**We need 6 total machines 2 SH, 2 Indexers, 1 deployer , 1 CM**

**Step 1**

uname -m (To check the OS version if 64 download splunk accordingly)

**Step 2**

Download Splunk with Wget

wget -O splunk-7.0.0-c8a78efdd40f-Linux-x86\_64.tgz 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86\_64&platform=linux&version=7.0.0&product=splunk&filename=splunk-7.0.0-c8a78efdd40f-Linux-x86\_64.tgz&wget=true'

wget -O splunk-7.1.1-8f0ead9ec3db-Linux-x86\_64.tgz 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86\_64&platform=linux&version=7.1.1&product=splunk&filename=splunk-7.1.1-8f0ead9ec3db-Linux-x86\_64.tgz&wget=true'

wget -O splunk-8.0.1-6db836e2fb9e-Linux-x86\_64.tgz 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86\_64&platform=linux&version=8.0.1&product=splunk&filename=splunk-8.0.1-6db836e2fb9e-Linux-x86\_64.tgz&wget=true'

unzip the downloaded folder

tar –xvzf splunk-7.0.0-c8a78efdd40f-Linux-x86\_64.tgz

**Step 3**

start splunk

/opt/splunk/bin ./splunk start - -accept-license

**Note :-** Splunk can also be started at boot time for that enable it

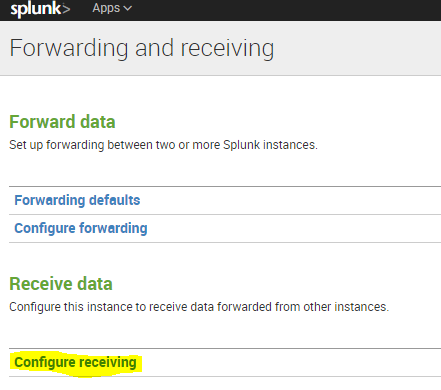
./splunk enable boot-start –user root or splunk

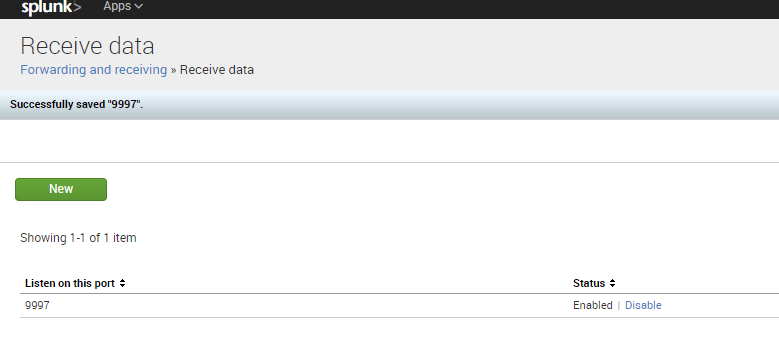
**Step4**

Repeat above 3 steps on all the machines

**Step5**

**Setup Indexers**





**Step 6:- Enable Clustering**

You ordinarily need to enable multiple [**peer nodes**](http://docs.splunk.com/Splexicon:Peernode) to deploy a cluster. Before enabling the set of peers, you must enable and restart the [**master node**](http://docs.splunk.com/Splexicon:Masternode).

**Enable the master**

o enable an indexer as the master node:

**1.** Click **Settings** in the upper right corner of Splunk Web.

**2.** In the **Distributed environment** group, click **Indexer clustering**.

**3.** Select **Enable indexer clustering**.

**4.** Select **Master node** and click **Next**.

**5.** There are a few fields to fill out:

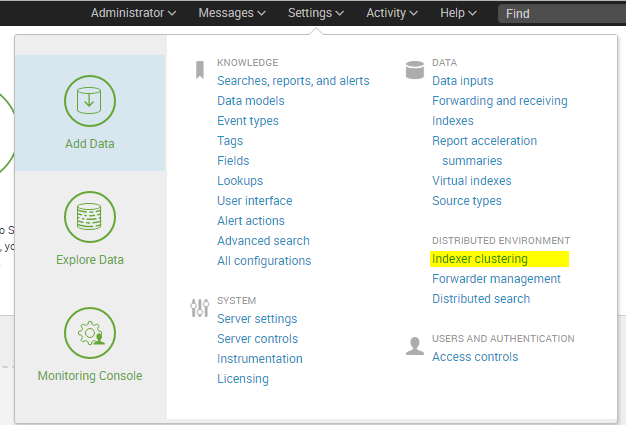
* **Replication Factor.**The [**replication factor**](http://docs.splunk.com/Splexicon:Replicationfactor) determines how many copies of data the cluster maintains. The default is 3. For more information on the replication factor, see [Replication factor](http://docs.splunk.com/Documentation/Splunk/6.6.1/Indexer/Basicclusterarchitecture#Replication_factor). Be sure to choose the right replication factor now. It is inadvisable to increase the replication factor later, after the cluster contains significant amounts of data.
* **Search Factor.** The [**search factor**](http://docs.splunk.com/Splexicon:Searchfactor) determines how many immediately searchable copies of data the cluster maintains. The default is 2. For more information on the search factor, see [Search factor](http://docs.splunk.com/Documentation/Splunk/6.6.1/Indexer/Basicclusterarchitecture#Search_factor). Be sure to choose the right search factor now. It is inadvisable to increase the search factor later, once the cluster has significant amounts of data.
* **Security Key**. This is the key that authenticates communication between the master and the peers and search heads. The key must be the same across all cluster nodes. The value that you set here must be the same that you subsequently set on the peers and search heads as well.
* **Cluster Label**. You can label the cluster here. The label is useful for identifying the cluster in the monitoring console.

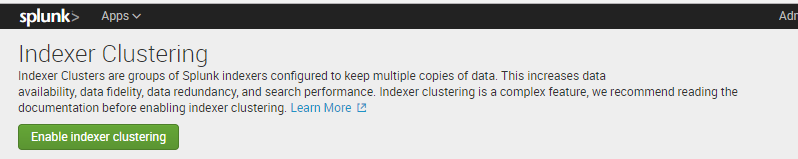
**6.** Click **Enable master node**.

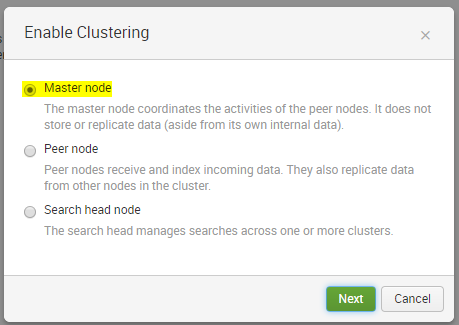
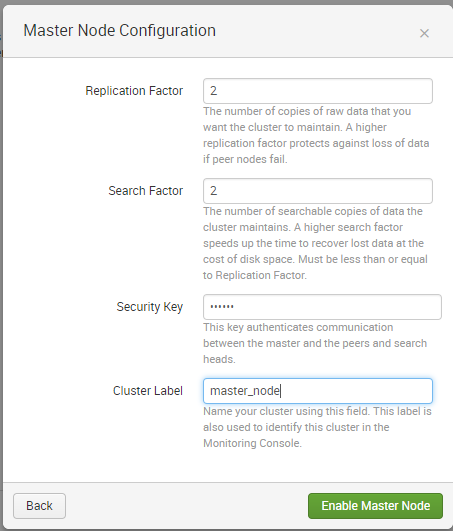
* The message appears, "You must restart Splunk for the master node to become active. You can restart Splunk from Server Controls."

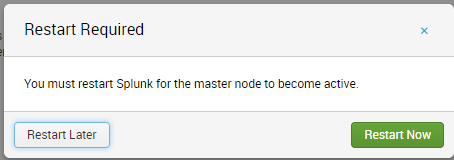
**7.** Click **Go to Server Controls**. This takes you to the Settings page where you can initiate the restart.

* **Important:** When the master starts up for the first time, it will block indexing on the peers until you enable and restart the full replication factor number of peers. Do not restart the master while it is waiting for the peers to join the cluster. If you do, you will need to restart the peers a second time.

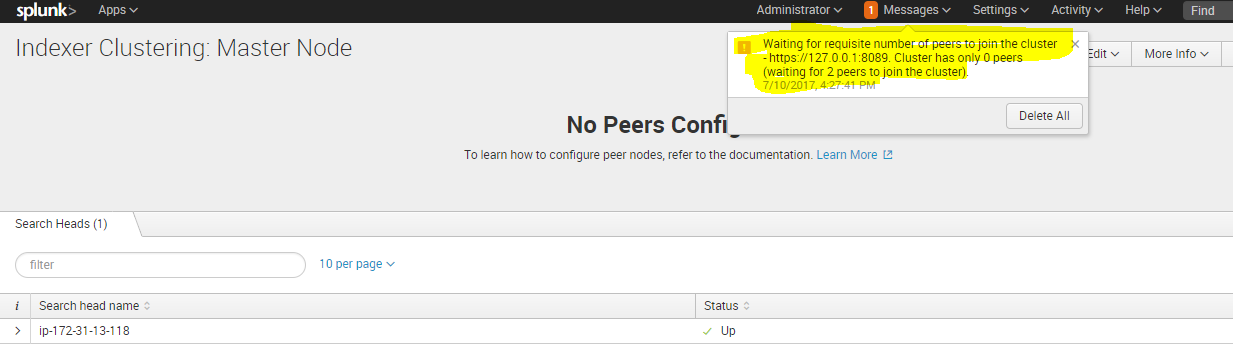


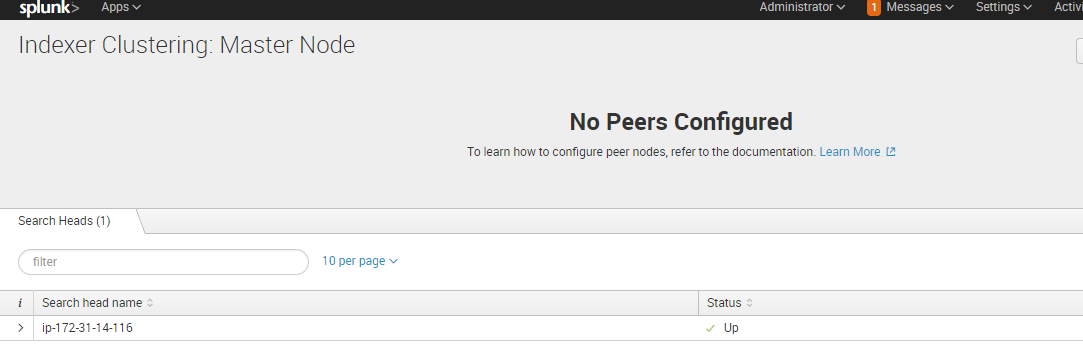




**Re-Login to master machine and you will find the below screen**





**This is because we have not set the peers (Indexers) yet in a cluster**

## Enable the peer

To enable an indexer as a peer node:

**1.** Click **Settings** in the upper right corner of Splunk Web.

**2.** In the **Distributed environment** group, click **Indexer clustering**.

**3.** Select **Enable indexer clustering**.

**4.** Select **Peer node** and click **Next**.

**5.** There are a few fields to fill out:

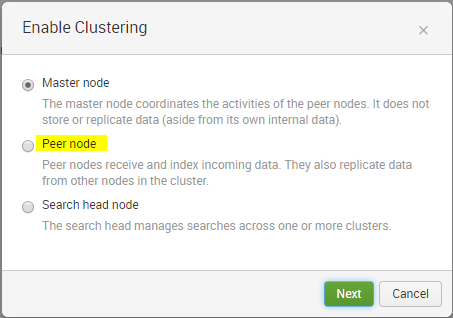
* **Master URI**. Enter the master's URI, including its management port. For example: [https://10.152.31.202:8089](https://10.152.31.202:8089/).
* **Peer replication port**. This is the port on which the peer receives replicated data streamed from the other peers. You can specify any available, unused port for this purpose. This port must be different from the management or receiving ports.
* **Security key**. This is the key that authenticates communication between the master and the peers and search heads. The key must be the same across all cluster nodes. Set the same value here that you previously set on the master node.

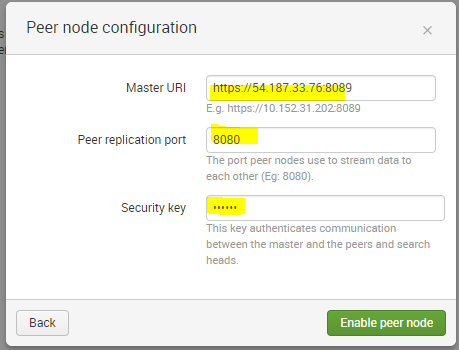
**6.** Click **Enable peer node**.

The message appears, "You must restart Splunk for the peer node to become active."

**7.** Click **Go to Server Controls**. This takes you to the Settings page where you can initiate the restart.

**8.** Repeat this process for all the cluster's peer nodes.

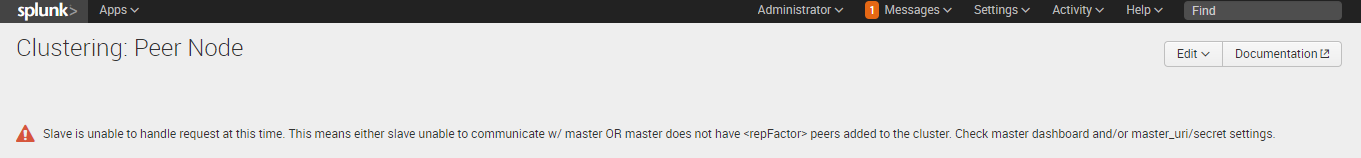




**Use the same Security Key which you have used while setting up Mater node.**

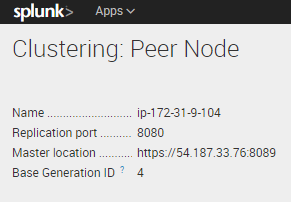
**Restart Indexer 1**

**After restart you will get below error on indexer 1 . This is because you haven’t met the replication factor yet . To remove this error repeat all the above steps on indexer 2.**



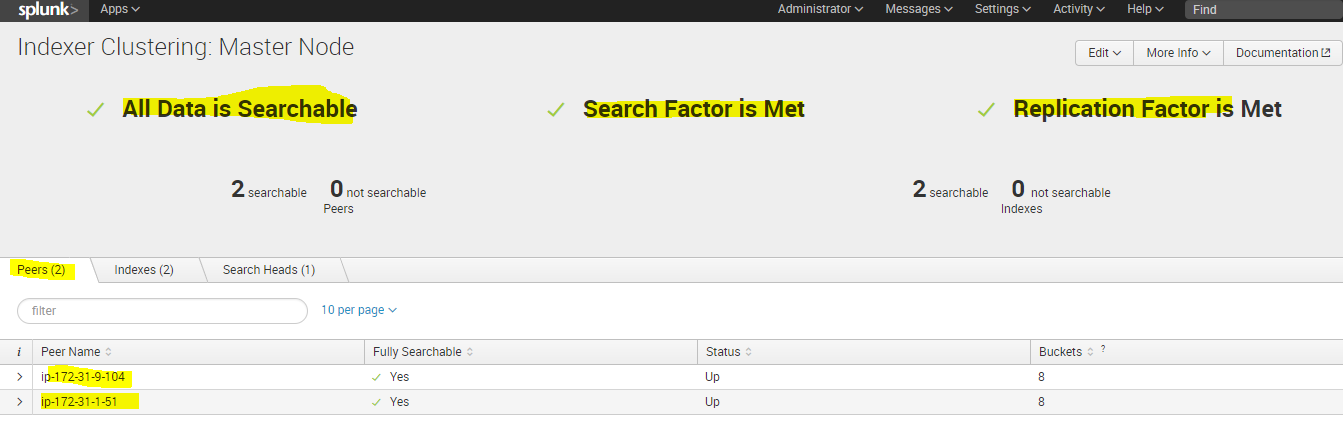
**Once you create second indexer as peer node take restart. Wait for couple of seconds and check the status now on both the indexer and on master node.**

**On Indexer you will see something below .**



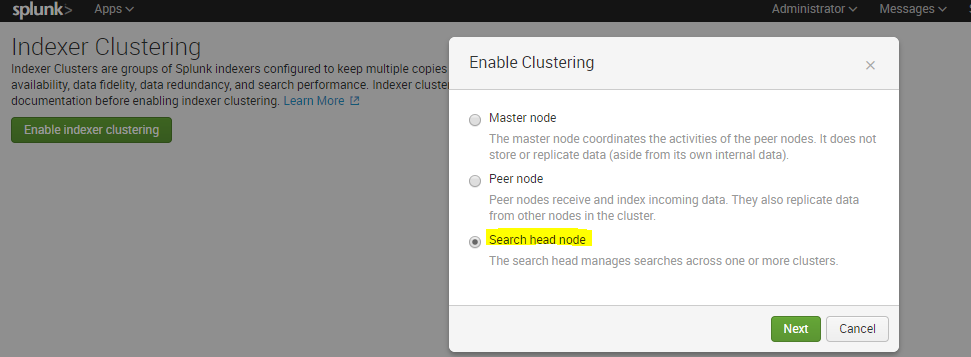
**If you see above in both the indexers indicates that your both peers are in cluster now and each can store data and they replicate on each other as we have mentioned RF 2 in our master node configuration.**

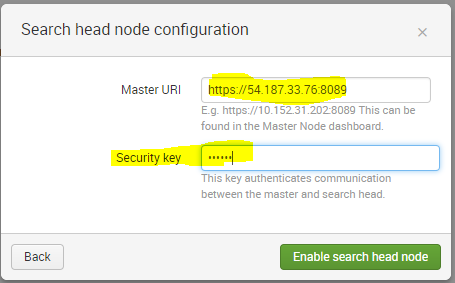
**On master node in settings🡪indexer clustering you will see as below.**

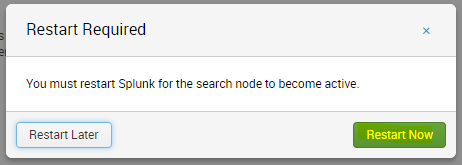


**Note: - Here if you noticed No search head is in cluster which Master can manage so do the following on all search heads.**

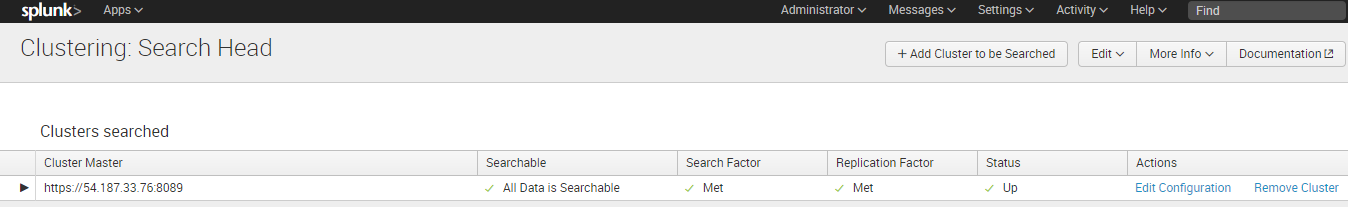
**On search head 1**





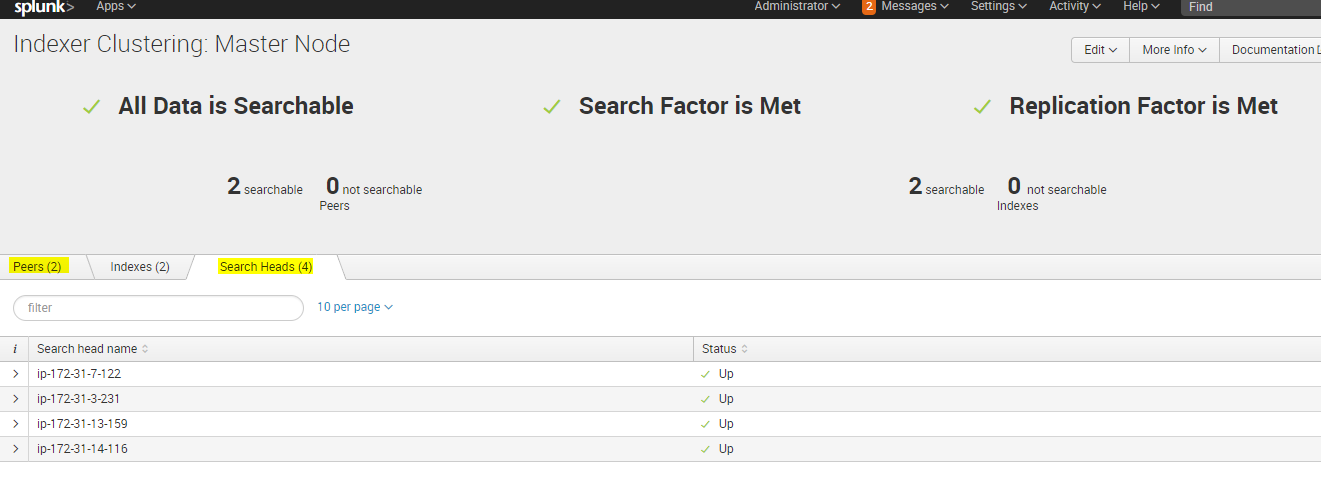


**On search head 1 you should see below**



**Now repeat above steps on all search heads and keep on restarting all SH.**

**Once done you will see your all SH and Peer nodes in cluster master webpage as below**



**We have total 4 machines 2 –SH and 2 –Indexers , why master node is showing 5 machines in search head tab . Note :- Master node enables it’s own Search head splunk recommends use this SH for dev purpose only do not use it in actual production .**

**Check the configurations on seach head and Indexers**

|  |  |  |
| --- | --- | --- |
| **Server** | **Config name** | **Stenza** |
| **SH1,2,3** | **Server.conf (/opt/splunk/etc/system/local)** | **[clustering]**  **master\_uri = https://54.187.33.76:8089**  **mode = slave**  **pass4SymmKey = $1$VkCsx3RpeA==** |
| **Indexer 1,2** | **Server.conf (/opt/splunk/etc/system/local)** | **[clustering]**  **master\_uri = https://54.187.33.76:8089**  **mode = slave**  **pass4SymmKey = $1$VkCsx3RpeA==** |

# Deploy a search head cluster

* [**1. Identify your requirements**](http://docs.splunk.com/Documentation/Splunk/6.6.2/DistSearch/SHCdeploymentoverview#1._Identify_your_requirements)
* [**2. Set up the deployer**](http://docs.splunk.com/Documentation/Splunk/6.6.2/DistSearch/SHCdeploymentoverview#2._Set_up_the_deployer)
* [**3. Install the Splunk Enterprise instances**](http://docs.splunk.com/Documentation/Splunk/6.6.2/DistSearch/SHCdeploymentoverview#3._Install_the_Splunk_Enterprise_instances)
* [**4. Initialize cluster members**](http://docs.splunk.com/Documentation/Splunk/6.6.2/DistSearch/SHCdeploymentoverview#4._Initialize_cluster_members)
* [**5. Bring up the cluster captain**](http://docs.splunk.com/Documentation/Splunk/6.6.2/DistSearch/SHCdeploymentoverview#5._Bring_up_the_cluster_captain)
* [**6. Perform post-deployment set-up**](http://docs.splunk.com/Documentation/Splunk/6.6.2/DistSearch/SHCdeploymentoverview#6._Perform_post-deployment_set-up)
* [**1. Identify your requirements**](http://docs.splunk.com/Documentation/Splunk/6.6.2/DistSearch/SHCdeploymentoverview#1._Identify_your_requirements)
* [**2. Set up the deployer**](http://docs.splunk.com/Documentation/Splunk/6.6.2/DistSearch/SHCdeploymentoverview#2._Set_up_the_deployer)
* [**3. Install the Splunk Enterprise instances**](http://docs.splunk.com/Documentation/Splunk/6.6.2/DistSearch/SHCdeploymentoverview#3._Install_the_Splunk_Enterprise_instances)
* [**4. Initialize cluster members**](http://docs.splunk.com/Documentation/Splunk/6.6.2/DistSearch/SHCdeploymentoverview#4._Initialize_cluster_members)
* [**5. Bring up the cluster captain**](http://docs.splunk.com/Documentation/Splunk/6.6.2/DistSearch/SHCdeploymentoverview#5._Bring_up_the_cluster_captain)
* [**6. Perform post-deployment set-up**](http://docs.splunk.com/Documentation/Splunk/6.6.2/DistSearch/SHCdeploymentoverview#6._Perform_post-deployment_set-up)

## Deploy the cluster

These are the key steps in deploying clusters:

**1.** Identify your requirements.

**2.** Set up the deployer.

**3.** Install the Splunk Enterprise instances.

**4.** Initialize cluster members.

**5.** Bring up the cluster captain.

**6.** Perform post-deployment set-up.

### Set up the deployer

This instance cannot be a member of the search head cluster, but, under some circumstances, it can be a Splunk Enterprise instance in use for other purposes. If necessary, install a new Splunk Enterprise instance to serve as the deployer. **Deployer functionality is automatically enabled on all Splunk Enterprise instances. The main configuration step is to specify the deployer's security key**

1. Configure the deployer's security key.

To set the key on the deployer, specify the pass4SymmKey attribute in either the [general] or the [shclustering] stanza of the deployer's server.conf file. For example:

[shclustering]

pass4SymmKey = yoursecuritykey

1. Set the search head cluster label on the deployer

The search head cluster label is useful for identifying the cluster in the monitoring console. This parameter is optional, but if you configure it on one member, you must configure it with the same value on all members, as well as on the deployer.

To set the label, specify the shcluster\_label attribute in the [shclustering] stanza of the deployer's server.conf file. For example:

[shclustering]

shcluster\_label = shcluster1

### 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

example

splunk init shcluster-config -auth admin:abc123 -mgmt\_uri https://ec2-54-190-5-3.us-west-2.compute.amazonaws.com:8089 -replication\_port 7111 -replication\_factor 2 -conf\_deploy\_fetch\_url https://ec2-34-212-230-56.us-west-2.compute.amazonaws.com:8089 -secret abc123 -shcluster\_label shcluster1

Note the following:

* This command is only for cluster members(SH). Do not run this command on the deployer.
* You can only execute this command on an instance that is up and running.
* The -auth parameter specifies your current login credentials for this instance. This parameter is required.
* The -mgmt\_uri parameter specifies the URI and management port for this instance(SH). You must use the fully qualified domain name. This parameter is required.
* The -replication\_port parameter specifies the port that the instance uses to listen for search artifacts streamed from the other cluster members. You can specify any available, unused port as the replication port. Do not reuse the instance's management or receiving ports. This parameter is required.
* The -replication\_factor parameter determines the number of copies of each search artifact that the cluster maintains. All cluster members must use the same replication factor. This parameter is optional. If not explicitly set, the replication factor defaults to 3.
* The -conf\_deploy\_fetch\_url parameter specifies the URL and management port for the deployer instance. This parameter is optional during initialization, but you do need to set it before you can use the deployer functionality. See ["Use the deployer to distribute apps and configuration updates."](http://docs.splunk.com/Documentation/Splunk/6.6.2/DistSearch/PropagateSHCconfigurationchanges)
* The -secret parameter specifies the security key that authenticates communication between the cluster members and between each member and the deployer. The key must be the same across all cluster members and the deployer.

### Bring up the cluster captain

**a.** Select one of the initialized instances to be the first cluster captain. It does not matter which instance you select for this role.

**b.** Run the splunk bootstrap shcluster-captain command on the selected instance:

splunk bootstrap shcluster-captain -servers\_list "<URI>:<management\_port>,<URI>:<management\_port>,..." -auth <username>:

Note the following:

* This command designates the specified instance as the first cluster captain.
* Run this command on only a single instance.
* The -servers\_list parameter contains a comma-separated list of the cluster members, including the member that you are running the command on. The members are identified by URI and management port. This parameter is required.
* **Important:** The URIs that you specify in -servers\_list must be exactly the same as the ones that you specified earlier when you initialized each member, in the -mgmt\_uri parameter. You cannot, for example, use [https://foo.example.com:8089](https://foo.example.com:8089/) during initialization and [https://foo.subdomain.example.com:8089](https://foo.subdomain.example.com:8089/) here, even if they resolve to the same node.

Here is an example of the bootstrap command:

splunk bootstrap shcluster-captain -servers\_list "https://sh1.example.com:8089,https://sh2.example.com:8089,https://sh3.example.com:8089,https://sh4.example.com:8089" -auth admin:changed

### Perform post-deployment set-up

# **Connect the search head cluster to search peers.** Integrate the search head cluster with an indexer cluster

If the search head cluster is connected to an indexer cluster, the master node on the indexer cluster provides the search heads with a list of peer nodes to search against.

Configure each search head cluster member as a search head on the indexer cluster. Use the CLI splunk edit cluster-config command. For example:

splunk edit cluster-config -mode searchhead -master\_uri https://10.152.31.202:8089 -secret newsecret123

splunk restart

./splunk edit cluster-config -mode searchhead -master\_uri https://ec2-54-187-33-76.us-west-2.compute.amazonaws.com:8089 -secret abc123

This example specifies:

* The instance is a search head in an indexer cluster.Run this command on all SH
* The master node of the indexer cluster resides at 10.152.31.202:8089.
* The secret key is "newsecret123". You must use the same secret key across all nodes in both the indexer cluster and the search head cluster.

You must do this for each member of the search head cluster.

This is all you need for the basic configuration. The search heads now run their searches against the peer nodes in the indexer cluster.

## Check search head cluster status

./splunk show shcluster-status -auth admin:abc123

## Deploy a configuration bundle

To deploy a configuration bundle, you push the bundle from the deployer to the cluster members.

### Push the configuration bundle

To push the configuration bundle to the cluster members:

Note :- Before start make sure you have set the pass4SymmKey on al the SH cluster member and on Deployer . Also note If the search head cluster is part of an indexer cluster, set the key in the [general] stanza, so that the instance uses the same key in its two roles of both a search head cluster member and an indexer cluster node.

Else

Directly edit server.conf on all SH nodes and on Deployer and add following

[shclustering]

pass4SymmKey = yoursecuritykey

**1.** Put the apps and other configuration changes in subdirectories under shcluster/ on the deployer. (Note :- Copy app folder under /etc/shcluster/apps folder , do not place directly under Schluter folder )

**2.** Untar any app.

**3.** Run the splunk apply shcluster-bundle command on the deployer:

splunk apply shcluster-bundle -target <URI>:<management\_port> -auth <username>:<password>

Note the following:

* The -target parameter specifies the URI and management port for any member of the cluster, for example, https://10.0.1.14:8089. You specify only one cluster member but the deployer pushes to all members. This parameter is required.
* The -auth parameter specifies credentials for the deployer instance.

In response to splunk apply shcluster-bundle, the deployer displays this message:

Warning: Depending on the configuration changes being pushed, this command

might initiate a rolling-restart of the cluster members. Please refer to the

documentation for the details. Do you wish to continue? [y/n]:

For information on which configuration changes trigger restart, see $SPLUNK\_HOME/etc/system/default/app.conf. It lists the configuration files that do not trigger restart when changed. All other configuration changes trigger restart.

**4.** To proceed, respond to the message with y.

**Note:** You can eliminate the message by appending the flag --answer-yes to the splunk apply shcluster-bundlecommand:

splunk apply shcluster-bundle --answer-yes -target <URI>:<management\_port> -auth <username>:<password>

This is useful if you are including the command in a script or otherwise automating the process.

**Warning: You must run splunk apply shcluster-bundle command only on a deployer. If you mistakenly run it on a non-deployer instance, such as a cluster member, it will cause your apps to be deleted.**

## View cluster information

There are a number of splunk list commands that return different types of cluster information. For example, to get detailed information on each peer in the cluster, run this command on the master:

splunk list cluster-peers

To get information on the cluster configuration, run this command from any node:

splunk list cluster-config

See the CLI clustering help for the full set of splunk list commands.

**UF**

1. **You have to download UF and start it on the machine**
2. **Create outputs.conf file on UF under /opt/splunk/etc/system/local/**

**[tcpout]**

**defaultGroup = default-autolb-group**

**[tcpout:default-autolb-group]**

**server = LP-PC0TA2E1:9997,LP-PC0TA2E2:9997**

**[tcpout-server://LP-PC0TA2E1:9997]**

**Restart UF**

1. **Check connection in \_internal index on Indexers**
2. **Cross check in the logs on UF under /opt/splunkUF/var/log/splunkd.log**