Day - 6

02 January 2025 14:43

1. Summary Index
2. Studio Dashboard
   - Base Search
   - Chain Search
   - Summary Index
   - filter
   - Panel
   - Visualization
   - json file / code.
3. mv
4. multikv.
5. eventstats.
6. streamstats.

---

1. Summary Index:

Search Query → Index = main | stats count by severity

output → Summary Index.

① No license Consumed → Sourcetype = stash → Splunk will be able to recognize that this data is not taking part in license.

② Source → ***. stash_new

testmode = true → its for preview, no ingestion

testmode = false → Default is false, Data ingestion happens.

2. Studio Dashboard:-

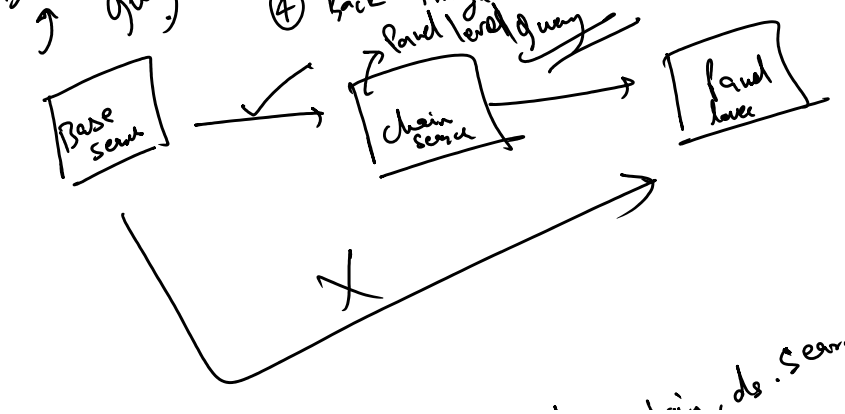
① It created on the top of json Code.

② Lot of Visual Customization like background, Image / icons / flowchart.

③ But in studio Dashboard, you need to create the baseSearch & chain search.

Generic textbox → Query

④ Each image is stored into kvstore.



formats of different sections in json file.

ds.search, ds.savedsearch)

① Datasource [ds. chain, ds. search, ds. savesearch]

② layout [layoutId]

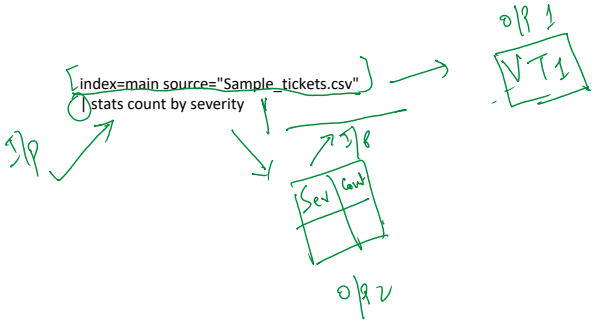
③ Input [token = dd_*]

④ Visualization → Viz_* [id format]

③ Eventstats:- *To add the statiscal output in the event section.

*Normally in stats, you have the output as per stats format rest of the field will ignored/ rejected.

* Using the eventstats, you will have the output added a field in the event & no stats will be generated.



④ Streamstats:- Streaming output.

```
| makeresults count=3
| streamstats count
```

⑤ Multikv:- multi value fields