Day - 4 & 5

11 July 2024 09:52

1. License setting.
2. Dashboard.
   i. classic Dashboard → XML
      a. Static Dashboard
      b. Dynamic Dashboard.
      c. optimization Dashboard.
      d. event Handler.
   ii. Studio Dashboard → - json

(1) License Setting :-

i. Trial license. → 500MB, 60 days.

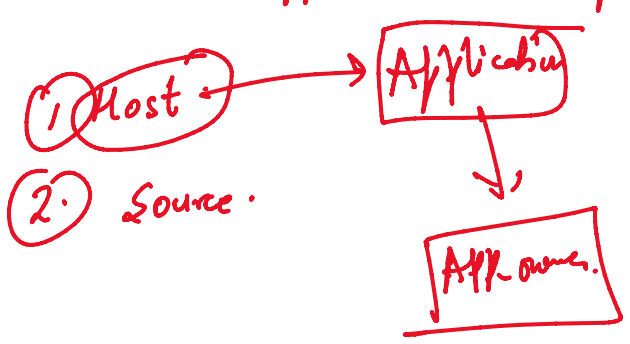
ii. Free license. → 500 MB/day, lot of feature disabled. Auth., User Role, Real Time, Alert Notification.

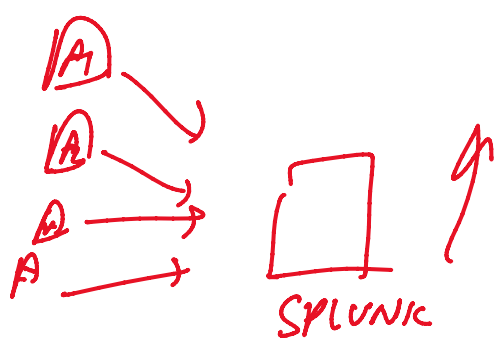
iii. Enterprise License. → Pay as you need.

5 GB/d → 1 year → Splunk sales.

$ $ $.

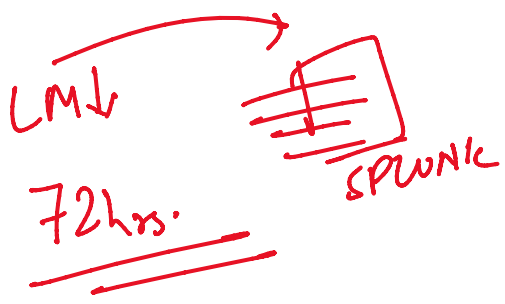
License ↑ → which App. led to spike in license.





A1 → Meant.
A2 → Meant
A3 → meant

Top 5 host
host → trend.

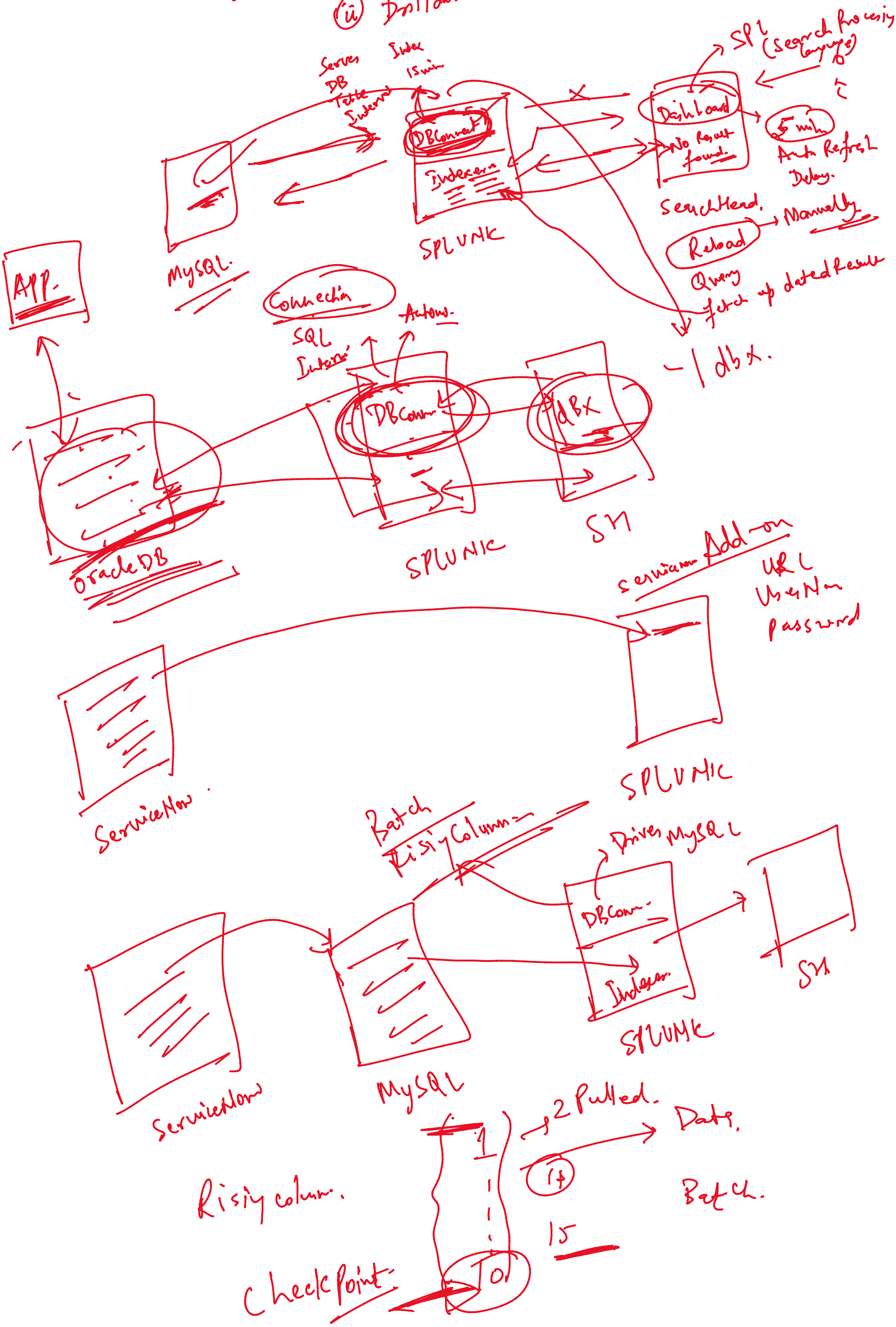


3 GB ↑ ↑ 4.8 GB

(2) Dashboard :- Combination of Panel is called Dashboard.

Classic → XML

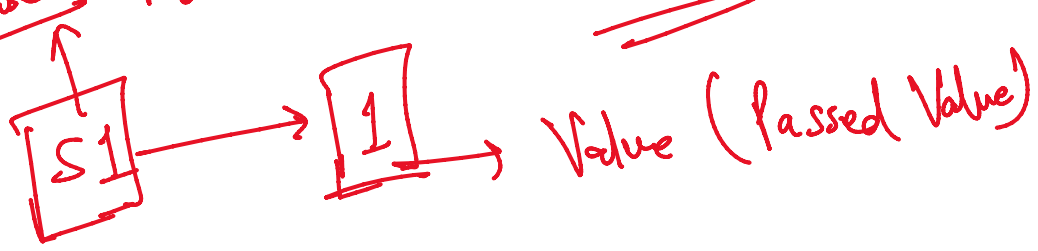
Dynamic → (i) Different input.
(ii) Drilldown.

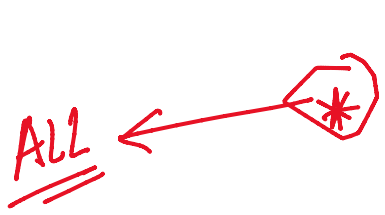


Concurrent Search Limit →

Label (Displayed)

limits.conf.





1
2
3
4

Assignment 2:-

① Radio Button. (Hint:- Functionality same as single dropdown)

② checkbox input (Hint:- Functionality same as multi dropdown.

Submit Button:-

Drilldown:-

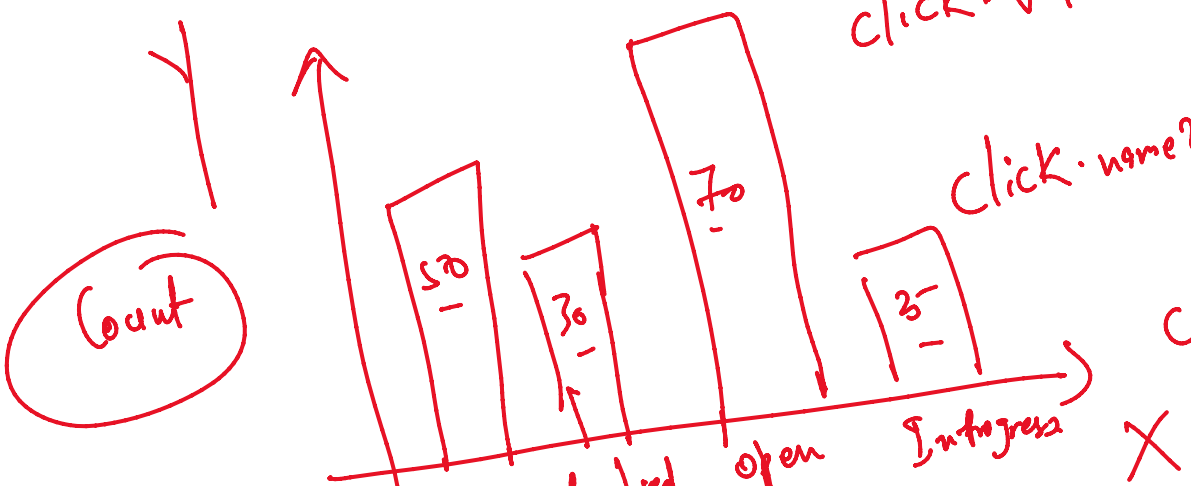
↳ Drilldown to the next set of Dashboard, same dashboard you want the specific value.

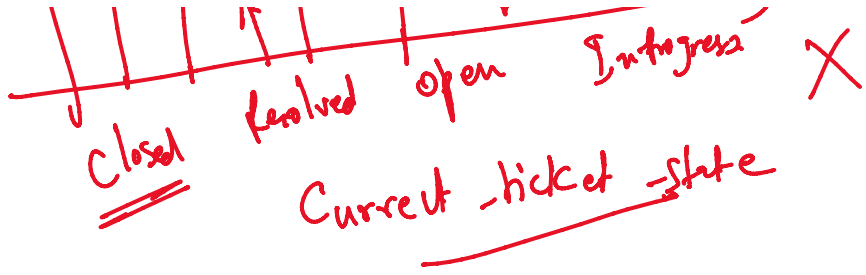
click.name = name of x Axis (Current ticket state)

click.value = Value of x Axis closed, Resolved, open, In-Progress

click.name2 = y-axis name [Count]

click.value2 = Value in y-axis (50, 30, 70, 25)





earliest →

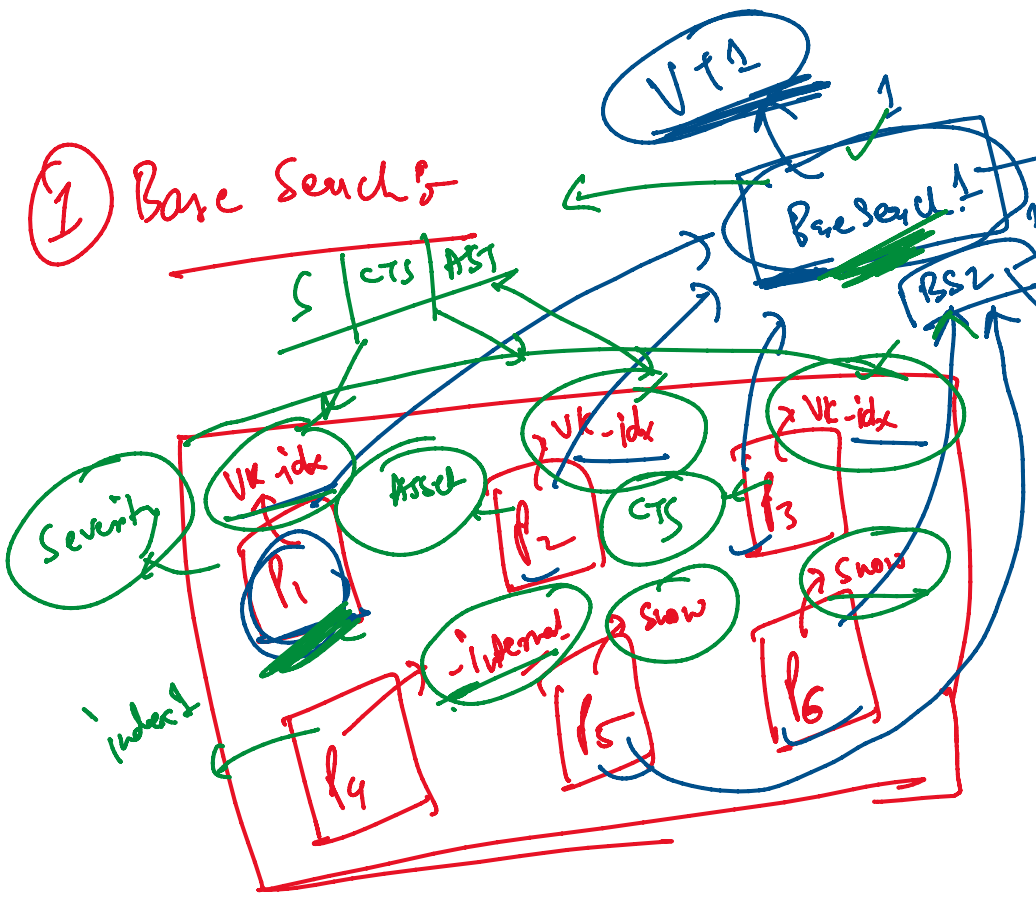
latest →

Optimization:-

① Base Search

② Saved Search

③ Summary Index



① Decrease no. of time hitting the index.

② VT to pull the data speed high compare hitting index.

3 → Same idx → VK-idx

2 → Same idx → Snow

1 → single idx → -Internal

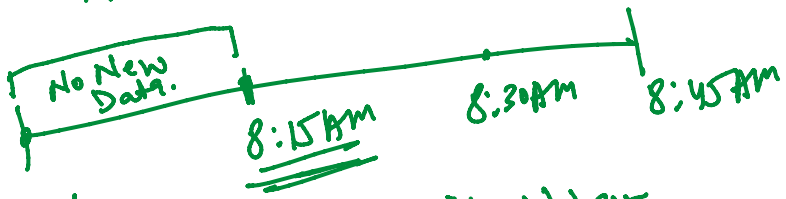
3 Panel → Same index

Base Search.

2 Panel → Same index

Refresh Dashboard → Base Search will run → Virtual Table → Panel will hit the Virtual Table & fetch the Result → o/p.

API call :- Interval Basis → every 15 min.



8AM → it will run

9AM → Refresh Dashboard → it will run
↳ loadjobs → No new o/p
→ Unnecessarily hitting the index.

Saved Search :- Define the interval when you want to run.

every 20 min. → hit the index 20 min.

Refresh Dashboard → Saved Search → No diff. → No indexer involved

Base Search → continuous data
Savedsearch → interval Basis

Avoid unnecessarily hitting the index.

Summary Index :-

S1 → o/p

index = VK-idx, sourcetype = csv | stats count by severity

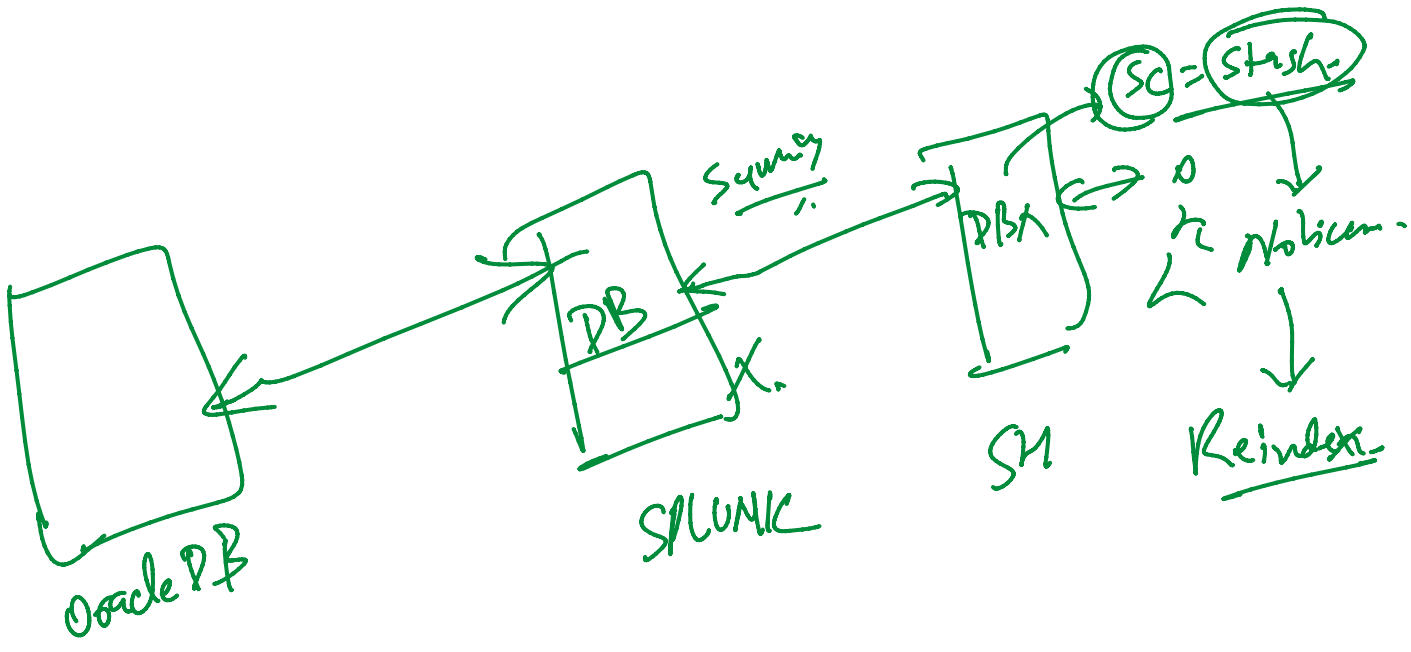
o/p ←

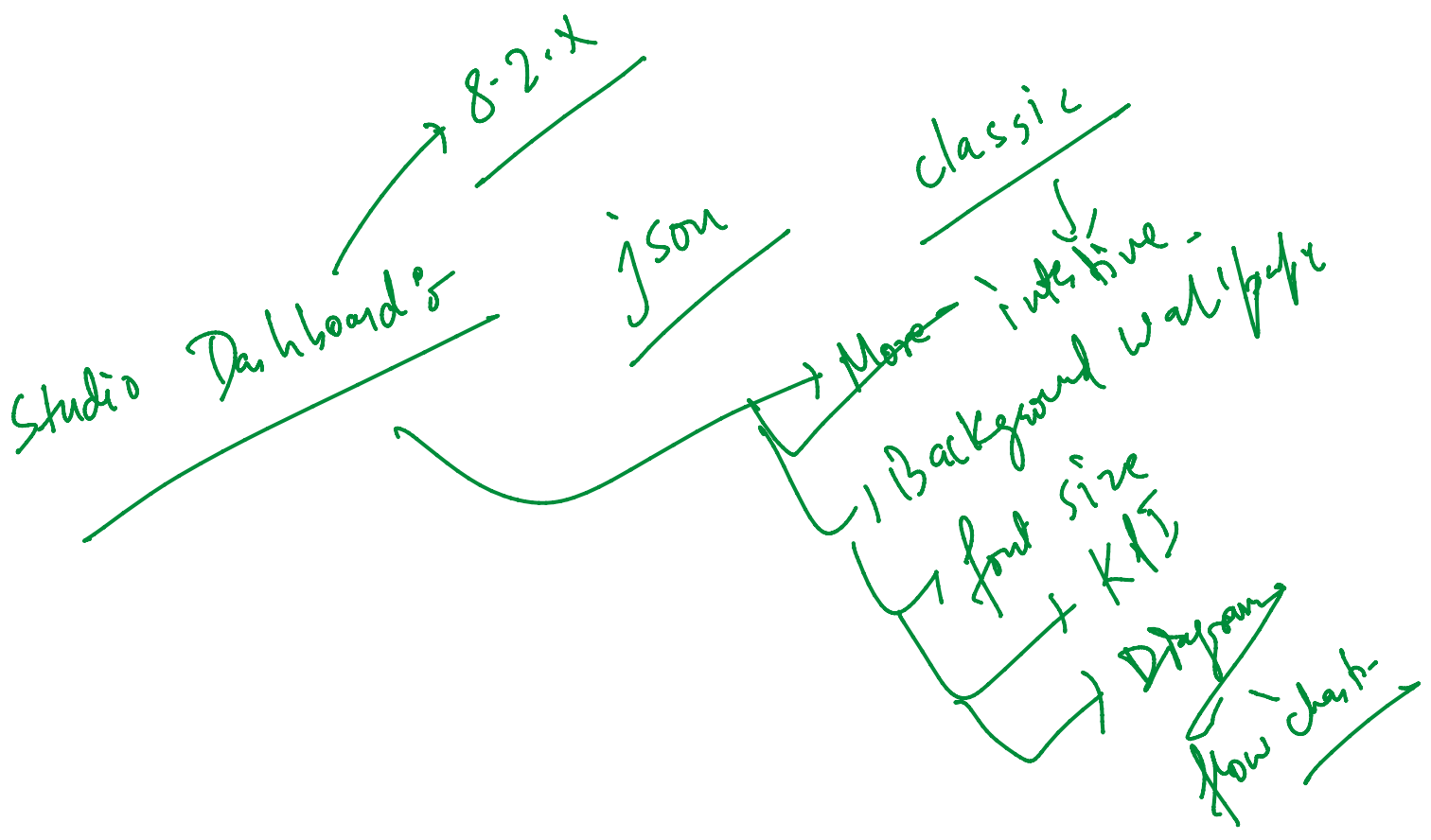
Severity	Count
1	5
2	10
3	25
4	30

log → I/p → Index

Reindexing → No. extra license consumed → Sourcetype = Stash.

Base Search	Saved Search	Summary index
① Continuous data coming in Splunk.	① data coming in interval.	① Push the last o/p as i/p in other index → Last o/p Huge Resource.


SC = Stash
Syslog
DB
DBX
Splunk
SM
Reindex


Studio Dashboards
8.2.x
json
classic
More interactive
Background wallpaper
font size
KPI
Diagram
flow chart