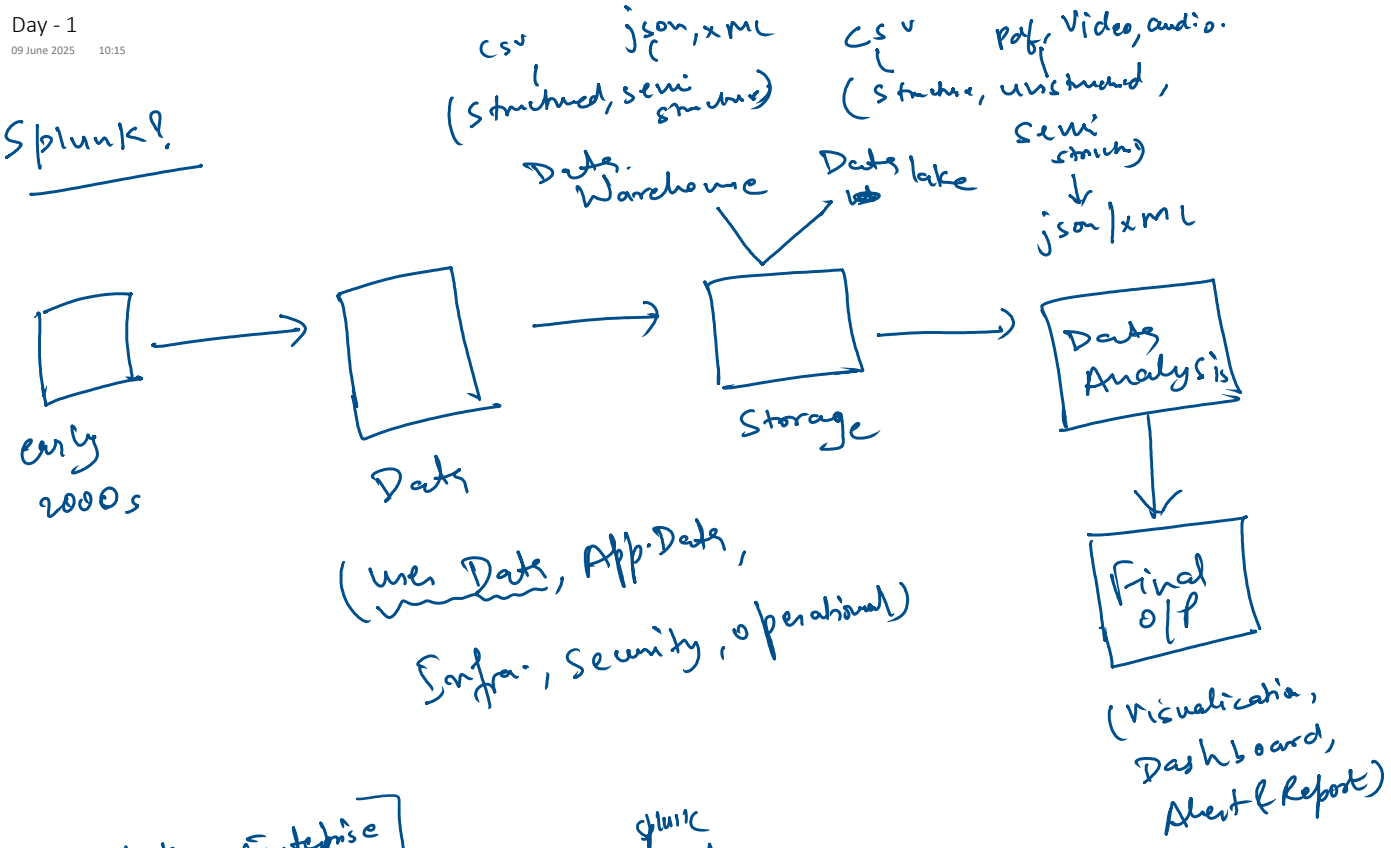
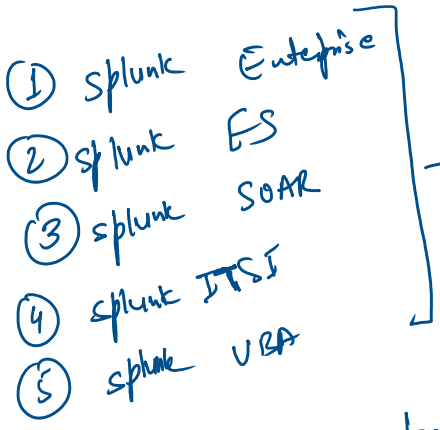
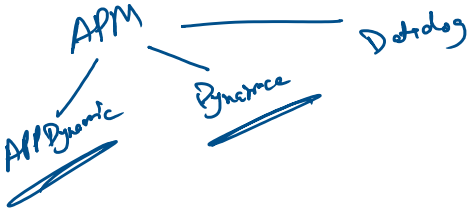
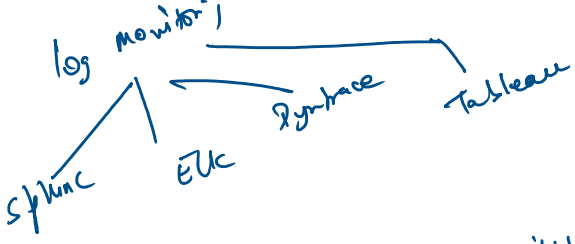
Day - 1

09 June 2025 10:15









Monitoring

1. Reactive measure

Observability

1. Proactive measure

CPU ↑ load ↑ server ↓

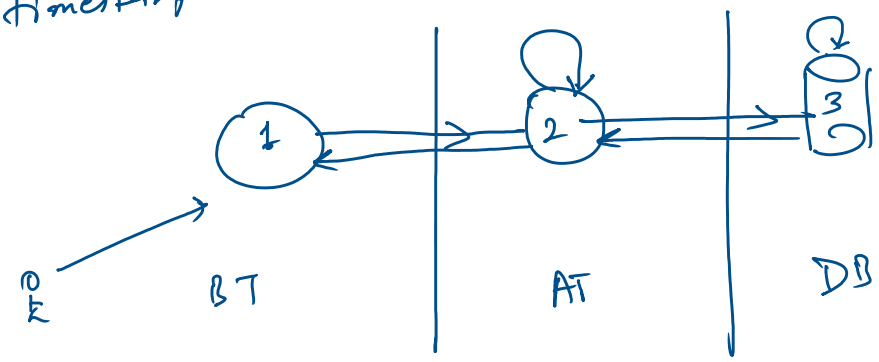
3 pillars

1. Metrics
2. logs
3. traces

Metrics → CPU = 40%

Logs → Timestamp

Traces →



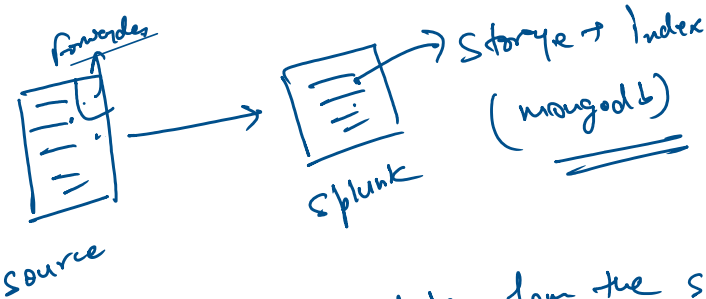
Splunk:-

Components:-

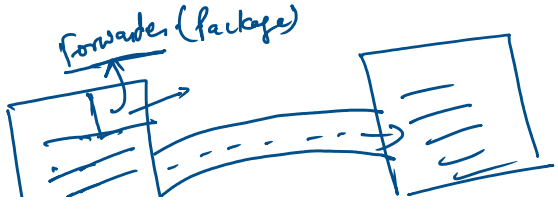
1. Indexer.
2. Forwarder
3. Search Head
4. License Master
5. Cluster Master
6. Deployment server
7. Deployer

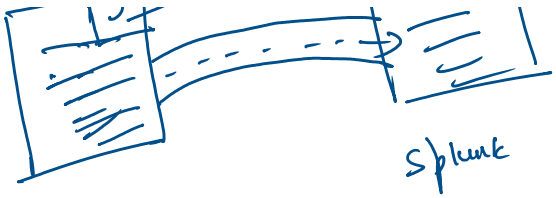
(5), (6), (7) → Management Instance.

(1) **Indexer:-** Database where all the incoming data indexed inside splunk.



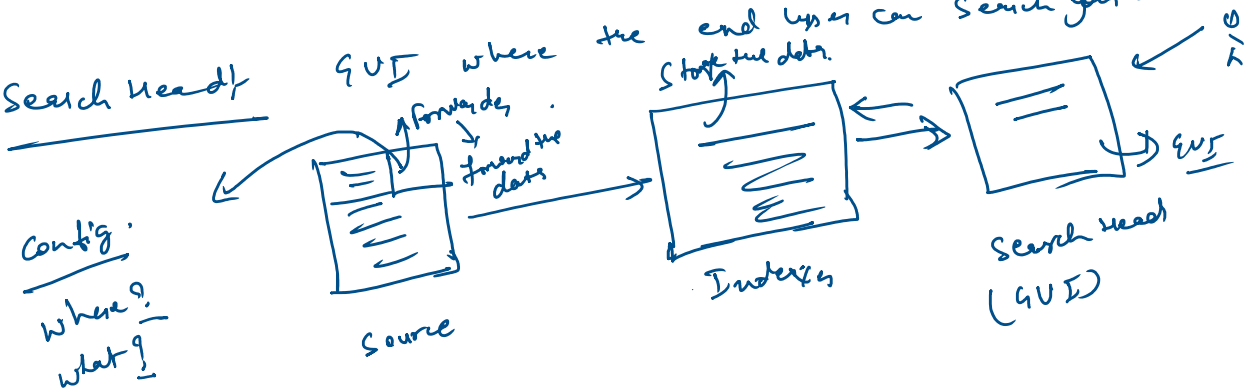
(2) **Forwarder:-** Agent that will send the data from the source to the splunk.





Source
(App.)
(palo Alto)

(3) Search Head:- GUI where the end users can search your data.

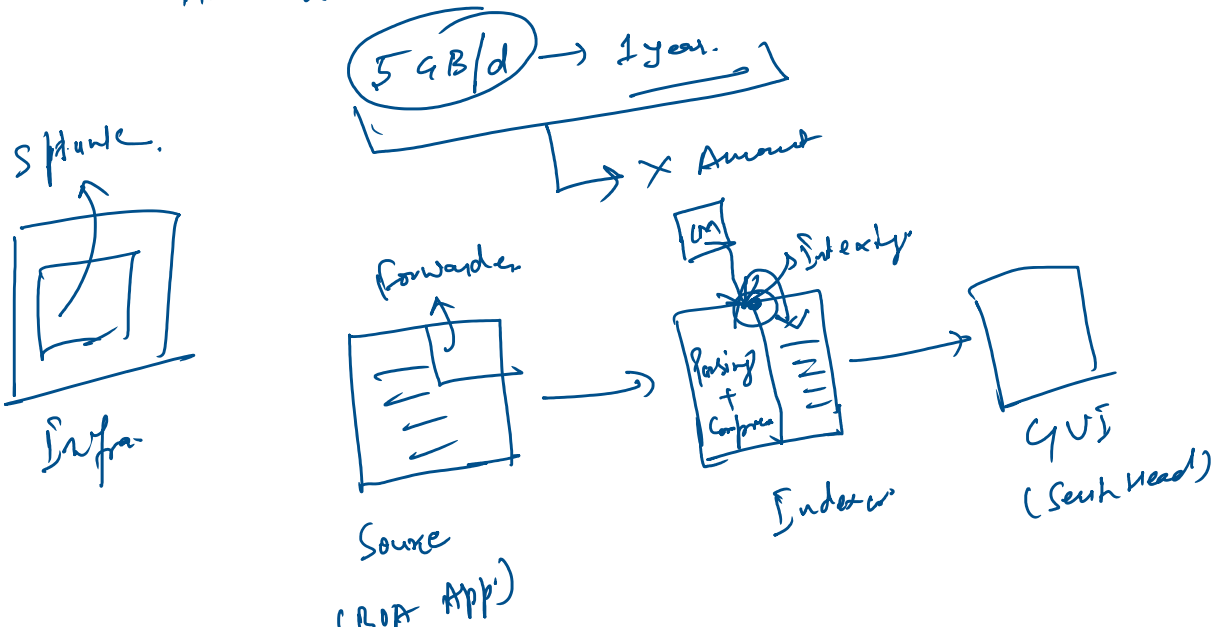


Config:
Where?
What?

Source

(4) License Master:- Check whether you are compliant with the licence.

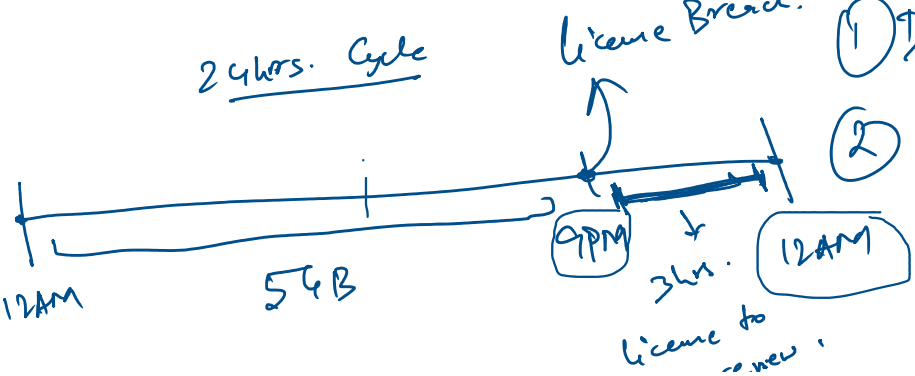
How much data you want to index on the daily basis?



Source
(BOA App)

Indexer

2 Ghrs. Cycle



License to renew.

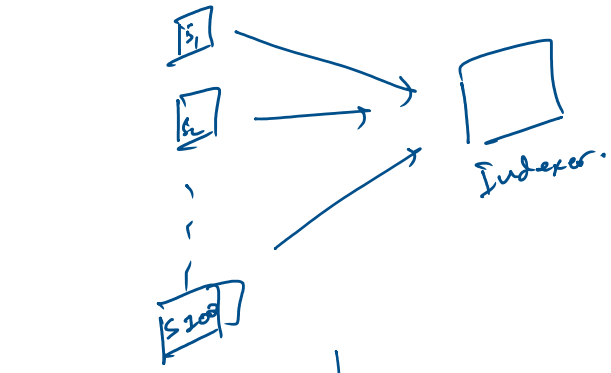
(1) Indexing will continue

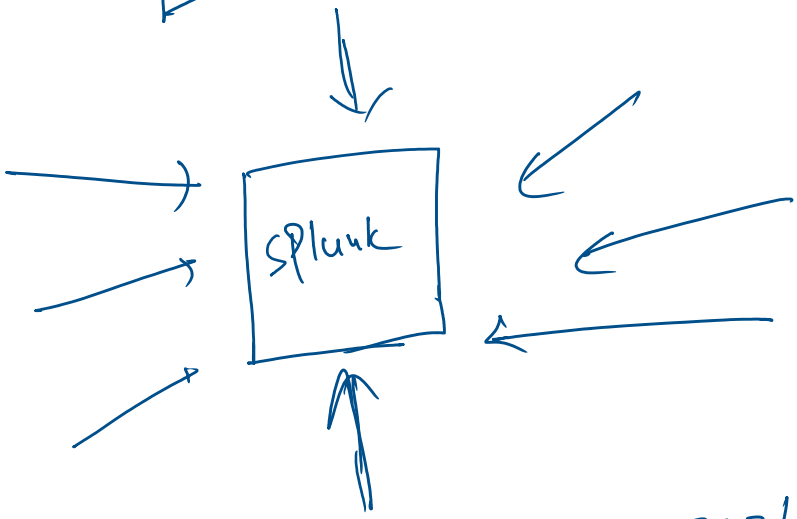
(2) Searching will be disabled.

12AM 5 GB

license to renew.

① Upfront Payment.





5 Violation → 30days window.

Splunk will blacklist.

5GB/d

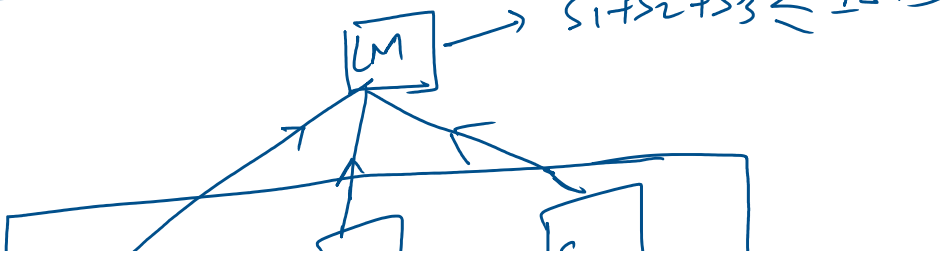
↓

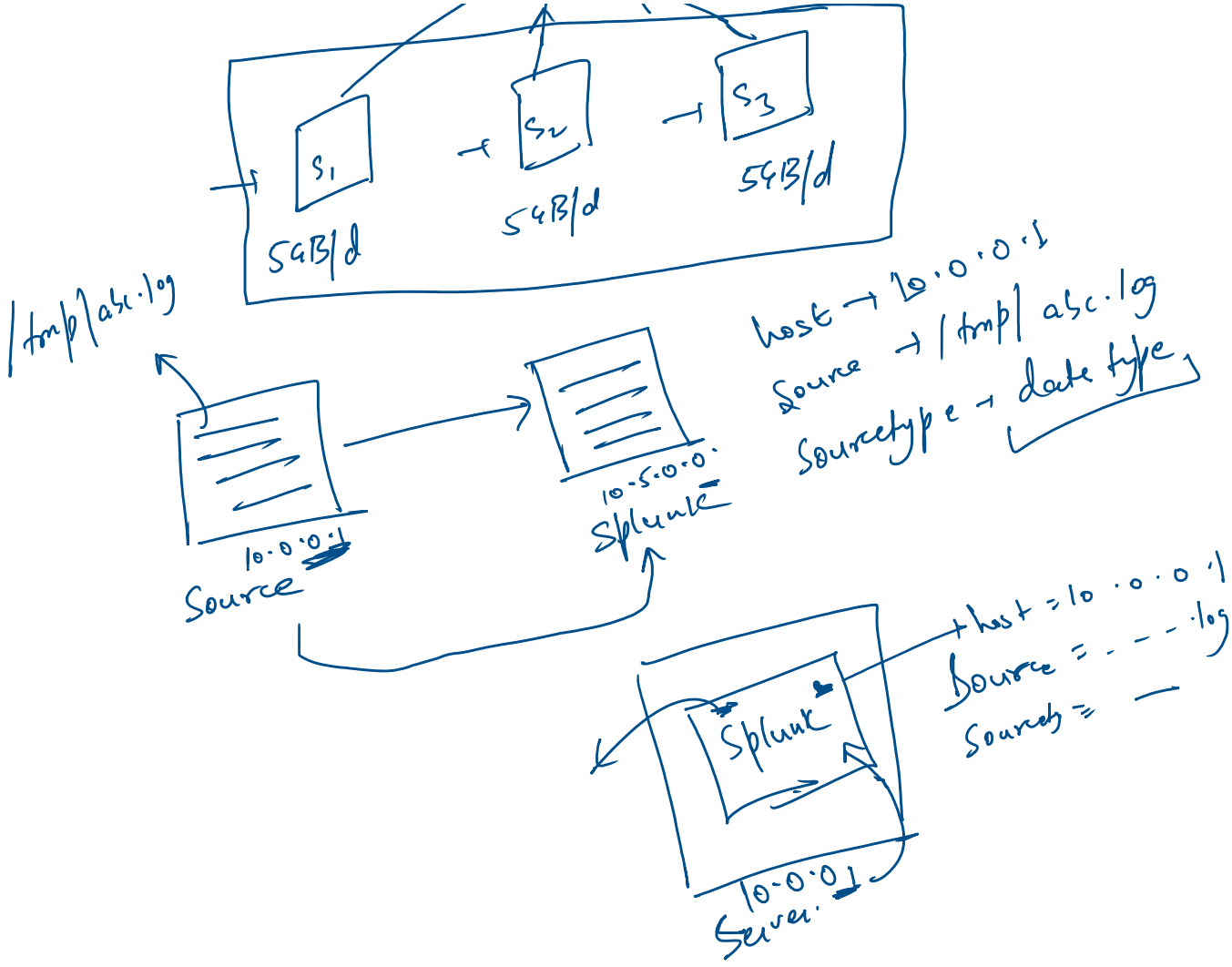
5 → 5.1 GB → Violation 1

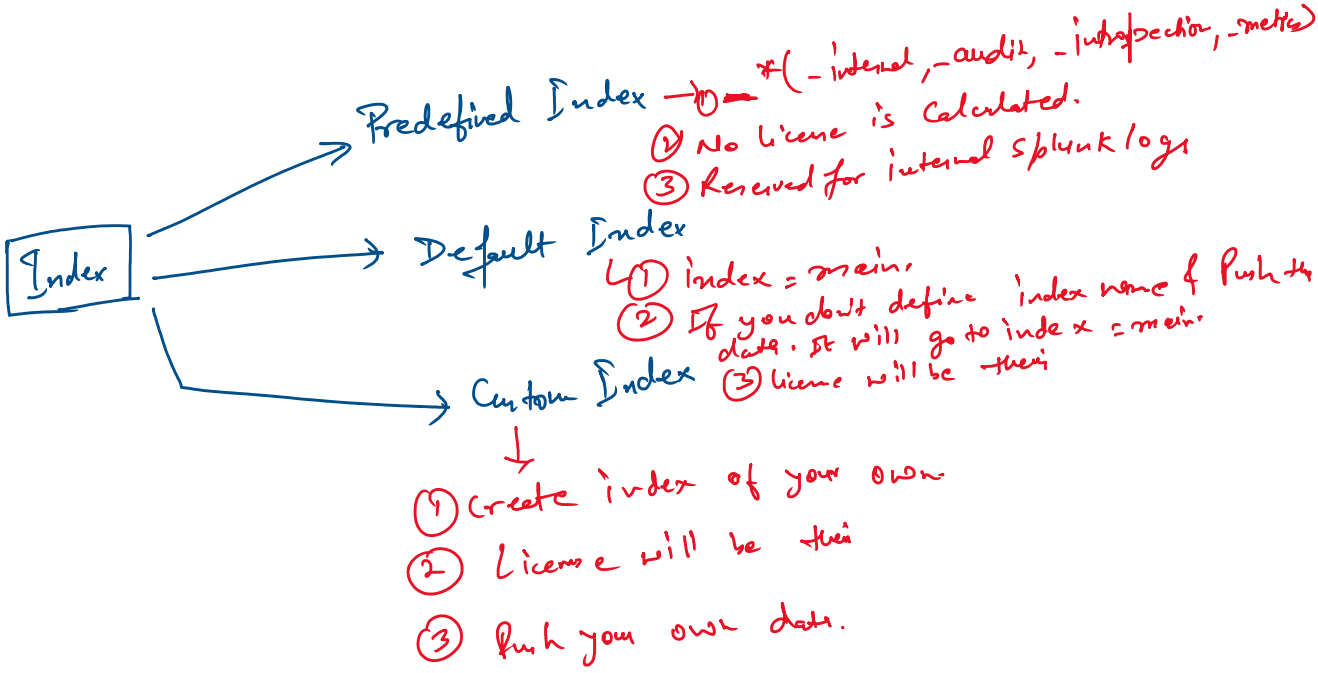
5 → 5.02 GB → Violation 2

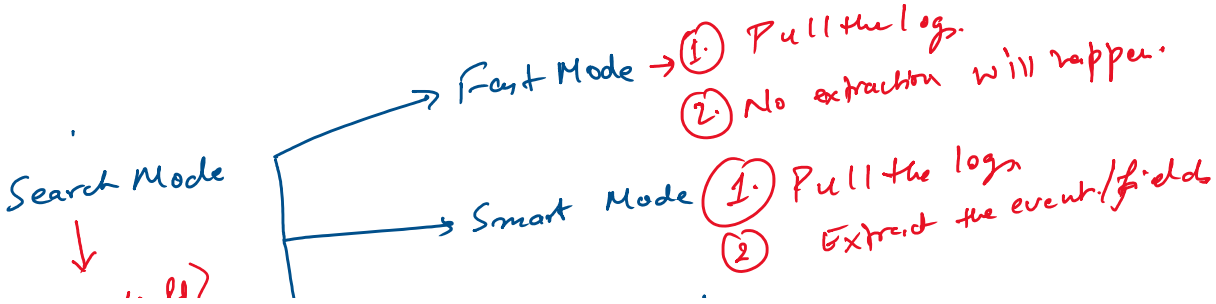
① License Estimation

License Pooling:-




S1
S2
S3
5GB/d
5GB/d
5GB/d
/tmp/abc.log
10.0.0.1
Source
10.5.0.0
Splunk
host → 10.0.0.1
Source → /tmp/abc.log
Sourcetype → data type
host = 10.0.0.1
Source = ---.log
Sourcetype = —
Splunk
10.0.0.1
Server


Index
Predefined Index → *(_internal, _audit, _introspection, _metrics)
① No license is calculated.
③ Reserved for internal splunk logs
Default Index
① index = main.
② If you don't define index name & Push the data. It will go to index = main.
③ License will be there
Custom Index
① Create index of your own
② License will be there
③ Push your own data.


Search Mode
Fast Mode → ① Pull the logs.
② No extraction will happen.
Smart Mode ① Pull the logs
② Extract the event/fields

↓

① Extract the field
② Pull the logs

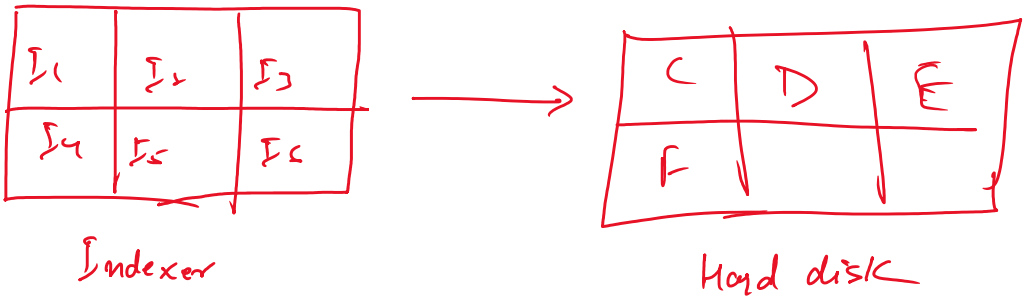
index: interact.

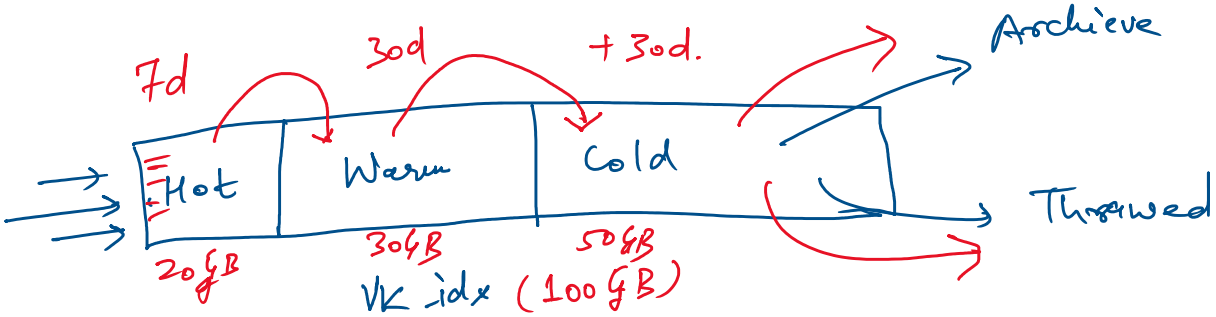
→ Smart

→ Verbose Mode

② Extract the even...

① Pull the logs.
② Extract the fields
③ Traverse b/w the tab

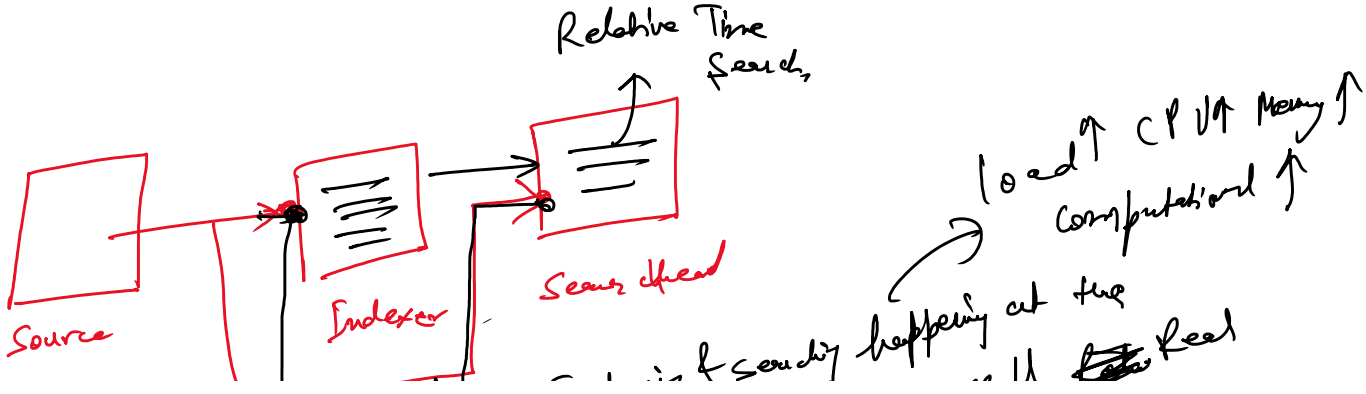


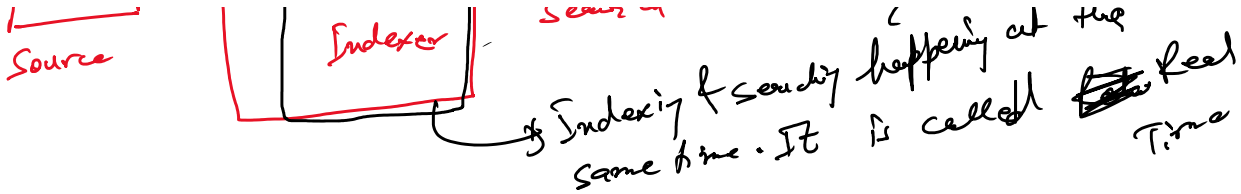


Retention Policy:

① Size of the bucket
② Age of the data.

→ Anyone condition is true. The data will move from one bucket to another bucket.





SPL Queries –

1. Table
2. Rename
3. Stats.
4. Eval
5. addcoltotal
6. addtotal
7. timechart
8. chart
9. Single value
10. geostats
11. Rex.
12. Dedup
13. Sort
14. fillnull
15. Head & tail.