Day - 3

11 June 2025 10:16

1. Rex Command.

2.

Raw → extract the particulafield.

↓

Regular exp. → field extraction.

↳ Pattern matching.

→ [Transforms. conf]

① Calculated field:-

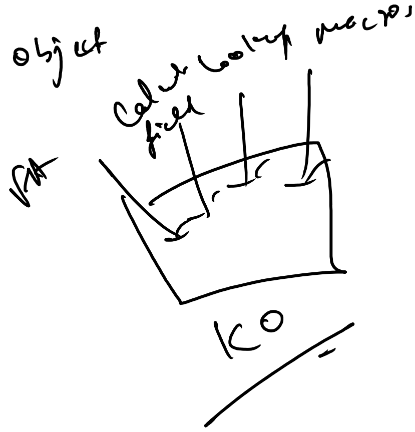
bytes → KB

eval KB = round(bytes / 1024)."Kb"

Kb

↳ template → KB → Any other Normal field.

Knowledge object



field. → new name

② Field Alias:- → [Transforms. conf]

1. Pull the NewName to field.

2. Severity → Priority.

↓ name

↓ NewName

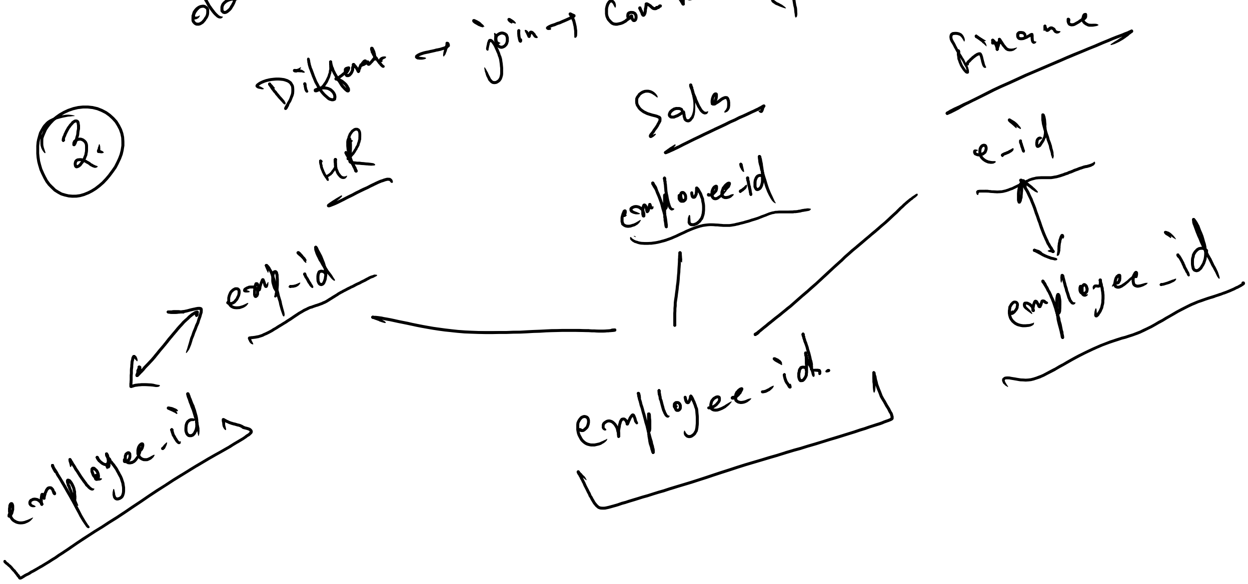
field.

2. NewNa

f
oldname

Different → join → Common field.

2.



3 Tag & Eventtype:-

Tags → Categorise the data.

Severity = 3 → tag = Normal

Severity = 1 → tag = Critical

2 New field will be generated. ←
1. tag → tag = Normal
2. tag::severity → 1|2|3

Eventtype:- Attach the value to the specific eventtype.

CTS = "Closed" OR CTS = "Resolved"

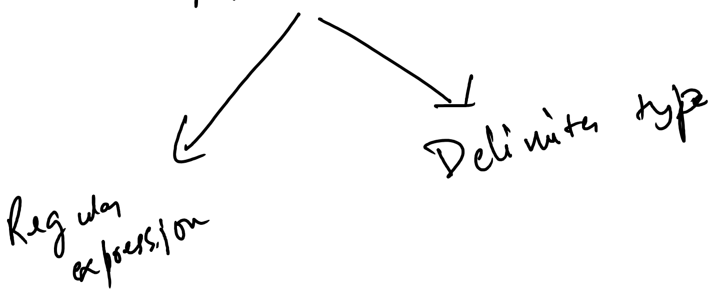
↓

"Completed"

eventtype = "Completed"

(4) field extraction:-

Rex type → manual Field extraction,



Regular expression

Delimiter type