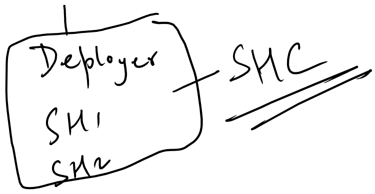
Day - 5

10 October 2025 09:40

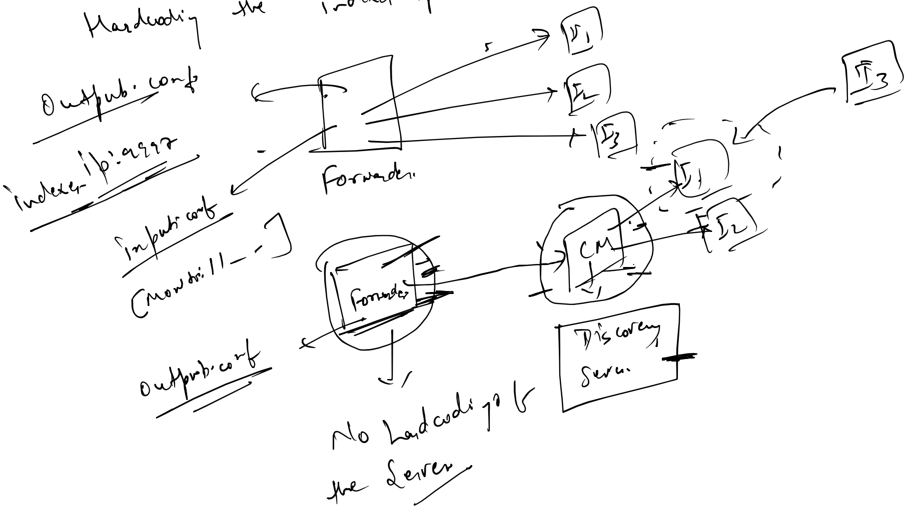
1. Search Head clustering.
2. Config file.
3. Connect SHC with indexer cluster. — 3 servers
4. Smartstore
5. Indexer discovery.
6. Multisite
7. Monitoring Console.
8. Splunk Application.



Config

1. inputs.conf — Monitor stanza
2. outputs.conf — connect with indexer
3. props.conf — Rule for sourcetype
4. transforms.conf — Regex (Index)
5. Deploymentclient.conf — Deploy users
6. servers.conf — [shclustering], [clustering], [Discovery]

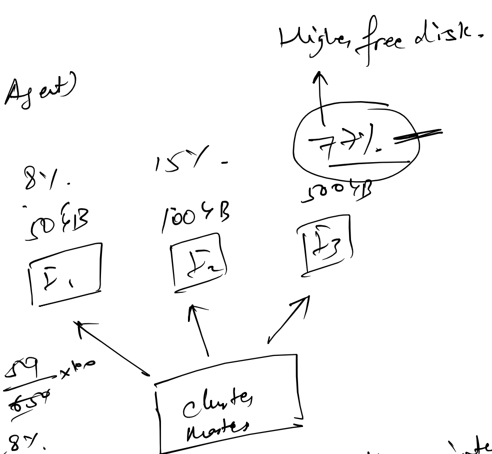
1. Indexer Discovery:- It will allow the forwarder to automatically discover & send data to the available indexers in a indexer cluster w/o Hardcoding the indexer ip address or host name.



1. 4 Servers.
2. All the 4 servers, we will install the splunk Enterprise.
3. First 3 Servers, Indexer clustering.
4. Server1 → CM, Server2 → I1, Server3 → I2
5. Server4 → HF
6. HF with cluster Master (Discovery Agent)

polling_rate = 10

indexerWeightByDiskCapacity = true



$$\frac{50}{50+100+500} = \frac{1}{13} \times 100 = 8\%$$

Pooling Rate

$$\left(\frac{\text{No. of forwarders}}{\text{polling\_rate}} + 30 \text{ sec}\right) * 1000 = \text{Polling interval in milliseconds}$$

polling_rate → 10

$$\left(\frac{1}{10} + 30\right) * 1000 = 30000\text{ms or } 30 \text{ sec.}$$

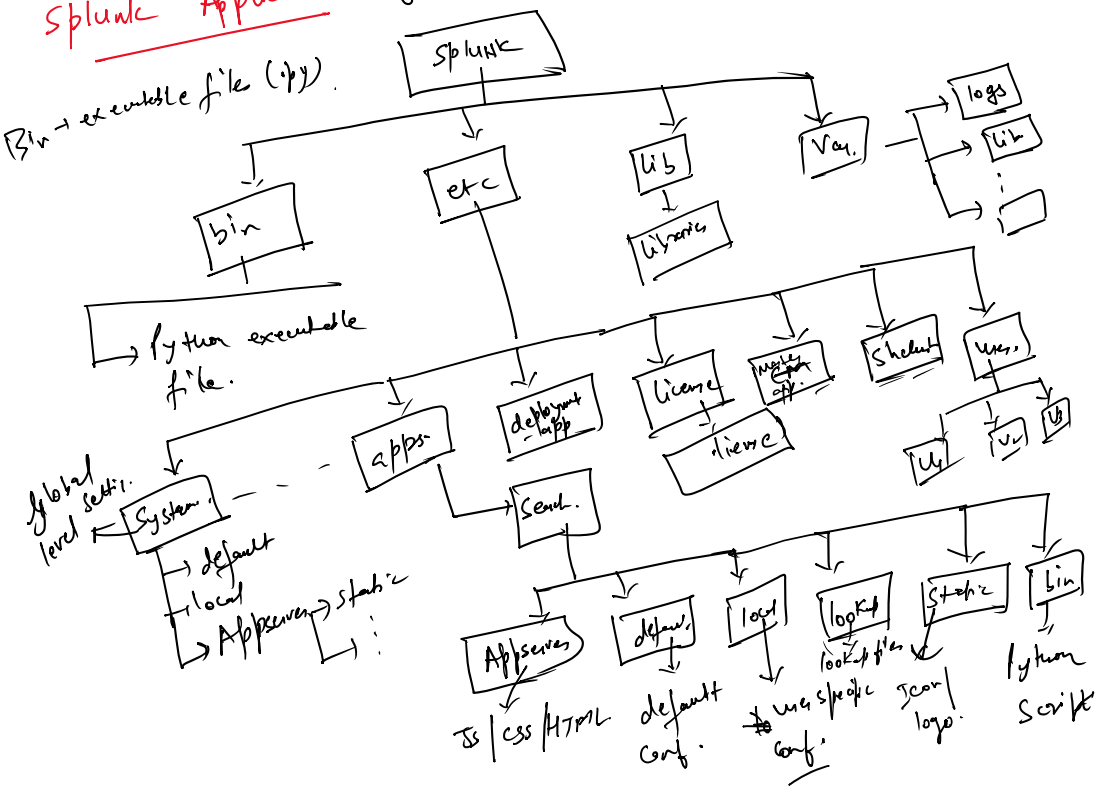
10 ✓

$\left(\frac{1}{10} + 30\right) * 1000 = \sim$

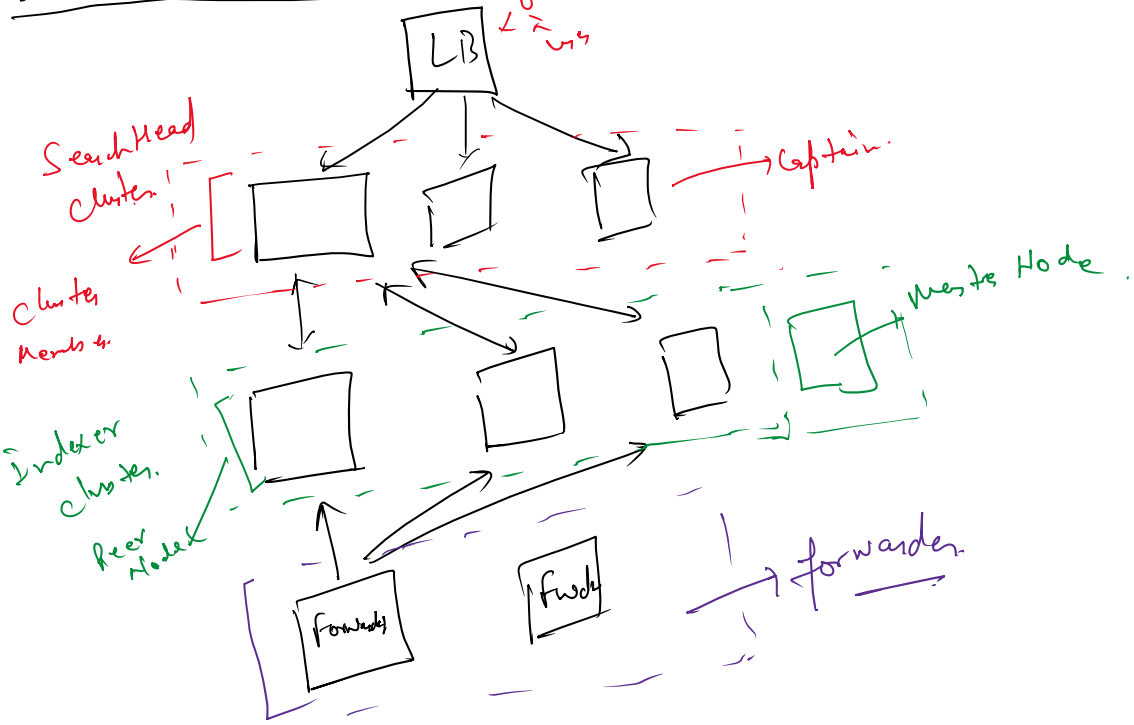
HF:- Outputs.conf

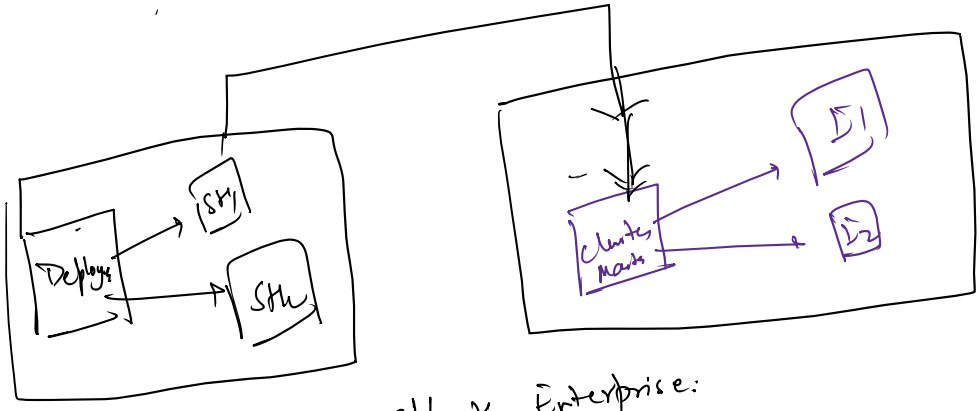
Splunk Application:- file & directory structure is pre defined.

Bin → executable file (.py).



Indexer cluster with SH cluster:-





1. 3 New Server – Splunk Enterprise:
2. Server 1 → Deployer.
3. Server 2, Server 3 → SH.
4. Captain election among SH1, SH2
5. Configure each member of SH in the indexer clustering.

Monitoring Console:- DMC (Distributed Monitoring Console)

Centralized dashboard – Monitor the Health, performance, & configuration of your entire splunk deployment.

Purpose:-

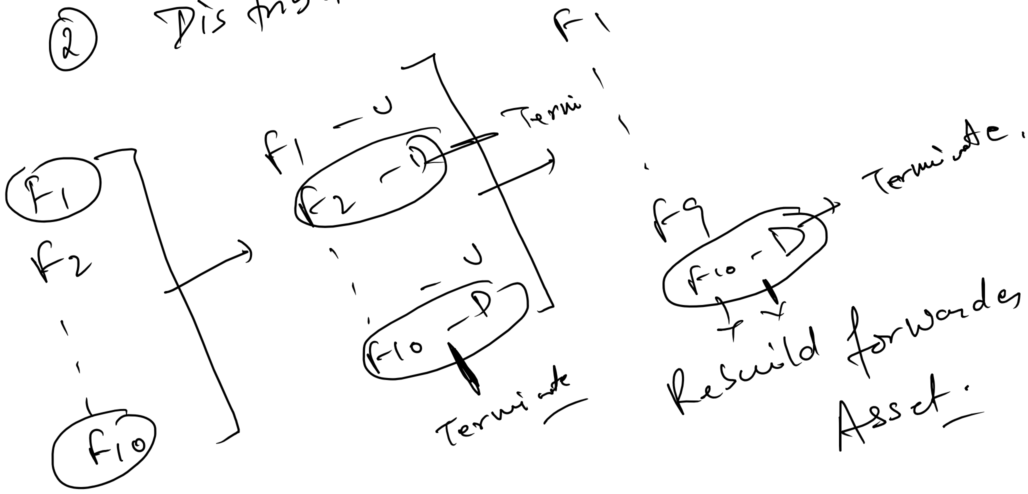
1. Track indexing, search & forwarder performance.
2. Identify resource bottlenecks.
3. Monitor license usage & violation.
4. Visualize cluster Health.
5. Diagnose I/O, CPU, memory, & Queue latency.

Mode of operation:-

1. Standard mode – Server on single instance,
2. Distributed mode – clustered.

→ F1

② Distributed.

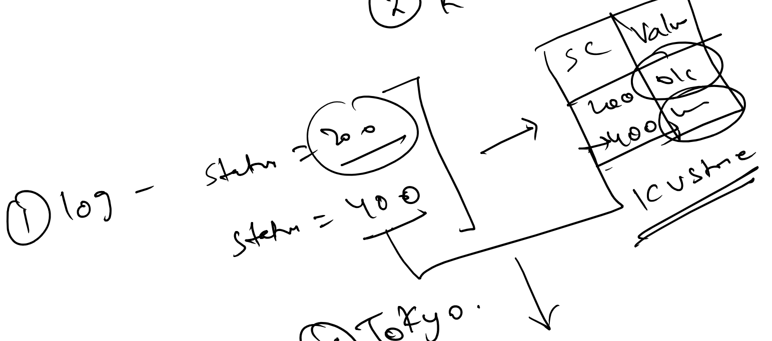


KVstore:- lookup.

KV
↳ key Value Pair

① each & every entry is tagged to the unique key.
② Dynamic & huge dataset.
③ upload in splunk

① via Index
② KV store.



Single site:- Same region → ① Tokyo.

Multi site:- Infra / env. diff. region.

① Tokyo
② Germany
③ US region

Appstore:-

. Mhb   re (splunk inhouse)

Appstore:-

1. Creator of the App
   - i) Splunk LLC → create (splunk inhouse)
2. Capability
   - 1) splunk Product
   - 2) splunk Version.