1. mv
2. multikv
3. eventstats.
4. streamstats.

5. Classic Dashboard — XML
   a) Input filter.
   b) Panel Creation.
   c) Drilldown.
   d) Event Handler — set, unset, done, reject, panel, change, condition.
   e) XML Tags.
   f) optimization — Base Search, Saved search & Summary index

6. Studio Dashboard — JS

1. Classic Dashboard:-
   1) XML
   2) Multiple Panel.
   3) Multiple Input filter.
   4) Drilldown

   5. Customize the xml

Input filter → gives flexibility to the end user to filter the events.

Drilldown → Try to make the token passing from the graphs to other Dashboards / redirect to report, Alert Search Query — It will be deep dive into dataset & is going to help into finding the root cause of an issue.

Count

Open closed Resolved IP CH
Current_ticket_State
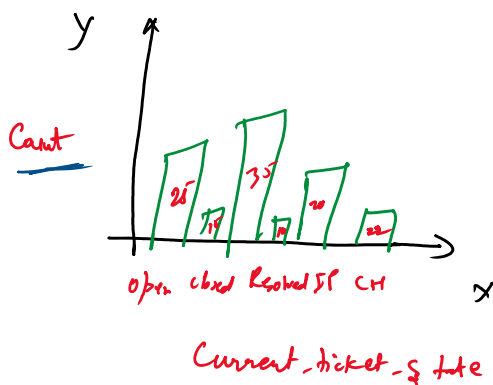
click. name → Name of x Axis (current_ticket_State)
click. value → Value of x Axis
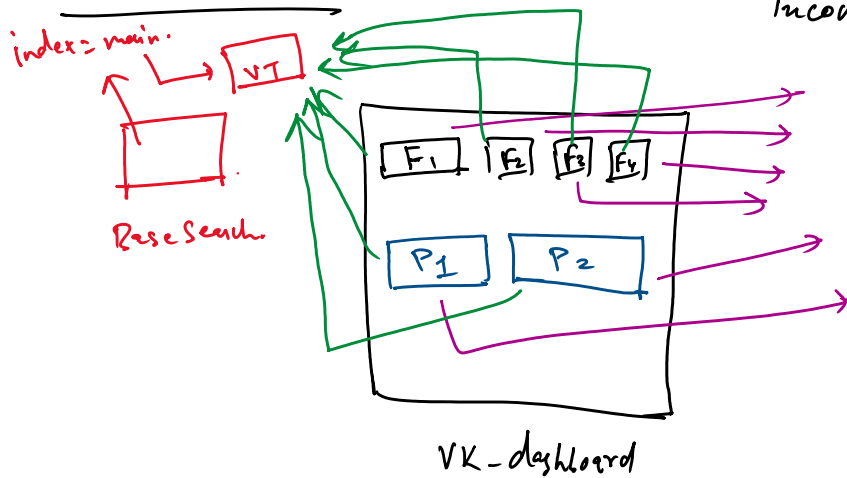   (open, closed, Inprogress, CH)

click. name2 → Name of y axis
          (Count)
click. value2 → 25, 15, 35, 10, 20, 22

earliest → earliest Time in epoc format

latest → Latest Time in epoc format.

Optimisation:-

Base Search:-

Ideal for the situation where there is continous data incoming in splunk.

index= main.

VT

Base Search

All Are Hitting the same Index. whenever, you are loading the index, all will be hitting the same index.

VK - dashboard

* Decrease the No. of Time, we are hitting the index.

* We have the Base Search, it will hit the index & create the Virtual Table. This VT, will be linked with the Panel level search.

Saved Search:-

Create the search that will run in the schedule basis.

Data coming in splunk is in internal basis.

↳ every 30 min, every 1hr. API call.