



## NIOS 7.3.0 Release Notes

INTRODUCTION .....	2
Supported Platforms.....	2
NEW FEATURES.....	7
NIOS 7.3.0 .....	7
CHANGES TO DEFAULT BEHAVIOR .....	11
NIOS 7.3.0 Release.....	11
NIOS 7.2.x Releases .....	12
NIOS 7.1.x Releases .....	12
NIOS 7.0.x Releases .....	13
CHANGES TO Infoblox API and RESTful API (WAPI) .....	13
WAPI Deprecation and Backward Compatibility Policy .....	14
NIOS 7.3.x Release .....	14
NIOS 7.0.x Releases .....	16
UPGRADE GUIDELINES .....	16
Upgrading to NIOS 7.3.x .....	16
Upgrading to NIOS 7.2.x .....	16
Upgrading to NIOS 7.0.x .....	17
BEFORE YOU INSTALL.....	18
ACCESSING GRID MANAGER .....	19
ADDRESSED VULNERABILITIES.....	20
RESOLVED ISSUES .....	23
Fixed in 7.3.0.....	23
KNOWN GENERAL ISSUES.....	31

## NIOS 7.3.0 Release Notes

### INTRODUCTION

Infoblox NIOS™ 7.3.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 7.3.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 7.3.x on these appliances. See [Upgrade Guidelines](#) on page 16 for additional upgrade information.
- Infoblox does not recommend operating the physical Trinzic TE-820 appliance as the Grid Master running NIOS 6.10.x or later due to memory constraints. Grid Manager (the Infoblox GUI) might appear sluggish after an upgrade or new installation. On rare occasions, running NIOS 6.10.x or later on the Trinzic TE-820 might result in less than optimal performance. To address this issue, you can deploy the latest version of the Infoblox 820 virtual appliance (IB-VM-820) as the Grid Master.
- You cannot upgrade to NIOS 7.3.x if your Grid uses a physical TE-810, TE-820, or an IB-VM-810 virtual appliance as the Grid Master or Grid Master Candidate. For the IB-VM-820 virtual Grid Master however, you can upgrade to NIOS 7.3.x provided that the virtual appliance is currently running NIOS 6.10.x or later. After the upgrade, ensure that you change the “Resource Allocation” for the appliance to reflect the 4 GB of RAM; or you can download and install the latest .ovf file for the IB-VM-820 to enable the 4 GB of RAM.
- **Infoblox Reporting and Analytics:** There are some significant changes in the functionality and user interface for the Infoblox Reporting solution. Infoblox recommends that you take some time to explore and navigate through the new user interface to get familiar with the new features and terminologies. If you are upgrading to NIOS 7.3.x from a previous NIOS release, your custom reports will be affected and you may need to take some actions to re-create them. For more information about these changes, see [Changes to Default Behavior](#) on page 11.

### Supported Platforms

Infoblox NIOS 7.3.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, Infoblox-4010, and Infoblox-4020
  - 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

## NIOS 7.3.0 Release Notes

- **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.x.x, 5.5.x, 5.1.x, or 5.0.x installed, and then configure it as a virtual appliance.

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

## NIOS 7.3.0 Release Notes

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 Limit	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	✓ <sup>3</sup>	✓	✓	✓ <sup>1</sup>	✗	No
IB-VM-800 (for reporting only; 2 GB daily limit)	300 (Primary & Reporting)	2	Range: 4 - 8 GB Default: 8 GB	3000 MHz	✓ <sup>3</sup>	✓	✓	✗	✗	No
IB-VM-810	55	2	2 GB	2000 MHz	✓	✓	✓	✓	✗	No
IB-VM-810	160	2	2 GB	2000 MHz	✓	✓	✓	✗	✗	No
IB-VM-820	55	2	4 GB	3000 MHz	✓	✓	✓	✓	✗	Yes <sup>2</sup>
IB-VM-820	160	2	4 GB	3000 MHz	✓	✓	✓	✗	✓	Yes <sup>2</sup>
IB-VM-1400 (for reporting only; 5 GB daily limit)	555 (Primary & Reporting)	4	Default: 8 GB	8000 MHz	✓ <sup>3</sup>	✓	✗	✗	✗	No
IB-VM-1410	55	4	8 GB	6000 MHz	✓	✓	✓	✗	✗	No
IB-VM-1410	160	4	8 GB	6000 MHz	✓	✓	✓	✗	✗	Yes <sup>2</sup>
IB-VM-1420	160	4	8 GB	8000 MHz	✓	✓	✓	✓	✓	Yes <sup>2</sup>
IB-VM-2210	160	4	12 GB	12000 MHz	✓	✗	✓	✗	✗	Yes <sup>2</sup>
IB-VM-2220	160	4	12 GB	12000 MHz	✓	✗	✓	✓	✓	Yes <sup>2</sup>

## NIOS 7.3.0 Release Notes

Network Insight Virtual Appliances	Overall Disk (GB)	# of CPU Cores	Memory Allocation	Virtual CPU Core Frequency Limit	vNIOS for VMware	vNIOS for MS Hyper-V	vNIOS for Xen	vNIO S for KVM	vNIOS for AWS	Supported as Grid Master and Grid Master Candidate
ND-V800	160	2	8 GB	3000 MHz	✓ <sup>3</sup>	✓	✓	✗	✗	No
ND-V1400	160	4	16 GB	8000 MHz	✓ <sup>3</sup>	✓	✓	✗	✗	No
ND-V2200	160	8	24 GB	24000 MHz	✓ <sup>3</sup>	✗	✓	✗	✗	No
Cloud Platform Virtual Appliances	Overall Disk (GB)	# of CPU Cores	Memory Allocation	Virtual CPU Core Frequency Limit	vNIOS for VMware	vNIOS for MS Hyper-V	vNIOS for Xen	vNIO S 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:

<sup>1</sup> For KVM hypervisor only. Not supported for KVM-based OpenStack. Does not support Elastic Scaling.

<sup>2</sup> 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. When configuring IB-VM 820 as the Grid Master, ensure that you upgrade the memory allocation to 4 GB.

<sup>3</sup> Does not support Elastic Scaling.



## NIOS 7.3.0 Release Notes

### 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 7.3.0 Release Notes

### NEW FEATURES

This section lists new features in the 7.3.0 release.

#### NIOS 7.3.0

##### Amazon Route 53 Integration

Infoblox DDI for AWS integrates the AWS Route 53 DNS service, providing a unified DNS view across AWS and hybrid cloud deployments through a centralized console that improves visibility and performance. Without Infoblox, AWS deployments utilizing Route 53 have limitations with private hosted zones, which restrict DNS resolution from outside AWS and hinder hybrid cloud deployments.

##### Enhancements for Cloud Network Automation

This NIOS release adds the following enhancements for Cloud Network Automation:

- **Delegated objects:** You can now add, modify, and delete fixed addresses and reservations in delegated networks and address ranges through the Grid Manager UI in addition to using cloud API calls.
- **vDiscovery:** vDiscovery now automatically removes unmanaged and discovered data for VMs that have been deleted in vSphere, OpenStack, and/or AWS EC2. Clear all discovered data; remove discovered data from vDiscovery tasks; perform vDiscovery jobs directly in the **Cloud** tab.
- **Visibility:** A new report and dashboard widget to show dynamic license utilization has been added.

##### Infoblox Reporting and Analytics

Infoblox Reporting and Analytics delivers an enhanced reporting interface so you can now create custom dashboards, reports, and alerts. You can continue to use the traditional NIOS reports in the new interface and customize them to meet your specific requirements, or you can create new custom dashboards and reports from the ground up using a powerful search and visualization language or a simple graphical interface.

##### Cisco ISE Integration

Infoblox integration with Cisco pxGrid (Cisco Platform Exchange Grid) enables Network Insight and Cisco ISE (Cisco Identity Services Engine) to exchange valuable networking, user, device, and security-event information, enriching both Infoblox DDI and ISE data. The pxGrid publish/subscribe architecture enables users to combine pxGrid ecosystem products into a unified solution that enhances security-response accuracy and timeliness; expands visibility of networks, users, and devices; and improves overall IT operations by sharing information between network and security teams. Infoblox participation in the pxGrid community makes Infoblox data indispensable for Cisco ISE customers.

##### STIX/TAXII Support

This release adds the TAXII (Trusted Automated eXchange of Indicator Information) service that enables NIOS to integrate with other security software using the TAXII/STIX protocol for cyber threat mitigation. In this release, the TAXII server is able to receive a mitigation request from a STIX/TAXII enabled third-party security platform that adds to the DNS Firewall (RPZ) an IP address or domain that is deemed malicious. This enables the third-party security platform to use the Infoblox Grid to apply a distributed mitigation policy.

##### Infoblox DNS Threat Analytics

DNS Threat Analytics mitigates DNS data exfiltration by employing analytics algorithms to detect DNS tunneling traffic. When you enable the analytics service, NIOS starts analyzing incoming DNS data and applying algorithms to detect security threats. Once threats are detected, NIOS blacklists the domains and transfers them to the designated mitigation RPZ (Response Policy Zone), and traffic from offending domains is blocked. DNS Threat Analytics also includes a whitelist that contains trusted domains on which NIOS allows DNS traffic. These are known good domains that carry legitimate DNS tunneling traffic for tools such as Avast, Sophos, McAfee, Boingo, Barracuda, and others. The whitelist is extensible so new whitelisted domains can be added and rolled out accordingly. This release provides automatic updates for Threat Analytics modules through Grid

## NIOS 7.3.0 Release Notes

Manager. When you configure automatic updates for Threat Analytics modules, NIOS automatically download the module set periodically. You can also view the current whitelist version and module set version in the **Updates** tab in the *Grid Threat Analytics Properties* editor.

**NOTE:** Infoblox highly recommends that you run the analytics service for a limited time to monitor and preview what has been detected before actually blocking any domains. To do so, set **Policy Override** to **Log Only (Disabled)** when you create the designated local RPZ. You can carefully review the list of detected domains and decide which domains you want to continue blocking and which domains you want to add to the analytics whitelist. You should review the blacklisted domains on a regular basis to make sure that no legitimate use of DNS tunneling is blocked. You can update the analytics whitelist by adding new custom whitelisted domains, moving legitimate domains from the blacklisted domain list, or using CVS import and export. Due to memory and capacity required to perform analytics, ensure that you install the Threat Analytics and RPZ licenses and enable the threat analytics service on an appliance that has big enough capacity. Following are the supported Infoblox appliance models on which you can run the threat analytics service: IB-4010, IB-4030, IB-4030-10GE, TE-2210, TE-2220, PT-2200, PT-4000, PT-4000-10GE, IB-VM-2220, and IB-VM-4010.

### VRF Integration for Network Insight

Through Infoblox Network Insight, the NIOS appliance is now able to discover network devices that are configured or deployed within virtual networks, such as VRF-based (Virtual Routing and Forwarding) networks. You now have visibility of your complete virtual network infrastructure, which allows you to view and manage overlapping IP addresses, VRF-specific data from VRF-enabled devices, and discovered end host data.

### Security Visibility (RFE-5732)

Grid Manage now provides the following features to increase visibility of your Infoblox security infrastructure:

- A comprehensive Security dashboard that displays the current security data, including Threat Protection events and RPZ hits. You can view information such as the top N Grid members by events, top N rules by volume, and more. To ensure that the Security dashboard displays correct data, use NTP to synchronize the time of the Grid members with that of the Grid Master.
- Threat Protection widgets that display security data based on the new “grouping” feature.
- New reports that display security information related to Infoblox External DNS Security and Infoblox Internal DNS Security.

### Infoblox Security Infrastructure Enhancements (RFEs: 5635, 5267, 5641, 5670, 5607, 5369, 4974, 5595, 6172, and 5712)

This release adds a few enhancements to the Infoblox Security Infrastructure features, as follows:

- Ability to reset the appliance to use the default Threat Protection ruleset.
- Specify the interface for downloading the latest ruleset.
- Configure the MGMT port as the interface for Reporting traffic.
- Display FQDN information for Threat Protection rule match the syslog.
- Display the current active ruleset version in Grid Manager

### Data Collection Virtual Appliances

Infoblox introduces phase one of the Data Collection feature in this release. You can set up a newly developed Data Collection appliance as the data collector to work with the Infoblox Reporting member for report generation. The purpose is to enhance the collector in a future release to enable scalable distribution of Grid data to the Reporting server and other third-party destinations.

### DNS Record Scavenging

The DNS record scavenging feature allows you to remove stale DNS resource records from zone data to prevent the accumulation of invalid records. A scavenging operation determines, based on predefined rules, which records became stale, i.e. reclaimable, and removes them.



## NIOS 7.3.0 Release Notes

### Secure Dynamic DNS Updates

The secure DDNS updates feature provides the following mechanisms to restrict DDNS updates:

- Protecting specific resource records so that clients cannot update them.
- For authenticated updates, tracking the Kerberos GSS-TSIG principal that created a record and preventing DDNS updates to the record created by a different GSS-TSIG principal.
- Defining FQDN patterns for domain names that prevent DDNS updates to matching FQDNs.

To handle principal authentication-based secure updates even more flexibly, you can create dynamic update groups.

### 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 Trinix virtual appliances for these hypervisors as the Grid Master or Grid members using Elastic Scaling. For information about supported vNIOS models, see the table on page 4.

### Improved Support for vNIOS for KVM on OpenStack

Issues with deploying vNIOS for KVM on certain OpenStack distributions (e.g., Red Hat Enterprise Linux OpenStack Platform 6) have been resolved. Property injection through cloud-init and ability to assign IP addresses and network properties via OpenStack DHCP for vNIOS for KVM network interfaces is now supported. Qcow2 images are now available in addition to OVA images.

### Auto-creation of DNS Records for Discovered VMs

When you configure a vDiscovery job, you can now enable the appliance to automatically create or update Host records or A/AAAA or PTR records for discovered VM instances in authoritative zones. You can also enter a formula that NIOS uses to create the DNS names for the discovered IP addresses based on their VM parameters such as vm\_name or discovered\_name. By doing so, NIOS is able to automatically create and update DNS records for private and public IPs discovered through vDiscovery.

### Support for HTTP or HTTPS Proxy Servers

NIOS now supports the configuration of HTTP or HTTPS proxy servers for automatic updates. You can use this feature to download automatic updates for Threat Protection rulesets and Threat analytics bundles. For an AWS cloud deployment, you can configure a proxy server for vDiscovery or use it as the AWS API Proxy.

### Enhancements for DNS Traffic Control (RFE-3315)

By adding support for the NAPTR record type to the DTC (DNS Traffic Control) solution, DTC is now in compliant with the 3GPP standards. You can also add an SNMP health monitor to track server availability and define the load balancing method for a DTC LBDN (Load Balancing Domain Name) record. DTC now responds to queries containing the EDNS0 (Extension Mechanisms for DNS) Client Subnet option by leveraging that address information in performing geographic load balancing.

### Support for match-recursive-only BIND option (RFE-469)

You can now enable the match-recursive-only option for the DNS view. When you enable this option, only recursive queries from matching clients match the selected DNS view. This option can be used in conjunction with the match client list and match destination list.

### Replication of syslog Rotated Files to External Servers (RFE-354/599)

You can configure the appliance to back up rotated syslog files to external servers through FTP or SCP. When you do so, the appliance forwards the rotated syslog files to the external servers that you configure. Configuring syslog external backup servers helps you conveniently send (archive) syslog files to different destinations by their logging categories. This allows you to split syslog files based on the service and efficiently perform troubleshooting.



## NIOS 7.3.0 Release Notes

### Shared Record Support for CNAMEs (RFE-498)

This release adds support for CNAME records to shared record groups.

### NIOS Audit Log Reporting (RFE-3777)

The newly added *Audit Log Events* report provides information about the administrator-initiated events, including login events, logout events, service restarts, appliance reboots, and write operations such as the addition, modification, and deletion of objects.

### Support for 'posixGroup' in LDAP Authentication (RFE-3805)

This release enhances LDAP authentication to include the support for group attributes and allow groups from the 'posixGroup' object class.

### Enabling Active Directory Authentication for Nested Groups (RFE-507)

Windows servers support nesting groups in which you can add a group of admin users as a member of another group. Nested groups consolidate admin accounts and help reduce the number of permissions required for individual users or groups. In NIOS, you can now enable nested group query so the appliance can recursively look up and use AD authentication service to authenticate members or admin accounts that are part of a nested group.

### Remote Authentication for Local Groups (RFE-910)

Depending on where admin user credentials are stored, you can configure the NIOS appliance to authenticate admins locally or remotely. When you configure the authentication type as "local," NIOS authenticates admins against its local database. When you configure the authentication type as "remote," NIOS authenticates admins whose user credentials are stored remotely on authentication servers, such as RADIUS servers, AD domain controllers, LDAP servers, or TACACS+ servers.

### Hostname and server-id Options (RFE-1661)

When you configure DNS anycast, more than one DNS name servers share a single IP address. To identify which DNS name server is answering queries, you can configure the hostname and server ID options so the NIOS appliance returns the hostname of the DNS name server that is currently answering queries.

### Controlling NS Records for AD-replicated Zones (RFE-6268)

When you have assigned a Microsoft server as the primary server for a DNS zone and if the zone is AD-integrated (Active Directory), you can now configure a list of domain controllers that are allowed to add NS records to the zone.

### DHCP Lease Scavenging (RFE-4594)

This release supports DHCPv6 lease scavenging.

### DHCP Failover Recovery (RFE-5142)

You can now perform a DHCP recovery for failover associations through Grid Manager. As result of the recovery, all conflicts are resolved on the passive node after a restart.

## NIOS 7.3.0 Release Notes

### CHANGES TO DEFAULT BEHAVIOR

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

#### NIOS 7.3.0 Release

- The Infoblox Reporting and Analytics solution delivers an enhanced interface through Grid Manager. Starting with this release, you will experience the following when using the Reporting solution:
  - **Product Terminology:** Reports and Searches in previous releases are now called dashboards and Reports respectively in the new user interface.
  - **Object Management:** NIOS no longer manages reporting objects such as searches, alerts, reports, and smart folders. You will not be able to perform operations such as global search, quick filtering, bookmarking, and others for these objects. You can now manage these objects through the new user interface.
  - **Permissions:** Permissions for all reporting objects are migrated to the new Reporting and Analytics solution and managed through the new user interface after an upgrade. You may see the new built-in role, **Everyone**, when configuring Reporting permissions. For best practices, do not alter permissions for this new built-in role. Note that the Reporting Dashboard and Reporting Search global permissions have been removed. If an admin group or admin role was granted these permissions before an upgrade, the permissions will still be displayed after an upgrade. However, they won't take any effect. The Grid Reporting Properties permission is retained. In addition, reporting object permissions for dashboards and searches (including global dashboards and searches) are migrated. These object permissions are retained for applicable migrated users. If permissions were granted to a specific admin group for a dashboard or search before an upgrade, only these admin users and superusers have permissions to access the migrated dashboard and report after an upgrade. If a limited-access user group is created through the new interface after the upgrade, users in this admin group will not be able to access the dashboard and report even if they are granted access to the Infoblox Reporting and Analytics App. Superusers must explicitly grant permissions to this limited-access admin group for users in this group to access the dashboard and report.
  - **Navigation and Visualization:** Navigations for some reporting functions, such as searches, alerts, email and page settings, and email PDF delivery, have changed. You can navigate through the new user interface to get familiar with the changes in this release. In addition, all pre-defined reports might look different than the traditional ones depending on your filtering configuration.
  - **Extensible Attributes:** There are some NIOS reports that support filtering by multiple extensible attributes. These reports are migrated into dashboards in which the new user interface supports filtering and grouping only by the extensible attribute **Site**. If you want to filter a report by multiple extensible attributes, you must clone the dashboards, add filter inputs, and then modify the view XML to support extensible attributes.
  - **Searches and Reports:** Only NIOS system and global reports and searches are migrated to the new dashboards and reports respectively after an upgrade. All user private reports are not migrated. If you want to keep the settings for the user private dashboards and reports, you can do one of the following:
    1. Create global reports using the same private settings before an upgrade so the reports can be migrated and the same private settings are retained.
    2. Clone the corresponding system or global dashboards and reports after an upgrade, and then reconfigure them using the original private settings such as filters and scheduling through the new user interface.



## NIOS 7.3.0 Release Notes

For detailed information about these changes in the Reporting and Analytics solution, refer to the *Infoblox NIOS Administrator Guide* and the Splunk documentation.

- vDiscovery now automatically removes unmanaged and discovered data for VMs that have been deleted in vSphere, OpenStack, and/or AWS EC2.
- The **RIR Organizations** tab under the **Administration** tab of Grid Manager has been changed to **RIR**. No functionality is affected; only the name of the tab is changed.
- In this release, the “RIPE Changed” extensible attribute definition for networks, network containers, and network template has been removed because RIPE has removed the “Changed” field in their database. During an upgrade to NIOS 7.3.x, the value for this extensible attribute will be removed if it exists in any networks and network containers.

### 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 longer 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-



## NIOS 7.3.0 Release Notes

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 2.3.

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, and 2.3.





## NIOS 7.3.0 Release Notes

### 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 7.3.x Release

#### WAPI new objects:

- adminrole : Admin Role object.
- allendpoints : All Endpoints object.
- allrecords : AllRecords object.
- allrpzrecords : DNS All RPZ Records object.
- awsrt53taskgroup : AWS Route53 task group object.
- awsuser : AWS User object.
- bulkhost : Bulkhost object.
- cacertificate : CA Certificate object.
- captiveportal : Captive portal object.
- ciscoise:endpoint : Cisco ISE Endpoint object.
- ciscoise:notificationrule : Cisco ISE notification rule object.
- ddns:principalcluster : DDNS Principal Cluster object.
- ddns:principalcluster:group : DDNS Principal Cluster Group object.
- dhcpfailover : DHCP Failover Association object.
- discoverytask : Discovery Task object.
- dtc:allrecords : DTC AllRecords object.
- dtc:monitor:snmp : DTC SNMP monitor object.
- dtc:record:naptr : DTC NAPTR Record object.
- filterfingerprint : DHCP Fingerprint Filter object.
- filtermac : DHCP MAC Address Filter object.
- filternac : DHCP NAC Filter object.
- filteroption : DHCP filter option object.
- fingerprint : DHCP Fingerprint object.
- grid:dashboard : Grid Dashboard object.
- ipam:statistics : IPAM statistics object.
- member:threatprotection : Member threat protection object.
- network\_discovery : Network discovery object.
- orderedresponsepolicyzones : Ordered Response Policy Zones object.
- record:rpz:a : Response Policy Zone Substitute A Record Rule object.
- record:rpz:a:ipaddress : Response Policy Zone Substitute IPv4 Address Rule object.





## NIOS 7.3.0 Release Notes

- 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.
- ruleset : DNS Ruleset object.
- scavengingtask : DNS scavenging task object.
- taxii : Taxii Member object.
- threatprotection:rule : Member Threat Protection Rule object.
- userprofile : User profile object.
- vdiscoverytask : Discovery task object.
- zone\_rp : DNS Response Policy Zone object.

### 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



## NIOS 7.3.0 Release Notes

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.

## UPGRADE GUIDELINES

### Upgrading to NIOS 7.3.x

- You cannot upgrade to NIOS 7.3.x if your Grid uses a physical TE-810, TE-820, or the IB-VM-810 virtual appliance as the Grid Master or Grid Master Candidate. For more information, see [INTRODUCTION](#) on page 1.
- Depending on your appliance model, the distribution step of the upgrade process may take longer than usual due to improvement made to the swap file space.
- Infoblox Reporting and Analytics delivers an enhanced reporting interface so you can continue to create custom dashboards, reports, and alerts. When you upgrade from a previous NIOS release, some of the reporting functions and terminologies might have changed. In addition, your custom reports might be affected. For information about the changes and new features, see [Changes to Default Behavior](#) on page 11 and refer to the *Infoblox NIOS Administration Guide* and the Splunk documentation.
- DNS Scavenging: Note the following changes to the last query settings for zones and RRs during an upgrade to 7.3.x:
  - There are no limitation for monitored zones and the lists are no longer available in the *Grid* and *Member Reporting Properties* editors.
  - For every monitored zone: The reclamation settings are set to the “overridden” state at the zone level; and the “Enable zone last queried monitoring,” “Enable RRs last queried monitoring” or both is set to the **Enabled** state. In addition, when enabling Grid-wide scavenging, zones with last queried monitoring enabled prior to an upgrade will not inherit reclamation settings from the Grid and they will not be part of the Grid-wide reclamation task (either manual or recurring).
  - The last queried monitoring for zones and RRs can now be enabled only at a given level (Grid, view, or zone). Enabling monitoring for a zone does not enable monitoring for sub zones.

### 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.



## NIOS 7.3.0 Release Notes

- 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 7.3.0 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.

7.2.4 and earlier 7.2.x releases  
 7.2.202-LD and earlier 7.2.2xx releases  
 7.1.8 and earlier 7.1.x releases  
 7.0.8 and earlier 7.0.x releases  
 6.12.14 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

### 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](mailto: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



## NIOS 7.3.0 Release Notes

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.



## NIOS 7.3.0 Release Notes

### 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-2015-8705**

In some versions of BIND, an error could occur when data that had been received in a resource record was formatted to text during debug logging. Depending on the BIND version in which this occurred, the error could cause either a REQUIRE assertion failure in buffer.c or an unpredictable crash (e.g. segmentation fault or other termination). This issue could affect both authoritative and recursive servers if they were performing debug logging. Note that NIOS 7.1.0 through 7.1.8 and NIOS 7.2.0 through 7.2.4 were affected by this vulnerability.

#### **CERT VULNERABILITY NOTE CVE-2015-8704**

A DNS server could exit due to an INSIST failure in apl\_42.c when performing certain string formatting operations. Examples included but might not be limited to the following:

- Slaves using text-format db files could be vulnerable if receiving a malformed record in a zone transfer from their masters.
- Masters using text-format db files could be vulnerable if they accepted a malformed record in a DDNS update message.
- Recursive resolvers were potentially vulnerable when logging, if they were fed a deliberately malformed record by a malicious server.
- A server which had cached a specially constructed record could encounter this condition while performing 'rndc dumpdb'.

#### **CERT VULNERABILITY NOTE CVE-2015-8605**

A badly formed packet with an invalid IPv4 UDP length field could cause a DHCP server, client, or relay program to terminate abnormally, causing a denial of service.

#### **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-2015-6564**

Fixed a use-after-free bug related to PAM support that was reachable by attackers who could compromise the pre-authentication process for remote code execution

#### **CERT VULNERABILITY NOTE CVE-2015-6563**

Fixed a privilege separation weakness related to PAM support. Attackers who could successfully compromise the pre-authentication process for remote code execution and who had valid credentials on the host could impersonate other users

#### **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**





## NIOS 7.3.0 Release Notes

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-2015-6364 and CVE-2015-5366**

A flaw was found in the way the Linux kernel networking implementation handled UDP packets with incorrect checksum values. A remote attacker could potentially use this flaw to trigger an infinite loop in the kernel, resulting in a denial of service on the system, or causing a denial of service in applications using the edge triggered epoll functionality.

### **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\_dataDecode function 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.



## NIOS 7.3.0 Release Notes

### **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-2014-6277, 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.



## NIOS 7.3.0 Release Notes

### 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 30.

#### Fixed in 7.3.0

ID	Severity	Summary
NIOS-57442	Critical	In certain situations, unable to import DS records even when the delegation NS records existed in the parent zone.
NIOS-57186	Critical	Addressed the following vulnerability: CVE-2015-8605: A badly formed packet with an invalid IPv4 UDP length field could cause a DHCP server, client, or relay program to terminate abnormally, causing a denial of service.
NIOS-57084	Critical	On some occasions, the appliance encountered issues when there were bulk AXFR requests to a zone with bulk hosts configured, causing DNS and DHCP service outage.
NIOS-56925	Critical	Under certain circumstances, reporting members in the Grid were not sending traffic.
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 an upgrade.
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-56280 NIOS-55902	Critical	In a particular Grid configuration, zone change notifications that included GSS-TSIG keys sent from the DNS primary to the secondary did not function properly.
NIOS-56097	Critical	On special occasions, creating a delegated zone could cause DNS outage.
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-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-55869	Critical	Performing some tasks in Grid Manager, such as adding a comment to a network or modifying authoritative zones, took longer than expected.
NIOS-55860	Critical	Unable to view the syslog messages when the auto synchronization was complete after joining a member to the Grid.
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-55820	Critical	Under certain circumstances, the reporting server could not generate reports after a power outage.



## NIOS 7.3.0 Release Notes

NIOS-55805	Critical	Addressed the following vulnerabilities: CVE-2015-5364 and CVE-2015-5366: A flaw was found in the way the Linux kernel networking implementation handled UDP packets with incorrect checksum values. A remote attacker could potentially use this flaw to trigger an infinite loop in the kernel, resulting in a denial of service on the system, or causing a denial of service in applications using the edge triggered epoll functionality.
NIOS-55757	Critical	This release addresses the change of IPv4 and IPv6 addresses for the DNS root zone H.ROOT-SERVERS.NET.
NIOS-55614	Critical	Unable to log in to Grid Manager after executing the <code>reset all</code> command.
NIOS-55519	Critical	Unable to convert the secondary peer of a DHCP failover association to a regular Grid member.
NIOS-55491	Critical	Standalone HA appliances might not be able to upgrade properly when the interface port speed was configured to 10/100 Full Duplex instead of auto-negotiate.
NIOS-55373	Critical	Under certain memory related circumstances, a process might fail and could not be restarted.
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-54036	Critical	Missing reporting data could occur due to unstable network connection and time synchronization issues between the Grid Master and members.
NIOS-53494	Critical	Under certain circumstances, the appliance experienced high DNS latency issues due to a large number of bulk hosts.
NIOS-53146	Critical	NIOS failed to return a normalized DNAME in lower case for the PTR record, causing a DNS service outage.
NIOS-52048	Critical	When the SCP or FTP server was unavailable, DNS query and response logs could cause disk usage to grow in the reporting partition.

ID	Severity	Summary
NIOS-57685	Major	Files uploaded to a Grid member through FTP were not properly synchronized to the Grid Master.



## NIOS 7.3.0 Release Notes

NIOS-57488	Major	<p>Addressed the following BIND security vulnerabilities:</p> <p>CVE-2015-8704: A DNS server could exit due to an INSIST failure in apL_42.c when performing certain string formatting operations. Examples included but might not be limited to the following:</p> <ul style="list-style-type: none"> <li>Slaves using text-format db files could be vulnerable if receiving a malformed record in a zone transfer from their masters.</li> <li>Masters using text-format db files could be vulnerable if they accepted a malformed record in a DDNS update message.</li> <li>Recursive resolvers were potentially vulnerable when logging, if they were fed a deliberately malformed record by a malicious server.</li> <li>A server which had cached a specially constructed record could encounter this condition while performing 'rndc dumpdb'.</li> </ul> <p>CVE-2015-8705: In some versions of BIND, an error could occur when data that had been received in a resource record was formatted to text during debug logging. Depending on the version in which this occurred, the error could cause either a REQUIRE assertion failure in buffer.c or an unpredictable crash (e.g. segmentation fault or other termination). This issue could affect both authoritative and recursive servers if they were performing debug logging. Note that NIOS 7.1.0 through 7.1.8 and NIOS 7.2.0 through 7.2.4 were affected by this vulnerability.</p>
NIOS-57396	Major	Unable to delete auto-generated records for IP reservations.
NIOS-57395	Major	In situations where the appliance applied a large number of configured ACEs and ACLs along with restricted access to the remote console and GUI/API access, SSH with authentication failed (even though the same authentication worked with GUI or HTTPS access).
NIOS-57283	Major	When running a traffic capture over the HA interface, the appliance did not capture DNS queries sent to the VIP.
NIOS-57188	Major	Under certain circumstances, the IB-4030 appliance might go offline if it was processing a high volume of traffic, such as running top domain/NXDomain reports.
NIOS-57155	Major	Cloud Network Automation: When trying to convert an IP address of a VM with multiple IPs to host, the appliance also selected the first listed IP regardless of which IP the user selected.
NIOS-57154	Major	vDiscovery: Users could not update the secret key for AWS endpoints through the WAPI.
NIOS-57139	Major	Users could not select "Discover Now" from the Action menu for a specific IP address.
NIOS-57111	Major	Under certain circumstances, the DNS service restarted due to capturing DNS responses for reporting.
NIOS-57040	Major	In the <i>Infoblox NIOS Administrator Guide</i> , added a note to indicate that traffic capture files were shared among different admin users.
NIOS-56998	Major	Unable to modify IPAM networks using CSV import.
NIOS-56972	Major	The DHCP server did not offer a fixed address when the client was identified only based on the client identifier (DHCP option 61).





## NIOS 7.3.0 Release Notes

NIOS-56829	Major	After executing the <code>set upgrade_forced_end</code> CLI command, some Grid members stayed in the “Synchronizing” state until the “upgrade_message_sent” file was cleared.
NIOS-56747	Major	The PT-1400 appliance encountered some issues with the smart NIC card.
NIOS-56578	Major	Unable to remove an authoritative reverse-mapping zone under certain circumstances.
NIOS-56564	Major	Added threat protection rules for DNS tunneling in the <i>Threat Protection Rules</i> appendix.
NIOS-56541	Major	Unable to join a member to the Grid due to invalid IFMAP objects in the database.
NIOS-56476	Major	The source IP address for downloading threat protection rules was different between NIOS releases.
NIOS-56473	Major	Multi-Grid Configuration: After upgrading sub Grids, users could not query extensible attributes and their values through the PAPI.
NIOS-56415	Major	Testing LDAP authentication failed against Active Directory servers failed.
NIOS-56402	Major	Grid Manager displayed an error in the <b>Dashboard</b> tab -> <b>Status</b> tab after users removed a Network Insight member from the Grid.
NIOS-56397	Major	Unable to configure all Grid member to have a specific Grid member as the conditional forwarder, which also had a conditional forwarder for the same zone to an external server.
NIOS-56289	Major	Addressed the following issues: <ul style="list-style-type: none"> <li>Instant javascript execution when entering HTML code in the <b>Username</b> field.</li> <li>Certain types of Java script were executed when used in the <b>Go to</b> field of the IP Map and NetMap panels.</li> <li>Javascript safe check for Smart Folder names.</li> </ul>
NIOS-56282	Major	Unable to access Grid Manager when using a certain version of Internet Explorer browser.
NIOS-56218	Major	Some IB-4030 appliances in the Grid experienced intermittent latency peaks in DNS query responses.
NIOS-56217	Major	A scheduled discovery job failed to start if the time zone was configured for UTC/CST.
NIOS-56209	Major	A CSV import triggered high CPU utilization.
NIOS-56357	Major	After enabling Microsoft synchronization, Grid Manager became sluggish and swap usage increased.
NIOS-56166	Major	DNS integrity check returned a “None” status for a domain that did not have delegation and had a dotted label between the parent label and the actual domain.
NIOS-56100	Major	DNS service failed to start due to an undefined ACL syntax error.
NIOS-56050	Major	Unable to remove Microsoft servers from the Grid due to undefined email address for a zone.
NIOS-56027	Major	The appliance logged DNSSEC error messages about missing private key files even though they were not required for pre-published keys.





## NIOS 7.3.0 Release Notes

NIOS-55986	Major	The appliance stopped counting DNS queries after an upgrade even though monitoring was enabled.
NIOS-55984	Major	Unable to save modified member DNS properties.
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-55901	Major	The appliance might send invalid email alerts when a change in the monitoring state happened without a valid monitoring object.
NIOS-55855	Major	The appliance was unable to load Global Smart Folders; and the folders were marked as invalid in Grid Manager.
NIOS-55851	Major	vNIOS for KVM could not run probably on certain NIOS versions.
NIOS-55842	Major	The permission table for resources was missing in the “Create Object Permissions” dialog for a network.
NIOS-55833	Major	The <i>DNS Query Rate by Server/Server Group</i> report might display incorrect data on the IB-4030 appliance due to data parsing issues.
NIOS-55830	Major	In the <i>Infoblox NIOS Administrator Guide</i> , added information about remote admin objects being purged after 180 days without activities.
NIOS-55827	Major	Captive Portal service failures occurred after deleting the self-signed certificate.
NIOS-55821	Major	High CPU usage was observed after an upgrade due to memory issues related to a large number of host objects and host address objects.
NIOS-55812	Major	Network Insight: The appliance returned an error when users tried to drill down to the Interface tab of a discovered device.
NIOS-55763	Major	DHCP service went into a restart loop on one of the DHCP failover peers, causing DHCP outage.
NIOS-55693	Major	Reporting: Downloading and emailing PDF for reports failed.
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-55667	Major	The reporting server failed to display reports for certain Grid members.
NIOS-55630	Major	Updated information about NTP service on different interfaces in the <i>Infoblox NIOS Administrator Guide</i> .
NIOS-55628	Major	Addressed the following vulnerabilities: CVE-2015-6563: Fixed a privilege separation weakness related to PAM support. Attackers who could successfully compromise the pre-authentication process for remote code execution and who had valid credentials on the host could impersonate other users. CVE-2015-6564: Fixed a use-after-free bug related to PAM support that was reachable by attackers who could compromise the pre-authentication process for remote code execution.
NIOS-55594	Major	The appliance treated a trailing escape character (\) as an invalid character in a TXT record.



## NIOS 7.3.0 Release Notes

NIOS-55567	Major	In an Anycast configuration, BGP peering was not automatically re-established after the connection dropped.
NIOS-55545	Major	Under certain circumstances, HA members experience DNS outage after an upgrade.
NIOS-55497	Major	WAPI: The <code>pxe_lease_time</code> 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-55496	Major	This release adds a few enhancements to the <i>DNAME Record</i> wizard and editor to avoid a DNAME loop, in which the owner name is identical to the RDATA.
NIOS-55489	Major	The FTP server failed to provide configuration files to VoIP phones after a PBX reset.
NIOS-55468	Major	IPv4 DHCP option logic filters associated with DHCP ranges were no longer visible in Grid Manager after an upgrade if DHCP option filters were deployed and inheritance was enabled before the upgrade.
NIOS-55467	Major	Unable to set up an HA passive node through the NIOS Setup Wizard.
NIOS-55458	Major	Menu items were missing from the Action menu of the static and pool licenses in the <b>Active Licenses</b> tab.
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-55264	Major	API: Users were able to configure the IB-100 appliance as a Grid Master, which is not supported.
NIOS-55239	Major	Unable to use the <code>set partnerdown</code> command on the secondary DHCP failover peer in the maintenance mode.
NIOS-55234	Major	The <code>reset all secure</code> command did not remove all data in the <i>/storage/reporting-capture-data</i> directory.
NIOS-55218	Major	Grid Master failed to display reports due to report timeouts, despite proper communications between the forwarder and indexer.
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-54860	Major	Cloud Network Automation: Unable to send WAPI calls using the cloud-api-only admin group.
NIOS-54762 NIOS-54263	Major	Required and inherited extensible attributes from the parent level were not populated after converting an unmanaged object to a host record.
NIOS-54721	Major	Incomplete CSV and PDF files received for exports of reporting data.
NIOS-54407	Major	The DHCP server was unable to update DNS entries and received REFUSED responses.
NIOS-54244	Major	The IPAM tab displays incorrect usage percentage for a network.



## NIOS 7.3.0 Release Notes

NIOS-52958	Major	Did not get leases for fixed addresses when the “Enable immediate fixed address configuration changes” option was selected in the <i>Grid DHCP Properties</i> editor.
NIOS-51536	Major	Performing certain tasks in Grid Manager took longer than expected.
NIOS-48008	Major	Unable to retrieve network names from some DHCP ranges.
NIOS-31917	Major	Unable to group discovered managed data in smart folders.
NIOS-57690	Minor	PAPI: Limited-access users could not perform a VM registration.
NIOS-57512	Minor	Clicking the syslog bookmark for a Grid member redirected users to the syslog for another member.
NIOS-57183	Minor	Clarified the online Help related to the “Keep local copy” when scheduling a Grid backup.
NIOS-57140	Minor	PAPI: Under certain circumstances, users could not copy an HA member.
NIOS-56950	Minor	Missing sysObjectIDs for PT appliances in the <i>Infoblox NIOS Administrator Guide</i> .
NIOS-56824	Minor	The CLI command <code>set partnerdown</code> for a DHCP failover peer did not function properly.
NIOS-56819	Minor	Cloud Network Automation: The VPN communication between the Consolidator and Probes was not documented.
NIOS-56782	Minor	Documented the reason for IP discovery to send packets to the UDP 40125 port.
NIOS-56737	Minor	Fixed the OID for IB-DNSQUERYRATE in the <i>Infoblox NIOS Administrator Guide</i> .
NIOS-56654	Minor	An SNMP manager failed to receive test SNMP traps from the NIOS appliance.
NIOS-56628	Minor	The appliance intermittently returned an error when users opened the <b>Administration</b> tab in Grid Manager.
NIOS-56606	Minor	Threat Protection: The name resolving time out interval was too short for threat protection test connection.
NIOS-56396	Minor	In the <i>Infoblox NIOS Administrator Guide</i> , added information about DHCP Utilization for network and range to include abandoned addresses or leases.
NIOS-56208	Minor	Fixed an error in the description of the <code>set transfer_supportbundle</code> CLI command.
NIOS-56188 NIOS-55506	Minor	When adding a DNAME record, users could use the domain name of a zone in the DNAME data portion, which could cause a circular reference.
NIOS-56176	Minor	Clarified the description for “Proxy Access Control” in the <i>Infoblox NIOS Administrator Guide</i> .
NIOS-56175	Minor	Added timestamp to the <code>show cores</code> CLI command.
NIOS-56170	Minor	PAPI: Traffic capture calls using API did not work when the interface was set to LAN/LAN1.
NIOS-56124	Minor	When generating a User Login History report using the filters “User Status equals Active” and “User Status equals Timed Out,” the report showed incorrect status.
NIOS-56116	Minor	A CSV import failed while trying to restore some host records.



## NIOS 7.3.0 Release Notes

NIOS-56105	Minor	On some occasions, users were unable to save extensible attribute values because the <b>Save</b> button was disabled.
NIOS-56083	Minor	A limited-access user group encountered an issue when trying to trying to navigate to a DNS zone.
NIOS-56054	Minor	Fixed the documentation to reflect that the IB-4030 appliance fully supports IPv4 and IPv6 queries.
NIOS-55967	Minor	Users encountered some LCD issues on the passive node of the HA Grid Master.
NIOS-55964	Minor	Unable to configure the “remove-subnet” field in the CSV import file due to an incorrect reference (“remove_subnet”) documented in the <i>CSV Import Reference</i> .
NIOS-55854	Minor	Secondary zone data was not available for the root zone.
NIOS-55845	Minor	Fixed AWS endpoint example in the <i>Infoblox NIOS Administrator Guide</i> .
NIOS-55829	Minor	Fixed a typo in the <i>DNS Top RPZ Hits by Client</i> report.
NIOS-55775	Minor	Added port information to the <i>Infoblox NIOS Administrator Guide</i> and the <i>Installation Guide for vNIOS for AWS</i> .
NIOS-55694	Minor	Reporting: Search results were not copied to the SCP server based on the configuration.
NIOS-55643	Minor	Updated version 3.0.1 and 3.0.2 of the <i>Installation Guide for IPAM Plug-In for vCO</i> to reflect the correct information.
NIOS-55629	Minor	Added threat protection rules for EARLY PASS UDP in the <i>Infoblox NIOS Administrator Guide</i> .
NIOS-55627	Minor	Unable to set external primary DNS servers to stealth mode.
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-55583	Minor	The SNMP values were swapped between the active and passive nodes of an HA pair.
NIOS-55552	Minor	Added a note to the WAPI documentation to remind users to set the zone_format value when creating reverse-mapping zones.
NIOS-55470	Minor	For the “Synchronize Network Users” option in Network Users tab of the Microsoft Server Properties editor, Grid Manger displayed “Inherited from Upper Level” instead of “Inherited from Grid.”
NIOS-55444	Minor	The Edit menu item was missing from the Action menu of DNS resource records.
NIOS-55405	Minor	The audit log history did not record the creation or modification of a host record.
NIOS-55284	Minor	Selecting a network view in the <i>Network View Selector</i> could slow down some operations if the page size for the selector was configured for a larger value.
NIOS-55277	Minor	API: Under certain circumstances, users could not retrieve all extensible attribute definitions through the API.
NIOS-54753	Minor	Inconsistent NIOS versioning could cause automated PAPI updates to fail.
NIOS-53793	Minor	Microsoft Management: Synchronization test could fail if the “Use same credential as DNS/DHCP services” option was enabled.



## NIOS 7.3.0 Release Notes

NIOS-53598	Minor	Grid Manager performance was affected when adding more than one record to a large DNS zone.
NIOS-53164	Minor	A CSV import failed when an ACL list contain a large number of entries.
NIOS-52351	Minor	A host record could appear twice in a smart folder.
NIOS-52035	Minor	The traffic capture limit was inadequate for threat protection appliances.
NIOS-51640	Minor	The tenant name was not included in the <i>VM Address History</i> report.
NIOS-49306	Minor	The modification of BOOTP properties of a host IP address was not recorded in the audit log.
RFE-6323	Enhance	Infoblox now provides an option to set the prefix length limit for RPZ-IP triggers so you can avoid the possibility of DNS outage resulting from errors in the RPZ policies received from external sources by the RPZ feed or due to errors in the RPZ rules added to the local RPZ.

### 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
N/A	Infoblox has upgraded the software for our user community ( <a href="http://community.infoblox.com">community.infoblox.com</a> ), which will offer users enhanced features and a more robust experience. This new community software however, is not compatible with our community dashboard widget. As a result, the functionality of the <i>Community Dashboard</i> widget is inconsistent. The <i>Community Dashboard</i> widget will subsequently be removed in the next NIOS maintenance release.
NIOS-58000	In AWS, if the admin-password set as part of the user data is modified later in virtual NIOS appliance, it will be reverted back to the original user data password during a NIOS upgrade.
NIOS-57932	Reporting and Analytics: Alerts are not generated for some of the reports in the DHCP Fingerprint category.
NIOS-57930	Reporting and Analytics: Object permissions for certain system searches are not migrated after an upgrade. Workaround: Superusers can fix these permissions for limited-access users when necessary.
NIOS-57850	Reporting and Analytics: Custom logos in report PDFs might not appear properly if the logo is in JPEG format. Workaround: Use logos that are in PNG format.





## NIOS 7.3.0 Release Notes

NIOS-56982	Reporting and Analytics: Unable to copy or bookmark a page using the “Link to Job” option in the Job Settings dialog in the <b>Splunk -&gt; Reports</b> page.
RPTNEXTGEN-558	Reporting and Analytics: You cannot set any dashboard as the home dashboard. The <b>Set as Home Dashboard</b> option available in the <b>Edit</b> drop-down will not add dashboards to the <b>Home Dashboard</b> tab.
RPTCLUSTER-337	Reporting and Analytics: Time zone information is not displayed for the following reports: <i>DNS Domains Queried by Client</i> , <i>Top DNS Clients by Query Type</i> , <i>Top DNS Clients Querying MX Records</i> , and <i>DNS Domain Query Trend</i> .
RPTCLUSTER-331	Reporting and Analytics: User might not be authorized to use the reporting service and cannot access the <b>Reporting</b> tab after restoring the NIOS Grid backup.
NIOS-57195	Microsoft Management: After configuring Microsoft AD servers in the Grid, the Microsoft managing member might go into a “synchronize” mode and restarts continuously.
NIOS-57041	MMDNS: Under certain circumstances, assigning multiple primaries to a Grid member might cause the member to fail.
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.
BEAU-443	Cloud Network Automation: In a scenario when you define extensible attributes that have the exact same name (such as Tenant ID) as the mandatory cloud extensible attribute before you install a cloud license in the Grid, the mandatory cloud extensible attribute creation will fail when you install the cloud license. Workaround: <ol style="list-style-type: none"> <li>1. Uninstalled the cloud license.</li> <li>2. Delete the extensible attributes that have the same name as the mandatory cloud extensible attributes.</li> <li>3. Install the cloud license again.</li> </ol>
DNSSDU-163	DNS Secure Dynamic Updates: Analysis might take longer than expected on the IB-4010 that has a 25% database capacity.
DNSSDU-222	DNS Secure Dynamic Updates: A Grid member might go offline if the record type for resource records is changed from “static” to “dynamic” after a DHCP failover.
ISE-249	Cisco ISE: Unable to create a network active user if the user is configured with Cisco ISE server using the standby server address.
NETMRI-26525	Network Insight: When adding seed routers through PAPI scripts, ensure that you specify the network view with which the seed router associates. Otherwise, the seed router object will be created without a network view association.