07-12-2026

Syslog

Syslog is a network-based logging protocol used to send and receive notification messages from a variety of different devices. Many of the most common data sources that power Splunk product use cases require a syslog server for data collection. Most administrators do not possess the specific expertise required to successfully design, deploy, and configure a syslog server to properly work with a Splunk deployment at scale. Additionally, the traditional Universal Forwarder or Heavy Forwarder approach to syslog collection has several issues with scale and complexity. Some customers send syslog events directly to Splunk to avoid architecting a syslog server, which introduces further problems.

To help customers address these issues, Splunk developed Splunk Connect For Syslog (SC4S), a Splunk open source community-developed product. SC4S is a containerized syslog-ng server with a configuration framework designed to simplify getting syslog data into Splunk Enterprise and Splunk Cloud Platform. This approach provides an agnostic solution allowing you to deploy using the container runtime environment of your choice.

Before looking at documentation for specific data sources, review the Splunk Help information on general data ingestion for Splunk Enterprise, Splunk Cloud Platform or Splunk Observability Cloud.

Getting data in

Source	Add-ons and Apps	Guidance
Syslog Syslog is a technology frequently employed, and considered a best practice, when collecting data from security devices such as firewalls and security appliances. You can set up a syslog server to collect data from its sources, and then forward it from the syslog server to a Splunk deployment. Further considerations with syslog are documented in the Spunk validated architecture whitepaper.	**Splunk Enterprise** • Splunk Connect For Syslog	**Configuration** • Installation and guidance for Splunk Connect For Syslog (SC4S) • How the Splunk

Source	Add-ons and Apps	Guidance
		platform handles syslog data over the UDP network protocol **Splunk Lantern Articles** • Understanding best practices for Splunk Connect for Syslog • Installing Splunk Connect For Syslog (SC4S) on a Windows network • Recovering lost visibility of IT infrastructure • Investigating a ransomware attack • Monitoring ingress and egress traffic across Operational Technology perimeters • Monitoring common Operational Technology protocol ports