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

Generated: 11/18/2022 1:01 pm

Table of Contents

Overview

Splunk Add-on for Sysmon for Linux

Version	1.0.0
Vendor Products	Sysmon for Linux v1.0.2
Add-on has a web UI	No. This add-on does not contain any views.

The Splunk Add-on for Sysmon for Linux allows a Splunk software administrator to create a Splunk software data input and **CIM**-compliant field extractions for Sysmon for Linux.

Download the Splunk Add-On for Sysmon for Linux from Splunkbase.

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

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

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

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

For Sysmon For Linux setup requirements, please refer to the product documentation at https://github.com/Sysinternals/SysmonForLinux#installation

Splunk admin requirements

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

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 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 Sysmon For Linux

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

1. Configure your Sysmon deployment to collect data
2. Install your add-on:
    - Install the Splunk Add-on for Sysmon For Linux on to your Splunk platform deployment
3. Configure your inputs:
    - Configure inputs for the Splunk Add-on for Sysmon For Linux.

Installation and Configuration

Configure your Sysmon for Linux deployment to collect data

Sysmon events are stored in Linux journald

Prepare your Sysmon configuration file based on your security team or SOC needs. You can start from attack_range/config. This is verbose, so adjust the filtering rules of each event type according to your environment needs.

To learn more about configuration file preparation and adjustment, see:

- Microsoft documentation on Sysmon
- TrustedSec Sysmon Community Guide
- Olaf Hartong's sysmon-modular
- SwiftOnSecurity sysmon-config

Install the Splunk Add-on for Sysmon For Linux

1. Get the Splunk Add-On for Sysmon For Linux by downloading it from https://splunkbase.splunk.com/app/6652/ or by 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 below.
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, or Splunk Cloud.

Distributed deployments

Use the tables below 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.

Install the Splunk Add-on for Sysmon For Linux on endpoints where the data should be collected from regardless of the Splunk role the machine possesses.

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 Sysmon knowledge management is required.
Indexers	Yes	Yes	
Heavy Forwarders			
Universal Forwarders			
Splunk Cloud			

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		
Indexer Clusters		
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

Configure inputs for the Splunk Add-on for Sysmon for Linux

The Splunk Add-on for Sysmon for Linux contains journald://sysmon input, which is enabled by default.

For more information, see https://docs.splunk.com/Documentation/Splunk/latest/Admin/Inputsconf.

Migrate from Add-on for Linux Sysmon to the Splunk Add-on for Sysmon for Linux

1. Install Splunk Add-on for Sysmon for Linux
2. Disable input for Add-on for Linux Sysmon:
    1. When both TAs use Journald for ingesting events, delete the inputs.conf file for the Add-on for Linux Sysmon folder
    2. When Add-on for Linux Sysmon uses File Monitoring:
        - ◊ Go to Settings > Data inputs > File & Directories
        - ◊ Find "/var/log/sysmon" and Disable it.
3. Restart Splunk
4. Update any sysmon related content as needed

The new Splunk Add-on for Sysmon For Linux will start ingesting data using Journald. The old events collected by the Add-on for Linux Sysmon will still be present in Splunk under sysmon_linux sourcetype. If switching from file to journald monitoring, some initial data duplication will occur as the Splunk Add-on for Sysmon for Linux will ingest all available events.

Troubleshooting

Troubleshoot the Splunk Add-on for Sysmon For Linux

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.

Events fail to show

If events fail to show after disabling input for the Add-on for Linux Sysmon. Go to the instance where add-on is installed and run:

```
setfacl -n -m u:splunk:r /var/log/journal/*/system.journal
```

If events still show under "sysmon_linux" sourcetype, go to **Settings** > **Data inputs** > **Systemd Journald Input** for Splunk > sysmon and change the sourcetype to "sysmon:linux".

Reference

Sysmon product comparisons

The following sections describe the differences between versions 1.0.4 of the Add-on for Linux Sysmon and 1.0.0 of the Splunk Add-on for Sysmon For Linux. Note that the most significant difference is that version 1.0.0 of the Splunk Add-on has source set as journald:sysmon and sourcetype as sysmon:linux. while versions 1.0.4 of the Add-on for Linux Sysmon has source set as Syslog:Linux-Sysmon/Operational and sourcetype as sysmon_linux. See the following table for information in field changes between versions 1.0.4 of the Add-on for Linux Sysmon and 1.0.0 of the Splunk Add-on for Sysmon For Linux

Field mapping comparison for 1.0.4 of the Add-on for Linux Sysmon and 1.0.0 of the Splunk Add-on for Sysmon For Linux

Source type	EventCode	Fields added	Fields removed	Fields modified	1.0.4 extractions
sysmon:linux	1	dvc user_id	Level RecordID Task EventRecordID Version Opcode Channel EventCode EventChannel EventData_Xml process_hash System_Props_Xml	Guild Name ProcessID UserId Eventtype Original_file_name vendor_product	{ff032593-a8d3-4f13-b0d6-01fc615a0f97} Linux-Sysmon 357197 0 Linux-sysmon-process (process report) Linux Sysmon
sysmon:linux	3	user_id	Level src_host RecordID Task EventRecordID Version Opcode EventCode Channel EventChannel EventData_Xml System_Props_Xml	Guid Name ProcessID UserId Eventtype protocol src vendor_product	{ff032593-a8d3-4f13-b0d6-01fc615a0f97} Linux-Sysmon 792 0 linux-sysmon-network (communicate network) ip Linux Sysmon
sysmon:linux	4	dvc user process_id user_id	Level RecordID Task EventRecordID Opcode EventCode Channel EventChannel EventData_Xml System_Props_Xml	Guid Name ProcessID UserId Version Eventtype service service_name vendor_product	{ff032593-a8d3-4f13-b0d6-01fc615a0f97} Linux-Sysmon 275293 0 3 1.0.2 linux-sysmon-service (report service) Sysmon Sysmon Linux Sysmon
sysmon:linux	5	dvc user_id	Level	Guid	{ff032593-a8d3-4f13-b0d6-01fc615a0f97}

Source type	EventCode	Fields added	Fields removed	Fields modified	1.0.4 extractions
			RecordID Task EventRecordID Version Opcode EventCode Channel EventChannel EventData_Xml System_Props_Xml	Name ProcessID UserId Eventtype vendor_product	Linux-Sysmon 357197 0 linux-sysmon-process (process report) Linux Sysmon
sysmon:linux	9	dvc user_id	Level RecordID Task EventRecordID Version Opcode EventCode Channel EventChannel EventData_Xml System_Props_Xml	Guid Name ProcessID UserId Eventtype vendor_product	{ff032593-a8d3-4f13-b0d6-01fc615a0f97} Linux-Sysmon 357197 0 linux-sysmon-process (process report) Linux Sysmon
sysmon:linux	11	dvc user_id tag::object_category	Level RecordID Task EventRecordID Version Opcode EventCode Channel EventChannel EventData_Xml System_Props_Xml	Guid Name ProcessID UserId Eventtype object_category vendor_product	{ff032593-a8d3-4f13-b0d6-01fc615a0f97} Linux-Sysmon 357197 0 linux-sysmon-filemod (endpoint filesystem) file Linux Sysmon
sysmon:linux	16	file_path dvc user user_id	Level RecordID Task EventRecordID Version Opcode EventCode Channel EventChannel EventData_Xml System_Props_Xml	Guid Name ProcessID UserId Eventtype process_id service service_name vendor_product	{ff032593-a8d3-4f13-b0d6-01fc615a0f97} Linux-Sysmon 275293 0 linux-sysmon-service (report service) 275293 Sysmon Sysmon Linux Sysmon
sysmon:linux	23	dvc user_id tag::object_category	Level RecordID Task EventRecordID Version Opcode file_hash EventCode Channel EventChannel EventData_Xml System_Props_Xml	Guid Name ProcessID UserId Eventtype object_category vendor_product	{ff032593-a8d3-4f13-b0d6-01fc615a0f97} Linux-Sysmon 357197 0 linux-sysmon-filemod (endpoint filesystem) file Linux Sysmon

Assumptions:

- Splunk Enterprise version: 9.0.1

- Sysmon For Linux version: 1.0.2
- Add-on for Linux Sysmon version: 1.0.4
- Splunk Add-on for Sysmon For Linux version: 1.0.0
- Input: Journald and File Monitoring

Initial environment configuration is a Splunk instance with the Splunk Add-on for Sysmon for Linux installed.

Source types for the Splunk Add-on for Sysmon for Linux

The Splunk Add-on for Sysmon for Linux supports the following sourcetypes.

Source type	Description	CIM data models
sysmon:linux	The Splunk Add-on for Sysmon collects data from Sysmon's dedicated Linux journald	Endpoint, Network_Traffic

Lookups for the Splunk Add-on for Sysmon for Linux

The Splunk Add-on for Sysmon for Linux has the following lookups that map fields from Sysmon to Common Information Model (CIM)-compliant values in the Splunk software. The lookup files are located in $SPLUNK_HOME\etc\apps\Splunk_TA_sysmon-for-linux/lookups

Filename	Description
sysmon_for_linux_eventid.csv	Maps EventID to EventDescription. For more information, see the Sysmon For Linux documentation.

Release notes

Release history