Day - 1

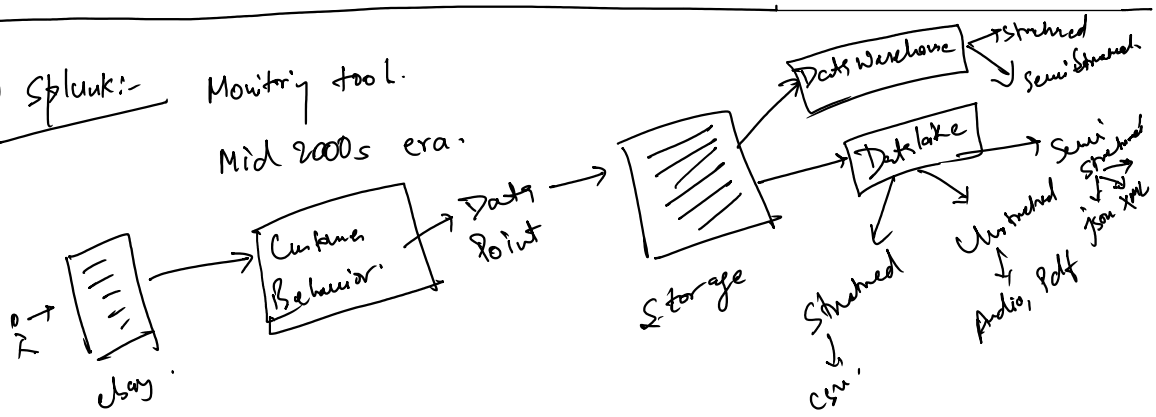
21 April 2025 09:56

1. Splunk.
2. Components.
3. Use Cases
4. Adv. & Disadv.
5. Feature.

---

1. Splunk:- Monitoring tool.

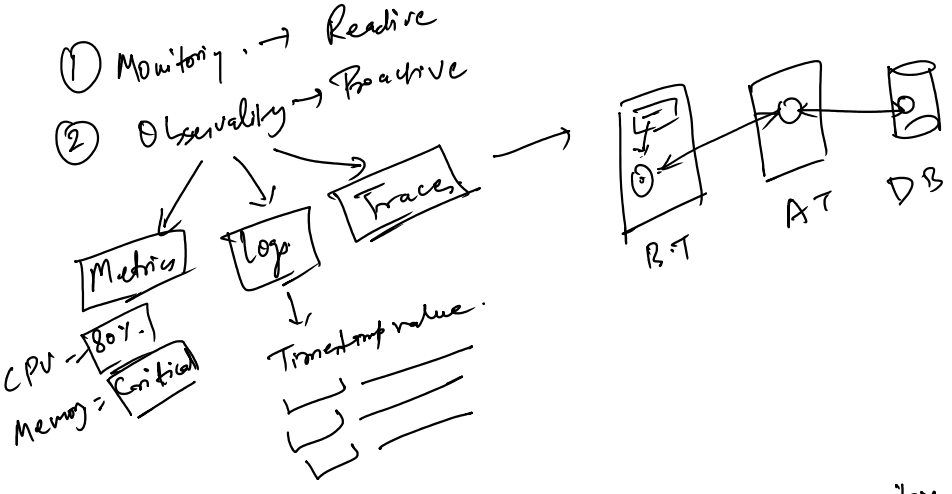
Mid 2000s era.

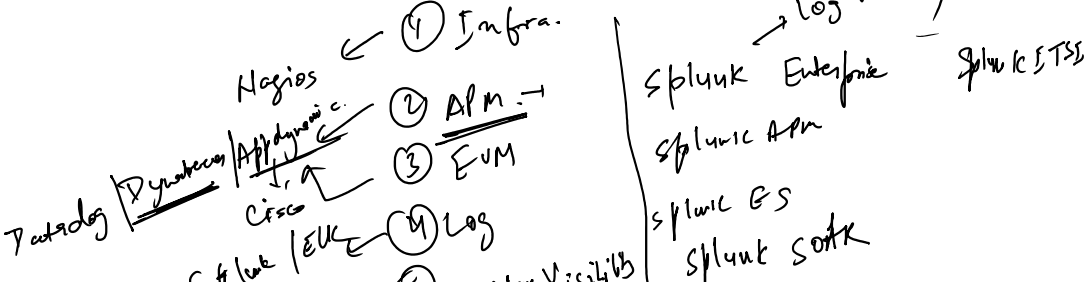


Data analysis:-

1. ELK → inverted index
2. Splunk → bucketing.
3. datadog
4. dynatrace.

→ Dashboard
Alert
Report
Visualization





Splunk | ELK (4) Log (5) Database Visibility | Splunk GS Splunk Soft

Splunk:- (Log Monitoring)

(1) Dashboard
(2) Report
(3) Alert
(4) MLTK

(2) Predict

Dashboard
- Classic (XML)
- Studio (+V 8.2.x +) (json)

MLTK → Train, Test
Train ↔ I/P, O/P

Components of splunk:-

(1) Indexer
(2) Search Head
(3) Forwarder

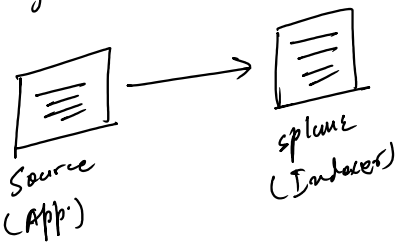
(4) License master
(5) Deployment server
(6) cluster master

(7) Deployer → Management Instance

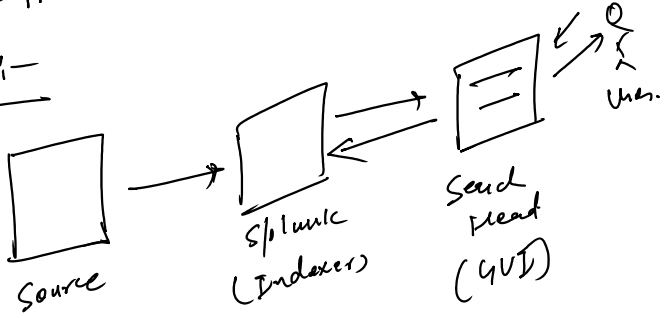
Splunk Enterprise

(1) Indexer

Storage your data.



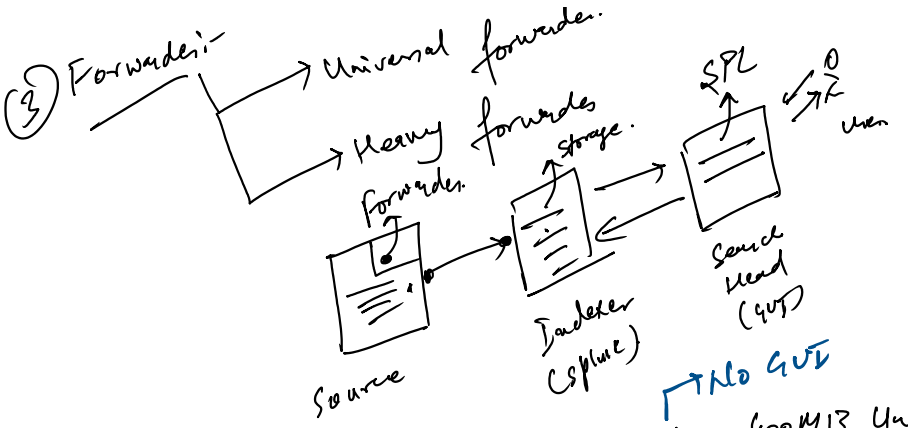
(2) Search Head:-



(3) Forwarder:- → Universal forwarder.

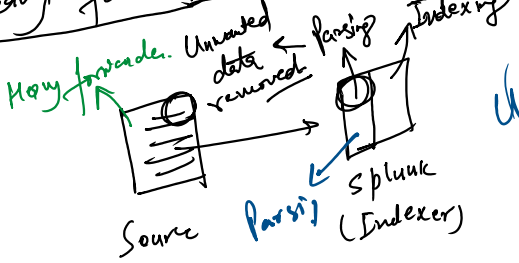
SPL

(3) Forwarders:-



Universal Forwarder :- Splunk Universal Forwarder → 400MB Unix. → No GUI

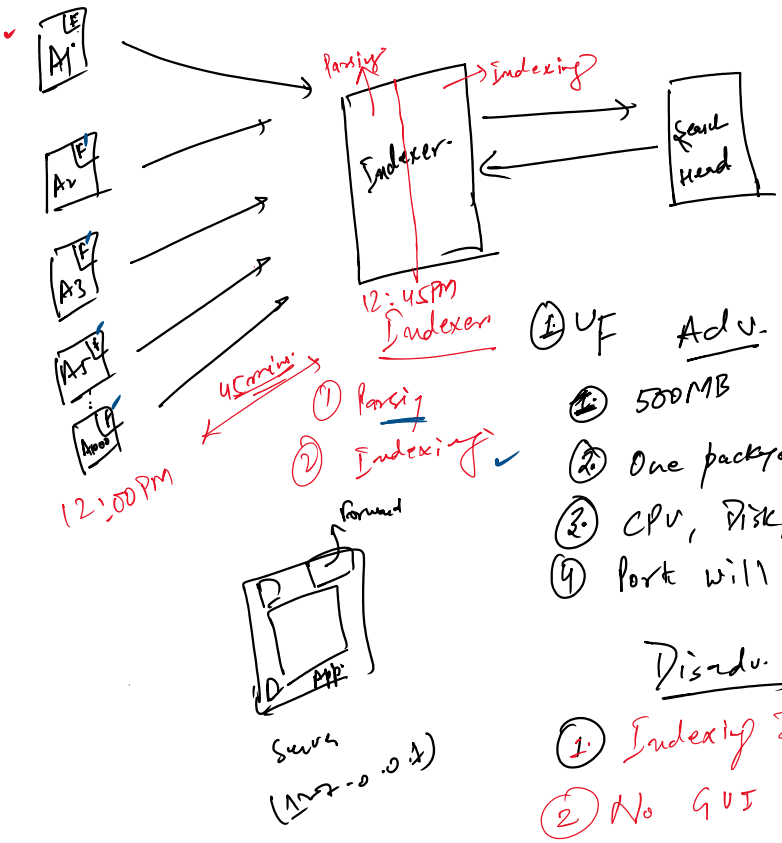
Heavy forwarder → splunk Enterprise → 5.78GB Unix → GUI



Parsing

Universal forwarder forward data same as it is.

(1) More Complex



(1) UF Adv.

(1) 500MB
(2) One package for one Component
(3) CPU, Disk, Memory, Server
(4) Port will be availble.

Disadv.

(1) Indexing Delay
(2) No GUI

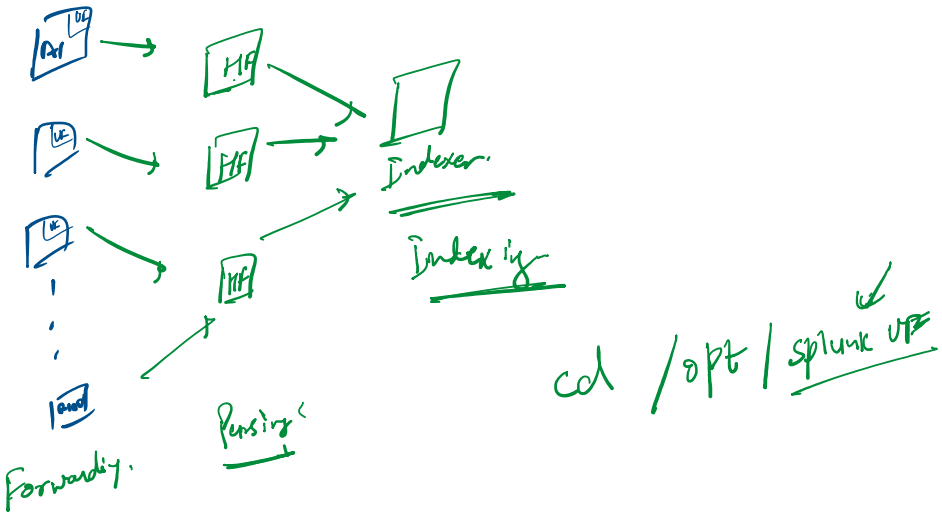
HF:-

Adv:-

1. GUI
2. Load on Indexer is very less
3. No or minimal Indexing Delay.

Disadv:-

1. Size – 6 GB
2. Computational.
3. Cost ↑
4. Root will be occupied.



4. License Master:-

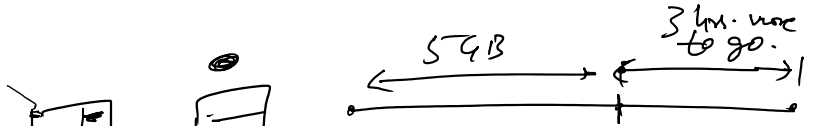
Check the license condition.

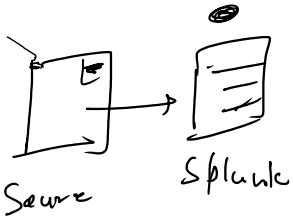
1. Timeframe
2. Feature usage.
3. Storage.
4. Size of Infra.

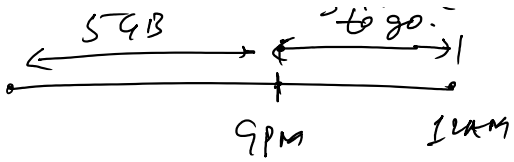
Amount of data ingested in splunk on the daily basis. 5GB/d → 1 year.

↓

License calculation is done.







(1) Data ingestion will continue.

Searching will be stopped.

↓

No data will be searable

↓

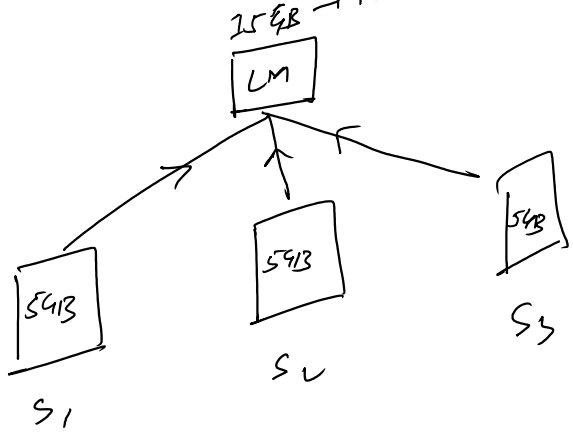
Breach → 5 times in a day.

(2) Upfront Payment.

(2.) No option carry forward or lending from other day.

License Pooling :-

$S_1 + S_2 + S_3 \neq 15GB$



Deployment Server → Forwarder. → Health of these forwarder.

→ Management Instance.

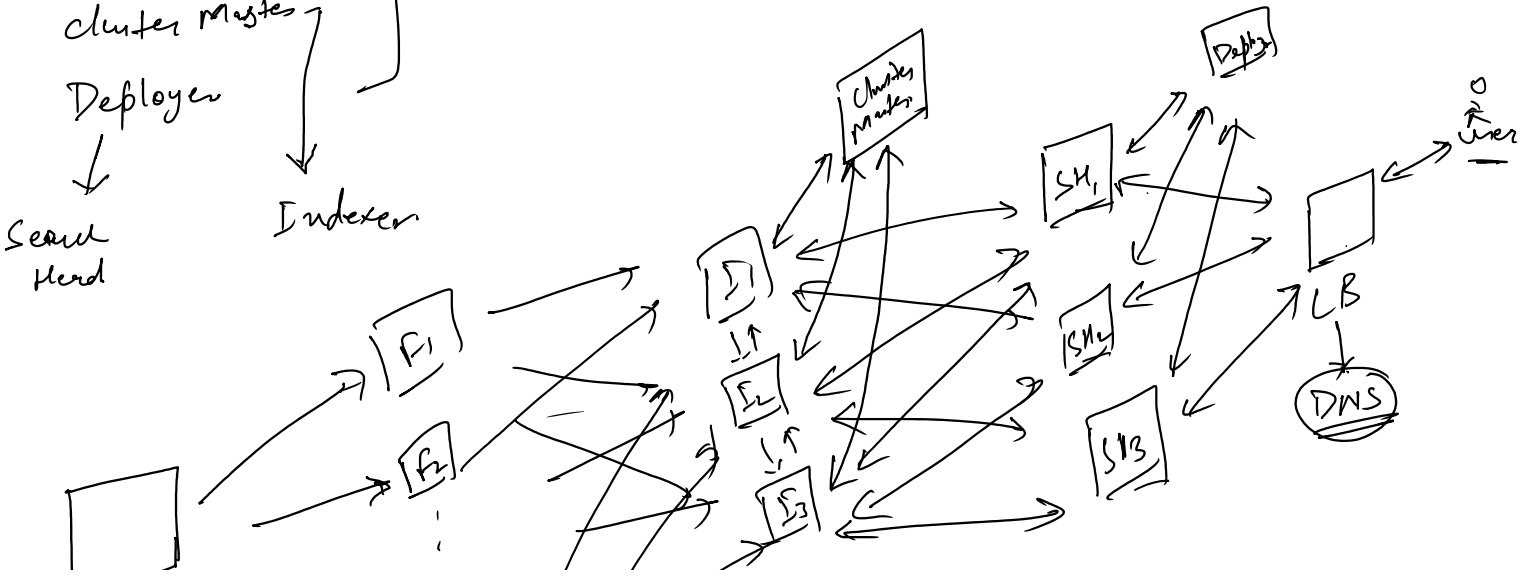
cluster Masters

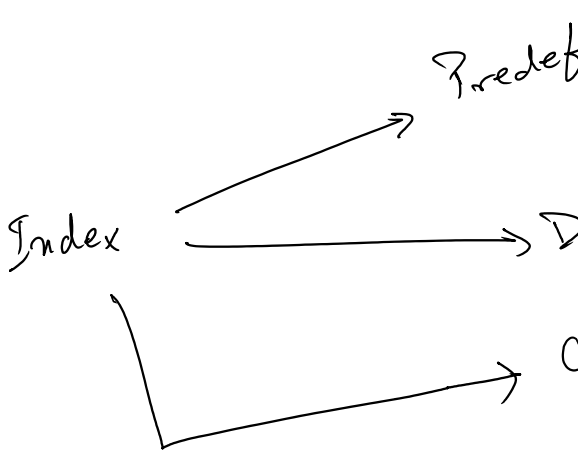
Deployer

↓

Search Head

Indexers





Predefined → ① Index starting with _* (_internal, _audit, _introspection, _telemetry)

② Licena is not calculated for internal logs of splunk

③ you can't ingest anyother application/custom data.

Default :- ① Index = "main"

② you can ingest app. / custom data.

③ License is consumed.

④ when user doesn't specify the index name in log forwarding, then log is ingested in default index (index = main)

Custom Index :- ① User can create the own index
ex - idx, show - idx.

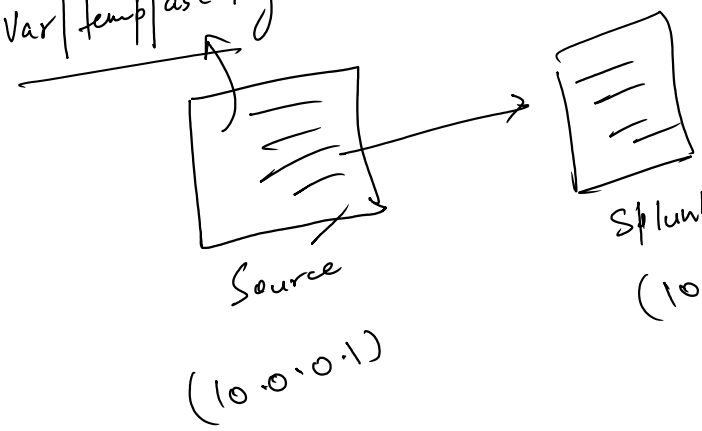
② Custom / App - data, you can ingest in splunk

③ License is consumed.

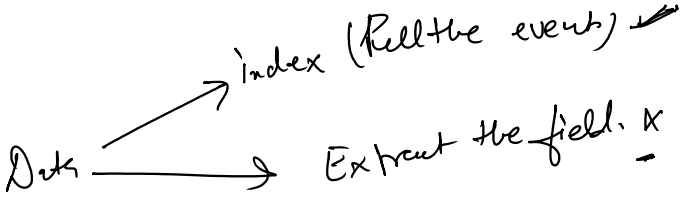
last = 10.0.0.5

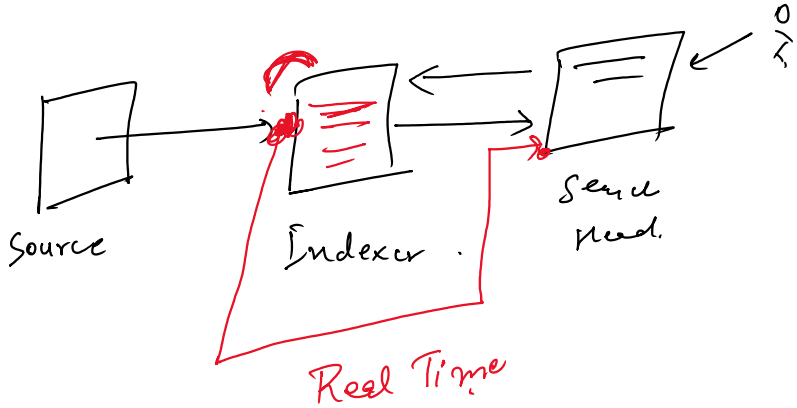
(3) Licence is consumed.

Log file
(/var/temp/abc.log)



host = 10.0.0.1
Source = /var/temp/abc.log
sourcetype = log.
↓
data type





SPL Commands:-

1. ~~Table~~
2. ~~Rename~~
3. ~~Sort~~
4. ~~Stats~~
5. Eval
6. Top
7. Rare.
8. chart
9. Timechart
10. Date & Time fun
11. Geomap
12. Single value Visualization
13. Append / Appendcol / Appendpipe
14. Addtotal / Addcoltotal.
15. Dedup
16. Rex

(6) Top

(7) Rare.

(14) Addtotal | AddColtotal.

(1) Table:- Tabular output.

Ex:- |table f1, f2, f3 - - -

(2) Rename:- Change the name of the field name at search time

Ex:- |rename IP AS Incident_number

(3) Stats:-

1. Count → No. of event.
   ↳ |stats count
2. Sum → |stats sum(—) as —
3. Avg → |stats avg(—), as →
4. Value. → Group the fields on specific value. Unique one
   " " " All the values.
5. List →

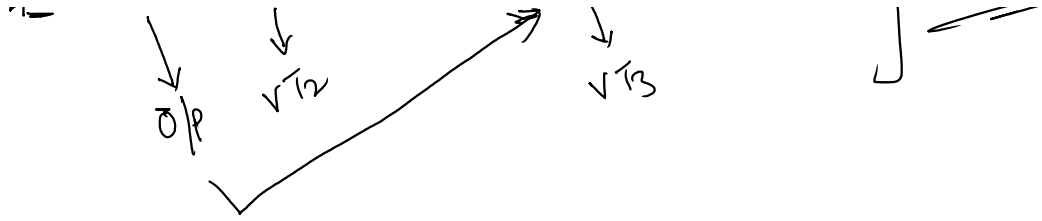
Virtual table

```
index="vk_idx" sourcetype="csv"
|stats count as total by current_ticket_state, severity
```

VT2 → Total VT=2

```
index="vk_idx" sourcetype="csv"
|stats count by current_ticket_state, severity | rename count as total
```

VT1, VT2, VT3 → Total VT=3



Sort:- Sorting purpose.

Ascending:- Sort count / Sort (+) count

Descending:- Sort - count.