Day - 3

27 December 2024 13:32

Knowledge object:-

1. Calculated field
2. Tags & eventtype.
3. Macros.
4. LookUp – csv
5. DataModel & Pivot
6. Alerts
7. Report.
8. Workflow Action.
9. Transaction.

1. Calculated field:-

Comply with eval based activities.
Template & define the calculation
Call the fields as any other normal fields

2. Tag & Eventtype:-

Tag → Categories the field values
When you create the Tag, 2 new fields will be created

1. tag.
2. tag :: severity

Further searching using above field.

tags.conf

```
[severity=3]
normal = enabled

[severity=4]
normal = enabled
```

Eventtype:- Way to categories the events on the basis of certain Conditions.

Command:- eventtype event-named

eventtype="completed"

eventtype.conf

Config. file where the eventtype stanza is saved

```
[completed]
color = et_green
search = index=vk_idx source="Sample_tickets.csv" current_ticket_state="Closed" OR current_ticket_state="Resolved"
```

3. Macros:-

Function.

1. To avoid writing many multiple

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

Argument

x(3,5)
x(7,8)
x(9,6)

→ call the function

① To avoid Query multiple times.

② for that you created the template & pass the Argument value.

{
c = a+b;
return c;
}

x(4,5)
x(9,6)

① No Arg. →
② Single Arg. →
③ Multi Arg →

Config.:- Macros.conf

Call the Macros:- `vk_noarg`

`vk_single_arg(4)`
↳ Argument Value.
↓
Name of Macro

Multi Arg.:-> More than one Arg.

```
[ec2-user@ip-172-X-X-3 local]$ cat macros.conf
[vk_noarg]
definition = index=vk_idx source="sample_tickets.csv" | stats count by severity
iseval = 0

[vk_single_arg(1)]
args = sev
definition = index=vk_idx source=Sample_tickets.csv severity=$sev$ | stats count by severity
iseval = 0
errormsg = severity should be number and should be less than 5
validation = isnum($sev$) AND $sev$<5

[vk_multiarg(2)]
args = sev,state
definition = index=vk_idx source=Sample_tickets.csv current_ticket_state="$state$" severity=$sev$ | chart count by severity, current_ticket_state
iseval = 0
```

Lookup - csv:-

① csv
② Kvstore
③ Geospatial
④ external
⑤ database

① csv:-

1. Small & Static in nature.
2. csv format
3. upload in the server. Not the part of index. No license

③ upload in the server.
Calculated.

① upload lookup file
② Lookup Definition
③ Automatic lookup
→ 3 features/options available in lookup.

or Output lookup → when you want to change any value in a lookup file.

|outputlookup lookupfile append=t/f

Lookup Editor Application:- ① easy to maintain the lookup file.
② Act as a spreadsheet where you can add the values.
③ Backup Maintain.
④ checkpoint for Rollback option.

Maintained by Splunk itself.

② KVstore lookup:- KV → Key Value paired

① each & every entry is tagged with the unique key.
② collections.conf → structure of the kvstore lookup.
③ huge & Dynamic in nature.

DataModel & Pivot:-

① Search data in index.
② Searching of events.
③ Extraction of fields.

② DataModel:- Props:-
① Help to increase Searching speed.

Cons:-

Cons:-

1. Effect your Computation resource.
   ex → CPU, Disk, Memory Consumption will increase.

Tips:-

1. Help to increase Searching speed.
2. Define the field in the advance itself.
3. Hit the tsidx file
   ↳ time summary index file
   ↳ Details about the entry done, timestamp wise.
4. Hierarchical Concept.
   Root → child + C'
   ↳ SC + C''
   ↳
   ↳

Use Case:-

1. Amount of Data is very huge.
2. Data is critical in nature ex → Security, operational.

Pivot:- Way to Visualize the data.

1. Click to Go option. No SPL Query needed like in chart & timechart command, we use in index time.
2. It will be dependent on Data Model.
   No Data Model = No Pivot.

Data Model Acceleration:-

1. Backfill → Retain the o/p of that period
2. Searching speed will increase more.
3. Increase Computation Resource consumption like CPU, Disk, memory will spike up.
4. When your DM is in acceleration mode, you can't make any changes in the DM. you need to Disable the acceleration to make change in DM.