Splunk Setup Guide: Deployment Server, Cluster Master, and Deployer

1. Setting up the Deployment Server

The deployment server is used to distribute configurations to forwarders and other Splunk instances.

Steps to Set Up Deployment Server:

1. Enable Deployment Server:

- On the instance you want to make a deployment server, go to Settings > Forwarder Management in Splunk Web.
- Alternatively, use the command line:

```
splunk enable deploy-server
```

2. Create Deployment Apps:

- Configuration files and apps to be distributed are organized into folders called deployment apps.
- Create these apps in the $SPLUNK_HOME/etc/deployment-apps/ directory. Each app should have its configuration files (e.g., inputs.conf, outputs.conf).

3. Define Server Classes:

- A server class defines which clients receive specific apps.
- Go to Forwarder Management in Splunk Web, and create a server class by specifying which deployment clients will receive which deployment apps.
- Assign apps to server classes and map them to deployment clients.

Configuration Files:

- Serverclass.conf: This file is used to define server classes and client mappings.

  Location: $SPLUNK_HOME/etc/system/local/serverclass.conf

Example:

```
[serverClass:forwarders]

whitelist.0 = *

[serverClass:forwarders:app:my_app]
```

2. Setting up the Cluster Master

The cluster master manages an indexer cluster, ensuring data redundancy and high availability.

Steps to Set Up Cluster Master:

1. Set Up the Cluster Master:

   - On the instance that you want to make a cluster master, edit the configuration file:

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

Example:

```
[clustering]

mode = master

replication_factor = 3

search_factor = 2

pass4SymmKey = <shared_secret_key>
```

2. Configure Indexer Nodes (Peers):

   - On each indexer, edit the server.conf file to join the cluster.

Example:

```
[clustering]

mode = slave
```

```
master_uri = https://<cluster_master>:8089

pass4SymmKey = <shared_secret_key>
```

3. Validate the Cluster:

- Use Splunk Web on the cluster master to monitor the indexer cluster status and verify that all nodes have joined properly.

Configuration Files:

- Server.conf: This file is essential to set up cluster configurations.

  Relevant Section: [clustering] block.

3. Setting up the Deployer

The deployer manages configuration updates for search head clusters.

Steps to Set Up Deployer:

1. Create Search Head Cluster Apps:

- Create the configurations and apps you want to distribute in $SPLUNK_HOME/etc/shcluster/apps/.

2. Deploy Apps to Search Head Cluster Members:

- Use the following command from the deployer instance to push the configurations:

```
splunk apply shcluster-bundle -target https://<search_head>:8089 -auth <username>:<password>
```

3. Configure Search Head Cluster Members:

- On each search head member, modify the server.conf to join the cluster.

Example:

```
[shclustering]

pass4SymmKey = <shared_secret_key>

mgmt_uri = https://<search_head>:8089
```

Configuration Files:

- Server.conf: Used to define search head cluster settings.

  Relevant Section: [shclustering] block.

- Apps Directory: Store the apps that need to be pushed to search head cluster members in $SPLUNK_HOME/etc/shcluster/apps/.

Summary of Configuration Files and Directories

1. Deployment Server:

   - Serverclass.conf ($SPLUNK_HOME/etc/system/local/): Defines server classes and app distribution rules.

   - Deployment Apps Directory ($SPLUNK_HOME/etc/deployment-apps/): Contains the configurations to distribute.

2. Cluster Master:

   - Server.conf ($SPLUNK_HOME/etc/system/local/): Set [clustering] mode to master and configure replication and search factors.

3. Deployer:

   - Server.conf ($SPLUNK_HOME/etc/system/local/): Set [shclustering] mode for search head cluster members.

   - Search Head Cluster Apps Directory ($SPLUNK_HOME/etc/shcluster/apps/): Contains the app bundles to deploy.