# Splunk Tutorial Part-2

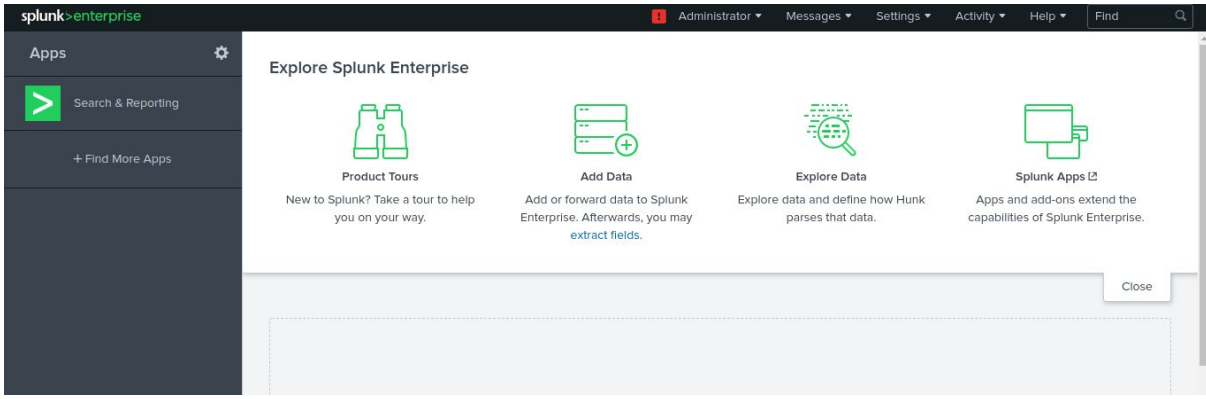
After creating all the instances with Splunk enterprise version we have to connect them

- First We start configuring Mastor 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

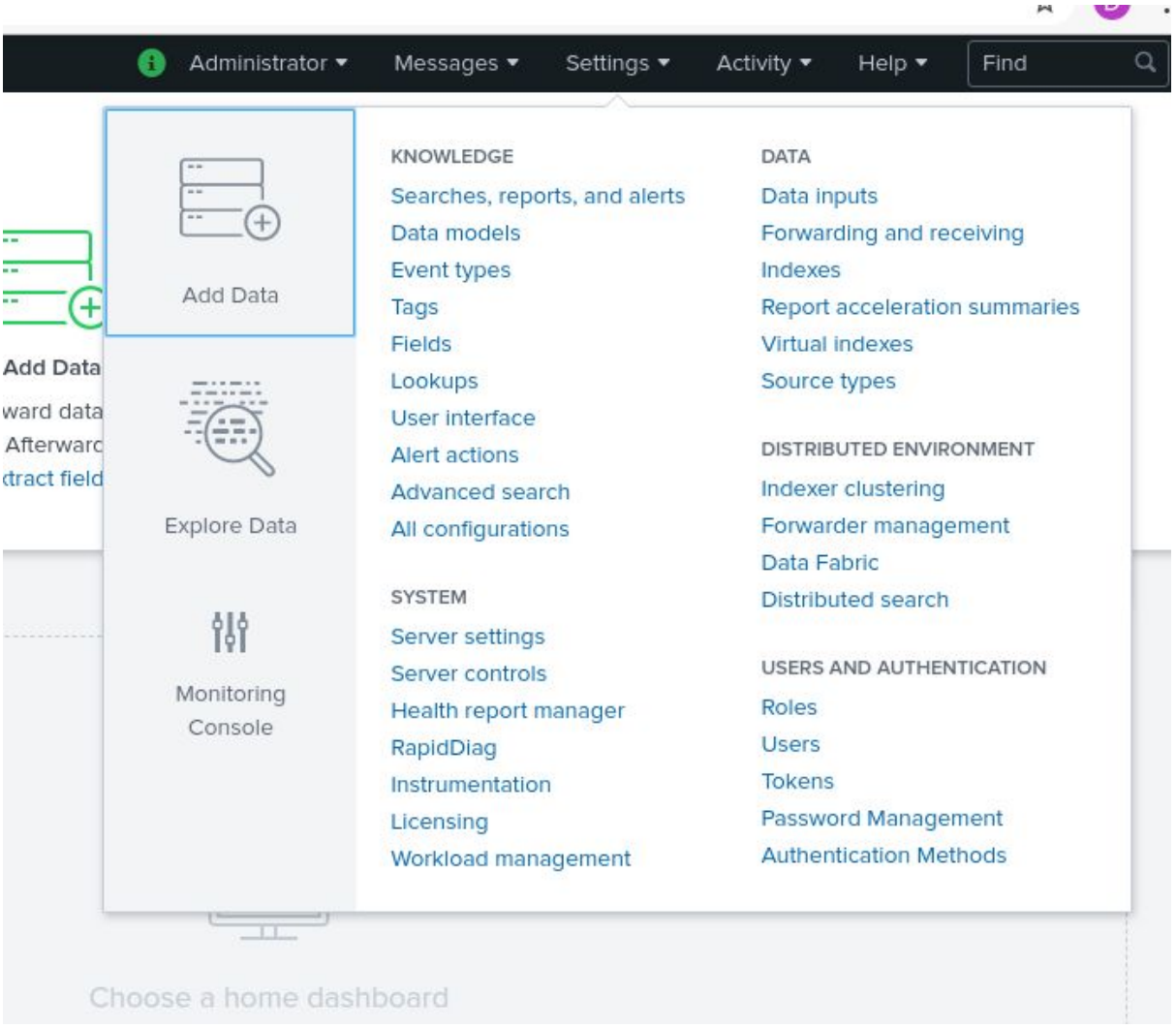
- Then Splunk login page will appear and we have to fill the details with which we created admin & password while setting Splunk enterprise on Instance

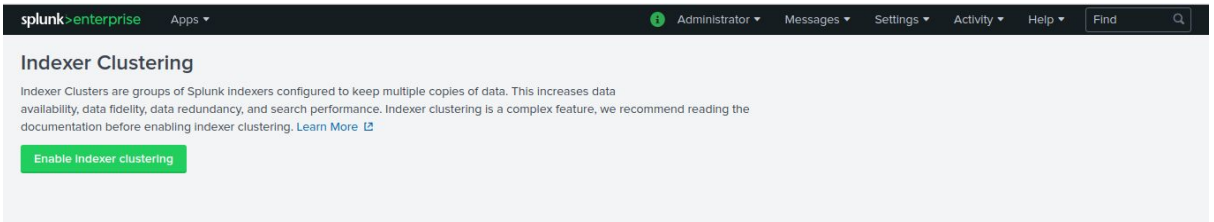

- After Logging in to the Splunk GUI it look similar to the below image

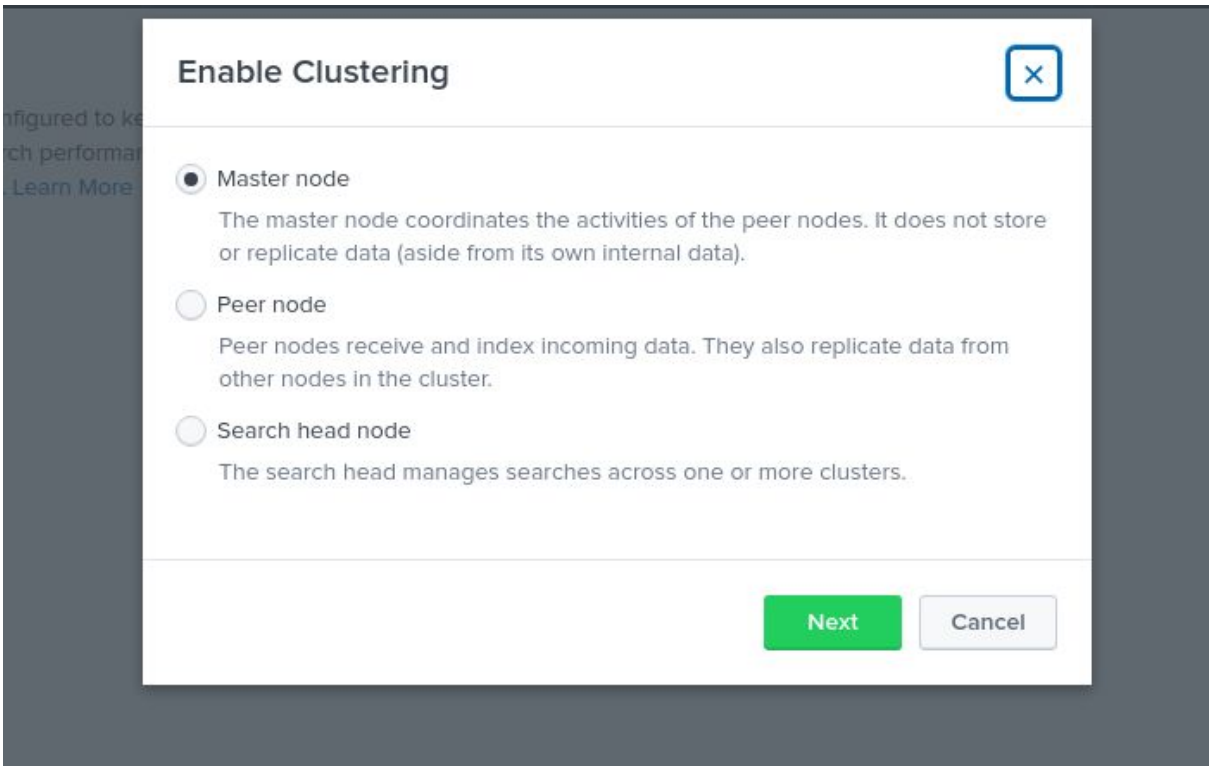



- # Configuring Master Node

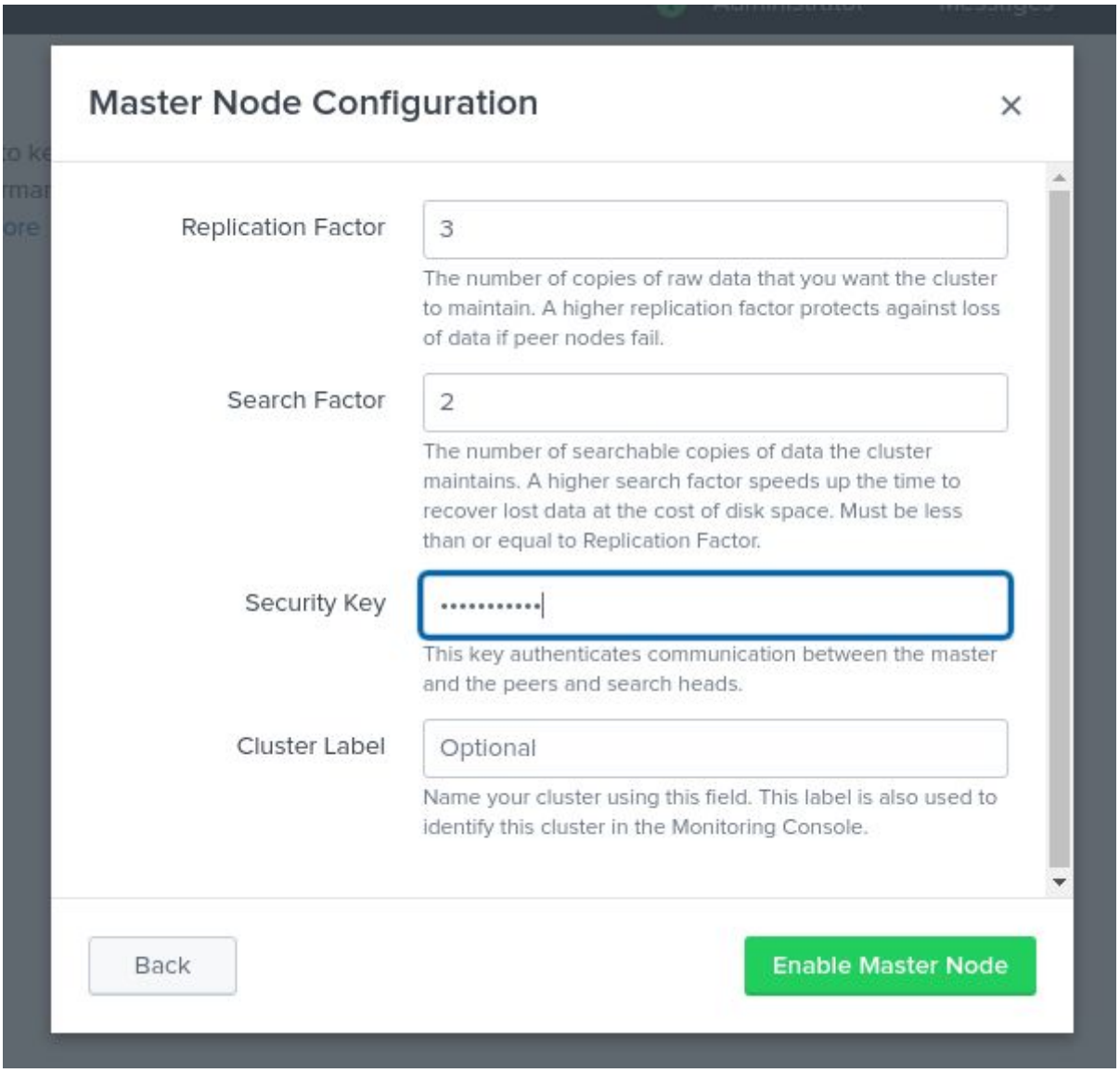
  Then we should go to settings - Indexer clustering - Enable Indexer clustering - (select)
  Master node - (click on) Next.


Administrator
Messages
Settings
Activity
Help
Find
Add Data
Explore Data
Monitoring Console
KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations
SYSTEM
Server settings
Server controls
Health report manager
RapidDiag
Instrumentation
Licensing
Workload management
DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Virtual indexes
Source types
DISTRIBUTED ENVIRONMENT
Indexer clustering
Forwarder management
Data Fabric
Distributed search
USERS AND AUTHENTICATION
Roles
Users
Tokens
Password Management
Authentication Methods
Choose a home dashboard


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Indexer Clustering
Indexer Clusters are groups of Splunk indexers configured to keep multiple copies of data. This increases data availability, data fidelity, data redundancy, and search performance. Indexer clustering is a complex feature, we recommend reading the documentation before enabling indexer clustering. Learn More
Enable Indexer clustering




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



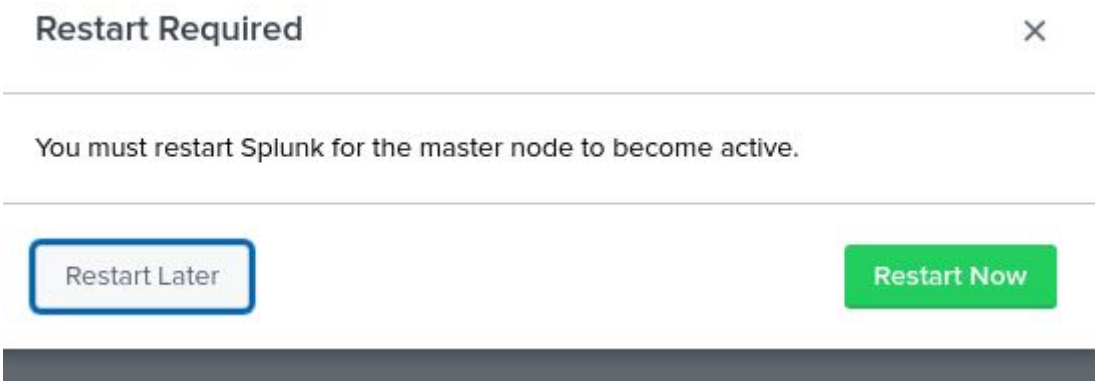

- Replication Factor - Keep the Replication Factor as 3 which is by default.

  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

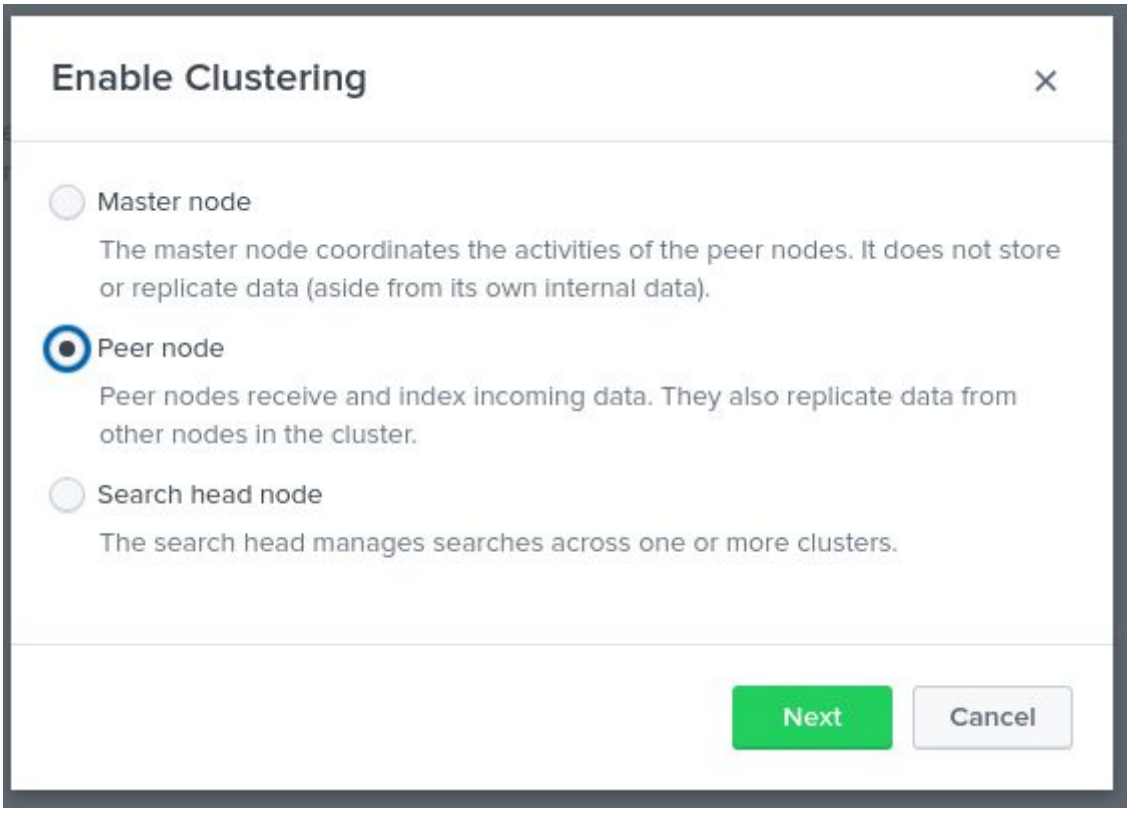
```
[c1index]
homePath   = $SPLUNK_DB/c1index/db
coldPath   = $SPLUNK_DB/c1index/colddb
thawedPath = $SPLUNK_DB/c1index/thaweddb
repFactor = auto
~
~
~
```

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

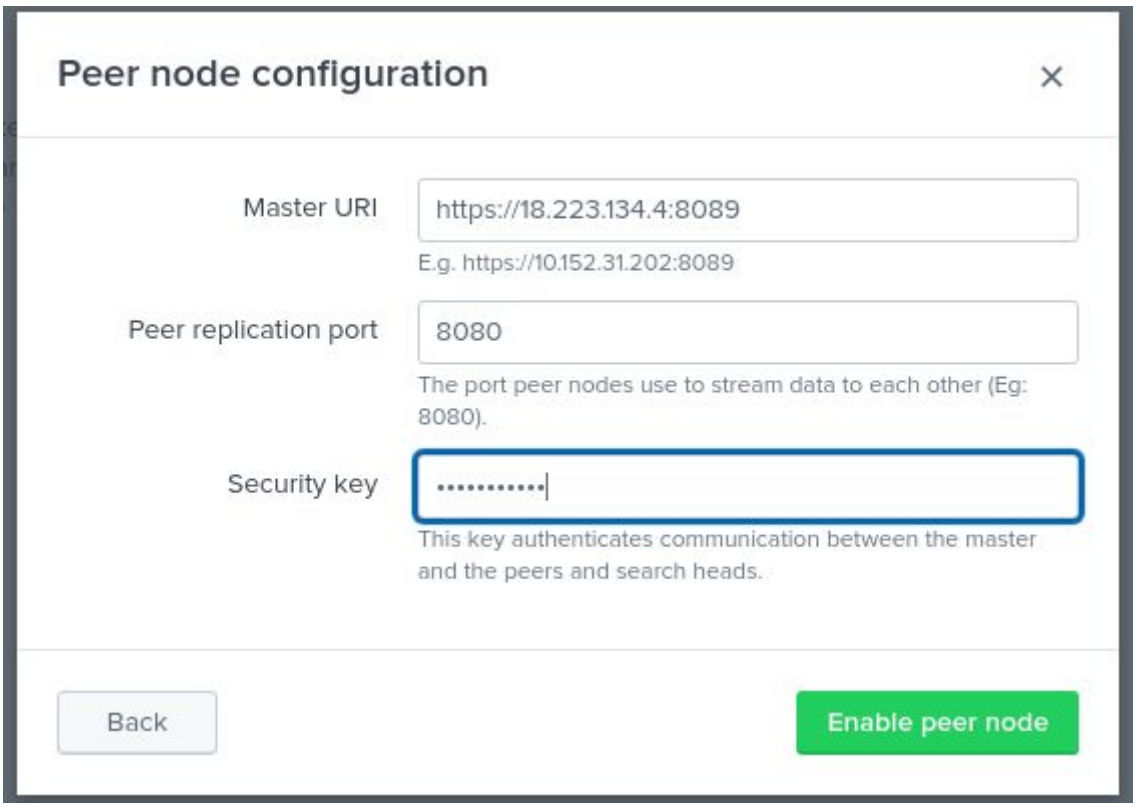
```
[root@ip-172-31-39-12 local]# cd /opt/splunk/bin/
[root@ip-172-31-39-12 bin]# ./splunk stop
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
..                                                          [  OK  ]
Stopping splunk helpers...
                           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



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




- NOTE : Use same Security Key which we used for configuring Master Node.

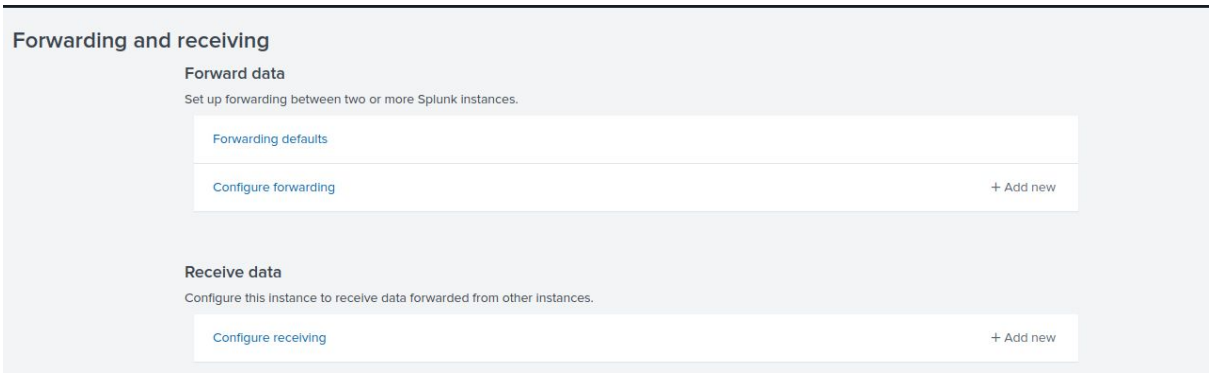
- After clicking on Enable Peer Node the Splunk has to be restarted.

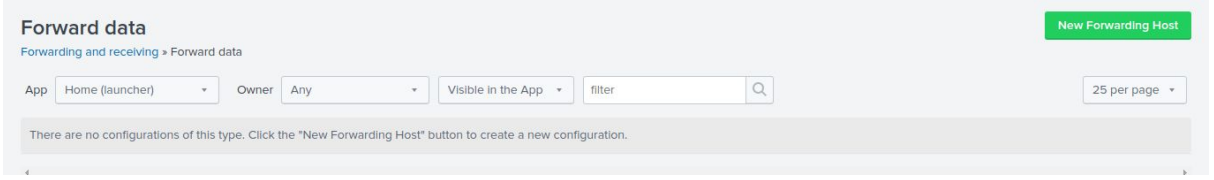

- Likewise connect other 2 (Indexer's) peer nodes to cluster.

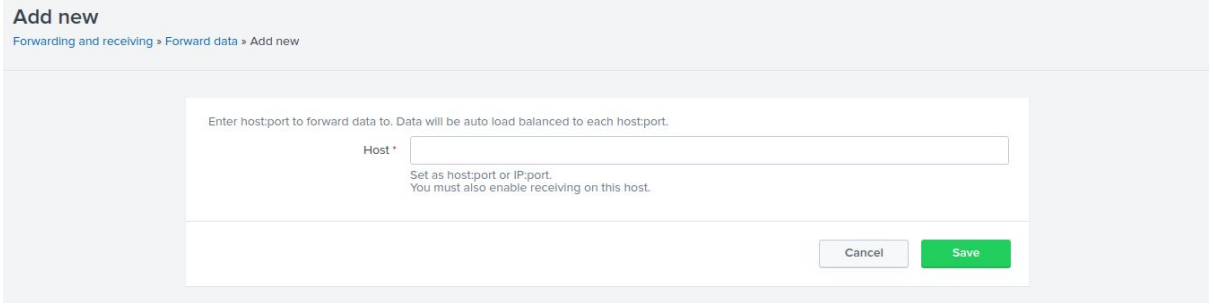
# Heavy Forwarder Configuration

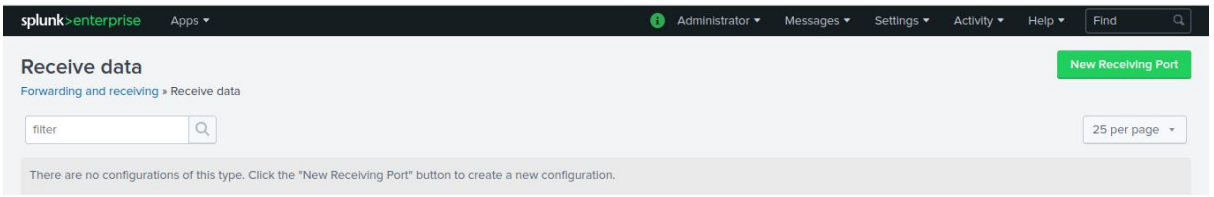
- Now for connecting peer nodes we should login to the Heavy Forwarder Instance.

- Then we should go to settings - Forwarding and Receiving - Configure forwarding - New Forwarding Host.

- 


- 


- 

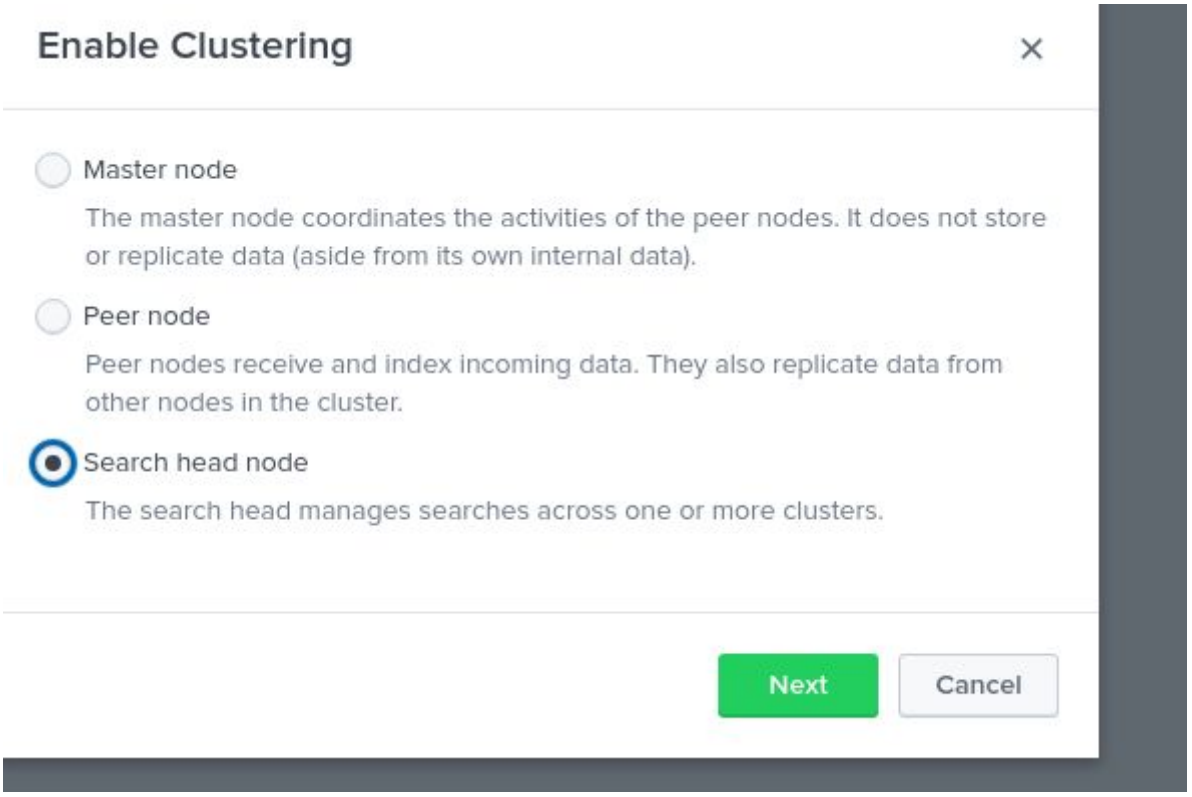
- After clicking on New Forwarding Host it will ask you to set Host.  Host = Host IP:9997
- NOTE : Host IP is nothing but Indexer IP
- After entering Host IP:9997 click on Save and Restart the Splunk.
- Likewise connect host for other 2 Indexers.
- Now Connect to Terminal using and login as root user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

- 

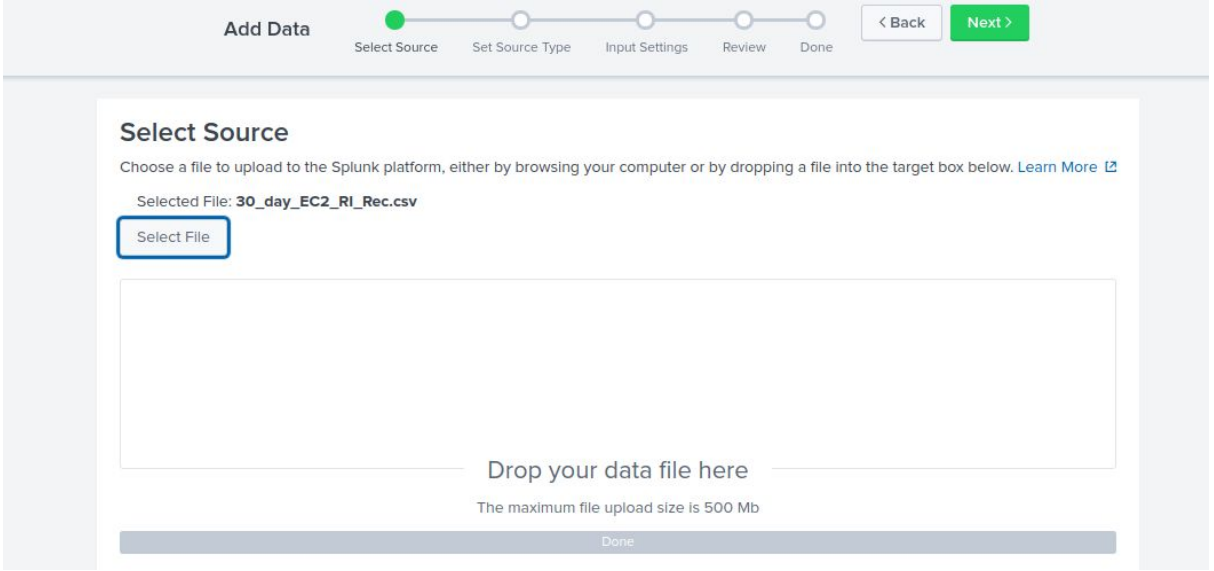

- 

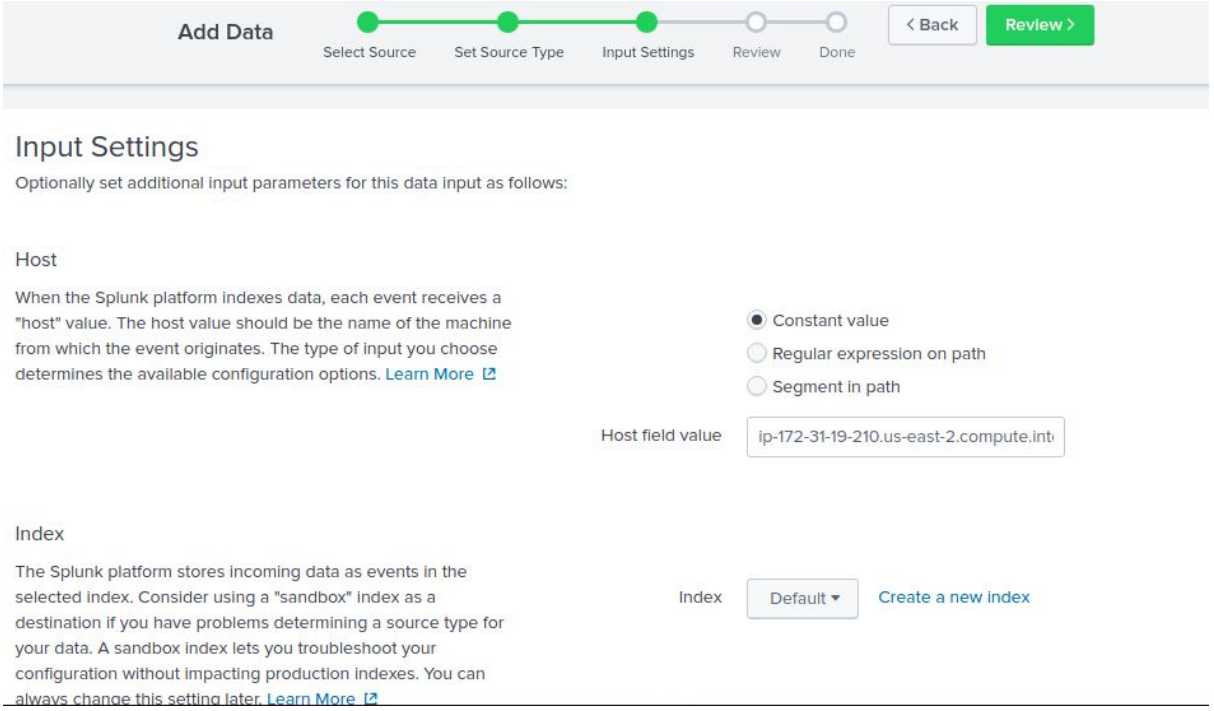
| Connecting Search Head to Cluster | |
|---|---|
| Master URI | Master IP:8089 |
| Security Key | Password |

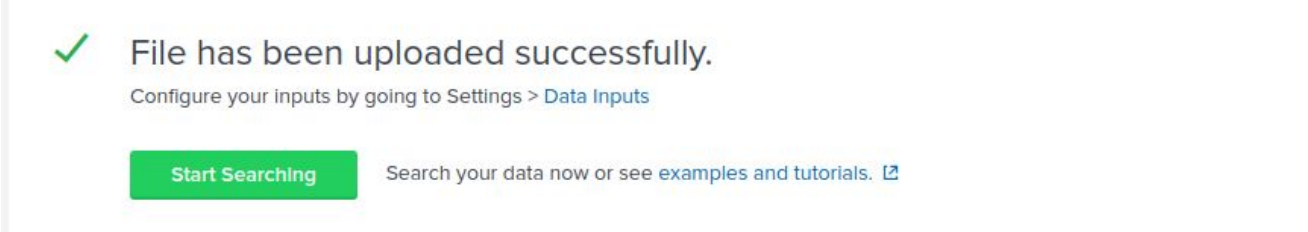
- Master IP = Master Node IP

- 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.
- 

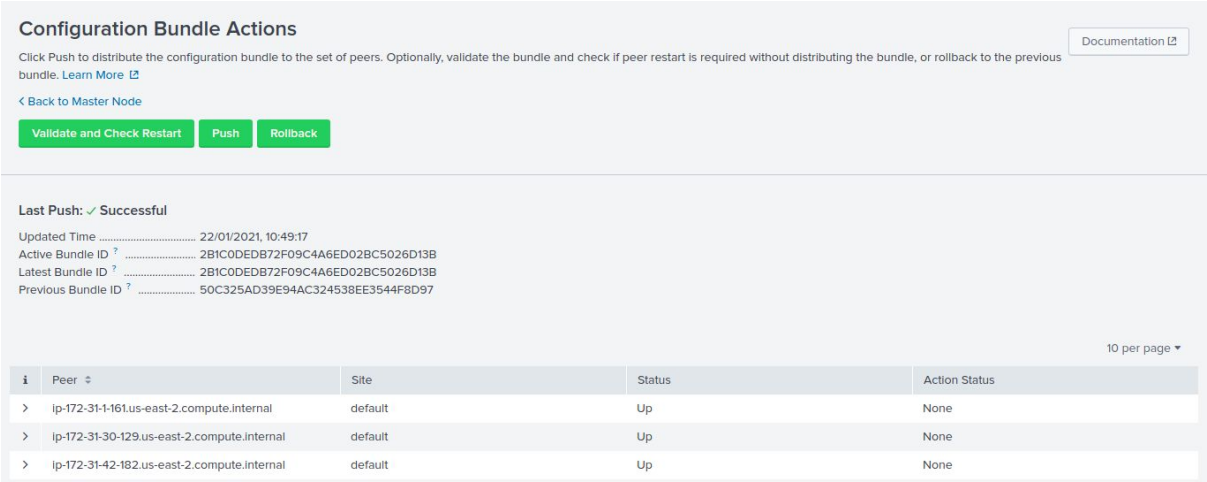


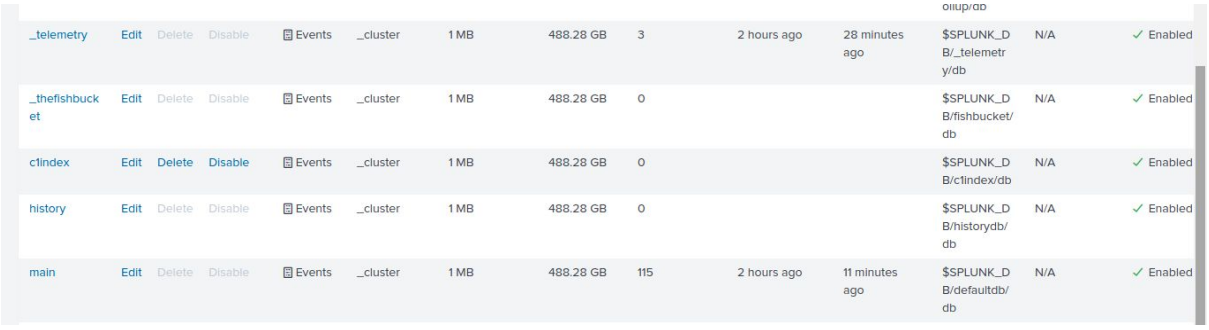

After entering the above Info (click on) SAVE - Review - Submit.

# 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




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




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