RELEASE NOTES

NIOS 9.0.4

June 2024

Table of Contents

Introduction

Infoblox NIOS™ 9.0.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 that the stated numbers and recommendations in this document are for reference only. They represent the results of lab testing in a controlled environment. To design and size a solution for a production environment, please contact your Infoblox Solution Architect.

Release Highlights

The NIOS 9.0.4 release contains the following number of feature enhancements, resolved issues, and addressed vulnerabilities.

Number of new features	23
Number of resolved issues	91
Number of addressed CVEs	6

Trinzic X6 Series

Infoblox NIOS 9.0.*x* introduces the new Trinzic X6 series of appliances that are more reliable, higher in performance, rich in features, and which have a lower carbon footprint than their earlier counterparts. The Trinzic X6 series comprises the following physical appliances:

- TE-906
- TE-1506
- TE-1606
- TE-2306
- TE-4106

The Trinzic X6 series appliances run only on NIOS 9.0.1 and later versions. The Trinzic X6 series physical appliances can also host Trinzic X5 series licenses. All the Trinzic X6 series appliances support the cloud platform. The Trinzic X6 series appliances report a 30% increase in DNS QPS and DHCP LPS performances.

For detailed information about the hardware and software appliances that comprise the Trinzic X6 series, see the detailed appliance documentation on the **Appliances** tab at docs.infoblox.com.

Supported Platforms

Infoblox NIOS 9.0.4 is supported on the following platforms:

- Trinzic Appliances: TE-815, TE-825, TE-1415, TE-1425, TE-2215, TE-2225, TE-4015, TE-4025, TE-926, TE-1516, TE-1526, TE-2326, TE-4126
- Trinzic Virtual Appliances: IB-V815, IB-V825, IB-V1415, IB-V1425, IB-V2215, IB-V2225, IB-V4015, IB-V4025, IB-FLEX, IB-V926, IB-V1516, IB-V1526, IB-V2326, IB-V4126
- Trinzic Reporting Appliances: TR-805, TR-1405, TR-2205, TR-4005, TR-5005 (can be configured on TE-1526, TE-2326, TE-4126).
- Trinzic Reporting Virtual Appliances: IB-V805, IB-V1405, IB-V2205, IB-V4005, IB-V5005
- Cloud Platform Appliances: CP-V805, CP-V1405, CP-V2205
- Network Insight Appliances: ND-805, ND-1405, ND-2205, ND-4005, ND-906, ND-1606, ND-2306, ND-4106
- Network Insight Virtual Appliances: ND-V805, ND-V1405, ND-V2205, ND-V4005, ND-V906, ND-V1606, ND-V2306, ND-V4106

NOTE: TE appliances are also known as IB appliances.

The following appliances are not supported in NIOS 9.0.*x*: PT-1405, PT-2205, PT-2205-10GE, IB-4030-10GE, and all of the X0 Series appliances such as the Infoblox 100 Series, Infoblox 800 Series, Infoblox 1400 Series, Infoblox 2200 Series, Infoblox 4000 Series, Infoblox 4010 Series, Infoblox 4030 Series.

Upgrade Paths/Before You Install

Infoblox NIOS 9.0.4 supports the following upgrade paths:

- 9.0.3 and earlier 9.0.*x* releases
- 8.6.4 and earlier 8.6.*x* releases
- 8.5.5 and earlier 8.5.*x* releases
- 8.4.8 and earlier 8.4.*x* releases

Even though Infoblox supports the upgrade paths mentioned above, Infoblox has tested and validated only the following upgrade paths for NIOS 9.0.4. Infoblox recommends that you upgrade to NIOS 9.0.4 from these tested and validated releases:

9.0.3, 9.0.2, 8.6.4, 8.6.3, 8.6.2, 8.5.5, 8.5.2, and 8.4.8

You cannot upgrade to NIOS 9.0.4 from NIOS 8.3.x and earlier releases.

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.

If there are pending actions such as a restart or a reboot from past hotfix applications, ensure that these are complete before starting the upgrade process. Failure to do so may cause irreparable harm to your installation. See the "Upgrade Guidelines" section in these Release Notes for information about how to gather pending action data and resolve the actions.

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.

Virtual vNIOS Appliances

Infoblox supports the following vNIOS virtual appliances. Note that Infoblox does not support running vNIOS in any nested VMs or VM-inside-VM configuration.

Note: When using vNIOS appliances, ensure that the host system supports synchronous power safe input output to obtain power redundancy.

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 8.0U2, 8.0b, 7.0.3, 7.0.2, 7.0, 6.7 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 capacities. Some vNIOS appliances are not supported as Grid Masters or Grid Master Candidates. For more information about vNIOS on VMware, refer to the Infoblox Installation Guide for vNIOS Software on VMware.

vNIOS for Microsoft Server 2019 and 2016 Hyper-V

The Infoblox vNIOS virtual appliance is now available for Windows Server 2019 and Windows Server 2016 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 for optimal performance, vNIOS for Hyper-V is not recommended as a Grid Master or Grid Master Candidate. For more information about vNIOS for Hyper-V, refer to the Infoblox Installation Guide for vNIOS on Microsoft Hyper-V.

NOTE: NIOS virtual appliance for Hyper-V is not recommended as a Grid Master or Grid Master Candidate.

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.

NOTE: KVM-based OpenStack deployments are supported on the RHOSP 17.1, 16.0 platforms.

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 carrier-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.

vNIOS for Azure

Infoblox vNIOS for Azure is an Infoblox virtual appliance designed for deployments through Microsoft Azure, a collection of integrated cloud services in the Microsoft Cloud. The vNIOS for Azure enables you to deploy robust, manageable, and cost effective Infoblox appliances in the Microsoft Cloud. Infoblox NIOS provides core network services and a framework for integrating all the components of the modular Infoblox solution. It provides integrated, secure, and easy-to-manage DNS (Domain Name System) and IPAM (IP address management) services. You can deploy one or more Infoblox vNIOS for Azure instances through the Microsoft Azure Marketplace and provision them to join the on-premises

NIOS Grid. You can then use the vNIOS for Azure instance as the primary DNS server to provide carrier-grade DNS and IPAM services in the Microsoft Cloud. You can also utilize Infoblox Cloud Network Automation with your vNIOS for Azure instances to streamline with IPAM, improve visibility of your cloud networks, and increase the flexibility of your cloud environment.

vNIOS for Azure is supported on the Microsoft Azure public cloud, Microsoft Azure Government, and Microsoft Azure Stack Hub flavors. For more information about vNIOS for Azure, refer to the Infoblox Installation Guide for vNIOS for Microsoft Azure.

vNIOS for GCP

Infoblox vNIOS for GCP is an Infoblox virtual appliance that enables you to deploy robust, manageable, and cost-effective Infoblox appliances in the Google Cloud. Infoblox vNIOS provides core network services and a framework for integrating all the components of the modular Infoblox solution. It provides integrated, secure, and easy-to-manage DNS (Domain Name System) and IPAM (IP address management) services. For more information, see the Infoblox Installation Guide for vNIOS for GCP.

vNIOS for Nutanix AHV

Infoblox vNIOS for Nutanix enables you to deploy large, robust, manageable, and cost-effective Grids. Infoblox NIOS virtual appliance for Nutanix functions as a hardware virtual machine guest on the Linux system. It provides integrated, secure, and easy-to-manage DNS, DHCP, and IPAM services and a framework for integrating all the components of the modular Infoblox solution. For more information, see the Infoblox Installation Guide vNIOS for Nutanix AHV.

vNIOS for Red Hat OpenShift

Infoblox vNIOS for Red Hat OpenShift is a virtual appliance designed for deployment on Red Hat® OpenShift®, an enterprise-ready Kubernetes container platform. The virtual appliance enables you to deploy large, high-performance, robust, manageable, and cost-effective Infoblox Grids. The NIOS virtual appliance for Red Hat OpenShift functions as a virtual machine running on KubeVirt virtualization. It provides integrated, secure, and easy-to-manage DNS service. For more information, see the *Infoblox Installation Guide vNIOS for Red Hat OpenShift*.

vNIOS for Oracle Cloud Infrastructure

Infoblox vNIOS for Oracle Cloud Infrastructure is a virtual appliance designed for deployment on Oracle Cloud Infrastructure, an infrastructure as a service that is offered by Oracle. The virtual appliance enables you to deploy large, robust, manageable, and cost-effective Infoblox Grids. The NIOS virtual appliance for Oracle Cloud Infrastructure functions as a hardware virtual machine guest on the Linux system. It provides integrated, secure, and easy-to-manage DNS, DHCP, and IPAM services. It also provides a framework for integrating all components of the modular Infoblox solution. For more information, see the *Infoblox Installation Guide vNIOS for Oracle Cloud Infrastructure*.

New Features

This section lists new features in the 9.0.*x* releases.

NIOS 9.0.4

High Availability Support on Public Clouds for vNIOS (RFE-12151)

Starting from NIOS 9.0.4, you can deploy vNIOS appliances in high availability (HA) configurations on public clouds. The following vNIOS instances are supported for HA in public cloud: vNIOS for AWS, vNIOS for Microsoft Azure, vNIOS for GCP. For more information, see the vNIOS documentation for the respective appliances at
https://docs.infoblox.com/space/Appliances/35364966/Virtual+Appliances

Turning Off Upstream IPv6 Queries When Dual Mode is Configured (RFE-11941)

From NIOS 9.0.4 onwards, you can restrict upstream queries to either IPv4 or IPv6 addresses without impacting downstream queries when the configuration allows dual network interfaces for DNS services. You can do this using the newly introduced *Member DNS Configuration* > **General** > **Basic** > **Upstream Address Family Preference** option. This feature works only if the **Allow recursion** checkbox is selected at the Grid or member level. For more information, see the "Configuring Upstream Address Family Preference" topic in the NIOS online documentation.

Extended DNS Support (EDNS0) for Device ID (RFE-13672)

NIOS 9.0.4 introduces Extended DNS Support (EDNS0) for Device ID (Type 26946). Subscriber services will utilize the EDNS0 data to enhance security and content-based DNS request filtering.

Unify Daylight Savings Across All Time Zones (RFE-13122)

Prior to NIOS 9.0.4, if the time zone of Grid Manager was UTC +2:00 Cairo (Egypt) and Daylight Saving Time (DST) had begun, NIOS was running one hour behind the actual time because it did not consider Egypt's DST.

From NOS 9.0.4 onwards, NIOS will not use static UTC offsets such as (UTC+2:00). Instead, it will only have time zone names with DST changes. To achieve this, NIOS fetches the time zone list from the Ubuntu tzdata package and updates the same in the database.

After upgrading to NIOS 9.0.4, certain time zone names are mapped to different names. For the list of the changed time zone names, see the "General Upgrade Guidelines" topic in the NIOS online documentation. Note that some of the new time zone formats contain an underscore "_" in the name.

vDiscovery to Support Discovery Across Multiple AWS and GCP Accounts (RFE-8680)

You can now configure a vDiscovery job on NIOS 9.0.4 or later to discover and synchronize data across multiple AWS or GCP accounts across a single or across multiple regions. For more information, see the "vDiscovery on AWS VPCs" topic in the vNIOS for AWS and the "Performing GCP vDiscovery"

topic in the “vNIOS for GCP” online documentation at https://docs.infoblox.com/space/Appliances/35364966/Virtual+Appliances

Configuring the Network Insight Polling Frequency Modifier (RFE-13024)

NIOS 9.0.4 introduces the Polling Frequency Modifier field that allows you to specify the polling frequency to occur once every two days or twice a day. You can set values between 0.5 and 2 in this field. For more information, see the “Configuring Discovery Properties” topic in the NIOS online documentation.

Support DNS Authoritative with DNS Cache Acceleration Recursive (RFE-11029)

You can now configure the virtual DNS Cache Acceleration (vDCA) member to also be an authoritative member. When the virtual DNS Cache Acceleration member is configured to authoritative zones, those authoritative queries will not be cached in virtual DNS Cache Acceleration.

TCP DNS Query Support for DNS Cache Acceleration (RFE-12976)

From NIOS 9.0.4 onwards, virtual DNS Cache Acceleration caches TCP queries and the cached queries are responded to from virtual DNS Cache Acceleration instead of BIND. The following new CLI commands are introduced that display the DNS Over TCP details such as the configuration settings, current status of DNS over TCP service, statistics related to DNS over TCP traffic, and so on. For more information see the “show dns-over-tcp-dca-stats”, “show dns-over-tcp-dca-status”, “show dns-over-tcp-dca-config”, and “set vdca-tcp-mode” topics in the NIOS online documentation.

- show dns-over-tcp-dca-stats
- show dns-over-tcp-dca-status
- show dns-over-tcp-dca-config
- set vdca-tcp-mode

When there is a TCP DNS query load, if you make changes to features that push new configurations to the virtual DNS Cache Acceleration file (for example, enable/disable TCP support on virtual DNS Cache Acceleration, toggling Advanced DNS Protection first/DNS Cache Acceleration first, and toggling single/multi TCP queries in a session), performing a DNS force restart may cause the Grid member to go offline. To recover from this issue, Infoblox recommends that you perform a product reboot.

TLS 1.3 Support (RFE-7727)

NIOS 9.0.4 supports TLS version 1.3 which provides the ability to enable or disable the TLS 1.3 protocol and the respective cipher suites in the CLI. TLS 1.3 will be enabled by default. However, Splunk does not support TLS version 1.3 and therefore NIOS reporting will not work when only TLS version 1.3 is enabled. A warning to this effect is displayed if you disable TLS version 1.2. If you have a reporting server in the NIOS Grid, you must ensure that TLS 1.2 is not disabled.

Specifying the Source IP Address using WAPI (RFE-10242)

From NIOS version 9.0.4 onwards, the `query_fqdn_on_member` WAPI function allows you to specify the source IP address. In versions prior to NIOS 9.0.4, the source IP address was automatically selected (internally), typically defaulting to LAN1.

Shared VPC Support in GCP (RFE-10561)

From NIOS 9.0.4 onwards, if you want to discover shared resources (resources deployed in a shared Virtual Private Cloud) using vDiscovery, ensure that the host project(s) and its service project(s) run on the same member or virtual node. Also ensure that you discover the host project(s) first followed by the service project(s).

vDiscovery Across Multiple AWS GovCloud Accounts (RFE-12012)

From NIOS 9.0.4 onwards, you can use vDiscovery to perform discovery across multiple AWS accounts for AWS GovCloud accounts.

Integrating the Cloud Sync Service for AWS Route 53 DNS Synchronization (NIOS-94340)

From NIOS 9.0.4 onwards when configuring Route 53 integration, you can enable the multi-account synchronization option on an existing or a new sync group. The option enables NIOS to discover multiple AWS accounts in an AWS organization and to synchronize the DNS data using the Route 53 service. You can configure the option to synchronize DNS data from all or specific accounts (children) in an AWS organization (parent). For more information, see the "Configuring Amazon Route 53 Integration" topic in the "vNIOS for AWS" online documentation at https://docs.infoblox.com/space/Appliances/35364966/Virtual+Appliances

vDiscovery Migration to the Cloud Sync Service in GCP (NIOS-95597)

From NIOS 9.0.4 onwards, the Cloud Sync Service needs be started before starting GCP vDiscovery.

Synchronization of Azure DNS (RFE-11046)

In NIOS 9.0.4, you can use the Azure DNS synchronization feature to enable NIOS to span across Azure virtual networks to discover and integrate Azure DNS data with the NIOS database to get a unified console experience in NIOS. You can configure it to discover and synchronize data across multiple subscriptions of an Azure tenant. For more information, see the "Integrating Azure DNS with NIOS" in the vNIOS Infoblox Installation Guide for Microsoft Azure at https://docs.infoblox.com/space/Appliances/35364966/Virtual+Appliances

Advanced DNS Protection and DNS Cache Acceleration Support on Mellanox Cards (RFE-12983)

The Advanced DNS Protection and DNS Cache Acceleration features are now supported on NVIDIA Mellanox 25 GbE cards.

IB-FLEX Support on Trinzic X6 Series Appliances (NIOS-87387)

All of the Trinzic X6 Series appliances can now function as IB-FLEX appliances if the hardware type is set to IB-FLEX using the `set hardware-type` CLI command. The DNS Cache Acceleration service runs on all Trinzic X6 Series appliances when used as IB-FLEX. However, Infoblox recommends to use DNS Cache Acceleration only on TE-2306 and TE-4106 appliances.

Splunk Updates

NIOS 9.0.4 supports Splunk version 9.1.3. NIOS 9.0.4 contains a new dashboard called the jQuery Upgrade dashboard in the **Reporting** > **Administration** tab that provides comprehensive instructions to identify affected dashboards and ensures their compatibility with jQuery 3.5 or higher.

Accelerated Advanced DNS Protection Support for TE-906 Appliances

The TE-906 series of appliances now supports fastpath enabled services such as encrypted DNS (DoH/DoT), Advanced DNS Protection (Threat Protection with acceleration), and DNSTAP.

Search Functionality for the binding_state Field (RFE-9219)

From NIOS 9.0.4 onwards, the DHCP lease object "binding_state" WAPI field is available for search.

Removal of the Deprioritize caching of NXDOMAIN responses option

From NIOS 9.0.4 onwards, in the *Grid DNS Properties* or *Member DNS Properties* editor, **Security** tab > **Bogus-query alerting and mitigation** section, the **Deprioritize caching of NXDOMAIN responses** option has been removed.

Support for Virtual Advanced DNS Protection and Virtual DNS Cache Acceleration in vNIOS for AWS (RFE-8736)

vNIOS AWS instances running on NIOS 9.0.1 or later can be configured with virtual Advanced DNS Protection (vADP) to detect DNS threats and prevent possible network attacks.

vNIOS AWS instances running on 9.0.1 or later also support virtual DNS Cache Acceleration, which when enabled configure the instances as high-speed DNS caching-only name servers.

For more information on virtual Advanced DNS Protection, see the “About Infoblox Advanced DNS Protection” topic in the NIOS online documentation and for the list of supported vNIOS for AWS appliances, see the Installation Guide for vNIOS for AWS at https://docs.infoblox.com/space/Appliances/35364966/Virtual+Appliances

VLAN Support for NIOS Appliances (RFE-99636)

VLAN tagging is now supported on all Trinzic X5 and X6 Series appliances.

NIOS 9.0.2

Support for IPv6 Relay Agent Option Filters (RFE-12987)

NIOS 9.0.2 introduces three IPv6 relay agent filters for the DHCPv6 option filter:

- dhcp6.subscriber-id(38) string
- dhcp6.remote-id(37) string
- dhcp6.interface-id(18) string

You can use the **IPv6 Option Filter option** to selectively filter and process specific options sent by the IPv6 relay agent. You can set the **Relay Agent** field to a value from 0 to 33.

For more information, see the "Defining Option Filters" topic in the NIOS online documentation.

DNS Type 64/ Type 65 Caching Support on Virtual DNS Cache Acceleration (RFE-12820)

NIOS 9.0.2 introduces the `expand` argument to the `show dns-accel-cache` CLI command. The `expand` argument displays the expanded DNS type 64/DNS type 65 records stored in the virtual DNS Cache Acceleration cache. The `expand` argument is only applicable to DNS type 64/DNS type 65 records. The `show dns-accel-cache` CLI command is restricted to 255 bytes in size and is compressed for DNS type 64 and DNS type 65 records.

For more information, see the "show dns-accel-cache" topic in the NIOS online documentation.

Trinzic X6 Series Appliance Support for vNIOS for OCI (RFE-13528)

From NIOS 9.0.2 onwards, vNIOS for Oracle Cloud Infrastructure (OCI) is supported on the Trinzic X6 series of appliances. Also from NIOS 9.0.2 onwards, you can deploy a vNIOS for OCI node as a Grid Master as well a Grid member. For more information, see *Infoblox Installation Guide vNIOS for Oracle Cloud Infrastructure* at https://docs.infoblox.com

NIOS 9.0.1

Trinzic X6 Series Appliances

Infoblox NIOS 9.0.1 introduces the new Trinzic X6 series of appliances. that are more reliable, higher in performance, rich in features, and which have a lower carbon footprint than their earlier counterparts. The Trinzic X6 series of hardware appliances comprises the following: TE-906, TE-1506, TE-1606, TE-2306, TE-4106

For detailed information about the hardware and software appliances that comprise the Trinzic X6 series, see the detailed appliance documentation on the **Appliances** tab at docs.infoblox.com.

Verifying Licenses

In NIOS 9.0.1, you can check if the licenses are valid, view the comparison between the existing and newly added licenses, and verify for any license conflicts by clicking **Verify License(s)** on the **Licenses**

tab > **Member** tab or **Pool** tab or **Grid-Wide** tab. If the licenses pass validation, they will be applied. You can either confirm or cancel applying new licenses. You can also view the licenses will be discarded or overwritten. For more information, see the "Managing Licenses" topic in the NIOS online documentation.

vNIOS X5 Series and X6 Series Appliance Specifications

Infoblox NIOS virtual appliances support any hardware that provides the required Hypervisor version, memory, CPU, and disk resources. To maintain high performance on your NIOS virtual appliances and to avoid not having enough resources to service all the NIOS virtual appliances, do not oversubscribe physical resources on the virtualization host. Required memory, CPU, and disk resources must be adequately allocated for each virtual appliance that is running on the virtualization host. For information about the required specification for each NIOS virtual appliance model, see the following table.

NOTE:

- Starting from NIOS 9.0.1, the default fixed size for a fresh NIOS installation has changed to 500 GB. However, you can still use resizable images to customize the VM disk size. Infoblox recommends a minimum disk size of 250 GB.
- The numbers in the tables are based on a broad reference and may vary depending on your deployment, shape selected, and other parameters. For the exact specifications, please see the specific vNIOS documentation at https://docs.infoblox.com/space/Appliances/35364966/Virtual+Appliances

vNIOS X5 Series Appliance Specifications

The following table lists the required memory, CPU, and disk allocation for each supported Infoblox virtual appliance model in the X5 series. The cloud platforms columns indicate vNIOS cloud platforms. For example, the VMware column indicates vNIOS for VMware.

NIOS Virtual Appliances	Primary Disk (GB)	# of vCPU Cores	Memory Allocation (GB)	VMware	MS Hyper-V	KVM	Azure, AWS, GCP	Nutanix AHV	Red Hat OpenShift	Grid Master and Grid Master Candidate
IB-V815	500	2	16	✓	✓	✓	×	✓	×	Yes
IB-V825	500	2	16	✓	✓	✓	✓	✓	×	Yes
IB-V1415	500	4	32	✓	✓	✓	×	✓	×	Yes
IB-V1425	500	4	32	✓	✓	✓	✓	✓	×	Yes
IB-V2215	500	8	64	✓	✓	✓	×	✓	×	Yes
IB-V2225	500	8	64	✓	✓	✓	✓	✓	✓	Yes
IB-V4015	500	14	128	✓	✓	✓	✓	×	✓	Yes
IB-V4025	500	16	128	✓	✓	✓	✓	×	×	Yes

Network Insight Virtual Appliances	Overall Disk (GB)	# of vCPU Cores	Memory Allocation (GB)	VMware	MS Hyper-V	KVM	AWS, Azure	Nutanix AHV	Grid Master and Grid Master Candidate
ND-V805	500	4	32	✓	✓	✓	✓	×	No
ND-V1405	500	8	32	✓	✓	✓	✓	✓	No
ND-V2205	500	16	64	✓	✓	✓	✓	×	No
ND-V4005	500	32	128	✓	✓	✓	✓	×	No

NOTE:

- X5 series ND appliances are not supported on GCP.
- The overall disk space in NIOS reporting virtual appliances is the value mentioned in the Overall Disk column plus user defined reporting storage.

NIOS Reporting Virtual Appliances	Overall Disk (GB)	# of vCPU Cores	Memory Allocation (GB)	VMware	MS Hyper-V	KVM	AWS, Azure	Nutanix AHV	Grid Master and Grid Master Candidate
IB-V805	500	2	32	✓	✓	✓	×	×	No
IB-V1405	500	4	128	✓	✓	✓	û	û	No
IB-V2205	500	8	64	✓	✓	✓	û	û	No
IB-V4005	500 (+ 1500 GB reporting storage	14	128	✓	✓	✓	û	û	No
IB-V5005	User defined reporting storage	User defined	User defined	✓	✓	✓	✓	✓	No

Cloud Platform Appliances	Overall Disk (GB)	# of vCPU Cores	Memory Allocation (GB)	VMware	MS Hyper-V	KVM	AWS, Azure, GCP	Nutanix AHV	Oracle Cloud Infrastructure	Grid Master and Grid Master Candidate
CP-V805	500	2	16	✓	✓	✓	✓	✓	×	No
CP-V1405	500	4	32	✓	✓	✓	✓	✓	×	No
CP-V2205	500	8	64	✓	✓	✓	✓	✓	✓	No

NOTE:

- When running NIOS in MS Hyper-V with dynamic memory allocation enabled, your system might experience high memory usage. To avoid this issue, Infoblox recommends that you disable dynamic memory allocation.
- For optimal performance, vNIOS for Hyper-V is not recommended as a Grid Master or Grid Master Candidate.
- Specifications of vNIOS for Microsoft Azure Stack Hub are different from the other vNIOS for Microsoft Azure flavors. For the exact specifications, see the *Infoblox Installation Guide vNIOS for Microsoft Azure* at https://docs.infoblox.com/space/Appliances/35364966/Virtual+Appliances
- To achieve best performance on your virtual appliances, follow the recommended specifications and allocate your resources within the limits of the licenses being installed on the appliances.
- vNIOS for AWS is supported on the IB-V4025 appliance from NIOS 8.5.2 onwards and on the IB-V4015 appliance running NIOS 8.6.2 and NIOS 8.6.3. vNIOS for Azure and vNIOS for GCP are supported on the IB-V4015 and IB-V4025 appliances running NIOS 8.6.2 and NIOS 8.6.3.
- NIOS for KVM is supported in the following environments: Red Hat OpenStack and Ubuntu.

vNIOS X6 Series Appliance Specifications

The following table lists the required memory, CPU, and disk allocation for each Trinzic X6 series appliance model. The cloud platforms columns indicate vNIOS cloud platforms. For example, the VMware column indicates vNIOS for VMware.

X6 Series Appliances	Primary Disk (GB)	# of vCPU Cores	Memory Allocation (GB)	VMware	MS Hyper-V	KVM	Azure, AWS, GCP	Nutanix AHV	Red Hat OpenShift	OCI	Grid Master and Grid Master Candidate
IB-V926	500	8	32	✓	✓	✓	✓	✓	×	✓	Yes
IB-V1516	500	12	64	✓	✓	✓	✓	✓	×	✓	Yes
IB-V1526	500	16	64	✓	✓	✓	✓	✓	×	✓	Yes
IB-V2326	500	20	192	✓	✓	✓	✓	✓	✓	✓	Yes
IB-V4126	500	32	384	✓	✓	✓	✓	✓	✓	✓	Yes

X6 Series ND Appliances	Primary Disk (GB)	# of vCPU Cores	Memory Allocation (GB)	VMware	MS Hyper-V	KVM	Azure, AWS	Nutanix AHV	Red Hat OpenShift	Grid Master and Grid Master Candidate
ND-V906	500	8	32	✓	✓	✓	✓	✓	×	No
ND-V1606	500	16	64	✓	✓	✓	✓	✓	×	No
ND-V2306	500	20	192	✓	✓	✓	✓	×	×	No
ND-V4106	500	32	384	✓	✓	✓	✓	×	×	No

NOTE:

- X6 series ND appliances are not supported on GCP.
- NIOS for KVM is supported in the following environments: Red Hat OpenStack and Ubuntu.

Appliance Specifications for Threat Protection

The following table lists the required CPU and memory allocation for each supported Infoblox appliance model when Threat Protection is enabled:

NIOS Virtual Appliances	# of vCPU Cores	Memory Allocation (GB)
IB-V1415	4	32
IB-V1425	8	32
IB-V2215	16	64
IB-V2225	16	64
IB-V4015	28	128
IB-V4025	28	128
IB-V926	8	32
IB-V1516	12	64
IB-V1526	16	64
IB-V2326	20	192
IB-V4126	32	384

NOTE:

If you are running virtual DNS Cache Acceleration on the supported versions of the appliances listed in the table above, make sure that the appliances match the virtual CPUs provided in the table.

vNIOS for KVM Specifications

The following is the configuration required in the KVM server for optimal performance of vNIOS for KVM Hypervisor and KVM-based OpenStack. These specifications are for 40 Gigabit and 25 Gigabit Intel NICs.

- adaptive tx = off
- adaptive rx = off
- rx-usecs = 50
- tx-usecs = 50
- ethtool -G rx/tx = 4096
- vf maxrate 2G
- txqueuelen = 10000
- netdev_maxbacklog=300000
- service irqblance stop

Changes to Default Behavior

This section lists changes to the default behavior in NIOS 9.*x* releases.

NIOS 9.0.4

- With the 8.2 release of OpenSSH, the ssh-rsa algorithm, which relies on the SHA-1 hash, has been deprecated due to security concerns. NIOS does not support deprecated SHA-1 signature algorithms.
- In NIOS 9.0.4 and in Splunk the secured webhook uses Python 3.0. If the secured webhook scripts are written to work on a version lower than 3.0, they will not work as those versions have been deprecated in Splunk.
- NIOS groups that need to access the reporting server must follow the Splunk naming convention guidelines such as the characters must be in lowercase and must not contain spaces, colons, semicolons, forward slashes and commas.
- Earlier than NIOS 9.0.4, all support bundles that were downloaded from multiple Grid members contained the same file name. From NIOS 9.0.4 onwards, downloaded support bundles will have the file names in the following format:
  sb_<member_name/host_name>_[virtual_node_id]_<GM | GM-HA | GMC | GMC-HA | MEM | MEM-HA>_<YYYYMMDD_HHMMSS>
  If the length of the Grid member name or host name is greater than 25 characters, the virtual node ID is appended to the file name.
- In Splunk, all Simple XML dashboards require the version attribute to be set to 1.1 to certify that they are compatible with jQuery 3.5 or higher. The default Infoblox reporting dashboards have been updated with the `version="1.1"` attribute. But custom dashboards that have been created before the NIOS 9.0.4 upgrade will not have the version attribute specified. Therefore, post upgrade a warning message is displayed for such custom dashboards.
- From NIOS 9.0.4 onwards, in the *Grid DNS Properties* or *Member DNS Properties* editor, **Security** tab > **Bogus-query alerting and mitigation** section, the **Deprioritize caching of NXDOMAIN responses** option has been removed.
- From NIOS 9.0.4 onwards, in a cloud HA setup, if you want to join a cloud HA Grid member to a Grid Master, the passive node of the Grid member waits for 2 minutes before joining the Grid Master.
- From NIOS 9.0.4 onwards, to start the vDCA service, you must enable recursion at the Grid level or at the member level or at the view level.
- From NIOS 9.0.4 onwards, the size of the resizable image is 150 GB. You can increase the size but do not reduce it.
- In newer versions of NIOS, database pages swing from available memory to used memory thus providing for a more accurate accounting of memory. Therefore, situations in which huge

pages are used for DNS Cache Acceleration or Advanced DNS Protection, NIOS memory utilization may increase by 40% to 45%.

- In NIOS 9.0.4, the default value of the `show ssl_security_level` CLI command is 0 instead of 1. With upgraded OpenSSL, older protocols such as TLS versions 1.0 and 1.1 are pushed down to SECLEVEL=0.
- After a NIOS 9.0.4 upgrade, a banner message is displayed in Grid Manager if certain time zone names were present before the upgrade. For the list of these time zone names, see the "General Upgrade Guidelines" topic in the NIOS online documentation. Note that some of the new time zone formats contain an underscore "_" in the name.
- After the ability to generate reports for hardware appliances, three alerts are generated instead of one. The 'Flex Grid Activation' and 'Flex Grid Activation for Managed Services' licenses now have their own set of alerts. The alerts filter members based on ReportingSPLA extensible attribute value and therefore, the ib-dns-usage-report-per-month alert may not generate data.
- If virtual Advanced DNS Protection is enabled on IB-906, then after an upgrade to NIOS 9.0.4, acceleration is automatically enabled by an additional reboot.
- If the Cloud Platform banner is displayed and you close it, the banner will be closed permanently.
- The following are the changes to behavior in the **CSP Configuration** screen:
    - In the *Grid Properties Editor/Grid Member Properties Editor*, the **CSP Config** tab has been renamed to the **CSP Configuration** tab, and the **CSP Config** screen is now called the **CSP Configuration** screen. The UI labels in this screen have also changed.
    - Even though the **Inherit**/**Override** button has been removed, the override and inherit functionalities continue to work as is.
    - The **Test Settings** button is applicable only to the **HTTP Proxy** field.
    - You can save the value in the **HTTP Proxy** field only if you test the proxy setting by clicking the **Test Settings** button and the test is successful.
- The following are the changes in behavior related to TLS protocols from NIOS 9.0.4 onwards:
    - Splunk does not support TLS version 1.3 and therefore NIOS reporting will not work if you disable all other TLS versions and enable only TLS version 1.3. A warning to this effect is displayed if you enable only TLS version 1.3.
    - Enabling or disabling a TLS protocol automatically adds or removes its corresponding enabled cipher suites for the Apache server.
    - The Apache/SAML service is not affected by enabling or disabling the TLS cipher suites of a disabled TLS protocol.

    - To ensure system integrity, prior to enabling a TLS protocol. it is necessary to enable one of its respective cipher suites.
    - Disabling the last cipher suite of an enabled TLS protocol is not allowed.
- The following are the changes in behavior related to the Cloud Sync service from NIOS 9.0.4 onwards:
    - The "Cloud DNS Sync" service name has been changed to "Cloud Sync" service (even in WAPI).
    - The Cloud Sync service must be started before starting a vDiscovery job.
    - The **Stop** button has been removed for vDiscovery jobs.
    - It is not mandatory to have the Cloud Network Automation (CNA) license on the Grid Master to run the Cloud Sync service.
    - In the Grid Manager, the **Amazon** tab under **Grid** > **Grid Manager** has been changed to **Cloud DNS**.

NIOS 9.0.2

- There is a change in behavior in the ADP ruleset for type64/65 rules. They have been changed from the default value of DROP to the value of PASS. However, note the following behavior:
    - On the upgrade of the node running ADP to 9.0.2 and later, these rules continue to DROP type64/65 queries because the setting of these rules in the earlier releases is inherited in the new ruleset that gets downloaded or uploaded. In this case, you must manually change the action to PASS to allow DNS type 64/65 queries. If the rules were manually changed to PASS in the old ruleset, then PASS action is inherited in the new ruleset and the queries are allowed.
    - Note: If you configure a new node in NIOS 9.0.2 or a later release and then download or upload the ADP ruleset, the type64/65 rules will be PASS by default. Because of this, you will see changes in the DNS query statistics.
- When you upgrade from NIOS 8.6.3 to 9.0.2, an additional product restart occurs to support Trinzic X6 Series appliances post upgrade. This holds good only when you have installed a hotfix to support Trinzic X6 licenses on an 8.6.3 version.
- If you upload a certificate to a NIOS 9.0.2 or later Grid, the checks are performed in compliance with RFC-5280. Therefore, the upload of invalid certificates will fail and the following error message is displayed: "Certificate violates RFC 5280. See the log for details. This strict check may be disabled."
- If you close the CP license banner message that is displayed when you first log in to NIOS, the banner will be permanently disabled.

NIOS 9.0.1

- You cannot add a Cloud Platform license to a standalone system, or on a standalone Grid Manager, or on a Grid Master Candidate. You can only add the license if the node is a Grid member and there are no other license conflicts. If you try to add the license to a standalone system, the license is not applied.
- You cannot downgrade any Trinzic X6 appliances to a NIOS version below 9.0.1.
- You cannot install a NIOS license type from the Grid Manager on Trinzic X6 series hardware appliances. You must use the CLI to install the licenses.
- In the Trinzic X6 series of appliances, you can install the Cloud Network Automation and the Cloud Platform licenses together on a Grid member.
- If you install a Multi-Grid Management license, you have to manually perform a product restart using either the CLI or the Grid Manager to set up Multi-Grid Management.
- When you configure an Trinzic X6 series appliance as TR-5005, repartitioning automatically takes place and a new partition is created for reporting.
- In NIOS 9.0.1, you cannot upload CA certificates that contain the md5WithRSAEncryption and sha1WithRSAEncryption ciphers.
- From NIOS 9.0.1 onwards, fetching threat details using the API displays the "Authorization Failure" error message if the dynamic token fetch fails and error messages are logged in the infoblox.log and syslog files.
- When you enable the threat indicator caching feature, you must configure the credentials to access the Cloud Services Portal for NIOS to interact with the Cloud Services Portal. For more information, see *Configuring Integration with BloxOne Threat Defense Cloud* in the BloxOne Threat Defense online documentation.
- In NIOS 9.0.1, the default image disk size has been changed from 250 GB to 500 GB. For public cloud deployments (such as Microsoft Azure, GCP, and so on), you must provision the minimum disk size as 250 GB if you are using the resizable image.
- In NIOS 9.0.1, discovery is part of the NIOS image. You must install the ND appliance license to be able to use the discovery feature.
- From NIOS 9.0.1 onwards, the value in the **License String** column in the *Verifying License(s)* screen is decoded from the actual license string and not from what you upload in the CSV file or from what you paste as the license type.
- You must first install a NIOS license type before installing any dependent license for the NIOS license type. For example, you must install NIOS license type IB-1526 before installing a Multi-Grid-Management license.
- The sequence of licenses must be maintained for dependent licenses. For example, if you are installing both the Threat Protection (Software add-on) license and the Threat Protection

Update license, install them in the order of Threat Protection (Software add-on), Threat Protection Update so that both the licenses are installed in the same session.

- The license type and other data related to licenses are decoded from the license key and displayed when you install the licenses.
- Grid Manager restarts immediately in the background when you install licenses that require UI restarts.

NIOS 9.0.0

- ISC has modified the dnssec-dsfromkey tool behavior for DS (Delegation Signer) record generation when no algorithm is passed. When no algorithm is passed:
    - In BIND 9.11, both SHA1 and SHA256 digests are generated when converting DNSKEY records to DS records.
    - In BIND 9.16, only SHA256 digest is generated when converting a DNSKEY record to a DS record.
- BIND 9.16 introduces a change in behavior for forwarders (for a particular fetch context) when an upstream query directed to the forwarder times out. The behavior is applicable in a "forward-first" configuration. The change marks a forwarder which does not respond to an query (for a particular fetch) sent by a resolver as a "bad server". The forwarder is no longer contacted for the rest of the delegation points for the fetch.
- In NIOS 9.0.0, LDAP requests to the LDAP server and Active Directory server cannot be sent using the MGMT IP address, because OpenLDAP version 2.4.49 (Ubuntu) removed the options of binding the source IP address on the client. Therefore, an LDAP request or an Active Directory authentication request is always sent through the LAN IP address, even though you have enabled the **Connect through Management Interface** option.
- From NIOS 9.0.0 onwards, in the Administration > Administrators > Authentication Policy > Authenticate users against these services in this order area, if the Authentication Server Groups is the authority for option is set to Passwords of Local users, the up and down arrows at the right will be disabled if you select the Local Admin checkbox. That is, you will not be able to change the order of the local admin user.
- Due to new validation checks introduced in BIND 9.16, a few resource records that were valid in BIND 9.11 are considered invalid in BIND 9.16. If you add such invalid resource records to a zone, the zone fails to load after an upgrade or a Grid restore. An error message is displayed if you add invalid resource records resource records with invalid RDATA under a zone.
- NIOS 9.0.0 introduces the `set rpz_add_soa` command that allows a local admin with superuser permission to add an SOA record to an RPZ response at a view level. If this command is togged to YES, any RPZ policy rule matches and results in a modified answer, then the modified answer will include in its additional section the SOA record of the policy zone whose rule was used to generate the modified answer. The SOA record includes the name of the DNS RPZ and the serial number of the policy data which was connected to the DNS control plane

when the answer was modified. This command is only available on the Grid Master. For more information, see the "set rpz_add_soa" topic in the NIOS 9.0 online documentation.

- In NIOS 9.0.0, the `additional-from-auth` option has been made obsolete by ISC. BIND does not follow CNAMEs and DNAMEs to zones other than the target zone. Hence, record chains do not work as expected.
- In NIOS 9.0.*x*, the Cisco ISE endpoint (Cisco pxGrid 1.0) has been deprecated.
- In NIOS 8.6.2, when you log on to FTP using as an anonymous user, the default path was /storage/tftpboot. In NIOS 9.0.*x*, the default path is /storage/tftpboot_anon with permission 0755.
- NIOS 9.0.0 introduces two new CLI commands to set the DDNS update quota and the DDNS update forwarding quota versions. For more information about these commands, see the "set dns_update_quota" and the "set dns_update_forwarding_quota" topics in the NIOS 9.0 online documentation.
    - set dns_update_quota : Use the `set dns_update_quota` command to set the maximum number of update events queued onto a zone task. The number must be between 200 and 2500 (inclusive). The default value is 1024.
    - set dns_update_forwarding_quota: Use the `set dns_update_forwarding_quota` command to set the maximum number of forwarding update events (queued onto a zone task).
- In NIOS 9.0.*x*, distribution fails when an Infoblox-generated Apache certificate is uploaded for keys lower than 2048 bits or if the certificate has expired.
- NIOS 9.0.0 supports the discovery resizable image with a minimum disk size of 100 GB.
- In NIOS 9.0.*x*, integration with BIND 9.16 increases the RPZs from 32 to 64. That is, subscriber services support an subscriber secure policy (SSP) of 64 bits. Only rules within the particular RPZs will be enforced by subscriber services. The first 5 RPZs are used as default and enforced on subscribers without an SSP. The number of default RPZs remains at 5. In a parental control configuration, the rules in RPZ 31 have a special use case as a proxy allow list. All rules (domains) are passthru to allow them to never proxy.
  There are no changes to the proxy allow list with the addition of 64 RPZ zones. Rules in the thirty first RPZ zone will be passthru rules as existing in earlier NIOS releases. The remaining RPZ zones (32 - 63) can be used just like other RPZ zones. All RPZ responses (modified or otherwise, including NXDOMAIN/NODATA) will not have the SOA record in the ADDITIONAL SECTION of the RPZ query response.
- In NIOS 9.0.*x*, when rotating log files, only the syslog rotated files are maintained.
- In NIOS 9.0.*x*, the cipher list order has changed compared to earlier NIOS versions.
- In NIOS 9.0.*x* the weak and vulnerable ciphers named RC4 and 3DES have been deprecated. Additionally, the SAML library also deprecates the DHE ciphers. Infoblox recommends that you

keep these weak ciphers disabled as this can affect both the Apache and SAML services. Even if these ciphers are enabled, they will be visible as enabled in the output but they will not be effective as they have been deprecated.

- Upgrading a NIOS 8.x Grid that is configured with Thales HSM to NIOS 9.0 is not supported. Also, configuring Thales HSM in a new NIOS 9.0 Grid is not supported. Infoblox recommends that you unsign zones that were signed using Thales and that you disable HSM signing before disabling Thales modules.
- From NIOS 9.0.0 onwards, bloxTools has been deprecated.
- From NIOS 9.0.0 onwards, the following appliances have been deprecated: PT-1405, PT-2205, PT-2205-10GE, IB-4030-10GE.
- FIPS is not supported in NIOS 9.0.*x*.
- From NIOS 9.0.0 onwards, the Unbound resolver has been deprecated and all the references to Unbound will be destroyed after a NIOS upgrade.
- From NIOS 9.0.0 onwards, during a restore operation or a CSV import, Unbound-related configurations (using the *Grid DNS Properties* screen), Unbound-related licenses, and DNS Unbound under external syslog categories will be removed.
- In NIOS 9.0.*x*, support for the DNSSEC algorithm 1 (RSAMD5), algorithm 3 (DSA), and algorithm 6 (DSA-NSEC3-SHA1) has been removed.

NIOS 8.6.x and Earlier

- The value of PLATFORM_NAMED_MAX_CACHE_SIZE for the IB-2215 and IB-2225 platforms has been increased from 2048 to 12288.
- From NIOS 8.6.3 onwards, all extensible attributes that are associated with the Network object type will also be associated with the Network Container object type and all extensible attributes that are associated with the IPv6Network object type will also be associated with the IPv6NetworkContainer object type.
- From NIOS 8.6.1 onwards, if you add a DNS resource record manually, then DNS scavenging does not recover or scavenge the resource record. Manually created resource records are protected and must be manually deleted. Only if you explicitly allow recovery or scavenging of the resource record via a configuration, does DNS scavenging recover or scavenge the manually added resource record.
- From NIOS 8.6.3 onwards, the maximum number of allowed and blocked domains has increased to 15.
- From NIOS 8.6.3 onwards, the "Flex Grid Licensing Features Enabled" report has been renamed to "SPLA Grid Licensing Features Enabled" and the “DNS Effective Peak Usage Trend for Flex Grid License" report has been renamed to “DNS Effective Peak Usage Trend for SPLA Grid License".

- If you upgrade to NIOS 8.6.3, all IB-FLEX appliances or Grids that have the FLEX Grid Activation license or the MSP license will have the ReportingSPLA external attribute assigned automatically for supported Grid members.
- Starting from NIOS 8.6.3, for Network Insight, AES (Advanced Encryption Standard) has been changed to AES-128 in Grid Manager and other means of data population.
- In NIOS 8.6.3, the Members filter and the SPLA Reporting filter were added for the following dashboards:
  - Managed DDI features enabled
  - SPLA Grid Licensing Features Enabled
  - Managed DDI Peak IP Usage Trend
  - Managed Trend DNS Peak Usage
  - DNS Effective Peak Usage Trend for SPLA Grid License
- From NIOS 8.6.3 onwards, only 5% of allowed blocklist subscribers is supported for virtual DNS Cache Acceleration (vDCA).
- In NIOS 8.6.3, “Thales HSM” has been rebranded to “Entrust nShield HSM” and “SafeNet HSM” has been rebranded to “Thales Luna HSM”. Accordingly, “HSM Thales Group” is now “Entrust nShield Group” and “HSM SafeNet Group” is now “Thales Luna Group”.
- In NIOS 8.6.2 and earlier, if you change a host name policy to a default policy, the host name policy table would be automatically populated with the default policy. From NIOS 8.6.3 onwards, you have to manually clear the existing host name policy in the table and enter the new one.
- In NIOS 8.6.3, If a ZVELO category database update failure occurs for three consecutive days, Grid Manager displays a yellow background with the "Domain category db is not latest" message in the **Grid Manager** > **Members** > **Status** column.
- From NIOS 8.6.3 onwards, the **Advanced** tab in the *Grid Properties Editor* > **CSP Config** tab has been removed.
- From NIOS 8.6.3 onwards, the **Data Collection and Opt-Out Notice** screen that is displayed when you first log in to NIOS has been removed.
- From NIOS 8.6.3 onwards, the **Disable Default Search Path** and the **Additional Search Paths** fields have been removed from the *Add Active Directory Authentication Service > Step 1 of 1* wizard.
- From NIOS 8.6.3 onwards, you must start the Cloud DNS Sync service on the Grid member on which you want to synchronize the Route 53 DNS data.
- The **Proxy RPZ Passthru** checkbox in the *Add Subscriber Site* wizard has been renamed to **Enforce the global proxy list**. If you select this checkbox, and have categorized the queried domains in the incoming traffic to the global proxy list (category 104), then the query resolves to an MSP virtual IP address and NIOS generates a "synthetic resolution”. This checkbox is disabled by default, and you must configure the **Content Proxy Addresses** field to enable it. If you do not select the checkbox, then the query resolves normally. If you have configured queries to specific domains (categorized to 104) to be proxied to the MSP server and have

enabled the **Enforce the global proxy list** checkbox, queries to these domains are proxied if subscriber secure policies with the NXDOMAIN rule are not set.

- In earlier NIOS versions, you were not able to add a delegated name server group if a Microsoft server was configured. From NIOS 8.6.2 onwards, you will not be able to add a delegated name server group only if DNS synchronization is enabled on any Microsoft server configured in NIOS. For more information, see the “New Features” section in these Release Notes. (RFE-10168)
- In NIOS 8.6.2, in the *DDNS Properties* dialog box, **ZONES TO UPDATE FOR HOSTS USING DHCP FQDN OPTION** area if you have configured more than one Grid DNS primary server for DDNS updates for multi-master zones, DHCP servers use the first available DNS primary server that is configured. If the first DNS primary server is not reachable or is offline, then the DHCP servers reach for the next DNS primary server in the preferred multi-domain DDNS list and so on. You can add upto a maximum of three DNS primary nameservers for each zone.
- In NIOS 8.6.2, If a ZVELO category database update failure occurs for three consecutive days, Grid Manager displays a red background with the "Category information data is unavailable" message in the **Grid Manager** > **Members** > **Status** column. Now if you enable or disable DCA subscriber allowed and blocked list support, the red background continues to be because red takes higher priority. Once you update to the latest ZVELO database, the background is supposed to change to green. But because the subscriber allowed and blocked list support is already enabled, a yellow background is displayed with the "To recover memory allocated for DCA subscriber Allowed and Blocked lists a manual reboot is required." message.
- During a NIOS upgrade, when configuring reporting clusters, ignore the "Unable to establish a connection to peer" message displayed on the **Reporting** tab.
- In NIOS 8.6.2, in the **Master Preferences for DDNS Updates to Multi-master DNS Zones** > **Add** screen, **DNS Primary** field, you can add up to a maximum of three DNS primary nameservers for each zone.
- From NIOS 8.6.2 onwards, you cannot enter special characters other than ~, : + in any file or directory path.
- In NIOS 8.6.2, the *Grid Properties Editor* > **CSP Config** > **Advanced** tab displays a link that redirects you to the BloxConnect program details.
- In versions earlier than NIOS 8.6.2, when querying a domain with a client subnet, if the EDNS Client Subnet (ECS) option was not enabled, the client used to receive a refused response. From NIOS 8.6.2 onwards, the client subnet option is ignored and the domain query is considered a normal request.
- In NIOS 8.6.1, ISC has disabled the lame server caching mechanism as part of CVE-2021-25219. The mechanism has been disabled by explicitly overriding the lame TTL value to 0 in the BIND server. Therefore, any changes to lame TTL configuration in Grid Manager will not have an impact as the lame server caching mechanism is disabled in the BIND server.
- The `show ospf config`, `show ipv6_ospf config`, `show bgp config`, and `show ipv6_bgp config` CLI commands display the password from the configuration in encrypted format.

- In NIOS 8.6.1 and NIOS 8.5.3, you can configure the value of the DNS recursive cache size for the IB-2215, IB-2225, and PT-2205 platforms from 2048 MB to 12288 MB.
- From NIOS 8.6.1 onwards, the name of the *DNS QPS Usage Report* has been changed to *DNS Effective Peak Usage Trend Report*.
- From NIOS 8.6.1 onwards, static records can be marked reclaimable but they cannot be reclaimed by DNS scavenging. To delete static records marked reclaimable, use the Delete icon.
- In NIOS 8.6.1, you cannot enter special characters such as `, !, @, #, $, %, ^, &, *, (,), =, [,], {, }, |, ;, ', ", <, >, ?, \ in the **Directory Path** field on the *Grid DNS Properties* > **Logging** > **Advanced** screen.
- In NIOS 8.6.1, running the `set regenerate_anycast_password` command restarts the anycast service on those Grid members on which it is running.
- Infoblox Subscriber Services is not supported in NIOS 8.6.0. Although Subscriber Services is supported in NIOS 8.6.1, Infoblox recommends that you do not use it in this version.
- In NIOS 8.6.1, the shared secret that you enter when adding a RADIUS authentication server in the *Add RADIUS Authentication Service* wizard > **RADIUS Servers** > **Shared Secret** field must be between 4 and 64 characters (inclusive) in length and must match the secret you entered in the RADIUS server.
- When DNS Cache Acceleration (DCA) and Infoblox Advanced DNS Protection (software or hardware) were both enabled in NIOS versions earlier than 8.6.1, by default Advanced DNS Protection was the first to receive an incoming packet. From NIOS 8.6.1 onwards, by default DNS Cache Acceleration is the first to receive an incoming packet.
- If the MGMT interface is listening to DNS queries on an IP address, do not add the IP address to the **Other IP Address** column in *Member DNS Properties* > **DNS Views** > **Basic** tab.
- In NIOS 8.6.1 and 8.5.3, a new check box named **Stop the anycast service when the subscriber service is in the interim state** in the *Add Subscriber Site* wizard has been introduced. The check box is selected by default and stops the anycast service from running when the subscriber service is in the interim state as in the previous releases. Deselecting the check box allows subscriber services to respond to DNS queries when anycast is in service during the interim state (initial state when the subscriber dataset is not fully populated).
- In NIOS 8.6.1 and 8.5.3, the **Data Management** > **DHCP** > **IPv4 Filters** menu item has been renamed to **Filters**.
- In NIOS 8.6.1 and 8.5.3, all filters in the logic filter list are displayed in the inherited mode for both IPv4 and IPv6 objects such as network, range, shared network, fixed address, host address, and the related edit pages of these objects.
- In NIOS 8.6.1 and 8.5.3, the *Member DHCP Properties* dialog box may not show the correct inherited logic filter list when you make changes to the member assignments. NIOS currently does not have the ability to filter out the logic filter list after you make changes to the member assignment. This does not affect functionality. If you refresh the *IPv4 Network editor* or the *IPv6 Network editor*, the correct list of logic filters is displayed.

- Prior to NIOS 8.5.3, DHCP class filters (MAC address, Option, NAC, Relay Agent, Fingerprint) were inconsistently enforced when multiple filter types were configured in a range. In older versions, if two or more class filter types are configured in a range, it is enough for the client to match any one of the class filter types. NIOS 8.5.3 and later versions correct this, requiring all configured class filter types to match before a lease is granted. In other words, NIOS 8.5.3 and later use the AND logic between two filter types in contrast to the OR logic used in older versions. For example, if there is a MAC filter and a fingerprint filter in a range, the client has to match both the MAC filter and fingerprint filter to get the lease as opposed to older versions where the client only had to match any of the filter types to be allowed. In both the older and newer versions, the AND logic is imposed only between different filter types and not between the same filter type. For example, if there are two MAC filters with permission set to 'Allow', it is not necessary that the client should be allowed into both the MAC filters. Note that the option 'Allow known/unknown clients' is indirectly considered a class filter and therefore the same AND logic will be used along with other class filter types. If any of the class filters is configured to deny a lease and a filter matches the client's request, the lease will be denied irrespective of whether the other filters allow or deny the client. A 'deny' result always takes precedence over any other filter result.
- In NIOS 8.6.1 and 8.5.3, in the *Member DHCP Properties* dialog box, you cannot override any one type of filter (either IPv4 or IPv6). If you want to override, you must override both IPv4 and IPv6 filters.
- If you are using threat analytics, you must have installed the minimum module set version (20210620) before upgrading to NIOS 8.6.1 or to NIOS 8.5.3.
- In NIOS 8.6.1 and 8.5.3, the OpenSSH server process `sshd` is binding only to primary interfaces. Additional interfaces like VLANs, loopback addresses are restricted.
- In NIOS 8.6.1 and 8.5.3, if the **Disable Concurrent Login** check box or the **Enable Account Lockout** check box is selected, then while logging in to NIOS as a local user, you will have read-write transactions.
  However, If the **Disable Concurrent Login** check box or the **Enable Account Lockout** check box is not selected, then while logging in to NIOS as a local user, you will have read-only transactions. After logging in, other permissions remain the same based on the group to which you belong.
- In NIOS 8.6.1 and 8.5.3, `certificate_usage`, `matched_type`, and `selector` fields are mandatory. Therefore, you must specify these through WAPI when adding TLSA records.
- The IPv6 loopback address in a NIOS OSPFv3 configuration is now assigned to an area causing this route to advertise as LSA type 9 instead of LSA type 5.
- For NIOS 8.6.*x*, 8.5.2 and later, and NIOS 8.4.8, by default the anycast service is restarted along with the DNS service. However, you can change the restart sequence based on your network topology.
- If you configure the HTTP proxy field on the **CSP Config** tab at the Grid level, all Grid members will immediately restart to update the configuration internally. If you configure the HTTP proxy field at the member level, only that Grid member will restart.

- If you upgrade NIOS when the **HTTP proxy** field on the **CSP Config** tab is set with a value, NIOS restarts after the upgrade to update the configuration internally.
- The original BIN2 file has been replaced by the BIN file. The new BIN file is signed with a longer key that provides greater protection against tampering. The content is identical.
- From NIOS 8.6.1, 8.5.3, and 8.5.2, CLI access to AWS appliances now requires that the Use AWS SSH authentication keys option be enabled for each user that needs CLI access to AWS appliances. You will not be able to access the CLI after you upgrade to 8.5.2 until you select the Use AWS SSH authentication keys option. That is, you cannot use the CLI to access vNIOS for AWS if you are a remote user or a SAML user. For more information, see the "Creating Local Admins" topic in the NIOS 8.5 online documentation.
- The NIOS login password is now encrypted instead of being in plain text. (RFE-9428)
- For NIOS 8.6.*x* and 8.4.8, when you change the member assignment of DHCP ranges from a failover association to a Grid member and then back to a failover association, leases in the primary and secondary server can fall out of sync. To ensure that the peers remain synchronized, the failover association is now put in the Recover-Wait state. It moves to the Recover-Done state immediately after synchronization without an MCLT delay. The servers come back to the normal state and are available for lease allocation.
- In NIOS 8.6.*x*, 8.5.2, and 8.4.8, the **Last Queried** column with respect to DNS scavenging now displays the timestamp of the last queried information only if the query is received from an external client and not from any other source. The Last Queried field is updated once a day with the timestamp of the last query. If there is no existing last queried timestamp and a query is received, the last queried timestamp is immediately updated. (RFE-8805).
- In NIOS 8.6.1, 8.5.3, and 8.5.2, for a Grid Master or a standalone vNIOS instance deployed on AWS, you are prompted to reset the password on the first login attempt. You must reset the default password as a security requirement.
- In NIOS 8.6.1 and 8.5.4, for Infoblox Subscriber Services, category-related information is now fetched by a different service provider and the following CLI commands have been introduced:
  - `show pc_domain`
  - `set pc_domain add`
  - `set pc_domain delete`

  For information about these commands, see the "show pc_domain", "set pc_domain_add", and "set pc_domain delete" topics in the NIOS 8.5 online documentation.
- You can now configure the number of top processes and the Ptop interval not only for the Grid Master but also for Grid members.
- In the System Activity Monitor widget, you can now view CPU utilization data for up to a maximum of the past 30 minutes.
- The following changes take place in output when you click the **Perform Dig** button:
  - If the response of the DNS lookup is below 8000 characters, the entire response is displayed.
  - If the response of the DNS lookup is greater than or equal to 8000 characters, the short output is displayed.

        - If the short output is greater than or equal to 8000 characters, the “The <FQDN> response is too large. Try using an external client to run the query.” error message is displayed.
- Prior to NIOS 8.5.3, DHCP class filters (MAC address, Option, NAC, Relay Agent, Fingerprint) were inconsistently enforced when multiple filter types were configured in a range. In older versions, if two or more class filter types are configured in a range, it is enough for the client to match any one of the class filter types. NIOS 8.5.3 and later versions correct this, requiring all configured class filter types to match before a lease is granted. In other words, NIOS 8.5.3 and later use the AND logic between two filter types in contrast to the OR logic used in older versions. For example, if there is a MAC filter and a fingerprint filter in a range, the client has to match both the MAC filter and fingerprint filter to get the lease as opposed to older versions where the client only had to match any of the filter types to be allowed. In both the older and newer versions, the AND logic is imposed only between different filter types and not between the same filter type. For example, if there are two MAC filters with permission set to ‘Allow’, it is not necessary that the client should be allowed into both the MAC filters. Note that the option 'Allow known/unknown clients' is indirectly considered a class filter and therefore the same AND logic will be used along with other class filter types. If any of the class filters is configured to deny a lease and a filter matches the client’s request, the lease will be denied irrespective of whether the other filters allow or deny the client. A ‘deny’ result always takes precedence over any other filter result.
- From NIOS 8.5.3 onwards, you can access the nios_version.txt file only through authentication by specifying your NIOS login credentials.

Changes to Infoblox API and Restful API (WAPI)

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

NOTE: The Perl API (PAPI) has been deprecated. The PAPI functionality is still supported. However, API calls enhancements after version 8.3 will only be introduced through the RESTful API (WAPI). The latest available WAPI version is 2.13.4.

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, 1.7.5, 2.0, 2.1, 2.1.1, 2.1.2, 2.2, 2.2.1, 2.2.2, 2.3.0, 2.3.1, 2.4, 2.5, 2.6, 2.6.1, 2.7, 2.7.1, 2.7.2, 2.7.3, 2.8, 2.9, 2.9.1, 2.9.5, 2.9.7, 2.10, 2.10.1, 2.10.2, 2.10.3, 2.10.5, 2.11, 2.12, 2.12.1, 2.12.2, 2.13, 2.13.1, and 2.13.4.

The following table describes the mapping of NIOS versions to WAPI versions:

NIOS Version	WAPI Version
8.0.0 to 8.0.9	2.5
8.1 to 8.1.8	2.6.1
8.2.0 to 8.2.3	2.7
8.2.4 to 8.2.5	2.7.1
8.2.6 to 8.2.9	2.7.3
8.3.0 to 8.3.1	2.9
8.3.2 to 8.3.5	2.9.1
8.3.6	2.9.5
8.4.0 to 8.4.1	2.10
8.4.2 to 8.4.3	2.10.1
8.4.4	2.10.3
8.4.5	2.10.5
8.4.6	2.10.5
8.5	2.11
8.6.0	2.12
8.6.1	2.12.1
8.6.2	2.12.2
8.6.3, 8.6.4	2.12.3
9.0	2.13
9.0.1, 9.0.2, 9.0.3	2.13.1
9.0.4	2.13.4

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 9.0.*x*

NIOS 9.0.*x* includes the following WAPI changes:

NIOS 9.0.4

New Structures:

- lanhaportsetting:ha_cloud_attribute
- setting:network:lan_gateway
- setting:network:lan_subnet_mask
- azurednstaskgroup

New Objects:

- member:ha_cloud_platform
- member:ha_on_cloud
- query_fqdn_on_member: source_ip
- vdiscoverytask:selected_regions
- vdiscoverytask:accounts_list
- vdiscoverytask:cdiscovery_file_token
- vdiscoverytask:govcloud_enabled
- vdiscoverytask:multiple_accounts_sync_policy
- vdiscoverytask:role_arn
- vdiscoverytask:selected_regions
- vdiscoverytask:sync_child_accounts
- azurednstaskgroup:multiple_subscriptions_sync_policy
- azurednstaskgroup:azure_subscription_ids_file_token
- azurednstaskgroup:sync_child_subscriptions
- azurednstaskgroup:comment
- azurednstaskgroup:consolidate_zones
- azurednstaskgroup:consolidated_view
- azurednstaskgroup:disabled
- azurednstaskgroup:grid_member

- azurednstaskgroup:multiple_subscriptions_sync_policy
- azurednstaskgroup:name
- azurednstaskgroup:network_view
- azurednstaskgroup:network_view_mapping_policy
- azurednstaskgroup:subscriptions_list
- azurednstaskgroup:sync_status
- azurednstaskgroup:task_list
- azurednstaskgroup:tenant_id

NIOS 9.0.1

New Structures:

- memberclouddnssync
- gmcgroup
- gmcshedule
- hsm:thaleslunagroup:thalesluna
- hsm:entrustnshieldgroup:entrustnshield_hsm
- validatecertificates.complete_verification_result
- validatecertificates.complete_verification_result.file_or_serial
- validatecertificates.complete_verification_result.verify_result

New Objects:

- parentalcontrol:subscriber:zvelo_update_failure_in_days
- parentalcontrol:subscribersite:enable_global_allow_list_rpz
- parentalcontrol:subscribersite:enable_rpz_filtering_bypass
- parentalcontrol:subscribersite:global_allow_list_rpz
- memberclouddnssync:cloud_dns_sync_enabled
- memberclouddnssync:host_name
- awsrte53taskgroup:role_arn
- awsrte53taskgroup:sync_child_accounts

- awsuser:govcloud_enabled
- gmcgroup:member
- grid:ntp_setting:ntp_keys:type:SHA1_ASCII
- member:ntp_setting:ntp_keys:type:SHA1_ASCII
- hsm:thaleslunagroup
- hsm:entrustnshieldgroup

Upgrade Guidelines

NIOS 9.0.4 Upgrade Guidelines

- Splunk does not support TLS version 1.3 and therefore NIOS reporting will not work if you disable all other TLS versions and enable only TLS version 1.3. A warning to this effect is displayed if you enable only TLS version 1.3.
- Accelerated Networking must be disabled in Microsoft Azure for NIOS members before upgrading to 9.0.*x* as it is not compatible with NIOS 9.0.*x* and may cause the member to not rejoin the Grid after upgrading. The VM or, if applicable, all VMs within the availability set may need to be stopped or deallocated before Accelerated Networking is disabled.
- After an upgrade to NIOS 9.0.4, the Cloud Sync service starts automatically on members that have AWS and GCP vDiscovery jobs configured.
- After an upgrade to NIOS 9.0.4, the Cloud Sync service will not start automatically on members that have VMWare, Azure, and Openstack vDiscovery jobs configured.

NIOS 9.0.2 Upgrade Guidelines

- Before upgrading the Grid to the latest version, check for any pending actions from previous hotfix applications and complete the actions to avoid unexpected behavior on Grid members during the upgrade. To check for pending actions, perform the following steps:
  - Run the `show upgrade_history` CLI command. The command lists down the latest hotfixes applied on Grid members.
  - If you have applied a hotfix, verify the actions based on the hotfix form. For example, if the hotfix requires a reboot post the hotfix application, run the `show log debug /REBOOT/` CLI command. If a reboot has not taken place after the hotfix applied time displayed in the command's output, Infoblox strongly recommends that you reboot the Grid member.
- When certificates present in the Grid are not in accordance with RFC-5280, the test upgrade will fail, and errors are captured in the syslog file. Infoblox recommends that you fix the certificates before upgrading to NIOS 9.0.2 (the upgrade does not fail but you must make the recommended changes).

NIOS 9.0.1 Upgrade Guidelines

- If you upgrade or replace your end-of-life Trinzic X5 series hardware appliance with a Trinzic X6 series hardware appliance but you have valid Trinzic X5 series software license, then you can use the X5 software license on an X6 hardware appliance till the license expires. However, you need to contact Infoblox Support to generate a new X5 software license so that it will work with the X6 hardware appliance. Note that this is applicable only to end-of-life X5 hardware appliances.
- If you try to upgrade to NIOS 9.0.1, distribution fails if CA certificates with the md5WithRSAEncryption or sha1WithRSAEncryption ciphers are present. Infoblox recommends that you delete the certificates before upgrading.
- Upgrading to NIOS 9.0.1 is restricted, subject to the following checks:
    - CA certificates violating RFC: Subject Key Identifier MUST exist if CA=TRUE
    - Certificate validity dates
    - Restrict MD5 and SHA1 for Apache certificates and CA certificates
    - OpenVPN certificates. If you have old OpenVPN certificates, contact Infoblox Support before proceeding with the distribution.
- If the Dual Engine DNS license is present in your Grid in the deleted or expired state (can be validated by running the show license CLI command on the node), contact Infoblox Support to have it removed. The NIOS upgrade fails if the license is not deleted.
- Unbound upgrade guidelines:
    - If an Unbound license is present in the Grid, then upgrading to 9.0.1 will fail. You must manually remove the Unbound license and then proceed with the upgrade.
    - If you have offline Grid members and are not able to delete the Unbound license, then you must bring the Grid members online, remove the license, and then proceed with the upgrade. You can also contact Infoblox Support about creating a hotfix to clean up the Unbound licenses for the offline members.
    - If you had a temporary Unbound license that you deleted from Grid Manager, the license will still be present in the database and the upgrade will fail. Please contact Infoblox Support to completely remove the temporary license.
    - If Unbound is configured, the upgrade test fails to indicate that references to Unbound are being completely destroyed during the upgrade process.

NIOS 9.0.0 Upgrade Guidelines

Upgrade to NIOS 9.0.0 fails in the following scenarios:

- Upgrading a NIOS 8.x Grid that is configured with Thales HSM to NIOS 9.0 is not supported. Also, configuring Thales HSM in a new NIOS 9.0.0 Grid is not supported. Using an unsupported algorithm such as, RSAMD5(1), DSA (3), DSA-NSEC3-SHA1(6).
- Using invalid key size for RSASHA1(5), RSA-NSEC3-SHA1(7), RSASHA256(8) (should be within range [1024 to 4096]).
- Manually creating (through the import keyset) a DS record with an unsupported algorithm or digest type SHA-1.
- If you are using Ubuntu and a CA certificate of key length 1024 and some unsupported ciphers, after a NIOS upgrade, services that depend on the unsupported ciphers cease to work.
- In NIOS 9.0, the Cisco ISE endpoint (Cisco pxGrid 1.0) has been deprecated.
- Infoblox recommends that you use a minimum size of 100 GB when using discovery resizable images. This applies even when upgrading a resizable discovery image whose size is lower than 100 GB.
- Infoblox recommends using a minimum size of 70 GB for any of the files that has resizable as part of the file name and you can resize them depending on your requirement and deployment.
- If you are logging on to NIOS using SSO, in IDP Configuration you must enter the following URL in the SP Entity ID field: <grid_virtual IP address>:8765/metadata. If you are using Okta, the SP Entity ID field is also called the Audience URI field.
- The shared secret that you enter when adding a RADIUS authentication server in the Add RADIUS Authentication Service wizard > RADIUS Servers > Shared Secret field must be between 4 and 64 characters (inclusive) in length. Otherwise, the upgrade will fail.
- Before you upgrade to NIOS 9.0.*x*, check the validity of the CA certificates uploaded. If the certificate is invalid, install a new certificate that is in compliance with RFCs (for example RFC 5280). Failure to do so may result in the Grid Manager UI/WAPI not being accessible after the upgrade. However, NIOS will continue to be functional. To check the validity of the certificate, contact Infoblox Support.
- A downgrade from NIOS 9.0.*x* to NIOS 8.4.*x* is not supported. Auto-synchronization from NIOS 9.0.*x* to NIOS 8.4.*x* is not supported.
- If there are Threat Protection members in your Grid for the 8.3 and later features (Grid Master Candidate test promotion, forwarding recursive queries to BloxOne Threat Defense Cloud, and CAA records), ensure that you upload the latest Threat Protection ruleset for these features to function properly.
- Infoblox recommends that you enable DNS Fault Tolerant Caching right after you upgrade to NIOS 8.2.x and later and keep this feature enabled to handle unreachable authoritative

servers. Note that enabling this feature requires a DNS service restart, which will clear the current cache. Therefore, if you enable this when you are trying to mitigate an ongoing attack on an authoritative server that is outside of your control, it will clear the DNS cache, which will magnify the issues that your system is experiencing.

- During a scheduled full upgrade to NIOS 8.1.0 and later versions, you can use only IPv4 addresses for NXDOMAIN redirection. You cannot use IPv6 addresses for NXDOMAIN redirection while the upgrade is in progress.
- If you set up your Grid to use Infoblox Threat Insight but have not enabled automatic updates for Threat Analytics module sets, you must manually upload the latest module set to your Grid or enable automatic updates before upgrading. Otherwise, your upgrade will fail.
- After a scheduled upgrade to NIOS 8.6.3 and later is complete, you must run the `update_rabbitmq_password` command on the Grid Master to get the Cloud DNS Sync service to be functional. Until that time, Route 53 synchronization does not start because the service has not been started.
- After an upgrade to NIOS 8.6.3 and later, the Cloud DNS Sync service starts automatically on the Grid member that is assigned to the Route 53 synchronization groups.
- After an upgrade to NIOS 8.6.3 and later, the **Disable Default Search Path** and the **Additional Search Paths** fields will no longer be displayed in the *Add Active Directory Authentication Service > Step 1 of 1* wizard.
- If you upgrade to NIOS 8.6.3 or later, all IB-FLEX appliances or Grids that have the FLEX Grid Activation license or the MSP license will have the ReportingSPLA external attribute assigned automatically for supported Grid members.
- After an upgrade to NIOS 8.6.3 and later, only 5% of allowed blocklist subscribers is supported for virtual DNS Cache Acceleration (vDCA).
- The shared secret that you enter when adding a RADIUS authentication server in the *Add RADIUS Authentication Service* wizard > **RADIUS Servers** > **Shared Secret** field must be between 4 and 64 characters (inclusive) in length. Otherwise, the upgrade will fail.
- If you are using threat analytics, you must have installed the minimum module set version (20210620) before upgrading to NIOS 8.6.1 or to NIOS 8.5.3 or later versions.

Technical Support

Infoblox technical support contact information:

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

Email: support@infoblox.com

Web: https://support.infoblox.com

Training

Training information is available at https://training.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 TLS version 1 and later connections. Infoblox recommends that you use a computer that has a 2 GHz CPU and at least 1 GB of RAM.

Infoblox has tested and validated the following browsers for Grid Manager:

OS	Browser
Microsoft Windows 11®	Microsoft Edge version 115.0.1901.203, Google Chrome 115.0.5790.102
Microsoft Windows 10®	Microsoft Internet Explorer® 11, Microsoft Edge 113.0.1774.57
Microsoft Windows 8®	Google Chrome 109.0.5414.75
Microsoft Windows 7®	Mozilla Firefox 101.0
Red Hat® Enterprise Linux® 7.4	Google Chrome 115.0.5790.170
Red Hat® Enterprise Linux® 7.3	Mozilla Firefox 114.0.1

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

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.

The following table lists the addressed vulnerabilities along with the NIOS versions that contain the fixes.

CVE	Fixed in NIOS Versions
CVE-2023-50868, CVE-2023-50387, CVE-2023-48795, CVE-2023-5680, CVE-2023-5679, CVE-2023-4408	NIOS 9.0.4
CVE-2023-3341	NIOS 9.0.2 and later
CVE-2022-3094	NIOS 9.0.0 and later
CVE-2023-2828, CVE-2023-0466, CVE-2023-0465, CVE-2023-0464, CVE-2023-0286, CVE-2023-0215, CVE-2022-38178,	NIOS 8.6.3 and later

CVE	Fixed in NIOS Versions
CVE-2022-38177, CVE-2022-23943, CVE-2022-22721, CVE-2022-22720, CVE-2022-22719, CVE-2022-4450, CVE-2022-4304, CVE-2022-3924, CVE-2022-3736, CVE-2022-3488, CVE-2022-2929, CVE-2022-2928, CVE-2022-2795, CVE-2021-43527 **Note:** CVE-2023-2828, CVE-2023-0466, CVE-2023-0465, CVE-2023-0464, CVE-2023-0286, and CVE-2023-0215 have not been addressed in NIOS 9.0.0	
CVE-2021-25220, CVE-2022-0778	NIOS 8.6.2 and later
CVE-2021-25219, CVE-2021-25215, CVE-2021-25214	NIOS 8.6.1 and later
CVE-2020-25705, CVE-2020-13817, CVE-2020-8622, CVE-2020-8617, CVE-2020-8616, CVE-2019-11043, CVE-2019-1551	NIOS 8.6 and later
CVE-2019-11477, CVE-2019-6477, CVE-2019-6471, CVE-2019-6469, CVE-2018-10239, CVE-2018-5743, CVE-2018-5391, CVE-2018-5390, CVE-2016-10126	NIOS 8.5 and later
CVE-2018-15473, CVE-2018-0732	NIOS 8.4 and later
CVE-2018-5733, CVE-2018-5732, CVE-2018-0739, CVE-2018-0733, CVE-2018-8781, CVE-2017-3738, CVE-2017-3737, CVE-2017-3735	NIOS 8.3 and later
CVE-2016-10229, CVE-2017-3143, CVE-2017-3142, CVE-2017-3140, CVE-2017-3137, CVE-2017-3136, CERT VULNERABILITIES for NTPD	NIOS 8.2 and later
CVE-2017-3135, CVE-2016-9444, CVE-2016-9147, CVE-2016-9131, CVE-2016-8864	NIOS 8.1 and later
CVE-2016-6306, CVE-2016-6304, CVE-2016-5696, CVE-2016-1286, CVE-2016-1285, CVE-2015-8705, CVE-2015-8704, CVE-2015-8605, CVE-2015-8000, CVE-2015-7547, CVE-2015-6564, CVE-2015-6563, CVE-2015-5986, CVE-2015-5722, CVE-2015-5477, CVE-2015-6364, CVE-2015-5366, CVE-2015-1792, CVE-2015-1790, CVE-2015-1789, CVE-2015-1781, CVE-2015-4620, CVE-2015-0235, CVE-2014-9298, CVE-2014-8500, CVE-2014-8104, CVE-2014-3567, CVE-2014-3566, CVE-2014-7187, CVE-2014-7186, CVE-2014-6271, CVE-3014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-3470, CVE-2014-0224, CVE-2014-0221, CVE-2014-0198, CVE-2014-0195, CVE-2014-0591	NIOS 8.0 and later

CVE-2023-50868

The Closest Encloser Proof aspect of the DNS protocol (in RFC 5155 when RFC 9276 guidance is skipped) allows remote attackers to cause a denial of service (CPU consumption for SHA-1 computations) via DNSSEC responses in a random subdomain attack, aka the "NSEC3" issue. The RFC 5155 specification implies that an algorithm must perform thousands of iterations of a hash function in certain situations.

CVE-2023-50387

Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the "KeyTrap" issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG records, the protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records.

CVE-2023-48795

The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC).

CVE-2023-5680

If a resolver cache has a very large number of ECS records stored for the same name, the process of cleaning the cache database node for this name can significantly impair query performance. This issue affects BIND 9 versions 9.11.3-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.45-S1, and 9.18.11-S1 through 9.18.21-S1.

CVE-2023-5679

A bad interaction between DNS64 and serve-stale may cause `named` to crash with an assertion failure during recursive resolution, when both of these features are enabled. This issue affects BIND 9 versions 9.16.12 through 9.16.45, 9.18.0 through 9.18.21, 9.19.0 through 9.19.19, 9.16.12-S1 through 9.16.45-S1, and 9.18.11-S1 through 9.18.21-S1.

NIOS is not vulnerable to this CVE.

CVE-2023-4408

A] The DNS message parsing code in `named` includes a section whose computational complexity is overly high. It does not cause problems for typical DNS traffic, but crafted queries and responses may cause excessive CPU load on the affected `named` instance by exploiting this flaw. This issue affects both authoritative servers and recursive resolvers. This issue affects BIND 9 versions 9.0.0 through 9.16.45, 9.18.0 through 9.18.21, 9.19.0 through 9.19.19, 9.9.3-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.45-S1, and 9.18.11-S1 through 9.18.21-S1.

CVE-2023-3341

A flaw was found in the Bind package. The code that processes control channel messages sent to named calls certain functions recursively during packet parsing. Recursion depth is only limited by the

maximum accepted packet size. Depending on the environment, this may cause the packet-parsing code to run out of available stack memory, causing named to terminate unexpectedly.

CVE-2023-2828

It has been discovered that the effectiveness of the cache-cleaning algorithm used in named can be severely diminished by querying the resolver for specific RRsets in a certain order, effectively enabling the configured max-cache-size limit to be significantly exceeded. By exploiting this flaw, an attacker can cause the amount of memory used by a named resolver to significantly exceed the configured max-cache-size limit. The effectiveness of the attack depends on a number of factors (e.g. query load, query patterns), but since the default value of the max-cache-size statement is 90%, in the worst case the attacker can exhaust all available memory on the host running named, leading to a denial-of-service condition.

CVE-2023-0466

The function X509_VERIFY_PARAM_add0_policy() is documented to implicitly enable the certificate policy check when doing certificate verification. However the implementation of the function does not enable the check which allows certificates with invalid or incorrect policies to pass the certificate verification. As suddenly enabling the policy check could break existing deployments it was decided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy() function. Instead the applications that require OpenSSL to perform certificate policy check need to use X509_VERIFY_PARAM_set1_policies() or explicitly enable the policy check by calling X509_VERIFY_PARAM_set_flags() with the X509_V_FLAG_POLICY_CHECK flag argument. Certificate policy checks are disabled by default in OpenSSL and are not commonly used by applications.

CVE-2023-0465

Applications that use a non-default option when verifying certificates may be vulnerable to an attack from a malicious CA to circumvent certain checks. Invalid certificate policies in leaf certificates are silently ignored by OpenSSL and other certificate policy checks are skipped for that certificate. A malicious CA could use this to deliberately assert invalid certificate policies in order to circumvent policy checking on the certificate altogether. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function.

CVE-2023-0464

A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function.

CVE-2023-0286

There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network.

CVE-2023-0215

The public API function BIO_new_NDEF is a helper function used for streaming ASN.1 data via a BIO. It is primarily used internally to OpenSSL to support the SMIME, CMS and PKCS7 streaming capabilities, but may also be called directly by end user applications. The function receives a BIO from the caller, prepends a new BIO_f_asn1 filter BIO onto the front of it to form a BIO chain, and then returns the new head of the BIO chain to the caller. Under certain conditions, for example if a CMS recipient public key is invalid, the new filter BIO is freed and the function returns a NULL result indicating a failure. However, in this case, the BIO chain is not properly cleaned up and the BIO passed by the caller still retains internal pointers to the previously freed filter BIO. If the caller then goes on to call BIO_pop() on the BIO then a use-after-free will occur. This will most likely result in a crash. This scenario occurs directly in the internal function B64_write_ASN1() which may cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() on the BIO. This internal function is in turn called by the public API functions PEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream, SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7. Other public API functions that may be impacted by this include i2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream and i2d_PKCS7_bio_stream. The OpenSSL cms and smime command line applications are similarly affected.

CVE-2022-38178, CVE-2022-38177

By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources.

CVE-2022-23943

Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

CVE-2022-22721

If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

CVE-2022-22720

Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling.

CVE-2022-22719

A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

CVE-2022-4450

The function PEM_read_bio_ex() reads a PEM file from a BIO and parses and decodes the "name" (e.g. "CERTIFICATE"), any header data and the payload data. If the function succeeds then the "name_out", "header" and "data" arguments are populated with pointers to buffers containing the relevant decoded data. The caller is responsible for freeing those buffers. It is possible to construct a PEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex() will return a failure code but will populate the header argument with a pointer to a buffer that has already been freed. If the caller also frees this buffer then a double free will occur. This will most likely lead to a crash. This could be exploited by an attacker who has the ability to supply malicious PEM files for parsing to achieve a denial of service attack.

CVE-2022-4304

A timing-based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack. To achieve a successful decryption an attacker would have to be able to send a very large number of trial messages for decryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5, RSA-OEAP and RSASVE.

CVE-2022-3924

This issue can affect BIND 9 resolvers with `stale-answer-enable yes;` that also make use of the option `stale-answer-client-timeout`, configured with a value greater than zero. If the resolver receives many queries that require recursion, there will be a corresponding increase in the number of clients that are waiting for recursion to complete. If there are sufficient clients already waiting when a new client query is received so that it is necessary to SERVFAIL the longest waiting client (see BIND 9 ARM `recursive-clients` limit and soft quota), then it is possible for a race to occur between providing a stale

answer to this older client and sending an early timeout SERVFAIL, which may cause an assertion failure. This issue affects BIND 9 versions 9.16.12 through 9.16.36, 9.18.0 through 9.18.10, 9.19.0 through 9.19.8, and 9.16.12-S1 through 9.16.36-S1.

CVE-2022-3736

BIND 9 resolver can crash when stale cache and stale answers are enabled, option `stale-answer-client-timeout` is set to a positive integer, and the resolver receives an RRSIG query. This issue affects BIND 9 versions 9.16.12 through 9.16.36, 9.18.0 through 9.18.10, 9.19.0 through 9.19.8, and 9.16.12-S1 through 9.16.36-S1.

CVE-2022-3488

Processing of repeated responses to the same query, where both responses contain ECS pseudo-options, but where the first is broken in some way, can cause BIND to exit with an assertion failure. 'Broken' in this context is anything that would cause the resolver to reject the query response, such as a mismatch between query and answer name. This issue affects BIND 9 versions 9.11.4-S1 through 9.11.37-S1 and 9.16.8-S1 through 9.16.36-S1.

CVE-2022-3094

Sending a flood of dynamic DNS updates may cause `named` to allocate large amounts of memory. This, in turn, may cause `named` to exit due to a lack of free memory. We are not aware of any cases where this has been exploited. Memory is allocated prior to the checking of access permissions (ACLs) and is retained during the processing of a dynamic update from a client whose access credentials are accepted. Memory allocated to clients that are not permitted to send updates is released immediately upon rejection. The scope of this vulnerability is limited therefore to trusted clients who are permitted to make dynamic zone changes. If a dynamic update is REFUSED, memory will be released again very quickly. Therefore it is only likely to be possible to degrade or stop `named` by sending a flood of unaccepted dynamic updates comparable in magnitude to a query flood intended to achieve the same detrimental outcome. BIND 9.11 and earlier branches are also affected, but through exhaustion of internal resources rather than memory constraints. This may reduce performance but should not be a significant problem for most servers. Therefore we don't intend to address this for BIND versions prior to BIND 9.16. This issue affects BIND 9 versions 9.16.0 through 9.16.36, 9.18.0 through 9.18.10, 9.19.0 through 9.19.8, and 9.16.8-S1 through 9.16.36-S1.

CVE-2022-2929

In ISC DHCP 1.0 -> 4.4.3, ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16-P1 a system with access to a DHCP server, sending DHCP packets crafted to include fqdn labels longer than 63 bytes, could eventually cause the server to run out of memory.

CVE-2022-2928

In ISC DHCP 4.4.0 -> 4.4.3, ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16-P1, when the function option_code_hash_lookup() is called from add_option(), it increases the option's refcount field.

However, there is not a corresponding call to option_dereference() to decrement the refcount field. The function add_option() is only used in server responses to lease query packets. Each lease query response calls this function for several options, so eventually, the reference counters could overflow and cause the server to abort.

CVE-2022-2795

By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service.

CVE-2022-0778

The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

CVE-2021-43527

NSS (Network Security Services) versions prior to 3.73 or 3.68.1 ESR are vulnerable to a heap overflow when handling DER-encoded DSA or RSA-PSS signatures. Applications using NSS for handling signatures encoded within CMS, S/MIME, PKCS \#7, or PKCS \#12 are likely to be impacted. Applications using NSS for certificate validation or other TLS, X.509, OCSP or CRL functionality may be impacted, depending on how they configure NSS.

CVE-2021-25220

BIND 9.11.0 -> 9.11.36 9.12.0 -> 9.16.26 9.17.0 -> 9.18.0 BIND Supported Preview Editions: 9.11.4-S1 -> 9.11.36-S1 9.16.8-S1 -> 9.16.26-S1 Versions of BIND 9 earlier than those shown - back to 9.1.0, including Supported Preview Editions - are also believed to be affected but have not been tested as they are EOL. The cache could become poisoned with incorrect records leading to queries being made to the wrong servers, which might also result in false information being returned to clients.

CVE-2021-25219

In BIND 9.3.0 -> 9.11.35, 9.12.0 -> 9.16.21, and versions 9.9.3-S1 -> 9.11.35-S1 and 9.16.8-S1 -> 9.16.21-S1 of BIND Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.18 of the BIND 9.17 development branch, exploitation of broken authoritative servers using a flaw in response processing can cause degradation in BIND resolver performance. The way the lame cache is currently

designed makes it possible for its internal data structures to grow almost infinitely, which may cause significant delays in client query processing.

CVE-2021-25215

A flaw was found in BIND. The way DNAME records are processed may trigger the same RRset to the ANSWER section to be added more than once which causes an assertion check to fail. The highest threat from this flaw is to system availability.

Red Hat has investigated whether a possible mitigation exists for this issue, and has not been able to identify a practical example.

CVE-2021-25214

Incremental zone transfers (IXFR) provide a way of transferring changed portion(s) of a zone between servers. An IXFR stream containing SOA records with an owner name other than the transferred zone's apex may cause the receiving named server to inadvertently remove the SOA record for the zone in question from the zone database. This leads to an assertion failure during the next SOA refresh query for that zone.

The mitigation is to disable incremental zone transfers (IXFR) by setting "request-ixfr no;" in the desired configuration block (options, zone, or server) to prevent the failing assertion from being evaluated.

CVE-2020-25705

Dubbed "SAD DNS attack" (short for Side-channel AttackeD DNS), the technique makes it possible for a malicious actor to carry out an off-path attack, rerouting any traffic originally destined to a specific domain to a server under their control, thereby allowing them to eavesdrop and tamper with the communications.

CVE-2020-13817

ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows remote attackers to cause a denial of service (daemon exit or system time change) by predicting transmit timestamps for use in spoofed packets. The victim must be relying on unauthenticated IPv4 time sources. There must be an off-path attacker who can query time from the victim's ntpd instance.

CVE-2020-8622

In BIND 9.0.0 -> 9.11.21, 9.12.0 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.9.3-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker on the network path for a TSIG-signed request, or operating the server receiving the TSIG-signed request, could send a truncated response to that request, triggering an assertion failure, causing the server to exit. Alternately, an off-path attacker would have to correctly guess when a TSIG-signed request was sent, along with other characteristics of

the packet and message, and spoof a truncated response to trigger an assertion failure, causing the server to exit.

CVE-2020-8617

Using a specially-crafted message, an attacker may potentially cause a BIND server to reach an inconsistent state if the attacker knows (or successfully guesses) the name of a TSIG key used by the server. Since BIND, by default, configures a local session key even on servers whose configuration does not otherwise make use of it, almost all current BIND servers are vulnerable. In releases of BIND dating from March 2018 and after, an assertion check in tsig.c detects this inconsistent state and deliberately exits. Prior to the introduction of the check the server would continue operating in an inconsistent state, with potentially harmful results.

This vulnerability has been modified since it was last analyzed. It is awaiting reanalysis which may result in further changes to the information provided.

CVE-2020-8616

A flaw was found in BIND, where it does not sufficiently limit the number of fetches that can be performed while processing a referral response. This flaw allows an attacker to cause a denial of service attack. The attacker can also exploit this behavior to use the recursing server as a reflector in a reflection attack with a high amplification factor.

CVE-2019-11477

The TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11.

CVE-2019-11043

In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 in certain configurations of FPM setup, it is possible to cause FPM module to write past allocated buffers into the space reserved for FCGI protocol data, thus opening the possibility of remote code execution.

CVE-2019-6477

By design, BIND is intended to limit the number of TCP clients that can be connected at any given time. The update to this functionality introduced by CVE-2018-5743 changed how BIND calculates the number of concurrent TCP clients from counting the outstanding TCP queries to counting the TCP client connections. On a server with TCP-pipelining capability, it is possible for one TCP client to send a large number of DNS requests over a single connection. Each outstanding query is handled internally as an independent client request, thus bypassing the new TCP clients limit.

When a TCP connection with a large number of pipelined queries is closed, the load on the server releasing these multiple resources can cause it to become unresponsive, even for queries that can be answered authoritatively or from the cache. (This is most likely to be perceived as an intermittent server problem.)

CVE-2019-6471

A rare condition leading to denial of service was found in the way BIND handled certain malformed packets. A remote attacker who could cause the BIND resolver to perform queries on a server could cause the DNS service to exit.

CVE-2019-6469

An error in the EDNS Client Subnet (ECS) feature for recursive resolvers could cause BIND to exit with an assertion failure when processing a response that contained malformed RRSIGs.

CVE-2019-1551

There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u (Affected 1.0.2-1.0.2t).

CVE-2018-10239

A vulnerability in the “support access” password generation algorithm on NIOS could allow a locally authenticated administrator to temporarily gain additional privileges on an affected device and perform actions within the super user scope. A locally authenticated administrative user may be able to exploit this vulnerability if the “support access” feature is enabled. This is because the administrator knows the support access code for the current session and the algorithm to generate the support access password from the support access code. “Support access” is disabled by default. When enabled, the access is automatically disabled (and support access code will expire) after 24 hours.

CVE-2018-5743

The named DNS service fails to properly enforce limits on the number of simultaneous TCP connections.

CVE-2018-0732

During a key agreement in a TLS handshake using a DH(E) based ciphersuite, a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long

period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack.

CVE-2018-15473

OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.

CVE-2018-5732

A specially constructed response from a malicious server could cause a buffer overflow in the DHCP client.

CVE-2018-5733

A malicious client that was allowed to send very large amounts of traffic (billions of packets) to a DHCP server could eventually overflow a 32-bit reference counter, potentially causing the DHCP daemon to crash.

CVE-2018-5391

The Linux kernel versions 3.9+, is vulnerable to a denial of service attack with low rates of specially modified packets targeting IP fragment re-assembly. An attacker may cause a denial of service condition by sending specially crafted IP fragments. This vulnerability became exploitable in the Linux kernel with the increase of the IP fragment reassembly queue size.

CVE-2018-5390

A flaw named SegmentSmack was found in the way the Linux kernel handled specially crafted TCP packets. A remote attacker could use this flaw to trigger time and calculation expensive calls to tcp_collapse_ofo_queue() and tcp_prune_ofo_queue() functions by sending specially modified packets within ongoing TCP sessions which could lead to a CPU saturation and hence a denial of service on the system.

CVE-2018-0739

Constructed ASN.1 type with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe.

CVE-2018-0733

Because of an implementation bug the PA-RISC CRYPTO_memcmp function is effectively reduced to only comparing the least significant bit of each byte. This allows an attacker to forge messages that

would be considered as authenticated in an amount of tries lower than that guaranteed by the security claims of the scheme.

CVE-2018-8781

The udl_fb_mmap function in drivers/gpu/drm/udl/udl_fb.c at the Linux kernel version 3.4 and up to and including 4.15 had an integer-overflow vulnerability allowing local users with access to the udldrmfb driver to obtain full read and write permissions on kernel physical pages, resulting in a code execution in kernel space.

CVE-2017-3738

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation).

CVE-2017-3737

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer.

CVE-2017-3735

If an X.509 certificate had a malformed IPAddressFamily extension, OpenSSL could do a one-byte buffer overread, resulting in an erroneous display of the certificate in text format.

CVE-2016-10229

udp.c in the Linux kernel before 4.5 allowed remote attackers to execute arbitrary code via UDP traffic that triggered an unsafe second checksum calculation during execution of a recv system call with the MSG_PEEK flag.

CVE-2017-3143

An attacker who was able to send and receive messages to an authoritative DNS server and who had knowledge of a valid TSIG key name for the zone and service being targeted might be able to manipulate NIOS into accepting a dynamic update.

CVE-2017-3142

An attacker who was able to send and receive messages to an authoritative DNS server might be able to circumvent TSIG authentication of AXFR requests via a carefully constructed request packet.

CVE-2017-3140

RPZ policy handling could affect servers using RPZ policies that included NSIP or NSDNAME triggers, resulting in additional recursions that consumed DNS resources indefinitely and caused performance issues or DNS outage.

Vulnerabilities for NTPD

Upgraded NTPD to ntp-4.2.8p10 to address the following medium to low severity vulnerabilities: CVE-2017-6464, CVE02017-6463, CVE-2017-6462, CVE-2017-6460, CVE-2017-6459, CVE-2017-6458, CVE-2017-6455, CVE-2017-6452, CVE-2017-6451, CVE-2016-9042, CVE-2016-7434.

CVE-2017-3137

Processing a response containing CNAME or DNAME records in an unusual order could cause a DNS resolver to terminate.

CVE-2017-3136

Using DNS64 with 'break-dnssec yes' could cause the DNS service to exit with an assertion failure.

CVE-2017-3135

Under some conditions when using both DNS64 and RPZ to rewrite query responses, the querying process could resume in an inconsistent state, resulting in either an INSIST assertion failure or an attempt to read through a NULL pointer.

CVE-2016-10126

Splunk Web in Splunk Enterprise 5.0.x before 5.0.17, 6.0.x before 6.0.13, 6.1.x before 6.1.12, 6.2.x before 6.2.12, 6.3.x before 6.3.8, and 6.4.x before 6.4.4 allowed remote attackers to conduct HTTP request injection attacks and obtain sensitive REST API authentication-token information via unspecified vectors, aka SPL-128840.

CVE-2016-9444

An unusually-formed answer containing a DS resource record could trigger an assertion failure and cause the DNS service to stop, resulting in a denial of service to clients.

CVE-2016-9147

An error handling a query response containing inconsistent DNSSEC information could trigger an assertion failure and cause the DNS service to stop, resulting in a denial of service to clients.

CVE-2016-9131

A malformed response to an ANY query can trigger an assertion failure during recursion and cause the DNS service to stop, resulting in a denial of service to clients.

CVE-2016-8864

While processing a recursive response that contained a DNAME record in the answer section, “named” could stop execution after encountering an assertion error in resolver.c.

CVE-2016-6306

The certificate parser in OpenSSL before 1.0.1u and 1.0.2 before 1.0.2i might allow remote attackers to cause a denial of service (out-of-bounds read) via crafted certificate operations, related to s3_clnt.c and s3_srvr.c.

CVE-2016-6304

Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allowed remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions.

CVE-2016-5696

The net/ipv4/tcp_input.c in the Linux kernel before 4.7 did not properly determine the rate of challenge ACK segments, which made it easier for man-in-the-middle attackers to hijack TCP sessions via a blind in-window attack.

CVE-2016-1285

A defect in the control channel input handling could cause the DNS service to fail due to an assertion failure in sexpr.c or alist.c when a malformed packet was sent to the control channel.

CVE-2016-1286

An attacker who controlled a server to make a deliberately chosen query to generate a response that contained RRSIGs for DNAME records could cause the DNS service to fail due to an assertion failure in resolver .c or db.c, resulting in a denial of service to clients.

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.

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:

Secondary servers using text-format db files could be vulnerable if receiving a malformed record in a zone transfer from their masters.

Primary servers 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'.

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.

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.

CVE-2015-7547

The glibc DNS client side resolver was vulnerable to a stack-based buffer overflow when the getaddrinfo() library function was used. Software using this function might be exploited with attacker-controlled domain names, attacker-controlled DNS servers, or through a man-in-the-middle attack.

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

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-2015-5986

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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). Note that SSL3 is still used for transmission of reporting data, but you can disable SSL3 on your reporting server to protect it from the vulnerability.

CVE-2014-3567

A denial of service vulnerability that is related to session tickets memory leaks.

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).

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.

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)."

CVE-2014-3470

Enabling anonymous ECDH cipher suites on TLS clients could cause a denial of service.

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.

CVE-2014-0221

Remote attackers could utilize DTLS hello message in an invalid DTLS handshake to cause a denial of service.

CVE-2014-0198

Enabling SSL_MODE_RELEASE_BUFFERS failed to manage buffer pointer during certain recursive calls that could cause a denial of service.

CVE-2014-0195

Remote attackers could trigger a buffer overrun attack through invalid DTLS fragments to an OpenSSL DTLS client or server, resulting in a denial of service.

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 table below.

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.

Fixed in NIOS 9.0.4

#	ID	Severity	Summary
1	NIOS-99443	Critical	Modifying a DNS zone such as adding a comment to the zone, and saving the changes caused the DNS service to become unresponsive for a minute, resulting in a brief outage.
2	NIOS-99014	Critical	Under a rare circumstance, high disk utilization occurred causing a DNS service impact.
3	NIOS-98114	Critical	Under a rare circumstance, fastpath cores were stuck in a loop.
4	NIOS-97010	Critical	Disabled Active Directory account users were allowed to authenticate and log in.
5	NIOS-95623	Critical	NIOS did not offer enabled ciphers and algorithms for pulling zone data from the Microsoft Active Directory.
6	NIOS-60625	Critical	Clicking **Grid Manager** > **Member** tab displayed an error and the DNS service could not be restarted from the Grid Manager.

#	ID	Severity	Summary
1	NIOS-101106	Major	After a NIOS upgrade, Grid Manager was slow when DNS Traffic Control objects were loaded because of additional checks introduced to improve performance.
2	NIOS-100787	Major	The NIOS documentation was missing the Audience URI/ SP Entity ID details needed for SAML configuration.
3	NIOS-100440	Major	The X6 Series appliances answered DNS Anycast servers either on LAN1 or LAN2 interfaces but not both.
4	NIOS-100388	Major	In the *Grid Properties Editor*, the fields in the **CSP Config** > **Advanced** tab needed to be moved to the **CSP Config** > **Basic** tab.z
5	NIOS-100345	Major	The ib-dns-usage-report-per-month alert did not generate data.
6	NIOS-100258	Major	The NIOS Release Notes contained an incorrect description regarding a known issue about DDNS updates bypassing the infoblox-last-queried-denylist ACLs.
7	NIOS-99989	Major	After a NIOS upgrade, swap usage increased and memory alerts were triggered.

#	ID	Severity	Summary
8	NIOS-99960	Major	Under certain circumstances, the DNS service crashed intermittently and the DNS server rebooted unexpectedly.
9	NIOS-99845	Major	After running an Azure vDiscovery job, certain subnet were missing and certain subnets were grouped wrongly though the job completed without errors.
10	NIOS-99841	Major	Under certain circumstances, several warning messages were displayed on the DNS Grid members during the AWS Route 53 synchronization tasks in the Grid.
11	NIOS-99733	Major	After a NIOS upgrade, ALIAS records did not work as expected.
12	NIOS-99571	Major	The NIOS documentation did not contain information about the newly introduced SNMP MIBs.
13	NIOS-99452	Major	The server performing the AWS cloud synchronization was frequently going offline.
14	NIOS-99416	Major	Under certain circumstances, RRSIG regeneration for DNS Traffic Control LBDN records failed thereby triggering an outage.
15	NIOS-99413	Major	The online help was not displayed for the *IPv4 Network Container/ IPv6 Network Container* > **Filters** screen.
16	NIOS-99372	Major	Subscriber service garbage collection was not allowed during a staged upgrade.
17	NIOS-99080	Major	Even after a hotfix was applied, users were getting logged out of Grid Manager.
18	NIOS-98985	Major	Continuous DB_SENTINEL VIOLATION errors occurred on one of the DNS members leading to product restarts and HA failovers, thus causing DNS outage.
19	NIOS-98731	Major	IP addresses, administration status, operation status and other information was not displayed for certain devices.
20	NIOS-98697	Major	Under certain circumstances, the smart subnet ping sweep did not work as expected.
21	NIOS-98681	Major	The NIOS documentation did not contain information about the BloxConnect port details.
22	NIOS-98584	Major	Under certain circumstances, the DNS server stopped responding to queries.
23	NIOS-98458	Major	NIOS was vulnerable to CVE-2023-48795.
24	NIOS-98175	Major	After a NIOS upgrade, the support bundle was not generated through the Grid Manager but it was getting generated by using the CLI.
25	NIOS-98117	Major	Automation of pstack, gcore, troubleshooting details when fastpath CPUs get stuck was required.
26	NIOS-98096	Major	Various devices in a network were not able to get the MAC address for one of the Grid members.
27	NIOS-98043	Major	After a NIOS upgrade, several host records did not get populated using the global search.
28	NIOS-98036	Major	After a NIOS upgrade, the device name and model were incorrect for several devices.
29	NIOS-98029	Major	After a NIOS upgrade, the Grid Manager was slow in loading the dashboard.
30	NIOS-97988	Major	The enable_discovery, discovery_exclusion_range, and discovery_member columns were missing from the header-ipv6network output in the CSV format file.
31	NIOS-97963	Major	Under certain circumstances, the “err TCP connection failed: socket is not connected” message was displayed in the syslog file.
32	NIOS-97956	Major	The NIOS documentation did not contain information about NIOS groups that access the reporting server to adhere to Splunk's naming convention guidelines,
33	NIOS-97853	Major	The NIOS documentation did not contain clear information about overriding Grid-level syslog settings and enabling syslog proxy for individual members.
34	NIOS-97850	Major	The AWS Route53 synchronization stopped working unexpectedly due to a RabbitMQ failure and core files were generated on the member that performed the synchronization.
35	NIOS-97791	Major	SSL certificate verification failed during VMware vDiscovery.

#	ID	Severity	Summary
36	NIOS-97733	Major	The Grid Manager displayed the Grid and the Grid member in a warning state when the Power Supply Unit 2 was not installed.
37	NIOS-97727	Major	The Grid Manager indicated that a filter was assigned to a network although the Grid Manager configuration did not indicate the same.
38	NIOS-97565	Major	
39	NIOS-97480	Major	Unable to send the manual Grid backup to the new SCP server.
40	NIOS-97055	Major	Under certain circumstances, the system-generated AAAA record was missing.
41	NIOS-97007	Major	Under certain circumstances, DNS resolution failed intermittently for a DNS Traffic Control server in an LBDN.
42	NIOS-96936	Major	An unexpected fault tolerant caching behavior occurred when blacklist rules were configured.
43	NIOS-96933	Major	Under certain circumstances, high CPU utilization occurred on the Grid Master.
44	NIOS-96774	Major	API and WAPI calls to NIOS did not work as expected and the API calls for DHCP leases could not be filtered by network.
45	NIOS-96720	Major	Even though the discovery CLI credentials were updated, they were not being used and the earlier CLI credentials were being used instead.
46	NIOS-96514	Major	A Grid member did not synchronize with the Grid Master and SNMP core files were continuously generated.
47	NIOS-96480	Major	After a NIOS upgrade, the NTP server went out of synchronization and there was a time difference of 35 minutes between the NTP server time and the actual time.
48	NIOS-96118	Major	There was a Splunk version disclosure on the Advanced DNS Protection (external DNS) members.
49	NIOS-96068	Major	The “Option Filter Match Rule” topic needed to be removed from the NIOS documentation.
50	NIOS-96008	Major	The smart folders filter 'Last discovered' did not display results when combined with the 'IPv4 Network' filter.
51	NIOS-95809	Major	Linked objects were not cleared properly from the database when the top -level virtual TFTP directory was removed from the Grid Manager thereby affecting the TFTP operation.
52	NIOS-95666	Major	The WAPI call displayed an error for network objects that had network containers associated with them.
53	NIOS-95603	Major	The source of the trusted domains database and the whitelist threat analytics domain list generation needed to be reassessed.
54	NIOS-95498	Major	A clickjacking vulnerability was detected on TCP port 9185.
55	NIOS-95412	Major	A database synchronization issue with the Grid members occurred after a set of IP addresses was reclaimed.
56	NIOS-94769	Major	Unable to disable the SSHD Kex algorithms in the Grid using the set `sshd_kexalgorithms` CLI command because the algorithms were not getting listed.
57	NIOS-94555	Major	The DNS restart groups did not work as expected.
58	NIOS-94520	Major	Unable to pre-provision IB-1415 and IB-1425 appliances using WAPI.
59	NIOS-94428	Major	Unable to synchronize DHCP data from Microsoft DHCP to NIOS DHCP in read-write mode.
60	NIOS-93918	Major	RPZ logs were not visible in the Cloud Services Portal.
61	NIOS-93514	Major	The DNS Traffic Control monitor health check displayed a blank output.
62	NIOS-93294	Major	IP addresses for the root servers needed to be changed.

#	ID	Severity	Summary
63	NIOS-92343	Major	The timestamp in the Grid Manager's syslog was one hour ahead compared to the actual time displayed in the CLI/SSH.
64	NIOS-91292	Major	
65	NIOS-91108	Major	Performing a reporting backup to the SCP server using the **Use Keys** option failed.
66	NIOS-90410	Major	The DNS service restarted every 1 to 2 minutes and the DNS resolver stopped responding to queries at random times.
67	NIOS-90063	Major	Under certain circumstances, a drop in the QPS rate occurred on a DNS server.
68	NIOS-88863	Major	Unable to create a reverse mapping zone in the default DNS view.
69	NIOS-88739	Major	It was possible to add an invalid record using WAPI.
70	NIOS-86180	Major	High disk usage occurred that was caused by a large number of DNS core files that kept generating.
71	NIOS-85351	Major	Executing a Python WAPI call resulted in an internal server error.
72	NIOS-85166	Major	The DNS scavenging schedule did not work as expected.
73	NIOS-84749	Major	Unable to use CSV import when the option filter name contained a comma.
74	NIOS-84097	Major	When accessing smart folders, looking for objects assigned to a specific extensible attribute resulted in an error.
75	NIOS-83823	Major	NIOS was vulnerable to CVE-2018-11409.
76	NIOS-83688	Major	When creating a network container, an IBAP exception error occurred.
77	NIOS-63430	Major	BloxTools could be exploited to perform remote command execution. The NIOS WAPI was vulnerable to a denial-of-service (DoS) attack due to insecure handling of the XML input.

#	ID	Severity	Summary
1	NIOS-99724	Minor	Certain MySQL and Apache parameters were lost after the Network Insight container was deleted or recreated.
2	NIOS-98812	Minor	The **Test Connection** option failed when the proxy server password contained certain special characters.
3	NIOS-98126	Minor	The WAPI command to fetch PTOP logs from the Grid member using WAPI version 2.9.7 did not work.
4	NIOS-98087	Minor	The CSV import and export for the number of records in subscriber sites needed to be limited.
5	NIOS-98004	Minor	The NIOS documentation contained an incorrect example of the DNS syslog message format.
6	NIOS-97959	Minor	CSV import did not work and the "EA update aborted due to 'ipv6_addresses'" error message was displayed.
7	NIOS-96845	Minor	The HTTPS_PROXY Docker restart took place silently, without any indication.
8	NIOS-95995	Minor	The follyd process consumed 100% CPU for extended periods of time during DHCP testing.

Fixed in NIOS 9.0.3

#	ID	Severity	Summary
1	NIOS-97493	Major	Unable to perform an advanced global search using Grid Manager.

#	ID	Severity	Summary
2	NIOS-97059	Major	The NIOS upgrade did not prevent hotfixes from being activated after the upgrade.
3	NIOS-96847	Major	The NIOS upgrade did not handle the csp_https_proxy setting.
4	NIOS-94359	Major	After a NIOS upgrade, WAPI calls returned the `Unknown argument/field: ipv4addrs` response.
5	NIOS-91711	Major	When a name server group containing a primary server and an external secondary server was assigned to an RPZ, the `allow-query` parameter was not updated with the secondary server in the named.conf file.

Fixed in NIOS 9.0.2

#	ID	Severity	Summary
1	NIOS-95256	Critical	Under a rare circumstance, Grid members failed to synchronize with the Grid Master.
2	NIOS-94339	Critical	When the DNS service was restarted on an ADP-enabled Grid member, after a restart, OSPF messages were being blocked by the ADP rule 130900300.
3	NIOS-92045	Critical	Under a rare circumstance, offline authoritative DNS servers were displayed as not being configured.

#	ID	Severity	Summary
1	NIOS-96730	Major	The LBDN returned the IP address of a DNS server whose status was “Down”.
2	NIOS-96731	Major	The NIOS documentation did not mention that the output of the `show ntp` CLI command for the `offset` argument has a limit of only 6 digits.
3	NIOS-96446	Major	The **MAC Address**, **OS**, and **NETBIOS NAME** fields needed to be added to the Infoblox Reporting and Analytics screen.
4	NIOS-96431	Major	Under certain circumstances, the passive node of a Grid Master disconnected frequently.
5	NIOS-96159	Major	After a NIOS upgrade, Active Directory users were not able to log on to Grid Manager.
6	NIOS-95970	Major	When attempting to convert numerous unmanaged subnets into managed subnets, an error message was displayed.
7	NIOS-95835	Major	Under certain circumstances, the Infoblox.log file exceeded its limit.
8	NIOS-95779	Major	The NIOS documentation did not mention that configuring the AWS Member Management (MGMT) network and the Grid Master’s LAN1 network on the same subnet is not supported and may cause connectivity issues.
9	NIOS-95663	Major	The NIOS documentation did not mention that the vDiscovery feature is not supported on ND appliances.
10	NIOS-95559	Major	After a NIOS upgrade, when vDiscovery jobs completed, warning messages were displayed.
11	NIOS-95509	Major	After a NIOS upgrade, AD authentication with nested groups failed.
12	NIOS-95459	Major	The NIOS documentation did not contain a statement on NTP RFC compliance.
13	NIOS-95102	Major	When DNS records were deleted using the **Reclaim** option on the **IPAM** tab, Grid Member Candidates lost connection to the Grid Master.
14	NIOS-94995	Major	On the **Global Smart Folders** tab, group results set to group by **Assigned VLAN ID** did not display data.

#	ID	Severity	Summary
15	NIOS-94680	Major	The DHCP server offered different IP addresses for the same client when unlimited lease time was configured.
16	NIOS-94640	Major	The **Cloud**> **Tenants** > **All Tenants** screen took a long time to load.
17	NIOS-94555	Major	DNS restart groups did not work as expected.
18	NIOS-94553	Major	If the dhcp6. prefix was not added to a custom DHCPv6 option name, custom options were not returned to the DHCPv6 client.
19	NIOS-94332	Major	The logging format for option 82 did not switch from plain text to hexadecimal or vice versa without an additional force service restart for DHCP.
20	NIOS-94179	Major	Unable to connect to the external syslog server using secure TCP as the external syslog server only allowed TLSv1.2 and the TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 cipher suites.
21	NIOS-93900	Major	The negative trust anchor was not added at the view level in the named.conf file even though recursion was enabled at the view level.
22	NIOS-93507	Major	Under certain circumstances, the system swap space usage exceeded the critical threshold value.
23	NIOS-93142	Major	Unable to add new values to the Site_ID extensible attribute. Also, the values already present did not load and displayed blank spaces.
24	NIOS-92665	Major	Clients periodically received responses that should have been captured by RPZs.
25	NIOS-92343	Major	The timestamp in the Grid Manager's syslog was one hour ahead compared to the actual time displayed in the CLI/SSH.
26	NIOS-92182	Major	The NIOS documentation did not mention that to execute the `set token join` CLI command on a Grid member, it is recommended to use a self-signed certificate on the Grid Master instead of a CA-signed certificate and that if the Grid Master has a CA-signed certificate, it is recommended to use the `set membership` CLI command instead of using the `set token join` CLI command.
27	NIOS-92103	Major	The extensible attribute table appeared twice when adding a host record.
28	NIOS-89867	Major	When an ACL was assigned to an authentication group, API calls generated the '500 Internal Server Error' response.
29	NIOS-86111	Major	The recursive DNS server did not look up other CNAME records in a chain when fault tolerant caching was enabled.
30	NIOS-85852	Major	The NIOS documentation did not contain information about the RPZ Substitute Domain Name rule.
31	NIOS-85796, NIOS-85739	Major	Amazon route 53 synchronization tasks could not have overlapping filters.
32	NIOS-84972	Major	SNMP did not display the correct status code for a broken Power Supply Unit (PSU).
33	NIOS-76979	Major	After a NOS upgrade, two AWS members went offline.
34	NIOS-73660	Major	When an ANY type query was received on a forwarded subzone, server failure responses were displayed in the log files.

Fixed in NIOS 9.0.1

#	ID	Severity	Summary
1	NIOS-94337	Critical	A high number of zone transfers with the same serial number occurred during the time of DNS service restarts thus causing DNS resolution issues.
2	NIOS-94001	Critical	After a NIOS upgrade, AWS Route 53 synchronization stopped using the configured proxy server.
3	NIOS-93264	Critical	The DHCP service kept restarting and entering the recovering state.
4	NIOS-91239	Critical	Running a vDiscovery job on the GCP platform failed and an error was displayed.
5	NIOS-90951, NIOS-90554	Critical	NIOS was vulnerable to CVE-2023-0286, CVE-2022-4304, CVE-20230215, and CVE-2022-4450.
6	NIOS-90485	Critical	Under a rare circumstance, a gradual increase in disk usage occurred.
7	NIOS-90188	Critical	After a NIOS upgrade, unable to access Grid Manager.
8	NIOS-89982	Critical	Memory usage on Grid Master gradually increased.
9	NIOS-86343	Critical	An HA failover was not triggered if Grid members were connected to the Grid Master through the management port.
10	NIOS-85626	Critical	The NIOS ecosystem did not work with the split network operation.

#	ID	Severity	Summary
1	NIOS-95022	Major	A database synchronization issue occurred with Grid members after a set of IP addresses was reclaimed.
2	NIOS-94756	Major	After a NIOS upgrade, unable to view and export alias records.
3	NIOS-94601	Major	If a client system queried multiple patterns associated with the same zone within the persistence period, the client system got a valid RRSIG for only the first queried pattern.
4	NIOS-94470	Major	After a NIOS upgrade, high CPU consumption occurred and several core files were generated.
5	NIOS-94136	Major	The NIOS documentation did not state that Grid members may restart all the services when the Grid Master recovers from the dual active state.
6	NIOS-94061	Major	The Device Inventory report did not display any data.
7	NIOS-93954	Major	Super host DHCP records associated with a subnet was not available in the drop-down list used to select a network.
8	NIOS-93933	Major	NIOS was vulnerable to stored cross-site scripting.
9	NIOS-93829	Major	Grid Manager stopped responding and an HA failover occurred when the RPZ tab was accessed.
10	NIOS-93285	Major	The Cloud Services Portal was sending trigger alerts regarding high memory usage and the memory computation in NIOS needed to be corrected.
11	NIOS-93252	Major	The total object count exported in the CSV export for A records was incorrect.
12	NIOS-93046	Major	A NIOS test upgrade failed and the “Existing IPv6 network template has two or more FA templates associated test upgrade failure” error message was displayed.
13	NIOS-93001	Major	The DNS service kept restarting after a NIOS hotfix was applied.
14	NIOS-92983	Major	The NIOS documentation required information about DNS exfiltration to be updated.
15	NIOS-92795	Major	The passive node of a Grid Master was restarting every few hours and email alerts were triggered.
16	NIOS-92663	Major	DDNS updates generated by domain controllers were not accepted by the Infoblox DNS members serving the relevant zone and no error messages were generated.

#	ID	Severity	Summary
17	NIOS-92658	Major	The Grid Master Candidate test promote did not work as expected.
18	NIOS-92653	Major	A DDoS attack occurred and the server performed a system restart.
19	NIOS-92439	Major	The NIOS documentation did not state that PAPI has been discontinued from NIOS 8.3 onwards.
20	NIOS-92410	Major	Unable to access Grid Manager and running CSV jobs caused issues.
21	NIOS-92369	Major	The Cloud Services Portal sent trigger alerts regarding high memory usage.
22	NIOS-92343	Major	The timestamp displayed in the syslog of the Grid Manager one hour ahead compared to the actual time displayed in the CLI.
23	NIOS-92321	Major	Under a rare circumstance, the threat analytics service was down and the health data was not displayed.
24	NIOS-92103	Major	The extensible attribute table was displayed twice when adding a host record.
25	NIOS-92093	Major	The NIOS documentation needed to be updated with the TLS cipher suites supported for the DOT/DOH feature.
26	NIOS-92047	Major	The NIOS documentation required updates on NTP behavior.
27	NIOS-92009	Major	The HSM Luna integration caused certain issues.
28	NIOS-91778	Major	After a NIOS upgrade, the 'Top Malware and DNS Tunneling events by client' dashboard did not display any data.
29	NIOS-91770	Major	A CLI command was required to to set different values to kernel/BIND parameters to address TCP incoming query handling issues.
30	NIOS-91729	Major	Running the set dns-auto-gen CLI command led to the removal of productive name server records.
31	NIOS-91341	Major	Unable to view the audit log in Grid Manager and the DBTypeError error was displayed.
32	NIOS-91340	Major	Modifying the fields in the *Grid Properties Editor* dialog box displayed the "An invalid value was entered" error message.
33	NIOS-91211	Major	The DNS Top RPZ Hits by Clients and DNS Top RPZ Hits reports displayed incorrect data.
34	NIOS-91159	Major	After a NIOS upgrade, login with Microsoft AD authentication did not work as expected.
35	NIOS-90975	Major	The output of the show interface all CLI command did not display the loopback interface address.
36	NIOS-90918	Major	Discovery diagnostics failed for Juniper Mist devices.
37	NIOS-90883	Major	NIOS was vulnerable to CVE-2006-20001, CVE-2022-36760, and CVE2022-37436 (Apache vulnerabilities).
38	NIOS-90872	Major	The CSV import failed and the "Bgp_config: cannot convert remote_as's "True" to internal format (int)" error was displayed.
39	NIOS-90827	Major	After an appliance was changed, the number of non-cache queries processed changed.
40	NIOS-90629	Major	There was a discrepancy between the maximum statistics and the average statistics in the DNS Daily Peak Hour Query Rate by Member report.
41	NIOS-90483	Major	NIOS reporting did not display ADP hits from several servers.
42	NIOS-90410	Major	The DNS service kept restarting frequently and the resolver stopped responding to queries at random times.
43	NIOS-90355	Major	After a NIOS upgrade, the TFTP process continually failed to start.
44	NIOS-90293	Major	After a NIOS upgrade, RabbitMQ errors were displayed in the log files.

#	ID	Severity	Summary
45	NIOS-90278	Major	OpenSSL version needed to be upgraded to version 1.1.
46	NIOS-90271	Major	Under certain circumstances, DDNS updates did not work as expected.
47	NIOS-90268	Major	The OVA image for ND-V1405 needed to be updated.
48	NIOS-90208	Major	The NIOS documentation did not contain information on DNS cookie support.
49	NIOS-90189	Major	The IP address of the DNS server instead of the actual IP address was being displayed in the CSP DNS Activity report.
50	NIOS-90164	Major	After a NIOS upgrade, Grid Manager was unresponsive.
51	NIOS-90151	Major	DNS queries including health checks were being dropped and UDPv4 errors were displayed in the log files.
52	NIOS-89996	Major	The tcpdump CLI command did not work after a NIOS hotfix was applied.
53	NIOS-89889	Major	Under certain circumstances, intermittent SERVFAIL responses were generated.
54	NIOS-89843	Major	VMware vDiscovery jobs failed and the "Error while running Job" error message was displayed.
55	NIOS-89772	Major	The DNS Traffic Control health check failed for a regular expression check.
56	NIOS-89736	Major	vDiscovery jobs failed and the "Error while running Job" error message was displayed.
57	NIOS-89723 NIOS-89467	Major	Passive nodes of HA Grid members were trying to communicate to the TCP port using the LAN1 interface.
58	NIOS-89548	Major	One of the vDiscovery jobs got stuck and that stopped the other jobs from running.
59	NIOS-89413	Major	When an invalid domain name was entered for a custom DHCP option, the DHCPD configuration file displayed a syntax error.
60	NIOS-89399	Major	DHCP resolution failed for a critical network.
61	NIOS-89353	Major	New admin users were unable to change the password from the Grid Manager when the Disable Concurrent Login option was enabled
62	NIOS-89351	Major	TCP “ANY” type queries were dropped most of the time.
63	NIOS-89039	Major	Infoblox VMs failed to boot after the host was rebooted.
64	NIOS-88970	Major	An object with an inherited value for an extensible attribute displayed an error during a WAPI search.
65	NIOS-88900	Major	Under certain circumstances, DNS was unavailable on some Grid members for several hours.
66	NIOS-88866	Major	IDP metadata calls against the NIOS SP failed due to a certificate path mismatch.
67	NIOS-88854	Major	The Grid Manager Members tab did not display all the Grid members and the “The system is taking longer than expected to complete your request. The data could not be retrieved within the maximum allowed time” error message was displayed.
68	NIOS-88674	Major	Under certain circumstances, all the DNS secondary nodes went offline and frequent product restarts took place.
69	NIOS-88563	Major	The discovered VLAN IDs and VLAN names of Cisco ACI networks kept updating with incorrect data.
70	NIOS-88384	Major	A scheduled backup did not work and no alerts or errors were triggered.
71	NIOS-88309	Major	Under certain circumstances, a new Grid member was unable to connect to the Grid.
72	NIOS-88071	Major	Unable to save VLAN data for Microsoft networks when synchronization is in read-only mode.
73	NIOS-88034	Major	The SOA serial number in the DNS notify messages sent from the lead secondary was different from what was displayed in the traffic capture bundle.

#	ID	Severity	Summary
74	NIOS-87802	Major	When the number of network views was greater than 127, the named.conf file failed to generate.
75	NIOS-87797	Major	Adding and saving a lookup file displayed the "Encountered the following error while trying to save: Client is not authorized to perform requested action" error message.
76	NIOS-87768	Major	Under certain circumstances, performance degradation and high latency issues occurred.
77	NIOS-87745	Major	Under certain circumstances, DNS dropped requests from queries.
78	NIOS-87576	Major	Creating a DNS Traffic Control monitor using WAPI failed because of a missing value.
79	NIOS-87356	Major	Restoring the database did not work as expected.
80	NIOS-87267	Major	vDiscovery failed as discovery did not receive the MAC address for a particular host.
81	NIOS-86893	Major	The ADP NTP rules were disabled when NTP service was disabled.
82	NIOS-86874	Major	The query_fqdn_on_member function did not work on the AXFR record.
83	NIOS-86852	Major	Attempting to edit a host record in an unmanaged network displayed an internal error.
84	NIOS-86381	Major	Deleting a delegated zone displayed an error message.
85	NIOS-86263	Major	Queries to an unknown upstream resolver used the UDP buffer size of 512 instead of the configured edns-udp-size value.
86	NIOS-86233	Major	The NIOS documentation needed to be updated about the 1.3.6.1.2.1.15.900.1.2 OID information.
87	NIOS-86228, NIOS-86225	Major	Under certain circumstances, the Grid stopped logging syslog messages.
88	NIOS-86130	Major	A scheduled SCP backup hung for a month until the SCP server was rebooted but no errors or alerts were generated.
89	NIOS-85974	Major	Unable to create DHCP range for MS_FAILOVER when using WAPI.
90	NIOS-85938	Major	Unable to apply the NIOS license by using the set license CLI command.
91	NIOS-85916	Major	Under certain circumstances, DDNS updates were dropped for no evident reason.
92	NIOS-85899	Major	An unexpected HA failover occurred on Grid Master due to a db_sentinel violation caused by Threat Analytics.
93	NIOS-85723	Major	The API GET call for object tracking did not return details regarding CAA, TLSA, DNAME, and Alias record response changes.
94	NIOS-85468	Major	Under certain circumstances, the **CONSOLIDATED HEALTH MONITOR SETTINGS** screen did not display all the applicable monitors.
95	NIOS-85356	Major	Restoring the database did not work as expected.
96	NIOS-84940	Major	Adding an extensible attribute of type string and then setting the maximum number of characters to 2147483648 turned the font in the Max field to red.
97	NIOS-84925	Major	After a NIOS upgrade, WAPI calls were unable to fetch the DNS Traffic Control health status for the DNS Traffic Control server, pool, and LBDN.
98	NIOS-84834	Major	Under certain circumstances, DNS Traffic Control health check based on HTTPS returned a false green status.
99	NIOS-84612	Major	Intermittent DNSSEC validation issues occurred when the smart cache feature was turned on.
100	NIOS-84480	Major	Under certain circumstances, high database utilization occurred and the Grid Manager could not be accessed.
101	NIOS-84227	Major	Unable to start the discovery service on the Network Insight member.

#	ID	Severity	Summary
102	NIOS-83934	Major	Unable to edit a CNAME record that starts with double quotes and which was present in a DNSSEC zone.
103	NIOS-83192	Major	The Grid Manager displayed a green status even though the CPU usage was at 100%.
104	NIOS-83124	Major	An upgrade test failure occurred because of TLSA records.
105	NIOS-80561	Major	The idns_healthd message was logged to the wrong facility in the syslog file.
106	NIOS-79628	Major	After a NIOS upgrade, sometimes the ProxyVIP address was resolved to non-subscriber sites.
107	NIOS-79471	Major	The Splunk REST API login failed after the reboot of the reporting search head until a Grid Manager login to reporting took place.
108	NIOS-79086	Major	LBDNs, pools, and servers went into a None status as soon as one of the nodes in an HA pair went down.
109	NIOS-77600	Major	The Grid reporting index percentage and the data retention value were not retained after a Grid Master Candidate promotion.
110	NIOS-76555	Major	Files and folders with world writable and world executable permission and with root privilege on NIOS servers were not being restricted.
111	NIOS-66570	Major	Unable to apply the license pool file and an error message was displayed.
112	NIOS-63430	Major	NIOS was vulnerable to a Denial of Service attack and to the BloxTools service exploitation.

#	ID	Severity	Summary
1	NIOS-93566	Minor	Discovered devices were not added to the IPAM IP tables.
2	NIOS-93127	Minor	When Treat Protection was enabled, some syslog messages were not displayed in the syslog file.
3	NIOS-92332	Minor	The SERVFAIL cache entries needed to be updated to include an "ms" suffix next to the TTL values to explicitly indicate that the values are in milliseconds.
4	NIOS-92084, NIOS-92082,	Minor	NIOS was vulnerable to OpenSSL vulnerabilities CVE-2023-0464, CVE2023-0465, and CVE-2023-0466.
5	NIOS-91022	Minor	The Use DHCP Routers as Seed Routers option triggered discovery service restarts during attempts to apply new the configuration.
6	NIOS-90577	Minor	After a NIOS upgrade, RADIUS authentication failed.
7	NIOS-90166	Minor	TCP “ANY” type queries were dropped most of the time.
8	NIOS-89652	Minor	IPAM IP synchronization from Network Insight to the Grid IPAM was slow.
9	NIOS-88697	Minor	NIOS was susceptible to certain vulnerabilities.
10	NIOS-88135	Minor	Alias A records did not move to the newly created sub-domain until the TTL of the record was updated.
11	NIOS-87262	Minor	The syslog backup feature did not work on a specific HA node.
12	NIOS-86886	Minor	The syslog for DHCP messages displayed an incorrect transaction ID.
13	NIOS-86387	Minor	After a NIOS upgrade, search report files sent to the external FTP/SCP server contained additional quotes.
14	NIOS-84457	Minor	A CSV import did not work as expected.
15	NIOS-84226	Minor	Microsoft synchronization erroneously generated the “Resolved by deleting the value from NIOS” message in the log files.
16	NIOS-83171	Minor	The syslog files were flooded with GSS-TISG secure update log messages.

17	NIOS-81176	Minor	The smart ping sweep setting of the IPAM network did not override the same setting at the Grid level.
18	NIOS-66608	Minor	The DNS Traffic Control licensing option needed to be removed from the TE-810 and TE-820 appliances.

Fixed in NIOS 9.0.0

#	ID	Severity	Summary
1	NIOS-87843	Critical	The NIOS OVA image took a long time to deploy.
2	NIOS-86923	Critical	Under certain circumstances, Amazon Route 53 sync tasks took very long to complete.
3	NIOS-86135	Critical	Under a rare circumstance, an HA failover occurred and caused more than 10 seconds of DNS down time.
4	NIOS-85707	Critical	Route 53 sync tasks too a long time to complete.
5	NIOS-85430	Critical	Remote authentication failed for users who had an account in both the RADIUS service as well as in NIOS.
6	NIOS-85207	Critical	Under a rare circumstance, NIOS logged the 'Failed to upload captured DNS log to remote FTP/SCP server' message and did not forward data to the Cloud Data Connector.
7	NIOS-84845	Critical	Under a rare circumstance, the DNS service did not respond and crashed.
8	NIOS-84614	Critical	Adding a record to a DNSSEC signed zone displayed an error message.
9	NIOS-84523	Critical	After a NIOS upgrade, the **Cloud** > **Network** tab displayed an error.
10	NIOS-84015	Critical	The threat protection service did not start on VMware VMs.
11	NIOS-83694	Critical	Under a rare circumstance, DHCP failover association failed.
12	NIOS-82210	Critical	Subscriber services needed to reduce the number of guest notifications.
13	NIOS-81406	Critical	A zVELO category mapping needed to be changed.
14	NIOS-79931	Critical	After a NIOS upgrade, SSH, MGMT, port flapping, and DNS issues occurred.
15	NIOS-78386	Critical	Under a rare circumstance, host records were deleted after discovery was complete and unable to login to Grid Manager when discovery is running.
16	NIOS-78347	Critical	NIOS was vulnerable to CVE 2021-23839, CVE-2021-23840, and CVE2021-23841.
17	NIOS-78323	Critical	An IB-4025 appliance did not restart after threat protection was enabled.
18	NIOS-78293	Critical	For IB-FLEX members deployed on vNIOS for KVM Hypervisor and enabled with virtual DNS cache acceleration and Advanced DNS Protection software,
19	NIOS-77329	Critical	When port redundancy on LAN1/LAN2 was enabled on Grid members in the OpenStack platform, the 'Fatal Error During Infoblox Startup' error message was displayed.
20	NIOS-74556	Critical	The DNS Cache Acceleration dashboard displayed 0% constantly for a particular server. The server also displayed high CPU usage.
21	NIOS-74414	Critical	NIOS was vulnerable to CVE-2017-12542, CVE-2018-7078, CVE-20187101, CVE-2016-4406, CVE-2015-5435, CVE-2018-7117, CVE-201911982, and CVE-2019-11983.

#	ID	Severity	Summary
1	NIOS-89434	Major	The DNS service crashed after recursive lookups exceeded the threshold value.

#	ID	Severity	Summary
2	NIOS-88294	Major	Restricted extensible attributes in network objects were being displayed in the Network View screen.
3	NIOS-88229	Major	When accessing Grid Manager on an appliance that has TLS 1.2 configured, an "SSL connect error" message was displayed in the log files.
4	NIOS-87823, NIOS-87822	Major	After a NIOS upgrade, unable to modify or create networks, zones, and extensible attributes and the "The database is locked by background tasks. Operation is not permitted." error message was displayed.
5	NIOS-87813	Major	After a NIOS upgrade, DNS resolution failed for some domains.
6	NIOS-87761	Major	The Grid Manager did not detect space in the Name field when creating an authoritative forward mapping zone that is mapped to some nameserver groups.
7	NIOS-87695	Major	Tasks submitted by SAML users disappeared once SAML users logged out of their accounts.
8	NIOS-87694	Major	NIOS was vulnerable to CVE-2022-3488.
9	NIOS-87669	Major	After a NIOS upgrade, access to the nios_version.txt file required authentication by specifying the NIOS login credentials.
10	NIOS-87611	Major	Converting multiple unmanaged networks failed.
11	NIOS-87606	Major	Extensible attribute settings were configured as required but the settings were not being saved.
12	NIOS-87298	Major	IB-FLEX systems running on OpenStack encountered issues while providing answers to clients for certain domains.
13	NIOS-87282	Major	The vNIOS documentation did not specify the permissions or authorization that were required for the Amazon Route 53 integration.
14	NIOS-87267	Major	vDiscovery failed as the discovery device did not receive the MAC address of a particular host system.
15	NIOS-87253	Major	After a NOS upgrade, a sharp increase in the CPU usage of the active node on an HA Grid Master occurred.
16	NIOS-87236	Major	After a NOS upgrade, the *Grid Member Properties Editor* displayed an "Internal Error" error message.
17	NIOS-87136, NIOS-81645	Major	WAPI nested fields did not return accurate values for paged responses that were in the original response.
18	NIOS-87061	Major	Certain vDiscovery jobs were getting stuck and some jobs were not running as per schedule.
19	NIOS-87020	Major	Using the Quick Filter option to filter by the Managed value did not work as expected.
20	NIOS-87012	Major	The NIOS HA documentation needed to be updated with information about LAN1 and HA ports.
21	NIOS-86947	Major	The DNS service did not respond after DNS Traffic Control changes thus impacting authoritative and recursive queries.
22	NIOS-86937	Major	A jQuery version used in NIOS Grids contained some vulnerabilities.
23	NIOS-86916	Major	Unable to sign zones with IDN names that contain Unicode characters after applying a hotfix.

#	ID	Severity	Summary
24	NIOS-86893	Major	Advanced DNS Protection NTP rules were disabled when the NTP service was disabled.
25	NIOS-86838	Major	An AWS Grid member displayed a different gateway address on the CLI compared to Grid Manager.
26	NIOS-86777	Major	A passive node of a Grid Master did not come back online after a manual reboot from the CLI.
27	NIOS-86759	Major	Unable to add networks with overridden settings in Network Insight because a validation was required that the number of overridden network settings cannot exceed 200.
28	NIOS-86738	Major	The WAPI REST call for ipv6network incorrectly treated a search using an empty regular expression.
29	NIOS-86737	Major	The WAPI REST call did not correctly handle the sharedrecordgroup attribute zone associations.
30	NIOS-86536	Major	The memory allocation was quoted wrongly for IB-V4015 and IB-V4025 in the *Infoblox Installation Guide vNIOS™ for VMware*.
31	NIOS-86391	Major	The DNSSEC zone became invalid because the DNSKEY record was not being updated when it should have been.
32	NIOS-86295	Major	DNS updates to zones that do not have a zone stanza in the dhcpd.conf file were being deferred.
33	NIOS-86208	Major	A vDiscovery job was stuck and the Grid Manager displayed the "Job in progress" message.
34	NIOS-86180	Major	A large number of DNS core files was generated resulting in high disk usage.
35	NIOS-86017	Major	Certain long running processes caused db_sentinel timeouts.
36	NIOS-85967	Major	A Grid Master Candidate was able to collect the snapshot of a record.
37	NIOS-85837	Major	Under certain circumstances, unable to delete a nameserver group.
38	NIOS-85820	Major	The DeduplicationTasks.pl script did not run on Network Insight as a result of which devices were not deduplicated on probes.
39	NIOS-85795	Major	A restriction regarding the PUT operation for security_setting had to added to the NIOS API documentation.
40	NIOS-85785	Major	Filtering DHCP leases by using external Microsoft servers as the filter results in No Data being displayed.
41	NIOS-85758	Major	The status of several DNS Traffic Control servers was displayed as Error even though the health checks worked correctly for several pools.
42	NIOS-85622	Major	Extensible attribute topology database rebuild failed.
43	NIOS-85581	Major	The NIOS documentation did not contain information about external attributes available during an Amazon Route 53 synchronization.
44	NIOS-85580	Major	Wrong security groups were assigned when two Active Directory users had the same first name and last name and one of them belonged to a different organizational unit (OU) than the default.
45	NIOS-85545	Major	The NIOS documentation needed more information about port 8765 that is required for SAML authentication.

#	ID	Severity	Summary
46	NIOS-85511	Major	NIOS did not have the ability to control TLS versions dynamically for the SAML port 8765.
47	NIOS-85480	Major	Disabling RPZ logging on the first RPZ in a list disables all CEF event logging for parent control policies for all RPZs irrespective of the individual setting.
48	NIOS-85406	Major	After a NIOS upgrade, a Grid member failed to join the Grid.
49	NIOS-85360	Major	The partial health update did not work as expected and an error was displayed when DNS Traffic Control server and pool were disabled without configuring the health monitor.
50	NIOS-85338	Major	NIOS was vulnerable to CVE-2020-11947.
51	NIOS-85317	Major	Application of Grid-wide Threat Analytics license on IB-v825 appliances failed after the existing license expired.
52	NIOS-85268	Major	The Grid Manager restarted when trying to sign zones that contained DNAME records.
53	NIOS-85203	Major	File distribution failed because a Splunk .tar file did not extract as expected.
54	NIOS-85182	Major	The Infoblox Installation Guide 1405 Series Appliances documentation indicated that fans can be replaced by a FRU (Field Replaceable Unit); but IB-1405 fans cannot be replaced.
55	NIOS-85156	Major	No SNMP trap was generated for Grid members that connected back to the Grid after a NIOS upgrade.
56	NIOS-85149	Major	The WAPI call for the DHCP range object accepted an invalid input.
57	NIOS-85148	Major	An IB-FLEX appliance did not join an HA pair.
58	NIOS-85122	Major	The SFP ports on TE-4005 appliances were in reverse order of the label.
59	NIOS-84946, NIOS-84944, NIOS-84942	Major	RIR RIPE updates failed to connect to the RIPE test database.
60	NIOS-84914	Major	The refresh interval of a zone transfer did not work when it was configured to be less than 300 seconds.
61	NIOS-84808	Major	When vDiscovery jobs were enabled, some of the jobs contained recurring errors.
62	NIOS-84697	Major	Under certain circumstances, recursive DNS queries did not resolve as expected.
63	NIOS-84665	Major	The DNSKEY record for KSK was deleted automatically for multiple zones.
64	NIOS-84648	Major	The SSO login prompt disappeared every time after an HA failover.
65	NIOS-84633	Major	When enabling IPv6 as the DNS interface a resource record error was displayed.
66	NIOS-84632	Major	The NIOS documentation did not correctly explain the change in behavior regarding DHCP filter logic.
67	NIOS-84564	Major	When trying to view Grid member by navigating from **Data Management** > **DNS** > **Members/servers**, instead of Grid members, the "An error has occurred. Contact technical support if the problem persists" error message was displayed.
68	NIOS-84520	Major	When using global smart folders, the Edit, Create link, and Delete icons were hidden.
69	NIOS-84505	Major	Only four multicast listener ICMP messages were being accepted unconditionally.

#	ID	Severity	Summary
70	NIOS-84487	Major	Under certain circumstances, an unexpected HA failover occurred on the Grid Master.
71	NIOS-84436	Major	NIOS was vulnerable to CVE-2022-0778.
72	NIOS-84412	Major	The Credential setting was automatically switched to the Use instance profile option in an Amazon Route 53 synchronization group when the member assignment was changed from one member to another.
73	NIOS-84407, NIOS-84332, NIOS-84135	Major	Unable to create the same zone as an authoritative zone after deleting the zone from Grid Manager.
74	NIOS-84351	Major	Unable to apply NIOS licenses after a hotfix was applied.
75	NIOS-84338	Major	Unable to add networks to Active Directory sites.
76	NIOS-84300	Major	Converting multiple unmanaged networks that had a /31 mask displayed an error message.
77	NIOS-84277	Major	The SHA1 algorithm being used by NIOS was prone to security scan vulnerabilities.
78	NIOS-84249	Major	The NIOS documentation contained incorrect information about DHCP failover
79	NIOS-84243	Major	Excessive OSPF routes prevented the updating of direct routes.
80	NIOS-84217	Major	Adding an IP address to an existing host displayed the "Enter a valid MAC address. Example: 01:0C:F1:DE:A9:40" error message.
81	NIOS-84216	Major	Unable to access a specific network in IPAM.
82	NIOS-84146	Major	A NIOS upgrade failed and the “1 of 1 node has failed upgrade - Upgrading: Syncing storage files..." error message was displayed.
83	NIOS-84050	Major	A simultaneous restart of all Grid members took place due to an HA failover on Grid Master.
84	NIOS-84047	Major	The NIOS documentation did not contain information about restrictions while adding host names.
85	NIOS-84034	Major	The health monitor did not work as expected.
86	NIOS-84027	Major	The NIOS documentation did not contain information about the restrictions imposed when adding a host name that contains characters.
87	NIOS-84001	Major	Unable to apply changes to a newly promoted Grid Master until the external NTP server usage was disabled using a WAPI call.
88	NIOS-83982	Major	Unable to remove DNSSEC signature from some zones.
89	NIOS-83911	Major	After a NIOS upgrade, the loopback IP address was removed from the allow-recursion list because of which recursive queries to the loopback IP address failed.
90	NIOS-83729, NIOS-83728	Major	Microsoft Azure cloud vDiscovery stopped working and an error message was displayed.
91	NIOS-83689	Major	The DHCPv6 server did not provide option 39 in its replies.
92	NIOS-83482	Major	Detailed debug logs for BFD needed to be enabled.
93	NIOS-83445	Major	Grid Manager incorrectly reported a failed upgrade for some Grid members.
94	NIOS-83439	Major	While trying to remove an offline Grid member, the "Object(s) referencing current object have not been removed" error message was displayed.

#	ID	Severity	Summary
95	NIOS-83293	Major	After adding two cloud platform appliances to the Grid and then modifying networks, the “Extensible Attribute Tenant ID is required“ error message is displayed.
96	NIOS-83285	Major	After restoring the NIOS database, the Grid automatically reverted to an earlier version.
97	NIOS-83257	Major	Microsoft Azure cloud vDiscovery stopped working and an error message was displayed.
98	NIOS-83204	Major	While enabling the Disable Concurrent Login option, the property was being inherited by the system generated 'splunk-reporting-group' group.
99	NIOS-83197	Major	IPv6 data was either displayed when not required or not displayed when required in certain reports.
100	NIOS-83193, NIOS-83188	Major	Inherited values of DHCP thresholds on DHCP range objects were not reflected in the WAPI calls.
101	NIOS-83187	Major	Under certain circumstances, Grid members were unable to query authoritative zones.
102	NIOS-83177	Major	Unable to search IPv4 networks through WAPI calls.
103	NIOS-83176	Major	Deleting a zone in Grid Manager did not work as expected.
104	NIOS-83175	Major	DNS resolution failed for authoritative zones and the SERVFAIL error was displayed in the log files.
105	NIOS-83173	Major	The Task Details column on the Workflow > Task Manager tab did not display data when the details were added using API calls.
106	NIOS-83155	Major	An HA Grid Master that was serving a DHCPv6 server started discarding renews after an HA failover.
107	NIOS-83152	Major	NIOS appliances were affected by an SNMP configuration injection vulnerability.
108	NIOS-83129	Major	Device status files displayed conflicting speed for appliance interfaces
109	NIOS-83079	Major	DHCP release messages were not processed correctly leading to pool exhaustion.
110	NIOS-83076	Major	ADP profiles that were created using the latest rulesets were reverted to the default values.
111	NIOS-83065	Major	vDiscovery failed if extensible attributes such as tenant ID, CMP type and so on were present before installing the Cloud Network Automation license.
112	NIOS-83048	Major	Even though full snapshots were successfully imported, generating incremental snapshots displayed an error.
113	NIOS-83006, NIOS-81687	Major	Editing an NTP member settings displayed the "expected single object, got 2" error message in Grid Manager.
114	NIOS-83002	Major	IPv6 lease exhaustion, multiple active IP addresses from the same subnet for the same client, IB DHCP failure to renew certain unicast requests generated a "NoBinding - Status 3" response.
115	NIOS-82980	Major	NIOS was vulnerable to CVE-2021-43527.
116	NIOS-82959	Major	Grid members on an ESXi segment were not able to ping their default gateway or each other using IPv6.

#	ID	Severity	Summary
117	NIOS-82940	Major	Under certain circumstance, IPMI ports on IB-22x5 appliances stopped responding.
118	NIOS-82883	Major	Attempting to join an existing Grid resulted in a failure and the "Error: Unable to sync release" error message was displayed.
119	NIOS-82775	Major	In Network Insight, errors were displayed during IP address consolidation and the synchronization to Grid Manager did not work as expected.
120	NIOS-82773	Major	An incorrect VLAN ID was displayed for end hosts in the IPAM view.
121	NIOS-82770	Major	Network insight queried Infoblox DNS servers even when the DNS resolver was set to query external Microsoft DNS servers.
122	NIOS-82769	Major	A reporting appliance returned an empty value for the "End host history" report.
123	NIOS-82767	Major	The discovery services failed constantly at regular Intervals and the Devices tab kept buffering.
124	NIOS-82765	Major	When SPM collection was disabled at the Grid level but enabled at the network level, no SPM data was collected.
125	NIOS-82764	Major	SNMPv3 credentials that do not have a privacy protocol were not saved in Network Insight.
126	NIOS-82761	Major	The CLI command to collect ARP data for Cisco devices needed to be changed.
127	NIOS-82760	Major	"Discovery Collector Service is inactive" SNMP trap messages were frequently received when the SDN engine was off.
128	NIOS-82756	Major	CIDRs were not pushed from the discovery_ranges table and unable to discover new devices.
129	NIOS-82755	Major	IPAM networks were not being updated with direct routes from certain devices.
130	NIOS-82754	Major	Bulk conversion to host records did not work when no zone was specified.
131	NIOS-82721	Major	Performing an AXFR query from a secondary server to a primary server through the dashboard widget in Grid Manager displayed “Unable to query domain name” error message.
132	NIOS-82716	Major	Restarting services using Grid Manager displayed the “Contact Technical Support” error message.
133	NIOS-82670	Major	When a named ACL was applied to an authoritative zone, it was propagated to only one Grid primary member.
134	NIOS-82663	Major	The “The configuration changes require a rebuild of the Extensible Attribute Topology Database. Use the Rebuild button to rebuild the database. The Ignore button will hide these warnings for the current user session” banner kept being displayed in Grid Manager.
135	NIOS-82662	Major	The hardware ID displayed an incorrect MAC address.
136	NIOS-82624	Major	The SNMP daemon restarted frequently thus affecting the monitoring and unit uptime changes.
137	NIOS-82623	Major	The threat protection service was inactive on newly added Grid members.
138	NIOS-82617	Major	Modifying a set of TXT DKIM records using CSV import failed for some records because the TXT string contained a backslash.

#	ID	Severity	Summary
139	NIOS-82530	Major	The Network Advisor client did not work correctly for certain devices of complex configuration (stack + several different chassis).
140	NIOS-82321	Major	The syslog was rotated before it reached the configured maximum syslog size.
141	NIOS-82304	Major	SOA records failed to validate with DNSSEC.
142	NIOS-82230	Major	Under certain circumstances, the threat analytics service displayed a warning message or was inactive.
143	NIOS-82215	Major	Under certain circumstances, the DNS service failed and caused a service impact.
144	NIOS-82178	Major	Grid Manager frequently restarted and logged the “Logging region out of memory; you may need to increase its size” error message.
145	NIOS-82087	Major	The passive node in an HA setup did not work with the 2151 year time setting when synchronized with an incorrect NTP server.
146	NIOS-81971	Major	When the swap usage rates and the CUP usage rates were high, a NIOS restart needed to be prevented.
147	NIOS-81865	Major	Restoring an HA Grid did not retain IP address on a standalone Grid Manager and thus the restoration of licenses failed.
148	NIOS-81847	Major	Restarting the DNS service generated SERVFAIL responses in the log files for almost 15 minutes.
149	NIOS-81839	Major	A RADIUS authentication server group was configured and accounting was enabled, but no accounting messages were sent to the RADIUS server.
150	NIOS-81834	Major	Gaps in fastpath virtual DCA statistics in the Ptop file impacted reporting.
151	NIOS-81794	Major	When importing an IPv6 reverse zone, the “Duplicate object '0.0.0.0.0.0.0.0” error was displayed in the log files.
152	NIOS-81787	Major	TLSv1.2 only needed to be enabled as well as the same set of ciphers present in port 443 for the SAML port 8765.
153	NIOS-81784	Major	DNSTAP stopped working when the destination server restarted or rebooted.
154	NIOS-81730	Major	NIOS was vulnerable to CVE-2021-20322: DNS cache poisoning attack based on ICMP fragment needed packets replies.
155	NIOS-81693	Major	Using the `sort` command without the `count` parameter in reports truncated the results.
156	NIOS-81681	Major	After a NIOS upgrade, for one of the reporting members, the “Indexer reporting service is failed" message was displayed in the **Status** column of the **Reporting** > **Members** tab.
157	NIOS-81668	Major	The **Data Management** > **IPAM** > **Network** column did not display the accurate VLAN ID for many networks.
158	NIOS-81642	Major	All licenses for a Grid member had been revoked after changing the IPv6 gateway address.
159	NIOS-81641	Major	The DHCP license was missing despite the license being applied.
160	NIOS-81636	Major	The NIOS WAPI documentation regarding authentication methods contained an error.
161	NIOS-81634	Major	Scheduled tasks were not getting executed as scheduled if a Grid Master Candidate promotion took place.

#	ID	Severity	Summary
162	NIOS-81632	Major	The set debug_tools db_sync CLI command needed to work for HA pairs.
163	NIOS-81614	Major	When deleting network containers and their child objects, orphaned hosts also needed to be deleted.
164	NIOS-81610	Major	Some of the authoritative DNS servers returned SERVFAIL responses for queries to a zone.
165	NIOS-81596	Major	Certain GET calls without credentials were displayed in the Active WebUI Users dashboard and in the audit logs when a SAML authentication was triggered at the same time.
166	NIOS-81481	Major	In spite of enabling the Retain current Grid Master IP setting option, the IP address was being inherited from the database backup.
167	NIOS-81464	Major	Users in a read-only group were able to add and remove DNS records.
168	NIOS-81429	Major	Certain infoblox.log files in the support bundle contain multiple errors from the duplicate_ipd utility which is used to detect duplicate IP addresses.
169	NIOS-81385	Major	Logging into NIOS using SAML authentication failed for Microsoft Azure IDP.
170	NIOS-81384	Major	NIOS required a restart after certain NIOS licenses were overwritten.
171	NIOS-81309	Major	NIOS was vulnerable due to weak ciphers suites over port 8765.
172	NIOS-81243	Major	On platforms on which virtual DNS Cache Acceleration was enabled, packets with a specific transaction ID were dropped.
173	NIOS-81237	Major	The Grid Manager permissions were disregarded when enabling CLI permissions.
174	NIOS-81235	Major	The count of database objects in the Grid Master and the Grid Master Candidate was inconsistent.
175	NIOS-81225, NIOS-73862	Major	Creating a vDiscovery job that had a non-breaking space character in its name was possible.
176	NIOS-81213	Major	Under certain circumstances, the threat analytics service restarted.
177	NIOS-81192	Major	If the SNMP options for a Grid member were set to inherit, the engine ID displayed in Grid Manager was different from the engine ID captured by WAPI queries and the SNMP trap packet capture.
178	NIOS-81144	Major	The DTC search using the `status_member` WAPI field did not work as expected.
179	NIOS-81128	Major	The swap memory kept increasing on HA appliances thus resulting in a failover.
180	NIOS-81086	Major	DNS forwarding proxy did not override global forwarders that were configured in the DNS view.
181	NIOS-80981	Major	A discrepancy in the SOA serial number occurred on the DNS Traffic Control zone when DNS Traffic Control was configured.
182	NIOS-80961	Major	Threat Insight in the cloud integration client failed to synchronize data and the "Unable to request data: Authorization error" error message was displayed.
183	NIOS-80940	Major	OSPF adjacency between DNS servers constantly flapping between the INIT state and the two-way state and continuously generating SNMP traps.
184	NIOS-80938, NIOS-80937	Major	A red health status was displayed when DNS Traffic Control members in a consolidated health monitor group belonged to an LBDN pool in which there were other external members and those members failed the health check.

#	ID	Severity	Summary
185	NIOS-80929	Major	The Microsoft Azure vDiscovery documentation did not contain information about copying the secret value.
186	NIOS-80926	Major	Deletion of PTR records returned SERVFAIL messages when the DNS host also exists for the address.
187	NIOS-80891	Major	Networks assigned to a DHCP member were unable to obtain addresses until an HA failover.
188	NIOS-80874	Major	Under certain circumstances, the threat protection service did not start on a new appliance.
189	NIOS-80840	Major	The NIOS Release Notes needed to be updated about the change in behavior for the **Disable Concurrent Login** checkbox.
190	NIOS-80834	Major	The DNS Traffic Control screen displayed a warning status for members whose consolidated health monitor settings were configured with the **Full Health Communication** checkbox not selected.
191	NIOS-80826	Major	Users who were given CLI permissions were able to perform tasks that required additional authority.
192	NIOS-80812	Major	A check for duplicate resource records was required.
193	NIOS-80726	Major	If a user whose authentication was denied because of wrong credentials logged in again using SSO SAML authentication, then the user account was locked from AD/LDAP.
194	NIOS-80658	Major	The DHCP service kept failing and the “No DHCPv4 configuration files found. Rebuilding conf file dhcpd.conf” error message was displayed in the log files.
195	NIOS-80644	Major	When creating a delegated zone under a root zone, the Grid Manager displayed an error message.
196	NIOS-80640	Major	Two IB-FLEX Grid members repeatedly went offline on all NICs for no evident reason.
197	NIOS-80576	Major	Under certain circumstances, DND Traffic Control and EDNS0 did not work reliably.
198	NIOS-80569	Major	A file that was stored on the file distribution members was removed after swapping the Grid Master cluster and the Grid members.
199	NIOS-80561	Major	The Facility value for the idns_healthd message in the syslog file was incorrectly displayed as “mail”.
200	NIOS-80546	Major	The NIOS documentation did not contain information about ACS (Assertion Consumer Service) which is required to configure SAML authentication.
201	NIOS-80537	Major	Under certain circumstances, threat analytics failed. An attempt to restart the threat analytics service displayed the following error message: “Threat Analytics Service cannot be enabled on ncrns3.ncr.com because Analytics Moduleset version 20210620 configured is incompatible. Please update to the latest Analytics Moduleset version before enabling service."
202	NIOS-80533	Major	The WAPI documentation to save array to a variable needed to be enhanced.
203	NIOS-80526	Major	Under certain circumstances, caching servers did not take any traffic.
204	NIOS-80480	Major	Unable to start the DNS service and the “Generation of DNSSEC records for resource records of type 'NS' failed” error message was displayed.

#	ID	Severity	Summary
205	NIOS-80401	Major	Under certain circumstances, a spike in the disk usage was observed.
206	NIOS-80381	Major	Under certain circumstances, certificate validation failed for HTTPS health monitors.
207	NIOS-80364	Major	A passive node went offline and the “Fatal error during Infoblox startup” error message was displayed.
208	NIOS-80294	Major	Under certain circumstances, pool reset did not take place.
209	NIOS-80108	Major	Under certain circumstances, the swap utilization was above the threshold limit on reporting appliances.
210	NIOS-80107	Major	SNMPv3 user credentials were not replicate to Grid members when the password was changed.
211	NIOS-80104	Major	CSV import failed and the "Insertion aborted due to 'NoneType' object has no attribute 'key'" the message was displayed in the support bundle log files.
212	NIOS-79929	Major	The “error fetching dhcp_range:/ for reporting event” error message was displayed in the syslog of an IB-1420 Grid member even after a DHCP service restart.
213	NIOS-79813	Major	vDiscovery jobs did not work after a hotfix was applied.
214	NIOS-79775	Major	During a KSK rollover, a WAPI error was displayed for Unicode DNS zones that had a numeric value in the FQDN name.
215	NIOS-79725	Major	Option 81 support settings were not being inherited from the Grid to the member level.
216	NIOS-79704	Major	The database usage information in the Grid Manager and the CLI was mismatched.
217	NIOS-79696	Major	During a CSV export, the password for the CLI credentials was displayed explicitly.
218	NIOS-79694	Major	The RFC2317 prefix was ignored in the *Add Authoritative Zone Wizard*.
219	NIOS-79686	Major	The reset database command did not work in the emergency prompt and IB-FLEX appliances experienced database issues.
220	NIOS-79662	Major	Under certain circumstances, nothing was being logged in the syslog file.
221	NIOS-79628	Major	Certain devices took time to resolve queries assigned to a public IP address and related to a domain requested by a subscriber for whom proxy-all is enabled.
222	NIOS-79624	Major	Forwarder members were not validating DNSSEC when Grid members in the same Grid were sending queries to it.
223	NIOS-79606	Major	After a NIOS upgrade, the “All fields for transfer settings are required if the transfer type is not 'NONE'” error message was displayed in the Member DNS Properties screen.
224	NIOS-79604	Major	"iftab.IB-FLEX" needed to be a part of the support bundle.
225	NIOS-79602	Major	The NIOS documentation did not contain information about the Customer Experience Improvement Program.
226	NIOS-79579	Major	After a NIOS upgrade, an Azure vDiscovery job ran and then deleted all the records it had discovered in the past.
227	NIOS-79471	Major	Splunk REST API login failed after a reboot of the reporting search head until a Grid Manager login to reporting takes place.
228	NIOS-79464	Major	AWS vDiscovery from a Cloud Platform member with an instance profile failed.

#	ID	Severity	Summary
229	NIOS-79453	Major	After a NIOS upgrade, the Grid Master and the Grid Master Candidate were in constant restart and make_bind_conf core files were generated.
230	NIOS-79412	Major	The NIOS documentation did not contain information that the Drop LBDN matched DNS queries during full health update option returns SERVFAIL as a response and does not drop LBDN queries.
231	NIOS-79392	Major	The threat protection service did not start on IB-FLEX Grid members after a NIOS upgrade.
232	NIOS-79367	Major	Under certain circumstances, DNSSEC timeout issues occurred.
233	NIOS-79352	Major	The "failed to determine candidate master" warning messages were displayed in the syslog file.
234	NIOS-79314	Major	Under certain circumstances, the secondary node in a DHCP failover was stuck in a recover-wait state.
235	NIOS-79302	Major	Smart folders displayed duplicate results when networks were grouped with external attributes.
236	NIOS-79287	Major	In the Add IPv4 Network Wizard, clicking the Select Network button to add a network displayed a limited number of sites and did not display all the sites.
237	NIOS-79268	Major	The Network Users tab intermittently stopped populating Cisco ISE data.
238	NIOS-79263	Major	After a disaster recovery test, a large number of truncated DNS queries was generated.
239	NIOS-79222	Major	The Grid secondary server and the lead secondary server did not synchronize on time.
240	NIOS-79198	Major	NIOS was vulnerable to CVE-2021-25217.
241	NIOS-79163, NIOS-79162	Major	Unable to add a Grid member to a name server group.
242	NIOS-79086	Major	The status of LBDN, pool, and servers is displayed as None as soon as one of the nodes in an HA pair is down.
243	NIOS-79058	Major	Unable to download threat protection rules when the proxy server setting is configured with an IPv6 address in a dual-stack Grid Master.
244	NIOS-79032	Major	Under certain circumstances, virtual appliances did not join the Grid.
245	NIOS-79009	Major	Starting NIOS on a new IB-FLEX appliance on the RHOSP 16 platform displayed a fatal error.
246	NIOS-78586	Major	Unable to view secondary zone data and an internal error was displayed.
247	NIOS-78577	Major	Grid Manager displayed an incorrect status for LBDN when all servers associated with the pool had a green status.
248	NIOS-78571	Major	Under certain circumstances, a NIOS upgrade failed.
249	NIOS-78511	Major	Changing the name of an SOA MNAME record did not reflect in Grid Manager.
250	NIOS-78506	Major	The DNS client failed to detect a UDP DNS response when there was an RPZ rule match and virtual DCA was enabled.
251	NIOS-78486	Major	Under certain circumstances, Microsoft Azure vDiscovery jobs failed and an internal error message was displayed.
252	NIOS-78479	Major	The show firmware CLI command did not display the Ethernet firmware version.

#	ID	Severity	Summary
253	NIOS-78461	Major	After a NIOS upgrade, SAML authentication using Ping Identity returned an internal server error.
254	NIOS-78455	Major	The trap values in the NIOS documentation and specific SNMP OIDs in traps did not match.
255	NIOS-78433	Major	The NIOS documentation did not state that the DNS recursive cache size for the IB- 2215, IB-2225, and PT-2205 platforms can be configured from 2048 MB to 12288 MB.
256	NIOS-78397	Major	A NIOS on-prem host was unable to connect to the CSP portal and the corresponding entry was not displayed in the CSP portal.
257	NIOS-78374	Major	The passive node of an HA pair experienced intermittent flapping issues thus causing a service outage.
258	NIOS-78366	Major	A NIOS upgrade caused the MAC address to change on the MGMT interface.
259	NIOS-78343	Major	Under certain circumstances, HA failover failed.
260	NIOS-78277	Major	The "Rabbitmq service is broken" error message was displayed on multiple PT-1405 appliances.
261	NIOS-78244	Major	After restarting a host address, there was no prompt to restart the service and a manual service restart was required.
262	NIOS-78222	Major	Under certain circumstances, IPv4 option filters did not work.
263	NIOS-78218	Major	Unable to retrieve the name of an LBDN from a pattern (FQDN) using WAPI.
264	NIOS-78130	Major	The REST APIs did not accept upper-case IPv6 addresses upon listing IPv6 addresses.
265	NIOS-78072	Major	When using CSV import to delete network containers, performance issues occurred.
266	NIOS-77961	Major	The reporting service was interrupted because the license applied was not enough.
267	NIOS-77814	Major	The show log CLI command did not work as expected.
268	NIOS-77800	Major	IPv6-only members experienced network issues after a product restart.
269	NIOS-77694, NIOS-76659	Major	The dependency on /infoblox/reporting/bin/get_splunk_admin_password had to be removed.
270	NIOS-77657	Major	Attempting to remove a node from the Grid by using the set nogrid CLI command resulted in the "Fatal error during Infoblox startup" error message being displayed in the log files.
271	NIOS-77519	Major	Under certain circumstances, false positive alerts regarding power supply were generated.
272	NIOS-77412	Major	Under certain circumstances, frequent SNMP failures occurred and core files were generated.
273	NIOS-77291	Major	After a NIOS upgrade, intermittent DNS timeouts and long delays in query resolution occurred
274	NIOS-77283	Major	The recursing clients parameter displayed a high value in the dns_stats.txt file.
275	NIOS-77282	Major	Grid members went offline after an HA failover of the Grid Master.
276	NIOS-77243	Major	High CPU utilization was observed on CP-V2200 appliances running on Microsoft Azure.

#	ID	Severity	Summary
277	NIOS-77242	Major	Downloading the threat analytics moduleset failed and an email notification was generated.
278	NIOS-77102	Major	DNS acceleration usage was always at 0% when virtual DCA was enabled on IB-xxx5 appliances.
279	NIOS-76916	Major	Under certain circumstances, BGP packet flapping occurred unexpectedly and some appliances experienced high DNS acceleration usage which impacted recursive querying.
280	NIOS-76866	Major	Under certain circumstances, the DNS Traffic Control SNMP health check did not work.
281	NIOS-76812	Major	Under certain circumstances, NIOS experienced intermittent BFD flapping issues.
282	NIOS-76787	Major	A series of configuration changes to threat analytics and RPZs caused database integration issues on Grid members.
283	NIOS-76739	Major	After a global network outage, Grid replication did not work as expected.
284	NIOS-76718	Major	After a firmware upgrade, external DNS resolution was lost.
285	NIOS-76617	Major	The process manager failed to trigger daily reporting scripts.
286	NIOS-76605	Major	Using the global search displayed the “An Error has occurred. Contact technical support if the problem persists” error message.
287	NIOS-76549	Major	An unexpected HA failover occurred during a import of zone data.
288	NIOS-75596	Major	NIOS returned an incorrect value in the supportedMech field of the GSSTSIG TKEY response.
289	NIOS-74984	Major	NIOS was vulnerable to CVE-2020-10726, CVE-2020-10725, CVE-202010724, CVE-2020-10723, CVE-2020-10722, CVE-2019-14818, CVE2018-1059, and CVE-2015-1142857.
290	NIOS-74958	Major	Under certain circumstances, the passive node of a Grid Master lost communication intermittently.
291	NIOS-74955	Major	After enabling DNS scavenging, static records were deleted.
292	NIOS-74948	Major	Grid Master exceeded the system swap space usage at the critical threshold value.
293	NIOS-74708	Major	After applying a hotfix, certain reports did not display.
294	NIOS-74605	Major	Using the global search displayed the ““An Error has occurred. Contact technical support if the problem persists” error message.
295	NIOS-74525	Major	After deleting the Grid-wide RPZ license, the disk usage was 100% due to RabbitMQ logs.
296	NIOS-73518	Major	The **Cloud** > **Tenants** > *All Tenants* screen did not display and an error message was displayed instead.
297	NIOS-73492	Major	Unable to change a nameserver from stealth to non-stealth in a nameserver group.
298	NIOS-73351	Major	Key exchange algorithms for SSH needed to be restricted.
299	NIOS-73234	Major	A KSK rollover caused issues with LBDN records.
300	NIOS-70653	Major	Unable to update or get a network template using WAPI when assigned an extensible attribute with no value.
301	NIOS-66570	Major	Under certain circumstances, unable to upload a pool license and an error message was displayed.
302	NIOS-66242	Major	NIOS was vulnerable to CVE-2017-15710, CVE-2017-15715, CVE-20181283, CVE-2018-1301, CVE-2018-1302, CVE-2018-1303, CVE-20181312.
303	NIOS-65835	Major	Swap memory gradually increased and reached up to 92% after a NIOS upgrade.

#	ID	Severity	Summary
304	NIOS-63100	Major	The maximum cache size for IB-22x5 appliances needed to be increased.
305	NIOS-60352	Major	Refreshing the query monitoring view caused Grid Manager to display a blank screen.

#	ID	Severity	Summary
1	NIOS-89556	Minor	The authentication.c file contained a typo.
2	NIOS-88304	Minor	Unable to click the center part of the + icon to add nameservers under a forward zone.
3	NIOS-87692	Minor	The WAPI documentation contained incorrect information about search using regular expressions.
4	NIOS-87644	Minor	After a NIOS upgrade, discovery setting entries were getting duplicated.
5	NIOS-87303	Minor	The NIOS appliance on-prem host was unable to connect to the Cloud Services Portal.
6	NIOS-87279	Minor	Changing the discovery VPN server port configuration of probe nodes displayed the “Discovery probe unit did not respond” error message.
7	NIOS-87249	Minor	MAC-based CLI commands needed to be added to forward collection from certain devices.
8	NIOS-87069	Minor	The NIOS documentation did not state that SAN (Subject Alternative Name) was mandatory was Google Chrome and some other browsers.
9	NIOS-86856	Minor	A progress log based on a rough estimate of the object count needed to be added in the log files.
10	NIOS-85962	Minor	The CPU temperature value for an IB-4030 appliance was displayed incorrectly.
11	NIOS-85748	Minor	Under certain circumstances, directly connected routes were not pushed to IPAM for certain devices.
12	NIOS-85279	Minor	Certain Cisco devices did not return interface data, yet the Data Management > Devices > Interfaces tab displayed data for such devices.
13	NIOS-84795	Minor	IPv4 addresses with /32 mask for certain devices were discarded.
14	NIOS-84404	Minor	The discovery engine did not take the comma into consideration while matching the fingerprint output, thus resulting in an inaccurate output.
15	NIOS-84287	Minor	The NIOS documentation did not contain clear information about file distribution.
16	NIOS-84056	Minor	After a NIOS upgrade, SCP backup failed because of an authentication error.
17	NIOS-83997	Minor	The NIOS documentation did not contain information about the sgm_admin user account.
18	NIOS-83995	Minor	The NIOS Release Notes did not contain information about the change in behavior regarding DNS scavenging.
19	NIOS-83835	Minor	The **IPAM** > **Action** icon > *Show Device View* screen did not display the devices correctly.
20	NIOS-83476	Minor	The term "ATC" was displayed on Grid Manager.
21	NIOS-83352	Minor	A best practice of when configuring NTP servers using the FQDN, an external DNS name resolver that is reachable by NIOS appliance must also be configured was not documented.

#	ID	Severity	Summary
22	NIOS-83349	Minor	Grid Manager displayed “CONSOLIDATED MONITOR HEALTH SETTINGS” instead of “CONSOLIDATED HEALTH MONITOR SETTINGS”.
23	NIOS-83200	Minor	The debug logs were flooded with host name rewrite log entries.
24	NIOS-83186	Minor	The support bundle collected using automated traffic capture did not include debug logs (infoblox.log) and syslogs (var/log/messages).
25	NIOS-83170	Minor	Replacing a shared record group in a zone triggered an error if old and new groups had the same record.
26	NIOS-83163	Minor	The object name OID 3.1.1.1.2.3.0 was incorrectly documented.
27	NIOS-83162	Minor	The NIOS documentation contained incorrect information about network views.
28	NIOS-82885	Minor	A deduplication issue occurred when a network was added without enabling SNMP on a consolidator-probe setup.
29	NIOS-82772	Minor	Cisco APIC connectivity failed with a certificate verification error and as a result the ACI fabric remained undiscovered.
30	NIOS-82763	Minor	EPG, tenant, and bridge domain data was updated only for known IP addresses.
31	NIOS-82762	Minor	The discovery engine ignored the management IP address setting for NIOS devices.
32	NIOS-82752	Minor	Port control changes made in the Data Management > Devices > Interfaces screen took some time to reflect in Grid Manager.
33	NIOS-82523	Minor	The licensing information in the NIOS documentation was not up-to-date.
34	NIOS-82218	Minor	The Python stack trace was being displayed in all error messages.
35	NIOS-81626	Minor	Reading of any files via path traversal using WAPI needed to be fixed.
36	NIOS-81556	Minor	Unable to swap a member from hardware to virtual if the DSCP setting was overridden in the Member Properties editor.
37	NIOS-81212	Minor	Extensible attribute inheritance did not work for existing hosts.
38	NIOS-81184	Minor	A CLI command to switch DHCP class filter behavior needed to be implemented.
39	NOS-81176	Minor	The smart ping sweep feature of an IPAM network or network container did not override that same setting at the Grid level.
40	NIOS-80442	Minor	The NIOS documentation did not contain the correct format for the CSV export of the CNAME record.
41	NIOS-80433	Minor	The warning message that is displayed when the Enable Time Based Retention checkbox is selected needed to be modified.
42	NIOS-80075	Minor	The set membership CLI command contained a typo in its message.
43	NIOS-80074	Minor	Active Directory authentication failed for users whose login ID included German characters such as ä” , “ü”, “ö”, “ß” and so on.
44	NIOS-79197	Minor	Importing a zone failed and the “Duplicate object in the database” error message was displayed.
45	NIOS-78374	Minor	Under certain circumstances in an HA setup, intermittent flip flop of the core DNS service occurred.
46	NIOS-78288	Minor	The global search did not return matches when searching for DHCID records using the DNS name.
47	NIOS-77619	Minor	Clarifications on encryption algorithms were required to encrypt communications between Grid members and reporting members.

#	ID	Severity	Summary
48	NIOS-77484	Minor	An unexpected HA failover occurred when creating a smart folder with a conflict filter.
49	NIOS-77067	Minor	Under certain circumstances, even when no modification is made to the host record. an event was triggered and sent to the endpoint.
50	NIOS-76694	Minor	Access to NIOS version URLs needed to be restricted to authenticated users.
51	NIOS-73837	Minor	The `next_available_network` WAPI function ignored the parameters that were passed.
52	NIOS-71003	Minor	CSV export of all records using WAPI displayed multiple entries for the same host address.
53	NIOS-70056	Minor	All licenses for a Grid member had been revoked after changing the IPv6 gateway address.

Known General Issues

ID	Summary
NEPTUNESEC-31	After a Grid Master Candidate promotion, NIOS adds the deleted blacklisted domains once again to the blacklisted RPZ zone in the new Grid Master. If you select the **Configure Domain Level to block Tunneling** option, NIOS adds the new domains to the blacklisted RPZ zone based on the top-level domain that you configured.
NIOS-100381	Scheduling an hourly backup using the SCP server may not work as expected at all hours.
NIOS-100234	Using WAPI to perform a Grid backup with the SCP option does not work as expected and the backup file is of size 0 KB.
NIOS-100092	When a stub zone has authoritative sub-zones that have name servers assigned from a name server group, then if you delete the stub zone, system-generated name server (NS) records are also removed for the authoritative sub-zones resulting in resolution issues of the records inside the authoritative sub-zone.
NIOS-100066	Under rare circumstances, when an HA failover occurs in vNIOS for Azure appliances, virtual IP assignment fails and the "CannotAddSecondaryIpConfigsPendingCleanup" and "AuthorizationFailed" errors are displayed on the new active node.
NIOS-99995	During the distribution phase of an upgrade, if the distribution to a Grid member is paused and resumed before the distribution to the node is complete, the distribution to the node may not be completed properly, even though the Grid Manager may indicate that the distribution has completed successfully. This may result in problems such as an inability to SSH to the Grid member. **Workaround:** Remove the node from the Grid, downgrade it and re-join to the Grid.

ID	Summary
NIOS-99089	When both port redundancy and a VLAN tag are configured, then DSCP (ToS) is not set on outgoing packets.
NIOS-96885	The NIOS upgrade is successful even if an invalid certificate is present in the Grid. **Workaround:** Disable strict checks for certificates using the CLI or remove the invalid certificates from the system.
NIOS-95199	On a Trinzic X6 series appliance that is a Grid member, the Grid member must leave the Grid Master in order to reshape, otherwise the reshape fails. **Workaround:** Run the `reset all licenses` CLI command on the Grid member, reshape, and join the Grid Master once again.
NIOS-95115	If the Dual Engine DNS license is present in your Grid in the deleted or expired state (can be validated by running the `show license` CLI command on the node), contact Infoblox Support to have it removed. The NIOS upgrade fails if the license is not deleted.
NIOS-94739	There may be a drop in QPS in the vNIOS for AWS r6i instances for the X5 series of appliances.
NIOS-94554	The `show upgrade_history` CLI command does not capture and display the downgrade failure logs.
NIOS-94171	The QPS value drops to zero if you run both UDP and TCP at the same time.
NIOS-93818	If you run the set license CLI command to install the Reporting subscription license on a standalone system, the license is installed even though the Reporting subscription license cannot be installed on a standalone system.
NIOS-93142	Under certain circumstances, you may be unable to add values to the Site_ID external attribute and the Site_ID values that are already present may take a long time to load.
NIOS-92747	Enabling certificate-based authentication using WAPI commands throws an error and does not work.
NIOS-92181	If you add an invalid license using the `set license` CLI command, the "License is installed" message is displayed even though the license is not applied.
NIOS-90291	There may be a drop in performance when DHCP lease expiry is in process for the Trinzic X6 series of appliances.
NIOS-89651	DNS Traffic Control objects that were disabled on an HA node are automatically enabled after a Grid Master Candidate promotion.
NIOS-89619	The maximum allowed blocklist string length in NIOS does not match the maximum allowed blocklist string length in the Harmony database.
NIOS-89599	When upgrading NIOS from version 8.4.6 to version 9.0.0, the Upload in progress bar in the **Grid** > **Upgrade** screen shows an abnormally high percentage number.
NIOS-89243	A vNIOS for Hyper-V deployment takes a long time to boot and sometimes hangs during the ""KASLR disabled: nokaslr" step of the deployment process.

ID	Summary
NIOS-89039	Under certain circumstances, Infoblox virtual appliances fail to boot after the host system or host computer has been restarted. Workaround: Follow the guidelines below to avoid the problem: An unclean host shutdown without PowerSafe storage causes such problems. This issue does not occur in hardware appliances that have NVRAM (powersafe) -backed RAID controllers. Infoblox VMs handle such issues better if the host system or host computer supports synchronous PowerSafe input/output.
NIOS-88982	When the number of subscribers in subscriber cache reaches the maximum limit, the “LRU 0 empty after get" message is logged for each query.
NIOS-88479	DNS Traffic Control objects that were enabled after an upgrade from NIOS 8.6.2 will be automatically disabled after a Grid revert operation. Database entries for the disabled objects will be present only for Grid Master and not for the Grid members. **Workaround:** Follow the steps below to avoid the problem: Enable the disabled DNS Traffic Control objects. After enabling, disabled objects of the Grid member will be retained in the Grid Master. To remove the stale database entries of the disabled objects, run the touch /infoblox/var/cleanup_dtc_disabled_objects command in the root session of Grid Master.
NIOS-88447	When you shut down a NIOS VM running on Oracle Cloud Infrastructure, even though NIOS shuts down, the Oracle Cloud Infrastructure console displays the VM state as RUNNING. To avoid this, Infoblox recommends that you shut down the NIOS VM from the Oracle Cloud Infrastructure console instead of using the NIOS CLI or Grid Manager.
NIOS-87394	Under certain circumstances, the `snmpwalk` CLI command does not work as expected on DNS services.
NIOS-87391	A NIOS deployment on a Hyper-V platform takes a long time to start.
NIOS-86966	Running the `snmpwalk` command displays an SNMP timeout error.
NIOS-86772	While enabling certificate-based authentication using WAPI commands, a 401 Authorization error and an OpenSSL read error occur.
NIOS-86596	A major drop in DNS performance is observed on IB-1415 appliances.
NIOS-86602	A major drop in recursion numbers is observed on IB-v1425 appliances on the GCP platform.
NIOS-86558	Queries per second drops occur on large deployment IB-FLEX appliances.
NIOS-85912	The cipher list order has changed in NIOS 9.0.0.
NIOS-85869	The NIOS container image needs to be installed at build time.

ID	Summary
NIOS-84938	
NIOS-85828	After upgrading to NIOS 9.0.0, a spike in memory consumption and CPU utilization occurred.
NIOS-85471	If you upgrade to NIOS 8.6.2 from an earlier version and if the ZVELO update fails, the SNMP trap and the member status take 3 days to be updated.
NIOS-85372	The Open in Search option does not work as expected for charts in the Splunk Dashboard Studio.
NIOS-85219	The `show firmware` CLI command does not list the SAS3808 controller.
NIOS-85082	On a NIOS IB-V5005 appliance without extra storage, if you manually try to install a license, the following error message is displayed: “You must provision the reporting disk before adding a license to the Reporting server". If you are installing a license on a VM that has the cloud-init parameter installed, ensure that you have attached extra storage for the reporting disk.
NIOS-84350	HSM Thales does not work in NIOS 9.0.0.
NIOS-84177, NIOS-82089, NIOS-78228	Queries per second drops occur in IB-FLEX appliances.
NIOS-84168	After a NIOS upgrade, HA replication takes place using the IPv4 address instead of the IPv6 address. This issue does not occur on a standalone Grid.
NIOS-83949	Under a rare circumstance packet loss may take place during file distribution and distribution may get stuck. This occurs during a network glitch for NIOS versions 8.6.1 or earlier. **Workaround:** Pause and resume the distribution or reboot the appliance.
NIOS-82251	Performance degradation occurs across DNS and DHCP features.
NIOS-82089	Queries per second drops occur on systems on which Advanced DNS Protection is installed.
NIOS-81393	If you enable and then disable auto-consolidated monitors, the log files generate the “transfer rabbit messages failed” message several times.
NIOS-81058	A soft reboot takes a long time on a vNIOS for KVM-based OpenStack appliance.
NIOS-80584	The NIOS 9.0.0 image size is bigger than expected.
NIOS-80176	Under rare circumstances, performance degradation occurred for the IPAM map and IPAM list on the IPAM tab.
NIOS-79718	If you want to view options such as View Configuration, View Debug Log, and other options that involve viewing configuration or log files in a new browser window or tab, a session logout takes place. You must modify your browser settings to open links in a new window or tab to avoid the session logout.

ID	Summary
NIOS-78421	If you configure the HTTP proxy field frequently, the value of the field may not be updated by the blox.noa environment variable even though the params.json file contains the correct value. **Workaround:** Scrape the containers and restart csp_control manually for the value of the HTTP proxy field to be updated.
NIOS-78335	If you have configured SAML after a Grid Master Candidate promotion, you have to manually get into the appliance to make certain changes on the configurations to make it work. If you have configured SAML prior to a Grid Master Candidate promotion, you have to change the IDP settings to use a new Grid Master IP address or FQDN for SAML to work.
NIOS-78228	Use IB-FLEX small appliance (10 vCPUs and 20 GB memory) only for small recursion (with acceleration). Authoritative DNS zones are not supported on this configuration.
NIOS-78177	Under rare circumstances, the reporting service may fail on a newly added Grid member and the "SSL certificate generation failed" message is displayed in the Infoblox.log file. **Workaround:** Contact Infoblox Support.
NIOS-77681	DHCP fingerprint leases whose option IDs were split and added or created to new fingerprint records, continue to point to the older fingerprint names after a NIOS upgrade.
NIOS-77617, NIOS-77616	Upgrading to Unbound version 1.10.1 may result in a performance impact.
NIOS-77576	DDNS updates bypass the "Prevent the following ACLs or ACEs from updating the last queried timestamp" ACL, and selecting the **Update DNS on DHCP Lease Renewal** checkbox may potentially interfere with DNS scavenging.
NIOS-75505	Under a rare circumstance, after a NIOS upgrade, Grid Manager may not launch. **Workaround:** Do a product restart or restart NIOS from the CLI.
NIOS-75238, NIOS-75237	Major drops in DNS features occur on Trinzic (IB) and cloud platform (CP) appliances on the GCP platform.
NIOS-73838	On the Cloud Services Portal, for both the nodes of an HA pair, make sure that the same services are enabled (example, DNS Forwarding Proxy). Failure to do so disables forwarding to BloxOne Threat Defense and may result in other unexpected behavior on failover.
NIOS-73715	After a NIOS upgrade, fastpath does not restart if it failed prior to the upgrade. **Workaround:** Restart NIOS before upgrading to later releases.
NIOS-73693	Under a rare circumstance, communication between the reporting cluster master and cluster peer fails and the "Search Factor is Not Met" and

ID	Summary
	"Replication Factor is Not Met" messages are displayed on the **Dashboards** > **Reporting Clustering Status** tab. **Workaround:** Restart the reporting service.
NIOS-73656	If you enable the threat context local cache, and then revert or upgrade the Grid to a release that does not support threat context local cache, the indexed CSP cache entries will still occupy disk space, even though they are not searchable in the upgraded or reverted release.
NIOS-73650	For threat indicator caching to work on a Grid, the Grid must have at least one user with can delete permission set up on the Grid. If you reset the reporting data on any reporting member or replace the reporting hardware before or after enabling threat indicator caching, you must log in to the Grid as the user with can delete permission so that the user details are pushed to the Splunk database for threat indicator caching to work.
NIOS-73649	If the reporting search head reboots or shuts down when a replication is in progress, all threat indicator indexes are removed, and therefore, all entries in the threat details report and the syslog threat context show as unknown. To fix this issue, disable and enable the threat indicator caching feature.
NIOS-73648	For generating RPZ hits in syslog, you must configure RPZ feed zones before or after enabling the threat indicator caching feature for the downloading of threat category information to start.
NIOS-73647	If you reset the reporting data on any reporting members or replace the reporting hardware, then for the downloading and indexing of threat indicator data to start on new members, perform the following: If the threat indicator feature is already enabled, disable the feature and enable it again. Log in to the Grid as a user with the delete permission so that the user details are pushed to the Splunk database.
NIOS-73088	After a NIOS upgrade, sometimes certain devices are displayed as duplicates on the Devices tab.
NIOS-70953	After enabling DNS Cache Acceleration, Grid Manager interfaces are not reachable on IBFLEX instances deployed on VMware ESXi 6.5.0 with SR-IOV enabled.
NIOS-64802	On the **Data Management** > **DNS** > **Zones** > **Records** tab, the Record Source column for a host record may change from Static to Dynamic if you add the host record with an existing name that is already added by DDNS.
NIOS-61565	Object Change Tracking: In situations that involve a large database, performing a full synchronization from the Grid Master Candidate while the previous file is still being synchronized to the Grid Master might cause the deletion of the original synchronization file.

ID	Summary
	Workaround: Do not perform a full synchronization from the Grid Master Candidate until the file from the previous synchronization is fully synchronized to the Grid Master.
NIOS-61562	Reporting and Analytics: The Destination Path is an optional field in a single-site cluster, which might cause a second reporting indexer to go offline and not being upgraded. **Workaround:** Ensure that you enter a value for the **Destination Path** field.
NIOS-60352	Under certain circumstances, the **Data Management** > **DNS** > **Query Monitoring** tab displays a blank screen if you navigate and toggle between the next and previous pages.
N/A	Infoblox has upgraded the software for our user community (community.infoblox.com), 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 *Community Dashboard* widget is inconsistent. The *Community Dashboard* widget will subsequently be removed in the next NIOS maintenance release.
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.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com