NIOS 6.11.0 Release Notes

NIOS 6.11.0 Release Notes

INTRODUCTION

Infoblox NIOS™ 6.11 software, coupled with Infoblox appliance platforms, enables customers to deploy large, robust, manageable and cost-effective Infoblox Grids. This next-generation solution enables distributed delivery of core network services—including DNS, DHCP, IPAM, TFTP, and FTP—with the nonstop availability and real-time service management required for today's 24x7 advanced IP networks and applications.

Please note the following:

- This release supports new hard disk drives on Trinzic 1400, 1410, 1420, 2200, 2210, and 2220 appliances.

- NIOS 6.1.0 and later versions do not support the IF-MAP service. You cannot upgrade Infoblox Orchestration Servers to NIOS 6.1.0 and later. The IF-MAP service is supported in 5.1r2-IBOS-1, 6.0.0-IBOS-1, IBOS 2.1.0 and later releases. For more information, visit the Infoblox Support web site at https://support.infoblox.com.

- NIOS 6.0 and later is not supported on Cisco's AXP platform (vNIOS for Cisco) due to the lack of 64-bit support on that platform. As a result, you cannot upgrade a Grid with a vNIOS for Cisco Grid member on AXP to NIOS 6.0 or later. If you'd like to run Infoblox NIOS 6.0 or later on your Cisco 2900 or 3900 series ISR routers, please choose the Cisco SRE-V (UCS Express) software platform, which supports Infoblox vNIOS for VMware virtual appliances.

Supported Platforms

Infoblox NIOS 6.11.0 is supported on the following platforms:

- **NIOS Appliances**
  - Infoblox Advanced Appliances: PT-1400, PT-2200, and PT-4000
  - Network Insight Appliances: ND-800, ND-1400, ND-2200, and ND-4000
  - Trinzic Appliances: TE-100, TE-810, TE-820, TE-1410, TE-1420, TE-2210, TE-2220, and Infoblox-4010
  - All Trinzic Rev-1 and Rev-2 appliances (For more information about Trinzic Rev-2 appliances, refer to KB article 17748, available on the Infoblox Support web site at https://support.infoblox.com.)
  - Trinzic Reporting: TR-800, TR-1400, TR-2000, and TR-4000
  - Infoblox-250-A, -550-A, -1050-A, -1550-A, -1552-A, -1852-A, -2000, and -2000-A
  - Infoblox-4030 DNS Caching Accelerator Appliance

  Infoblox NIOS 6.11.x is not supported on the Infoblox-250, -500, -1000, -1200, -550, -1050, -1550, and -1552 appliances.

  Please see **Upgrade Guidelines** on page 34 if you are upgrading a Grid that contains these appliances and for additional upgrade information.

- **vNIOS for Microsoft Server 2008 R2 and 2012 R2 Hyper-V**
  The Infoblox vNIOS virtual appliance is now available for Windows Server 2008 R2 and Windows Server 2012 R2 that have DAS (Direct Attached Storage). Administrators can install vNIOS virtual appliance on Microsoft Windows® servers using either Hyper-V Manager or SCVMM. A Microsoft Powerscript is available for ease of installation and configuration of the virtual appliance. Note that vNIOS for Hyper-V is not recommended as a Grid Master or Grid Master Candidate. With this release, you can deploy certain vNIOS appliances with a 50 GB, 55 GB, or 160 GB hard disk. You can also deploy the IB-VM-800 and IB-VM-1400 virtual appliances as reporting servers. For more information about vNIOS for Hyper-V, refer to the *Infoblox Installation Guide for vNIOS on Microsoft Hyper-V*.

The following table lists the supported vNIOS for Hyper-V appliance models:

vNIOS Appliances	Storage (GB)	# of CPU Cores	Memory Allocation
IB-VM-100	55	1	1 GB
IB-VM-800 (for reporting only; 1 GB daily limit)	50	2	Range: 2 – 8 GB Default: 8 GB
IB-VM-800 (for reporting only; 2 GB daily limit)	50	2	Range: 4 – 8 GB Default: 8 GB
IB-VM-810	55	2	2 GB
IB-VM-810	160	2	2 GB
IB-VM-820	55	2	2 GB
IB-VM-820	160	2	2 GB
IB-VM-1400 (for reporting only; 5 GB daily limit)	55	4	Default: 8 GB
IB-VM-1410	55	4	8 GB
IB-VM-1410	160	4	8 GB
IB-VM-1420	160	4	8 GB
Network Insight vNIOS Appliances	**Storage (GB)**	**# of CPU Cores**	**Memory Allocation**
ND-VM-800	160	2	8 GB
ND-VM-1400	160	4	16 GB

- **vNIOS for VMware on ESX/ESXi Servers**
  The Infoblox vNIOS on VMware software can run on ESX or ESXi servers that have DAS (Direct Attached Storage), or iSCSI (Internet Small Computer System Interface) or FC (Fibre Channel) SAN (Storage Area Network) attached. You can install the vNIOS software package on a host with VMware ESX or ESXi 4.1, 5.0, 5.1 or 5.5 installed and configure it as a virtual appliance. Note that IB-VM-100 virtual appliances can only run on ESXi 5.1 servers.

  vSphere vMotion is also supported. You can migrate vNIOS virtual appliances from one ESX or ESXi server to another without any service outages. The migration preserves the hardware IDs and licenses of the vNIOS virtual appliances. VMware Tools is automatically installed for each vNIOS virtual appliance. Infoblox supports the control functions in VMware Tools. For example, through the vSphere client, you can shut down the virtual appliance.

  You can deploy certain vNIOS virtual appliances with different hard disk capacity. Some vNIOS appliances are not supported as Grid Masters or Grid Master Candidates. Note that the IB-VM-800 and IB-VM-1400 virtual appliances are designed for reporting purposes. For more information about vNIOS on VMware, refer to the *Infoblox Installation Guide for vNIOS Software on VMware*. For information about vNIOS virtual appliances for reporting, refer to the *Infoblox Installation Guide for vNIOS Reporting Virtual Appliances*.

The following table shows the supported vNIOS for VMware appliance models:

A-Series Virtual Appliances	Disk (GB)	# of CPU Cores	Memory Allocation	Virtual CPU Core Frequency	Supported as Grid Master and Grid Master Candidate (Yes/No)
IB-VM-250	50	1	2 GB	700 MHz	No
IB-VM-250	120	1	2 GB	700 MHz	No
IB-VM-550	50	1	2 GB	1200 MHz	No
IB-VM-550	120	1	2 GB	1200 MHz	Yes
IB-VM-1050	50	1	2 GB	2000 MHz	No
IB-VM-1050	120	1	2 GB	2000 MHz	Yes
IB-VM-1550	120	2	8 GB	5500 MHz	Yes
IB-VM-1850	120	4	8 GB	10000 MHz	Yes
IB-VM-2000	120	4	12 GB	12000 MHz	Yes

Trinzic Series Virtual Appliances	Disk (GB)	# of CPU Cores	Memory Allocation	Virtual CPU Core Frequency	Supported as Grid Master and Grid Master Candidate (Yes/No)
IB-VM-100	55	1	1 GB	1300 MHz	No
IB-VM-800 (for reporting only; 1 GB daily limit)	50	2	Range: 2 – 8 GB Default: 8 GB	3000 MHZ	No
IB-VM-800 (for reporting only; 2 GB daily limit)	50	2	Range: 4 – 8 GB Default: 8 GB	3000 MHZ	No
IB-VM-810	55	2	2 GB	2000 MHz	No
IB-VM-810	160	2	2 GB	2000 MHz	Yes
IB-VM-820	55	2	2 GB	3000 MHz	No
IB-VM-820	160	2	2 GB	3000 MHz	Yes
IB-VM-1400 (for reporting only; 5 GB daily limit)	55	4	Default: 8 GB	8000 MHz	No
IB-VM-1410	55	4	8 GB	6000 MHz	No
IB-VM-1410	160	4	8 GB	6000 MHz	Yes
IB-VM-1420	160	4	8 GB	8000 MHz	Yes
IB-VM-2210	160	4	12 GB	12000 MHz	Yes
IB-VM-2220	160	4	12 GB	12000 MHz	Yes

Network Insight Virtual Appliances	Disk (GB)	# of CPU Cores	Memory Allocation	Virtual CPU Core Frequency	Supported as Grid Master and Grid Master Candidate (Yes/No)
ND-VM-800	160	2	8 GB	3000 MHz	No
ND-VM-1400	160	4	16 GB	8000 MHz	No
ND-VM-2200	160	4	24 GB	24000 MHz	No

- **vNIOS for VMware on Cisco UCS Express/SRE-V**
  The Infoblox vNIOS on VMware software can also run on Cisco SRE-V (Services Ready Engine Virtualization), which is part of the Cisco UCS (Unified Computing System) Express. Infoblox has certified running vNIOS for VMware on Cisco SRE-V v1.5 (for ESXi 4.1) and v2.0 (for ESXi 5.0). Cisco SRE-V enables the VMware vSphere Hypervisor to be provisioned on Cisco SRE 700/710 and 900/910 Service Modules. The Cisco SRE Service Module can reside in the Cisco 2900 and 3900 series ISRs G2.

  The following table lists the supported vNIOS on VMware virtual appliances on SRE 700/710 and SRE 900/910:

vNIOS on VMware Virtual Appliances	Cisco SRE 700/710	Cisco SRE 900/910
IB-VM-100	Yes	Yes
IB-VM-250	Yes	Yes
IB-VM-550	Yes	Yes
IB-VM-1050	No	Yes
IB-VM-810	No	Yes
IB-VM-820	No	Yes

  Note that all vNIOS on VMware virtual appliances running on Cisco SRE-V are not recommended as Grid Masters or Grid Master Candidates. The IB-BOB virtual appliance has been renamed to IB-VM-100, For new installation, use the 55 GB software image. IB-VM-100 only supports configuration as a Grid member.

- **vNIOS on Riverbed® Steelhead Appliances**
  Infoblox has certified the vNIOS on Riverbed software with the following Riverbed Steelhead models and software versions:

Riverbed Models	Supported RiOS and EX versions
1050, 2050, 5050	RiOS 7.5, RiOS 8.0, RiOS 8.5
EX560, EX760, EX1160, EX1260	EX 1.0 (RiOS 7) EX 2.0 (RiOS 8.0), EX 2.5 (RiOS 8.0), EX 3.0 (RiOS 8.5.0), EX 3.1 (RiOS 8.5.1)

  For additional information, refer to the *Infoblox Installation Guide for vNIOS Software on Riverbed Steelhead Platforms.*
  NOTE: You can upgrade a Grid with a Riverbed virtual member to NIOS 6.11. Ensure that the Riverbed model has 64 bit support.

- **vNIOS for Xen Hypervisor**
  The Infoblox vNIOS for Xen is a virtual appliance designed for Citrix XenServer 6.1 and 6.2 running Xen hypervisor and for Linux machines running Xenproject.org 4.3 hypervisor. You can deploy vNIOS for Xen virtual appliances as the Grid Master, Grid members, or reporting servers depending on the supported models. Note that the IB-VM-800 virtual appliances are designed for reporting purposes only. For more information about vNIOS for Xen, refer to the *Infoblox Installation Guide for vNIOS for Xen Hypervisor*. For information about vNIOS virtual appliances for reporting, refer to the *Infoblox Installation Guide for vNIOS Reporting Virtual Appliances*.

The following table shows the supported vNIOS for Xen appliance models:

Trinzic Series Virtual Appliances	Disk (GB)	# of CPU Cores	Memory Allocation	Supported as Grid Master and Grid Master Candidate (Yes/No)
IB-VM-100	55	1	1 GB	No
IB-VM-800 (for reporting only; 1 GB daily limit)	50	2	Range: 2 – 8 GB Default: 8 GB	No
IB-VM-800 (for reporting only; 2 GB daily limit)	50	2	Range: 4 – 8 GB Default: 8 GB	No
IB-VM-810	55	2	2 GB	No
IB-VM-810	160	2	2 GB	Yes
IB-VM-820	55	2	2 GB	No
IB-VM-820	160	2	2 GB	Yes
IB-VM-1410	55	4	8 GB	No
IB-VM-1410	160	4	8 GB	Yes
IB-VM-1420	160	4	8 GB	Yes
IB-VM-2210	160	4	12 GB	Yes
IB-VM-2220	160	4	12 GB	Yes

NEW FEATURES

This section lists new features in each NIOS 6.x release.

NIOS 6.11.0

Infoblox Advanced DNS Protection Enhancements

This release adds the following enhancements for Infoblox Advanced DNS Protection:

- **HA Support**: You can now configure two appliances as an HA (high availability) pair to provide hardware redundancy for Advanced DNS Protection.
- **Ruleset Updates**: Before you manually publish a ruleset, you can now view differences between the current ruleset and the newly downloaded one. You can also modify some changed parameters and then merge the changes from the old version into the new one. The appliance retains up to nine (9) rulesets, including up to five (5) old rulesets, one (1) newly downloaded ruleset, and three (3) additional rulesets that you can mark as “Do Not Delete” at the Grid level.
- **Rate Limiting Rules**: This release adds new DNS response based rate limiting rules for the following threats: NXDOMAIN floods, NXRRSET floods, SERVFAIL floods, and DNS tunneling. These rate limiting rules are supported for queries originated through UDP.
- **Monitoring Mode**: This release adds a monitoring mode for the threat protection service. You can enable or disable the monitoring mode for each Grid member through a newly added CLI command. When the monitoring mode is enabled, the appliance logs DNS packets (instead of dropping them) that would have been blocked by specific threat protection rules.

Advanced DNS Protection employs hardware-accelerated security rules to detect, report upon, and stop DoS (Denial of Service), DDoS (Distributed Denial of Service) and other network attacks targeting DNS caching and authoritative applications. This feature helps minimize “false positives” and ensures that your mission-critical DNS services continue to function even when under attack. For more information about the enhancements, refer to the *Infoblox NIOS Administrator Guide*.

DNS Integrity Check

To protect your authoritative DNS server against DNS domain hijacking, you can configure the appliance to periodically monitor DNS data for top-level or parent authoritative zones. Based on your configuration, the appliance periodically checks DNS data in the NS RRsets for these zones and compares the data with that in the appliance database. It then reports data discrepancies through SNMP traps and logs related events in the syslog. DNS integrity check is supported on all Infoblox appliances, including Advanced Appliances used primarily for Infoblox Advanced DNS Protection.

IPAM Enhancements for Microsoft Management

This release adds the following IPAM enhancements for Microsoft Management:

- You can now enable or disable the monitor and control settings for DNS and DHCP services for Microsoft servers.
- Synchronizing IP addresses with invalid MAC addresses.
- Output destinations for Microsoft server log messages in the syslog.
- Synchronization and configuration of Microsoft DHCP failover relationships.
- RPC (Remote Procedure Call) timeout setting.
- Maximum concurrent connections for Microsoft servers.
- Enabling and Disabling DNS zone synchronization.

Multiple Primary Servers for DNS Authoritative Zones

You can now define multiple primary servers for DNS authoritative zones. When you configure multiple primaries for a zone, each primary has a copy of the zone's authoritative data that can be updated independently. When you modify zone data, the appliance replicates updated data among all primary servers. You can also define the default primary server that the appliance uses to perform DDNS updates for a zone that has multiple primary servers.

For more information about this feature, refer to the *Infoblox NIOS Administrator Guide*. Before you deploy this feature, Infoblox recommends that you carefully review the "Best Practices for Defining Multiple Primaries for Authoritative Zones" section in the Admin Guide.

Improved Authoritative DNS Performance

Improvements have been made to the following:

- DNS query processing to improve query throughput for authoritative queries with random existent or non-existent domain names.
- Performance of the zone transfer operation.

GSS-TSIG Enhancements

This release adds the ability to allow (on a single DDI Grid member) GSS-TSIG based DDNS updates from multiple clients in a single forest or multiple forests using keys that are appropriate for their respective domains.

Network Insight Enhancements

This release adds the following Network Insight enhancements:

- **Switch Port Reservation**: When creating or editing hosts, fixed addresses, reservations or Grid members, you can reserve specific switch ports for the object IP addresses or the Grid member network interfaces.
- **Switch Port Configuration**: You can perform switch port configuration for a device interface's admin status, VLANs, or descriptions in several places. This can be done in the wizards while doing switch port reservation, or in the views for the device interfaces, IP addresses, or assets. In the device related views, switch port configuration can be done through inline editing or through editors that allow a single or multi-edit of interfaces. The interface list view displays the run-time status of the switch port configuration. Extensible attributes can also be configured for devices and interfaces.
- **Network Provisioning and De-provisioning**: You can provision networks and de-provision (remove) networks from individual devices. Provisioning can be done while adding a new network or for an existing network. When networks are provisioned, an existing interface can be selected or a new VLAN can be created for the network (if supported by the device). You can also de-provision a network, whether it is a discovered network (not present or seen by IPAM), an unmanaged network, or a managed network. The IPAM network view will display the run-time status of the provisioning progress.
- **Discover Now**: You can use the Discover Now feature to discover an existing object. Objects selected for immediate discovery are given a one-time priority over other devices for data collection. The Discover Now status for the object will display the run-time status for the discovery.
- **Conflict Resolution**: Conflicts can occur when the configuration information is different than the discovered information. For this release, new conflicts can occur due to the added features. These include device information conflicts and port reservation conflicts. To identify these conflicts, you can locate them using the *Conflicts Smart Folder*. A new conflict resolution dialog allows resolution of multiple conflicts for the same IP address.
- **Discovery Blackout Periods**: You can now define scheduled time periods in which the appliance does not perform discovery or port control operations, which include network provisioning and switch port configuration. These time periods are called blackouts. All protocols associated with discovery (SNMP,

CLI through Telnet and SSH, port scanning, fingerprinting and ping sweeps) can be blocked during discovery blackout periods.

- **Task Manager**: The Task Manager has been updated to display and manage both object change and port control tasks.
- **Reporting**: New discovery reports are available when using the Reporting feature. These include reports for inactive IP addresses and reports related to port capacity.

DNSSEC Updates

This release adds the following DNSSEC enhancements:

- Performing tasks on multiple zones in one operation (signing, unsigning, rolling over KSK, rolling over ZSK).
- Ability to perform several KSK rollovers and ZSK rollovers.
- Schedule the rollover of one KSK or multiple KSKs for a zone.
- Manual rollover of a ZSK.
- Automatic KSK rollover and improved notifications.
- Configuration of NSEC3 salt length and hashing iterations.
- Ability to disable DNSSEC validation for non-authoritative zones.
- Support of pre-publish rollover method for ZSK.
- Ability to delete a key to perform an emergency KSK rollover or ZSK rollover.

Reporting Enhancements

This release adds a few enhancements for reporting. You can now do the following:

- Generate PDFs from any reports, which now support multiple pages, table panels, and chart panels. The PDF report names consist of the report or panel names and a timestamp.
- In addition to configuring scheduled email delivery for PDF reports, you can choose to email the reports immediately.
- Immediately download PDF reports to your local computer.
- Modify the logo image and embed it in the PDF reports.
- Override page size and page orientation for PDF reports.
- When emailing reporting PDFs or configuring alerting emails, you can override email addresses at the reporting member level, or at the report/search level.
- View and configure the index (storage space) allocated for each report category on the reporting server.
- For reports with TopN for members, TopN is now configurable. You can enter any number or use the predefined values of 5, 10, 20, 50, 100, 200, 150, or 500.
- For specific reports, you can enable the reporting server to group members with the same extensible attribute value and generate a single report for grouped members. You can also use the extensible attributes as filters. When you enable this feature, you can select an extensible attribute that is associated with a member. In addition, you can set the data calculation method to decide which statistic value you want to be displayed for grouped members. Following are the specific reports:
    - DNS Daily Query Rate by Server
    - DNS Daily Peak Hour Query Rate by Server
    - DNS Query Rate by Server
    - Traffic rate by Server
    - Threat Protection Event Count by Member
    - Threat Protection Event Count by Member Trend
    - DNS Response Latency Trend

  - DNS Cache hit ratio broken down by server
  - CPU Utilization trend (Detailed)
  - Memory Utilization trend

This release also adds the following internal reports:

- Reporting Index Usage Statistics
- Reporting Volume Usage Trend per Category
- Reporting Volume Usage Trend per Member

Enabling ARP on Passive Nodes of HA Pairs
You can now enable ARP (Address Resolution Protocol) on the passive node of an HA pair and monitor its status externally. For example, when the active node of an HA pair fails over to the passive node, you can conveniently ping the passive node from an external location and monitor its status. By default, the ARP is disabled on the passive node of an HA pair.

IPAM Utilization Email and SNMP Trap Alerts
You can define thresholds for IPAM utilization in a network or network container and configure the appliance to send SNMP traps and email notifications to a designated destination when IPAM utilization in a network or network container crosses the configured thresholds.

Enhancements for the bloxTools Service
This release enhances the bloxTools service so you can configure the service on port 443, 444 or on a port between 1024 and 63999. You can also enable HTTP to HTTPS redirection for the bloxTools service from the default HTTP port 80 to any specified HTTPS port. When you enable HTTP to HTTPS redirection, all the requests sent to the HTTP port are redirected to the HTTPS port configured for the bloxTools service. By default, NIOS appliance does not redirect HTTP requests to HTTPS.

Custom Feed Zones
Infoblox Custom Feed Zones is a new capability that allows you to specify your own aggregated threat feeds for the Infoblox DNS Firewall. You can use this feature to tailor DNS Firewall behavior in accordance with your organization security needs and policies. You can pick and choose from a variety of primary feed sources, threat types, and locations through an interface that will be available on the Infoblox Support Portal.
NOTE: This feature is not delivered as part of the NIOS software. Contact your Infoblox representatives for information about how to access this through the Support Portal when the feature becomes available.

vNIOS Virtual Appliances for Citrix XenServer and Xenproject.org Hypervisor
The Infoblox vNIOS for Xen is a virtual appliance designed for Citrix XenServer 6.1 and 6.2 running Xen hypervisor and for Linux machines running Xenproject.org 4.3 hypervisor. You can deploy vNIOS for Xen virtual appliances as the Grid Master, Grid members, or reporting servers depending on the supported models. Note that the IB-VM-800 (with 1 GB or 2 GB daily reporting limit) virtual appliances are designed for reporting purposes only.

Support for New Physical and Virtual Reporting Appliances
This release adds support for the TR-800 (2 GB daily reporting limit) physical appliance and the following vNIOS reporting virtual appliances: IB-VM-800 (with 1 GB or 2 GB daily reporting limit) and IB-VM-1400 (with 5 GB daily reporting limit). You can deploy the vNIOS virtual reporting appliances on Microsoft Windows Server 2008 R2 or 2012 R2 running Hyper-V Manager or SCVMM (System Center Virtual Machine Manager), and on VMware ESX or ESXi servers. You can also deploy the IB-VM-800 (with 1 GB or 2GB daily reporting limit) on Citrix XenServers or Linux systems running Xenproject.org 4.3 hypervisor.

New Permissions for DNS Resources

This release adds new permissions for DNS resources that have associated IP addresses in network containers, networks, and ranges so you have more control over who can perform which tasks for these DNS resources without affecting permissions defined for the networks and ranges to which these resources belong.

DNSSEC for RPZs, DNS Backlists, and NXDOMAIN Rules

You can now configure the NIOS appliance to always apply RPZ policies, DNS blacklists, and NXDOMAIN rules to DNS responses, regardless of whether DNS queries request DNSSEC records.

Authentication for BGP Neighbors

To avoid malicious interferences by ASs (Autonomous Systems), you can configure authentication for BGP neighbors to ensure that routing information exchanged between BGP peers is authentic, and that the information is accepted only when the authentication is successful.

DHCP Option 82 Logging Formats

When you define the circuit ID or remote ID of a relay agent as a host identifier, you can define the logging format (hexadecimal or plain text) that Grid Manager uses to display the relay agent ID, circuit ID, and remote ID in the detailed lease information panel.

Node ID String for Syslog Server Configuration

NIOS now provides options for defining the node ID string that identifies the appliance from which syslog messages are originated. This string appears in the header message of the syslog packet. You can choose whether to use the IP address and/or host name of the LAN1 port or MGMT port of the originating appliance, depending on whether the MGMT port is configured.

DHCP Fingerprint Updates

This release adds new DHCP fingerprints and updates existing ones. When you upgrade to NIOS 6.11.x, the appliance automatically updates DHCP fingerprints to reflect the new and updated ones. New fingerprints include AP Meraki, RHEL 6.4 or Centos 6.4, Iomega Backup Center, Samsung GT-S5690M (Galaxy Ruby), Kindle HD, and Samsung S5260 Start II. Updated fingerprints include Microsoft Windows Vista/7/Server 2008, Avaya IP Phone, Nortel IP Phone, D-Link Wireless Router, Quanta Microsystems Router, HP ProCurve Controller, RedHat/Fedora-based Linux, HP Printer, Kyocera Printer, RIM Blackberry, Samsung S8500, and Android Phone/Tablet (Generic).

NIOS 6.10.5

Next Available IP Enhancements

This release adds the following enhancements for the **Next Available IP** functionality:

- When multiple users simultaneously request for the next available IP address, only the user who first saves the configuration gets the IP address. Other users can request another IP address or enter a new one.
- To avoid IP address conflicts, the appliance validates the next available IP address to ensure that it is not used for other objects or associated with another operation, such as a scheduled task or an approval workflow.

NIOS 6.10.4

TR-800 Appliance and vNIOS Virtual Appliances for Reporting

This release adds support for the Trinzic 800 reporting appliance (TR-800 with 2 GB daily reporting limit) and the following vNIOS reporting virtual appliances: IB-VM-800 (with 1 GB or 2 GB daily reporting limit) and IB-VM-1400 (with 5 GB daily reporting limit). You can deploy the vNIOS virtual appliances as reporting servers in an Infoblox Grid. They are designed to run on VMware ESX or ESXi 4.1, 5.0, and 5.1 servers.

Pre-Provisioning Enhancements

The pre-provisioning feature now supports RPZs (Response Policy Zones) and FireEye integrated zones. It also enhances the hardware selection options in Grid Manager.

Microsoft Windows Server 2012 R2 Support

This release adds support for Microsoft Management and GSS-TSIG on Microsoft Windows Server 2012 R2.

F5 TMOS 11.4 Support

This release adds support for Global Load Balancers that run TMOS version 11.4.x.

NIOS 6.10.2

Auto-Provisioning NIOS Appliances

You can now set up a NIOS appliance using the auto-provisioning feature, which allows a DHCP server to automatically assign an IP address to the appliance. You can then configure and join the auto-provisioned appliance to the Grid.

Pre-Provisioning NIOS Appliances

Before joining a member to the Grid, you can enable provisional licenses and make necessary configurations on the offline member and associate DNS and DHCP data with the member prior to its deployment.

Support for NTP Anycast

When you configure DNS anycast on an appliance and use it as an NTP server, the appliance can answer NTP requests through the anycast IP address.

NIOS Support on HP Appliances

With valid licenses installed, HP Managed Services and Professional Services personnel can now install and configure Infoblox NIOS software on HP hardware, specified and certified by Infoblox.

NIOS 6.10.0

Infoblox Advanced DNS Protection

The Infoblox Advanced DNS solution employs hardware-accelerated security rules to detect, report upon, and stop DoS (Denial of Service), DDoS (Distributed Denial of Service) and other network attacks targeting DNS caching and authoritative applications. This feature helps minimize “false positives” and ensures that your mission-critical DNS services continue to function even when under attack. Advanced DNS Protection is designed to provide visibility and protection against network floods and DNS threats. It detects DNS attacks through predefined and custom threat protection rules, and mitigates DNS threats by dropping problematic packets while responding only to legitimate traffic. With valid licenses installed, you can subscribe to automatic rule updates that deliver near real-time protection against new and emerging attacks. You may also manually perform the rule update process based on your configuration. Advanced DNS Protection runs on Infoblox Advanced Appliances that support subscriber-facing DNS caching and external DNS authoritative applications. It supports both IPv4 and IPv6 and can be enabled on the Infoblox-4030 Rev-2 appliance and the following Infoblox Advanced Appliances: PT-1400, PT-2200 and PT-4000.

Infoblox Network Insight

Network Insight delivers network intelligence by integrating (in real-time) DNS, DHCP, and IPAM data with network infrastructure data, providing visibility across your entire network. The collection and correlation of this data enables network administrators to easily gather necessary information, analyze it, then take appropriate actions to better manage their networks, validate designs, effectively provision, troubleshoot and deliver network services. Network Insight improves decision making, reduces security and service interruption risk, and breaks down operational silos. Network Insight is supported on the following physical Infoblox appliances and vNIOS virtual appliances: ND-800, ND-1400, ND-2200, ND-4000, ND-VM-800, ND-VM-1400, ND-VM-2200, and ND-VM-4000.

FireEye Adapter for Infoblox DNS Firewall

Infoblox DNS firewall now provides a mechanism to further protect your network from malware and Advanced Persistent Threats through the integration of FireEye appliances. When your NIOS appliance is properly integrated with a FireEye appliance, it receives periodic alerts from the FireEye appliance when it identifies such threats. Based on your configuration, the NIOS appliance translates these alerts into RPZ rules that not only further protect your network from malicious attacks, but also aid in identifying clients that have been compromised.

Infoblox DNS Firewall Enhancements

This release supports the following DNS Firewall enhancements:

- New *Response Policy Zone (RPZ) Statistics* widget on the Dashboard
- New *DNS Top RPZ Hits* report
- New fields added to the Local RPZ Rulesets panel

Support for VLAN Tagging

You can now assign VLANs (Virtual Local Area Networks) to the LAN1, LAN2, and VIP (for HA pairs) interfaces on the appliance so the appliance can provide DNS service to different subnetworks on the same interface**.** You can set up VLANs on these interfaces to provide segmentation services to address issues such as scalability, security, and network management. This feature is currently supported on the following Infoblox appliances: Trinzic 2210, Trinzic 2220, and Infoblox-4010. For information about these appliances, refer to the respective installation guides on the Infoblox Support web site at https://support.infoblox.com.

Support for Disabling EDNS0

The NIOS appliance supports EDNS0 (Extension Mechanisms for DNS) by default. As defined in RFC 2671, EDNS0 provides extended UDP packet size that supports additional DNS functionality, such as DNSSEC. On occasions in which you have end servers that do not support EDNS0 and you want to ensure that they respond to recursive queries from the NIOS appliance while improving DNS performance, you can disable EDNS0 for the Grid and individual Grid members.
NOTE: When you disable EDNS0, all outgoing DNSSEC queries to zones within trusted anchors will fail even if DNSSEC validation is enabled.

Max Cache and Max Negative Cache TTL Configuration

For recursive DNS servers, you can now specify the maximum cache TTL value that establishes the time limit for the name server to cache positive responses, and the maximum negative cache TTL value that specifies the time limit for the name server to cache negative responses.

Global NAC Filters

You can now disable all NAC filters that specify authentication results from a remote, backend RADIUS server so you can perform maintenance on it. When you disable NAC filters for the Grid, the appliance bypasses evaluations of all NAC filters, and there are no configuration changes, service down times, or service restarts on the Grid.

DNS Top RPZ Hits by Client Report

This release adds the *DNS Top RPZ Hits by Client* report, which lists the total number of RPZ hits from a client during a specified time interval, irrespective of the rules and mitigation actions. You can view the IP address of the client, total RPZ hits, and the date and time during which the hits were received.

DHCP Enabled Host Address Permission

This release supports new admin permissions for IPv4 and IPv6 host addresses. Limited-access users now have the ability to create, modify, and delete IPv4 and IPv6 DHCP enabled host addresses in a specified network when granted read-write permission to IPv4 Host Address or IPv6 Host Address.

Support for Scheduled Local Backups

To avoid missing a backup when a remote server is unavailable during a scheduled automatic backup, you can now select to save a local copy of the backup on your appliance while backing up to the remote server.

Support for Link Local Address as the IPv6 Default Gateway

You can now define a link local address as the default IPv6 gateway and isolate the LAN segment so the local router can provide global addressing and access to the network and Internet. This is supported for both LAN1 and LAN2 interfaces as well as LAN1 and LAN2 in the failover mode.

Captive Portal Modifications

This release supports the following Captive Portal enhancements.

- Support for mobile browsers.
- Addition of detected devices in IPv4 filters.

Infoblox RESTful Web API

This release adds newly supported objects to the Infoblox RESTful Web API.

DHCP Fingerprint Enhancements

This release supports the following DHCP fingerprint enhancements.

- Support for IPv6 mobile devices and DHCP fingerprint configuration for IPv6.
- New reports to further identify top devices and device trends.
- Reporting on devices whose fingerprints have changed, which could indicate potential MAC spoofing attacks.
- A new status dashboard (Mobile Device Status) to track active leases of mobile devices.

NIOS 6.8.0

Access Control Using Named ACLs (Access Control Lists)

To effectively manage your core network services, you can grant legitimate hosts access to specific operations on the appliance using an ACL (access control list) or anonymous ACEs (access control entries). You can now configure a named ACL and apply it to multiple operations, such as file distribution and DNS zone transfers.

Inheritable Extensible Attributes

You can now enable the inheritance of extensible attributes. When you enable the inheritance of an extensible attribute, all descendants in the inheritance chain can inherit the attribute so you do not have to configure it at the object levels. For example, if you define an inheritable extensible attribute for a network, DHCP ranges and fixed addresses in the network can inherit the same attribute and its value. You can also define other options for inheritable extensible attributes. The appliance currently supports the Network View -> Network Container -> Network -> Range -> Host/Fixed Address/Reservation inheritance chain.

Multiple Status Dashboards

In addition to the default dashboard, you can now configure your own status dashboards to which you add widgets that help you manage core network services and data. Configuring multiple dashboards helps organize widgets in a meaningful way and improves dashboard and widget performance. This feature is especially useful when you have a Grid serving a large number of Grid members.

Additional Objects in Infoblox RESTful Web API

In this release, the RESTful Web API has been enhanced to support additional objects. For more information about the new objects, refer to the *Infoblox RESTful API Documentation*.

Implementing Quality of Service Using DSCP

You can implement DiffServ (Differentiated Services) on the appliance by configuring the DSCP (Differentiated Services Code Point) value. When you configure the DSCP value for DiffServ, the appliance sets priorities for all outgoing IP traffic. It implements QoS (quality of service) rules so you can effectively classify and manage your critical network traffic. To ensure that core network services, such as DNS services, continue to operate in the event of network traffic congestion, you can set the DSCP value for the entire Grid and override it at the member level.

Port Redundancy Support on IB-4030

This release adds port redundancy support for the Infoblox-4030 appliance. You can now configure the LAN2 port to be a redundant port for LAN1 on an Infoblox-4030 appliance to provide fault tolerance in your network. Port redundancy supports both IPv4 and IPv6 transports.

DNS Response Logging

In addition to DNS queries, you can also capture DNS responses in the syslog or export them in a capture file through the reporting server.

NOTE: Enabling the logging and capturing of DNS queries and responses at the same time will increase disk space usage. It will also adversely affect DNS services and system performance. Infoblox strongly recommends that you do not enable query and response logging at the same time, and that you constantly monitor the FTP or SCP server configured for capturing DNS query and response information from the reporting server to ensure that it has sufficient space.

Support for Recurring Discovery

When you configure a network discovery, you can now define a recurrence pattern that repeats on a regular basis. The appliance automatically starts the recurring discovery based on the configured schedule.

Restrictions on Recursive Deletions of Networks and Zones

You can now restrict recursive deletions of networks and zones to specific groups of users through the Infoblox GUI. Users who can perform recursive deletions are presented with the options of deleting a parent object only or deleting the parent object and all its child objects, when they delete a network container or DNS zone.

Notice and Consent Banner

You can now configure and publish a notice and consent banner as the first login screen that includes specific terms and conditions you want end users to accept before they log in to the Infoblox Grid. When you enable the notice and consent banner, users must accept the terms and conditions displayed on the consent screen before accessing the login screen of Grid Manager.

DNS Firewall Enhancements

This release supports the following Infoblox DNS firewall enhancements:

- Enhances DNS firewall to function in a multi-tiered recursion architecture.
- Improves reporting by reducing the indexing interval for RPZ events.
- Removes the ability to enable implicit pass-through logging.
- Improves syslog filtering to display RPZ events in the syslog.

10 Gigabit Ethernet Card Support on Infoblox Appliances

This release adds support for an optional 10 gigabit Ethernet card on the following Infoblox appliances: Trinzic 1400, Trinzic 2200, Infoblox-4010, Trinzic Reporting 1400, 2200, and 4000 appliances. Infoblox offers this factory-installed card option that accepts SFP+ modules for either 10 gigabit RJ-45 copper or 10 gigabit optical interfaces. For more information about this option, contact your Infoblox representatives.

NIOS 6.7.1

Network Deletion Enhancement

You can now select a specific group of users that are allowed to delete or schedule the deletion of a network container and its subnetworks. Depending on the configuration, users can choose to delete only the network container and re-parent its subnetworks, or delete the network container and all its subnetworks.

NIOS 6.7.0

DHCP Fingerprint Detection

The appliance now utilizes DHCP fingerprint detection to identify mobile devices, such as laptop computers and smart phones, on your network. You can use DHCP fingerprint detection to track devices on your network, block those that are not allowed (such as gaming consoles and home routers), and plan for future growth by accessing trending information such as the number of Apple iPhones versus that of Android phones.

Support for Internationalized Domain Names

Infoblox supports IDNs (Internationalized Domain Names) for DNS zones and resource records to provide the flexibility of specifying domain names in non-English characters. You can now enter zone and DNS record names in your native characters through the Infoblox GUI to deliver IDNs and other DNS data. IDNs are encoded in multi-byte Unicode and are decoded into ASCII strings using a standardized mechanism known as punycode transcription. The appliance automatically converts the data into punycode to support IDNs.

DNS Firewall and Reporting on Infoblox-4030 Appliances

In this release, you can enable Infoblox DNS Firewall on Infoblox-4030 appliances. You can use the DNS firewall feature to protect against bot/malware related threats, provide feedback about clients that attempt to connect to malicious domains, and reduce network and carrying cost associated with malicious traffic. You can also generate reports to monitor DNS performance and security concerns.

Support for Different Forwarding Rules per Grid Member

The appliance now supports different forwarding rules per Grid member. You can override the default forwarders for a forward-mapping zone at the member level and configure custom forwarders for each member. You can use this feature to forward regional queries of a forward-mapping zone to regional remote name servers.

Zone Transfer Enhancements

You can now configure the number of concurrent inbound and outbound zone transfers to optimize the zone transfer operation. You can also configure the number of concurrent queries a secondary name server sends to the primary server to optimize the query rate on the network.

Small Network Discovery

Infoblox expands network discovery to include /31 and /32 networks. For the appliance to discover addresses in these networks, the possible addresses can be used only as source addresses for point-to-point links.

Additional Objects in Infoblox RESTful Web API

In this release, the RESTful Web API has been enhanced to support additional objects. For more information about the new objects, refer to the *Infoblox WAPI Documentation*.

Microsoft Management Enhancement
This release adds Microsoft management support for Windows Server 2012.

NIOS 6.6.0

Support for RIR (Regional Internet Registry) Registration Updates

You can now configure the Grid to manage RIR allocated addresses and submit registration updates to the RIPE (Réseaux IP Européens) database. RIPE is one of the five RIRs in the world that manages the allocation and registration of Internet number resources for Europe, Russia, the Middle East, and Central Asia.

Infoblox DNS Firewall
Infoblox DNS Firewall uses DNS RPZ (Response Policy Zones), a technology developed by the ISC (Internet System Consortium) for allowing reputable sources to dynamically communicate reputation domain names so you can implement policy controls for DNS lookups. On an Infoblox appliance with an RPZ license installed, you can configure RPZ rulesets to block DNS resolutions for malicious or unauthorized domain names, or redirect clients to a walled garden by substituting responses. You can also configure a recursive Grid member to act as a lead secondary that receives RPZ updates from external reputation sources and redistributes the updates to other Grid members. Note that when you enable this feature, DNS performance will be affected.

Approval Workflows

You can now define approval workflows to control who in your organization can perform which mission critical tasks and whether and when the tasks require approvals before execution. In an approval workflow, you can add submitter and approver admin groups and define when and to whom email notifications are sent. You can also configure options such as whether submitters or approvers must enter a comment or a ticket number when they submit tasks for approvals.

Enhancements for Scheduling Full Upgrades
Infoblox enhances the NIOS upgrade process by enabling dynamic provisioning of many DNS, DHCP, and IPAM parameters during the upgrade. When you schedule a full upgrade from NIOS 6.6.0 to a later release, the Grid Master immediately replicates most DNS and DHCP data and operations to all Grid members, even when the members have not been upgraded.

Infoblox RESTful Web API
Infoblox now offers a new interface to NIOS based on REST (REpresentational State Transfer), also called a RESTful web API. The RESTful API does not require any Infoblox client software. It enables clients (without making changes) to automatically work with future NIOS releases. The RESTful API uses HTTP methods for operations and supports input and output in JSON and XML, and it uses HTTPS (HTTP over SSL/TLS) as the transport mechanism. The server certificate used for the RESTful API is the same certificate used by NIOS for the GUI and PAPI. This version of RESTful API supports objects commonly used in daily NIOS operations.

Support for LDAP Administrator and Captive Portal Authentication
You can now configure NIOS to authenticate administrators and Captive Portal users against LDAP (Lightweight Directory Access Protocol) servers, in addition to RADIUS servers, TACACS+, and AD domain controllers. When used by the Captive Portal, LDAP fields are automatically mapped to Extensible Attributes to enhance MAC filter management.

Load Balancer Synchronization Groups
Infoblox now supports dynamic grouping of load balancers that are in the same synchronization group. With this feature, you can avoid creating multiple copies of the same configuration records of load balancers. The Infoblox Load Balancer Manager enables the Grid to manage Global Load Balancers (GLBs), load balancer synchronization groups, and their associated objects and data. The appliance synchronizes data with every

member of a synchronization group and manages GLBs independently if they are not part of a synchronization group.

Infoblox Reporting Solution Enhancements

This NIOS release supports the following enhancements to the reporting solution:

- Enhances the DNS query capturing feature by introducing exclusion lists. This enhancement allows users to capture all DNS queries while excluding queries for certain domains.
- Supports the configuration of IP block groups so users can generate DNS query trends by IP block groups.
- Adds the capability to view reporting volume sent by each member.

This release provides the following new report: DNS Query Trend Per IP Block Group Report.

Specifying TTL Settings for Lame Servers

You can now specify the TTL (Time to Live) value the appliance uses to cache a lame delegation or lame server. Lame TTL indicates the amount of time a name server remembers information about a remote name server that is not authoritative for a zone.

Ignoring DHCP Client ID

You can now configure the appliance to ignore the UID (unique client identifier) of a DHCP client when it requests a new lease to ensure that the client receives the same IP address irrespective of its UID. When you enable this feature and a DHCP client requests a lease, the appliance identifies the DHCP client and allocates the same IP address based on the client's physical MAC address, not its UID.

Support for Multiple Interfaces on the Same Network on Infoblox-4030

You can now configure LAN1, LAN2 and MGMT interfaces on the same IPv4 or IPv6 subnet on the IB-4030. You can provide the same netmask for IPv4, or a CIDR prefix for IPv6, as the LAN1 interface. Alternatively, you can use a /32 netmask (255.255.255.255) for IPv4, or /128 CIDR prefix for IPv6 with the same subnet as LAN1 interface to configure multiple interfaces. The IB-4030 can replace three DNS cache servers that are active on the same network.

NIOS 6.5.0

Global Load Balancer (GLB) Integration

You can now configure the Grid to integrate with the F5 Global Traffic Manager (GTM) as a global load balancer solution that provides load-balancing services between multiple data centers. The Infoblox Load Balancer Manager enables the Infoblox Grid to manage F5 GTMs and their associated objects and data. The Infoblox GLB integration solution provides the following:

- An easy-to-use and centralized interface (Grid Manager) for managing GLBs and GLB-related objects
- Configuration of Load Balanced Domain Name (LBDN) and other supported objects with the Infoblox DNS service
- Extension of the current permission models to support the newly added F5 GLB objects and the flexibility in delegating tasks to different admins
- Associating Extensible Attribute meta data with GLB-related objects to enable Smart Folders, search and filters in Grid Manager

Note: If you have configured multiple GTMs in a single GTM sync group, Infoblox recommends that you add only one GTM from the sync group for synchronization with the NIOS appliance.

Disconnected Grid

Multi-Grid Manager administrators can now manage a larger number of Grids using the concept of attach and detach. Grid(s) that are detached from the Multi-Grid Master remain operational. When a Grid attaches or detaches, a snapshot of the Grid's current state is taken and stored on an external FTP server. These snapshots can be used for resetting the Grid to a known state on failure and can also be saved as a template for creating multiple Grids of the same DNS, DHCP and IPAM configuration. Additional new tools include:

- External FTP Storage Manager: For configuring the monitoring of the FTP storage space

- Snapshot Manager: For viewing the list of available snapshots to clone, create a template or reset the Grid
- Template Manager: Lists available templates to apply or delete
- Delta Viewer: For viewing all administrator changes performed between two snapshots
- Grid Connection Dashboard Widget: Displays the current state of each Grid

Grid Master Candidate Promotion Enhancement
The CLI command *set promote_master* has an option to force sequential notification to its Grid members to join the new Grid Master. You can also provide the wait time for each Grid member.

IB-4030 IPV6 Enhancements
This release enables administrators to process IPv6 traffic in non-accelerated mode over single LAN1, LAN2 and MGMT ports. It also supports DNS64 for queries over IPv6 transport in non-accelerated mode and queries over IPv4 transport in accelerated mode. This release provides IB-4030 DNS cache dump to support download and export the DNS cache on the acceleration NIC card.

- Anycast v6 NIOS appliances can be configured to advertise routing information of the IPv6 Anycast addresses through OSPF v3 and/or BGP v6 Protocols
- Support for querying CHR and QPS values via SNMP

CSV Import Enhancements
This release allows limited-access users to perform CSV imports based on their permissions. In addition, administrators can use the *Import Job Manager* wizard to perform CSV imports, manage import jobs and view import status. When multiple users initiate CSV imports simultaneously, the jobs will be queued and are processed in the order they are received. Each user is allowed to have only one import job at a time. Users can view their own job in the queue and are allowed to cancel it if it is not executed already. Superusers can view all pending jobs.

UI Security Level Banner
You can now publish a security banner that indicates the security level of the Infoblox Grid. There are five levels to choose from, beginning with **Top Secret**.

UI Informational Level Banner
The informational banner has multiple uses, such as for indicating whether the Infoblox Grid is in production or a lab system. The banner can also be used for issuing messages of the day.

Wide Area Bonjour Support
You can now add PTR records to forward mapping zones to support zero configuration Networking (zeroconf), such as wide-area Bonjour.

One Lease per Client
Grid member running DHCP can now assign only one IP address to each DHCP client. The DHCP server will terminate existing leases associated with the client when it assigns a new address.

Infoblox Reporting Solution Enhancements
This release includes the Alerting and Capture DNS Queries features. The Alerting feature allows administrators to define conditions on summary and detail searches. The user configured alert actions (email, syslog, SNMP trap) are triggered when events satisfy these conditions. The Capture DNS Queries feature allows administrators to define a list of domain names. Infoblox appliances capture queries related to the domain names and sub domain names into log files in syslog format and move compressed log files to customer configured FTP/SCP servers. Following are the new reports:

- DNS Top NXDOMAIN / NOERROR (no data) Report
- DNS Top SERVFAIL Errors Received Report
- DNS Top SERVFAIL Errors Sent Report

- DNS Top Timed-Out Recursive Queries Report
- DNS Top Clients Per Domain Report

NIOS 6.4.0

Two-Factor Authentication

Infoblox now provides two-Factor authentication for administrators. The current Microsoft AD, RADIUS, TACACS+ and local administrator authentication is enhanced to also support X.509 client certificates embedded in smart cards, such as the US Dept. of Defense Common Access Card. Two-factor authentication functionalities include:

- Certificate validation by the Certificate Authority (CA)
- Certificate status validation by Online Certificate Status Protocol (OCSP) Responder
- Support for Direct and Delegated trust models

Scheduling Full Upgrades

Infoblox enhances the NIOS upgrade process by enabling dynamic provisioning of many DNS parameters during the upgrade. When you schedule a full upgrade from NIOS 6.4.0 to a later release, NIOS supports the following enhancements:

- DNS record and host management during a Grid upgrade
- Single member upgrade and revert

Lights Out Management (LOM)

NIOS 6.4 adds support for Lights Out Management (LOM) on the following platforms: Trinzic 800, 1400, 2200 and 4000 series. LOM provides system administrators with the ability to monitor and manage servers remotely. LOM allows the administrators to configure and enable the IPMI 2.0 standards compliant implementation and control the main NIOS system through this dedicated remote management system and network port. LOM features include reboot and power up/down of NIOS, as well as Serial Over LAN (SOL) access to the NIOS serial console.

File Distribution for VoIP and Virtualization

The following File distribution enhancements are designed to better support VoIP and Virtualization environments:

- The Grid capacity for file distribution has been increased to 10GB for all Infoblox physical appliances, excluding vNIOS virtual appliances.
- TFTP, HTTP and FTP uploads to Grid members are now supported. Files uploaded are synchronized to all other members that offer File Distribution services through the Grid Master.
- Named FTP accounts can now be defined to allow for control of who can upload or download specific files. Anonymous FTP is still supported.
- Multiple files can be uploaded simultaneously either by selecting them individually or by uploading a zip or tar file that is extracted automatically on upload.
- Virtual root folders can be defined for TFTP. This allows different files to be made available to clients based on the client network address by configuring specific folders on the Grid as the ‘root’ folder for that client.

Infoblox Reporting Solution Enhancements

The following new reports have been added to the reporting solution:

- DNS Resource Records Last Queried
- DNS Zones Last Queried
- DNS Statistics per Zone
- DNS Daily Query Rate by Server
- DNS Daily Peak Hour Query Rate by Server

New filters have been added to allow users to view IPAM data associated with Microsoft Servers.

IPv6 on Management Interfaces

The following services and functions are now available over IPv6 transport protocol.

- DNS over IPv6 LAN1/LAN2/MGMT interfaces
- DHCP over IPv6 LAN1/LAN2 interfaces
- IPv6 address on Loopback interface
- CLI (SSH) access over IPv6
- GUI access over IPv6
- PAPI access over IPv6
- Sending SNMP traps over IPv6
- SNMP query over IPv6
- Sending messages to external syslog servers over IPv6
- Email relay over IPv6
- IPv6 Static routes

IPv6 Anycast

NIOS appliances can now be configured to advertise routing information of the IPv6 Anycast addresses through OSPF v3 and/or BGP v6 Protocols.

DHCP Ping Timeout Enhancement

NIOS 6.4 adds the option to set the DHCP Ping timeout in sub-second values.

DDNS Hostname Rewrite Policy

This release includes a feature that replaces characters in DNS host names that are not compatible with certain non-Infoblox DNS servers when those servers are secondary to Infoblox primary servers. You can create a hostname rewrite policy in which you define valid characters in a host name, and a replacement character that NIOS uses to replace incompatible characters. When you enable this policy, NIOS keeps the valid characters in the host name and automatically replaces invalid characters with the replacement character that you define in the policy.

NTP Engine Update

Infoblox is updating the underlying NTP protocol engine to keep current and prepare for future NTP enhancements. There are no customer visible features related to this update.

Customer Experience Improvement Program (Phone Home Enhancement)

Infoblox appliances now prompt users to participate in the Infoblox customer experience improvement program in both the initial Setup Wizard and End User License Agreement (EULA). This optional program allows customer to provide Infoblox with feedback on how the product is used. Infoblox encourages customers to enable this feature so Infoblox can provide future enhancements to the product that match customer needs.

NIOS 6.3.6

Reverse-Mapping Zones with Leading Zero Octets

In this release, the appliance supports the creation of reverse-mapping zones for networks that contain leading zero octets.

NIOS 6.3.5

Infoblox Trinzic DDI Appliances

NIOS 6.3.5 supports the new Trinzic 810, 820, 1410, 1420, 2210, and 2220 appliances. For more information about all Infoblox appliances, refer to the Infoblox web site at: http://www.infoblox.com/en/products/infoblox-appliances.html.

NIOS 6.3.3

API: Grid Upgrades
The Infoblox API now provides methods for managing the Grid upgrade process. For more information, refer to the *Infoblox API Documentation*.

NIOS 6.3.0

Task Automation
Infoblox supports a few new features that automate the management of core network services (DNS, DHCP, and IPAM). You can now select the Tasks Dashboard or Status Dashboard as your home page when you log in to Grid Manager. The Tasks Dashboard provides easy access to commonly performed IPAM tasks, such as adding networks and host records. Tasks are grouped by task packs. 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. You can now add networks, host records, fixed addresses as well as the CNAME record, TXT record, and MX record through the Tasks Dashboard.

Dashboard Templates and Tasks Dashboard Only Restriction
As part of the Task Automation features, superusers can now specify the tasks that 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.

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.
- Bare Metal Provisioning: This task is triggered by the network infrastructure discovery service within the Trinzic Automation Engine. Provisioning templates and parameters and configured to allow specific network configuration for new network infrastructure devices.

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.

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.

Trinzic Reporting
Infoblox provides tools that support reporting of core network services in an Infoblox Grid. You can now add any of the Trinzic Reporting platforms 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 organization's needs.

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.

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.

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.

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.

Scheduling Full Upgrades
You can now schedule a full upgrade, which allows for member-to-Master data replication, from NIOS 5.1r5-3, 5.1r5-4, 5.1r5-5, 5.1r5-6 to NIOS 6.3.0. 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.

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.

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.

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.

LAN2 Failover in HA

This NIOS release supports NIC redundancy between LAN1 and LAN2 for HA configurations.

Grid/System Manager and API Enhancements

This release introduces a number of enhancements to Grid/System Manager and the API.

Grid/System Manager

- You can now scroll through the list of global smart folders. In earlier releases, NIOS displayed the first 20 folders and you could not scroll through the list.
- When you delete a delegation that is a parent zone, you now have the option to delete the parent zone only or to delete its subzones as well.
- The Type filter in the Zones panel now allows users to select the 'does not equal' operator.
- The "Server Address" column was added to the "DNS Updates to External Zones" section of the Configure DDNS wizard.

API

- There is an API call to retrieve all CNAMEs based on the canonical name.

NIOS 6.2.3

DNS Optimization and Network Tuning

Infoblox now provides a CLI command for tuning the BIND receive socket buffer memory to a maximum of 8 MB. You can use the `set named_recv_sock_buf_size` command to adjust the BIND receive socket buffer size for occasional DNS burst traffic and high volume DNS recursive queries. For more information about this feature, refer to the *Infoblox CLI Guide*.

SNMP Trap for CPU Usage

This release includes a new CLI command, `set thresholdtrap`, which you can use to enable the SNMP trap for CPU usage and to configure the trigger and reset values of the trap. When CPU usage of your appliance exceeds the trigger value or dips below the reset value, it sends an SNMP trap about the event. For more information about this command, refer to the *Infoblox CLI Guide*. For information about Infoblox SNMP traps, refer to the *Infoblox NIOS Administrator Guide*.

Global DNS Statistics

You can now retrieve global statistics for the DNS server by querying ibZoneStatisticsTable and ibZonePlusViewStatisticsTable in the Infoblox ibDNSOne MIB. These SNMP tables contain DNS statistics of all zones in the default and user-defined views. The “summary” zone in ibZoneStatisticsTable contains global DNS statistics of all zones in all views. You can use the information in these tables to calculate the total number of recursive queries.

Download the DNS Statistics File

Through the Infoblox API, you can now specify the new “dnsStats” type in the export_data ( ) method to download the DNS statistics file from a specific member. Note that the performance of the DNS service may be affected if you download the DNS statistics file frequently. For information about this method, refer to the *Infoblox API Documentation*.

NIOS 6.2.2

Microsoft Management Enhancements

This release includes enhancements to the management of Microsoft DNS and DHCP servers:

- NIOS now supports Microsoft 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. You can synchronize split-scopes from Microsoft servers to the Grid and configure split-scopes from Grid Manager as well.
- NIOS now supports synchronizing scopes assigned to more than two Microsoft servers.
- You can now edit DHCP options synchronized from Microsoft servers. You can do so from the IPv4 DHCP Options tab of the DHCP Range Editor, Fixed Address editor and Microsoft Server DHCP Properties editors.
- 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. NIOS now support synchronizing these delegations from Microsoft servers.

NIOS 6.2.1

Sort List for DNS Views

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. Starting with this release, NIOS supports configuring sort lists for DNS views, as well as for Grids and members.

NIOS 6.2.0

Multi-Grid Management

Infoblox now provides centralized management of multiple Grids. You can now configure a Master Grid from which you can manage and monitor up to 50 individual Grids. For example, you can create multiple Grids by region or functional group, and then control them from the Multi-Grid Manager. The Multi-Grid Manager also provides visibility into your entire IP address space, enabling you to assign IPv4 and IPv6 networks or blocks of networks. You can also monitor the member and service status of the managed Grids. The Grids regularly synchronize their data with the Multi-Grid Manager, ensuring updates in real time.

This feature requires a Multi-Grid Management license. For more information, refer to the *Infoblox Multi-Grid Manager Administrator Guide*.

IB-4010

The IB-4010 is a high performance network appliance that provides core network services, including DNS (Domain Name System) caching and authoritative services, and IPAM (IP Address Management). The integrated Infoblox approach combines the simplicity of appliances with the power of advanced distributed database technology to control and automate network services, while achieving availability, manageability, visibility, and control unmatched by conventional solutions based on legacy technologies. You configure and manage the IB-4010 through an easy-to-use Infoblox GUI that works seamlessly in Windows, Linux, and Mac environments using standard web browsers. For more information, refer to the *Infoblox-4010 Installation Guide*.

Advanced DHCP Option Logic

To further control how the NIOS appliance allocates IPv4 addresses, you can now configure Logic Filter and Class Filter lists so the appliance can determine the class statement it writes to the dhcpd configuration file, when to grant or deny a lease to the matching client, and which DHCP options to return to the matching client. You can also create complex match rules that use the AND and OR logic to further define filter criteria in option and NAC filters. The appliance provides an expression builder that automatically builds the rules after you define them.

IF-MAP Client Enhancements for DHCP Servers

When you configure an Infoblox DHCP server as an IF-MAP client, you can now configure the client to publish ip-mac and ipv6-duid metadata for specific leases. You can also define how the IF-MAP server handles the existing ip-mac and ipv6-duid information before the client sends the next update. For example, you can specify the IF-MAP server to always delete existing ip-mac and ipv6-duid information before the next update. With these enhancements, you can also view IF-MAP connection status of an IF-MAP client, create smart folders using the IF-MAP enabled client as a filter criterion, and validate the IF-MAP server certificate.

TACACS+ AAA

You can now configure NIOS to authenticate admins against TACACS+ (Terminal Access Controller Access-Control System Plus) servers, in addition to RADIUS servers and AD domain controllers. TACACS+ provides separate authentication, authorization, and accounting services.

Thales HSM Support

You can integrate a Grid with third-party, network-attached Thales 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.

Forwarders for DNS Views

In addition to defining DNS forwarders for the entire Grid and for each Grid member, you can now define forwarders for each DNS view. So if you defined a DNS view for different user groups or regions, you can define a different set of forwarders for each DNS view.

Match Destination Views

You can now define a Match Destinations list that identifies destination addresses and TSIG keys that are allowed access to a DNS view. The NIOS appliance can determine which hosts can access a DNS view by matching the destination IP address or TSIG key with its Match Destinations list.

RFC 2317 Exclusion

The Add Delegation wizard now provides an option for performing “strict delegation” while delegating RFC 2317. This allows users to create labels corresponding to IP addresses in the delegated address space in the parent zone.

NIOS 6.1.0

DHCPv6

Due to the exhaustion of IPv4 address space and the resulting demand for IPv6, Infoblox DHCP servers now support DHCP for IPv6 as well as IPv4. You can configure and manage IPv6 networks, ranges, fixed addresses, leases and hosts. You can also view and monitor DHCP IPv6 and IPv4 data.

DNS64

To support an increasing number of IPv6 only devices, Infoblox DNS servers now support DNS64, a mechanism that synthesizes AAAA records from A records when no AAAA record exists. Together with a NAT64 server, DNS64-enabled servers allow IPv6 only nodes to communicate with only IPv4 nodes without any changes to either of the devices.

RRset Order Support

You can now configure the order that the appliance uses to return resource records of a host through the Infoblox GUI. This feature is useful when you want the appliance to return resource records of a host in a specific order. For example, if you want a management address to appear first in a list of multiple IP addresses that are associated with a router, you can configure the order of the IP addresses so the management address is always returned first on the list. When you enable this feature and there are multiple IP addresses associated with a host, you can specify one of the following RRset orders: Fixed, Random, and Cyclic.

Synchronization with Microsoft Servers

With this release, there is an option to create a Microsoft user account that does not require Administrator Group rights to synchronize Microsoft servers.

IPv6 Support for NIC Redundancy

This release supports both IPv4 and IPv6 addresses for NIC (Network Interface Controller) redundancy using the LAN2 port.

SNMPv3 Support

The NIOS appliance now supports USM (User-based Security Model) in SNMPv3 for the authentication, encryption, and decryption of SNMP data. SNMPv3 adds security and remote configuration enhancements to SNMPv1 and SNMPv2c. You can configure SNMPv3 users on the appliance to enable secure 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.

Setting SNMP System Information for HA Members

You can now assign a unique SNMP sysName for node 1 and node 2 of an HA Grid member pair.

SNMP Test

There are now two options for testing your provisioning of SNMP. The first is a test button available in the Grid toolbar. This can be used to test your community string settings (SNMPv1 and SNMPv2c) as well as SNMPv3 access, privacy and encryption settings. The second is the ability to generate any available trap and payload via the command line. This is very useful for testing SNMP management and root cause analysis solutions.

Quick Filters

You can now save filter criteria that you define in a specific panel as a quick filter. You can reuse the quick filter to find updated information in a panel without redefining the filter criteria each time you log in to the appliance. You can create up to 10 global and 10 local quick filters in each panel that supports filters. The NIOS appliance supports three types of quick filters: system, global, and local.

Third-Party URL Links
In the Finder panel, you can add the URL links of frequently used third-party portals and destination pages in the URL Links section. 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 the section. Superusers can save links globally so they are available to all users. Nonsuperusers can save their own set of links.

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.

License Transfer for vNIOS for VMware
With this release, you can transfer the valid licenses of a vNIOS virtual appliance from one ESX/ESXi 4.1, 5.0 or 5.1 server to another without going through the RMA (returned materials authorization) process. For more information, refer to the *Infoblox Installation Guide for vNIOS Software on VMware*.

New Platforms for vNIOS on ESX/ESXi Servers
Infoblox now supports the following additional vNIOS for VMware appliances on ESX/ESXi servers: IB-VM-550 and IB-VM-1850. For information about the new platforms, refer to the *Infoblox Installation Guide for vNIOS Software on VMware*.

vNIOS for VMware on Cisco UCS Express/SRE-V
You can now install the vNIOS for VMware software on Cisco SRE-V, which is part of the Cisco UCS Express. Infoblox supports the following vNIOS for VMware virtual appliances on Cisco SRE-V: IB-BOB, IB-VM-250, IB-VM-550, and IB-VM-1050. For more information about the supported virtual appliances, see the section **Supported Platforms** on page 2. For information about Cisco SRE-V, refer to the Cisco documentation.

Support for Google Chrome Frame Plug-in
This release includes support for the Google Chrome Frame™ plug-in for Internet Explorer. To enhance performance on Internet Explorer 7.x and 8.x browsers, Infoblox recommends that you install the Google Chrome Frame plug-in. For additional information, refer to the Knowledgebase Article 15953 on the Infoblox Support website at http://support.infoblox.com.

NIOS 6.0.0

NXDOMAIN

You can configure a recursive DNS member to send a synthesized DNS response with predefined IP addresses to the DNS client, in place of the NXDOMAIN response. In addition, you can create rules that specify how a DNS member responds to queries for A records of certain domain names, not just non-existent domain names.

Blacklist
Your organization can prevent customers or employees from accessing certain Internet resources, particularly web sites, by prohibiting a recursive DNS member from resolving queries for domain names that you specify. You can configure a recursive DNS member to redirect the DNS client to predefined IP addresses or return a REFUSED response code (indicating that resolution is not performed because of local policy), depending on the domain name.

Lease Scavenging

You can enable member DHCP servers to automatically delete free and backup leases that remain in the database beyond a specified period of time. When you enable this feature, the appliance permanently deletes the free and backup leases, and you can no longer view or retrieve the lease information.

BGP Anycast Support

In addition to OSPF (Open Shortest Path First), the appliance now supports BGP (Border Gateway Protocol) as the routing protocol for DNS anycast advertising. You can configure BGP, OSPF, or both as the anycast addressing protocol on the loopback interface of the appliance.

Bulk Changes through CSV Import

Infoblox now provides a feature that allows you to make bulk changes to DNS, DHCP, and IPAM data in NIOS from CSV files. You can import new data, update existing data, or overwrite existing data in bulk. For example, you can export data to a CSV file, update the file, and then import the modified data back into NIOS. You can access the *Import Manager* editor from the **Data Management** tab of Grid Manager. For information about format specifications and sample data files, refer to the *Infoblox CSV Import Reference*.

bloxTools on Grid Members

NIOS 6.0.0 no longer supports running the bloxTools environment on a Grid Master, a Grid Master candidate, or a vNIOS virtual appliance for Riverbed or VMware. You can now run the bloxTools environment on an independent appliance or a Grid member. In a Grid, you can run the bloxTools service on one Grid member only. You can also move the bloxTools service from one member to another. After an upgrade, running the bloxTools service on the Grid Master is allowed only to facilitate the transition of the bloxTools service to a Grid member. Infoblox strongly recommends that you move the bloxTools service to a Grid member as soon as possible. For more information, refer to KB article 17199.

Synchronization with Microsoft Servers

With this release, there is an option to create a user account that does not require Administrator Group rights to synchronize Microsoft servers.

Change to Software Versioning

Starting with NIOS 6.0.0, Infoblox uses a new software versioning scheme. Infoblox now uses “x.y.z” instead of “x.yrz” to represent the major release, minor release, and patch number of a software release. For example, this release is NIOS 6.3.5 and a previous release was NIOS 5.1r3.

CHANGES TO DEFAULT BEHAVIOR

This section lists the changes to default behavior in each NIOS 6.x release.

NIOS 6.11.x

- API: The following changes for keytabs have been made in the Infoblox API:
  - `remove_data/keytab` has been removed
  - `import_data/keytab` has been removed
  - `import_data/upload_keytab` has been added

  This release also supports multiple TSIG keys. To use a keytab, you must now upload it and manually assign it to individual members or to DHCP; you cannot complete this task in one operation. If you have only one keytab, you can still use the `old gss_tsig` members. However, Infoblox recommends that you switch to the new `gss_tsig_keys/ipv6_gss_tsig_keys` members.

API: The following objects have been deprecated:

- `Infoblox::Grid::MSServer::DNS` (new object: `Infoblox::Grid::MSServer::ServerDNS`)
- `status_last_updated member` in `Infoblox::Grid::MSServer::DNS` (new object: `status_last_updated_ts member` in epoc format)

Though the deprecated objects will continue to function for backward compatibility purposes, Infoblox recommends that you use the new objects in your new code.

- Reporting: The "Domain Name" and "Mitigation Action" filters are no longer supported in the *Top RPZ Hits by Client* report.

NIOS 6.10.4

- In previous releases, the appliance added grace period to the KSK (Key Signing Key) and ZSK (Zone Signing Key) rollover periods. In this release, the rollover periods for a particular zone start as soon as it is signed.
- In previous releases, you could assign read-only permission for hosts in a network to restrict admins to only viewing hosts in the specified network. In this release, assigning read-only permission for hosts in a network does not affect the visibility of hosts in the specified network.

NIOS 6.10.2

- For Network Insight, enabling discovery for an IPv4 network or DHCP range is no longer required if a seed router has not been configured, as long as the "Disable discovery for networks in IPAM" option is not selected in the **Advanced Settings** tab of the *Grid Discovery Properties* editor. A seed router is still required for enabling discovery IPv6 networks or DHCP ranges.

NIOS 6.8.0

- In this release, DNS responses and DNS queries are stored in the same file. To reflect this implementation, the file name `reporting-query-[nnnnnn]` has been changed to `capture-dns-[nnnnnn]`, where `[nnnnnn]` represents the timestamp when the file is created. The file continues to reside in the `/storage/reporting-capture-date/` folder. To avoid backward compatibility issues, ensure that you update your scripts to handle both file naming conventions.

NIOS 6.7.0

- The Infoblox::Grid::Admin::User object password method and the Infoblox::Grid object secret method have been modified to adhere to Infoblox security policies.
- In this release, when you create a new host record or reorder an existing one, the default cyclic ordering for RRset order is reversed compared to previous releases.
- API and RESTful API: After upgrading to NIOS 6.7.x, all international domain names (IDNs) in punycode are converted to Unicode (in the respective API way of encoding Unicode strings). You can use the dns_[…] fields in relevant objects to retrieve read-only IDNs in punycode. For more information about IDNs, refer to the *Infoblox NIOS Administrator Guide*. For information about API and RESTful API, refer to the *Infoblox API Documentation* and *Infoblox RESTful API Documentation*.

NIOS 6.6.9

- In all selector dialogs, the **Go To** field has been changed to **Find**, which is similar to the filtering function that allows you to quickly locate specific objects.

- In Global Search, a new check box is added for including or excluding extensible attributes in the search.

NIOS 6.6.0

- The default UDP socket buffer size has been increased from 109 KB to 1.5 MB.

NIOS 6.5.4

- In this release, a permission change made in NIOS 6.4.6 has been reverted. Specifically, users with read/write permission to create a host record can now add fixed addresses (by enabling DHCP) to the host without specific permissions for fixed addresses. Host permission is considered inclusive of fixed address permission in this context.

NIOS 6.5.0

- Changed the OIDs of "ibMemberNode1ServiceStatus" and "ibMemberNode2ServiceStatus" to "ibMemberNodeServiceStatus" and "ibMemberPassiveNodeServiceStatus."

NIOS 6.3.0

- Changed IB-TRAPONE-MIB to IB-TRAP_MIB, and removed the trailing zeros in the OIDs of the objects in the IB-TRAP MIB. The MIB objects and OIDs are as follows:

OID	Object
1.3.6.1.4.1.7779.3.1.1.1.1.1	ibEquipmentFailureTrap
1.3.6.1.4.1.7779.3.1.1.1.1.2	ibProcessingFailureTrap
1.3.6.1.4.1.7779.3.1.1.1.1.3	ibThresholdCrossingEvent
1.3.6.1.4.1.7779.3.1.1.1.1.4	ibStateChangeEvent
1.3.6.1.4.1.7779.3.1.1.1.1.5	ibProcStartStopTrap
1.3.6.1.4.1.7779.3.1.1.1.1.6	ibRevokedLicenseTrap

Infoblox recommends that you upload the latest MIBs.

NIOS 6.1.0

- In earlier releases, the DNS service automatically started when you installed a DNS license on an appliance. Starting with this release, you will need to start the DNS service manually after you install the license. You can check the status of an appliance's services, by navigating to the Grid -> Grid Manager or System -> System Manager tab.
- 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.

NIOS 6.0.0

- In previous releases, when you defined Group By rules in a smart folder to group filtered data by extensible attributes, Grid Manager included objects that did not contain attribute values in the results table. In this release, the appliance excludes objects that do not contain attribute values. When you choose to include these objects, the appliance may take longer to process the results. If you upgrade from a previous release, Grid Manager continues to include objects that do not contain attribute values when you define Group By rules. You can configure the smart folder exclude these objects by clearing the **Include objects with no values for the Group By attributes** check box to achieve better performance.

- In previous releases, you could add or edit associated zones assigned to shared record groups in the *Shared Record Group* editor of Grid Manager. In this release, you can drill down from the **Data Management** tab -> **DNS** tab -> **Shared Record Groups** tab -> *shared_record_group* -> **Associated Zones** tab to add and edit associated zones.
- In previous releases, if you enabled DDNS updates, the DNS server accepted DDNS updates from a DHCP client even if the server was not allowed to receive DNS queries from that client. In this release, the DNS server no longer accepts DDNS updates from such DHCP clients. In addition, the DDNS tab of the Network, Address Range Fixed Address, Roaming Host and DHCP Template editors now displays a message informing users that they must click Override and select Enable DDNS Updates for DDNS settings to take effect at the specific level.

UPGRADE GUIDELINES

This section lists the guidelines for upgrading to NIOS 6.11.x. It includes general guidelines for upgrading to any NIOS 6.x release. Note that upgrading from NIOS 5.x is not supported.

Upgrading to NIOS 6.11.x

- Infoblox Advanced DNS Protection: Before upgrading to NIOS 6.11.x, ensure that you have less than 500 custom rules for each rule template. Otherwise, the upgrade may fail.
- After upgrading to NIOS 6.11.x from an earlier release, a legacy ruleset generated for Infoblox Advanced DNS Protection will have a "-0" prefix.
- When upgrading to NIOS 6.11.x, the following limitations apply to DNSSEC if you schedule a full upgrade:
    - You cannot configure new settings that are added to the authoritative zone object while the upgrade is still in progress. This restriction is not applicable to future upgrades.
    - You can sign or unsign an authoritative zone only if the Grid Master Candidate and the associated serving members are upgraded. This restriction is not applicable to future upgrades.
    - An authoritative zone can have its KSK rollover only if the Grid Master Candidate and all the serving members are upgraded to NIOS 6.11.0. This restriction is not applicable to future upgrades.
    - An authoritative zone can have its ZSK rollover by the daemon only if the Grid Master Candidate and all the serving members are upgraded to NIOS 6.11.0. This restriction is not applicable to future upgrades.
    - You cannot delete keys while the upgrade is still in progress.
    - You cannot update DNSSEC related parameters at the member level while the upgrade is still in progress. Example: rollover mechanism, NSEC3 salt length and iterations, and enable or disable automatic KSK rollover.
- Before you upgrade to NIOS 6.11.x, the bloxTools environment provides Perl version 5.10. When you upgrade to NIOS 6.11.x, Perl modules have been upgraded to version 5.14, which may affect the existing bloxTools Perl scripts due to additions, modifications, and deletions of some Perl modules.
- NIOS upgrade will not be restricted and no warning messages will be displayed, even if you have configured multiple interfaces on the same network with either /32 or /128 netmasks, which are not supported. Infoblox recommends that you change these unsupported netmasks to valid ones (non /32 or /128) after the upgrade.

Upgrading to NIOS 6.10.x

- When you upgrade from NIOS 5.1r6-12 or earlier releases, the **Try Snapinstall** option may not be available in the bloxTools environment after the upgrade. To work around this issue, stop bloxTools service on the member, console connect to the member through the CLI and execute the `set bloxtools reset all` command. Once the reset process is complete, restart the bloxTools service to access the **Try Snapinstall** option.

Upgrading to NIOS 6.8.x

- When you upgrade from NIOS 6.6.x or earlier releases, the email address in the SOA resource record that was entered in punycode will be converted into IDN (Internationalized Domain Name) after the upgrade. You can convert the IDN back to punycode using the IDN converter utility through Grid Manager. For information about IDN, refer to the *"Infoblox Grid Manager"* chapter in the *Infoblox NIOS Administrator Guide*.

Upgrading to NIOS 6.7.x

- When you schedule a full upgrade from an earlier NIOS release to NIOS 6.7.x, the following applies until the entire Grid has been upgraded:
  - DHCP fingerprint detection is disabled
  - You cannot add DHCP fingerprint filters
  - You cannot apply DHCP fingerprint filters to any DHCP address range

  For information about DHCP fingerprints, refer to the "*DHCP Fingerprint Detection*" chapter in the *Infoblox NIOS Administrator Guide*, Releases 6.7.

- API and RESTful API: After upgrading to NIOS 6.7.x, all international domain names (IDNs) in punycode are converted to Unicode (in the respective API way of encoding Unicode strings). You can use the dns_[…] fields in relevant objects to retrieve read-only IDNs in punycode. For more information about IDNs, refer to the *Infoblox NIOS Administrator Guide*. For information about API and RESTful API, refer to the *Infoblox API Documentation* and *Infoblox RESTful API Documentation*.

Upgrading to NIOS 6.6.x

- When you schedule a full upgrade from an earlier NIOS release to NIOS 6.6.x, the appliance puts certain rules in place to ensure data integrity and controls data that can cause undesirable results during the upgrade process. During an upgrade, there are tasks and operations that the Grid Master immediately replicates to members while it puts others in queue until the members have been upgraded. These rules vary depending on the releases you are upgrading from. For detailed information about the rules, refer to the "*Managing NIOS Software and Configuration Files*" chapter in the *Infoblox NIOS Administrator Guide*, Releases 6.4, 6.5, and 6.6.

- After an upgrade, Grid members configured as caching name servers before the upgrade may not function properly because recursion data for the members was not written properly in the DNS configuration file. You can perform the following workaround to correct the issue: Disable recursion at the member level, and then inherit the Grid level settings to enable recursion for the member.

Upgrading to NIOS 6.5.x

If you are running NIOS 6.3.7 or earlier releases on a Trinzic Reporting 4000 or IB-2000-A appliance, ensure that you apply a hot fix to the reporting server before you upgrade to NIOS 6.5.0. For information about how to obtain the hot fix, contact Infoblox Technical Support.

Upgrading to NIOS 6.4.x

A number of new traps have been added as well as new statistical information to poll for. Some changes were also made to some of the MIB, as described in the section **Changes to Default Behavior** on page 18. Infoblox recommends that you upload the latest MIBs.

Upgrading to NIOS 6.2.2

Starting with NIOS 6.2.2, a name server group cannot include Microsoft name servers. During the upgrade, NIOS will delete these name server groups from the zones, and will assign the name servers from the deleted groups directly to the zones.

Upgrading to NIOS 6.1.0

Infoblox recommends that you review these guidelines before upgrading appliances to NIOS 6.1.0.

- When you upgrade a VM-5, VM-25, VM-35, or VM-55 virtual appliance to NIOS 6.1.0 or later, you must deploy the appliance with at least 120GB of disk space. The vNIOS licenses that contain the old vNIOS model numbers are preserved after an upgrade. The display names of the vNIOS for VMware models however, change based on the following:
    - VM-5 to IB-VM-250
    - VM-25 to IB-VM-550
    - VM-35 to IB-VM-1050
    - VM-55 to IB-VM-2000

  For information about the supported vNIOS for VMware models, refer to the *Infoblox Installation Guide for vNIOS Software on VMware*.
- Global administrator permissions for DHCP objects will be converted to global permissions for IPv4 DHCP objects. For example, permissions for “All DHCP Ranges” and “All Shared Networks” will be converted to “All IPv4 DHCP Ranges” and “All IPv4 Shared Networks.”
- In this release, DHCP options spaces and IPv4 filters are displayed in separate tabs under the Data Management tab -> DHCP tab. In earlier releases, DHCP filters and option spaces were displayed in one tab, the Filters/Options Spaces tab.

Upgrading to NIOS 6.x.x

Infoblox recommends that you review these guidelines before upgrading appliances to a NIOS 6.x release.

- 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.

- NIOS 6.0.0 no longer supports running the bloxTools environment on a Grid Master, a Grid Master candidate, or a vNIOS virtual appliance for Riverbed or VMware. You can now run the bloxTools environment on an independent appliance or a Grid member. In a Grid, you can run the bloxTools service on one Grid member only. You can also move the bloxTools service from one member to another. After an upgrade, running the bloxTools service on the Grid Master is allowed only to facilitate the transition of the bloxTools service to a Grid member. Infoblox strongly recommends that you move the bloxTools service to a Grid member as soon as possible. For more information, refer to KB article 17199.

- Infoblox NIOS 6.x is not supported on the IB-250, IB-500, IB-1000, IB-1200, IB-550, IB-1050, IB-1550 and IB-1552 appliances. IB-2000 appliances support NIOS 6.1.0, but not NIOS 6.0. On a Grid or appliance running NIOS 5.1r3, you can use the CLI command `show_upgrade_compatible` to verify whether your Grid or appliance can be upgraded to NIOS 6.x. For information about this command, refer to the *Infoblox CLI Guide*. You can also download the support bundle to obtain the *upgrade_comptability_report.txt* file for a summary of the hardware incompatibility.
- You cannot upgrade a Grid with a Cisco virtual member to NIOS 6.x.
- Infoblox recommends that you run an upgrade test before performing the actual upgrade so you can resolve any potential data migration issues before the upgrade.
- Infoblox recommends that when you enable the Lease Scavenging feature after upgrading from a previous version, that you do so during off-peak hours, as it may impact DHCP services.
- NIOS 5.1r2-1 and later releases do not support records with duplicate IP addresses in the same network view. For example:
  - Two host records, configured for DHCP, with the same IP address in the same network view
  - A host record and a fixed address record with the same IP address in the same network view

  During the upgrade, if the DHCP configuration is the same for the host addresses or for the host address and fixed address, the appliance will remove the DHCP configuration from one host address and will log a warning message in syslog. If the DHCP configuration is different, then the appliance will log an error message in syslog and fail the upgrade.

BEFORE YOU INSTALL

NOTE: You cannot upgrade from NIOS 5.x to NIOS 6.11.x. To ensure that new features and enhancements operate properly and smoothly, Infoblox recommends that you evaluate the capacity on your Grid before you upgrade from a previous NIOS release.

Infoblox recommends that administrators planning to perform an upgrade from a previous release create and archive a backup of the Infoblox appliance configuration and data before upgrading. You can run an upgrade test before performing the actual upgrade. Infoblox recommends that you run the upgrade test, so you can resolve any potential data migration issues before the upgrade.

You can also schedule a full upgrade. Following are NIOS releases from which you can schedule a full upgrade:

6.11.0-EA, 6.11.0-LD
6.10.200
6.10.6 and earlier 6.10.x releases
6.9.201-LD and 6.9.200-LD
6.9.0
6.8.8 and earlier 6.8.x releases
6.7.7 and earlier 6.7.x releases
6.6.13 and earlier 6.6.x releases
6.5.10 and earlier 6.5.x releases
6.4.12 and earlier 6.4.x releases

Following is a list of upgrade and revert paths that are supported in this release:

6.11.0-EA, 6.11.0-LD
6.10.200
6.10.6 and earlier 6.10.x releases
6.9.201-LD and 6.9.200-LD

6.9.0
6.8.8 and earlier 6.8.x releases
6.7.7 and earlier 6.7.x releases
6.6.13 and earlier 6.6.x releases
6.5.10 and earlier 6.5.x releases
6.4.12 and earlier 6.4.x releases

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: https://support.infoblox.com

GUI Requirements

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 recommends that you use a computer that has a 2 GHz CPU and at least 1 GB of RAM.

Infoblox supports the following browsers for Grid Manager:

OS	**Browser**
Microsoft Windows 8®	Microsoft Internet Explorer® 11.x*, 10.x* Mozilla Firefox 25.x, 21.x, 16.x, and 10.x Google Chrome 30.x, 27.x, 22.x, and 16.x
Microsoft Windows 7®	Microsoft Internet Explorer® 11.x*, 10.x*, 9.x, and 8.x Mozilla Firefox 25.x, 21.x, 16.x, and 10.x Google Chrome 30.x, 27.x, 22.x, and 16.x
Microsoft Windows XP® (SP2+)	Microsoft Internet Explorer 7.x and 8.x Mozilla Firefox 25.x, 21.x, 16.x, and 10.x Google Chrome 30.x, 27.x, 22.x, and 16.x
Red Hat® Enterprise Linux® 6.x	Mozilla Firefox 25.x, 21.x, 16.x, and 10.x Google Chrome 30.x, 27.x, 22.x, and 16.x
Red Hat® Enterprise Linux 5.x	Mozilla Firefox 25.x, 21.x, 16.x, and 10.x Google Chrome 30.x, 27.x, 22.x, and 16.x
Apple® Mac OS X 10.8.x	Safari 6.x Mozilla Firefox 25.x, 21.x, 16.x, and 10.x Google Chrome 30.x, 27.x, 22.x, and 16.x
Apple® Mac OS X 10.7.x	Safari 5.x Mozilla Firefox 25,x, 21.x, 16.x, and 10.x Google Chrome 30.x, 27.x, 22.x, and 16.x
Apple® Mac OS X 10.6.x	Safari 5.x Mozilla Firefox 25,x, 21.x, 16.x, and 10.x Google Chrome 30.x, 27.x, 22.x, and 16.x

* **NOTE**: Grid Manager fully supports Microsoft Internet Explorer® 11.x and 10.x when you enable compatibility view in the browser. Features in the **Reporting** tab may not function properly if you disable compatibility view. In the browser, go to **Tools** -> **Compatibility View** to enable the feature.

Infoblox recommends using the latest release of the supported versions of Internet Explorer, Mozilla Firefox or Google Chrome for best performance.

When viewing Grid Manager, set the screen resolution of your monitor as follows:

Minimum resolution: 1280 x 768
Recommended resolution: 1280 x 1024 or better

Documentation

You can download the *Infoblox NIOS Administrator Guide* from the appliance. From Grid Manager, expand the **Help** panel, and then click **Documentation** -> **Admin Guide**.

Training

Training information is available at http://inter.viewcentral.com/events/uploads/infoblox/login.html.

ACCESSING GRID MANAGER

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 product, 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.
2. Enter your user name and password, and then click **Login** or press Enter. The default user name is **admin** and password is **infoblox**.
3. Read the Infoblox End-User License Agreement and click **I Accept** to proceed. Grid Manager displays the Dashboard, your home page in Grid Manager.

ADDRESSED VULNERABILITIES

This section lists security vulnerabilities that were addressed in this and earlier NIOS releases. For additional information about these vulnerabilities, including their severities, please refer to the National Vulnerability Database (NVD) at http://nvd.nist.gov/. The Infoblox Support website at https://support.infoblox.com also provides more information, including vulnerabilities that do not affect Infoblox appliances.

CERT VULNERABILITY NOTE CVE-2014-0591

A crafted query against an NSEC3-signed zone could cause the named process to terminate.

CERT VULNERABILITY NOTE CVE-2013-5211

Remote attackers could utilize the monlist feature in the ntpd process in NTP to cause a denial of service on NTP servers through forged GETLIST requests.

CERT VULNERABILITY NOTE CVE-2013-4854

A specially crafted query could cause the named process to terminate, resulting in a denial of service.

CERT VULNERABILITY NOTE CVE-2012-5689

An error might occur when a name server was configured to use both DNS64 and RPZs (Response Policy Zones), which could cause the name server to terminate with an assertion failure while processing queries.

CERT VULNERABILITY NOTE CVE-2012-5688

A specially crafted query sent to a name server using the DNS64 IPv6 transition mechanism could cause a denial of service on the server.

CERT VULNERABILITY NOTE CVE-2012-5166

When specific combinations of RDATA were loaded into a name server, through cache or an authoritative zone, a subsequent query for a related resource record could cause the named process to lock up and become non-responsive to queries and control commands.

CERT VULNERABILITY NOTE CVE-2012-4244
If a specially crafted resource record with RDATA exceeding 65535 bytes was injected into a name server, then a subsequent query for that record could cause the named process to terminate with an assertion failure.

CERT VULNERABILITY NOTE CVE-2012-3955
Reducing the expiration time of an IPv6 lease could cause the dhcpd process to terminate with an assertion failure.

CERT VULNERABILITY NOTE CVE-2012-3954
On a server that has been running for a long time without restarting or on a server that handled a large amount of traffic from DHCP clients, a memory leak could consume all memory available to the DHCP server process, preventing further operation by the DHCP server process and potentially interfering with other services hosted on the same server.

CERT VULNERABILITY NOTE CVE-2012-3817
On recursive servers with DNSSEC validation enabled, a high number of DNSSEC validation queries could cause an assertion failure in “named” when it accessed the “Bad Cache” data before it was fully initialized.

CERT VULNERABILITY NOTE CVE-2012-3571
An error in the handling of malformed client identifiers could cause a DHCP server to enter a state where further client requests were not processed and the server process went into an endless loop, consuming all available CPU cycles and resulting in a denial or service.

CERT VULNERABILITY NOTE CVE-2012-3570
An unexpected client identifier parameter could cause the ISC DHCP daemon to experience segmentation fault when running in DHCPv6 mode, resulting in a denial of service to further client requests.

CERT VULNERABILITY NOTE CVE-2012-1667
Processing DNS resource records with zero-length rdata fields could cause unexpected issues, such as zone data corruption and termination of the named process.

CERT VULNERABILITY NOTE CVE-2012-2110
This release updated the SSL handling of certain certificate formats.

CERT VULNERABILITY NOTE CVE-2012-1033
This release restricts the TTL value of the NS RRset to no more than that of the old NS RRset when replacing it in the cache. This change was made to address CVE-2012-1033.

CERT VULNERABILITY NOTE CVE-2011-4868
Improper handling of Dynamic DNS information associated with DHCPv6 leases could cause a segmentation fault in ISC DHCP servers using IPv6 and Dynamic DNS, resulting in denial of service to clients. Infoblox NIOS is not vulnerable because of additional validation that Infoblox added to the DHCP code. NIOS 6.3.1 contains the ISC fix to be consistent with the ISC code.

CERT VULNERABILITY NOTE CVE-2011-4313
After a recursive name server caches an invalid record, subsequent queries for that record could crash the resolver with an assertion failure and the following error message: "INSIST(! dns_rdataset_isassociated(sigrdataset))"

CERT VULNERABILITY NOTE CVE-2011-3192
The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 could allow remote attackers to cause a denial of service.

CERT VULNERABILITY NOTE CVE-2011-2748 | CVE-2011-2749
DHCP: A remote attacker could cause the "dhcpd" process to exit using a specially crafted packet.

CERT VULNERABILITY NOTE VU#142646 (CVE-2011-2464)
BIND 9: Denial-of-service vulnerability in recursive and authoritative DNS servers in which a specially crafted packet sent to the servers could cause the “named” process to fail.

CERT VULNERABILITY NOTE VU#795694 (CVE-2011-1910)
BIND 9: Very large DNSSEC RRSIG RRsets in a negative cache could trigger an assertion failure that could cause the “named” daemon to fail.

CERT VULNERABILITY NOTE CVE-2011-0419
Denial-of-service vulnerability in which a carefully crafted HTTP request could cause excessive CPU usage under some circumstances.

CERT VULNERABILITY NOTE VU# 159528 (CVE-2010-3616)
DHCP: Server hangs with TCP to failover peer port.

CERT VULNERABILITY NOTE VU#360341 (CVE-2010-3613)
BIND 9: Cache incorrectly allows a ncache entry and a rrsig for the same type

CERT VULNERABILITY NOTE VU#360341 (CVE-2010-3614)
BIND 9: Key algorithm rollover bug

CERT VULNERABILITY NOTE VU#360341 (CVE-2010-3615)
BIND 9: Allow-query processed incorrectly

CERT VULNERABILITY NOTE VU#360341 (CVE-2010-0097)
BIND 9 DNSSEC validation code could cause fake NXDOMAIN responses

CERT VULNERABILITY NOTE VU#568372 (CVE-2009-3563)
NTP denial-of-service vulnerability

CERT VULNERABILITY NOTE VU#418861 (BIND 9.6.1-P2) (CVE-2009-4022)
Cache Update from Additional Section

CERT VULNERABILITY NOTE VU#120541 (CVE-2009-3555)
TLS renegotiation MITM attacks

CERT VULNERABILITY NOTE VU#723308 (CVE-2008-4609)
State vulnerabilities triggered by sockstress

CERT VULNERABILITY NOTE CVE-2009-3111
Denial-of-service condition from malformed Tunnel-Password attribute

CERT VULNERABILITY NOTE VU#725188 (CVE-2009-0696)
Denial-of-service condition when processing a specially-crafted dynamic DNS update packet

RESOLVED ISSUES

The following issues were reported in previous NIOS releases and resolved in this release. The resolved issues are listed by severity. For descriptions of the severity levels, refer to **Severity Levels** on page 53.

Fixed in 6.11.0

ID	Severity	Summary
NIOS-48223	Critical	This release fixes issues that caused some appliances to reboot under rare conditions.
NIOS-47920	Critical	Cached DNS responses on the Infoblox-4030 Rev-2 appliance with DNS cache acceleration enabled were sent through the interface on which the queries arrived, not the interface that was configured for the static route.
NIOS-47540 NIOS-47506	Critical	Updated the *Infoblox NIOS Administrator Guide* and online help to clarify information about the default setting of the NTP Access Control functionality.
NIOS-47511	Critical	The DHCP service restarted when user changed networks from a member to a failover association.
NIOS-47457	Critical	API: No objects were returned when using Infoblox::DNS::Host and regular expression ".*" to perform a host export.
NIOS-47408	Critical	When uploading large files such as ISO images, the file distribution service on the Grid Master truncated the files.
NIOS-47310	Critical	DHCP service was intermittently interrupted for DHCP clients belonging to subnets that had NAC filtering configured.
NIOS-46941	Critical	To improve GUI and API performance, this release adds a new CLI command to enable and disable Microsoft DNS server.
NIOS-46808	Critical	When configured to send DDNS updates using GSS-TSIG, DHCP service was degraded when the Kerberos server was unreachable.

ID	Severity	Summary
NIOS-49099	Major	Using global search to find devices and interfaces took longer than expected on a medium size network.
NIOS-49067	Major	Processing a large number of child networks in a network container could affect performance on Grid Manager.
NIOS-48188	Major	This release adds a **Clear** check box so users can remove a Grid member that was previously selected as a DHCP lease history log member.
NIOS-48439	Major	The appliance might return incorrect log messages if the DHCP thresholds were set to 0 for high reset, low trigger, and low reset.
NIOS-48436	Major	The IB-4030 appliance could encounter high CPU usage when using certain support bundle tools.
NIOS-48198	Major	Excessive temp files that did not get cleaned up caused a high disk usage on a vNIOS virtual member.
NIOS-43516	Major	This release clarifies the meanings of "Last Changed" and "Last Updated" for Microsoft synchronization.

NIOS-48026	Major	Users could not delete auto-created A records.
NIOS-48001	Major	On rare occasions, the IB-4030 appliance rebooted spontaneously.
NIOS-47985	Major	The appliance returned an error when users tried to modify the alias value in a host record.
NIOS-47944	Major	Users could not set the NAPTR record flag to an empty value.
NIOS-47881	Major	A DIW import failed to import zones that contained punycode data.
NIOS-47879	Major	Global search failed to display results when searched for "All" objects.
NIOS-47848	Major	The error message "Duplicate object of type 'lease' already exists in the database" appeared when users tried to edit a DHCP range.
NIOS-47844	Major	The appliance did not show any warning messages when users click the *Network/Range Selector* dialog box.
NIOS-47838	Major	Users could not set empty strings for NAPTR records through the Infoblox GUI or CSV import.
NIOS-47803	Major	In this release, the "Synchronize the Grid with NTP Servers" has been renamed to "Synchronize the Grid with these External NTP Servers" in the *Grid NTP Properties* editor and "Enable this Member as an NTP Server" has been renamed to "Enable the NTP Server on this Member" in the *Member NTP Properties* editor.
NIOS-47791	Major	Enabling the diskcheck process on the vNIOS virtual appliance could cause the appliance to reboot unexpectedly.
NIOS-47772 NIOS-47758	Major	In a DHCP failover association, a MD5 digest related configuration mismatch between the peers could cause the failover association to stay in a degraded state.
NIOS-47767	Major	Users could not import a zone containing an A record with IP address "0.0.0.0".
NIOS-47766	Major	The appliance returned an error when users tried to access `snapin-workflow` in the bloxTools environment.
NIOS-47746	Major	Reporting: The appliance failed to generate some reports due to limitation of resources.
NIOS-47714	Major	The "named" process ended unexpectedly.
NIOS-47647	Major	Reporting: The appliance displayed an error and users were unable to view the reports when they used the start date and end date as the filtering criteria.
NIOS-47634	Major	Grid members could not rejoin the Grid after an upgrade due to some VPN certification issues.
NIOS-47608	Major	Regardless of which VLAN interface was configured for the OSPF advertising interface, the appliance used the LAN1 interface.
NIOS-47576	Major	When users tried to add a static route, it was considered as a duplicate because the subnet was not factored.
NIOS-47471	Major	Grid Manager might display an incorrect network when users opened a network from the **Finder** -> **Smart Folders** panel.

NIOS-47437	Major	When users tried to create a second host record in step two of the *Add Host* wizard by selecting "**Save and New**," the Inheritance State column for all required and recommended extensible attributes defaulted to "**Overridden**" instead of "**Inherited**" even when the **Enable Inheritance** check box was selected.
NIOS-47405	Major	A database transaction timeout due to user authentication issues could cause an HA Grid member to restart services and consequently caused a failover.
NIOS-47304	Major	API: When querying host records that were associated with multiple IP addresses, the appliance returned an error.
NIOS-47272	Major	**DHCP options spaces** and **IPv4 filters** were displayed in separate tabs under the **Data Management** tab -> **DHCP** tab.
NIOS-47237	Major	Error messages related to RADIUS were logged in the syslog. They have now been moved from the syslog to Infoblox.log.
NIOS-47186	Major	While importing the zone data using the **Import Zone** option, CPU usage was high and it took a longer time to complete the task while all the other Grid Manager operations were pushed to the background.
NIOS-47143	Major	The appliance was rebooted each time users used maintenance mode commands to remove name server records.
NIOS-47137	Major	API: Records returned from existing API scripts did not include "host alias."
NIOS-47117	Major	Grid Manager did not return an appropriate error message when a signed certificate was imported to a wrong member.
NIOS-47115	Major	On rare occasions, an unexpected shutdown of a reporting server could cause filesystem corruption.
NIOS-47111	Major	SRV records were not transferred correctly to external secondaries if the records were created as shared records.
NIOS-47071	Major	Grid Manager displayed an intermittent error message while performing administrative tasks.
NIOS-46883	Major	Malformed DNS header fields might result in an unexpected product restart on IB-4030 appliances.
NIOS-46787	Major	Database performance was affected when innermost queries did not return any results.
NIOS-45743	Major	The syslog messages and SNMP traps displayed the LAN1 IP address even when the MGMT port was configured for syslog and SNMP traps and when actual packets originated from the MGMT port.
NIOS-46738	Major	An auto-provisioned member did not use the default gateway IP address provided by the DHCP server.
NIOS-46673	Major	When the DHCP range threshold was crossed, the SNMP trap and syslog message displayed a different format for the DHCP range.
NIOS-46626	Major	The appliance generated excessive messages related to high SWAP memory usage.
NIOS-46576	Major	Services on the Grid Master were briefly interrupted when a scheduled discovery started.
NIOS-46453	Major	Grid Manager displayed incorrect time for Russian time zones.

NIOS-46163	Major	When there were a huge number of zone/network associations, selecting a network in the Network Selector might require a lot of querying, which could cause the HA Grid Master to fail over.
NIOS-46106	Major	This release changes how the appliance handles an expired or expiring VPN certificate.
NIOS-45891	Major	The syslog reported that a scheduled backup to an FTP server was successful when the backup actually failed.
NIOS-45863	Major	Under certain circumstances, the appliance experienced a brief DHCP service interruption.
NIOS-43997	Major	A CLI command was added to reset the system and shred all deleted files.
NIOS-43450	Major	In a Multi-Grid configuration, Multi-Grid Manager failed to synchronize with a sub Grid.
NIOS-43261	Major	API: The appliance returned a “Can’t locate object method” error when users tried to search for all DHCP fixed addresses using the Infoblox::Session->new_cursor() method.
NIOS-38898	Major	An appliance reported an LCD failure even though the appliance and the LCD were functioning properly.
NIOS-31201	Major	DHCP service could be affected if an FQDN instead of an IP address was used for the Next Server and Boot Server if the DHCP could not resolve the FQDNs.
NIOS-31025	Major	A newly added extensible attribute value did not appear in the Smart Folder when using the Group by filter.
NIOS-29022	Major	The appliance performed an overwrite action instead of a merging action when users tried to merge DHCP network data through CSV import.
NIOS-49015	Minor	Under certain circumstances, users could not convert an unmanaged IP to a host record.
NIOS-49014	Minor	In the IP Map panel, all IP addresses were represented as devices when only infrastructure devices should be.
NIOS-48681	Minor	GUI sessions might time out when users tried to populate or search for a reverse mapping zone in Grid Manager.
NIOS-48426	Minor	The appliance did not display the RDATA from the DNSKEY in Grid Manager.
NIOS-48142	Minor	This release updates hardware model names in the **Pre-provision** tab to reflect the correct hardware models.
NIOS-48132	Minor	Memory and CPU usage specifications for the IB-VM-2200 virtual appliance were missing in the NIOS 6.10.6 and 6.11.0-LD release notes.
NIOS-48082	Minor	SCP backup failed when HPN patch for OpenSSH was enabled.
NIOS-48054	Minor	A forwarding server returned a SERVFAIL response when a RPZ (Response Policy Zone) was defined with a QNAME that triggered the forwarder to return NXDOMAIN responses.
NIOS-47954	Minor	Reporting: Information reported in the DNS Daily Query Rate by Server report was different from the information delivered in the results.csv file through an alert email.
NIOS-47950	Minor	The “Network Associations” label was missing in the **General** tab -> **Advanced** tab in the zone editor.
NIOS-47921	Minor	When creating a global smart folder that included an extensible attribute as a filter for a zone, resource records in the zone were not displayed.

NIOS-47886	Minor	The appliance returned an incorrect error message when users tried to modify zone properties.
NIOS-47870	Minor	The *Infoblox NIOS Administrator Guide* did not include support for IPv6 on multiple interfaces.
NIOS-47827	Minor	Users could not add "." to the **Target** field in an SRV record.
NIOS-47824	Minor	The bloxTools environment URL was incorrect in the *Infoblox NIOS Administrator Guide.*
NIOS-47814	Minor	The page numbers on the Index page was incorrect in the *Infoblox NIOS Administrator* Guide.
NIOS-47811	Minor	The time zone was not updated properly when a task was rescheduled.
NIOS-47797	Minor	Updated the installation guides for 1400 and 2200 Series appliances to include grounding post instructions and pictures for DC installation.
NIOS-47572	Minor	When users tried to import a CSV file, the appliance displayed an error and the CSV import failed.
NIOS-47566	Minor	Fixed a minor error in the *Infoblox NIOS Administrator Guide*.
NIOS-47539	Minor	Removed the duplicate trap description for “Shutting down services due to database snapshot” in the *Infoblox NIOS Administrator Guide*.
NIOS-47538	Minor	Updated the *Infoblox NIOS 6.10.4 Release Notes* to include IB-2000 appliance in the supported platforms list.
NIOS-47510	Minor	The trap severity for the “Backup Failed” trap was incorrect in the *Infoblox NIOS Administrator Guide*.
NIOS-47494	Minor	The appliance reported an error when a named ACL was applied to the NTP service.
NIOS-47476	Minor	A new IPv6 address was added to c.root.servers.net, but the root hint file for NIOS was not updated.
NIOS-47398	Minor	API: When performing a search for network containers, the appliance ignored the views specified in the search, which resulted in a search error if the network container was in two different views.
NIOS-47382	Minor	After an upgrade from NIOS 6.7.6 to NIOS 6.10.3, when users disabled the auto-provisioning for the Grid Master, it was not automatically disabled for the Grid member.
NIOS-47200	Minor	The appliance did not return certain information when users filtered their results based on external attributes in the **IPAM** -> **List** tab.
NIOS-47138	Minor	The *IPv4 DHCP Failover Status* dialog box showed incorrect date and time in the **Event Date** field for both primary and secondary failover objects.
NIOS-47070	Minor	This release updated the internal version of some crypto libraries.
NIOS-47049	Minor	Updated the **Advanced Discovery Polling** section of the *Infoblox NIOS Administrator Guide* to display “no longer seen on the network” instead of “not reachable”.
NIOS-47018	Minor	Grid Manager did not return an appropriate error message when the domain name, while defining RPZ rules, had trailing or leading spaces.

NIOS-46869	Minor	Network Insight: After a discovery, not all routers in all networks were displayed in the **Device** tab and Grid Manager did not show any conflicts regarding the discover data and current data in the networks.
NIOS-46867	Minor	This release modifies the check boxes for LAN1 in the **General** tab of the *Member DHCP Properties* editor. Users can now select these check boxes to reflect the state of the DHCP service.
NIOS-46861	Minor	When an hourly discovery was scheduled, the logs recorded excessive warnings.
NIOS-46705	Minor	Under certain circumstances, the serial_console process consumed a higher than usual CPU usage.
NIOS-46586	Minor	Network Insight: Grid Manager did not display the device name for regular Grid members.
NIOS-46584	Minor	The appliance did not save the time settings made on the Reporting Dashboard.
NIOS-46582	Minor	There was no indicator in the *Distribution Schedule* dialog to inform users that the appliance was uploading upgrade groups.
NIOS-45456	Minor	The syslog logged "RSA_verify failed" messages after an upgrade.
NIOS-43800	Minor	Reporting data on a Grid member was not properly synchronized with the reporting server due to some time zone issues.
NIOS-43580	Minor	On rare occasions, the appliance might not send NOTIFY messages to external servers.
NIOS-43458	Minor	Grid fingerprint data for fixed addresses was not populated in the IPAM view, though the data appeared in dynamic leases.
NIOS-43247	Minor	Intermittent performance issues might occur when DNS service used a high-water/low-water mark for cache cleaning.
NIOS-39535	Minor	The "Enable All Email Notifications" option was disabled after an upgrade even though this option was enabled in the previous release before the upgrade.
NIOS-36223	Minor	This release modifies the *Grid NTP Properties* editor so users can now select a preferred NTP server for synchronization.
NIOS-34991	Minor	Grid Manager limited the length of a shared network name to 32 characters, which did not match the ISC standard of no limit.
NIOS-34145	Minor	In IP Map, the first IP address was not marked as **Unmanaged** for a /31 discovered network.
NIOS-28668	Minor	This release removes the "Include objects with no values…" check box. The appliance continues to include objects that do not contain extensible attribute values when using the Group by filter.
NIOS-28489	Minor	SNMP traps and email notifications were sent even when SNMP queries and SNMP traps were disabled.
NIOS-12682	Minor	CLI commands were not sorted alphabetically.
NIOS-12206	Minor	Not all CNAME records were converted into host aliases during a DIW zone import.
NIOS-10800	Minor	The appliance did not log an event or SNMP trap when a core network service returned to a functional state after it went out of service.

NIOS-48211	Enhance	This release adds improvements to the bloxTools editor, which include indenting the "Redirect bloxTools HTTP to HTTPS" check box and adding a message next to the HTTPS port setting.
NIOS-48180	Enhance	This release enhances the UI message for the "Enable ARP on HA Passive Node" feature.
NIOS-47306	Enhance	This release enhances the CLI commands show firmware, show hardware_status, and show interface so they now display all FRUs that have associated firmware such as motherboards and disks. They also display serial numbers for these components.
NIOS-47281	Enhance	This release adds the **Index%** and **Used%** fields to the reporting category to indicate the maximum index size and maximum retention days for a report category.

Fixed in 6.11.0-LD

ID	Severity	Summary
NIOS-46107	Critical	DNS query responses could be dropped when port redundancy was enabled due to a misconfiguration of the bonding interface.
NIOS-36178	Critical	On rare occasions, the appliance did not restart due to a race condition.

ID	Severity	Summary
NIOS-46989	Major	Updated the *Infoblox NIOS Administrator Guide* to reflect information about NTP communications related to HA pairs and HA failover.
NIOS-46974	Major	Updated the *Infoblox NIOS Administrator Guide* and online Help to clarify information about the "Restrict GUI/API Access" functionality.
NIOS-46925	Major	Users could not modify a Grid secondary zone after a zone transfer.
NIOS-46821	Major	After an upgrade, the appliance returned an error indicating that the swap file was reaching a critical threshold.
NIOS-46712	Major	Grid Manager did not allow users to assign a member or modify the assignment of member after they created and saved a DHCP range.
NIOS-46672	Major	The Traffic Capture tool continued to capture traffic after the configured duration time.
NIOS-46653	Major	When users modified a host address using CSV import, the appliance removed the DHCP-enabled host record.
NIOS-46651	Major	Users could not use escape characters in the bulk host name format.
NIOS-46648	Major	Users could not access the remote console when CIDR netmask configured in the list of ACEs was smaller than /24.
NIOS-46641	Major	A reporting related message still existed after users removed the reporting server from the Grid.
NIOS-46635	Major	The appliance failed to notify the external secondary servers when a host record was imported using CSV import for reverse-mapping zones.
NIOS-46629	Major	Deleting the A record for an external secondary within the zone changed the IP address of the external server to 255.255.255.255 for all remaining zones.

NIOS-46612	Major	When users modified a host address using CSV import, the appliance did not increment the SOA serial number.
NIOS-46580	Major	DIW logs indicated that certain A and PTR records were not allowed in reverse-mapping zones even after the records were successfully imported through DIW.
NIOS-46568	Major	It took longer than expected to delete a large number of MAC addresses in a MAC filter.
NIOS-46561	Major	Updated the *Infoblox CSV Import Reference* to reflect information about fingerprint filter rules for IPv4 DHCP ranges.
NIOS-46550	Major	Users could not upload a file through the file distribution service.
NIOS-46534	Major	Updated the *Infoblox NIOS Administrator Guide* to reflect information about DHCP snooping.
NIOS-46530	Major	Global search provided a hyperlink for a Microsoft secondary zone even though zone data did not get synchronized to NIOS.
NIOS-46510	Major	The appliance failed to copy A and AAAA records of a DNS zone from one DNS view to another.
NIOS-46487	Major	The appliance did not show error messages when users entered non-octal numbers (such as “08” or “09”) while defining custom DHCP options.
NIOS-46443	Major	The passive node of an HA pair synchronized its time with an external NTP server.
NIOS-46437	Major	The Captive Portal web page was unexpectedly cached and users had to clear the browser cache in order to open the configured Home page.
NIOS-46333	Major	Updated the Infoblox NIOS Administrator Guide to include information about SCP uses the LAN1 port for communication with external servers.
NIOS-46332	Major	A warning message about missing query redirection license still appeared after users restored a database backup.
NIOS-46298	Major	Addressed CVE-2013-5211: Remote attackers could utilize the monlist feature in the ntpd process in NTP to cause a denial of service on NTP servers through forged GETLIST requests.
NIOS-46249	Major	If the **MAC Address** column was included for viewing, Grid Manager displayed an error when users tried to open a network from the **Data Management** tab -> **DHCP** tab.
NIOS-46248	Major	The filters in the *DNS Top RPZ Hits* report failed to filter the first IP address in the list.
NIOS-46240	Major	The DHCP server messages (DHCPOFFER and DHCPPACK) displayed different lease values.
NIOS-46180	Major	A Grid secondary did not sent notify messages to an external secondary that was defined only in the “also-notify” list but not explicitly defined in the zone’s NS server list as an external secondary.
NIOS-46177	Major	The **Go to** field of the Infoblox GUI failed to find a MAC address that was written in uppercase characters.
NIOS-46169	Major	The offset in time on the Grid Master caused Grid members to constantly reset their times, which resulted in service interruptions on the members.

NIOS-46136	Major	This release adds a warning message that indicates no NS record will be added for a forward-mapping zone when users add or modify the zone in an authoritative zone that uses an external primary or a Microsoft primary in read-only mode.
NIOS-46091	Major	Users could not use escape characters in the bulk host name format.
NIOS-46079	Major	In a Multi-Grid configuration, Multi-Grid Manager displayed an “Inactive” status for a Grid that had a status of “Joined” or a connection status of “Attached.”
NIOS-46038	Major	Users were able to add Safenet HSM servers individually, but they could not add the same servers to an HSM group.
NIOS-46002	Major	On appliances running NIOS 4.x, users could not set the date and time beyond a certain date.
NIOS-45975	Major	While navigating to the **Grid** tab -> **HSM Group** tab in Grid Manager, the GUI session unexpectedly timed out.
NIOS-45964	Major	Users could not log in to the bloxTools environment through SFTP.
NIOS-45821	Major	A GUI session timed out after users tried to modify networks and host records through Grid Manager but failed to do so.
NIOS-45778	Major	Changes made to a Microsoft synchronized zone through NIOS were not replicated to the Microsoft DNS servers.
NIOS-45756	Major	In a Multi-Grid configuration, limited-access users could not view all networks in the **Data Visualization** tab.
NIOS-45743	Major	The appliance displayed incorrect port in the syslog messages for SNMP traps.
NIOS-45737	Major	NIOS failed to synchronize DHCP data from Microsoft Windows 2012 servers in read-only mode.
NIOS-45649	Major	Some clients were refused responses from DNS caching servers due to certain ACL (Access Control List) related issues.
NIOS-45434	Minor	The Smart Folder failed to filter networks that are created through the **Dashboard** tab -> **Status** tab -> **My Commands** -> **Add IPv4 Reservation**.
NIOS-45309	Major	A delay in non-authoritative name resolution occurred when the query-source port was set to a single static port
NIOS-45265	Major	API: DNS statistics returned from existing API scripts did not include certain information.
NIOS-45225	Major	API: When adding a sort list object that included an IP address and its network mask in CIDR format, the appliance displayed only the IP address but not the network mask.
NIOS-45157	Major	Minimum anycast and BGP outage occurred when users disconnected the LAN1 interface.
NIOS-45571	Major	When users disconnected the LAN1 interface, the appliance did not automatically switch the default route to LAN2.
NIOS-45535	Major	Under certain circumstances, the Grid Master restarted frequently.
NIOS-44856	Major	Updated the installation guides for NIOS appliances to include requirements for the LOM (Light Out Management) port connectivity.

NIOS-44773	Major	One of the Grid members reported a failure in its distribution status during an upgrade.
NIOS-44697	Major	The syslog reported that SNMP traps and syslog messages were originated from the LAN1 port when they were actually originated from the MGMT port.
NIOS-44169	Major	Users received DNS responses when querying MX records for delegated domains, which was the incorrect behavior.
NIOS-43920	Major	In Grid Manager, users were not clear about the GUI options related to NTP configuration for slew time synchronization with externals NTP servers versus local server.
NIOS-43798	Major	The appliance was unable to extract the OCSP responder certificate when users uploaded a trusted CA certificate.
NIOS-42861	Major	The TFTP process failed due to issues related to the tftpd lock file.
NIOS-42366	Major	The warning message “Grid name server must be recursive” appeared after users had already configured but could not save an external feed RPZ, which resulted in loss of the configuration data.
NIOS-39614	Major	In a Multi-Grid configuration, a manual snapshot process failed due to unsupported FTP server configurations.
NIOS-30950	Major	In certain web browsers, users experienced some navigation and visibility issues when viewing IP addresses in an address range.
NIOS-47276	Minor	Updated the *Infoblox NIOS Administrator Guide* to include trap severity for the Grid queue replication problem.
NIOS-47094	Minor	The format of the user name for authenticating an AD domain was not clearly documented in the *Infoblox NIOS Administrator Guide*.
NIOS-47007	Minor	The *DHCP Statistics* widget on the Dashboard was not updated properly when DHCP was running on the LAN2 port.
NIOS-46747	Minor	Updated the *Infoblox NIOS Administrator Guide* to reflect information about MIB variables (ibDNSOne) for cache hit rate and queries per second.
NIOS-46703	Minor	CPU utilization of the serial console process was unexpectedly high.
NIOS-46660	Minor	Modifying a DHCP exclusion range opened up an incorrect menu option.
NIOS-46604 NIOS-46583	Minor	Active Web UI user sessions on the Dashboard did not expire after an idled session timeout.
NIOS-46581	Minor	The *Restart Grid Services* panel had a fixed size and could not display all the impacted members and services for larger Grids.
NIOS-46541	Minor	The vNIOS virtual appliance did not display offline status for a Grid member when users set CPU resources to ‘unlimited’ through vSphere.
NIOS-46515	Minor	The existence of an unused and harmless sftp-server subsystem that did not have executable permissions could trigger a security scanning tool to report it as an issue.
NIOS-46364	Minor	In a Multi-Grid configuration, bookmarks in a sub Grid did not refresh automatically.
NIOS-46334	Minor	The string value to override an inherited value was incorrectly documented in the *Infoblox CSV Import Reference*.

NIOS-46277	Minor	Fixed inconsistencies between the online help file and the *Infoblox NIOS Administrator Guide* about backing up the reporting database.
NIOS-46189	Minor	In certain web browsers, Grid Manager did not display icons properly in the **System Manager** tab.
NIOS-46164	Minor	When users launched *Network Selector* from the *Add Networks* wizard (through Next Available IP) in **IPAM Task** on the **Dashboard**, the selector contained searches other than the default “All Networks” search that was used when launching the selector through other wizards.
NIOS-46160	Minor	DNS cache acceleration service unexpectedly restarted.
NIOS-46135	Minor	Global search failed to display results when searched for a MAC address.
NIOS-46034	Minor	The PXE lease time displayed the last configured value instead of the latest configured value during CSV export.
NIOS-45998	Minor	Updated the *Infoblox NIOS Administrator Guide* to reflect information about the list of certain characters that required manual escape while configuring a DHCP boot file name.
NIOS-45575	Minor	When starting a discovery from the **Data Management** tab -> **IPAM** tab, the timestamps for “Current Status” displayed incorrect information.
NIOS-45104	Minor	Updated the online help to reflect correct CPU usage trigger and reset values for SNMP thresholds.
NIOS-45055	Minor	Updated the *Infoblox NIOS Administrator Guide* to clarify the example for specifying a zero-padded bulk host name format.
NIOS-44359	Minor	Updated the *Infoblox NIOS Administrator Guide* to include the support of Microsoft Windows Server 2012 for Active Directory and GSS-TSIG.
NIOS-44243	Minor	Updated the *Infoblox NIOS Administrator Guide* to remove information related to DNS service was enabled by default.
NIOS-43745	Minor	When users added a new GSS-TSIG key, the appliance returned an error indicating that the key already existed.
NIOS-43636	Minor	Users could not disable the bloxTools environment after an upgrade.
NIOS-42084	Minor	Verified and added RFC 4075 compliance to the *Infoblox NIOS Administrator Guide*.
NIOS-35391	Minor	The **Restart** button for restarting DNS service did not appear on the primary name server after users enabled DDNS in DHCP.
NIOS-34876	Minor	The appliance added grace period to the KSK (Key Signing Key) and ZSK (Zone Signing Key) rollover periods.
NIOS-29665	Minor	The *CSV Import Reference* incorrectly indicated that inherited values could be overridden with a string of “\<empty\>.”
NIOS-19991	Minor	In the NetMap panel of Grid Manager, the zoom in and zoom out controller did not function according to expectations.
NIOS-46255	Enhance	This release adds a feature that excludes Grid members from the “infoblox-deny-rpz” list if the members do not have the RPZ license

NIOS-7906	Enhance	The appliance can now automatically pre-populate the host name and zone name when users convert a lease, a lease with A record, a lease with PTR record, or a lease with A and PTR record into a host record.

Severity Levels

Severity	Description
Critical	Core network services are significantly impacted.
Major	Network services are impacted, but there is an available workaround.
Moderate	Some loss of secondary services or configuration abilities.
Minor	Minor functional or UI issue.
Enhance	An enhancement to the product.

KNOWN GENERAL ISSUES

ID	Summary
NIOS-49123	Network Insight: When scheduling a discovery or port control blackout, the scheduled time and time zone will always be standard time. No time adjustments are made if the selected time zone is currently in daylight savings time and no adjustments are made when the time zone switches to daylight savings time.
AUGUSTA2-1606	Network Insight: Some devices, such as the Cisco 3750X, may report interfaces (that are not actually functional) as available through SNMP, which could cause Port Control jobs on these non-functional interfaces to fail.
NIOS-48944	Reporting: When there are disconnected data points in the reporting data for reports (such as the *DNS Query Rate by Query Type* report) that support the stacked area panel type, the stacked area that represents the disconnected data in the PDF report may not fill up accordingly and may cause it to look like a line chart when it is actually a stacked area chart. Workaround: Interpret the information correctly when reading the stacked area charts that contain disconnected data points.
NIOS-48912	Network Insight: Is a device is not connected to another host through a network, the appliance will not be able to detect the Voice VLAN information
NIOS-48897	Network Insight: Alcatel Omniswitches can operate in two modes—Working mode and Certified mode. Alcatel OmniSwitch 6000 devices must run in Working mode to allow Port Control jobs to work on these devices.
NIOS-48704	Reporting: When you configure a search for *Top Devices Denied an IP Address* using **Member**, **Network View**, **Network**, and **CIDR** as alerting filters, the alerts are triggered correctly, but the alerting conditions are not included in the alerting email and the **Query Terms** field in the email may show "**unconditioned**." Workaround: Define the alerting and email titles to reflect the specified conditions.
NIOS-48560	Network Insight: Before joining the Network Data Consolidator to the Grid, use the CLI command `reset net-automation database` to ensure that previously discovered device information is removed from the database.
NIOS-48399	You cannot restore the existing deleted resource records from the Recycle Bin after you promote a Grid Master Candidate to the Grid Master.

NIOS-48135	bloxTools data prior to NIOS 6.4.0 cannot be restored on NIOS 6.11.x. Workaround: Upgrade to NIOS 6.4.x first to get a backup before upgrading to NIOS 6.11.x.
NIOS-48030	You may not be able to log in to the bloxTools Workflow environment if you download the snapin-workflow file from the bloxTools Community site.
NIOS-47959	Through the API and RESTful API, users can add records and data without entering values for required extensible attributes. Users cannot do the same through Grid Manager.
NIOS-46356	An upgrade may fail if you clone reports and searches with duplicate names for the following reports: DNS Query Rate by Server, DNS Daily Query Rate by Server, DNS Daily Peak Hour Query Rate by Server, DHCP Device Operating System Trend, DHCP Top Device Operating System, and Traffic Rate.
NIOS-46290	In some scenarios, upgrading from NIOS 6.7.x to NIOS 6.10.x on an Infoblox-4030 appliance may require a manual restart to complete the upgrade.
NIOS-46102	Advanced DNS Protection: You may not be able to join an independent appliance to the Grid if the appliance has threat protection service enabled and only the LAN interface configured. Workaround: Disable threat protection service on the appliance before joining the Grid, or configure the MGMT port and enable VPN on MGMT before joining the offline appliance to the Grid.
NIOS-46051	Reporting: When you configure a search for *Threat Protect Event Count by Severity Trend* using **Member**, **Category**, and **Rule ID** as alerting filters, the alerts are triggered correctly, but the alerting conditions are not included in the alerting email and the **Query Terms** field in the email may show "**unconditioned**." Workaround: Define the alerting and email titles to reflect the specified conditions.
NIOS-45906	Network Insight: On rare occasions when there is incomplete, inaccurate, or misinterpreted data in discovered spanning tree information, the appliance may not be able to determine the correct switch to which an end host is attached. In this scenario, the appliance may display inaccurate discovered data.
NIOS-45904	Network Insight: In Grid Manager, the same end host on different VLANs may appear as duplicates that contain the same VLAN information.
NIOS-45872	Content in the *bloxHub* widget on the Status Dashboard may not be displayed in certain versions of Google Chrome, Mozilla FireFox, and Microsoft Internet Explorer browsers due to security updates implemented by these browsers. Workarounds: For Chrome: Click the security shield icon next to the URL and select **Load unsafe script**. For FireFox: Click the security shield icon next to the URL and select **Disable Protection on This Page** from the drop-down list. For IE: Click **Show all content** in the **Only secure content is displayed** message bar at the bottom of the page.
NIOS-45598	Network Insight: When a seed router is specified for an IP address that has already been assigned as a fixed address, the IP will still be discovered even if the fixed address is excluded from discovery.
NIOS-45233	Reporting: When you use Microsoft Internet Explorer 10.x and disable "Compatibility View," you may not be able to view reports in the **Reporting** tab. Workaround: In the Internet Explorer 10 browser, go to **Tools** -> **Compatibility View** to enable the feature.

NIOS-45220	When you upgrade from NIOS 5.1r6-12 or earlier releases, the **Try Snapinstall** option may not be available in the bloxTools environment after the upgrade. Workaround: Stop bloxTools service on the member, console connect to the member through the CLI and execute the `set bloxtools reset all` command. Once the reset process is complete, restart the bloxTools service to access the **Try Snapinstall** option.
VLAN-324	If you have assigned multiple VLANs to the LAN1 or LAN2 interfaces on the appliance, you may receive messages about having "multiple interfaces that match the same subnet" during dhcpd process startups or restarts. Note that these are not error messages and no actions are required.
NIOS-44055	If you use certain versions of Mozilla FireFox to run Grid Manager, the auto-detected time zone feature may not function properly even if you have enabled it in your User Profile.
NIOS-43957	When you upgrade from NIOS 6.6.x or earlier releases, the email address in the SOA resource record that was entered in punycode will be converted into IDN (Internationalized Domain Name) after the upgrade. Workaround: Convert the IDN back to punycode using the IDN converter utility through Grid Manager.
NIOS-43569	You may not be able to view reverse-mapping zones in an internal DNS view. Workaround: Set the table size to 10 in **User Profile**, log out, and then log back in to the system again.
NIOS-41136	Reporting: When you use certain versions of Mozilla Firefox and Google Chrome browsers on Windows 7 or Linux, you may not be able to properly print reports.
NIOS-39922	On Trinzic 2200 series appliances, it may take up to three minutes for the LOM (Light On Management) LED to stop blinking after you have disabled the LOM feature.
NIOS-38870	When you change the member type of an appliance from **Infoblox** to **vNIOS**, the appliance might display an error message indicating that all network port settings of the vNIOS member must be changed to **Automatic**. Workaround: Through the Infoblox API, use `Infoblox::Grid::Member` and the functions `lan_port_duplex( )` and `lan_port_speed ( )` to change the network port settings for the vNIOS member.
NIOS-38579	Reporting: If you have a quick filter that includes a filter criterion with report comment equals to a value that NIOS automatically translates to another value, the quick filter may not function properly after an upgrade to NIOS 6.5 or 6.6. NIOS automatically translates the following: "IPAM Utilization" to "DDI Utilization"; "DNS Zone Statistics per DNS View" to "DNS Statistics per DNS View"; "DNS Zone Statistics per DNS Zone" to "DNS Statistics per Zone"; "DNS Member QPS Trend" to "DNS Query Rate by Server" and "DNS Queries per Second Trend" to "DNS Query Rate by Query Type". Workaround 1: Edit the original report comment values to match the translated values. For example, if you have entered "IPAM Utilization" in the comment field of a report, change it to "DDI Utilization." Workaround 2: Edit the quick filter names to match the original comment values. For example, if you have entered "QF1" as a quick filter name and "IPAM Utilization" as the report comment, change the quick filter name to "IPAM Utilization".
NIOS-37415	Users cannot execute Trinzic Automation Engine (TAE) if they log out of NetMRI during an active NetMRI session.
NIOS-33600	There is an issue with SafeNet HSMs in that configuration changes do not immediately take effect, such as when adding a new member to an existing SafeNet HSM Group, deleting a client from the HSM or making member changes. You can perform a forced restart of services to apply the changes immediately.

sNIOS-31864	Modifying a zone from a client increments the zone's serial number even if the zone contents did not change. This causes unnecessary AXFRs to secondary servers and if the zone is served by a Microsoft Server that is managed in read-write mode, it causes extra synchronizations as well.
NIOS-31501	When a Microsoft server is the primary server for a zone and another Microsoft server is hosting the same zone as a stub zone, and the NIOS appliance synchronizes DNS data with only one of these zones, it will synchronize the zone as an authoritative or stub zone, depending on which Microsoft server it synchronizes with first. For more information, please refer to KB article 17593.
NIOS-25064 (45488)	If you configured a member DHCP server to authenticate DHCP clients with a RADIUS authentication server group and RADIUS is disabled (the server group is disabled, all RADIUS servers in the group are disabled, or the member DHCP server was not assigned an authentication server group), NAC filters with "does not equal" rules will always match. Workaround: Do not disable RADIUS.
NIOS-21512 (39917)	When you stop the DNS service of an independent appliance with temporary DNS and DHCP licenses, Grid Manager displays the Restart Services panel regardless of which function you select.
NIOS-21499 (38968)	An admin cannot display DNS views created by other admins during the same browser session. To display the DNS views created by other admins, you must log out and log in again.
NIOS-19853 (31668)	Grid Manager does not display an error when you move a DNS view to a network view that contains a host record that has the same MAC address as a host record in the DNS view that is being moved.
NIOS-19144 (30208)	Grid Manager does not sort columns correctly in the IPAM and Network list panels when the columns contain UTF-8 data.
NIOS-18163 (27831)	The appliance allows users with read-only permission to A records to view DNSSEC resource records as well.
NIOS-17636 (26233)	Syslog messages generated during a TFTP file transfer display the incorrect time zone.
NIOS-17513 (26080)	Adding, updating, or deleting reverse zones could fail due to unsupported PTR records in the root zone.
PAPIPASS-39	When you use Mozilla Firefox 16.x, 17.x, or Mozilla Firefox Beta 18.0b3 browser, the hidden password in the *Add Administrator* Wizard of Grid Manager may disappear when you click the **Password** field after you have confirmed the password. This is a known issue when you use Firefox browsers.
MME-154	When a NIOS user deletes a Microsoft AD domain's primary zones and subzones, NIOS should display a more specific message warning users about the consequences of the operation instead of the general warning message it currently displays.
MME-129	When a Microsoft admin creates a delegation on the Microsoft server and the delegation is synchronized to the NIOS appliance, the glue A record of the delegation name server is synchronized to the appliance as a manually created record. If on the NIOS appliance, an admin changes the IP address on the NS record of the delegation name server, two A glue records are generated: one with the original address, one with the new address. NIOS retains the original glue A record because it's marked as a manually created record, and it can only be changed or deleted either manually on Grid Manager or through the API. When synchronization occurs, the Microsoft server correctly updates the existing glue A record and does not retain the original. Note that NIOS retains the original A record only after the initial update. If you update the A record again, NIOS just updates the existing record without retaining the original.
MME-23	NIOS displays an "Internal Error" message when you try to apply a quick filter for a range that equals 1 when you display a range in the IPv4 Microsoft Superscopes tab.

MME-6	If you add a hostname to the Target field of an SRV record on Grid Manager, when the member synchronizes the SRV record to a Microsoft server, it adds a new SRV record with the hostname instead of modifying the existing record.
MSSS-11 (45296)	When you run a discovery on a network served by Microsoft servers, and Grid Manager discovers a MAC address that does not match any of the fixed addresses associated with an IP address, it reports a conflict and lists the associated fixed address objects in the Related Objects table. You cannot select which fixed address to resolve in the Related Objects table. You can only resolve the conflict for the first address.
VNIOS-36 (41215)	If a virtual NIOS member does not start up due to a license violation, Grid Manager displays the status of the vNIOS member as “online/running” even though the member is not online.