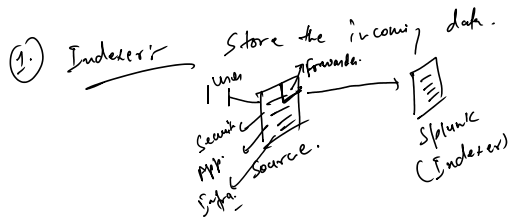
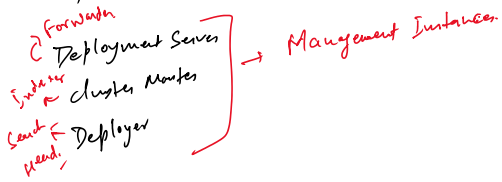


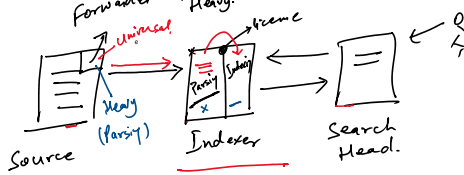
1. Component:-

- ① Indexer.
- ② Forwarder.
- ③ Search Head.
- ④ Deployment Server
- ⑤ License Master.
- ⑥ Cluster Master.
- ⑦ Deployer.

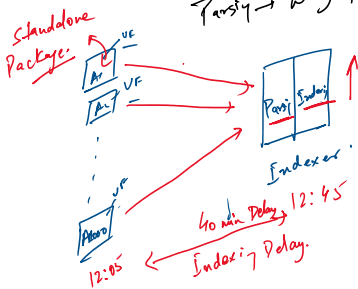


Forwarder → Universal forwarder -

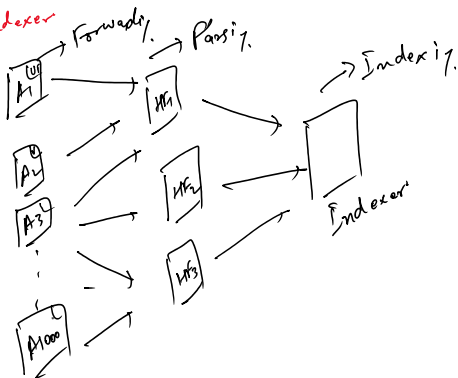
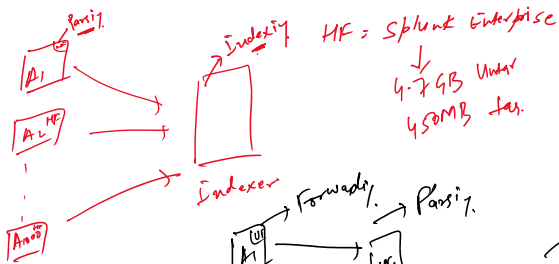
Forwarder → Heavy forwarder



Parsify → Way to eliminate unwanted data.



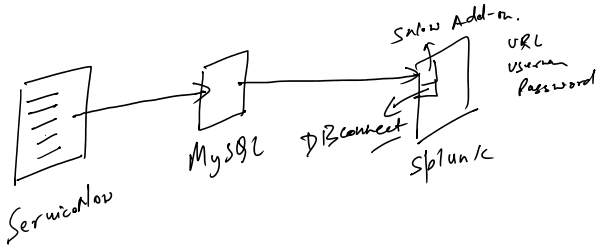
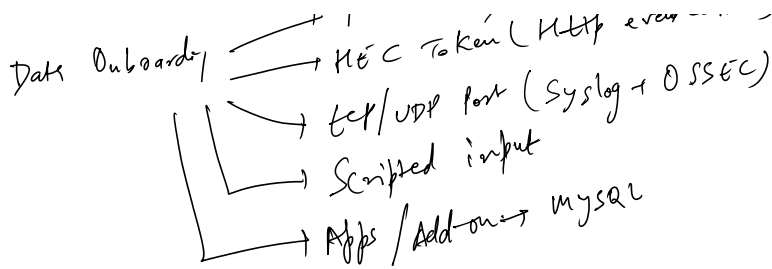
VF → 15MB for 150MB data.



Data Outboardy → Forwarder → Postman

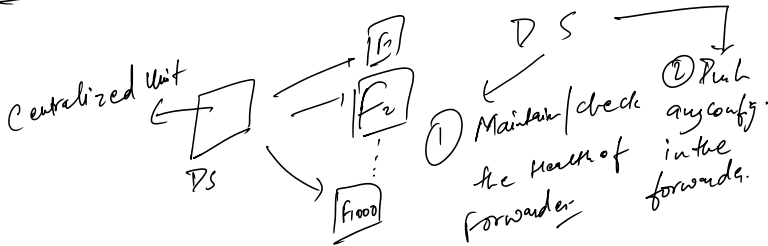
HEC Token (HTTP event collector)

1001 port (Syslog + OSSEC)

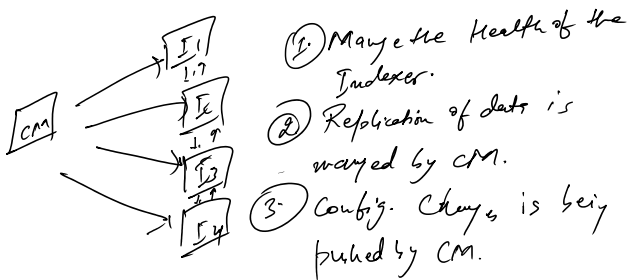


Management Interfaces:

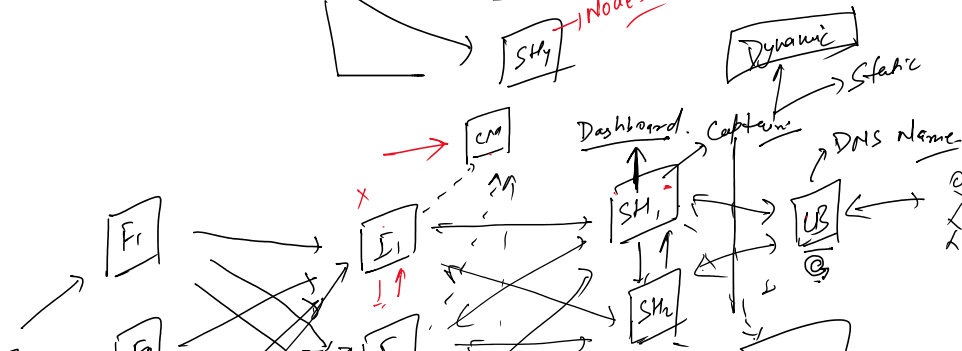
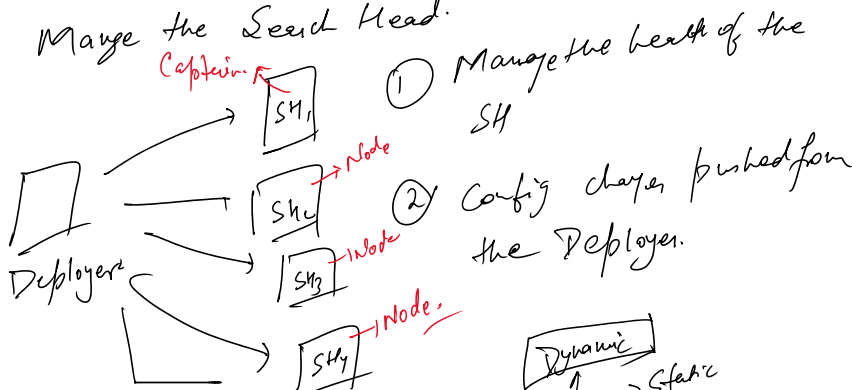
① Deployment Server:-

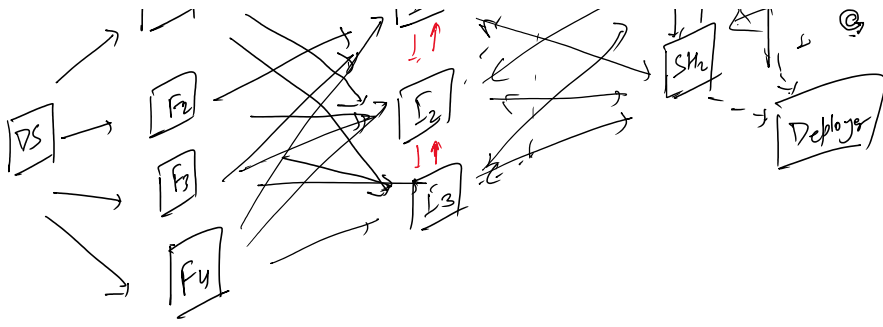


② Cluster Master:- ① Indexer Management:-

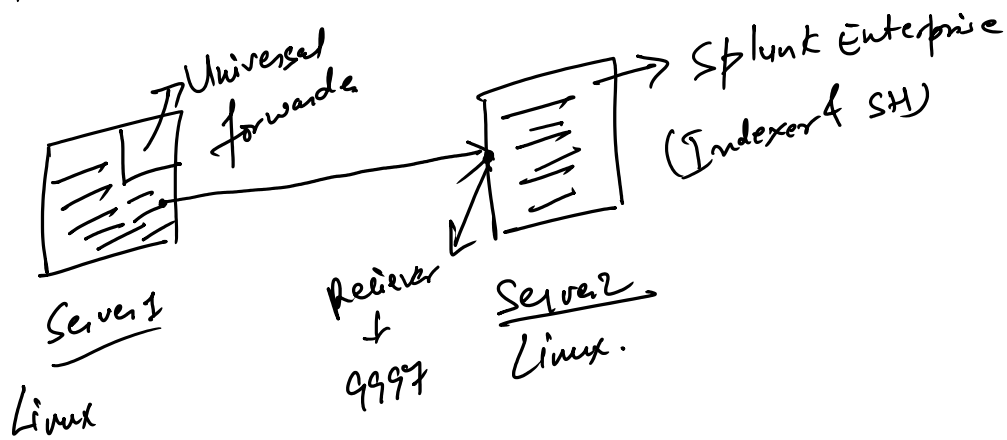


③ Deployer Manage the Search Head.





① Raw Linux Server.



② Universal forwarder.

① Install UF in Server1 & Splunk Enterprise in Server2

Server1 - IP1 - UF
Server2 - IP2 - SE

② Enable the receiving port in the Server2
↳ SE (Indexer)

③ Connect the UF with SE
↓ Server1 ↓ Server2

④ Validate if the connection is successful or not.
... in default index.

- ④ Validate '5
- ⑤ Forward the logs in ^{default index.}
(Main)
- ⑥ Forward the specific log to specific index & source type.
(Custom)
- ⑦ Validate the data ingestion.
- ⑧ Troubleshooting Method. & Configuration files involved.

Output.conf → ip: 9997


input.conf → stanza → what exact data you want to forward?

vi input.conf
 press i → insert
 Esc + : wq! → save the file
 Esc + : q! → close w/o saving.

UF




index = VK -id x



Indexer

Config. → input.conf → stanza input/monitor
 Config. → output.conf → indexer detail

Troubleshooting Splunkd.log

(2) ping. indexip

(3) tcpdump indexip 9997

(1) HF to Splunk Enterprise.
↓
Server 1

(1)

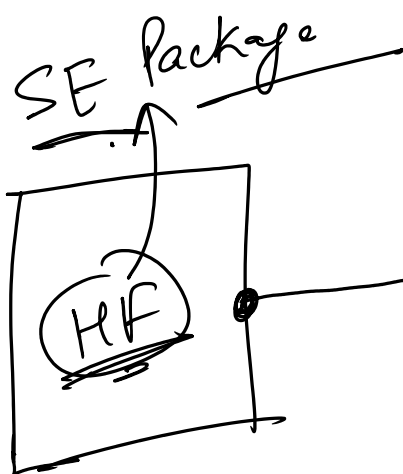
Uninstall the VF

(2)

Splunk Enterprise = HF

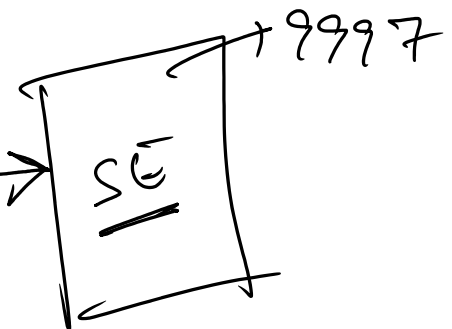
(3)

Connect HF with SE → Server



Server 1

9997 - 9997



Server 2
(Indexer)

ver 2

Tomorrow:-

① Linux:-

① cd

⑤ nano

⑨ ps

② ll

⑥ vi

⑩ kill -9

③ mv

⑦ tar

④ cp

⑧ rm

② HEC Token, Scripted input, Aps & Add-on.

③ Syslog & Db Connect

plid