Splunk® Enterprise Distributed Deployment Manual 7.3.1

Scale your deployment with Splunk Enterprise components

Generated: 9/22/2019 11:56 am
Scale your deployment with Splunk Enterprise components

In single-instance deployments, one instance of Splunk Enterprise handles all aspects of processing data, from input through indexing to search. A single-instance deployment can be useful for testing and evaluation purposes and might serve the needs of department-sized environments.

To support larger environments, however, where data originates on many machines and where many users need to search the data, you can scale your deployment by distributing Splunk Enterprise instances across multiple machines. When you do this, you configure the instances so that each instance performs a specialized task. For example, one or more instances might index the data, while another instance manages searches across the data.

This manual describes how to distribute Splunk Enterprise across multiple machines. Distributed deployment provides the ability to:

- Scale Splunk Enterprise functionality to handle the data needs for enterprises of any size and complexity.
- Access diverse or dispersed data sources.
- Achieve high availability and ensure disaster recovery with data replication and multisite deployment.

How Splunk Enterprise scales

Splunk Enterprise performs three key functions as it processes data:

1. It ingests data from files, the network, or other sources.
2. It parses and indexes the data.
3. It runs searches on the indexed data.

To scale your system, you can split this functionality across multiple specialized instances of Splunk Enterprise. These instances can range in number from just a few to many thousands, depending on the quantity of data that you are dealing with and other variables in your environment.

In a typical distributed deployment, each instance occupies one of three tiers that correspond to the key processing functions:

- Data input
- Indexing
• Search management

You might, for example, create a deployment with many instances that only ingest data, several other instances that index the data, and one instance that manages searches.

It is possible to combine some of these tiers or configure processing in other ways, but these three tiers are typical of most distributed deployments.

**Splunk Enterprise components**

Specialized instances of Splunk Enterprise are known collectively as components. With one exception, components are full Splunk Enterprise instances that have been configured to focus on one or more specific functions, such as indexing or search. The exception is the universal forwarder, which is a lightweight version of Splunk Enterprise with a separate executable.

There are several types of Splunk Enterprise components. They fall into two broad categories:

- Processing components. These components handle the data.
- Management components. These components support the activities of the processing components.

This topic discusses the processing components and their role in a Splunk Enterprise deployment. For information on the management components, see "Components that help to manage your deployment."

**Types of processing components**

There are three main types of processing components:

- Forwarders
- Indexers
- Search heads

**Forwarders** ingest data. There are a few types of forwarders, but the universal forwarder is the right choice for most purposes. It uses a lightweight version of Splunk Enterprise that simply inputs data, performs minimal processing on the data, and then forwards the data to an indexer. Because its resource needs are minimal, you can co-locate it on the machines that produce the data, such as web servers.
Indexers and search heads are built from Splunk Enterprise instances that you configure to perform the specialized function of indexing or search management, respectively. Each indexer and search head is a separate instance that usually resides on its own machine.

**Processing components in action**

This diagram provides a simple example of how the processing components can reside on the various processing tiers. It illustrates the type of deployment that might support the needs of a small enterprise.
Starting from the bottom, the diagram illustrates the three tiers of processing, in the context of a small enterprise deployment:

- **Data input.** Data enters the system through forwarders, which consume external data, perform a small amount of preprocessing on it, and then forward the data to the indexers. The forwarders are typically co-located on the machines that are generating data. Depending on your data sources, you could have hundreds of forwarders ingesting data.

- **Indexing.** Two or three indexers receive, index, and store incoming data from the forwarders. The indexers also search that data, in response to requests from the search head. The indexers reside on dedicated machines.

- **Search management.** A single search head performs the search management function. It handles search requests from users and distributes the requests across the set of indexers, which perform the actual searches on their local data. The search head then consolidates the results from all the indexers and serves them to the users. The search head provides the user with various tools, such as dashboards, to assist the search experience. The search head resides on a dedicated machine.

To scale your system, you add more components to each tier. For ease of management, or to meet high availability requirements, you can group components into **indexer clusters** or **search head clusters.** See "Use clusters for high availability and ease of management."

This manual describes how to scale a deployment to fit your exact needs, whether you are managing data for a single department or a global enterprise, or for anything in between.

**What comes next**

The rest of this chapter focuses primarily on the **data pipeline**, from the point that the data enters the system to when it becomes available for users to search. It then correlates the Splunk Enterprise processing components with their roles in facilitating the data pipeline.

Other topics discuss indexer and search head clusters, the management components, and the manuals that provide configuration details for each type of component.
The remaining chapters in this manual offer practical guidance for implementing a distributed deployment. First, they discuss representative deployment types. Next, they provide end-to-end frameworks for implementing each of those deployments. Finally, they describe the post-deployment activities that an administrator needs to perform.