Nov 2024

Splunk4Admins - Clustering

Lab Guide

Overview

This lab guide contains the hands-on exercises for the Splunk4Admins - Clustering workshop. Before proceeding with these exercises, please ensure that you have a copy of the workshop slide deck, which will help to put into context the tasks you are carrying out.

Download the workshop slide deck: https://splk.it/S4A-CLU-Attendee

Prerequisites

In order to complete these exercises, you will need your own Splunk instance. Splunk's hands-on workshops are delivered via the Splunk Show portal and you will need a splunk.com account in order to access this.

If you don't already have a Splunk.com account, please create one here before proceeding with the rest of the workshop.

⚠️ Troubleshooting Connectivity

If you experience connectivity issues with accessing either your workshop environment or the event page, please try the following troubleshooting steps. If you still experience issues please reach out to the team running your workshop.

- **Use Google Chrome** (if you're not already)
- If the event page (i.e. *https://show.splunk.com/event/<eventID>*) didn't load when you clicked on the link, try **refreshing the page**
- **Disconnect from VPN** (if you're using one)
- **Clear your browser cache and restart your browser** (if using Google Chrome, go to: Settings > Privacy and security > Clear browsing data)
- **Try using private browsing mode** (e.g. Incognito in Google Chrome) to rule out any cache issues
- **Try using another computer** such as your personal computer - all you need is a web browser! Cloud platforms like AWS can often be blocked on corporate laptops.

Table of Contents

Exercise 1 – Build an indexer cluster

Description

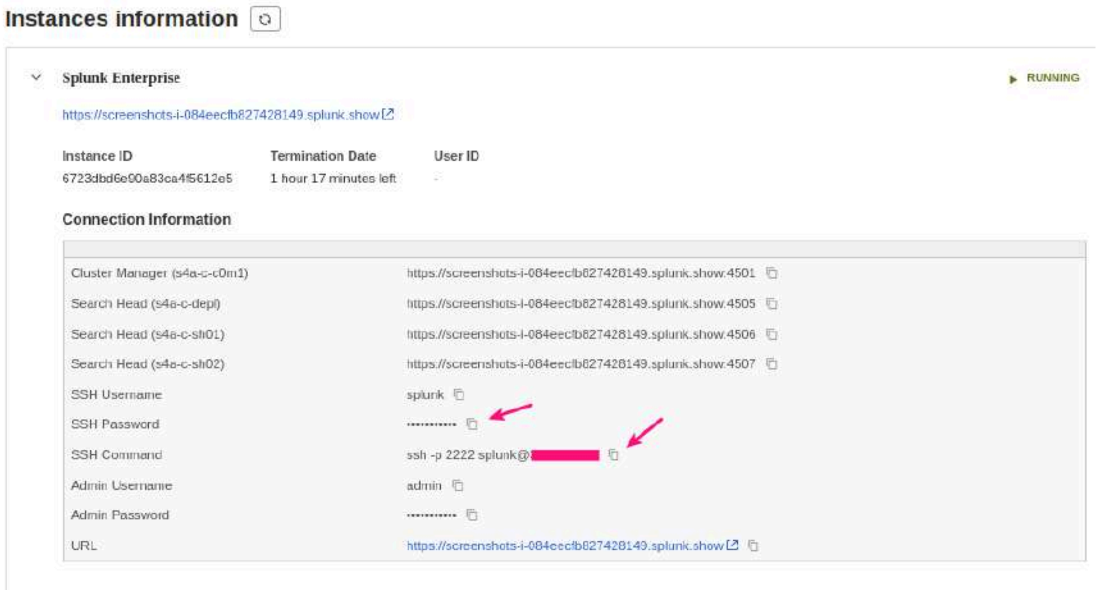
Build an indexer cluster by building a cluster manager and connecting the indexers to the CM.

Summary

- Access the node to be CM
- Create app (using server.conf file) on the CM in $SPLUNK_HOME/etc/apps
- Restart Splunkd
- Observe the "Indexer Clustering" menu item as available
- Access the first indexer node, Create an app to integrate into the cluster
- Restart Splunkd
- Observe (on the CM in the "Indexer Clustering" menu item, the first indexer node registered with the CM
- Repeat the previous steps on the second indexer node (5 through 8, modified to reflect connecting to the second indexer node)
- Observe (on the CM in the "Indexer Clustering" menu item, the second indexer node registered with the CM

Steps

1. Access the lab node
    a. Username "`splunk`" (in the copy/paste below)
    b. Password "`5p1unk.conf`"
    c. Hit the "copy" icon in the Instances Information section for the 'ssh command



Instances information

Splunk Enterprise

RUNNING

https://screenshots-i-084eecfb827428149.splunk.show

Instance ID	Termination Date	User ID
6723dbd6e90a83ca4f5612e5	1 hour 17 minutes left	-

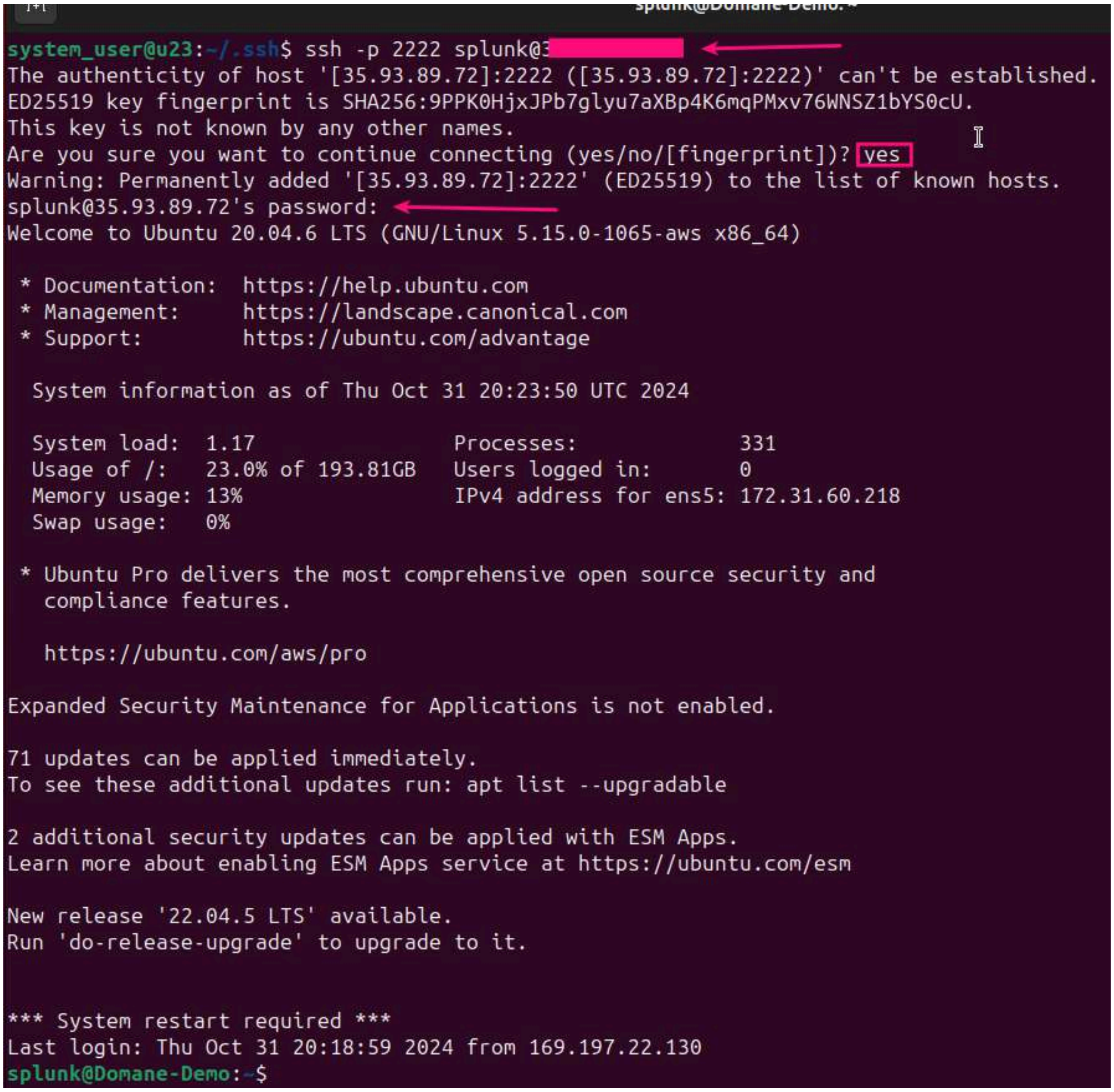
Connection Information

Cluster Manager (s4a-c-c0m1)	https://screenshots-i-084eecfb827428149.splunk.show:4501
Search Head (s4a-c-depl)	https://screenshots-i-084eecfb827428149.splunk.show:4505
Search Head (s4a-c-sh01)	https://screenshots-i-084eecfb827428149.splunk.show:4506
Search Head (s4a-c-sh02)	https://screenshots-i-084eecfb827428149.splunk.show:4507
SSH Username	splunk
SSH Password	•••••••••••
SSH Command	ssh -p 2222 splunk@[redacted]
Admin Username	admin
Admin Password	•••••••••••
URL	https://screenshots-i-084eecfb827428149.splunk.show

d. Paste into a terminal or a Putty window, hit return, and then type “yes” to “continue “connecting”

e. Then, hit the “copy” icon next ‘SSH Password’ and paste it into the terminal to log in to the node.

```
ssh -p 2222 splunk@<<IP_address_of_node_from_your_SHOW_Lab_information>>
```



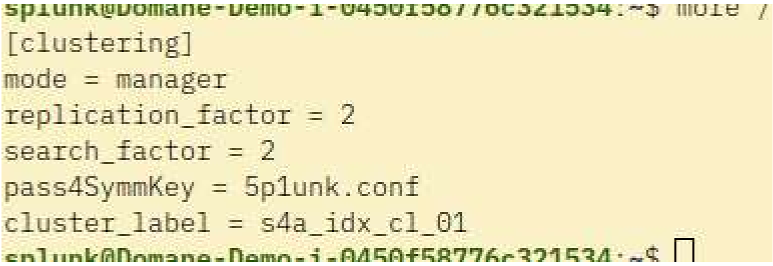
```
system_user@u23:~/.ssh$ ssh -p 2222 splunk@3[redacted]
The authenticity of host '[35.93.89.72]:2222 ([35.93.89.72]:2222)' can't be established.
ED25519 key fingerprint is SHA256:9PPK0HjxJPb7glyu7aXBp4K6mqPMxv76WNSZ1bYS0cU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[35.93.89.72]:2222' (ED25519) to the list of known hosts.
splunk@35.93.89.72's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1065-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Oct 31 20:23:50 UTC 2024

  System load:  1.17               Processes:             331
  Usage of /:   23.0% of 193.81GB  Users logged in:       0
  Memory usage: 13%                IPv4 address for ens5: 172.31.60.218
  Swap usage:   0%

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

   https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

71 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

2 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

New release '22.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


*** System restart required ***
Last login: Thu Oct 31 20:18:59 2024 from 169.197.22.130
splunk@Domane-Demo:~$
```

2. Create the app to make the node the CM

```
cp -rp /opt/s4a-cluster/s4a_clustering_idx_build_c0m1 /opt/s4a-c-c0m1/splunk/etc/apps/
```

3. Examine the file created

```
more /opt/s4a-c-c0m1/splunk/etc/apps/s4a_clustering_idx_build_c0m1/local/server.conf
```

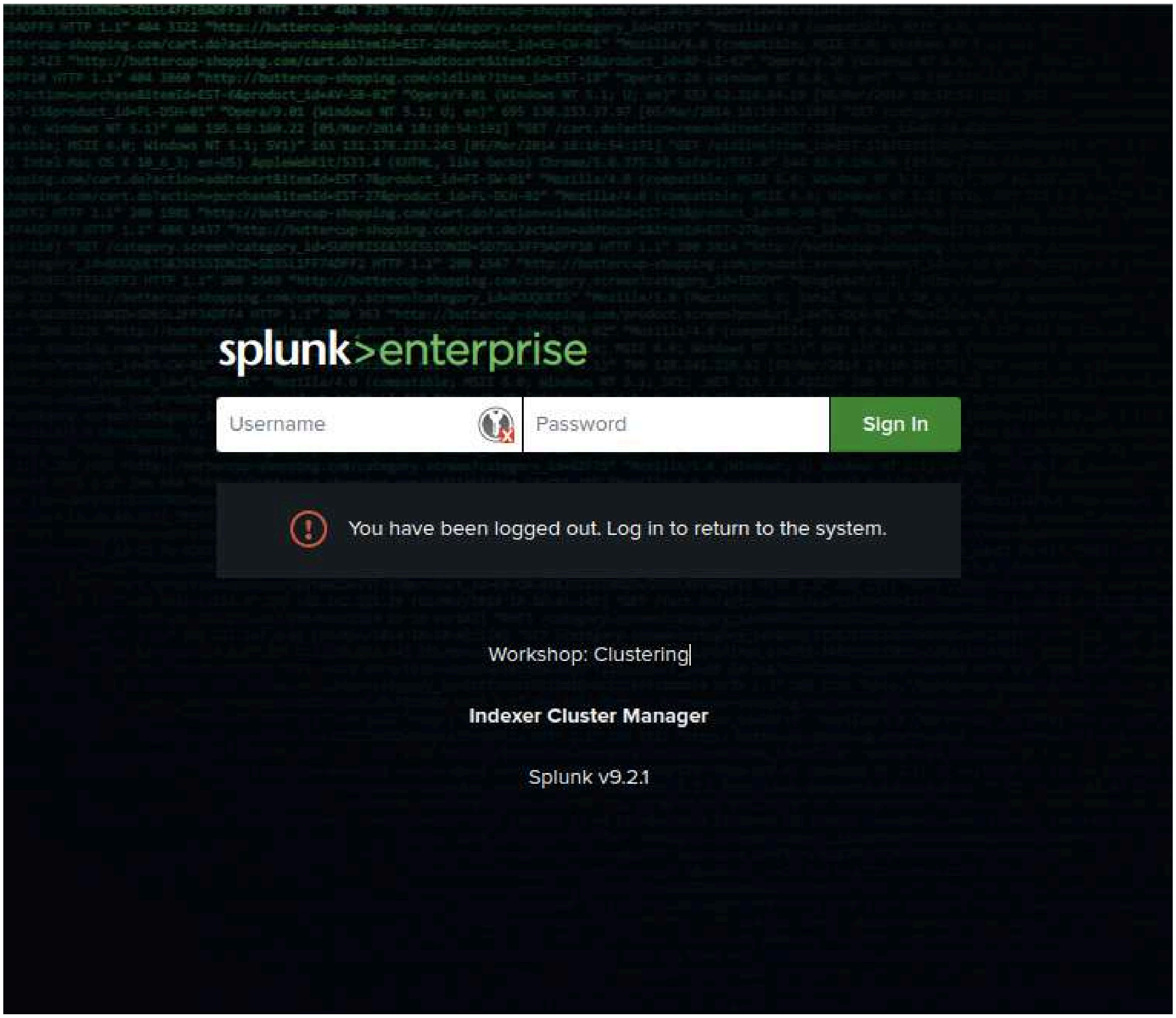


```
splunk@Domane-Demo-i-0450f58776c321534:~$ more /
[clustering]
mode = manager
replication_factor = 2
search_factor = 2
pass4SymmKey = 5p1unk.conf
cluster_label = s4a_idx_cl_01
splunk@Domane-Demo-i-0450f58776c321534:~$
```

4. Restart splunk

```
/opt/s4a-c-c0m1/splunk/bin/splunk restart
```

5. Login to the CM splunk instance (https://your_IP_address:4501) with username = “admin” and password = “5p1unk.conf”



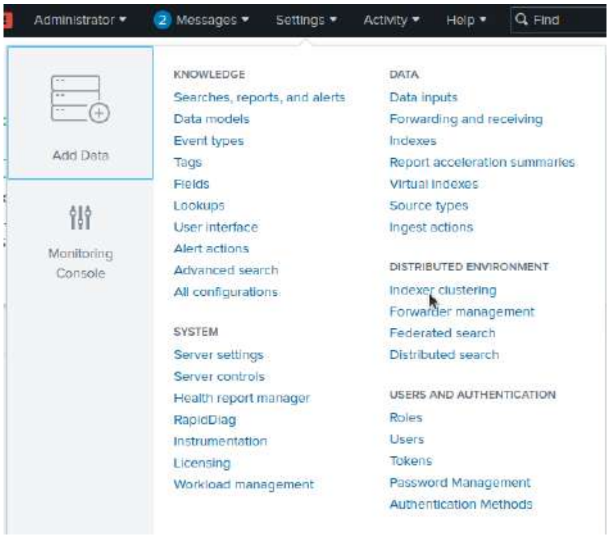
You have been logged out. Log in to return to the system.

Workshop: Clustering

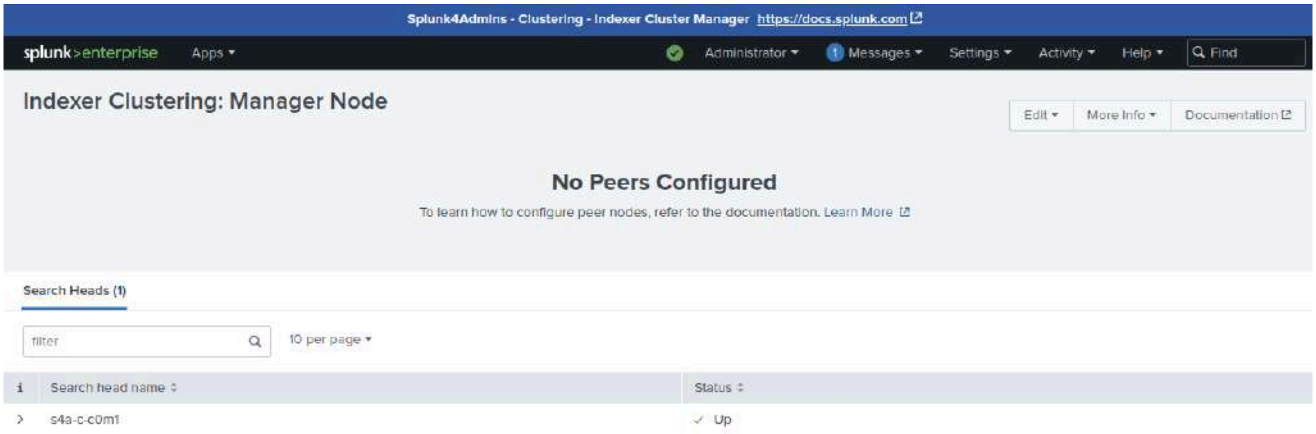
Indexer Cluster Manager

Splunk v9.2.1

6. Click on the black bar “Settings”, and select “Indexer Clustering”



7. Observe the resulting screen, including the fact that clustering is not configured (yet)



Indexer Clustering: Manager Node

No Peers Configured

To learn how to configure peer nodes, refer to the documentation. Learn More

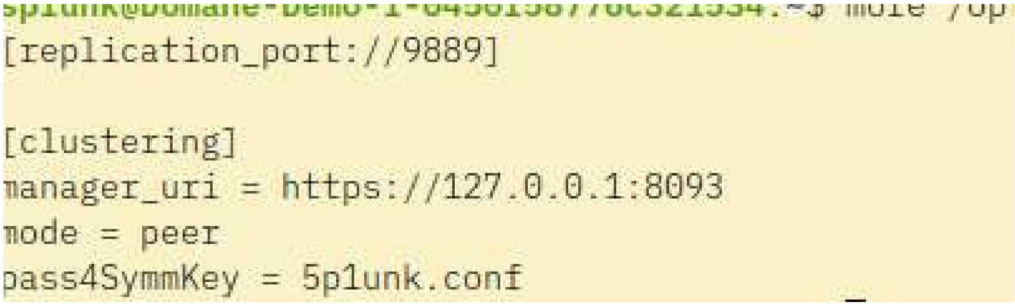
i	Search head name	Status
›	s4a-c-cOm1	✓ Up

8. Connect node 01 to the Cluster Manager via server.conf

```
cp -rp /opt/s4a-cluster/s4a_clustering_idx_build_member_idx01
/opt/s4a-c-idx01/splunk/etc/apps
```

   a. View the file

```
more
/opt/s4a-c-idx01/splunk/etc/apps/s4a_clustering_idx_build_member_idx01/local/server.conf
```



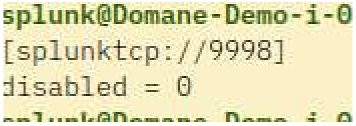
```
[replication_port://9889]

[clustering]
manager_uri = https://127.0.0.1:8093
mode = peer
pass4SymmKey = 5p1unk.conf
```

b. Enable the instance to receive data - different from a real environment as we are using a single node with differing ports to simulate a multi-node environment with single instances on each. Note the port difference from the normal node:8089

```
cp -rp /opt/s4a-cluster/s4a_clustering_idx01_receive /opt/s4a-c-idx01/splunk/etc/apps
```

c. View the file

```
more /opt/s4a-c-idx01/splunk/etc/apps/s4a_clustering_idx01_receive/local/inputs.conf
```

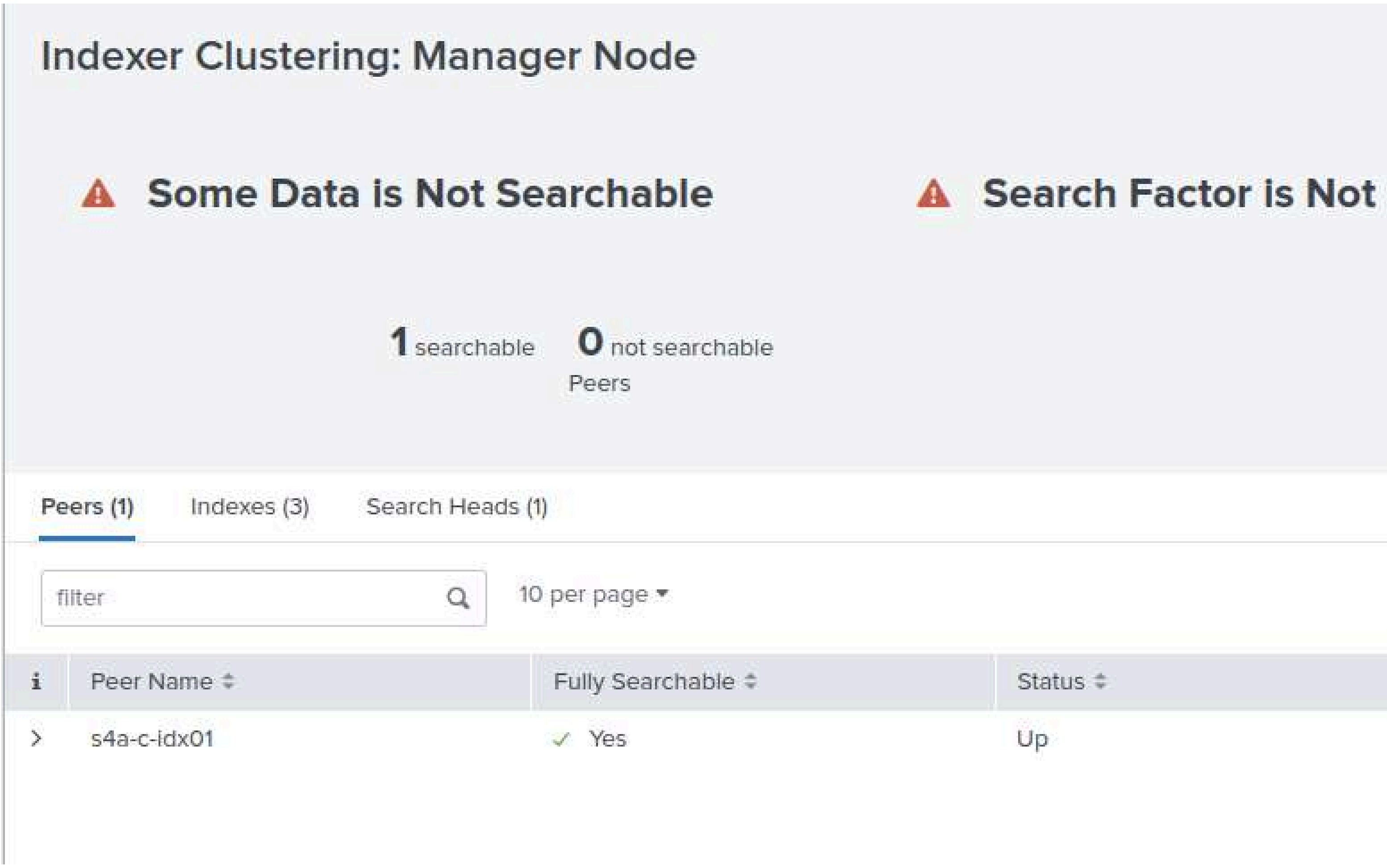


```
splunk@Domane-Demo-i-0
[splunktcp://9998]
disabled = 0
splunk@Domane-Demo-i-0
```

d. Restart the instance to enable the connection

```
/opt/s4a-c-idx01/splunk/bin/splunk restart
```

e. See the node connected, but replication requirements not met



Indexer Clustering: Manager Node

⚠ Some Data is Not Searchable

⚠ Search Factor is Not

1 searchable 0 not searchable
Peers

i	Peer Name ⇕	Fully Searchable ⇕	Status ⇕
›	s4a-c-idx01	✓ Yes	Up

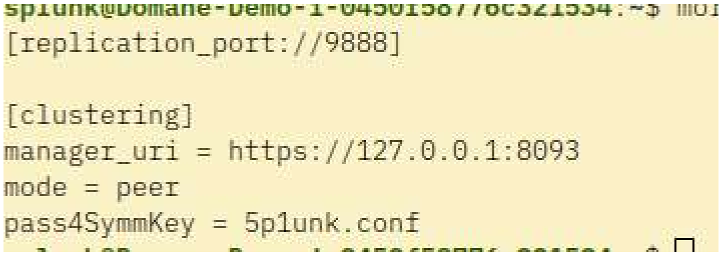
f. Connect node 02 to the Cluster Manager via server.conf

```
cp -rp /opt/s4a-cluster/s4a_clustering_idx_build_member_idx02
```

```
/opt/s4a-c-idx02/splunk/etc/apps
```

g. View the file

```
more
/opt/s4a-c-idx02/splunk/etc/apps/s4a_clustering_idx_build_member_idx02/local/server.conf
```



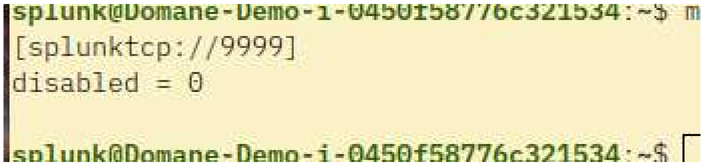
```
splunk@Domane-Demo-i-0450f58776c321534:~$ mor
[replication_port://9888]

[clustering]
manager_uri = https://127.0.0.1:8093
mode = peer
pass4SymmKey = 5p1unk.conf
```

h. Enable the instance to receive data - different from a real environment as we are using a single node with differing ports to simulate a multi-node environment with single instances on each

```
cp -rp /opt/s4a-cluster/s4a_clustering_idx02_receive /opt/s4a-c-idx02/splunk/etc/apps
```

i. View the file

```
more /opt/s4a-c-idx02/splunk/etc/apps/s4a_clustering_idx02_receive/local/inputs.conf
```



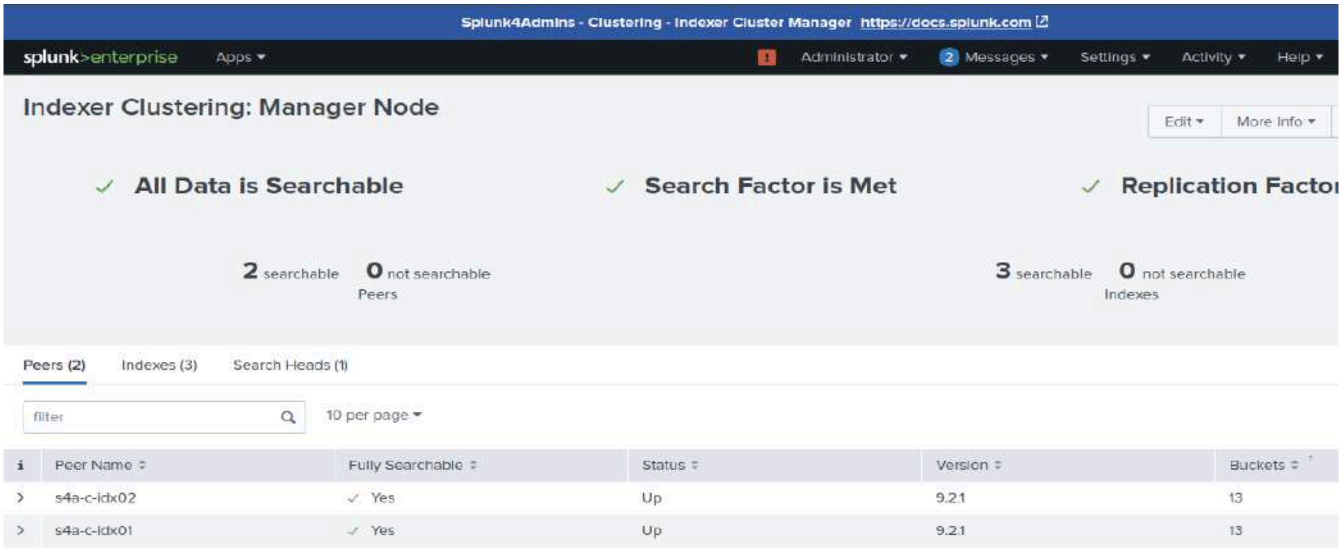
```
splunk@Domane-Demo-i-0450f58776c321534:~$ m
[splunktcp://9999]
disabled = 0

splunk@Domane-Demo-i-0450f58776c321534:~$
```

j. Restart the instance to enable the connection

```
/opt/s4a-c-idx02/splunk/bin/splunk restart
```

9. As per the prior connection, check the CM GUI at “Settings” -> “Indexer Clustering”

    a. Observe the end condition of the cluster



Splunk4Admins - Clustering - Indexer Cluster Manager https://docs.splunk.com

Indexer Clustering: Manager Node

✓ All Data is Searchable ✓ Search Factor is Met ✓ Replication Factor

2 searchable 0 not searchable
Peers

3 searchable 0 not searchable
Indexes

i	Peer Name	Fully Searchable	Status	Version	Buckets
>	s4a-c-idx02	✓ Yes	Up	9.2.1	13
>	s4a-c-idx01	✓ Yes	Up	9.2.1	13

Exercise 2 – Push an app to indexer cluster members

Description

To enable consistent configuration across the indexer cluster, all apps should be pushed from the CM. This is facilitated by a GUI and a CLI interface. This lab uses the GUI, but the docs references all include the how-to to accomplish the same action via the CLI.

Summary:

- Access the CM
- Create the app to be pushed in $SPLUNK_HOME/etc/manager_apps
- On the CM GUI, Validate and test for restart
- Push the apps to the indexers
- Observe the apps as having been pushed

Steps

1. Access the lab node (should already have a terminal window open …)

```
ssh -p 2222 splunk@<<IP_address_of_node>>
```

2. Place the apps into the $SPLUNK_HOME/etc/manager/apps directory

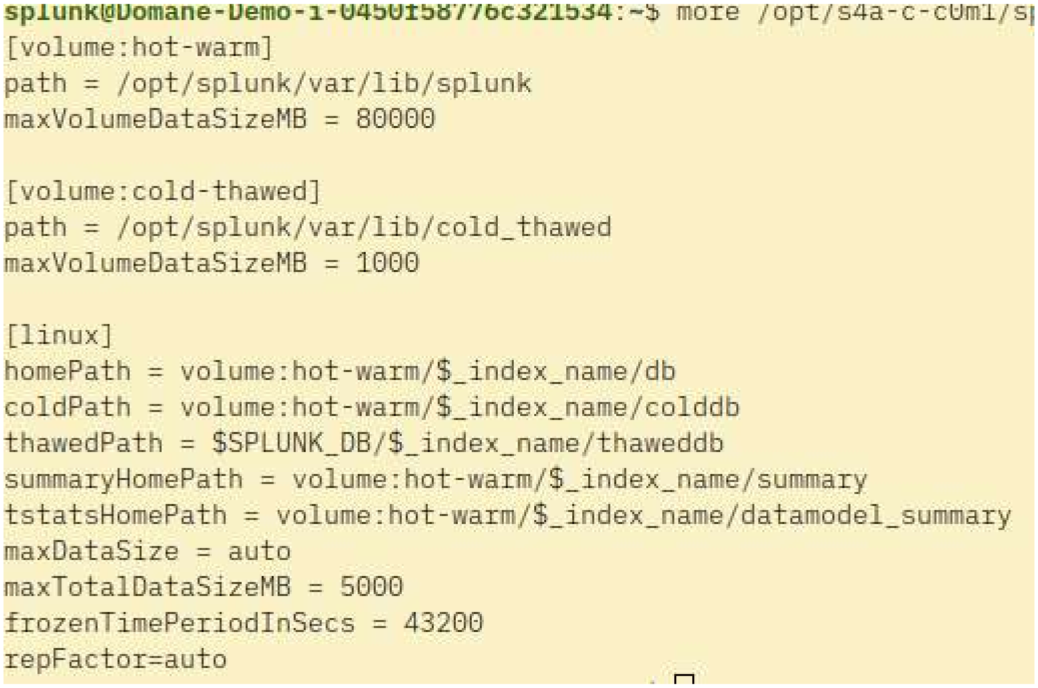
```
cp -rp /opt/s4a-cluster/s4a_clustering_idx_push_to_members_indexes
/opt/s4a-c-c0m1/splunk/etc/manager-apps
```

```
cp -rp /opt/s4a-cluster/s4a_clustering_idx_push_to_members_web
/opt/s4a-c-c0m1/splunk/etc/manager-apps
```

3. Review the apps

    a. s4a_clustering_idx_indexes - defines the ‘linux’ index for linux OS logs

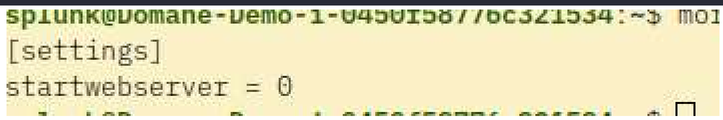
```
more
/opt/s4a-c-c0m1/splunk/etc/manager-apps/s4a_clustering_idx_push_to_members_indexes/local/
indexes.conf
```



```
splunk@Domane-Demo-1-0450f58776c321534:~$ more /opt/s4a-c-c0m1/sp
[volume:hot-warm]
path = /opt/splunk/var/lib/splunk
maxVolumeDataSizeMB = 80000

[volume:cold-thawed]
path = /opt/splunk/var/lib/cold_thawed
maxVolumeDataSizeMB = 1000

[linux]
homePath = volume:hot-warm/$_index_name/db
coldPath = volume:hot-warm/$_index_name/colddb
thawedPath = $SPLUNK_DB/$_index_name/thaweddb
summaryHomePath = volume:hot-warm/$_index_name/summary
tstatsHomePath = volume:hot-warm/$_index_name/datamodel_summary
maxDataSize = auto
maxTotalDataSizeMB = 5000
frozenTimePeriodInSecs = 43200
repFactor=auto
```

b. s4a_clustering_idx_web - disable the web interface on all indexers, a best practice

```
more
/opt/s4a-c-c0m1/splunk/etc/manager-apps/s4a_clustering_idx_push_to_members_web/local/web.
conf
```

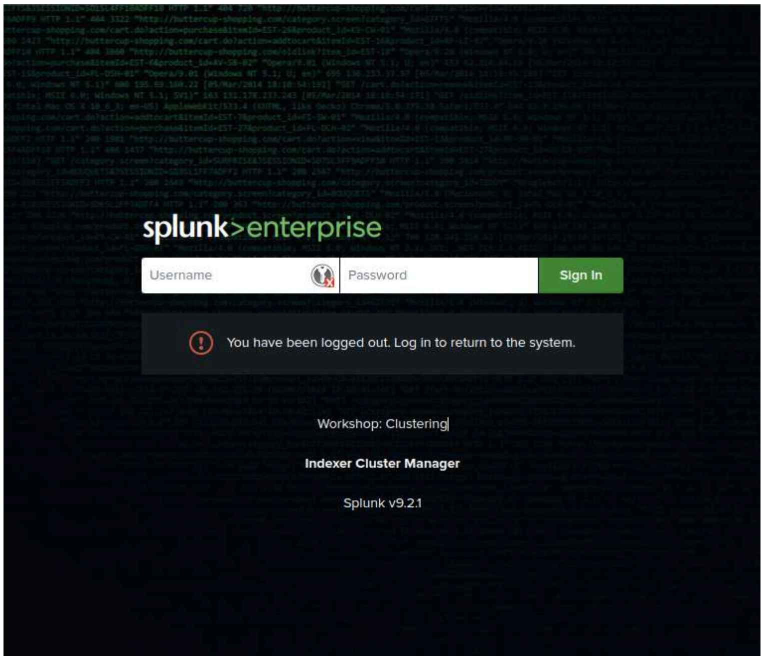


```
splunk@Domane-Demo-1-0450f58776c321534:~$ mor
[settings]
startwebserver = 0
```

4. Log in to the CM Splunk instance (should have an already open window …)

   i. https://<name|IP_address>:4501

   ii. username - “admin”, password - “5p1unk.conf”



splunk>enterprise

You have been logged out. Log in to return to the system.

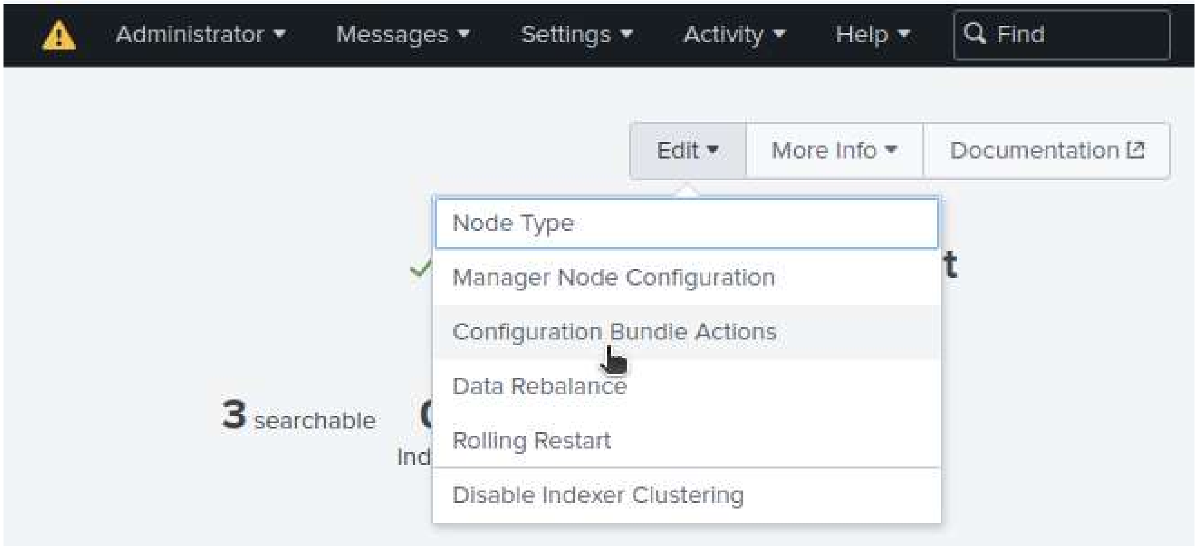
Workshop: Clustering

Indexer Cluster Manager

Splunk v9.2.1

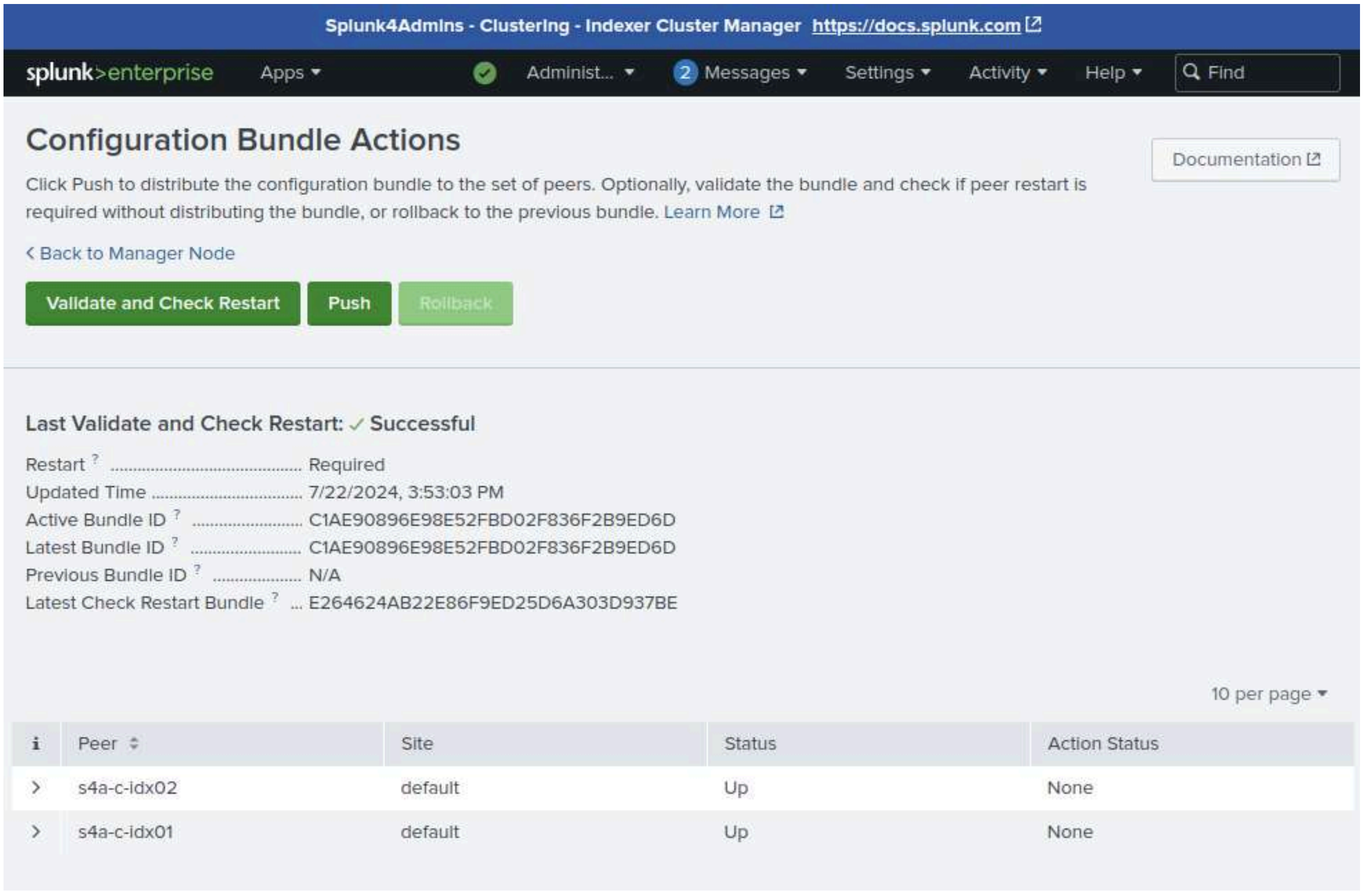
5. On the CM black bar “Settings”, “Indexer Clustering”

   a. Select “Edit”, and “Configuration Bundle Actions”



6. Validate the apps to be pushed

   a. Click on the button “Validate and Check Restart”, and then the dialogue “Validate and Check Restart” again



Splunk4Admins - Clustering - Indexer Cluster Manager https://docs.splunk.com
splunk>enterprise
Apps
Administ...
2 Messages
Settings
Activity
Help
Find
Documentation

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

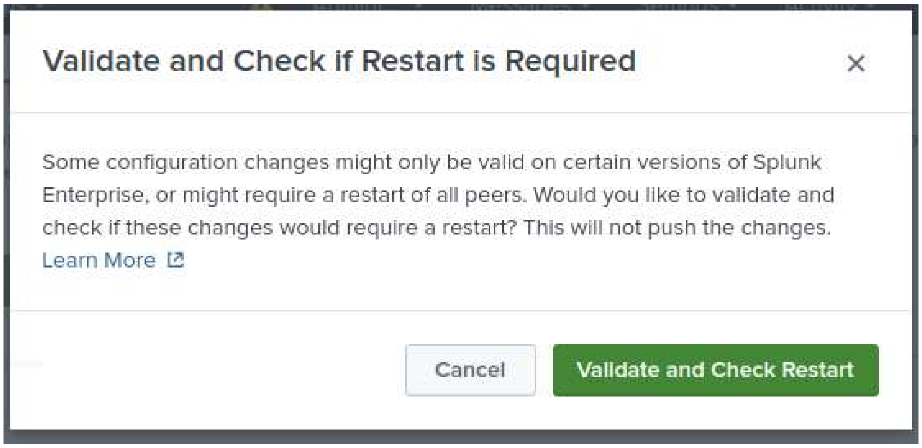
< Back to Manager Node

Validate and Check Restart
Push
Rollback

Last Validate and Check Restart: ✓ Successful

```
Restart ? ............................ Required
Updated Time ......................... 7/22/2024, 3:53:03 PM
Active Bundle ID ? ................... C1AE90896E98E52FBD02F836F2B9ED6D
Latest Bundle ID ? ................... C1AE90896E98E52FBD02F836F2B9ED6D
Previous Bundle ID ? ................. N/A
Latest Check Restart Bundle ? ... E264624AB22E86F9ED25D6A303D937BE
```

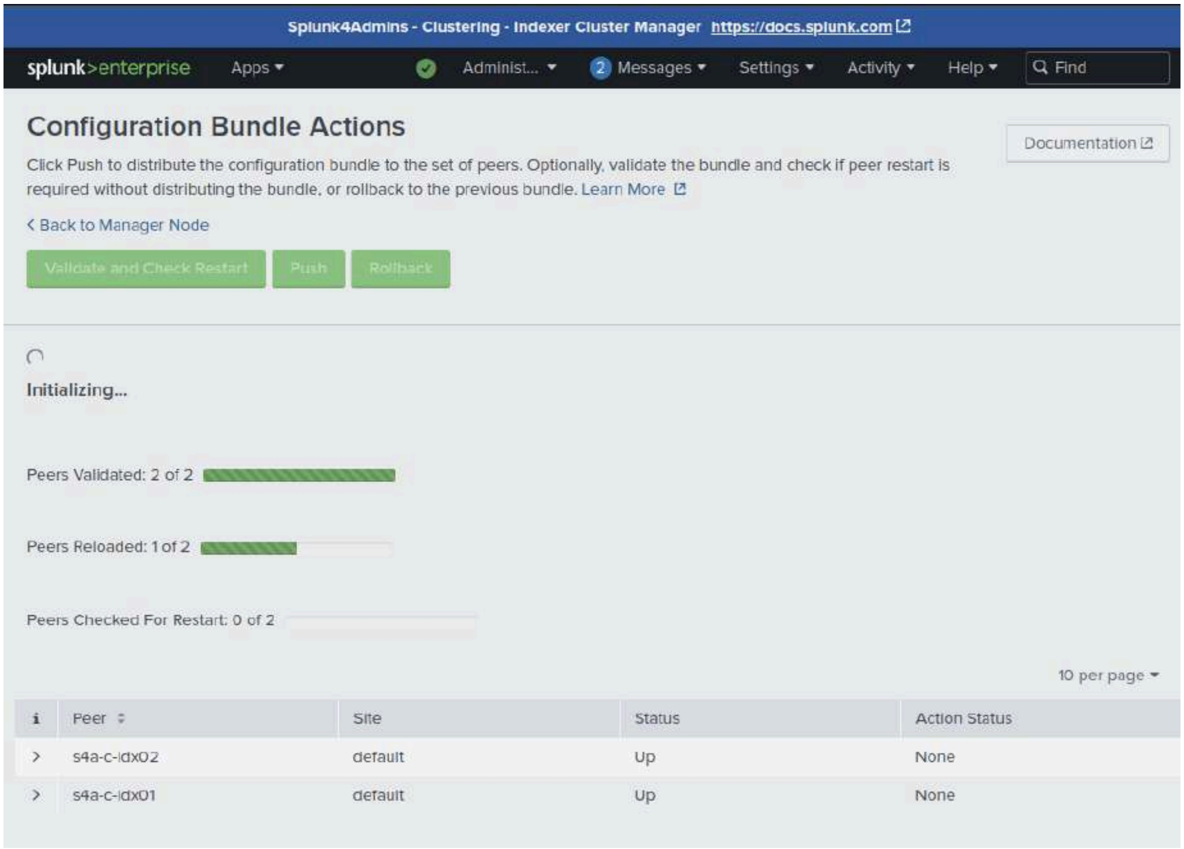
i	Peer	Site	Status	Action Status
>	s4a-c-idx02	default	Up	None
>	s4a-c-idx01	default	Up	None



Validate and Check if Restart is Required

Some configuration changes might only be valid on certain versions of Splunk Enterprise, or might require a restart of all peers. Would you like to validate and check if these changes would require a restart? This will not push the changes. Learn More

b. See the events on the GUI during the check


Splunk4Admins - Clustering - Indexer Cluster Manager https://docs.splunk.com
splunk>enterprise
Apps
Administ...
2 Messages
Settings
Activity
Help
Find
Documentation
Validate and Check Restart
Push
Rollback
10 per page

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 Manager Node

Initializing...

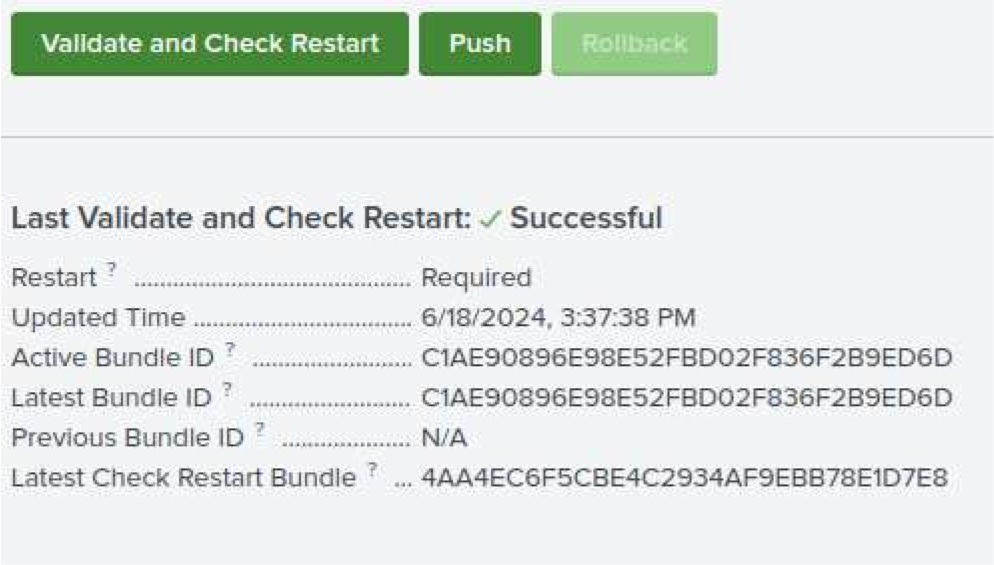
Peers Validated: 2 of 2

Peers Reloaded: 1 of 2

Peers Checked For Restart: 0 of 2

i	Peer	Site	Status	Action Status
>	s4a-c-idx02	default	Up	None
>	s4a-c-idx01	default	Up	None

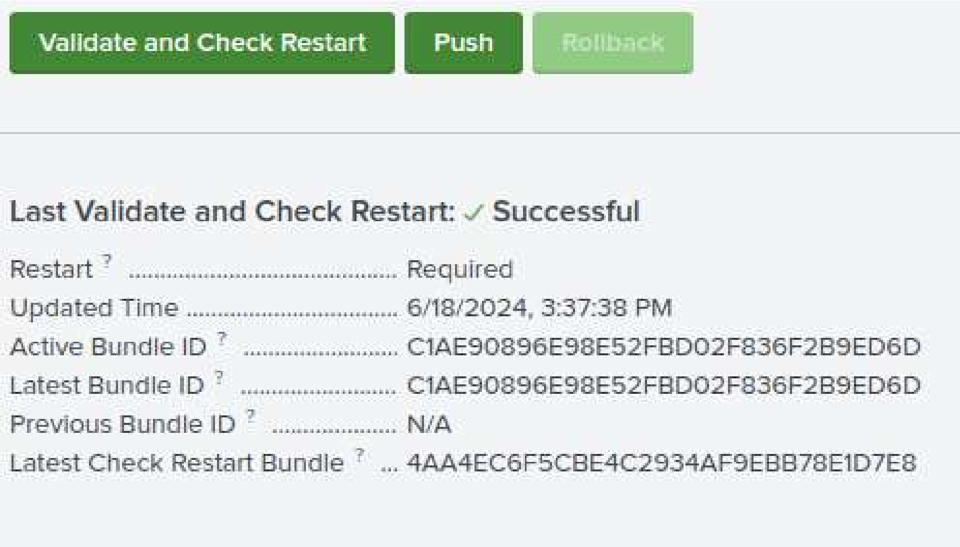
c. Upon a successful return



Last Validate and Check Restart: ✓ Successful

Restart ? .... Required
Updated Time .... 6/18/2024, 3:37:38 PM
Active Bundle ID ? C1AE90896E98E52FBD02F836F2B9ED6D
Latest Bundle ID ? C1AE90896E98E52FBD02F836F2B9ED6D
Previous Bundle ID ? .... N/A
Latest Check Restart Bundle ? ... 4AA4EC6F5CBE4C2934AF9EBB78E1D7E8

d. Observe (and if necessary, record) the ‘Active Bundle ID’ and the ‘Latest Check Restart Bundle’ values. They should be different. After the push, they will be the same

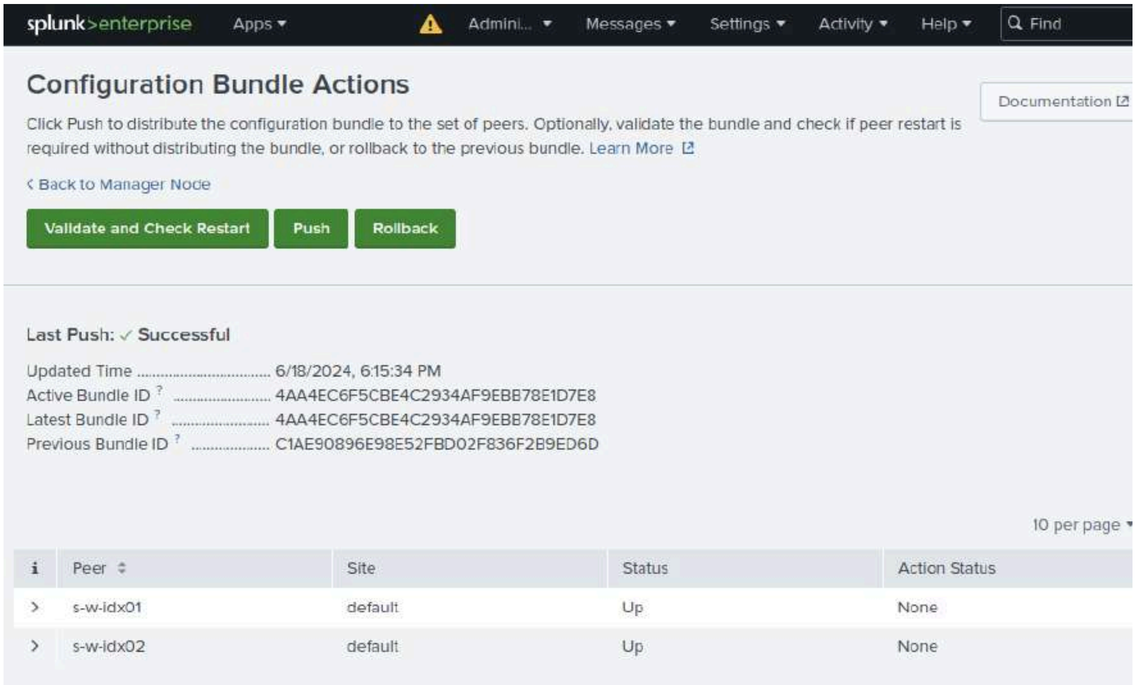
e. 

Last Validate and Check Restart: ✓ Successful

Restart ? .... Required
Updated Time .... 6/18/2024, 3:37:38 PM
Active Bundle ID ? C1AE90896E98E52FBD02F836F2B9ED6D
Latest Bundle ID ? C1AE90896E98E52FBD02F836F2B9ED6D
Previous Bundle ID ? .... N/A
Latest Check Restart Bundle ? ... 4AA4EC6F5CBE4C2934AF9EBB78E1D7E8

7. Execute the app "push"

   a. Push the "Push" green button



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

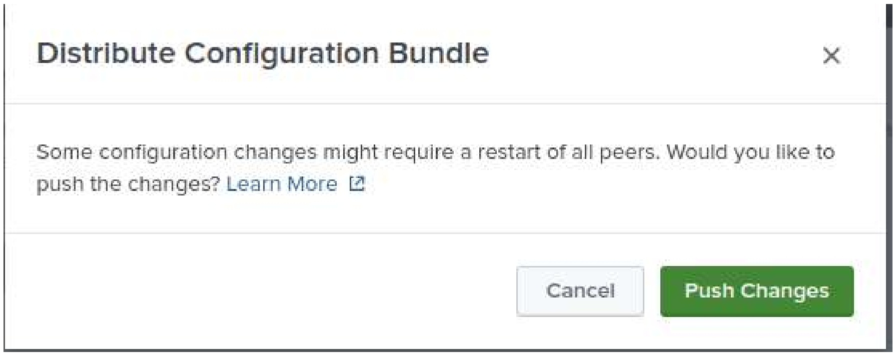
‹ Back to Manager Node

Last Push: ✓ Successful

Updated Time .... 6/18/2024, 6:15:34 PM
Active Bundle ID ? 4AA4EC6F5CBE4C2934AF9EBB78E1D7E8
Latest Bundle ID ? 4AA4EC6F5CBE4C2934AF9EBB78E1D7E8
Previous Bundle ID ? C1AE90896E98E52FBD02F836F2B9ED6D

10 per page ▾

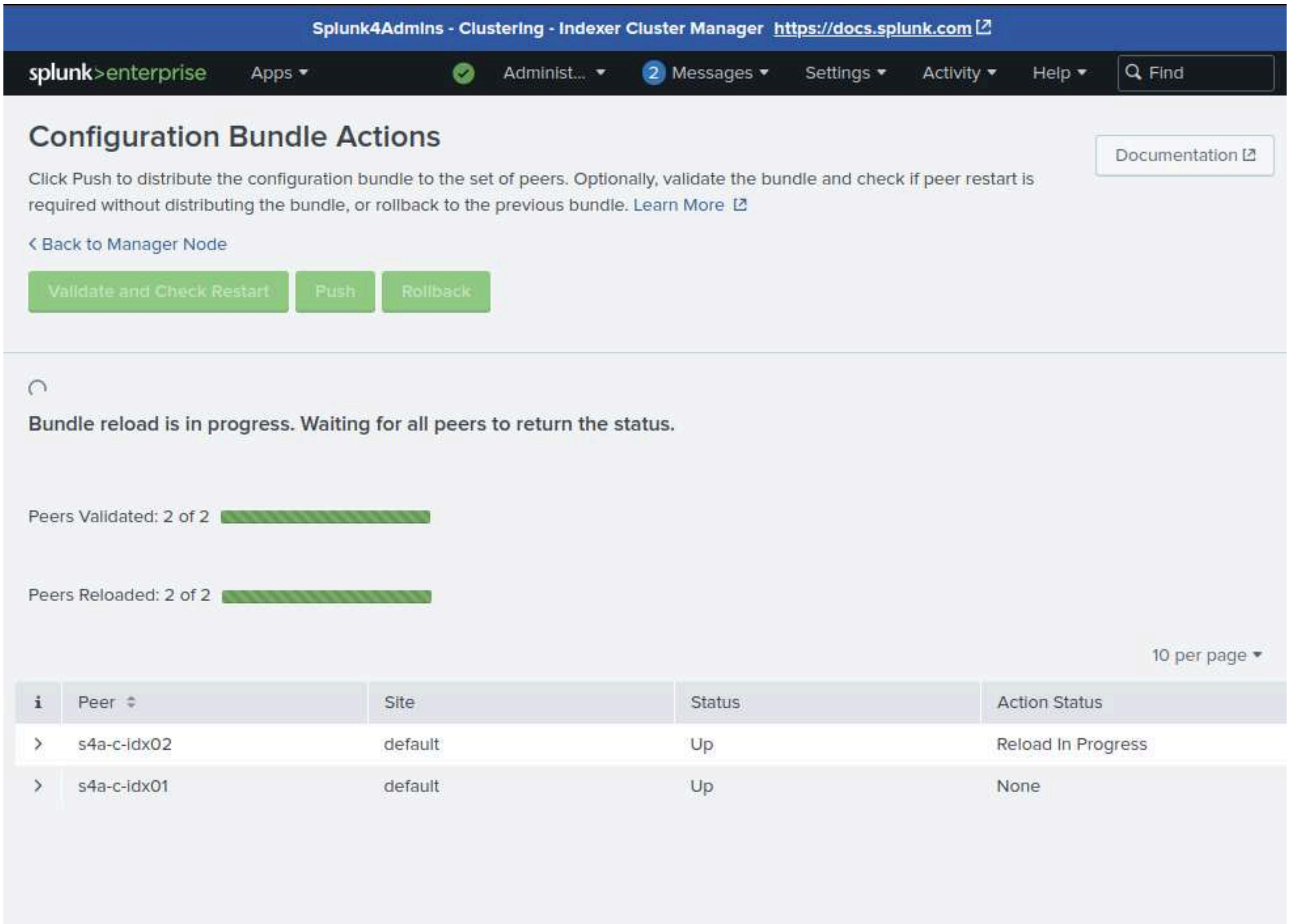
i	Peer ⇕	Site	Status	Action Status
›	s-w-idx01	default	Up	None
›	s-w-idx02	default	Up	None



Distribute Configuration Bundle

Some configuration changes might require a restart of all peers. Would you like to push the changes? Learn More

b. See the actions as the process unfolds



Splunk4Admins - Clustering - Indexer Cluster Manager https://docs.splunk.com
splunk>enterprise
Apps
Administ...
2 Messages
Settings
Activity
Help
Find
Documentation

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 Manager Node

Validate and Check Restart
Push
Rollback

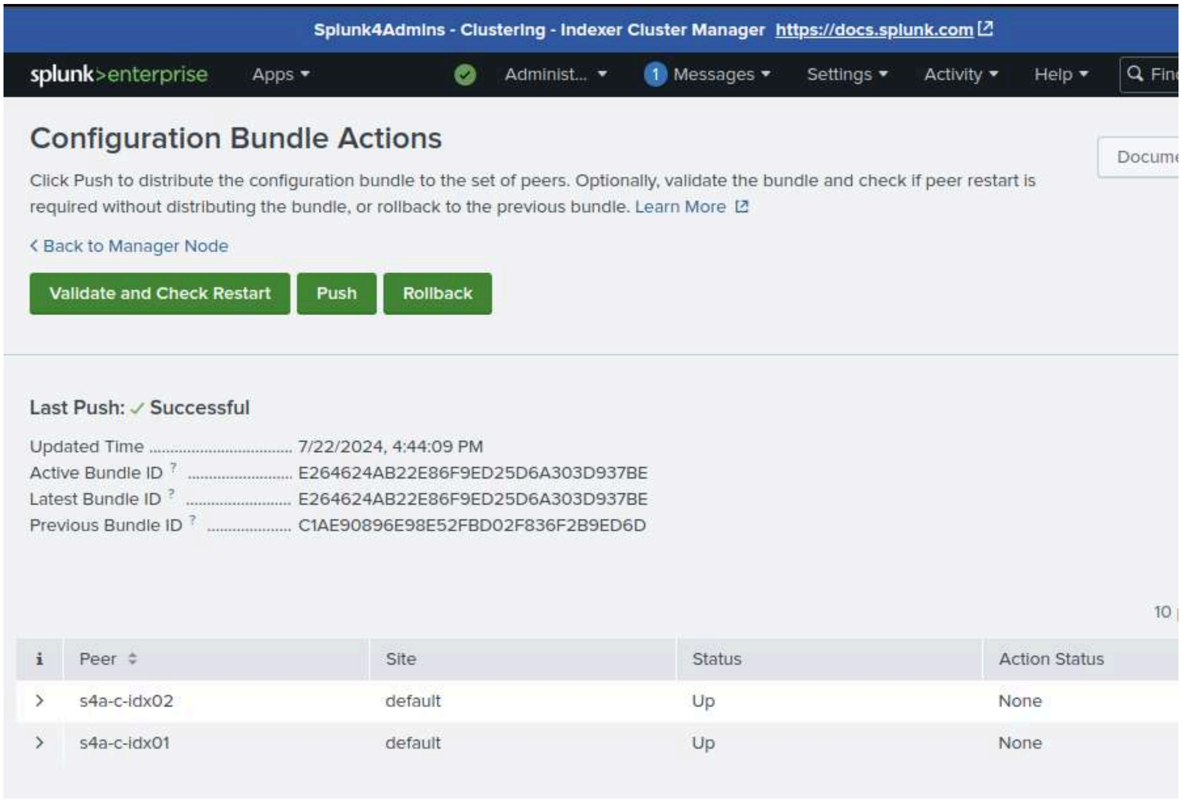
Bundle reload is in progress. Waiting for all peers to return the status.

Peers Validated: 2 of 2

Peers Reloaded: 2 of 2

i	Peer	Site	Status	Action Status
>	s4a-c-idx02	default	Up	Reload In Progress
>	s4a-c-idx01	default	Up	None

c. And success


Splunk4Admins - Clustering - Indexer Cluster Manager https://docs.splunk.com
splunk>enterprise
Apps
Administ...
1 Messages
Settings
Activity
Help
Find
Docume
Validate and Check Restart
Push
Rollback
10

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 Manager Node

Last Push: ✓ Successful

Updated Time .... 7/22/2024, 4:44:09 PM
Active Bundle ID ? E264624AB22E86F9ED25D6A303D937BE
Latest Bundle ID ? E264624AB22E86F9ED25D6A303D937BE
Previous Bundle ID ? C1AE90896E98E52FBD02F836F2B9ED6D

i	Peer	Site	Status	Action Status
›	s4a-c-idx02	default	Up	None
›	s4a-c-idx01	default	Up	None

d. Compare the bundle IDs again, the ‘Active Bundle ID’ and ‘Latest Bundle ID’ should be the same, and ‘Previous Bundle ID’ should be different

8. Validate the successful push by finding the files mentioned during the lab

   i. Access either indexer node via ssh (normally), or, here in the lab …

   ii. Find the various apps

```
find /opt/s4a-c-idx0?/splunk/etc/peer-apps -name "s4a*" -ls
```

   iii. On the CM, search for “index=linux”

   iv. Attempt to access the GUI of one of the indexers

      1. https://<name|IP_address>:4502 - see the FAIL

Exercise 3 – Build a search head cluster

Description

Create a search head cluster (SHC), consisting of a deployer and two members

Summary:

- Access the node selected to be the DEPLOYER
- Create the app to cause the node to be the deployer
- Restart Splunkd
- Create the members
- Force a Captain
- Validate

Steps

1. Access the lab node

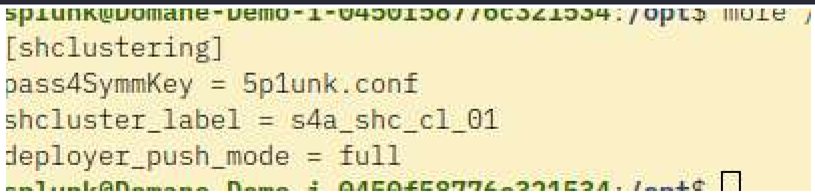
```
ssh -p 2222 splunk@<<IP_address_of_node>>
```

2. Create the app to make the node the deployer

```
cp -rp /opt/s4a-cluster/s4a_clustering_shc_build_deployer/
/opt/s4a-c-depl/splunk/etc/apps
```

3. Examine the file created

```
more /opt/s4a-c-depl/splunk/etc/apps/s4a_clustering_shc_build_deployer/local/server.conf
```



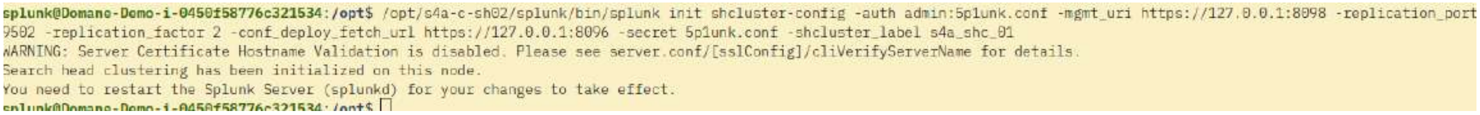
```
splunk@Domane-Demo-i-0450f58776c321534:/opt$ more /
[shclustering]
pass4SymmKey = 5p1unk.conf
shcluster_label = s4a_shc_cl_01
deployer_push_mode = full
splunk@Domane-Demo-i-0450f58776c321534:/opt$
```

4. Restart splunk

```
/opt/s4a-c-depl/splunk/bin/splunk restart
```

5. Initialize the first SHC member as a member

```
/opt/s4a-c-sh02/splunk/bin/splunk init shcluster-config -auth admin:5p1unk.conf -mgmt_uri
https://127.0.0.1:8098 -replication_port 9502 -replication_factor 2
-conf_deploy_fetch_url https://127.0.0.1:8096 -secret 5p1unk.conf -shcluster_label
s4a_shc_01
```



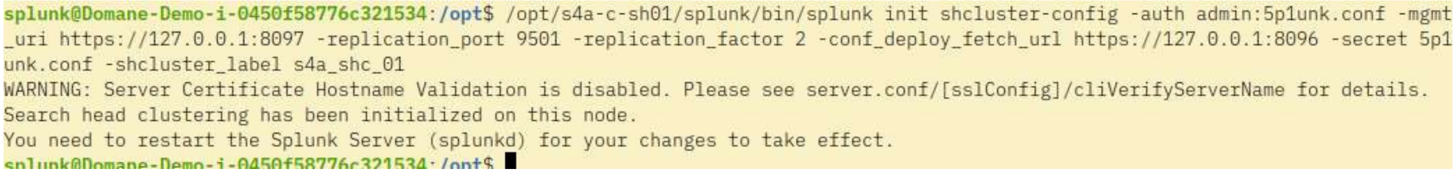
```
splunk@Domane-Demo-i-0450f58776c321534:/opt$ /opt/s4a-c-sh02/splunk/bin/splunk init shcluster-config -auth admin:5p1unk.conf -mgmt_uri https://127.0.0.1:8098 -replication_port
9502 -replication_factor 2 -conf_deploy_fetch_url https://127.0.0.1:8096 -secret 5p1unk.conf -shcluster_label s4a_shc_01
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Search head clustering has been initialized on this node.
You need to restart the Splunk Server (splunkd) for your changes to take effect.
splunk@Domane-Demo-i-0450f58776c321534:/opt$
```

   a. Restart Splunkd

```
/opt/s4a-c-sh02/splunk/bin/splunk restart
```

6. Initialize the new node to be a member

```
/opt/s4a-c-sh01/splunk/bin/splunk init shcluster-config -auth admin:5p1unk.conf -mgmt_uri
https://127.0.0.1:8097 -replication_port 9501 -replication_factor 2
-conf_deploy_fetch_url https://127.0.0.1:8096 -secret 5p1unk.conf -shcluster_label
s4a_shc_01
```



```
splunk@Domane-Demo-i-0450f58776c321534:/opt$ /opt/s4a-c-sh01/splunk/bin/splunk init shcluster-config -auth admin:5p1unk.conf -mgmt
_uri https://127.0.0.1:8097 -replication_port 9501 -replication_factor 2 -conf_deploy_fetch_url https://127.0.0.1:8096 -secret 5p1
unk.conf -shcluster_label s4a_shc_01
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Search head clustering has been initialized on this node.
You need to restart the Splunk Server (splunkd) for your changes to take effect.
splunk@Domane-Demo-i-0450f58776c321534:/opt$
```

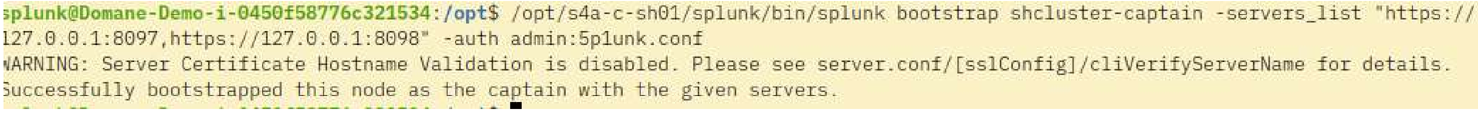
   a. Restart Splunkd

```
/opt/s4a-c-sh01/splunk/bin/splunk restart
```

7. Declare the “Captain”

   a. On either node execute (here we’ll use sh01):

```
/opt/s4a-c-sh01/splunk/bin/splunk bootstrap shcluster-captain -servers_list
"https://127.0.0.1:8097,https://127.0.0.1:8098" -auth admin:5p1unk.conf
```



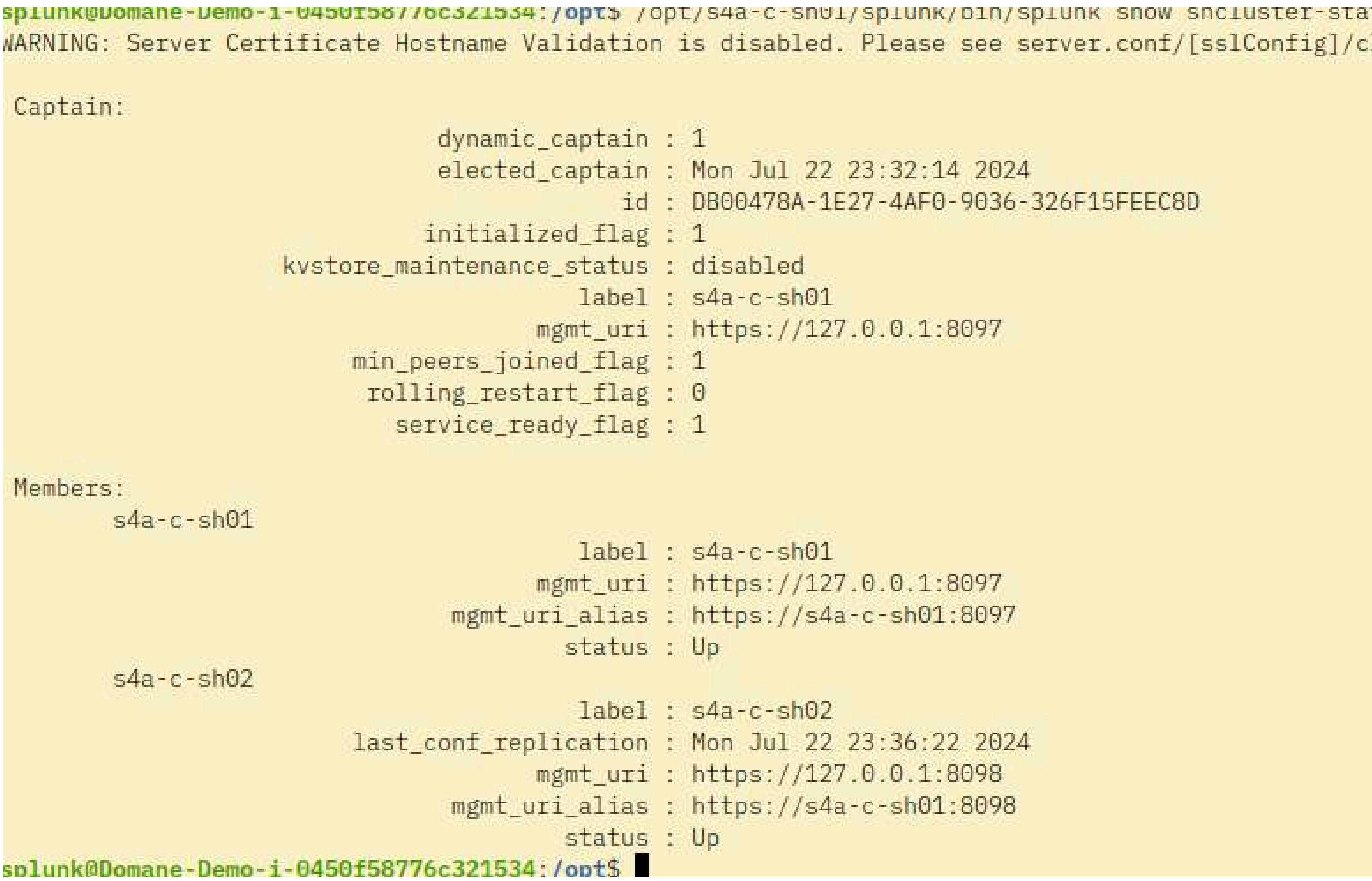
```
splunk@Domane-Demo-i-0450f58776c321534:/opt$ /opt/s4a-c-sh01/splunk/bin/splunk bootstrap shcluster-captain -servers_list "https://
127.0.0.1:8097,https://127.0.0.1:8098" -auth admin:5p1unk.conf
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Successfully bootstrapped this node as the captain with the given servers.
```

8. Validate the cluster membership

   a. On either node, execute:

      i. Get the status of the cluster

```
/opt/s4a-c-sh01/splunk/bin/splunk show shcluster-status -auth admin:5p1unk.conf
```



```
splunk@Domane-Demo-i-0450f58776c321534:/opt$ /opt/s4a-c-sh01/splunk/bin/splunk show shcluster-sta
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/c

 Captain:
                               dynamic_captain : 1
                               elected_captain : Mon Jul 22 23:32:14 2024
                                            id : DB00478A-1E27-4AF0-9036-326F15FEEC8D
                              initialized_flag : 1
                    kvstore_maintenance_status : disabled
                                         label : s4a-c-sh01
                                      mgmt_uri : https://127.0.0.1:8097
                         min_peers_joined_flag : 1
                          rolling_restart_flag : 0
                            service_ready_flag : 1

 Members:
        s4a-c-sh01
                                         label : s4a-c-sh01
                                      mgmt_uri : https://127.0.0.1:8097
                                mgmt_uri_alias : https://s4a-c-sh01:8097
                                        status : Up
        s4a-c-sh02
                                         label : s4a-c-sh02
                         last_conf_replication : Mon Jul 22 23:36:22 2024
                                      mgmt_uri : https://127.0.0.1:8098
                                mgmt_uri_alias : https://s4a-c-sh01:8098
                                        status : Up
splunk@Domane-Demo-i-0450f58776c321534:/opt$
```

Exercise 4 – Push an app to search head cluster members

Description

Use of the deployer permits consistent app (and other KO management). Frequently this will consist of a connection to the SSO, “production” dashboards, KV Store connections, lookup files, and other configuration settings.

Summary:

- Access the deployer node
- Create the apps to be deployed
- Use the apps in place in $SPLUNK_HOME/etc/shcluster/apps (extracted from a tar file)
  - SA_hywels_dashboards
  - s4a_ALL_IndexAndForwarder
  - s4a_ALL_outputs
  - s4a_clustering_shc_integrate_with_idxCluster/
- Push the apps

Steps

1. Access the lab node to configure the deployer

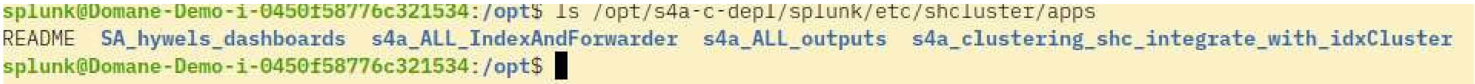
```
ssh -p 2222 splunk@<<IP_address_of_node>>
```

2. Place the apps to replicated into the ‘etc/shcluster/apps’ directory of the deployer

```
tar -xf /opt/s4a-cluster/deployer_apps.tgz -C /opt/s4a-c-depl/splunk/etc/shcluster/apps/
```

3. Observe the files in place in $SPLUNK_HOME/etc/shcluster/apps

```
ls /opt/s4a-c-depl/splunk/etc/shcluster/apps
```

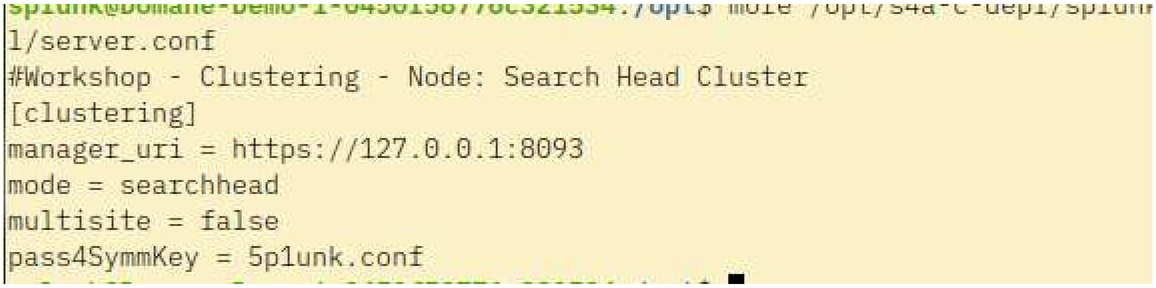


```
splunk@Domane-Demo-i-0450f58776c321534:/opt$ ls /opt/s4a-c-depl/splunk/etc/shcluster/apps
README  SA_hywels_dashboards  s4a_ALL_IndexAndForwarder  s4a_ALL_outputs  s4a_clustering_shc_integrate_with_idxCluster
splunk@Domane-Demo-i-0450f58776c321534:/opt$ 
```

4. Review the files - be sure to copy the “more” for each line, otherwise you will experience a “...Permission denied” error.

```
more /opt/s4a-c-depl/splunk/etc/shcluster/apps/s4a_ALL_outputs/local/outputs.conf
```

```
#--
more
/opt/s4a-c-depl/splunk/etc/shcluster/apps/s4a_ALL_IndexAndForwarder/local/outputs.conf
#--
more
/opt/s4a-c-depl/splunk/etc/shcluster/apps/s4a_clustering_shc_integrate_with_idxCluster/lo
cal/server.conf
```



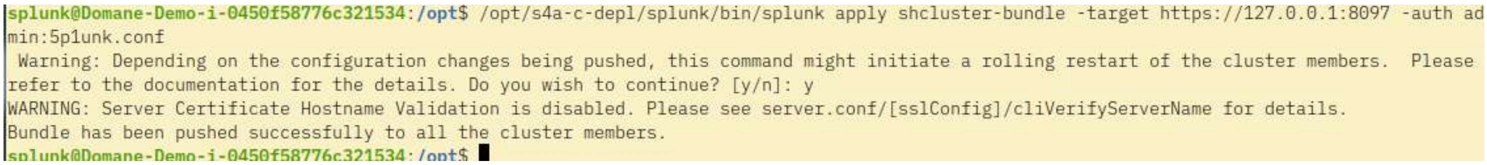
```
splunk@Domane-Demo-i-0450f58776c321534:/opt$ more /opt/s4a-c-depl/splun
l/server.conf
#Workshop - Clustering - Node: Search Head Cluster
[clustering]
manager_uri = https://127.0.0.1:8093
mode = searchhead
multisite = false
pass4SymmKey = 5p1unk.conf
```

a. To demonstrate that the app was pushed successfully, find the many files in ‘ SA_hywels_dashboards’ app directory with the following command.

```
find /opt/s4a-c-depl/splunk/etc/shcluster/apps/SA_hywels_dashboards/ -ls
```

5. Push the bundle to the SHC members

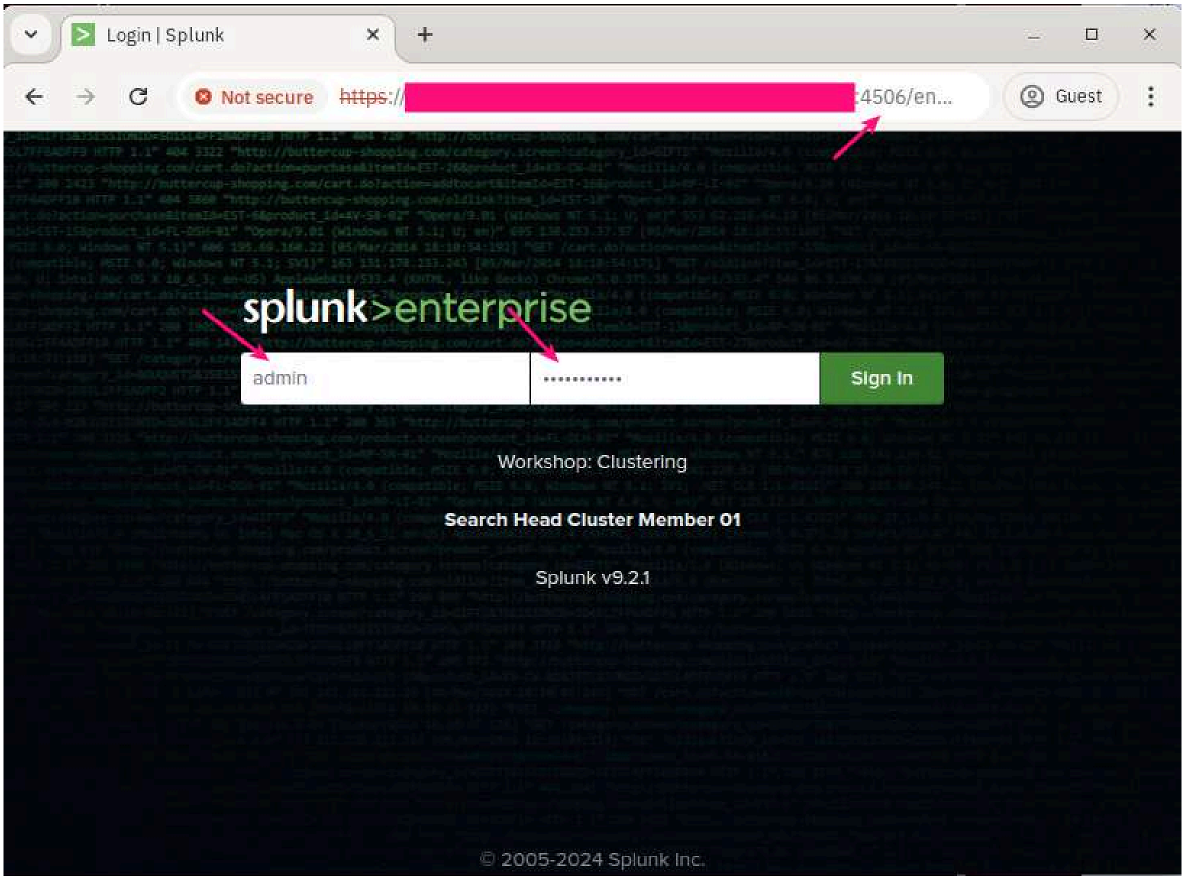
```
/opt/s4a-c-depl/splunk/bin/splunk apply shcluster-bundle -target https://127.0.0.1:8097
-auth admin:5p1unk.conf
```



```
splunk@Domane-Demo-i-0450f58776c321534:/opt$ /opt/s4a-c-depl/splunk/bin/splunk apply shcluster-bundle -target https://127.0.0.1:8097 -auth ad
min:5p1unk.conf
 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]: y
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Bundle has been pushed successfully to all the cluster members.
splunk@Domane-Demo-i-0450f58776c321534:/opt$
```

Wait a bit … up to 120 seconds!

6. Validate the push, access the GUI on either of the SHC members
    a. https://<<node_name|IP_address>>:4506
    b. username - “admin”, password - “5p1unk.conf”



https://[redacted]:4506/en...

admin

•••••••••••

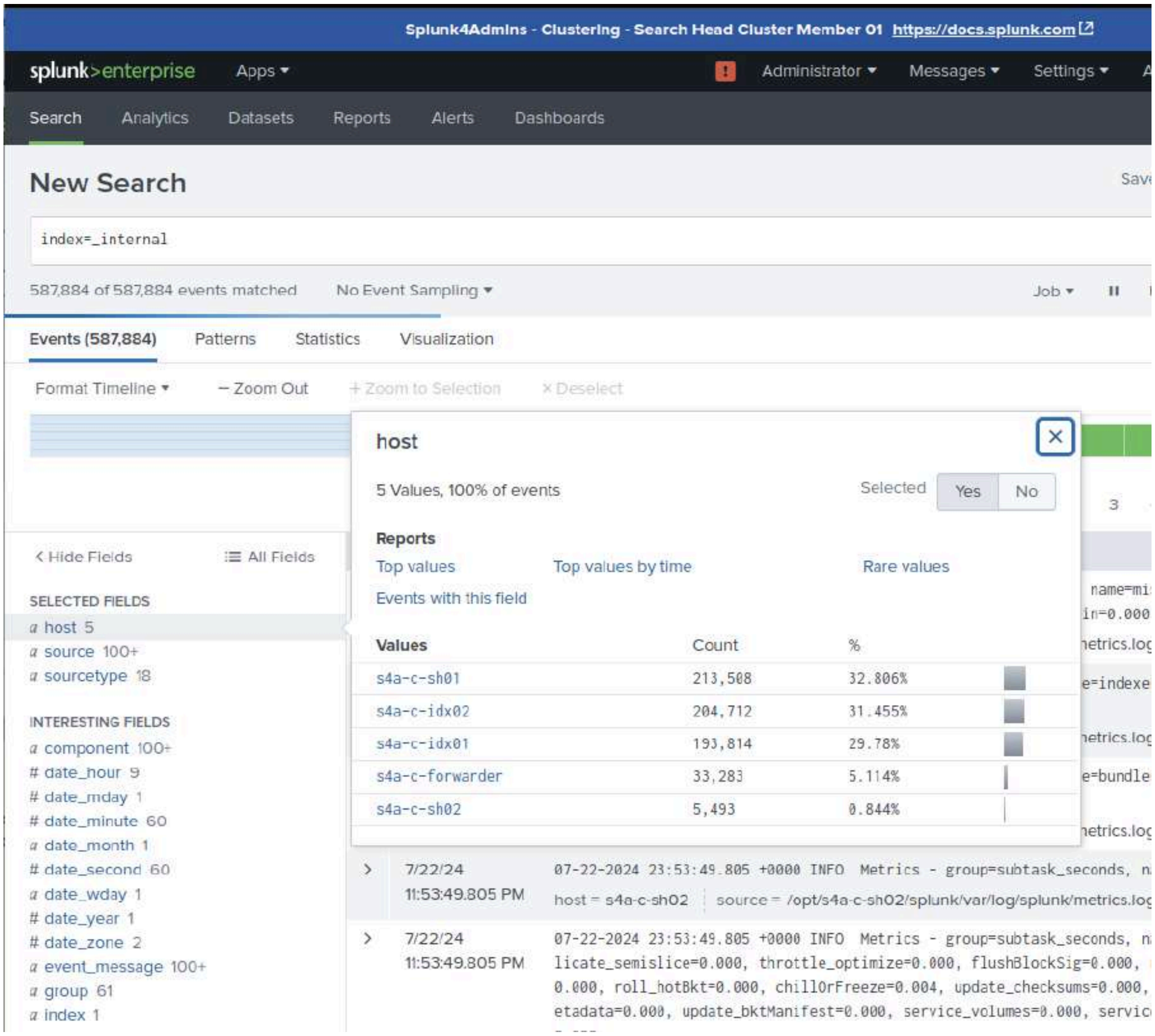
Workshop: Clustering

Search Head Cluster Member 01

Splunk v9.2.1

© 2005-2024 Splunk Inc.

c. Search for “`index=_internal`”, on the left in “SELECTED FIELDS” click on “host” and see that all of the nodes (including an already configured forwarder) are sending their data to the central indexer cluster due to the “IndexAndForward” setting configured (on all nodes, but the last configuration was the SHC).



```
index=_internal
```

587,884 of 587,884 events matched   No Event Sampling ▾

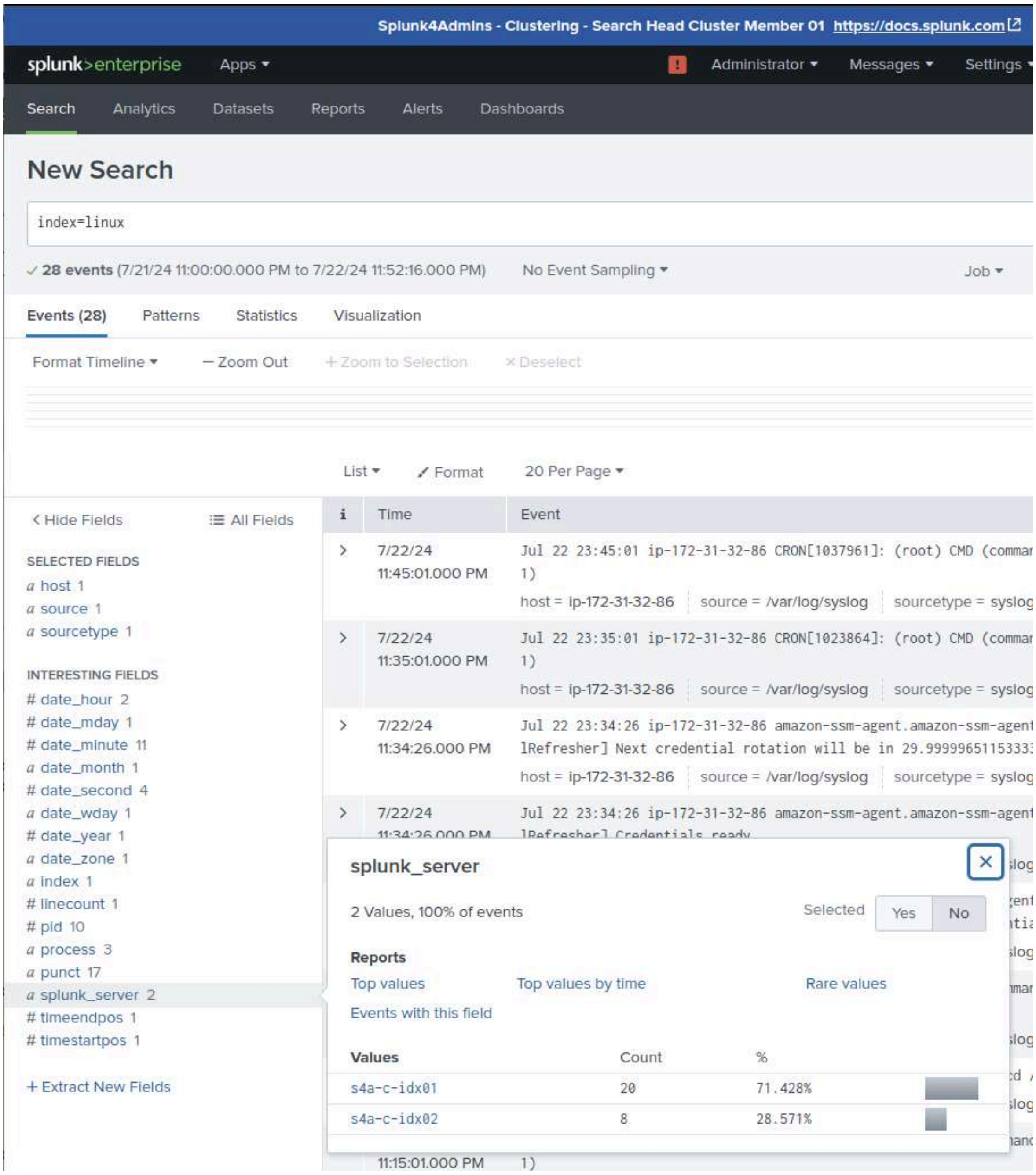
host

5 Values, 100% of events

Values	Count	%
s4a-c-sh01	213,508	32.806%
s4a-c-idx02	204,712	31.455%
s4a-c-idx01	193,814	29.78%
s4a-c-forwarder	33,283	5.114%
s4a-c-sh02	5,493	0.844%

```
> 7/22/24          07-22-2024 23:53:49.805 +0000 INFO  Metrics - group=subtask_seconds, n
  11:53:49.805 PM  host = s4a-c-sh02 | source = /opt/s4a-c-sh02/splunk/var/log/splunk/metrics.log

> 7/22/24          07-22-2024 23:53:49.805 +0000 INFO  Metrics - group=subtask_seconds, n
  11:53:49.805 PM  licate_semislice=0.000, throttle_optimize=0.000, flushBlockSig=0.000,
                   0.000, roll_hotBkt=0.000, chillOrFreeze=0.004, update_checksums=0.000,
                   etadata=0.000, update_bktManifest=0.000, service_volumes=0.000, servic
```

d. Search for "`index=linux`" and click on the "splunk_server" field … see that there are events from the actual VM /var/log/syslog ingested from the forwarder configured, and the only location for the search is against the two indexers (the integration app pushed).



```
index=linux
```

✓ 28 events (7/21/24 11:00:00.000 PM to 7/22/24 11:52:16.000 PM)

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- # date_hour 2
- # date_mday 1
- # date_minute 11
- a date_month 1
- # date_second 4
- a date_wday 1
- # date_year 1
- a date_zone 1
- a index 1
- # linecount 1
- # pid 10
- a process 3
- a punct 17
- a splunk_server 2
- # timeendpos 1
- # timestartpos 1

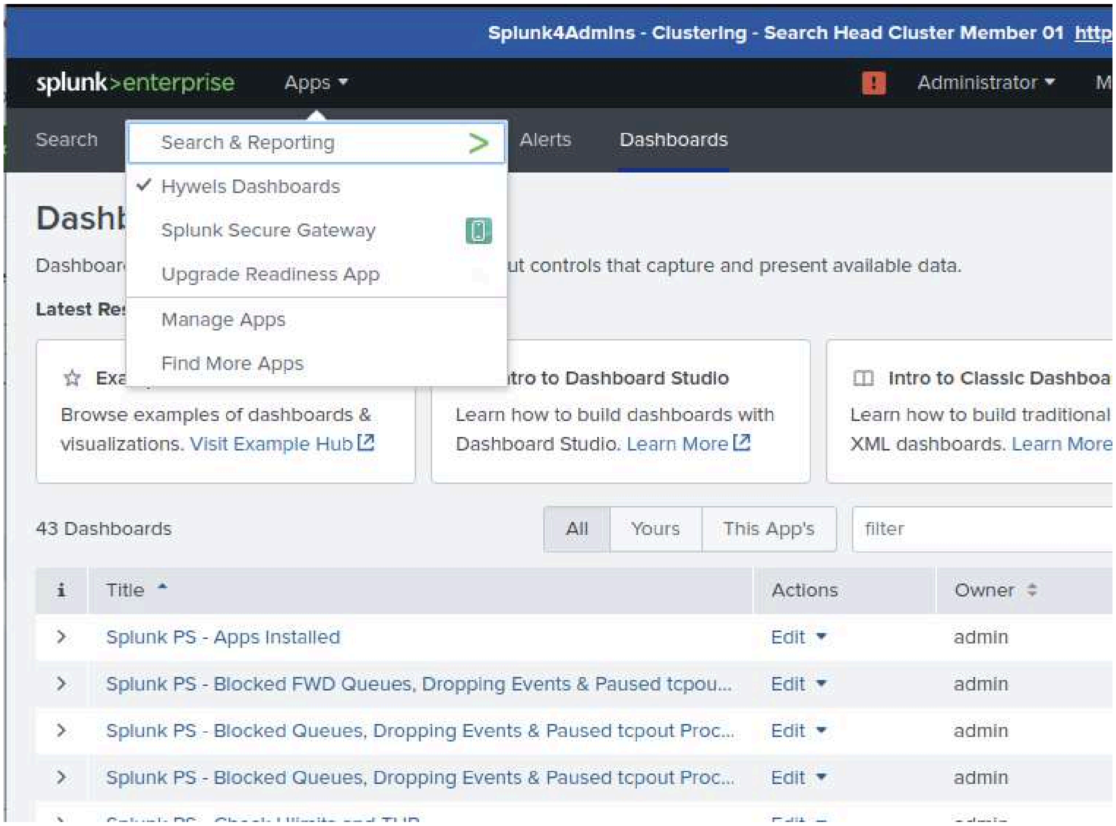
```
i  Time                   Event
>  7/22/24                Jul 22 23:45:01 ip-172-31-32-86 CRON[1037961]: (root) CMD (commar
   11:45:01.000 PM        1)
                          host = ip-172-31-32-86   source = /var/log/syslog   sourcetype = syslog
>  7/22/24                Jul 22 23:35:01 ip-172-31-32-86 CRON[1023864]: (root) CMD (commar
   11:35:01.000 PM        1)
                          host = ip-172-31-32-86   source = /var/log/syslog   sourcetype = syslog
>  7/22/24                Jul 22 23:34:26 ip-172-31-32-86 amazon-ssm-agent.amazon-ssm-agent
   11:34:26.000 PM        lRefresher] Next credential rotation will be in 29.99999651153333
                          host = ip-172-31-32-86   source = /var/log/syslog   sourcetype = syslog
>  7/22/24                Jul 22 23:34:26 ip-172-31-32-86 amazon-ssm-agent.amazon-ssm-agent
   11:34:26.000 PM        lRefresher] Credentials ready
   11:15:01.000 PM        1)
```

splunk_server

2 Values, 100% of events

Values	Count	%
s4a-c-idx01	20	71.428%
s4a-c-idx02	8	28.571%

e. Select “Apps” from the top black bar, click on “Hywels Dashboards” and see the many dashboards available



Dashb

Dashboar ut controls that capture and present available data.

Latest Re

☆ Exa

Browse examples of dashboards & visualizations. Visit Example Hub

tro to Dashboard Studio

Learn how to build dashboards with Dashboard Studio. Learn More

Intro to Classic Dashboa

Learn how to build traditional XML dashboards. Learn More

43 Dashboards

i	Title ▴	Actions	Owner ⇕
>	Splunk PS - Apps Installed	Edit ▾	admin
>	Splunk PS - Blocked FWD Queues, Dropping Events & Paused tcpou...	Edit ▾	admin
>	Splunk PS - Blocked Queues, Dropping Events & Paused tcpout Proc...	Edit ▾	admin
>	Splunk PS - Blocked Queues, Dropping Events & Paused tcpout Proc...	Edit ▾	admin
>	Splunk PS - Check Ulimits and THP	Edit ▾	admin

Links

Title	Link
System requirements for use of Splunk Enterprise on-premises	https://docs.splunk.com/Documentation/Splunk/latest/Installation/Systemrequirements
Indexing and search architecture	https://lantern.splunk.com/Splunk_Success_Framework/Platform_Management/Indexing_and_search_architecture
Configuration updates that the cluster replicates	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/HowconfrepoworksinSHC
Configure peer nodes with server.conf	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configurepeerswithserverconf
Configure the manager node with server.conf	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configuremanagerwithserverconf
Configure the peer indexes in an indexer cluster	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configurethepeerindexes
Enable the indexer cluster manager node	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Enablethemanagernode
Enable the peer nodes	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Enablethepeernodes
Indexer cluster deployment overview	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Clusterdeploymentoverview
indexes.conf.spec	https://docs.splunk.com/Documentation/Splunk/latest/Admin/Indexesconf
inputs.conf.spec	https://docs.splunk.com/Documentation/Splunk/latest/Admin/Inputsconf
Manage app deployment across all peers	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Manageappdeployment
Manage common configurations across all peers	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Managecommonconfigurations
Peer node configuration overview	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configurethepeers
System requirements and other deployment considerations for indexer clusters	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Systemrequirements
Update common peer configurations and apps	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Updatepeerconfigurations
Use Splunk Web to apply the bundle	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Updatepeerconfigurations#:~:text=currently%20in%20progress.-,Use%20Splunk%20Web%20to%20apply%20the%20bundle,-To%20apply%20the
Use Splunk Web to validate the bundle and check restart	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Updatepeerconfigurations#:~:text=or%20the%20CLI.-,Use%20Splunk%20Web%20to%20validate%20the%20bundle%20and%20check%20restart,-Use%20the%20Validate

web.conf.spec	https://docs.splunk.com/Documentation/Splunk/latest/Admin/Webconf
Bring up the cluster captain	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCdeploymentoverview
Check search head cluster status	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCdeploymentoverview
Choose a deployer push mode	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/PropagateSHCconfigurationchanges
Configuration updates that the cluster replicates	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/HowconfrepoworksinSHC
Configuration updates that the cluster replicates	Configuration updates that the cluster replicates - Splunk Documentation
Deploy a configuration bundle	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/PropagateSHCconfigurationchanges
Deploy a search head cluster	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCdeploymentoverview
How configuration changes propagate across the search head cluster	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/HowconfigurationworksinSHC
How the cluster handles search artifact	Search head clustering architecture - Splunk Documentation
Initialize cluster members	Deploy a search head cluster - Splunk Documentation
Initialize cluster members	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCdeploymentoverview
Integrate the search head cluster with an indexer cluster	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCandindexercluster
Integrate the search head cluster with an indexer cluster	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCandindexercluster
Manage app deployment across all peers	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Manageappdeployment
Role of the captain	Search head clustering architecture - Splunk Documentation
Set up the deployer	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/PropagateSHCconfigurationchanges
Use a load balancer with search head clustering	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/UseSHCwithloadbalancers
Use the deployer to distribute apps and configuration updates	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/PropagateSHCconfigurationchanges
Use the deployer to distribute apps and configuration updates	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/PropagateSHCconfigurationchanges
Using the deployer	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Using_the_deployer