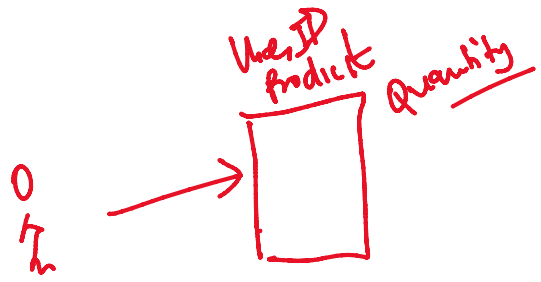
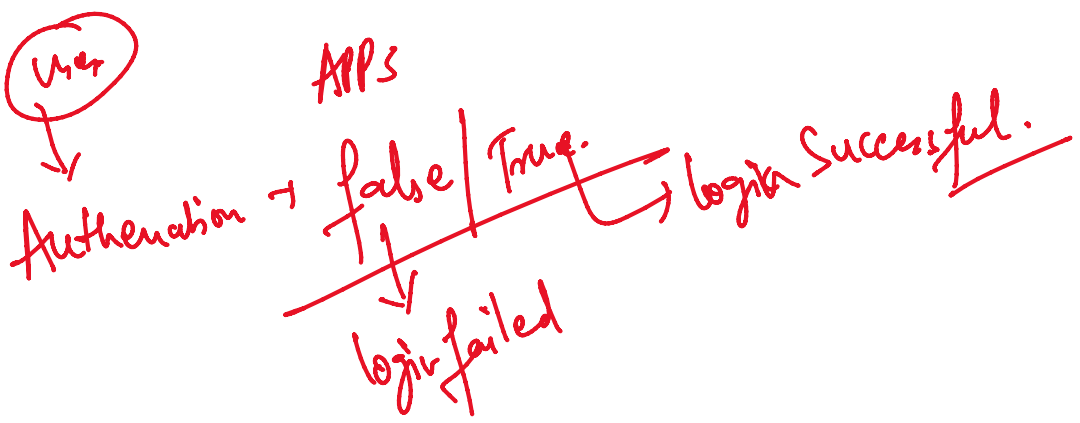
Day - 1

19 August 2024 09:24

1. splunk.
2. History
3. Architecture (Components of splunk)
4. Use Cases.

1. History :-





1. Data Storage :-

Structured Data → CSV,

Semi-structured → XML, json.

Unstructured → Audio, Video, Image.

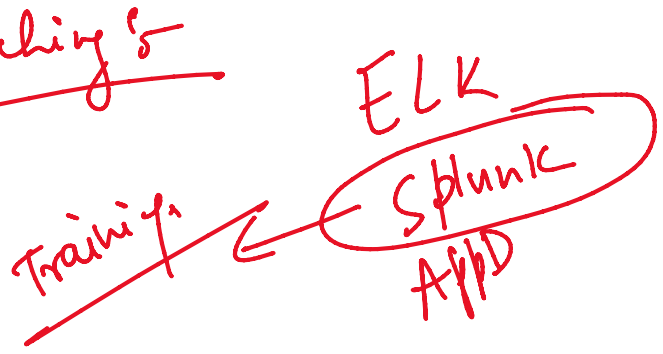
1. Real Time Monitoring
2. Trend Analysis.
3. Prediction.

ML

DL

Model

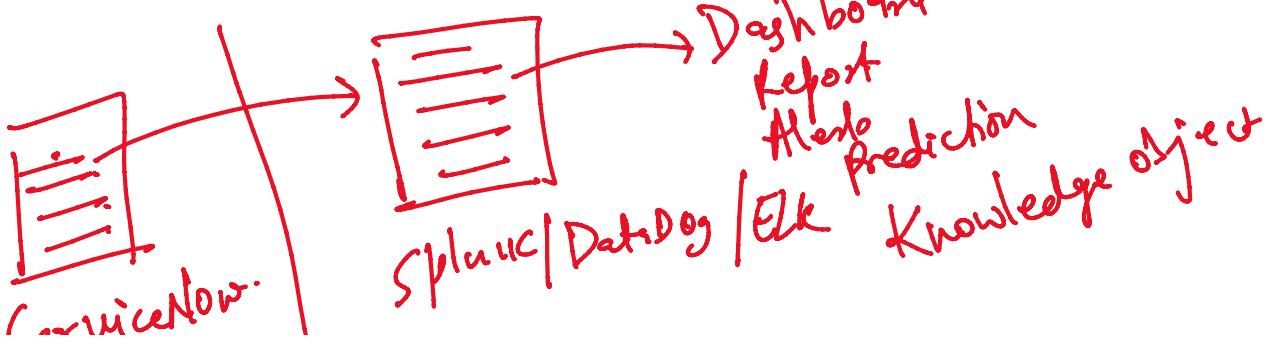
2. Searching :-



DataDog

Nagios

Dynatrace.



ServiceNow. | Splunk/...
(ITSM)

③ Splunk :- Monitoring Tool

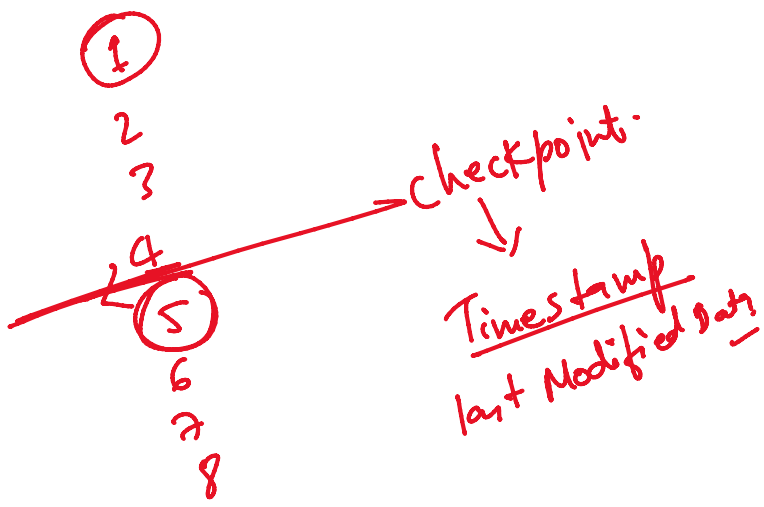
① Any source → Linux, Windows, AWS, Azure | Twitter, SNOW, Jira, Netflow, Fiscore, Pabitra

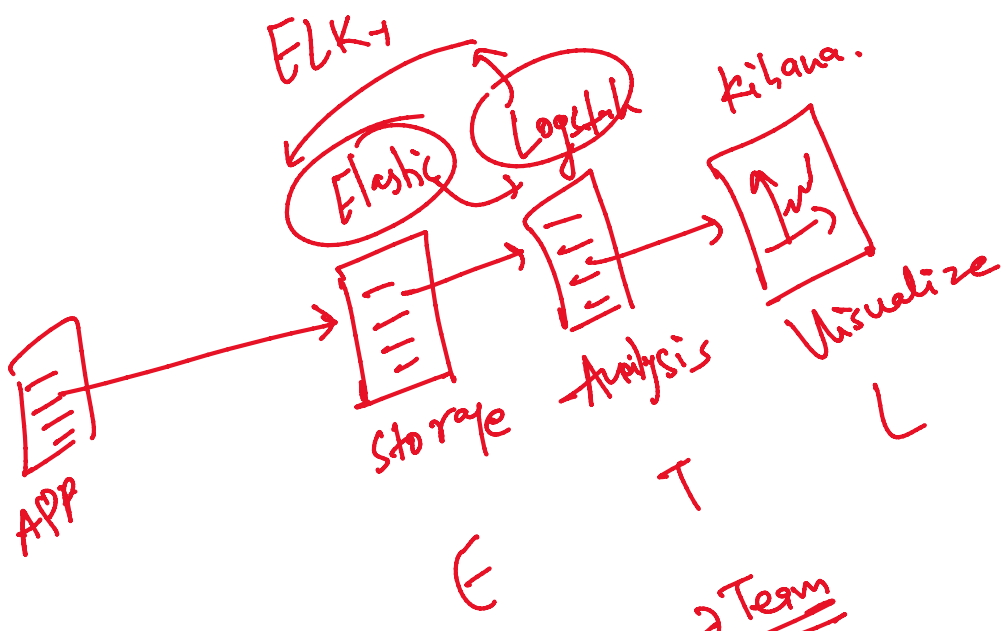
② Any Data type.

① Dashboard
② Report
③ Trend Analysis
④ Prediction.
⑤ Visualization
⑥ Knowledge object

Benefit splunk:-

① Any Source & Any type of Data.
② Integration with the Same Application.
③ Customer support.
④ All Component Comin in Style Package.
⑤ SPL → Search Processing Language → MySQL

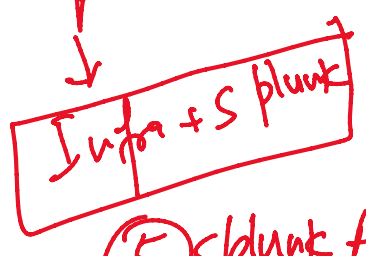


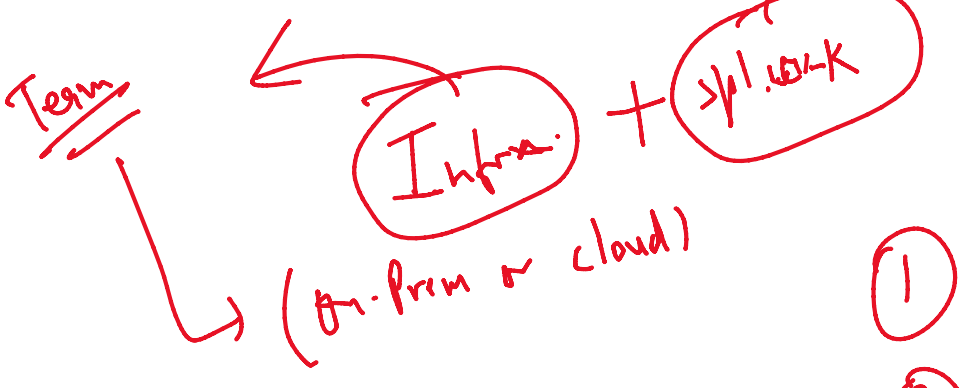


Cons:-

① Mid Size Org.
Costly.

② splunk cloud.





① Splunk ES
② Splunk SOAR
③ Splunk ITSI
④ Splunk UBA
⑤ Splunk APM

Management Interface

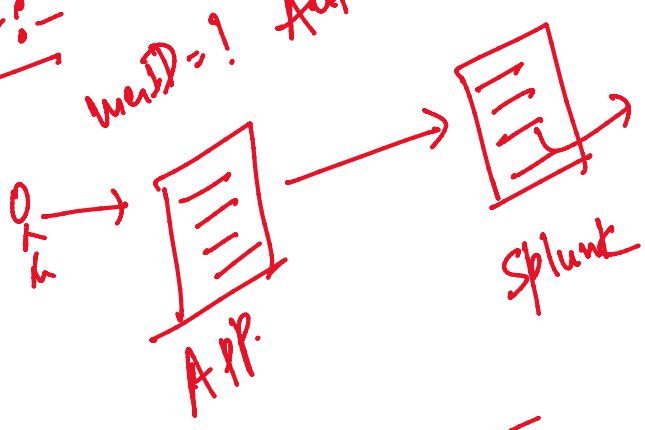
④ Splunk

Component of splunk :-

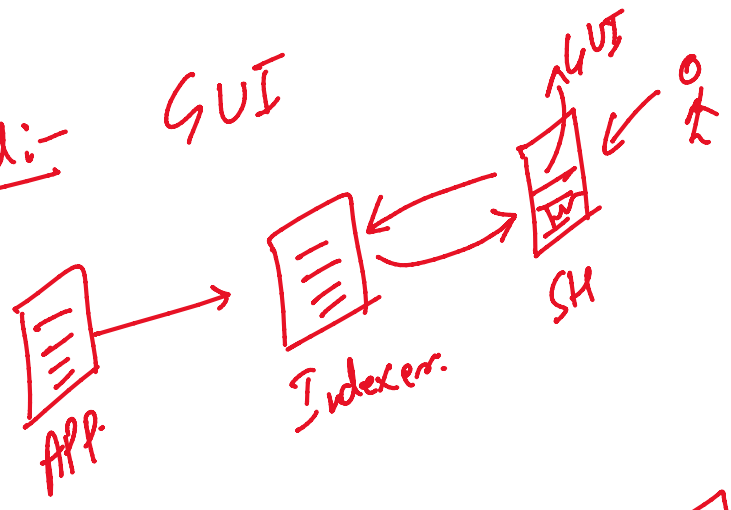
- ① Indexer.
- ② Search Head
- ③ Forwarder.
- ④ Licence Master.
- ⑤ cluster Master.
- ⑥ Deployer.
- ⑦ Deployment Server.
- ⑧ Search Captain

① Indexer :-

storage / Repository where you can store the incoming data.

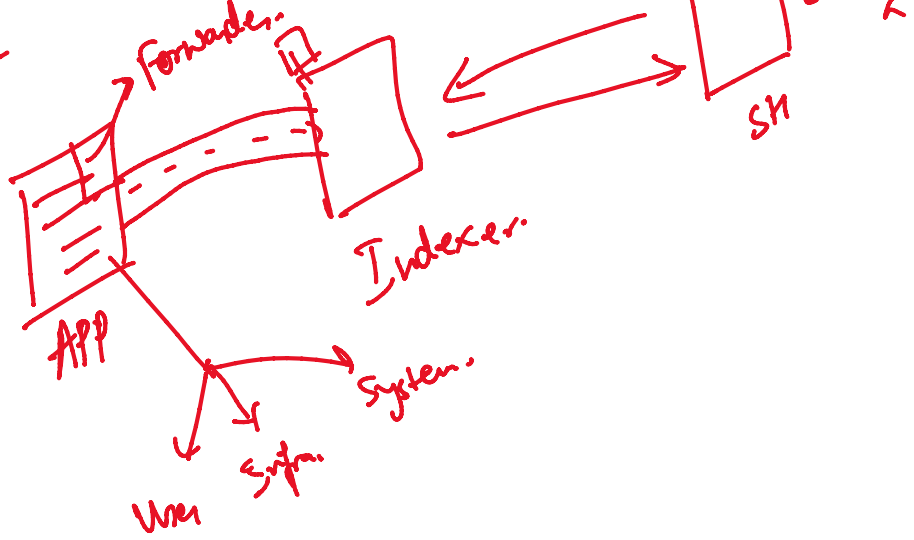


② Search Head :-



③ Forwarder :-

forward the data from the source to the Indexer level.



④ License Master :-

Pay to splunk.

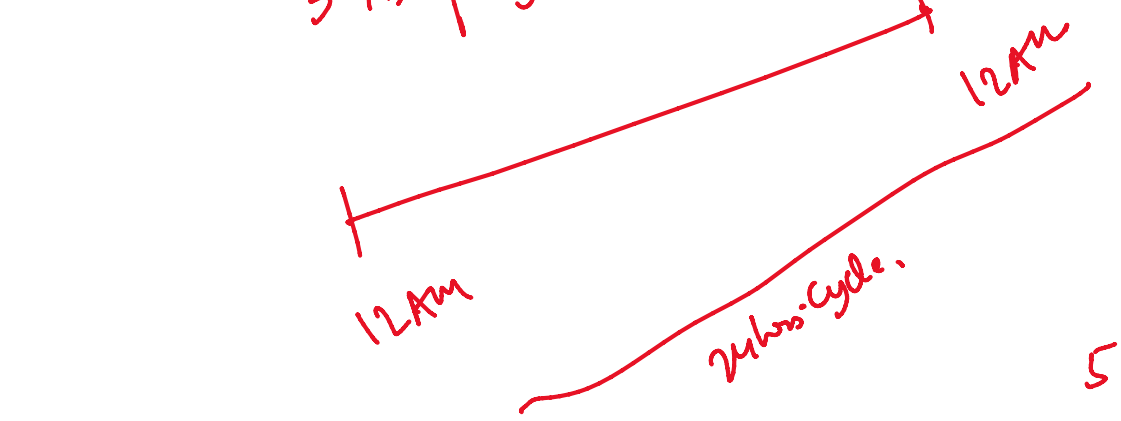
Parameter the license is calculated?

① Data Volume.

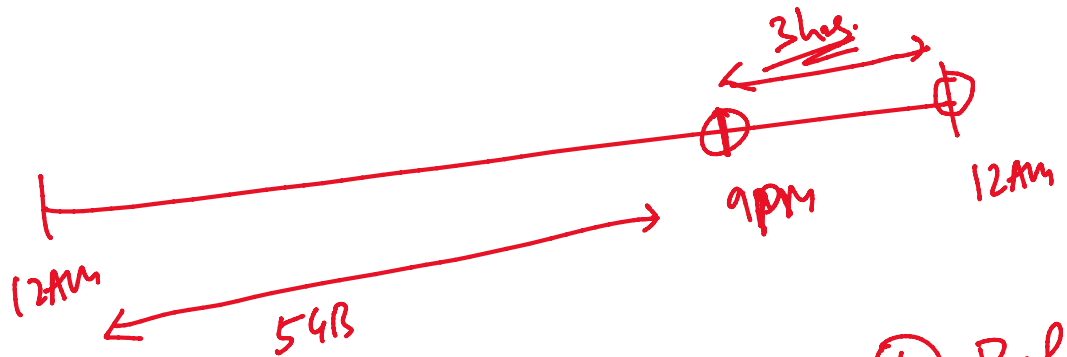
② Consumption of Computational Resources

e.g. 1 day → 1 year.] → $$$

5GB/day → 1 year.

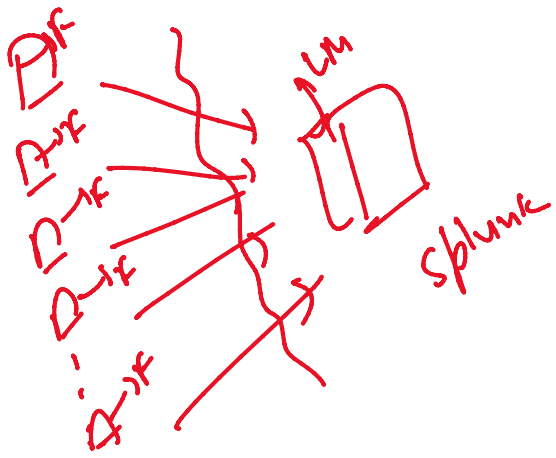


5GB/day.



① Before License Breach.

② After License Breach.



① Backup DB

②

① Indexing will continue.

② Search will be Disabled

↳ Stable Mode

↳ Dashboard

↳ Alert

↳ Report

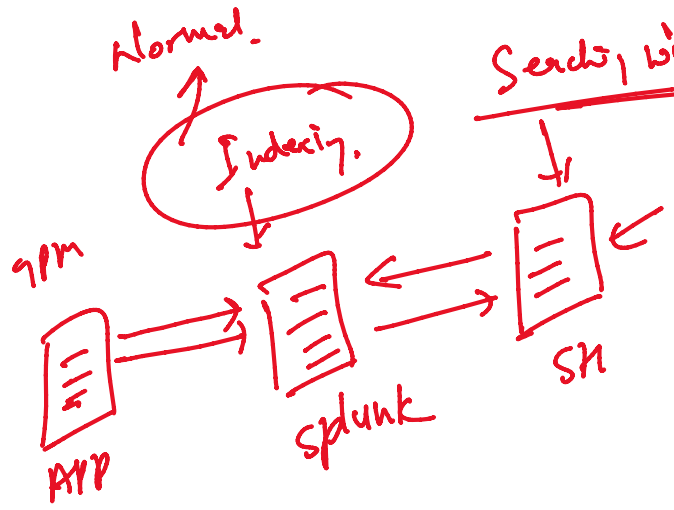
↳ Data Model

↑ Search Query

Nothing will work.

↑

Stopped



Advance / Up front payment.

Factors:-

① How many data Source?
② How much data flowing?

③ Future prediction.

④ Budget.

① Admin. → Source → splunk

② Developer → splunk → DB
↳ Read
↳ Write

③ Format
④ Buffer

Index :-

① Type of Data.
② How much Data eps
③ why I.I
④ Start date

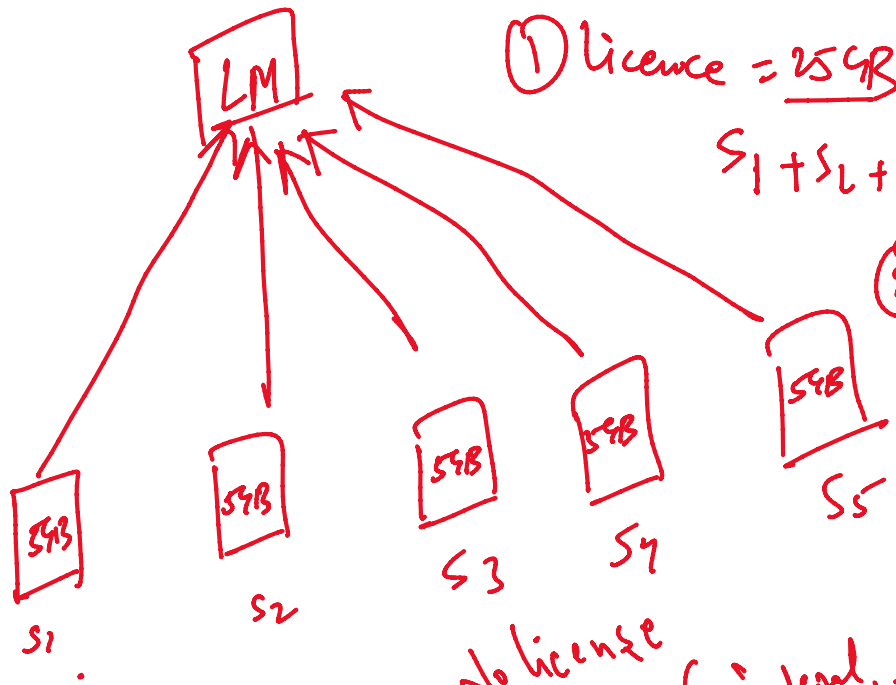
⑤ Sample Data.
xx xx
Format
, skip , No Data Ingestion.

⑥ PII

⑦ Retention of Data.

CAB → Change Advisionary Board.

License Pooling :-



① licence = 25GB
$S_1 + S_2 + S_3 + S_4 + S_5 \neq 25GB$
② Management
③ Cost will change

no license
↑ * (_intent, _audit, _introspection...)

Index
- Predefined = _
- Default = main → Index Name.
- Custom Index := User create own index

→ License Consumed.
→ App. Specific data Comy.

① New stanza.
② Force (salt)

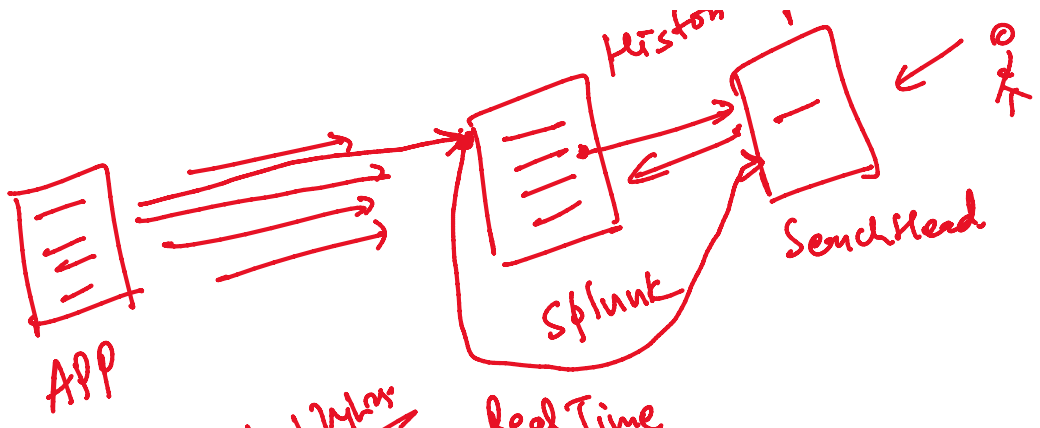
1 → main.
2
3
4
5 → Snow

[———] disabled = 0 → rewrite index = main → 3 event

[———] index = Snow, sourcetype = src-sc, disabled = 0 → 4,5 event

Historical/Relative.

Disadv. Real Time :-



Disadv. Real Time:-

① Indexer → Ingestion Should across the SH.

② Computation Resource Consumption is higher.

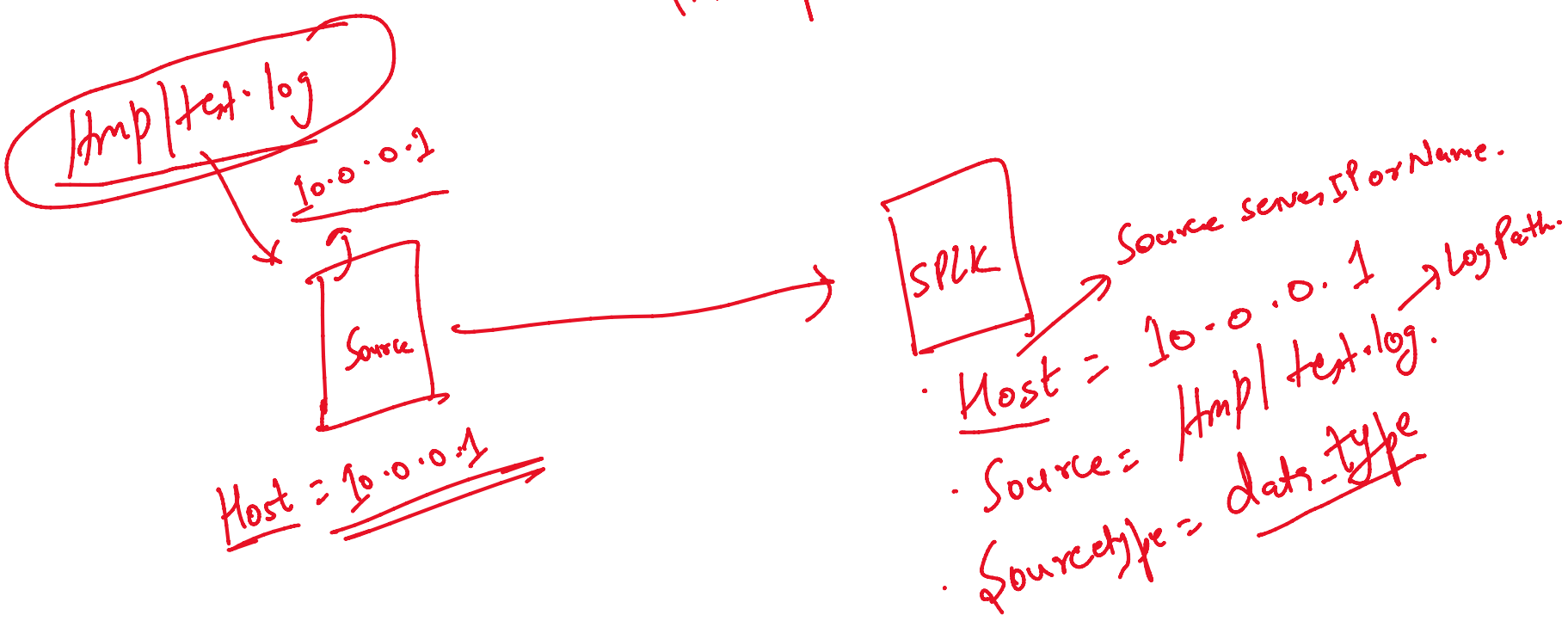
Relative vs Real Time → last 24hrs

↓

No clarity

Real Time

Not to use the Real Time Search - Or. Use for minimal Timespan like last 1 min, but 5 min. max.



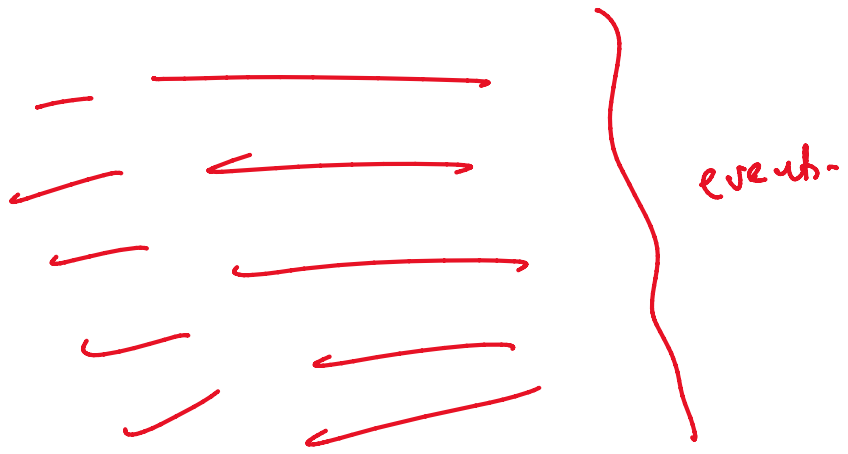
Fast mode > Smart Mode > Verbose Mode.

Run the search Query → Events, fields.

Verbose: Fields + Events + Statistics

Fast Mode :- Event

Smart Mode :- Events + Fields.



10. Top & Rare

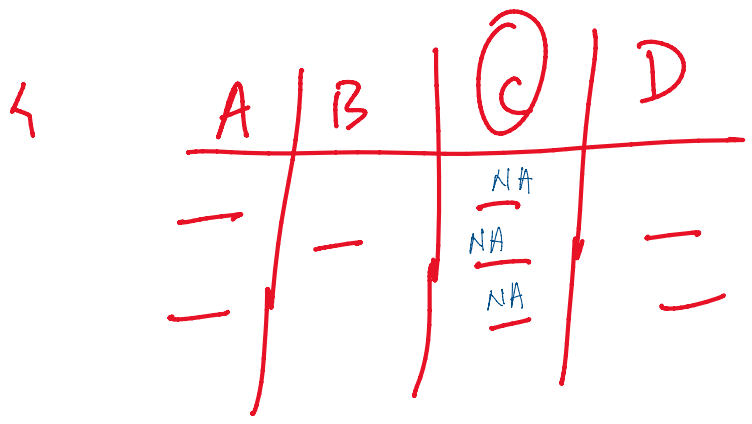
Commands:

~~1.~~ Table
~~2.~~ Rename
~~3.~~ Dedup
~~4.~~ Sort
~~5.~~ fillNull.
~~6.~~ stats.
~~7.~~ Eval
8. Where
9. Search.

① Table :- Showcase data in tabular format.

Stats → statistical outputs

- Count —
- Avg — } → Numeric field.
- Sum —
- List
- Values



fillnull value = "NA"

fi line "N"

Fillnull:- ① Default value of fillnull command is 0.

② fillnull value = "NULL" → Customize the value of all the column.

③ fillnull value = "NULL" total_bytes → Customize the blank spaces for total_bytes column.

List & Values:- Group of data on the basis of field.

int(a)

a = 3+4

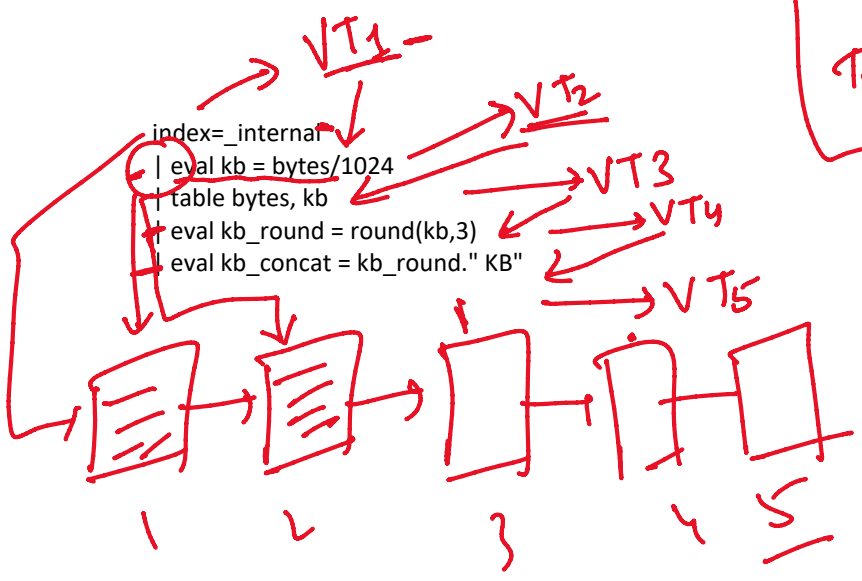
Eval ___ = ___

eval

Calculation if-else Case Statement.

bytes → Kb

eval Kb = bytes/1024



Total VT = 5

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

eval ——— = if (condition, true, false)

Resolved → Completed.

Closed

In-Progress

Customer Hold

Pending. → InComplete

Case statement :

↓

Switch.

Case(0): Mon

Case(1): Tue

⋮

default: Sunday

Mon

Tue

Wed

⋮

Sunday

Case(Cond1, True, Cond2, True, Cond3, True ----, 1=1, ———)

Ex

1 → Critical

2 → High

3 → Normal

4 → Low