Day - 4

24 April 2025 10:09

1. Data Model.
2. Transaction.
3. Workflow Action

SPL:-

1. eventcount
2. addcoltotal.
3. join
4. xyseries.
5. multisv | multikv
6. spath
7. append | appendcols | appendpipe.
8. where
9. eventstats | streamstats.
10. Tstats.

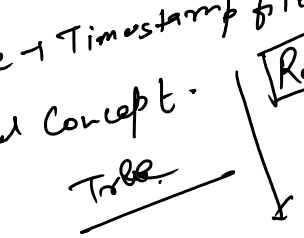
1. Data Model:-

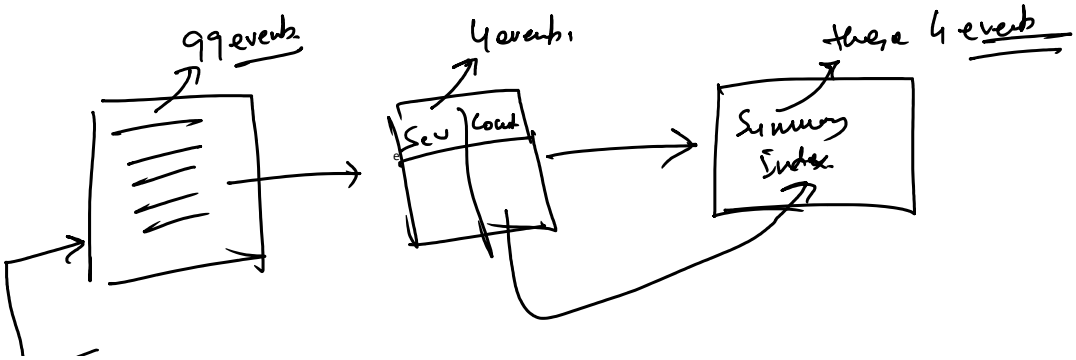
1 Million record → IP pattern

index = ——

1. Pull event
2. extract the field

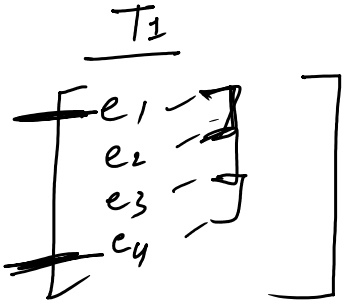
1. Define the required field in advance → Auto → Coldid → Rex → lookup.
2. Tsidx file → Timestamp file.
3. Hierarchical Concept. Tree.



(2.) Transaction:- Group the event on the basis of certain Condition.

- maxevent → Max no. of event in a singletransaction. ex: 4
  maxspan → $(e_4 - e_1)$ → Time diff.
  maxpause → $(e_2 - e_1)$, $(e_3 - e_1)$ → Time diff.




(3) Workflow Action:- Capture the certain field value & send to the external website/customsearch.

↓

Sharepoint, confluence, snow etc.

SPL:-

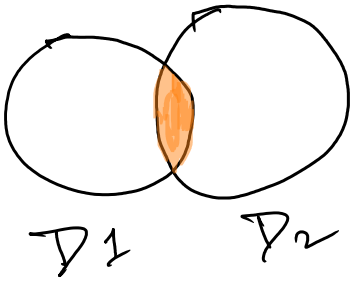
(1) Addcoltotal & Addtotal:-

↓ Addition of column wise

→ Addition of row wise.

## ② join:-

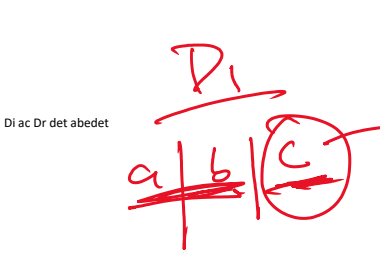
### ① Inner join:-




abcde

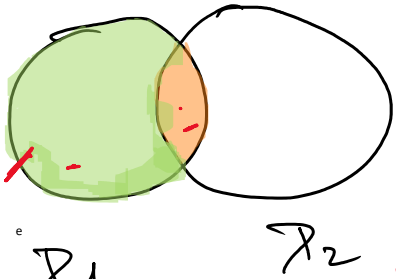
abefgh

↳ abe





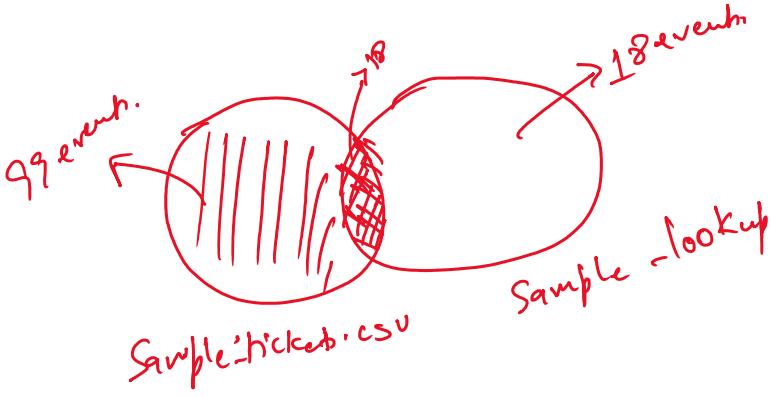
### ② leftJoin:-




abcdef

abefcd

abefghi




## ③ Append | Appendcols | Appendbips:-

Append:- Combine two Datasets

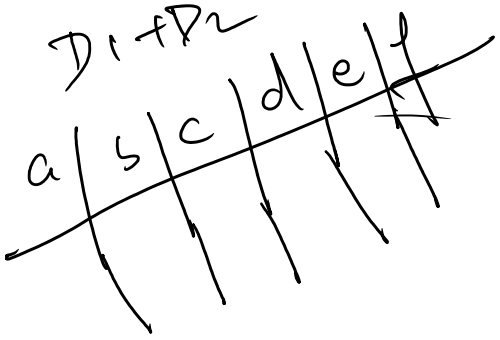
D1

| a | b | c |
|---|---|---|

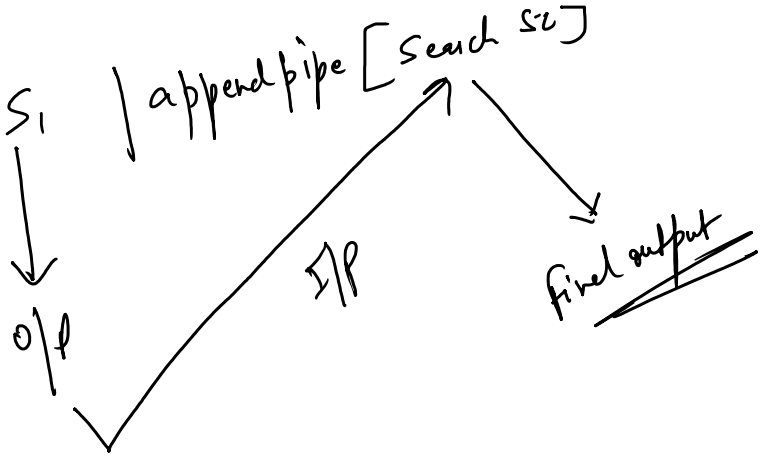
D2

| d | e | f |
|---|---|---|

D1+D2 . . . . . left




Appendpipe:-




(4) where:-

filter → search (filter on the basis of field value)

→ where (filter/compare b/w two different fields)

(5.) Eventstats / streamstats

stats → statistical output.

Eventstats:- → output → event format.

Streamstats:- incremental / streaming fields

(6) Tstats :- find the statistical output.

Very quick → Tsidx file.

↳ timestamp & the scheme of data.

(7) spath :- → XML

→ json Data.