot environment. For information about the QIP_CLI commands, see the *Infoblox CLI Guide*.

NIOS 4.2r3 FEATURES

Root Name Servers – The Infoblox device enables you to specify Internet root name servers or custom root name servers at the grid, member, or custom view-level. If you enable recursive queries and the Infoblox device receives a recursive query for DNS data it does not have, it queries specified forwarders (if any) and then queries the root name servers you configure.

DDNS Domain Name – You can now enter a DDNS Domain Name at the network and DHCP range level. In addition, you can enter the DDNS Domain Name and Host Name at the Fixed Address level.

Stub Zone Enhancement – When you configure a stub zone, you can now specify a grid member as the primary server for the stub zone. In past releases, you could only specify an external primary server.

DHCP Option 61 – You can now assign fixed addresses to resources such as printers and servers based on the DHCP client identifier (option 61), which is either the MAC address or any string that uniquely identifies the client. The client sends the unique client identifier as option 61 in the DHCP DISCOVER and REQUEST packets, as described in RFC2132, DHCP Options and BOOTP Vendor Extensions. This feature also allows you to reserve an address without supplying a fake MAC address.

MAC Filter Partitioning – MAC filters are only replicated to grid members that require the MAC filter present at the local member. This feature makes more efficient use of the local member’s database objects.

Split Network to /31 – When you split a network, you can now set the netmask to /31 in the *Split Network* dialog box.

Enhanced Search in IPAM View – In the *IP Address Management* panel of the DHCP/IPAM perspective, you can now search for a record by entering a host name.

FTP – The Infoblox device provides support for file transfers using TFTP, HTTP, and FTP. You can upload files using the Infoblox GUI or public API to the Infoblox device. You can then allow specific network devices to retrieve the files using TFTP, or HTTP, or FTP.

Network devices, such as VoIP phones, can use the DHCP service on the Infoblox appliance for IP address assignments and the File Distribution services (TFTP, HTTP, or FTP) for IP device configuration downloads.

Download SNMP MIBs – You can now download the SNMP MIBs from the Infoblox device through the API and Infoblox GUI. Refer to the Session section of the API documentation for instructions on downloading the MIBs through the API. To download the MIB through the GUI, navigate to the Grid perspective and click *grid* > **Tools** > **Download SNMP MIBs**.

Audit Log Reporting – You can search and filter the Audit Log based on parameters you specify, such as the Admin Name and Message/Value, which can be any word or sentence from the message to be searched, or the value of the object created, modified, or deleted. For example, if you change the end IP address of a DHCP range from 10.0.20.0 to 10.0.30.0, you can enter 30 in the Message/Value field to find the log for this change.

You can also restrict the search by specifying the DNS object type and narrow it down further by specifying the DNS object name. For example, if you selected the DNS Object Type: DNS Authoritative Zone, you can enter Forward Mapping Zone as the DNS Object Name.

You can select a predefined time range or specify your own custom range and use this to search the audit log. For example, you can select the Predefined Range, **Last Week** to display all audit log activity that occurred one week before the current time. You can also produce a history report of an administrator's activity. For example, you can filter on specific administrator within a given timeframe.

Additional UTF-8 Support — The Infoblox GUI now supports UTF-8 characters for all Comment fields.

Reset Database — When you execute the `reset database` command, the device retains MGMT port settings, if enabled, in addition to the LAN port settings.

CLI Command to Revert Grid — You can now use the `set revert_grid` command to revert to the previous version of software that was running on your Infoblox device.

Additional Syslog Messages — The Infoblox device now generates syslog messages when scheduled backups fail due to an invalid user account or invalid path.

BloxSDB Database Performance and Scalability Enhancements — The Infoblox bloxSDB database has been enhanced to provide higher capacity and better performance. After the 4.2r3 upgrade you will experience a significant reduction in the percentage of "DB Capacity Used" when you view the status in the GUI or when you use the `show capacity` CLI command.

NIOS 4.2r2 FEATURES

Infoblox Grid Connector for Active Directory v2 (IGC/AD v2) — The Infoblox Grid Connector for Active Directory securely replicates users and groups from Microsoft Active Directory to the Infoblox grid master, where the data is stored in the built-in Infoblox bloxSDB™ database. The users and groups are then replicated over a secure VPN to Infoblox grid members.

IGC/AD v2 provides improved security, robustness and scalability with the following features:

- The communication between the grid connector and grid master is SSL protected. The grid connector has a Certificates dialog where you can install and manage SSL certificates.
- IGC/AD v2 can replicate multiple AD domains to the grid master, which then replicates the appropriate domains used by each grid member. In addition, when the grid master imports a domain, it imports all users and user groups, preserving the domain structure.
- The Infoblox device supports international characters in single-byte character sets from Windows XP and Vista RADIUS clients. It supports international characters in RADIUS user names, passwords, and comments.

Note: Upgrading the Infoblox device to NIOS 4.2r2 results in the removal of all the replicated users, as well as the AD domain configuration. After upgrading to 4.2r2, you must install IGC/AD v2 on the domain controller(s) and configure the Infoblox device to communicate with the new connector(s).

Combined User Name, IP Address and MAC Address in DHCP Lease History — The Infoblox lease history database now includes user names in the lease history record. The Infoblox device captures user names when users log in through the captive portal, a component of the NAC foundation module, and then displays the user names in the DHCP Leases, DHCP Lease History and IP Address Management panels. The addition of the user name means that the Infoblox device maintains a history of all users, their network addresses and the devices they were using with a time stamp. Users can now include user name as a filter criteria along with time stamp, MAC address, host name, etc. This record is of particular interest to auditors and compliance managers who occasionally perform forensic investigations and report on user network activity. Users can produce a report of a specific user's DHCP lease history and the device(s) they used to access the network. Note that you can use this feature only with the NAC Foundation module of the Infoblox device.

IPAM Device Types Custom Fields — The Infoblox IPAM feature provides predefined and custom labels you can use to classify systems in your network. The Infoblox device now supports 20 custom labels, Custom1 through Custom20. Before this release, the device supported 5 custom labels.

E-mail Address for SOA Record — You can now add an administrator e-mail address for an SOA record at the grid level. To enter the email address at the grid level, from the DNS Perspective, click **DNS Members > grid > Edit > Grid DNS Properties > General**, and enter the email address in the **E-mail Address (for SOA RRNAME field)** field.

Enhanced Forwarders List — The Forwarders section in the Grid DNS Properties editor now provides **Move Up** and **Move Down** buttons so you can change the order in which the servers are listed.

SNMP OID — The ibPlatformOne MIB contains the following new OIDs:

- `ibHardwareType` provides the model number of the Infoblox hardware platform.
- `ibHardwareId` provides the hardware ID of the Infoblox device.
- `ibSerialNumber` provides the serial number of the Infoblox hardware platform.

CLI Command for LCD Information — You can now use the command `show lcd_info` to view the information displayed on the LCD of the Infoblox device. This includes information about the device status, network, installed licenses, and hardware status.

New Options for Ping Command — The `ping` command now supports the following options: `ttl`, `packetsize`, and `count`.

API Search () Considerations — When using the `search ()` method, you could retrieve more information than expected. Include additional checks for exact matches. For examples, refer to the API Documentation.

SOAP::Lite Package Required for API — The Infoblox API now requires SOAP::Lite version 0.69 or higher, which allows you to make method calls to classes and objects that exist on the Infoblox device. For Windows, SOAP::Lite is not part of the core Perl distribution. For most UNIX versions, SOAP::Lite version 0.68 is part of the core distribution and you must then install SOAP::Lite version 0.69 or higher. Note that Soap::Lite 0.69 will cause existing ID Aware deployments to fail when upgrading the API.

To install SOAP::Lite version 0.69 or higher on your Windows or Linux management system, refer to the Infoblox API Documentation. To access the documentation from an Infoblox device, click **Help > API Documentation**.

NIOS 4.2r1 FEATURES

Shared Record Groups — Shared Record Groups (SRG) enable administrators to create groups of DNS records and then associate these groups with multiple views and zones. When a shared record is changed, it is dynamically updated in all associated views and zones.

For example, to add the same group of records in three different zones, you can just add the records in a shared record group and link the group to the three zones. To add another set of records in only two of the zones, create another group and link the group to the two specific zones.

You can create several zones that contain the same shared records. For example, if you have three views with two zones containing 100 records each, you need not create and maintain 600 individual records. You can simply create the 100 records and share them between two zones and three different views.

A unique icon identifies shared records both in the shared record group view and the regular DNS zone view and a unique icon identifies any zone with shared records.

You can use shared records to

- Include multiple A, AAAA, SRV, MX, and TXT resource records in a group and share the group between many zones.
- Simplify and expedite the administration of resource records. When you create or update a shared record, the device automatically updates it in all associated zones.
- Reduce object count by using one shared record instead of the creating the same record in multiple zones.

DNS Bulk Host Templates — Bulk host name formats provide a flexible way to define bulk host names. You can either define and use bulk host formats at the grid level, or override them at the bulk host level. You can also customize the number of octets, the separator, and whether the digits are zero-padded.

For the IP address 10.100.0.10, the format -\$1-\$2-\$3-\$4 generates the host name suffix -10-100-0-10. The format #1-#2-#3-#4 generates the host name suffix -010-100-000-010.

The following example shows the host name that each format generates for the zone test.com:

Four Octets: \$1-\$2-\$3-\$4 (Default) generates foo-192-168-1-15.test.com

One Octet: -\$4 generates foo-15.test.com

Three Octets: -\$2-\$3-\$4 generates foo-168-1-15.test.com

Two Octets: -\$3-\$4 generates foo-1-15.test.com

Delegated MAC Filter Administration — This feature enables granular control and security in the administration of MAC address filters. The superuser can grant read-only, read/write permission or deny access to **All MAC Address Filters** or to specific MAC Address Filters. Admin groups with read/write access to all MAC Address Filters can add, modify and delete MAC Address Filters and their associated MAC addresses. Admin groups with read-only access to specific MAC Address Filters can view those filters and their MAC address entries only. Admin groups with read/write access to specific MAC Address Filters can view, modify and delete those filters and their MAC address entries.

RADIUS LDAP Authentication — The RADIUS server has been enhanced to provide support for querying an LDAP server for user authentication, including OpenLDAP, Novell eDirectory, and Sun DS (but not Microsoft AD). The LDAP server must allow RADIUS server access to the clear text password. The Infoblox device supports all RADIUS methods such as PAP and MSCHAPv2. The Infoblox RADIUS server can be configured to query multiple LDAP servers; for example, you can specify that it check the LDAP server at 10.1.1.1 then the LDAP server at 10.1.1.2 if the first server is unavailable.

Configurable Authentication Process — The Infoblox RADIUS server can be configured to use multiple authentication mechanisms. The device checks the list of authentication services in the order you specify. You can configure the Action on Success and Failure fields to enable complex authentication schemes. For example, you can configure the device to first check the LDAP authentication service and if it does not succeed, check the local Infoblox user database.

Admin Authentication using Active Directory — Infoblox NIOS enables you to authenticate administrators using Active Directory (similar to RADIUS authentication). The device retrieves the administrator's group membership from Active Directory. When you configure the authentication policy, Active Directory appears in the list of authentication methods. The device uses the authentication methods in the order they are listed. After you add authentication methods, you can change the order of the list.

Adding Zones for DDNS Updates — You can manually add zones (not selected automatically) to the DHCP configuration file so that DDNS updates work correctly. This is useful when you use DHCP option 81 and the client specifies the domain used for the DDNS update. If the zone is not defined in the DHCP configuration file, then you can add it to the DNS Updates section of the Grid DHCP Properties editor.

CHANGES TO DEFAULT BEHAVIOR IN NIOS 4.2r1

- In previous releases, communication between the GUI and the device determined session timeout. The first request after the timeout registered the lack of activity and restarted services. Starting with this release, the GUI tracks mouse and keyboard activity. If there is no activity for the specified timeout interval, the first mouse or keyboard activity registers the timeout and restarts the GUI.
- The timeout interval setting in the Grid -> Edit -> Grid Properties -> Security (or from the Device perspective, click Device -> Edit -> Device Properties-> Security) panel no longer forces the GUI to restart. Also, it does not apply to the user session that sets it. It applies to all new users after it is set. The user that set it must log out and log back in to apply the new timeout value to the session.
- The names for PTR records appear as fully qualified domain names. For example, an IP address 10.0.0.1 in a 10.0.0.0/24 zone appears as 1.0.0.10.in-addr.arpa. In previous versions, the GUI only displayed the record name such as 1.
- You cannot search zones based only on the zone type. You can filter search results based on the zone type.
- The Infoblox device sorts records in a zone in a different way than the previous versions. IP addresses or partial IP addresses appear first in the sorted list in the Name column; sorted on IP addresses in the Value column, not alphabetically. All non-IP address entries (alphabetically sorted) follow.

BEFORE YOU INSTALL

Infoblox recommends that administrators planning to perform an update from a previous release create and archive a backup of the Infoblox device configuration and data before upgrading.

Note: You cannot upgrade from 3.x releases directly to NIOS 4.2r5-3. You must first upgrade to NIOS 4.1x and then to NIOS 4.2r5-3. Contact Infoblox Technical Support for assistance with upgrades.

NIOS 4.2r5-3 supports the following upgrade and revert paths:

4.2r5-2, 4.2r5-1, 4.2r5-0
4.2r4-3, 4.2r4-2, 4.2r4-1-sp1, 4.2r4-1, 4.2r4-0
4.2r3-8, 4.2r3-7, 4.2r3-6, 4.2r3-5, 4.2r3-4, 4.2r3-3, 4.2r3-2, 4.2r3-1, 4.2r3-0
4.2r2-2, 4.2r2-1, 4.2r2-0
4.2r2i-2, 4.2r2i-1, 4.2r2i-0
4.1r7-3, 4.1r7-2, 4.1r7-1, 4.1r7-0
4.1r6-3, 4.1r6-2, 4.1r6-1
4.1r5-3, 4.1r5-2, 4.1r5-1, 4.1r5-0
4.1r4-5, 4.1r4-4, 4.1r4-3, 4.1r4-2, 4.1r4-1
4.1r3-4, 4.1r3-3, 4.1r3-2, 4.1r3-1, 4.1r3-0
4.1r2-7, 4.1r2-6, 4.1r2-5, 4.1r2-4, 4.1r2-3, 4.1r2-2, 4.1r2-1, 4.1r2-0
4.1r1-8, 4.1r1-7, 4.1r1-6, 4.1r1-5, 4.1r1-4, 4.1r1-3, 4.1r1-2, 4.1r1-1, 4.1r1-0
4.0r3-6, 4.0r3-5, 4.0r3-4, 4.0r3-2, 4.0r3-1, 4.0r3-0

Note: You can only upgrade from NIOS 4.1r4-0 to 4.1r4-1. NIOS 4.2r5-3 does not support 4.1r4-0 as an upgrade or revert path.

Technical Support

Infoblox technical support contact information:

Telephone: 1-888-463-6259 (toll-free, U.S. and Canada); +1-408-625-4200, ext. 1

E-mail: support@infoblox.com

Web: <http://www.infoblox.com/support>

GUI Requirements

To use the NIOS 4.2r5-3 GUI, administrators must have one of the following installed on their management systems.

OS	Browser
Microsoft® Windows XP®	Microsoft Internet Explorer® 6.0+ Firefox 1.7+
Microsoft Windows Vista®	Microsoft Internet Explorer® 7.0+
Red Hat® Enterprise Linux®	Firefox 1.7+
Fedora Core 5 or higher	Firefox 1.7+

In addition, the Infoblox Management GUI requires Java Runtime Environment (JRE) version 1.5.0_14 or version 1.6. Infoblox recommends that you use the latest JRE 1.6 version for your platform. Note that JRE 1.6 and JRE 6.0 are the same version. You can download JRE from: <http://java.sun.com/javase/downloads/index.jsp>

Documentation

The *Quick Start Guide for Installing NIOS Software on Riverbed Services Platforms*, *Infoblox Administrator Guide*, *Infoblox CLI Guide*, and installation guides for the Infoblox-250, Infoblox-550, and Infoblox-1050, Infoblox-1550, Infoblox-1552, and Infoblox-2000 appliances are available in PDF format on the documentation CD that ships with the product and on the Support website: <http://www.infoblox.com/support/>

Training

Training webinars are also available on: <http://infoblox.com/support/webinars.cfm>. Access to this site requires the user ID and password you receive when you register your product at http://www.infoblox.com/support/product_registration.cfm

RESOLVED ISSUES IN 4.2r5-3

ID	Summary
26007	Dynamic DNS updates to zones override grid-level settings and added invalid email addresses for zones.
25697	When you used DIW to import a zone that had an A record, and the appliance searched for a corresponding PTR record, it erroneously returned IPv6 reverse zones as well as IPv4 reverse zones, causing the zone import to fail.
25696	When you created a host record from the IP Address Management panel, the "Select Zone" button in the Add Host editor disappeared after you selected a zone, but before you saved the host record. This prevented you from changing the zone after your initial selection.

25584	After creating an NS group with secondary servers that were either grid members or external servers, you could not select the group as the default NS group for a zone.
25531	The appliance generated an excessive amount of DHCP failover pool balancing messages in the syslog file.
25530	API: When you searched for fixed addresses by subnet, the fixed addresses were returned with incorrect network assignments.
25475	API: The Infoblox API did not support searching for host records by IP address.
25371	Upgrade failed because the name server check found a duplicate secondary server.
25347	Users could not access the Infoblox GUI after an upgrade due to an authentication failure. The failure happened when the MGMT port was enabled for remote admin authentication but MGMT settings were not configured at a grid member level.
25214	API: Using a "get" to retrieve a host record without a name failed.
25154	The appliance sent an SNMP trap when the LAN port went down. After the appliance restarted, it did not send an SNMP trap to indicate that the LAN port was back up.
25114	The Infoblox Trap MIB file included a definition with a missing semicolon (;). Because of this syntax error, the NetQos MIB browser was not able to open this MIB file.
25050	There were memory allocation errors while searching all leases, and this caused an HA failover.
25047	DHCP 3.1 supports different data types than DHCP 3.0 for some DHCP custom options. Starting with this release, the Infoblox device will treat values stored in the following four DHCP custom options as text: <ul style="list-style-type: none"> • host-name • nwip-domain • nds-tree-name • nds-context
25033	After an upgrade, the appliance did not store certain administrative permissions correctly.
25012	When using the PEAP or TTLS EAP authentication method, the appliance failed to append reply attributes in the Access-Accept packets to the outer tunnel when using policies that matched on Group-Internal attributes.
25001	The Infoblox-250 appliance did not save LAN port settings that were defined manually.
24883	API: After upgrading to 4.2r4-2 running a script to retrieve DHCP range based on start address caused the product to restart
24851	The grid master failed to start up after an upgrade because of an invalid VIP (Virtual IP address) in the upgrade policy. The invalid VIP pointed to an appliance that did not exist in the grid.
24837	Partial members would get stuck in "synchronizing" state when trying to join the grid.
24831	Adding exclusion addresses that exceeded the maximum limit caused the HA pair grid master to fail over due to a segmentation fault in the HTTPD process.
24819	Admins with read/write permission to all DNS views and all grid members were not allowed to reorder DNS views.

24755	Disabling the network to which a grid member belonged caused a syntax error in the DHCP configuration file that caused the DHCP service to fail.
24753	API: When you tried to delete a record from an Infoblox view, the record was deleted from all Infoblox views.
24737	Under certain circumstances, the NIOS GUI did not allow you to create new DNS views due to an incorrect new view key computation.
24632	When processing a dynamic DNS update that would change the TTL of existing resource records, the appliance sometimes encountered an internal problem and failed to perform the update. Now, when resource records for the same domain name and type have different TTLs, the appliance will deterministically select one of the TTLs for all records in the set.
24622	DHCP failover pool messages were logged at least 10 times per second.
24504	Disabling the network to which a grid member belonged caused a syntax error in the DHCP configuration file that caused the DHCP service to fail.
24447	API: Improved performance when using the API to assign a large number of DHCP ranges to relay agent filters.
24419	In an HA pair, the Infoblox device could not restart services because the passive node did not have valid service licenses.
24316	Disabling the network to which a grid member belonged caused a syntax error in the DHCP configuration file that caused the DHCP service to fail.
24190	Vulnerability Note VU#800113 (CVE-2008-1447) related to cache poisoning exploits that could be launched against various name servers, including BIND. NOTE: This fix resulted in changes to how BIND serves recursive queries. For additional information, see <i>Changes to Default Behavior in NIOS 4.2r5-1</i> .
24086	Lookup of a DNS wildcard record one or more levels inside a zone could trigger an internal data validity error and cause the premature exit of 'named'.
23893	Under certain circumstances, a grid master candidate could use excessive disk space.
23868	API: The Infoblox API did not support searching for host records by IP address.
23827	The support bundle included all the rotated logs, except for the first log file (log file with the extension "0.gz").
23797	The NIOS appliance generated a system error message when you tried to view a zone that had a subzone with an SOA record that did not specify a primary server.
23722	The Manage Grid Restart Services dialog box did not display the correct status of a disabled DHCP service.
23672	Improved performance when validating grid DNS updates for datasets with a large number of zones.
23633	The NIOS appliance did not support non-tunneled MS-CHAP and MS-CHAPv2 authentication methods.
23625	API: The Infoblox API did not support searching for host records by MAC address.
23564	API: The get and search functions have a new attribute—served_by—that you can use to retrieve the IP address of the server that handed out an active lease in a DHCP failover configuration.
23392	A member would remain in the "synchronizing" state when trying to join the grid.
23062	API: Resolved some performance issues with searching for zones using the Infoblox API.

23006	IP addresses used in a CNAME record within an RFC 2317 reverse zone were in conflict with IP addresses in the bulk host range.
22388	After a DHCP service restart, the NIOS appliance sent invalid threshold notifications stating that it was running out of IP addresses.
22043	API: The NIOS appliance experienced high memory utilization when users searched for host records using the <code>\$session->search()</code> expression in an API script.
21979	The forced restore operation failed when the target was a standalone appliance and the option to retain IP settings was selected.
18808	The <code>/etc/mtab~</code> file that was generated by internal processes might have inhibited distribution on an appliance and caused the distribution to fail during an upgrade.

KNOWN GENERAL ISSUES

ID	Summary
25745	Before NIOS 4.2r3-6, PTR records in reverse zones that were not assigned to a DNS server or name server group were resolved as if they were coming from the parent zone. After upgrading to NIOS 4.2r3-6, the appliance stopped resolving the PTR records in the child zone. For additional information on this issue and how to repair it, log in to the Infoblox Technical Support Knowledge Base and access article #12892.
25719	Configuration changes made to the <code>0.0.127.in-addr.arpa</code> zone were not stored by the appliance after upgrading to NIOS 4.2r4. Note that this is a system-defined zone and cannot be configured in NIOS 4.2r4 and later.
19475	A single grid member sometimes fails to boot up if removed from the grid. If you need assistance with removing a node from the grid and if you run into this problem, please contact Infoblox Support.
18629	NIOS 4.1r4-1 and later do not support IPv6 Link-local addresses.
18059	When you upload a file into TFTP storage, the device does not display an error message when it reaches the maximum storage limit.
18028	Do not configure an IPv4 zone primary (master) with IPv6 secondary devices (slaves). The server validation does not allow you to configure an IPv4-only device to communicate with IPv6 addresses. If you use IPv6 in the primary, then the device can communicate with IPv6 secondaries.
17547	If downgrade fails midway through the process, some elements might not be properly cleaned; therefore, a subsequent downgrade may fail. Workaround: Reboot the device to clean up all of the elements so that the downgrade can proceed.
17458	You cannot use global search to search RADIUS properties (RADIUS authentication) by specifying the IP address of the RADIUS server.
17324	The front power supply LED status on the Infoblox-2000 stays lit when the power supply goes offline.
17314	The service restart icon blinks after changing the host name policy check. This is not the correct behavior.

ID	Summary
17273	If the last node in a tree within the GUI is expandable, the GUI only displays as many branches as there is room to accommodate in the GUI view; the scroll bar do not adjust for you to see the remaining branches. This is a known issue in Linux Fedora Core 4 and appears to be addressed in Fedora Core 5, and the issue does not exist in Windows. Workaround: Expand any node above the last node. This adjusts the scroll bar accordingly.
17195	Opening zone statistics after disabling that zone causes a popup error dialog box to appear.
17054	The GUI allows read/write permissions to be assigned to the secondary zones and stub zones but only read-only and deny permissions apply to these zone types. The read/write permission for these zone types exhibits the same behavior as a read-only permission.
16799	For zones with a primary that is external to the grid, it may take up to 15 minutes for changes to the zone to become visible in the zone viewer in the GUI. This happens because the 'named' defers writing to the zone file in order to avoid constant rewrites caused by frequent updates to the zone.
16103	VIM: Infoblox does not support or recommend serial interface access to the VitalQIP restricted shell.

KNOWN LIMITATIONS OF THE NIOS VIRTUAL APPLIANCE

The NIOS virtual appliances support most of the features of the Infoblox NIOS software. However, due to limited system resources on the RSP (Riverbed Services Platform), such as CPU time, RAM memory, and storage disk space, the NIOS virtual appliance has the following limitations:

- NIOS virtual appliances are designed to function as grid members only. They do not support configuration as an HA (high availability) pair, a grid master, or a grid master candidate.
- On a grid with a NIOS virtual appliance as a grid member, the maximum storage space for HTTP, FTP and TFTP is limited to 1GB (a grid with only Infoblox appliances provides a maximum of 5GB for these services).
- On a NIOS virtual appliance, the maximum size of core files is limited to 100 MB, and syslog and infoblox.log files are limited to 20MB each.
- The LAN interface is the only network interface available on the NIOS virtual appliances. You cannot configure the speed and transmission type (full or half duplex) of the network interface.
- You can control the IP traffic capture only on the LAN port.
- The NIOS virtual appliances do not support the following features:
 - Anycast addressing
 - Configuration as a DHCP lease history logging member
 - Configuration as a RADIUS accounting server
 - Dedicated MGMT port
- On a NIOS virtual appliance, the **shutdown** command restarts the NIOS virtual appliance instead of halting it. Infoblox recommends that you use the Riverbed **no rsp enable** command to perform a shutdown.