**What's New**

**Contents**

*Expand all  Collapse all*

The NIOS 8.2 release includes the following new features and enhancements:

**Software-based DNS Cache Acceleration (vDCA) with Capacity Licensing (FLEX)**

You can configure the IB-FLEX virtual platform as a high-performance high-speed and very low latency caching-only name server by enabling virtual DNS cache acceleration on it.

**Threat Insight**

This feature performs analytics to detect malicious activities based on DDI data from your on-premises Grid when the Grid is running NIOS 7.3 or later. (Note: You need the Infoblox Data Connector to transport the data from your on-premises Grid to the Cloud.) If your Grid is running NIOS 8.2.x, you can also configure the on-premises Grid to pull detected malicious domains from Threat insight in the Cloud so you can block applicable traffic using the on-premises DNS firewall configuration.

**RPZs for Blacklisted Domains (RFE-7158)**

You can now add any Response Policy Zones (RPZs) from different DNS and network views to the RPZ list that you use to block malicious domains detected by Threat Insight in the Cloud (on-premises or in the Cloud).

**DNSMessenger Module Support for Threat Insight**

Threat Insight can now detect DNS tunneling activities instigated by the DNSMessenger malware. DNSMessenger is a Remote Access Trojan (RAT) that attackers use to conduct malicious Powershell commands on compromised devices. DNSMessenger uses DNS record queries and responses to create a bidirectional C&C channel that allows the submission of Powershell commands to infected devices and the return of responses back to the attackers.

**Data Exchange Layer (DXL) Support for Outbound Notifications**

In addition to REST (REpresentational State Transfer) enabled endpoints, NIOS also supports sending outbound notifications to DXL (Data Exchange Layer) endpoints.

**Network Insight Enhancements**

This release adds the following enhancements to Network Insight:

- **Cisco ACI Configuration**: Integrating Cisco Application Policy Infrastructure Controller (APIC) on NIOS provides visibility into your Cisco APIC infrastructure, which allows you to view and manage discovered IP addresses through the Cisco ACI cluster. Once the Cisco ACI is integrated, Threat Insight can discover the SDN Controller and Elements (Spine, Leaf, and End Points). You can also view devices that are discovered by a discovery member.
- **Cisco ISE Integration for NetMRI (RFE-6984)**: After you successfully register a NetMRI appliance with NIOS, you can use the Cisco ISE integration feature without having to install the Discovery license. This feature enables you to enhance identity management across devices and applications that are connected to your network routers and switches. You can monitor domain users, the IP addresses they log on to, the login status, and the time duration of the current status in the IPAM tab of Grid Manager.
- **Discovery Diagnostic Tool Improvements (REF-6303)**
  - This release adds the following improvements to the Discovery Diagnostics dialog:
    - View all existing discovery diagnostic tasks that have been executed in the last 12 hours.
    - Enable or disable SNMP debugging for the device.
- **Device Support Data for Discovered Devices (RFE-5452)**
  - Network Insight now provides advanced visibility into device support data, such as the timestamp of the most recent data collection, data function and whether it is supported for the device, as well as the values collected for the device vendor, device model, and device version.

- **Discovered Wi-Fi Data**: Network Insight now saves the discovered data for Wi-Fi access points and displays it in the IPAM tab -> Discovered Data tab of Grid Manager as well as the End Host History dashboard.
- **DNS Resolution for End Hosts (RFE-6541)**: You can now specify whether you want to perform DNS lookups for discovered network devices and end hosts. You can also adjust the throttle for the lookup to control the number of requests sent to the DNS server.
- **VLAN Smart Folder Improvements**: When using smart folders, you can now find VLANs and group objects such as networks, interfaces, and unmanaged IP addresses by discovered VLANs.

Cisco ISE 2.2 Support
This release adds support for Cisco ISE version 2.2. You can integrate Cisco ISE with NIOS to exchange valuable network, user, device, and security-event information.

Cloud Network Automation Enhancement

This release adds the following enhancement for Cloud Network Automation:

- High Performance Virtual Appliances Support for AWS and Azure: This NIOS release supports the following virtual appliances in AWS and Azure: IB-V825, IB-V1425, and IB-V2225. For detailed appliance specifications, see the table on page 4.

vDiscovery Enhancements

This release adds the following enhancements for vDiscovery:

- Support for Multiple DNS Views (RFE-6828): When you configure vDiscovery jobs, you can enable NIOS to automatically create DNS records for discovered IP addresses of VM instances that are served by the appliance. You can now configure NIOS to add DNS records to a specific DNS view so NIOS can handle the auto-creation of DNS records associated with multiple views that manage the same DNS zones.
- Capturing Tags from AWS and Azure: The metadata in the form of tags in AWS and Azure for NIOS can now be captured through a vDiscovery process and saved as extensible attributes.
- Support of Keystone v3 for OpenStack (RFE-7622): NIOS now supports the Keystone server identity service version v2 and v3 when you configure OpenStack as the endpoint server for a vDiscovery job.

Microsoft Management Enhancements

- Microsoft 2016 Support: This release adds support for Microsoft Windows Server 2016.
- SMB Versions 2 and 3 Upgrade (RFE-7216): Infoblox now supports the following versions of SMB (Server Message Block) protocol for Microsoft Windows servers: SMB version 1 (SMBv1), SMB version 2.x (SMBv2.x), and SMB version 3.x (SMBv3.x).
- Synchronizing Microsoft DNS Reporting Data (RFE-5140): You can now configure NIOS to synchronize DNS reporting data with Microsoft servers so you can view both Microsoft and NIOS data in the same NIOS DNS reports. You can also configure the synchronization interval using a newly added CLI command.

DTC Enhancements

This release adds the following enhancements to the DNS Traffic Control feature:

- DTC Health Check (RFE-7044): If you have a multi-tier network architecture and want to monitor the availability of separate components for the DTC server, you can now add a health monitor for each individual IP address or domain configured for the DTC server.
- DNS Scavenging Modifiable Timestamp for DDNS Records (RFE-7114): You can now enable the appliance to modify the creation time of resource records even when the records are unchanged during a DDNS update. This helps prevent unwanted DNS scavenging of valid records.
- Dynamic Load Balancing Methods (RFE-6407): This release adds the following dynamic load balancing methods for DTC: Round Trip Delay (RTD) and SNMP.

Fault Tolerant DNS Caching (RFE-7343)

When an authoritative DNS server experiences an outage, all websites served by the DNS server become inaccessible. Enabling the DNS fault tolerant caching option allows you to access the websites served by the DNS server despite the DNS outage. When you enable this feature, DNS records are retained in the recursive cache even after they expire. Whenever recursive query times out or returns a SERVFAIL response, the appliance returns the cached response to the client instead of the SERVFAIL response.

**NOTE:** Infoblox recommends that you enable this feature right after you upgrade to NIOS 8.2. Enabling this during production requires a DNS service restart, which will clear the current cache.