Day - 1

16 July 2025 19:02

Splunk :- log Monitoring tool

1. Alert
2. Report
3. Dashboards.
4. Knowledge object.
5. MLKT (Machine learning toolkit)

1. ~~log Monitoring.~~
2. splunk APM
3. splunk Observability
4. ~~splunk ES~~
5. ~~splunk ITSI~~
6. splunk MLTK
7. ~~splunk SOAR~~
8. splunk UBA
9. splunk Vector.

Adv.:-

1. Ingest data from any Sources.
   .. of Any Data Type
   (XML, json, txt, csv, etc.)
   → Structured / semi structure / Mixed Data
   ↓ ↓ CSV + json
   CSV ↓ CSV + XML
   XML/json
2. "
3. Customer Support.
4. Transformation.

CST
EST
MT

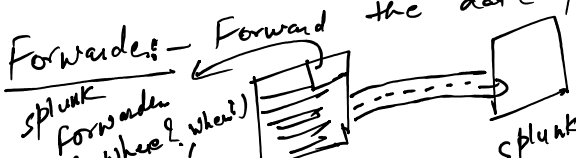
1PM EST - Lunch Break
11:30 AM EST - Tea 1
3:30 PM EST - Tea 2.

Disadv:-

1. Cost of license.
2. seperate setup for every features.

Component of splunk :-

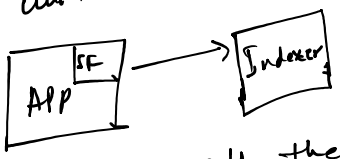
1. Forwarder:- Forward the data from the source to the splunk end.



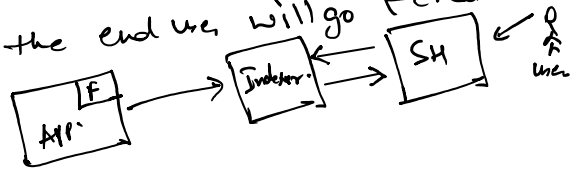
store your data.

1. splunk forwarder (What?, Where?, When?) → App. → splunk.

2. Indexer:- Storage unit where you can store your data.



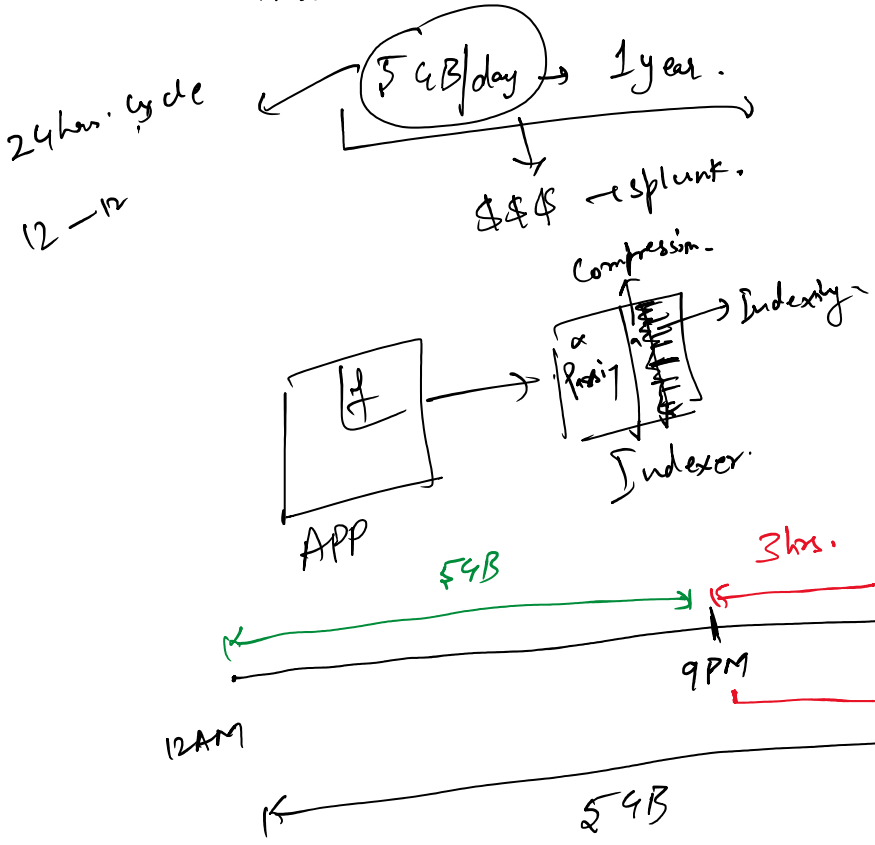
3. Search Head:- GUI where all the end user will go & create Dashboards, Alerts, Reports.



4. License Master:-

What is parameter on which licene is calculated?

How much data ingested in splunk on a daily basis



(1) Data ingestion will continue.
(2) Searching will be disabled

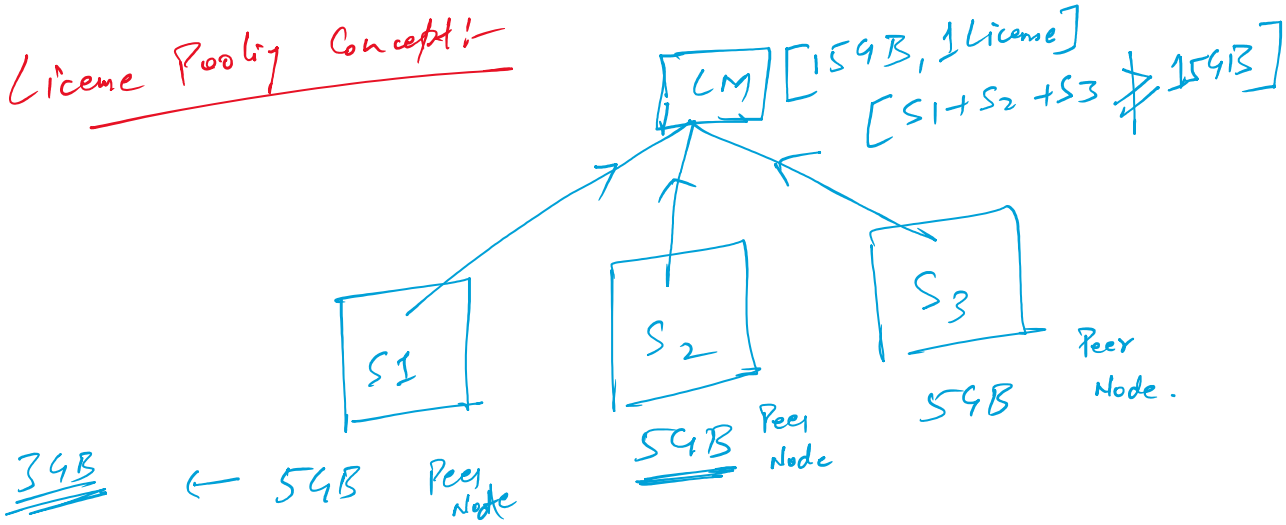
Blacklist ← 5 times → Violation → 30 days.

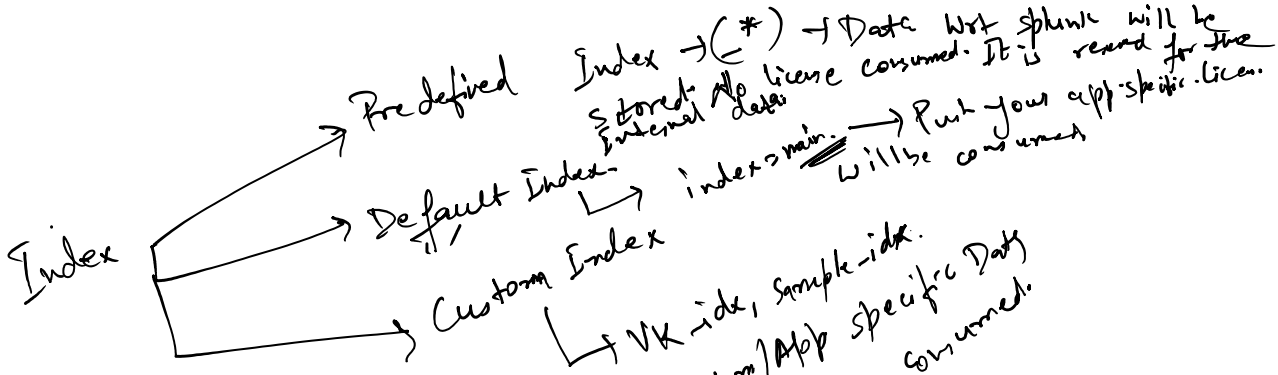
2 times / month → 2GB X2 = 4GB X12 = 48GB → data.

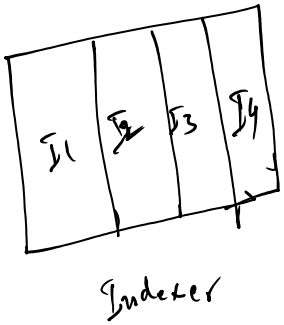
4GB → 1 Month

Free of Cost

License Pooling Concept:-





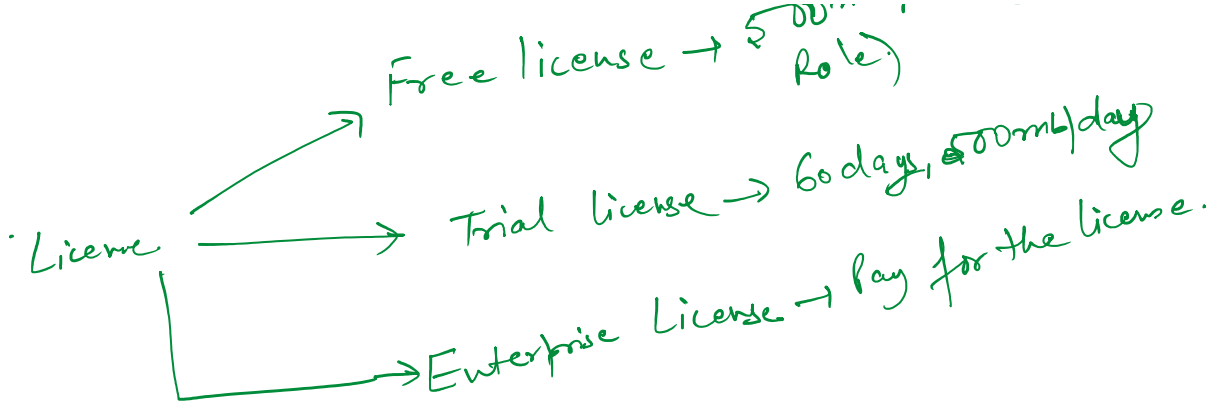


Search Mode:-

1. Fast Mode – Pull the list of event.
2. Smart Mode – Pull the event + Extract the field.
3. Verbose Mode – Pull all the event.

1. Pull the list of event.
2. Extract the field.

Free license → 500mb/day (Not work like Real time Authentication Role)



Commands:-

1. Table.
2. Rename.
3. stats
4. eval
5. fillnull
6. sort
7. addcoltotal
8. addtotal
9. chart
10. timechart
11. append
12. Conversion.
13. string.
14. Comparision & Conditional.
15. Info.
16. Mathematical
17. Cryptographic.
18. Multimv
19. mvexpand.
20. makemv.
21. Transaction.

1) Table:- tabular output.
Syn:- |table f1, f2, f3 - - -

2) Rename:- rename <old name> AS <new name>

3) Stats:- statistical output.
(1) count - |stats Count by asset_id.
- |stats sum(field) as field_name.

(3) Stats →

1. count –
2. sum –
3. Avg
4. list
5. Values

| stats sum(field) as field...

Sort – Sort – <fieldName> → Descending

Sort <fieldName> | Sort + <fieldName> → Ascending order

(4) Eval:- eval command used for evaluation activity.

int / var / str } eval a = Calculation

1. Calculation. →
2. if-else statement. →
3. Switch statement →

if (a>b, a, b) → True / false

Condition

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

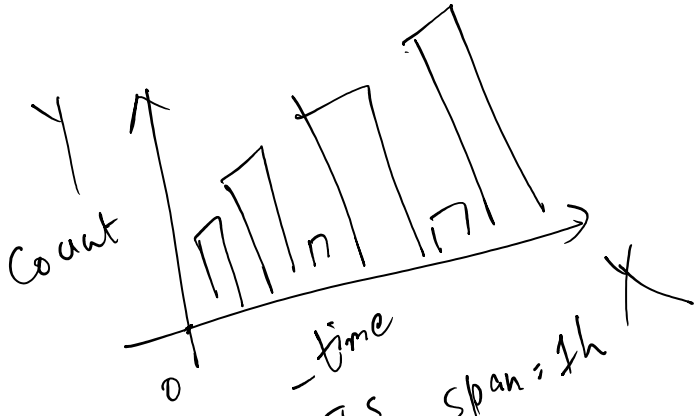
```
Switch (a):
Switch (b):
Switch (c):
default (1=1):
```

→ case (cond1, "—", cond2, "—", cond3, "—", 1=1, "—")

Visualization

① chart →:- | chart count by current_ticket_state
count → y axis
current_ticket_state → x-axis

② timechart



| timechart count by CTS span=1h

③ Single Value — Single output in the Letters / Digits

Addcoltotal → Addition column wise.

Addtotal. → Addition row wise.