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

Generated: 11/05/2022 12:00 pm

Table of Contents

Overview

Introduction to the Splunk Add-on for Juniper

Version	1.5.5
Vendor Products	Junos OS 16.2R1, 17.1R1, 17.2R1, 17.3R1, 17.4R1, 17.4RU2, 18.2R1, 18.4R1, 19.1R1, 19.2R1, 19.3R1, 19.4R1, 20.1R1
Add-on has a web UI	No. This add-on does not contain any views.

Use the Splunk Add-on for Juniper to pull system logs and traffic statistics from Junos OS versions listed in the table into the Splunk platform. 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 Juniper from Splunkbase. See Deploy the Splunk Add-on for Juniper for information about installing and configuring this add-on.

See Release Notes for the Splunk Add-on for Juniper for a summary of new features, fixed issues, and known issues.

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

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

See the following information to ensure your system meets the requirements to run the Splunk Add-on for Juniper.

Juniper setup requirements

You need access to the Juniper installation directory to configure your Juniper device to send data to the Splunk platform.

Splunk platform requirements

There are no Splunk platform requirements specific to the Splunk Add-on for Juniper.

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

Installation overview for the Splunk Add-on for Juniper

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

1. Install the Splunk Add-on for Juniper.
2. Configure your Juniper device to send data to the Splunk Add-on for Juniper.
3. Configure inputs for the Splunk Add-on for Juniper.

Installation and Configuration

Install the Splunk Add-on for Juniper

1. Download the Splunk Add-on for Juniper from http://splunkbase.splunk.com/app/2847 or Splunk Web.
2. Use the tables in this topic to determine where to install this add-on.
3. Perform any prerequisite steps specified in the tables before installing.
4. Use the links in the "Installation walkthrough" section to perform the installation.

Distributed deployment

Use the following tables to install the Splunk Add-on for Juniper in a deployment that uses forwarders to get data in, such as a distributed deployment. Note that you might 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 the Splunk platform:

Splunk platform instance type	Supported	Required	Actions required / Comments
Search Heads	Yes	Yes	Install this add-on to all search heads where Juniper knowledge management is required. As a best practice, turn add-on visibility off on your search heads. This prevents data duplication errors that can result from running inputs on your search heads rather than your data collection node.
Indexers	Yes	Conditional	Not required if you use heavy forwarders to collect data. Required if you use universal forwarders to collect data.
Heavy Forwarders	Yes	No	This add-on supports forwarders of any type for data collection.
Universal Forwarders	Yes	No	This add-on supports forwarders of any type for data collection.

Distributed deployment feature compatibility

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

Distributed deployment feature	Supported	Actions required / Comments
Search Head Clusters	Yes	Disable add-on visibility on search heads.
Indexer Clusters	Yes	
Deployment Server	Yes	Supported for deploying the configured add-on to multiple nodes.

Installation walkthrough

See About installing add-ons in *Splunk Add-Ons* for detailed instructions on installing a Splunk add-on in the following deployment scenarios:

- Single-instance Splunk Enterprise
- Distributed Splunk Enterprise
- Splunk Cloud

Configure your Juniper device to send data to the Splunk Add-on for Juniper

> Although Juniper supports both syslog and key-value output, the Splunk Add-on for Juniper only supports syslog.

Enable the Splunk Add-on for Juniper to collect data by configuring your Juniper devices to produce syslog output. Set the output format to **default** or **splunk** and push the output to the data collection node or universal forwarder of your Splunk deployment.

Search the name of the Juniper product that you are using at https://www.juniper.net/us/en/ for its specific syslog configuration instructions.

Next, see Configure inputs for the Splunk Add-on for Juniper to enable your data collection node to receive data on the port that matches your Juniper device configuration file.

Configure inputs

> Although Juniper supports both syslog and key-value output, the Splunk Add-on for Juniper only supports syslog. See Configure your Juniper device to send data to the Splunk Add-on for Juniper.

Configure inputs using Splunk Connect for Syslog

Splunk recommends that you use Splunk Connect for Syslog (SC4S) to collect data. To collect data using SC4S, refer to the steps described in https://splunk.github.io/splunk-connect-for-syslog/main/sources/Juniper/.

Configure inputs for the Splunk Add-on for Juniper

The Splunk Add-on for Juniper handles inputs through UDP. Match the input configuration in your Splunk platform's data collection node to the port that you configured in your Juniper configuration file. If you have not yet done this, see Configure your Juniper device to send data to the Splunk Add-on for Juniper.

In the Splunk platform node handling data collection, configure the UDP input to match your configurations in Juniper, and set your source type to `juniper`. The CIM mapping and dashboard panels depend on the `juniper` source type.

See Get data from TCP and UDP ports in *Getting Data In* manual for how to configure a Splunk forwarder or single-instance to receive syslog input.

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

```
sourcetype = juniper*
```

If you are bringing in data from Juniper NetScreen Firewall, run the following search:

```
sourcetype = netscreen:firewall
```

Troubleshoot the Splunk Add-on for Juniper

General troubleshooting

For troubleshooting tips that 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 checking the following:

- You configured the correct IP address of the Splunk platform node responsible for data collection in your Juniper configuration file.
- The port configured in your Juniper configuration file 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 your Splunk platform software is not parsing events or extracting fields, check that your output is in syslog format. While Juniper devices can produce syslog and key-value output, the Splunk Add-on for Juniper only supports syslog. See Configure your Juniper device to send data to the Splunk Add-on for Juniper.
- Your syslog input is configured to set the source type to `juniper`.
- You are searching the correct index. By default, this add-on uses the `main` index.

Reference

Source types for the Splunk Add-on for Juniper

The Splunk Add-on for Juniper can collect the following kinds of events: risks, authentication, alerts, and traffic. The add-on includes the following source types and event types, which map the Juniper data to the Splunk **Common Information Model (CIM)**:

Source type	Event type	CIM data models
`netscreen:firewall`	`netscreen_firewall`	n/a
	`netscreen_firewall_communicate`	Network Traffic
	`netscreen_firewall_translation_mac_to_ip`	n/a
	`netscreen_authentication`	Authentication
	`netscreen_authentication_default`	Authentication - Default_Authentication
	`netscreen_authentication_privileged`	Authentication - Privileged_Authentication
	`netscreen_firewall_modify_policy`	Change
	`netscreen_restart`	n/a
	`netscreen_alert`	Alerts
`juniper:junos:idp`	`juniper_junos_idp`	n/a
	`juniper_junos_idp_attack`	Intrusion Detection
`juniper:junos:idp:structured`	`juniper_junos_idp`	n/a
	`juniper_junos_idp_attack`	Intrusion Detection
`juniper:junos:firewall`	`juniper_junos_firewall`	Network Traffic
	`juniper_junos_firewall_utm_attack`	Intrusion Detection
	`juniper_junos_firewall_web`	Web
`juniper:junos:firewall:structured`	`juniper_junos_firewall`	Network Traffic
	`juniper_junos_firewall_utm_attack`	Intrusion Detection
	`juniper_junos_firewall_utm_web`	Web
`juniper:junos:aamw:structured`	`juniper_junos_aamw`	Intrusion Detection
`juniper:junos:secintel:structured`	`juniper_junos_secintel`	Intrusion Detection
`juniper:junos:snmp`	`juniper_junos_change_network`	Change - Network_Changes

Lookups for the Splunk Add-on for Juniper

Lookup files are located in `$SPLUNK_HOME/etc/apps/Splunk_TA_juniper/lookups` on *nix systems and `%SPLUNK_HOME%\etc\apps\Splunk_TA_juniper\lookups` on Windows systems. They map fields from Juniper Networks to CIM-compliant values in the Splunk platform. The Splunk Add-on for Juniper has the following lookups:

Filename	Description
juniper_netscreen_firewall_actions.csv	Maps Netscreen `vendor_action` and `action_type` to `action` and `status`.
juniper_netscreen_firewall_ids_info.csv	Maps `alert_id` to `ids_type` and `signature`.
juniper_transport_protocols.csv	Maps `transport_id` to `protocol` and `transport`.

Release Notes

Release notes for the Splunk Add-on for Juniper

Version 1.5.5 of the Splunk Add-on for Juniper was released on December 15, 2020.

About this release

Version 1.5.5 of the Splunk Add-on for Juniper is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	7.3, 8.0, 8.1
CIM	4.18
Platforms	Platform independent
Vendor Products	Junos OS 16.2R1, 17.1R1, 17.2R1, 17.3R1, 17.4R1, 17.4RU2, 18.2R1, 18.4R1, 19.1R1, 19.2R1, 19.3R1, 19.4R1, 20.1R1.

> The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

New Features

- Added Splunk Connect for Syslog Support for new message tags.
- Added support for CIM version 4.18.
- Added Add-On support for EX4200 switches and MX80 routers.
- The following SNMP tags are supported under a new sourcetype `sourcetype=juniper:junos:snmp`:
    - `SNMP_TRAP_LINK_UP`
    - `SNMP_TRAP_LINK_DOWN`
- The following event types are added:
    - `juniper_junos_change_network`
- Support for the following message tags have been added under sourcetype: `sourcetype=juniper:junos:firewall`:
    - `PFE_FW_SYSLOG_ETH_IP`
    - `ESWD_STP_STATE_CHANGE_INFO`
    - `ESWD_DAI_FAILED`
    - `EVENT <UpDown>`

See Source types for the Splunk Add-on for Juniper for more information.

Fixed issues

Version 1.5.5 of the Splunk Add-on for Juniper has the following fixed issues:

Date resolved	Issue number	Description

2020-12-23	ADDON-31343	Splunk Add-on for Juniper support for JunOS 15.1X49 and 18.3R1.9

Known issues

Version 1.5.5 of the Splunk Add-on for Juniper contains no known issues.

Third-party software attributions

Version 1.5.5 of the Splunk Add-on for Juniper does not incorporate any third-party software or libraries.

Release history for the Splunk Add-on for Juniper

The latest release of the Splunk Add-on for Juniper is version 1.5.5. See Release notes for the Splunk Add-on for Juniper for the release notes of this latest version.

Version 1.4.0

Version 1.4.0 of the Splunk Add-on for Juniper was released on June 16, 2020.

About this release

Version 1.4.0 of the Splunk Add-on for Juniper is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	7.2, 7.3, 8.0
CIM	4.15
Platforms	Platform independent
Vendor Products	Junos OS 16.2R1, 17.1R1, 17.2R1, 17.3R1, 17.4R1, 17.4RU2, 18.2R1, 18.4R1, 19.1R1, 19.2R1, 19.3R1, 19.4R1, 20.1R1.

New Features

- Removed support of deprecated source types.
- Removed unsupported source types.
- Added support of `netscreen:firewall` source type.
- The structured events for Firewall and IDP now fall under `juniper:junos:firewall:structured` and `juniper:junos:idp:structured` sourcetypes. The unstructured events for Firewall and IDP now fall under `juniper:junos:firewall` and `juniper:junos:idp` sourcetypes.
- Analyzed and updated Splunk Connect for Syslog filter.
- Added support for `webfilter_url_permitted` and `webfilter_url_blocked` logs.

Note the following changes:

- The CIM mapping won't work with structured data for `juniper:junos:firewall` and `juniper:junos:idp` sourcetypes when those source types were already indexed with Add-on v1.3.0. The CIM mapping will remain as it is for the unstructured data.
- CIM data model mapping was removed from the `netscreen_restart` event type.

- CIM data model maps for `juniper_junos_aamw` and `juniper_junos_secintel` eventtypes now follow the Intrusion Detection data model instead of the Malware data model.

- The following source types are no longer supported:
- `juniper:idp`
- `juniper:nsm:idp`
- `juniper:nsm`
- `juniper:sslvpn`

- The following event types are no longer supported:
- `netscreen_attack`
- `juniper_idp`
- `juniper_idp_attack`
- `juniper_nsm`
- `juniper_nsm_communicate`
- `juniper_sslvpn`
- `juniper_sslvpn_authentication`
- `juniper_sslvpn_authentication_default`
- `juniper_sslvpn_start`
- `juniper_sslvpn_end`
- `juniper_sslvpn_connected`
- `juniper_sslvpn_network_traffic`
- `juniper_junos_firewall_utm_network`
- `juniper_junos_firewall_utm_malware`

Following event types have been added:

- `juniper_junos_firewall_utm_attack`
- `juniper_junos_firewall_utm_web`

Fixed issues

Version 1.4.0 of the Splunk Add-on for Juniper has no fixed issues.

Known issues

Version 1.4.0 of the Splunk Add-on for Juniper contains no known issues.

Version 1.3.0

Version 1.3.0 of the Splunk Add-on for Juniper was released on March 25, 2020.

About this release

Version 1.3.0 of the Splunk Add-on for Juniper is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	7.2.x, 7.3.x, 8.0
CIM	4.15
Platforms	Platform independent
Vendor Products	

	Junos OS 16.2R1, 17.1R1, 17.2R1, 17.3R1, 17.4R1, 17.4RU2, 18.2R1, 18.4R1, 19.1R1, 19.2R1, 19.3R1, 19.4R1, 20.1R1.

New Features

The Splunk Add-on for Juniper has the following new features:

- Support for RT_UTM, RT_AAMW and RT_SECINTEL events for JunOS v20.1R1
- New field extractions to support Juniper JunOS 16.2+
- Support for Junos firewall and Junos IDP structured data
- Support for CIM 4.15.0
- For Junos OS, Splunk add-on for Juniper supports the following message tags:
    - RT_FLOW_SESSION_CREATE
    - RT_FLOW_SESSION_CLOSE
    - RT_FLOW_SESSION_DENY
    - RT_SCREEN_TCP
    - RT_SCREEN_UDP
    - RT_SCREEN_ICMP
    - APPTRACK_SESSION_CREATE
    - APPTRACK_SESSION_CLOSE
    - APPTRACK_SESSION_VOL_UPDATE
    - WEBFILTER_URL_PERMITTED
    - WEBFILTER_URL_BLOCKED
    - AV_VIRUS_DETECTED_MT
    - CONTENT_FILTERING_BLOCKED_MT
    - IDP_ATTACK_LOG_EVENT
    - AAMW_ACTION_LOG
    - AAMW_HOST_INFECTED_EVENT_LOG
    - SECINTEL_ACTION_LOG
- The following source types are deprecated:
    - netscreen:firewall
    - juniper:idp
    - juniper:nsm:idp
    - juniper:nsm
    - juniper:sslvpn

Fixed issues

Version 1.3.0 of the Splunk Add-on for Juniper has no fixed issues.

Known issues

Version 1.3.0 of the Splunk Add-on for Juniper contains no known issues.

Third-party software attributions

Version 1.3.0 of the Splunk Add-on for Juniper does not incorporate any third-party software or libraries.

Version 1.2.0

Version 1.2.0 of the Splunk Add-on for Juniper is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0
CIM	4.13
Platforms	Platform independent
Vendor Products	Juniper IDP device (IDP75, IDP250, IDP800, IDP8200), Juniper Netscreen Firewall 6.x, Juniper NSM, Juniper NSM IDP, Juniper SSLVPN series, Junos OS 11.4-12.2, Junos OS 15.1x49-D80 for RT_FLOW_SESSION_CLOSE Event, vSRX

New Features

The Splunk Add-on for Juniper has the following new feature:

- Support for vSRX data parsing

Fixed issues

Version 1.2.0 of the Splunk Add-on for Juniper has no fixed issues.

Known issues

Version 1.2.0 of the Splunk Add-on for Juniper contains no known issues.

Third-party software attributions

Version 1.2.0 of the Splunk Add-on for Juniper does not incorporate any third-party software or libraries.

Version 1.1.0

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

Splunk platform versions	6.6.x, 7.0.x, 7.1.x, 7.2.0
CIM	4.11
Platforms	Platform independent
Vendor Products	Juniper IDP device (IDP75, IDP250, IDP800, IDP8200), Juniper Netscreen Firewall 6.x, Juniper NSM, Juniper NSM IDP, Juniper SSLVPN series, Junos OS 11.4-12.2, Junos OS 15.1x49-D80 for RT_FLOW_SESSION_CLOSE Event

New Features

The Splunk Add-on for Juniper has the following new feature:

- Support for logging changes in Junos Release 15.1x49-D80

Fixed issues

Version 1.1.0 of the Splunk Add-on for Juniper has the following fixed issues:

Date resolved	Issue number	Description
2018-07-24	ADDON-17332, SPL-149386	Incorrect search results when filtering by 'severity' due to misconfiguration in TA-juniper

Known issues

Version 1.1.0 of the Splunk Add-on for Juniper contains the following known 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 Juniper does not incorporate any third-party software or libraries.

Version 1.0.2

Version 1.0.2 of the Splunk Add-on for Juniper is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.4 or later
CIM	4.2 or later
Platforms	Platform independent
Vendor Products	Juniper IDP device (IDP75, IDP250, IDP800, IDP8200), Juniper Netscreen Firewall 6.x, Juniper NSM, Juniper NSM IDP, Juniper SSLVPN series, Junos OS 11.4+, Junos SRX (SRX 100, SRX110, SRX 210, SRX 220, SRX 240, SRX 550, SRX 650, SRX 3600, SRX 5400, SRX 5600, SRX 5800)

Fixed issues

Version 1.0.2 of the Splunk Add-on for Juniper has the following fixed issues:

Date resolved	Issue number	Description
2017-05-15	ADDON-14782	Product security issue in development support files
2016-03-09	ADDON-8228	Incorrect tag of netscreen_authentication and juniper_sslvpn_authentication eventtypes

Known issues

Version 1.0.2 of the Splunk Add-on for Juniper contains the following known issues:

Date filed	Issue number	Description

Date filed	Issue number	Description
2018-07-09	ADDON-18669	App Inspect Fail-3 : Unused capturing groups in transforms.conf
2018-03-05	ADDON-17332, SPL-149386	Incorrect search results when filtering by 'severity' due to misconfiguration in TA-juniper
2017-08-14	ADDON-15528	Juniper add-on does not list "SRX" in its lookup file. Workaround: add this line to the lookup: Â juniper:srx:firewall,Juniper,SRX Firewall,
2017-05-17	ADDON-14810	"dest" field for eventtype "netscreen_alert", "netscreen_authentication" is not extracted on the Linux platform
2017-05-17	ADDON-14811	"dest_ip" field for eventtype "netscreen_alert" and "netscreen_authentication" is not extracted on the Windows and Linux platforms

Third-party software attributions

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

Version 1.0.1

Version 1.0.1 of the Splunk Add-on for Juniper is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.2.2 or later
CIM	4.2 or later
Platforms	Platform independent
Vendor Products	Juniper IDP device (IDP75, IDP250, IDP800, IDP8200), Juniper Netscreen Firewall 6.x, Juniper NSM, Juniper NSM IDP, Juniper SSLVPN series, Junos OS 11.4+, Junos SRX (SRX 100, SRX110, SRX 210, SRX 220, SRX 240, SRX 550, SRX 650, SRX 3600, SRX 5400, SRX 5600, SRX 5800)

Fixed issues

Version 1.0.1 of the Splunk Add-on for Juniper has the following fixed issues.

Resolved Date	Issue number	Description
2015-09-29	ADDON-5766	SSLVPN events are not tagged properly

Known issues

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

Third-party software attributions

Version 1.0.1 of the Splunk Add-on for Juniper does not incorporate any third-party software or libraries.

Version 1.0.0

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

New features

Version 1.0.0 of the Splunk Add-on for Juniper has the following new features.

Date	Issue number	Description
06/12/14	ADDON-1548	Update the Juniper add-on included with the Splunk App for Enterprise Security and make available as a standalone add-on on Splunkbase.

Known issues

Version 1.0.0 of the Splunk Add-on for Juniper contains the following known issues.

Date Reported	Issue number	Description
2015-09-23	ADDON-5766	SSLVPN events are not tagged properly

Third-party software attributions

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