Day - 2

17 December 2024 10:03

1. SPL Command.
2. Visualization.
3. Lookup [csv, Kvstore, geospatial, External Lookup]
4. Tag & Eventtype

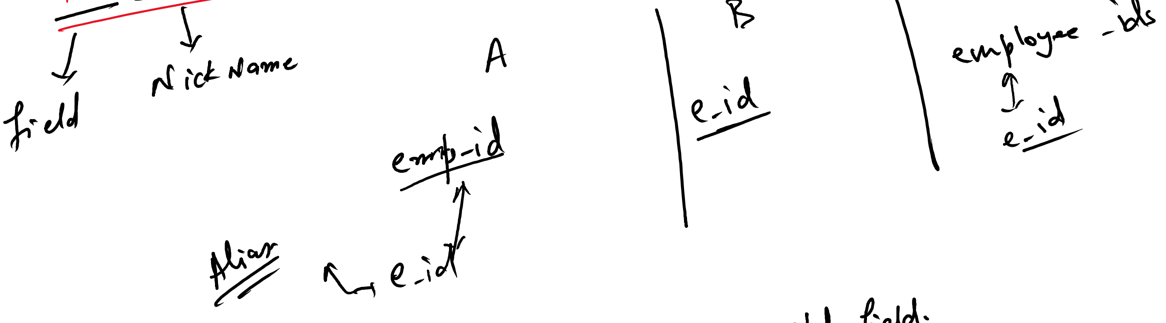
Knowledge object.

SPL Commands:-

1. chart. → x-axis & y-axis with specific field
2. timechart → By default x-axis → time., y-axis → field name.
3. Single Value Visualization. → Single Numeric Value.
4. Trend chart. → Works across the time.
5. Geostats → Counts in the geo map. Latitude & longitude.
6. addcoltotal. → Column wise Addition.
7. addtotal. → Row wise Addition.
8. Rex. → |rex field=fn "______"
9. Append → Attach the o/p of two diff. search Query.
10. Appendpipe. → Use the o/p of the 1st Search Query as the I/p of the 2nd Search Query. next to Sub Search.
11. AppendCols. → Attach the o/p of 1st Search Query
12. Eventstats. → output of statistics is attached with events not in a tabular format.
13. Streamstats. → streaming output / Incremental output
14. Makeresults → Create the sample Events.
15. join
16. eventcount → Summary of the count value.
17. field Summary

```
index=vk_idx source="sample_tickets.csv" | chart count by current_ticket_state, severity | addcoltotals
label=sum labelfield=current_ticket_state| addtotals fieldname=summation
```

Field Alias:- Create the field with other name.



Attach the new fields along with the old field.

Calculated field:-

byts → Kb

eval Kb =r(bytes/1024,3)."KB"

Template Calculation, fields.

Field Extraction:-

① Regular exp → Rex Query.

② Delimiter type → Split the events on the basis of certain symbols.

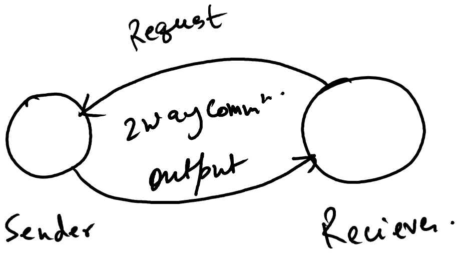
Alerts:-

[Definition → SPL Timeperoid. interval]

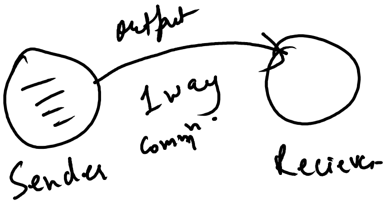
[Trigger Condition → When Alert will fire]

[Trigger Action. ↳ Email, Webhook SMS, Script.]

API:-



Webhook:-



Transaction:-

Combine multiple events into one event.

maxevent

maxpause

max span.

T1

e1
e2
e3
e4
e5

Maxevent → Max. event in a siyle trasaction.

5

Maxpause → Max. interval b/w two consecutive event in a siyle transation

e2 - e1

e3 - e2

e4 - e3

Maxspan:-) Max. interval b/w first event & last event.

(e5 - e1)

Lookups:-

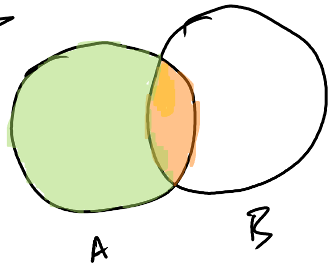
① CSV:- ⓐ Small static file
ⓑ extension .csv

① upload lookup file.
② lookup definition.
③ Automatic lookup.

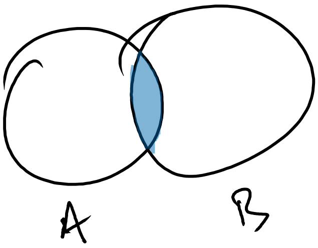
join:-

① left join.
② Innerjoin.

① left join:-



2. Innerjoin:-



Tag:- Categorise the fields on the basis of Certain Values,
Whenever create tag, it will create two field.

① tag = normal.
② tag :: severity = normal } → 2 fields getting generated.

Eventtyper Categorise the event using eventtype.