Day - 4

19 December 2024 09:40

1- Classic Dashboard.
   a) Static Dashboard
   b) Dynamic Dashboard.
2. Filters / Input.
3. Drilldown.
4. Optimization of Dashboard - Base Search, Saved Search, Summary Index
5. Customizing Dashboard using XML.
6. Eventhandler Concept.
7. Studio Dashboard.
8. Functionality / Setting of Dashboard.
9. Integration of Dashboard with js.

10) Splunk MLTK Toolkit

Classic Dashboard:-

1. XML - Tags Concept, Sequence.
2. Multiple Panel. → Representation of Certain Use Case
3. Add Multiple filter.
4. Submit - Restrict the Sending of Filters in a bit wise, Single shot.

Static → Dashboard you create is fixed.

Dynamic → Create the filter, User can filter out the results.

Tstats:- Statistical Output

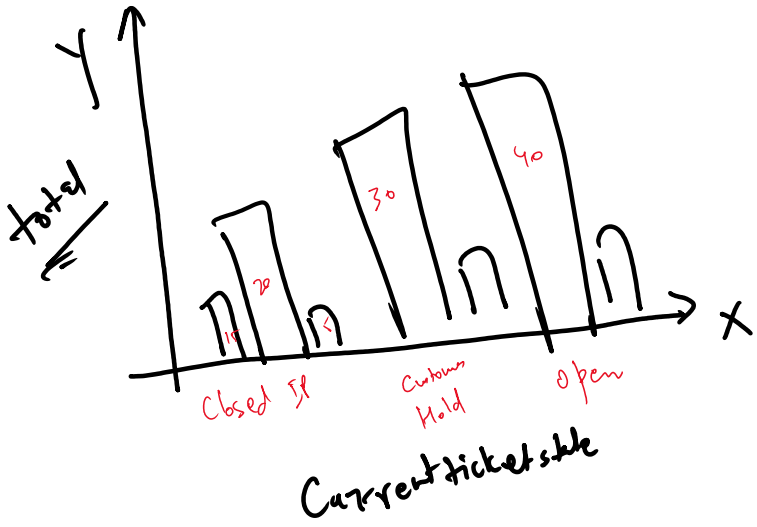
- Timestamp indexfile
- tsidx file
  - timestamp wise data ingestion
    - ↖ Tsidx file
  - Quick Result.
    - | stats Count
      - ↖ | tstats Count
      - → full index
        1. event
        2. Field
        3. stats

Drill down: ... the graph from one Dashboard

Drill down:-

① Send the value from the graph from one Dashboard to Another Dashboard.

② Deep Dive into the Dataset:-



click.name – X axis
– Current ticket state

click.value = x-axis Value
= closed, Inprogress, open, Customer Hold.

click.name2 = y-axis name = total

click.value2 = y-axis value = 10, 20, 15, 5, 30

$earliest = Earliest Time

$latest = latest Time

② Optimization of Dashboard:-

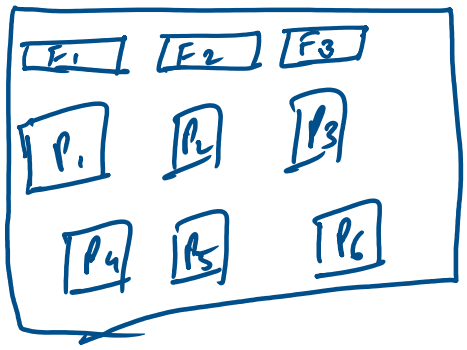
① Base Search.

② Saved Search.

③ Summary Index

① Base Search:-

P1, P2, P3 → Vk-idx



$P_1, P_2, P_3 \rightarrow$ Vk_idx

$P_4, P_5 \rightarrow$ main

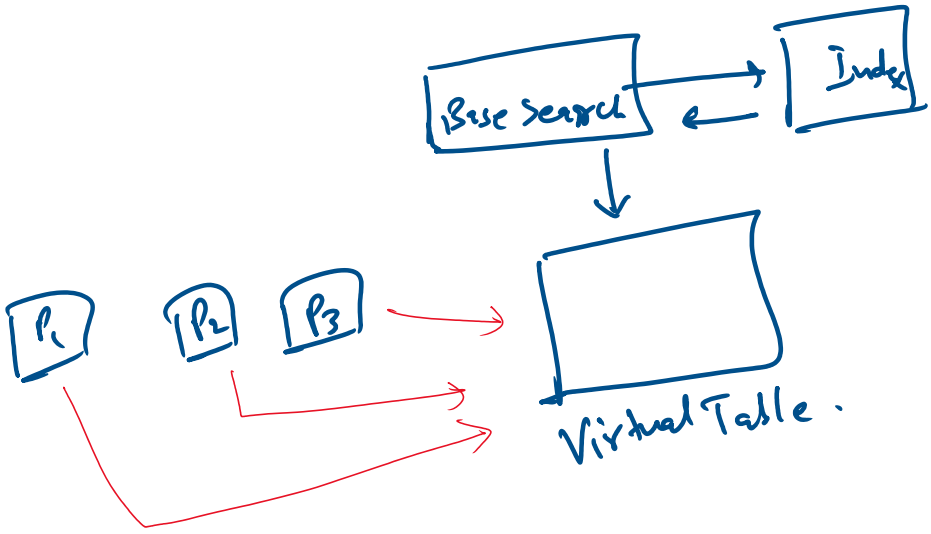
$P_6 \rightarrow$ _internal.

$F_1, F_2 \rightarrow$ Vk_idx

$F_3 \rightarrow$ main.

5 Times Vk_idx

3 Times main.



API call

↓

Data Ingestion Happen in interval Basis.

30min.

(2.) Saved Search:-

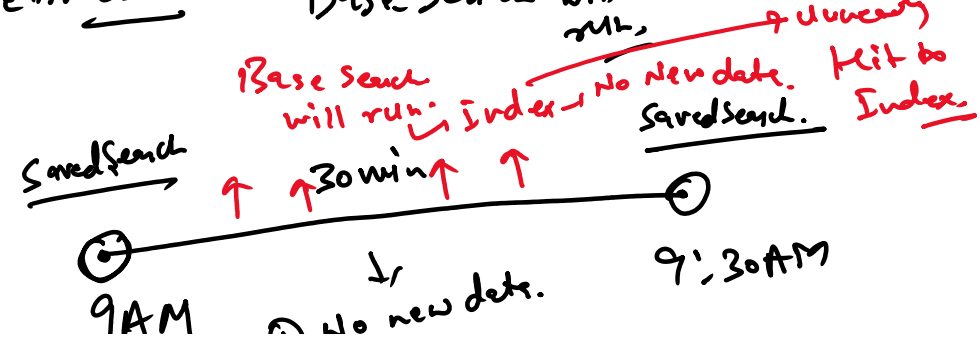
↓

Schedule search.

Even though you refresh Dashboard Multiple time. It will share the old data. It will run only at schedule time.

9AM —(TAT every time)→ 9:30AM

↑ Base Search will run. ↓ Base Search.



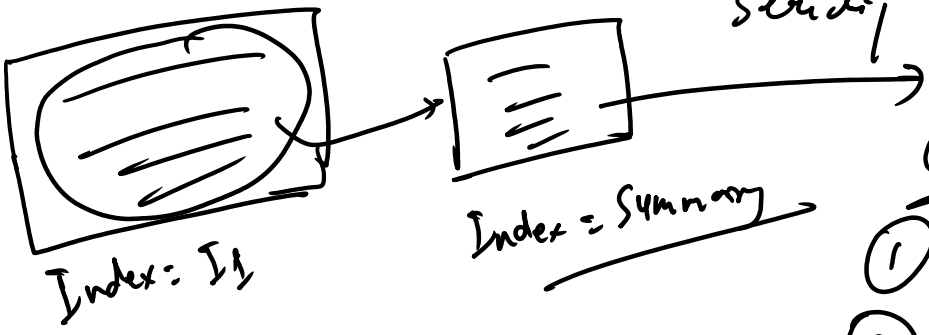
9AM → 9:30AM

1) No new data.
2) Schedule search.

Data is coming in the interval basis → Saved Search.

Data is coming Continously → Base Search.

3. Summary Index:- We are creating the subset of the output & saving it in other Index. This will increase the searching speed.



Cons:-
1) Disk space.
2) Computation Resource Consumption is high.

Pros:-
1) Speed is high.
2) No extra license Consumed.