

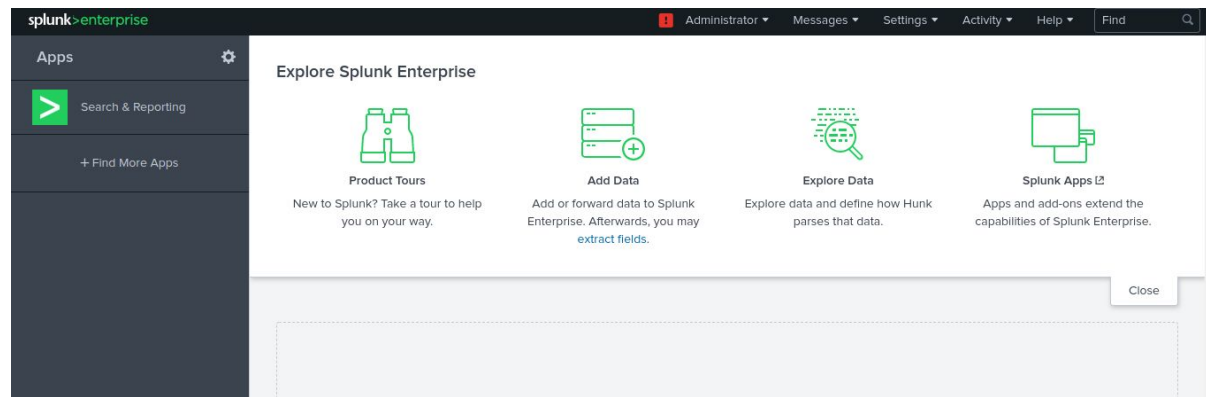
# Splunk Tutorial Part-2

After creating all the instances with Splunk enterprise version we have to connect them

- First We start configuring Master Node
- For setting up the Master node, we have to connect to Splunk GUI by entering the http://Master Node's [Public IP]:8000 in search bar
- Then Splunk login page will appear and we have to fill the details with which we created admin & password while setting Splunk enterprise on Instance



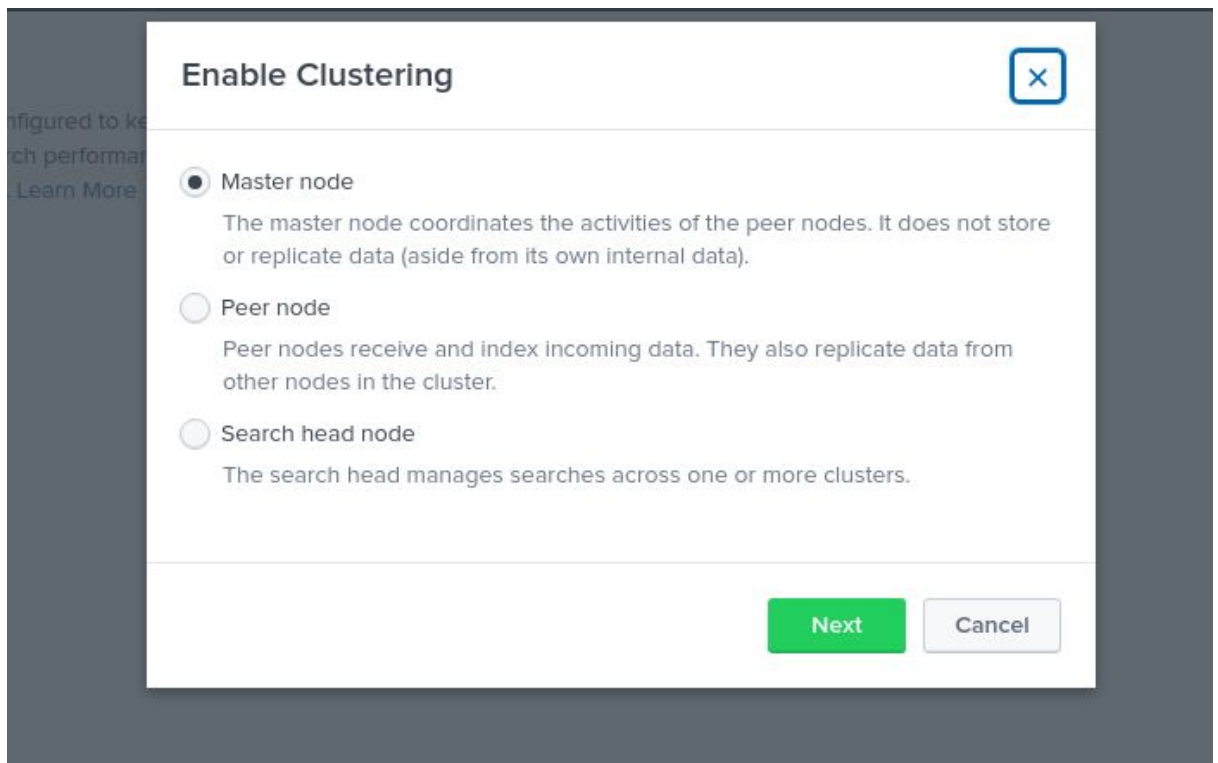
- After Logging in to the Splunk GUI it look similar to the below image



## ● Configuring Master Node

Then we should go to settings - Indexer clustering -  
Enable Indexer clustering - (select)  
Master node - (click on) Next.

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍



- After clicking on next it will ask you to set Replication Factor, Search Factor, Security Key, Cluster Label.

**Master Node Configuration** [X]

Replication Factor: 3  
The number of copies of raw data that you want the cluster to maintain. A higher replication factor protects against loss of data if peer nodes fail.

Search Factor: 2  
The number of searchable copies of data the cluster maintains. A higher search factor speeds up the time to recover lost data at the cost of disk space. Must be less than or equal to Replication Factor.

Security Key: .....|  
This key authenticates communication between the master and the peers and search heads.

Cluster Label: Optional  
Name your cluster using this field. This label is also used to identify this cluster in the Monitoring Console.

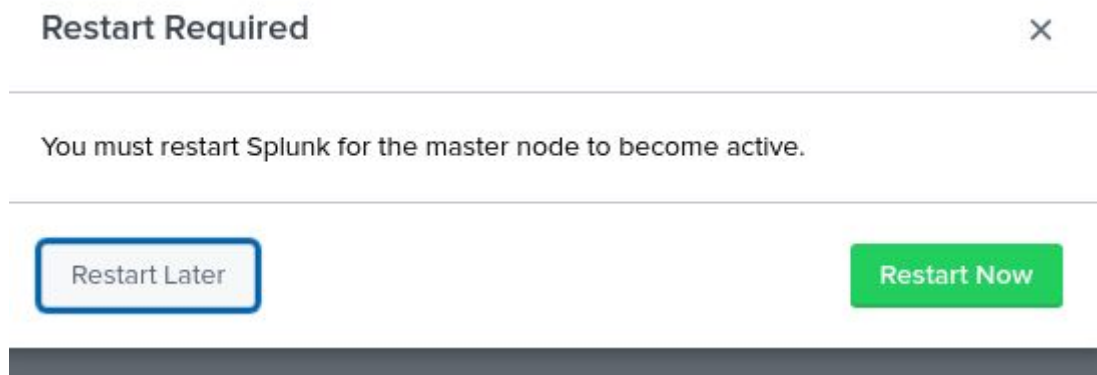
[Back] [Enable Master Node]

- Replication Factor - Keep the Replication Factor as 3 which is by default.

NOTE : Indexers (peer nodes) should not be less than Replication Factor value.

- Search Factor - Keep the Search Factor as 2 which is by default.

- NOTE : The password which you enter should be same for setting up the peer nodes.
- After clicking on Enable Master Node the Splunk has to be restarted.



- Now Connect to Terminal using SSH and login as root user in terminal.

```
[root@ip-172-31-39-12 local]# cd /opt/splunk/etc/master-apps/_cluster/local
[root@ip-172-31-39-12 local]# vi indexes.conf
```

- Now insert the below text in indexes.conf file

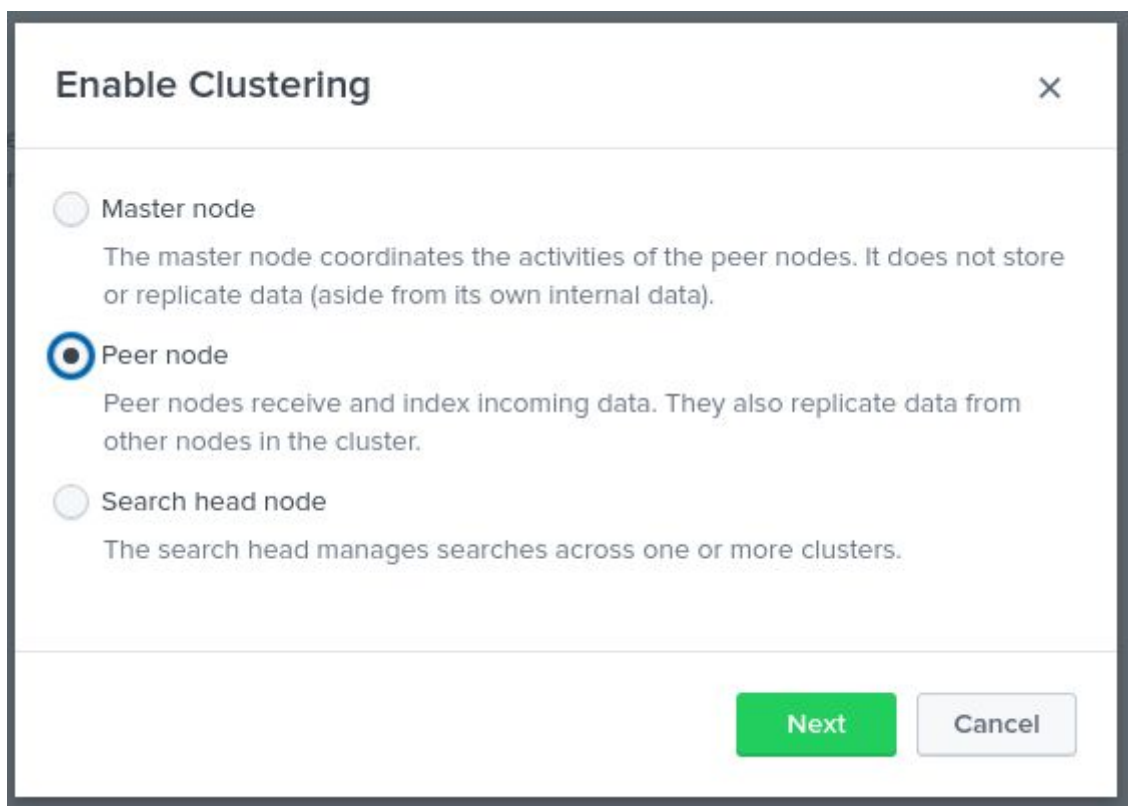
```
[c1index]
homePath    = $SPLUNK_DB/c1index/db
coldPath    = $SPLUNK_DB/c1index/colddb
thawedPath  = $SPLUNK_DB/c1index/thaweddb
repFactor   = auto
```

- After pasting the above text SAVE the file and Restart the server.

```
[root@ip-172-31-39-12 local]# cd /opt/splunk/bin/
[root@ip-172-31-39-12 bin]# ./splunk stop
Stopping splunkd...
Shutting down. Please wait, as this may take a few minutes.
.. [ OK ]
Stopping splunk helpers...
[ OK ]
Done.
[root@ip-172-31-39-12 bin]# ./splunk start
```

## Connecting Peer Nodes To Cluster

- Now for connecting peer nodes we should login to the Indexer Instance.
- Then we should go to settings - Indexer clustering - Enable Indexer clustering - (select) Peer node -(click on) Next.



**Enable Clustering** [X]

☐ Master node  
The master node coordinates the activities of the peer nodes. It does not store or replicate data (aside from its own internal data).

☒ Peer node  
Peer nodes receive and index incoming data. They also replicate data from other nodes in the cluster.

☐ Search head node  
The search head manages searches across one or more clusters.

**Next** **Cancel**

- After clicking on next it will ask you to set Master URI, Peer replication port, Security key.

**Peer node configuration** ×

Master URI   
E.g. https://10.152.31.202:8089

Peer replication port   
The port peer nodes use to stream data to each other (Eg: 8080).

Security key   
This key authenticates communication between the master and the peers and search heads.

- NOTE : Use same Security Key which we used for configuring Master Node.
- After clicking on Enable Peer Node the Splunk has to be restarted.



Restart Later

Restart Now

- Likewise connect other 2 (Indexer's) peer nodes to cluster.

## Heavy Forwarder Configuration

- Now for connecting peer nodes we should login to the Heavy Forwarder Instance.
- Then we should go to settings - Forwarding and Receiving - Configure forwarding - New Forwarding Host.

### Forwarding and receiving

#### Forward data

Set up forwarding between two or more Splunk instances.

[Forwarding defaults](#)

[Configure forwarding](#)

+ Add new

#### Receive data

Configure this instance to receive data forwarded from other instances.

[Configure receiving](#)

+ Add new

### Forward data

[Forwarding and receiving](#) » Forward data

[New Forwarding Host](#)

App  Owner  Visible in the App

25 per page

There are no configurations of this type. Click the "New Forwarding Host" button to create a new configuration.

### Add new

[Forwarding and receiving](#) » [Forward data](#) » Add new

Enter host:port to forward data to. Data will be auto load balanced to each host:port.

Host \*

Set as host:port or IP:port.  
You must also enable receiving on this host.

Cancel

Save

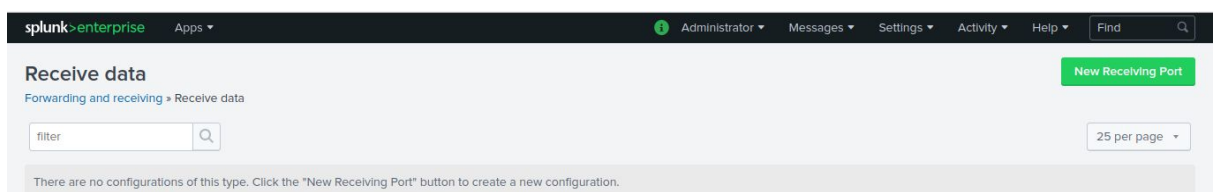
- After clicking on New Forwarding Host it will ask you to set Host. Host = Host IP:9997
- NOTE : Host IP is nothing but Indexer IP
- After entering Host IP:9997 click on Save and Restart the Splunk.
- Likewise connect host for other 2 Indexers.
- Now Connect to Terminal using and login as root user in terminal

```
[root@ip-172-31-43-19 ~]# cd /opt/splunk/bin/
[root@ip-172-31-43-19 bin]# ./splunk add monitor /var/log
Your session is invalid. Please login.
Splunk username: admin
Password:
Added monitor of '/var/log'.
[root@ip-172-31-43-19 bin]#
```

- To check whether the file has created or not we should use the below commands.

```
[root@ip-172-31-43-19 bin]# cd /opt/splunk/etc/apps/search/local/
[root@ip-172-31-43-19 local]# ls
inputs.conf
[root@ip-172-31-43-19 local]#
```

- Above you can see the file has been created.
- Now come to Peer Nodes GUI and go to settings - Forwarding and Receiving - Configure Receiving - New Receiving Port.



- Likewise set port for other 2 Indexers.

## Connecting Search Head to Cluster

- Login to Search Head Splunk GUI.
- Then we should go to settings - Indexer clustering  
- Enable Indexer clustering - (select)  
Search Head node - (click on) Next.

Enable Clustering

☐ Master node  
The master node coordinates the activities of the peer nodes. It does not store or replicate data (aside from its own internal data).

☐ Peer node  
Peer nodes receive and index incoming data. They also replicate data from other nodes in the cluster.

☒ Search head node  
The search head manages searches across one or more clusters.

Next

Cancel

•

Connecting Search Head to Cluster	
Master URI	Master IP:8089
Security Key	Password

•

- Master IP = Master Node IP

- Security Key : Use same Security Key which we used for configuring Master Node.
- After clicking on Enable Search Head Node the Splunk has to be restarted.
- **Download & Upload  
aws\_30\_days.csv file**

- Download the aws\_30\_days.csv and now upload it in Heavy Forwarder GUI by going to settings - Add Data - Upload Data - (click on) Next - (Again click on) Next - Create a new Index.
- After clicking on Create a New Index it will ask you to set the below information.

The screenshot shows the 'Add Data' section of the Splunk Heavy Forwarder GUI. At the top, a progress bar indicates the current step is 'Select Source', with other steps being 'Set Source Type', 'Input Settings', 'Review', and 'Done'. Navigation buttons for '< Back' and 'Next >' are visible. The main content area is titled 'Select Source' and instructs the user to 'Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below.' A 'Selected File' section shows '30\_day\_EC2\_RI\_Rec.csv' with a 'Select File' button. Below this is a large rectangular drop zone with the text 'Drop your data file here' and a note that 'The maximum file upload size is 500 Mb'. A 'Done' button is located at the bottom right of the interface.

Add Data

< Back

Review >

Select Source

Set Source Type

Input Settings

Review

Done

### Input Settings

Optionally set additional input parameters for this data input as follows:

#### Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

☒ Constant value

☐ Regular expression on path

☐ Segment in path

Host field value

ip-172-31-19-210.us-east-2.compute.int

#### Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can [always change this setting later. Learn More](#)

Index

Default

Create a new index



File has been uploaded successfully.

Configure your inputs by going to Settings > [Data Inputs](#)

Start Searching

Search your data now or see [examples and tutorials](#).

After entering the above Info (click on) SAVE - Review - Submit.

## Configuration Bundle: Validate and Push

- Now login to Mastor Node web interface and Edit Configuration Bundle Actions to Click Validate and Check Restart and push

## Configuration Bundle Actions

Click Push to distribute the configuration bundle to the set of peers. Optionally, validate the bundle and check if peer restart is required without distributing the bundle, or rollback to the previous bundle. [Learn More](#)

[Back to Master Node](#)

Validate and Check Restart

Push

Rollback

Last Push: ✓ Successful

Updated Time ..... 22/01/2021, 10:49:17  
Active Bundle ID ? ..... 2B1CODEDB72F09C4A6ED02BC5026D13B  
Latest Bundle ID ? ..... 2B1CODEDB72F09C4A6ED02BC5026D13B  
Previous Bundle ID ? ..... 50C325AD39E94AC324538EE3544F8D97

10 per page ▼

i	Peer	Site	Status	Action Status
>	ip-172-31-1161.us-east-2.compute.internal	default	Up	None
>	ip-172-31-30-129.us-east-2.compute.internal	default	Up	None
>	ip-172-31-42-182.us-east-2.compute.internal	default	Up	None

Then automatically creates c1index on PEER Nodes. See the below Image

telemetry	Edit	Delete	Disable	Events	_cluster	1 MB	488.28 GB	3	2 hours ago	28 minutes ago	\$SPLUNK_DB/telemetry/db	N/A	✓ Enabled
telemetry	Edit	Delete	Disable	Events	_cluster	1 MB	488.28 GB	0			\$SPLUNK_DB/telemetry/db	N/A	✓ Enabled
c1index	Edit	Delete	Disable	Events	_cluster	1 MB	488.28 GB	0			\$SPLUNK_DB/c1index/db	N/A	✓ Enabled
history	Edit	Delete	Disable	Events	_cluster	1 MB	488.28 GB	0			\$SPLUNK_DB/historydb/db	N/A	✓ Enabled
main	Edit	Delete	Disable	Events	_cluster	1 MB	488.28 GB	115	2 hours ago	11 minutes ago	\$SPLUNK_DB/defaultdb/db	N/A	✓ Enabled

Now go to one of the Search head GUI and search for index="c1index". You get information similar to below image,

## New Search

Save As ▼

Create Table View

Close

index="c1index"

Last 24 hours ▼



✓ 32,445 events (21/01/2021 05:00:00.000 to 22/01/2021 05:35:52.000) No Event Sampling ▼

Job ▼



Smart Mode ▼

Events (32,445)

Patterns

Statistics

Visualization

Format Timeline ▼

Zoom Out

+ Zoom to Selection

× Deselect

1 hour per column

List ▼

Format

20 Per Page ▼

< Prev

1

2

3

4

5

6

7

8

...

Next >

< Hide Fields	All Fields	i	Time	Event
SELECTED FIELDS		>	22/01/2021 05:14:56.000	2013,Level 3,ZZ11,Food product manufacturing,Percentage,H41,Liabilities structure,Financial ratios,46,"ANZSIC06 groups C111, C112, C113, C114, C115, C116, C117, C118, and C119" host = ip-172-31-19-210.us-east-2.compute.internal source = annual-enterprise-survey-2019-financial-year-provisional-csv.csv sourcetype = csv
a host 1		>	22/01/2021 05:14:56.000	2013,Level 3,ZZ11,Food product manufacturing,Percentage,H40,Return on total assets,Financial ratios,5,"ANZSIC06 groups C111, C112, C113, C114, C115, C116, C117, C118, and C119" host = ip-172-31-19-210.us-east-2.compute.internal source = annual-enterprise-survey-2019-financial-year-provisional-csv.csv sourcetype = csv
a sourcetype 1		>	22/01/2021 05:14:56.000	2013,Level 3,ZZ11,Food product manufacturing,Percentage,H39,Return on equity,Financial ratios,12,"ANZSIC06 groups C111, C112, C113, C114, C115, C116, C117, C118, and C119" host = ip-172-31-19-210.us-east-2.compute.internal source = annual-enterprise-survey-2019-financial-year-provisional-csv.csv sourcetype = csv
INTERESTING FIELDS				
a index 1				
a Industry_aggregation_NZSIOC 3				
a Industry_code ANZSIC06 100+				

