Day - 4

24 July 2025 10:14

Workflow Action:-

asset_id = "directory" → URL, Pages → inventory, confluence, Service now spreadsheet.

Data Model & Pivot:-

1. Why?
2. What?
3. How?
4. Where?

Why! → Increase your searching speed.

Where? → / Both ←
1. Data is very huge.
2. Critical in Nature. (eg. security, operation) where you need immediate result.

What? →
1. Tsidx file → Timestamp summary file.
2. Extraction of fields. → you have to get the selected field in the advance itself.
3. Hierarchical concept.

```
Root
 └→ child + c'
      └→ child + c''
           └→ child + c'''
```

Cons:- 1. Increase in computational resource - ex → CPU, Disk & Memory.

1 million index → 4s
datamodel = 2s

How →?

* json ~~format~~ dm is saved

Data Model Acc.:-

1. Adv. - Increase the searching speed further.
   How! → it will save the o/p in the summary data.

2. Dis Adv.:-
   1. more the time range, more data is saved as summary, Hence consume more disk & memory.
   2. you can't edit the data model when it is in acceleration mode. You need to de-accelerate, make the change & Accelerate back.

Pivot:- Visualization purpose.

chart & dirge chart → index.

w/o dM, you cannot create the

Chart & time chart → index.

Pivot → data Model. w/o dM, you cannot create the Pivot.

* classic Dashboard:

Splunk Dashboard → Classic → XML → Feature driven.

Splunk Dashboard → Studio → -json → V.8.2.x → Cosmetic Part.