Splunk® Supported Add-ons Splunk Add-on for Citrix NetScaler released

Generated: 9/04/2019 6:29 pm
# Table of Contents

Overview.................................................................................................................................1  
   About the Splunk Add-on for Citrix NetScaler.................................................................1
   Splunk Add-on for Citrix Netscaler...................................................................................1
   Source types for the Splunk Add-on for Citrix NetScaler................................................1
   Release notes for the Splunk Add-on for Citrix NetScaler...............................................3
   Release history for the Splunk Add-on for Citrix NetScaler............................................3
   Hardware and software requirements for the Splunk Add-on for Citrix NetScaler...........10
   Installation and configuration overview for the Splunk Add-on for Citrix NetScaler........11

Installation..............................................................................................................................12
   Install the Splunk Add-on for Citrix NetScaler...............................................................12

Configuration.........................................................................................................................15
   Configure Citrix NetScaler to produce data via IPFIX or syslog.................................15
   Configure NITRO API inputs for the Splunk Add-on for Citrix NetScaler......................15
   Configure IPFIX inputs for the Splunk Add-on for Citrix NetScaler.............................22
   Configure syslog inputs for the Splunk Add-on for NetScaler.........................................22

Troubleshooting....................................................................................................................24
   Troubleshoot the Splunk Add-on for Citrix NetScaler...................................................24

Reference..................................................................................................................................25
   Lookups for the Splunk Add-on for Citrix NetScaler.........................................................25
Overview

About the Splunk Add-on for Citrix NetScaler

Splunk Add-on for Citrix NetScaler

<table>
<thead>
<tr>
<th>Version</th>
<th>6.3.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor products</td>
<td>Citrix NetScaler versions 10-12</td>
</tr>
<tr>
<td>Add-on has a web UI</td>
<td>Yes. This add-on contains views for configuration.</td>
</tr>
</tbody>
</table>

The Splunk Add-on for Citrix NetScaler allows a Splunk software administrator to collect data from Citrix NetScaler servers using syslog, IPFIX, and the NITRO API.

This add-on provides the inputs as well as CIM-compatible and ITSI-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 Citrix Netscaler from Splunkbase.

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

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

See Questions related to Splunk Add-on for Citrix Netscaler on Splunk Answers.

Source types for the Splunk Add-on for Citrix NetScaler

The Splunk Add-on for Citrix NetScaler supplies or expects the following source types, depending on the data sources and collection methods that you configure: syslog, IPFIX, or the NITRO API.

<table>
<thead>
<tr>
<th>Collection method</th>
<th>Description</th>
<th>Source type</th>
<th>CIM and ITSI module</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Source/Source Type</th>
<th>Description</th>
<th>Source Type</th>
<th>Compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>NITRO API</td>
<td>To collect NetScaler status data from any of the more than 1000 endpoints of the NITRO API, configure the modular input provided in this add-on.</td>
<td>citrix:netscaler:nitro</td>
<td>Inventory, Load Balancer</td>
</tr>
<tr>
<td>IPFIX</td>
<td>Information about network sessions and connections, as well as syslog data for logins, logouts, device status changes, and network status changes. To collect data using the IPFIX protocol, use the Splunk Add-on for IPFIX, then configure IPFIX inputs. Manually set the source type to <code>citrix:netscaler:ipfix</code> for all IPFIX input data. The add-on automatically appends <code>:syslog</code> to data that is in this format.</td>
<td>citrix:netscaler:ipfix:syslog</td>
<td>Web, Load Balancer, Authentication, Network Traffic, Load Balancer</td>
</tr>
<tr>
<td>UDP</td>
<td>Events including logins, logouts, device status changes, and network status changes. If you configure your Citrix NetScaler device to produce data over syslog, use this source type when you set up a UDP listener on your collector node.</td>
<td>citrix:netscaler:syslog</td>
<td>Authentication, Network Traffic, Load Balancer</td>
</tr>
<tr>
<td>Internal logs</td>
<td>The add-on's internal logs are automatically source typed as</td>
<td>citrix:netscaler</td>
<td>None</td>
</tr>
</tbody>
</table>
Release notes for the Splunk Add-on for Citrix NetScaler

Version 6.3.0 of the Splunk Add-on for Citrix NetScaler was released on January 14, 2019.

Compatibility

Version 6.3.0 of the Splunk Add-on for Citrix NetScaler is compatible with the following software, CIM versions, and platforms.

- Splunk platform versions 7.2.x, 7.1.x, 7.0.x, 6.6.x
- CIM 4.11
- Platforms Platform independent
- Vendor Products Citrix NetScaler versions 10, 11, and 12

Migration guide

Upgrading from 6.2.0 to 6.3.0 of the Splunk Add-on for Citrix NetScaler is not supported. You must reconfigure all inputs, appliances and templates after upgrading. To avoid data loss, back up your local configurations before upgrading.

This version of the add-on drops support for Splunk platform versions older than 6.6.x. If you are running older versions of the Splunk platform, upgrade them to a minimum of 6.6.x before upgrading.

New features

Version 6.3.0 of the Splunk Add-on for Citrix NetScaler has the following new features.

- Shows warning when a newly added account duplicates an existing endpoint mapping
- Proxy support
- Validates credentials for newly added appliances
- Supports HTTPS as the default

Fixed issues

Version 6.3.0 of the Splunk Add-on for Citrix NetScaler contains the following fixed issues:

<table>
<thead>
<tr>
<th>Date resolved</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-07-12</td>
<td>ADDON-17633</td>
<td>duplicate line in Default tags.conf</td>
</tr>
<tr>
<td></td>
<td>ADDON-8326</td>
<td>citrix_netscaler_availability.status.csv header line is broken</td>
</tr>
</tbody>
</table>

Known issues

Version 6.3.0 of the Splunk Add-on for Citrix NetScaler has the following known issues. If no issues appear below, no issues have yet been reported:

<table>
<thead>
<tr>
<th>Date filed</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-05-11</td>
<td>ADDON-3993</td>
<td>Description field can be interpreted as binary instead of string</td>
</tr>
</tbody>
</table>

Third-party software attributions

Version 6.3.0 of the Splunk Add-on for Citrix NetScaler incorporates the following third-party software or libraries.

- jQuery
- select2
- jquery-ui
- moment.js
- jqTree
- bootstrap
- underscore
- Backbone.Validation
- jquery-resize-plugin
- low-pro-for-jquery
- sax.js
- lodash
- intro.js
- highcharts

Release history for the Splunk Add-on for Citrix NetScaler

The latest version of the Splunk Add-on for Citrix NetScaler is version 6.3.0. See Release notes for the Splunk Add-on for Citrix NetScaler for the release notes of this latest version.
Version 6.2.0

Version 6.2.0 of the Splunk Add-on for Citrix NetScaler is compatible with the following software, CIM versions, and platforms.

<table>
<thead>
<tr>
<th>Splunk platform versions</th>
<th>6.3.X and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIM</td>
<td>4.2 and later</td>
</tr>
<tr>
<td>Platforms</td>
<td>Platform independent</td>
</tr>
<tr>
<td>Vendor Products</td>
<td>Citrix NetScaler versions 10.X and later</td>
</tr>
</tbody>
</table>

Migration guide

This add-on is intended to replace the community-supported app, Splunk for Citrix NetScaler with AppFlow. If you are currently using Splunk for Citrix NetScaler with AppFlow, disable the app so that this add-on's inputs do not conflict with it.

This version of the add-on drops support for Splunk platform versions older than 6.3.X. If you are running older versions of the Splunk platform, upgrade them to a minimum of 6.3.X before upgrading the add-on.

New features

Version 6.2.0 of the Splunk Add-on for Citrix NetScaler has the following new features.

<table>
<thead>
<tr>
<th>Date</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-05-27</td>
<td>ADDON-9718</td>
<td>Improved add-on configuration UI.</td>
</tr>
<tr>
<td>2016-05-23</td>
<td>ADDON-7770</td>
<td>Mapped to new fields in the ITSI Load Balancer module.</td>
</tr>
</tbody>
</table>

Fixed issues

Version 6.2.0 of the Splunk Add-on for Citrix NetScaler contains no fixed issues.

Known issues

Version 6.2.0 of the Splunk Add-on for Citrix NetScaler has the following known issues.

<table>
<thead>
<tr>
<th>Date filed</th>
<th>Defect</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Number</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2016-01-30</td>
<td>ADDON-7646</td>
<td>FIPS mode is not supported by this add-on. For a workaround, see Add-ons and FIPS mode in the <em>Splunk Add-ons</em> manual.</td>
</tr>
<tr>
<td>2016-01-13</td>
<td>ADDON-5325</td>
<td><code>requireClientCert=true</code> in <code>server.conf</code> is not supported by add-ons using modular inputs and REST. If this setting is enabled in <code>server.conf</code>, communication is broken between the modular input and splunkd and the add-on stops collecting data. The following error appears in the <code>splunkd.log</code>: &quot;SSL3_GET_CLIENT_CERTIFICATE: peer did not return a certificate.&quot; The workaround is to set <code>requireClientCert=false</code>.</td>
</tr>
<tr>
<td>2015/11/20</td>
<td>ADDON-6592 / SPL-110199</td>
<td>Add-on has a warning upon startup &quot;Invalid key in stanza [citrix_netscaler] in /opt/splunk/etc/apps/Splunk_TA_citrix-netscaler/default/inputs.conf, line 4: start_by_shell (value: false).&quot; when running on Splunk 6.3. This warning is invalid and can be ignored.</td>
</tr>
<tr>
<td>2015/11/20</td>
<td>ADDON-6122</td>
<td>The field &quot;mem&quot; gives spurious data due to a bug in the NetScaler API.</td>
</tr>
<tr>
<td>2015/10/29</td>
<td>SPL-104398</td>
<td>For users running the Splunk platform on Ubuntu on versions prior to 6.3.0, the <code>start_by_shell=false</code> setting will not take effect and the Splunk platform will display a warning message on startup. Workaround: update your Splunk software to version 6.3.0 or later.</td>
</tr>
<tr>
<td>2015/06/10</td>
<td>ADDON-4219</td>
<td>In the template configuration screen of the modular input, if the user includes a metric and endpoint name that exceeds the width of the Selected Metrics field, there is no scroll to see the full name.</td>
</tr>
<tr>
<td>2015/06/10</td>
<td>ADDON-4219</td>
<td>In the template configuration screen of the modular input, if the number of metrics added to the template is larger than the Selected Metrics field can display by default, the user must scroll to the bottom of the Selected Metrics field manually to see the latest metric added.</td>
</tr>
<tr>
<td>2015/06/05</td>
<td>ADDON-4177</td>
<td>Endpoint field in the modular input configuration does not support spaces. Workaround: If your API call requires spaces, encode them using <code>%20</code>.</td>
</tr>
<tr>
<td>2015/05/14</td>
<td>SPL-101449 / ADDON-3993</td>
<td>If you enter either &quot;t&quot; or &quot;f&quot; in the description field of a Task, Splunk Enterprise interprets it as binary instead of a string and stores the value as 1 or 0, respectively.</td>
</tr>
</tbody>
</table>
**Third-party software attributions**

Version 6.2.0 of the Splunk Add-on for Citrix NetScaler incorporates the following third-party software or libraries.

- Bootstrap
- HttpLib2
- select2
- SortedContainers

**Version 6.1.0**

Version 6.1.0 of the Splunk Add-on for Citrix NetScaler is compatible with the following software, CIM versions, and platforms.

<table>
<thead>
<tr>
<th>Splunk platform versions</th>
<th>6.0 and above</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIM</td>
<td>4.2 and above</td>
</tr>
<tr>
<td>Platforms</td>
<td>Platform independent</td>
</tr>
<tr>
<td>Vendor Products</td>
<td>Citrix NetScaler versions 10.X and above</td>
</tr>
</tbody>
</table>

**Migration guide**

This add-on is intended to replace the community-supported app, Splunk for Citrix NetScaler with AppFlow. If you are currently using Splunk for Citrix NetScaler with AppFlow, disable the app so that this add-on’s inputs do not conflict with it.

**New features**

Version 6.1.0 of the Splunk Add-on for Citrix NetScaler has the following new features.

<table>
<thead>
<tr>
<th>Date</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015/11/08</td>
<td>ADDON-6060</td>
<td>Modify the add-on to collect data needed to populate the load balancer module for ITSI.</td>
</tr>
<tr>
<td>2015/11/03</td>
<td>ADDON-6282</td>
<td>Add tags to map to load balancer module.</td>
</tr>
</tbody>
</table>
**Fixed issues**

Version 6.1.0 of the Splunk Add-on for Citrix NetScaler fixes the following issues.

<table>
<thead>
<tr>
<th>Resolved date</th>
<th>Defect number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015/11/24</td>
<td>ADDON-6513</td>
<td>Should collect AVL_STATUS and FAILOVER_STATUS as 0 or 1 rather than strings.</td>
</tr>
<tr>
<td>2015/11/24</td>
<td>ADDON-6509</td>
<td>Missing the field storage_used_percent.</td>
</tr>
<tr>
<td>2015/11/11</td>
<td>ADDON-6383</td>
<td>Additional fields need to be collected by the add-on to support load balancer module in ITSI.</td>
</tr>
<tr>
<td>2015/11/11</td>
<td>ADDON-6379</td>
<td>Alias needed from memusagepcnt to mem_used_percent.</td>
</tr>
<tr>
<td>2015/11/09</td>
<td>ADDON-4052</td>
<td>Configuration objects such as servers and templates defined in different add-ons with same Destination App encounter naming conflicts.</td>
</tr>
<tr>
<td>2015/11/09</td>
<td>ADDON-4052</td>
<td>Configuration objects such as servers and templates defined in different add-ons with same Destination App encounter naming conflicts.</td>
</tr>
<tr>
<td>2015/11/08</td>
<td>ADDON-5531</td>
<td>Typos in props.conf and deviations from best practices for timestamping, index-time settings, and some field aliases.</td>
</tr>
</tbody>
</table>

**Known issues**

Version 6.1.0 of the Splunk Add-on for Citrix NetScaler has the following known issues.

<table>
<thead>
<tr>
<th>Date filed</th>
<th>Defect number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-01-30</td>
<td>ADDON-7646</td>
<td>FIPS mode is not supported by this add-on. For a workaround, see Add-ons and FIPS mode in the Splunk Add-ons manual.</td>
</tr>
<tr>
<td>2016-01-13</td>
<td>ADDON-5325</td>
<td>requireClientCert=true in server.conf is not supported by add-ons using modular inputs and REST. If this setting is enabled in server.conf, communication is broken between the modular input and splunkd and the add-on stops collecting data. The following error appears in the splunkd.log: &quot;SSL3_GET_CLIENT_CERTIFICATE:peer did not return a certificate.&quot; The workaround is to set requireClientCert=false.</td>
</tr>
<tr>
<td>2015/11/20</td>
<td>ADDON-6592 / SPL-110199</td>
<td>Add-on has a warning upon startup &quot;Invalid key in stanza [citrix_netscaler] in /opt/splunk/etc/apps/Splunk_TA_citrix-netscaler/default/inputs.conf,</td>
</tr>
<tr>
<td>Date filed</td>
<td>Defect number</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>2015/11/20</td>
<td>ADDON-6122</td>
<td>The field &quot;mem&quot; gives spurious data due to a bug in the NetScaler API.</td>
</tr>
<tr>
<td>2015/10/29</td>
<td>SPL-104398</td>
<td>For users running the Splunk platform on Ubuntu on versions prior to 6.3.0, the <code>start_by_shell=false</code> setting will not take effect and the Splunk platform will display a warning message on startup. Workaround: update your Splunk software to version 6.3.0 or later.</td>
</tr>
<tr>
<td>2015/06/10</td>
<td>ADDON-4219</td>
<td>In the template configuration screen of the modular input, if the user includes a metric and endpoint name that exceeds the width of the Selected Metrics field, there is no scroll to see the full name.</td>
</tr>
<tr>
<td>2015/06/10</td>
<td>ADDON-4219</td>
<td>In the template configuration screen of the modular input, if the number of metrics added to the template is larger than the Selected Metrics field can display by default, the user must scroll to the bottom of the Selected Metrics field manually to see the latest metric added.</td>
</tr>
<tr>
<td>2015/06/05</td>
<td>ADDON-4177</td>
<td>Endpoint field in the modular input configuration does not support spaces. Workaround: If your API call requires spaces, encode them using <code>%20</code>.</td>
</tr>
<tr>
<td>2015/05/14</td>
<td>SPL-101449 / ADDON-3993</td>
<td>If you enter either &quot;t&quot; or &quot;f&quot; in the description field of a Task, Splunk Enterprise interprets it as binary instead of a string and stores the value as 1 or 0, respectively.</td>
</tr>
</tbody>
</table>

**Third-party software attributions**

Version 6.1.0 of the Splunk Add-on for Citrix NetScaler incorporates the following third-party software or libraries.

- Bootstrap
- Bootstrap table
- jqBootstrapValidation
- Httplib2
- select2
- SortedContainers

**Version 6.0.0**

Version 6.0.0 of the Splunk Add-on for Citrix NetScaler has the same
compatibility specifications as 6.1.0.

**Migration guide**

This add-on is intended to replace the community-supported app, Splunk for Citrix NetScaler with AppFlow. If you are currently using Splunk for Citrix NetScaler with AppFlow, disable the app so that this add-on's inputs do not conflict with it.

**New features**

Version 6.0.0 of the Splunk Add-on for Citrix NetScaler has the following new features.

<table>
<thead>
<tr>
<th>Date</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/26/15</td>
<td>ADDON-2268</td>
<td>New Splunk-supported add-on for Citrix NetScaler data collection and CIM mapping.</td>
</tr>
</tbody>
</table>

**Known issues**

Version 6.0.0 of the Splunk Add-on for Citrix NetScaler has the following known issues.

<table>
<thead>
<tr>
<th>Date</th>
<th>Defect number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015/09/15</td>
<td>ADDON-5531</td>
<td>Typos in <code>props.conf</code> and deviations from best practices for timestamping, index-time settings, and some field aliases.</td>
</tr>
<tr>
<td>2015/06/10</td>
<td>ADDON-4219</td>
<td>In the template configuration screen of the modular input, if the user includes a metric and endpoint name that exceeds the width of the Selected Metrics field, there is no scroll to see the full name.</td>
</tr>
<tr>
<td>2015/06/10</td>
<td>ADDON-4219</td>
<td>In the template configuration screen of the modular input, if the number of metrics added to the template is larger than the Selected Metrics field can display by default, the user must scroll to the bottom of the Selected Metrics field manually to see the latest metric added.</td>
</tr>
<tr>
<td>2015/06/05</td>
<td>ADDON-4177</td>
<td>Endpoint field in the modular input configuration does not support spaces. Workaround: If your</td>
</tr>
<tr>
<td>Date</td>
<td>Defect number</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>API call requires spaces, encode them using %20.</td>
</tr>
<tr>
<td>2015/05/26</td>
<td>ADDON-4052</td>
<td>Configuration objects such as servers and templates defined in different add-ons with same Destination App encounter naming conflicts.</td>
</tr>
<tr>
<td>2015/05/14</td>
<td>SPL-101449 / ADDON-3993</td>
<td>If you enter either &quot;t&quot; or &quot;f&quot; in the description field of a Task, Splunk Enterprise interprets it as binary instead of a string and stores the value as 1 or 0, respectively.</td>
</tr>
</tbody>
</table>

**Third-party software attributions**

Version 6.0.0 of the Splunk Add-on for Citrix NetScaler incorporates the following third-party software or libraries.

- Bootstrap
- Bootstrap table
- jqBootstrapValidation
- Httplib2
- select2
- SortedContainers

**Hardware and software requirements for the Splunk Add-on for Citrix NetScaler**

To install and configure the Splunk Add-on for Citrix NetScaler, you must be a member of the admin or sc_admin role.

**Data collection dependencies**

The Splunk Add-on for Citrix NetScaler supports multiple data inputs, each capable of collecting different data from your Citrix NetScaler appliances. For more information about which kind of data you can collect with which input, refer to the source types page.

If you want to collect data using the IPFIX protocol, install the Splunk Add-on for IPFIX on your data collection nodes.
Sizing guidelines

The Splunk Add-on for Citrix NetScaler uses a multiple thread and multiple process design. It can collect data from up to 15 NetScaler appliances on an 8-core machine with 8 GB of memory.

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.

Installation and configuration overview for the Splunk Add-on for Citrix NetScaler

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

1. Install the Splunk Add-on for Citrix NetScaler.
2. If you want to gather data via IPFIX or syslog, configure your Citrix NetScaler appliance to produce logs in those formats.
3. On the part of your Splunk platform architecture that is performing data collection for the add-on, configure the inputs that you want to use:
   1. Configure modular inputs.
   2. Configure an IPFIX input.
   3. Configure a syslog input.
Installation

Install the Splunk Add-on for Citrix NetScaler

1. Get the Splunk Add-on for Citrix NetScaler by downloading it from Splunkbase or browsing to it using the app browser within Splunk Web.
2. Determine where and how to install this add-on in your deployment, using the tables on this page.
3. Perform any prerequisite steps before installing, if required and specified in the following tables.
4. Complete your installation.

If you need step-by-step instructions on how to install an add-on in your specific deployment environment, see the following installation walkthrough section for links to installation instructions specific to a single-instance deployment, distributed deployment, Splunk Cloud, or Splunk Light.

Distributed deployments

Use the following tables to determine where and how to install this add-on in a distributed deployment of Splunk Enterprise or any deployment for which you are using forwarders to get your data in. Depending on your environment, your preferences, and the requirements of the add-on, you may need to install the add-on in multiple places.

Where to install this add-on

Unless otherwise noted, all supported add-ons can be safely installed to all tiers of a distributed Splunk platform deployment. See Where to install Splunk add-ons in Splunk Add-ons for more information.

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

<table>
<thead>
<tr>
<th>Splunk instance type</th>
<th>Supported</th>
<th>Required</th>
<th>Actions required / Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Heads</td>
<td>Yes</td>
<td>Yes</td>
<td>Install this add-on to all search heads where Citrix NetScaler knowledge management is required.</td>
</tr>
</tbody>
</table>
Splunk recommends that you turn add-on visibility off on your search heads to prevent data duplication errors that can result from running inputs on your search heads instead of (or in addition to) on your data collection node.

<table>
<thead>
<tr>
<th>Splunk instance type</th>
<th>Supported</th>
<th>Required</th>
<th>Actions required / Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indexers</td>
<td>Yes</td>
<td>Conditional</td>
<td>Not required if you use heavy forwarders to collect data. Required if you use universal or light forwarders to collect data.</td>
</tr>
<tr>
<td>Heavy Forwarders</td>
<td>Yes</td>
<td>See comments</td>
<td>Required for modular inputs. If you are not using the NITRO API modular inputs, any forwarder type is supported.</td>
</tr>
<tr>
<td>Universal Forwarders</td>
<td>Yes</td>
<td>See comments</td>
<td>Supported for IPFIX and UDP inputs only.</td>
</tr>
</tbody>
</table>

**Distributed deployment feature compatibility**

This table describes the compatibility of this add-on with Splunk distributed deployment features.

<table>
<thead>
<tr>
<th>Distributed deployment feature</th>
<th>Supported</th>
<th>Actions required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Head Clusters</td>
<td>Yes</td>
<td>Disable add-on visibility on search heads. You can install this add-on on a search head cluster for all search-time functionality, but configure inputs on forwarders to avoid duplicate data collection. Before installing this add-on to a cluster, make the following changes to the add-on package: 1. Remove the <code>eventgen.conf</code> files and all files in the <code>samples</code> folder 2. Remove the <code>inputs.conf</code> file.</td>
</tr>
<tr>
<td>Indexer Clusters</td>
<td>Yes</td>
<td>Before installing this add-on to a cluster, make the following changes to the add-on package:</td>
</tr>
</tbody>
</table>
1. Remove the `eventgen.conf` files and all files in the `samples` folder
2. Remove the `inputs.conf` file.

### Deployment Server

<table>
<thead>
<tr>
<th>Supported</th>
<th>Actions required</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Supported for deploying unconfigured add-ons only. Using a deployment server to deploy the configured add-on to multiple forwarders acting as data collectors causes duplication of data.</td>
</tr>
</tbody>
</table>

### Installation walkthroughs

The *Splunk Add-Ons* manual includes an Installing add-ons guide that helps you successfully install any Splunk-supported add-on to your Splunk platform.

For a walkthrough of the installation procedure, follow the link that matches your deployment scenario:

- Single-instance Splunk Enterprise
- Distributed Splunk Enterprise
- Splunk Cloud
- Splunk Light
Configuration

Configure Citrix NetScaler to produce data via IPFIX or syslog

The Splunk Add-on for Citrix NetScaler supports multiple data input methods. If you are only collecting data via the modular input, which pulls data from your Citrix NetScaler devices using the NITRO API, you can skip this step.

If you want to collect data about traffic on your network, authentication activity, and web server data, collect data via IPFIX as well, as this data is not available via the NITRO REST API. You also have the option to collect authentication and network data via syslog, if you prefer.

Configure Citrix NetScaler to produce IPFIX data

1. Follow the instructions in the AppFlow configuration guide and set your Splunk Enterprise data collection node as the collector.
2. If you have not already done so, install the Splunk Add-on for IPFIX on your data collection node.
3. Next, configure the IPFIX input on your Splunk Enterprise data collection node.

Configure Citrix NetScaler to produce syslog data

1. Follow the instructions to configure syslog on a Citrix NetScaler appliance.
2. Next, configure the syslog input on your Splunk Enterprise data collection node.

Configure NITRO API inputs for the Splunk Add-on for Citrix NetScaler

The Splunk Add-on for Citrix NetScaler collects data from your Citrix NetScaler appliances from the NITRO REST API using a modular input. You can configure this input using Splunk Web on your heavy forwarder, or manually in the configuration files by following these steps:

1. Specify your communication method.
2. Configure a connection to your Citrix NetScaler appliances to define where the add-on should get the data.
3. Create one or more metric templates made up of one or many NITRO API metric endpoints to define what data to collect.
4. Configure inputs. For each input, you select one or more appliances, one or more templates, and set the polling interval and destination index for the data.

The following sections describe these steps in more detail.

**Specify your communication method**

By default, communication from the Splunk Add-on for Citrix Netscaler to your Netscaler servers are encrypted via HTTPS with SSL-certificate validation enabled. If your Netscaler server is configured with HTTPS and a valid CA signed certificate, then the communication to Netscaler server works with default configurations.

**HTTPS using a self-signed certificate**

If your Netscaler server is configured with HTTPS using a self-signed certificate, follow these steps:

1. Download the CA certificate of the Netscaler server in PEM format.
2. Place the CA certificate in your $SPLUNK_HOME/etc/apps/Splunk_TA_citrix-netscaler/local folder.
4. Provide the path of the CA certificate file, including the file name, in $SPLUNK_HOME/etc/apps/Splunk_TA_citrix-netscaler/local/splunk_ta_citrix_netscaler_settings.conf in the additional_parameters stanza.
5. Save your changes.
6. Restart the Splunk platform.

Alternatively, you can follow these steps:

1. Download the CA certificate of the Netscaler server in PEM format.
2. Copy the content of your CA certificate in $SPLUNK_HOME/etc/apps/Splunk_TA_citrix-netscaler/bin/Splunk_TA_citrix_netscaler/t
3. Save your changes.
**HTTP configuration**

If your Netscaler server only supports HTTP communications, follow these steps:

1. Change the value of the `http_scheme` field to HTTP instead of HTTPS in your `$SPLUNK_HOME/etc/apps/Splunk_TA_citrix-netscaler/local/splunk_ta_citrix_netscaler.conf` file under the `additional_parameters` stanza.
2. Save your changes.
3. Restart the Splunk platform.

**Configure modular inputs using Splunk Web**

Access the Splunk Add-on for Citrix NetScaler by selecting it from the left banner on the Splunk Web home screen, or, from anywhere else in Splunk Web, by selecting **Apps > Manage Apps**, then selecting **Launch app** in the row for Splunk Add-on for Citrix NetScaler.

You can now configure inputs using the Configuration menu.

**Note:** Do not go to the **Splunk Add-on for Citrix NetScaler** configuration page under **Settings > Data Inputs** to configure NITRO API inputs. This page has been deprecated.

**Configure appliances**

1. Under **Configuration**, select **Appliance**.
2. Click **Add New Appliance**.
3. Fill out the fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for the appliance.</td>
</tr>
<tr>
<td>Description</td>
<td>Optional. A description for the appliance.</td>
</tr>
<tr>
<td>Host</td>
<td>The host or IP address of your Citrix NetScaler appliance.</td>
</tr>
<tr>
<td>Username</td>
<td>Only required if your Citrix NetScaler appliance requires authentication.</td>
</tr>
<tr>
<td>Password</td>
<td>Only required if your Citrix NetScaler appliance requires authentication.</td>
</tr>
</tbody>
</table>

4. Click **Add**.
5. Repeat steps 2 - 4 for each Citrix NetScaler appliance from which you want to collect data.

**Configure templates**

1. Under **Configuration**, select **Template**.
2. Click **Add New Template** and fill out the fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for the template.</td>
</tr>
<tr>
<td>Description</td>
<td>Optional. A description for the template.</td>
</tr>
<tr>
<td>Metrics</td>
<td>The Citrix NetScaler metrics that you want to collect data from. You can theoretically include any number of metrics in a single template, but for best results, you should limit the number of metrics that you include in a single template to avoid overloading the Citrix NetScaler server. Metrics should be limited to no more than 15 within one template. You should also avoid creating many individual templates, each with just one or very few metrics, to avoid overloading the Citrix NetScaler server with too many concurrent sessions. If the metrics you select require additional parameters, the <strong>Parameters</strong> textbox appears. Add additional resource specifications, arguments, filters, or parameters to specify the API call you want to make. Encode any spaces using <code>%20</code>. Examples: <code>&lt;metriccategory&gt;/&lt;metric&gt;/&lt;value&gt;</code> <code>&lt;metriccategory&gt;/&lt;metric&gt;?&lt;param&gt;=&lt;value&gt;</code> <code>&lt;metriccategory&gt;/&lt;metric&gt;?&lt;param&gt;=&lt;value%20with%20spaces&gt;</code> <code>&lt;metriccategory&gt;/&lt;metric&gt;?args=&lt;param1&gt;:&lt;value&gt;,&lt;param2&gt;:&lt;value&gt;</code> For more information on the Citrix NetScaler NITRO API, refer to the NITRO API documentation.</td>
</tr>
</tbody>
</table>

3. After you have added the metrics that you want to collect, click **Add**.
4. You can return to this screen later to edit your existing templates, add new ones, or delete them.

**Configure inputs**

1. Select **Inputs**.
2. Click **Create New Input** and fill out the fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for the input.</td>
</tr>
<tr>
<td>Description</td>
<td>Optional. A description for the input.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Appliances</td>
<td>The Citrix NetScaler appliances from which to collect data for this input.</td>
</tr>
<tr>
<td>Templates</td>
<td>The Citrix NetScaler templates to be used in this input. Although you can</td>
</tr>
<tr>
<td></td>
<td>select as many templates as you want, for best results you should limit</td>
</tr>
<tr>
<td></td>
<td>the number of templates that you invoke with a single task to avoid</td>
</tr>
<tr>
<td></td>
<td>creating too many concurrent sessions.</td>
</tr>
<tr>
<td>Collection</td>
<td>How long to wait before running the data collection task again, in seconds.</td>
</tr>
<tr>
<td>Interval</td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td>The index in which to store Citrix NetScaler data. The default is main.</td>
</tr>
</tbody>
</table>

You cannot override the source type for the input using Splunk Web. If you want to override the source type, do so in the configuration files.

3. Click **Add** to create the input.
4. Enable the input using **Status** toggle.
5. Repeat these steps for any additional inputs you want to configure.

To validate that your inputs are working as expected, go to the Search & Reporting app and search for `sourcetype=citrix:netscaler:nitro` to confirm that Splunk Enterprise is indexing events through the add-on. See the **Troubleshooting** page for more guidance.

**Configure a proxy**

If you are using a proxy, complete these steps on the **Configuration** tab:

1. Under **Configuration**, select **Proxy**
2. Check **Enable Proxy**.
3. Specify the **ProxyHost**, **ProxyPort**, **ProxyUsername**, and **ProxyPassword** values.
4. Check **DNS resolution** if you want to perform DNS resolution through your proxy.
5. Select the type of proxy to use in the **Proxy Type** field.
6. Click **Save**.

**Configure logging**

If you want to change the logging level, complete these steps:

1. Under **Configuration**, select **Logging**.
2. Select your preferred logging level.
3. Click **Save**.

**Configure modular inputs manually in the configuration files**

A best practice is to configure inputs using the UI to avoid typos. However, you can also configure them manually by creating a set of configuration files in `$SPLUNK_HOME/etc/apps/Splunk_TA_citrix-netscaler/local`.

**Create `citrix_netscaler_servers.conf`**

1. Create a file called `citrix_netscaler_servers.conf` in `$SPLUNK_HOME/etc/apps/Splunk_TA_citrix-netscaler/local`.
2. Copy the following example stanza into the file and provide values for each argument:

```
[FriendlyNameforYourAppliance]
account_name =
account_password =
description = <A useful description goes here>
server_url = <Your Citrix NetScaler IP address>
```

The Splunk platform encrypts the values for `account_name` and `account_password` when you save the file.

**Create `citrix_netscaler_templates.conf`**

1. Create a file called `citrix_netscaler_templates.conf` in `$SPLUNK_HOME/etc/apps/Splunk_TA_citrix-netscaler/local`.
2. Copy the following example stanza into the file and enter a list of correctly-formatted metrics, semicolon-separated, as the value for the `content` argument:

```
[FriendlyNameforYourTemplate]
content = config/aaaglobal_binding;
config/aaagroup_aaauser_binding?action=enable
```

For assistance choosing metrics, use the Splunk Web configuration UI for this add-on to search and browse for the metrics and determine which ones require additional parameters. For a more information on the Citrix NetScaler NITRO API, refer to the NITRO API documentation.

For best results, limit the number of metrics that you include in a single template to avoid overloading the Citrix NetScaler server. Limit metrics to 20.
no more than 15 within one template. Also avoid creating many individual templates, each with just one or very few metrics, to avoid overloading the Citrix NetScaler server with too many concurrent sessions.

**Create inputs.conf**

1. Create a file called `inputs.conf` in
   `$SPLUNK_HOME/etc/apps/Splunk_TA_citrix-netscaler/local`.
2. Copy the following example stanza into the file and provide values for each argument. If you have multiple servers or templates in one input, separate them with a pipe as shown in the following example:

```conf
[citrix_netscaler://FriendlyNameforYourInput]
disabled = 0
index = default
duration = 360
servers = FriendlyNameforYourAppliance | AnotherAppliance
templates = FriendlyNameforYourTemplate | AnotherTemplate
```

For best results, limit the number of metrics that you include in a single template to avoid overloading the Citrix NetScaler server. Limit metrics to no more than 15 within one template. Also avoid creating many individual templates, each with just one or very few metrics, to avoid overloading the Citrix NetScaler server with too many concurrent sessions.

To validate that the input is working as expected, go to the Splunk Search & Reporting app and search for `sourcetype=citrix:netscaler:nitro` to confirm that the Splunk platform is indexing events through the add-on. See [Troubleshooting](#) for more guidance.

**Create splunk_ta_citrix_netscaler_settings.conf**

1. Create a file called `splunk_ta_citrix_netscaler_settings.conf` in
   `$SPLUNK_HOME/etc/apps/Splunk_TA_citrix-netscaler/local`.
2. For Proxy, copy the following stanza into the file and provide values for each argument.
   
   ```conf
   [proxy]
   proxy_enabled = [0|1]
   proxy_type = [http|socks4|socks5]
   proxy_url = <string>
   proxy_port = <integer>
   proxy_username = <string>
   proxy_password = <string>
   proxy_rdns = [0|1]
   ```
3. For Logging, copy the following stanza into the file and provide value for log level.
   ```conf
   [logging]
   loglevel = [DEBUG|INFO|ERROR]
   ```
Configure IPFIX inputs for the Splunk Add-on for Citrix NetScaler

To create an IPFIX input for the Splunk Add-on for Citrix NetScaler, you must first configure your Citrix NetScaler appliance to produce IPFIX data and send it to your collection node.

When prompted to configure a source type, set it to `citrix:netcaler:ipfix`.

Configure syslog inputs for the Splunk Add-on for NetScaler

If you want to collect syslog data using the Splunk Add-on for NetScaler, first ensure that you have configured your Citrix NetScaler appliance to produce syslog data.

There are two ways to capture the syslog data from Citrix NetScaler.

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

2. Create a UDP input to capture the data sent on the port you have configured in your Citrix NetScaler server.

Note: For information about timestamp processing options for syslog events, see Syslog and timestamps in Splunk Add-ons.

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 `citrix:netcaler:syslog`. The CIM mapping and dashboard panels are dependent on this source type.

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

In the Splunk platform node handling data collection, configure the UDP input to match your configurations in your Citrix NetScaler server and set your source type to `citrix:netscaler:syslog`. 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.

Validate data collection

Once you have configured the input, run this search to check that you are ingesting the data that you expect.

```
sourcetype=citrix:netscaler:syslog
```
Troubleshooting

Troubleshoot the Splunk Add-on for Citrix NetScaler

For 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.

HTTPError: 407, Proxy Authentication Required

If you have http proxy configured, you are using unencrypted communication, and you get this error, go to Configuration > Proxy and change the Proxy Type to http_no_tunnel.

Citrix Netscaler supported syslog format

The following format of Citrix Netscaler syslogs is supported:
<time-stamp> <ns-name> <packet-engine-name>:<> <event-source> <event-name> <event-id> 0 :<syslog-message>

Configure logging level

The Splunk Add-on for Citrix NetScaler allows you to configure logging levels in the configuration UI or in splunk_ta_citrix_netscaler_settings.conf. Allowed log levels are DEBUG, INFO, and ERROR. The default is INFO. To configure logging using the UI:

1. Go to Splunk Web on your data collection node.
2. Access the Splunk Add-on for Citrix NetScaler UI.
3. From the configuration menu, select Configuration > Logging.
4. Choose a log level and click Save.
Reference

Lookups for the Splunk Add-on for Citrix NetScaler

The Splunk Add-on for Citrix NetScaler has two lookups. The lookup files map fields from Citrix NetScaler systems to CIM-compliant values in the Splunk platform. The lookup files are located in $SPLUNK_HOME/etc/apps/Splunk_TA_citrix-netscaler/lookups.

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>citrix_netscaler_availability_status.csv</td>
<td>Maps state to avl_status_string, avl_status</td>
</tr>
<tr>
<td>citrix_netscaler_ha_states.csv</td>
<td>Maps hacurstate to failover_status_string, failover_status</td>
</tr>
</tbody>
</table>