NIOS 7.2.4 Release Notes

NIOS 7.2.4 Release Notes

INTRODUCTION

Infoblox NIOS™ 7.2.x 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:

- NIOS 7.2.x is not supported on the following appliances: IB-250, IB-250-A, IB-500, IB-550, IB-550-A, IB-1000, IB-1050, IB-1050-A, IB-1550, IB-1550-A, IB-1552, IB-1552-A, IB-1852-A, IB-2000, IB-2000-A, IB-VM-250, IB-VM-550, IB-VM-1050, IB-VM-1550, IB-VM-1850, IB-VM-2000, and Trinzic Reporting TR-2000 and TR-2000-A series appliances. You cannot upgrade to NIOS 7.2.x on these appliances. See **Upgrade Guidelines** on page 19 for additional upgrade information.

Supported Platforms

Infoblox NIOS 7.2.x is supported on the following platforms:

- **NIOS Appliances**
  - Infoblox Advanced Appliances: PT-1400, PT-2200, PT-4000, and PT-4000-10GE
  - 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.)
  - Cloud Network Automation: CP-V800, CP-V1400, and CP-V2200
  - Trinzic Reporting: TR-800, TR-1400, TR-2200, and TR-4000
  - DNS Cache Acceleration Appliances: IB-4030 and IB-4030-10GE

- **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 6.0.x, 5.5.x, 5.1.x or 5.0.x installed, and then 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*.

- **vNIOS for Microsoft Server 2008 R2, 2012, and 2012 R2 Hyper-V**
  The Infoblox vNIOS virtual appliance is now available for Windows Server 2008 R2 and Windows Server 2012 and 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*.
  Note: All virtual appliances for reporting purposes are supported only for Windows Server 2012 R2.

- **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*.

- **vNIOS for KVM Hypervisor**
  The Infoblox vNIOS for KVM is a virtual appliance designed for KVM (Kernel-based Virtual Machine) hypervisor and KVM-based OpenStack deployments. The Infoblox vNIOS for KVM functions as a hardware virtual machine guest on the Linux system. It provides core network services and a framework for integrating all components of the modular Infoblox solution. You can configure some of the supported vNIOS for KVM appliances as independent or HA (high availability) Grid Masters, Grid Master Candidates, and Grid members. For information about vNIOS for KVM hypervisor, refer to the *Infoblox Installation Guide for vNIOS for KVM Hypervisor and KVM-based OpenStack*.

- **vNIOS for AWS (Amazon Web Services)**
  The Infoblox vNIOS for AWS is a virtual Infoblox appliance designed for operation as an AMI (Amazon Machine Instance) in Amazon VPCs (Virtual Private Clouds). You can deploy large, robust, manageable and cost effective Infoblox Grids in your AWS cloud, or extend your existing private Infoblox NIOS Grid to your virtual private cloud resources in AWS. You can use vNIOS for AWS virtual appliances to provide enterprise-grade DNS and IPAM services across your AWS VPCs. Instead of manually provisioning IP addresses and DNS name spaces for network devices and interfaces, an Infoblox vNIOS for AWS instance can act as a standalone Grid appliance to provide DNS services in your Amazon VPC, as a virtual cloud Grid member tied to an on-premises (non-Cloud) NIOS Grid, or as a Grid Master synchronizing with other AWS-hosted vNIOS Grid members in your Amazon VPC; and across VPCs or Availability Zones in different Amazon Regions. For more information about vNIOS for AWS, refer to the *Infoblox Installation Guide for vNIOS for AWS*.

The following table shows available vNIOS virtual appliances and their specifications:

Trinzic Series Virtual Appliances	Overall Disk (GB)	# of CPU Cores	Memory Allocation	Virtual CPU Core Frequency	vNIOS for VMware	vNIOS for MS Hyper-V	vNIOS for Xen	vNIOS for KVM	vNIOS for AWS	Supported as Grid Master and Grid Master
IB-VM-100	55	1	1 GB	1300 MHz	✓	✓	✓	✓	×	No
IB-VM-800 (for reporting only; 1 GB daily limit)	300 (Primary & Reporting)	2	Range: 2 – 8 GB Default: 8 GB	3000 MHZ	✓[3]	✓	✓	✓[1]	×	No
IB-VM-800 (for reporting only; 2 GB daily limit)	300 (Primary & Reporting)	2	Range: 4 – 8 GB Default: 8 GB	3000 MHZ	✓[3]	✓	✓	×	×	No
IB-VM-810	55	2	2 GB	2000 MHz	✓	✓	✓	✓	×	No
IB-VM-810	160	2	2 GB	2000 MHz	✓	✓	✓	×	×	Yes[2]
IB-VM-820	55	2	2 GB	3000 MHz	✓	✓	✓	✓	×	No
IB-VM-820	160	2	2 GB	3000 MHz	✓	✓	✓	×	✓	Yes[2]
IB-VM-1400 (for reporting only; 5 GB daily limit)	555 (Primary & Reporting)	4	Default: 8 GB	8000 MHz	✓[3]	✓	×	×	×	No
IB-VM-1410	55	4	8 GB	6000 MHz	✓	✓	✓	×	×	No
IB-VM-1410	160	4	8 GB	6000 MHz	✓	✓	✓	✓	×	Yes[2]
IB-VM-1420	160	4	8 GB	8000 MHz	✓	✓	✓	✓	✓	Yes[2]
IB-VM-2210	160	4	12 GB	12000 MHz	✓	×	✓	✓	×	Yes[2]
IB-VM-2220	160	4	12 GB	12000 MHz	✓	×	✓	✓	✓	Yes[2]

Network Insight Virtual Appliances	Overall Disk (GB)	# of CPU Cores	Memory Allocation	Virtual CPU Core Frequency	vNIOS for VMware	vNIOS for MS Hyper-V	vNIOS for Xen	vNIOS for KVM	vNIOS for AWS	Supported as Grid Master and Grid Master Candidate
ND-VM-800	160	2	8 GB	3000 MHz	✓[3]	✓	✓	×	×	No
ND-VM-1400	160	4	16 GB	8000 MHz	✓[3]	✓	✓	×	×	No
ND-VM-2200	160	4	24 GB	24000 MHz	✓[3]	×	✓	×	×	No
Cloud Platform Virtual Appliances	**Overall Disk (GB)**	**# of CPU Cores**	**Memory Allocation**	**Virtual CPU Core Frequency**	**vNIOS for VMware**	**vNIOS for MS Hyper-V**	**vNIOS for Xen**	**vNIOS for KVM**	**vNIOS for AWS**	**Supported as Grid Master and Grid Master Candidate**
CP-V800	160	2	2 GB	2000 MHz	✓	✓	✓	✓	✓	No
CP-V1400	160	4	8 GB	6000 MHz	✓	✓	✓	✓	✓	No
CP-V2200	160	4	12 GB	12000 MHz	✓	✓	✓	✓	✓	No

NOTES:
[1] For KVM hypervisor only. Not supported for KVM-based OpenStack. Does not support Elastic Scaling.
[2] vNIOS virtual appliance for Hyper-V is not recommended as a Grid Master or Grid Master Candidate. The Identity Mapping feature is not supported on the IB-VM-810 and IB-VM-820 appliances.
[3] Does not support Elastic Scaling.

vNIOS for VMware on Cisco UCS Express/SRE-V

The Infoblox vNIOS for VMware software can 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 2.0 (for ESXi 5.0 and ESXi 6.0). 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 on Cisco 2900 and 3900 series ISRs G2.

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

vNIOS on VMware Virtual Appliances	Disk (GB)	# of CPU Cores	Memory Allocation	Virtual CPU Core Frequency	Cisco SRE 700/710	Cisco SRE 900/910
IB-VM-100	55	1	2 GB	2000 MHz	Yes	Yes
IB-VM-810	55	2	2 GB	2000 MHz	Yes	Yes
IB-VM-810	160	2	2 GB	2000 MHz	Yes	Yes
IB-VM-820	55	2	2 GB	3000 MHz	Yes	Yes
IB-VM-820	160	2	2 GB	3000 MHz	Yes	Yes

Note that all vNIOS for 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 for Riverbed® Steelhead Appliances**

Infoblox has certified the vNIOS for Riverbed software with the following Riverbed Steelhead models and software versions:

Riverbed Models	Supported EX and RiOS versions
EX560, EX760, EX1160, EX1260	EX 1.0 with RiOS 7.0.x EX 2.5 with RiOS 8.0.x EX 3.1 with RiOS 8.5.x

The vNIOS for Riverbed virtual appliance can only operate as an independent Grid member. For additional information, refer to the *Infoblox Installation Guide for vNIOS Software for Riverbed Steelhead Platforms.*

NOTE: You can upgrade a Grid with supported Riverbed virtual members to NIOS 7.x. Ensure that the Riverbed model has 64 bit support.

NIOS 7.2.4 Release Notes

NEW FEATURES

This section lists new features in the 7.x releases.

NIOS 7.2.4

Elastic Scaling for vNIOS for KVM and vNIOS for VMware Appliances

This release adds Elastic Scaling support for the following vNIOS virtual appliances: vNIOS for KVM and vNIOS for VMware. You can now provision and deploy certain models of these virtual appliances as Grid members using Elastic Scaling. For information about supported vNIOS models, see the table on page 4.

NIOS 7.2.0

Infoblox Solution for AWS (Amazon Web Services)

You can deploy Infoblox Grid in Amazon VPCs (Virtual Private Clouds) to leverage the following: DNS service in AWS, IPAM for EC2 instances, automated IP address assignments, DNS records provisioning, and vDiscovery to improve visibility into AWS networks. You can also use the newly developed Elastic Scaling feature to automatically pre-provision and spin up vNIOS virtual cloud appliances in AWS.

Elastic Scaling for vNIOS and Cloud Deployments

Elastic Scaling provides the capability to automatically pre-provision and deploy vNIOS appliances on-demand for IPAM (IP Address Management), DNS, and/or DHCP. Compared to standard appliance deployment and licensing management, you now have the flexibility to purchase multiple service and feature licenses (dynamic licenses) in advance, install and save them in a license pool for future vNIOS or cloud deployments based on your evolving business needs and deploy them as needed. When you remove a vNIOS or cloud appliance from the Grid, the dynamic licenses on the appliance are automatically released and returned to the license pool on the Grid Master for reuse at a later time. Elastic scaling includes a full set of APIs for pre-provisioning, deployment, and de-provisioning vNIOS appliances, making it simple to add or remove DNS or DHCP capacity on-demand to meet changing infrastructure requirements, which is critical for realizing the benefits of dynamic Cloud environments.

vDiscovery

This is an expansion of the former VM discovery capability, in which the NIOS appliance discovers virtual entities on VMware vCenter and vSphere servers, to support discovery of VMs and networks in OpenStack and AWS EC2 environments. You can start a vDiscovery job immediately after you configure it, schedule it for a later date and time, or configure a recurring vDiscovery based on a recurrence pattern enabling NIOS to obtain up-to-date IPAM information from VMware, OpenStack and AWS EC2 environments. vDiscovery imports critical network and system metadata along with VM and IP Address data, enabling NIOS Administrators to have access to the same information through the **Cloud** tab in Grid Manager, which normally would only be available in the VMware, OpenStack, or AWS EC2 consoles.

Enhancements for Infoblox Internal and External DNS Security

- Enables DHCP service to be run on Infoblox Advanced Appliances. You can download and install a DHCP license on the Advanced Appliance to utilize the DHCP service.
- Adds auto threat protection rules that mitigate DHCP DDoS attacks on the Advanced Appliances.
- Support for “smart rate limiting” on networks that use PNAT (port-based NAT) on the Infoblox Advanced Appliance or the IB-4030 running the threat protection service.
- Grid Manager now displays the “Rule Parameters” column for each threat protection rule.

Core NIOS Security

This release adds the following features to the core Infoblox security:

- RRL (Response Rate Limiting) feature for the Infoblox CLI.
- DNS attack mitigation for non-responsive servers through Grid Manager instead of the CLI.
- Bogus query alerting and mitigation through Grid Manager.

Enhancements for Infoblox DNS Firewall

This release adds the following enhancements to the Infoblox DNS Firewall:

- Supports RPZ-Client-IP with Passthru, Block (NXDomain/No Data), and Substituted domain name responses.
- Change to the default behavior of RPZ (Response Policy Zone): no longer recurses for domains that are already in the RPZ feed.

Identity Mapping

The Infoblox Identity Mapping feature integrates with Microsoft's Active Directory to intelligently discover the relationship of network devices and their users (Network Users). This feature empowers DDI administrators with a new level of understanding of how network users consume and interact with the network.
NOTE: Identity Mapping is not supported on the TE-810, TE-820, IB-VM-810 and IB-VM-820 appliances.

DNS and DHCP Service Restart Enhancements

You now have the ability to group DNS and DHCP services for restarting when required. Together with the ability to establish a recurring schedule, this enhancement enables DNS and DHCP service restarts to better comply with operational guidelines. For example, DNS servers can be grouped by a geographic location (such as Eastern US) and a recurring schedule for 2300 EDT, which means all restarts affecting DNS services located in Boston, NYC, and Miami would restart automatically at 2300 EDT.

Global Search Enhancements

There is now a **Basic** search tab that includes the most common search criteria: IP, MAC address, DUID and FQDN. This enhancement simplifies the search process and improves search responses. **Advanced** search now supports global filtering.

NS Group Performance Improvement

You will see improvement in performance when you modify the settings of NS groups that are assigned to a large number of zones. The performance of the following functions also improves when you assign an NS group to a zone, instead of specifying multiple name servers:

- Starting and stopping DNS service
- Re-parenting zones after removing or restoring a zone
- Modifying zone data.

GUI and API Access on LAN1/VIP and MGMT Ports

In previous releases, when the MGMT port was configured for DDI, API and GUI access was only through the MGMT port, not the LAN1 (for standalone) or VIP (for HA) port. This release provides an option to manage GUI and API access through these interfaces simultaneously. To provide GUI access on both interfaces, HTTP service listens on both interface IP addresses. Since API is also through the same HTTP service, this feature provides GUI and API access through both the LAN1/VIP and MGMT interfaces.

Dual Engine DNS for IB-4030-10GE

The Infoblox Dual Engine DNS feature provides the option to switch between BIND and Unbound DNS resolvers for better protection against DNS server targeted attacks and DNS server vulnerabilities. It also improves DNS performance in networks that have lower cache hit ratio.

DNS Cache Acceleration Enhancements

The DNS Cache Acceleration servers now support the following features: Stub Zone, support for clearing a specific cache entry, VLAN2, and NAT Mapping for Port Block Allocation.

Using SHA-2 for Requests to Sign Auto-Generated SSL Certificates

This release adds support for SHA2 algorithms in certificate and CSR generation for use with NIOS. It also adds support for 4096 byte key size.

SHA-2 Algorithms Support

This release adds support for SHA-2 set of digest algorithms in self-signed certificates and in CSR generation for use with HTTPS/SSL certificates. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. But NIOS 'openssl' only supports the first four and it does not support SHA-512/224, SHA-512/256.
This feature adds support for only SHA-256 of the SHA-2 algorithms to generate CSRs and self-signed certificates, in addition to the existing SHA-1 hash algorithm. This feature also adds support for 4096 byte key size, in addition to existing 2048 key size for SHA-256.

DHCP Option Logic Filters

In previous releases, IPv4 logic filters could be applied only at the range level. You can now configure DHCP option logic filters at the member, network, shared network, fixed address, and IPv4 reservation levels.

DHCP Options at the Network Container Level

This release introduces DHCP option support in a network container. In previous releases, you were only able to override a DHCP option defined for networks and shared networks at the Grid or member level. You can now define DHCP options at the network container level. In the inheritance hierarchy, the network container is anchored between the shared network and member.

OID Changes in the OnePlatform MIB

In this release, the following OID numbers have been changed respectively:
From

ibCPU1Temperature 1.3.6.1.4.1.7779.3.1.1.2.1.2.0
ibCPU2Temperature 1.3.6.1.4.1.7779.3.1.1.2.1.3.0

to

ibCPU1Temperature 1.3.6.1.4.1.7779.3.1.1.2.1.17.0
ibCPU2Temperature 1.3.6.1.4.1.7779.3.1.1.2.1.18.0

Note that the old ibCPUTemperature OIDs will be deprecated in NIOS 7.4.

GUI Improvements

This release adds the following enhancements to the Infoblox GUI, Grid Manager:

- You can now display all network containers and networks in the **IPAM** tab without drilling down to specific networks by selecting the newly added flat view option.
- You can group Grid members using extensible attributes in any panels or views that display the members and in the *Grid Status* widget on the Dashboard.
- You can change the setting in the **Grid Properties** tab -> **General** tab -> **Advanced** tab to hide the Grid visualization. This is hidden by default for all new installations.
- You can now specify the minimum value of object counts in the Capacity Report.
- The Recycle Bin now has filters, quick filters, and the Go to function.
- The following improvements to the **Advanced** tab of Global Search:
  - The setting for “Include Extensible Attributes” is persisted per user.
  - You can create quick filters.

- New columns are added for the "Comment" and "Extensible Attributes" values (also available in the **Basic** tab).

NIOS 7.1.0

Infoblox Advanced DNS Protection Enhancements

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

- **Rate Algorithm Parameter for Rate-Limiting Rules:** The new **Rate algorithm** parameter defines how the appliance handles incoming traffic when the traffic exceeds the rate limit (defined in **Packets per second**). You can set this to "blocking" or "rate limiting." The default is "rate limiting." When you set **Rate algorithm** to "blocking," the appliance allows client traffic to go through until it hits the rate limit. It then blocks all traffic for the duration of the drop interval. If client traffic continuously exceeds the rate limit, the appliance continues to block all traffic for subsequent drop intervals without letting through any traffic, which could result in an indefinite traffic blockage. When you set this to "rate limiting," the appliance allows client traffic to go through until traffic hits the rate limit. It then blocks all traffic for the rest of the drop interval. The appliance re-evaluates client traffic at the beginning of each drop interval and repeats the same behavior for subsequent intervals.

  To avoid resource exhaustion and limit frauds, you can limit the query rate for each source IP, and then set **Drop interval** to one second and **Rate algorithm** to "rate limiting," which results in a rate-limiting behavior that allows some traffic to go through before the rest of the traffic is blocked. In this case, the appliance re-evaluates the client behavior every second. If the client traffic exceeds the rate limit, the appliance processes only queries up to the rate limit and drops all excessive queries for the remainder of the second.
- **Updates to DNS Tunneling Rules**: When possible DNS tunneling traffic triggers a DNS tunneling rule, the appliance drops only DNS tunneling response traffic that matches the configured DNS packet size. All other traffic is allowed to go through and processed by subsequent threat protection rules.
- **New Threat Protection Reports**:
  - *Threat Protection Top Rules Logged*: This report lists the top 10 threat protection rules that are triggered by a given source IP within a given time frame.
  - *Threat Protection Top Rules Logged by IP*: This report provides statistics about events being triggered by the top 10 source clients within a given time frame. You can use this report to identify clients that have triggered the most threat protection rules within a given time frame.

New Reports for Infoblox DNS Firewall

This release adds new reports that capture security information so CISO (Chief Information Security Officer) can make executive decisions about the security outlook for their organizations. You can generate the following reports:

- *Top DNS Firewall Hits* report: This report lists the top RPZ rules triggered over a given time frame. It lists information such as RPZ rules, percentage of RPZ rule hits, number of hits per RPZ rule, and description of the threat that triggered the RPZ rules. The default report displays the top 10 RPZ rules triggered within the past week.
- *Malicious Activity by Client* report: This report lists the clients that have the most malicious activities. The default report shows a bar chart that lists clients that have the most total counts of malicious activities that triggered the RPZ rule over a given time frame. The default report displays the top 10 clients within the past week.
- *DNS Firewall Executive Threat* report: This is a predefined custom report that combines the *Top DNS Firewall Hits* and *Malicious Activity by Client* reports. You can download this report in PDF format that includes a three-panel report.

vNIOS Virtual Appliances for KVM Hypervisor

This NIOS release supports the Infoblox vNIOS virtual appliance for KVM (Kernel-based Virtual Machine) hypervisor. The vNIOS for KVM appliance is designed for KVM hypervisor and KVM-based OpenStack deployments. Supported models are IB-VM-800, IB-VM-820, IB-VM-1420, IB-VM-2220, and CP-V1400. You can configure some of the supported vNIOS for KVM models as independent or HA (high availability) Grid Master, Grid Master Candidates, and Grid members. For information about the vNIOS appliance models and their specifications, see the specifications table on page 3. For information about vNIOS for KVM appliances, refer to the *Infoblox Installation Guide for vNIOS for KVM Hypervisor and KVM-based OpenStack*.

Enhancements for the IB-4030 and IB-4030-10GE Appliances

This release adds the following enhancements for the IB-4030 and IB-4030-10GE appliances:

- Preserving the RRset order for cached DNS responses: When a client queries a domain name, the DNS caching appliance returns the A and AAAA records of the domain name in cyclic order by default. You can now override this default behavior if you have enabled and configured (at the Grid level) fixed RRset order for hosts that have multiple addresses. When you override the default behavior and preserve the fixed RRset order for cached DNS responses, the DNS caching appliance returns A and AAAA records associated with domain names in the order they were received from an upstream server.
- Defining sort lists: You can define sort lists for the cached DNS responses on an Infoblox-4030 appliance to prioritize A and AAAA records on certain networks, sorting them to the beginning of the list in the response. For example, you can define a sort list when a recursive server has two interfaces and you want the DNS clients to prefer one interface because it has a faster link.
- VLAN tagging support: The Infoblox-4030 appliance now supports VLAN (Virtual Local Area Network) interfaces on LAN1, LAN2, and HA ports. Only the DNS service can listen on the VLAN interfaces. You can define default routes on VLAN, LAN1 and LAN2 interfaces. Use the `set network` command to set the primary IPv4 and IPv6 LAN1 networks as a tagged or an untagged VLAN interface. To view the VLANs on each port, use the `show interface` command.

Enhancements for NTP Configuration

This NIOS release adds support for the following NTP options based on RFC 5905 (*Network Time Protocol Version 4*):

- **BURST**: You can configure the NTP client to send a burst of eight packets if the external NTP server is reachable and a valid source of synchronization is available. The NTP client transmits each packet at a regular interval of two seconds.
- **IBURST**: You can configure the NTP client to send a burst of eight packets if the external NTP server is not reachable when the client sends the first packet to the server. The NTP client transmits each packet at a regular interval of two seconds.
- **KoD** (Kiss-o'-Death) packet configuration: When an NTP server denies service to an NTP client that has exceeded the rate limit, it typically drops the packets without notifying the client. In this case, the client, unaware of the situation, continues to transmit packets. To notify the client so it either slows down or stops the packet transmission, you can enable the NIOS appliance (when acting as an NTP server) to transmit a KoD packet. This packet contains the stratum field which is set to zero, implying the sent packet was invalid; and the ASCII string that contains RATE in the reference identifier field, indicating the status of the transmitted packet and access control. When the client receives the KoD packet, it may reduce transmission rate or stop packet transmission to the server.

CSV Import Enhancements

This release adds the following enhancements to the CSV import feature:

- New functionality, such as the **Global CSV Export** option, to support the export of multiple CSV objects and the management of CSV export jobs.
- New fields and functions to support Infoblox Migration Wizard, a standalone software tool that facilitates the migration of DNS and DHCP data from Microsoft servers to the Infoblox Grid. For more

information about Infoblox Migration Wizard, refer to the *Infoblox Migration Wizard Administrator Guide*.

Read-only API Access through Grid Master Candidates

You can now enable read-only API access on the Grid Master Candidate. This feature provides scalability for read/write API requests on the Grid Master, which can help improve its performance. Read-only API access is disabled by default for new installations and upgrades to NIOS 7.1.0 from previous releases.

Network Insight: SNMP Traps and Email Notifications for Unmanaged Devices

For Network Insight, you can now configure the appliance to send SNMP and email notifications when it discovers unmanaged devices and networks. You can also manage these notifications by configuring the maximum number of unmanaged objects the appliance detects before it sends notifications and how often it notifies about these events.

Ability to Copy Host Records

You can now copy an existing host record and turn it into a new one. When you copy a host record, other than the new host name and IP address, all DHCP and IPAM configurations, including the MAC address and extensible attributes, apply to the new record.

Enabling and Disabling RPZ Query Name Recursion

Starting with this release, RPZ query name recursion is disabled by default. When RPZ query name recursion is disabled, the DNS recursive name server sends responses for the domains being queried, without forwarding queries to the authoritative name servers. This can speed up recursive RPZ lookups by eliminating unnecessary recursions for domains that are known to be malicious, possibly caused by internal DDoS attacks on the recursive server. You can enable RPZ query name recursion by selecting the **Enable RPZ query name recursion (qname-wait-recurse)** check box. When you select this check box, the appliance performs RPZ query name recursions. You can configure this at the Grid, member, and DNS view levels.

Auto-Provisioning Enhancements

This release adds new CLI commands for managing auto-provisioning, which is disabled by default when you upgrade or downgrade to a NIOS release that includes auto-provisioning. You can now use the following commands to manage auto-provisioning:

- `set auto_provision on|off`: Enables and disables auto-provisioning on the appliance.
- `reset all auto_provision`: Re-establishes factory settings and re-enables auto-provisioning.
- `reset database auto_provision`: Resets the database and re-enables auto-provisioning.

Deleting PTR Records Associated with A or AAAA Records

You can now configure the appliance to confirm whether to delete a PTR record when its corresponding A or AAAA record is being deleted. This feature is valid if you have configured the appliance to automatically generate a PTR record when you create an A or AAAA record.

SNMP Traps for Recursive Clients

You can now enable the appliance to send SNMP traps for recursive clients after you configure the recursive client limit. The appliance sends SNMP traps when the number of recursive client queries exceeds the configured thresholds. Enabling this feature can help you identify possible DNS flood attacks on the DNS recursive server.

Reverse-Mapping Zone Management at the arpa Level

You can now add arpa as the top-level forward-mapping zone and manage resource records within the zone. You can also add reverse-mapping zones in-addr.arpa (for IPv4) and ip6.arpa (for IPv6) to the arpa zone and manage them accordingly. Note that you must manually create these zones since they are not auto-created.

Ability to Search DHCP Option 82 Using Infoblox API and RESTful API

This release adds the ability to search for DHCP option 82 through the Infoblox API and RESTful API. For information, refer to the *Infoblox API Documentation* and *Infoblox WAPI Documentation*.

Support for Infoblox Migration Wizard

Infoblox Migration Wizard is a standalone software tool that facilitates the migration of DNS and DHCP data from Microsoft servers to the Infoblox Grid. This tool synchronizes DNS and DHCP data from Microsoft servers and generates a CSV file based on conversion rules you set up through the tool. You can then import the CSV data to the Infoblox Grid through CSV import.
You can download the Infoblox Migration Wizard software package from the Infoblox Support website. You must log in using the user ID and password that you receive when you register your product online at http://www.infoblox.com/support/customer/evaluation-and-registration.

NIOS 7.0.2

VM Address History Report

This release adds the *VM Address History* Report for Cloud Network Automation. You can generate this report to view activities over time for specific VM interfaces in the cloud environment. This report lists information such as IP address, Action, MAC address, Port ID, FQDN, VM Name, Network, Tenant ID, and other fields associated with the VM interfaces.

Support for Infoblox IPAM Plug-In for VMware as a Cloud Adapter

This NIOS release supports the Infoblox IPAM Plug-In for VMware version 3.0.0 as a cloud adapter for Cloud Network Automation. You can install and configure the IPAM Plug-In for VMware in your cloud environment and use it as a cloud adapter to send cloud API calls to the Infoblox Grid or standalone Grid Master. For information about the plug-in and how to configure it, refer to the *Infoblox IPAM Plug-In for VMware User's Guide version 3.0.0*, available on the Support site.

NIOS 7.0.0

Cloud Network Automation

The Infoblox Cloud Network Automation solution automates IPAM (IP address management) for physical and virtual network devices on your CMP (Cloud Management Platform). Instead of manually provisioning IP addresses and DNS name spaces for network devices and interfaces, you can use Cloud Network Automation to provision and manage IPAM, DNS, and DHCP within the Grid automatically as VMs (Virtual Machines) are created and destroyed. When your Cloud consists of a large number of servers and VMs (virtual machines) that have multiple associated network interfaces, manually provisioning and de-provisioning IP addresses and managing DNS and DHCP data can be error-prone and time consuming. Utilizing Cloud Network Automation minimizes human errors by streamlining IP Address and DNS record management, improves visibility of your cloud networks, and maximizes the flexibility, efficiency, and agility of your cloud environment.

Cloud Network Automation includes two components: the Grid Master that has a Cloud Network Automation license installed and one or more Cloud Platform Appliances. The Cloud Network Automation license enables visibility and reporting on cloud tenant, network, VM IP address, and DNS record allocation. Cloud Platform Appliances enable processing of API requests from your CMP locally on the same appliances that serve DNS and DHCP to your cloud. These appliances provide local survivability and additional scalability of Cloud API

requests within your data centers in addition to the visibility provided by the Cloud Network Automation license on the Grid Master.

DNS Traffic Control

Infoblox DNS Traffic Control provides a load balancing solution by adjusting DNS responses based on DNS query source IP, server availability, and network topology. Through DNS Traffic Control, you can set up multiple global sites and configure supported objects and load balancing methods to direct responses to the best available servers.

Support for IPv6 Grid

The Infoblox appliance now supports IPv6 networking configuration in most deployments. You can deploy a Grid and configure a Grid Master, Grid Member, reporting member and an HA pair in one of the following modes: IPv4 only, IPv6 only, or IPv4 and IPv6 dual mode. You can also configure the default communication protocol settings using IPv4 or IPv6. In addition, services and functionality such as NTP service, DNS Firewall, and admin notifications now support both IPv4 and IPv6 addresses. In addition, Grid communication can now support IPv6 only, and you can configure an appliance with only IPv6 addresses (no IPv4 addresses are required).

Support for Microsoft Sites

This release enhances the Microsoft Management solution by adding support for managing Microsoft Active Directory Sites and Subnets on Microsoft servers through Grid Manager.

DNS Firewall Enhancements

This release adds the following enhancements for DNS Firewall:

- Threat severity levels for RPZ zones
- Threat details in the syslog
- Categorization and filtering for DNS and Advanced DNS Protection syslog messages
- Severity level in the DNS Top RPZ Hits report

Automated Mitigation of Phantom Domain Attacks

This release provides a few CLI commands for mitigating phantom domain attacks in which a flood of queries are sent to resolve non-existent domains. When phantom domain attacks happen, the recursive server continues to query non-responsive servers, spending valuable resources waiting for responses. When resources are fully consumed, the recursive server may drop legitimate queries, causing serious performance issues. To mitigate phantom domain attacks, you can use the following CLI commands to control queries to non-responsive servers: `set holddown`, `set fetches_per_server`, `set fetches_per_zone`, and `set recursion_query_timeout`. For information about these commands, refer to the *Infoblox CLI Guide*.

DNSSEC Enhancement

You can now add multiple cryptographic algorithms that the Grid Master uses when it generates the KSK and ZSK. When you add multiple algorithms at the Grid level, you can override them at the zone level. By default, the appliance uses RSA/SHA1 for both KSK and ZSK. You can now add DSA, RSA/MD5, RSA/SHA1, RSA/SHA-256, or RSA/SHA-512 algorithms.

Configuring Fixed Addresses without Restarting DHCP Service

When you configure or modify a fixed address, a DHCP service restart is required by default in order for the new configuration to take effect. You can now override this default behavior by enabling the appliance to take immediate action without restarting DHCP service when you configure or modify a fixed address that is outside a DHCP range. You can enable this feature at the Grid or member level. For Cloud Network Automation deployment, this feature is automatically enabled on the Cloud Platform Appliance that has a valid Cloud Platform license installed.

Ignoring MAC Addresses for New Leases

In addition to the UID (unique client identifier), you can now set the DHCP server to ignore the MAC address (hardware address) of a DHCP client when it places a request to the DHCP server for a new lease. When you configure the appliance to ignore the MAC addresses of DHCP clients, you can specify up to 10 MAC addresses to be ignored.

Name Server Groups for Delegated Zones

When you configure a name server group, you can now create a set of external name servers as a delegation name server group and assign it to delegated zones. Specifying a single delegation name server group instead of configuring multiple name servers individually for delegated zones can significantly reduce configuration efforts.

Network Insight Assets for Trunk Reports

Device discovery now includes in the **Asset** tab all hosts (physical and virtual) connected to a trunk port.

Reporting Enhancement

This release adds the capability to email reporting search results.

Infoblox API and RESTful API Enhancement

This release adds newly supported objects for the API and RESTful API.

CHANGES TO DEFAULT BEHAVIOR

This section lists changes to default behavior in NIOS 7.x releases.

NIOS 7.2.x Releases

- Starting with NIOS 7.2.3, you can add up to 200 sort lists (instead of 50) on the IB-4030 appliance.
- In previous releases, when you used DNAME in your configuration, querying a DNS zone returned the A record. In NIOS 7.2.x when DNAME configuration is in effect, querying a DNS zone no long returns the A record, instead it follows the DNAME redirection.
- The following CLI commands have been deprecated: `set holddown`, `set fetches_per_server`, `set fetches_per_zone`, and `set recursion_query_timeout`. You can now use configurable parameters to mitigate bogus domain attacks through Grid Manager.
- In this release, the former VM Discovery is now called vDiscovery and has been extended to support discovery of VMs and networks in OpenStack and AWS EC2 environments. vDiscovery uses SSL certificate validation for all discovery connections.
  NOTE: When discovering VMware endpoint servers, ensure that you upload a self-signed certificate to the Infoblox certification database. Otherwise, VMware connections might fail.
- In this release, the OID numbers for the following have been changed respectively:
  ibCPU1Temperature 1.3.6.1.4.1.7779.3.1.1.2.1.2.0
  ibCPU2Temperature 1.3.6.1.4.1.7779.3.1.1.2.1.3.0
  to
  ibCPU1Temperature 1.3.6.1.4.1.7779.3.1.1.2.1.17.0
  ibCPU2Temperature 1.3.6.1.4.1.7779.3.1.1.2.1.18.0
- CSRs (Certificate Signing Requests) and self-signed certificates now have new defaults. They are defaulted to SHA-256 algorithm with 2048 key size instead of SHA-1 with 2048 key size.

- Infoblox DNS Firewall: RPZ (Response Policy Zone) no longer recurses for domains that are already in the RPZ feed.

NIOS 7.1.x Releases

- In previous releases, a forward-mapping zone defined using the wildcard character asterisk (*) was used for forwarding to a proxy DNS server for records that did not fall under the main authoritative zone. Queries that contain these records were forwarded to the proxy server for responses. Starting with this release, this configuration is invalid.
- Infoblox Advanced DNS Protection: For threat protection rules that contain the **Packets per second** parameter, a new parameter **Rate algorithm** is added. The default for **Rate algorithm** is set to "rate-limiting," which provides a rate-limiting behavior that allows some traffic to go through before the rest of the traffic is dropped for each drop interval. In previous releases however, these rules adopted the "blocking" behavior in which the appliance allows client traffic to go through until it hits the rate limit. It then blocks all traffic for the duration of the drop interval. If client traffic continuously exceeds the rate limit, the appliance continues to block all traffic for subsequent drop intervals without letting through any traffic, which could result in an indefinite traffic blockage. You can change the parameter from "rate-limiting" to "blocking" for any affected rules after an upgrade.
- For CSV Import, the "use_known_clients" and "use_unknown_clients" fields have been deprecated and merged into the "known_clients_option" and "unknown_clients_option" fields respectively.
- In previous releases, when client traffic triggered DNS tunneling rules, all traffic from the offending client was blocked. Starting with this release, only DNS tunneling response traffic that matches the configured DNS packet size is blocked when these rules are triggered. All other traffic is processed by subsequent threat protection rules.
- In previous releases, there was no limit to the number of RPZs (Response Policy Zones) you could configure. Starting with NIOS 7.1.0, you can add up to a total of 32 RPZs, including local and FireEye integrated RPZs. The appliance returns an error when you try to add more than 32 RPZs. If you have more than 32 RPZs configured in a previous NIOS release, the appliance returns an error in the Upgrade Test when you upgrade to NIOS 7.1.0 and later.
- In previous releases, RPZ query name recursion was enabled by default. The DNS recursive name server performed RPZ recursive lookups for the fully qualified domain name that was part of an RPZ. Starting with NIOS 7.1.0, RPZ query name recursion is disabled by default for all new installations and upgrades. When RPZ query name recursion is disabled, the DNS recursive name server sends responses for the domains being queried, without forwarding queries to the authoritative name servers. This can speed up recursive RPZ lookups by eliminating unnecessary recursions for domains that are known to be malicious, possibly caused by internal DDoS attacks on the recursive server.
  NOTE: Queries to domain names that end with "rpz-xxx" (where xxx can be one of the following: ip, client-ip, nsdname, or nsip) might hit an RPZ rule before recursion is complete even when the queries do not match any CLIENT-IP or QNAME rules.

NIOS 7.0.x Releases

- Starting with NIOS 7.0.0, you must have IPv6 addresses for both nodes in an HA pair if one of them has an IPv6 address. This was optional in previous releases.
- In previous releases when you apply a non-global DHCP option filter to a DHCP range, the appliance may return option 43 in the response. Starting with 7.0.0, the appliance does not return option 43 in any responses when you apply a non-global DHCP option filter to a range.

CHANGES TO Infoblox API and RESTful API (WAPI)

This section lists changes made to the Infoblox API and RESTful API in NIOS releases. For detailed information about the supported methods and objects, refer to the latest versions of the *Infoblox API Documentation* and the *Infoblox WAPI Documentation*, available through the NIOS products and on the Infoblox Support web site.

The latest available WAPI version is 2.2.2. This release adds support for the Grid upgrade and join operations. For information, refer to the WAPI documentation for the "grid" and "fileop" objects.

This NIOS release supports the following WAPI versions: 1.0, 1.1, 1.2, 1.2.1, 1.3, 1.4, 1.4.1, 1.4.2, 1.5, 1.6, 1.6.1, 1.7, 1.7.1, 1.7.2, 1.7.3, 1.7.4, 2.0, 2.1, 2.1.1, 2.2, 2.2.1, 2.2.2.

WAPI Deprecation and Backward Compatibility Policy

This policy covers the interfaces exposed by the Infoblox WAPI and the protocol used to communicate with it.

Unless explicitly stated in the release notes, previously available WAPI versions are intended to remain accessible and operative with later versions.

The planned deprecation of a given version of the WAPI will normally be announced in the release notes at least one year in advance. Upon deprecation, the announced WAPI version and all prior versions will no longer be supported in subsequent releases. For example, if the current WAPI release is v3.4 and the release notes contain an announcement of the v1.5 deprecation, v1.4 and v1.5 API requests would continue to work with later releases for one year from the announcement date. After that, some or all requests for these deprecated versions may not work with versions later than v1.5. API requests adherent to versions later than v1.5 (v2.0 for example) would continue to work with subsequent releases. Infoblox seeks to avoid any deprecation that has not been announced in advance, however product modifications and enhancements may affect specific API requests without a prior announcement; Infoblox does not warrant that all API requests will be unaffected by future releases. This policy applies to both major and minor versions of the WAPI. Infoblox reserves the right to change this policy.

NIOS 7.2.x Releases

WAPI new objects:

- vdiscoverytask - object represents vDiscovery Task
- nsgroup – DNS name server group object
- record:rpz:a - Response Policy Zone Substitute A Record Rule object
- record:rpz:a:ipaddress - Response Policy Zone Substitute IPv4 Address Rule object
- record:rpz:aaaa - Response Policy Zone Substitute AAAA Record Rule object
- record:rpz:aaaa:ipaddress - Response Policy Zone Substitute IPv6 Address Rule object
- record:rpz:cname - DNS Response Policy Zone CNAME record object
- record:rpz:cname:clientipaddress - DNS RPZ CNAMEClientIpAddress record object
- record:rpz:cname:clientipaddressdn - Substitute Domain Name Based on Client IP Address rule object
- record:rpz:cname:ipaddress - DNS RPZ CNAMEIpAddress record object
- record:rpz:cname:ipaddressdn - Substitute Domain Name Based on IP Address rule object
- record:rpz:mx - Response Policy Zone Substitute MX Record Rule object
- record:rpz:naptr - Response Policy Zone Substitute NAPTR Record Rule object
- record:rpz:ptr - Response Policy Zone Substitute PTR Record Rule object
- record:rpz:srv - Response Policy Zone Substitute SRV Record Rule object
- record:rpz:txt - Response Policy Zone Substitute TXT Record Rule object
- zone_rp - DNS Response Policy Zone object
- networkuser - Network User

- msserver - Microsoft Server
- msserver:dhcp - Microsoft Server DHCP properties
- msserver:dns - Microsoft Server DNS properties
- grid:servicerestart:group - Service Restart Group
- grid:servicerestart:status - Restart Status
- grid:servicerestart:request - Restart Request
- grid:servicerestart:group:order - Restart Group Order
- member:license - Member License
- grid:license_pool - Grid License Pool
- grid:license_pool_container - Grid License Pool Container
- grid:cloudapi:vm - Grid Cloud API virtual machine

WAPI objects with changed/enhanced functionality:

- view - added 'match-recursive-only' option.
- discovery data structure - extended with new attributes.
- member:dhcpproperties - added the enable_dhcp field.
- member:dns - added the enable_dns field.
- member - create, update, and delete enabled for this object. Added support of new fields and functions, most of the existing fields made read-write.
- extensibleattributedef – create, update, and delete enabled for this object. Added support of new fields. Most of the existing fields were also made read-write.
- networkcontainer/ipv6networkcontainer - added support for DHCP options.
- Search - added support for targeted searches by DNS name, DUID, IP address, or MAC address.

Supported Perl and Dependency Versions for the Infoblox API

OS	Perl Version	Crypt::SSLeay Version	LWP::UserAgent Version	XML::Parser Version	Net::INET6Glue Version
Microsoft Windows 8.1®	5.22.0 5.12.3	0.72	6.13	2.44	0.603
Microsoft Windows 8®	5.22.0	0.72	6.13	2.44	0.603
Microsoft Windows 7®	5.22.0 5.20.2	0.72	6.13	2.44	0.603
Red Hat® Enterprise Linux® 7.1	5.16.3	0.72	6.13	2.44	0.603
Fedora core 2.6.25.6-45.fc14.i686	5.12.3	0.72	6.13	2.44	0.603
Ubuntu x86_64 GNU/Linux	5.18.2	0.72	6.13	2.44	0.603
Apple® Mac OS X 10.10.3	5.18.2	0.72	6.13	2.44	0.603
Apple® Mac OS X 10.9.5	5.22.0 5.16.2	0.72	6.13	2.44	0.603

NIOS 7.0.x Releases

- When executing a RESTful API request from version 2.0 and later, the XML data format has been updated to accommodate tag names (used primarily in extensible attributes) that contain spaces and/or invalid XML characters.

NIOS 6.x Releases

- The RESTful API (WAPI) sample code advises using 'curl -k3' to access the RESTful API through SSLv3. SSLv3 is no longer supported, and the –k3 option in curl is no longer supported. To correctly use curl to access the RESTful API, specify 'curl -k1' to force the use of TLS.
- 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

  The API also supports multiple TSIG keys. To use a keytab, you must 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.
- The following objects have been deprecated in the Infoblox API:
  - `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.
- The Infoblox::Grid::Admin::User object password method and the Infoblox::Grid object secret method have been modified to adhere to Infoblox security policies.
- 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*.

UPGRADE GUIDELINES

Upgrading to NIOS 7.2.x

- In a Multi-Grid configuration, upgrading to NIOS 7.2.0 might fail if there is a Cloud Platform member in the sub Grid.
- You cannot upgrade to NIOS 7.x on the following appliances: IB-250-A, IB-550-A, IB-1050-A, IB-1550-A, IB-1552-A, IB-1852-A, IB-2000, IB-2000-A, IB-VM-250, IB-VM-550, IB-VM-1050, IB-VM-1550, IB-VM-1850, IB-VM-2000, and Trinzic Reporting TR-2000 series appliances. For information about supported platforms, see **Supported Platforms** on page 1.
- If your Grid consists of RSP (Riverbed Services Platform) virtual members, upgrading to NIOS 7.x and later will fail. For information about which Riverbed virtual members are supported, see the **vNIOS on Riverbed® Steelhead Appliances** section on page 5.
- Note the following if you have scheduling settings configured for discovery, blackout periods, port polling and threat protection ruleset updates before an upgrade:

  - The appliance does not account for non-UTC time zones and DTS (Daylight Savings Time) in your scheduling settings after an upgrade. To avoid time shifts in your schedules, ensure that you update all scheduling settings for these features after the upgrade.

- Scheduled full upgrades have the following restrictions:
  - Add, modify, or delete DNS zones that are assigned to an NS group or member.
  - Add, modify, or delete any name server groups.
  - Start or stop DNS service.
  - Perform service restarts from Grid Manager.

- When you upgrade to NIOS 7.2.x, RPZ query name recursion (qname-write-recurse) is disabled by default.

- When you use vDiscovery to discover VMware endpoint servers, ensure that you upload a self-signed certificate to the Infoblox certification database. Otherwise, VMware connections might fail.

Upgrading to NIOS 7.0.x

Note the following for IPv6 Grid support:

- If your Grid Master is configured with an IPv6 VIP, all Grid Master Candidates must also include an IPv6 VIP. For an HA pair, both nodes of the HA pair must have IPv6 addresses for the Grid Master and the Grid Master Candidate.
- After you upgrade to NIOS 7.0.x, Infoblox recommends that you back up the configuration after you change network connectivity to a different mode (IPv4, IPv6, or IPv4 and IPv6 dual mode). Restoring an old backup by performing a forced restore may prevent some Grid members from rejoining the Grid after the restore.
- IPv6-only configuration does not support the following:
  - HSM
  - LCD
  - NAT groups
  - OSPF and BGP

When you schedule a full upgrade from a previous release to NIOS 7.0.x, the following DNSSEC limitations are applicable:

- 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.
- When you upgrade, 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. 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. 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.

NIOS 7.2.4 Release Notes

BEFORE YOU INSTALL

To ensure that new features and enhancements operate properly and smoothly, Infoblox recommends that you evaluate the capacity on your Grid and review the upgrade guidelines 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.

Following is a list of upgrade and revert paths. You can also schedule a full upgrade from these releases.

7.2.3 and earlier 7.2.x releases
7.1.7 and earlier 7.1.x releases
7.0.7 and earlier 7.0.x releases
6.12.13 and earlier 6.12.x releases
6.11.12 and earlier 6.11.x releases
6.10.14 and earlier 6.10.x releases
6.10.203 and earlier 6.10.2xx releases
6.9.0
6.9.201-LD and 6.9.200-LD releases
6.8.13 and earlier 6.8.x releases
6.7.9 and earlier 6.7.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 8.1 and 8.0®	Microsoft Internet Explorer® 11.x*, 10.x* Mozilla Firefox 37.x, 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 41, 40, 37.x, 36.x, 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 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x
Microsoft Windows XP® (SP2+)	Microsoft Internet Explorer 7.x and 8.x Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x
Red Hat® Enterprise Linux® 7.x	Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x
Red Hat® Enterprise Linux® 6.x	Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x

Red Hat® Enterprise Linux 5.x	Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x
Apple® Mac OS X 10.10.x	Safari 8.x, 7.x Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x
Apple® Mac OS X 10.9.x	Safari 7.x Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x
Apple® Mac OS X 10.8.x	Safari 6.x Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x
Apple® Mac OS X 10.7.x	Safari 5.x Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x
Apple® Mac OS X 10.6.x	Safari 5.x Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 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.

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://*<IPv4 address or hostname of your NIOS appliance> or https://[IPv6 address] 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 the past 12 months. For vulnerabilities that are not listed in this section, refer to Infoblox KB #2899. 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-2015-8000
If responses from upstream servers contained an invalid class parameter for certain record types, DNS service might terminate with an assertion failure.

CERT VULNERABILITY NOTE CVE-2015-5986
An incorrect boundary check could cause DNS service to terminate due to a REQUIRE assertion failure. An attacker could deliberately exploit this by providing a maliciously constructed DNS response to a query.

CERT VULNERABILITY NOTE CVE-2015-5722
Parsing a malformed DNSSEC key could cause a validating resolver to exit due to a failed assertion. A remote attacker could deliberately trigger this condition by using a query that required a response from a zone containing a deliberately malformed key.

CERT VULNERABILITY NOTE CVE-2015-5477
A remotely exploitable denial-of-service vulnerability that exists in all versions of BIND 9 currently supported. It was introduced in the changes between BIND 9.0.0 and BIND 9.0.1.

CERT VULNERABILITY NOTE CVE-2015-1789
The X509_cmp_time function in crypto/x509/x509_vfy.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allowed remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1_TIME data, as demonstrated by an attack against a server that supported client authentication with a custom verification callback.

CERT VULNERABILITY NOTE CVE-2015-1790
The PKCS7_dataDecodefunction in crypto/pkcs7/pk7_doit.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allowed remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that used ASN.1 encoding and lacks inner EncryptedContent data.

CERT VULNERABILITY NOTE CVE-2015-1792
The do_free_upto function in crypto/cms/cms_smime.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allowed remote attackers to cause a denial of service (infinite loop) via vectors that triggered a NULL value of a BIO data structure, as demonstrated by an unrecognized X.660 OID for a hash function.

CERT VULNERABILITY NOTE CVE-2015-1781
A buffer overflow flaw was found in the way glibc's gethostbyname_r() and other related functions computed the size of a buffer when passed a misaligned buffer as input. An attacker able to make an application call any of these functions with a misaligned buffer could use this flaw to crash the application or, potentially, execute arbitrary code with the permissions of the user running the application.

CERT VULNERABILITY NOTE CVE-2015-4620
A recursive resolver configured to perform DNSSEC validation, with a root trust anchor defined, could be deliberately crashed by an attacker who could cause a query to be performed against a maliciously constructed zone.

CERT VULNERABILITY NOTE CVE-2015-0235
Addressed an internal issue in C library (GNU C Library gethostbyname*). Although it was not possible to exploit this as a security issue in NIOS, it could cause some incorrect error conditions and messages while administering the product.

CERT VULNERABILITY NOTE CVE-2014-9298
An attacker could bypass source IP restrictions and send malicious control and configuration packets by spoofing ::1 addresses because NTP's access control was based on a source IP address.

CERT VULNERABILITY NOTE CVE-2014-8500
Failure to place limits on delegation chaining could allow an attacker to crash named or cause memory exhaustion by causing the name server to issue unlimited queries in an attempt to follow the delegation.

CERT VULNERABILITY NOTE CVE-2014-8104
The OpenVPN community issued a patch to address a vulnerability in which remote authenticated users could cause a critical denial of service on Open VPN servers through a small control channel packet.

CERT VULNERABILITY NOTE CVE-2014-3566
SSL3 is vulnerable to man-in-the-middle-attacks. SSL3 is disabled in NIOS, and connections must use TLSv1 (which is already used by all supported browsers).

CERT VULNERABILITY NOTE CVE-2014-3567
A denial of service vulnerability that is related to session tickets memory leaks.

CERT VULNERABILITY NOTE CVE-2014-7187
Off-by-one error in the read_token_word function in parse.y in GNU BASH through v. 4.3 allowed remote attackers to cause a denial of service (out-of-bounds array access and application crash) or possibly an unspecified impact through deeply nested for loops (also known as the "word_lineno" issue).

CERT VULNERABILITY NOTE CVE-2014-7186
The redirection implementation in parse.y in GNU BASH through v. 4.3 allowed remote attackers to cause a denial of service (out-of-bounds array access and application crash) or possibly an unspecified impact through the "redir_stack" issue.

CERT VULNERABILITY NOTE CVE-2014-6271, CVE-3014-6277, CVE-2014-6278, AND CVE-2014-7169
GNU Bash through v. 4.3 processed trailing strings after function definitions in the values of environment variables, which allowed remote attackers to execute arbitrary code via a crafted environment (also known as the "ShellShock" vulnerability)."

CERT VULNERABILITY NOTE CVE-2014-3470
Enabling anonymous ECDH cipher suites on TLS clients could cause a denial of service.

CERT VULNERABILITY NOTE CVE-2014-0224
A specially crafted handshake packet could force the use of weak keying material in the SSL/TLS clients, allowing a man-in-the-middle (MITM) attack to decrypt and modify traffic between a client and a server.

CERT VULNERABILITY NOTE CVE-2014-0221
Remote attackers could utilize DTLS hello message in an invalid DTLS handshake to cause a denial of service.

CERT VULNERABILITY NOTE CVE-2014-0198
Enabling **SSL_MODE_RELEASE_BUFFERS** failed to manage buffer pointer during certain recursive calls that could cause a denial of service.

CERT VULNERABILITY NOTE CVE-2014-0195
Remote attackers could trigger buffer overrun attack through invalid DTLS fragments to an OpenSSL DTLS client or server, resulting in a denial of service.

CERT VULNERABILITY NOTE CVE-2014-0591
A crafted query against an NSEC3-signed zone could cause the named process to terminate.

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 33.

Fixed in 7.2.4

ID	Severity	Summary
NIOS-56643	Critical	Grid members communicating with the Grid Master through the MGMT port that was hardcoded with port speed and duplex settings might fail to join the Grid after upgrading to the latest NIOS 7.2.x from earlier releases.
NIOS-56423	Critical	Addressed the following vulnerability: CVE-2015-8000: If responses from upstream servers contained an invalid class parameter for certain record types, DNS service might terminate with an assertion failure.
NIOS-55882	Critical	When logging in from the serial console, the primary TACACS authentication failed while using an RSA token.
NIOS-55872	Critical	Observed a reduction in GUI performance for superusers.
NIOS-55757	Critical	This release addresses the change of IPv4 and IPv6 addresses for the DNS root zone H.ROOT-SERVERS.NET.

ID	Severity	Summary
NIOS-56218	Major	Some IB-4030 appliances in the Grid experienced intermittent latency peaks in DNS query responses.

Fixed in 7.2.3

ID	Severity	Summary
NIOS-56280	Critical	Under certain circumstances, the appliance could experience intermittent DNS issues due to a large number of recursive queries.
NIOS-56036	Critical	Under certain circumstances, DHCP failover peers stayed in the “Communication Interrupt” state even when connection was established and DHCP service was restored.
NIOS-55847	Critical	An RPZ (Response Policy Zone) was not properly transferred to the Grid Secondary due to missing NS records in the zone.
NIOS-55614	Critical	After performing a “reset all” on the appliance, Grid Manager became unavailable.

NIOS-55491	Critical	Grid members might not be able to communicate with the Grid Master when port speed was configured to 10/100 Full Duplex instead of auto-negotiate.
NIOS-55152	Critical	The appliance encountered false RAID array warning messages.
NIOS-55050	Critical	The appliance experienced high disk utilization due to data buildup in the reporting directory.
NIOS-53494	Critical	After an upgrade to a NIOS release that supports the configuration of multiple primaries (MMDNS support), you might notice DNS response latency for bulk host record queries. While authoritative query performance had greatly increased in MMDNS releases, non-cached (first pass) query performance for bulk host RRs in zones that contained a large number of bulk hosts (e.g. in the thousands) decreased.
NIOS-53146	Critical	NIOS failed to return a normalized DNAME in lower case for the PTR record, causing a DNS service outage.

NIOS-56114 NIOS-56051	Major	Under certain circumstances, upgrade to NIOS 7.2.2 failed with an “integrity check” error.
NIOS-56100	Major	DNS service failed to start due to an undefined ACL syntax error.
NIOS-55986	Major	The appliance stopped counting DNS queries after an upgrade even though monitoring was enabled.
NIOS-55977	Major	In a configuration that supported multiple primaries for a zone (MMDNS support), DDNS updates sent by one of the Grid members were not resolved for a few days.
NIOS-55855	Major	The appliance was unable to load Global Smart Folders; and the folders were marked as invalid in Grid Manager.
NIOS-55833	Major	The *DNS Query Rate by Server/Server Group* report might display incorrect data on the IB-4030 appliance due to data parsing issues.
NIOS-55688	Major	On a Network Insight member, the swap space usage increased unexpectedly.
NIOS-55685	Major	WAPI requests for discovered data could fail if the queried objects did not have any discovered data for display.
NIOS-55583	Minor	The SNMP values were swapped between the active and passive nodes of an HA pair.
NIOS-55549	Major	Updated the documentation to include a warning about using the “Unlimited Lease Time” feature.
NIOS-55497	Major	WAPI: The pxe_lease_time option could only be used to modify an existing setting. Users could not use this option to configure new settings for any objects except for host records that were enabled for DHCP.
NIOS-55489	Major	The FTP server failed to provide configuration files for VoIP phones after a PBX reset, causing service outage.
NIOS-55399	Major	Zone transfers between the lead secondary and the PT Grid member functioned only in the monitoring mode. The zone transfers did not happen in the block mode.
NIOS-55337	Major	The NTP service encountered segmentation faults.
NIOS-55284	Minor	Selecting a network view in the *Network View Selector* could slow down some operations if the page size for the selector was configured for a larger value.

NIOS-55218	Major	Grid Master failed to display reports due to report timeouts, despite proper communications between the forwarder and indexer.
NIOS-55141	Major	IB-4030 cache hit rate statistics were not directed to the reporting server due to some hardware format issues.
NIOS-55120	Major	Under certain circumstances, DHCP service outage occurred.
NIOS-55079	Major	Under certain circumstances, Microsoft synchronization failed for specific servers.
NIOS-55059	Major	The passive node of an HA Grid Master encountered a replication failure due to a heartbeat timeout on the active node.
NIOS-55040	Major	The appliance failed to forward Cache Hit Rate statistics to the Reporting server.
NIOS-54407	Major	The DHCP server was unable to update DNS entries and received REFUSED responses.
NIOS-55591	Minor	Unable to change permissions for FTP file distributions; and no additional details were logged to the debug log or the infoblox.log.
NIOS-53598	Minor	Grid Manager performance was affected when adding more than one record to a large DNS zone.
NIOS-56200	Enhance	This release increases the supported number of sort lists from 50 to 200 on the IB-4030 appliance.
NIOS-55574	Enhance	This release adds a CLI command so you can enable or disable the match-recursive-only option for a specific DNS view on a specific member.

Fixed in 7.2.2

ID	Severity	Summary
NIOS-55860	Critical	Unable to view syslog messages on the appliance after an auto-synchronization.

NIOS-55851	Major	When starting up a vNIOS for KVM instance in NIOS 7.2.1, the vNIOS instance continued to reboot.

Fixed in 7.2.1

ID	Severity	Summary
NIOS-55422	Critical	Addressed the following vulnerabilities: CVE-2015-5986: An incorrect boundary check could cause DNS service to terminate due to a REQUIRE assertion failure. An attacker could deliberately exploit this by providing a maliciously constructed DNS response to a query. CVE-2015-5722: Parsing a malformed DNSSEC key could cause a validating resolver to exit due to a failed assertion. A remote attacker could deliberately trigger this condition by using a query that required a response from a zone containing a deliberately malformed key.

NIOS-55545	Major	When an external syslog server configured to use TCP became unreachable (e.g. because the syslog server crashes or TCP buffer overflows), DNS and DHCP service outage on the appliance could happen.

Fixed in 7.2.0

ID	Severity	Summary
NIOS-52529	Critical	Under certain circumstances, a Microsoft server could not synchronize properly if it was assigned to an Infoblox managing member.
NIOS-53522	Critical	During a scheduled full upgrade, the primary name server was not sending NOTIFYs to secondaries when resource records were added or deleted through Grid Manager or the API. This issue could be exposed only during a scheduled full upgrade when the primary DNS server and the Grid Master were running different versions of NIOS and the Grid Master was already upgraded. The result was that resource records added through Grid Manager would not be served by the secondary servers until refresh TTL of the zone expires, prompting an incremental zone transfer (IXFR).
NIOS-53093	Critical	Under certain circumstances, DHCP service interruptions occurred on networks being served by a failover association peer.

ID	Severity	Summary
NIOS-55068	Major	Addressed the following vulnerability: CVE-2015-5477: A remotely exploitable denial-of-service vulnerability that exists in all versions of BIND 9 currently supported. It was introduced in the changes between BIND 9.0.0 and BIND 9.0.1
NIOS-54983	Major	This release resolves the frame misuse vulnerability, which could result in cross-frame scripting attacks.
NIOS-54843	Major	Changed the Restart Status of “Not Required” to “Restart was not required” to clarify the actual status.
NIOS-54774	Major	The “Last discovered” field for managed data was not updated after an IP discovery.
NIOS-54594	Major	The DHCP server did not establish a connection with the IF-MAP client.
NIOS-54453	Major	Updated the *Infoblox NIOS Administrator Guide* to clarify that if a zone import fails, the zone to which the data is imported will be disabled and the appliance does not create records and delegated subzones.
NIOS-54396	Major	Updated the *CSV Import Reference* with the following: “When performing a CSV export of automatically created NS records using the Infoblox API, the “zone_nameservers” field will have an empty value. Therefore, if you import the previously exported CSV file that includes automatically created NS records through the Infoblox GUI, then the CSV import fails and Grid Manager displays an error message.”
NIOS-54280	Major	The appliance allowed adding DHCP options with the same value in different cases (i.e. abc and ABC), which caused the DHCP service to fail when applying the options.
NIOS-54084	Major	The appliance experienced high swap space usage on the Grid Master when it was not running any protocol services or API activities.

NIOS-54040	Major	After clearing the DNS cache, DNS service was not resolving external queries.
NIOS-54052	Major	WAPI: Unable to search for a specific object using type “All” and IPAMObject.
NIOS-53776	Major	Unable to add a host through Grid Manager if the Cloud Platform member and another Grid member were Grid primaries for the zone, and the network in which the host fell was not delegated.
NIOS-53735	Major	This release addressed the following glibc security vulnerability: CVE-2015-1781: A buffer overflow flaw was found in the way glibc's gethostbyname_r() and other related functions computed the size of a buffer when passed a misaligned buffer as input. An attacker able to make an application call any of these functions with a misaligned buffer could use this flaw to crash the application or, potentially, execute arbitrary code with the permissions of the user running the application.
NIOS-53730	Major	Addressed the following OpenSSL vulnerabilities: CVE-2015-1789: The X509_cmp_time function in crypto/x509/x509_vfy.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allowed remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1_TIME data, as demonstrated by an attack against a server that supported client authentication with a custom verification callback. CVE-2015-1790: The PKCS7_dataDecodefunction in crypto/pkcs7/pk7_doit.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allowed remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that used ASN.1 encoding and lacks inner EncryptedContent data. CVE-2015-1792: The do_free_upto function in crypto/cms/cms_smime.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allowed remote attackers to cause a denial of service (infinite loop) via vectors that triggered a NULL value of a BIO data structure, as demonstrated by an unrecognized X.660 OID for a hash function.
NIOS-53703	Major	Grid Manager did not open the default network view in the IPAM tab when it first started up.
NIOS-53626	Major	Under certain circumstances, inbound zone transfers did not happen after an HA failover. This could happen to any secondary zones using zone transfers or zones configured to use external primaries. A commonly seen scenario was a failure after refreshing RPZ feed zones.
NIOS-53503	Major	A newly created member was associated to a DNS view, which should not have happened.
NIOS-53457	Major	When enabled, the threat protection rule “Drop unexpected protocol” dropped valid DNS packets.
NIOS-53451	Major	This release resolved some kernel issues.
NIOS-53419	Major	This release addressed the NTP security vulnerability: CVE-2014-9298: An attacker could bypass source IP restrictions and send malicious control and configuration packets by spoofing ::1 addresses because NTP's access control was based on a source IP address.

NIOS-53368	Major	Modified ACL changes did not take effect until a product restart or reboot was performed on the Grid Master.
NIOS-53363	Major	Grid Manager was unresponsive when trying to access reports.
NIOS-53297	Major	Unexpected restarts of the watchdog process on the active node of an HA pair.
NIOS-53071	Major	Under certain circumstances, the PT-2200 appliance restarted unexpectedly.
NIOS-53042	Major	Unable to remove the internal server IP addresses from the *infoblox-deny-rpz* list even after removing the RPZ licenses from the internal servers and restarting services.
NIOS-53039	Major	Unable to stop the scheduled discovery process when discovery was still in progress.
NIOS-53032	Major	The appliance returned an error when performing a CSV import after users added the extensible attribute "**Site**."
NIOS-53024	Major	The DHCP server did not remove PTR records for expired leases.
NIOS-52940	Major	Under certain circumstances, a GUI session timed out while viewing a network in the **IP MAP** panel.
NIOS-52885	Major	In a specific configuration, DNS clients did not get responses for their queries until a forced restart or HA failover was performed due to a race condition.
NIOS-52853	Major	The appliance returned an error when users tried to generate reports due to a missing read-only user account.
NIOS-52836	Major	API: The method $import_id for CSV import did not function properly.
NIOS-52834	Major	Timestamps were not displayed in the syslog messages.
NIOS-52814	Major	Under certain circumstances, the DHCP server granted zero second to a lease when the lease was renewed.
NIOS-52682	Major	Global Search did not return any results when a Network Insight appliance was added to the Grid and started running discovery tasks.
NIOS-52557	Major	The appliance might not respond when trying to modify a large number of zones using CSV import.
NIOS-52492	Major	The NIOS appliance did not update the TTL settings for an MX record.
NIOS-52466	Major	On rare occasions, Grid Master failed.
NIOS-52360	Major	Users could not modify the GSS-TSIG setting for specific zones.
NIOS-52217	Major	The appliance returned an error message when trying to delete objects from Global Search.
NIOS-52164	Major	Users could not import more than one blank MX records through the Infoblox GUI.
NIOS-52119	Major	The name server was up and running but it had stopped recursion, answering, and logging data.
NIOS-52032	Major	In a unique situation, user was unable to join an HA pair to the Grid Master through the Infoblox GUI.
NIOS-51882	Major	WAPI: While modifying a host IP address and scheduling the task (or routing it for approval), the original and newly created IP addresses were not marked as "in use."

NIOS-51779	Major	Users had to reboot the appliance in order to start the bloxTools service correctly.
NIOS-51107	Major	Grid Manager did not validate the value entered in the "Rate Limited FQDN" field while adding a threat protection rule to the Infoblox Advanced Appliances.
NIOS-50981	Major	The SOA serial numbers for unsigned single-primary zones are now subject to reconciliation, similar to the behavior for multi-primary zones. Replicated secondaries for single-primary zones now track SOA serial numbers of the Grid Master instead of that of the primary. These changes resolve the following issues: • DDNS updates refusal due to reloading, which was a result of SOA issues. • Excessive zone reloading due to SOA issues. Records were not propagated because of missing notification, resulting from SOA issues.
NIOS-54790	Minor	Usability: Changed the "Network Users" tab back to the original "Microsoft Integration" tab and added a sub label for "Network Users."
NIOS-54359	Minor	WAPI: It took longer than expected to run a network query that specified a specific network to search.
NIOS-54095	Minor	Added the DNS cache acceleration Tier 4 license with up to 150K qps capacity.
NIOS-54076	Minor	Under certain circumstances, GUI performance was slower for limited-access users.
NIOS-53841	Minor	In the *Infoblox NIOS Administrator Guide*, updated the description for the "Last checked for updates" field in the *Grid Security Properties* editor after clicking "Download now."
NIOS-53811	Minor	Data was not filtered correctly based on the filter criteria configured for the filtering function.
NIOS-53787	Minor	Updated the documentation to reflect the correct behavior of the Global Smart Folder.
NIOS-53528	Minor	The appliance displayed excessive log messages for Infoblox DNS Firewall.
NIOS-53447	Minor	Updated the *RPZ Feed Quick Start Guide* to correct one of the feed zone names.
NIOS-53369	Minor	Updated the file names of the threat protection rules PDFs so that they are accessible from the appliance.
NIOS-53335	Minor	Enhanced the NIC bonding feature to avoid port flopping by continuing to use LAN2 after it takes over when LAN1 goes down, even when LAN1 becomes active again.
NIOS-53227	Minor	The following OIDs have been changed respectively: From ibCPU1Temperature 1.3.6.1.4.1.7779.3.1.1.2.1.2.0 ibCPU2Temperature 1.3.6.1.4.1.7779.3.1.1.2.1.3.0 to ibCPU1Temperature 1.3.6.1.4.1.7779.3.1.1.2.1.17.0 ibCPU2Temperature 1.3.6.1.4.1.7779.3.1.1.2.1.18.0
NIOS-53080	Minor	The appliance returned excessive log messages when it was not performing qname matches for RPZs or RPZ feeds.
NIOS-53068	Minor	Under certain circumstances, the appliance experienced high swap usage.
NIOS-53067	Minor	Swapping valid licenses between old and new appliances caused a "member eviction" error message.

NIOS-53066	Minor	DNS service did not respond after an upgrade.
NIOS-53001	Minor	The Infoblox IPAM Plug-In release notes did not mention the requirement of the Cloud Network Automation license for the Plug-In to function properly.
NIOS-52903	Minor	The color displayed for conflict data in the “Last Discovered” column was not consistent.
NIOS-52879	Minor	Users were able to add a DNAME record for a domain consisting of a subdomain.
NIOS-52835	Minor	The **IPAM** tab displayed IP address conflicts for deleted exclusion ranges.
NIOS-52730	Minor	API: The method $session->default_maximum_objects_returned(int) did not return CNAME records.
NIOS-52509	Minor	Cloud Network Automation: When the cloud network automation license is installed on the appliance, users could not view the network details by clicking the network filtered by the smart folder.
NIOS-52242	Minor	The appliance logged a “DNS format error” to the syslog when requesting a lease with DHCP option 82 that contained double quotes.
NIOS-50531	Minor	Smart Folder: When using an incorrect regular expression in the first query, matching objects might not appear in the smart folder.
NIOS-50152	Minor	Added instructions to enable PHP in the bloxTools environment.
NIOS-48241	Minor	Reporting: The appliance did not search reports when using the Go To function due to the case sensitivity of the Go To field.
NIOS-44498 NIOS-44456	Minor	Grid Manager did not accept the maximum TTL value (4294967295) for IPv6 fixed address. This release adds the **Unlimited Lease Time** check box so you can now configure infinite lease time for IP addresses. Note that inadvertently selecting this check box or using this option incorrectly could cause a network outage when the address range runs out of IP addresses.
NIOS-43602	Major	The appliance returned an error message when trying to restore Microsoft zone from the recycle bin.
NIOS-39523	Minor	A newly added network interface in the *Grid Member Properties* editor was not displayed in the first row.
NIOS-33371	Minor	A smart folder with maximum number of characters was not displayed in the smart folder list panel.
NIOS-53321	Enhance	Usability: Added an extra column to the DNS zone panel for “Grid Primary Servers.”
NIOS-18743	Enhance	The “Grid Primary Servers” column was added to the zone viewer for displaying names of the primary servers associated with zones.

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-55312	An RPZ rule that was deleted and then added to an RPZ feed again might not take effect immediately. This delay is mandated by the effective DNS cache setting and might cause some traffic to go through before the RPZ rule takes effect. **Workaround**: To ensure that the RPZ rule takes effect immediately, clear the DNS cache before adding the rule.
NIOS-55163	vDiscovery: When you remove a VM object (that was previously discovered) from an endpoint server and run a vDiscovery again, the last discovered data for this VM still exists in NIOS. Workaround: Manually clear unmanaged data to remove the VM object from NIOS.
NIOS-55035	Cloud Network Automation: When delegating an IPv4 or IPv6 network or network container to a Cloud Platform member while creating the network or container through the wizard, the name of the selected member is not displayed in the **Delegated To** field (even though the delegation is successful when saving the configuration). Workaround: In the wizard, select the delegated member before defining the network or network container.
NIOS-55029	Cloud Network Automation: The appliance might not generate reports that contain Cloud data if configuration changes are made through Grid Manager instead of API calls. Workaround: To generate Cloud related reports, ensure that you make configuration changes through API calls.
NIOS-55023	Cloud Network Automation: After allocating an elastic IP in AWS to a Host record, the *VM Address History* report displays the IP as “Deallocated” and “Floating” instead of “Allocated” and “Fixed.”
NIOS-55011	Unbound DNS: When you change DNS resolver from BIND to Unbound, certain threat protection rules such as transfer might not be disabled.
NIOS-54534	Cloud Network Automation: In Grid Manager, the **Cloud VMs** count in the *Cloud Statistics* widget on the Dashboard might not be updated properly after a vDiscovery. Workaround: Go to the **Cloud** tab -> **Tenants** tab to view the **VMs** count.
NIOS-54881	Unbound DNS: When you use Unbound DNS and need to change the IP address for the LAN port, ensure that you click **Restart Services** to restart services. Otherwise, Unbound DNS might not function properly.
NIOS-54406	Cloud Network Automation: Port IDs are not discovered when performing a vDiscovery job for OpenStack endpoint servers.
NIOS-54216	After a system restart or reset, the DNS cache acceleration service is not starting if Unbound is configured as the DNS resolver.

NIOS-54213	Unbound DNS: When using Unbound DNS, the order of ACLs is not taken into consideration by Unbound if there is overlapping in the ACL configuration while cache acceleration honors the order of ACLs (same as BIND). This may result in queries answered by Unbound and refused by the appliance (if cache acceleration is enabled) when being cached. Workaround: Make sure that cache acceleration is enabled for the order of ACLs to function properly, or do not use overlapping ACLs if you use Unbound DNS.
NIOS-54063	Modifying Name Server Groups on an IB-1410 that contains a large number of DNS zones might result in a service outage.
NIOS-53499	You might not be able to restore the database when you configure VLAN tagging on a vNIOS virtual Grid Master.
NIOS-53242	Queries to domain names that end with "rpz-xxx" (where xxx can be one of the following: ip, client-ip, nsdname, or nsip) might hit an RPZ rule before recursion is complete even when the queries do not match any CLIENT-IP or QNAME rules.
NIOSSPT-2283	HA members may fail to serve authoritative queries after upgrading to a NIOS release that supports the configuration of multiple primaries (MMDNS support). This issue may be exposed only when the following prerequisites are met: • Grid upgrades from pre-MMDNS to post-MMDNS support. Example: upgrading from NIOS 6.10.0 (pre-MMDNS) to NIOS 6.11.9 or 6.12.7(post-MMDNS). • Affected member is in an HA configuration. • Zones must be using zone transfer replication. • Newly upgraded passive member restarts and immediately assumes the passive role again, prompting zone database file transfers from the active member (running an older release). • Zone database format mismatch occurs and zone loading fails when this member becomes ACTIVE. **Workaround**: Force restart the DNS services on the HA member.
NIOS-53522 (NIOSSPT-2816)	During a scheduled full upgrade, the primary name server is not sending NOTIFYs to secondaries when resource records are added or deleted through Grid Manager or the API. This issue can be exposed only during a scheduled full upgrade when the primary DNS server and the Grid Master are running different versions of NIOS and the Grid Master is already upgraded. The result is that resource records added through Grid Manager would not be served by the secondary servers until refresh TTL of the zone expires, prompting an incremental zone transfer (IXFR). **Workaround**: Use the 'nsupdate' tool to add the resource records through DDNS updates.
NIOS-53494 (NIOSSPT-2744)	After an upgrade to a NIOS release that supports the configuration of multiple primaries (MMDNS support), you may notice DNS response latency for bulk host record queries. While authoritative query performance has greatly increased in MMDNS releases, non-cached (first pass) query performance for bulk host RRs in zones that contain a large number of bulk hosts (e.g. in the thousands) has decreased. **Workaround**: Set the primary DNS server as a hidden primary; configure the secondary members to learn the zones in question through zone transfers.
SRTLST4030-32	When you configure both RRset order and sort list on the IB-4030 or IB-4030-10GE appliance with DNS cache acceleration service enabled, the appliance sorts responses based on the order listed in the defined sort list.
KVMVNIOS-118	vNIOS for KVM hypervisor: The vNIOS instances deployed in the OpenStack environment do not support HSM Safenet groups.

KVMVNIOS-115	vNIOS for KVM hypervisor: Connection to the FTP service might fail after the virtual appliance enters the passive mode. Workarounds: 1. Use active mode instead of passive mode. 2. Modify the *vnios-sec-group* security group to open ports 1023 and above. 3. Use the FTP client inside the internal network.
NIOS-51323	DNS Traffic Control: The appliance may return a timeout error while loading the **Traffic Management** tab in Grid Manager if you have configured health monitoring for a lot of DTC servers.
NIOS-51287	Cloud Network Automation: Modifying resource records through the cloud API will cause extensible attribute values to be removed.
NIOS-51235	In a Multi-Grid configuration, converting network connectivity for the Master Grid and its sub Grids to IPv6 only is not supported even though Grid Manager may allow you to do so.
NIOS-51134	Infoblox appliances currently do not support HP passive copper cables.
NIOS-51054	After you upgrade to NIOS 7.0.0, Infoblox recommends that you back up the configuration after you change network connectivity to a different mode (IPv4, IPv6, or IPv4 and IPv6 dual mode). Restoring an old backup by performing a forced restore may prevent some Grid members from rejoining the Grid after the restore.
NIOS-50873	When you enable DNS and DHCP services for IPv6 only, DDNS updates may not function properly for certain configurations. Infoblox recommends that you do not enable DDNS updates in an IPv6-only Grid.
NIOS-50859	Creating custom IPv6 NS records and pointing a zone to a particular IPv6 name server is not supported in this release.
NIOS-50994	Cloud Network Automation: When there is no tenant associated with a network or VM, or if a network or VM is created by a cloud adapter but the tenant ID is not specified in the cloud API request, the **Name** or **ID** column for the tenant or VM is left blank in Grid Manager, which implies "N/A" or not applicable for the specified network or VM.
N/A	Reporting: When there is too much data being displayed in a graph, data can overlap each other and make it difficult for viewing. You can expand the graph to view specific data by stretching the graph on display. However, you will not be able to download the expanded graph in a PDF. Workaround: Right-click the expanded graph, and then select **This Frame** -> **Print Frame** from the drop-down menu to print the graph.
NIOS-49238	Network Insight: Under certain circumstances, deleting networks may not remove the corresponding IP helper addresses from the device configuration.
NIOS-49208	Microsoft Management: A failover association created using Microsoft servers as the primary and secondary peers may not appear in Grid Manager after you remove the secondary peer. Workaround: Manually remove the partial failover association while removing the Microsoft server that is part of the failover association.
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.

NIOS-49107	Network Insight: If a recurring port control blackout is scheduled and it includes the current time, port control tasks will be delayed during the current blackout period. However, you may not be warned until the next blackout period. If a recurring discovery blackout is scheduled and it includes the current time, the **Discover Now** functionality may not be blocked until the next blackout period.
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-48311	On the IB-4010 appliance, the maximum resource records allowed in a single signing zone is 800K, not 25% of the object limit as in other platforms. Exceeding this limit may result in a system restart.
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.
NIOS-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.