Splunk® Enterprise Getting Data In 9.0.0

What data can I index?

Generated: 7/01/2022 9:34 am

Copyright (c) 2022 Splunk Inc. All Rights Reserved

What data can I index?

The Splunk platform can **index** any kind of data. In particular, the Splunk platform can index any and all IT streaming, machine, and historical data, such as Microsoft Windows event logs, web server logs, live application logs, network feeds, **metrics**, change monitoring, message queues, archive files, and so on.

Types of data sources in Splunk Cloud Platform

Splunk Cloud Platform provides tools to configure many kinds of data inputs, including those that are specific to particular application needs. Splunk Cloud Platform also provides the tools to configure any arbitrary data input types. In general, you can categorize Splunk Cloud Platform inputs as follows:

- Files and directories
- Network events
- Windows sources
- HTTP Event Collector (HEC)
- Metrics

Files and directories

A lot of data comes directly from files and directories. You can use **universal** and **heavy forwarders** to monitor those files and directories and send them to Splunk Cloud Platform. As a best practice, install universal forwarders on every machine where you want to monitor files and directories and send that data to a heavy forwarder which then sends the data to Splunk Cloud Platform. To monitor files and directories, see Get data from files and directories.

Network events

You might want to collect data from network ports, such as network data from machines that run syslog. To do this in Splunk Cloud Platform, use a heavy or universal forwarder to collect the network data and then send that data to Splunk Cloud Platform. To get data from network ports, see Get data from TCP and UDP ports.

Windows sources

To get data from Windows sources into Splunk Cloud Platform, install the Splunk Add-on for Windows on your universal forwarder. In this scenario, you can use a deployment server to deliver the Splunk Add-on for Windows to the Windows machines you want to monitor. The add-on collects the data and sends it to Splunk Cloud Platform.

For additional information on getting Windows data into Splunk Cloud Platform, see Get Windows Data into Splunk Cloud Platform in the Splunk Cloud Platform *Admin Manual*.

HTTP Event Collector

In Splunk Cloud Platform, you can use the HTTP Event Collector to get data directly from a source with the HTTP or HTTPS protocols. For more information, see The HTTP Event Collector endpoint.

Metrics

You can also get metrics data from your technology infrastructure, security systems, and business applications. For more information, see Metrics.

Types of data sources in Splunk Enterprise

Because Splunk Enterprise is on-premises, you can either get data into the instance directly or use universal or heavy forwarders to get data in. In general, you can categorize Splunk Enterprise inputs as follows:

- Files and directories
- Network events
- Windows data
- Other sources

Files and directories

You can use the files and directories **monitor** input processor to get data from files and directories. To monitor files and directories, see Get data from files and directories.

Network events

You can index data from any network port, such as remote data from syslog-ng or any other application that transmits over the TCP protocol. It can also index UDP data, but use TCP whenever possible for enhanced reliability.

Splunk Enterprise can also receive and index SNMP events and alerts fired off by remote devices.

To get data from network ports, see Get data from TCP and UDP ports in this manual.

To get SNMP data, see Send SNMP events to your Splunk deployment in this manual.

Windows data

The Windows version of Splunk Enterprise accepts a wide range of Windows-specific inputs directly. With Splunk Web, you can configure the following Windows-specific input types:

- Windows Event Log data
- Windows Registry data
- Windows Management Instrumentation (WMI) data
- Active Directory data
- Performance monitoring data

To index and search Windows data on a non-Windows instance of Splunk Enterprise, you must first use a Windows instance to gather the data. See Considerations for deciding how to monitor remote Windows data.

For a more detailed introduction to using Windows data in Splunk Enterprise, see Monitoring Windows data in this manual.

Other sources

Splunk Enterprise can collect the following data sources directly:

- You can use the HTTP Event Collector to get data directly from a source with the HTTP or HTTPS protocols. See The HTTP Event Collector endpoint.
- You can also get metrics data from your technology infrastructure, security systems, and business applications. See Metrics.

- You can monitor First In, First Out (FIFO) queues. See Monitor First In, First Out (FIFO) queues.
- You can get data from APIs and other remote data interfaces and message queues. See Scripted inputs.
- You can define a custom input capability to extend the Splunk Enterprise framework. See Create custom data inputs for Splunk Cloud Platform or Splunk Enterprise on the Splunk Developer Portal.

Get started with getting data in

Now that you know what kind of data the Splunk platform can index, you can start getting data in to the Splunk platform. See Get started with getting data in.