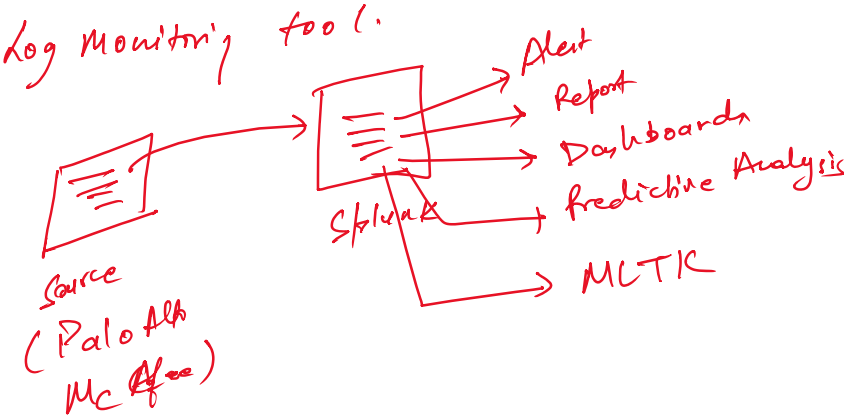
Day - 1

20 January 2026 19:31

Splunk :- Log Monitoring tool.



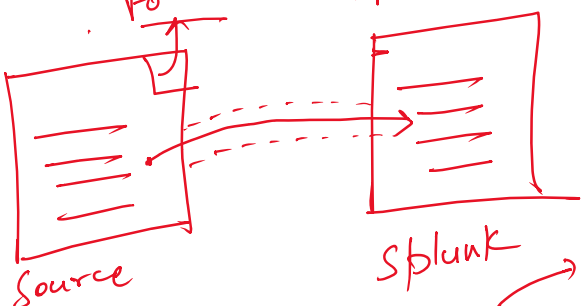
Components :-

1. Indexer
2. Forwarder.
3. Search Head.
4. License Master.

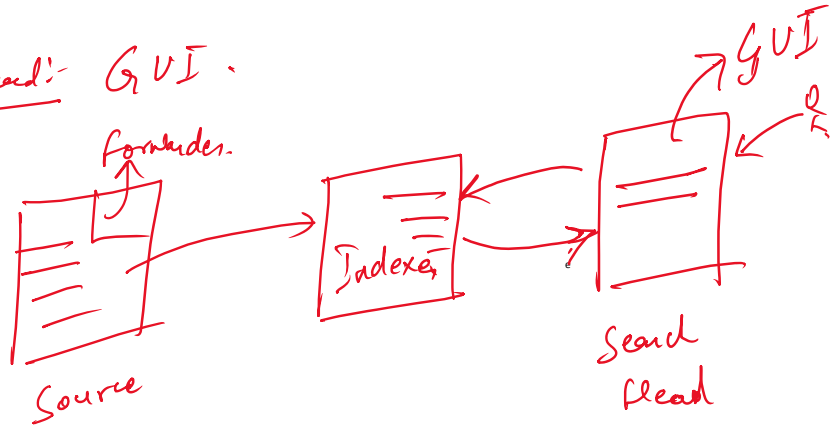
1) Indexer :-

→ Storage unit that will store the data in splunk.

2) Forwarder :-



(3) Search Head:- GUI.



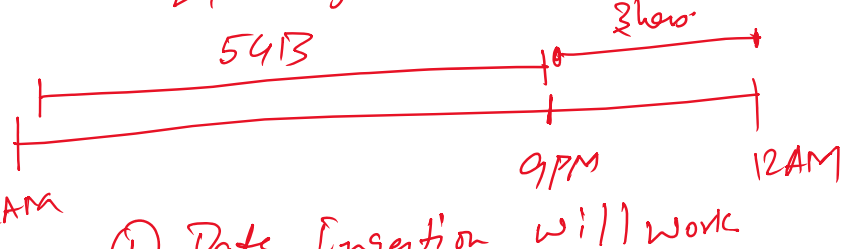
(4) Licence Master:- Policy Agent that will identify whether you have breached License or Not.

Parameters ?!! → Amount of Data, you are ingesting in Splunk.

5 GB/d → 1 year ⇒ $$

↓

24hour Cycle.

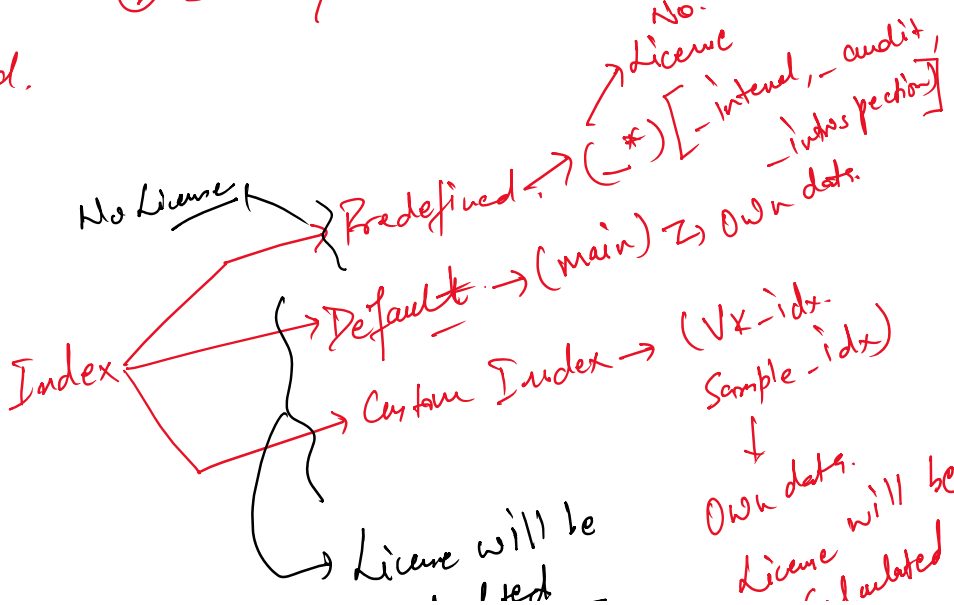


① Data Ingestion will work

② Searching will be disabled.

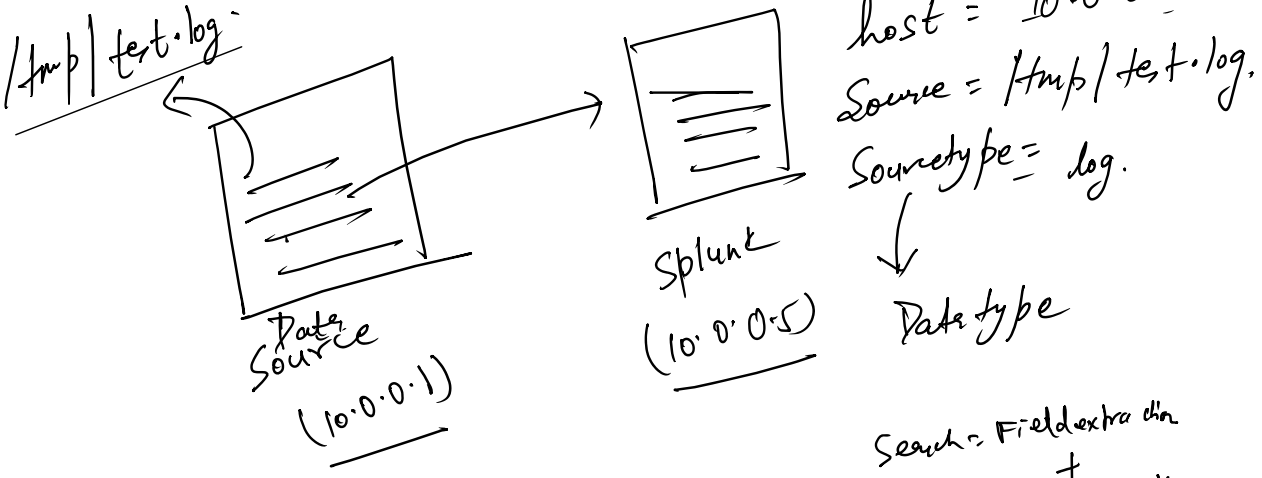
20-25 GB

50 GB/d.

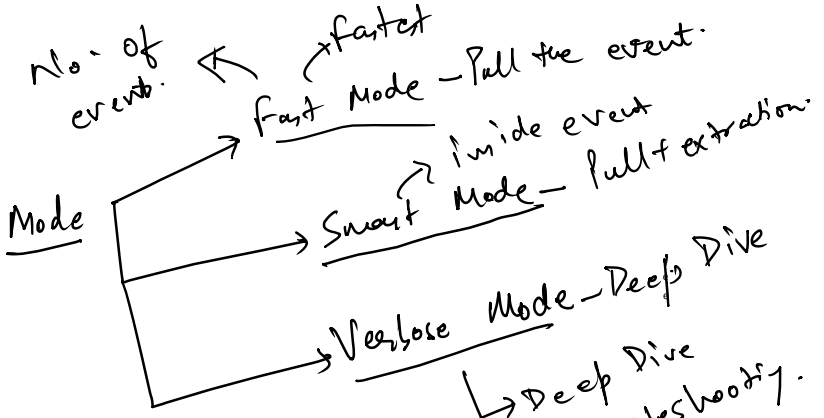


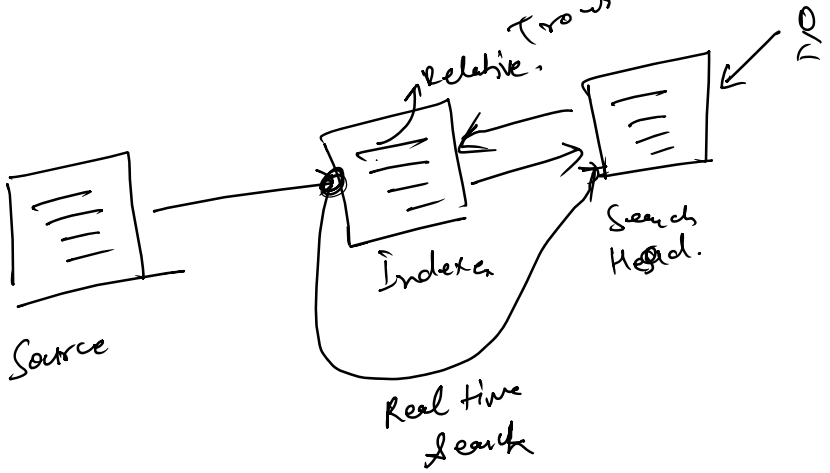
↳ Licence will be calculated

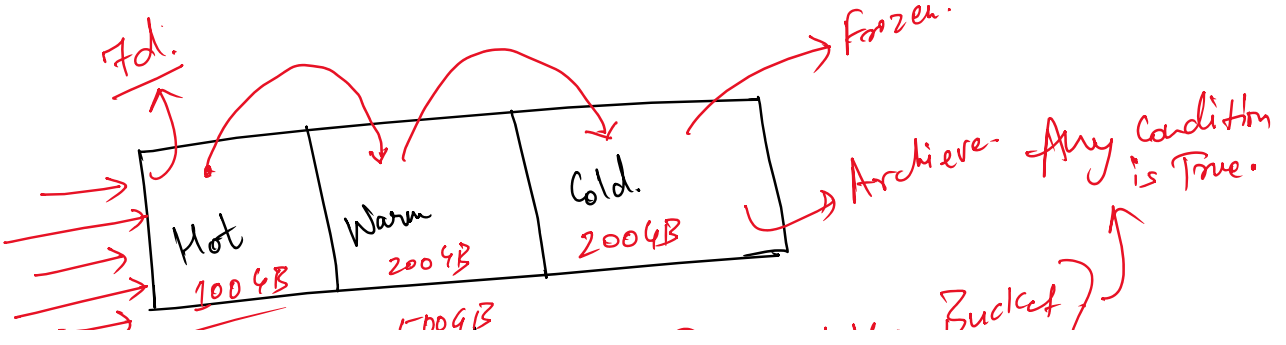
Licence will be Calculated

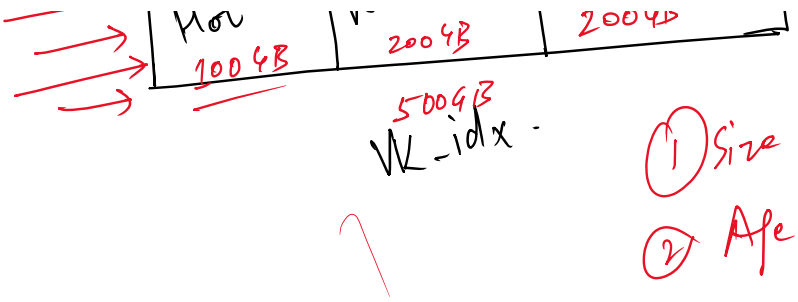


Search = Field extraction + Pulling of the events.









① Size of the Bucket
② Age of the data.

SPL :-

① Table.
② Rename.
③ Stats.
④ Eval.
⑤ Search.
⑥ Where.
⑦ fillnull.
⑧ top.
⑨ rare.

① Table :- Tabular output.

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

② Rename :- ex :- |rename oldname AS newname,

③ Stats :- Statistical output.

① count. - count of event.
② Avg.] → Number field. → |stats (avg(f1) AS ——
③ Sum.
④ List] → grouping Activity
⑤ Values]

|stats list(source) by sourcetype.
, values(source) by sourcetype

(5) Values -1 | stab

| stab values (source) by

fillnull - It goiy to handle the blank spaces.

fillnull → default = 0

A	B
25	15

Filtering :-

(1) Search = search A > 15

(2) where = where A > B

A	B
10	5
25	15

A	B
10	5
5	35
15	45
25	15

Eval = Evaluation purposes.

int a
str b
var c

eval a = b+c

(1) Calculation.
(2) if - else.
(3) Case.

eval. Kb = (bytes | 1024)

↓ initialize.

if - else :-

if-else:-

```
if (a>b)
  {
   print(a);
  }
else {
   print(b);
  }
```

→ if (a>b, a, b)

- a>b ↳ Condition.
- a ↳ True
- b ↳ false.

Case:-

```
switch(—): —
switch(—) : —
 .
 .
 .
default(—) : —
```

→ ~~switch (cond~~

Case (cond1, —, cond2 —, cond3, —, — — — — —, — — —, 1=1, "—")

1=1 ↳ Universal condition.

Top / Rare:-

| top sourcetype → By default, it will give top 10 values.

| top limit=3 sourcetype

| top limit=0 sourcetype
↳ Unlimited count.

① fields → Include | exclude the field from the output

② dedup → remove the duplicate values.

③ Sort → Sort severity → ascending, Sort -severity → descending.

④ head → pick the value from the top.

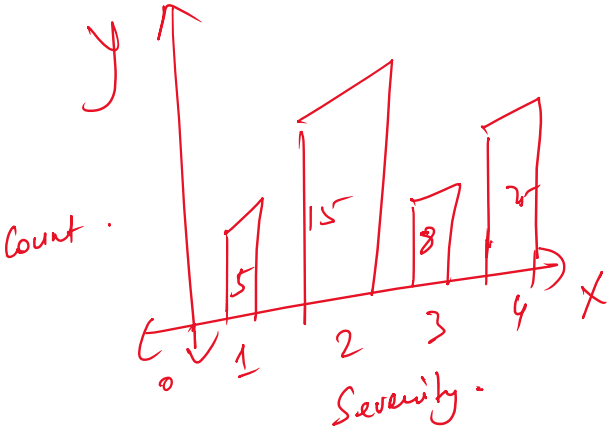
⑤ tail → pick the value from the bottom

Chart:-

| chart count by Severity

count → y-axis

Severity → x-axis.



Tomorrow:-

① timechart.

② geoMap

③ Style Value Visualization

④ Field Extraction.

⑤ Tags & eventtype.