Splunk® Supported Add-ons Splunk
Add-on for Infoblox released

Generated: 12/23/2019 12:32 pm

Copyright (c) 2019 Splunk Inc. All Rights Reserved
# Table of Contents

**Overview**
- About the Splunk Add-on for Infoblox
- Sourcetypes for the Splunk Add-on for Infoblox
- Release notes for the Splunk Add-on for Infoblox
- Release history for the Splunk Add-on for Infoblox
- Installation overview for the Splunk Add-on for Infoblox

**Installation**
- Hardware and software requirements for the Splunk Add-on for Infoblox
- Install the Splunk Add-on for Infoblox

**Configuration**
- Configure Infoblox to send data to the Splunk Add-on for Infoblox
- Configure inputs for the Splunk Add-on for Infoblox

**Troubleshooting**
- Troubleshoot the Splunk Add-on for Infoblox

**Reference**
- Lookups for the Splunk Add-on for Infoblox
Overview

About the Splunk Add-on for Infoblox

<table>
<thead>
<tr>
<th>Version</th>
<th>1.1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Products</td>
<td>Infoblox NIOS 6.10, NIOS 8.x for DNS Response and threat-protect log and RPZ QNAME event logs</td>
</tr>
<tr>
<td>Add-on has a web UI</td>
<td>No. This add-on does not contain any views.</td>
</tr>
</tbody>
</table>

The Splunk Add-on for Infoblox allows a Splunk software administrator to collect DNS and DHCP logs in syslog format from Infoblox NIOS. This add-on provides the inputs and CIM-compatible knowledge to use with other Splunk apps, such as Splunk Enterprise Security and the Splunk App for PCI Compliance.

Download the Splunk Add-on for Infoblox from Splunkbase.

For a summary of new features, fixed issues, and known issues, see Release Notes for the Splunk Add-on for Infoblox.

For information about installing and configuring the Splunk Add-on for Infoblox, see Installation and configuration overview for the Splunk Add-on for Infoblox.

See Questions related to Splunk Add-on for Infoblox on Splunk Answers.

Sourcetypes for the Splunk Add-on for Infoblox

The Splunk Add-on for Infoblox includes the following source types and event types which map the data to the Splunk Common Information Model (CIM).

<table>
<thead>
<tr>
<th>Sourcetype</th>
<th>Event type</th>
<th>Event example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source type</td>
<td>Event type</td>
<td>Event example</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| infoblox_dn2_rpz            | 2017-03-13T09:48:30-07:00 10.1.1.20 named CEF:0|Infoblox|NIOS|7.3.9-343507|RPZ-QNAME|PASSTHRU|4|app=DNS|dst=10.0.1.10 src=10.0.1.20 spt=55555 view=_default qtype=A msg="rpz QNAME PASSTHRU rewrite z.zzz.com [A] via a.aaa.com"

| infoblox_dhcp               | Sep 8 20:06:30 156.144.4.154 dhcpd[12508]: 220.219.156.13 to 09:bf:58:10:04:09 (SCOTRL1-VM8) via eth1 relay 194.93.83.7 lease-duration 120 |
| infoblox:session_start      | Sep 8 20:04:29 1.80.36.233 dhcpd[12508]: DHCPRELEASE of 131.131.197.150 from cc:88:11:55:78:f3 via e |
| infoblox:threatprotect      | 2017-11-24T12:31:31-08:00 111.111.111.111 adp: CEF:0|Infoblox|NIOS Threat|8.2.1-359366|200001105|DROP NTP TIME requests|4|src=111.222.333.444 spt=123 dst=111.222.333.444 dpt=123 act="DROP" cat="NTP" nat=0 nfpt=0 |

**Release notes for the Splunk Add-on for Infoblox**

Version 1.1.0 of the Splunk Add-on for Infoblox was released on November 2, 2018.

**Compatibility**

Version 1.1.0 of the Splunk Add-on for Infoblox is compatible with the following software, CIM versions, and platforms.

<table>
<thead>
<tr>
<th>Splunk platform versions</th>
<th>6.6.x, 7.0.x, 7.1.x, 7.2, 8.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIM</td>
<td>4.11</td>
</tr>
<tr>
<td>Platforms</td>
<td>Platform independent</td>
</tr>
<tr>
<td>Vendor Products</td>
<td>NIOS 6.10, NIOS 8.x</td>
</tr>
</tbody>
</table>
New features

- Support for the NIOS 8.x log format
- The new sourcetype `infoblox:threatprotect` supports the threat-protect event log of NIOS-8.x
- Existing sourcetype `infoblox:dns` now supports RPZ QNAME messages

Fixed issues

Version 1.1.0 of the Splunk Add-on for Infoblox fixes the following issues:

Known issues

Version 1.1.0 of the Splunk Add-on for Infoblox fixes the following issues. If no issues appear below, no issues have yet been reported:

Third-party software attributions

Version 1.1.0 of the Splunk Add-on for Infoblox does not incorporate any third-party software or libraries.

Release history for the Splunk Add-on for Infoblox

Latest release

The latest version of the Splunk Add-on for Infoblox is version 1.1.0. See Release notes for the Splunk Add-on for Infoblox for the release notes of this latest version.

Version 1.0.2

<table>
<thead>
<tr>
<th>Splunk platform versions</th>
<th>6.3 or later</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIM</td>
<td>4.3 or later</td>
</tr>
<tr>
<td>Platforms</td>
<td>Platform independent</td>
</tr>
<tr>
<td>Vendor Products</td>
<td>Infoblox NIOS 6.10</td>
</tr>
</tbody>
</table>
Fixed issues

Version 1.0.2 of the Splunk Add-on for Infoblox fixes the following issues.

<table>
<thead>
<tr>
<th>Date</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-07-01</td>
<td>ADDON-7931</td>
<td>The Add-on doesn't provide all the fields required by CIM Network Resolution(DNS) data model. The fields such as answer, query, dest are not mapped and extracted.</td>
</tr>
<tr>
<td>2016-06-23</td>
<td>ADDON-9979</td>
<td>Incorrect regex of the action field in sourcetype infoblox:dhcp.</td>
</tr>
<tr>
<td>2016-06-21</td>
<td>ADDON-7032</td>
<td>The src_ip and dest_ip are not correct in DHCPREQUEST, DHCPINFORM, DHCPRELEASE message.</td>
</tr>
</tbody>
</table>

Known issues

Version 1.0.2 of the Splunk Add-on for Infoblox contains no known issues.

Third-party software attributions

Version 1.0.2 of the Splunk Add-on for Infoblox does not incorporate any third-party software or libraries.

Version 1.0.1

Version 1.0.1 of the Splunk Add-on for Infoblox has the same compatibility specifications as version 1.0.2.

Fix issues

<table>
<thead>
<tr>
<th>Resolved date</th>
<th>Defect number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-11-02</td>
<td>ADDON-6305</td>
<td>Errors in eventgen.</td>
</tr>
</tbody>
</table>

Known issues

Version 1.0.1 of the Splunk Add-on for Infoblox contains no known issues.
Version 1.0.0

Version 1.0.0 of the Splunk Add-on for Infoblox has the same compatibility specifications as version 1.0.1.

New features

Version 1.0.0 of the Splunk Add-on for Infoblox had the following new features.

<table>
<thead>
<tr>
<th>Date</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-08-31</td>
<td>ADDON-1370</td>
<td>Create a new add-on for Infoblox NIOS.</td>
</tr>
</tbody>
</table>

Known issues

Version 1.0.0 of the Splunk Add-on for Infoblox contained no known issues.

Third-party software attributions

Version 1.0.0 of the Splunk Add-on for Infoblox does not incorporate any third-party software or libraries.

Installation overview for the Splunk Add-on for Infoblox

Complete the following steps to install and configure this add-on on your supported platform.

1. Install the Splunk Add-on for Infoblox.
2. Configure Infoblox to send data to the Splunk Add-on for Infoblox.
3. Configure inputs for the Splunk Add-on for Infoblox.
Installation

Hardware and software requirements for the Splunk Add-on for Infoblox

Infoblox setup requirements

You must have access to the Grid Manager web interface so that you can configure your NIOS appliances and management stations to send data to the Splunk platform over syslog.

Splunk platform requirements

Because this add-on runs on the Splunk platform, all of the system requirements apply for the Splunk software that you use to run this add-on.

- For Splunk Enterprise system requirements: see "System Requirements" in the Splunk Enterprise Installation Manual.
- For Splunk Light system requirements: see "System Requirements" in the Splunk Light Installation Manual.
- If you are managing on-premises forwarders to get data into Splunk Cloud, see "System Requirements" in the Splunk Enterprise Installation Manual, which includes information about forwarders.

Install the Splunk Add-on for Infoblox

Use the tables below to determine where and how to install this add-on in a distributed deployment of Splunk Enterprise. See the "installation walkthrough" section at the bottom for links to installation instructions specific to a single-instance deployment, distributed deployment, Splunk Cloud, or Splunk Light.

Distributed installation of this add-on

This table provides a quick reference for installing this add-on to a distributed deployment of Splunk Enterprise.

<table>
<thead>
<tr>
<th></th>
<th>Supported</th>
<th>Required</th>
<th>Comments</th>
</tr>
</thead>
</table>

6
<table>
<thead>
<tr>
<th>Splunk instance type</th>
<th>Supported</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Heads</td>
<td>Yes</td>
<td>Install this add-on to all search heads where Infoblox knowledge management is required.</td>
</tr>
<tr>
<td>Indexers</td>
<td>Yes</td>
<td>Conditional</td>
</tr>
<tr>
<td>Heavy Forwarders</td>
<td>Yes</td>
<td>See comments</td>
</tr>
<tr>
<td>Universal Forwarders</td>
<td>Yes</td>
<td>Supported for deploying the configured add-on.</td>
</tr>
<tr>
<td>Light Forwarders</td>
<td>Yes</td>
<td>Supported for deploying the configured add-on.</td>
</tr>
</tbody>
</table>

**Distributed deployment compatibility**

This table provides a quick reference for the compatibility of this add-on with Splunk distributed deployment features.

<table>
<thead>
<tr>
<th>Distributed deployment feature</th>
<th>Supported</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Head Clusters</td>
<td>Yes</td>
<td>You can install this add-on on a search head cluster for all search-time functionality, but only configure inputs on a forwarder to avoid duplicate data collection. Before installing this add-on to a cluster, remove the <code>eventgen.conf</code> files and all files in the <code>Samples</code> folder.</td>
</tr>
<tr>
<td>Indexer Clusters</td>
<td>Yes</td>
<td>Before installing this add-on to a cluster, remove the <code>eventgen.conf</code> files and all files in the <code>Samples</code> folder.</td>
</tr>
<tr>
<td>Deployment Server</td>
<td>Yes</td>
<td>Supported for deploying the configured add-on.</td>
</tr>
</tbody>
</table>
Installation walkthrough

See "Installing add-ons" in Splunk Add-Ons for detailed instructions describing how to install a Splunk add-on in the following deployment scenarios:

- single-instance Splunk Enterprise
- distributed Splunk Enterprise
- Splunk Cloud
- Splunk Light
Configuration

Configure Infoblox to send data to the Splunk Add-on for Infoblox

To enable the Splunk Add-on for Infoblox to collect data from Infoblox NIOS, you need to use the Grid Manager web interface to configure your NIOS appliances and management stations to produce syslog output and push it to the data collection node of your Splunk platform installation. You can configure Infoblox to send data to Splunk over TCP or UDP or you can export the syslog data into a dump file and configure the add-on to monitor the dump file.

For instructions on how to configure syslog, see pages 1013 - 1016 in the Infoblox NIOS Administrator Guide at http://dloads.infoblox.com/direct/appliance//NIOS/NIOS_AdminGuide_6.10.pdf. For instructions on how to download the syslog file to a directory, see page 1017 in the Infoblox NIOS Administrator Guide.

Next, configure your data collection node to receive data from Infoblox NIOS as described in "Configure inputs for the Splunk Add-on for Infoblox".

Configure inputs for the Splunk Add-on for Infoblox

The Splunk Add-on for Infoblox handles inputs through TCP or UDP. There are two ways to capture this data.

1. Create a TPC/UDP input to capture the data sent on the port you have configured in Infoblox NIOS.

2. If you are using a syslog aggregator, create a monitor input to monitor the file or files generated by the aggregator.

TCP/UDP input

In the Splunk platform node handling data collection, configure the TCP/UDP input to match your configurations in Infoblox NIOS and set your source type to infoblox:port. The CIM mapping and dashboard panels are dependent on this source type.
For information on how to configure a Splunk forwarder or single-instance to receive a syslog input, see "Get data from TCP and UDP ports" in the Getting Data In manual.

**Monitor input**

If you are using a syslog aggregator, on the Splunk platform node handling data collection, set up a monitor input to monitor the file or files that are generated and set your source type to `infoblox:file`. The CIM mapping and dashboard panels are dependent on this source type.

See "Monitor files and directories" in the Getting Data In manual for information about setting up a monitor input.

**Validate data collection**

Once you have configured the input, run this search to check that you are ingesting the data that you expect. The add-on converts the `infoblox:port` and `infoblox:file` source types to `infoblox:dhcp` and `infoblox:dns` according to the content of events.

```
sourcetype=infoblox*
```
Troubleshooting

Troubleshoot the Splunk Add-on for Infoblox

General troubleshooting

For helpful troubleshooting tips that you can apply to all add-ons, see "Troubleshoot add-ons" in Splunk Add-ons. For additional resources, see "Support and resource links for add-ons" in Splunk Add-ons.

Data ingestion problems

Verify that you have configured the input correctly by confirming that:

- you have configured the correct IP address of the Splunk platform node responsible for data collection in your Infoblox NIOS configuration.
- the port that you configured in your Infoblox NIOS configuration matches the port you configured in your syslog input configuration.
- the port that you are using for this input does not conflict with any other inputs.
- If monitored through TCP or UDP, the input is configured to set the source type to infoblox:port and if monitored through file monitoring, the input is configured to set the source type to infoblox:file.
- you are searching the correct index. By default, this add-on uses the main index.
Reference

Lookups for the Splunk Add-on for Infoblox

The Splunk Add-on for Infoblox has 3 lookups. The lookup files map fields from Infoblox systems to CIM-compliant values in the Splunk platform. The lookup files are located in $SPLUNK_HOME/etc/apps/Splunk_TA_infoblox/lookups.

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>infoblox_dns_query_type.csv</td>
<td>Maps the_query_type, such as A and SRV, to expected values required by DNS model.</td>
</tr>
<tr>
<td>infoblox_dns_reply_code_id.csv</td>
<td>Maps reply_code_id to reply_code.</td>
</tr>
<tr>
<td>infoblox_severity_lookup</td>
<td>Maps severity_id to expected values required by Intrusion Detection and Alert Models.</td>
</tr>
</tbody>
</table>