

1. Macros - No arg., single Arg., Multi Arg.

9. Best Practices.

2. Data Model

3. Pivot.

4. Acceleration & Report.

5. Workflow Action

6. KVStore Lookup

7. External Lookup

8. Geospatial Lookup.

## ① Macros:-

function a (b, c)

```
{
  d = b+c;
  return d;
}
```

a(3, 5)

a(9, 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 =  $a_{macro\_name}$  → Title Symbol

## ② Data Models:-

- ① Hierarchical Concept → root event  
↳ child event  
↳ 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 Tside summary file → timestamp file generated at the time of ingestion.  
Use the Tside file, extra edge.

Whenever we use the DM, the searching speed is relatively higher.

Combustional Resources. That's why we create DM, only on

When...

Cons:- Will consume extra Computational Resources. That's why we create DM, only on security or high priority dataset only. Ex: Palo Alto, McAfee, fireeye etc.

Amount of data  $\uparrow$  Analysis time  $\uparrow$  Search Time  $\uparrow$

Data Model

Root

$\rightarrow$  child + c'

$\rightarrow$  SC + c''

$\rightarrow$  SSC + c'''

Pivot:- Create the Visual Representation of your system.

Data Model is Required to create the Pivot.

Alert  $\rightarrow$  Trigger Condition  
Report  $\rightarrow$  No Trigger Condition.

③ Report:-

[ Definition. ]

[ Trigger Action ]

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 to change very frequently.

④ Set up the configuration in backend. Then lookup Def. directly.

CSV:-

① Small file.

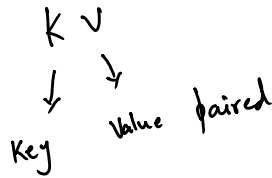
② Static in nature.

③ CSV extension file that we upload in Splunk.

- (2) csv extension file
- (3) csv extension file

Collections.conf

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

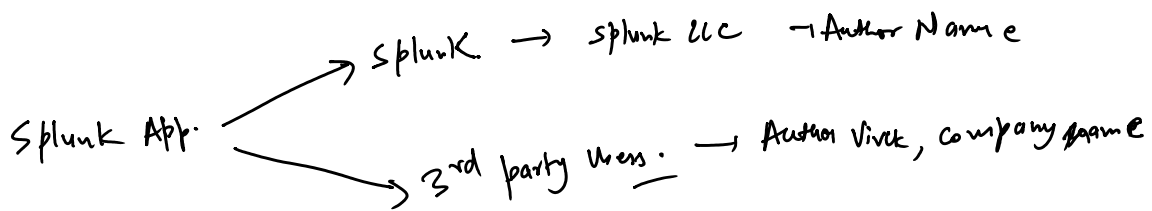


\* Each entry in this lookup, will be mapped with the unique key (\_key).

## 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



1. Splunk Application Author
2. Compatibility → 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