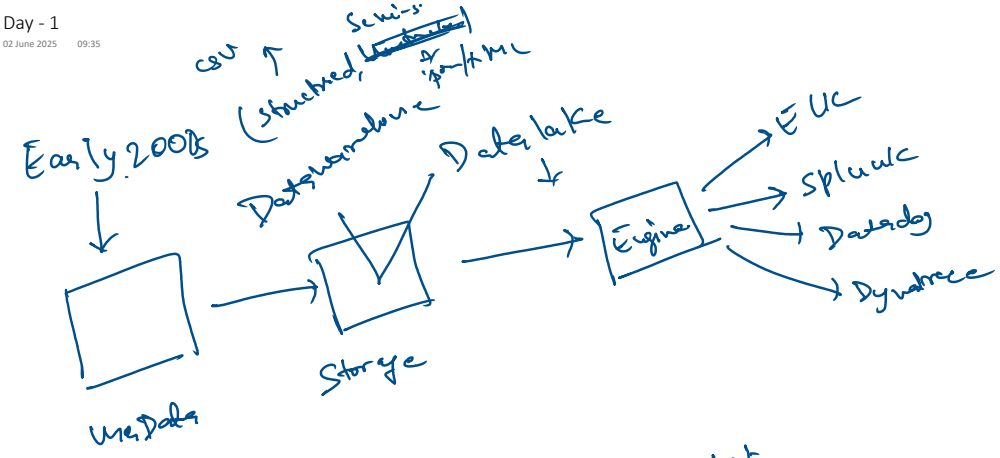
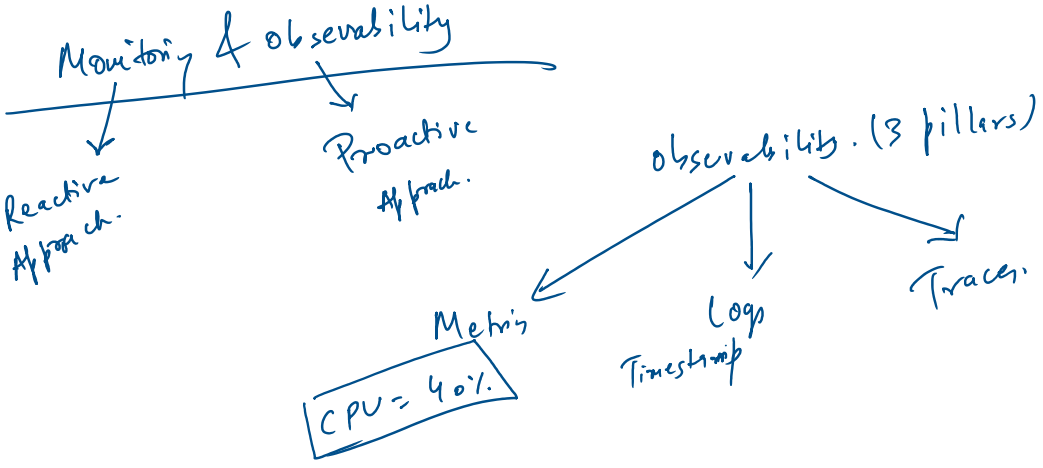
Day - 1

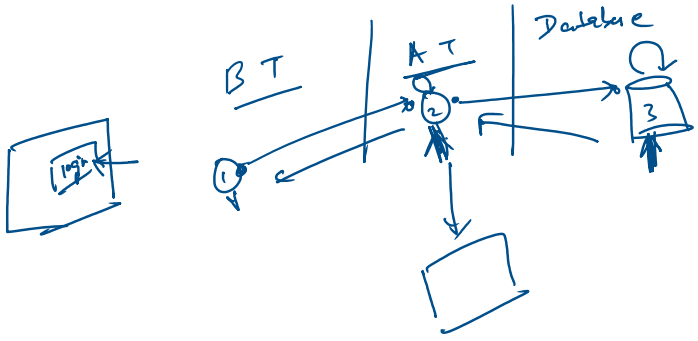
02 June 2025 09:35



Splunk (enterprise) → log Monitoring Tool → logs → Alert, Visualization, Report, Dashboard.

1. Splunk ES
2. Splunk ITSI
3. Splunk Phantom → Splunk SOAR
4. Splunk APM
5. Splunk Victor
6. Splunk UBA





SLI vs SLO vs SLA

↓ Service Level Agreement between.

SLI vs SLO vs SLA

SLI → Service level Indicator

SLO → Service level objective

SLA → Service level Agreement
Aggrement b/w two parties.
(98.5%)

B/w your team:

99% → SLO

Error Budget:- 1% (1%) → either effort b/w down time if any kind of updation/patch.

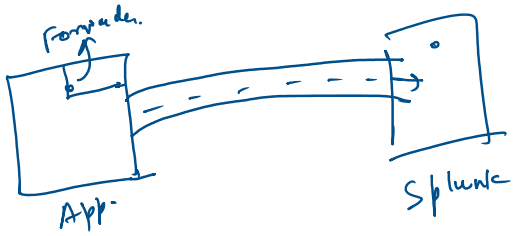
→ Splunk Enterprise

1. Forwarder
2. Indexer
3. Search head
4. License master.

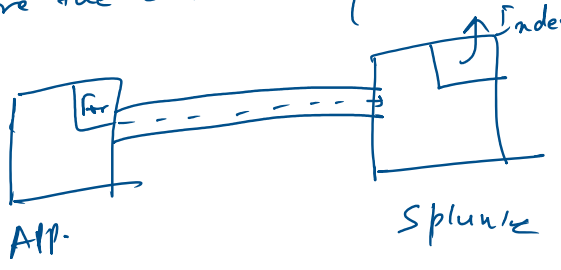
5. Cluster master
6. Deployment Server
7. Deployer

→ Management Server

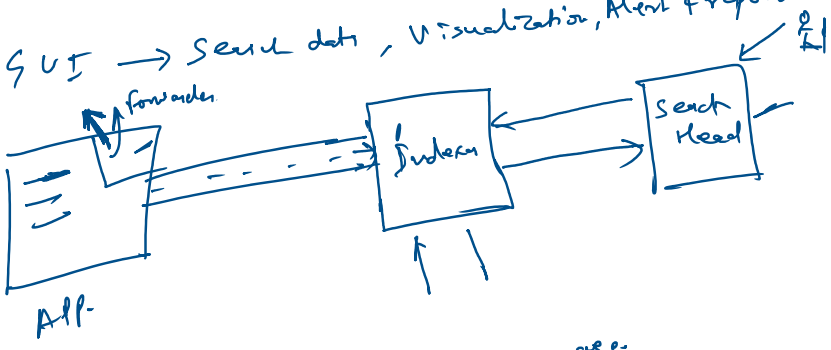
(1) Forwarder:- Forward the data from the source to Splunk



(2) Indexer:- Store the data coming in splunk



(3) Search Head:- GUI → Search data, Visualization, Alert & report.

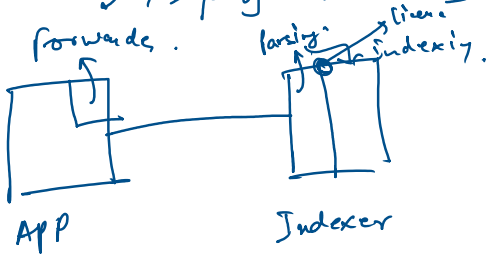


License usage.

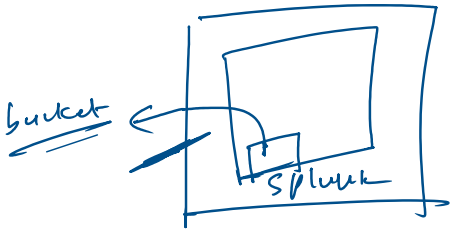
App.

④ License Master → Agent → check the licence usage.

5 GB/day → 1 year.] → $$$

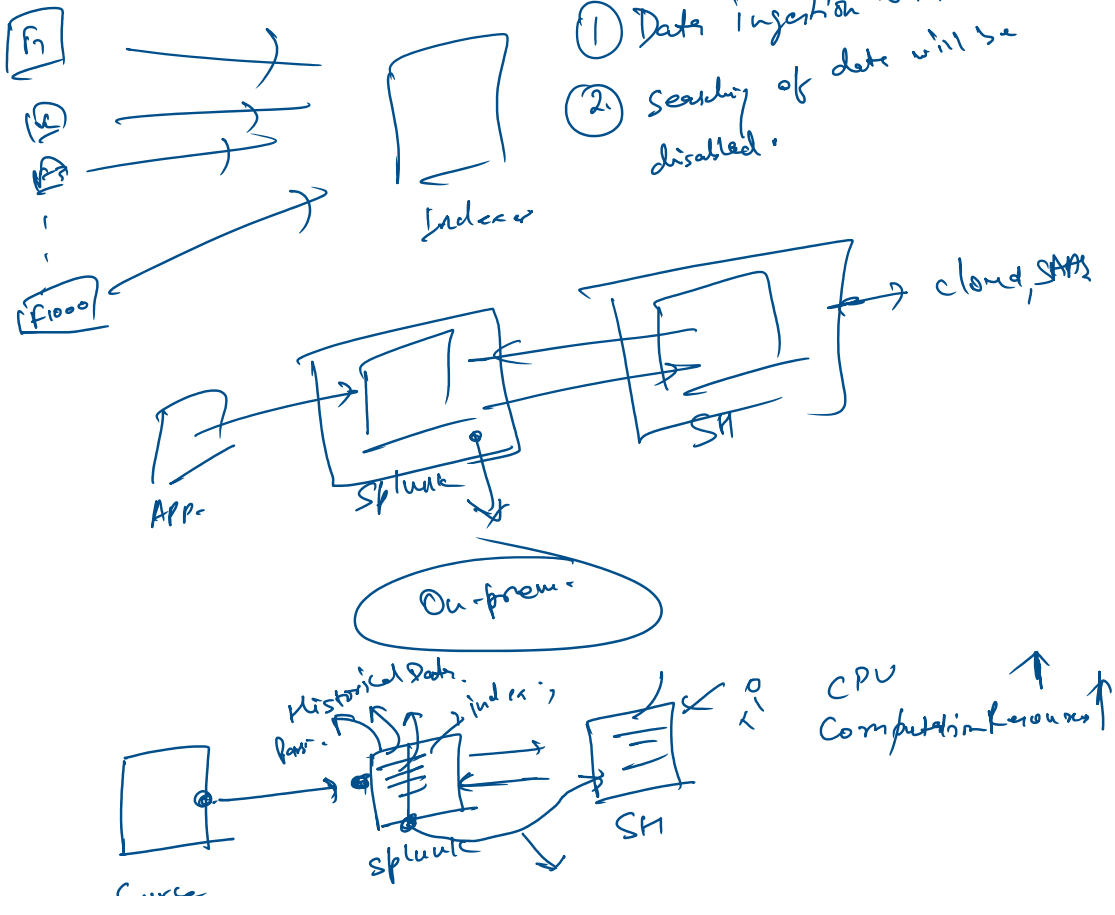


5 GB/day → 24 hrs cycle - 12AM – 11PM
4PM

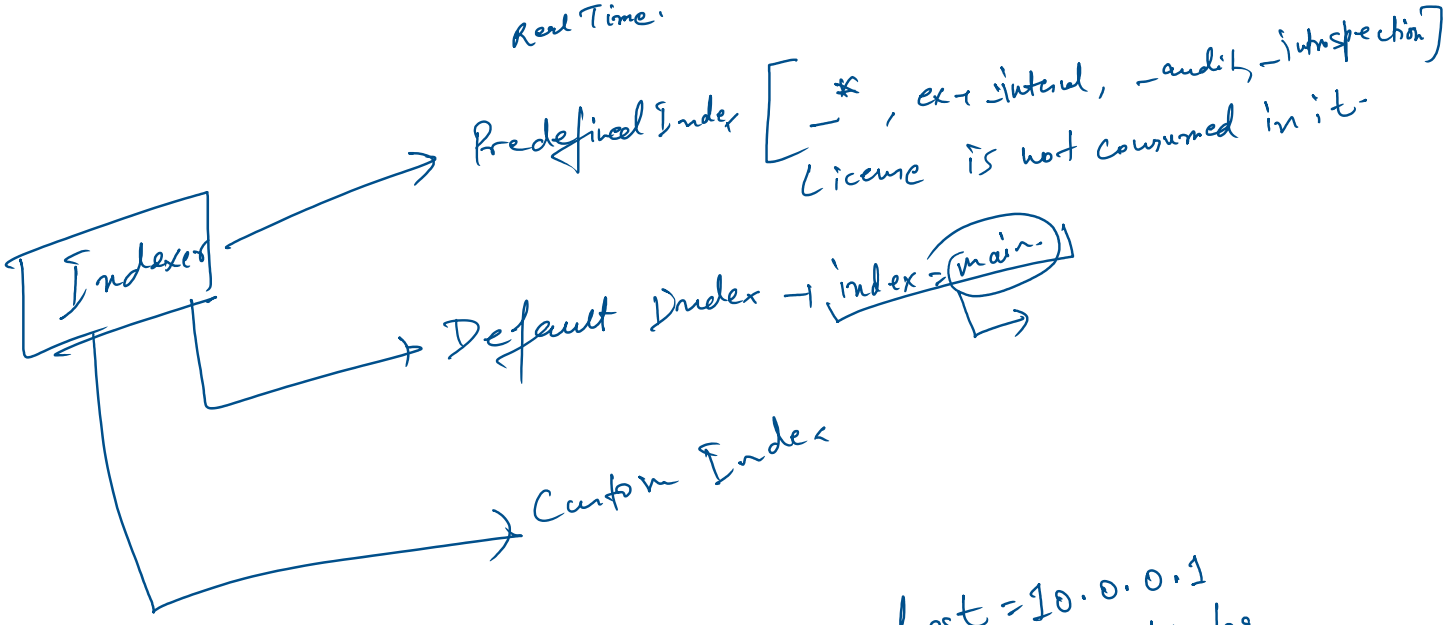


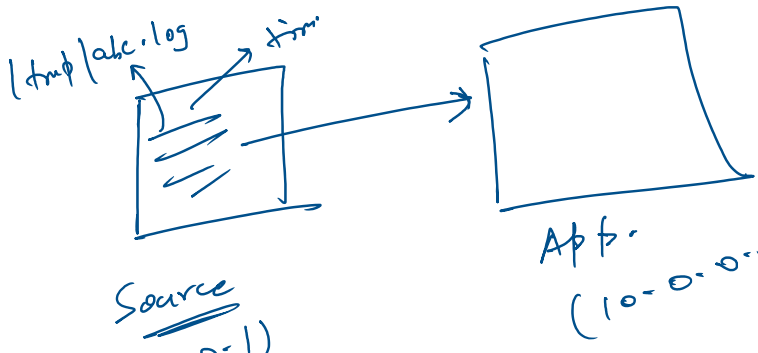
Servers

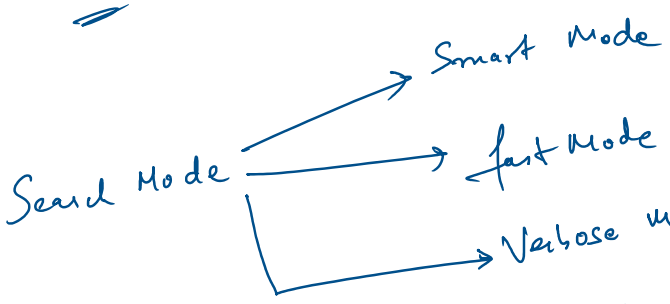
On prem / cloud.



Real Time.







Search → Pulling the events + Extraction of fields

Smart Mode:- Pull the data. As well as extraction of fields.

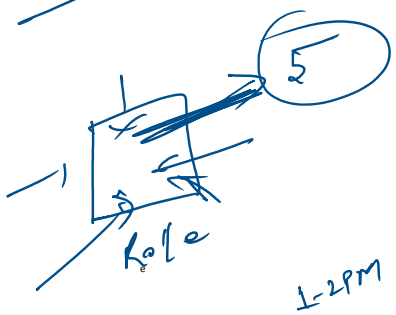
Fast mode:- Pull the data. No extraction of field

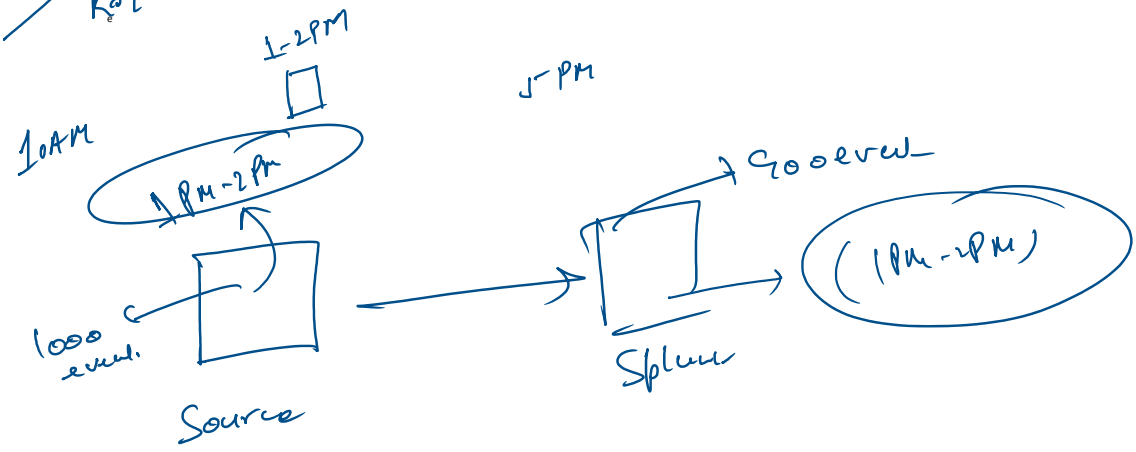
Pull + extraction + Navigate b/w diff. tab.

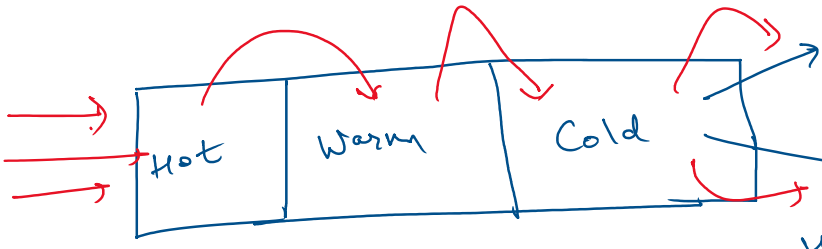
Mode:-

Pull Type

Verbose Mode







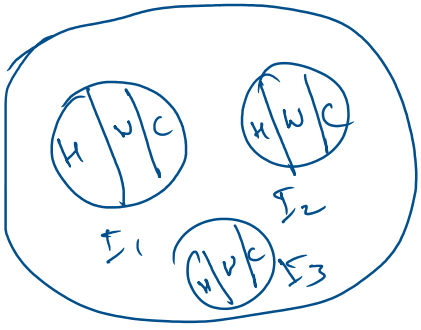
UK-idx

Define the retention period:

① Age of the data ✓ → 30d

② Size of the Bucket ✓ → 100 GB

Any condition matches, Data will move from hot to warm or warm to cold.



4 Indexer

Indexer

SPL:-

1. Table
2. dedup
3. Stats
4. Sort
5. rename
6. fillnull

1. Table:-

Tabular output.

ex- |table field1, field2, field3

fieldxlame - Case sensitive

field value - Case insensitive.