Day - 3

03 September 2025 10:14

DQL → Dynatrace Query language :

1. fetch.
2. fieldsSummary
3. Summarize
4. fields
5. fieldsAdd.
6. if-else
7. fieldsRemove - exclude the field from the o/p.
8. fieldsRename - Rename the field
9. filter - filter on the basis of certain condition.
10. filterout - filter/exclude that particular option.

```
if (Condition)
{
True
}
else
{
False
}
```

→ `if (Condition, "True", else: "False")`

Parse content "

Management zone :- Categorise your Artifact into diff. A/p category wise.

Tags :- Map the certain value with a defined context

1. Manual → Tag → Add
2. Automated → Rule → Automatically Tag will be added.

Alert :-

1. Body
2. — Email, Jira, Servicenow

Alert

(1) Issue

(2) Integration — Email, Jira, ...

Davis Security score :-

Score :- 0 to 100

Higher Score means more Secure env.

Purpose :- Prioritize remidation by defining risk.

Factor :-

(1) No. & severity of Vulnerability

(2) Exposure of vulnerability comp. to the internet.

(3) Risk context provided by Davis AI

Calculation :-

(1) Vulnerability Detection -

(2) Risk Assessment of each Vulnerability.

(1) CVSS Score - Common Vulnerability Scoring System.

(2) Exploit Availability

(3) Public exposure - Accessibly internet.

(4) Affected business Service

(3) Entity Weighting -

(4) Aggregate risk calculation.

(5) Normalization to a Score (0-100)

90-100 - Excellent

70-89 - Good

70-89 - Good

50-69 - Risky

0-49 - Critical.

(6) Continue update.

Ex:- (1) 50 Vulnerabilities → 85 ↑

(2) 5 vulnerabilities - critical CVEs → below 50

How to improve Score:-

(1) Prioritize fixing internet-exposed CVEs

(2) Exploits

(3) Patch or update

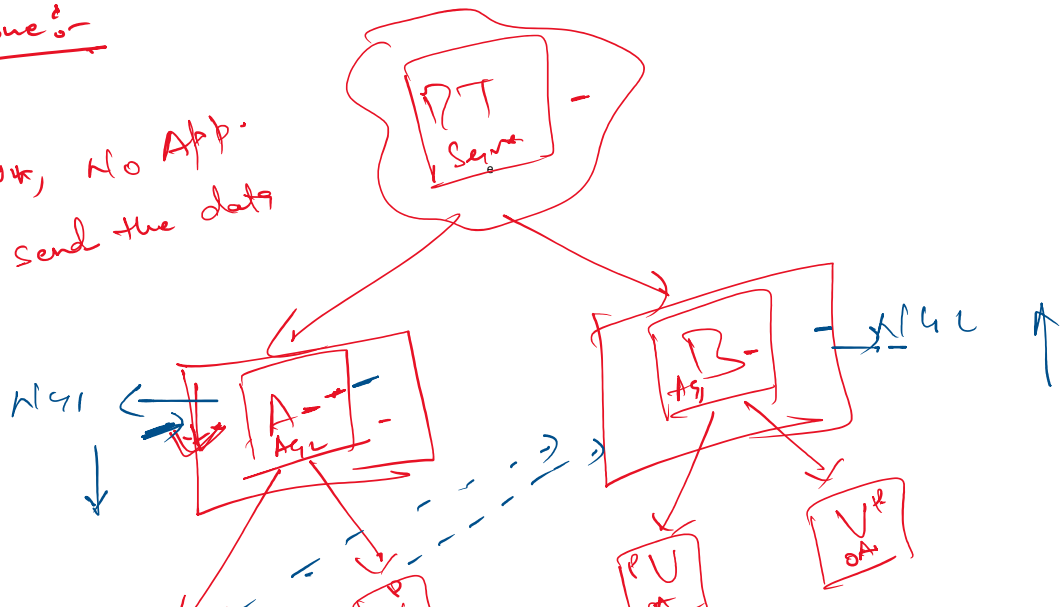
(4) Automate

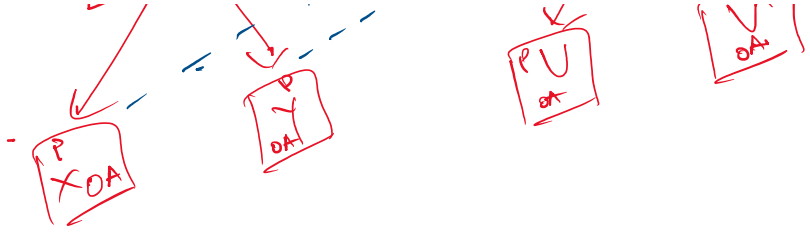
(5) Monitor trend

* Network Zones:-

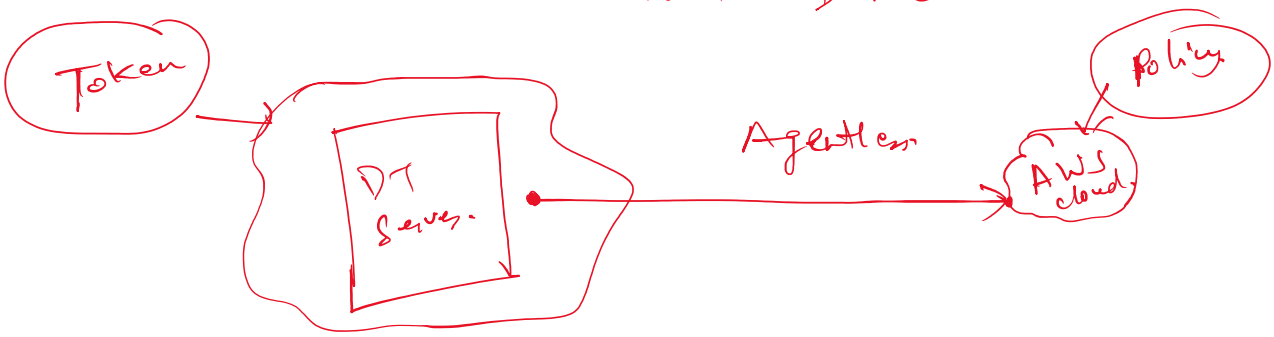
(1) If AG goes down, No App. is able to send the data

(2)





* cloud Monitoring :- AWS Account Push the data to the DT end.



Tomorrow :-

1. SLO Creation.
2. Containers monitoring.
3. Apache Kafka.
4. Process group setting
5. Davis AI