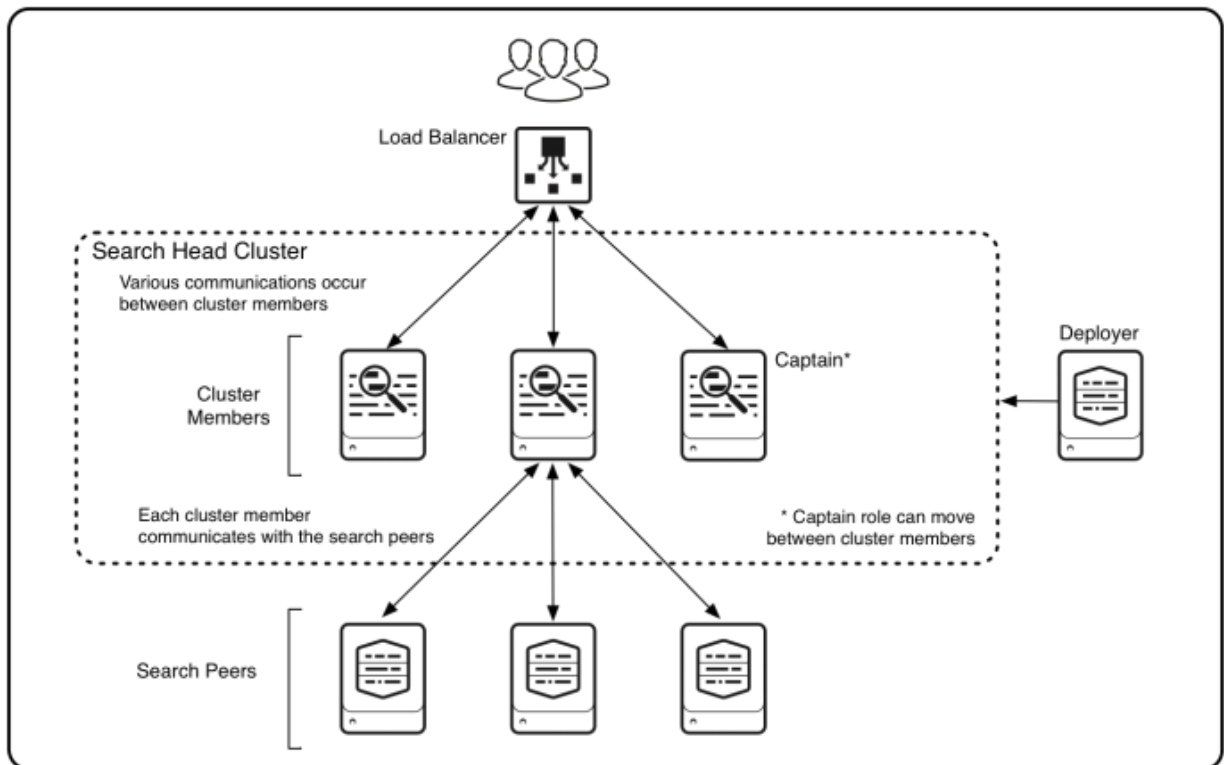


Search Head Clustering

A search head cluster is a group of Splunk Enterprise search heads that serves as a central resource for searching. The members of a search head cluster are essentially interchangeable. You can run the same searches, view the same dashboards, and access the same search results from any member of the cluster.



Search head clustering setup

Set up the deployer

In Deployer edit **server.conf** file present in the location `splunk/etc/system/local/`

```
[shclustering]
pass4SymmKey = your security key
shcluster_label = shcluster1
```

And restart the splunk in `splunk/bin` folder by using the command

```
./splunk restart
```

Initialize cluster members

For each instance that you want to include in the cluster, run the splunk init shcluster-config command and restart the instance:

```
./splunk init shcluster-config -auth <username>:<password> -mgmt_uri  
<URI>:<management_port> -replication_port <replication_port>  
-replication_factor <n> -conf_deploy_fetch_url <URL>:<management_port>  
-secret <security_key> -shcluster_label <label>
```

```
./splunk restart
```

Setting up the captain

Select one of the initialized instances to be the first cluster captain and run the following command

```
./splunk bootstrap shcluster-captain -servers_list  
"<URI>:<management_port>,<URI>:<management_port>,..." -auth  
<username>:<password>
```

See the cluster status

To check the overall status of your search head cluster, run this command from any member:

```
./splunk show shcluster-status -auth <username>:<password>
```

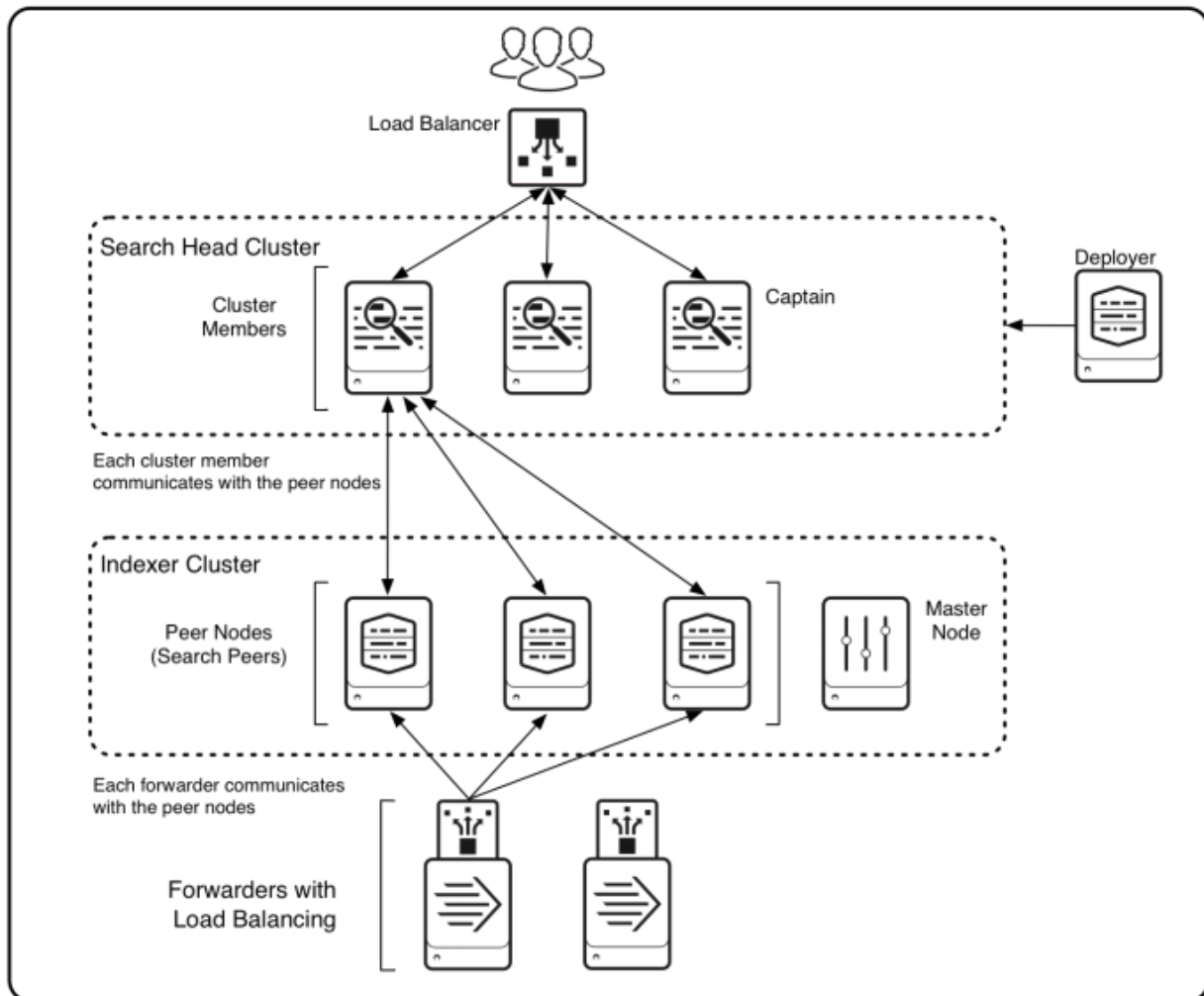
See the cluster configurations

To see the Search Head Configuration of all the members present in the cluster run the following command from any cluster member

```
./splunk list shcluster-config -auth admin:monitor
```

Integrate the search head cluster with an indexer cluster

To integrate a search head cluster with an indexer cluster, configure each member of the search head cluster as a search head on the indexer cluster. Once you do that, the search heads get their list of search peers from the manager node of the indexer cluster.



Configure each search head cluster member as a search head on the indexer cluster. Use the command

```
./splunk edit cluster-config -mode searchhead -master_uri  
<URI>:<management_port> -secret <security_key>
```