Day - 4

05 December 2024 10:03

1. Classic Dashboard

/0 i. Static Dashboard

ii. Dynamic Dashboard

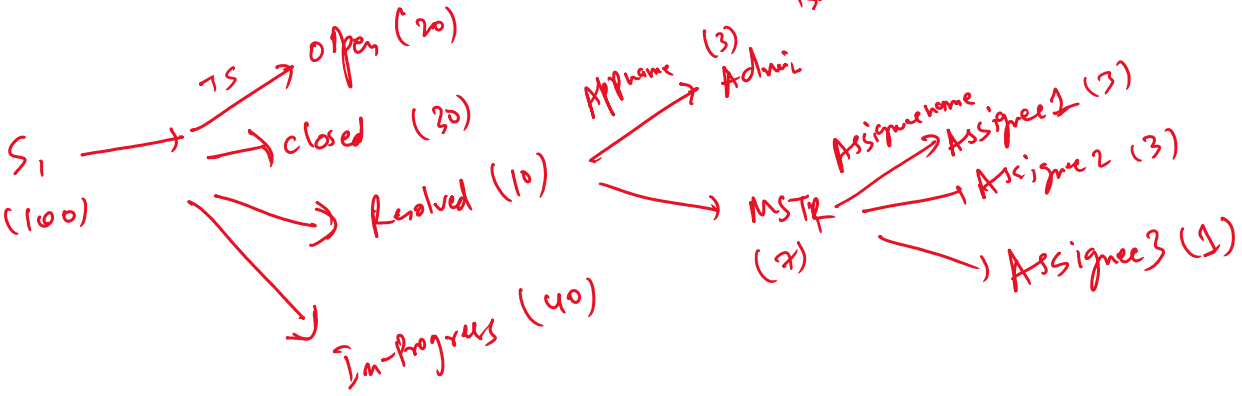
iii. Drilldown.

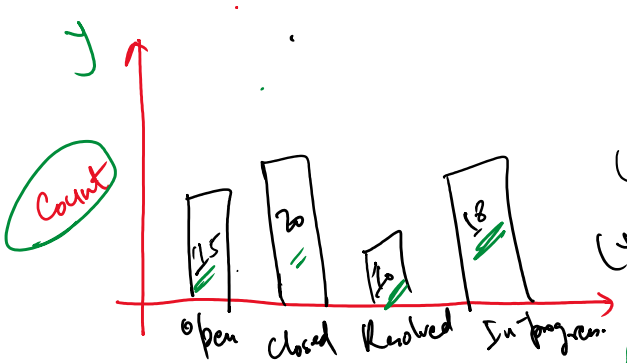
iv. Optimization - 1. Base search
2. Saved Search
3. Summary Index.

v. EventHandler. - set, unset, depend, reject, Condition, change

vi. Integrate js with Dashboard
↳ js in folder → call in our xml.

1. Dashboard → Classic Dashboard → xml
→ Studio Dashboard → json → 8.2.4 ↑
flowchart
icon.
Base search.





(x-axis) click.name = Current_ticket-state
(x-axis) click.value = Open, closed, Resolved, In-progress.
(y-axis) click.name2 = Count
(y-axis) click.value2 = 15, 20, 10, 18

$earliest → start time
$latest → End time.

Optimization:-

effective & efficient Query
any HeavyCommand.

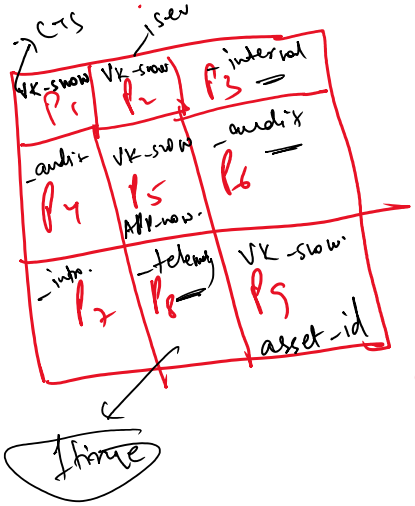
Optimization:-

1. Query writing method → effective & efficient Query
   - ① ex → Avoid Append, join or any HeavyCommand.
   - ② use dedup as early as possible
   - ③ Avoid using unnecessary command.
   - → | Stats count by Severity | rename Count as total
   - → | stats count as total by Severity
2. Panels involved in the Dashboard
   ex → BaseSearch, SavedSearch & Summary Index

Tagging seq. is important.

```
<change>
  <condition>
    <set>  </set>
    <unset> </unset>
  </condition>
</change>
```

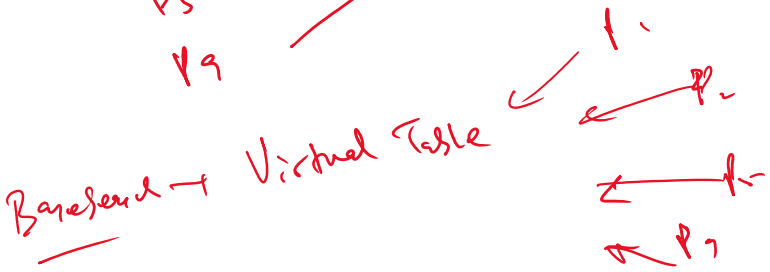
3. optimization:- ① Base Search.

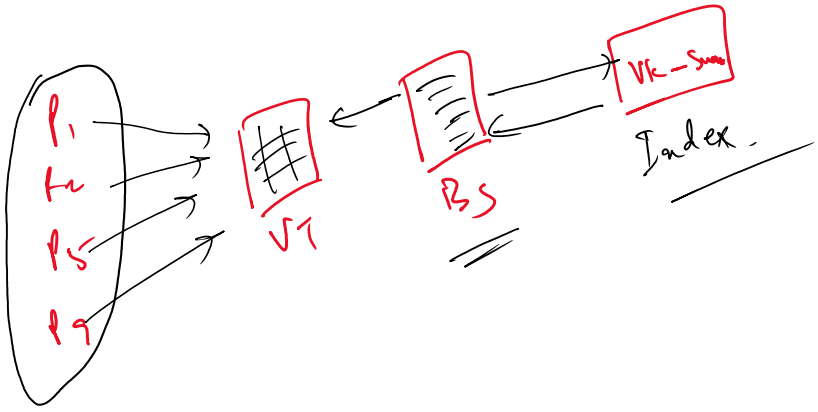


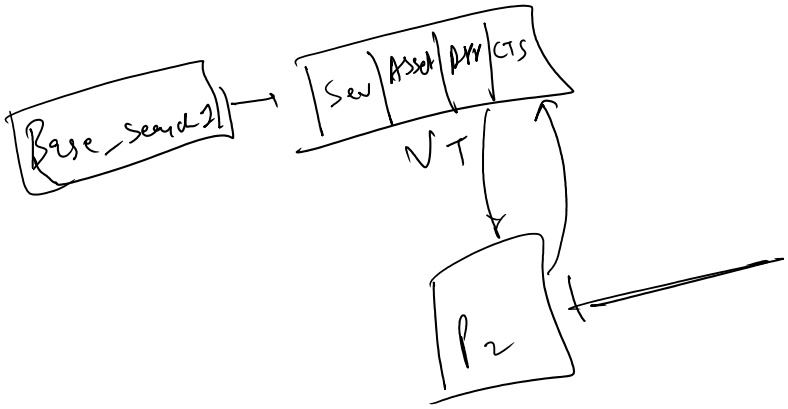
P1, P2, P5, P9 → VK-snow

① Load the Dashboard, all the panel will at the same Time.

② P1, P2, P5, P9 → hitting same index VK-snow







Load the Dashboard → Base Search → Virtual Table

API → 15-30 min

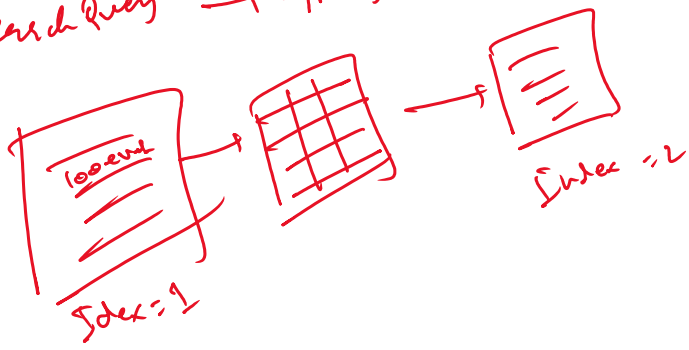
30 min
@ - 8:30 AM

Continous Data Ingestion

Saved Search Scheduled time

Summary Index:-

Search Query → o/p Query → Index



Splunk has already charged. That's why for reindexing no license consumed.

Sourcetype = stash. → splunk use.

↖ No license Consumed.

① Make any Index as Summary index.

② Push data → manual.
→ Automated [Report] → Schedule the search → search Trigger → Push the data Automatically.

100 forwards → indexer.

How forwarder is connected & Active?

10 forwarder → Terminate
90 forwards → Active/Actually
↓ Result
90 forwarder.

→ 100 forwards.

→ final Asset list.