Splunk Universal Forwarder

A type of forwarder, which is a Splunk Enterprise instance that sends data to another Splunk Enterprise instance or to a third-party system.

The universal forwarder is a dedicated, streamlined version of Splunk Enterprise that contains only the essential components needed to forward data. The universal forwarder does not support python and does not expose a UI.

In most situations, the universal forwarder is the best way to forward data to indexers. Its main limitation is that it forwards only unparsed data. You must use a heavy forwarder to route event-based data.

We can forward data to Splunk Enterprise, Splunk Light, and Splunk Cloud deploymen ts as well as to systems that don't run the Splunk platform.

A Splunk instance that receives data from one or more forwarders is called a receiver. The receiver is usually a Splunk indexer, but can also be another forwarder.

Indexer

A Splunk Enterprise instance that indexes data, transforming raw data into events and placing the results into an index. It also searches the indexed data in response to search requests.

The indexer also frequently performs the other fundamental Splunk Enterprise functions: data input and search management. In larger deployments, forwarders handle data input and forward the data to the indexer for indexing. Similarly, although indexers always perform searches across their own data, in larger deployments, a specialized Splunk Enterprise instance, called a search head, handles search management and coordinates searches across multiple indexers.

The indexer is sometimes referred to by more specific terms, according to its context.

- Search peer. An indexer in a distributed search topology.
- Peer node. An indexer in an indexer cluster.