The universal forwarder

About the universal forwarder

The universal forwarder collects data from a data source or another forwarder and sends it to a forwarder or a Splunk deployment. With a universal forwarder, you can send data to Splunk Enterprise, Splunk Light, or Splunk Cloud. It also replaces the Splunk Enterprise light forwarder. The universal forwarder is available as a separate installation package.

The universal forwarder offers advantages over using a heavy or light forwarder. The most notable benefit is that it uses significantly fewer hardware resources than other Splunk software products. It can, for example, coexist on a host that runs a Splunk Enterprise instance. It also is more scalable than the other Splunk products, as you can install thousands of universal forwarders with little impact on network and host performance.

Another benefit is its availability for installation on many diverse computing platforms and architectures. You can install it on more platforms than you can Splunk Enterprise.

The universal forwarder includes only the essential components that it needs to forward data to other Splunk platform instances. While it does not have a Web interface, you can still configure, manage, and scale it by editing configuration files or by using the Forwarder Management or Monitoring Console interfaces in Splunk Web.

This manual discusses the universal forwarder

This manual discusses the universal forwarder and how to plan, download, install, and configure it. There are two other types of forwarders. To learn about heavy and light forwarders and how they forward data, see About forwarding and receiving data in the Forwarding Data Manual.

To achieve higher performance and a lighter resource footprint, the universal forwarder has a subset of the functionality provided by a full Splunk platform deployment, specifically:

- Cannot search or index data.
- Cannot send alerts.
- Does not parse incoming data, except in certain cases, such as structured data or some forms of Windows data.
• Cannot send data to syslog servers as it has no syslog pipeline.
• Does not include a version of Python.

How the universal forwarder compares to the light forwarder

The light forwarder is a full Splunk Enterprise instance with certain features that have been disabled to achieve a smaller resource footprint. The universal forwarder differs from the light forwarder in the following ways:

• It puts less load on the host CPU, uses less memory, and has a smaller disk space footprint.
• It cannot be converted to function as a heavy forwarder or other Splunk Enterprise role.
• It does not have Splunk Web, which means that you cannot perform any configuration with that user interface.

The light forwarder was deprecated in Splunk Enterprise version 6.0, which means that support for it can be removed in a future version of Splunk Enterprise. When you install the universal forwarder, you can migrate from an existing light forwarder that runs version 4.0 or later. See Migrate a Windows light forwarder or Migrate a *nix light forwarder for details.

Information on Windows third-party binaries that ship with the universal forwarder

For information on third-party Windows binaries provided with the Windows version of the universal forwarder, see Information on Windows third-party binaries distributed with Splunk Enterprise in the Splunk Enterprise Installation Manual.

For information about running the universal forwarder in Windows Safe Mode, see Splunk Enterprise Architecture and Processes also in the Installation Manual.