Day - 5

28 March 2025 09:38

1.) Deployer.

2.) Folder structure.

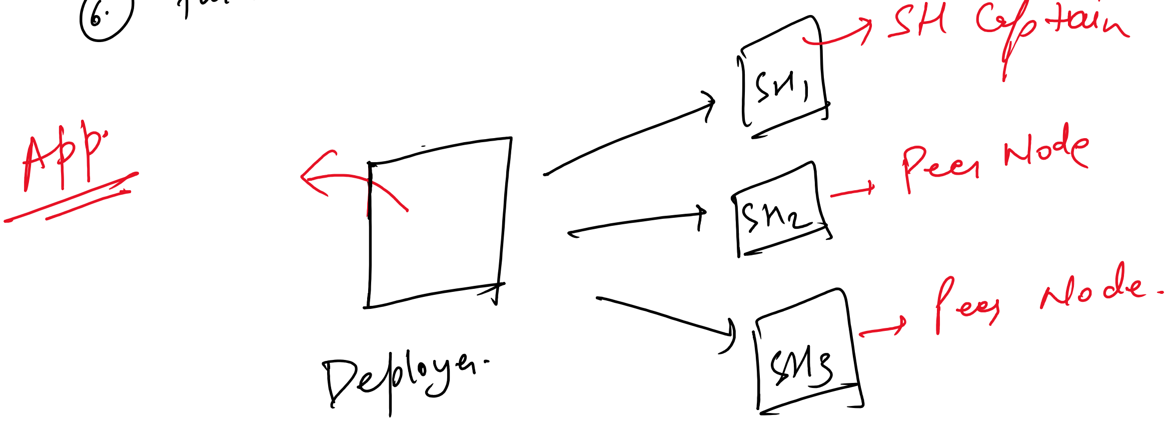
3.) syslog.

4.) Config. files.

5.) Regular expression.

1.) Deployer:-

1. Install splunk Enterprise (SE) on the All 4 server
2. Initialize Server 1 to act as Deployer.
3. Connect other 3 server to the Deployer & make it as dedicated Search Head.
4. Election to elect the captain from the set of Search Head.
5. Create the dummy app on the deployer end.
6. Push the Bundle, Config. & Troubleshooting.



https://SH1:8089

Search Head server username

Password.

9000

3, bcoz we have 3 SHs

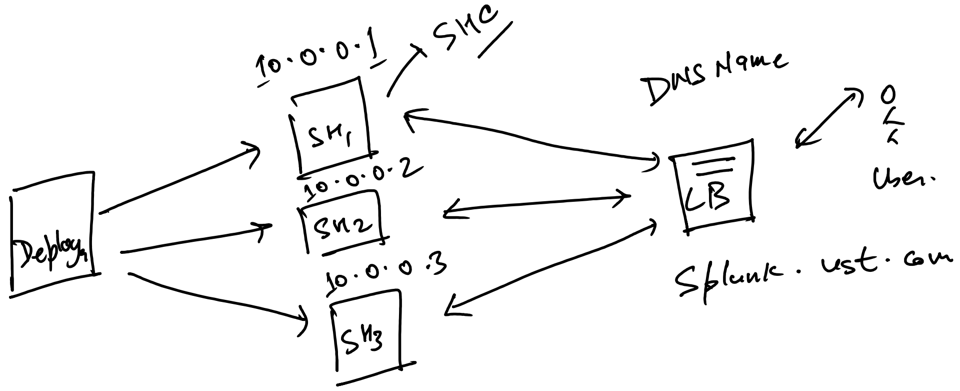
```
./splunk init shcluster-config -auth <username>:<password> -mgmt_uri
<URI>:<management_port> -replication_port <replication_port> -replication_factor <n> -
conf_deploy_fetch_url <URL>:<management_port> -secret <security_key> -shcluster_label
<label>
```

shcluster1

https://deployer:8089

admin@123 whatever is set at deployer level.

Need to Run on all the 3 SHs



Need to run on anyone of the search heads

```
./splunk bootstrap shcluster-captain  -servers_list "SH1,SH2,SH3" -auth <username>:<password>
```

Lookup:-

- CSV
- KV store
- Geospatial
- External
- Database.

CSV

1. Static
2. Small size

KVstore

1. Dynamic.
2. Large Size.

Collections.conf

↓

Structure of your KVstore

Studio Dashboard

↓

json

↓

Adding background image

↳ KVstore

Collections.conf .

```
[VK-Kvstore]
id. name = string
id. place = string
enforcetype = true/false
```

→ Lookup Definition.

KVstore →
↓
KeyValue Pair

Vivek Bangalore ← abcde123

Value ⟷ Key

Btool :- Btool- troubleshoot the syntax of config.file.