Day - 4(30th May)

29 May 2024 18:02

1. Field Extraction
2. Transaction.
3. Classic Dashboard
4. MC on Indexes
5. Licensing.

1) Field Extraction:-

1. Regular Expression →
2. Delimiter → split the event on the basis of certain Symbol.

(space, comma, Tab & Pipe).

2) Licensing:-

1. Trial license
2. free licence.
3. Enterprise licen.

1) Trial license:-

60 days → 500 MB day ingestion per day.

2) Free license:-

500MB of data ingestion per day.

Disabled:-

1. Authentication.
2. Real time search.
3. User & Role.
4. Data Model.
5. Saved search.

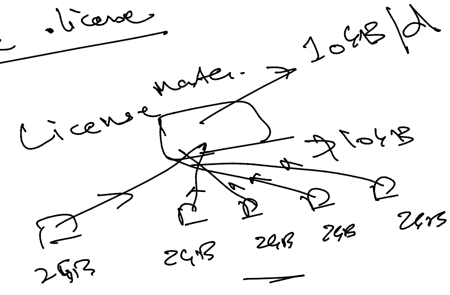
3) Enterprise license:-

Pay as per the requirement. Upfront payment.

③ Enterprise License:- Pay as per the requirement payment.

5 GB data/day → 1 year → $$$

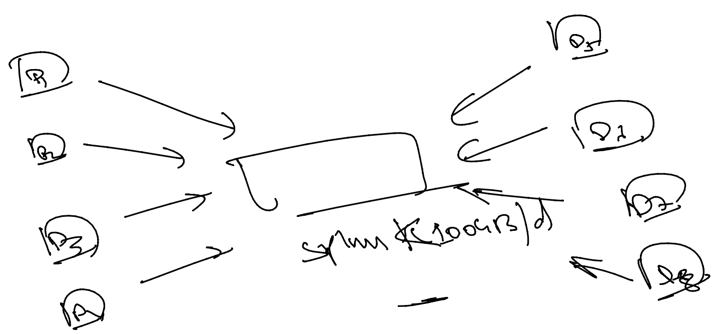
License Policy:- → flexibility to ingest amount of data you want to each server - But it should be less than over all Quota. abc license



(no restriction)

② Bulk buying, 5 servers:- 2GB per server
it will be cheaper.

↑ Costly →



③ Dashboard:-

→ Classic Dashboard → XML

→ Studio Dashboard → json, V8.2.x

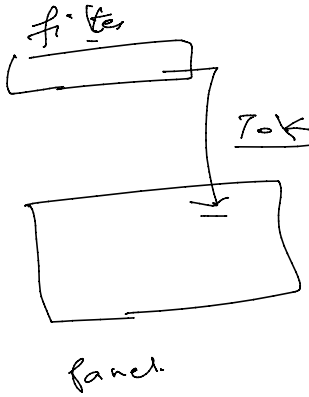
Classic Dashboard (XML)
→ Static Dashboard →
→ Dynamic Dashboard →

① Add input
② optimization → saved search, Base search, summary
③ Drill Down.

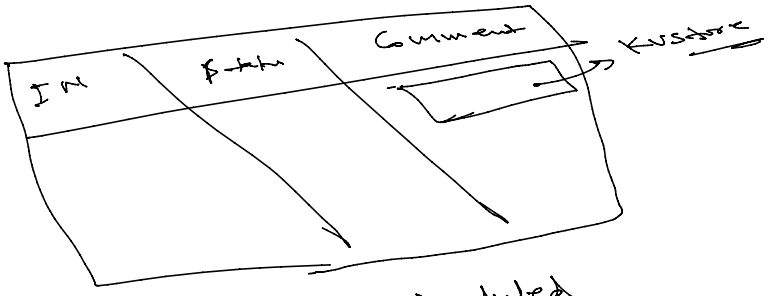
① Add Input.

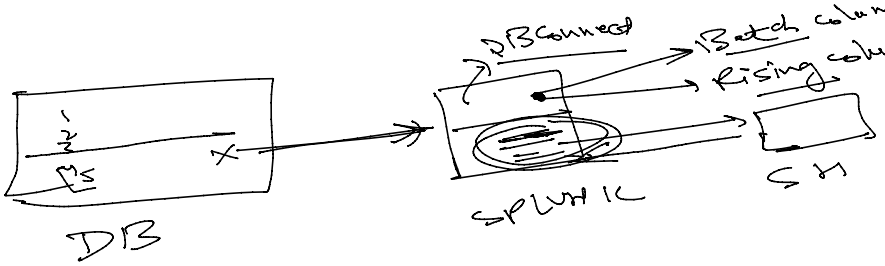
① Time filter
② Drop down
③ Multiselect
④ Radio
⑤ Check box
⑥ Submit

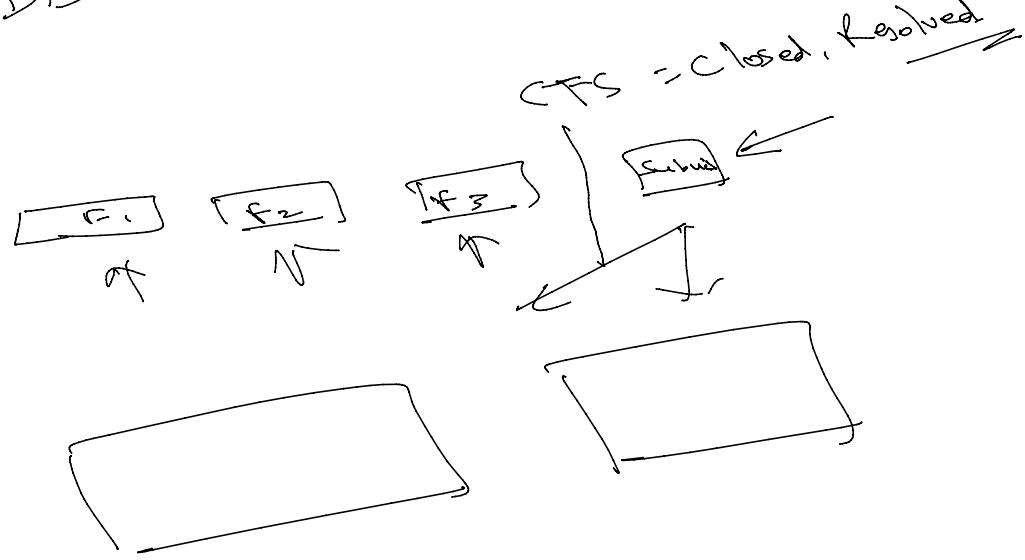
→ Single dropdown
→ Multi select



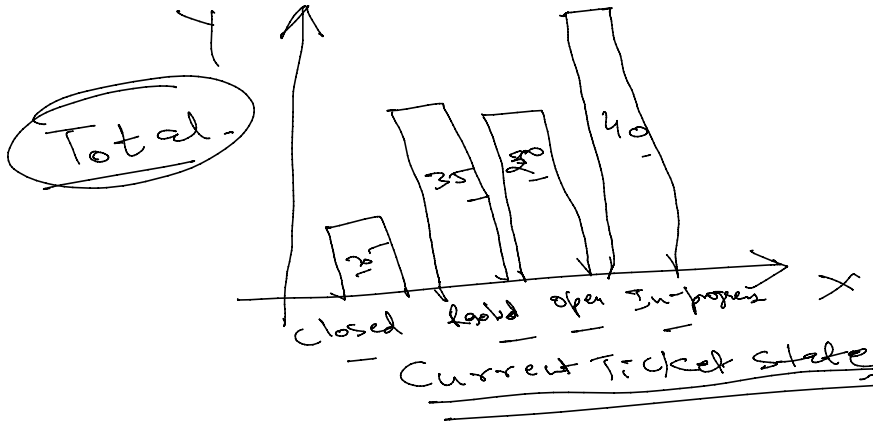
Token (Carry the selected Value from the filter to the Panel level)







② Drilldowns



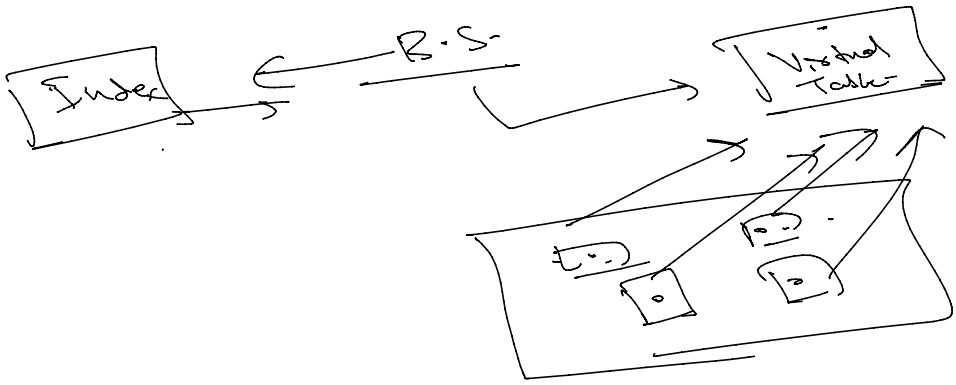
click-name = CTS

click-value = closed, Resolved, open

click.name2 = Total

click.value2 = 25, 35, 30, 40

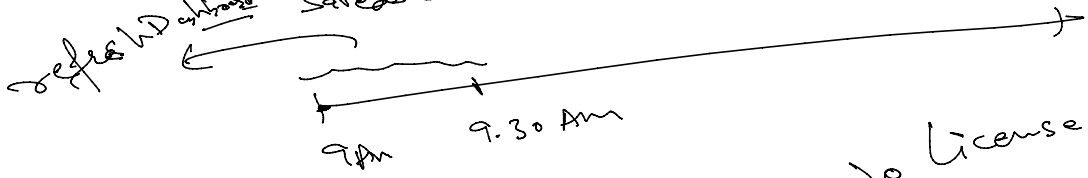
① Base Search :- 4 times hitting the Index.



① Base Search.
↓
Statistical o/p
↓
table, stats, tstats, more.

Base Search → contains Data.

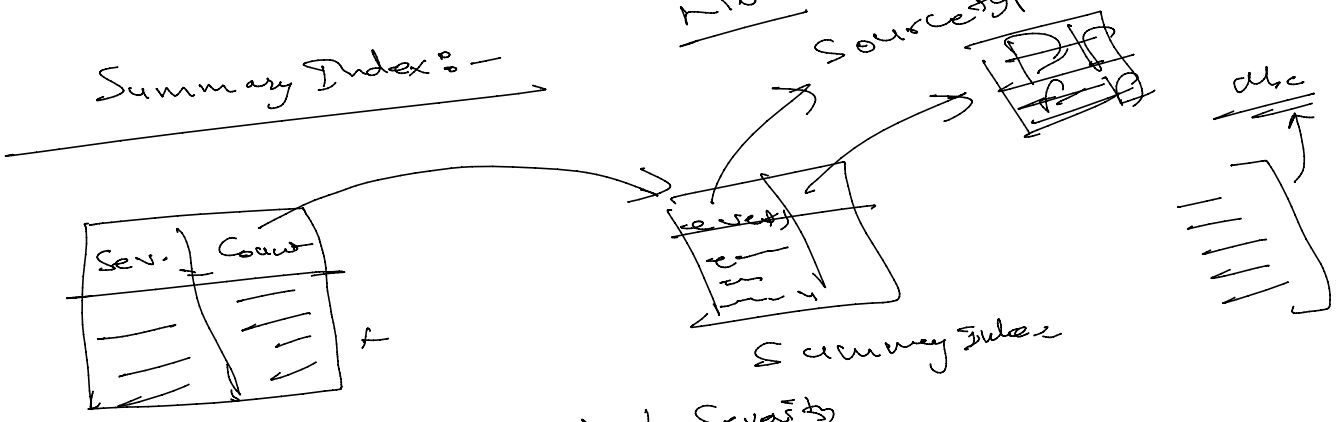
SavedSearch → Interval Basis. every 15min, every 30min



Summary Index :-

No License

sourcetype = stash



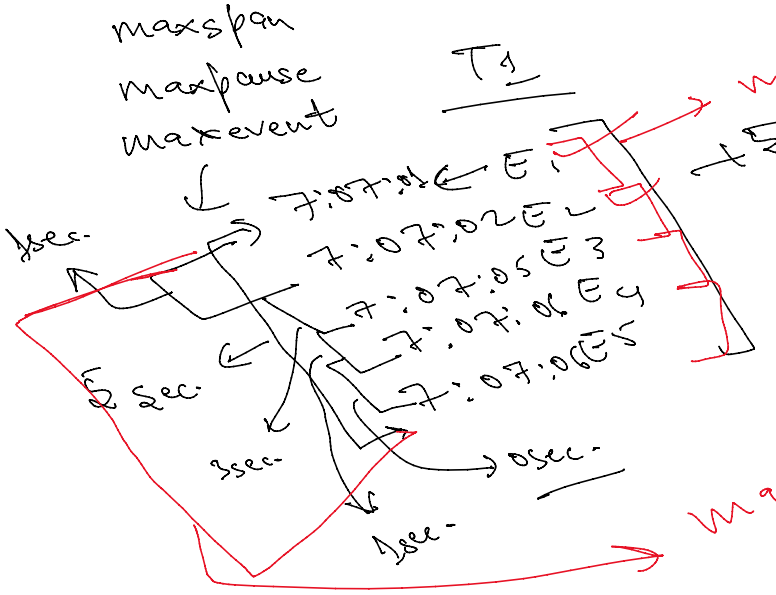
index = main | stats count of Severity

* Transactions

Bank Transaction:-

Beneficiary Name
Account
Sender Account
Time
How much.
Device
Which Bank
IMPS / NEFT / RTGS

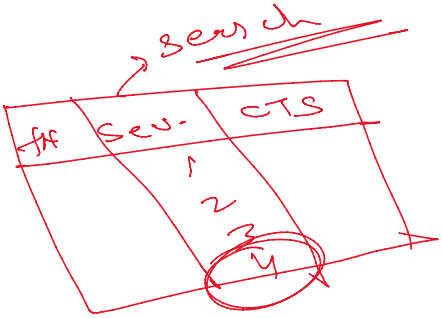
Transaction
I
Combination of events or steps
Certain parameters
↳ TransactionID, IP
Statistical o/p



maxpause = 5 sec.
0, 1, 2, 3, 4, 5

maxspan → 10sec. [0-10]

Search & where Commands



Search sev=4

Where: TT > Threshold

tt	Threshold	TT
	1800	15000
	1800	1600
	1800	1900

Conditional statements

if ——

else ——

Set

Unset

1. Inputs
2. optimized
3. Integrated with js.

Assignments

1. Radio Button.
2. checkBox Button.