**What is Splunk Search Head?**

* A Splunk Enterprise instance that handles [search management](https://docs.splunk.com/Splexicon:Searchmanagement) functions, directing search requests to a set of [search peers](https://docs.splunk.com/Splexicon:Searchpeer) (aka indexers) and then merging the results back to the user.
* A Splunk Enterprise instance can function as both a search head and a search peer. A search head that performs only searching, and not any indexing, is referred to as a dedicated search head.
* Search head is simply a Splunk instance that distributes searches to other indexers, and usually doesn't have any indexes of its own. It has no local indexes, all results come from remote nodes.

**What is distributed search?**

In [distributed search](http://docs.splunk.com/Splexicon:Distributedsearch), a Splunk Enterprise instance called a [search head](http://docs.splunk.com/Splexicon:Searchhead) sends search requests to a group of indexers, which perform the actual searches on their indexes. The search head then merges the results back to the user.

The Splunk Enterprise instance that does the searching is referred to as the [search head](http://docs.splunk.com/Splexicon:Searchhead). The indexers that participate in a distributed search are called [search peers](http://docs.splunk.com/Splexicon:Searchpeer).

A search head by default runs its searches across all its search peers. You can limit a search to one or more search peers by specifying the splunk\_serverfield in your query.



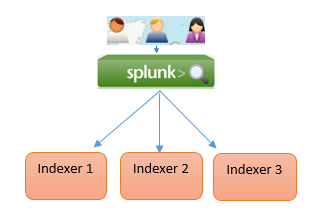
Indexer 3

Indexer 2

Indexer 1

**How search head run the queries against indexer**

**What search heads send to search peers?**



Search Query

Knowledge Bundle +

User Authorization

$SPLUNK\_HOME/var/run/searchpeers

$SPLUNK\_HOME/var/run

Saved Searches

Event types

Tags

Field Extractions

Lookups

Transactions

Fields

Data Models

Workflow Actions

Reports / Alerts

A user-defined entity that enriches the existing data in Splunk Enterprise. You can use knowledge objects to get specific information about your data. When you create a knowledge object,you can keep it private or you can share it with other users.

* When initiating a distributed search, the search head replicates and distributes its [knowledge objects](http://docs.splunk.com/Splexicon:Knowledgeobject) to its [search peers](http://docs.splunk.com/Splexicon:Searchpeer), or indexers.
* Set of knowledge objects is called the [knowledge bundle](http://docs.splunk.com/Splexicon:Knowledgebundle).
* The search head needs to distribute this material to its search peers so that they can properly execute queries on its behalf.
* The search peers use the search head's knowledge bundle to execute queries on its behalf. When executing a distributed search, the peers are ignorant of any local knowledge objects. They have access only to the objects in the search head's knowledge bundle.
* Bundles typically contain a subset of files (configuration files and assets) from $SPLUNK\_HOME/etc/system, $SPLUNK\_HOME/etc/apps and $SPLUNK\_HOME/etc/users.
* On the search head, the knowledge bundles resides under the $SPLUNK\_HOME/var/run directory. The bundles have the extension .bundle for full bundles or .delta for delta bundles. They are tar files, so you can run tar tvf against them to see the contents.
* The knowledge bundle gets distributed to the $SPLUNK\_HOME/var/run/searchpeers directory on each search peer.

## **User authorization**

All authorization for a distributed search originates from the search head. At the time it sends the search request to its search peers, the search head also distributes the authorization information. It tells the search peers the name of the user running the search, the user's role, and the location of the distributed authorize.conf file containing the authorization information.

## **Compatibility between search heads and search peers**

6.x search heads are compatible with 6.x and 5.x search peers, in a non-clustered environment. The search head must be at the same or higher level than the search peers:

* A 6.x search head is compatible with a 5.x search peer.
* A 5.x search head is not compatible with a 6.x search peer.

Note: All cluster nodes (master, peers, and search heads) must run the same version of Splunk Enterprise. Even with non-clustered deployments, it is best to upgrade search heads and search peers at the same time, to take full advantage of the latest search capabilities.

# Overview of configuration

## **Configure distributed search**

Setting up distributed search consists of three basic steps:

1. Designate a Splunk Enterprise instance as the search head. Get a physical server and install Splunk full instance

2.  Add search peers to the search head (See below)

3. Add data inputs to the search peers. You add inputs directly on the search peer or through forwarders connecting to the search peer.

**Important: Do not configure the search head for indexing of external data, since that will violate its license.A search head should not perform a dual function as a search peer**

# Add search peers to the search head

* To activate [distributed search](http://docs.splunk.com/Splexicon:Distributedsearch), you add [search peers](http://docs.splunk.com/Splexicon:Searchpeer), or [indexers](http://docs.splunk.com/Splexicon:Indexer), to a Splunk Enterprise instance that you designate as a [search head](http://docs.splunk.com/Splexicon:Searchhead). You do this by specifying each search peer manually.

**To set up the connection between a search head and its search peers, configure the search head through one of these methods:**

* Splunk Web
* Splunk CLI
* The distsearch.conf configuration file

Splunk Web is the simplest method for most purposes.

The configuration occurs on the search head. For most deployments, no configuration is necessary on the search peers. Access to the peers is controlled through public key authentication.

## ***Use Splunk Web***

### **Specify the search peers**

1. Log into Splunk Web on the search head and click Settings at the top of the page.

2. Click Distributed search in the Distributed Environment area.

3. Click Search peers.

4. On the Search peers page, select New.

5. Specify the search peer, along with any authentication settings.

6. Click Save.

7. Repeat for each of the search head's search peers.

***Use CLI***

1. Navigate to the $SPLUNK\_HOME/bin/ directory on the search head.

2. Invoke the splunk add search-server command for each search peer you want to add.

For example:

splunk add search-server -host 1.1.1.1:8089 -auth admin:password -remoteUsername admin -remotePassword passremote

Note the following:

* Use the -host flag to specify the IP address and management port for the search peer.
* Provide credentials for both the local (search head) and remote (search peer) instances. Use the -auth flag for the local credentials and the -remoteUsername and -remotePassword flags for the remote credentials. The remote credentials must be for an admin-level user on the search peer.

***Use Configuration***

1. Create or edit a distsearch.conf file on the search head.

2. Add the set of search peers to the [distributedSearch] stanza as a set of comma-separated values (IP addresses with management ports). For example:

[distributedSearch]

servers = 1.1.1.1:8089,1.1.1.2:8089

3. Restart the search head.

### **Distribute the key files**

If you add search peers via Splunk Web or the CLI, Splunk Enterprise automatically configures authentication. However, if you add peers by editing distsearch.conf, you must distribute the key files manually. After adding the search peers and restarting the search head, as described above:

1. Copy the file $SPLUNK\_HOME/etc/auth/distServerKeys/trusted.pem from the search head to$SPLUNK\_HOME/etc/auth/distServerKeys/<searchhead\_name>/trusted.pem on each search peer.

The <searchhead\_name> is the search head's serverName, specified in [server.conf](http://docs.splunk.com/Documentation/Splunk/6.2.0/admin/Serverconf).

2. Restart each search peer.

 For multipler search heads, on the search peer, create the directories $SPLUNK\_HOME/etc/auth/distServerKeys/A/ and$SPLUNK\_HOME/etc/auth/distServerKeys/B/.

**Additional Configurations**

 Configure the search head as a forwarder. Create an outputs.conf file on the search head that configures the search head for load-balanced forwarding across the set of search peers (indexers). You must also turn off indexing on the search head, so that the search head does not both retain the data locally as well as forward it to the search peers.

Here is an example outputs.conf file:

# Turn off indexing on the search head

[indexAndForward]

index = false

[tcpout]

defaultGroup = my\_search\_peers

forwardedindex.filter.disable = true

indexAndForward = false

[tcpout:my\_search\_peers]

server=10.10.10.1:9997,10.10.10.2:9997,10.10.10.3:9997

autoLB = true

**Grouping the Search heads and Peers**

In distsearch.conf, create these stanzas:

[distributedSearch]

# This stanza lists the full set of search peers.

servers = 192.168.1.1:8089, 192.168.1.2:8089, 175.143.1.1:8089, 175.143.1.2:8089, 175.143.1.3:8089

[distributedSearch:NYC]

# This stanza lists the set of search peers in New York.

default = false

servers = 192.168.1.1:8089, 192.168.1.2:8089

[distributedSearch:SF]

# This stanza lists the set of search peers in San Francisco.

default = false

servers = 175.143.1.1:8089, 175.143.1.2:8089, 175.143.1.3:8089

This example creates two search groups, NYC and SF, which you can then specify in searches.

Note the following:

* The servers attribute lists groups of search peers by IP address and management port.
* The servers list for each search group must be a subset of the list in the general [distributedSearch] stanza.
* The group lists can overlap. For example, you can add a third group named "Primary\_Indexers" that contains some peers from each location.
* If you set a group's default attribute to "true," the peers in that group will be the ones queried when the search does not specify a search group. Otherwise, if you set all groups to "false," the full set of search peers in the[distributedSearch] stanza will be queried when the search does not specify a search group.

To use a search group in a search, specify the search group like this:

sourcetype=access\_combined status=200 action=purchase splunk\_server\_group=NYC | stats count by product

This search runs against only the peers in the NYC location.

Note: This feature is not valid for indexer clustering.