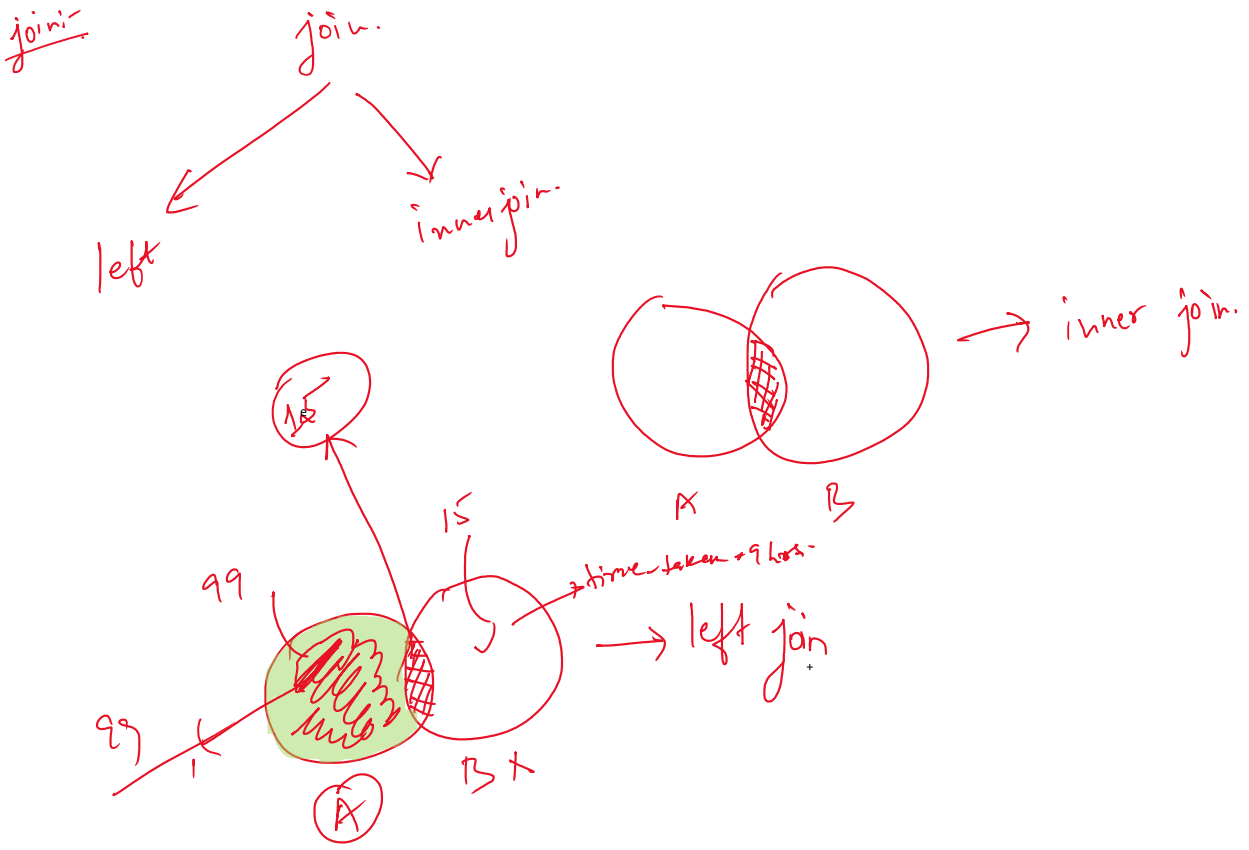
Day - 3

09 July 2025 10:13

joins



Knowledge object:-

1. Calculated field.
2. Tag & eventtype.
3. Field Alias.
4. Macros.
5. lookup. — csv, lookup editor.
6. Data Models & Pivot

(1) Calculated field:-

evalKb = round(bytes/1024, 2) . "Kb"

Template → Kb = bytes/1024

Template → Kb = (bytes / 1024)

② Tag & eventtype :- Tag → Categorization.

① tag = normal.

② tag :: Severity = normal. } → 2 fields will be created.

③ Field Alias :- → New Name / Nick / Pet Name.

field.

Why ?

A

emp-id

B

id → emp_id

C

employee_id.

↓

emp_id.

④ Macros :-

function a (b, c)

{

① No Arg.

② Single Arg.

(4) ...

function ...
{
d=b+c;
return d;
}

a(3,4) a(5,7)
a(1,2)

(2) Single arg
(3) Multi Arg.

(5.) Lookup → csv:

(1) upload the lookup in the ~~computer~~ splunk
(2) No index the lookup.
(3.) No licence is consumed.
(4) Small csv file with Not frequent changes.

Lookup → kvs tore. → Key value pair
Lookup → csv.
Lookup → Geospatial → Geographical.
Lookup → external.
Lookup → Database lookup.

Outputlookup → update. file in the lookup.

|outputlookup append = t/f VK-sample-lookup.csv

Tomorrow:-

1. Field extraction.
2. Alert. -
3. Report. -
4. DataModel & Pivot -
5. Workflow Action -
6. Predict

→ By lunch Break

7. Classic Dashboard. → Post lunch break