Splunk Guide

Install Splunk Enterprise On Windows

1.I have Launched AWS Windows Instance

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zon
Windows-Ec2	i-02dc43e20ed49e0a5	Running	t2.micro	2/2 checks ...	No alarms	us-east-2c

2. My Local system is Ubuntu..so using default Remmina software to access my Windows Instances

3.Download Splunk Enterprise

Splunk Enterprise 8.1.2

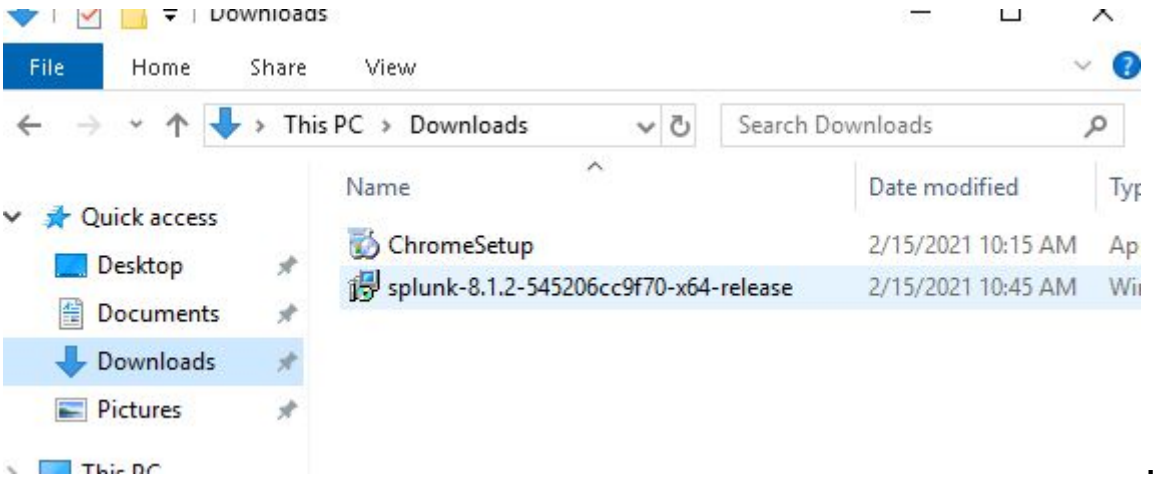
Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

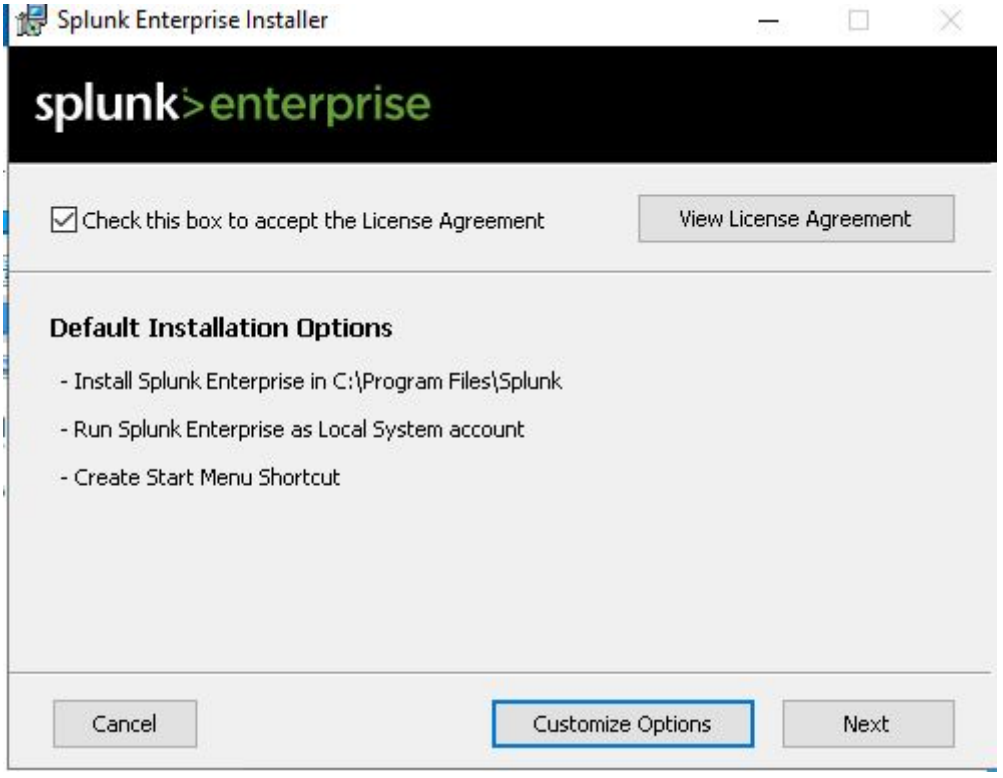
Choose Your Installation Package

Windows | Linux | Mac OS

64-bit	Windows 10 Windows Server 2016, 2019	.msi	289.81 MB	Download Now

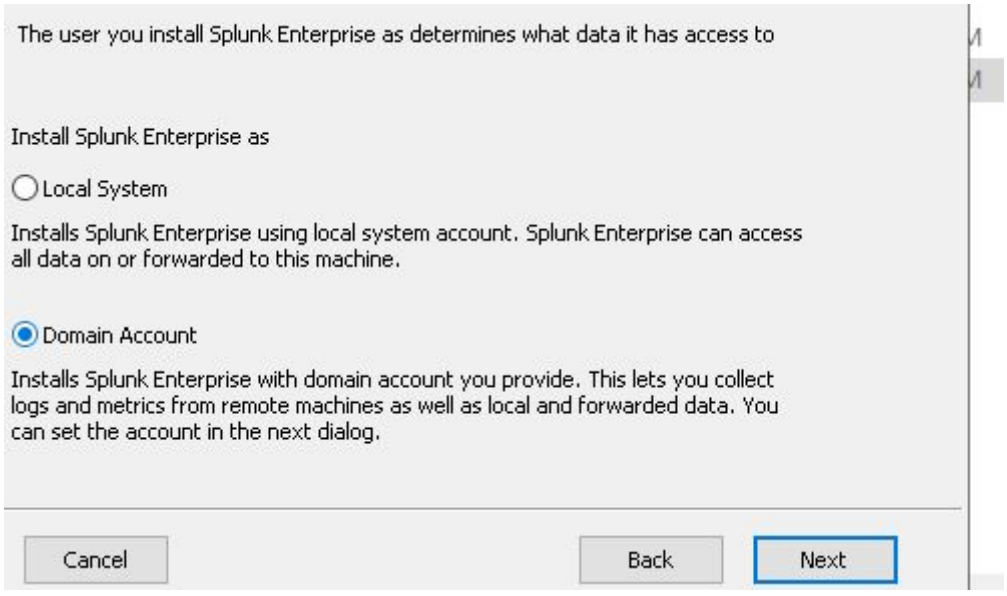
4.Install on manually





4.Prepare your Windows network to run Splunk Enterprise as a network or domain user.

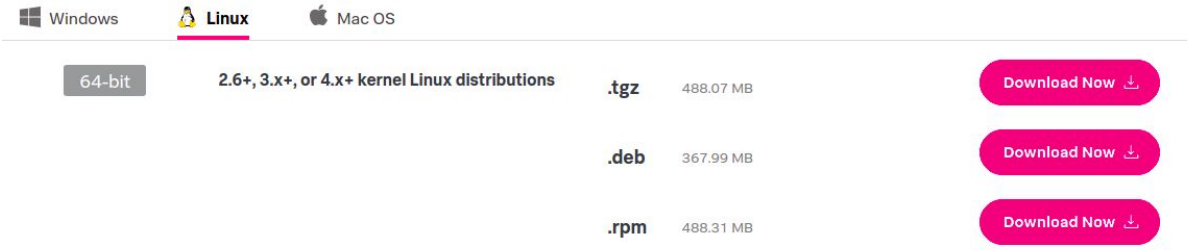
Username:administrator
password:whatever(for eg.development)



5.Complete Installation:

Install Splunk on Linux:

1.Select the format from option and download



2. using Command line to download:

```
dhana@dhana-Ubuntu:~$ cd /opt/
dhana@dhana-Ubuntu:/opt$ sudo su
[sudo] password for dhana:
root@dhana-Ubuntu:/opt# wget -O splunk-8.1.2-545206cc9f70-Linux-x86_64.tgz 'http
s://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platfo
rm=linux&version=8.1.2&product=splunk&filename=splunk-8.1.2-545206cc9f70-Linux-x
86_64.tgz&wget=true'
```

3.Extract the file is store in /opt

```
dhana@dhana-Ubuntu:~$ cd /opt/
dhana@dhana-Ubuntu:/opt$ sudo su
[sudo] password for dhana:
root@dhana-Ubuntu:/opt# tar -xvf splunk-8.1.2-545206cc9f70-Linux-x86_64.tgz
```

4.Start using

```
cd /opt/splunk/bin
```

```
./splunk -start --accept-license
```

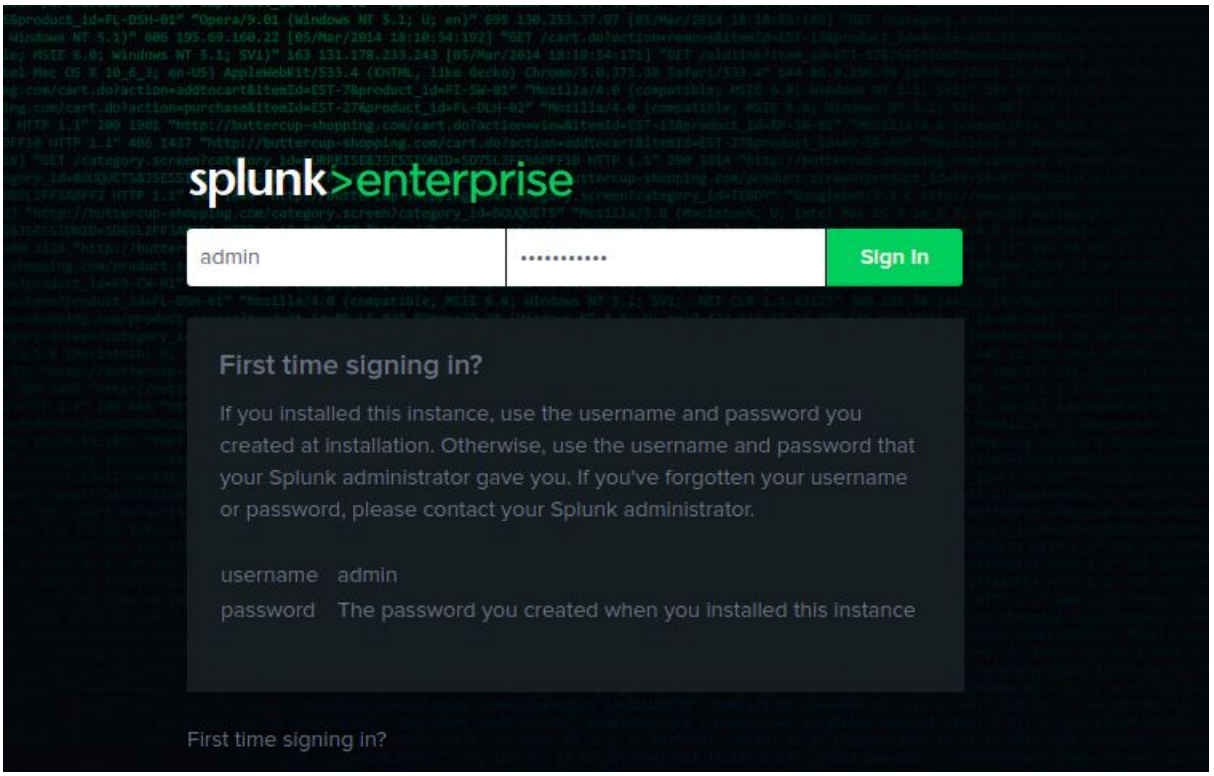
Username=admin
Password= whatever (For eg: development)

First Look with splunk

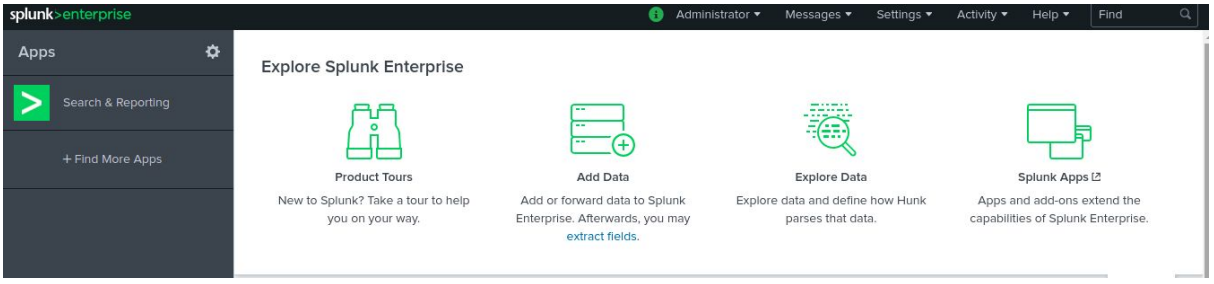
1. Now splunk is running on host<Public IP>:8000

(public IP address is used outside the network Otherwise Use localhost:8000)

2.Enter username and password used in Terminal While Installation:



3. Yes, You reached the Home Page 👏👏



File Hierarchy in Splunk

1.Main log file - splunkd.log

a .Location: cd /opt/splunk/var/log/splunk/splunkd.log

```
[root@ip-172-31-35-24 splunk]# cd /opt/splunk/var/log/splunk/
[root@ip-172-31-35-24 splunk]# vi splunkd.log
[root@ip-172-31-35-24 splunk]#
```

2.Default files (Do not edit these preconfigured files.):

a.$SPLUNK_HOME/etc/system/default

```
[root@ip-172-31-35-24 ~]# cd /opt/splunk/etc/system/default/
[root@ip-172-31-35-24 default]# ls
alert_actions.conf    global-banner.conf    serverclass.conf
app.conf              health.conf           server.conf
audit.conf            indexes.conf          source-classifier.conf
authentication.conf   inputs.conf           sourcetypes.conf
authorize.conf        limits.conf           telemetry.conf
collections.conf      literals.conf         times.conf
commands.conf         livetail.conf         transactiontypes.conf
conf.conf             messages.conf         transforms.conf
data                  metric_alerts.conf    ui-prefs.conf
datamodels.conf       metric_rollups.conf   ui-tour.conf
datatypesbnf.conf     multikv.conf          viewstates.conf
default-mode.conf     outputs.conf          visualizations.conf
distsearch.conf       procmon-filters.conf  web.conf
eventdiscoverer.conf  props.conf            workflow_actions.conf
event_renderers.conf  restmap.conf          workload_policy.conf
eventtypes.conf       savedsearches.conf    workload_pools.conf
federated.conf        searchbnf.conf        workload_rules.conf
fields.conf           segmenters.conf
[root@ip-172-31-35-24 default]#
```

3.Editable local files: $SPLUNK_HOME/etc/system/local

```
[root@ip-172-31-35-24 apps]# cd /opt/splunk/etc/system/local/
[root@ip-172-31-35-24 local]# ls
deploymentclient.conf  migration.conf  serverclass.conf
distsearch.conf        README          server.conf
[root@ip-172-31-35-24 local]#
```

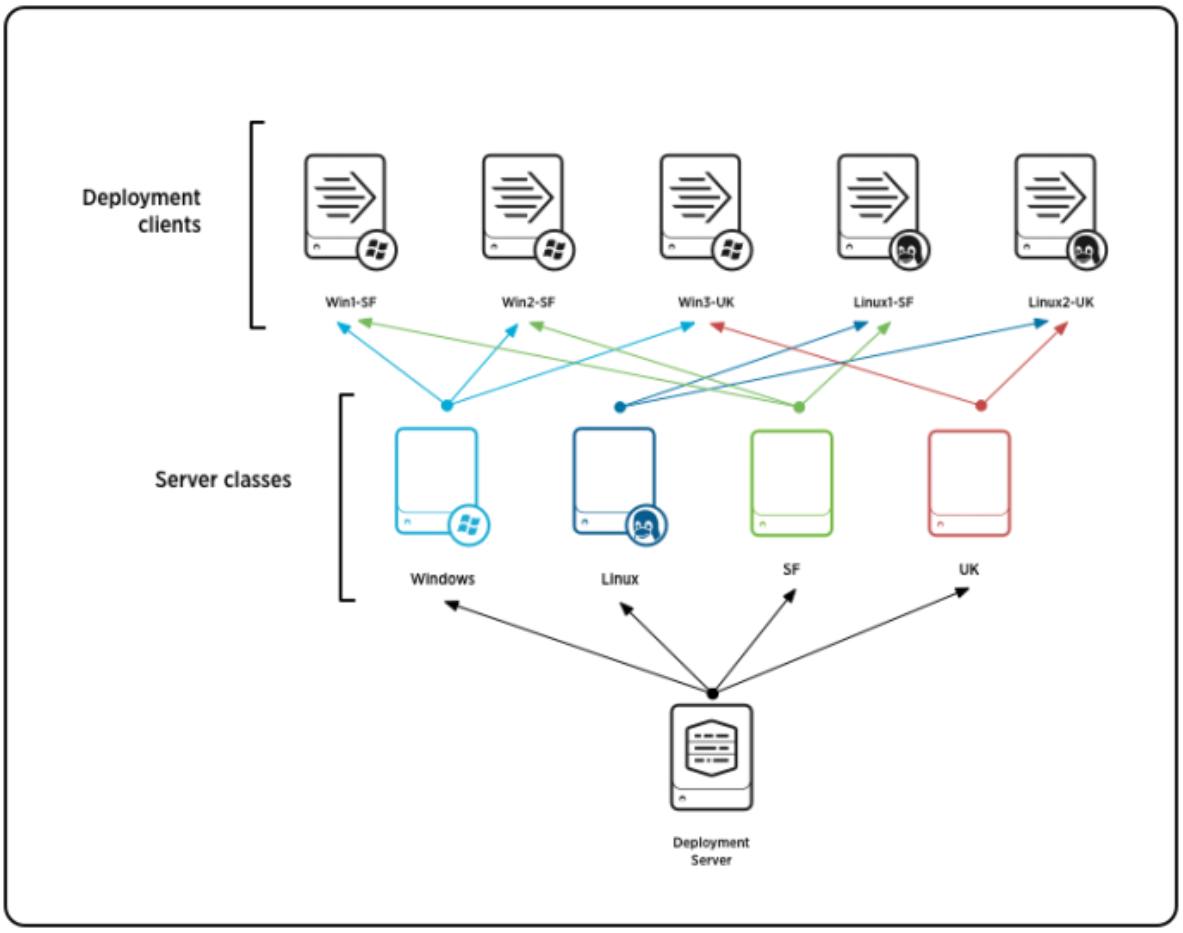
4.App files: $SPLUNK_HOME/etc/apps/

```
[root@ip-172-31-35-24 ~]# cd /opt/splunk/etc/apps/
[root@ip-172-31-35-24 apps]# ls
alert_logevent                  SplunkForwarder
alert_webhook                   splunk_gdi
appsbrowser                     splunk_httpinput
introspection_generator_addon   splunk_instrumentation
journald_input                  splunk_internal_metrics
launcher                        SplunkLightForwarder
learned                         splunk_metrics_workspace
legacy                          splunk_monitoring_console
sample_app                      splunk_rapid_diag
search                          splunk_secure_gateway
splunk_archiver                 user-prefs
[root@ip-172-31-35-24 apps]# +
```

Deployment Server

The deployment server is the tool for distributing configurations, apps, and content updates to groups of Splunk Enterprise instances.You can use it to distribute updates to most types of Splunk Enterprise components: forwarders, non-clustered indexers, and search heads.

A deployment client is a Splunk instance remotely configured by a deployment server. Deployment clients can be universal forwarders, heavy forwarders, indexers, or search heads. Each deployment client belongs to one or more server classes.



Set up :

Create six instances and name them as Deployment server,Windows forwarder,Linux Universal Forwarder,Heavy Forwarder,Receiver and Receiver2.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zon
Linux Forwar...	i-0d2213ac7499b1c6d	Running	t2.micro	–	No alarms	us-east-2b
Heavy Forwa...	i-07d2e6093d78d942c	Running	t2.micro	2/2 checks ...	No alarms	us-east-2b
WIndows	i-0bef31af8457a9470	Running	t2.micro	2/2 checks ...	No alarms	us-east-2b
Deployment ...	i-0d52e1c1f3559aa5b	Running	t2.micro	2/2 checks ...	No alarms	us-east-2b
Receiver	i-0387a83957345ddda	Running	t2.micro	2/2 checks ...	No alarms	us-east-2b
Receiver-2	i-0ce0a061c9e0484b5	Running	t2.micro	2/2 checks ...	No alarms	us-east-2b

Method:

Receiver & Receiver2: Go to “Forwarding and Receiving” enable the receiving port to 9997.

Listen on this port	Status	Actions
9997	Enabled | Disable	Delete

Deployment Client Configuration:

Cd /opt/splunk/bin

splunk set deploy-poll <DeploymentIP_address/hostname>:<management_port>

splunk reload deploy-server

Windows Forwarder:

Asking Deployment server Ip address and management port in Manually installation wizard

```
C:\Users\Administrator>cd \Program Files\SplunkUniversalForwarder\bin

C:\Program Files\SplunkUniversalForwarder\bin>splunk restart
```

Heavy Forwarder:

```
[root@ip-172-31-18-125 ec2-user]# cd /opt/splunk/bin/
[root@ip-172-31-18-125 bin]# ./splunk set deploy-poll 18.223.184.52:8089
Splunk username: admin
Password:
Configuration updated.
[root@ip-172-31-18-125 bin]# ./splunk reload deploy-server
Reloading serverclass(es).
[root@ip-172-31-18-125 bin]# cd /opt/splunk/etc/system/local/
[root@ip-172-31-18-125 local]# ls
deploymentclient.conf  migration.conf  outputs.conf  README  server.conf
[root@ip-172-31-18-125 local]# vi deploymentclient.conf
```

Linux Universal Forwarder:

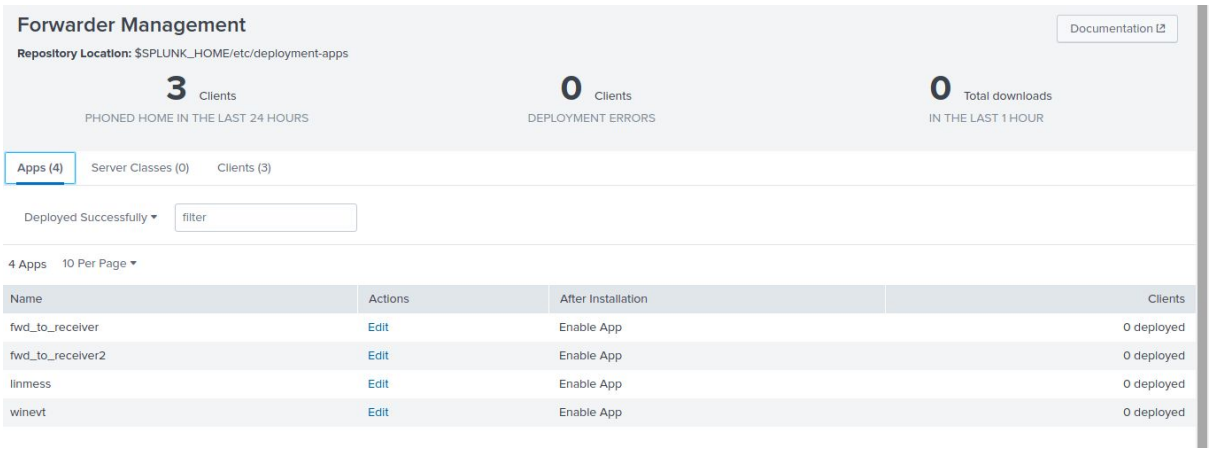
```
[root@ip-172-31-29-139 local]# cd /opt/splunkforwarder/bin/
[root@ip-172-31-29-139 bin]# ./splunk set deploy-poll 18.223.184.52:8089
Splunk username: admin
Password:
Configuration updated.
```

Finally Restart the Deployment clients

Create Apps:

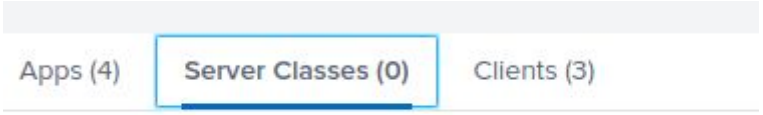
Create apps in Deployment Server

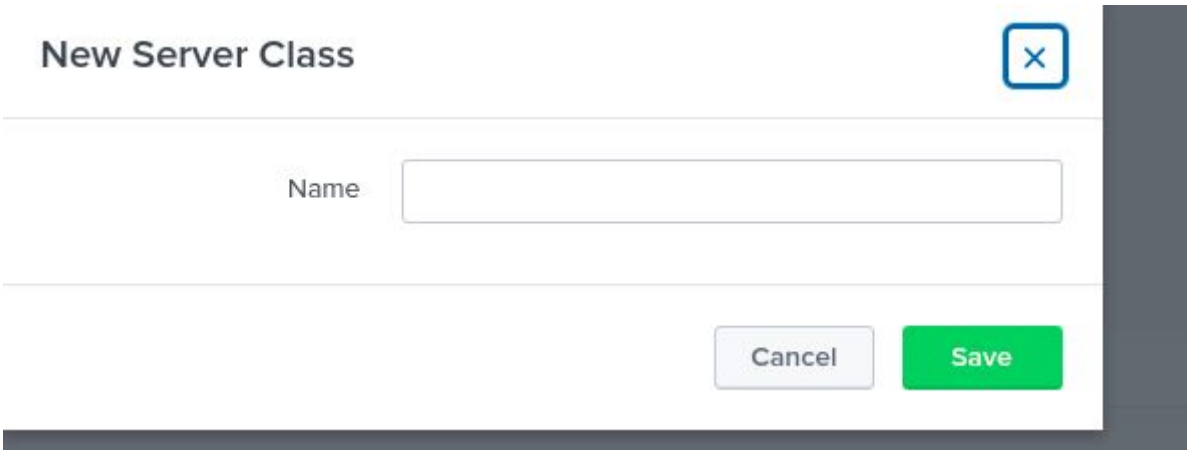
```
[root@ip-172-31-31-114 deployment-apps]# mkdir fwd_to_receiver  fwd_to_receiver2
  linmess  winevt
```

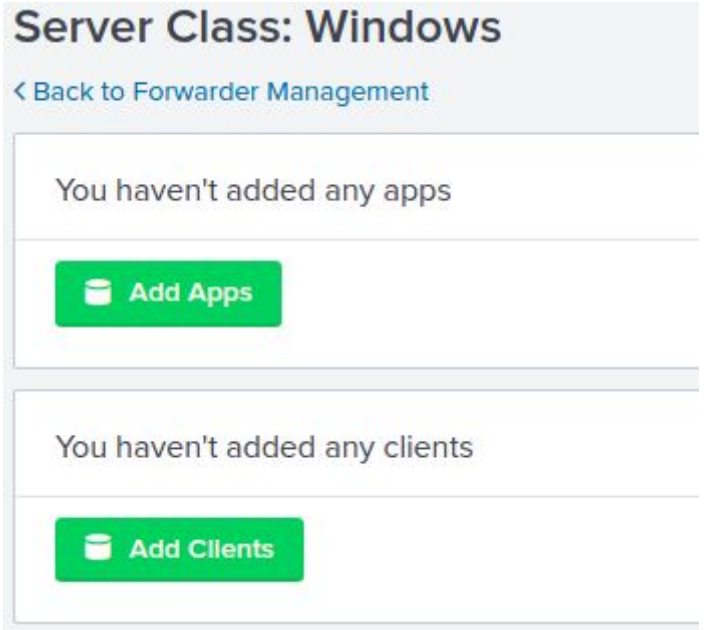


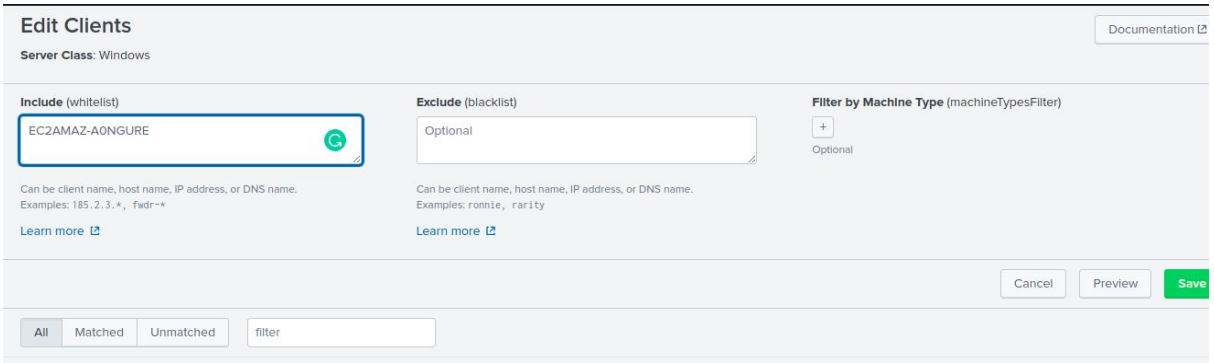
Server Class:

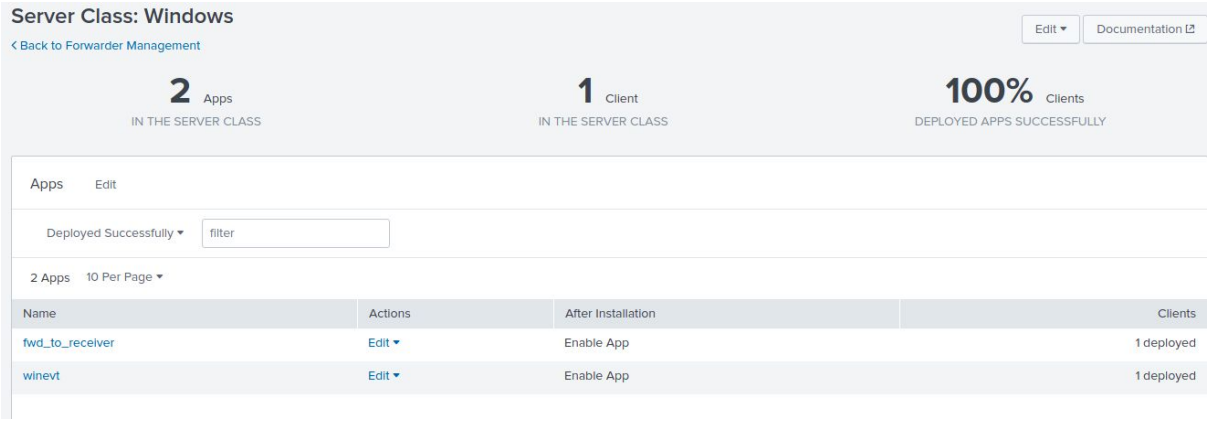
A server class is a group of deployment clients that share one or more defined characteristics. For example, you can group all Windows clients into one server class and all Linux clients into another server class. You use server classes to map a group of deployment clients to one or more deployment apps. By creating a server class, you are telling the deployment server that a specific set of clients should receive configuration updates in the form of a specific set of apps.


Apps (4)
Server Classes (0)
Clients (3)


New Server Class
Name
Cancel
Save


Server Class: Windows
Back to Forwarder Management
You haven't added any apps
Add Apps
You haven't added any clients
Add Clients


Edit Clients
Server Class: Windows
Documentation
Include (whitelist)
EC2AMAZ-A0NGURE
Can be client name, host name, IP address, or DNS name.
Examples: 185.2.3.*, fwdr-*
Learn more
Exclude (blacklist)
Optional
Can be client name, host name, IP address, or DNS name.
Examples: ronnie, rarity
Learn more
Filter by Machine Type (machineTypesFilter)
Optional
Cancel
Preview
Save
All
Matched
Unmatched
filter



Create Configuration files in Deployment server apps:

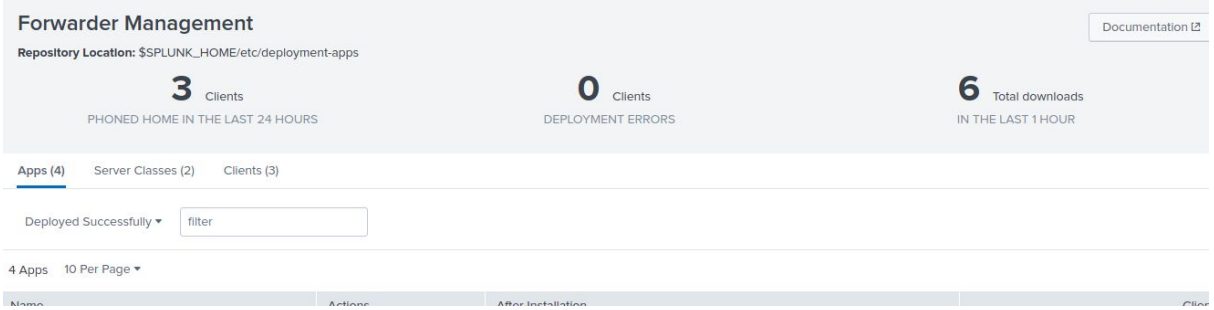
```
$SPLUNK_HOME/etc/deployment-apps/fwd_to_receiver
[tcpout]
defaultGroup=receiver
[tcpout:receiver]
server=Receiver  :9997

$SPLUNK_HOME/etc/deployment-apps/fwd_to_receiver2
[tcpout]
defaultGroup=receiver2
[tcpout:receiver2]
server=Receiver 2 :9997


$SPLUNK_HOME/etc/deployment-apps/winevt
[WinEventLog:Application]
disabled=0
[WinEventLog:Security]
disabled=0
[WinEventLog:System]
disabled=0

$SPLUNK_HOME/etc/deployment-apps/linmess
[monitor:///var/log/]
disabled=false
sourcetype=syslog
```

```
[root@ip-172-31-31-114 ec2-user]# cd /opt/splunk/etc/deployment-apps/
[root@ip-172-31-31-114 deployment-apps]# cd fwd_to_receiver
[root@ip-172-31-31-114 fwd_to_receiver]# mkdir default
[root@ip-172-31-31-114 fwd_to_receiver]# cd default/
[root@ip-172-31-31-114 default]# vi outputs.conf
```

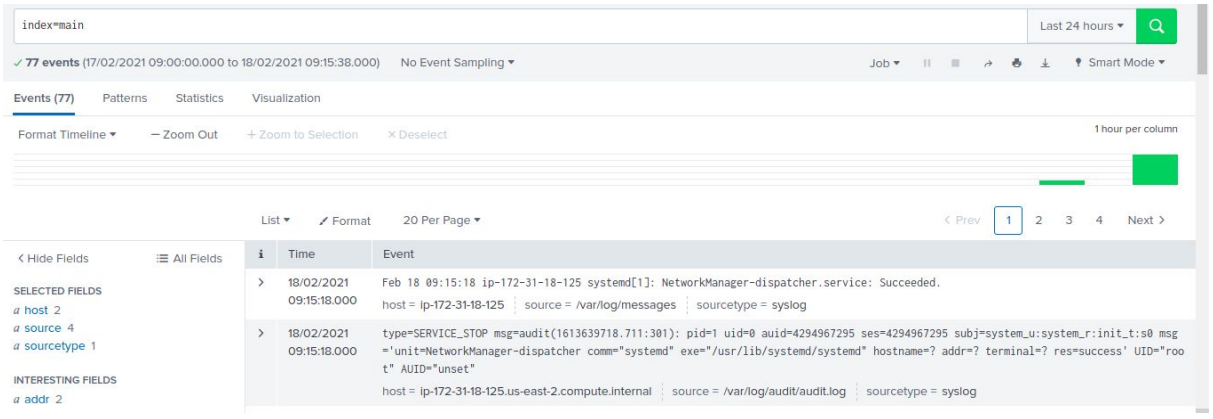
```
[root@ip-172-31-31-114 deployment-apps]# cd linmess/
[root@ip-172-31-31-114 linmess]# mkdir default
[root@ip-172-31-31-114 linmess]# cd default/
[root@ip-172-31-31-114 default]# vi inputs.conf
```

```
[root@ip-172-31-31-114 deployment-apps]# cd winevt/
[root@ip-172-31-31-114 winevt]# mkdir default
[root@ip-172-31-31-114 winevt]# cd default/
[root@ip-172-31-31-114 default]# vi inputs.conf
```

After these settings We are able to see in Forward management

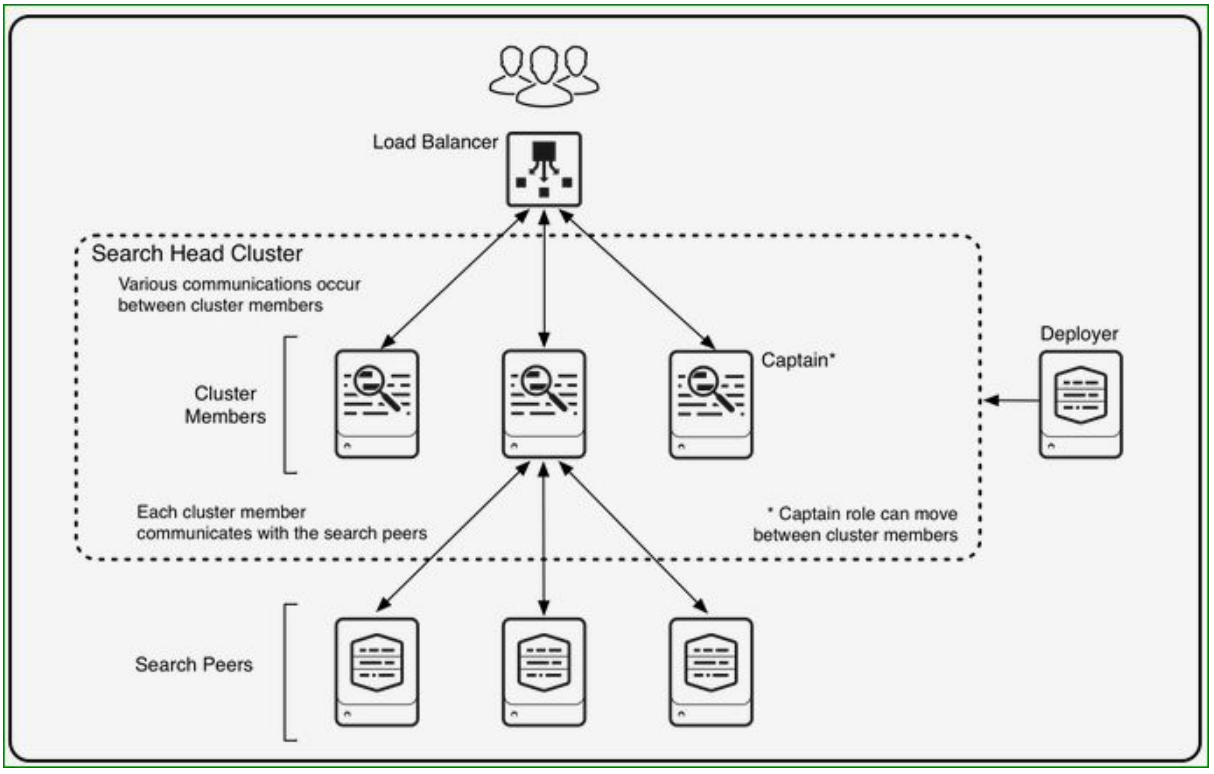


Now go to one of the Receiver GUI and Search index main.you get information similar to below image.



Search Head Clustering Setup

A search head cluster is a group of Splunk Enterprise search heads that serves as a central resource for searching.



- I Have Launched 4 EC Instances and Installed Splunk. All Instances are RedHat 8 Platform
- One Instance acting as a Deployer and another three instances as Search Heads

Name	Instance ID	Instance state	Instance type	Status check
Deployer	i-0145b1a786a7e4e47	Running	t2.micro	2/2 checks ...
Search Head-1	i-013ca0752e32bf09d	Running	t2.micro	2/2 checks ...
Search Head-2	i-06a7d590074da17f5	Running	t2.micro	Initializing
Search Head-3	i-0bc311461c044778a	Running	t2.micro	Initializing

#) Deployer Configuration:

This is a Splunk Enterprise instance that distributes apps and other configurations to the cluster members. It stands outside the cluster and cannot run on the same instance as a cluster member. It can, however, under some circumstances, reside on the same instance as some other Splunk Enterprise components, such as a deployment server or an manager node

```
dhana@dhana-Ubuntu:~$ ssh ec2-user@13.59.141.166 -i Downloads/ubuntu.pem
Last login: Sun Feb 14 10:07:43 2021 from 157.51.79.200
[ec2-user@ip-172-31-4-85 ~]$ sudo su
[root@ip-172-31-4-85 ec2-user]# cd /opt/splunk/etc/system/local/
[root@ip-172-31-4-85 local]# ls
migration.conf  README  server.conf
[root@ip-172-31-4-85 local]# vi server.conf
```

Using Vi editor to open the **server.conf file** and put the following Configuration. File location is **$SPLUNK_HOME/etc/system/local/server.conf**

```
[shclustering]
pass4SymmKey = test1234
shcluster_label = shcluster1
```

Restart the Splunk

```
[root@ip-172-31-4-85 local]# cd /opt/splunk/bin/
[root@ip-172-31-4-85 bin]# ./splunk restart
```

#) In all the SH cluster members (don't run it for deployer)

Search Head 1:

Enter the following command in Search Head 1:

```
./splunk init shcluster-config -auth admin:development -mgmt_uri https://18.191.208.126:8089 -replication_port 9000 -replication_factor 3 -conf_deploy_fetch_url http://13.59.141.166:8089 -secret test1234 -shcluster_label shcluster1
```

Finally Restart the splunk:

```
[root@ip-172-31-14-39 bin]# ./splunk init shcluster-config -auth admin:development
-mgmt_uri https://18.191.208.126:8089 -replication_port 9000 -replication_factor
3  -conf_deploy_fetch_url http://13.59.141.166:8089 -secret $7$vIhUJsDDRLw6QW2+jfs
l8Cu+fWg8BrsThjfbUwgtThMbGWagSYlKAg==  -shcluster_label shcluster1
```

- **Likewise Setup other 2 Search Heads and Restart the Splunk**

```
[root@ip-172-31-15-139 bin]# ./splunk init shcluster-config -auth admin:developm
ent -mgmt_uri https://3.15.25.64:8089 -replication_port 9100 -replication_factor
 3  -conf_deploy_fetch_url http://13.59.141.166:8089 -secret $7$vIhUJsDDRLw6QW2+
jfsl8Cu+fWg8BrsThjfbUwgtThMbGWagSYlKAg==  -shcluster_label shcluster1
```

```
[root@ip-172-31-13-55 bin]# ./splunk init shcluster-config -auth admin:developme
nt -mgmt_uri https://18.224.65.217:8089 -replication_port 9200 -replication_fact
or 3  -conf_deploy_fetch_url http://13.59.141.166:8089 -secret $7$vIhUJsDDRLw6QW
2+jfsl8Cu+fWg8BrsThjfbUwgtThMbGWagSYlKAg== -shcluster_label shcluster1
```

#) setting up the captain (any cluster member can be chosen to this command, that particular instance will be the first captain

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

```
[root@ip-172-31-14-39 bin]# ./splunk bootstrap shcluster-captain -servers_list "
https://18.191.208.126:8089,https://3.15.25.64:8089,https://18.224.65.217:8089"
-auth admin:development
Successfully bootstrapped this node as the captain with the given servers.
[root@ip-172-31-14-39 bin]#
```

see the cluster status
./splunk show shcluster-status
-auth <username>:<password>

```
[root@ip-172-31-14-39 bin]# ./splunk show shcluster-status -auth admin:development

 Captain:
                                dynamic_captain : 1
                                elected_captain : Sun Feb 14 11:42:49 2021
                                             id : 379B6787-D13B-4B62-996C-2059150CA59C
                            initialized_flag : 1
                                          label : ip-172-31-14-39.us-east-2.compute.internal
                                       mgmt_uri : https://18.191.208.126:8089
                         min_peers_joined_flag : 1
                          rolling_restart_flag : 0
                            service_ready_flag : 1

 Members:
        ip-172-31-14-39.us-east-2.compute.internal
                                          label : ip-172-31-14-39.us-east-2.compute.internal
                                       mgmt_uri : https://18.191.208.126:8089
                                  mgmt_uri_alias : https://18.191.208.126:8089
                                         status : Up
        ip-172-31-13-55.us-east-2.compute.internal
                                          label : ip-172-31-13-55.us-east-2.compute.internal
                         last_conf_replication : Pending
                                       mgmt_uri : https://18.224.65.217:8089
                                  mgmt_uri_alias : https://18.224.65.217:8089
                                         status : Up
        ip-172-31-15-139.us-east-2.compute.internal
                                          label : ip-172-31-15-139.us-east-2.compute.internal
                         last_conf_replication : Pending
                                       mgmt_uri : https://3.15.25.64:8089
                                  mgmt_uri_alias : https://3.15.25.64:8089
                                         status : Up
[root@ip-172-31-14-39 bin]#
```

see the cluster configurations
./splunk list shcluster-config
-auth admin:development

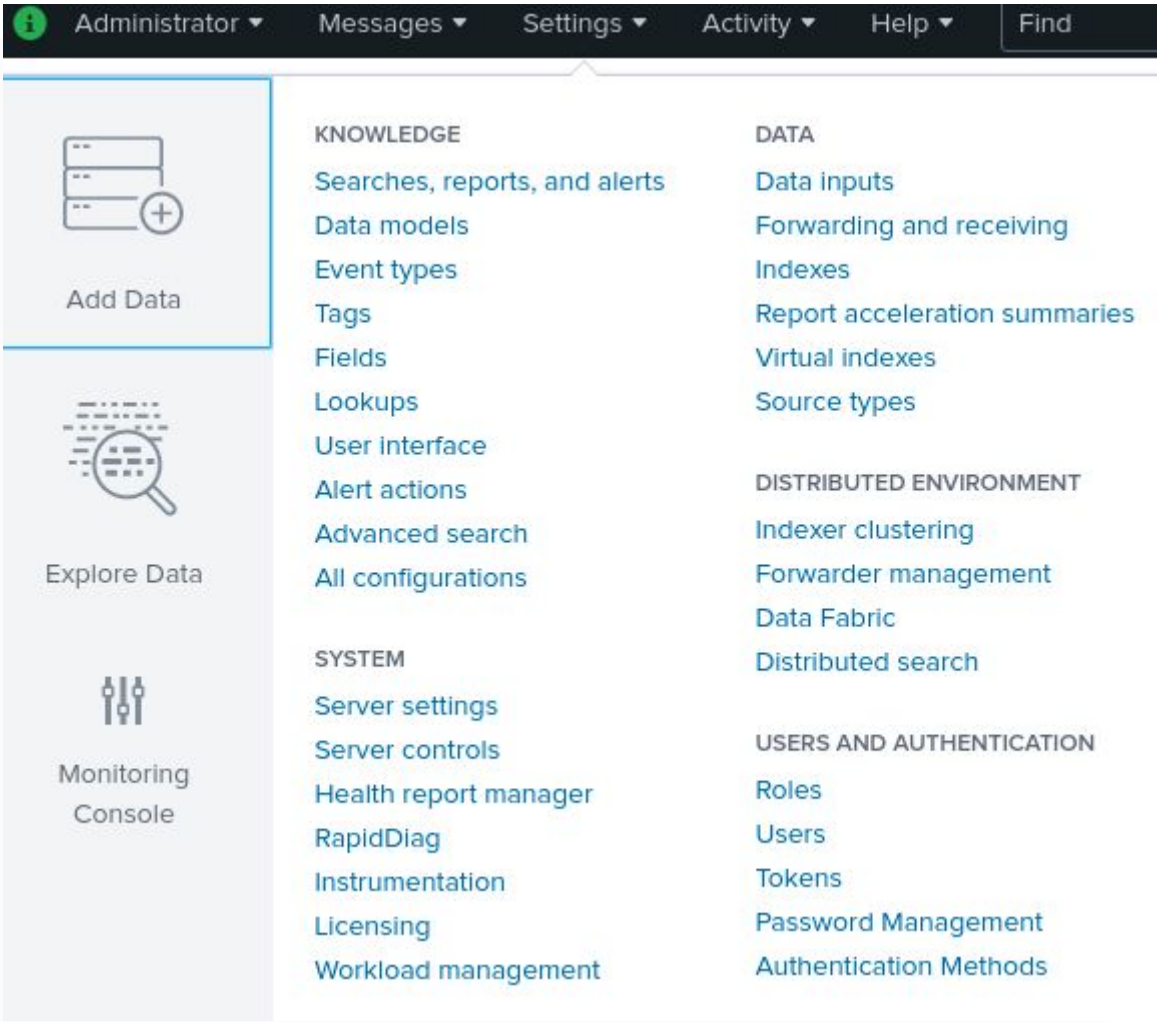
```
[root@ip-172-31-15-139 bin]# ./splunk list shcluster-config -auth admin:development
        config
                adhoc_searchhead:0
                async_replicate_on_proxy:1
                captain_is_adhoc_searchhead:0
                conf_deploy_fetch_url:http://13.59.141.166:8089
                cxn_timeout:60
                decommission_search_jobs_wait_secs:180
                disabled:0
                dispatching_mode:push
                dynamic_captain:1
                heartbeat_period:5
                heartbeat_timeout:60
                id:379B6787-D13B-4B62-996C-2059150CA59C
                manual_detention:off
                max_peer_rep_load:5
                mode:dynamic_captain
                percent_peers_to_restart:10
                ping_flag:1
                preferred_captain:1
                quiet_period:60
                rcv_timeout:60
                rep_cxn_timeout:60
                rep_max_rcv_timeout:600
                rep_max_send_timeout:600
                rep_rcv_timeout:60
                rep_send_timeout:60
                replication_factor:3
                replication_port:9100
                replication_use_ssl:0
                restart_timeout:600
                rolling_restart:restart
                secret:********
                send_timeout:60
```

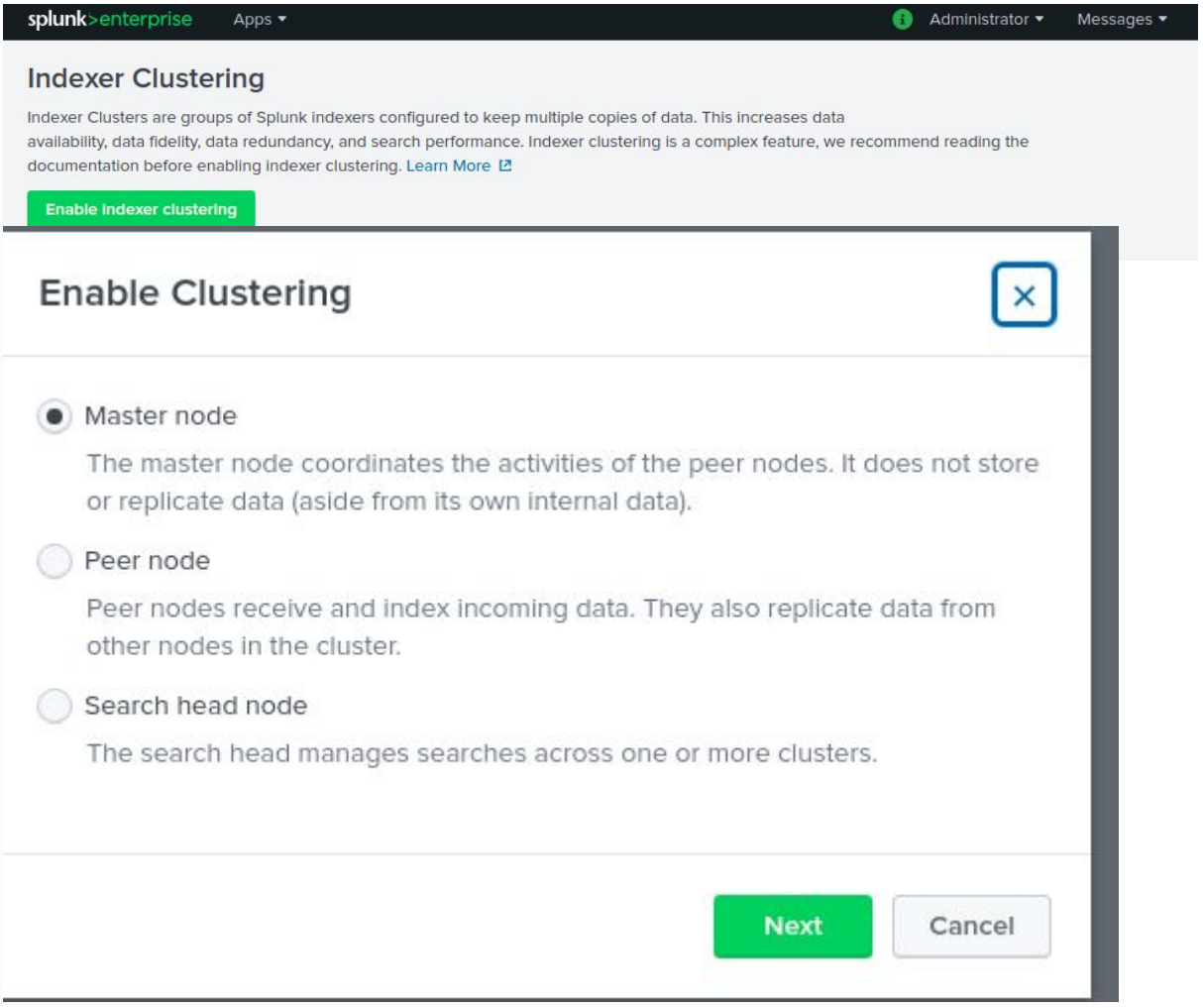
Indexer clustering setup

- I have launched Cluster-Master and 3 Indexers

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
Cluster-Master	i-09676e772c99e668a	Running	t2.micro	2/2 checks ...	No alarms	us-east-2a
Indexer1	i-0ae98a5d5284da1ff	Running	t2.micro	2/2 checks ...	No alarms	us-east-2a
Indexer2	i-0fc1de971e5011e5b	Running	t2.micro	Initializing	No alarms	us-east-2a
Indexer3	i-088c1e685fcb39222	Running	t2.micro	–	No alarms	us-east-2a

In Cluster Master:


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



$SPLUNK_HOME/etc/system/local/server.conf:

```
[clustering]
mode = master
pass4SymmKey = $7$38l0WC03OSURFYu4yR5sxl61QxKfu/+EB4pFSHiQjLbj6qFlOKo+6mnMxA=
~
```

In each Indexer $SPLUNK_HOME/ etc/system/ local/server.conf:

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

Peer node configuration

Master URI: https://3.137.199.66:8089

E.g. https://10.152.31.202:8089

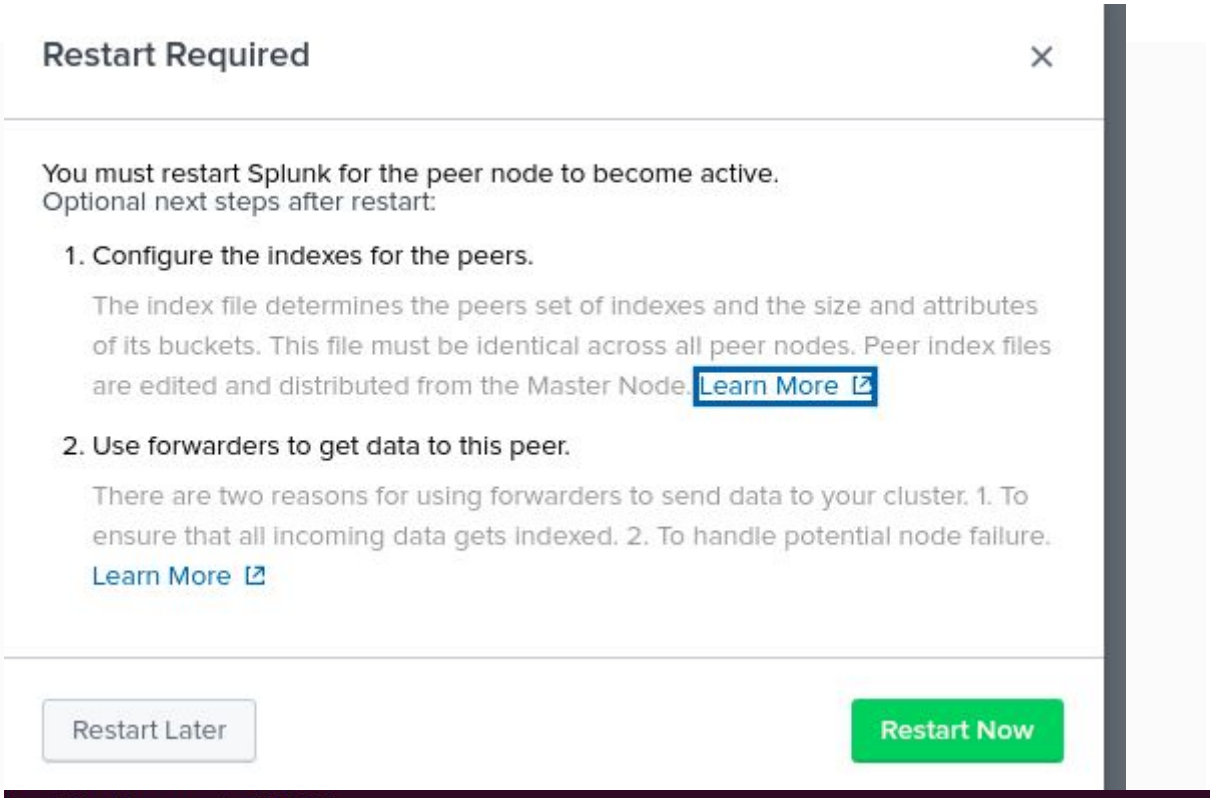
Peer replication port: 8080

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

Security key: ••••••••••••

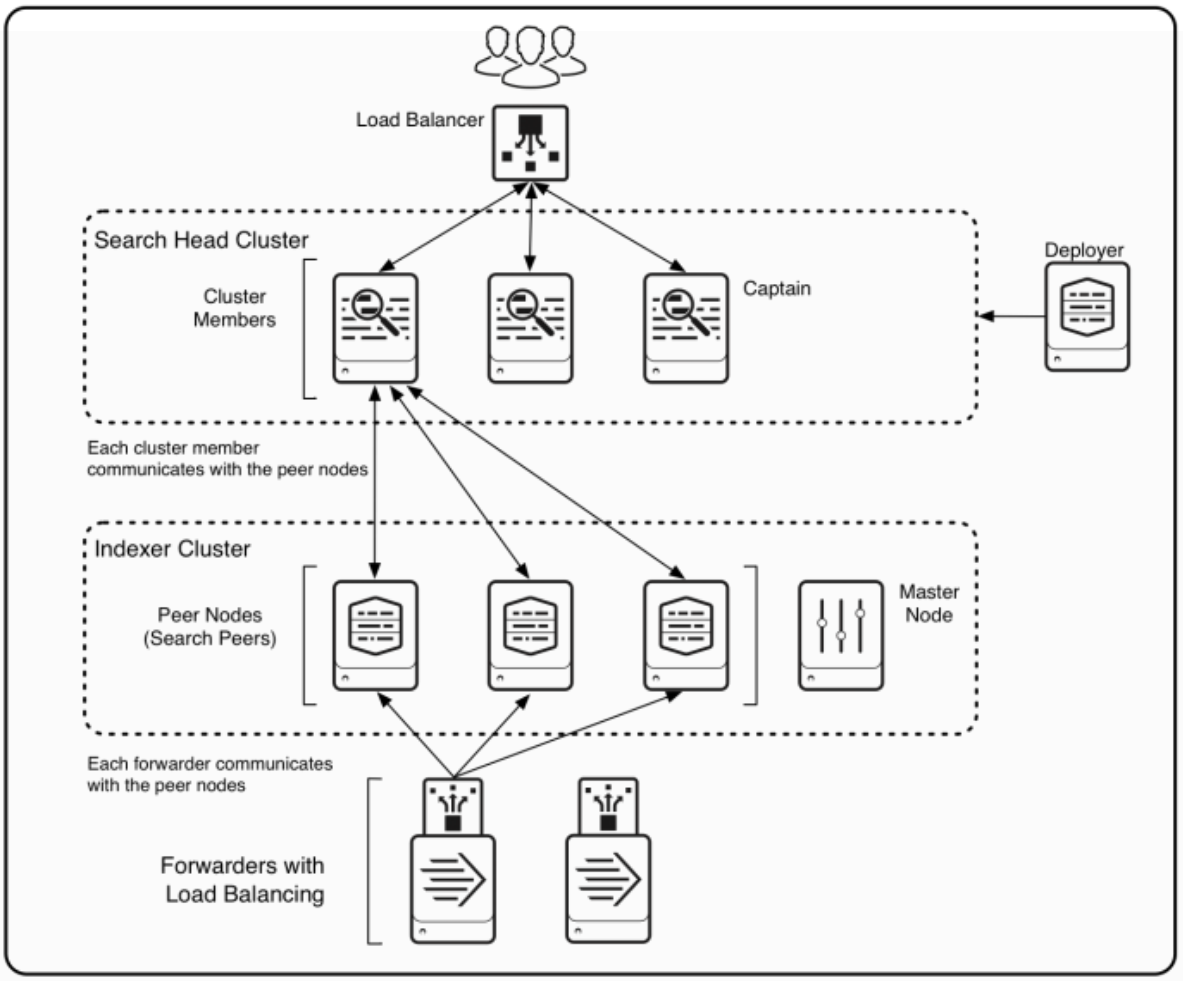
This key authenticates communication between the master and the peers and search heads.

Back Enable peer node




```
[replication_port://8080]

[clustering]
master_uri = https://3.137.199.66:8089
mode = slave
pass4SymmKey = $7$YIf1i9H4pxA6QrgbnmDg4oFmSG+gINkkGRWZwVy5T4KrzOu3RzwzonPdYg==
~
```

Configure each member of the SH cluster as search head in Indexer cluster:



Search Head-2	i-06a7d590074da17f5	Running	t2.micro	2/2 checks ...	No alarms	us-east-2a
Indexer3	i-088c1e685fcb39222	Running	t2.micro	2/2 checks ...	No alarms	us-east-2a
Search Head-3	i-0bc311461c044778a	Running	t2.micro	2/2 checks ...	No alarms	us-east-2a
Cluster-Master	i-09676e772c99e668a	Running	t2.micro	2/2 checks ...	No alarms	us-east-2a
Deployer	i-0145b1a786a7e4e47	Running	t2.micro	2/2 checks ...	No alarms	us-east-2a
Indexer1	i-0ae98a5d5284da1ff	Running	t2.micro	2/2 checks ...	No alarms	us-east-2a
Indexer2	i-0fc1de971e5011e5b	Running	t2.micro	2/2 checks ...	No alarms	us-east-2a
Search Head-1	i-013ca0752e32bf09d	Running	t2.micro	2/2 checks ...	No alarms	us-east-2a

```
./splunk edit cluster-config
   -mode search_head
  -master_uri <Indexer Cluster Master URI>
   -secret <Indexer pass4SymmKey>
```

Search Head-1:

```
[root@ip-172-31-14-39 bin]# ./splunk edit cluster-config -mode searchhead -master_uri http
s://3.137.199.66:8089 -secret development
The cluster-config property has been edited.
You need to restart the Splunk Server (splunkd) for your changes to take effect.
[root@ip-172-31-14-39 bin]# ./splunk restart
```

Search Head-2:

```
[root@ip-172-31-15-139 bin]# ./splunk edit cluster-config -mode searchhead -master_uri htt
ps://3.137.199.66:8089 -secret development
Your session is invalid.  Please login.
Splunk username: admin
Password:
The cluster-config property has been edited.
You need to restart the Splunk Server (splunkd) for your changes to take effect.
[root@ip-172-31-15-139 bin]# ./splunk restart
```

Search Head-3:

```
[root@ip-172-31-13-55 bin]# ./splunk edit cluster-config -mode searchhead -master_uri http
s://3.137.199.66:8089 -secret development
Your session is invalid.  Please login.
Splunk username: admin
Password:
The cluster-config property has been edited.
You need to restart the Splunk Server (splunkd) for your changes to take effect.
[root@ip-172-31-13-55 bin]# ./splunk restart
```