Splunk® Enterprise Getting Data In 7.2.5

Use forwarders to get data in

Generated: 4/05/2019 8:36 am

Use forwarders to get data in

Splunk **forwarders** consume data and send it to an indexer. Forwarders require minimal resources and have little impact on performance, so they can usually reside on the machines where the data originates.

For example, if you have a number of Apache Web servers that generate data that you want to search centrally, you can set up forwarders on the Apache hosts. The forwarders take the Apache data and send it to your Splunk deployment for indexing, which consolidates, stores, and makes the data available for searching. Because of their reduced resource footprint, forwarders have minimal performance impact on the Apache servers.

Similarly, you can install forwarders on your employees' Windows desktops. These can send logs and other data to your Splunk deployment, where you can view the data as a whole to track malware or other issues. The Splunk App for Windows Infrastructure relies on this kind of deployment.

What forwarders do

Forwarders get data from remote machines. They represent a more robust solution than raw network feeds, with their capabilities for the following actions:

- Tagging of metadata (source, sourcetype, and host)
- Configurable buffering
- Data compression
- SSL security
- Use of any available network ports
- Running scripted inputs locally

Forwarders usually do not index the data, but rather forward the data to a Splunk deployment that does the indexing and searching. A Splunk deployment can process data that comes from many forwarders. For detailed information on forwarders, see the *Forwarding Data* or *Universal Forwarder* manuals.

In most Splunk deployments, forwarders serve as the primary consumers of data. In a large Splunk deployment, you might have hundreds or even thousands of forwarders that consume data and forward for consolidation.

How to configure forwarder inputs

The following procedure is a general procedure. See the *Forwarding Data Manual* or the *Universal Forwarder Manual* for details on how to configure forwarding and receiving.

1. Configure a Splunk Enterprise host to receive the data.
2. Determine the kind of forwarder you want to put on the host with the data.
   - ♦ You can use a heavy forwarder, which is a full Splunk Enterprise instance with forwarding turned on, or a universal forwarder, which its its own installation package.
   - ♦ The type of forwarder you use depends on the performance requirements you have on the host and whether or not you need to transform the data in any way as it comes into Splunk.
3. Download Splunk Enterprise or the universal forwarder for the platform and architecture of the host with the data.
4. Install the forwarder onto the host.
5. Enable forwarding on the host and specify a destination
6. Configure inputs for the data that you want to collect from the host. You can use Splunk Web if the forwarder is a full Splunk Enterprise instance.
7. Confirm that data from the forwarder arrives at the receiving indexer.

Here are the main ways that you can configure data inputs on a forwarder:

- Specify inputs during initial deployment.
- For Windows forwarders, specify common inputs during the installation process.
- For *nix forwarders, specify inputs directly after installation.
- Use the CLI.
- Edit inputs.conf.
- Install an app that contains the inputs you want.
- Use Splunk Web to configure the inputs and a deployment server to copy the resulting `inputs.conf` file to forwarders.

Forwarder Topologies and Deployments

- For information on forwarders, including use cases, typical topologies, and configurations, see About forwarding and receiving in the *Forwarding Data* manual.
- For details on how to deploy the universal forwarder, including how to use the **deployment server** to simplify distribution of configuration files and apps to multiple forwarders, see Example forwarder deployment topologies in the *Universal Forwarder* manual.