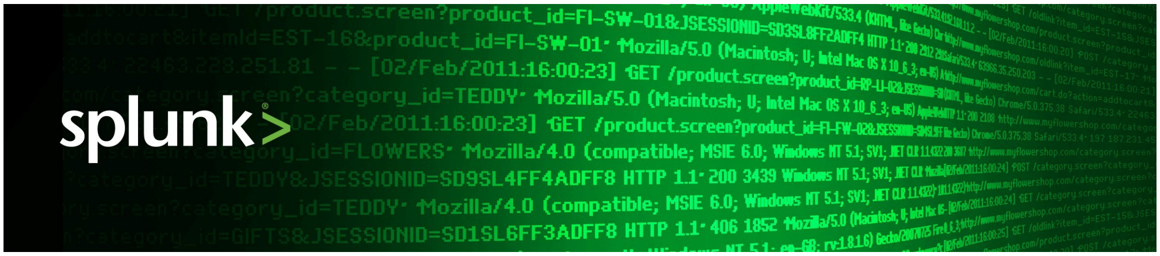

Splunk® Enterprise Forwarding Data 6.5.0

Types of forwarders

Generated: 11/10/2016 8:20 am

Types of forwarders

There are three types of forwarders:

- The **universal forwarder** contains only the components that are necessary to forward data. Learn more about the universal forwarder in the *Universal Forwarder* manual.
- A **heavy forwarder** is a full Splunk Enterprise instance that can index, search, and change data as well as forward it. The heavy forwarder has some features disabled to reduce system resource usage.
- A **light forwarder** is also a full Splunk Enterprise instance, with more features disabled to achieve as small a resource footprint as possible. The light forwarder has been deprecated as of Splunk Enterprise version 6.0. The universal forwarder supersedes the light forwarder for nearly all purposes and represents the best tool for sending data to indexers.

The universal forwarder

The sole purpose of the universal forwarder is to forward data. Unlike a full Splunk instance, you cannot use the universal forwarder to index or search data. To achieve higher performance and a lighter footprint, it has several limitations:

- The universal forwarder cannot search, index, or produce alerts with data.
- The universal forwarder does not **parse** data. You cannot use it to route data to different Splunk indexers based on its contents.
- Unlike full Splunk Enterprise, the universal forwarder does not include a bundled version of Python.

The universal forwarder can get data from a variety of inputs and forward the data to a Splunk deployment for indexing and searching. It can also forward data to another forwarder as an intermediate step before sending the data onward to an indexer.

The universal forwarder is a separately downloadable piece of software. Unlike the heavy and light forwarders, you do not enable it from a full Splunk Enterprise instance. Learn more about the universal forwarder in the *Universal Forwarder* manual.

To learn how to download, install, and deploy a universal forwarder, see Install the universal forwarder software in the *Universal Forwarder* manual.

Heavy and light forwarders

While the universal forwarder is the preferred way to forward data, you might need to use heavy or light forwarders if you need to analyze or make changes to the data before you forward it, or you need to control where the data goes based on its contents. Unlike the universal forwarder, both heavy and light forwarders are full Splunk Enterprise instances with certain features disabled. Heavy and light forwarders differ in capability and the corresponding size of their resource footprints.

A **heavy forwarder** (sometimes referred to as a "regular forwarder") has a smaller footprint than an indexer but retains most of the capability, except that it cannot perform distributed searches. Some of its default functionality, such as Splunk Web, can be disabled, if necessary, to reduce the size of its footprint. A heavy forwarder parses data before forwarding it and can route data based on criteria such as source or type of event.

One key advantage of the heavy forwarder is that it can index data locally, as well as forward data to another Splunk instance. You must activate this feature. See Configure forwarders with outputs.conf in this manual for details.

A **light forwarder** has a smaller footprint with much more limited functionality. It forwards only unparsed data. The universal forwarder, which provides very similar functionality, supersedes it. The light forwarder has been deprecated but continues to be available mainly to meet legacy needs.

When you install a universal forwarder, you can migrate checkpoint settings from any (version 4.0 or greater) light forwarder that resides on the same host. See About the universal forwarder in the *Universal Forwarder* manual for a more detailed comparison of universal and light forwarders.

For detailed information on the capabilities of heavy and light forwarders, see Heavy and light forwarder capabilities in this manual.

Forwarder comparison

This table summarizes the similarities and differences among the three types of forwarders:

Features and capabilities	Universal forwarder	Light forwarder	Heavy forwarder
Type of Splunk Enterprise instance	Dedicated executable	Full Splunk Enterprise, with	Full Splunk Enterprise, with

		most features disabled	some features disabled
Footprint (memory, CPU load)	Smallest	Small	Medium-to-large (depending on enabled features)
Bundles Python?	No	Yes	Yes
Handles data inputs?	All types (but scripted inputs might require Python installation)	All types	All types
Forwards to Splunk Enterprise?	Yes	Yes	Yes
Forwards to 3rd party systems?	Yes	Yes	Yes
Serves as intermediate forwarder?	Yes	Yes	Yes
Indexer acknowledgment (guaranteed delivery)?	Optional	Optional (version 4.2 and later)	Optional (version 4.2 and later)
Load balancing?	Yes	Yes	Yes
Data cloning?	Yes	Yes	Yes
Per-event filtering?	No	No	Yes
Event routing?	No	No	Yes
Event parsing?	Sometimes	No	Yes
Local indexing?	No	No	Optional, by setting `indexAndForward` attribute in `outputs.conf`
Searching/alerting?	No	No	Optional
Splunk Web?	No	No	Optional

For detailed information on specific capabilities, see the rest of this topic, as well as the other forwarding topics in the manual.

Types of forwarder data

Forwarders can transmit three types of data:

- Raw
- Unparsed
- Parsed

The type of data a forwarder can send depends on the type of forwarder it is, as well as how you configure it. Universal forwarders and light forwarders can send raw or unparsed data. Heavy forwarders can send raw or parsed data.

With raw data, the forwarder sends the data unaltered over a TCP stream. it does not convert the data into the Splunk communications format. The forwarder collects the data and sends it on. This is particularly useful for sending data to a non-Splunk system.

With unparsed data, a universal forwarder performs minimal processing. It does not examine the data stream, but it does tag the stream with metadata to identify source, source type, and host. It also divides the data stream into 64-kilobyte blocks and performs some rudimentary timestamping on the stream that the receiving indexer can use in case the events themselves have no discernible timestamps. The universal forwarder does not identify, examine, or tag individual events except when you configure it to parse files with structure data (such as comma-separated value files.)

With parsed data, a heavy forwarder breaks the data into individual events, which it tags and then forwards to a Splunk indexer. It can also examine the events. Because the data has been parsed, the forwarder can perform conditional routing based on event data, such as field values.

The parsed and unparsed formats are both referred to as **cooked** data, to distinguish them from raw data. By default, forwarders send cooked data (universal forwarders send unparsed data and heavy forwarders send parsed data.) To send raw data instead, set the `sendCookedData=false` attribute/value pair in outputs.conf.

Forwarders and indexes

Forwarders forward and route data on an index-by-index basis. By default, they forward all external data, as well as data for the `_audit` internal index. In some cases, they also forward data for the `_internal` internal index. You can change this behavior as necessary. For details, see Filter data by target index.