Day - 1

03 January 2025 11:32

~~1.~~ Basic of Splunk & Architecture.

2. SPL Query – Basic SPL Query.
   Advance SPL Query

Basic – table, rename, sort, dedup, stats, eval, addcoltotal, addtotal, fillnull

Advance – append, join, multikv, spath, rex, tstats

(8) Demo on clustered Master & Deployment DS.

3. Visualization – chart, timechart.
4. Knowledge object – Alert, Report, Data model & Pivot.
5. Dashboard – classic Dashboard.
6. Index Time field Extraction – props, transforms.
7. Timestamp extraction.

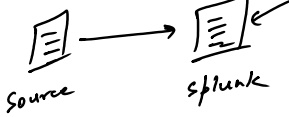
(1.) Splunk

(1.) Monitoring Tool helps to monitor logs & get the insight out of it. Ex – Dashboard, Alert, Report, Visualization, MLKT

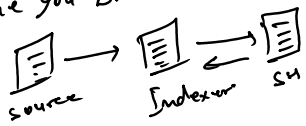
- XML (classic)
- json (studio)

Component:-

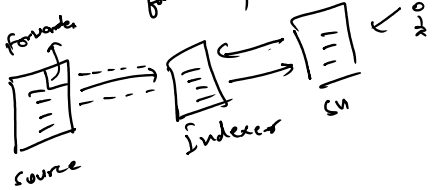
(1.) Indexer:- Database where the incoming data from the source will be captured.



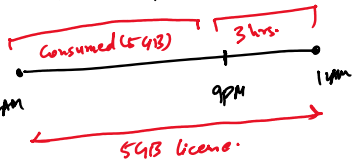
(2.) Search Head:- GUI, where you write search Query & you get visualization.



(3.) Forwarder:- Install on the source end, where you can go & setup the data forwarding.



(4.) License Master:- Amount of data ingested a the daily basis. Agent that will make sure that you should be cross the limit. Ex – 5 GB/d → 1 yr.



Package

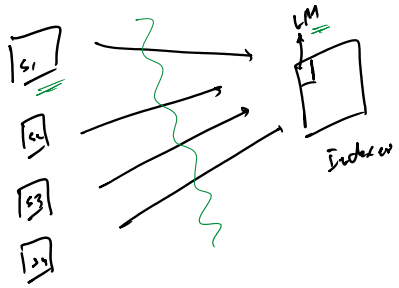
- Splunk Enterprise
  1. License mstr
  2. SH
  3. Indexer
  4. HF
  5. CM – cluster Master
  6. Deployer
  7. DS → Deployment Server.
- Splunk Universal Forwarder (splunkUF)

(a) Indexing of data will continue.

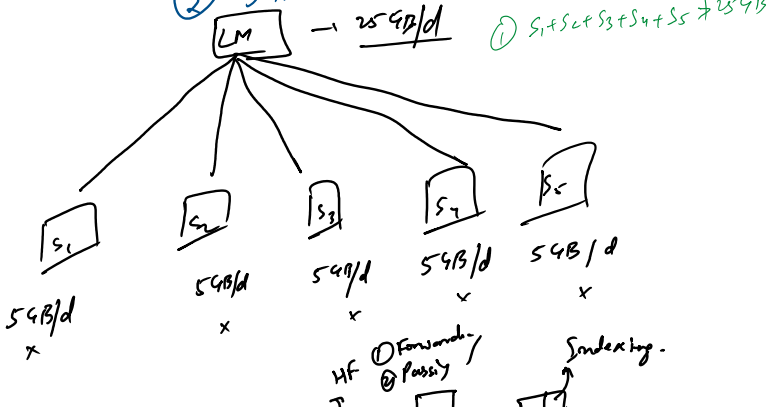
12AM → 11:59PM

5GB license.

1. Indexing of data will continue.
2. Searching of data will be disabled.
   1. Dashboard
   2. Report
   3. Alert
   → nothing will work.



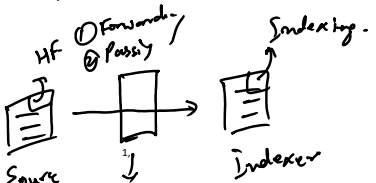
3. 5 times breach in a window 30 days



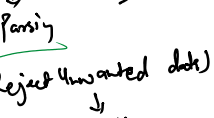
① S1+S2+S3+S4+S5 ≠ 25GB

License Pooling:-

Trial license
① 500 MB/d
② 60 days → Free
→ Paid/Enterprise



Forwarders:-
- Heavy forwarder
  1. Parse the data at the source end.
  2. GUI
  3. Splunk Enterprise (450MB Tar / 5GB Untar)
- Universal forwarder
  1. Forward the data as it is. No Parsing happens.
  2. No GUI
  3. Standalone package. (25MB Tar / 295MB Untar)

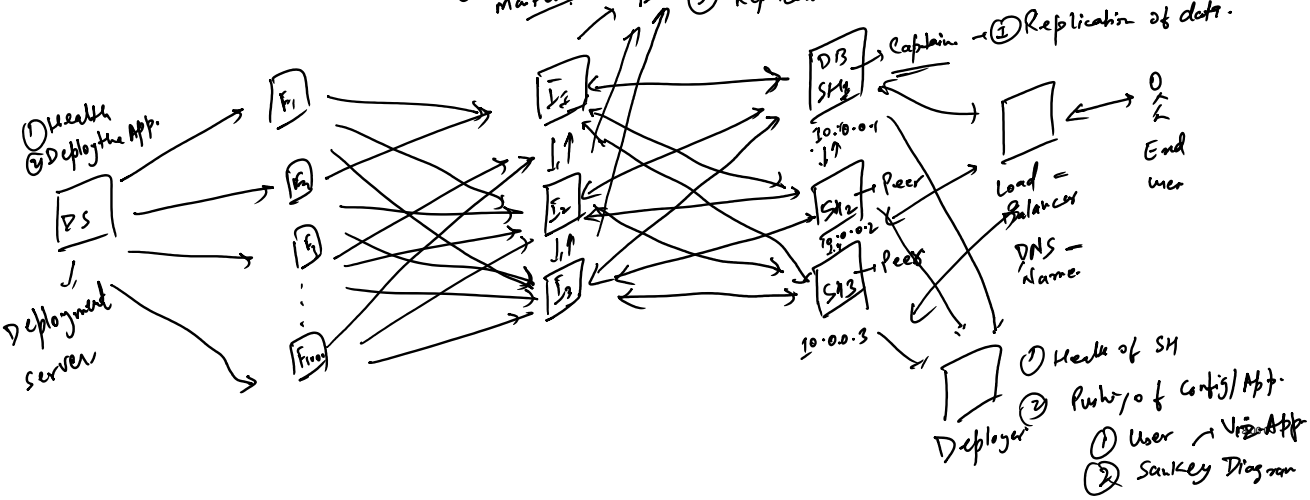


1. HF vs UF Benefit?
2. Best Solution for Data forwarding.

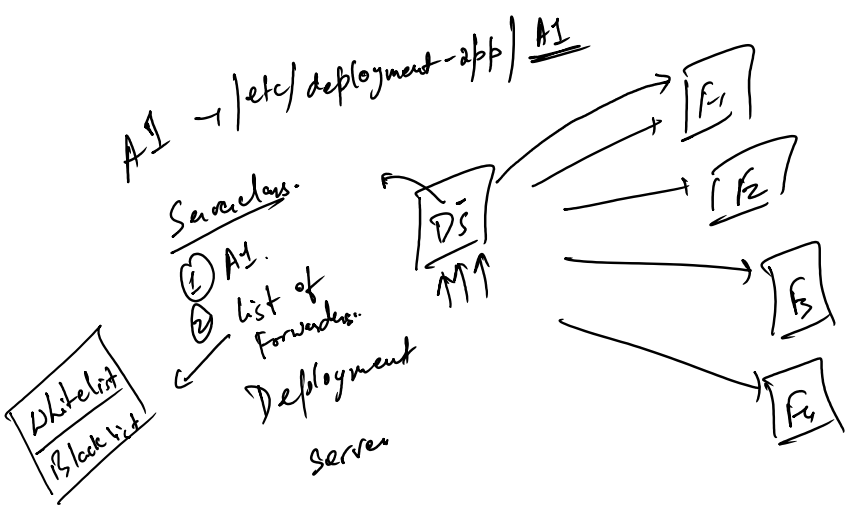
pip

3 Mangment Instances:-

1. cluster master → Manage the Indexers, Deploy the App, Health Management of the Indexer.
2. Deployment Server → Manage the Forwarder, Deploy the config, Health Management of forwarder
3. Deployer → Manage the Search Head.



Multiple Indexers:- (1) Replication of Data
(2) Distributed Mangement.
(3) Backup of Data.



(1) Default → Pre configured files
(2) Local → User create Config
(1.) Splunk Upgrade.
(2.) Rollback Prospective.
(3.) Default config → Override.
local high Precidence than Default folder.
(4.) Backup → local folder