Infoblox

RELEASE NOTES

NIOS 8.6.2

Table of Contents

Introduction

Infoblox NIOS™ 8.6.x software, coupled with Infoblox appliance platforms, enables customers to deploy large, robust, manageable and cost-effective Infoblox Grids. This next-generation solution enables distributed delivery of core network services—including DNS, DHCP, IPAM, TFTP, and FTP—with the nonstop availability and real-time service management required for today's 24x7 advanced IP networks and applications.

Please note the following:

NIOS 8.6.x is not supported on the following appliances which are past their End of Life (EOL) dates:

IB-250, IB-250-A, IB-500, IB-550, IB-550-A, IB-1000, IB-1050, IB-1050-A, IB-1550, IB-1550-A, IB-1552, IB-1552-A, IB-1852-A, IB-2000, IB-2000-A, IB-VM-250, IB-VM-550, IB-VM-1050, IB-VM-1550, IB-VM-1850, IB-VM-2000, PT-1400, PT-2200, ND-800, ND-1400, ND-2200, TE-810, TE-820, TE-1410, TE-1420, TE-2210, TE-2220, TR-800, TR-1400, TR-2200, IB-4030, ND-V800, ND-V1400, ND-V2200, TE-V810, TE-V820, TE-V1410, TE-V1420, TE-V2210, TE-V2220, TR-V2200, TR-V800, TR-V1400, TR-2000, and TR-2000-A series appliances.

NIOS 8.6.x is not supported on the following appliances which will End Of Life (EOL) by the end of CY21:IB-4010, IB-4020, TE-100, TE-V100, IB-V4010, IB-V4020, TR-4000, IB-4030-1GE

Because these appliances are not supported, Infoblox recommends that you do not upgrade to NIOS 8.6.x on these appliances.

Supported Platforms

Infoblox NIOS 8.6.x is supported on the following platforms:

- Infoblox Advanced Appliances: PT-1405, PT-2205, PT-2205-10GE
- Network Insight Appliances: ND-805, ND-1405, ND-2205, ND-4005
- Network Insight Virtual Appliances: ND-V805, ND-V1405, ND-V2205, ND-V4005
- Trinzic Appliances: TE-815, TE-825, TE-1415, TE-1425, TE-2215, TE-2225, TE-4015, TE-4025
- Trinzic Virtual Appliances: IB-V815, IB-V825, IB-V1415, IB-V1425, IB-V2215, IB-V2225, IB-V4015, IB-V4025, IB-FLEX
- Trinzic Reporting Appliances: TR-805, TR-1405, TR-2205, TR-4005
- Trinzic Reporting Virtual Appliances: IB-V805, IB-V1405, IB-V2205, IB-V4005, IB-V5005
- Cloud Platform Appliances: CP-V805, CP-V1405, CP-V2205
- Infoblox Virtual NIOS Appliances for AWS, Azure, and GCP: IB-V825, IB-V1425, IB-V2225, CP-V805, CP-V1405, CP-V2205

NOTE: TE appliances are also known as the IB appliances.

The following appliances are still supported in NIOS 8.6.x. However, they are not available for purchase from Infoblox: PT-4000-1G, PT-4000-10GE, IB-4030-10GE

The following appliances are supported only when you upgrade to NIOS 8.6.x from an earlier version. They are not supported for a new NIOS 8.6.*x* installation: CP-V800, CP-V1400, CP-V2200

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.

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 7.0, 6.7, 6.5.x, 6.0.x installed, and then configure it as a virtual appliance. Note that VMware ESX/ESXi 7.0 is not supported on NIOS versions earlier than 8.5.3.

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 Wallaby RHOSP 16.0 (over Ubuntu), Victoria (over Ubuntu) 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

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.

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. Currently, only CP-V2205 is supported on Oracle Cloud Infrastructure. This appliance runs only as a Grid member; you cannot deploy it as a Grid Master or Grid Master Candidate. For more information, see the *Infoblox Installation Guide vNIOS for Oracle Cloud Infrastructure*.

vNIOS 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.

The following table lists the required memory, CPU, and disk allocation for each supported Infoblox virtual appliance model:

NIOS Virtual Appliances	Primary Disk (GB)	# of CPU Cores	Memory Allocation (GB)	Recommended CPU Per Core Clock Rate	NIOS for VMware	NIOS for MS Hyper-V *	NIOS for KVM	NIOS for Azure*, AWS, GCP	NIOS for Nutanix	NIOS for Red Hat Open Shift	Supported as Grid Master and Grid Master Candidate
IB-V815 **	250	2	16	1100 MHz	✓	✓	✓[1]	×	✓	×	Yes
IB-V825 **	250	2	16	1600 MHz	✓	✓	✓[1]	✓	✓	×	Yes
IB-V1415 **	250	4	32	1200 MHz	✓	✓	✓[1]	×	✓	×	Yes
IB-V1425 **	250	4	32	1800 MHz	✓	✓	✓[1]	✓	✓	×	Yes
IB-V2215 **	250	8	64	2100 MHz	✓	✓	✓[1]	×	✓	×	Yes
IB-V2225 **	250	8	64	2100 MHz	✓	✓	✓[1]	✓	✓	✓	Yes
IB-V4015 **	250	14	128	2400 MHz	✓	✓	✓[1]	✓[2]	×	✓	Yes
IB-V4025 **	250	16	128	2400 MHz	✓	✓	✓[1]	✓[2]	×	×	Yes

Network Insight Virtual Appliances	Overall Disk (GB)	# of CPU Cores	Memory Allocation (GB)	Recommended CPU Per Core Clock Rate	NIOS for VMware	NIOS for MS Hyper-V *	NIOS for KVM	NIOS for AWS, Azure, GCP	NIOS for Nutanix	Supported as Grid Master and Grid Master Candidate
ND-V805 **	500	2	32	2700 MHz	✓	✓	✓[1]	×	×	No

ND-V1405 **	500	4	32	3600 MHz	✓	✓	✓[1]	×	✓	No
ND-V2205 **	500	8	64	2100 MHz	✓	✓	✓	×	×	No
ND-V4005 **	500	14	128	2400 MHz	✓	✓	✓	×	×	No

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 CPU Cores	Memory Allocation (GB)	Recommended CPU Per Core Clock Rate	NIOS for VMware	NIOS for MS Hyper-V *	NIOS for KVM	NIOS for AWS, Azure	NIOS for Nutanix	Supported as Grid Master and Grid Master Candidate
IB-V805 **	250	2	32	2700 MHz	✓	✓	✓[1]	×	×	No
IB-V1405 **	250	4	32	3600 MHz	✓	✓	✓[1]	×	×	No
IB-V2205 **	250	8	64	2100 MHz	✓	✓	✓[1]	×	×	No
IB-V4005	250 (+ 1500 GB reporting storage)	14	128	2400 MHz	✓	×	×	×	×	No
IB-V5005	User defined reporting storage	User defined	User defined	N/A	✓	✓	✓	✓	✓	No

Cloud Platform Appliances	Overall Disk (GB)	# of CPU Cores	Memory Allocation (GB)	Recommended CPU Per Core Clock Rate	NIOS for VMware	NIOS for MS Hyper-V *	NIOS for KVM	NIOS for AWS, Azure, GCP	NIOS for Nutanix	NIOS for Oracle Cloud Infrastructure	Supported as Grid Master and Grid Master Candidate
CP-V805	250	2	16	2000 MHz	✓	✓	✓	✓	✓	×	No
CP-V1405	250	4	32	6000 MHz	✓	✓	✓	✓	✓	×	No
CP-V2205	250	8	64	12000 MHz	✓	✓	✓	✓	✓	✓	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.

** 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. vNIOS for Azure and vNIOS for GCP are supported on the IB-V4015 and IB-V4025 appliances running NIOS 8.6.2.

[1] NIOS for KVM is supported in the following environments: Red Hat OpenStack and Ubuntu. Note that only IB-V1405 as a reporting server has been qualified for Red Hat OpenStack.

Appliance Specification 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 CPU 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

NOTE:

For the IB-V1425, IB-V4015, and IB-V4025 appliances, the # of CPU Cores column indicates the number of virtual CPUs assuming that hyperthreading is enabled.

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

New Features

This section lists new features in the 8.6.*x* releases.

NIOS 8.6.2

Enabling and Disabling DNS Traffic Control Objects (RFE-7088)

NIOS 8.6.2 introduces the *Enable Traffic Management Objects* and the *Disable Traffic Management Objects* screens using which you can enable or disable individual DNS Traffic Control objects. You can also disable the health monitoring of a particular object to stop performing health checks. You can access the new screens from the **Traffic Control** panel on the **Data Management** > **DNS** > **Traffic Control** tab. For more information about enabling and disabling DNS Traffic Control objects, see the “Managing DNS Traffic Control Objects” topic in the NIOS 8.6 online documentation.

Multi-Master DNS Failover for DDNS (RFE-5514)

In NIOS 8.6.2, 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.

Configuring Microsoft Servers and Delegated Name Servers (RFE-10168)

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. You also cannot enable DNS synchronization for Microsoft servers in NIOS if delegated name servers are configured on them.

Support for Upgraded Splunk Version 8.2.4

NIOS 8.6.2 supports Splunk version 8.2.4.

vNIOS for Azure and vNIOS for AWS Support in IB-V5005 (RFE-7962)

IB-V5005 support is now extended to vNIOS for Azure and vNIOS for AWS. For detailed information see the *Infoblox Installation Guide for vNIOS for AWS* and the *Installation Guide for vNIOS for Microsoft Azure*.

vNIOS for GCP Support in IB-V4015 and IB-V4025 (RFE-11349)

IB-V4015 and IB-V4025 now support vNIOS for GCP. For detailed information see the *Infoblox Installation Guide for vNIOS for GCP*.

DHCP Support on vNIOS for GCP (RFE-9945)

vNIOS for GCP instances running on NIOS 8.6.2 offer DHCP services for on-premise networks. For more information see the *Infoblox Installation Guide for vNIOS for GCP*.

vNIOS for Nutanix 6.5.1.6 (RFE-11997)

NIOS 8.6.2 supports the deployment of vNIOS on Nutanix 6.5.1.6 long-term supported (LTS) release. For more details, see the *Infoblox Installation Guide vNIOS for Nutanix*.

Enabling and Disabling BFD Internal DNS Monitoring (SPTYRFE-49)

NIOS 8.6.2 introduces a new checkbox called **BFD Internal DNS Monitoring** in the *Grid Member Properties* editor > **Anycast** tab. Selecting this checkbox enables the internal DNS monitor to send and receive DNS responses and to retract the OSPF or BGP route if it does not receive a DNS response.

You can enable or disable the **BFD Internal DNS Monitoring** checkbox only if you select the **Enable BFD** checkbox. When you enable the **BFD Internal DNS Monitoring** checkbox, you have the option to toggle between enabling or disabling the internal DNS monitor. When you select this checkbox, Infoblox recommends that you also select the **Enable DNS Health Check** checkbox in the *Grid Properties Editor* or the *Member Properties Editor*. The **BFD Internal DNS Monitoring** checkbox is enabled by default.

For more information see the “About BFD” topic in the NIOS 8.6 online documentation.

Support for Cisco ISE Integration Through Outbound Endpoint

NIOS 8.6.2 supports Cisco ISE versions 3.0 and 3.1. Infoblox recommends that you configure Cisco ISE 3.0 and 3.1 using the **Outbound Endpoint** tab. Cisco ISE version 3.1 (pxGrid 2.0) is supported only through the Cisco outbound endpoint. For more information see the “Configuring Outbound Endpoints” topic in the NIOS 8.6 online documentation.

Enforcing the Global Proxy List

In NIOS 8.6.2, if you want to proxy the traffic through the MSP (Multi-Services Proxy) server and have categorized the queried domains in the incoming traffic to the global proxy list, then the query resolves to an MSP virtual IP address and NIOS generates a "synthetic resolution”. For more information, see the “Scaling Subscriber Sites” topic in the NIOS 8.6 online documentation.

NIOS 8.6.1

New DNSKEY Algorithm (RFE-6068 and RFE-9845)

You can now add the ECDSAP/SHA-256 and ECDSAP/SHA-384 cryptographic algorithms which the Grid Master can use when it generates the Key-Signing Key Rollover (KSK) and Zone-Signing Key Rollover (ZSK).

Extensible Attribute -based Topology Rulesets (RFE-9107 and RFE-11133)

You can now specify IPAM objects types, network containers, networks, ranges, and hosts and their external attribute (EA) values in the **Extensible Attributes Source Types for Topology Rules** field to be used as source types when defining DNS Traffic Control topology rules. For more information, see the “DNS Traffic Control Properties” topic in the NIOS 8.6 online documentation.

vNIOS Support for Microsoft Azure Stack Hub (RFE-8303)

You can now deploy the NIOS virtual appliance on Microsoft Azure Stack Hub. vNIOS for Microsoft Azure Stack Hub which is a hybrid cloud platform that enables a vNIOS appliance to deliver Azure services in an on-prem environment. You can deploy vNIOS for Azure Stack Hub instances from the Azure CLI or the Azure Stack Hub portal. For more information, see the *vNIOS Infoblox Installation Guide for Microsoft Azure* at docs.infoblox.com

Grid Master Candidate to Display the Health Status of Servers/Pools/LBDNs in API Responses (RFE-9893)

The Grid Master Candidate now provides the health status of DNS Traffic Control objects such as servers, pools, and LBDNs through WAPI requests.

Regenerating the Anycast Password (RFE-11117)

This release of NIOS introduces the `set regenerate_anycast_password` command that regenerates the anycast service password. The regenerated 8-character alphanumeric password is saved to the NIOS database and is used across all anycast configuration files (ospf.conf/bgp.conf/bfd.conf) for the following CLI commands: `show ospf`, `show bgp`, `show ipv6_ospf`, `show ipv6_bgp`, `show bfd`

This command is a maintenance mode command and has no arguments. Only superusers can execute this command. The password and value of the enable password in the output of the configuration file commands such as `show bfd` are encrypted when you run the command. For more information, see the "set regenerate_anycast_password" topic in the NIOS 8.6 online documentation.

Viewing Lightweight Access Point Details in Network Insight (RFE-9556)

You can now view the discovered lightweight access points on the **Data Management** > **Devices** page. The table displays the following information about the discovered lightweight access points: their name, IP address, device type, model, vendor, and device version. You can also view the discovery statuses and other information in the **Discovery Status** table (**Data Management** > **Devices** > **Discovery Status**).

Displaying the Lead Secondary Column in Name Server Group (RFE-2804)

You can now determine which member is configured as a lead secondary by adding in a column to the **Authoritative Zone** > **Name Servers** tab.

Support for creation_time for Host Records (RFE-8509)

You now have the option of adding, updating, listing the creation timestamp value of DNS and non-DNS host records using Grid Manager and WAPI.

Support for IB-V4015 on Red Hat OpenShift (RFE-11545)

Red Hat OpenShift is now supported on IB-V4015 virtual appliance. For more information, see the *Infoblox Installation Guide vNIOS for Red Hat OpenShift* at https://docs.infoblox.com.

New Port Placements for the Infoblox 2205 and Infoblox 4005 Series Appliances

The front panels of the Infoblox 2205 Series and the Infoblox 4005 Series have been modified to have slots for the four ports (LAN2, HA, LAN1, MGMT) at the right. However, the Infoblox 2205 and Infoblox 4005 Series models that have the ports located at the center are also being shipped. There is no difference in software functionality between the models that have ports on the right and those that have ports in the center. Both the models will support NIOS versions prior to 8.5.4 and earlier.

For a visual representation of these models, see the *Infoblox Installation Guide for 2205 Series Appliances* and the *Infoblox Installation Guide for 4005 Series Appliances* documentation at https://docs.infoblox.com

Synchronizing the System Time with the NTP Server Time (SPTYRFE-205)

This release of NIOS introduces the **synctime** command to synchronize the system time with the time of an external NTP server or a Grid Manager. When you run the synctime command, NIOS checks to verify whether there are already configured NTP servers present. If they are present, it displays the list of NTP servers and you have to choose from the list. If there are no NTP servers that are configured, you must specify the IP address of the NTP server or Grid Manager with which you want to synchronize the system time.

NIOS 8.6.0

ACL Support for the Last Queried Time in DNS Scavenging (RFE-7933)

You can now create an ACL or ACE for the Last Queried Time field in DNS scavenging and thus prevent a specified set of ACLs or ACEs from updating the last queried timestamp. A new GUI field called Prevent the following ACLs or ACEs from updating the last queried timestamp in the *Grid DNS Properties* > **DNS Scavenging** > Basic tab has been introduced. The set of ACL or ACEs can include IPv4 and IPv6 addresses and networks. For more information, see the "DNS Record Scavenging" topic in the NIOS 8.6 online documentation.

New DNS Traffic Control Load Balancing Method to Add Persistence (RFE-6827)

This release of NIOS introduces a new load balancing method called Source IP Hash to configure DNS Traffic Control pools. In this method, requests are distributed based on the hash value of an IP address from an incoming query and the health status of the pool or server. Here, clients have their own pool or server and are always associated with the same pool or server for the same query as long as the pool or server is green. If the health status of the pool or server turns red, NIOS switches the clients to the working pool or server and switches back when the health restores to green. For more information about the source IP hash load balancing method, see the "Load Balancing Methods for DNS Traffic Control" topic in the NIOS 8.6 online documentation.

New DNS Responses When No DNS Traffic Control Responses are Available (RFE-10212)

You now have the option to allow NIOS to either drop LBDN queries, or return DNS responses, or not return DNS responses when DNS Traffic Control responses are not available. Two new options have been introduced in the **Data Management** > **DNS** > *Grid DNS Properties*/*Member DNS Properties* > **Traffic Control** tab:

- Drop LBDN matched DNS queries during full health update: This option drops all LBDN queries when the DNS service is waiting to receive a full health status update.
- No specific behavior: This option does not return DNS responses when DNS Traffic Control responses are not available.

These options are in addition to the existing Return DNS response if there are no DNS Traffic Control responses available option which is selected by default. For more information, see the "Configuring DNS Traffic Control Properties" topic in the NIOS 8.6 online documentation.

Consolidated Health Checking for DNS Traffic Control Grid Members (RFE-9427)

You can now choose the Grid members that must monitor health and share the health status. You can also select with which other members the health status is to be shared. You can do this by enabling or disabling the new **Full Health Communication** checkbox on the **Data Management** > **DNS** > **Traffic Control** > **Health Monitors** > **Advanced** tab. For more information, see the "Configuring DTC Monitors" topic in the NIOS 8.6 online documentation.

Notification Rule Enhancements

NIOS now includes the Delete operation type in the Outbound notification rules. The Delete operation type has been included for the DB Change DNS Record, DB Change DNS Zone, and Object Change Discovery Data event types. For more information, see the “Configuring Notification Rules” topic in the NIOS 8.6 online documentation.

Infoblox BloxConnect

The Infoblox Customer Experience Improvement Program is now called Infoblox BloxConnect. This screen appears when you first log in to Grid Manager. The Infoblox Customer Experience Improvement Program check box used to configure BloxConnect, has now been renamed to BloxConnect Data Collection and Opt-Out Notice. For information about configuring BloxConnect, see the “Setting Login Options” topic in the NIOS 8.6 online documentation.

IP Address in DHCP address conflict notification (RFE-5170)

NIOS now displays the conflicting IP address along with the conflict category when an email notification is sent in case of an IPAM IP address conflict.

The content of the IB-TRAP-MIB::ibTrapDesc.0 SNMP trap is updated to STRING: DHCP address conflicts with an existing host address. [IP address].

New Cluster Logout Event in the Syslog File (RFE-9840)

The syslog file now contains a cluster logout message to easily identify between network-related disconnects and distribution-related logouts in real time. The message is in the following format:

```
<date:time> daemon infoblox.localdomain INFOBLOX-Grid[]: notice Cluster logout for
node <node_name>, for node clean restart.
```

WAPI Performance Optimization (RFE-9986)

The performance of the WAPI GET method has been optimized for SRV, CNAME, and DNAME records.

Grid Backup Details in the Audit Log (RFE-9614)

The audit log file now logs information about who started the database backup and where the database backup file is stored. For more information, see the “Audit Log” topic in the NIOS 8.6 online documentation.

New CLI Command to Set DNS and Anycast Start and Restart (RFE-10176)

This release of NIOS introduces the following commands:

- `set restart_anycast_with_dns_restart`: Sets DNS and anycast start and restart sequences. This command brings down the anycast service during the DNS restart or stops and redirects the traffic on the IP address of anycast to another site. You can use this command only on Grid Master.
- `show restart_anycast_with_dns_restart`: Displays the status of the set `restart_anycast_with_dns_restart` command.

For more information about these commands, see the “set restart_anycast_with_dns_restart” and “show restart_anycast_with_dns_restart” topics in the NIOS 8.6 online documentation.

Hybrid HA Support

In NIOS 8.6, an HA setup can comprise a physical appliance and a virtual appliance. This setup is called a hybrid HA setup. For information about hybrid HA and its limitations, see the “About HA Pairs” topic in the NIOS 8.6 online documentation.

Single Network Interface of vNIOS for GCP (RFE-9995 and RFE-9807)

This release of NIOS introduces an option to deploy vNIOS for GCP as a single network interface instance using VPC (Virtual Private Cloud) and shared VPC networks on GCP. This instance provides core network services such as DNS and IPAM services on a modular Infoblox solution. For more information, see the online Installation Guide for vNIOS for GCP at https://docs.infoblox.com/display/ILP/Appliances

Resolving CNAME and DNAME Chains in A and AAAA Alias Records (RFE-9129)

NIOS now follows CNAME and DNAME chains if they appear as a target of an A or AAAA alias record and returns the RDATA in the final link of the CNAME and DNAME chain as the answer. The chain itself will not be present as part of the answer.

Resetting SNMP and CLI Credentials in Network Insight (SPTYRFE-97)

If SNMP or CLI credentials become obsolete for devices polled by Network Insight, this release of NIOS introduces the following new CLI commands to reset the credentials for all affected devices at once:

- `reset snmp`: Clears obsolete SNMP credentials (community strings) of devices polled by Network Insight.
- `reset cli`: Clears obsolete CLI credentials (community strings) of devices polled by Network Insight.

After clearing obsolete credentials, Network Insight reguesses the credentials for each device. For information about these commands, see the “reset snmp” and “reset cli” topics in the NIOS 8.6 online documentation.

Credential Grouping for Discovery Devices in Network Insight

In Network Insight, you can now group credentials and assign them to devices based on their group. You can do this for devices globally, for probe members, or for individual devices.

Credentials apply to devices at the following levels:

- Grid Manager: Settings apply across the Grid and all probe appliances licensed for discovery.
- Discovery probe appliances: You can use inherited Grid settings or override them.
- Individual devices: You can use inherited Grid or probe settings or override them with device-specific settings.

For more information, see the “Configuring Discovery Properties” topic in the NIOS 8.6 online documentation.

Microsoft Server 2019 Support (RFE-10227)

NIOS 8.6 is supported on Microsoft Server 2019.

Discovery of Cisco Viptela SDN and SD-WAN devices

You can now discover SDN and SD-WAN devices from Cisco Viptela on-premise or cloud infrastructure using Network Insight. For more information, see the “Adding and Configuring Cisco Viptela Discovery” topic in the NIOS 8.6 online documentation.

Adjustable Support Bundle Download Timeout

You can override the default timeout value for support bundle download by a custom value. For more information, see the “Downloading Support Bundles” topic in the NIOS 8.6 online documentation.

Support for New Vendors Using Advisor

A few more new vendors can use the Advisor service to monitor their device lifecycle and vulnerabilities. For more information, see the “Monitoring Device Lifecycle and Vulnerabilities Using Advisor” topic in the NIOS 8.6 online documentation.

Display of Source Device for Discovered Networks

You can now view the device on which a network is discovered by Network Insight. For more information, see the “Network Inventory” topic in the NIOS 8.6 online documentation.

Unbound Upgrade

The Unbound version has been upgraded to 1.10.1

Enabling DDNS Updates from IPv6-Only DHCP Members (RFE-5118)

You can now enable DDNS updates from IPv6-only DHCP members.

DHCP Fingerprint Updates

NIOS now contains new and updated DHCP fingerprints and the fingerprint configuration file has been upgraded to version 10. For details about the fingerprint format, see the “DHCP Fingerprint Detection” topic in the NIOS 8.6 online documentation.

Changes to Default Behavior

This section lists changes to the default behavior in NIOS 8.x releases.

NIOS 8.6.x

- From NIOS 8.6.1 onwards, the name of the *DNS QPS Usage Report* has been changed to *DNS Effective Peak Usage Trend Report*.
- 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 “What’s New” section in these Release Notes. (RFE-10168)
- 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 displayed because red takes the 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.
- 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 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.
- 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 upto 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.
- From NIOS 8.6.2 onwards, the *Grid Properties Editor* > **CSP Config** > **Advanced** tab displays a link that redirects you to the BloxConnect program details.
- From NIOS 8.6.2 onwards, the canonical_name field in the CSV export file is a mandatory field and contains an asterisk next to it.
- 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, 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.

NIOS 8.5.x

- During a staged upgrade, if the NIOS source version to be upgraded from is earlier than 8.5.3, RabbitMQ will continue to use the unsecure mode until the RabbitMQ password is toggled through the CLI after the Grid is completely upgraded to make it secure.
  NOTE: If you run the `set update_rabbitmq_password` command on Grid Master, once ND members rejoin the Grid, RabbitMQ fails to establish connection with the ND members. Perform a product restart on the ND members for the RabbitMQ changes to be reflected.
- In NIOS 8.5.5 and later, for subscriber service devices that have parental control enabled, guest device CEF logs are now throttled to minimise overloading on reporting servers. That is, the generation of CEF logs for guest devices is reduced. This is disabled by default and you can enable disable it by running the newly introduced `set log_guest_lookups` CLI command. The duration of the throttling is for 2.5 minutes and the cache size is 4096 entries. However, RPZ violations will continue to be logged even during the throttling time period.
- In NIOS 8.5.5 and later, subscriber data replication happens through IPv6 for dual mode by default.
- In NIOS 8.5.5 and later, parental control can be enabled on IPv6-only devices.
- NIOS 8.5.5 and later require the ruleset engine version 13 for parental control.
- In NIOS 8.5.5 and later, any domain that categorizes as 0 is considered “fail open” irrespective of whether the database is running or expired. Unknown or dummy domains fail even if Proxy-All is set. “Fail open” means getting a regular response and allowed on the Internet.
- In NIOS 8.5.5 and later, if you add a blocking server, adding a policy management address or a Multi-Service Proxy (MSP) address is optional. In earlier NIOS versions, it was mandatory to add a policy management address or a Multi-Service Proxy if you added a blocking server.
- In NIOS 8.5.5 and later, the **Platform** column in the **Grid Manager** > **Members** tab has been renamed to **Host Platform**.
- In NIOS 8.5.5 and later, you must restart the Grid member if you apply a NIOS subscription license after a NIOS temporary license expires.
- During a staged upgrade to NIOS 8.5.5 and later, you cannot add, update, or delete the following subscriber site attributes: policy management addresses, content proxy addresses, NAS gateways.
- In NIOS 8.5.3, you cannot perform an SSH login if the remote console access is set to disabled.
- In NIOS 8.5.3 and NIOS 8.6, 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. Adding an IP address may result in an error. Conversely, if you add an MGMT IP address to the **Other IP Address** column, you will not be able to enable the DNS service on the IP address.
- When DNS Cache Acceleration and Infoblox Advanced DNS Protection software were both enabled in NIOS versions earlier than 8.5.3, by default Advanced DNS Protection was the first to receive an incoming packet. From NIOS 8.5.3 onwards, by default DNS Cache Acceleration is the first to receive an incoming packet.
- From NIOS 8.5.3 onwards, the DNS over TLS and DNS over HTTPS features support only TLS version 1.2 and TLS version 1.3 cipher suites.

- In NIOS 8.5.3 and later, support has been removed for some special characters in SCP/FTP passwords to fix a potential vulnerability. The allowed special characters are as follows: . - _ / ! @ ^ + % , :
- You can now reset the UDP and EDNS0 buffer to default 1220, if you are using DoT/DoH. This is because TCP handshake is now supported for DoT and DoH queries.
- In NIOS 8.5.3, when Intel® Ethernet controllers XXV710/XL710 are used for the instance and port redundancy is enabled on the node, the fail_over_mac mode is set to “active or 1”. For other NICs, the fail_over_mac mode is set to the default value.
- The NIOS installer files are now available in 2 sizes: 250 GB and 70 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. For information about the resizable files and their limitations, see the “Installing NIOS” topic in the NIOS online documentation.

NIOS 8.4.x

- If you choose to manually update a Threat Analytics whitelist set, it now gets activated automatically.
- The VMXNET virtual network adapter for vNIOS is not supported from NIOS 8.4.x onwards.
- If you select the Enable DNSSEC validation check box and add a trust anchor, the Responses must be secure check box is no longer enabled by default. (RFE-6478)
- Threat Insight whitelists have been updated and are now synchronized with the whitelists on BloxOne Threat Defense Cloud. (RFE-9171)
- You can now perform traffic capture on multiple members at the same time. For more information see the “Monitoring Tools” topic in the NIOS online documentation.

NIOS 8.3.x

- Threat Insight in the Cloud now uses credentials instead of an API key for authorization. If you use Threat Insight in the Cloud, you must configure the email address and password for ActiveTrust Cloud integration in the *Grid Properties Editor* > **ActiveTrust Cloud Integration** tab. The Cloud Services Portal uses these credentials for authorization when you enable the cloud client for Threat Insight in the Cloud or ActiveTrust Cloud for Outbound.
- You can override the Grid or member zone transfer setting at the zone level. Due to an implementation issue in previous releases, when you set the zone transfer setting at the zone level to “None,” the zone still inherited the Grid or member setting. For example, the appliance would still perform zone transfers when you overrode the zone transfer setting to “None” at the zone level if your Grid or member setting allowed zone transfers. When you set zone transfers to “None” at a zone level, the appliance denies zone transfers, and all zone transfers for that zone will fail.
- From NIOS 8.3 onwards, RPZ events require more storage to enable detailed reporting. If you experience a high level of RPZ events, you must either acquire more reporting capacity or change your RPZ configuration to reduce event generation. Post upgrade from NIOS 8.2.7, RPZ hits consume greater memory.

NIOS 8.2.x and Later

- OpenSSH disabled certain legacy vulnerable ciphers that some Cisco devices and versions relied on for CLI collection. To ensure successful CLI collection for such devices, download and install the hotfix referenced as NIOS-69328 in the Infoblox Knowledge Base article 10068 at https://support.infoblox.com
- In NIOS 8.2.x, the appliance adds IP addresses of the external secondary servers to the “also-notify” statement for all master zones. You will see this change when you install or upgrade to NIOS 8.2.x.

NIOS 8.0.0

- The Infoblox DNS Traffic Control solution delivers an enhanced user interface through Grid Manager. Starting with this release, you will experience the following changes:

    - The DTC Server wizard has been integrated with IPAM and DNS. DNS records can be selected under DNS or IPAM, and you can launch the DTC Server wizard. The wizard will then use information from the selected record to create a DTC server. Also, when the DTC server wizard is launched from the Traffic Control tab, you can select a DNS record to provide information for creating a DTC Server.
    - Management of Health Monitors and Topology Rulesets have been moved to dialogs that are launched from the Traffic Control tab.
    - The Traffic Control Visualization can now be viewed in two panels: A panel that is displayed next to the Traffic Control list view or in an expanded full size panel.
    - The visualization panel has many improvements for visualizing and managing traffic control structures, including tooltip menus for directly editing Traffic Control objects.
    - New menu actions have been added to the Action menu (the gear icon) and the visualization tooltip. You can use these actions to quickly add servers to pools and pools to LBDNs.
- Starting with this release, the IB-4030 and IB-4030-10GE appliances use the cache pre-fetch option to replace the old cache refresh. Cache pre-fetch detects cached records that are about to expire and fetch another copy before the actual expiration. When a query asks for data that has been cached, in addition to returning the data, the appliance fetches a fresh copy from the authoritative server if the pre-fetch condition (Eligible and Trigger settings) is met. This option helps minimize the time window in which no answer is available in the cache.
- When configuring DNSSEC, you can select the resource record type (NSEC or NSEC3) you want to use for handling non-existent names in DNS for the Resource Record Type for Nonexistent Proof option. The default is now NSEC3 versus NSEC in previous releases.
- In previous releases, bloxTools is not supported on NIOS virtual appliances. bloxTools is now supported on NIOS virtual appliances.
- In previous release, when port redundancy was configured and if LAN1 was not available, the Infoblox appliance failed over to LAN2. Once the LAN1 connection was available, the appliance reverted to LAN1 automatically. Starting with this release, this behavior has changed. After a failover, the appliance no longer reverts automatically back from LAN2 to LAN1. You can select the Use LAN1 when available option when you enable port redundancy to always use LAN1 when it is available. If this option is not selected, the appliance does not automatically revert from LAN2 to LAN1 even when the LAN1 interface is available.

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 since NIOS 8.3 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 2.12.2.

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, and 2.12.2.

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

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 8.6.*x*

NIOS 8.6.*x* includes the following WAPI changes:

NIOS 8.6.2

New Objects:

- grid:dtc_get_object_grid_state
- grid:dtc_object_disable
- grid: dtc_object_enable
- grid:enable_bfd_dnscheck
- grid:enable_bfd_dnscheck

NIOS 8.6.1

New Objects:

- grid:dns.gen_eadb_from_network_containers
- grid:dns.gen_eadb_from_networks
- grid:dns.gen_eadb_from_ranges
- grid:dns.gen_eadb_from_hosts
- record:host.creation_time

NIOS 8.6.0

New Structures:

- preferred_method

New Objects:

- grid:dns.dtc_dns_queries_specific_behavior
- member:dns.dtc_dns_queries_specific_behavior
- member:dns.use_dtc_dns_queries_specific_behavior
- dtc:pool.auto_consolidated_monitors
- dtc:pool.lb_preferred_method
- dtc:pool.lb_alternate_method
- dtc:pool.full_health_communication
- dtc:lbdn.auto_consolidated_monitors
- dtc:lbdn.lb_method
- grid:dns.last_queried_acl

- grid:view.last_queried_acl
- grid:zone_auth.last_queried_acl

Upgrade Guidelines

- 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.
- 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.
- If you are upgrading from 7.3.200 or 7.3.201 to NIOS 8.0.x or later and have reporting clustering configured, you must download and upgrade to IBRA 1.2.0 (for the Splunk app) after the NIOS upgrade.
- There are special restrictions for configuration changes when upgrading to NIOS 8.0.0 and later releases. For detailed information about the restrictions, see the “Upgrading NIOS” section at https://docs.infoblox.com/

Before You Install

Infoblox supports the following upgrade paths:

- 8.6.1 and earlier 8.6.x releases
- 8.5.5 and earlier 8.5.x releases
- 8.4.8 and earlier 8.4.x releases
- 8.3.8 and earlier 8.3.x releases

Even though Infoblox supports the upgrade paths mentioned above, Infoblox has tested and validated only the following upgrade paths for NIOS 8.6.2. Infoblox recommends that you upgrade to NIOS 8.6.2 from these tested and validated releases:

8.6.1, 8.5.5, 8.4.8, and 8.3.8

If you must upgrade from other NIOS releases, you must first upgrade to the validated paths before upgrading to NIOS 8.6.2. For example, if you want to upgrade from 8.2.x to 8.6.2, you must first upgrade to 8.5.5, and then upgrade to 8.6.2.

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

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

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 only SSL version 3 and TLS version 1 connections. Infoblox recommends that you use a computer that has a 2 GHz CPU and at least 1 GB of RAM.

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

OS	Browser
Microsoft Windows 10®	Microsoft Internet Explorer® 11.*x**, Internet Explorer 10.*x* Microsoft Edge 10 and later
Microsoft Windows 8®	Google Chrome 61.0 and later
Microsoft Windows 7®	Mozilla Firefox 59.*x*
Red Hat® Enterprise Linux® 7.4	Google Chrome 61.0 and later
Red Hat® Enterprise Linux® 7.3	Mozilla Firefox 59.*x*
Apple® Mac OS	Safari 9, Safari 10, Safari 11

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.

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-2021-25220

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-2021-25220

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-2021-25214

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.

Fixed in NIOS 8.6.2

ID	Severity	Summary
NIOS-84523	Critical	After a NIOS upgrade, the **Cloud** > **Network** tab displayed an error.
NIOS-83694	Critical	Under a rare circumstance, DHCP failover association failed.
NIOS-82210	Critical	Subscriber services needed to reduce the number of guest notifications.
NIOS-81406	Critical	A zVELO category mapping needed to be changed.

ID	Severity	Summary

NIOS-85265	Major	The NIOS documentation contained incorrect information that the port 7911 informs the functioning Grid member in a DHCP failover pair that its partner is down.
NIOS-85203	Major	During a NIOS upgrade, file distribution failed and the "Extracting Splunk vanilla Error" error message was displayed.
NIOS-85182	Major	The *Infoblox Installation Guide 1405 Series Appliances* documentation contained erroneous information that it is possible to replace the appliance fans with FRUs.
NIOS-85148	Major	The NIOS documentation did not contain information that configure the LAN interface must be mandatorily configured before joining HA nodes to a Grid.
NIOS-85122	Major	NIOS did not correctly read the ports on the Silicom NIC card on TE-4005 appliances.
NIOS-85110	Major	The “Managing Resource Records” topic in the NIOS documentation contained broken links.
NIOS-84946, NIOS-84944, NIOS-84942	Major	Adding a network using APIs failed and the “certificate verify failed" error was displayed.
NIOS-84914	Major	The refresh interval of a zone transfer did not work when it was configured to be less than 300 seconds.
NIOS-84863	Major	During a NIOS 8.5.5 to NIOS 8.6.2 upgrade, uploading from the **Grid** > **Upload** tab failed.
NIOS-84808	Major	When vDiscovery jobs were enabled, some of the jobs contained recurring errors.
NIOS-84779	Major	Rebuilding the extensible attribute topology database failed.
NIOS-84633	Major	When enabling IPv6 as the DNS interface a resource record error was displayed.
NIOS-84632	Major	The NIOS Release Notes did not contain correct information about the change in behavior of DHCP class filters.
NIOS-84412	Major	Credentials setting was automatically switched to the **Use instance profile** authentication method in the Route 53 sync group when the member assignment was changed from one member to another.
NIOS-84407, NIOS-84332, NIOS-84135	Major	Unable to create the same zone as an authoritative zone after deleting the zone from Grid Manager.
NIOS-84355, NIOS-84351	Major	Unable to apply NIOS licenses after a hotfix was applied.
NIOS-84338	Major	Unable to add networks to Active Directory sites.
NIOS-84333	Major	NIOS was vulnerable to the CVE-2022-0778.
NIOS-84280, NIOS-84277	Major	The SHA1 algorithm being used by NIOS was prone to security scan vulnerabilities.
NIOS-84249	Major	The NIOS documentation contained incorrect information about DHCP failover.
NIOS-84243	Major	Excessive OSPF routes prevented direct route updates.
NIOS-84227	Major	Under certain circumstances, unable to start the discovery service on a Network Insight member.
NIOS-84146	Major	A NIOS upgrade failed and the “1 of 1 node has failed upgrade - Upgrading: Syncing storage files..." error message was displayed.
NIOS-84027	Major	The NIOS documentation did not contain information about restrictions while adding host names.

NIOS-83982	Major	Unable to remove DNSSEC signature from some zones.
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.
NIOS-83729, NIOS-83728	Major	Microsoft Azure cloud vDiscovery stopped working and an error message was displayed.
NIOS-83691	Major	The threat protection service was inactive on newly added members.
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.
NIOS-83285	Major	After restoring the NIOS database, the Grid automatically reverted to an earlier version.
NIOS-83269, NIOS-83076	Major	ADP profiles that were created using the latest rulesets were reverted to the default values.
NIOS-83257	Major	Microsoft Azure cloud vDiscovery stopped working and an error message was displayed.
NIOS-83193, NIOS-83188	Major	Inherited values of DHCP thresholds on DHCP range objects were not reflected in the WAPI calls.
NIOS-83177	Major	Unable to search IPv4 networks through WAPI calls.
NIOS-83175	Major	DNS resolution failed for authoritative zones and the SERVFAIL error was displayed in the log files.
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.
NIOS-83152	Major	NIOS appliances were affected by an SNMP configuration injection vulnerability.
NIOS-83132	Major	RabbitMQ needed to be upgraded from version 3.5.7 to version 3.8.x.
NIOS-83129	Major	Device status files displayed conflicting speed for appliance interfaces.
NIOS-83119	Major	IP address collection took place for virtual IP addresses with incorrect MAC addresses.
NIOS-83079	Major	DHCP release messages were not processed correctly leading to pool exhaustion.
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.
NIOS-83048	Major	Even though full snapshots were successfully imported, generating incremental snapshots displayed an error.
NIOS-82959	Major	Grid members on an ESXi segment were not able to ping their default gateway or each other using IPv6.
NIOS-82754	Major	A bulk conversion of unmanaged devices to host records failed.
NIOS-82693	Major	Under certain circumstances, one of the DNS severs high cache acceleration usage after a sudden increase and decrease of QPS.
NIOS-82624	Major	The SNMP daemon restarted frequently thus affecting the monitoring and unit uptime changes.
NIOS-82623	Major	The threat protection service was inactive on newly added Grid members.
NIOS-82530	Major	Network Advisor did not work as expected with devices of complex configuration.
NIOS-82321	Major	NIOS was rotating the syslog before it reached the configured maximum syslog size.

NIOS-82230	Major	Under certain circumstances, the threat analytics service displayed a warning message or was inactive.
NIOS-82215	Major	Under certain circumstances, the DNS service failed and caused a service impact.
NIOS-82178	Major	Grid Manager frequently restarted and logged the “Logging region out of memory; you may need to increase its size” error message.
NIOS-82103	Major	In Google Chrome and Microsoft Edge browsers, the Accept button in the consent page did not work as expected.
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.
NIOS-81971	Major	When the swap usage rates and the CUP usage rates were high, a NIOS restart needed to be prevented.
NIOS-81847	Major	Restarting the DNS service generated SERVFAIL responses in the log files for almost 15 minutes.
NIOS-81846	Major	When joining a discovery member to a Grid, the join process did not work and the “License not supported by Grid Master” error message was displayed.
NIOS-81839	Major	A RADIUS authentication server group was configured and accounting was enabled, but no accounting messages were sent to the RADIUS server.
NIOS-81865	Major	Restoring an HA Grid did not retain IP address on a standalone Grid Manager and thus the restoration of licenses failed.
NIOS-81862	Major	A scheduled restart on an hourly basis did not work on one of the DHCP failover nodes.
NIOS-81794	Major	When importing certain IPv6 reverse zones, a “Duplicate object '0.0.0.0.0.0.0.0'” error message is displayed.
NIOS-81787	Major	TLSv1.2 and the same set of ciphers as in port 443 needed to be enabled for SAML authentication.
NIOS-81784	Major	DNSTAP stopped working when the destination server restarted or rebooted.
NIOS-81774	Major	The NIOS documentation did not contain information about named ACL limitations.
NIOS-81731	Major	The SQL delimiter for CLI credentials needed to be changed.
NIOS-81668	Major	Inactive IP addresses are displayed as used in IPAM with incorrect discovery data.
NIOS-81574, NIOS-73862	Major	A vDiscovery job with a non-breaking space character could be created.
NIOS-81464	Major	Users in a read-only group were able to add and remove DNS records.
NIOS-81385	Major	Logging into NIOS using SAML authentication failed for Microsoft Azure IDP.
NIOS-81384	Major	NIOS required a restart after certain NIOS licenses were overwritten.
NIOS-81309	Major	NIOS was vulnerable due to weak ciphers suites over port 8765.
NIOS-81213	Major	Under certain circumstances, the threat analytics service restarted.
NIOS-81131	Major	NIOS was vulnerable to the following CVEs: CVE-2021-34798,CVE-2021-34798, CVE-2021-36160,CVE-2021-39275, CVE-2021-40438
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.

NIOS-80826	Major	Users who were given CLI permissions were able to perform tasks that required additional authority.
NIOS-80795	Major	The IP map did not display correct results for a DHCP range when a lease was cleared.
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.
NIOS-80576	Major	Under certain circumstances, DNS Traffic Control and EDNS0 did not work as expected.
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.
NIOS-80474	Major	A possible DNS attack occurred and high CPU utilization was observed.
NIOS-80364	Major	A passive node went offline and the “Fatal error during Infoblox startup” error message was displayed.
NIOS-79967	Major	Under certain circumstances, the anycast loopback address was unreachable.
NIOS-79287	Major	The **Network Selector** > **Networks by Site** screen displayed only 50 sites at a time.
NIOS-79268	Major	The **Network Users** tab intermittently stopped populating Cisco ISE data.
NIOS-78072	Major	A CSV import performance issue occurred for network deletions.
NIOS-76679	Major	The global search by DNS name did not include Network Insight devices.
NIOS-74605	Major	When performing a global search, the “An Error has occurred. Contact technical support if the problem persists” error message was displayed.
NIOS-70653	Major	Unable to update or obtain a network template using WAPI when an extensible attribute was assigned with no value.

ID	Severity	Summary
NIOS-84795	Minor	The data engine discarded IPv4 addresses with /32 mask for certain devices.
NIOS-84404	Minor	The discovery engine fingerprint matching logic needed to be changed.
NIOS-83997	Minor	The NIOS documentation did not contain information about the sgm_admin user account.
NIOS-83995	Minor	The NIOS Release Notes did not contain clear information about DNS scavenging for static records.
NIOS-83491	Minor	The NIOS documentation did not contain information about passwords restrictions for the LOM user account.
NIOS-83476	Minor	The term "ATC" was displayed on Grid Manager.
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.
NIOS-83349	Minor	Grid Manager displayed “CONSOLIDATED MONITOR HEALTH SETTINGS” instead of “CONSOLIDATED HEALTH MONITOR SETTINGS”.
NIOS-83273	Minor	The NIOS documentation contained information about pay-as-you-go content.

NIOS-83201	Minor	The log files were filled with the “Ignoring event IpamEvent:ips_gone/ips_seen .....error: An event processing failed, because no view matches netmri_id = 0” error message for different IP addresses.
NIOS-83186	Minor	The support bundle collected through automated traffic capture did not include debug logs (infoblox.log) and syslogs (var/log/messages).
NIOS-83170	Minor	Replacing a shared record group in a zone triggered an error if old and new groups had the same record.
NIOS-82953	Minor	Unable to run WAPI calls to obtain discovered devices.
NIOS-82885	Minor	The IPAM utilization data was not accurate because of a deduplication issue when a network without SNMP-enabled was added on a consolidator-probe setup.
NIOS-82772	Minor	Cisco APIC connectivity failed with a certificate verification error and as a result the ACI fabric remained undiscovered.
NIOS-82681	Minor	Certain devices needed to be added to the discovery process.
NIOS-82523	Minor	The licensing information in the NIOS documentation was not up-to-date.
NIOS-82218	Minor	The Python stack trace was being displayed in all error messages.
NIOS-82082	Minor	Network Insight attempted SNMP credentials authentication on SNMP-disabled networks.
NIOS-81556	Minor	Unable to swap a member from hardware to virtual if the DSCP setting was overridden in the Member Properties editor.
NIOS-81184	Minor	A CLI command was required to switch DHCP class filter behavior.
NIOS-81155	Minor	An ASCII encode error was displayed in the **Devices** page.
NIOS-80769	Minor	The NIOS WAPI documentation needed an example of an API function to add a consolidated health monitor to an existing DTC pool.
NIOS-80442	Minor	The NIOS documentation did not contain the correct format for the CSV export of the CNAME record.
NIOS-79887	Minor	The NIOS Release Notes contained the same issue in both the Resolved Issues and the Known General Issues sections.
NIOS-77895	Minor	Advanced scheduling options needed to be added in Network Insight.
NIOS-74630	Minor	Extensible attributes were not visible if the **Restricted to Objects** column was made visible.
NIOS-72577	Minor	Deploying a Network Insight appliance caused high memory utilization.

Fixed in NIOS 8.6.1

ID	Severity	Summary
NIOS-81407	Critical	Subsriber services parental control category information needed to be modified.
NIOS-79931	Critical	After a NIOS upgrade, SSH, MGMT, port flapping, and DNS issues occurred.
NIOS-79171	Critical	When port redundancy on LAN1/LAN2 was enabled on vNIOS OpenStack members, a fatal error was displayed in the log files.
NIOS-78568	Critical	Logging out from a WAPI session using cookie-based authentication displays an internal error.

NIOS-78480	Critical	Under a rare circumstance, Grid Master crashed and restarted when configuring SAML.
NIOS-78386	Critical	Host records were deleted after the discovery task was complete and unable to access Grid Manager when discovery aggregator is running.
NIOS-78347	Critical	NIOS was vulnerable to CVE 2021-23839, CVE-2021-23840, and CVE-2021-23841.
NIOS-78323	Critical	An IB-4025 appliance did not restart after threat protection was enabled.
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, DB_SENTINEL VIOLATION errors were displayed on the serial console.
NIOS-76565	Critical	Under a rare circumstance, the DNS service crashed and restarted and subscriber service errors were displayed in the log files.
NIOS-74566	Critical	After a NIOS upgrade, DNS cache acceleration sent all the traffic to the BIND server.

ID	Severity	Summary
NIOS-81645	Major	Using paging for large requests did not return WAPI nested fields.
NIOS-81564	Major	Under certain circumstances, query logging was skipped.
NIOS-81505	Major	The vNIOS for AWS documentation did not contain information that **V2 (token required)** value is not supported in the **Metadata version** field.
NIOS-81243	Major	On platforms on which vritual DNS Cache Acceleration was enabled, packets with a specific transaction ID were dropped.
NIOS-81134	Major	The NIOS documentation did not contain clear information about the change in behavior when clicking the **Cancel** button versus when clicking the **Save & Close** button when the **Enable Automatic Ruleset Downloads** option is enabled.
NIOS-81086	Major	DNS forwarding proxy did not override global forwarders that were configured in the DNS view.
NIOS-81071	Major	A bulk conversion of host records was broken when no zone is specified.
NIOS-81034	Major	The threat analytics service seemed to restart randomly.
NIOS-80981	Major	A discrepancy in the SOA serial number occurred on the DNS Traffic Control zone when DNS Traffic Control was configured.
NIOS-80961, NIOS-80534	Major	Data synchronization failed during an integration with BloxOne Threat Defense Cloud and the log files contained the “Unable to request data: Authorization error” error.
NIOS-80939	Major	If the Grid Master goes offline (because of a shutdown or a disconnecting network, and so on), the Grid Master Candidate and Grid members synchronize with external NTP servers.
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.
NIOS-80891	Major	Networks assigned to a DHCP member were unable to obtain addresses until an HA failover.
NIOS-80874	Major	Under certain circumstances, the threat protection service did not start on a new appliance.

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** check box not selected.
NIOS-80713	Major	The management IP assignment algorithm needed to be revisited.
NIOS-80710	Major	The IPAM network was not being updated with direct routes from certain devices.
NIOS-80709	Major	DDNS updates only succeeded on one primary server; therefore, some clients failed to register and lost access to specific resources.
NIOS-80706	Major	All licenses for a Grid member had been revoked after changing the IPv6 gateway address.
NIOS-80676	Major	Under certain circumstances, the DHCP service failed and the log files contained the “No DHCPv4 configuration files found. Rebuilding conf file dhcpd.conf” error message.
NIOS-80642	Major	Under certain circumstances, two IB-FLEX members repeatedly went offline on all NICs.
NIOS-80548, NIOS-80546	Major	The NIOS documentation did not contain information about ACS (Assertion Consumer Service) which is required to configure SAML authentication.
NIOS-80539	Major	The DHCP license was missing despite the license being applied.
NIOS-80526	Major	Under certain circumstances, caching servers did not take any traffic.
NIOS-80504	Major	Under certain circumstances, Network Insight was unbale to discover new devices.
NIOS-80447	Major	The change in behavior regarding MAC address filters was not documented in the NIOS Release Notes.
NIOS-80381	Major	Under certain circumstances, certificate validation failed for HTTPS health monitors.
NIOS-80325	Major	If you tried to export VLAN names in the visible data format, the **Assigned To** field in the CSV file displayed non-readable entries.
NIOS-80320	Major	While creating an authoritative IPv4 reverse-mapping zone with the RFC-2817 prefix, step 3 in the wizard displays an alert message that the prefix must not be empty even though the prefix was added in step 2.
NIOS-80225	Major	Under certain circumstances, the **Status** column in the **Grid Manager** > **Reporting** tab displayed the “Indexer reporting service is failed” error message.
NIOS-80186	Major	Modifying a set of TXT records using CSV import in the override mode failed because of a backslash problem.
NIOS-80178	Major	When SDN polling was disabled, "Discovery Collector Service is inactive" SNMP trap messages were frequently generated.
NIOS-80144	Major	The CLI command to get the ARP date for Cisco devices needed to be changed.
NIOS-79968	Major	SNMPv3 credentials that did not have a privacy protocol were not saved.
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.
NIOS-79919	Major	Changing the IPv6 gateway address revoked all the licenses of a Grid member.
NIOS-79918	Major	Splunk admin password dependencies needed to be removed.
NIOS-79890	Major	If the Unicode DNS zones contained a numeric value in the FQDN name, the WAPI call displayed an error during a KSK rollover.

NIOS-79871	Major	“iftab.IB-FLEX” was not a part of the support bundle.
NIOS-79779	Major	After a NIOS upgrade, unable to log in using the certificate authentication service.
NIOS-79735	Major	Option 81 settings were not being inherited from the Grid to Grid members.
NIOS-79734	Major	DNSSEC validation failed for DNS Traffic Control records because of expired RRSIG only for DNS Traffic Control LBDN records.
NIOS-79716	Major	The Grid secondary did not synchronize with the lead secondary on time.
NIOS-79713	Major	In the CSV export file, the password for CLI credentials was displayed in plain text.
NIOS-79710	Major	While creating an authoritative IPv4 reverse-mapping zone with the RFC-2317 prefix, step 3 in the wizard displays an alert message that the prefix must not be empty even though the prefix was added in step 2.
NIOS-79692	Major	Renaming the in-built “admin-group” group in NIOS prevented a NIOS upgrade.
NIOS-79689	Major	The `reset database` command did not work in the emergency mode. Under certain circumstances, IB-FLEX appliances experienced database issues.
NIOS-79683	Major	The named.conf file for an RPZ Grid member contained a syntax error.
NIOS-79654	Major	Topology rules did not work for Grid members that had external attributes.
NIOS-79649	Major	The collector discovery service failed constantly and at regular intervals and the number of devices disovered by Network Insight was greater than the number of devices present.
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.
NIOS-79627, NIOS-79585	Major	Creating a host record in an authority-delegate DNS zone generated an error.
NIOS-79606	Major	After a NIOS upgrade, the Member DNS Properties screen displayed an error message for Grid members that inherited the **None** setting from the Grid under **Zone Transfers**.
NIOS-79594	Major	After a NIOS upgrade, the Azure vDiscovery job deleted all the records it had discovered in the past.
NIOS-79592	Major	The NIOS documentation did not contain information that the **Enable GSS-TSIG Updates** field must be overridden in the *Member DHCP Properties* dialog box to use the KDC configured in the *Member DHCP Properties* dialog box.
NIOS-79586	Major	An Active Directory authentication error message was displayed after a SAML authentication even if SAML was not configured on the authentication policy.
NIOS-79581	Major	IP address lease exhaustion issues occurred and multiple active IPv6 addresses were issued from the same subnet for the same client.
NIOS-79543	Major	AWS vDisovery jobs from cloud platform members with instance profiles failed.
NIOS-79505	Major	Restarting services using Grid Manager displayed a contact technical support error message.
NIOS-79456	Major	The Cisco ISE integration with NIOS did not work as expected.
NIOS-79455	Major	After a NIOS upgrade, the Grid Master and Grid Master Candidate constantly restarted and core file were generated.
NIOS-79427	Major	Under certain circumstances, the passive node of a Grid Master lost connection intermittently.

NIOS-79413, 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.
NIOS-79394	Major	After a NIOS upgrade, the threat protection service did not start on IB-FLEX members.
NIOS-79391, NIOS-79390	Major	An NTP forced synchronization did not take place when a product reebot or restart was performed.
NIOS-79368	Major	Large UDP responses timed out but were displayed in the packet captures.
NIOS-79338	Major	Accessing the **Cloud** > **Tenants** > **All Tenants** option displayed an error message.
NIOS-79316	Major	A DHCP failover association recovered after waiting for the MCLT period when the DHCP range was moved from a single member to a failover.
NIOS-79314	Major	Under certain circumstances, the secondary node in a DHCP failover was stuck in a recover-wait state.
NIOS-79302	Major	Smart folders displayed duplicate results when networks were grouped with external attributes.
NIOS-79286	Major	Rule 130000800 blocked truncated DNS queries after disaster recovery.
NIOS-79275, NIOS-79163	Major	Unable to add a Grid member to a name server group.
NIOS-79272	Major	Network Insight used the wrong name to tagged VLAN interfaces with NIC bonding.
NIOS-79268	Major	The **Data Management** > **Network Users** tab was not populated with Cisco ISE data.
NIOS-79232	Major	Rebuilding the EA topology database did not work.
NIOS-79229	Major	The NTP service stopped responding when ACLs were added.
NIOS-79138	Major	Some of the cloud-related screens of Grid Manager took a long time to display.
NIOS-79088	Major	Unable to download threat protection rules when proxy server settings were configured with an IPv6 address in a dual stack Grid Master.
NIOS-79066	Major	Editing an NTP member settings displayed an error message.
NIOS-79025	Major	If the reporting backup path contained a backslash, the backup did not succeed.
NIOS-79024	Major	WAPI updates to ACEs for DDNS returned an internal error.
NIOS-79011	Major	When NIOS is launched on a new IB-FLEX appliance on the Red Hat OpenStack platform, a fatal error is displayed.
NIOS-79004	Major	A reporting appliance did not display data for the End Host History report.
NIOS-78855	Major	The Ptop files in var/log have gaps where no fastpath line is included as a result of which the DNS process does not restart.
NIOS-78611	Major	Network Insight queried internal DNS servers even when the DNS resolver was set to external Microsoft DNS servers.
NIOS-78593	Major	After a NIOS upgrade, unable to view secondary zone data and the “An error has occurred. Contact technical support if the problem persists” error message was displayed.
NIOS-78577	Major	Grid Manager displayed an incorrect status for LBDN when all servers associated with the pool had a green status.

NIOS-78522	Major	After a NIOS upgrade, CPU usage and memory increases occurred.
NIOS-78515	Major	The DNS client failed to detect UDP DNS responses when there is an RPZ rule match and virtual DNS cache acceleration was enabled
NIOS-78513	Major	When editing the Primary name server (for SOA MNAME field) field in the **Authoritative Zone** > **Settings** > **Basic** tab, the value reverts to the inherited value in Grid Manager.
NIOS-78503	Major	Under certain circumstances, GSS-TSIG DDNS failed on certain devices.
NIOS-78486	Major	Under certain circumstances, Microsoft Azure vDiscovery jobs failed and an internal error message was displayed.
NIOS-78484	Major	The show firmware CLI command did not display the Ethernet firmware version.
NIOS-78461	Major	After a NIOS upgrade, SAML authentication using Ping Identitiy returned an internal server error.
NIOS-78460	Major	After a NIOS upgrade and after performing a Grid Master Candidate promotion, SSO did not work and the SAML authentication service could not be added.
NIOS-78456	Major	A NIOS upgrade caused the MAC address to change on the MGMT interface.
NIOS-78455	Major	The trap values in the NIOS documentation and specific SNMP OIDs in traps did not match.
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.
NIOS-78402	Major	A Microsoft Azure vDiscovery job failed when a proxy server connection was required.
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.
NIOS-78385	Major	The global search did not return matches when searching for DHCID records using the DNS name.
NIOS-78314	Major	Under certain circumstances, the reporting service failed to start.
NIOS-78244	Major	After restarting a host address, there was no prompt to restart the service and a manual service restart was required.
NIOS-78222	Major	Under certain circumstances, IPv4 option filters did not work.
NIOS-78219	Major	Unable to retrieve the name of an LBDN from an FQDN pattern using WAPI.
NIOS-78180	Major	An event was triggered and sent to an endpoint even when no modification was made to the host record.
NIOS-78134	Major	When network containers and their child objects were deleted, orphaned hosts were not cleared.
NIOS-78132	Major	When querying IPv6 addresses inside a given IPv6 network, the REST engine recognized only lower case letters IPv6 addresses, not IPv6 addresses with capital letters.
NIOS-78072	Major	Deleting networks using CSV import caused performance issues.
NIOS-78064	Major	The reporting service failed because of license overuse.
NIOS-77939	Major	Grid members and the Grid Master were unable to function as NTP servers to clients if NTP was enabled on the Grid.
NIOS-77913	Major	If the subscriber cache entry did not have PCP:Parental-Control-Policy, the proxy VIP allocation process was not initated towards the MSP.

NIOS-77869	Major	The parental control policy was being checked before the subscriber service policy which caused all whitelisted domains to be ignored during a pause internet phase.
NIOS-77816	Major	The show log CLI command did not work as expected and stopped after the `Enter <return> for next page or q<return> to cancel the command` line.
NIOS-77800	Major	IPv6-only Grid members experiences network issues after a product restart.
NIOS-77790	Major	When deleting an extensible attribute value at the parent network container level using API, the value was not removed from the child network container even when specified to do so.
NIOS-77738	Major	Calls without credentials were displayed in the Active WebUI Users dashboard and in audit logs when a SAML authentication was triggered at the same time.
NIOS-77730	Major	Retrieving a CA certificate for the Cisco ACI SDN connection displayed an error message.
NIOS-77728	Major	An incorrect VLAN was displayed in IPAM for end devices.
NIOS-77726	Major	The IPMI tool was not upgraded and thus NIOS was vulnerable to CVE-2020-5208.
NIOS-77561	Major	After an HA synchronization, multiple issues caused a DNS outage.
NIOS-77558	Major	Under certain circumstances, categories could not be downloaded when using proxy without credentials.
NIOS-77519	Major	Under certain circumstances, false positive notifications and email alerts regarding power supply were generated.
NIOS-77283	Major	The dns_stats.txt file displayed a very high value for recursing clients.
NIOS-77243	Major	High CPU utilization was observed on CP-V2200 that was running on the Microsof Azure platform.
NIOS-77242	Major	Downloading the threat analytics moduleset failed and an email notification was generated.
NIOS-77221	Major	An anycast IP address timeout occurred after the netmask changed.
NIOS-77102	Major	The DNS cache acceleration usage was always at 0% when virtual DNS cache acceleration was enabled on IB-4025 appliances.
NIOS-76916	Major	Under certain circumstances, BGP packet flapping occurred unexpectedly and some appliances experienced high DNS acceleration usage which impacted recursive querying.
NIOS-76676	Major	Global search by IP address did not work and and returned an error.
NIOS-76442	Major	Creating an ACL for an administrator group blocked login using the serial console.
NIOS-76313	Major	The `set debug_tools db_sync` command did not work on HA pairs.
NIOS-75572	Major	SSH did not work after a NIOS upgrade.
NIOS-75520	Major	Under certain circumstances, synchronization to the Grid Master did not work as expected and errors were displayed in the log files.
NIOS-75043	Major	Under certain circumstances, one zone always displayed the serial number as one lower than the actual number on both the DNS primary and secondary servers.
NIOS-74955	Major	After enabling DNS scavenging, static records were deleted.
NIOS-74852	Major	The .bash_history history file did not get automatically cleaned after each logout.

NIOS-74849	Major	Disclosure of sensitive information aided staging attacks.
NIOS-74848	Major	Certain error messages contained technical details.
NIOS-74779	Major	Some of the authoritative DNS servers returned SERVFAIL errors for queries to a zone.
NIOS-74708	Major	The reporting functionality did not work as expected after a hotfix was applied.
NIOS-74652	Major	Using option 81 to allow DDNS updates to an external Active Directory domain also updated other zones.
NIOS-74521	Major	The DHCP service did not restart while performing a service restart using the **If Needed** option after adding the DOW_DHCP_AllScopes MAC address filter to a range.
NIOS-73862	Major	Creating a vDiscovery job whose name contains special characters displayed an error message.
NIOS-73598	Major	NIOS lacked protection against brute force attacks.
NIOS-71536	Major	SOA records failed to validate with DNSSEC.
NIOS-70675	Major	Updating the `Infoblox:Grid:DNS` object using PAPI deleted all name server groups that were not of the type authoritative.
NIOS-70603	Major	Scheduled tasks were not executed as scheduled if a Grid Master Candidate promotion took place.
NIOS-69765	Major	An RPZ blocked domains and the NODATA response was recorded in the log files even though no such rule was configured.
NIOS-67551	Major	Using the `sort` command without a count value in reports truncated the results.

ID	Severity	Summary
NIOS-81626	Minor	Reading files through path traversal using WAPI needed to be prevented.
NIOS-81527	Minor	The NIOS documentation needed to be updated with information about upgrading NIOS when the DHCP expert mode is enabled.
NIOS-81253	Minor	When the interface description in the **Data Management** > **Devices** > **Interfaces** page was updated, the changes did not reflect immediately.
NIOS-81209	Minor	The NIOS documentation needed to contain more information about scheduling upgrades.
NIOS-81103	Minor	The NIOS documentation did not contain information about BloxOne rules such as BloxOne Threat Defense Cloud Hit Class, BloxOne Threat Defense Cloud Hit Property, BloxOne Threat Defense Cloud Hit Type, and Threat Origin when the **DNS RPZ** event was selected from the **Event** drop-down list in the *Add Notification* wizard.
NIOS-80831	Minor	When using global smart folders, icons such as Edit, Create link, Delete were hidden.
NIOS-80717	Minor	Editing a network container caused Grid Manager to log out and a system error message was displayed.
NIOS-80687	Minor	On the **Grid** > **Grid Manager** > **Members** tab, navigating the horizontal scroll bar to the right caused the table contents to display incorrectly.
NIOS-80433	Minor	The warning message that is displayed when the **Enable Time Based Retention** check box is selected needed to be modified.

NIOS-80121	Minor	The discovery engine ignored the management IP address for NIOS appliances.
NIOS-80074	Minor	Active Directory authentication failed for users whose login ID included German characters such as ä" , "ü", "ö", "ß" and so on.
NIOS-80032	Minor	The EPG, tenant, and bridge domain information was missing for certain devices.
NIOS-79764	Minor	When SNMP collection was disabled on the Grid but enabled on the network, no data was collected.
NIOS-79602	Minor	The NIOS documentation did not contain clear information about the Customer Experience Improvement Program.
NIOS-79600	Minor	The NIOS documentation did not contain information that Infoblox supports only basic authentication for vDiscovery jobs performed over a proxy server as not all proxy options are validated.
NIOS-78552	Minor	NAT mapping was not recognized by the ADP NXDOMAIN rate limit rule.
NIOS-78551	Minor	DNS queries and other domain responses were not being resolved as expected.
NIOS-78495	Minor	The WAPI documentation stated that WAPI supports only HTTP basic authentication and not certificate-based authentication.
NIOS-78374	Minor	Under certain circumstances in an HA setup, intermittent flip flop of the core DNS service occurred.
NIOS-77732	Minor	Under certain circumstances, the **Auto-detect time zone** option in the **Time Zone** drop-down list of the *User Profile* screen did not work as expected.
NIOS-77619	Minor	Encrypytion algorithms for Grid members and reporting members needed to be changed.
NIOS-77177	Minor	The DHCPv6 option code for the domain-name option was not clear.
NIOS-76456	Minor	The subscriber service error message "PCP config result: Subscriber Config not fully applied" was not easy to understand.
NIOS-75532	Minor	Certain messages displayed in the log files when Subscriber Services was deployed were not clear.
NIOS-72920	Minor	Using the Grid Manager to perform a query on an AXFR record failed.
NIOS-71003	Minor	Using WAPI for a CSV export of all records listed multiple entries for the same host address.

Fixed in NIOS 8.6.0

ID	Severity	Summary
NIOS-77720	Critical	Memory issues occurred on VMware appliances that had 12000 LBDNs.
NIOS-77582	Critical	The **Data Management** > **DNS** > **Traffic Control** > **Traffic Control** page did not load 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.
NIOS-77155	Critical	Limit parameters needed to be added for ND-1405.
NIOS-77091	Critical	Certain world-writable files were located that were executed as the root user thus leading to privilege escalation or root-level compromise of the system.
NIOS-76645	Critical	The NIOS online help metadata disclosed machine information.

NIOS-76536	Critical	The SNMP clear trap was not sent for the NTP Sync Down event after a Grid Master Candidate promotion.
NIOS-76487	Critical	Under a rare circumstance, an unexpected HA failover occurred during a zone data import.
NIOS-76425	Critical	Under a rare circumstance, unable to add members to a nameserver group and the “Invalid value was entered" error message was displayed.
NIOS-76421	Critical	An SNMP trap did not work after a Grid Master Candidate promotion.
NIOS-76334	Critical	Unexpected change in behavior occurred on some members after running the set subscriber_secure_data bypass command.
NIOS-76330	Critical	Under a rare circumstance, threat protection did not work on the IB-4025 appliance.
NIOS-76236	Critical	SNMP traps were not triggered for DNS tunneling detection even though the Threat Analytics DNS Tunneling event type was enabled.
NIOS-76216	Critical	Packet drops increased between the production environment and vNIOS.
NIOS-75687	Critical	After disabling a parent zone, unbale to query PTR records and PTR requests failed.
NIOS-75658	Critical	Unable to automatically create a reverse zone when creating a network using CSV.
NIOS-75433	Critical	The value of the snmpEngineBoots SNMPv3 trap did not increment.
NIOS-75339	Critical	Applying a hotfix to an upgrade group applied the hotfix to the entire Grid instead.
NIOS-75382	Critical	Under a rare circumstance, subscriber service category blocking did not work as expected.
NIOS-75186	Critical	vNIOS did not send a report ready indication to Microsoft Azure when the provisioning was complete.
NIOS-75139	Critical	Under a rare circumstance, when subscriber services were running, CPU utilization was at 100% on some nodes and non-cache latency also increased.
NIOS-75126	Critical	The DNS service was interrupted after subscriber services was enabled.
NIOS-75003	Critical	Unable to start the DHCP service because no valid configuration files were available.
NIOS-74808	Critical	Under a rare circumstance, the IB-FLEX server restarted constantly.
NIOS-74771	Critical	The Infoblox Installation Guide vNIOS for VMware was not updated with the latest VMware ESX and ESXi supported versions.
NIOS-74756	Critical	A DNS core file was generated after enabling subscriber services on a server.
NIOS-74681	Critical	After a NIOS upgrade, NIOS restarted every 1 to 2 days on the active node resulting in an HA failover.
NIOS-74661	Critical	After a NIOS upgrade, alerts were displayed on IB-FLEX appliances and services were restarted.
NIOS-74597	Critical	Under a rare circumstance, DNS servers stopped responding after a NIOS upgrade.
NIOS-74557	Critical	After a NIOS upgrade, swap usage increased and may eventually impact DHCP services on Grid members.
NIOS-74556	Critical	After a NIOS upgrade, DNS cache acceleration sent all of the traffic to the BIND server.
NIOS-74518	Critical	DNS Traffic Control initialization failures were displayed in the log files after a hotfix was applied.

NIOS-74440	Critical	Under a rare circumstance, the IB-V1415 appliance frequently restarted and the log files displayed the “Logging region out of memory; you may need to increase its size” message.
NIOS-74434	Critical	Under a rare circumstance, system swap space usage exceeded the critical threshold value.
NIOS-74378	Critical	The /etc/hosts file was replaced with a 0 length file.
NIOS-73857	Critical	The NIOS documentation did not contain clear details about the password length for the LOM user account.
NIOS-73688	Critical	Certain vNIOS appliances did not auto-synchronize with the Grid Manager and the “System restart: sync release failure” error message was displayed in the log files.
NIOS-73424	Critical	The Infoblox Customer Experience Improvement Program screen contained a typo.
NIOS-73400	Critical	After a NIOS upgrade, the reporting license changed to freemium.
NIOS-73118	Critical	Under a rare circumstance, DNS members dropped queries and generated slower responses.
NIOS-73010	Critical	After a NIOS upgrade, there was an increase in memory utilization, and in turn swap usage, on some Grid members.
NIOS-72741	Critical	The CVE-2016-9138 vulnerability was addressed.
NIOS-72552	Critical	Under certain circumstances, DNS views were erroneously populated into the DNS member configuration even though **View Recursion** was disabled.
NIOS-71011	Critical	Under certain circumstances, unable to change the nameserver group of a subzone when parent zone is signed.
NIOS-70715	Critical	Under a rare circumstance, there was high CPU utilization on multiple Grid members as well as latency in DNS responses.

ID	Severity	Summary
NIOS-78003	Major	The **SSO metadata URL** field in the in *SAML Authentication Service* dialog box was incorrectly populated when using the metadata file for SAML configuration.
NIOS-77997	Major	NIOS was vulnerable to an XML bomb attack if SAML authentication was used.
NIOS-77947	Major	The entity ID in the NIOS metadata file used for SAML authentication could be exploited and could lead to a Denial-of-Service attack.
NIOS-77862	Major	Under certain circumstances, logging in using SAML authentication did not log in directly to the Grid Manager home page; instead, it displayed the login page once again.
NIOS-77807	Major	Installing a temporary license for vNIOS on Microsoft Hyper-V 2016 on an IB-V5005 appliance displayed the following error message: “You must provision the reporting disk before adding a license to the Reporting server.”
NIOS-77614	Major	The NIOS documentation needed to be enhanced to explain the use/integration of the extensible attribute -based topology rulesets with DNS Traffic Control.
NIOS-77563	Major	The DNS Traffic Control round robin load balancing method did not work as expected after a NIOS upgrade.
NIOS-77482	Major	When generating a certificate signing request (CSR), the default constraint parameter CA was to true, causing connectivity issues in certain browsers and appliances.

NIOS-77449	Major	Under certain circumstances, DNS servers intermittently did not respond to dynamic updates.
NIOS-77372	Major	Certain Grid DNS members kept getting disconnected from the Grid.
NIOS-77352	Major	File distribution synchronization errors were displayed in the debug log of a Grid member even though FTP or TFTP was not enabled on the member or Grid Manager.
NIOS-77350	Major	Under certain circumstances, DNS Traffic Control and EDNS0 did not work reliably.
NIOS-77291	Major	Intermittent DNS timeouts and long delays in query resolution (up to 3 seconds) occurred after a NIOS upgrade.
NIOS-77270	Major	Under certain circumstances, the DNS service caused swap issues in several Grid members.
NIOS-77146	Major	Grid Manager became unstable when the object change tracking feature was enabled.
NIOS-77096	Major	Grid Manager was very slow especially when viewing VLAN views.
NIOS-77095, NIOS-77009	Major	NIOS was vulnerable to CVE-2020-25705.
NIOS-76927	Major	The DNS server did not detect the configured blocking server CNAME record.
NIOS-76911	Major	Data in the DNS Query Rate by Member report and data in the PTop graphs were different.
NIOS-76893	Major	The NIOS documentation did not contain information about the use of MGMT interface being configured and used for Grid traffic on members that have Advanced DNS Protection.
NIOS-76785	Major	Certain world-writable files were located that were executed as the root user thus leading to privilege escalation or root-level compromise of the system.
NIOS-76776	Major	A NIOS upgrade failed because of incorrect index processing in the NetMRIModeSettings.pl file.
NIOS-76734	Major	Under certain circumstances, Grid Manager crashed when making DNS Traffic Control changes and then restarted.
NIOS-76679	Major	Performing a global search by DNS name did not include Network Insight devices.
NIOS-76676	Major	Performing a global search by IP addresses did not work when the Network Insight member was disconnected from the Grid and the “No response from discovery service: Connection refused." error message was displayed.
NIOS-76656	Major	A warning banner was displayed that the Grid license will expire in 60 days. However, the license was to expire after 89 days.
NIOS-76629	Major	DNS resolution for the host record failed after creating a reverse mapping zone.
NIOS-76573	Major	Unable to access Grid Manager and the API after an HA failover.
NIOS-76491	Major	The extensible attribute rebuild prompt was not displayed when deleting the extensible attribute from a network.
NIOS-76363	Major	A user configured to use local authentication was able to login with the remote password if the same user name existed in the remote authentication server.
NIOS-76362	Major	The “Cluster master service failure due to search factor is not met” message was displayed on the **SERVICE STATUS** column of the **Reporting** tab as a result of which the cluster was not in a working state.
NIOS-76349	Major	TCP quota logs were never hit even though the TCP client quota was exceeded.

NIOS-76312	Major	vDiscovery did not work for the “eu-central-1.console.aws.amazon.com” AWS region.
NIOS-76300	Major	vDiscovery failed and the “ip_owner_id” error message was displayed in the log files.
NIOS-76282	Major	Under certain circumstances, the reporting server did not display data for the Device Interface Inventory report.
NIOS-76273	Major	Under certain circumstances, some Grid members did not respond to SNMP queries.
NIOS-76142	Major	The NIOS documentation contained an incorrect DNS query log format.
NIOS-75659	Major	Zone-Signing Keys (ZSKs) that were rolled over were not being automatically deleted.
NIOS-75657	Major	During a NIOS upgrade, vNIOS for Azure Grid members were unable to rejoin the Grid because Grid Manager did not set the correct time.
NIOS-75646	Major	The Nmap version on a Network Insight member was incorrect.
NIOS-75631	Major	SSH did not work on MGMT after a NIOS restart when the **Restrict Remote Console and Support Access to MGMT Port** option was enabled.
NIOS-75564	Major	Query per second (QPS) reports displayed an abnormal pattern after a NIOS upgrade.
NIOS-75561	Major	DNS servers did not accept or acknowledge RADIUS messages that were over 1077 bytes.
NIOS-75540	Major	The NTP server did not set the absolute time early.
NIOS-75539	Major	Time reset did not work on vNIOS for Azure instances.
NIOS-75534	Major	After installing a certificate file, Grid Manager became unavailable and displayed the SSL_ERROR_RX_MALFORMED_HANDSHAKE error message in FIrefox.
NIOS-75465	Major	Under certain circumstances, the threat protection service crashed unexpectedly after which some Grid members were offline.
NIOS-75435	Major	The RADIUS class AVP needed to be of the string value type.
NIOS-75432	Major	The NIOS documentation contained incorrect field names for ca_value and ca_tag in the example for adding a CAA record.
NIOS-75391	Major	An unexpected HA failover occurred and there were many differences in the dhcpd.conf files of the active node and the passive node.
NIOS-75374	Major	Unable to add a job using the bloxTools scheduler.
NIOS-75361	Major	After a NIOS restart, SSH did not work on the MGMT port when the **Restrict Remote Console and Support Access to MGMT Port** option was enabled.
NIOS-75326	Major	The status of the consolidator had turned red and the “Discovery Consolidator Service has failed” error message was displayed.
NIOS-75231, NIOS-75229	Major	Unable to join the discovery node to the Grid after a NIOS upgrade.
NIOS-75228	Major	Unable to reset the password after expiry of the old password.
NIOS-75094	Major	Mismatch in Grid Manager and the NIOS documentation regarding enabling DNS servers to accept DDNS updates.
NIOS-75031	Major	When the time zone was changed, after logging out of Grid Manager and logging back in, the updated time zone was not retained.
NIOS-75010	Major	Running the set reporting_reset_license CLI command caused an HA failover.

NIOS-74986	Major	The threat protection rule publishing failed and generated IMC core files.
NIOS-74981	Major	Unable to view debug logs after configuring an outbound endpoint.
NIOS-74947	Major	The NIOS servers went offline after running the set dns flush tree command.
NIOS-74946	Major	Certain extensible attributes were not displayed in the DNS Traffic Control and topology rulesets.
NIOS-74923	Major	Under certain circumstances, DNS servers did not synchronize subscriber service data.
NIOS-74860	Major	If a delegation was created in the disabled state, the delegation deleted the parent records that were within the delegation.
NIOS-74860	Major	Colors for the reserved range values and DHCP exclusion range values were displayed incorrectly in the *IP Map* page.
NIOS-74842, NIOS-74841	Major	Unable to perform dynamic updates because of the prerequisite check being dropped by Advanced DNS Protection.
NIOS-74831	Major	Information about RPZ events requiring more storage to enable detailed reporting was not documented in the “Changes to Default Behavior” section of the NIOS 8.3.x and later Release Notes.
NIOS-74821	Major	After a NIOS upgrade, one of the Grid members failed the upgrade and the “Upgrading: Syncing storage files” message was displayed in the log files.
NIOS-74818	Major	Selecting the **Copy Audit Log Messages to Syslog** check box and then selecting the syslog facility displayed incorrect values in the **Administration** > **Logs** > **Syslog** screen.
NIOS-74815	Major	Grid members went offline after the NIOS license expired on Grid Manager.
NIOS-74795	Major	After a NIOS upgrade, the DNS service failed to start.
NIOS-74772	Major	Unable to poll certain OIDs introduced for IB-4030.
NIOS-74769	Major	The threat analytics service kept restarting and errors were displayed in the debug log files.
NIOS-74742	Major	Under certain circumstances, disk usage on Grid Master was over the threshold value.
NIOS-74722	Major	Unable to delete stale NS records from the NIOS database.
NIOS-74713	Major	After a NIOS upgrade, unable to log in to Grid Master via SSH Active Directory authentication.
NIOS-74686	Major	When creating a DNS Traffic Control server using the *DTC Server Wizard*, the **IP Address** field was not getting auto-populated.
NIOS-74685	Major	If you created a global smart folder and applied the “Type equals VLAN View” filter, clicking the folder did not navigate to the VLAN view. This is expected behavior.
NIOS-74665	Major	A CLI command was required that swiftly halts the subscriber services parental control DNS process on a Grid member.
NIOS-74613	Major	Under certain circumstances, the reset all CLI command did not work.
NIOS-74612	Major	The NIOS documentation did not contain information that associating a DHCP fingerprint filter with a DHCP range on a DHCP member or a failover association does not require a DHCP service restart.
NIOS-74587	Major	Under certain circumstances, regular failovers occurred on the HA members of the Grid.

NIOS-74579	Major	The ibSystemMonitor section of the NIOS documentation was not in synchronization with the actual MIB file.
NIOS-74533	Major	The NIOS documentation did not contain information about creating different VLAN names for the same VLAN object in overlapping VLAN ranges under a single view.
NIOS-74492	Major	Grid members were upgraded without a scheduled upgrade or a manual upgrade when the passive node in an HA setup joined back to the Grid.
NIOS-74480	Major	Unable to create an IPv6 network using the IPv6 template that contained multiple IPv6 fixed address templates.
NIOS-74450	Major	Under certain circumstances, the threat analytics service did not start on some Grid members.
NIOS-74449	Major	In the emergency mode, the reset database CLI command did not work as expected.
NIOS-74436	Major	Under certain circumstances, database utilization in Grid Master was very high.
NIOS-74408	Major	Unable to obtain a lease because of a DHCP outage accompanied by a high replication queue.
NIOS-74331	Major	The “Comparison method violates its general contract” error message was displayed in the **VRF Mapping** screen.
NIOS-74330	Major	The NIOS documentation did not contain information about removing the external NTP configuration before promoting the Grid Master Candidate.
NIOS-74066	Major	In a Multi-Gird Master setup, a Grid Master stopped synchronizing with its sub-Grids.
NIOS-74051	Major	The NIOS documentation did not detail the disable_ns_generation field for import of forward zones.
NIOS-73976	Major	Accessing the **DNS** > **Members/Servers** tab caused the “KeyError:build_epoch” error message to be displayed.
NIOS-73951	Major	Auto created records of forward zones were not deleted after the subzones were deleted.
NIOS-73939	Major	After a NIOS upgrade, Active Directory users were unable to access the **Reporting** tab.
NIOS-73937	Major	Under certain circumstances, the scheduled Grid upgrade was disabled automatically.
NIOS-73900	Major	Unable to add a nameserver to an authoritative zone.
NIOS-73896	Major	The DHCP failover association went into the RECOVER-WAIT state after a range was modified.
NIOS-73890	Major	The NIOS documentation did not contain information that existing extensible attributes are automatically enrolled for cloud usage when cloud licensed are installed.
NIOS-73831	Major	The NIOS documentation did not contain information about the usage parameter that is used for the clear_discovery_data function.
NIOS-73810	Major	Information that NIOS is not vulnerable to CVE-2019-18609 was not mentioned.
NIOS-73809	Major	The **RPZ logging** check box was greyed out when a nameserver group was assigned to an RPZ zone.
NIOS-73794, NIOS-73707	Major	The **DNS Cache Acceleration** tab displayed the green color inspite of virtual DNS Cache Acceleration not being started.
NIOS-73705	Major	BloxOne Threat Defense was erroneously mentioned as BloxOne DDI in the NIOS documentation about forwarding recursive queries.

NIOS-73689	Major	Unable to add multiple extensible attributes using WAPI.
NIOS-73659	Major	After promoting a Grid Master Candidate to Grid Master, some older HA members and other Grid members were offline.
NIOS-73601	Major	After enabling external syslog servers, the primary DNS server was offline.
NIOS-73545	Major	Unable to view data on the **Data Management** > **DNS** > **Members** > **Records** tab.
NIOS-73519	Major	Under certain circumstances, DNS reports did not populate data and summary indexes in reporting were not updates on scheduled runs.
NIOS-73503	Major	The “err error fetching dhcp_range:/ for reporting event” error message was displayed in the syslog file of an IB-1420 appliance even after restarting the DHCP service.
NIOS-73465	Major	After a Grid replication, a different SOA serial number was displayed in the primary member and the secondary member.
NIOS-73463	Major	Adding Active Directory domain certificates broke the SSL chain for the WAPI endpoint.
NIOS-73420	Major	Logging in to Grid Manager on the Chrome browser using Citrix NetScaler displayed an error message.
NIOS-73392	Major	A Microsoft Azure vDiscovery job failed and the “HTTP Status Code: 400"error was displayed.
NIOS-73368	Major	A DHCP protocol violation occurred when option overload (Option 52) was required.
NIOS-73365	Major	SSH login using Active Directory credentials over the MGMT interface of the Grid member needed to be allowed when the MGMT interface of Grid Master was disabled.
NIOS-73364	Major	Under certain circumstances, a slow memory leak caused a UDPv4 possible attack.
NIOS-73318	Major	The 8.3.0 EA upgrade path and the CAA upgrade restriction had to be removed.
NIOS-73281	Major	The **Last Queried** column on **DNS** > **Zones** > **default** > **Records** tab displayed **Not Monitored** for shared records.
NIOS-73274	Major	Grid Manager restarted when the discovery conversion policy was added.
NIOS-73266, NIOS-73151	Major	Latency and traffic increased on both LAN1 and LAN2 interfaces after a hotfix installation.
NIOS-73246	Major	The NIOS documentation did not contain a note that L2 packets were dropped on the bond0 passive interface if port redundancy was enabled.
NIOS-73234	Major	A KSK rollover caused issues with LBDN records.
NIOS-73231	Major	During a Grid replication, the SOA serial number was different between the primary and secondary Grid members.
NIOS-73173	Major	PTR records were not getting resolved after being converted to host records.
NIOS-73140	Major	After applying a hotfix to a Multi-Grid Master, the status of a sub-Grid kept changing between a working status and an offline status.
NIOS-73137	Major	Unable to create a TLSA record in an unsigned zone.
NIOS-73045	Major	The DNS service restarted unexpectedly when no restart was required and no restart prompt was displayed.

NIOS-73033	Major	Under certain circumstances, the threat analytics service failed to start.
NIOS-73022	Major	The set reset_rabbitmq CLI command needed to work without logging in as a root user.
NIOS-73012	Major	The OpenSSL vulnerability CVE-2019-1551 was fixed.
NIOS-72972	Major	Under certain circumstances, the system swap space usage exceeded the critical threshold value.
NIOS-72945	Major	Non-superusers were unable to view data using the global smart folders search but could view the same data on the **Data Management** > **Devices** tab.
NIOS-72868	Major	Auto-resilvering reset the network settings thereby resulting in lost data and services on the node. It has now been enhanced to not reset networking settings.
NIOS-72844	Major	A reporting member was not generating SNMP traps.
NIOS-72849	Major	Under certain circumstances, the permanent reporting license caused problems in the TE-5005 appliance.
NIOS-72839	Major	Email notifications for inactive users were sent the next day itself instead of the time specified in the notification configuration.
NIOS-72783	Major	After a NIOS upgrade, if you tried to edit the properties of a Grid member, the "Must be a fully qualified domain name" message was displayed next to the **Host Name** field.
NIOS-72753	Major	Renaming a named ACL caused **No data** to be displayed in the **Access Control Lists** box.
NIOS-72725	Major	The restriction of preventing Grid replication for local RPZ zones needed to be removed.
NIOS-72722	Major	A host record that was locked by a super admin could be deleted by another super admin, whereas an A record could not be deleted.
NIOS-72694	Major	SNMP traps were generated incorrectly when they were triggered from the CLI.
NIOS-72637	Major	The show rpz_recursive_only command was vulnerable to a sprintf based buffer overflow.
NIOS-72616	Major	DNS latency occurred in upstream communication when a single forwarder failed.
NIOS-72584	Major	Under certain circumstances, a Grid member in an anycast pool fluctuated between online and offline status caused due to BFD (Bidirectional Forwarding Detection).
NIOS-72562	Major	DNS message compression did not take place after a NIOS upgrade.
NIOS-72520	Major	An error message was displayed when users belong with roles with limited permissions tried to edit DNS zones.
NIOS-72447	Major	The set snmptrap command used 0 as the value of the msgAuthoritativeEngineBoots and msgAuthoritativeEngineTime variables and this caused the trap receiver to drop traps.
NIOS-72443	Major	Unable to move DHCP ranges from one failover association to another using CSV import.
NIOS-72328	Major	Unable to discover VMs in an Azure vDiscovery environment.
NIOS-71447	Major	The **Unmanaged** column needed to be added to the End Host History report.
NIOS-71303	Major	Unable to log in to Grid Manager because of CSV import issues before the login.

NIOS-71199	Major	The DHCP exclusion range was not displayed on the **IP Map** tab.
NIOS-71121	Major	Unable to delete TLSA records after the HSM group went offline and was replaced by a new group.
NIOS-71004	Major	A service restart took a long time to complete in certain Grid members.
NIOS-70951	Major	Processing of discovery settings was taking a very long time in very large networks.
NIOS-70887	Major	Unable to configure the SAML authentication service and the ““An invalid value was entered” error message was displayed.
NIOS-70767	Major	Splunk API calls did not work after changing the NIOS password.
NIOS-70705	Major	After a NIOS upgrade, an IB-810 or IB-820 appliance in a Grid Master or Grid Master Candidate role needed to be displayed in amber or yellow color.
NIOS-70638	Major	After a NIOS upgrade, the reporting license usage spiked.
NIOS-70588	Major	Core files were generated and subsequent HA failovers occurred after viewing a DHCP range.
NIOS-70586	Major	Additional fields needed to be added in the database to store raw data.
NIOS-70558	Major	Secondary name servers that were made primary did not have the new SOA record.
NIOS-70491	Major	Grid Manager restarted and generated httpd core files after starting the zone signing process.
NIOS-70117	Major	Enabling DNS fault tolerant caching displayed server failure errors in the traffic capture logs.
NIOS-69810	Major	Certain ADP rules were blocking legitimate resource records because of which the connection timed out.
NIOS-69731	Major	The DHCP failover status was degraded and DHCP clients did not respond to a lease request.
NIOS-69634	Major	The timestamps of the ptop log and the syslog were different.
NIOS-69408	Major	A local RPZ zone refused queries from the LAN2 IP address of the secondary server.
NIOS-69319	Major	When DHCP exclusion ranges are added to an IP map, the boxes appear to be misaligned.
NIOS-69094	Major	An empty dhcpd.conf file was generated when performing a WAPI call to export the DHCPD configuration file.
NIOS-69049	Major	ICMP packet drops occurred on PT-2200 appliances.
NIOS-68338	Major	LBDN failed and did not respond until the DNS service was restarted.
NIOS-68208	Major	Under certain circumstances, Grid member were getting disconnected and the number of replication queues increased.
NIOS-68135	Major	The NIOS documentation did not contain a list of appliances that support auto-provisioning.
NIOS-66901	Major	When an API call to search zones to print names and comments was performed, some zones did not return comments.
NIOS-65835	Major	Swap memory gradually increased and reached up to 92% after a NIOS upgrade.

NIOS-65072	Major	The following vulnerabilities were fixed: CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, CVE-2017-14496, CVE-2017-13704
NIOS-63390	Major	A DNS outage occurred because the DNS service kept getting restarted due to a missing certificate.

ID	Severity	Summary
NIOS-78066	Minor	After a NIOS upgrade, the hardware type was incorrectly modified.
NIOS-77504	Minor	The NIOS documentation contained incorrect information about leasing IP addresses from multiple DHCP ranges.
NIOS-77322	Minor	The loopback IP address was not available for selection as the management IP address because the network range was added to **Exclude from Network Discovery** on the probe.
NIOS-77236, NIOS-77002	Minor	The NIOS documentation did not contain information that certain CLI commands fail if the password contains special characters.
NIOS-77163	Minor	Documentation for minimum disk space for vNIOS for VMware had to be added.
NIOS-76803	Minor	Logs were generated every 8 seconds instead of 600 seconds.
NIOS-76677	Minor	In the *Add CNAME Record* wizard, if you added a CNAME record, entered an alias, and then clicked Select Zone to select a different zone, the previously selected zone was prefixed to the alias.
NIOS-76477	Minor	Under certain circumstances, when a node became a passive node or a Grid Master Candidate, the “Connection refused” error message was displayed in the debug logs.
NIOS-76476	Minor	The NIOS documentation contained confusing information about uploading CA certificates versus uploading HTTPS certificates.
NIOS-76396	Minor	Under certain circumstances, performing a global search for certain domains displayed an error message.
NIOS-76283	Minor	Network Insight pushed a few public networks to IPAM even after the **Disable discovery networks not in IPAM** option was enabled.
NIOS-76131	Minor	The NIOS documentation did not contain the host name and IP address of the Grid Manager in the output of the show status CLI command.
NIOS-75533	Minor	The **Failure** counter of the DNS Statistics widget did not work as expected.
NIOS-75494	Minor	The UI text in the **Health Monitors** > **Advanced** > **CONSOLIDATED HEALTH MONITOR SETTINGS** screen had to be updated.
NIOS-75431	Minor	The CVE-2020-13817 vulnerability was fixed.
NIOS-75375	Minor	The NIOS documentation erroneously mentioned the existence of a **TEST GSS-TSIG** button in Grid Manager.
NIOS-75265	Minor	The NIOS documentation did not have clear information about the IPMI/LOM port operation speeds.
NIOS-75170	Minor	In a WAPI call, the search field FQDN for dtc_lbdn did not return expected results.
NIOS-75097	Minor	The NIOS 8.5.1 and 8.4.7 Release Notes did not document TR-800 as a supported model.
NIOS-75084, NIOS-74990	Minor	Certain vulnerabilities were detected after a vulnerability scan.

NIOS-74997	Minor	The NIOS documentation did not contain detailed information about the **Events per Second per Rule** field.
NIOS-74945	Minor	The NIOS 8.5.x Release Notes did not contain information about the limitation of running DNS Forwarding Proxy on IB-100, IB-810, IB-820, IB-V810, and IB-V820 appliances.
NIOS-74900	Minor	Certain IPAM data caused high load on Grid Master.
NIOS-74890	Minor	WAPI calls requesting the DHCP failover association status worked when sent to Grid Master but not when sent to the Grid Master Candidate.
NIOS-74855	Minor	The show network command displayed duplicate IP addresses.
NIOS-74832	Minor	TR-800 was not listed as a supported appliance is the NIOS 8.5.0 and 8.4.7 Release Notes.
NIOS-74674	Minor	In a Multi-Grid Master setup, after upgrading the master Grid followed by the sub-Grid, the sub-Grid was in an offline status.
NIOS-74491	Minor	The SNMP scan attempted to connect to a subnet that was SNMP disabled.
NIOS-74439	Minor	The trap description for “DNS service is in warning state” needed to be modified in the NIOS documentation.
NIOS-74412	Minor	An upgrade check for Docker bridge network conflict needed to be performed.
NIOS-74387	Minor	BIND version 9.11.18 reported a security issue.
NIOS-74074	Minor	In Network Insight, the end hosts did not display model and version information. Also some of the end hosts displayed fingerprints as disabled whereas this option was enabled in the discovery network.
NIOS-74072	Minor	The scrape and resilver CLI commands were not maintenance mode commands.
NIOS-74056	Minor	The NIOS documentation did not contain information about the change in behavior when threat protection is enabled.
NIOS-73984	Minor	The NIOS documentation did not contain information about the maximum file size while uploading a file.
NIOS-73816	Minor	ActiveTrust Cloud was not replaced by BloxOne Threat Defense Cloud in the NIOS online help.
NIOS-73682	Minor	After a NIOS upgrade, a Grid member reported errors in DNS Cache Acceleration configuration.
NIOS-73329	Minor	Under certain circumstances, the Indiana (east) time zone did not work.
NIOS-73287	Minor	The NIOS documentation incorrectly stated that an appliance selects the IP address of another candidate and sends it a ping.
NIOS-72950	Minor	Logging in to NIOS as a user belonging to the LDAP authentication group displayed an LDAP error message.
NIOS-72920	Minor	Adding an AFXR record using Grid Manager did not work.
NIOS-72478	Minor	CLI commands to collect network interface statistics and support bundle data were required.
NIOS-72177	Minor	The PDF format of the reporting online help was not formatted and was difficult to read.
NIOS-71446	Minor	Logging data for Network Insight with respect to license and interface utilization needed to be increased.

NIOS-71010	Minor	When DNS response logging was enabled, long responses were split to multiple lines and were not displayed properly.
NIOS-70691	Minor	An RPZ configured to block data did not work when DNS64 was enabled.
NIOS-70311	Minor	Unable to remove an empty DNS view.
NIOS-70137	Minor	The restart banner at the top of Grid Manager was always displayed even though there were no pending changes.
NIOS-70136	Minor	The VLAN option was not available as an extensible attribute in the *DTC (Grid DNS Properties)* > **Traffic Control** > **Basic** screen.
NIOS-69246	Minor	Adding a fixed address using the **Add Fixed Addresses** task on the Grid Manager dashboard did not add IPv4 filters configured in the template.
NIOS-65208	Minor	Unable to remove a Microsoft server that has a CNAME record in its label.
NIOS-65064	Minor	Editing custom forwarders on a forward zone did not work.

Severity Levels

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

Known General Issues

ID	Summary
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-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-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-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-81393	If you enable and then disable auto-consilidated monitors, the log files generate the “transfer rabbit messages failed” message several times.
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.
NIOS-78854	Under rare circumstances, when upgrading to NIOS 8.6.0, the status of DNS Forwarding Proxy may become "NIOS/DFP service is stopped by user". Infoblox recommends that you start the DNS Forwarding Proxy service from Grid Manager to resume queries to BloxOne Threat Defense.
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, user will 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 ACLs, and selecting the **Update DNS on DHCP Lease Renewal** check box may prevent DNS scavenging from working properly.
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-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 “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-73162	Deduplication does not work for Cisco APIC fabric devices previously added as regular network devices.
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 IB-FLEX 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. **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.
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 is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empowerorganizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com