Day - 3

05 September 2025 19:43

1. Dashboard:-

1. classic Dashboard,
2. Studio Dashboard

1 Classic Dashboard:-

1. xml
2. Panels & Visualization
3. Feature driven.

2 Studio Dashboard:-

1. json
2. Visualization specific

2. Alert.

3 Report.

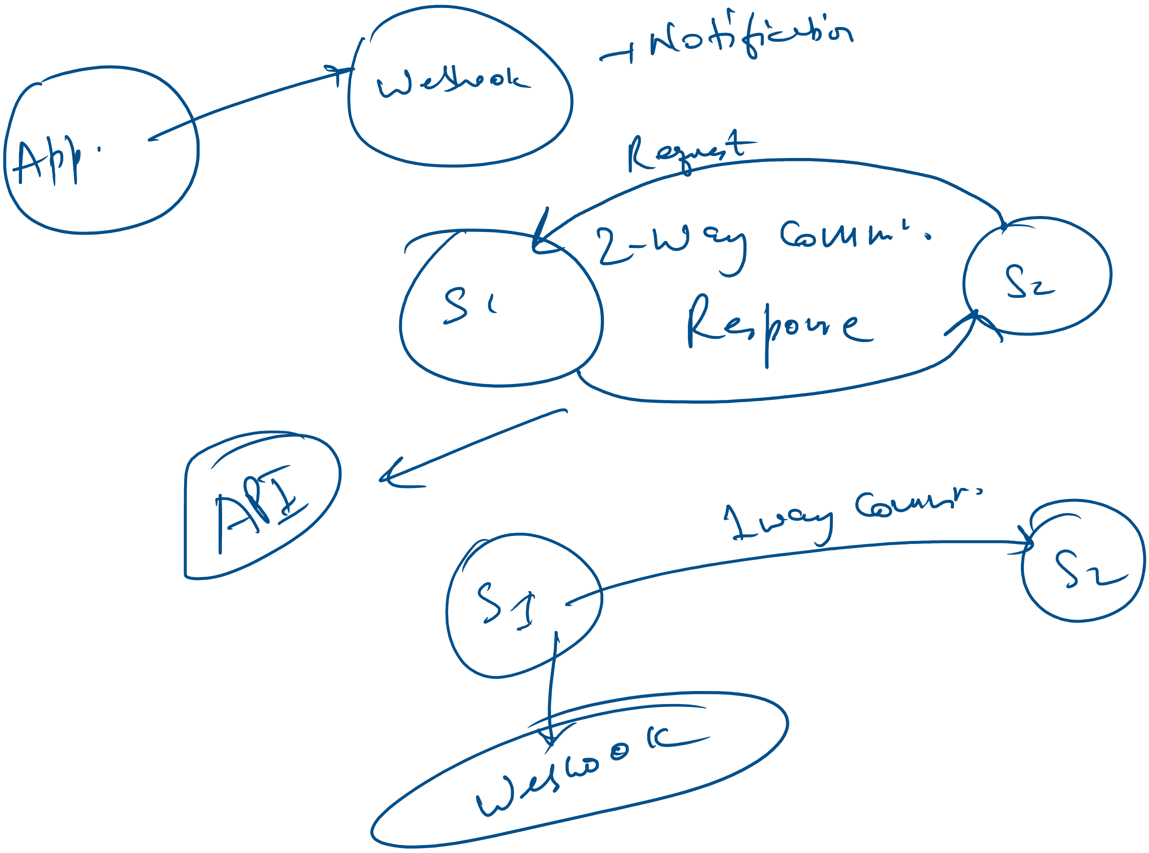
4 Data model & Pivot

Alert:-

Defination SPL, schedule.

Trigger Condition.

Trigger Action.



Report:-

Definition.

Trigger Action.

Alert & Report

Trigger condition

Not need Trigger condition

Data Model & Pivot:- → security, operation.

Data Model & Pivot :-

1. Extraction of fields] → security, operation.
2. Listing the events

↓

Datamodel
→ 1. Define the field in advance.
→ 2. Hierarchical concept
Root
↓
child
↳ sc'

3 Define the data mapped with tidx file
↓
timestamp summary file.

Pivot → use for Visualization
↓
only when Datamodel is available.

filter status=500

last 24hrs.

```
index=web_logs sourcetype=access_combined status=500 earliest=-24h@h latest=now
| stats count AS error_count by clientip
| sort - error_count
| head 5
| join type=inner clientip
  [ search index=web_logs sourcetype=access_combined earliest=-24h@h latest=now
  | stats count AS total_requests by clientip ]
| eval error_percent = round((error_count/total_requests)*100,2)
| lookup geoip clientip AS clientip OUTPUTNEW city country
| table clientip, city, country, error_count, total_requests, error_percent
| sort - error_percent
```

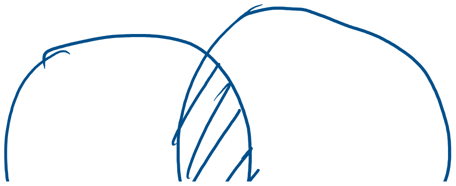
Descending order.

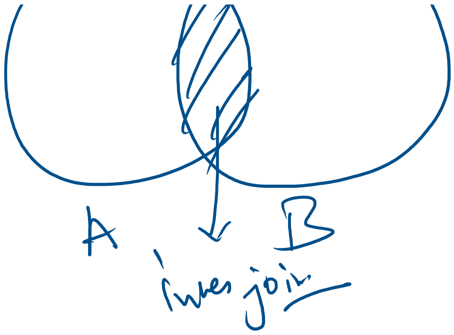
→ first 5 data record

S1

S2

file name in lookup.




A
B
inner join