Day - 4

30 December 2024 14:38

1. Alert
2. Report
3. Workflow Action.
4. Transaction.

Adv. Command:-

1. append | appendcol | appendpipe.
2. join.
3. spath.
4. multikv.
5. mv.
6. eventstats.
7. streamstats.

(1) Alert:-

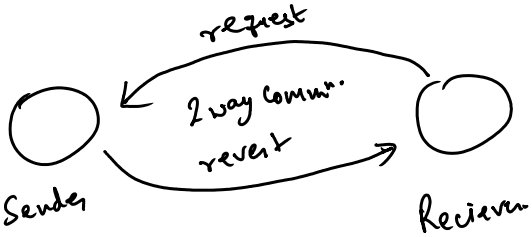
1. Certain Condition Met → it will trigger.
2. After trigger → Alert Action.

[Definition.
1. SPL Query
2. Schedule time
3. Interval.

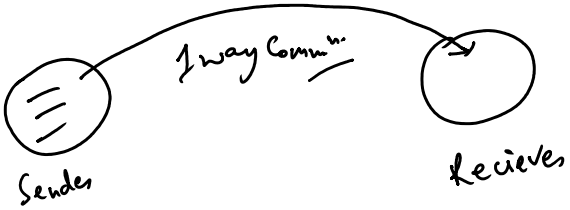
[Alert Condition
1. when?

[Alert Action.
1. Email
2. SMS
3. Triggered Alert
4. Custom Alert.

API:-




Webhook:-




Report:-

[Definition]

[Action]

No Alert Condition.

Maj. diff. b/w Alert & Report

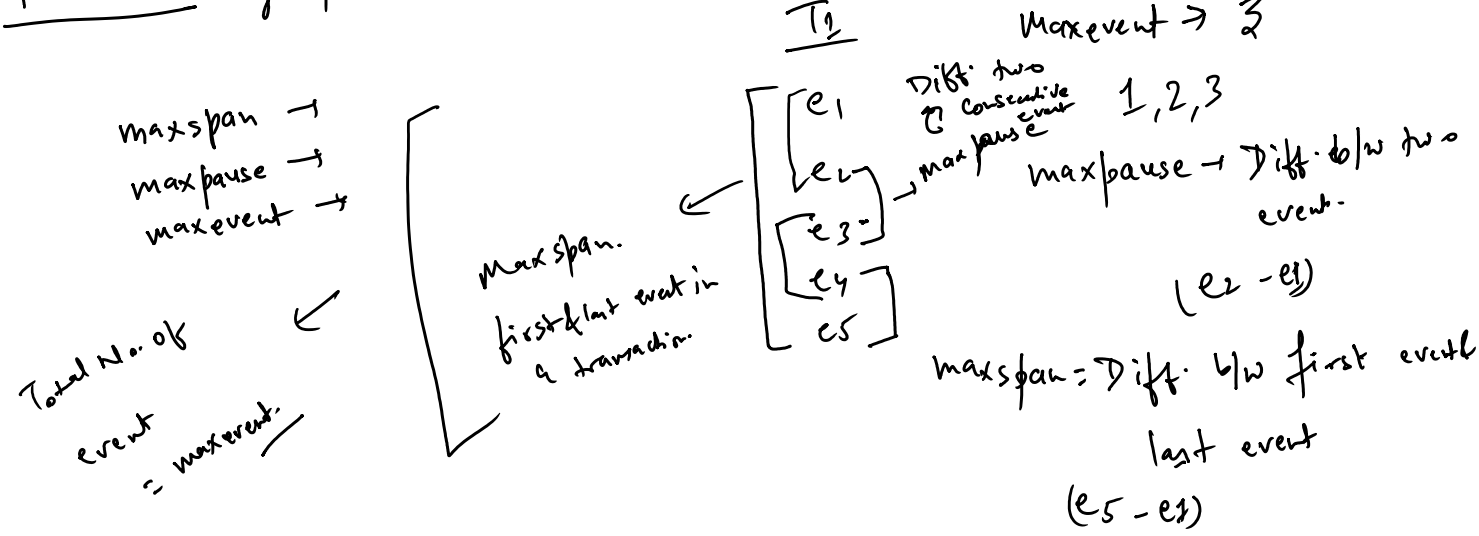
↓

In report, there is no Condition.

whereas in alert, you are going to define Alert Condition.

wherein in alert, you are going to define.

**Transaction:-** group the event on the basis of certain fields.

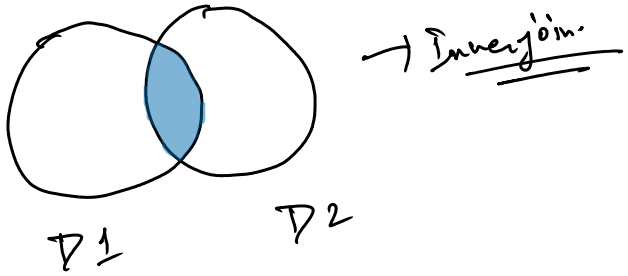



**Workflow Action:-**

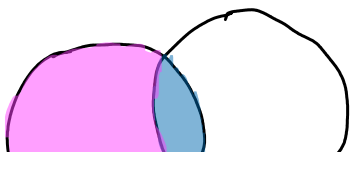
field value → redirect to other website/link/search in that case we use the workflow Action.

**join:-** ① inner join.
② left join.

① **Inner join:-** it will only consider the common value.

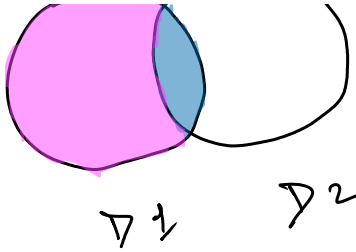



② **Left join:-**



① Conside the common value.
② Left set of Data is

(2.) Left join

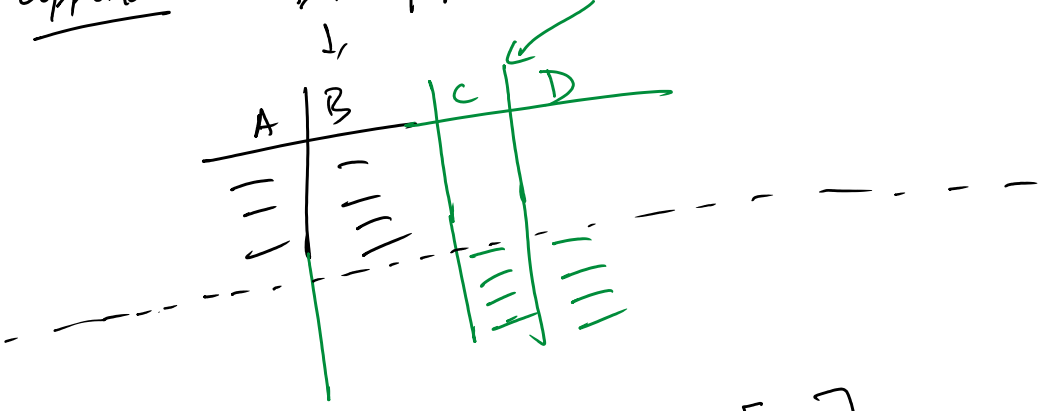


D1 D2

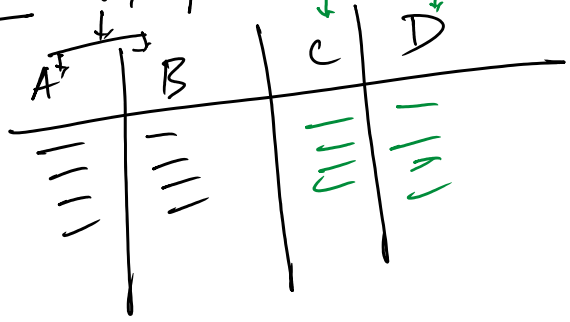
(2.) Left set of Data is consider (D1).

* Append / Appendcol / Appendpipe :- Combine / append field from two dataset :-

append :- D1 | append [D2]




appendcols :- D1 | appendcols [D2]




appendpipe :- Output of first search Query, will be the input of the second search Query.

D1 | appendpipe [D2]

output ↓

A, B, C

Input →