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

Generated: 11/05/2022 11:55 am

Table of Contents

Overview

Splunk Add-on for Linux

Version	2.1.0
Vendor Products	Linux as supported by CollectD and AuditD. See also Unix operating systems.
Add-on has web UI	No. This add-on does not contain any views.

The Splunk Add-on for Linux allows Splunk to collect Linux-related performance metrics and data generated by the open source CollectD project using HTTP Event Collector (HEC) or Transmission Control Protocol (TCP). The Splunk Add-on for Linux collects the following types of data:

- CPU metrics
- Memory metrics
- Swap metrics
- Mount point and file system usage
- Network interface traffic
- Disk utilization
- System load
- Process information
- Network protocol information
- IRQ metrics
- TCP connections information
- Thermal information
- System uptime statistics

Download the Splunk Add-on for Linux from Splunkbase.

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

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

Search the Splunk Community page for questions related to the Splunk Add-on for Linux.

Source types for the Splunk Add-on for Linux

The Splunk Add-on for Linux provides the index-time and search-time knowledge for CollectD and AuditD.

- `linux:collectd:http:json` is for performance metrics sent to the Splunk platform via HEC in JSON format
- `linux:collectd:graphite` is for performance metrics sent to the Splunk platform via TCP in Graphite format
- `linux:collectd:http:metrics` is for performance metrics sent to the Splunk platform via HEC.

CollectD data works with ITSI data models.

Source type	Event type	ITSI data models

Source type	Event type	ITSI data models
linux:collectd:http:json or linux:collectd:graphite	linux_collectd_cpu	ITSI OS Model Performance.CPU
	linux_collectd_memory	ITSI OS Model Performance.Memory
	linux_collectd_swap	ITSI OS Model Performance
	linux_collectd_df	ITSI OS Model Performance.Storage
	linux_collectd_interface	ITSI OS Model Performance.Network
	linux_collectd_disk	ITSI OS Model Performance.Storage
	linux_collectd_load	ITSI OS Model Performance
	linux_collectd_processes	ITSI OS Model Performance.CPU
	linux_collectd_protocols	ITSI OS Model Performance
	linux_collectd_irq	ITSI OS Model Performance
	linux_collectd_tcpconns	ITSI OS Model Performance.Network
	linux_collectd_thermal	ITSI OS Model Performance
	linux_collectd_uptime	ITSI OS Model Performance.OS

The two source types linux:collectd:http:json and linux:collectd:graphite collect the same data from CollectD. However, the collection method and the data format are different for these two source types.

Splunk recommends sending data in JSON format via HEC. The data collected in JSON format contains more information than Graphite provides. Using JSON via HEC improves knowledge mapping to the Splunk IT Service Intelligence (ITSI) data model for Linux KPIs. For example, a network interface measurement in **Graphite** format is presented as two strings:

- `localhost-234.interface-eno16777984.if_octets.tx 573.300503â  â  1481692948`
- `localhost-234.interface-eno16777984.if_octets.rx 783.017354 1481692948`

The same measurement in **JSON** format is presented as a single event:


```
{"values":[783.017354110699,573.300503324745],"dstypes":["derive","derive"],"dsnames":["rx","tx"],"time":14816
92948.296,"interval":60.000,"host":"localhost-234","plugin":"interface","plugin_instance":"eno16777984","type":"if
_octets","type_instance":"","meta":{"network:received":true}}
```


AuditD data works with CIM data models.

Source type	Event type	CIM data models
linux:audit	linux_audit_account_change	Change
	linux_audit_authentication	Authentication
	linux_audit_endpoint	Endpoint
	linux_audit_endpoint_services	Endpoint

When to use the Splunk Add-on for Linux

There are two Splunk supported add-ons applicable for Linux: the Splunk Add-on for Linux and the Splunk Add-on for Unix and Linux. Depending on your use case, you may want to use either or both:

User scenario	Use this add-on
Collect performance metrics from Linux using CollectD	Splunk Add-on for Linux
Collect events from Linux using AuditD	Splunk Add-on for Linux
Collect performance metrics from Unix hosts or Linux hosts without CollectD	Splunk Add-on for Unix and Linux
Collect security events from Unix or Linux hosts	Splunk Add-on for Unix and Linux

See What data the Splunk Add-on for Unix and Linux collects and what data the Splunk Add-on for Linux collects for more details about the data these two add-ons collect.

The Splunk Add-on for Unix and Linux and the Splunk Add-on for Linux are unrelated add-ons. There is no upgrade or migration from one to the other. If you want to replace the Splunk Add-on for Unix and Linux with the Splunk Add-on for Linux, you must disable any metrics inputs configured in the Splunk Add-on for Unix and Linux to prevent duplicate data collection.

Release notes for the Splunk Add-on for Linux

Version 2.1.0 of the Splunk Add-on for Linux was released on July 25, 2022.

Compatibility

Version 2.1.0 of the Splunk Add-on for Linux is compatible with the following software, CIM versions, and platforms:

Splunk platform version	8.1.x, 8.2.x, 9.0.x
CIM	5.0.1
Supported OS for data collection	Linux
Vendor products	Red Hat 7.8, Red Hat 8.5, Red Hat 8.6, CentOS 7, CentOS Stream 8.2015, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, SUSE 15 SP3, Debian 9, Debian 10.9, Debian 11.

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.

Upgrade

Follow the installation instructions to upgrade an existing installation of the Splunk Add-on for Linux. See Install the Splunk Add-on for Linux.

No data migration is required to upgrade the Splunk Add-on for Linux from version 2.0.0 to version 2.1.0.

New features

Version 2.1.0 of the Splunk Add-on for Linux has the following new features.

- Support for CIM v 5.0.1
- Support for Ubuntu v22.04 and Red Hat v8.6 OS
- Added the `linux_audit_endpoint_services` eventtype for SERVICE_START and SERVICE_STOP audit logs.
- Removed the extraction for `user=unset` for `type=USER_LOGIN` in the audit logs.

Fixed issues

Version 2.1.0 of the Splunk Add-on for Linux has the following, if any, fixed issues. If no issues appear below, no issues have yet been reported:

Known issues

Version 2.1.0 of the Splunk Add-on for Linux contains the following known issues. If no issues appear below, no issues have yet been reported:

Third-party software attributions

Version 2.1.0 of the Splunk Add-on for Linux does not incorporate any third-party software or libraries.

Release history for the Splunk Add-on for Linux

Latest release

The latest version of the Splunk Add-on for Linux is version 2.1.0. See Release notes for the Splunk Add-on for Linux for the release notes of this latest version.

Version 2.0.0

Version 2.0.0 of the Splunk Add-on for Linux was released on February 8, 2022.

Compatibility

Version 2.0.0 of the Splunk Add-on for Linux is compatible with the following software, CIM versions, and platforms:

Splunk platform version	8.1.x, 8.2.x
CIM	4.20
Supported OS for data collection	Linux

Vendor products	Red Hat 7.8, Red Hat 8.5, CentOS 7, CentOS Stream 8.2015, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, SUSE 15 SP3, Debian 9, Debian 10.9, Debian 11.

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.

Upgrade

Follow the installation instructions to upgrade an existing installation of the Splunk Add-on for Linux. See Install the Splunk Add-on for Linux.

No data migration is required to upgrade the Splunk Add-on for Linux from version 1.1.1 to version 2.0.0.

New features

Version 2.0.0 of the Splunk Add-on for Linux has the following new features.

- New CIM Mapping

Fixed issues

Version 2.0.0 of the Splunk Add-on for Linux has the following, if any, fixed issues. If no issues appear below, no issues have yet been reported:

Known issues

Version 2.0.0 of the Splunk Add-on for Linux contains the following known issues. If no issues appear below, no issues have yet been reported:

Third-party software attributions

Version 2.0.0 of the Splunk Add-on for Linux does not incorporate any third-party software or libraries.

Version 1.1.1

Version 1.1.1 of the Splunk Add-on for Linux was released on May 4, 2021.

Compatibility

Version 1.1.1 of the Splunk Add-on for Linux is compatible with the following software, CIM versions, and platforms:

Splunk platform version	7.3.x, 8.0.x, 8.1.x
CIM	4.11
Supported OS for data collection	Linux

Vendor products	Linux as supported by CollectD. See also Unix operating systems.

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.

Upgrade

Follow the installation instructions to upgrade an existing installation of the Splunk Add-on for Linux. See Install the Splunk Add-on for Linux.

No data migration is required to upgrade the Splunk Add-on for Linux from version 1.0.1 to version 1.1.1.

New features

Version 1.1.1 of the Splunk Add-on for Linux has the following new features.

- Removed messages for "restart required" on the SH/SHC during new installations or upgrades.

Fixed issues

Version 1.1.1 of the Splunk Add-on for Linux has the following, if any, fixed issues. If no issues appear below, no issues have yet been reported:

Known issues

Version 1.1.1 of the Splunk Add-on for Linux contains the following known issues. If no issues appear below, no issues have yet been reported:

Third-party software attributions

Version 1.1.1 of the Splunk Add-on for Linux does not incorporate any third-party software or libraries.

Version 1.1.0

Version 1.1.0 of the Splunk Add-on for Linux was released on April 20, 2018.

Compatibility

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

Splunk platform version	7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0
CIM	4.11
Supported OS for data collection	Linux
Vendor products	Linux as supported by CollectD. See also Unix operating systems.

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.

Upgrade

Follow the installation instructions to upgrade an existing installation of the Splunk Add-on for Linux. See Install the Splunk Add-on for Linux.

No data migration is required to upgrade the Splunk Add-on for Linux from version 1.0.0 to version 1.1.0.

New features

Version 1.1.0 of the Splunk Add-on for Linux has the following new features.

- CollectD metrics data
- AuditD support

Fixed issues

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

Date resolved	Issue number	Description
2018-04-27	ADDON-12473	Linux events are tagged with an eventtype linux_scripted_input(tag=check and tag=report) when the Splunk Add-on for Linux and the Splunk Add-on for Unix and Linux are installed at the same time
2018-04-18	ADDON-12258	collecd_host is incorrectly extracted with prefix or postfix when they contain a dot
2018-04-03	ADDON-11995	collecd_host is incorrectly extracted when EscapeCharacter is set to '.'

Known issues

Version 1.1.0 of the Splunk Add-on for Linux contains the following known issues:

Date filed	Issue number	Description
2016-11-21	ADDON-12259	Fields are incorrectly extracted when SeparateInstances is set to true
2016-11-15	ADDON-12192	No restart messages shown when Add-on is installed with ITSI

Third-party software attributions

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

Version 1.0.0

Version 1.0.0 of the Splunk Add-on for Linux is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.4 and 6.5

ITSI	ITSI Model for OS 2.4.0
Platforms	Linux
Vendor Products	RHEL/Centos 6.x, 7.2+, Ubuntu/ Debian 12.x, 16.04+, SUSE 12

New features

Version 1.0.0 of the Splunk Add-on for Linux provides ITSI normalization for Linux metric data gathered from CollectD.

Known issues

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

Date Filed	Issue Number	Description
2016-11-30	ADDON-12473	Splunk_TA_linux's events will get tagged with an eventtype linux_scripted_input(tag=check and tag=report) when both TA's are installed together.
2016-11-21	ADDON-12259	fields are wrongly extracted with option SeparateInstances.
2016-11-21	ADDON-12258	collectd_host is wrongly extracted with prefix or postfix when they contain dot characters.
2016-11-21	ADDON-12192	no restart message is shown when TA is installed with ITSI.
2016-11-21	ADDON-11995	collectd_host is wrongly extracted when EscapeCharacter is set to '.'

Workaround: To workaround ADDON-11995, ADDON-12258 and ADDON-12259, Splunk recommend you collect data in JSON format or follow the instructions on how to configure the `write_graphite` CollectD *plugin* in Configure Collectd to send data to Splunk.

Third-party software attributions

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

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

Third-party requirements

If you want to collect Linux-related data via HEC or TCP, you must first install a CollectD server. CollectD is a daemon which periodically collects system and application performance metrics.

- If you use HEC to receive CollectD data in Splunk, the CollectD server must be version 5.6 or later.
- If you use TCP to receive CollectD data in Splunk, there is no specific version requirement for CollectD.

As a best practice, send your data via HEC.

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*.
- If you plan to run this add-on entirely in Splunk Cloud, there are no additional Splunk platform requirements.
- 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 Linux

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

1. Install the Splunk Add-on for Linux.
2. Configure CollectD to send data to the Splunk Add-on for Linux.
    1. If you want to collect data in JSON format via HEC, Configure HEC inputs for the Splunk Add-on for Linux.
    2. If you want to collect data in Graphite format via TCP, Configure TCP inputs for the Splunk Add-on for Linux.
3. Configure AuditD to send data to the Splunk Add-on for Linux.

Installation

Install the Splunk Add-on for Linux

1. Get the Splunk Add-on for Linux by downloading it from https://splunkbase.splunk.com/app/3412 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 tables on this page.
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 installation walkthroughs section at the bottom of this page for links to installation instructions specific to a single-instance deployment, distributed deployment, Splunk Cloud, or Splunk Light.

Distributed deployments

Use the tables on this page 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

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:

Splunk platform instance type	Supported	Required	Actions required / Comments
Search heads	Yes	Yes	Install this add-on to all search heads where Linux knowledge management is required.
Indexers	Yes	Conditional	Not required if you use heavy forwarders to collect data because the parsing operations occur on the heavy forwarders. Required if you use universal or light forwarders to collect data.
Heavy forwarders	Yes	Conditional	This add-on supports forwarders of any type for data collection. Not required if you use universal/light forwarders to collect data. Required if you use heavy forwarders to collect data.
Universal forwarders			
Light forwarders			

Distributed deployment feature compatibility

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

Distributed deployment feature	Supported	Actions required
Search head clusters	Yes	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:

Distributed deployment feature	Supported	Actions required
		1. Remove the `eventgen.conf` file and all files in the `samples` folder.
Indexer Clusters	Yes	Before installing this add-on to a cluster, make the following changes to the add-on package: 1. Remove the `eventgen.conf` file and all files in the `samples` folder.
Deployment Server	No	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 data duplication. The add-on uses the credential vault to secure your credentials, and this credential management solution is incompatible with the deployment server.

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 CollectD to send data to the Splunk Add-on for Linux

The Splunk Add-on for Linux depends on data sent from CollectD to the Splunk HTTP Event Collector (HEC) or a TCP input. CollectD is a daemon which includes a rich set of plugins for gathering system and application performance metrics. The following picture illustrates how CollectD gathers data from the Linux host (as CollectD client) and sends data to Splunk (as CollectD server).

Data is gathered from a Linux host and sent through a CollectD server and then to Splunk.

You can customize your CollectD deployment based on your needs and environment. You can configure the CollectD client and CollectD server on the same Linux host, or you can configure several CollectD clients to send data to a single CollectD server.

Download and install CollectD

Prerequisites

Review the hardware and software requirements for the Splunk Add-on for Linux. See Hardware and software requirements.

Steps

1. Go to https://collectd.org/download.shtml to download CollectD.
2. Follow the instructions from https://collectd.org/wiki/index.php/First_steps to install CollectD.

Configure CollectD for Linux

You must configure CollectD to collect data and send the data to Splunk. The default location for `collectd.conf` is `/etc/collectd.conf` or `/etc/collectd/collectd.conf`.

See the CollectD manpage to learn more about `collectd.conf`.

Configure CollectD client to collect data from Linux

Data Collected	Plugin in CollectD	Configuration Suggestion

CPU metrics	Plugin CPU
	
	Enable the plugin just by deleting the hash-symbol (#) in front of the plugin.
	
	For example, change the syntax `#LoadPlugin cpu` to `LoadPlugin cpu` to enable plugin CPU.
		`<Plugin cpu>`
		`#  ReportByCpu true`
		`#  ReportByState true`
		`  ValuesPercentage true`
		`</Plugin>`

Memory metrics	Plugin memory	`<Plugin memory>` `  ValuesAbsolute true`

Data Collected	Plugin in CollectD	Configuration Suggestion
		ValuesPercentage true </Plugin>
Swap metrics	Plugin swap	<Plugin swap> ReportByDevice true # ReportBytes true # ValuesAbsolute true ValuesPercentage true </Plugin>
VMEM metrics	Plugin vmem	<Plugin vmem> Verbose false </Plugin>
Mountpoint usage/FS usage	Plugin df	<Plugin df> # Device "/dev/hda1" # Device "192.168.0.2:/mnt/nfs" # MountPoint "/home" # FSType "ext3" ReportByDevice true # ReportInodes false # ValuesAbsolute true ValuesPercentage true </Plugin>
Network interface traffic	Plugin interface	None. Use the default configuration.
Disk utilization	Plugin disk	
System load	Plugin load	<Plugin load> ReportRelative true </Plugin>
Process information	Plugin processes	<Plugin processes> ProcessMatch "all" "(.*)" </Plugin>
Network protocols information	Plugin protocols	None. Use the default configuration.
IRQ metrics	Plugin irq	
TCP connections information	Plugin tcpconns	
Thermal information	Plugin thermal	
System uptime statistics	Plugin uptime	

Configure the CollectD client to send data to the CollectD server

> If you configure the CollectD client and the CollectD server on the same machine, you can skip this step.

See Plugin network in the CollectD manpage for information on how to configure the Plugin network. See Networking introduction on the CollectD Wiki for a detailed walkthrough.

Configure the CollectD server to send data to Splunk

Plugin write_http and Plugin write_graphite submit values to Splunk. Plugin write_http sends data via HTTP and encoding metrics with JSON, and Plugin write_graphite writes data to Graphite via TCP.

Configure plugin write_http

If you want to send Linux performance metrics data to Splunk in JSON format via HTTP, configure `URL`, `Header` and `Format` as follows:

Field name	Description	Syntax	Example
URL	URL to which the values are submitted to. The values for `IP`, `Port`, and `Token Value` must be the same as the values you define for the HEC inputs. See Configure HEC inputs for the Splunk Add-on for Linux.	URL "https://*Splunk Server IP:Port Number*/services/collector/raw?channel=*Token Value*"	URL "https://10.66.104.127:8088/services/collector/raw?channel=693E90D4-91A5-49A3-99B1-CFE
Header	A HTTP header to add to the request.	Header "Authorization: Splunk *Token Value*"	Header "Authorization: Splunk 693E90D4-91A5-49A3-99B1-CFE8828A0711"
Format	The data format.	Format "JSON"	Format "JSON"

Example

```
LoadPlugin write_http
```

```
<Plugin write_http>
  <Node "node-http-1">
    URL "https://10.66.104.127:8088/services/collector/raw?channel=693E90D4-91A5-49A3-99B1-CFE8828A0711"
    Header "Authorization: Splunk 693E90D4-91A5-49A3-99B1-CFE8828A0711"
    Format "JSON"
    Metrics true
    StoreRates true
  </Node>
</Plugin>
```

Configure plugin write_graphite

If you want to send Linux performance metrics data to Splunk in Graphite format, configure plugin write_graphite as follows:

1. Set `AlwaysAppendDS` to `true`.
2. Set `SeparateInstances` to `false`.
3. Make sure the values for `Host` and `Port` are the same as the values you define for the TCP inputs. See Configure TCP inputs for the Splunk Add-on for Linux.

If dots (.) are used in the metric name (including prefix, EscapeCharacter, hostname, and postfix), Splunk cannot recognize the key-value pair in the data.

Example

```
LoadPlugin write_graphite
<Plugin write_graphite>
  <Node "node-graphite-1">
    Host "10.66.108.127"
    Port "2104"
    Protocol "tcp"
    EscapeCharacter "_"
    AlwaysAppendDS true
    SeparateInstances false
  </Node>
</Plugin>
```

Configure HEC inputs for the Splunk Add-on for Linux

HTTP Event Collector (HEC) is an endpoint that lets you send application events to your Splunk deployment using the HTTP or Secure HTTP (HTTPS) protocols. CollectD sends data to the Splunk Add-on for Linux in JSON format.

Paid Splunk Cloud customers must open a ticket with Splunk Support to enable HEC.

Configure HEC inputs for Linux using Splunk Web

1. Click **Settings** > **Data Inputs** > **HTTP Event Collector**.
2. Define a new data input and set the source type to `linux:collectd:http:json`. The mapping and dashboard panels for Splunk IT Service Intelligence (ITSI) are dependent on this source type.

For more information on how to configure data inputs, see Configure your inputs.

For more detailed guidelines on how to configure HEC inputs, see Set up and use HTTP Event Collection.

If you need to validate your data input configuration, see Validate data collection.

Configure HEC inputs to use metrics data

If you want to collect metrics data, you must configure Splunk to index metrics and configure the HEC inputs to use the metrics source type. You can do this by either editing the props.conf file directly, or by setting the source type in Splunk Web.

For more information on how to configure data inputs, see Configure your inputs.

If you need to validate your data input configuration, see Validate data collection.

Edit the props.conf file to set the metrics source type

1. Configure Splunk to create the metrics indexes. See Create metrics indexes.
2. Add the following stanza to `$SPLUNK_HOME/etc/apps/Splunk_TA_Linux/local/props.conf`:
   ```
   [linux:collectd:http:metrics]
   METRICS_PROTOCOL = COLLECTD_HTTP
   ```
3. Restart Splunk.
4. Go to Splunk Web.
5. Click **Settings** > **Data Inputs** > **HTTP Event Collector**.
6. Define a new data input and set the source type to `linux:collectd:http:metrics`. The mapping and dashboard panels for Splunk IT Service Intelligence (ITSI) are dependent on this source type.

Use Splunk Web to set the metrics source type

See Get metrics in from CollectD.

Configure TCP inputs in CollectD for the Splunk Add-on for Linux

You can collect data from any TCP port. You can use this method to capture data from various network services such as syslog or netcat.

You cannot collect metrics by TCP. To collect metrics, you must use HEC. See Configure HEC inputs to use metrics data.

Configure the TCP inputs for Linux using Splunk Web

1. Click **Settings** > **Data Inputs** > **TCP**.
2. Define a new data input and set the source type to `linux:collectd:graphite`. The mapping and dashboard panels are dependent on this source type.

For more information on how to configure data inputs, see Configure your inputs.

For more detailed guidelines on how to get data inputs from TCP ports, see Get data from TCP and UDP ports.

If you need to validate your data input configuration, see Validate data collection.

Configure AuditD to send data to the Splunk Add-on for Linux

AuditD is a default linux daemon for audit data generation. The AuditD daemon must be in the running state to generate AuditD logs.

You can collect data by monitoring the audit logs, or by collecting data via TCP.

Configure AuditD to collect data

You must configure AuditD to collect data and send the data to Splunk. The default location for `auditd.conf` is `/etc/audit/auditd.conf`.

Configure the property `log_format` with option RAW or ENRICHED. If set to RAW, the audit records will be stored in a format exactly as the kernel sends it. The ENRICHED option will resolve all uid, gid, syscall, architecture, and socket address information before writing the event to disk.

> Splunk best practice is to set log_format=ENHANCED to allow proper CIM mapping of auditd event data.

See the AuditD manpage to learn more about `auditd.conf`.

Collect data from the audit logs

1. Click **Settings** > **Data Inputs** > **Files & directories**.
2. Define a new data input and set the source type to `linux:audit`.

For more information on how to configure data inputs, see Configure your inputs.

If you need to validate your data input configuration, see Validate data collection.

Collect data from a TCP port

1. Click **Settings** > **Data Inputs** > **TCP**.
2. Define a new data input and set the source type to `linux:audit`.

For more information on how to configure data inputs, see Configure your inputs.

If you need to validate your data input configuration, see Validate data collection.

Troubleshooting

Troubleshoot the Splunk Add-on for Linux

General troubleshooting

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*.

Cannot launch add-on

This add-on does not have views and is not intended to be visible in Splunk Web. If you are trying to launch or load views for this add-on and you are experiencing results you do not expect, turn off visibility for the add-on.

For more details about add-on visibility and instructions for turning visibility off, see Check if the add-on is intended to be visible or not in the *Splunk Add-ons* Troubleshooting topic.

Validate data collection

Validate the data inputs to make sure that you are ingesting the data you expect.

- HEC:

```
sourcetype=linux:collectd:http:json index=<collectd-source-index>
```

- HEC with metrics data:

```
mstats count(_value) where metric_name=* AND index=<metrics index name> by metric_name
```

- TCP:

```
sourcetype=linux:collectd:graphite index=<collectd-source-index>
```

- AuditD:

```
sourcetype=linux:audit index=<auditd-source-index>
```

The default search uses `index="main"`.

Audit data not collected

Create a new TCP data input configuration and make sure the source type is set to to `linux:audit`.

If you are collecting audit data in a syslog source type using TCP, then you must assign the correct source type.

1. Add the following stanza to `$SPLUNK_HOME/etc/apps/Splunk_TA_Linux/local`:
```
[syslog]
TRANSFORMS-linux_syslog = linux_syslog_audit
```
2. Add the following stanza to `$SPLUNK_HOME/etc/apps/Splunk_TA_Linux/local/props.conf`:
```
[linux_syslog_audit]
DEST_KEY = MetaData:Sourcetype
REGEX = type=\S+\s+msg=audit
FORMAT = sourcetype::linux:audit
```

3. Restart Splunk.

Reference

Version comparisons

See the following sections for information on the differences between versions 1.1.0 of the Splunk Add-on for Linux and 2.1.0 of the Splunk Add-on for Linux

2.0.0 - 2.1.0

Field Added/Removed

Sourcetype	type, op	Added Fields	Removed Fields
['linux:audit']	ADD_USER adding user, add-user	src_user	
['linux:audit']	ADD_USER adding user to group	src_user	
['linux:audit']	DEL_USER deleting user entries, deleting user from group	src_user	
['linux:audit']	USER_ACCT changing /etc/passwd; group group_2/222222, new gid: 276, changing /etc/passwd; group group_2/222222, new gid: 10, changing /etc/passwd; group group_2/222222, new gid: 191, changing /etc/passwd; group group_2/222222, new gid: 177, changing /etc/passwd; group group_2/222222, new gid: 6	src_user, src_user_name	
['linux:audit']	USER_ACCT changing /etc/passwd; group group_2/222222, new gid: 136, changing /etc/passwd; group group_2/222222, new gid: 90, changing /etc/passwd; group group_2/222222, new gid: 76, changing /etc/passwd; group group_2/222222, new gid: 167	src_user, src_user_name	
['linux:audit']	USER_ACCT changing /etc/passwd; group group_2/222222, new gid: 18, changing /etc/passwd; group group_2/222222, new gid: 266, changing /etc/passwd; group group_2/222222, new gid: 250, changing /etc/passwd; group group_2/222222, new gid: 203, changing /etc/passwd; group group_2/222222, new gid: 89, changing /etc/passwd; group group_2/222222, new gid: 62, changing /etc/passwd; group group_2/222222, new gid: 28	src_user, src_user_name	
['linux:audit']	USER_CHAUTHTOK changing uid	object, src_user	
['linux:audit']	USER_STARTPAM:session_open	user_id	

Sourcetype	type, unit	Added Fields	Removed Fields
['linux:audit']	SERVICE_START auditd	tag::eventtype, service, status, user, eventtype, service_name, process_id, tag	
['linux:audit']	SERVICE_START collectd	tag::eventtype, service, status, user, eventtype, service_name, process_id, tag	
['linux:audit']	SERVICE_START systemd-timedated	tag::eventtype, service, user, eventtype, service_name, process_id, tag	
['linux:audit']			

Sourcetype	type, unit	Added Fields	Removed Fields
	SERVICE_START systemd-tmpfiles-clean	tag::eventtype, service, status, user, eventtype, service_name, process_id, tag	
['linux:audit']	SERVICE_START update-notifier-download	tag::eventtype, service, user, eventtype, service_name, process_id, tag	
['linux:audit']	SERVICE_STOP auditd	tag::eventtype, service, status, user, eventtype, service_name, process_id, tag	
['linux:audit']	SERVICE_STOP collectd	tag::eventtype, service, status, user, eventtype, service_name, process_id, tag	
['linux:audit']	SERVICE_STOP systemd-timedated	tag::eventtype, service, status, user, eventtype, service_name, process_id, tag	
['linux:audit']	SERVICE_STOP systemd-tmpfiles-clean	tag::eventtype, service, user, eventtype, service_name, process_id, tag	
['linux:audit']	SERVICE_STOP update-notifier-download	tag::eventtype, service, status, user, eventtype, service_name, process_id, tag	

CIM Data Model Changes

Sourcetype	type	Previous CIM model	New CIM model
linux:audit	SERVICE_START, SERVICE_STOP		Endpoint.Services

Fields Modified

Sourcetype	type, op	Field	v2.0.0	v2.1.0
linux:audit	USER_LOGIN, login	user	unset	

1.1.0 - 2.0.0

Field mapping comparison

SourceType linux:collectd:graphite

Fields	1.1.0 extractions	2.0.0 extractions
src	centos-7-202112200858	-
dest	-	centos-7-202112200858
tag	oshost performance inventory storage	oshost performance storage memory

Fields	1.1.0 extractions	2.0.0 extractions
	memory network cpu os process	network cpu os process uptime
tag::eventtype	oshost performance inventory storage memory network cpu os process	oshost performance storage memory network cpu os process uptime

SourceType linux:collectd:http

src	ubuntu-16-202112200858	-
dest	-	ubuntu-16-202112200858
mount	xvda2 devtmpfs tmpfs	xvda1 xvda2 devtmpfs tmpfs
tag	oshost performance inventory storage network	oshost performance storage network memory

	memory cpu os process	cpu os process uptime
tag::eventtype	oshost performance inventory storage network memory cpu os process	oshost performance storage network memory cpu os process uptime

SourceType linux:audit

Fields	1.1.0 extractions
src_user	-
object	-
process_path	-
user_name	-

Fields	1.1.0 extractions
object_category	-
vendor_product	-
user_id	-
process_id	-
src_user_name	-

Fields	1.1.0 extractions
signature_id	-

Fields	1.1.0 extractions

Fields	1.1.0 extractions
result	-
process_name	-
process	-
tag::action	-

Fields	1.1.0 extractions
change_type	-
process_exec	-
signature	-
object_id	-
src_user_id	-
dest	-
process_current_directory	-
linux_ev_ch_mgmt_user	-
src_ip	-
reason	-
action	success 1 failed

Fields	1.1.0 extractions
tag	account change authentication privileged
tag::eventtype	account change authentication privileged
app	/usr/sbin/sshd /usr/sbin/useradd /usr/sbin/userdel /usr/sbin/groupdel /usr/bin/sudo /usr/sbin/groupadd /usr/sbin/usermod /usr/sbin/groupmod /usr/sbin/cron

Fields	1.1.0 extractions
status	success 1 failed
eventtype	linux_audit_account_change linux_audit_authentication linux_audit_privileged
command	/bin/sh -c echo BECOME-SUCCESS-dhtumxxtkcrxahvfesdyntewfpidbinb ; /usr/libexec/platform-python /home/ec2-user/.ansible/tmp/ansible-tmp-1640006084.935285-85400-258159253623075/AnsiballZ_group.py /bin/sh -c echo BECOME-SUCCESS-qcssdifrutuskiaslrjulauiloilshzb ; /usr/libexec/platform-python /home/centos/.ansible/tmp/ansible-tmp-1640006080.967474-85356-163360540330224/AnsiballZ_group.p /bin/sh -c echo BECOME-SUCCESS-rxaezcaecyjzdwtcgzrnvrczebzdteux ; /usr/bin/python /home/admin/.ansible/tmp/ansible-tmp-1640006080.997857-85362-116590561680052/AnsiballZ_group.py /bin/sh -c echo BECOME-SUCCESS-tgrgbwfdpnprhqxomgoraaqxyjojcwpx ; /usr/bin/python /home/admin/.ansible/tmp/ansible-tmp-1640006080.972403-85358-162199036065355/AnsiballZ_group.py /bin/sh -c echo BECOME-SUCCESS-txxfnpggclncjhsqgaknpbzspzithxec ; /usr/bin/python /home/centos/.ansible/tmp/ansible-tmp-1640006080.94751-85355-75901484427407/AnsiballZ_group.py /bin/sh -c echo BECOME-SUCCESS-vqovioujwxvzhqadkoplmolqagqhioeg ; /usr/bin/python3 /home/ubuntu/.ansible/tmp/ansible-tmp-1640006088.9018528-85444-80063304780089/AnsiballZ_group.p /bin/sh -c echo BECOME-SUCCESS-wfevtrhxsnwdxtnmjdydxdhxmbnufgat ; /usr/bin/python3 /home/ubuntu/.ansible/tmp/ansible-tmp-1640006088.885395-85443-191111467693802/AnsiballZ_group.p /bin/sh -c echo BECOME-SUCCESS-xzisnyvrwjlborofkkiquvyglfrzpors ; /usr/bin/python3 /home/admin/.ansible/tmp/ansible-tmp-1640006080.991161-85360-123082352417003/AnsiballZ_group.py /bin/sh -c echo BECOME-SUCCESS-zcnurlegkdamxdgcdjbhhfufazcqmiud ; /usr/bin/python /home/ec2-user/.ansible/tmp/ansible-tmp-1640006084.904531-85399-214089969652421/AnsiballZ_group /bin/sh -c echo BECOME-SUCCESS-zrutaialratlpiralyjuydqmarrwajeq ; /usr/bin/python3.6 /home/ec2-user/.ansible/tmp/ansible-tmp-1640006084.962355-85403-198294693487419/AnsiballZ_group /bin/sh -c echo BECOME-SUCCESS-zzaswnvpdtgsqqpwnkaandhuaxwdxfik ; /usr/bin/python3 /home/ubuntu/.ansible/tmp/ansible-tmp-1640006085.35588-85411-67206222024209/AnsiballZ_group.py
user	root user_2 group_2

Fields	1.1.0 extractions
	28696E76616C6964207573657229 (unknown) ec2-user centos user1 admin
src	splunk

Event Type comparison

SourceType	EventType	1.1.0 search term	2.0.0 search term
linux:audit	linux_audit_authentication	linux:audit (type=USER_LOGIN OR type=USER_CMD OR type=GRP_AUTH OR type=USER_AUTH)	linux:audit type IN ("LOGIN", "USER_LOGIN", "USER_START", "CRED_ACQ")
linux:audit	linux_audit_privileged	eventtype=linux_audit_authentication type=USER_CMD OR acct=root	-
linux:audit	linux_audit_account_change	sourcetype=linux:audit (type=ADD_* OR type=CHGRP_ID OR type=CHUSER_ID OR type=GRP_MGMT OR type=USER_MGMT OR type=DEL_*)	linux:audit type IN ("ADD_GROUP", "DEL_GROUP", "GRP_MGMT", "USER_ACCT", "ADD_USER", "DEL_USER", "USER_MGMT", "USER_CHAUTHTOK")

DM comparison

SourceType	EventType	1.1.0 DM	2.0.0 DM
linux:audit	linux_audit_anomalies	Intrusion Detection, Alerts	
linux:audit	linux_audit_account_change	Change Analysis	Change
linux:audit	linux_audit_privileged	Authentication	