Day - 3

04 December 2024 10:06

Knowledge objects:-

1. Eventtype
2. Tags.
3. Macros.
4. Calculated field.
5. lookup (CSV)
6. Data Model & Pivot.
7. Alerts.
8. Report.
9. Workflow

1. tag → Way to Categorise the data.
   Label the particular data value / field value
   Generate 2 new fields →
   - tag
   - tag::severity

2. Macros:- Function.

```
fun a(b,c)
{
d = b+c;
return d;
}
```

a(3,4)
a(5,6)
a(7,8)

1. No repetition.
2. Flexible, enter argument.

i) No Arg.
ii) Single Arg.
iii) Multi Arg.

abcde
edcba

3. Calculated field:-

eval Kb = bytes/1024

Template → calculation → field.

Lookups:-

1. csv
2. Kvstore.
3. Geospatial
4. External
5. Database lookup

(1) csv lookup:-

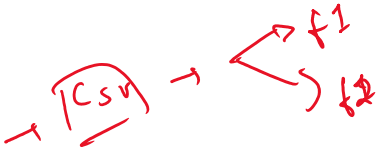
(1) upload in splunk. No license. No Index.
(2) small file which is fixed or not suppose to change frequently.

(1) inputlookup
(2) lookup
(3) outputlookup.
(4) lookup Definition.
(5) Automatic lookup.

(1) inputlookup → | inputlookup file-name.csv
(2) lookup → Command that will compare & combine the data that is coming from index & lookup file.

(3) output lookup:- update the lookup file. In that case we use the output lookup command.
Ex→ | outputlookup append=t | lookup-file-name.csv

(4) Lookup Definition:- It will extract the field from the lookup file in the advance.



(5) Automatic Lookup:- Merge | join data b/w index & Lookup

Lookup filename i/p Output o/p.

↓

Template

Data Models:-

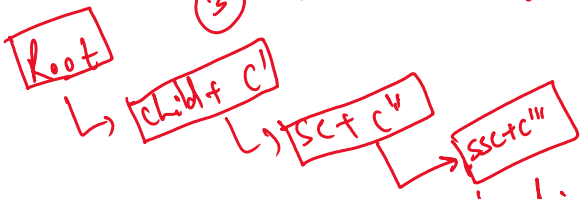
Index → Extraction of Fields from event + Processing of the fields

index-VK-idx → EN, CTS, sev., TS

Datamodel → ① Define the required fields in advance.

② Hierchal Concept

③ Tsidx file → Timestamp summary file which have details about the fields / data in it.



Adv:- ① Searching speed is very high

② Amount of data is high & Urgency of data.

Dis:- ① Computational Resource Consumption is high.

CPU ↑ Memory ↑

We don't create DM for all the index.

Data is high ↑ Urgency / Priority of → increase speed of → create DM

Pivot - Way to Visualize the data.

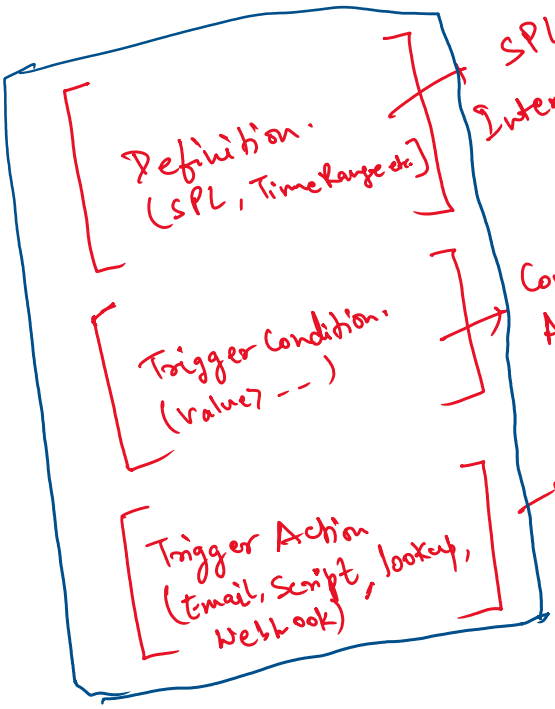
Exactly of chart / timechart

Diff- → It will work only with Data model.

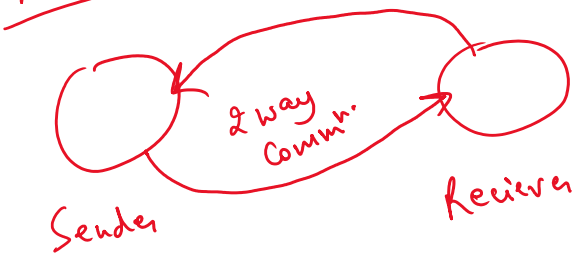
No much worry on Coding part.

click so yo → options are their →

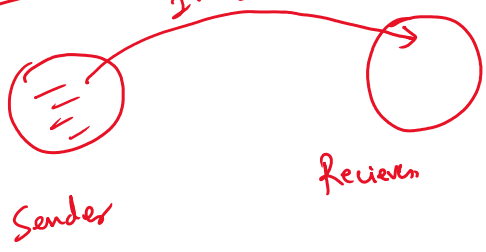
Alerts:-



API:-



Webhook:-



every 15 min → 10 AM — No Data.
10:15 AM — No Data.
10:30 AM → No Data.
→ 2 No data time

→ Set the time range 30 min. (I)
→ Lookup file (II)

(I) + (II) → lookup file

No result
No result
No result
→ lookup | count ≥ 2 → Trigger Alert.

Report:-

Definition
SPL, Interval, time range etc.

Report:-

[Definition
SPL, Interval, time range etc.]

[Trigger Action]

Workflow Action:- collect certain field values & send it to the outside App. | DeepDive with the help of Specific SPL.