Day - 4

27 March 2025 09:42

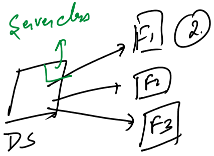
1. Clustes :-

① Deployment Serve.

② Cluster Master.

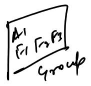
③ Deployer

① Deployment Server:-



① Mange the health of forwarde

② Push the app/config. from DS to the forwarder via Serverclass



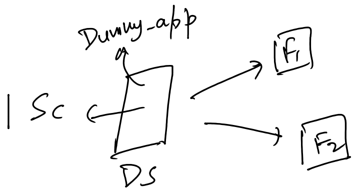
Serverclass → group the App & the forwarders.

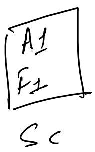
Lab:-

1. 3 Servers :-
   1 — Deployment Server. (Splunk Enterprise)
   Other 2 → Universal forwarder. (Splunk UF)
   Initialize the DS.
2. Connect the DS with UF → Deploy sample App. on the DS
3. Create the Serverclass on the DS.
4. Push the changes to the forwarder.
5. Make some modification on the existing App
6. Configuration file & CLI Command.
7. Trouble shooting.

Splunk/etc/deployment-app → where you deploy any app that is meant to be pushed to UF.

↳ folder location





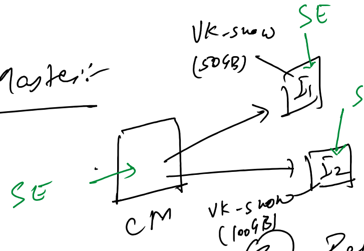
Configuration file → deployment clients.conf

Universal forwarder

(splunk/etc/system/local/ __)

Splunkd.log → (splunk/var/log/~~Splunk~~/splunkd.log)

② Cluster Master:-



① Mange health of indexer.

② Push config/app to the indexer.

③ Replication of data

① DS → CM =

(SE) (SE)

(SF)

(1) DS → CM =
(SE) (SE)

(2) (UF) (SE)
UF1 → I1
UF2 → I2

(3) Initialize DS Server to act as Cluster Master.
(4) Connect the Indexers with CM
(5) Deploy Dummy app on the CM & we will push it.
Pushing work bundle wise.
(6) All feature like rolling restart
(7)
(8) Config file → servers.conf & CLI Command
(9) Troubleshooting.

Deploy the App.

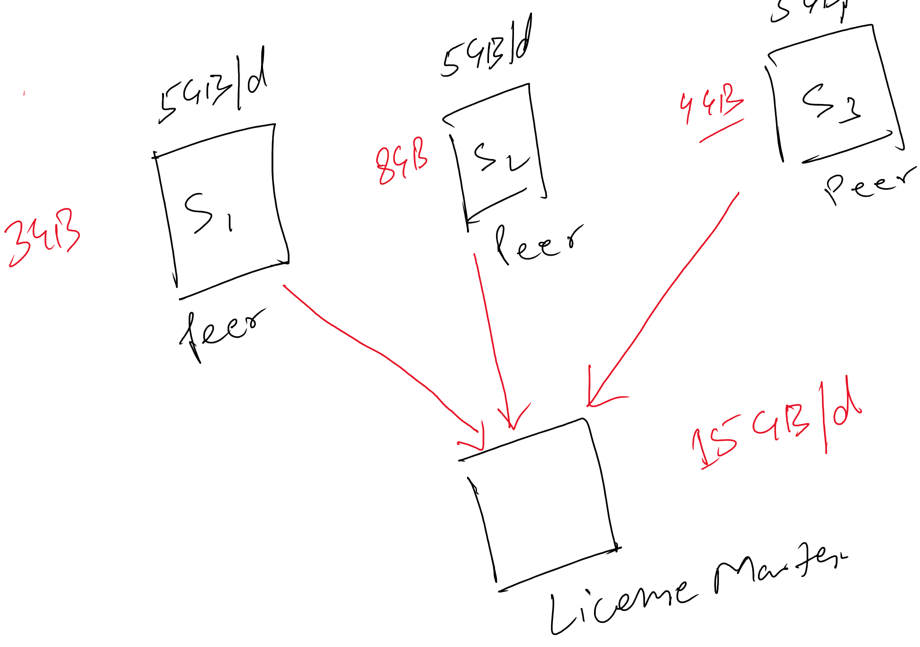
App location → splunk/etc/master app

(3) License Management:-

(1) Trial license – 60 day
500 MB / day

(2) Free license – 500 MB/d → Realtime, User & Role, cluster, Authentication, DM & Pivot, Acceleration } Can't do

(3) Enterprise license – Pay → Per GB/day → 1 year



S1+S2+S3 ≯ 15GB

(1) Flexibility

(2) cheaper cost

(3) Management of

license

Splunk / etc/ license → Folder where you save

license file.

the