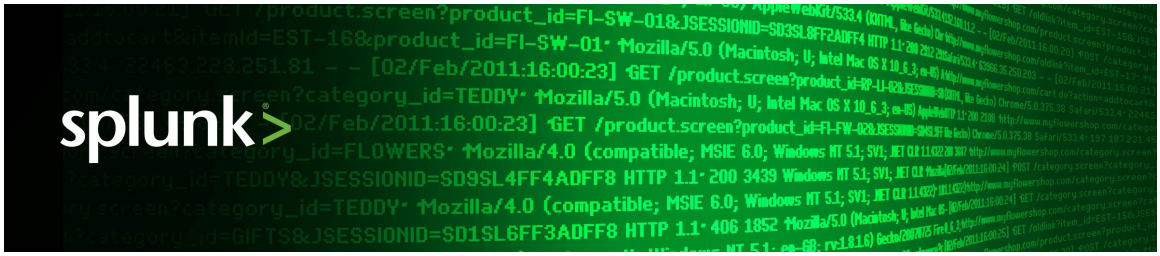


Splunk® Enterprise Capacity Planning Manual 6.5.0

Components of a Splunk Enterprise deployment

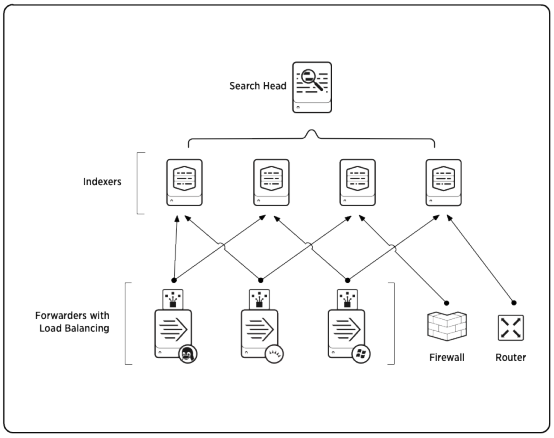
Generated: 10/31/2016 12:30 am

Components of a Splunk Enterprise deployment

By using a single software component and easy to understand configurations, Splunk Enterprise can coexist with existing infrastructure or be deployed as a universal platform for accessing IT data.

The simplest deployment is the one you get by default when you install Splunk Enterprise: indexing and searching on the same server. You log into Splunk Web or the CLI on the server and configure data inputs to collect machine data. You then use the same server to search, monitor, alert, and report on the incoming data.

You can also deploy components of Splunk Enterprise on different servers to address your load and availability requirements. This section introduces the types of components. See the *Distributed Deployment* manual, particularly the topic, Scale your deployment with Splunk Enterprise components.



Indexer

Splunk **indexers** provide data processing and storage for local and remote data and host the primary Splunk data store. See How indexing works in the *Managing Indexers and Clusters* manual for more information.

Search head

A **search head** is a Splunk Enterprise instance that distributes searches to indexers (referred to as "search peers" in this context). Search heads can be either dedicated or not, depending on whether they also perform indexing. Dedicated search heads don't have any indexes of their own, other than the usual internal indexes. Instead, they consolidate and display results that originate from remote search peers.

To configure a search head to search across a pool of indexers, see What is distributed search in the *Distributed Search Manual*

Forwarder

Forwarders are Splunk instances that forward data to remote indexers for data processing and storage. In most cases, they do not index data themselves. See the About forwarding and receiving topic in the *Forwarding Data* manual.

Deployment server

A Splunk Enterprise instance can also serve as a **deployment server**. The deployment server is a tool for distributing configurations, apps, and content updates to groups of Splunk Enterprise instances. You can use it to distribute updates to most types of Splunk components: forwarders, non-clustered indexers, and non-clustered search heads. See About deployment server and forwarder management in the *Updating Splunk Enterprise Instances* manual.

Functions at a glance

Functions	Indexer	Search head	Forwarder	Deployment server
Indexing	x			
Web		x		
Direct search		x		
Forward to indexer			x	
Deploy configurations	x		x	x

Index replication and indexer clusters

An **indexer cluster** is a group of indexers configured to replicate each others' data, so that the system keeps multiple copies of all data. This process is known as **index replication**. By maintaining multiple, identical copies of data, indexer clusters prevent data loss while promoting data availability for searching.

Splunk Enterprise clusters feature automatic failover from one indexer to the next. This means that, if one or more indexers fail, incoming data continues to get indexed and indexed data continues to be searchable.

In addition to enhancing data availability, clusters have other features that you should consider when you are scaling a deployment, for example, a capability to

coordinate configuration updates easily across all indexers in the cluster. Clusters also include a built-in distributed search capability. See About clusters and index replication in the *Managing Indexers and Clusters of Indexers* manual.