Splunk4Admins

Clustering

splunk> a CISCO company

Forward-looking statements

This presentation may be deemed to contain forward-looking statements, which are subject to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995. Any statements that are not statements of historical fact (including statements containing the words “will,” “believes,” “plans,” “anticipates,” “expects,” “estimates,” “strives,” “goal,” “intends,” “may,” “endeavors,” “continues,” “projects,” “seeks,” or “targets,” or the negative of these terms or other comparable terminology, as well as similar expressions) should be considered to be forward-looking statements, although not all forward-looking statements contain these identifying words. Readers should not place undue reliance on these forward-looking statements, as these statements are management’s beliefs and assumptions, many of which, by their nature, are inherently uncertain, and outside of management’s control. Forward-looking statements may include statements regarding the expected benefits to Cisco, Splunk and their respective customers from the completed transaction, the integration of Splunk’s and Cisco’s complementary capabilities and products to create an end-to-end platform designed to unlock greater digital resilience for customers, our expectations regarding greater resiliency and better product outcomes, including for security and observability, plans for future investment, our development and use of AI and the role that our innovation plays as our customers adopt AI. Statements regarding future events are based on Cisco’s current expectations, estimates, and projections and are necessarily subject to associated risks related to, among other things, (i) the ability of Cisco to successfully integrate Splunk’s market opportunities, technology, personnel and operations and to achieve expected benefits, (ii) Cisco’s ability to implement its plans, forecasts and other expectations with respect to Splunk’s business and realize expected synergies, (iii) the outcome of any legal proceedings related to the transaction, (iv) the effects on the accounting relating to the acquisition of Splunk, (v) legislative, regulatory, and economic developments, (vi) general economic conditions, and (vii) the retention of key personnel. Therefore, actual results may differ materially and adversely from the anticipated results or outcomes indicated in any forward-looking statements. For information regarding other related risks, see the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the “Risk Factors” section of Splunk’s most recent reports on Form 10-Q filed with the SEC on February 20, 2024 and November 21, 2023, respectively. The parties undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

splunk>

Enroll in Today's Workshop

Tasks

1. Get a splunk.com account if you don't have one yet:
   https://splk.it/SignUp
2. Enroll in the Splunk Show workshop event:
   https://show.splunk.com/event/<eventID>
3. Download the hands-on lab guide:
   https://splk.it/S4A-CLU-Lab-Guide

   Contains step-by-step instructions for all of today's exercises!
4. Download a copy of today's slide deck:
   https://splk.it/S4A-CLU-Attendee

Goal

Enroll in today's event

Please introduce yourself!

- Name
- Company/organisation
- Role
- Are you currently using Splunk?
- What are you interested in using Splunk for?

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is a cluster?
  - Search head
  - Indexer
- What does clustering provide?
- Explore: Build an indexer cluster - Lab 1
- Explore: Push an app to indexer cluster members - Lab 2
- Explore: Build a search head cluster - Lab 3
- Explore: Push an app to search head cluster members - Lab 4
- Specifics regarding SHC KO push and replication
- Summary

Audience

Who is this Workshop for?

- Those who are interested in how to build and manage clusters in Splunk
  - Splunk Admins
  - “Required”: Power User Certified
  - “Preferred”: Splunk Admin enabled (at least started …), Certified

Expectations for Workshop

What are clusters?

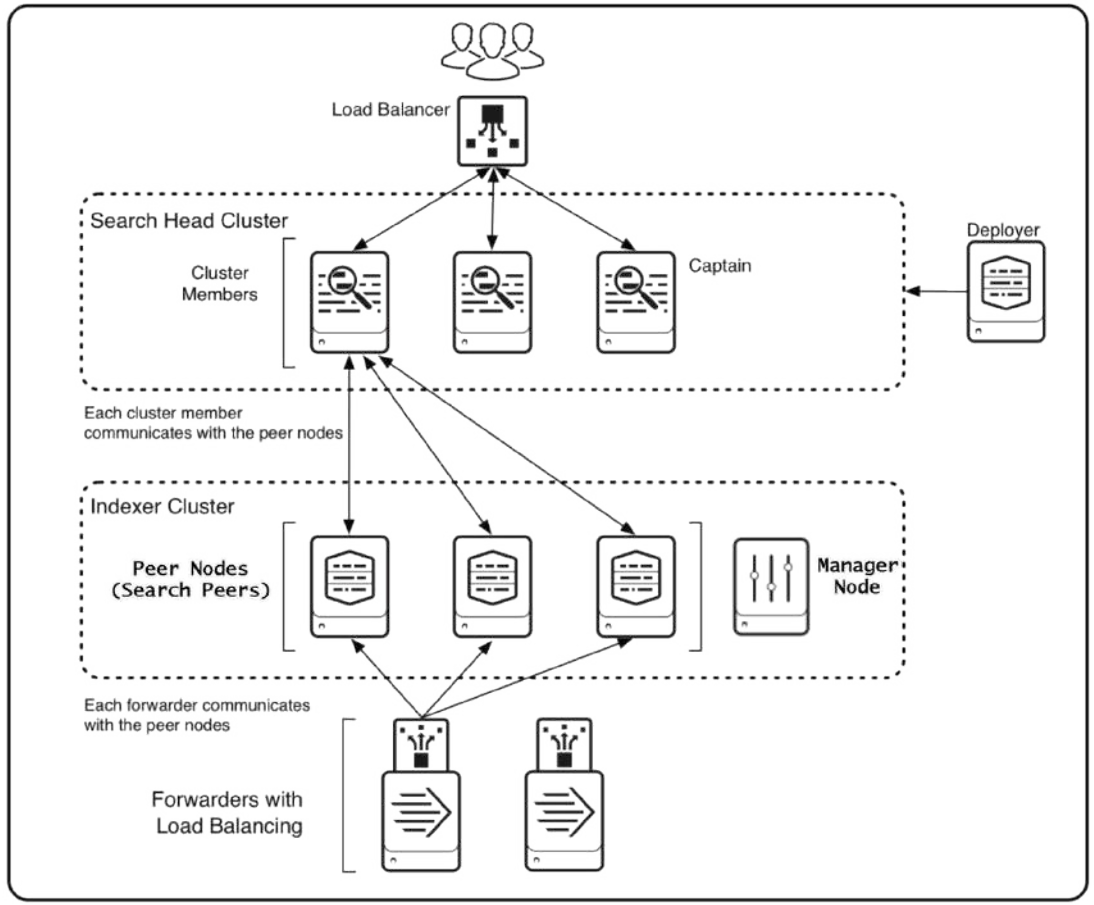
- Last roughly 90 - 120 minutes
- Experience setup and configuration of:
  - Indexer cluster
  - Search head cluster
- Push an app or TA out to:
  - Indexer cluster members
  - Search head cluster members
- Search head cluster: Discuss the differences in Knowledge Object (KO) replication vs. deployer pushes

What is a “cluster”?

- Discuss … what is a cluster?
- Indexer cluster
  - Cluster Manager (CM)
  - Indexers
- Search head cluster
  - Deployer
  - Captain + search head cluster members

Indexing and search architecture	https://lantern.splunk.com/Splunk_Success_Framework/Platform_Management/Indexing_and_search_architecture

What is a “cluster”?



Real production environment - at least three indexers, our lab only has two. Not representative of “real life”

Indexing and search architecture	https://lantern.splunk.com/Splunk_Success_Framework/Platform_Management/Indexing_and_search_architecture

What does clustering provide?

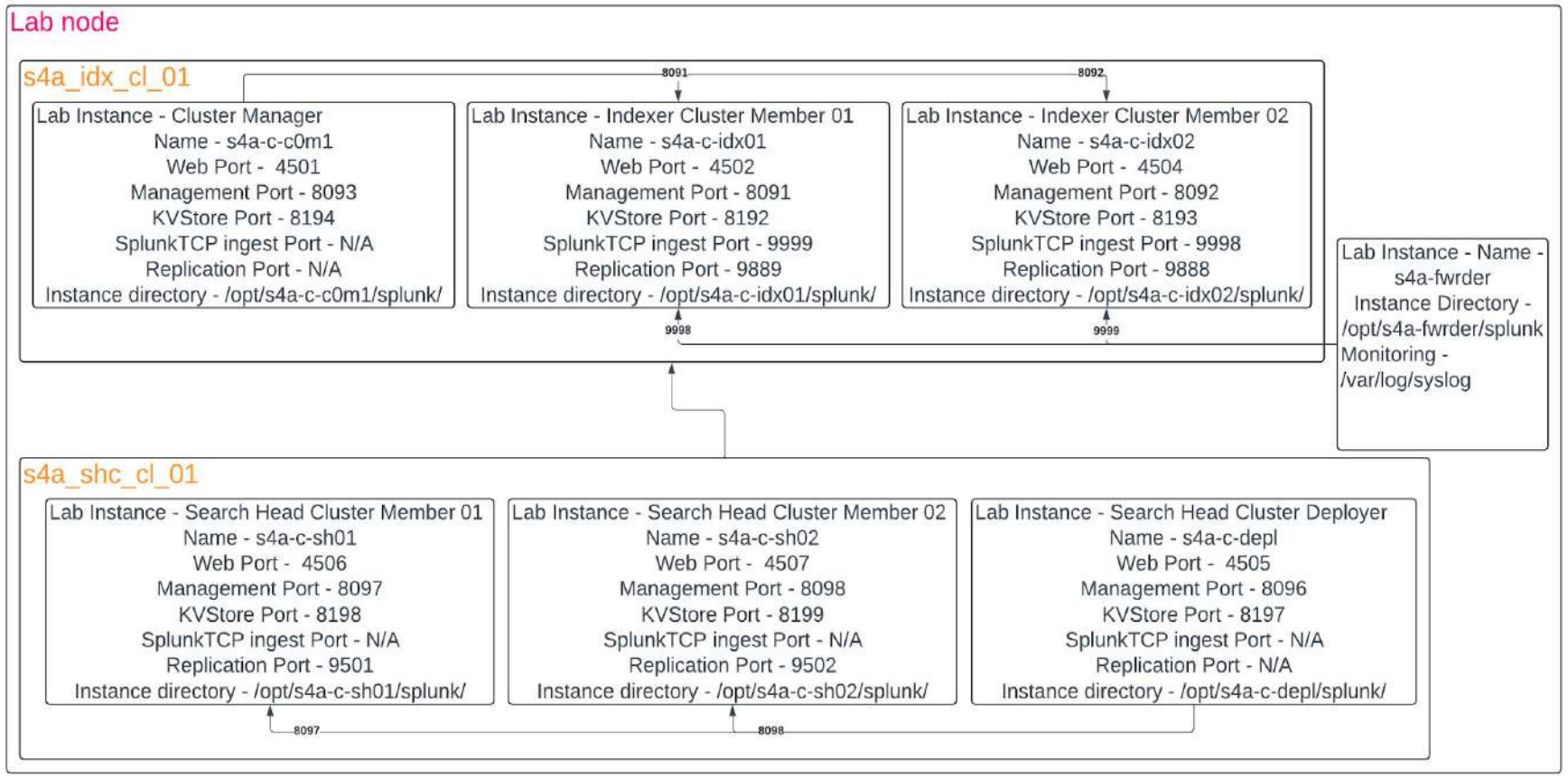
- Indexer cluster
  - Centralized management
  - Resilience (data is replicated among the members based on the replication- and search-factors defined, but not Disaster Recovery)
  - Performance - scale via parallelism provides and increased performance envelope
- Search head cluster
  - Centralized management
  - Resilience (load-balancer can act in front of cluster, KOs and user objects replicated quickly among members)
  - Performance - can scale via load-balancer “parallelism” provides increased performance envelope and scheduled search selection more evenly spreads the load

Workshop Agenda

- Discuss Who?|What?|Why?
- Expectations
- What is a cluster?
  - Search head
  - Indexer
- What does clustering provide?
- Explore: Build an indexer cluster - Lab 1
- Explore: Push an app to indexer cluster members - Lab 2
- Explore: Build a search head cluster - Lab 3
- Explore: Push an app to search head cluster members - Lab 4
- Specifics regarding SHC KO push and replication
- Summary

Build an indexer cluster

Virtual Machine Configuration



Lab node

- Lab prefix is 's4a-c-<task>'
- Universal login username :: "**splunk**"
- Universal login password :: "**5p1unk.conf**"
- Universal splunk pass4SymmKey = "**5p1unk.conf**"
- Directory for all apps/TAs employed - "/opt/s4a-cluster" - naming of apps/TAs should assist in which apps go where
- A universal forwarder pulling form the actual node's /var/log/syslog is running from /opt/s4a-fwrder
- Running Splunk Enterprise instances all start and execute as the user "splunk"
- Universal forwarder (to alleviate any issues regarding the access to /var/log/syslog) is running as "root"
- All network pathing uses 127.0.0.1:<appropriate_port>

Build an indexer cluster

Cluster Manager

- Requirements
  - Standard Splunk system requirements, but scale-up in the event that many indexers will be managed
- Few logins
  - Only admins, no standard user should ever login
  - Build an “admin” group on SSO/AD and ONLY that group has login privileges

System requirements and other deployment considerations for indexer clusters	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Systemrequirements
Indexer cluster deployment overview	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Clusterdeploymentoverview

Build an indexer cluster

Cluster Manager

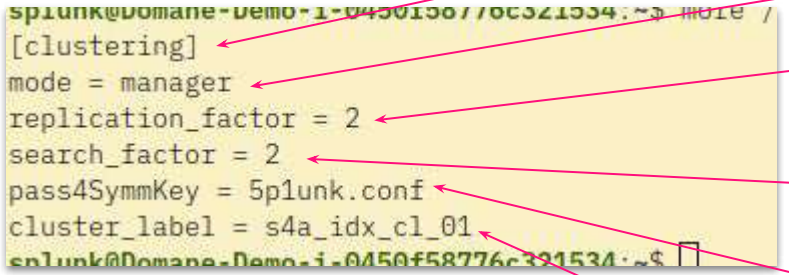
- Login to the node (using the password “5p1unk.conf”)
  - `ssh -p 2222 splunk@<<IP_address_of_node_from_your_SHOW_Lab_information>>`
- Move app to $SPLUNK_HOME/etc/apps
  - `cp -rp /opt/s4a-cluster/s4a_clustering_idx_build_c0m1 /opt/s4a-c-c0m1/splunk/etc/apps/`
- Review the file …
  - `more /opt/s4a-c-c0m1/splunk/etc/apps/s4a_clustering_idx_build_c0m1/local/server.conf`

Enable the indexer cluster manager node	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Enablethemanagernode
Configure the manager node with server.conf	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configuremanagerwithserverconf

Build an indexer cluster

Cluster Manager

- Review the file …
  - more /opt/s4a-c-c0m1/splunk/etc/apps/s4a_clustering_idx_build_c0m1/local/server.conf



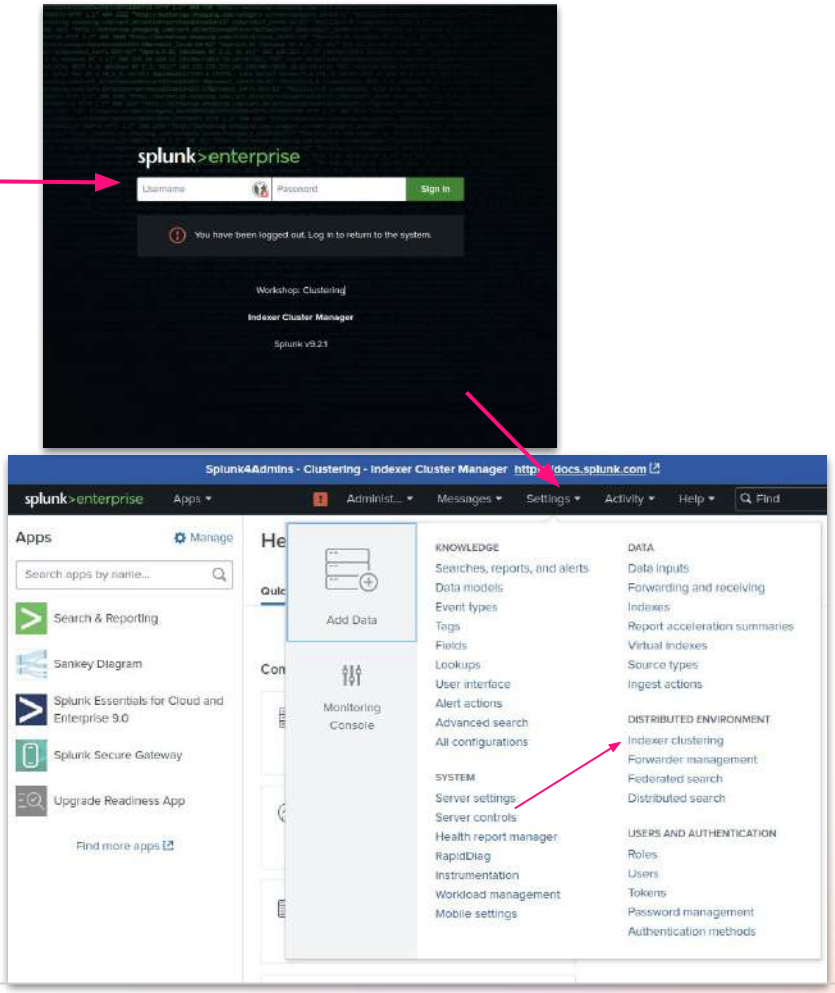
[clustering]	Defines the configuration set
mode = manager	Define the node as the CM
replication_factor = 2	Default number of copies expected to be created (can be index specific)
search_factor = 2	Default number of copies expected to be created for search (can be index specific)
pass4SymmKey = 5p1unk.conf	A “secret” key, will be encrypted at Splunkd startup, must be identical across cluster
cluster_label = s4a_idx_cl_01	A label, optional, but highly recommended. Ensures easier identification

Enable the indexer cluster manager node	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Enablethemanagernode
Configure the manager node with server.conf	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configuremanagerwithserverconf

Build an indexer cluster

Cluster Manager

- Restart splunk
  - `/opt/s4a-c-c0m1/splunk/bin/splunk restart`
- Log in to the CM Splunk instance …
  - https://<your_IP_address>:4501
  - username - “`admin`”, password - “`5p1unk.conf`”
- Click black bar “Settings->Indexer clustering”

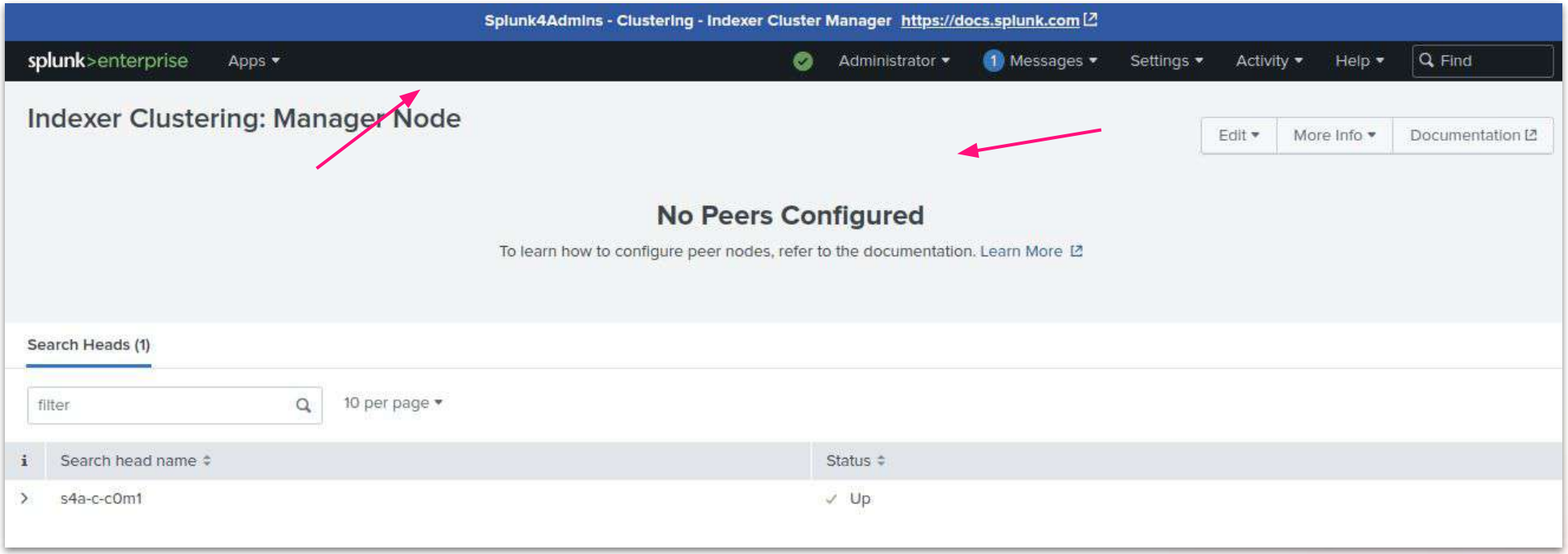


Enable the indexer cluster manager node	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Enablethemanagernode
Configure the manager node with server.conf	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configuremanagerwithserverconf

Build an indexer cluster

Cluster Manager

- Upon login, the page will now look like this



Enable the indexer cluster manager node	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Enablethemanagernode
Configure the manager node with server.conf	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configuremanagerwithserverconf

Build an indexer cluster

Connect node 01 to Cluster Manager

- Use the already existing terminal window to the node …
- Move app to the $SPLUNK_HOME/etc/apps directory
  - `cp -rp /opt/s4a-cluster/s4a_clustering_idx_build_member_idx01 /opt/s4a-c-idx01/splunk/etc/apps`
- Review the file …

```
[replication_port://9889]

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

Enable the peer nodes	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Enablethepeernodes
Peer node configuration overview	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configurethepeers
Configure peer nodes with server.conf	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configurepeerswithserverconf

Build an indexer cluster

Connect node 01 to Cluster Manager

- Review the file …
  - `more /opt/splunk/etc/s4a_clustering_idx_build_member_idx01/server.conf`

```
[replication_port://9889]

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

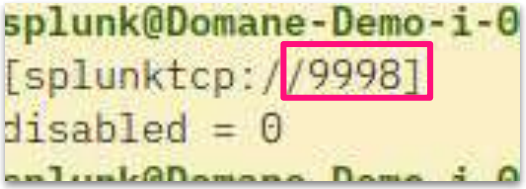
`[replication_port://9989]`	The port across which the indexers will send replication buckets
`[clustering]`	Defines the configuration set
`manager_uri = https://127.0.0.1:8089`	Defines the network address, port, and protocol of the node to which the indexer will connect to as the CM. Normally IP:8089
`mode = peer`	What sort of node will this be … and indexer (in Splunk-speak “peer”)
`pass4SymmKey = 5p1unk.conf`	A “secret” key, will be encrypted at Splunkd startup, must be identical across cluster

Enable the peer nodes	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Enablethepeernodes
Peer node configuration overview	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configurethepeers
Configure peer nodes with server.conf	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configurepeerswithserverconf

Build an indexer cluster

Connect node 01 to Cluster Manager

- Because this is a lab, slight difference in the inputs.conf per node
  - Copy the file
    - cp -rp /opt/s4a-cluster/s4a_clustering_idx01_receive /opt/s4a-c-idx01/splunk/etc/apps
    - more /opt/s4a-c-idx01/splunk/etc/apps/s4a_clustering_idx01_receive/local/inputs.conf



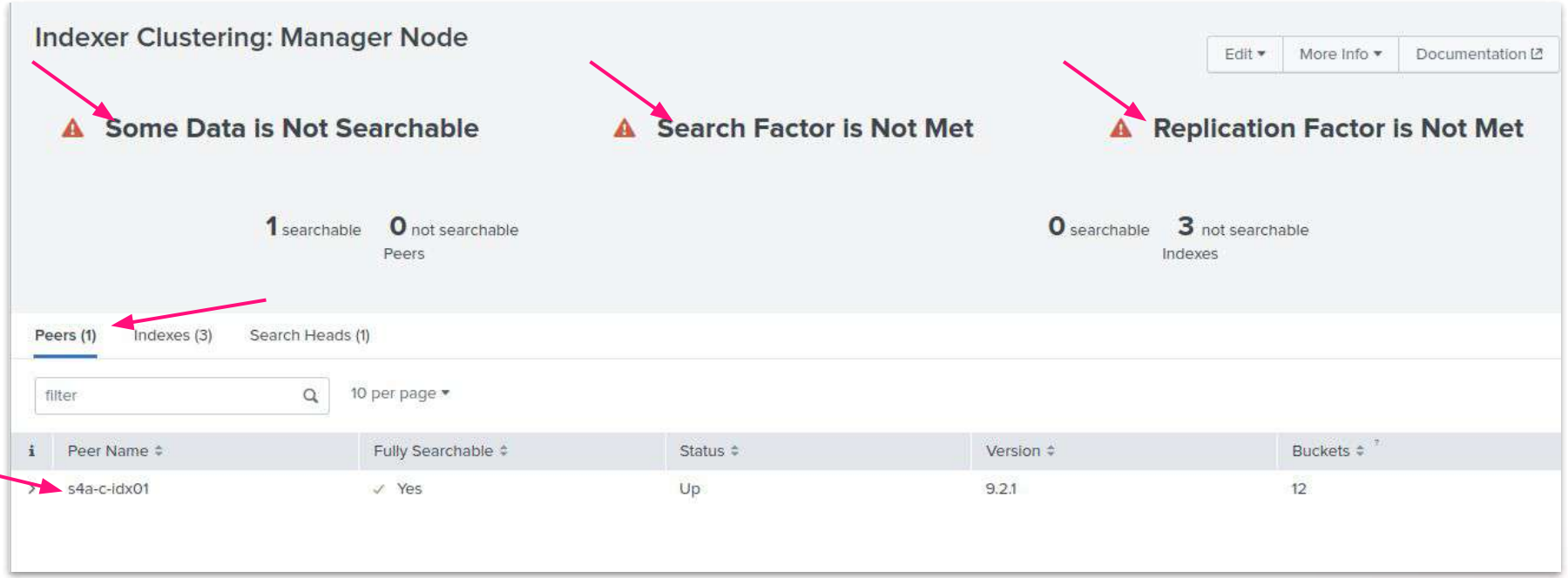
- Restart Splunk
  - `/opt/s4a-c-c0m1/splunk/bin/splunk restart`

Enable the peer nodes	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Enablethepeernodes
Peer node configuration overview	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configurethepeers
Configure peer nodes with server.conf	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configurepeerswithserverconf

Build an indexer cluster

Connect node to Cluster Manager

- Back at the “Settings->Indexer Clustering” GUI see …



Enable the peer nodes	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Enablethepeernodes
Peer node configuration overview	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configurethepeers
Configure peer nodes with server.conf	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configurepeerswithserverconf

Build an indexer cluster

Connect node 02 to Cluster Manager

- Use the already existing terminal window to the node …
- Execute the same sequence as before (with slight modifications) on the idx02 instance
  - cp -rp /opt/s4a-cluster/s4a_clustering_idx_build_member_idx02 /opt/s4a-c-idx02/splunk/etc/apps
  - cp -rp /opt/s4a-cluster/s4a_clustering_idx02_receive /opt/s4a-c-idx02/splunk/etc/apps
  - /opt/s4a-c-idx02/splunk/bin/splunk restart

```
[replication_port://9888]

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

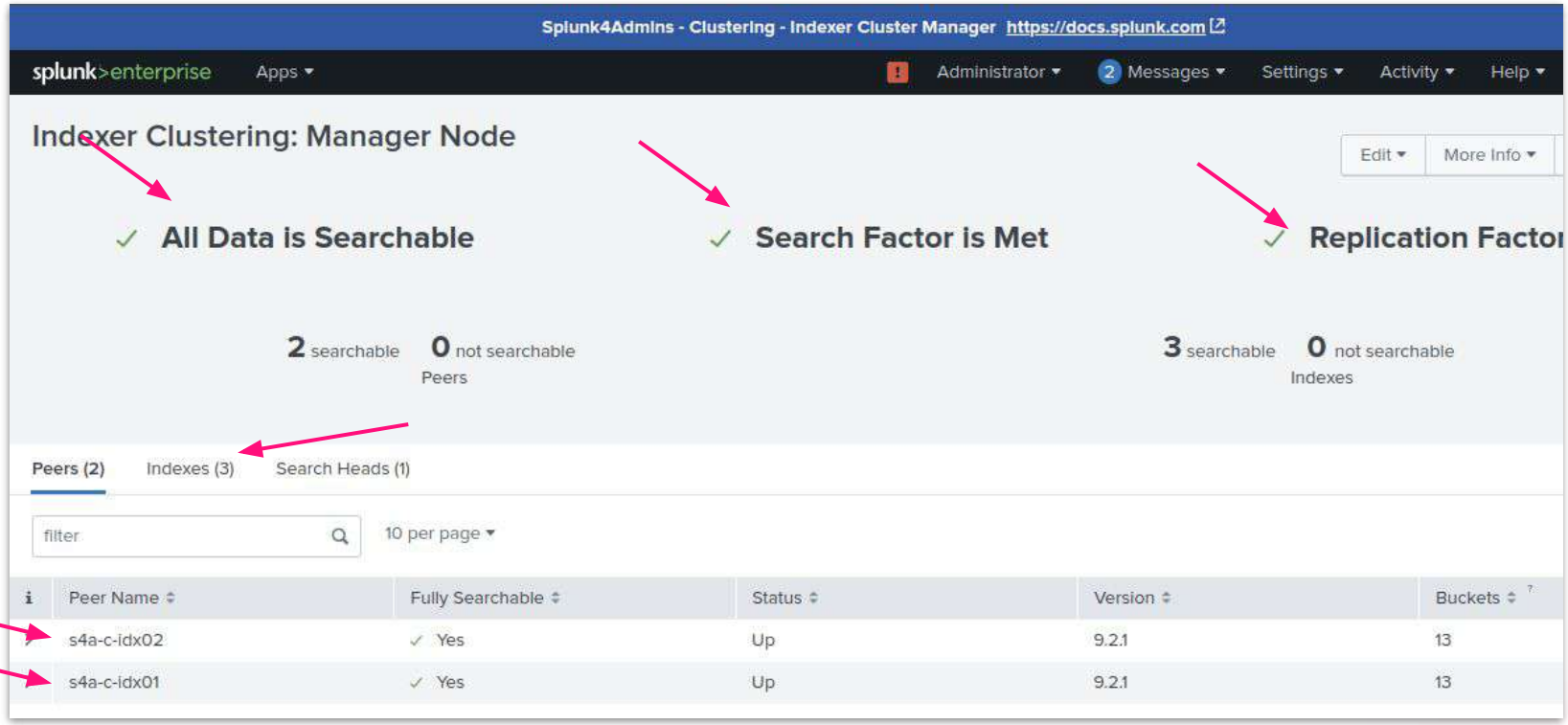
```
[splunktcp://9999]
disabled = 0
```

Enable the peer nodes	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Enablethepeernodes
Peer node configuration overview	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configurethepeers
Configure peer nodes with server.conf	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configurepeerswithserverconf

Build an indexer cluster

Connect node to Cluster Manager

- See …



Enable the peer nodes	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Enablethepeernodes
Peer node configuration overview	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configurethepeers
Configure peer nodes with server.conf	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configurepeerswithserverconf

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is a cluster?
  - Search head
  - Indexer
- What does clustering provide?
- Explore: Build an indexer cluster - Lab 1
- Explore: Push an app to indexer cluster members - Lab 2
- Explore: Build a search head cluster - Lab 3
- Explore: Push an app to search head cluster members - Lab 4
- Specifics regarding SHC KO push and replication
- Summary

Push apps to indexer cluster

Put apps in “manager-apps”

- Major purpose of indexer cluster is consistency across configurations
- Use the CM to “push” apps/TAs for indexing to indexers
- Push process determines whether a restart is required on the peers (indexers) and provides feedback
- If Splunkd restart required, the Cluster Manager will manage a rolling restart that will help reduce user disruption

Manage app deployment across all peers	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Manageappdeployment

Push apps to indexer cluster

Put apps in “manager-apps”

- “ssh” to the node `ssh -p 2222 splunk@<your_IP_address || password = 5p1unk.conf`
- Move app to the $SPLUNK_HOME/etc/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`
- Review the files …

Manage app deployment across all peers	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Manageappdeployment

Push apps to indexer cluster

Put apps in “manager-apps”

- Review the files … indexes.conf
  - more /opt/s4a-c-c0m1/splunk/etc/manager-apps/s4a_clustering_idx_push_to_members_indexes/local/indexes.conf

```
splunk@Domane-Demo-1-0450158776c321534:~$ 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
```

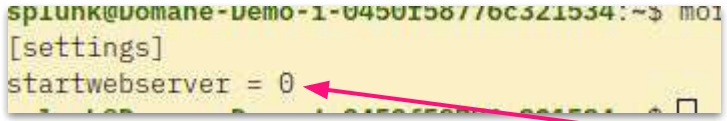
Configure volumes: name	A more effective and easier way to manage storage
Configure volumes: drive location	Where on the “drive” are the indexes to be stored
Configure volumes: total size	Maximum size for all indexes in volume, in megabytes
Define an index: disk location	Where to store the data - hot-warm-cold
Define an index: bucket size	How large should the buckets be permitted to be, indexes.conf.spec
Define an index: size	How large, in megabytes, should the index be permitted to grow
Define an index: freezing period	How long to keep on the “warm” storage until the bucket is moved to “cold”
Define an index: replicate	Should the index be replicated

indexes.conf.spec	https://docs.splunk.com/Documentation/Splunk/latest/Admin/Indexesconf

Push apps to indexer cluster

Put apps in “manager-apps”

- Review the files … web.conf
  - more /opt/s4a-c-c0m1/splunk/etc/manager-apps/s4a_clustering_idx_push_to_members_web/local/web.conf



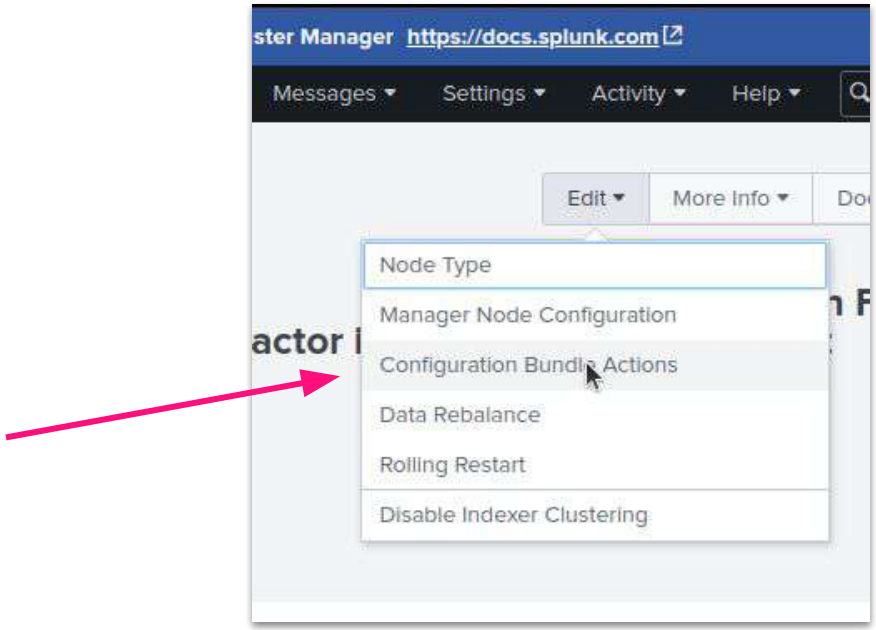
`startwebserver = 0`	Disable the web interface. Better to NOT have the GUI available. It helps ensure that only modifications to the apps/TAs on the indexers is done via the CM.

web.conf.spec	https://docs.splunk.com/Documentation/Splunk/latest/Admin/Webconf

Push apps to indexer cluster

Prepare to push the apps out

- At the CM black bar “settings”, “Indexer clustering”
- Select “Edit”, and “Configuration Bundle Actions”

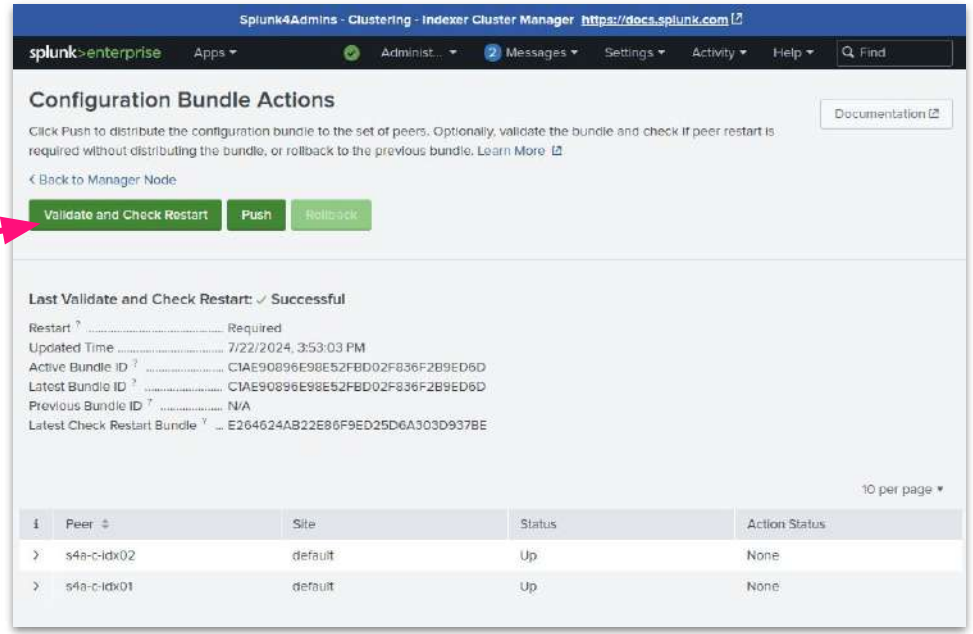


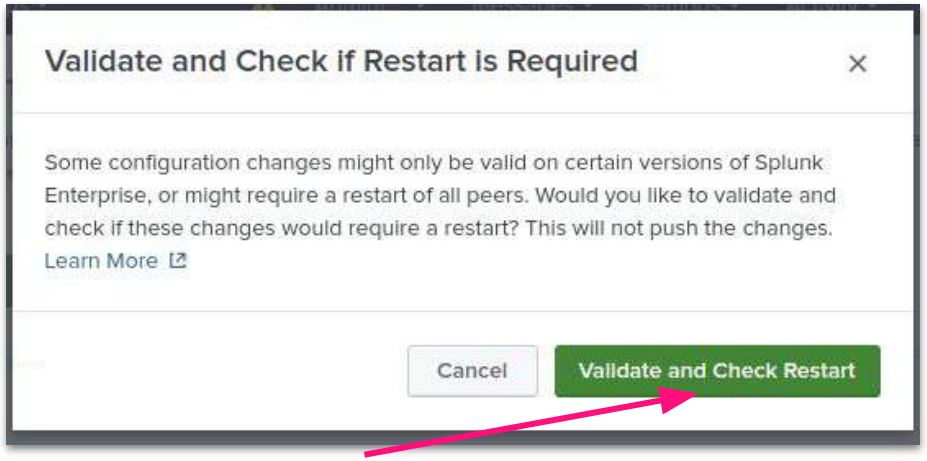
Use Splunk Web to validate the bundle and check restart	Update common peer configurations and apps - Splunk Documentation

Push apps to indexer cluster

Process to push apps

- See this page
- Select “Validate and Check Restart”



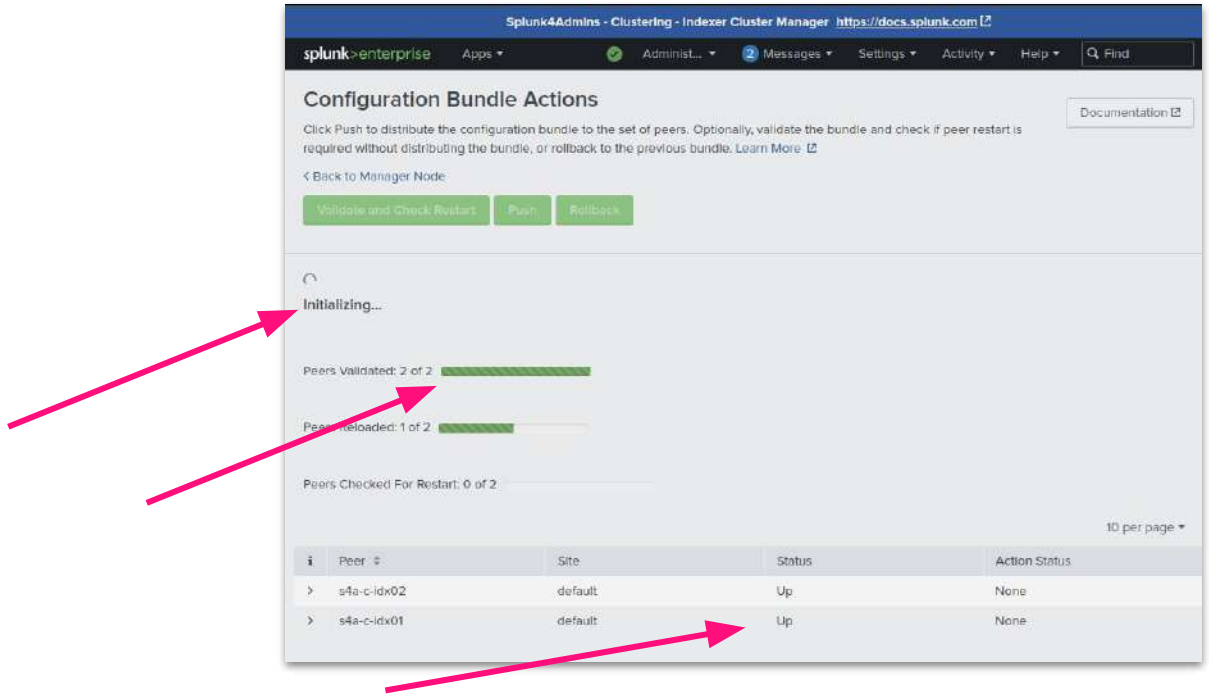


Use Splunk Web to validate the bundle and check restart	Update common peer configurations and apps - Splunk Documentation

Push apps to indexer cluster

Process to push apps

- During the validation …

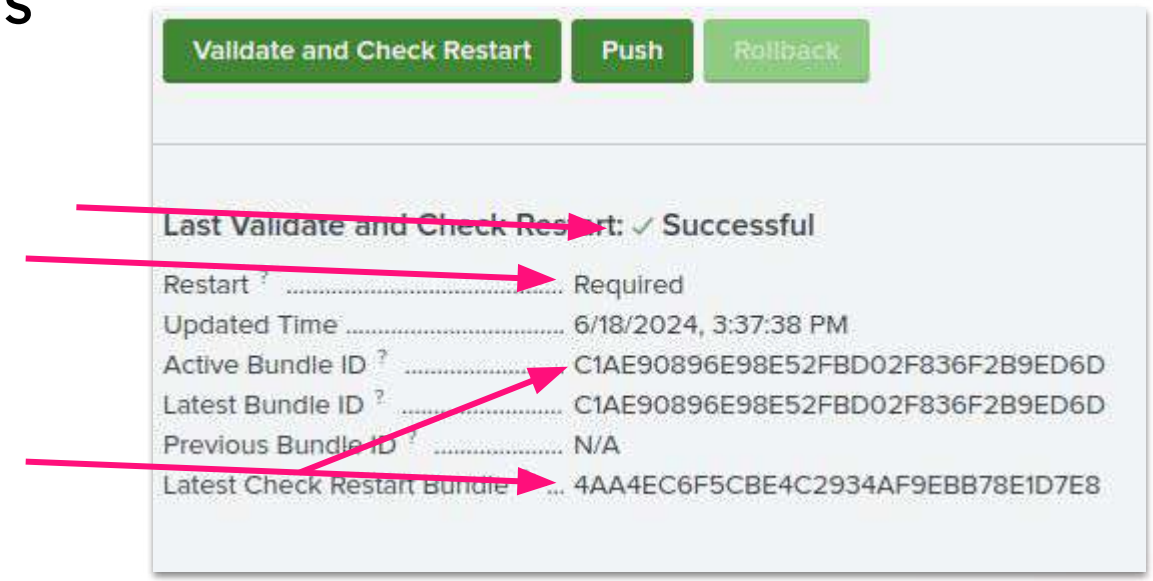


Use Splunk Web to validate the bundle and check restart	Update common peer configurations and apps - Splunk Documentation

Push apps to indexer cluster

Process to push apps

- See the check is successful
  - However - A restart is required, due to the changes (webserver stop)
  - Also, see the Bundle IDs

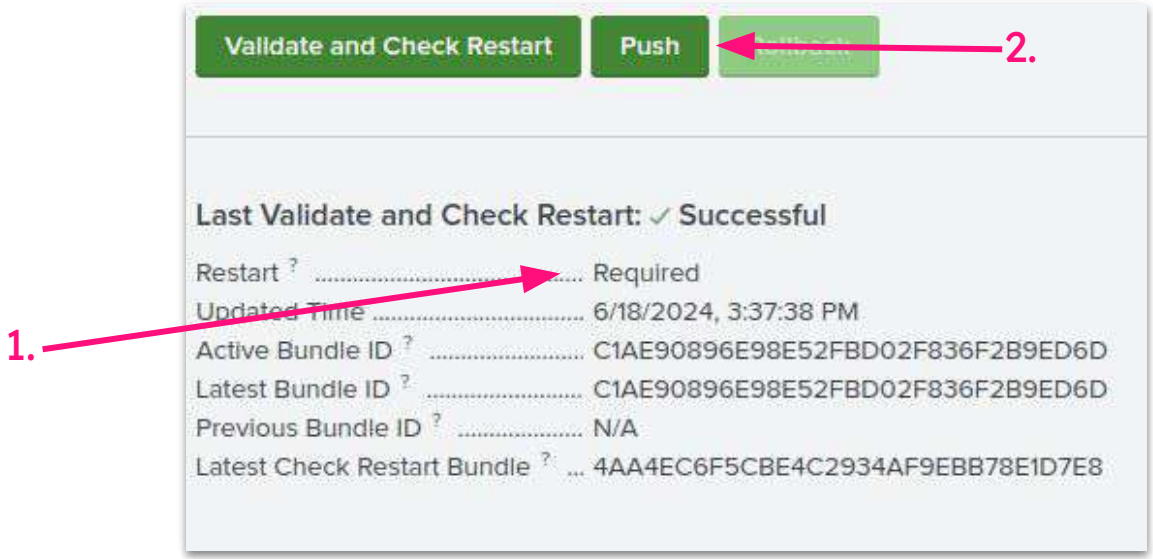


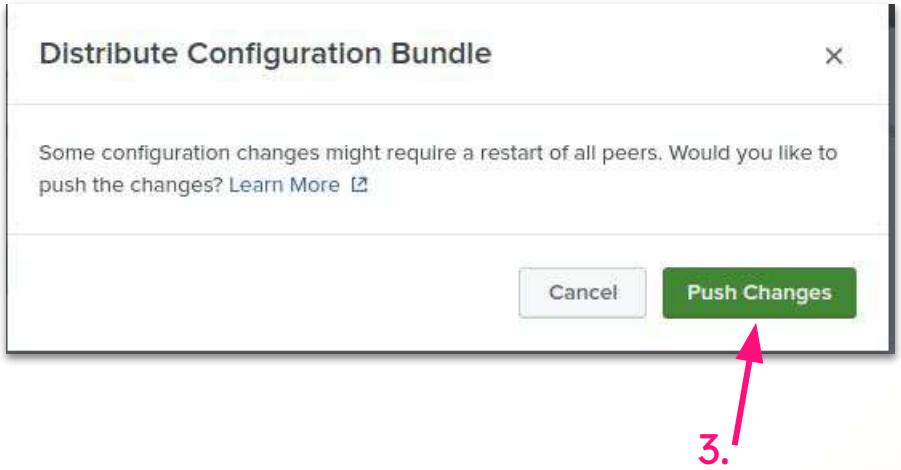
Use Splunk Web to validate the bundle and check restart	Update common peer configurations and apps - Splunk Documentation

Push apps to indexer cluster

Process to push apps

- See this page
- Select “Validate and Check Restart”



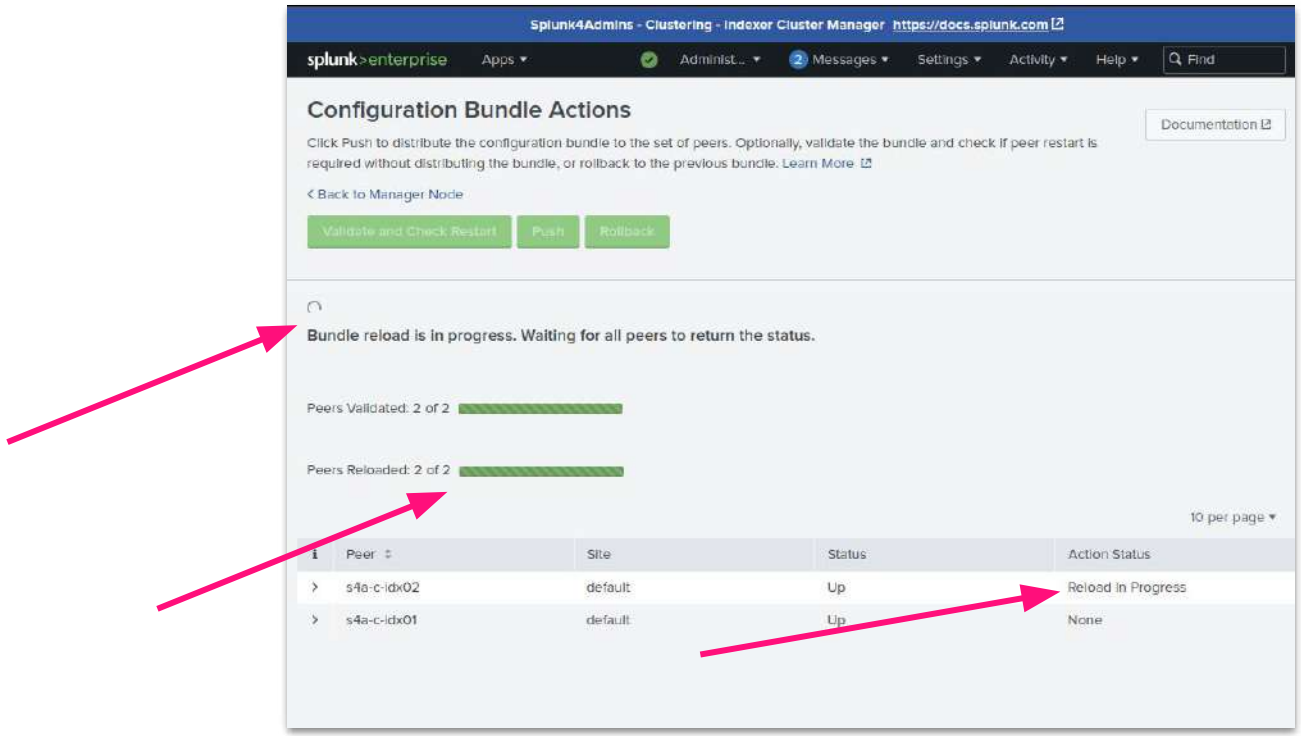


Use Splunk Web to apply the bundle	Update common peer configurations and apps - Splunk Documentation

Push apps to indexer cluster

Process to push apps

- Successful push

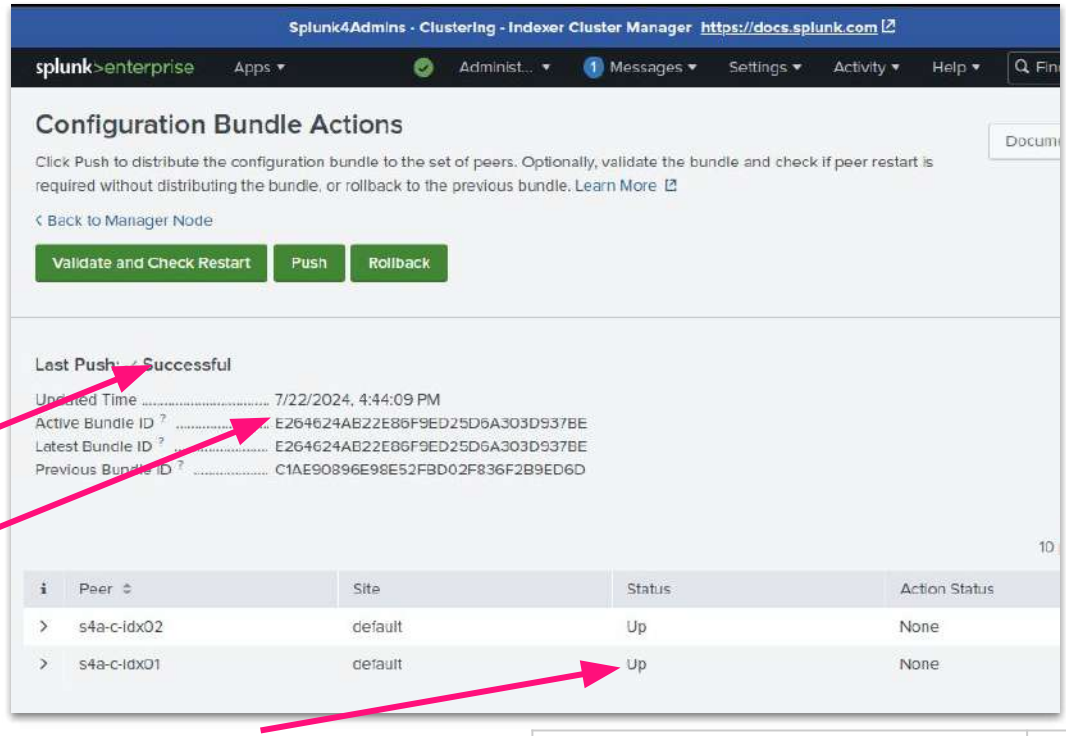


Use Splunk Web to apply the bundle	Update common peer configurations and apps - Splunk Documentation

Push apps to indexer cluster

Process to push apps

- Successful push



Use Splunk Web to apply the bundle	Update common peer configurations and apps - Splunk Documentation

Push apps to indexer cluster

Validate apps push

- Check the directories and files that have been pushed
- ‘ssh’ out to a cluster member `ssh -p 2222 splunk@<your_IP_address || password = 5p1unk.conf`
- Find the various apps, check that they have been deployed
  - `find /opt/s4a-c-idx0?/splunk/etc/peer-apps -name "s4a*" -lsa`
- Sending data to “linux” index, use search on CM to execute
  - `index = linux`
- Attempt to access the indexer nodes via GUI
  - `https://<your_indexer_01>:4502 - FAIL`

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is a cluster?
  - Search head
  - Indexer
- What does clustering provide?
- Explore: Build an indexer cluster - Lab 1
- Explore: Push an app to indexer cluster members - Lab 2
- Explore: Build a search head cluster - Lab 3
- Explore: Push an app to search head cluster members - Lab 4
- Specifics regarding SHC KO push and replication
- Summary

Build search head cluster

Description of a search head cluster

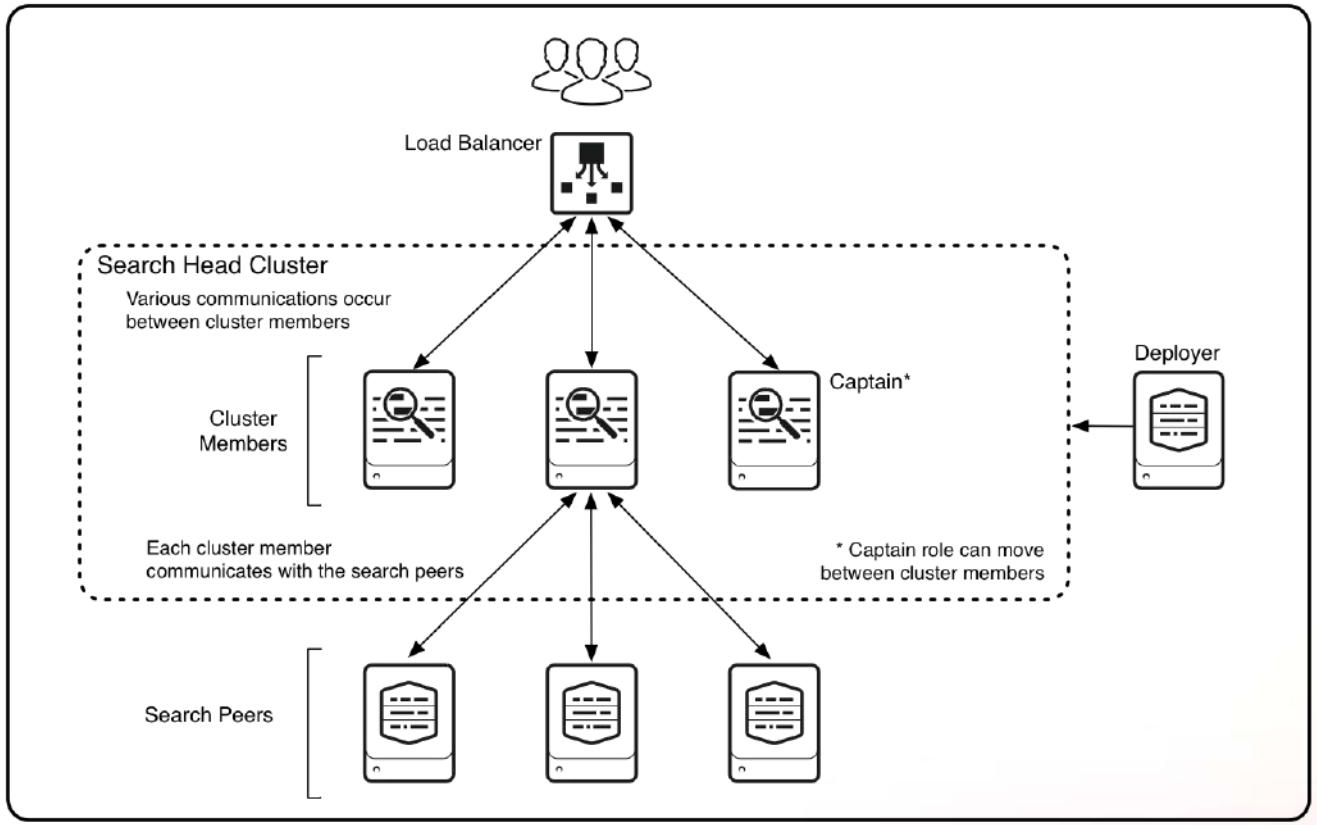
- A search head cluster (SHC) consists of
  - Deployer - the originating node of apps and user contexts, not actually part of the cluster!
  - Captain - the “organizer” of the cluster
  - Members - the worker nodes of the cluster
- Once deployed workers replicate Knowledge Objects (KO) among themselves
  - This is quick but not immediate
  - Includes runtime KOs such as user field extractions, saved searches, lookup tables, dashboards, and others

Deploy a search head cluster	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCdeploymentoverview
Using the deployer	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Using_the_deployer

Build search head cluster

Enterprise architecture - SHC

- A load balancer providing access to
- 3-node SHC with a Captain and 2 other members
- Three search peers (indexers) not necessarily in cluster - but should be …



Deploy a search head cluster	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCdeploymentoverview
System requirements for use of Splunk Enterprise on-premises	https://docs.splunk.com/Documentation/Splunk/latest/Installation/Systemrequirements
Using the deployer	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Using_the_deployer

Build search head cluster

Enable the deployer

- “ssh” to the deployer node `ssh -p 2222 splunk@<your_IP_address || password = 5p1unk.conf`
- Move app to the $SPLUNK_HOME/etc/apps directory
  - `cp -rp /opt/s4a-cluster/s4a_clustering_shc_build_deployer/ /opt/s4a-c-depl/splunk/etc/apps`
- Review the file …

Set up the deployer	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/PropagateSHCconfigurationchanges
Using the deployer	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Using_the_deployer

Build search head cluster

Enable the deployer

- Review the files … server.conf - ON THE DEPLOYER
  - more /opt/s4a-c-depl/splunk/etc/apps/s4a_clustering_shc_build_deployer/local/server.conf

```
[shclustering]
pass4SymmKey = 5p1unk.conf
shcluster_label = s4a_shc_cl_01
deployer_push_mode = full
```

[shclustering]	Define the section for configuration of search head clustering
pass4SymmKey = 5p1unk.conf	A “secret” key, will be encrypted at Splunkd startup, must be identical across cluster
shcluster_label = w-c-shc	Descriptive label that permits easier monitoring and management
deployer_push_mode = full	How are the pieces of the app pushed? Covered in more detail later …

```
[shclustering]
pass4SymmKey = $7$n0x+4nEOTgFXtJZwOfwb2RcJaaGovs5KymeoutPE1Hwtv2cCPNduybZjKw==
shcluster_label = s4a_shc_cl_01
deployer_push_mode = full
splunk@Domane-Demo-i-0450f58776c321534:/opt$
```

- Then restart the node
  - /opt/s4a-c-depl/splunk/bin/splunk restart

Set up the deployer	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/PropagateSHCconfigurationchanges
Using the deployer	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Using_the_deployer

Build search head cluster

Lab 3

Connect the members to each other and the deployer

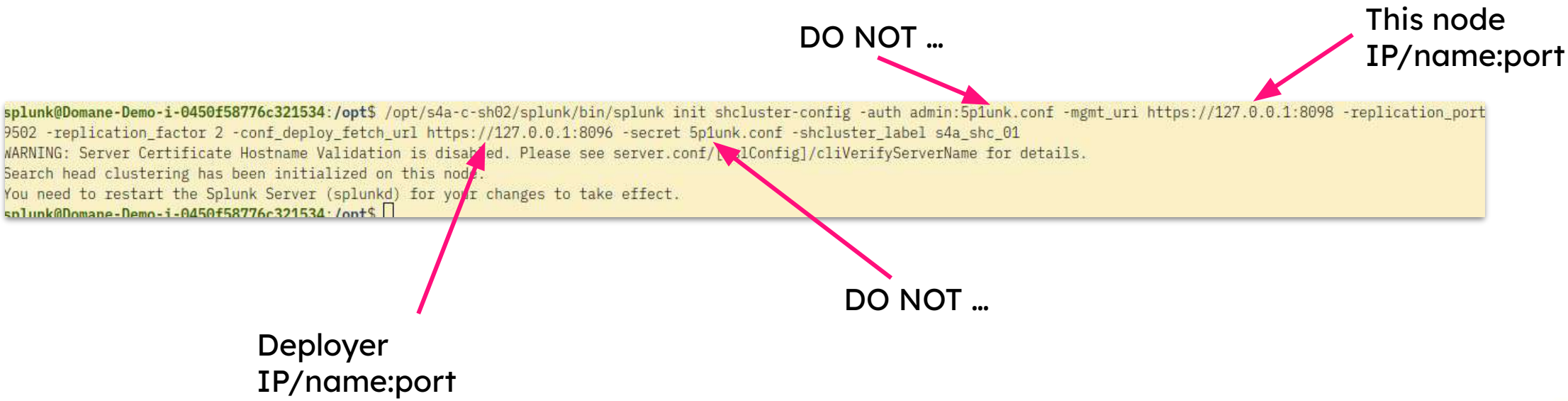
- On each new member -
- In /opt/s4a-c-sh01 and /opt/s4a-c-sh02
- Initialize the cluster member(s) - on each prospective member
  - `/opt/s4a-c-sh02/splunk/bin/splunk init shcluster-config -auth admin:5p1unk.conf -mgmt_uri https://127.0.0.1:8098 -replication_port 9502 -replication_factor 2 -conf_deploy_fetch_url https://127.0.0.1:8096 -secret 5p1unk.conf -shcluster_label s4a_shc_01`
- Restart Splunkd on the node
  - `/opt/s4a-c-sh01/splunk/bin/splunk restart ; splunk status`

Initialize cluster members	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCdeploymentoverview
Using the deployer	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Using_the_deployer

Build search head cluster

Connect the members to each other and the deployer

- Output of the previous slide's commands



Initialize cluster members	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCdeploymentoverview
Using the deployer	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Using_the_deployer

Build search head cluster

Connect the members to each other and the deployer

- Do the same ‘init’ command, on the other node, with the other node’s IP address - output in lab guide …
- Bootstrap the Captain
  - `/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`

This node IP/name

```
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.
```

The other node’s IP/name

DO NOT …

Bring up the cluster captain	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCdeploymentoverview
Initialize cluster members	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCdeploymentoverview
Using the deployer	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Using_the_deployer

Build search head cluster

Connect the members to each other and the deployer

- Check the SHC status …

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

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$
```

Check search head cluster status	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCdeploymentoverview
Using the deployer	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Using_the_deployer

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is a cluster?
  - Search head
  - Indexer
- What does clustering provide?
- Explore: Build an indexer cluster - Lab 1
- Explore: Push an app to indexer cluster members - Lab 2
- Explore: Build a search head cluster - Lab 3
- Explore: Deploy an app to search head cluster members - Lab 4
- Specifics regarding SHC KO push and replication
- Summary

Deploy an app to SHC members

Apps to push from the deployer

- Place apps on deployer
  - `tar -xf /opt/s4a-cluster/deployer_apps.tgz -C /opt/s4a-c-depl/splunk/etc/shcluster/apps/`
  - `ls /opt/splunk/etc/shcluster/apps`
    - Dashboard app - something to push, lots of really useful dashboards
    - DisableIndexandforward - stop local indexing and send everything to …
    - outputs - Indexer destination definition
    - s4a_clustering_shc_integrate_wiht_idxCluster - Integrate the SHC tightly with the already built indexer cluster

```
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$
```

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

Deploy an app to SHC members

Review the files

- … all_outputs
  - Define the group,send to the group

```
splunk@domane-demo-1-0450158776c321534:/opt$
[tcpout]
defaultGroup = s4a_ALL_destinations

[tcpout:s4a_ALL_destinations]
server=127.0.0.1:9999,127.0.0.1:9998
```

- … all_Disableandforward
  - Disable local indexing and provide selections to forward. Best Practice to ensure that internal logs are sent to the indexers

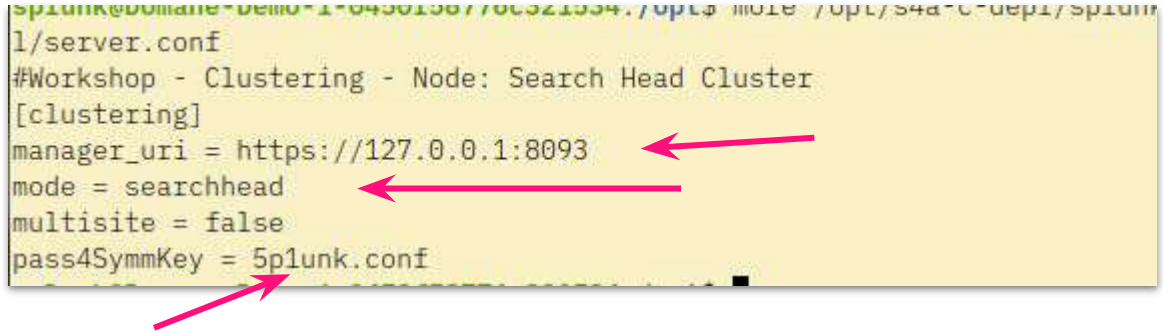
```
splunk@domane-demo-1-0450158776c321534:/opt$
# Turn off indexing on the search head
[indexAndForward]
index = false

[tcpout]
forwardedindex.0.whitelist = .*
# disable these
forwardedindex.1.blacklist =
forwardedindex.2.whitelist =
```

- SA_hywels_dashboards - A set of extremely useful dashboards that enhance monitoring

Build search head cluster

Integrate the SHC members with an indexer cluster

- Configure the SHC members to search an indexer cluster …
  - more /opt/s4a-c-depl/splunk/etc/shcluster/apps/s4a_clustering_shc_integrate_with_idxCluster/local/server.conf



DO NOT USE THIS AS A PASSWORD - LAB USE ONLY …

Integrate the search head cluster with an indexer cluster	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCandindexercluster
Using the deployer	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Using_the_deployer

Deploy an app to SHC members

Push the bundle

- 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

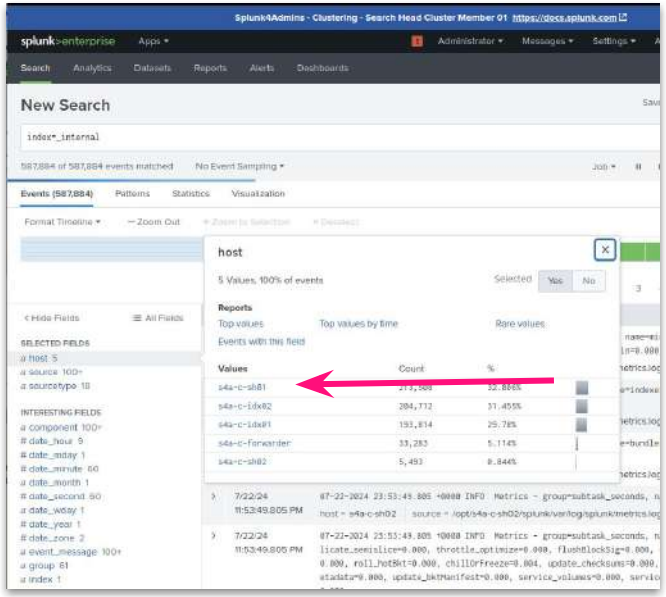
DO NOT USE THIS AS A PASSWORD - LAB USE ONLY …

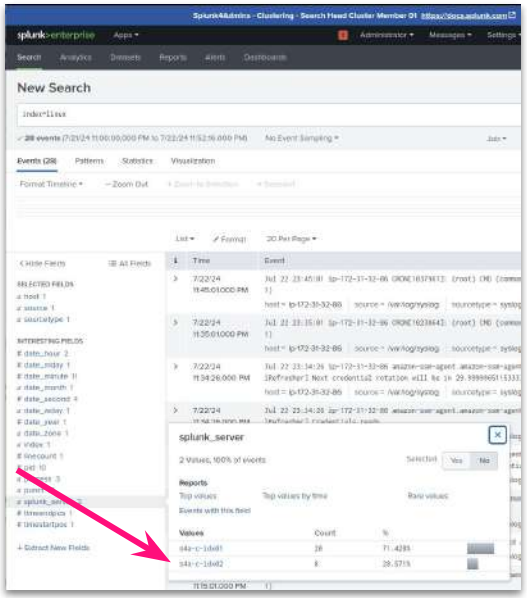
```
splunk@Domane-Demo-i-0450f58776c321534:/opt$ /opt/s4a-c-depl/splunk/bin/splunk apply shcluster-bundle -target https://127.0.0.1:8097 -auth ad
min:5p1unk.conf
 Warning: Depending on the configuration changes being pushed, this command might initiate a rolling restart of the cluster members.  Please
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$
```

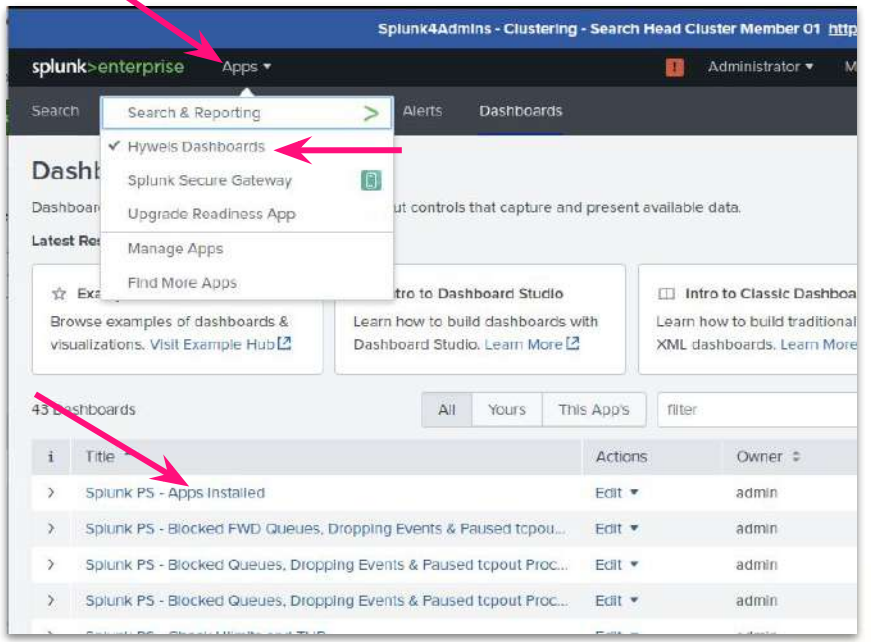
Deploy a configuration bundle	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/PropagateSHCconfigurationchanges
Using the deployer	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Using_the_deployer

Deploy an app to SHC members

Validate the push







Validate the push by searching for:

- index=_internal, see the indexers - validating the _internal forwarding
- index=linux, see the indexers, validating the forwarder sending data
- Select the Hywel's Dashboard app and see the new dashboards

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is a cluster?
  - Search head
  - Indexer
- What does clustering provide?
- Explore: Build an indexer cluster - Lab 1
- Explore: Push an app to indexer cluster members - Lab 2
- Explore: Build a search head cluster - Lab 3
- Explore: Deploy an app to search head cluster members - Lab 4
- Specifics regarding SHC KO push and replication
- Summary

SHC Bundle & KO Replication

Deployer “push” mode

- Determines how the deployer distributes the configuration bundle
  - full - everything pushed **as-is**, overwrites what is in place, but merges, with on-node existing taking precedence
  - local_only - only pushes local, merges into existing bundle on members, push for modifiable configurations, uses captain to replicate
  - default_only - overwrites ‘default’ and all non ‘local’ directories
  - merge_to_default (default configuration) - merges all ‘local’ settings into ‘default’ and sends the combined directory to the members. ‘local’ settings on deployer apps take precedence over ‘default’
  - System default and app-specific, all apps should be configured with “push” mode
  - Parallel push - “`deployerPushThreads`” setting in deployer’s `server.conf - auto`

Deploy a search head cluster	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCdeploymentoverview
Using the deployer	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Using_the_deployer

SHC Bundle & KO Replication

Captain election

- Captain is necessary
  - schedules jobs, coordinate alerts, KO push, artifact replication, conf updates
  - RAFT election
    - Keep one node out of search (load-balancer, in ad hoc) to ensures election
- There can be only one …
  - Initially manually set, but afterwards, elected

Role of the captain	Search head clustering architecture - Splunk Documentation

SHC Bundle & KO Replication

Knowledge Object replication

- Captain replicates
  - Ensures that sufficient search replications are occurring, coordinates loss of node to ensure adequate copies
  - Captain replicates deployer ‘local’
- Artifact replication and proxy
  - SHC does not cluster KOs from ‘ad hoc’ or scheduled real-time
  - If a member requires an artifact from scheduled saved search, will retrieve from a member that has it
- Distribution of configuration changes
  - Replicated changes - dashboards, KV store, lookup files, others, automatically replicated among the members
  - Deployed changes - from the deployer (‘local’ via the Captain)

How the cluster handles search artifact	Search head clustering architecture - Splunk Documentation
Configuration updates that the cluster replicates	Configuration updates that the cluster replicates - Splunk Documentation

SHC Bundle & KO Replication

"User" management

- authentication.conf (default) and authorize.conf (local) replicated from deployer initially
- authorization (roles) managed by admin and replicated by standard cluster replication or only pushed from deployer - DO NOT MIX
- KOs should be pushed entirely in local during a migration, and then replicated via standard cluster replication afterward

How the cluster handles search artifact	Search head clustering architecture - Splunk Documentation
Configuration updates that the cluster replicates	Configuration updates that the cluster replicates - Splunk Documentation

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is a cluster?
  - Search head
  - Indexer
- What does clustering provide?
- Explore: Build an indexer cluster - Lab 1
- Explore: Push an app to indexer cluster members - Lab 2
- Explore: Build a search head cluster - Lab 3
- Explore: Deploy an app to search head cluster members - Lab 4
- Specifics regarding SHC KO push and replication
- Summary

Summary

Indexer cluster and search head clustering

- Built an indexer cluster
  - Created CM
  - Connected indexers to CM
  - Pushed apps to provide “baseline” cluster
- Built a search head cluster
  - Created deployer
  - Connected SHC members, and connected to indexer cluster
  - Pushed apps (beware of “push mode”)
  - Validated with search
- Be aware of Best Practices to ensure easier scaling

Links

System requirements for use of Splunk Enterprise on-premises	https://docs.splunk.com/Documentation/Splunk/latest/Installation/Systemrequirements
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	Update common peer configurations and apps - Splunk Documentation
Use Splunk Web to validate the bundle and check restart	Update common peer configurations and apps - Splunk Documentation
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
Indexing and search architecture	https://lantern.splunk.com/Splunk_Success_Framework/Platform_Management/Indexing_and_search_architecture

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	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
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

Thank you

splunk> a CISCO company