Day - 3

20 March 2025 18:37

1. Lookup.

2. Data Model.

3. Dashboard.

① classic Dashboard.

- static
- input filter.
- Panel.
- Drilldown.
- optimization

① Lookups

- csv
- KV store
- geospatial.
- Database.
- External Lookup

① csv lookups

① csv file

② static in Nature.

③ small file

④ upload file in splunk.

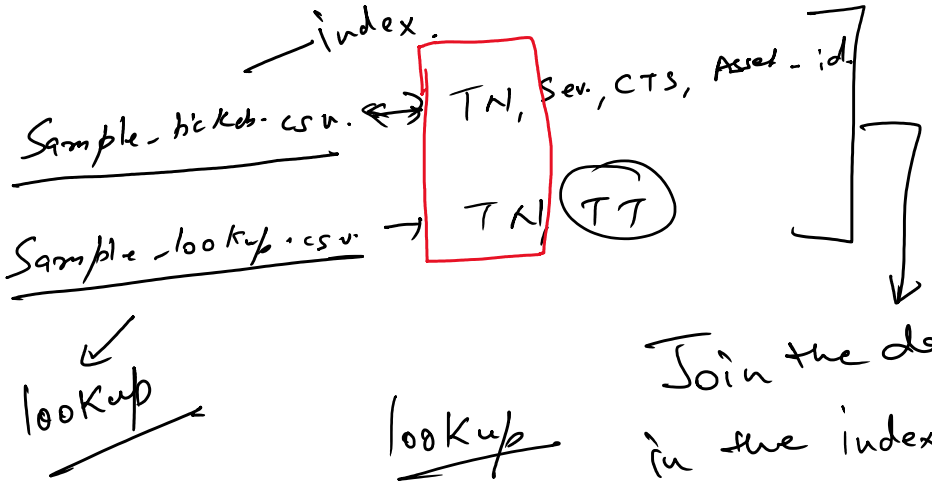
⑤ No License is consumed.

1. upload lookup
2. Lookup Definition.
3. Automatic lookup

Command:-

1. inputlookup - search data inside lookup file.
2. Lookup.
3. outputlookup.

1. Sample - lookup.csv



Lookup Definition

Lookup → Search event → fields

Schema of the csv file.

Automatic lookup:- | lookup lookuptable ——— output ———

Automatic lookup → Template. → Unique field
Output
Mapped to

Automatic lookup → Template → Unique field Output Mapped to

Outputlookup:- lookup | inputlookup → View | Read the data from the lookup.

Outputlookup → Write/update the entry in the lookup file.

(2.) DataModel:- Increase the searching speed.

index = svow_idx. ↩
→ fetching the event.
→ fully extracting of the field.

index = svow_idx.
① All the list of fields
②

DataModel

① Define the required field in Advance.

② Hierarchical Concept.

Root
↳ child + C'
↳ SC + C''
↳ SSC + C'''

Pivot → Way to Visualize the Data.

But in Pivot, it will pick the dataModel only.

You need to have the dataModel to create a pivot.

③ Dashboard:-

Dashboard → classic Dashboard
- ↳ xml
- ↳ Feature Driven.

→ Studio Dashboard
- ↳ json
- ↳ V.8.2.0+
- ↳ Visualization & Cosmetic Part

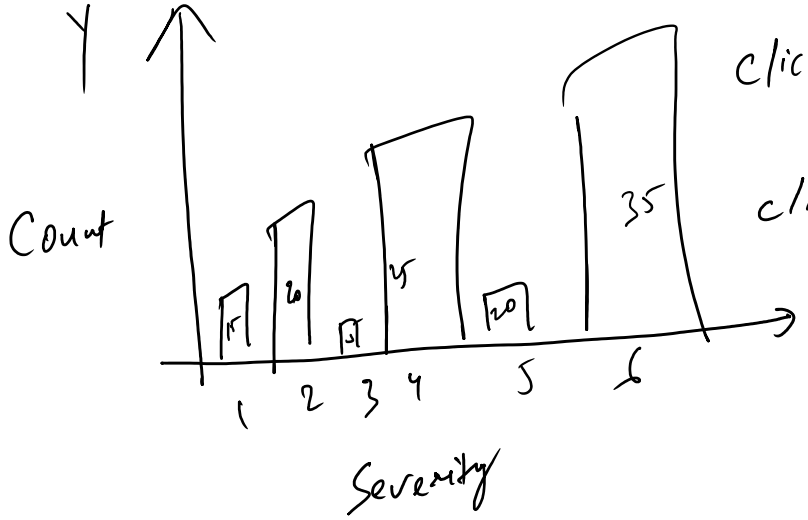
Data Ingestion →
- Forwarder.
- HEC Token.
- Python script.
- tcp or udp.
- Apps or Add on.

Input filter

1. Filter.
2. Token.
3. Pass the token to the dashboard.

Drilldown:-

Drilldown.



click.name = X-axis
= severity

click.value = X axis
= 1, 2, 3, 4, 5

click.name2 = y-axis
= Count

click.value2 = y-axis
= 15, 20, 5, 25, 35

Optimization:- 2 things :-

(1) Search Query level

(2) XML Level.

(1) CPU Level:- (1) Heavy Commands- Append, join, spath etc.
- execution time↑

① SPL Level:- ① Heavy Command - Filt
Allocation cost ↑ Execution time ↑

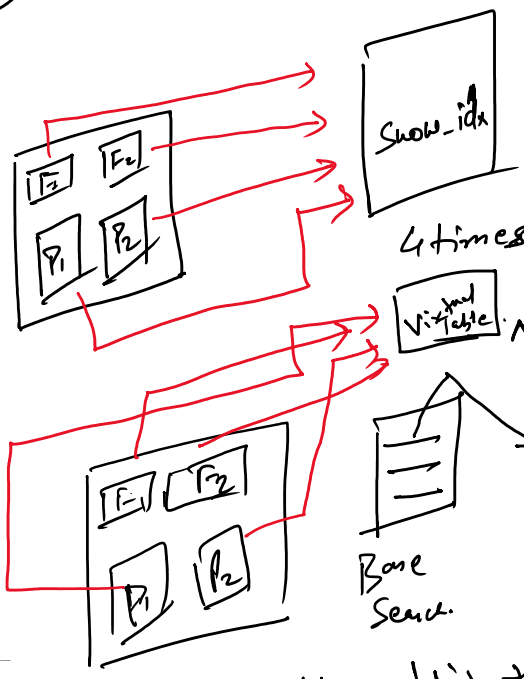
② Dedup Command - Remove duplicate

③ stats/Rename - In the log
↓
"Total time"

② Dashboard level:-

① Base Search
② Saved Search.
③ Summary Index..

① Base Search:-



Hitting the index 4 time, because of the Virtual Table generated from base search. It will only hit once. Now, all the Panel & Filter will hit the VT instead of Splunk Index.

Con:- Wherever the refresh is going to happen, Base will again create the fresh Virtual Table. in every 30 sec.

Cons:- Wherever the [illegible]
Search will work create the [illegible]
API call is happening & data is coming in every 30 sec;
Even though refresh the same search, No New data will come,
It will unnecessarily hit your index.

(2) Saved Search:- Schedule Save.
Main SPL Query will run at the schedule time.
No impact even though you refresh page multiple times.

(3) Summary Index:-

index = summary_idx | stats Count by Severity

Severity	Count
1	5
2	15
3	25
4	7

Summary Index