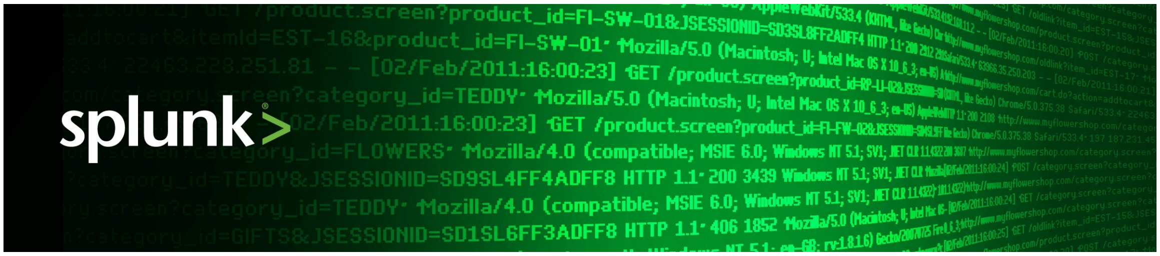


# Splunk® Enterprise Forwarding Data 6.5.0

## Forwarder deployment topologies

Generated: 11/12/2016 11:27 pm

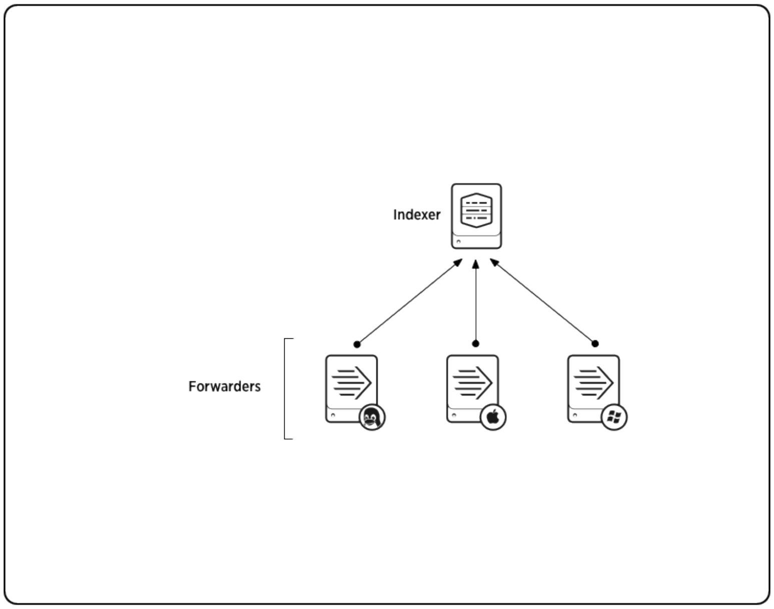
# Forwarder deployment topologies

You can deploy forwarders in a wide variety of scenarios. This topic provides an overview of some of the most useful topologies that you can create with forwarders. For detailed information on how to configure various deployment topologies, see Consolidate data from multiple hosts.

## Data consolidation

Data consolidation is one of the most common topologies, with multiple forwarders sending data to a single Splunk instance. The scenario typically involves universal forwarders forwarding unparsed data from workstations or production servers to a central Splunk Enterprise instance for consolidation and indexing. In other scenarios, heavy forwarders can send parsed data to a central Splunk indexer.

Here, three universal forwarders are sending data to a single indexer:



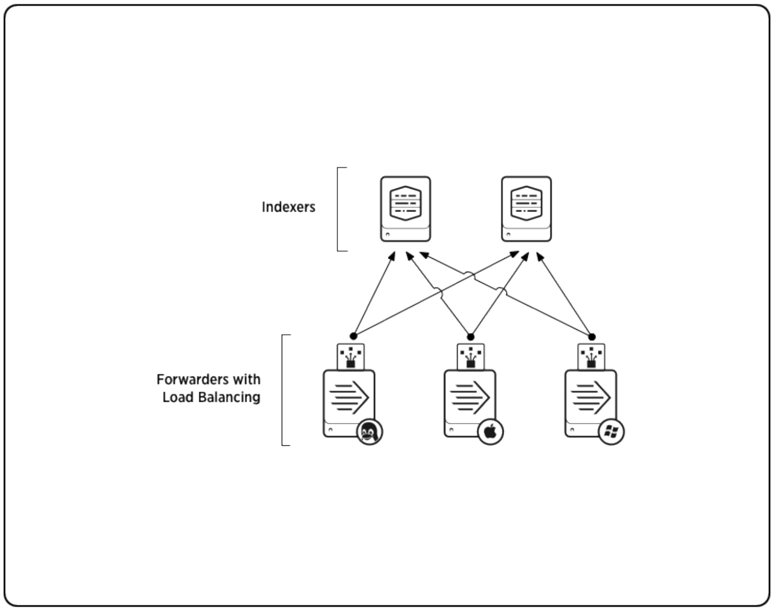
For more information on data consolidation, read Consolidate data from multiple hosts.

## Load balancing

**Load balancing** simplifies the process of distributing data across several indexers to handle considerations such as high data volume, horizontal scaling for enhanced search performance, and fault tolerance. In load balancing, the forwarder routes data sequentially to different indexers at specified intervals.

Forwarders perform automatic load balancing, in which the forwarder switches receivers at set time intervals. If parsing is turned on (for a heavy forwarder), the switching will occur at event boundaries.

In this diagram, three universal forwarders perform load balancing between two indexers:



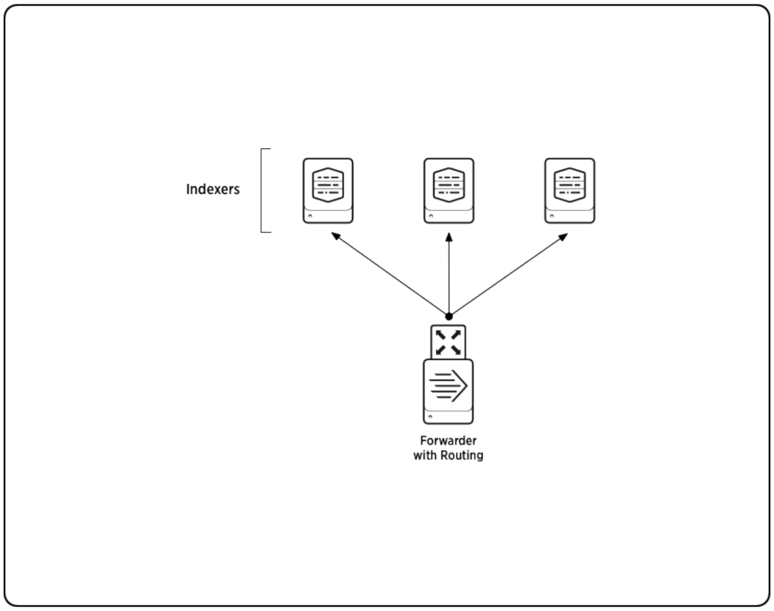
For more information on load balancing, read "Set up load balancing".

## Routing and filtering

In **data routing**, a forwarder routes events to specific hosts, based on criteria such as source, source type, or patterns in the events themselves. Routing at the event level requires a heavy forwarder.

A forwarder can also filter and route events to specific queues, or discard them altogether by routing to the null queue.

Here, a heavy forwarder routes data to three indexers based on event patterns:

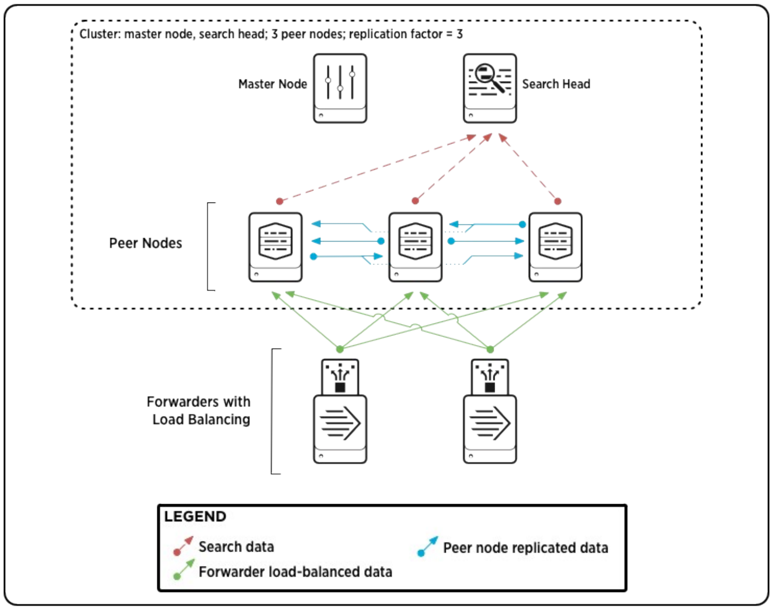


For more information on routing and filtering, see Route and filter data in this manual.

## Forwarders and indexer clusters

You can use forwarders to send data to peer nodes in an indexer cluster. A Splunk best practice is to use load-balanced forwarders for that purpose.

This diagram shows two load-balanced forwarders sending data to a cluster:

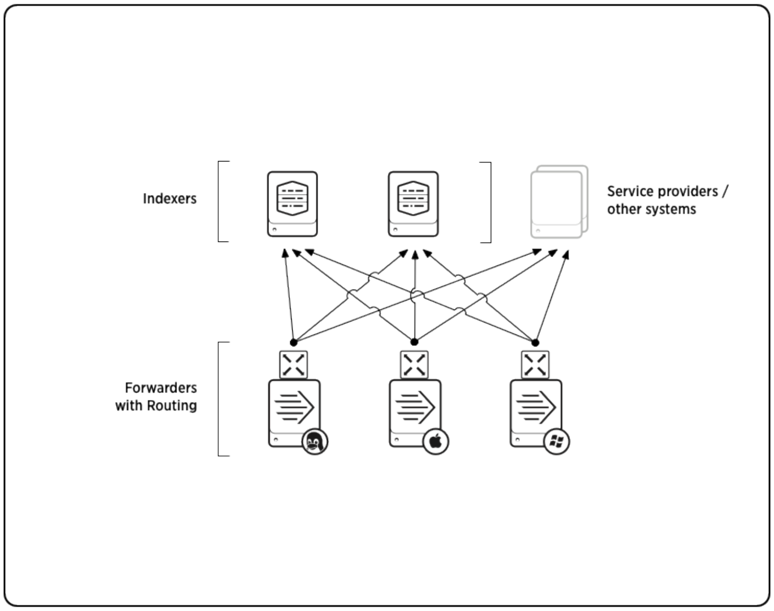

Cluster: master node, search head; 3 peer nodes; replication factor = 3
Master Node
Search Head
Peer Nodes
Forwarders with
Load Balancing
LEGEND
Search data
Forwarder load-balanced data
Peer node replicated data

To learn more about forwarders and indexer clusters, see Use forwarders to get your data in *Managing Indexers and Clusters of Indexers*. To learn more about indexer clusters in general, see About indexer clusters and index replication.

## Forward to non-Splunk systems

With a heavy forwarder, you can send raw data to a third-party system such as a syslog aggregator. You can combine this with data routing, sending some data to a non-Splunk system and other data to one or more Splunk instances.

In this diagram, three forwarders route data to two Splunk instances and a non-Splunk system:



For more information on forwarding to non-Splunk systems, see Forward data to third-party systems.

## Intermediate forwarding

To handle some advanced use cases, you might want to insert an intermediate forwarder between a group of forwarders and the indexer. In this type of scenario, the originating forwarders send data to a consolidating forwarder, which then forwards the data on to an indexer. In some cases, the intermediate forwarders also index the data.

Typical use cases are situations where you need an intermediate index, either for "store-and-forward" requirements or to enable localized searching. (In this case, you would need to use a heavy forwarder.) You can also use an intermediate forwarder if you have some need to limit access to the indexer machine; for instance, for security reasons.

To enable intermediate forwarding, see Configure an intermediate forwarder.