Day - 4

25 September 2025 10:12

1. DSL :-

1. fetch.
2. fields
3. fieldsRename.
4. fieldsAdd.
5. filter.
6. filterout.
7. sort
8. dedup.
9. Summarize
10. fieldsRemove.

I. Dashboard
II. Notebook.
III. Workflow.
IV. Anamoly Detection
V. Alert.
VI. Integration.
VII. Containes monitoring.

1. DSL:- 1. fetch:- Pull the logs from the set of dataset.

|fetch logs

2. filter:- used to filter the specific value.

|filter status == "Info"

|filter Contains(status, "Info")

↳ wildcard

— info —

3. filterout - Remove the value from the filter.

4. Summarize:- Create aggregate value.

| summarize count()

(5) fields:- Table format.

| fields a, b, c

(6) fields Rename

= | fieldRename New_name = old_Name

(7) fieldsRemove = Remove the fields from the o/p.

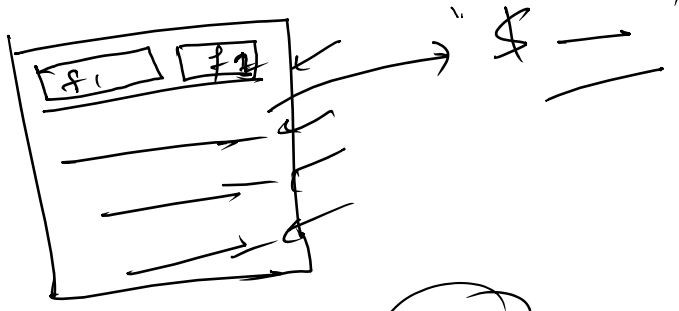
= | fieldRemove status
↓
Remove status field.

(8) sort - Sorting purpose → | sort A asc / desc | | sort A (Ascend.)

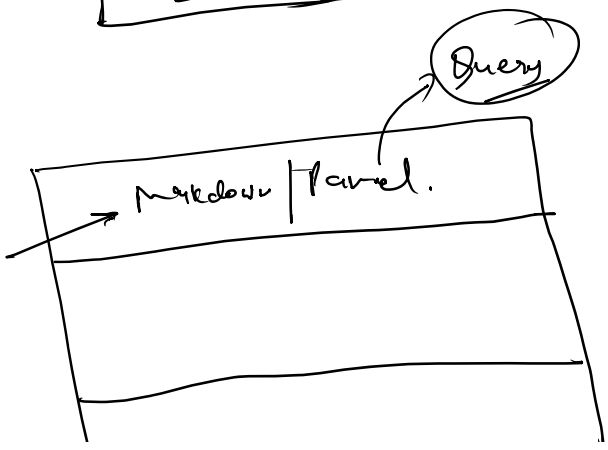
| sort - A
↓
Descend.

(9) dedup - Remove duplicate values
↳ | dedup status.

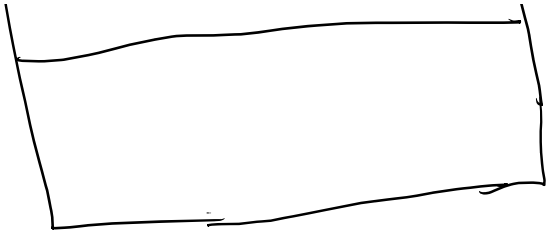
Dashboard:-



Notebook's



Testing | Intervals ago



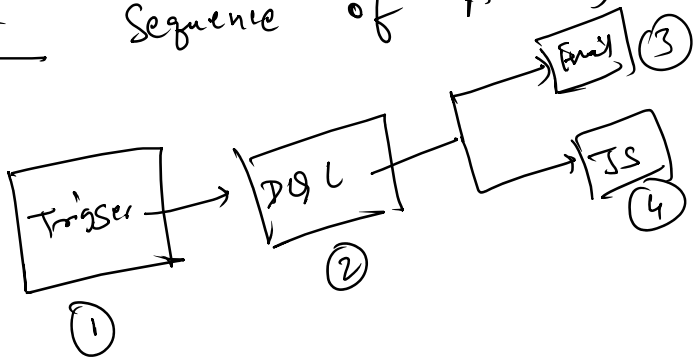
1000 — 1K

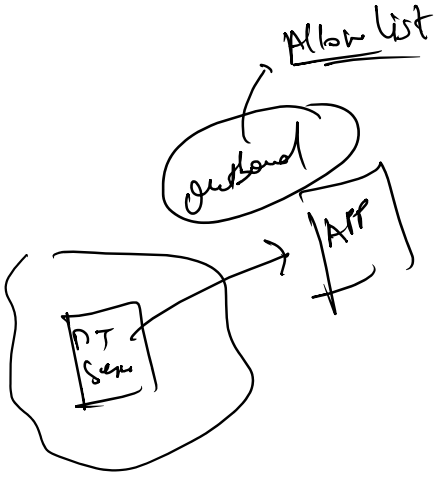
1000000 — 1M

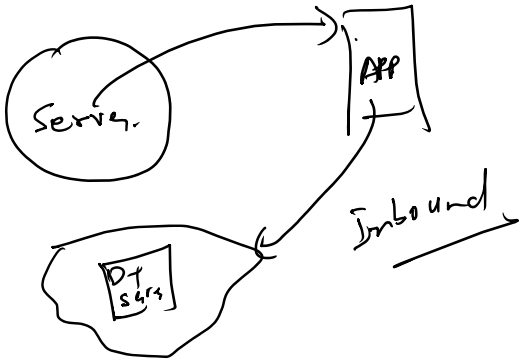
Dashboard - Real time monitoring, Context (Visualization), static in structure → Status Board, Summaries, end user

Notebook - exploration, Analysis & Investigation, engineer/developer, deep dive, Ad-hoc troubleshooting, root cause Analysis or performance investigation.

Workflow :- Sequence of Activity :







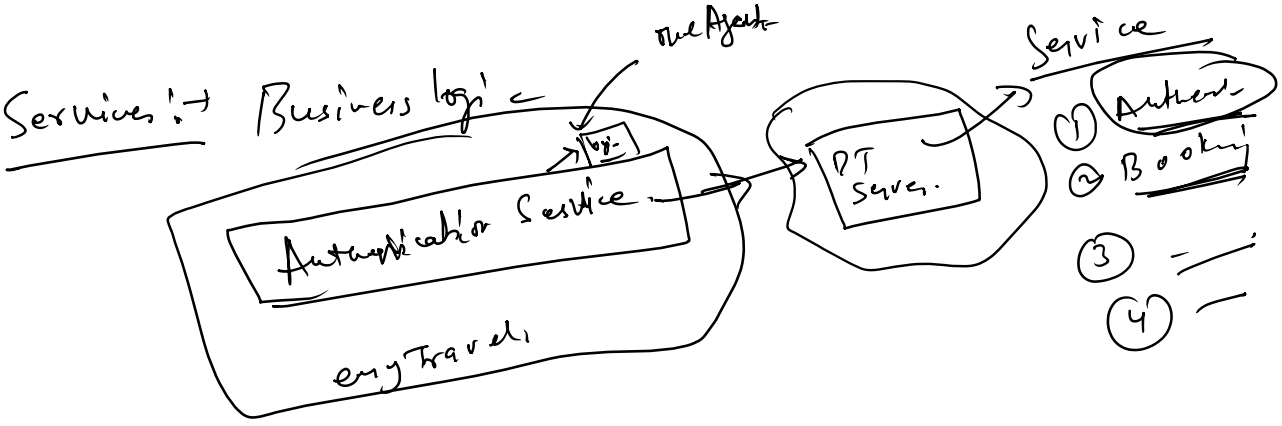
Process Grouping :- Group the list of process into a single group.

→ OneAgent → DT OneAgent

Single Group.

ex:- java → java group

OneAgent → DT OneAgent



Tomorrow:-

1. Anamoly Detection.
2. Alert
3. Integration
4. Davis AI
5. Database visibility