Day - 3

17 September 2025 10:09

1. Calculated field

Bytes → KB

eval KB = round(Bytes/1024, "KB")

Template, where we set up this scenario. So, that we don't have to use same expression again & again.

① Private - Only you will be able to access.

② App - Role - Read/write. It is confined to certain App

③ Global - All app level access.

2. Field Alias -

Field → Nick Name.

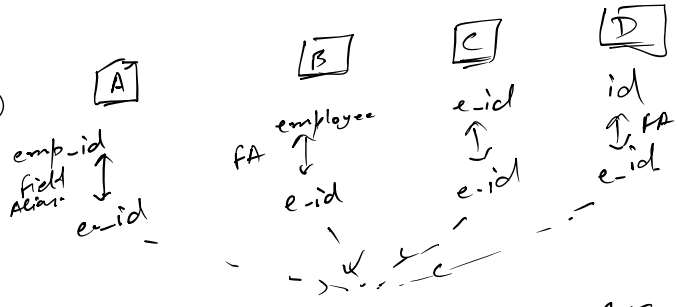
It will not delete the old field. It will only add the new field.

Source = abc.csv.

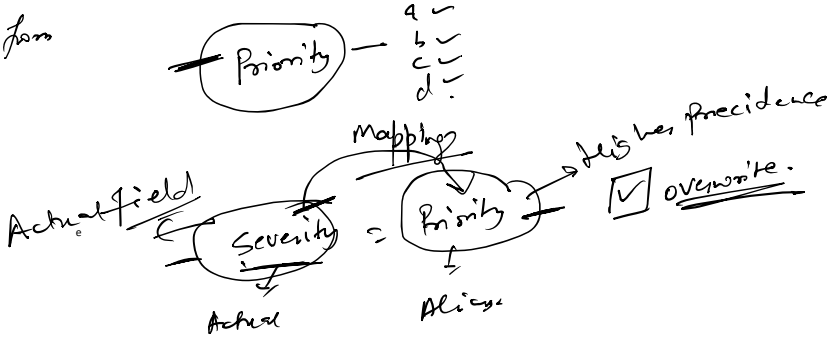
Severity.

Priority. → Created new field with same value.

Why? ①



Easy to combine the data from diff. sources.



3. Field Extractions -

Regex - Regular expression → which is generated by splunk.

Delimiter → Extract the field via data breaking using symbols.

data ...

Inline → Regex. Type.

Users Transforms → Delimiter Type

(4.) Macro :- Function.

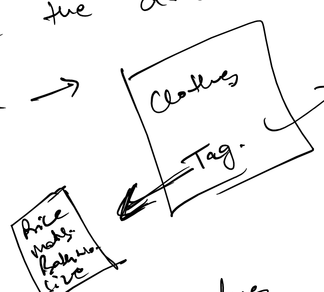
```
fun a(b,c)            a(3,4)
{               →     a(5,7)
d = b+c;
return d;
}
```

macro → No Arg.
macro → Single Arg.
macro → Multi Arg.

No Arg :- No Argument is passed.

Single Arg :- Pass only one Argument.

Tag :- Categorize the data.

Showroom → 

→ Categorise the product.

Tag to the field values.

Two new fields will be generated. → Searching going further with any field

1. Tag = tag = normal
2. tag::severity = normal.

② tag = Severity

Eventtype – Categorize the event on the basis of condition.

ex → [index=VIC idx source=S_ticket.csv CTS="closed" OR CTS="Resolved"

→ Completed → eventtype

tag = Severity = 3

Normal

Lookup:-

① csv

② Kvstore -

③ Geospatial

④ Database

⑤ External

① csv lookup :-

Lookup file.

Index Data. + csv. → Final o/p.

① Small & static file.

② Not updated frequently.

→ lookup is uploading (server), Not indexed

↓

No license is consumed.

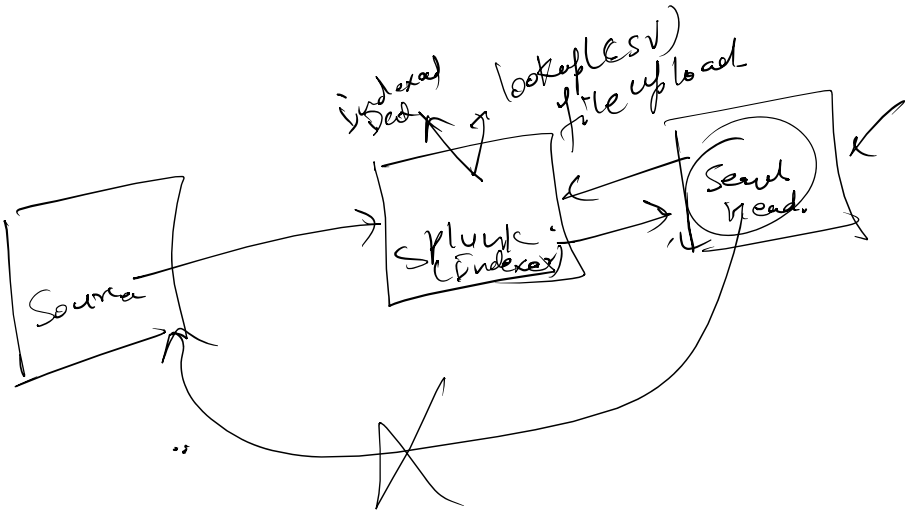
① Sample_lookup.csv →

| lookup VK_sample_lookup.csv

SPL :- | inputlookup VK_sample_lookup.csv

↓

lookup file name.



Lookup Definition:-

↳ Define schema of the Lookup file.

Ticket Number,	Time taken

Automatic lookups:-

```
index=vk_idx source=Sample_tickets.csv
| table ticket_number, severity, current_ticket_state
| lookup vk_lookup_definition ticket_number OUTPUT time_taken as
time_consumed
```

Avoid this one.

field extracted

Data model:-

Use searching speed.

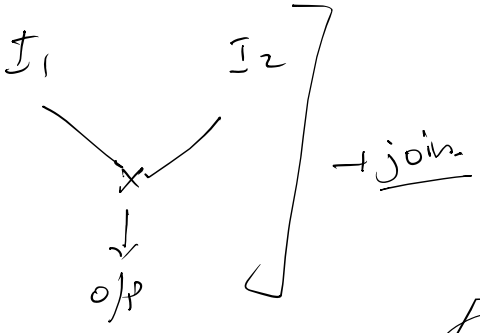
Data model:-

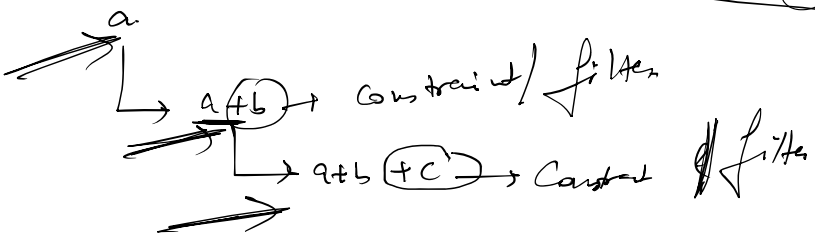
1. Increase the searching speed.

2. How? (1) Define the fields in advance itself.
   (2) ts idx file - timestamp summary file.
   (3) Hierarchical concept.

flow

Root
↳ child+C'
↳ Sub-child+C''
↳ Sub-sub child+C'''





datamodel.

Pivot:- Visualize your data.

Data model, it will refer.

index + timechart, chart.

Pivot → Data model.

→ click to go

Pivot → click to go

Tomorrow's

1. Alert
2. Report
3. Workflow Action
4. Transaction.
5. Classic Dashboard.