Day -3

18 December 2024 10:07

1. Macros – No arg., Single Arg., Multi Arg. 9. Best Practices.
2. Data Model
3. Pivot
4. Acceleration & Report.
5. Workflow Action
6. KV store lookup
7. External Lookup
8. Geospatial lookup.

---

## 1. Macros:-

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

a(3, 5)

a(4, 7)

(1) No Arg. → Call the Macros Directly. Not Passing any Argument.

(2) Single Arg. → call the Macros, by passing one Arg. only.

(3) Multi Arg. → call the Macros, by passing more than one Arg.

Call the Macros = `macro_name(a)` → Tidle Symbol

## 2. Data Models:-

(1) Hierarchical Concept → root event
↳ childevent
↳ Sub child event.

(2) Define the ref. field in Advance.

(3) Spend time only on fetching the event.

(4) No time spent on extraction of fields during searching process.

(5) Tsidx summary file → timestamp file generated at the time of ingestion.
Use the Tsidx file, extra edge.

Whenever using the DM, the search speed is relatively higher.

Computational Resources. That why we create DM, only on

Cons:- Will Consume extra Computational Resources. Thats why we create DM, only on search or high priority dataset only. Ex- Splapps, Mcafee, fireeye etc.

Amount of data ↑ Analysis time ↑ Search Time ↑

DataModel

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

Pivot:- Create the visual Representation of your system.
DataModel is Required to create the Pivot.

(3) Report:- [ Definition. ]
[ Trigger Action ]

Alert → Trigger condition
Report → No Trigger Condition.

(4) Workflow Action:- Send the value of the specific event from the event page in splunk to the outside Website | Drilldown.

(5) KVstore lookup:- (1) Dynamic
(2) Large file.
(3) Data is going change very frequently.
(4) Set up the Configuration in backend. Then lookup Def. directly.

CSV:- (1) Small file.
(2) Static in nature.
(3) csv extension file that we upload in splunk.

(2) ...

(3) csv extension file ...

Collections.conf

```
[vk_kvstore]
enforceType = false
field.id = number
field.name = string
accelerated_fields.my_accl = {"id":1}
```

K V
↓ ↓
Key  Value paired

* Each entry in this lookup will be mapped with the unique key (_key).

## (6) Geospatial LookUp:- Geographical Map.

```
| makeresults
| eval latitude="15.317277" , longitude="75.713890"
| lookup vk_geo_lookup latitude, longitude
| stats count by featureId
| geom vk_geo_lookup
```

Feature ID Element ----> //Placemark/ExtendedData/Data[@name='Name']/value

Splunk App.
- → Splunk → Splunk LLC → Author Name
- → 3rd party Users. → Author Vivek, company name

1. Splunk Application Author
2. Compatability → Splunk Product
   → Version of Splunk.

(1) CSV lookup → csv file
(2) KVstore → Key value paired file (Collections.conf)
(3) Geospatial lookup → kml file → zip(kmz file)
(4) External LookUp → Script (Python) → result → support field

→ No. license consumed
→ Disk