NIOS 8.5.5 Release Notes

NIOS 8.5.5 Release Notes

INTRODUCTION

Infoblox NIOS™ 8.5 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.

SUPPORTED PLATFORMS

Infoblox NIOS 8.5.*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-4000, ND-4005
- Network Insight Virtual Appliances: IB-V805, IB-V1405, IB-V2205, IB-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, GCP, and Oracle Cloud Infrastructure: IB-V825, IB-V1425, IB-V2225, CP-V805, CP-V1405, CP-V2205

The following appliances are supported only when you upgrade to NIOS 8.5 from an earlier version. They are **not** supported on a new NIOS 8.5 installation:
ND-V800, ND-V1400, ND-V2200, TE-V810, TE-V820, TE-V1410, TE-V1420, TE-V2210, TE-V2220, TR-V2200, IB-V4010, IB-V4020, TE-V800, TE-V1400, TE-V2200, CP-V800, CP-V1400, and CP-V2200.

NOTE: Using NIOS on appliances supported but not available for purchase or on appliances supported only when you upgrade may result in a performance degrade.

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

NOTE: DNS forwarding proxy is not supported on any appliance that is running on a memory lower than 4 GB.

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 versions 7.0, 6.7, 6.5.x, 6.0.x installed, and then configure it as a virtual appliance.

  vSphere vMotion is also supported. You can migrate vNIOS virtual appliances from one ESX or ESXi server to another without any service outages. The migration preserves the hardware IDs and licenses of the vNIOS virtual appliances. VMware Tools is automatically installed for each vNIOS virtual appliance. Infoblox supports the control functions in VMware Tools. For example, through the vSphere client, you can shut down the virtual appliance. You can deploy certain vNIOS virtual appliances with different hard disk 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 2012 R2, 2016, 2019 Hyper-V**
  The Infoblox vNIOS virtual appliance is now available for Windows Server 2019, Windows Server 2016, and 2012 R2 that have DAS (Direct Attached Storage). Administrators can install vNIOS virtual appliance on Microsoft Windows® servers using either Hyper-V Manager or SCVMM. A Microsoft Powerscript is available for ease of installation and configuration of the virtual appliance. Note that 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 Red Hat OpenStack 16.0, Rocky RHOSP 14 (Red Hat Enterprise Linux 7.6), Queens RHOSP 13 (Red Hat Enterprise Linux 7.6), Newton RHOSP 10 (Red Hat Enterprise Linux 7.4), and Stein PackStack (Red Hat Enterprise Linux 7.6) 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. For more information about vNIOS for Azure, refer to the *Infoblox Installation Guide for vNIOS for Microsoft Azure*.

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

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

- **vNIOS for 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 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*.

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

NOTE: Deploying vNIOS on Xen Hypervisor is not supported, but you can upgrade from earlier versions to 8.3 and then upgrade to 8.5.*x*.

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 AHV	NIOS for Red Hat OpenShift	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]	×	×	×	Yes
IB-V4025 **	250	14	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 Azure, AWS, GCP	NIOS for Nutanix AHV	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 Azure, AWS, GCP	NIOS for Nutanix AHV	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 Azure, AWS, GCP	NIOS for Nutanix AHV	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.

** 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.

[1] NIOS for KVM is supported in the following environments: OpenStack, RHEL, SUSE Enterprise and Cloud, and CentOS.
[2] NIOS for AWS is supported on IB-V4025 from NIOS 8.5.2 onwards.

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.

NEW FEATURES

This section lists new features in the 8.5.*x* releases.

NIOS 8.5.5

Displaying the Correct Cloud Platform Types (RFE-11596)
The **Grid Manager** > **Members** tab now displays two new columns: **Host Platform** and **Hypervisor**. These columns respectively display the platform or the virtual platform on which NIOS is running and the hypervisor of the appliance.

The values of the host platform and hypervisor are also displayed in the output of the `show hardware-type` CLI command.

IPv6 Support for Subscriber Services (RFE-10975)
Subscriber services now support IPv6 address types. You can now run subscriber services and send RADIUS message communication on IPv4, IPv6, and dual-mode (IPv4+IPv6) devices. NIOS now also supports proxy API calls and expire profile API calls over IPv6 to MSPs and SPMs respectively. However, the MSP/SPM in version 9.2.1.0 do not yet support IPv6.

Support for SafeNet Luna SA 7 (RFE-10477)
NIOS now supports SafeNet Luna SA 7 devices.

NIOS 8.5.4

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

NIOS 8.5.3

DHCPv6 Option Filters (RFE-9401)
You can now configure DHCPv6 option filters using the **Data Management** > **DHCP** > **Filters** > **IPv6 Option Filter** option. The **Filters** tab now displays the filter type and you can associate DHCPv6 option filters with these IPv6 objects: IPv6 networks, IPv6 ranges, IPv6 network containers, IPv6 shared networks, IPv6 fixed addresses, IPv6 network templates, IPv6 range templates, IPv6 fixed address templates, Grid DHCP, and member DHCP properties. For more information, see “Configuring Option Filters” topic in the NIOS 8.5 online documentation.

NAC Authentication Messages in Syslog (RFE-10028)
Network Access Control or RADIUS messages related to DHCP authentication are now part of syslog logging.

Bypass Subscriber Services (RFE-10709)
The `set subscriber_secure_data bypass` and the `show subscriber_secure_data bypass` commands now contain the following new parameters:

- `grid`: Enables or disables the subscriber service policies bypass for all members of each site on the entire Grid.
- `site`: Enables or disables the subscriber service policies bypass for all members of a site.

The earlier parameters such as `on`, `off`, and `dca` have been deprecated. For more information about the syntax, arguments, and examples of these commands, see the “set subscriber_secure_data bypass” and the “show subscriber_secure_data bypass” topics in the NIOS 8.5 online documentation.

Multi-Grid Master and Sub Grid Synchronization (RFE-7653)
You can now configure the way in which Multi-Grid Master gathers updates from its connected sub Grids. You can choose the communication mode of the Master Grid to be sub Grid initiated or MGM initiated. If you choose sub Grid initiated, the sub Grid initiates the connection request to join Multi-Grid Master and synchronization takes place from the sub Grid to the Multi-Grid Master and from the Multi-Grid Master to the sub Grid. If you choose MGM initiated, Multi-Grid Master initiates the connection request to the sub Grid and it also initiates the synchronization request regularly with the sub Grids that are already joined.

For more information about the communication modes, see the *Multi-Grid Manager Administrator Guide* at https://docs.infoblox.com

ACL for DNS Domains (RFE-6181)
You can now add, update, or delete an allow query domain ACL for the domain of a DNS view. Allow query domain is an ACL that allows or denies a client request for query access to a domain. The following new CLI commands have been introduced:

- `set allow_query_domain`: Adds, updates, or deletes an allow query domain ACL for the domain of a DNS view.

- `show allow_query_domain`: Displays the list of all domain names in the DNS view specified or its default DNS view.
- `show allow_query_domain_views`: Displays the list of DNS views that have allow query domain ACLs configured.

For more information about the syntax, arguments, and examples of these commands, see the "set allow_query_domain", "show allow_query_domain", and "show allow_query_domain_views" topics in the NIOS 8.5 online documentation.

Defining the NTP Orphan Mode (RFE-11096)
Grid members including the Grid Master can now function as NTP servers to clients if NTP is enabled on the Grid. You can even configure a stratum value that enables Grid members to continue serving NTP uninterruptedly using the disconnected NTP service in the absence of external NTP servers. This mode is called the orphan mode. When the external NTP servers are reachable again, the Grid connects to the server to serve NTP and derive the NTP stratum values and automatically switches to the connected mode.

For more information about the orphan mode, see the "Configuring Orphan Mode" and the "Using NTP for Time Settings" topics in the NIOS 8.5 online documentation.

vNIOS for Red Hat OpenShift (RFE-10707)
vNIOS is now supported on the Red Hat OpenShift platform. For more information, see the *Infoblox Installation Guide vNIOS for Red Hat OpenShift* at https://docs.infoblox.com

Deploying vNIOS instances Using Managed Disks in Azure (RFE-8690)
You can now deploy NIOS instances on Microsoft Azure using managed disks. For more information see the *Infoblox Installation Guide vNIOS for Microsoft Azure* at https://docs.infoblox.com

Microsoft Server 2019 Support (RFE-10227)
NIOS 8.5.3 is supported on Microsoft Windows Server 2019.

NIOS 8.5.2

DNS Over HTTPS (RFE-9826)
You can now avoid DNS query spoofing and eavesdropping by using the newly introduced DNS over HTTPS service. When you enable the DNS over HTTPS feature, DNS traffic is encrypted through the HTTPS protocol to prevent eavesdropping and tampering of DNS data. You can enable this feature by selecting the **Enable DoH Service** check box. This check box is present in the *Member DNS Properties* editor, **Toggle Advanced Mode** > **Queries** tab.

You can also view the status, configuration, and details of the DNS over HTTPS service by using the following new commands:

- `show doh-status`: Displays the status of the DNS over HTTPS service.
- `show doh-config`: Displays the DNS over HTTPS configuration and includes DNS over HTTPS servers that are listening on port 443.
- `show doh-stats`: Displays statistics such as active HTTPS sessions and number of queries or responses received or sent over HTTPS.

NIOS appliances must have the required base memory configuration for the DNS over TLS and the DNS over HTTPS features to be displayed. For information about the required memory footprint, see the "Base Configuration Requirements" section in the "Configuring DNS over TLS and DNS over HTTPS Services" topic in the NIOS 8.5 online documentation.

For detailed information about the appliances that support DNS over HTTPS, limitations, and configuration, see the “Configuring DNS over TLS and DNS over HTTPS Services” topic in the NIOS 8.5 online documentation. For information about the commands, see the “show doh-status”, “show doh-config”, and “show doh-stats” topics.

DNS Over TLS (RFE-6979)
NIOS appliances that support vDCA or vADP now include the DNS over TLS capability that helps increase DNS security and privacy. When you enable the DNS over TLS feature, DNS traffic is encrypted through the TLS protocol to prevent eavesdropping and tampering of DNS data. You can enable this feature by selecting the select the **Enable DoT Service** check box. This check box is present in the *Member DNS Properties* editor, **Toggle Advanced Mode** > **Queries** tab.

You can also view the status, configuration, and details of the DNS over TLS service by using the following new commands:

- `show dns-over-tls-status`: Displays the status of the DNS over TLS service.
- `show dns-over-tls-config`: Displays the DNS over TLS configuration and includes DNS over TLS servers that are listening on port 853.
- `show dns-over-tls-stats`: Displays statistics such as active TLS sessions and number of queries or responses received or sent over TLS.

NIOS appliances must have the required base memory configuration for the DNS over TLS and the DNS over HTTPS features to be displayed. For information about the required memory footprint, see the “Base Configuration Requirements” section in the “Configuring DNS over TLS and DNS over HTTPS Services” topic in the NIOS 8.5 online documentation.

For detailed information about the appliances that support DNS over TLS, limitations, and configuration, see the “Configuring DNS over TLS and DNS over HTTPS Services” topic in the NIOS 8.5 online documentation. For information about the commands, see the “show dns-over-tls-status”, “show dns-over-tls-config”, and “show dns-over-tls-stats” topics.

Proxying RPZ Passthru Rules (RFE-9982)
You can now proxy RPZ passthru rules for parental control through a configured MSP (Multi-Services Proxy) server by selecting the newly introduced **Proxy RPZ Passthru** check box. If you select this check box, and a passthru rule from any RPZ zone is hit, then the query resolves to an MSP proxy virtual IP address and NIOS generates a "synthetic resolution”. If you do not select this check box, the query resolves normally.
Note: If an RPZ passthru rule is triggered and the **Proxy RPZ Passthru** check box is selected, queries are proxied to the MSP (Multi-Services Proxy) server only if the passthru rule is not blocked by other policies (for example, blacklist, whitelist, parental control) in NIOS.

For more information, see the “Scaling Using Subscriber Sites” topic in the NIOS 8.5 online documentation.

Changing the Default Password During the First Login for Standalone AWS Members (RFE-10280)
For an AWS standalone member, NIOS now displays the **New Password** and **Retype Password** fields when you log in for the first time. You must change the default password. For more information, see the “xxx” topic in the NIOS 8.5 online documentation.

Key Pair Authentication for CLI Access (RFE-7968)
To prevent CLI login failures after upgrade, you must enable the **Use AWS SSH authentication keys** option for each user that needs CLI access to AWS appliances. When you select the **Use AWS SSH authentication keys** option, you can either select the **Key pair** option to gain access to the CLI without entering a password or the **Key pair + password** option to gain access after entering a password and uploading the SSH public key. You can upload the public key using the **Manage SSH Public Keys** field. For more information, see the “Creating Local Admins” topic in the NIOS 8.5 online documentation.

vNIOS Support for Oracle Cloud Infrastructure (RFE-10643)
You can now deploy the NIOS virtual appliance on Oracle Cloud Infrastructure. You can deploy an Infoblox vNIOS for Oracle Cloud Infrastructure instance as a virtual cloud member tied to an on-premise (non-cloud) NIOS Grid. The NIOS virtual appliance for Oracle Cloud Infrastructure functions as a hardware virtual machine guest on the Linux system. For more information about vNIOS for Oracle Cloud Infrastructure, see the *Infoblox vNIOS for Oracle Cloud Infrastructure Installation Guide* at docs.infoblox.com

vNIOS for AWS Support for IB-V4025 (RFE-10374)
You can now deploy vNIOS for AWS instances with IPv4 and IPv6 addresses. However, Infoblox provides support for IPv6 network connectivity only on the IB-V4025 appliance.

Service-Level Black and White Lists (RFE-9981)
The allowed and blocked listing feature allows you to specify well-known names (for example, “linkedin” or “netflix”) for well-known domain names. For information about the rules that are applied if a dotless name is the allowed list or blocked list, see the “Scaling Using Subscriber Sites” topic in the NIOS 8.5 online documentation.

Enabling Parental Control Subscriber Policies Through DNS Cache Acceleration (RFE-9980)
This release of NIOS introduces parental control at DNS Cache Acceleration using cached domain and subscriber data. To this effect, the following new check boxes have been added on the **Parental Control** > **Advanced** tab:

- **Enable DCA subscriber Query count logging**: Select this check box to use DNS Cache Acceleration to generate subscriber logs and to record query counts greater than or equal to zero.
- **Enable DCA subscriber Allowed & Blocked list support**: Select this check box to use DNS Cache Acceleration to provide the blocked and allowed list of subscribers.

The following new CLI commands have been introduced:

- `show subscriber_secure_data bypass`: Allows you to view the status of the subscriber data bypass for a member.

- `set subscriber_secure_data bypass`: Bypasses subscriber service policies at the local cache and DNS Cache Acceleration (when available).
- `show subscriber_secure_data garbage_collect`: Displays the status of garbage collection for the specific member
- `set subscriber_secure_data garbage_collect`: Designates the specific member for the garbage collection service.

A new report called Query Count Details by Subscriber ID is generated at every DNS Cache Acceleration subscriber cache update. It is based on the query counter per subscriber ID.

For more information about these check boxes, see the “Scaling Using Subscriber Sites” topic in the NIOS 8.5 online documentation. For more information about the CLI commands, see the “show subscriber_secure_data bypass”, “set subscriber_secure_data bypass”, “show subscriber_secure_data garbage_collect” and the “set subscriber_secure_data garbage_collect” topics.

NIOS appliances require additional memory if you intend to run Parental Control features such as proxy RPZ passthru, DNS Cache Acceleration subscriber query count logging, and DNS Cache Acceleration subscriber allowed and blocked listing simultaneously. For information about memory requirements, see the “Configuration Requirements if Parental Control is Enabled” section in the in the “Configuring DNS over TLS and DNS over HTTPS Services” topic in the NIOS 8.5 online documentation.

Extensible Attribute Support for VLAN and DNS Objects (RFE-10056)

This release of NIOS introduces the following extensible attribute inheritance chain:

- Network view > DNS view > Network > Zones (including response policy) > Subzone or Resource Record
- VLAN view > VLAN range or static VLAN

For more information, see the "Managing Extensible Attributes" topic in the NIOS 8.5 online documentation.

Enabling and Disabling the FIPS Mode

You can now enable or disable the FIPS mode in NIOS. You can enable or disable the FIPS mode on a Grid Master, a standalone system, or on the active Grid Master node in a HA setup. In an HA setup, you can set the FIPS mode only on the standalone Grid Master node and then form an HA pair. You cannot change the setting on the HA Grid Master or HA Grid member. For more information see, the "Enabling/Disabling the FIPS Mode" topic in the NIOS 8.5 online documentation.

New CLI Commands 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 8.5 online documentation.

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

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

Caching Threat Category Information from the Cloud Services Portal (RFE-9249)

You can configure the Cloud Services Portal and and schedule the entire threat indicator database download from the Cloud Services Portal. The threat category information is then sent to the reporting server to augment RPZ hits and reports are generated. Caching threat category information from the Cloud Services Portal helps enhance the performance of threat reports as data is fetched from the cache that is stored locally.

You can also download incremental updates from the threat indicators of the Cloud Services Portal. The incremental threat indicator is downloaded only after the whole threat indicator is downloaded from the Cloud Services Portal.

You can configure threat indicator caching by using the **Threat Indicator Caching** > **Basic** tab in the *Grid Reporting Properties* editor. For more information, see the "Grid Reporting Properties" topic in the NIOS 8.5 online documentation.

New Supported Cisco ISE Version

NIOS now supports the integration of Cisco ISE versions 2.6 and 2.7. For information about integrating NIOS with Cisco ISE, see the "Cisco ISE Integration" topic in the NIOS 8.5 online documentation.

NIOS 8.5.1

Additional Validation on Host Names (RFE-7507)

You can now enable or disable additional validation on host names when creating zones, subzones, and records of type A, AAAA, host record, ALIAS, CAA, MX, and NS. The following new CLI commands have been introduced to enable or disable the additional validation:

- `set extra_dns_name_validations`: Enables or disables additional DNS name validation.
- `show extra_dns_name_validations`: Displays the status of the additional DNS name validation.

Additional validation is disabled by default. For more information about these commands, see the "set extra_dns_name_validations" and "show extra_dns_name_validations" topics in the NIOS 8.5 online documentation.

High Performance Query Logging (RFE-7747)
You can now use the dnstap log format to achieve performance query logging. NIOS logs all valid DNS queries and responses that are not dropped by Advanced DNS Protection. You can configure high performance query logging by using the **Logging** tab in the *Grid DNS Properties* or *Member DNS Properties* editor.

The following new commands have been introduced to configure the use of dnstap:

- `set enable_dnstap`: Enables or disables using dnstap to log DNS queries and responses.
- `show dnstap-status`: Displays the status of the dnstap configuration.
- `show dnstap-stats`: Displays the statistics of the dnstap configuration.

For information about configuring high performance query logging, see the "Capturing DNS Queries and Responses" topic in the NIOS 8.5 online documentation. For information about the new commands, see the "set enable dnstap", "show dnstap-status", and "show dnstap-stats" topics in the NIOS 8.5 online documentation.

Support for More Intel NICs (RFE-8677)
NIOS now supports SR-IOV Virtual Function drivers for Intel® Ethernet Controller XL710 and Intel Ethernet Network Adapter XXV710 NICs. These NICs are supported on KVM platforms.

Configuring the edns-udp-size and max-udp-size Attributes (RFE-4795)
You can now configure the edns-udp-size and max-udp-size attributes by entering byte values in the **EDNS0 Buffer Size** and **UDP Buffer Size** fields in the *Grid DNS Properties/Member DNS Properties/DNS View* > **General** > **Advanced** tab. The minimum and maximum values of both these attributes are 512 and 4096 respectively. By default, the buffer size is set to 1220 bytes. For information about configuring these attributes, see the "Using Extension Mechanisms for DNS (EDNS0)" topic in the NIOS 8.5 online documentation.

Configuring Root Name Server Inheritance (RFE-10347)
You now have the option to configure whether customized root name servers must apply only to the default DNS view or to all DNS views. You can do this using the **Applies to default DNS view only** and the **Applies to all DNS views on this member** options in *Member DNS Properties* > **Root Name Servers** > **Basic** tab.

Capturing CSV Errors After NetMRI Synchronization (RFE-9097)
After an IPAM synchronization in NetMRI, CSV import errors if any are now logged in a separate file named discovery_csv_error.log.*xxxxxx* located at /infoblox/var/discovery_csv_error

Collecting NIOS Database Performance Data (RFE-9550)
You can now download Ptop log files that comprise database metrics which you can use to determine the health of the NIOS database and baseline its performance. Based on the database performance, you can ascertain the impact of changes such as adding a Grid member or enabling features such as Grid replication for DNS zones or multi-master DNS, on the database performance. You can download the Ptop log files by using a WAPI call. For more information, see the "Collecting Database Performance Data" topic in the NIOS 8.5 online documentation.

Adding TLSA Records in Unsigned Zones (RFE-10324)
You can now add TLSA records in both DNSSEC signed zones or unsigned zones.

NIOS 8.5.0

Infoblox Customer Experience Improvement Program

The Infoblox Customer Experience Improvement program is an alert feature that sends encrypted network infrastructure and product usage data to Infoblox on a periodic basis. Infoblox uses this data to improve product functionality and to provide better customer service.

The *Infoblox Customer Experience Improvement Program* screen is displayed only when you login for the first time. You can choose whether or not you want to participate in the program. You can configure the Infoblox Customer Experience Improvement program on the **Grid Properties** > **Edit** > **CSP Config** > **Advanced** tab.

vDCA Support on 22x5 and 40x5 Appliances (RFE-9242)

vDCA is now supported on the IB-2215, IB-2225, IB-V2215, IB-V2225, IB-4015, IB-4025, IB-V4015, and IB-V4025 appliances. For more information, see the “Configuring DNS Cache Acceleration” topic in the NIOS 8.5 online documentation.

CSV Import for Subscriber Records (RFE-8672)

You can now import subscriber site data by using the **CSV Import** option and export subscriber site data by using the **Export Subscriber Data** option. However, you cannot perform merge, custom, and replace operations for subscriber records. For information about supported object types for subscriber records and their corresponding fields for CSV import and export, see the “Subscriber Record” topic in the NIOS 8.5 online documentation.

You can also add, update, and delete subscriber records using NIOS APIs. For more information, see the NIOS WAPI documentation.

Scalable Installer Image on IB-FLEX (RFE-7533)

The NIOS 8.5 installer image files are available in the following two variants:

- Default image files of size 250 GB
- Resizable files of size 68 GB. You can resize these images depending on your requirement and deployment. You can resize up to a maximum of 2.5 terabytes.

For more information, see the “Installing NIOS” topic in the NIOS 8.5 online documentation. For limitations about the scalable installer image, see the “Limitations of Using the Scalable Image File” section in the “Installing NIOS” topic.

vNIOS Support on Nutanix AHV (RFE-7970)

vNIOS is now supported on the Nutanix AHV platform. For more information, see the vNIOS on Nutanix AHV documentation at https://docs.infoblox.com

Infoblox IPAM Driver for Terraform (RFE-7614)

NIOS is now supported on Infoblox IPAM Driver for Terraform version 1.0. For installation details, see the Infoblox IPAM Driver for Terraform online documentation at https://docs.infoblox.com

Splunk Upgrade (RFE-9484)

NIOS 8.5 now works with the upgraded Splunk version 7.2.6.

DHCP Support for Subscriber Policy (RFE-8538)

You can now use extensible attributes to populate the subscriber cache with subscriber policies. Fixed addresses, reserved addresses and networks can use extensible attributes to add a subscriber policy during creation and remove the subscriber policy when they are removed. Supported extensible attributes are Subscriber-Secure-Policy, Parental-Control-Policy, PC-Category-Policy, User-Name, Proxy-All, Black-List and

White-List. The DHCP member serving subscriber services must belong to a single subscriber secure site. This feature is not supported when the **Allow NATed Subscribers only** option is enabled in the subscriber site.

New Dashboard Reports
This release of NIOS introduces the following new reports:

- DNS QPS Usage Report: Displays the five-day rolling average of the total peak DNS queries per second calculated for all Grid members.
- IP Address Usage Report: Displays the five-day rolling average of peak values of the total count of IP addresses aggregated across all networks in the Grid.
- DHCP LPS Usage Report: Displays the five-day rolling average of the total peak DHCP leases per second calculated for all Grid members.

For more information, see the “DNS Dashboards”, “IPAMv4 Utilization Dashboards”, and “DHCP Dashboards” topics in the NIOS 8.5 online documentation.

Configuring LAN1/LAN2 for Automated Failover (RFE-9114)
LAN1 and LAN2 interfaces both support DNS recursion in such a way that if the default route interface goes down, the route redundancy feature removes the failed interface so that there is automatic failover of recursion traffic. This provides for a seamless flow of recursive traffic movement.
You can configure automated failover by selecting the **Enable default route redundancy on LAN1/LAN2** check box on the **Network** tab of the *Grid Member Properties* editor. For more information, see the “Using the LAN2 Port” topic in the NIOS 8.5 online documentation.

New Match Rule Filters for Outbound ObjectChange Events
This release of NIOS introduces two new rule filters in the **Match the following rule** section when you add notification rules. The new filters are Username and Usergroup. These filters are applicable only to the ObjectChange events.

New Cisco ISE Endpoint (RFE-9236)
You can now add a Cisco ISE endpoint using the **Grid** > **Ecosystem** > **Outbound Endpoint** > **Add Cisco ISE Endpoint** option. For more information, see the “Configuring Outbound Endpoints” topic in the NIOS 8.5 online documentation.

HA Support for Outbound Notifications
NIOS now provides HA support and performs a failover to a standby node without loss of data when a large number of Outbound events is triggered.

Support for Bulk CSV Operations (RFE-8789)
NIOS 8.5 supports bulk CSV operations for heavy loads of DBChange objects.

Testing the Grid Master Candidate Connection Before Promotion (RFE-1737)
You can now test the connection and also schedule a test connection of the Grid Master Candidate with the other Grid members before promoting it to Grid Master. You can do this either by using the **GMC Promote Test** option on the Grid Manager or by using the NIOS CLI.

The following new commands have been introduced to test the connection:

- `show test_promote_master`: Enables you to view the results of the test promotion of a Grid Master Candidate to Grid Master.
- `set test_promote_master`: Enables you to check whether the Grid Master Candidate is connected to the rest of the Grid members.

You need the new ADP ruleset version to use this feature. For information about the **GMC Test** option, see the “Managing a Grid” topic in the NIOS 8.5 online documentation. For information about the CLI commands, see the “show test_promote_master” and the “set test_promote_master” commands.

SSH CLI Access to Non Super Users (RFE-504)
Super users can now give SSH and CLI access to non-super users by selecting the **CLI** option in the **Allowed Interfaces** section of *Admin Group Wizard*. For more information, see the “About Admin Groups” topic in the NIOS 8.5 online documentation.

Faster Refresh Rates for DNS Traffic Control Status Updates (RFE-6258)
DNS Traffic Control status updates are now refreshed every 10 seconds compared to the earlier refresh rate of 2 minutes. Therefore, you can now view the latest DNS Traffic Control update every 10 seconds.

Selecting NOERROR/NODATA or NXDOMAIN as a Response (RFE-7113)
You can now select **NOERROR/NODATA** or **NXDOMAIN** as a **Destination/Response** option when configuring a topology ruleset for destination types other than pools or servers. For more information, see the “Configuring Topology Rules and Rulesets” topic in the NIOS 8.5 online documentation.

Increase in the DNS Traffic Control Scale (RFE-8771)
DNS Traffic Control now is more scalable and supports more numbers of DTC objects and health monitors.

Increase in the DNS Traffic Control Persistency (RFE-9150)
You can now enter a value up to 2 hours in the **Persistence** field of the *DTC LBDN* wizard. This has been increased from the maximum persistence value of 30 minutes in earlier releases.

DNS Forwarding Proxy as a Service (RFE-9137)
DNS Forwarding Proxy is now a NIOS service called DFP and automatically handles DNS query forwarding. You can start and stop the DFP service just like other NIOS services. You can configure the connection between NIOS and BloxOne Threat Defense Cloud Services Portal by using the new **CSP Config** tab in *Grid Properties Editor* or *Grid Member Properties Editor*. For more information, see the Using Forwarders topic in the NIOS 8.5 online documentation.

NIOS Grid Connector
NIOS 8.5 enables the BloxOne DDI NIOS Grid Connector that allows you to view NIOS Grid DHCP and IPAM data from the SaaS based Infoblox Cloud Services Portal. You can configure access to Cloud Services Portal in NIOS through the **CSP Config** tab in the *Grid Properties* editor. The NIOS Grid Connector service is then configured using the Cloud Services Portal GUI. Viewing the NIOS Grid Connector in the Cloud Services Portal requires BloxOne DDI licensing using BloxOne DDI 2.3 or later.

Discovery of SDN and SD-WAN Devices
You can now discover SDN and SD-WAN devices from Cisco ACI and Cisco Meraki using Network Insight. For more information, see the “Configuring Discovery Properties” topic in the NIOS 8.5 online documentation.

Enabling or Disabling RPZ Logging (RFE-7574)
You can now enable or disable RPZ logging for an RPZ zone by using the **RPZ logging** check box on the **Logging** tab of the Response Policy Zone editor. For more information, see the “Managing RPZs” topic in the NIOS 8.5 online documentation.

Inheritance Permissions for Host Objects Not Enabled in DHCP and DNS (RFE-9521)
You can now apply permissions to a network and have those permissions inherited by a host object that is not enabled in DHCP and DNS.

NAT Port as IPSD (RFE-9527)
This release of NIOS supports CGNAT (Carrier Grade NAT). Multiple subscribers share the same public IP address. In specific NATing algorithms that use port block (known port range allocation), the IP address and the first usable port (which is a new AVP called Deterministic-NAT-Port) for the subscriber are provided in a

RADIUS accounting AVP. You can select this AVP from the **IP Space Discriminator** drop-down list. For more information, see the “Scaling Using Subscriber Sites” topic in the NIOS 8.5 online documentation.

Searching Host by IP Addresses or Networks (RFE-9231)
You can now search for hosts by IP addresses or networks using the NIOS API. For more information, see the NIOS WAPI documentation.

Viewing CPU Utilization and Top N Processes (SPTYRFE-18)
You can now monitor the top number of processes and the CPU utilization of all individual CPU cores in the *System Activity Monitor* widget. You can either track the live CPU utilization data or you can view the CPU utilization data for up to a maximum of the past 60 minutes based on the time range you specify. You can also determine the frequency with which the Ptop tool must run and collect data and also configure the number of top processes to be displayed. For more information, see the “Status Dashboard” topic in the NIOS 8.5 online documentation.

You can configure the number of top processes and the Ptop interval only for the Grid Master. It is mostly for use of the Infoblox Technical Support team.

CHANGES TO DEFAULT BEHAVIOR

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

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, 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, subscriber data replication happens through IPv6 for dual mode by default.

- In NIOS 8.5.5 parental control can be enabled on IPv6-only devices.

- NIOS 8.5.5 requires the ruleset engine version 13 for parental control.

- In NIOS 8.5.5, 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, 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, the **Platform** column in the **Grid Manager** > **Members** tab has been renamed to **Host Platform**.

- In NIOS 8.5.5, 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, you cannot add, update, or delete the following subscriber site attributes: policy management addresses, content proxy addresses, NAS gateways.

- In NIOS 8.5.3 and later, 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 8.5.3 and later, 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 filters were configured. NIOS 8.5.3 corrects this, requiring all configured class filters to match before a lease is granted. This description presumes that all filters are configured to grant lease when the filter matches the client's request. Note that if any of the filters is configured to grant lease when the filter matches the client's request and the match fails, the lease will be denied regardless of the result of any of the other filters. Similarly, if any class filter is configured to deny lease and the filter matches the client's request, the lease will be denied. A deny result always takes precedence over any other filter result.

- In NIOS 8.5.3 and later, the **Data Management** > **DHCP** > **IPv4 Filters** menu item has been renamed to **Filters**.

- In NIOS 8.5.3 and later, 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.

- In NIOS 8.5.3 and later, 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.

- 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 and later, 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.

- In NIOS 8.5.3 and later, the OpenSSH server process `sshd` is binding only to primary interfaces. Additional interfaces like VLANs, loopback addresses are restricted.

- If you are using threat analytics, you must have installed the minimum module set version (20210620) before upgrading to NIOS 8.5.3 or later.

- In NIOS 8.5.3 and later, the `certificate_usage`, `matched_type`, and `selector` fields are mandatory. Therefore, you must specify these through WAPI when adding TLSA records.

- In NIOS 8.5.3 and later, 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 8.5.3 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: . - _ / ! @ ^ + % , :

- The value of PLATFORM_NAMED_MAX_CACHE_SIZE for the IB-2215 and IB-2225 platforms has been increased from 2048 to 12288.

- For NIOS 8.5.2 and later, when you change the member assignment of DHCP ranges from a failover association to a Grid member and then back to failover association, leases in the primary and secondary server fall out of sync. To resynchronize the peers, the failover association of the secondary server is now put in the Recover-Wait state and then it moves to the Recover-Done state immediately after synchronization without any MCLT delay. Therefore, both the servers come back to the normal state and are available for lease.

- For NIOS 8.5.2 and later, by default the anycast service is restarted along with the DNS service. However, you can change the restart sequence based on your network topology.

- From NIOS 8.5.2 onwards, 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.

- In NIOS 8.5.2 and later, passwords are stored using the SHA-512 hashing algorithm. Because of this, the password fields now range between 4 to 128 characters.

- In NIOS 8.5.2 and later, 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.

- NIOS 8.5.2 introduces the following changes 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.

- 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 the *System Activity Monitor* widget, you can now view CPU utilization data for up to a maximum of the past 30 minutes.

- You can now configure the number of top processes and the Ptop interval not only for the Grid Master but also for Grid members.

- For Infoblox Subscriber Services, category-related information is now fetched by a different service provider and the following new 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.

- The **IP Space Discriminator** field has been removed in NIOS 8.5.2. All WAPI objects related to this field have also been removed. Infoblox does not recommend using PAPI to add or update the IP space discriminator.

- The **Go to** field in the **Data Management** > **Security** page is not available by default (tree view) in the following screens:
  - **Data Management** > **Security** > **Threat Protection Rules** > **Threat Protection Rules Home**
  - **Data Management** > **Security** > **Members** > <*selected member*> > **Threat Ruleset**
  - **Data Management** > **Security** > **Profiles** > <*selected profile*> > **Threat Ruleset**

  As a workaround, use the flat view to see the **Go to** field.

- From NIOS 8.5.1 onwards, the default UDP buffer size has changed from 4096 to 1220 bytes.

NIOS 8.4.x

- For 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.
- For NIOS 8.4.8, when you change the member assignment of DHCP ranges from a failover association to a Grid member and then back to failover association, leases in the primary and secondary server fall out of sync. To resynchronize the peers, the failover association of the secondary server is now put in the Recover-Wait state and then it moves to the Recover-Done state immediately after synchronization without any MCLT delay. Therefore, both the servers come back to the normal state and are available for lease.

- 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.

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 2.11.5.

This NIOS release supports the following WAPI versions: 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, 2.11.1, 2.11.2, 2.11.3, and 2.11.5.

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

NIOS Version	WAPI Version
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

8.3.7 to 8.3.8	2.9.7
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 to 8.4.7	2.10.5
8.5	2.11
8.5.1	2.11.1
8.5.2	2.11.2
8.5.3, 8.5.4	2.11.3
8.5.5	2.11.5

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 8.5

NIOS 8.5.*x* includes the following WAPI changes:

New Structures:

- `csp_grid_setting`
- `csp_member_setting`

New Objects:

- `parentalcontrol:subscribersite:dca_sub_bw_list`
- `parentalcontrol:subscribersite:dca_sub_query_count`
- `parentalcontrol:subscribersite:proxy_rpz_passthru`

- adminuser
- adminuser:auth_method
- adminuser:use_ssh_keys
- adminuser:ssh_keys:key_name
- adminuser:ssh_keys:key_type
- adminuser:ssh_keys:key_value
- member:dns:doh_service
- member:dns:doh_https_session_duration
- member:dns:dns_over_tls_service
- member:dns:tls_session_duration
- admingroup:admin_set_commands
- admingroup:admin_show_commands
- admingroup:admin_toplevel_commands
- admingroup:cloud_set_commands
- admingroup:database_set_commands
- admingroup:database_show_commands
- admingroup:dhcp_set_commands
- admingroup:dhcp_show_commands
- admingroup:dns_set_commands
- admingroup:dns_show_commands
- admingroup:dns_toplevel_commands
- admingroup:docker_set_commands
- admingroup:docker_show_commands
- admingroup:grid_set_commands
- admingroup:grid_show_commands
- admingroup:licensing_set_commands
- admingroup:licensing_show_commands
- admingroup:machine_control_toplevel_commands
- admingroup:networking_set_commands
- admingroup:networking_show_commands
- admingroup:security_set_commands
- admingroup:security_show_commands
- admingroup:trouble_shooting_toplevel_commands
- parentalcontrol:subscriberrecord
- pxgrid:endpoint

UPGRADE GUIDELINES

- If you have configured DNS forwarding proxy and forwarders for the DNS view (**DNS** tab > **Zones** tab > *dns_view* check box), contact Infoblox Support before upgrading to NIOS 8.5.3 or later.

- If you are using threat analytics, you must have installed the minimum module set version (20210620) before upgrading to NIOS 8.5.3 or later.

- During a staged upgrade, you cannot apply the latest ruleset. Therefore, if all the subscriber site members are dual-mode and the threat protection service is running, then replication of subscriber data takes place only if the **Collect on the MGMT interface only** checkbox is selected.

- If the subscriber site is using HA and the HA passive node is the first to upgrade, the data repository connectivity uses the IPv4 protocol for the site members. If you want the data repository to be connected over the IPv6 protocol, you must stop and restart the subscriber service in the upgraded Grid. You may lose subscriber cache data after stopping and restarting the subscriber service. Therefore, perform the stop and restart one member at a time.

- The Infoblox Docker bridge uses the 169.254.251.1/24 network by default. If this network is used in your environment, you must change the Infoblox Docker bridge network. Use the `show docker_bridge` CLI command to view the current setting and the `set docker_bridge` CLI command to change the setting. For information about these CLI commands, see the “show docker_bridge” and the “set docker_bridge” topics in NIOS online documentation.

- If there are Threat Protection members in your Grid for the 8.3 and later features (Infoblox Subscriber Services, 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, the upgrade will fail.

BEFORE YOU INSTALL

Infoblox supports the following upgrade paths:

- 8.5.4 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 8.5.5. Infoblox recommends that you upgrade to NIOS 8.5.5 from these tested and validated releases:
8.5.4, 8.4.8, 8.3.8

If you must upgrade from other NIOS releases, you must first upgrade to the validated paths before upgrading to NIOS 8.5.5. For example, if you want to upgrade from 8.3.*x* to 8.5.5, you must first upgrade to 8.3.8, and then upgrade to 8.5.5.

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.

Should you need assistance with your upgrade, contact your preferred Infoblox Partner, Infoblox Professional Services or by contacting your Account Team for further information. Our offering for Upgrade Assessment Service is also available for your further information.

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

Training
Training information is available at https://training.infoblox.com

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 https://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-2021- 25220
When using forwarders, bogus NS records supplied by, or via, those forwarders may be cached and used by named if it needs to recurse for any reason, causing it to obtain and pass on potentially incorrect answers. If applicable, modify your configuration to either remove all forwarding or all possibility of recursion. Depending on your use-case, it may be possible to use other zone types to replace forward zones.

CVE-2021- 25217
A flaw was found in the Dynamic Host Configuration Protocol (DHCP). There is a discrepancy between the code that handles encapsulated option information in leases transmitted "on the wire" and the code which reads and parses lease information after it has been written to disk storage. This flaw allows an attacker to deliberately cause a situation where dhcpd while running in DHCPv4 or DHCPv6 mode, or the dhclient attempts to read a stored lease that contains option information, to trigger a stack-based buffer overflow in the option parsing code for colon-separated hex digits values. The highest threat from this vulnerability is to data confidentiality and integrity as well as service availability.

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.

CVE-2021- 25214
In BIND 9.8.5 -> 9.8.8, 9.9.3 -> 9.11.29, 9.12.0 -> 9.16.13, and versions BIND 9.9.3-S1 -> 9.11.29-S1 and 9.16.8-S1 -> 9.16.13-S1 of BIND 9 Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.11 of the BIND 9.17 development branch, when a vulnerable version of named receives a malformed IXFR triggering the flaw described above, the named process will terminate due to a failed assertion the next time the transferred secondary zone is refreshed.

CVE-2021- 23841
The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However, it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack.

CVE-2021- 23840
Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissible length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue.

CVE-2021- 23839
OpenSSL 1.0.2 supports SSLv2. If a client attempts to negotiate SSLv2 with a server that is configured to support both SSLv2 and more recent SSL and TLS versions, then a check is made for a version rollback attack when unpadding an RSA signature. Clients that support SSL or TLS versions greater than SSLv2 are supposed to use a special form of padding. A server that supports greater than SSLv2 is supposed to reject connection attempts from a client where this special form of padding is present, because this indicates that a version rollback has occurred (i.e. both client and server support greater than SSLv2, and yet this is the version that is being requested). The implementation of this padding check inverted the logic so that the connection attempt is accepted if the padding is present, and rejected if it is absent. This means that such as server will accept a connection if a version rollback attack has occurred. Further the server will erroneously reject a connection if a normal SSLv2 connection attempt is made. Only OpenSSL 1.0.2 servers from version 1.0.2s to 1.0.2x are affected by this issue.

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-2020-16166
The Linux kernel through 5.7.11 allows remote attackers to make observations that help to obtain sensitive information about the internal state of the network RNG, aka CID-f227e3ec3b5c. This is related to drivers/char/random.c and kernel/time/timer.c.

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
An error in BIND code which checks the validity of messages containing TSIG resource records can be exploited by an attacker to trigger an assertion failure in tsig.c, resulting in denial of service to clients.

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-2020-1971
The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack.

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-2019-6477
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-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:

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

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 Encrypted Content 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 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 8.5.5

ID	Severity	Summary
NIOS-83694	Critical	Under a rare circumstance, a high replication queue was observed on DHCP members.
NIOS-78480	Critical	Grid Manager crashed when configuring SAML.

ID	Severity	Summary
NIOS-83911	Major	The loopback IP address was not added to the allow recursion list in the DHCP configuration file as a result of which recursive queries to the loopback IP address failed.
NIOS-83298	Major	Permissions of certain writable and executable files and folders on NIOS had to be restricted.
NIOS-83269, NIOS-83076	Major	On NIOS systems that had Advanced DNS Protection enabled, if a ruleset within a profile was modified, the modification did not take effect.
NIOS-83194	Major	Under certain circumstances, the DNS service crashed and was unstable.
NIOS-83150	Major	Under certain circumstances, unable to communicate with IPv6 Grid members.
NIOS-83130	Major	The device status log files did not display the correct interface speed and duplex value for appliances.
NIOS-82873	Major	A CP-V2200 appliance running on Microsoft Azure experienced high CPU utilization.
NIOS-82860	Major	Certificate validation failed for an HTTPS health monitor.
NIOS-82849	Major	The status of DNS Traffic Control LBDN and pools was warning and the server status was unknown when consolidated health monitors were configured with the **Full Health Communication** checkbox not selected, even though the selected Grid member was capable of performing a health check and sharing the status with non-selected DNS Traffic Control licensed members.
NIOS-82847	Major	Grid Manager displayed a red status even though servers within a consolidated health monitor group did not fail a health check but servers in an external LBDN pool failed the health check.
NIOS-82745	Major	If the name of a Lightweight Access Point Protocol (LWAPP) device was changed, the change did not take effect.
NIOS-82670	Major	Client-generated DDNS updates only succeeded on one primary server; therefore, some clients failed to register and access specific resources.

NIOS-82631	Major	The delimiter in an SQL query needed to be changed for CLI credentials to work correctly.
NIOS-82543	Major	Under certain circumstances, the threat analytics service restarted repeatedly.
NIOS-82541	Major	A few vulnerabilities over port 8765 were reported due to unsecured ciphers.
NIOS-82540	Major	Under certain circumstances, DNS Traffic Control and EDNS0 did not work as expected.
NIOS-82534, NIOS-82511	Major	A certain subscriber service category needed to be removed.
NIOS-82533	Major	Data without credentials was displayed in *Active WebUI Users* dashboard and also in the audit logs when a SAML authentication was triggered at the same time.
NIOS-82530	Major	The Advisor client did not work correctly with certain devices of complex configuration (stack + several different chassis).
NIOS-82515	Major	The Ptop files in var/log had gaps where no fastpath line was included, thus impacting reporting data.
NIOS-82450	Major	Unable to swap a Grid member from hardware to virtual if the DSCP setting was overridden in *Grid Member Properties Editor*.
NIOS-82436	Major	A vDiscovery job that has one or more non-breaking space characters in the job name could be created.
NIOS-82305	Major	SOA records failed to validate with DNSSEC.
NIOS-82187	Major	NIOS was vulnerable to CVE-2021-33193, CVE-2021-34798, CVE-2021-36160, CVE-2021-39275, and CVE-2021-40438.
NIOS-82153	Major	Retrieving a CA certificate for SDN displayed an error.
NIOS-82141	Major	Conversion of unmanaged objects to host records did not work as expected.
NIOS-82026	Major	Under certain circumstances, the swap usage rate and CPU usage were very high.
NIOS-82009	Major	NIOS rotated the syslog before it reached the configured maximum syslog size.
NIOS-81890	Major	Using the WAPI `status_member` search field for a DNS Traffic Control search did not work as expected.
NIOS-81848	Major	Restarting the DNS service generated “Server failed” responses in the log files.
NIOS-81846	Major	When joining a Network Insight member to Grid Manager using IPv6, the “A Discovery License is incompatible with an IPv6 only Member" message was displayed in the debug log.
NIOS-81796	Major	DNSTAP stopped working when the destination server restarted or rebooted.
NIOS-81726	Major	Modifying a set of TXT DKIM records using CSV import failed because the record string contained backslash characters.
NIOS-81694	Major	The *Audit log events* report returned a discrepancy in the number of results when they filtered results for a specific admin name because the sort command used in the search string did not have a count value with it.

NIOS-81688	Major	Editing the settings of an NTP member displayed the following error message on Grid Manager: "expected single object, got 2"
NIOS-81683	Major	DHCP failed to renew certain unicast requests from certain members and multiple IP addresses were active from the same subnet for the same client.
NIOS-81682	Major	After a NIOS upgrade, the "Indexer reporting service is failed" error message was displayed in the Grid Manager > **Reporting** > **Members** > **Status** column of a Grid reporting member.
NIOS-81643	Major	All licenses for a Grid member were revoked after changing the IPv6 gateway address.
NIOS-81634	Major	Scheduled tasks did not get executed as scheduled when a Grid Master Candidate promotion took place.
NIOS-81633	Major	The `set debug_tools db_sync` CLI command did not work for HA pairs.
NIOS-81629	Major	During a CSV export, the password for CLI credentials was displayed.
NIOS-81615	Major	When network containers and their child objects were deleted, orphaned host systems were not cleared.
NIOS-81611	Major	Some of the authoritative DNS servers returned server failed responses for queries to zones and the log files contained the "has no NS records" error message.
NIOS-81581	Major	Restarting NIOS services using the Grid Manager displayed the "Contact Technical Support" message.
NIOS-81574	Major	Able to create a vDiscovery job that contained a non-breaking character in its job name.
NIOS-81555	Major	Option 81 support settings were not being inherited from the Grid to its members.
NIOS-81552	Major	Users on networks only assigned to a particular member were unable to get addresses until an HA failover took place.
NIOS-81540	Major	MAC addresses were incorrectly assigned.
NIOS-81469	Major	Users in read-only group were able to add and remove DNS records.
NIOS-81429	Major	Traffic arriving at the secondary VLAN interface was being answered by the primary VLAN interface.
NIOS-81248	Major	Admin groups for which the CLI permission was allowed were able to perform operations outside the scope of the permission.
NIOS-81243	Major	Virtual DNS cache acceleration dropped packets that contained a specific transaction ID.
NIOS-81131	Major	NIOS was vulnerable to CVE-2021-34798,CVE-2021-34798, CVE-2021-36160, CVE-2021-39275, and CVE-2021-40438.
NIOS-80961	Major	Threat Insight data failed to synchronize in the Cloud Services Portal and the "Unable to request data: Authorization error" error message was displayed.
NIOS-80928	Major	Unable to add a member to a nameserver group.

NIOS-80877	Major	The threat protection service did not start on a new NIOS appliance.
NIOS-80795	Major	When a DHCP lease was cleared from a range, the **IP Map** tab displayed IP addresses as unused whereas they should have been marked in green.
NIOS-80755	Major	In an HA setup, the passive node seemed to be stuck and the “Fatal error during Infoblox startup” error was displayed in the log files.
NIOS-80749	Major	The threat protection service did not start on certain appliances.
NIOS-80740	Major	After a NIOS upgrade, the *Member DNS Properties* dialog box displayed an error message.
NIOS-80683	Major	The log files displayed the “DHCP service enabled, but a DHCP license is missing.” message despite the DHCP license being applied.
NIOS-80578	Major	Certificate validation failed for the HTTPS health monitor.
NIOS-80563	Major	The syslog logging facilities of DNS Traffic Control monitors for the "idns_healthd" process were tagged as "mail".
NIOS-80554	Major	Unable to start the member DNS service and an error message was displayed.
NIOS-80445	Major	NIOS was vulnerable to CVE-2021-3517.
NIOS-80444	Major	NIOS was vulnerable to CVE-2017-16931.
NIOS-80443	Major	NIOS was vulnerable to CVE-2017-7376.
NIOS-80441	Major	NIOS was vulnerable to CVE-2016-4658.
NIOS-79949	Major	The Grid secondary did not synchronize with the lead secondary on time thus leading to inconsistencies in the SOA record data.
NIOS-79889	Major	The WAPI output displayed an error for Unicode DNS zones that have a numeric value in their FQDN names during a KSK rollover.
NIOS-79627	Major	In Grid Manager, creating a host record in authority delegated DNS zones displayed an error message.
NIOS-79604	Major	"iftab.IB-FLEX" was not part of the support bundle.
NIOS-79586	Major	An AD authentication error was displayed in the log files after an SAML authentication.
NIOS-79456	Major	Cisco ISE integration with NIOS did not work.
NIOS-79411	Major	All screens under the **Cloud** tab took a long time to be displayed.
NIOS-79314	Major	A secondary peer in a DHCP failover was stuck in the recover-wait state.
NIOS-79268	Major	The **Data Management** > **Network Users** tab stopped populating the Cisco ISE data.
NIOS-78460	Major	When adding an SAML authentication service, the “An invalid value was entered” error message was displayed in the *Add SAML Authentication Service* dialog box.
NIOS-77738	Major	Data without credentials was displayed in the *Active WebUI Users* dashboard and also in the audit logs when SAML authentication was triggered at the same time.

NIOS-77621	Major	Unable to start the discovery service on a Network Insight member.
NIOS-76803	Major	The logging interval of stats.log needed to be changed to 600s.
NIOS-76687	Major	Certain API calls that result in errors included a trace field thus exposing file paths.
NIOS-76676	Major	After a NIOS upgrade, unable to run global searches for IP addresses when a Network Insight member is disconnected from the Grid.
NIOS-75657	Major	vNIOS for Microsoft Azure Grid members were unable to rejoin the Grid during an upgrade due to an incorrect time on Grid Master.
NIOS-75572	Major	After a NIOS upgrade, SSH did not work as expected.
NIOS-75381	Major	A scheduled restart on an hourly basis did not working on one of the DHCP failover pairs.
NIOS-74955	Major	After DNS scavenging was enabled, over a thousand static records were deleted.
NIOS-69003	Major	The named.conf file for an RPZ on an IB-FLEX member displayed a syntax error.

ID	Severity	Summary
NIOS-83476	Minor	The term "ATC" continued to be displayed in Grid Manager even though it is no longer used.
NIOS-83350	Minor	In the *DTC Pool* > **Health Monitors** > **Advanced** tab, the UI label read **CONSOLIDATED MONITOR HEALTH SETTINGS** instead of **CONSOLIDATED HEALTH MONITOR SETTINGS**.
NIOS-83146	Minor	In Network Insight, discovery data was being sent for devices whose `network_view_id` was of the value `0`.
NIOS-82885	Minor	A deduplication issue occurred when a network was added without SNMP enabled on a Consolidator-Probe appliance.
NIOS-81793	Minor	The global search did not return matches when searching for DHCID records using the DNS name.
NIOS-81674	Minor	NIOS required to be restarted after a NIOS license was overwritten.
NIOS-81636	Minor	The Transport and Authentication section of the NIOS WAPI documentation contained an error regarding authentication methods.
NIOS-81626	Minor	Reading of files using path traversal in WAPI did not work as expected.
NIOS-81449	Minor	Changing the public network configuration from dual stack to IPv6 caused the "Cannot delete MGMT configuration when Subscriber Services Properties 'Collect on the MGMT interface only' is enabled" error message to be displayed.
NIOS-81155	Minor	The **Data Management** > **Devices** page failed to load and an error message was displayed.
NIOS-80831	Minor	When using global smart folders, some icons such as edit, create link, delete were hidden.
NIOS-80771	Minor	The CSV exported file for CNAME records did not contain * for required fields.

NIOS-80717	Minor	Clicking the Edit icon to edit a network container caused a logout of the Grid Manager and a system error was displayed.
NIOS-80687	Minor	Table formats of Grid members did not display correctly on Firefox browsers.
NIOS-80433	Minor	The warning message that is displayed when the Enable Time Based Retention check box is selected needed to be reworded.
NIOS-80379	Minor	AD authentication failed for users whose login name included German characters.
NIOS-78374	Minor	A discrepancy in the process manager caused a service outage.
NIOS-72950	Minor	Logging into Grid Manager using LDAP authentication displayed an LDAP server failure error message.

Fixed in NIOS 8.5.4

ID	Severity	Summary
NIOS-80659	Major	The DHCP service kept failing and the “No DHCPv4 configuration files found. Rebuilding conf file dhcpd.conf” error message was displayed in the log file.
NIOS-80641	Major	IB-Flex members went offline repeatedly when virtual DNS cache acceleration and subscriber services with proxy services were running. This was because of a subscriber service proxy hash table collision that caused a deadlock.
NIOS-80639	Major	On a vNIOS for OpenStack with SRIOV deployment, interfaces did not respond when bonding interfaces flapped on a node that had port redundancy enabled and was running features such as virtual DNS cache acceleration and Advanced DNS Protection software.

Fixed in NIOS 8.5.3

ID	Severity	Summary
NIOS-79934	Critical	After a NIOS upgrade, SSH, MGMT port flapping, and DNS service issues occurred.
NIOS-78347	Critical	NIOS was vulnerable to CVE 202021-23839, CVE-2021-23840, and CVE-2021-23841.
NIOS-78293, NIOS-78309	Critical	DB_SENTINEL VIOLATION errors were displayed in the serial console of IB-FLEX appliances on which virtual DNS Cache Acceleration and Advanced DNS Protection software licenses were installed.
NIOS-76236, NIOS-78212	Critical	SNMP traps for DNS tunneling activity detection were not triggered even though the Threat Analytics DNS Tunneling Detection event type was enabled.
NIOS-75658	Critical	Unable to automatically create a reverse zone when creating a network using CSV.
NIOS-75330	Critical	The CPU utilization of a Grid member was 100% when it started to receive RADIUS packets.
NIOS-68362	Critical	In a specific scenario, the password was visible in the core files.

ID	Severity	Summary
NIOS-79968	Major	SNMPV3 credentials that had the privacy protocol set to None were not being saved in Network Insight.
NIOS-79720	Major	When creating an authoritative IPv4 reverse mapping zone containing the RFC2817 prefix, the "RFC2317 prefix must not be empty for classless reverse zones" was displayed in Grid Manager even though the prefix was entered.
NIOS-79693	Major	Renaming the built-in “admin-group” administrator group prevented a NIOS upgrade from taking place.
NIOS-79686	Major	On IB-FLEX appliances, in a large deployment, CPU configurations were changed based on specific deployment numbers.
NIOS-79647	Major	When extensible attributes in a network were modified, the “Cannot create DHCP seed *X.X.X.X* within the network view default, because it duplicates the discovery seed router” error message was displayed in Grid Manager.
NIOS-79628	Major	Under certain circumstances, MSP proxy virtual IP addresses were resolved for non -subscriber sites.
NIOS-79607	Major	LDAP authentication failed and the "LDAP authentication error: list index out of range" error message was displayed during a login attempt.
NIOS-79605	Major	The NIOS documentation contained incomplete information about the Infoblox Customer Experience Improvement Program.
NIOS-79592	Major	The NIOS documentation did not contain information about the **Enable GSS-TSIG Updates** field being overridden to use the KDC server configured in the *Member DHCP Properties* dialog box.
NIOS-79579	Major	After a NIOS upgrade, Azure vDiscovery ran a vDiscovery job and then deleted all the records it had discovered in the past.
NIOS-79542	Major	Unable to perform vDiscovery on a cloud platform member.
NIOS-79502	Major	If you change the case of an extensible attribute value in a smart folder filter, then duplicate results are displayed for the same extensible attribute.
NIOS-79454	Major	After a NIOS upgrade, Grid Master and Grid Master Candidate restarted continuously and core files were generated.
NIOS-79426	Major	The passive node of a Grid Master was unable to communicate with the Grid at intermittent intervals.
NIOS-79393	Major	The threat protection service did not start on IB-FLEX appliances after a NIOS upgrade.
NIOS-79388	Major	An incorrect status was displayed for the LBDN object in the **DNS** > **Traffic Control** screen.
NIOS-79343	Major	A false positive alert that the power supply is up was sent though the power supply was down.
NIOS-79319	Major	Exporting VLAN names is visible data format displayed non-readable entries in the Assigned To column in the CSV file.

NIOS-79292	Major	The NIOS documentation did not contain information that a Grid member cannot act as an NTP server to the Grid Master.
NIOS-79285	Major	After a disaster recovery, truncated DNS queries were dropped for certain Grid members.
NIOS-79276	Major	Unable to add back an external secondary nameserver to the default nameserver group.
NIOS-79273	Major	The security vulnerability QID 48001 "Content-Security-Policy HTTP Security Header Not Detected on port 443/tcp" was detected after a vulnerability scan.
NIOS-79200	Major	The message size sent by certain devices exceeded the maximum SNMP packet size.
NIOS-79170, NIOS-79010	Major	On a vNIOS for OpenStack with SRIOV deployment, when port redundancy was enabled on LAN1/LAN2, the appliance restarted and encountered a fatal error.
NIOS-79165	Major	When the threat protection service was enabled on an TE-4025 appliance, the appliance tried to reboot but was not up and running after the reboot.
NIOS-79137, NIOS-79015	Major	On the **IPAM** tab, Network Insight displayed a VLAN configured against the interface IP address but there were no VLANs configured on the interface.
NIOS-79112	Major	A reporting appliance returned empty data for the End Host History report.
NIOS-79058	Major	Unable to download threat protection rules when the proxy server setting is configured with an IPv6 address in a dual stack Grid Master.
NIOS-79025	Major	The reporting backup did not work if the directory path contained a backslash (\); however, the Grid backup worked with a backslash in the directory path.
NIOS-79021	Major	During a logout using WAPI and cookies on appliances that had the Cloud Network Automation license installed, the “500 Internal Server Error” error message was displayed.
NIOS-79001	Major	On the **Net Map** tab, if you hover over a network, the Comments field displayed the comments of the network container instead of the network itself.
NIOS-78582	Major	Unauthenticated users could determine the NIOS version by parsing nios_version.txt in the URL.
NIOS-78573	Major	After a NIOS upgrade, the *Discovery Status* screen displayed an error message.
NIOS-78522	Major	Under certain circumstances, CPU and memory utilization increased after a NIOS upgrade.
NIOS-78514	Major	The DNS client failed to detect the UDP DNS response when the was an RPZ rule match and virtual DNS Cache Acceleration was enabled.
NIOS-78512	Major	In the *Authoritative Zone* screen, when editing the **Settings** > **Primary name server (for SOA MNAME field)** field the value reverted to the inherited value.
NIOS-78487	Major	A Microsoft Azure vDiscovery job failed and the “Complete discovering for task name: vDiscovery InfoBloxProd, result: 'NoneType' object has no attribute 'get'” error message was displayed.
NIOS-78483	Major	The `show firmware` command did not display the Ethernet firmware version.
NIOS-78461	Major	SAML authentication using PingID SSO displayed the “"Internal Server Error 500" error message.

NIOS-78461	Major	Adding SAML authentication displayed an “An invalid value was entered” error message.
NIOS-78455	Major	The NIOS documentation contained an incorrect value for ibProbableCause.
NIOS-78434, NIOS-78415	Major	The NIOS Release Notes did not contain information that the value of PLATFORM_NAMED_MAX_CACHE_SIZE for the IB-2215 and IB-2225 platforms has been increased from 2048 to 12288.
NIOS-78403	Major	Azure vDiscovery did not work if a proxy authorization was required.
NIOS-78397	Major	A NIOS on-prem host appliance was unable to connect to the CSP portal and the corresponding entry was not displayed in the CSP portal.
NIOS-78387	Major	Report generation on a cloud member caused high database usage for hosts that had many IP addresses.
NIOS-78384	Major	The global search did not return matches when using the DNS name to search for DHCID records.
NIOS-78382	Major	A NIOS upgrade caused a MAC address to change on the MGMT interface.
NIOS-78347	Major	NIOS was vulnerable to CVE 2021-23839, CVE-2021-23840, and CVE-2021-23841.
NIOS-78328	Major	Under certain circumstances, VRF data collection failed.
NIOS-78313	Major	The NIOS documentation did not contain information that for reporting members, a minimum disk space of 250 GB by default.
NIOS-78299	Major	Installing a permanent reporting license created issues in a TE-5005 appliance.
NIOS-78281	Major	New parsing rules for VRRP addresses needed to be added.
NIOS-78268	Major	In an HA setup, whenever a node became passive or became a Grid Master Candidate, the "System Call failed with Connection refused" error was displayed in the debug log files.
NIOS-78261	Major	The “error fetching dhcp_range:/ for reporting event” error was displayed in the syslog file even after a DHCP restart.
NIOS-78246, NIOS-78244	Major	The NIOS documentation contained incorrect information regarding restarting DHCP services.
NIOS-78242	Major	Unable to find the loopback interface IP address to be selected as the management IP address of a device.
NIOS-78241	Major	The device license limit had to be modified for ND-1405 appliances.
NIOS-78240	Major	Upgrade failed due to incorrect index processing in the NetMRIModeSettings.pl file.
NIOS-78239	Major	Global search by DNS name did not include Network Insight devices.
NIOS-78236	Major	End hosts did not display model and version information. And discovery diagnostics collected for certain end hosts displayed fingerprints as disabled even though the fingerprinting option was enabled.
NIOS-78235	Major	The Gird Master restarted when adding a conversion policy for the discovery service.

NIOS-78234	Major	The End Host History report did not contain information about unmanaged devices.
NIOS-78233	Major	Logging data for Network Insight needed to be increased.
NIOS-78232	Major	Discovery processing took a long time when a large number of networks was included in the discovery process.
NIOS-78229	Major	The 'privProtocol is unknown' error message is displayed when trying to create a session.
NIOS-78227	Major	Unable to reset the password after expiry and the error "Old password is invalid" error message is displayed.
NIOS-78226	Major	IPv6 networks were not discovered correctly.
NIOS-78223	Major	IPv4 DHCP filters did not work as expected.
NIOS-78221	Major	Unable to search for an FQDN for an LBDN pattern using WAPI.
NIOS-78205	Major	Time reset did not work on a NIOS VM on Microsoft Azure.
NIOS-78195	Major	DNS cache acceleration sent all the traffic to the BIND server after a NIOS upgrade.
NIOS-78181	Major	The failure counter of the DNS Statistics widget did not increment as expected.
NIOS-78164, NIOS-70117	Major	When DNS fault tolerant caching was enabled, SERVFAIL errors were displayed in the configuration file.
NIOS-78163	Major	Unable to apply hotfixes on upgrade groups.
NIOS-78131	Major	The WAPI REST engine did not recognize IPv6 addresses that contained upper-case.
NIOS-78112	Major	A subscriber client remained offlline in the Cisco ISE server.
NIOS-77939	Major	Grid members including the Grid Master were not able to function as NTP servers to clients if NTP is enabled on the Grid.
NIOS-77913	Major	If the subscriber cache entry did not contain the `PCP:Parental-Control-Policy` parameter, the proxy virtual IP address allocation process was not initiated towards the MSP. If the RPZ zone had the override action of passthru, the proxy virtual IP address allocation process was not initiated towards MSP even though the domain inside RPZ was passthru.
NIOS-77893	Major	Unable to download categories when using a proxy server without credentials.
NIOS-77871	Major	The parental control policy was checked before the subscriber secure policy which caused all domains whitelisted for passthrough to be ignored when the Internet was paused.
NIOS-77864	Major	Certain appliances with over 12000 LBDNs experienced DTC memory exhaustion.
NIOS-77815	Major	The `show log` CLI command did not work as expected.
NIOS-77808	Major	After a NIOS upgrade, the RPZ dashboard and certain reports did not work.

NIOS-77800	Major	After a NIOS restart, IPv6-only members experienced network issues.
NIOS-77786	Major	Some DNS members started to flap and were disconnected from the Grid due to an FQDN gateway violation.
NIOS-77772	Major	A Border Gateway Protocol (BGP) packet was dropped due to SNIC issues.
NIOS-77752	Major	Grid Manager became unstable when object change tracking was enabled.
NIOS-77707	Major	NIOS was vulnerable to CVE 2020-16166.
NIOS-77697, NIOS-77694	Major	Splunk password dependencies needed to be removed.
NIOS-77675	Major	The dns_stats.txt file displayed a high number of recursive queries.
NIOS-77664	Major	SNMP traps were being dropped due to a mismatch in the SNMP engine ID.
NIOS-77662	Major	Unable to use the SSH command to log in to the NIOS CLI after a NIOS upgrade.
NIOS-77619	Major	NIOS encryption algorithms may have caused conflicts with internal policies.
NIOS-77607	Major	When generating a Certificate Signing Request (CSR) on the Grid, the CA parameter is set to true thus causing connectivity issues in Mozilla Firefox and other vendor appliances.
NIOS-77584	Major	After a NIOS upgrade, DNS Traffic Control objects did not load in to Grid Manager.
NIOS-77563	Major	DNS Traffic Control round robin load balancing did not work as expected after a NIOS upgrade.
NIOS-77560	Major	The passive node of a Grid Master remained in a synchronization state and many members went offline after an HA failover.
NIOS-77487	Major	The threat protection service failed to start on one of the Grid members in an IB-1415 appliance.
NIOS-77450	Major	Under certain circumstances, DNS servers did not respond to dynamic updates.
NIOS-77352	Major	File distribution between Grid Master and Grid members did not synchronize correctly.
NIOS-77349	Major	NIOS was vulnerable to CVE-2020-1971.
NIOS-77292	Major	After a NIOS upgrade, intermittent DNS timeouts and long delays query resolution (up to 3 seconds) occurred.
NIOS-77246	Major	The "Threat Analytics Auto Download has failed." email notification was received about a threat analytics download failure on the passive node LAN1 IP address.
NIOS-77102	Major	The DNS acceleration usage was 0% when virtual DNS Cache Acceleration was enabled.
NIOS-76821	Major	Virtual data collection for a Citrix device was required.
NIOS-76743	Major	SAML authentication service failed and the "HTTP/1.0 500 INTERNAL SERVER ERROR" error was displayed in the trace log.
NIOS-76713	Major	The SNMP clear trap was not sent for the NTP_SYNC_DOWN event.

NIOS-76662	Major	RabbitMQ service uses more secured password for user NIOS.
NIOS-76654	Major	An end-of-life version of Apache HTTP was in use.
NIOS-76653	Major	Account passwords were stored using the salted SHA-1 hashing algorithm.
NIOS-76651	Major	SSH services applied relaxed security settings on remote users.
NIOS-76650	Major	The host system used an outdated version of the Linux kernel (3.14.25).
NIOS-76491	Major	The extensible attribute rebuild prompt was not displayed when deleting the extensible attribute from a network.
NIOS-76485	Major	A CSV export of all records using WAPI gives multiple entries for the same host address.
NIOS-76447	Major	The priority number and inventory collection for certain devices needed to be changed.
NIOS-76445	Major	Unable to log in to the remote console when creating an ACL for an administrator group.
NIOS-76362	Major	Single-site cluster configuration for reporting servers did not work and the “Cluster master service failure due to search factor is not met” error message is displayed.
NIOS-76261	Major	Data collection for a certain device needed to be supported.
NIOS-76237	Major	When trying to install a temporary license in an IB-V5005 appliance for a vNIOS for Microsoft Hyper-V instance, the “'You must provision the reporting disk before adding a license to the Reporting server” error message was displayed.
NIOS-75598	Major	NIOS returned an incorrect value in the supportedMech field of the GSS-TSIG TKEY response.
NIOS-75534	Major	After installing a .crt file with many number of intermediate and root certificates, the SSL_ERROR_RX_MALFORMED_HANDSHAKE error message was displayed.
NIOS-74815	Major	Grid members were offline after the NIOS license expired on Grid Master.
NIOS-74480	Major	Unable to create an IPv6 network using an IPv6 template that contained multiple IPv6 fixed address templates.
NIOS-73951	Major	Auto-created records of forward zones (subzones) were not deleted after the subzones were deleted.
NIOS-72516	Major	The DNS service stopped responding to queries when the soft limit of the recursion client quota was reached.
NIOS-72478	Major	Tools such as a CLI command to collect network interface statistics (such as packet drops) in the support bundle was required.
NIOS-69319	Major	When DHCP exclusion ranges are added to an IP map, the boxes appear to be misaligned.

ID	Severity	Summary
NIOS-78552	Minor	An ADP rule did not recognize the NAT mapping.
NIOS-78237	Minor	Network Insight pushed a few public networks to IPAM even after the **Disable discovery networks not in IPAM** option was enabled.
NIOS-77645	Minor	A new check box named **Stop the anycast service when the subscriber service is in the interim state** in the *Add Subscriber Site* wizard was required. 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).
NIOS-77067	Minor	Modifications made to the host record and sent to an Outbound endpoint did not work with HOST_ADDRESS events.
NIOS-76694	Minor	NIOS version URL access had to be allowed only to authenticated users.
NIOS-76663	Minor	RabbitMQ Erlang cookies strengthened to have 200 bytes of alphanumeric characters instead of the standard 20 bytes.
NIOS-73157	Minor	The `reset storage` CLI command failed.
NIOS-70056	Minor	All licenses for a Grid Member were revoked when the IPv6 gateway address was changed.
NIOS-69309	Minor	In an HA setup, some discovered networks were marked grey and not propagated to IPAM.

Fixed in NIOS 8.5.2

ID	Severity	Summary
NIOS-77003	Critical	Under a rare circumstance, the anycast service went down when a Grid Master Candidate was promoted to Grid Master.
NIOS-76826	Critical	Under a rare circumstance, unable to resolve DNS queries after a NIOS upgrade.
NIOS-76658, NIOS-76693	Critical	Several world-writable files were generated that could lead to privilege escalation or root-level compromise of the system.
NIOS-76565	Critical	Under a rare circumstance, the DNS service crashed unexpectedly.
NIOS-76517	Critical	Under a rare circumstance, applying a hotfix resulted in DNS Traffic Control service issues.
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-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-75433	Critical	The value of the `snmpEngineBoots` SNMPv3 trap not incrementing.
NIOS-75382	Critical	Subscriber services category blocking did not take place consistently.
NIOS-75139	Critical	Under a rare circumstance, CPU usage was at 100% and the non-cache latency had increased.
NIOS-75003	Critical	Unable to start the DHCPv4 service, because no valid configuration files were available.
NIOS-74808	Critical	Under a rare circumstance, an IB-FLEX appliance was constantly rebooting.
NIOS-74756	Critical	After enabling Subscriber Services, DNS core files were generated.
NIOS-74681	Critical	After a NIOS upgrade, NIOS restarted on the active node resulting in an HA failover.
NIOS-74661	Critical	After a NIOS upgrade, fastpath restarted on IB-FLEX appliances.
NIOS-74597	Critical	After a NIOS upgrade, DNS queries were not being resolved by DNS servers.
NIOS-74557	Critical	Under a rare circumstance, after a NIOS upgrade, swap usage gradually increased.
NIOS-74517	Critical	DNS Traffic Control initialization failures were encountered after a hotfix was applied on the Grid members without applying it on Grid Master.
NIOS-74440	Critical	Under a rare circumstance, an IB-V1415 appliance frequently restarted and stopped responding to DNS queries.
NIOS-74433	Critical	Under certain circumstances, system swap space usage exceeded the critical threshold value.
NIOS-74378	Critical	The /etc/hosts file was replaced by a 0 length file causing WAPI requests to fail and causing NTP to go out of sync.
NIOS-73857	Critical	Unable to connect to an IPMI device on the IB-1425 appliance.
NIOS-73359	Critical	The NIOS Release Notes did not contain information about the change in behavior of the DHCP failover association wherein it is put in the Recover-Wait state for the entire duration of MCLT.
NIOS-73127	Critical	An RPZ was not being refreshed by a zone transfer and alerts were being generated.
NIOS-72552	Critical	Views were erroneously populated into the DNS member configuration even though recursion was disabled and the member was not authoritative for any zone within those views.
NIOS-72396	Critical	The subscriber ID needed to be un-escaped (by using the `imc_cleanup_exckude()` function) before adding it to the proxy API.
NIOS-71011	Critical	Under a rare circumstance, unable to change the name server group of a particular sub-zone.

NIOS-70993	Critical	Unable to edit the name server group properties and the "An error occurred while getting the model object for Component" error message was displayed.
NIOS-67224	Critical	A PAPI `get` call for fixed address in a specified network returned too much data.

ID	Severity	Summary
NIOS-77096	Major	The performance of the Grid Manager was very slow especially on the **VLAN** tab.
NIOS-77009	Major	The CVE-2020-25705 vulnerability was fixed.
NIOS-77004	Major	The vendor name had to be changed in certain tables.
NIOS-76980	Major	Forwarding data was not collected successfully for certain devices.
NIOS-76972	Major	Unable to find the network view when the **Include Extensible Attributes Values** check box was selected in the **Smart Folders** tab.
NIOS-76927	Major	The restart banner was not displayed after adding additional blocking servers.
NIOS-76911	Major	The DNS Query Rate by Member report and data collected by the Ptop tool displayed different information.
NIOS-76870	Major	Unable to make configuration change in Grid Manager.
NIOS-76734	Major	Grid Manager crashed after DNS Traffic Control was configured.
NIOS-76720	Major	The CVE-2020-25705 and CVE-2020-8617 vulnerabilities were fixed.
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-76568	Major	The NIOS 8.5.*x* Release Notes did not state whether or not TE-4030 is a supported appliance.
NIOS-76523	Major	An incorrect timestamp was displayed for the last discovered hosts in the **Data Management** > **IPAM** > **IPAM Home** > **Last Discovered** column.
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-76349	Major	TCP quota logs were never hit even though the TCP client quota was exceeded.
NIOS-76300	Major	vDiscovery failed and the “ip_owner_id” error message was displayed in the log files.
NIOS-76180	Major	The netmask format was changed in the NetMRI, SDN, and ACI .pm files.
NIOS-76142	Major	The NIOS documentation contained an incorrect DNS query log format.
NIOS-75659	Major	Rolled zone-signing keys (ZSKs) were not being deleted automatically.

NIOS-75646	Major	Because the network map version was not upgraded, the version displayed was inconsistent with the network check version.
NIOS-75579	Major	Under certain circumstances, the database was over-utilized and alerts were generated in Grid Manager.
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-75527	Major	The entity ID in the SAML metadata could have led to a denial of service vulnerability.
NIOS-75498	Major	The SSO metadata URL was populated automatically and incorrectly while using the metadata file in the SAML authentication service configuration.
NIOS-75465	Major	A vADP member was offline during a Grid replication start and core files were generated.
NIOS-75435	Major	The value type of RADIUS class AVP needed to be of type string.
NIOS-75374	Major	Unable to add a job using the bloxTools scheduler.
NIOS-75361	Major	SSH did not work on MGMT after restarting when the **Restrict Remote Console** and **Support Access to MGMT Port** check boxes were enabled.
NIOS-75326	Major	The consolidator status had turned red and the “Discovery Consolidator Service has failed” message was displayed.
NIOS-75275	Major	Inconsistent VLAN data was displayed across hosts and networks on the **IPAM** tab.
NIOS-75242	Major	Under certain circumstances, VRF collection skipped a few IP addresses thus causing duplicate instances.
NIOS-75186	Major	vNIOS did not send a "report ready" indication to Microsoft Azure that the provisioning was complete as per Azure Marketplace guidelines.
NIOS-75171	Major	Adding an authoritative zone and enabling the DNS Cache Acceleration service caused an internal error.
NIOS-75122	Major	A DNS Traffic Control query failed if the server was configured with a domain name and if consolidated health check was enabled on the pools.
NIOS-75031	Major	After the time zone was changed to Moscow, St. Petersburg, Volgograd (UTC +3), logging out and logging back in changed the time zone to Nairobi (UTC +3).
NIOS-75010	Major	Running the `set reporting_reset_license` CLI command caused an HA failover.
NIOS-74986	Major	Threat protection rule publishing failed and IMC core files were generated.
NIOS-74981	Major	Unable to view debug logs for an endpoint.
NIOS-74946	Major	Some of the extensible attribute values were not displayed for the DNS Traffic Control and topology rulesets.
NIOS-74943	Major	High disk utilization on Grid Master caused by the contents of the /storage/infoblox.var/msmgmt/reporting-capture-data file.

NIOS-74923	Major	The DNS server was no longer synchronizing subscriber data.
NIOS-74896	Major	After a NIOS upgrade, outbound API integration failed.
NIOS-74880	Major	Under certain circumstances, RabbitMQ failed.
NIOS-74865	Major	Under certain circumstances, fastpath crashed and an unexpected reebot occurred.
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	Microsoft clusters were unable to perform dynamic updates against NIOS leaving behind discrepancies in the DNS entries in the log files.
NIOS-74821	Major	During a NIOS upgrade, one of the virtual members in the Grid failed to upgrade and the "1 of 1 node has failed upgrade - Upgrading: Syncing Storage files" message was displayed.
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-74795	Major	After a NIOS upgrade, the DNS service failed to start.
NIOS-74792	Major	Under certain circumstances, the Cisco ISE integration with NIOS did not work.
NIOS-74769	Major	The threat analytics service restarted repeatedly and the "java.io.FileNotFoundException" error message was displayed in the log files.
NIOS-74742	Major	Disk usage on Grid Master was over the threshold value.
NIOS-74739	Major	The status of decommissioned IP addresses was displayed as **Used** in the **IPAM** tab.
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 NIOS using SSH AD authentication.
NIOS-74708	Major	Unable to generate certain reports.
NIOS-74665	Major	A CLI panic procedure was required to swiftly stop 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	After adding a the DOW_DHCP_AllScopes MAC address filter, the DHCP service did not restart.
NIOS-74533	Major	The NIOS documentation did not contain clear information about the **Allow VLAN Range Overlapping** check box.
NIOS-74516	Major	The NIOS documentation contained incorrect information about the **Log Only** option.
NIOS-74451	Major	The NIOS documentation did not contain information about support for SNMPv3 AES data encryption.
NIOS-74450	Major	The threat analytics service could not be enabled on certain appliances.

NIOS-74449	Major	The `reset database` command did not work in the emergency prompt.
NIOS-74436	Major	Under certain circumstances, database utilization was at 84%.
NIOS-74420	Major	Unable to send traffic through the LAN1 and LAN2 interfaces and an unexpected restart occurred after changing the maximum client recursion.
NIOS-74408	Major	Under certain circumstances, a DHCP outage occurred along with a high replication queue.
NIOS-74335	Major	The Cisco route collection methodology needed to be improved.
NIOS-74331	Major	An error message was displayed when opening the **VRF Mapping** page.
NIOS-74066	Major	A Multi-Grid Master stopped synchronizing with one of the sub Grids.
NIOS-74058	Major	The NIOS on-prem host joined twice to the Cloud Services Portal.
NIOS-74053	Major	Devices that were viewed as discovered under probes and validated were not displayed on the **Devices** tab.
NIOS-73976	Major	Accessing the **DNS** > **Member/Servers** tab caused an error message to be displayed.
NIOS-73953	Major	DNS Traffic Control health check failed due to multiple search heads responding to the TCP port 9185.
NIOS-73939	Major	Active Directory users were unable to access reports after a NIOS upgrade.
NIOS-73937	Major	Under certain circumstances, the scheduled Grid upgrade was disabled automatically.
NIOS-73901	Major	The NIOS 8.3.8 Release Notes did not mention NIOS-73636 as a resolved issue.
NIOS-73896	Major	The DHCP failover association went into the RECOVER-WAIT state after a range was modified.
NIOS-73813	Major	Unable to launch the reporting appliance and the "The Reporting App is currently unavailable" error message was displayed.
NIOS-73809	Major	Unable to override RPZ logging when a nameserver group is assigned to an RPZ zone and the **RPZ logging** check box is greyed out.
NIOS-73689	Major	Adding multiple extensible attributes to a network container resulted in an Ibap internal error.
NIOS-73659	Major	After promoting a Grid Master Candidate to Grid Master, the status of HA members and some Grid members was offline.
NIOS-73621	Major	The threat analytics service restarted continuously, because DNS tunneling took a while to start.
NIOS-73601	Major	The primary DNS server went offline after external syslog servers were enabled.
NIOS-73571	Major	The SAML login did not directly sign in to Grid Manager. Instead it displayed the login page once again even after a successful authentication.
NIOS-73488	Major	SAML authentication was prone to XML bomb attacks.

NIOS-73474	Major	Under certain circumstances, the threat protection service displayed a failed status.
NIOS-73463	Major	Adding Active Domain certificates broke the SSL certificate chain for the WAPI endpoint.
NIOS-73368	Major	A DHCP protocol violation occurred when option overload (Option 52) was required.
NIOS-73140	Major	In a Multi-Grid Master, the status of a sub Grid fluctuated regularly between **Working** and **Offline**.
NIOS-73137	Major	Unable to create a TLSA record in an unsigned zone.
NIOS-73006	Major	When a forward zone was added inside another forward zone, and a forwarder was added, the records were not displayed during an advanced search. Instead an error message was displayed.
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	SNMPv3 traps were not being generated from a reporting member.
NIOS-72725	Major	The restriction of preventing Grid replication for local RPZ zones needed to be removed.
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-72557	Major	Virtual Routing and Forwarding (VRF) data collection needed to be added to the H3C FF59 series.
NIOS-71303	Major	Unable to log in to Grid Manager after entering the user name and password.
NIOS-71185	Major	When DNS Cache Acceleration was enabled on a DNS server, the `infoblox-dtc-enable` yes line was removed from the DNS configuration file and the status of the hosts in the pool was unlicensed in the *DTC LBDN Visualization* screen.
NIOS-70968	Major	After enabling subscriber services, an upgraded Grid member displayed the warning status.
NIOS-70767	Major	A Splunk API request did not work after a password change.
NIOS-70638	Major	After a NIOS upgrade, the reporting license usage spiked.
NIOS-70386	Major	Unable to log in to NIOS using SAML authentication.
NIOS-70376	Major	Unable to resolve DNS entries for a newly joined Grid member to the name server group for zone replication.
NIOS-70371	Major	Unable to delete network containers that were discovered from Microsoft Azure cloud.
NIOS-69003	Major	The named.conf file for an RPZ displayed a syntax error.

NIOS-66097	Major	The **Data Management** > **Devices** > **Network View** screen displayed the “An error has occurred. Contact technical support if the problem persists” error message.
NIOS-65621	Major	SRV record case-sensitivity caused certain issues with respect to the target response.

ID	Severity	Summary
NIOS-77139	Minor	The IPAM IP list was incorrectly updated when a neighboring device was dropped.
NIOS-77024, NIOS-76967	Minor	The **Data Management** > **IPAM** > **List** tab displayed an incorrect VLAN ID and VLAN name against an interface IP address.
NIOS-77006	Minor	The “"Network Insight has detected unassigned VRFs" message was displayed in Grid Manager but the VRF was already assigned to a network.
NIOS-76803	Minor	Logs were generated every 8 seconds instead of 600 seconds.
NIOS-76796	Minor	Inactive host devices were displayed as used devices on the **IPAM** tab.
NIOS-76695	Minor	Some of the devices displayed an incorrect VLAN ID.
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-76511	Minor	When modifying the value of an external attribute, the “ "An invalid value was entered" error message was displayed.
NIOS-76456	Minor	When parental control was configured, the “"PCP config result: Subscriber Config not fully applied" error message was generated.
NIOS-75567	Minor	The WAPI call for `atc_fwd_forward_first` and `dfp_forward_first` did not return any value.
NIOS-75532	Minor	Subscriber services error messages were not clear and needed more information.
NIOS-75431	Minor	The CVE-2020-13817 vulnerability was fixed.
NIOS-75375	Minor	The NIOS documentation mentioned a TEST GSS-TSIG button when none such existed in Grid Manager.
NIOS-75174	Minor	The NIOS documentation for discovered data for managed objects description needed to be updated.
NIOS-75170	Minor	A WAPI call to get the DTC LBDN data yielded unexpected search results.
NIOS-75097	Minor	TR-800 was not listed as a supported appliance in the NIOS 8.5.1 and 8.4.7 Release Notes.
NIOS-75087	Minor	The **IPAM** tab displayed an incorrect value for the last discovered timestamp of the end hosts.
NIOS-75009	Minor	The **VLAN Name** column displayed an incorrect value when the interface IP address did not have a VLAN assigned to it.

NIOS-74970	Minor	Device type recognition needed to be updated.
NIOS-74900	Minor	Certain IPAM data caused high load on Grid Master.
NIOS-74674	Minor	After a NIOS upgrade, a MGM Grid did not synchronize with the sub Grid.
NIOS-74491	Minor	The SNMP scan attempted to scan a network for which SNMP and other polling options were disabled.
NIOS-74439	Minor	The NIOS documentation needed to be updated with information about certain SNMP traps.
NIOS-74412	Minor	An upgrade check for Docker bridge network conflict needed to be performed.
NIOS-72768	Minor	Information on the blue power LED indication was missing in the *Infoblox Installation Guide 1405 Series Appliances* documentation,
NIOS-72623	Minor	Under certain circumstances, DNS Traffic Control visualization produced unexpected results.
NIOS-72442	Minor	An HA failover occurred when trying to create a smart folder with the **Discovered VLAN ID** filter.
NIOS-72178	Minor	The header of the reporting help PDF file was displayed as “anonymous”.
NIOS-70512	Minor	After a NIOS upgrade, the hardware model was modified.
NIOS-70137	Minor	The restart banner was displayed in Grid Manager even when there were no pending changes.
NIOS-69273	Minor	The DNS service was stopped before or at the same time as the BGP service resulting in anycast queries and LAN1 queries failing at the same time.
NIOS-65064	Minor	Editing custom forwarders did not work.

Fixed in NIOS 8.5.1

ID	Severity	Summary
NIOS-73535	Critical	Under a rare circumstance, the system swap usage exceeded the critical threshold value.
NIOS-73445	Critical	Unable to log on to SSH using TACACS+ after a NIOS upgrade.
NIOS-73400	Critical	After a NIOS upgrade, the reporting license limits dropped from 5 GB to 500 MB.
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-72523	Critical	Under a rare circumstance, single-site reporting cluster backup failed.

ID	Severity	Summary
NIOS-74042	Major	After a NIOS upgrade, the status of DNS forwarding proxy on an HA node was inactive.
NIOS-74039	Major	Unable to add NIOS Grid members to the Cloud Services Portal after a NIOS upgrade.
NIOS-73943	Major	Under certain circumstances, performing a global search did not return results for NIOS on Microsoft Azure but returned results for NIOS on VMware.
NIOS-73900	Major	Under certain circumstances, a new nameserver could not be added to a zone.
NIOS-73890	Major	The NIOS documentation did not state that existing extensible attributes are automatically enrolled for cloud usage when cloud licensed are installed.
NIOS-73862	Major	A vDiscovery job with a non-breaking space character could be created.
NIOS-73800	Major	The **Discovery Status** table displayed an incorrect controller type in the **Type** column.
NIOS-73794	Major	Fastpath and virtual DNS Cache Acceleration were not started; however, their status was displayed as green in the **DNS Cache Acceleration** tab.
NIOS-73730	Major	Supported GCP parameters for the **The DNS name will be computed from the formula** field were not documented in the NIOS documentation.
NIOS-73705	Major	The NIOS documentation erroneously mentioned that when DNS forwarding proxy is enabled on a NIOS member, queries are forwarded to BloxOne DDI instead of BloxOne Threat Defense.
NIOS-73670	Major	After a NIOS upgrade, the **SSO Login** button was hidden in the NIOS login page.
NIOS-73664	Major	The ufclient log file had to be updated to establish a connection through a proxy server.
NIOS-73653	Major	Unable to use WAPI to update or get a network template that has an extensible attribute with no value.
NIOS-73645	Major	Grid Manager displayed different versions of the module set for module sets downloaded manually versus those downloaded automatically.
NIOS-73612	Major	After a NIOS upgrade, disk usage from both the active and passive nodes of an HA pair reached almost 100%.
NIOS-73545	Major	Unable to view records in the **Data Management** > **DNS** > **Members** > **Records** tab.
NIOS-73541	Major	Configuration changes were not synchronized with the Network Insight consolidator (type, time, and interfaces).
NIOS-73540	Major	The SDN API refresh did not take into account the difference between the local time and the Cisco ACI controller clock.
NIOS-73531	Major	The threat analytics service kept restarting continuously.
NIOS-73515	Major	Both physical and virtual IP addresses were not getting synchronized with NIOS.
NIOS-73501	Major	A Microsoft Azure vDiscovery job failed for all subscriptions when a valid but inactive free trial subscription was found during vDiscovery.

NIOS-73499, NIOS-73478	Major	The threat protection service was in a failed status for several second and then restarted unexpectedly.
NIOS-73465, NIOS-73231	Major	During a Grid replication, the SOA serial number was different between the primary and secondary Grid members.
NIOS-73464	Major	Testing a domain against the EDNS Compliance Tester displayed a timeout error message.
NIOS-73462	Major	End host device information was missing on the **IPAM** tab for networks that were not included in discovery but for which the VRFs were mapped with network views.
NIOS-73397	Major	The **Attached Device Port Name** and **Device Port Name** fields on the **IPAM** tab contained different values.
NIOS-73318	Major	The NIOS 8.3.0 EA upgrade path and the CAA record upgrade restriction needed to be removed.
NIOS-73281	Major	The **Last Queried** column on the **Records** tab did not display **Not Monitored** for shared records.
NIOS-73266, NIOS-73151	Major	Both, latency and traffic increased on LAN1 and LAN2 interfaces after a hotfix installation.
NIOS-73260	Major	The **End Hosts Present** field displayed an incorrect interface name.
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-73215	Major	The `set interface_mtu` command did not work when port redundancy was enabled.
NIOS-73209, NIOS-72562	Major	DNS message compression did not take place after a NIOS upgrade.
NIOS-73173	Major	PTR records were not getting resolved after being converted to host records.
NIOS-73168	Major	The reporting data restore operation was being triggered inadvertently resulting in loss of reporting data.
NIOS-73137	Major	Unable to create a TLSA record in an unsigned zone.
NIOS-73108	Major	MTU size needed to be added for OpenVPN tunnels between consolidators and probes.
NIOS-73068	Major	WAPI calls performed against a cloud member failed.
NIOS-73022	Major	The `set reset_rabbitmq` CLI command needed to be modified.
NIOS-72972	Major	Under certain circumstances, the system swap space usage exceeded the critical threshold value.
NIOS-72967	Major	Under certain circumstances, CPU usage was high on a passive HA node.
NIOS-72955	Major	The computation of the database cache size needed to be based on a formula.

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-72926	Major	Perl modules had to be upgraded to download third-party data using the HTTPS protocol.
NIOS-72839	Major	Notification emails to inactive users were not sent as per schedule.
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-72627	Major	Bookmarks and customization of columns were lost for users using SAML authentication who logged out and logged in back again.
NIOS-72616	Major	DNS latency occurred in upstream communication when a single forwarder failed.
NIOS-72615	Major	Certain CLI commands were vulnerable to SSH implementation security.
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-71004	Major	A service restart took a long time to complete in certain Grid members.
NIOS-70653	Major	Unable to update or get a network template using WAPI when assigned an extensible attribute with no value.
NIOS-70588	Major	Core files were generated and subsequent HA failovers occurred after viewing a DHCP range.
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-71385	Major	Unable to set time-based retention policy for the ib_security_summary summary index.
NIOS-71199	Major	The IP map did not display the DHCP exclusion range.
NIOS-71169	Major	A SAML authentication login redirected the host name to the IP address thus breaking the SSL certificate.
NIOS-71029	Major	Grid Manager was unable to download the third-party category information data.
NIOS-70558	Major	Secondary name servers that were made primary did not have the new SOA record.
NIOS-70149	Major	Unable to use PuTTY to SSH into NIOS after disabling cipher suites.
NIOS-70047	Major	Under certain circumstances, CPU usage was high on an HA passive node.
NIOS-69878	Major	Automatically updating resource records according to conversion rules did not work correctly if several associated objects existed.

NIOS-68195	Major	The MAC address of the client system was displayed as the MAC address of VIP in the security report.
NIOS-63430	Major	NIOS was susceptible to certain vulnerabilities that did not have a CVE number.

ID	Severity	Summary
NIOS-74413	Minor	The NIOS Release Notes did not state that the Infoblox Docker bridge uses the 169.254.251.1/24 network by default and if this network is being used, to change the Docker bridge network.
NIOS-73817	Minor	The NIOS documentation incorrectly stated that a NetBIOS discovery returned the MAC address and the operating system.
NIOS-73682	Minor	After a NIOS upgrade, one of the Grid members displayed an error on the **DNS Cache Acceleration** tab.
NIOS-73494	Minor	End host information was not displayed on the **IPAM** tab.
NIOS-73428	Minor	The Microsoft Azure vDiscovery configuration steps were not documented correctly.
NIOS-73425	Minor	The NIOS Release Notes did not document CVE-2019-11477 as an addressed vulnerability.
NIOS-73329	Minor	The `show date` command did not display the correct time zone for Indiana (East) Time Zone even though this time zone was set in Grid Manager.
NIOS-73317	Minor	On the **IPAM** tab, Network Insight displayed a VLAN configured against an interface even though no such VLAN was configured.
NIOS-72885	Minor	Stopping and restarting the DNS service increased the zone serial number.
NIOS-72834	Minor	The `set snmptrap` CLI command did not work if ibTrapDesc contained special characters such as a single quote (').
NIOS-72704	Minor	When Advanced DNS Protection was not running, a vulnerability was detected on port 8089.
NIOS-72276	Minor	A disabled network was not greyed out on the **Members** tab.
NIOS-72274	Minor	After every successful Grid Manager login, an HTTP 500 server error was displayed in the response log.
NIOS-72273	Minor	The color scheme for the DHCP range on the IP map did not match with the color scheme in the legend.
NIOS-72177	Minor	The PDF file of the reporting help was not formatted correctly.
NIOS-72172	Minor	The count of the number of events on the reporting dashboard was not displayed correctly.
NIOS-71362	Minor	Sending the enable command at the device level was possible.
NIOS-71171	Minor	NIOS always returned 0 as the value of ibSystemMonitorSwapUsage.
NIOS-70691	Minor	An RPZ configured to block data did not work when DNS64 was enabled.

NIOS-67066	Minor	Unable to create a TLSA record correctly.

Fixed in NIOS 8.5.0

ID	Severity	Summary
NIOS-73150	Critical	The DNS service did not start after a NIOS upgrade.
NIOS-73127	Critical	Under a rare circumstance, RPZs were not refreshed after a zone transfer and alerts were generated.
NIOS-73091, NIOS-73044	Critical	When events occurred, responses were delayed.
NIOS-73002	Critical	DNS query responses for EDNS-enable queries were dropped when DNS Cache Acceleration was enabled.
NIOS-72810	Critical	The Infoblox Installation Guide vNIOS for VMware did not contain information about installing temporary licenses while deploying Trinzic virtual appliances.
NIOS-72797	Critical	After a NIOS upgrade, the named.conf file contained syntax errors.
NIOS-72789	Critical	Splunk instances failed to recognize timestamps that start from January 1, 2020.
NIOS-72553	Critical	DNS views were erroneously populated in the DNS member configuration even though recursion was disabled and the DNS member was not authoritative for any zones within those views.
NIOS-72441	Critical	Restoring accidentally deleted objects from the Recycle Bin took a very long time.
NIOS-72396	Critical	The subscriber ID needed to be unescaped before adding it to the proxy API.
NIOS-72388	Critical	Fatal error messages were displayed in the log files in a vNIOS KVM-based OpenStack Newton deployment and numerous core files were generated.
NIOS-71567	Critical	Under certain circumstances, Grid Master's disk space usage had reached up to 82%.
NIOS-71216	Critical	RPZ local zones were not transferred to Grid members that joined the Grid with the IPv6 only MGMT port.
NIOS-71069	Critical	NIOS encountered a high swap issue after setting the server for consolidated health monitor settings.
NIOS-70956	Critical	The Grid Manager LAN1 interface failed during a NIOS upgrade.
NIOS-70917	Critical	Unable to start threat protection service because it was greyed out.
NIOS-70903, NIOS-70764	Critical	Statistics for the DNS Effective Peak Usage Trend for Flex Grid License report were incorrect and the QPS did not represent the actual value.
NIOS-70786, NIOS-70738	Critical	Devices at two sites went down and a restart did not recover the systems.
NIOS-70770	Critical	Unable to upload the NIOS image file on the **Upgrade** tab of Grid Manager.

NIOS-70762	Critical	A NIOS test upgrade failed and the "upgrade cannot proceed since /mnt/usr/conf/dhcp_fingerprints.conf not found" error message was displayed in the syslog file.
NIOS-70698	Critical	An IPv6 loopback address that was not assigned to an area in OSPFv3 caused it to be displayed as LSA type 5 in the neighboring router instead of LSA type 1.
NIOS-70657	Critical	Under certain circumstances, the name server configuration was removed for AWS zones.
NIOS-70654	Critical	Editing workflows in the BloxTools environment caused an internal error message to be displayed.
NIOS-70650	Critical	The Identity Mapping feature did not work correctly even after a hotfix was applied.
NIOS-70577	Critical	The `join` WAPI function did not work on IB-FLEX appliances.
NIOS-70573	Critical	On an HDD failure, SSD was reformatted.
NIOS-70547	Critical	A NIOS upgrade test failed and the "Test status DB Import Fail" error message was displayed.
NIOS-70484	Critical	During a failover in an HA cluster, the virtual IP address became unavailable.
NIOS-70336	Critical	Editing fields in the *SAML Authentication Service* dialog box did not work.
NIOS-70331	Critical	DNS Forwarding Proxy on NIOS did not work as Docker containers failed to start.
NIOS-70324	Critical	Restarting DNS services on Grid members took 20 minutes or longer.
NIOS-70234	Critical	A local RPZ zone with 150 records was slow to open.
NIOS-70222	Critical	During a NIOS upgrade, the "Member is not connected" error message was displayed even though there were no offline members.
NIOS-70008	Critical	A Grid member that was evicted after the vNIOS license expired was not able to rejoin the Grid until you restarted Grid Master.
NIOS-69995	Critical	Under certain circumstances, NIOS upgrade on IB-4010 systems failed.
NIOS-69887	Critical	The DCHP service crashed soon after it started, went into a restart loop, and generated core files.
NIOS-69883	Critical	Reporting of Subscriber Services categories for DNS resolutions by CNAME was incorrect.
NIOS-69755	Critical	PTR records were removed from Microsoft DNS as a result of changes to TTL values.
NIOS-69742	Critical	Modifying the configuration of a Grid member took longer than 10 minutes.
NIOS-69711	Critical	The OCSP two-factor authentication could easily be bypassed.
NIOS-69676	Critical	Modifying extensible attributes caused Grid members to go offline.
NIOS-69668	Critical	Custom extensible attributes in Cisco ISE and NIOS did not synchronize.
NIOS-69650	Critical	Many RPZ refresh failure error messages were generated in the log files after cleaning up some invalid records.

NIOS-69606	Critical	Some SNMP trap CLI commands did not work as expected.
NIOS-69250	Critical	DDNS updates made using the GSS-TSIG authentication did not work Apple Mac clients.
NIOS-69052	Critical	The system swap space usage exceeded the critical threshold value on the Grid Master Candidate.
NIOS-68305	Critical	Under certain circumstances, the DNS latency was too high and caused service disruption.
NIOS-68297	Critical	Under certain circumstances, the **Test SNMP** button did not send an SNMP trap.
NIOS-67997	Critical	Under certain circumstances, Grid Master restarted every 10 minutes.
NIOS-67742	Critical	Under certain circumstances, some Grid members were dropped from the Grid after a NIOS upgrade.
NIOS-67562	Critical	A bloxTools member reported high memory utilization after a NIOS upgrade.
NIOS-67488	Critical	During a NIOS upgrade, an error message was displayed on the Grid Master Candidate stating that the passive node had to be upgraded even though the passive node upgrade was complete.
NIOS-67412	Critical	High CPU utilization caused by an intermittent DNS resolution problem.
NIOS-67150	Critical	Converting a Grid Master and a Grid Master Candidate to IPv6 displayed an error message.
NIOS-66179	Critical	Active Directory automatically created underscore zones did not inherit DNZ scavenging last queried time configurations in the named.conf file.
NIOS-65869	Critical	Under certain circumstances, a high replication queue caused a DNS outage.
NIOS-65678	Critical	Some of the Grid members in a Grid went down, came up again, and tried to rejoin the Grid leading to a high replication queue.
NIOS-64851	Critical	On vNIOS for OpenStack, LAN2 was unavailable when LAN1 was allowed to obtain an IP address from the DHCP server.
NIOS-62679	Critical	The CVE-2016-10126 vulnerability was fixed.

ID	Severity	Summary
NIOS-73272	Major	Network Insight did not populate IPAM information across network views.
NIOS-73103	Major	DNS queries and ICMP requests were unresponsive when port redundancy was enabled.
NIOS-72864	Major	SAML authenticated users were unable to access or edit objects on the **DHCP** > **IPv4 Filters** tab and the **DHCP** > **Option Spaces** tab.
NIOS-72808	Major	DHCP fingerprinting scanned devices that were excluded from discovery.
NIOS-72746	Major	Unable to collect management and virtual IP addresses.
NIOS-72729	Major	After a NIOS upgrade, some domains were resolved with an increase in latency.

NIOS-72723	Major	Unable to add an external secondary name server to a name server group and an error message was displayed.
NIOS-72720	Major	Unable to collect IP address data from VRF using SNMP.
NIOS-72718	Major	An offline IP address that was previously connected to a leaf network was still being discovered.
NIOS-72698	Major	DNS Traffic Control health check failed because multiple search heads responded to a TCP port.
NIOS-72696, NIOS-72614	Major	Running certain commands enabled NIOS administrators to gain root access.
NIOS-72695	Major	The NIOS documentation did not contain enough information about the **Retry Up Count** field.
NIOS-72693	Major	The MAC Address filter type is ignored after a DHCP fingerprint filter type is added to the same DHCP range.
NIOS-72688	Major	A hardcoded password was found in the libibone_authenticate.so library.
NIOS-72686	Major	Under certain circumstances, making changes in Grid Manager displayed an error message.
NIOS-72657	Major	NIOS did not have a mechanism to check for deprecated VMXNET virtual network adapters.
NIOS-72637	Major	Running the `show rpz_recursive_only` command caused the serial console to crash.
NIOS-72634	Major	Under certain circumstances, Grid Master failed to join the Multi-Grid Master.
NIOS-72534	Major	Non-superusers were unable to create a smart folder with the **Type Equals Device** filter.
NIOS-72513	Major	Perl modules had to be upgraded to download third-party data.
NIOS-72483	Major	NIOS changed the load balance split of the Microsoft failover association thus causing synchronization issues.
NIOS-72473	Major	An LBDN object was resolving with an offline DTC server.
NIOS-72415	Major	The set hotfix CLI command allowed full root access to the NIOS system.
NIOS-72403	Major	Under certain circumstances, running the `set certificate_auth_services` CLI command caused memory corruption.
NIOS-72402	Major	Under certain circumstances, running the `set admin_group_acl` CLI command caused memory corruption.
NIOS-72384	Major	DNS resolution stopped; however, after some time the DNS service recovered by itself.
NIOS-72369	Major	Under certain circumstances, high CPU utilization was observed.
NIOS-72351	Major	Multiple records were not obtained for the same IP address behind the home gateway (CPE).
NIOS-72349	Major	The CVE-2019-6477 vulnerability issue was fixed.

NIOS-72348	Major	The **Advisor** tab displayed errors in the **Last Scheduled Execution Result** and **Last Run Now Result** fields.
NIOS-72328	Major	Unable to discover VMs in an Azure vDiscovery environment.
NIOS-72321	Major	vDiscovery failed on a VMware endpoint.
NIOS-72315	Major	Console login was denied to groups that contained a named ACL.
NIOS-72282	Major	Grid Manager displayed the status incorrectly as Running even when DNS Forwarding Proxy did not work.
NIOS-72280	Major	If you disabled synchronization for a Microsoft managed server, it was not grayed out in Grid Manager.
NIOS-72278	Major	CSV export failed and an error message was displayed.
NIOS-72277	Major	Disabled zones were not grayed out in Grid Manager.
NIOS-72271	Major	The NOERR and NODATA response types did not work with subnet rules.
NIOS-71665	Major	Subscriber services was logging a report of all guests irrespective of whether their CPE had the opt-in policy or not.
NIOS-71660	Major	Assigning proxy addresses to a subscriber policy included multiple sets of IP addresses.
NIOS-71659	Major	Multiple core files that were generated caused one of the Grid members to hang.
NIOS-71616	Major	Under certain circumstances, a test NIOS upgrade failed and displayed error messages in the log files.
NIOS-71613	Major	The system swap space usage exceeded the critical threshold and increased constantly on PT-2205 systems.
NIOS-71597	Major	When a non-superuser tried to access a global smart folder, an error message was displayed.
NIOS-71497	Major	Under certain circumstances, vDiscovery did not run on Google Cloud Platform.
NIOS-71479	Major	Adding entries to an ACL (Access Control List) caused a DNS outage.
NIOS-71477	Major	The DHCPv6 service failed to restart.
NIOS-71474	Major	Legitimate domains were automatically added to blacklisted RPZs.
NIOS-71454	Major	Delegated name servers via Microsoft synchronization were being deleted.
NIOS-71398	Major	Wildcard A records with a second label were prevented from being created by the default host name policy.
NIOS-71395, NIOS-71009	Major	Running Discover Now on the networks or IP addresses caused the status to be in a pending state.
NIOS-71375	Major	The “Primary drive is full” warning message was displayed for a consolidator.
NIOS-71356	Major	Enabling a threat protection ruleset displayed an error message during a zone transfer.

NIOS-71330	Major	The Threat Analytics log files filled up 100% of the disk space.
NIOS-71298	Major	Software ADP dropped external notification messages.
NIOS-71277	Major	The VRRP priority was always 1 in the traffic capture file after a NIOS upgrade.
NIOS-71263	Major	The *Member Selector* dialog box took a very long time to load.
NIOS-71251	Major	Accessing the **DNS** tabs in Grid Manager displayed an error message.
NIOS-71217	Major	DTC load balancing did not work as expected with DNSSEC.
NIOS-71209	Major	An ND appliance encountered high CPU utilization.
NIOS-71208	Major	The RouteLimit variable had to be added to the CLI route collection.
NIOS-71197	Major	Upgrading NIOS caused excessive messages to be logged in the syslog file.
NIOS-71192, NIOS-71184	Major	When DNS Cache Acceleration was enabled on a DNS server, the `infoblox-dtc-enable yes` line was removed from the DNS configuration and the status of the hosts in the pool were displayed as Unlicensed in the DTC LBDN Visualization window.
NIOS-71191	Major	A disabled zone caused a DNS outage.
NIOS-71174	Major	The NIOS 8.3.4 Release Notes contained internal issues in the Resolved Issues section.
NIOS-71155, NIOS-71142	Major	After a NIOS upgrade, Grid members went offline causing a DNS outage.
NIOS-71153, NIOS-71198	Major	After a NIOS upgrade, the **Go to IPAM View** and **Go to DHCP View** options were not visible in Grid Manager.
NIOS-71152	Major	ARP, route and IP address data collection needed to be added in NIOS.
NIOS-71141	Major	A new appliance was stuck at startup with the "Fatal error during Infoblox startup" error message.
NIOS-71128, NIOS-67706	Major	The DNS service was in a restart loop because of DTC configuration issues.
NIOS-71053, NIOS-70614	Major	The NIOS documentation had to be updated with a note that regular expressions cannot be used in a basic global search.
NIOS-71107	Major	Under certain circumstances, a bunch of SNMP alerts was generated.
NIOS-71086	Major	The maximum value of maximum concurrent transfers was too low and had to be increased.
NIOS-71029	Major	Category information data was unavailable for some Grid members.
NIOS-70989	Major	Reporting volume usage thresholds and the associated GUI banner were incorrect for single or multiple site clusters.
NIOS-70984	Major	A DHCP service outage occurred due to multiple segmentation fault.
NIOS-70955	Major	Running the `show subscriber_secure_data` command closed the SSH connection to the server.

NIOS-70943	Major	A memory error caused Grid Manager to reset.
NIOS-70929	Major	Unable to run Discover Now on a physical probe.
NIOS-70927	Major	Performing operations such as adding a record caused the Grid Manager to hang.
NIOS-70888	Major	The admin status under **Administration** >**Administrators** > **Admins** was disabled if you tried to modify a setting for the admin.
NIOS-70835	Major	NIOS crashed during DTC health monitoring and a critical message was displayed on the **Syslog** tab.
NIOS-70832	Major	The DNS service stopped responding and a manual service restart had to be performed.
NIOS-70809	Major	If you selected the **Enable DNSSEC validation** check box and added a trust anchor, the **Responses must be secure** check box was enabled by default.
NIOS-70774	Major	Adding a new CA certificate broke the existing session along with the Certificate Authentication Service.
NIOS-70765	Major	Adding a new zone after a data import caused Grid Manager to slow down.
NIOS-70729	Major	Health checks did not function correctly after a NIOS upgrade.
NIOS-70726	Major	Under certain circumstances, an IB-1410 member restarted unexpectedly.
NIOS-70713	Major	Running the `set promote_master` CLI command did not display the `Primary reporting site candidates` input.
NIOS-70705	Major	After a NIOS upgrade, in IB-810 and IB-820 platforms, members in a Grid Master or Grid Master Candidate role needed to be displayed in yellow in Grid Manager.
NIOS-70671	Major	The reporting license usage exceeded after a NIOS upgrade.
NIOS-70635	Major	Certain configured parameters for the SIP health monitor did not work during the health monitor checks.
NIOS-70633	Major	Unable to add an IP address in the **Virtual TFTP Root** tab.
NIOS-70619	Major	During a NIOS upgrade, the internal version was displayed.
NIOS-70609	Major	Using WAPI, unable to create records in a shared record group.
NIOS-70604	Major	Information about restrictions on addition and deletion of DS records was required.
NIOS-70592	Major	Synchronization of delegate zones between Microsoft and NIOS did not work as expected.
NIOS-70591	Major	Unable to access the IPMI interface.
NIOS-70581	Major	The NIOS documentation incorrectly mentioned the presence of a **Notification Address** field.
NIOS-70579	Major	The service status of Grids fluctuated between online and offline.
NIOS-70569	Major	Unable to import LBDN records using CSV import.

NIOS-70557	Major	Removing system generated records caused shared delegated records to also be removed thus resulting in an outage.
NIOS-70502	Major	Under certain circumstances, high disk usage was reported on the IB-1410 appliance.
NIOS-70476	Major	Using a non-superuser account to edit the port interface displayed an internal error message.
NIOS-70473	Major	IB-820 appliances encountered a memory leak with high swap disk usage.
NIOS-70445	Major	The NIOS documentation did not contain information about the way to determine whether an extensible attribute is required or not.
NIOS-70441	Major	Using an API query returned an error message.
NIOS-70434	Major	An HA Grid member went offline after the Threat Protection monitoring mode was disabled.
NIOS-70411	Major	Certain IPAM interfaces displayed incorrect VLAN information.
NIOS-70392	Major	A software distribution caused the HA passive node to randomly restart.
NIOS-70365	Major	A warning message had to be added in Grid Manager if IB-820 or IB-810 were upgraded into a Grid Master or Grid Master Candidate.
NIOS-70351	Major	The “err infoblox_find_host_by_haddr” message was displayed in the syslog file.
NIOS-70346	Major	If you modified the MAC address associated with a host record, the update did not get logged in the audit log file.
NIOS-70341	Major	The `delete leases` command did not work.
NIOS-70340	Major	Unable to log on to NIOS using Citrix NetScaler.
NIOS-70328	Major	The SNMP engine ID displayed different values in Grid Manager versus a WAPI call.
NIOS-70322	Major	Threat Analytics did not block tunneling traffic.
NIOS-70313	Major	The Data Management > IPAM tab displayed incorrect VLAN information.
NIOS-70295	Major	The hardserver.log file was large and did not get truncated or rotated.
NIOS-70278	Major	When both the alias record and the host record are present in the same zone, the zone failed to load.
NIOS-70276	Major	Under certain circumstances, the Threat Analytics service kept restarting continuously.
NIOS-70228	Major	The Threat Protection log file logged a DROP error message even though the transfer was successful.
NIOS-70138	Major	Unable to find the network view using the **Include Extensible Attributes Values** filter on the **Smart Folders** tab.
NIOS-70128	Major	The OSPF protocol did not work after a NIOS upgrade.
NIOS-70116	Major	AD authentication for a nested group query failed for a canonical name that contained commas.

NIOS-70108	Major	The DNS integrity check failed after signing a zone with DNSSEC.
NIOS-70091	Major	Modifying an LBDN record displayed an SOA response.
NIOS-70085	Major	A NIOS upgrade failed and the database reset took longer than 1.5 hours to complete.
NIOS-70081	Major	Pre-provisioned clients were hitting a non-subscriber RPZ.
NIOS-70075	Major	Using WAPI, MAC address filters and MAC addresses could be added in the Grid Master Candidate that read-only API access enabled.
NIOS-70020	Major	Running the `set reporting_reset_license` CLI command caused the SSH session to close.
NIOS-70000	Major	Unable to edit a Grid member during SNMPv3 configuration.
NIOS-69980	Major	Logic filter lists were not inherited dynamically in the DHCP range template.
NIOS-69975	Major	If ARP data was collected using the CLI, then it was not collected using SNMP after disabling CLI access.
NIOS-69966	Major	The Data Connectors documentation contained incorrect information about hard disk drives for the Data Connector VM.
NIOS-69954	Major	The DNS Cache Hit Ratio widget in the dashboard displayed data for only the last 5 minutes.
NIOS-69929	Major	The NIOS upgrade failed on multiple members of a Grid.
NIOS-69898	Major	The Threat Analytics service kept restarting on a Grid member.
NIOS-69896	Major	A Grid member was not visible in reports and neither was it visible in the **Members** drop-down list on the **Reporting** tab.
NIOS-69891	Major	DNS fault tolerant caching did not work when the **Enable Recursive ECS** option was selected.
NIOS-69860	Major	DNS did not start on an HA Grid member and generated a message in the IBAP log file.
NIOS-69859	Major	The zone-signing key rollover did not happen as scheduled.
NIOS-69857	Major	Reporting traffic was sent over the MGMT interface irrespective of the selected interface.
NIOS-69855	Major	NIOS did not accept the BGP advertised default route for IPv6.
NIOS-69844	Major	File uploads failed after two-factor authentication was enabled.
NIOS-69831	Major	On the **IPAM** tab, the device model for certain Cisco devices did not display correctly.
NIOS-69825	Major	DHCP failover peer offered a new dynamic lease to a client that had an existing lease in the same shared network.
NIOS-69785	Major	The DNS integrity check did not account for the fact that DNS is not case-sensitive.

NIOS-69773	Major	When query monitoring was enabled to use the data in DNS scavenging, the last queried data was modified without a DNS query towards the authoritative servers.
NIOS-69759	Major	Unable to create A record in Grid Manager.
NIOS-69734	Major	Reports did not display data for all the days.
NIOS-69717	Major	The NIOS documentation needed detailed information about synchronizing Active Directory domains on a domain controller.
NIOS-69712	Major	The CSV import had to be manually broken down into multiple files to avoid errors.
NIOS-69677	Major	The `set snmp trap` command did not include the sysUpTime variable.
NIOS-69651	Major	High CPU utilization on Grid Manager caused an HA failover.
NIOS-69623	Major	Amazon Route 53 synchronization groups did not synchronize to AWS and because of this, zone data was not updated.
NIOS-69578	Major	Pending changes on the **View Pending Changes** tab were not logged in the audit log files.
NIOS-69532	Major	Unable to download the support bundle using both Grid Manager and the CLI.
NIOS-69519	Major	A newly configured LDAP authentication for remote admins failed.
NIOS-69499	Major	Running the `set dns transfer` command displayed an error message.
NIOS-69412	Major	You had to enter the OPSF authentication key each time you edited the system properties.
NIOS-69377	Major	A WAPI call that does not have `extarrs` added is successful even though the **Required** column on the **Extensible Attributes** tab is set to **Yes**.
NIOS-69307	Major	The AD authentication nested group query failed for a canonical name that contained parenthesis.
NIOS-69306	Major	The wrong certificate was displayed when connecting to the Splunk API.
NIOS-69248, NIOS-69239	Major	Performance when adding a DHCP member to a network needed to be improved.
NIOS-69236	Major	The DHCP service stopped working after a failover to a passive node.
NIOS-69219	Major	Non-Superuser users are not getting data when trying to access a global Smart folder filtered with the Location extensible attribute.
NIOS-69093	Major	Access to Grid Manager was lost after emptying the Recycle Bin.
NIOS-69080	Major	A user not associated with any role or permission was able to view the host record in Grid Manager as well as by using the WAPI.
NIOS-69054	Major	On the **Data Management** > **Devices** tab, the list of devices did not load.
NIOS-69051	Major	Unable to search for the FQDN of records using the search WAPI object.
NIOS-69022	Major	Able to access blocked settings of Splunk when the reporting appliance was very slow.

NIOS-68431	Major	The start and stop performance of the DNS service from Grid Manager needed to be improved.
NIOS-68414	Major	Under certain circumstances, the DNS latency was too high and caused service disruption.
NIOS-68294	Major	The NIOS WAPI did not retrieve networks associated with an AD site that also had a network container associated with it.
NIOS-68220	Major	Under certain circumstances, high disk usage occurred on IB-VM-1410 Grid members.
NIOS-68201	Major	When creating a new range, Infoblox DHCP scope options were not replicated in Microsoft DHCP.
NIOS-68085	Major	Certain devices in Network Insight needed to be merged.
NIOS-67862	Major	Environmental data and port control needed to be added in Network Insight.
NIOS-67854	Major	The conflict_types field of an IP address always returned NONE irrespective of whether there was a conflict or not.
NIOS-67707	Major	The system primary hard disk usage was over the threshold value.
NIOS-67644	Major	After rebooting the system, the DNS Cache Acceleration service failed and error messages were displayed in the Infoblox.log file.
NIOS-67633	Major	Under a rare circumstance, the performance of some NIOS appliances was very slow.
NIOS-67601	Major	Delay in communication occurred between the Grid Master and Grid members.
NIOS-67569	Major	The primary hard disk usage of a system was over the threshold value on one of the passive node of the Grid member.
NIOS-67494	Major	Network Insight did not display the model number and serial number for certain devices.
NIOS-67493	Major	The number of routes during VRF collection had to be adjusted to the route limit.
NIOS-67352	Major	Unable to download the support bundle using both Grid Manager and the CLI.
NIOS-67280	Major	Grid Master disk usage increased because of RabbitMQ files.
NIOS-67266	Major	Signing a zone displayed an error message.
NIOS-67158	Major	The DNS service crashed and many core files were generated.
NIOS-67067	Major	Primary disk usage on the Grid Master increased.
NIOS-66960	Major	Unable to access all the events in the audit log files.
NIOS-66866	Major	The NIOS documentation did not contain information about the SNMP trap MIB.
NIOS-66744	Major	Unable to resolve a CNAME record until the record was deleted and manually added again.
NIOS-66658	Major	The reporting server restarted the cluster.

NIOS-66478	Major	The Grid Master disk usage was consistently increasing.
NIOS-66235	Major	Newly added records were not propagated to some servers in the Grid.
NIOS-65915	Major	Unable to access Grid Manager after promoting Grid Master Candidate to Grid Master.
NIOS-65838	Major	After enabling the LAN2 port on the vNIOS HA Grid Master, an error message was displayed.
NIOS-65755	Major	A NIOS appliance blocked ICMP requests and replies.
NIOS-65467	Major	The Grid Master Candidate promotion failed and the Grid Master Candidate was not set as the Grid Master after the promotion.
NIOS-65317	Major	The Inactive IP Addresses report included active IP addresses.
NIOS-65279	Major	An IB-1400 appliance was disconnected from Grid Master and later restarted.
NIOS-65222	Major	Individual SSH ciphers that were to be disabled were not disabled.
NIOS-65197	Major	Irrespective of the static routes used, SNMP traps were always sent through the MGMT interface.
NIOS-64844	Major	An autogenerated A record that was created with an IP address that belonged to an external primary member existed in another nameserver group.
NIOS-64840	Major	After upgrading BIOS on a TE-1415 appliance, it failed to start and displayed error messages.
NIOS-64739	Major	The API documentation for list_values parameters was incorrect.
NIOS-64397	Major	The IB-14x5 and IB-8x5 systems failed to restart.
NIOS-63901	Major	DDNS entries for newly added roaming hosts were removed from the log files.
NIOS-63790	Major	A discovery member was deployed; however, the `set temp_license` command returned licenses for a normal member type.
NIOS-63763	Major	A synchronization failure was indicated by the 'hardware uncompatible' error message.
NIOS-63655	Major	A vulnerability assessment on the IB-4010 LOM interface yielded a number of critical vulnerabilities with the SSL implementation.
NIOS-62203	Major	After a NIOS upgrade, DNS reports did not contain data.
NIOS-61967	Major	Host records in reverse zones did not resolve PTR queries.
NIOS-53575	Major	Smart NIC crashed on the PT-2200 appliance.
NIOS-49787	Major	A large number of multi-master DNS messages were logged in the syslog and Infoblox.log files.

ID	Severity	Summary
NIOS-73038	Minor	Horizontal scrolling on certain tables in Grid Manager does not work as expected.

NIOS-72764	Minor	The timestamp needed to be updated if the device was reachable using ICMP ping.
NIOS-72748	Minor	The Grid Manager banner displayed incorrect expiry days for temporary licenses.
NIOS-72692	Minor	Running DiscoverNow on an inactive IPv4 address updates Grid Manager with the last discovered timestamp.
NIOS-72648	Minor	Synchronization between Grid Manager and ND devices was not successful.
NIOS-72410	Minor	NIOS inserted backslashes when passing the fixed line ID for MAC address formats.
NIOS-72376	Minor	When merging ADP rulesets, Grid Manager hung and Java exceptions were displayed in the Infoblox.log file.
NIOS-72272	Minor	The `threatanalytics:whitelist` object was missing from the WAPI schema output.
NIOS-72190	Minor	When printing the Home Dashboard on the **Reporting** tab, the PDF generated displayed the title as **Home Dashboard | Splunk** instead of **Home Dashboard | Infoblox**.
NIOS-71480	Minor	Global search did not yield results as expected.
NIOS-71478	Minor	An alert trap sent the wrong severity level.
NIOS-71450	Minor	The PDF link to the NIOS documentation pointed to an internal Google drive location.
NIOS-71361	Minor	Duplicate requests to the API needed to be eliminated when using the `IfAddrs` API request.
NIOS-71178	Minor	Apex records that were masked by LBDN did not display in strikethrough font.
NIOS-71115	Minor	Devices of type NIOS and vNIOS needed to be excluded from CLI collection.
NIOS-71094	Minor	The **Enable DHCP** option was almost hidden because of the default window size.
NIOS-71030	Minor	Time zone changes related to Daylight Savings Time were incorrectly computed.
NIOS-70991	Minor	The **IPAM** tab displayed VLAN as Multiple for networks even when the IP addresses within the network have only one value for Discovered.
NIOS-70954	Minor	High CPU utilization because certain consolidator queries were not optimized.
NIOS-70932	Minor	The NIOS documentation contained incorrect information about CSV export limit restrictions.
NIOS-70873	Minor	The reporting service restarted every 30 minutes after a NIOS upgrade.
NIOS-70808	Minor	Inheritance of DHCP threshold email settings at the network container level was incorrect.
NIOS-70734	Minor	The routing table index was reverted for certain devices.
NIOS-70659	Minor	The **Discover Now** option displayed **Failed** for all devices and networks.
NIOS-70655	Minor	The audit log entry for the `set smartnic-debug` command was incorrect.

NIOS-70534	Minor	Deleting a record did not trigger an event for Outbound API.
NIOS-70531	Minor	Tenant, bridge, and domain information was not available for networks in IPAM.
NIOS-70411	Minor	Certain IPAM interfaces displayed incorrect VLAN information.
NIOS-70387	Minor	The NIOS documentation did not contain information about the report categories that are required for the DNS Effective Peak Usage Trend for Flex Grid License dashboard.
NIOS-70368	Minor	The Threat Protection Status for Member dashboard widget did not update the **Megabits Dropped** value.
NIOS-70359	Minor	A global search for a MAC or DNS name resulted in an error message being displayed.
NIOS-70339	Minor	The `set license` command accepted invalid licenses.
NIOS-70259	Minor	Users with read-only access were able to modify extensible attributes.
NIOS-70202	Minor	The **IPAM** > **Network View** > **BGP AS** column displayed both local and remote values.
NIOS-70195	Minor	The session timeout value set in the *SAML Authentication Services* dialog box also sets the session timeout for the Grid.
NIOS-70179	Minor	Selecting a string containing the & character from the IPAM Home > **List** > **Extensible Attributes** > **Value** drop-down list displayed an error.
NIOS-70079	Minor	Configuration synchronization between a Grid Manager and a Network Insight virtual appliance failed.
NIOS-70030	Minor	During a NIOS upgrade on a virtual machine, the IP address is not retained.
NIOS-69870	Minor	After a NIOS upgrade, the RPZ report was missing several fields.
NIOS-69776	Minor	The threshold at which smart NIC drops SNMP packets had to be lowered.
NIOS-69663	Minor	The **Enable GSS-TSIG authentication of clients** option was available at the Grid DNS level but took effect only when enabled at the member level.
NIOS-69397	Minor	The grammatical mistake in the 'Forwarder is running but it fails to connect to none of the indexers' message was fixed.
NIOS-69383	Minor	Microsoft synchronization displays an ERROR status even though the synchronization is successful.
NIOS-69376	Minor	The **Export visible data** option did not export all the members during a Grid upgrade.
NIOS-69311	Minor	When creating a smart folder using the “VLAN ID - has a value” criteria, an HA failover occurred.
NIOS-69160	Minor	During a CSV import, the DHCP option 1 was added instead of DHCP option 52.
NIOS-69105	Minor	In *Grid Reporting Properties*, the *Used %* column displayed **100** for the **Device** category even though the device was unused.
NIOS-69102	Minor	The exported PDF file of the reporting dashboard was not formatted correctly.

NIOS-68989	Minor	The **Send to Syslog** alert action sent only the first line of the alert to the syslog file.
NIOS-68400	Minor	Under certain circumstances, devices are not being completely discovered by Network Insight.
NIOS-68367	Minor	NIOS time zones for certain locations had to be changed.
NIOS-68364	Minor	Documentation about supported NIOS virtual appliances was incomplete.
NIOS-68272	Minor	The DHCP fingerprint database needed to be upgraded.
NIOS-67921	Minor	When creating rules in IPv4 option filters, the “An invalid value was entered” error message was displayed.
NIOS-67559	Minor	Some of the Grid members failed to upload DNS logs to the data collector VM.
NIOS-67479	Minor	If LAN1 was down, the default route in the routing table was not being changed to LAN2.
NIOS-65526	Minor	Unable to update the IP address of a Grid member.
NIOS-65064	Minor	Editing custom forwarders did not work.
NIOS-64958	Minor	When updating the resource_type field of a permission object using the API, although the update was successful, the reference returned as a response to the update was incorrect.
NIOS-64810	Minor	The "httpd config file generation failed" messages were displayed in the debug log files.
NIOS-59901	Minor	Unable to remove a blacklisted RPZ after removing the analytics node from the Grid.

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-84863	During an upgrade from NIOS 8.5.5 to NIOS 8.6.2, upload from the **Grid** > **Upgrade** tab fails.

NIOS-84138	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. **Workaround: Perform a product restart on the ND members for the RabbitMQ changes to be reflected.**
NIOS-82918	Signing a zone fails on SafeNet Luna SA 7 devices and an RSA_generate_key_ex failed error message is displayed. **Workaround:** Restart the DNS service and perform the zone signing operation once again.
NIOS-80276	If you create, modify, or delete IPAM objects, you may experience performance degradation in Grid Manager for these objects.
NIOS-80069	The DNS service is not able to stop and restart by itself when a database initialization is in progress.
NIOS-79971	If you have configured to download the threat protection ruleset on a customized schedule, the latest ruleset does not get downloaded. **Workaround**: Download latest ruleset by clicking the **Download Rules Now** button.
NIOS-79832	If you add a TLSA record in NIOS to a zone that is synchronized with Microsoft Windows Server, a synchronization error may occur because Microsoft Windows Server does not support TLSA records.
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-78494	If you upgrade a NIOS appliance that supports both SR-IOV devices and virtio devices, and in which NIC bonding is enabled, MAC addresses are swapped and one of the nodes is shut down. **Workaround:** Restart the NIOS instance to get the node up and running.
NIOS-77527	Do not make changes to parental control configurations (site properties) during a NIOS upgrade. Modifying the configuration will not take effect on older members waiting to upgrade. This in turn may lead to failure in processing incoming RADIUS messages on the members waiting to upgrade because these changes are not propagated to the DNS service.
NIOS-77388	On NIOS virtual appliances, time is shifted by approximately 6 minutes when you perform a resilver operation. **Workaround:** Turn off automatic time synchronization on ESXi hosts.
NIOS-77382	There is a difference in behaviour between BIND and DNS Cache Acceleration if there are overlapping networks under subscriber data such that the octets do not match the CIDR. For example, 10.120.0.0/16 and 10.120.20.0/16.
NIOS-77375	Major query timeouts occurred during the performance testing of vNIOS for Oracle Cloud Infrastructure.
NIOS-77361	If you create or update a zone or any other record that has a descendant at one or more levels, you may experience some performance degradation.
NIOS-76518	After you upgrade Cisco ISE from version 2.4 to 2.7, the Cisco ISE outbound endpoint does not connect and an error is displayed in the log file.
NIOS-76517	Publishing DHCP data fails for Cisco ISE servers. **Workaround:** Override the publish settings in the notification rule for the DHCP publish in the Cisco ISE endpoint.

NIOS-74196	If the vDCA or vADP service has failed before a NIOS upgrade, Infoblox recommends that you manually reboot the node after the upgrade to see if it recovers.
NIOS-73897	When running NIOS with Intel XXV710 cards on KVM, if you perform a product restart with accelerated Advanced DNS Protection or DNS Cache Acceleration running, a kernel crash occurs. **Workaround:** Terminate the NIOS instance and restart.
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-73650	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 a user with delete permission so that the user details are pushed to the Splunk database for threat indicator caching to work. **Workaround:** Disable and enable the threat indicator caching feature.
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. **Workaround:** Disable and enable the threat indicator caching feature.
NIOS-73648	You must configure an RPZ feed zone before or after enabling threat indicator caching to start the download of threat category information.
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 are duplicated on the **Devices** tab.
NIOS-72977	If you add notification rules with RPZ or Software ADP event notifications, data publish fails.
NIOS-72871	In a multi-site reporting cluster, on the Reporting Clustering Status dashboard > **Search Heads** tab, a reporting member from each site is displayed as an active search head in the following scenarios: • If you change the primary site using the *Grid Reporting Properties* > **Clustering** tab. • If you upgrade a single-site cluster to multi-site and select the new members added to the Grid primary site members. **Workaround:** After the new configuration is completely active and the cluster master shows one reporting member from each site as an active search head, restart the reporting service on the secondary site.
NIOS-72791	NIOS is vulnerable to the Extended Master Secret TLS extension (TLS triple handshake).
NIOS-71369	When a Grid Master Candidate is selected as a subscribing member, then after the Grid Master Candidate promotion, subscription still takes place through the previous Grid Master Candidate member which is a new Grid member.
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-70257	On some occasions during an upgrade or revert process, vNIOS on Azure might become non-responsive. **Workaround:** Reboot the VM to complete the upgrade or revert.

NIOS-69728	Cisco ISE extensible attributes are not configured for DHCP networks.
NIOS-69117	When a reporting member goes offline from the cluster, clustering may be disabled on that peer indexer. So, the hot buckets that were created when clustering was enabled roll into standalone buckets after the peer is restarted. The standalone buckets are not compatible when the reporting member rejoins the cluster. This may result in the search factor and replication factor not being met. This may happen more likely in testing where you may be enabling or disabling clustering. The Splunk documentation mentions it as known behavior. **Workaround:** Rename all the peer standalone buckets (in all the indexes) that have issues as non-standalone buckets by adding the peer GUID. Then reboot all the peers to recover. For example: `mv db_<newest_time>_<oldest_time>_<bucketid> db_<newest_time>_<oldest_time><bucketid>_<guid>`
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.
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.