Day - 3

03 September 2025 10:14

DQL → Dynatrace Query language.

1. fetch.
2. fieldsSummary.
3. Summarize
4. fields
5. if-else
6. fieldsAdd.
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:- Categories your Artifact into diff. A/p category wise.

Tags:- Map the certain value with a defined context

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

Alert:-

1. Body
2. Integration - Email, Jira, Servicenow

② Integration

Davis Security score :-

Score :- 0 to 100

High Score means more secure env.

Purpose :- Prioritize remediation by defining risk.

Factor :-

1. No. & severity of vulnerability
2. Exposure of vulnerability comp. to threat 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 - Access by 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

50-69 - Risky

50-69 – Risky

0-49 – Critical.

6. Continuous update.

Ex:- 1. 50 Vulnerabilities → 85 ↑

2. 5 vulnerabilities – critical CVEs – below 50

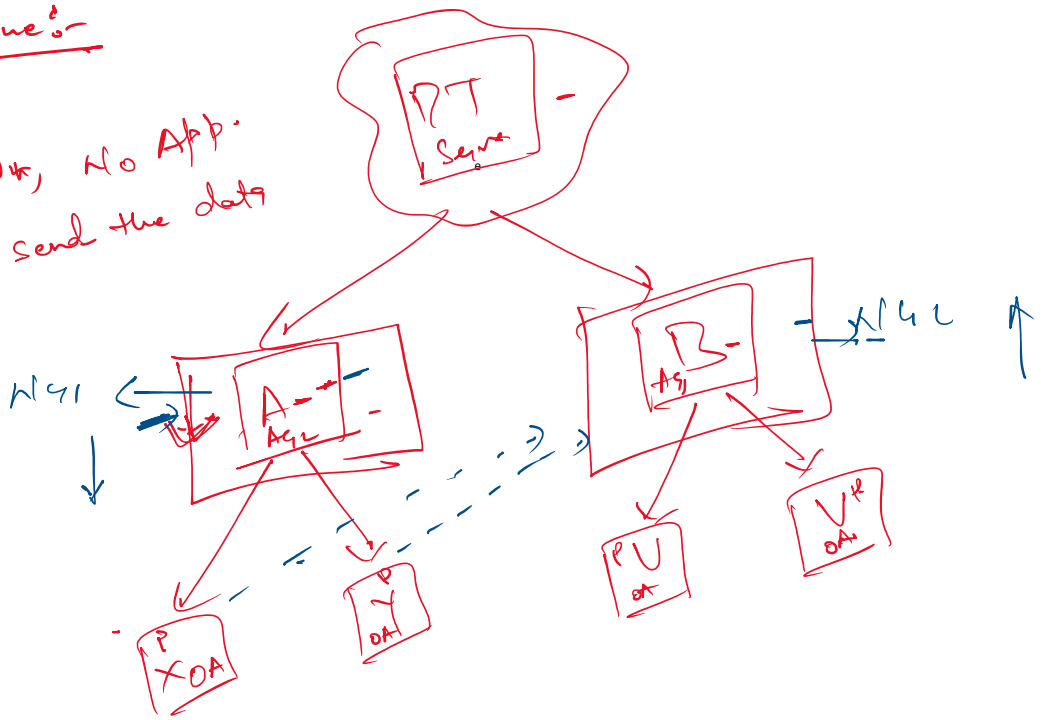
How to improve Score:-

1. Prioritize fixing internet-exposed CVEs
2. Exploits
3. Patch or update
4. Automate
5. Monitor trends

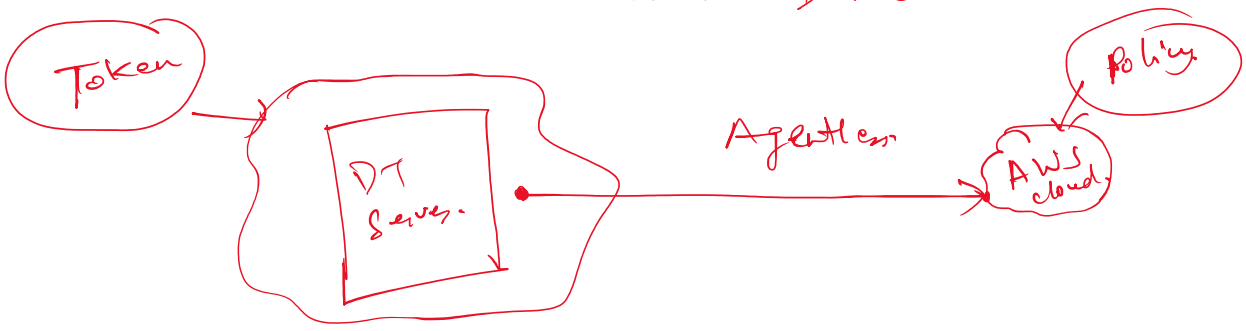
* Network Zones:-

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

Pending from myside

1. DQL Document

Davis's AI :-

1. what?
2. what it actually does?
3. Use Cases on Davis AI
4. Why it is diff..?
5. Quick setup & tuning tip.

1. **What?**

combine causal AI, Predictive AI & Generative AI (Davis copilot)

(1.) What:

AI engine combine casual AI, Predictive AI & Generative AI (Davis copilot)

Detect Anomalies, auto correlate symptom - sig le root Analysis

DQL

(2) What?

(1) Casual, topology - aware detection.

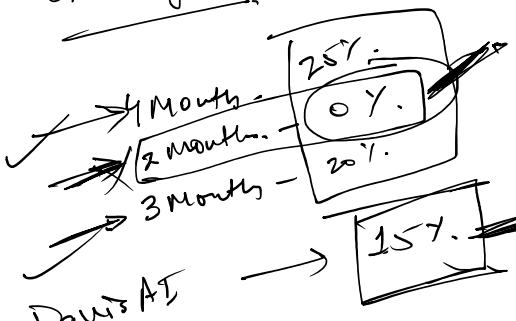
(2.) Automated Anomaly Detection - Baseline Behavior,

(3.) Predictive & Statistical Analysis:- Forecast & model based Anomaly Detection.

(4.) Generative Assistant (Davis copilot) - Query → DQL

(5) Unified data (Grail):- Datalake of Dynatrace.

(1.) CPU usage:-



22-5% → fixed threshold

Threshold Auto Adaption

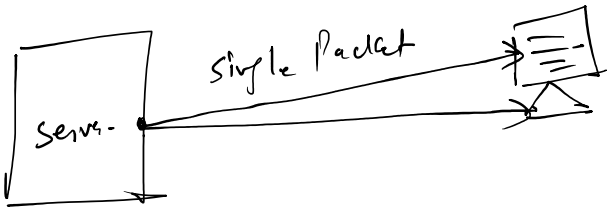
(2.) Timeshoot:- 1-20 → less users.

20-25 + max users → fixed → 15% / 25%

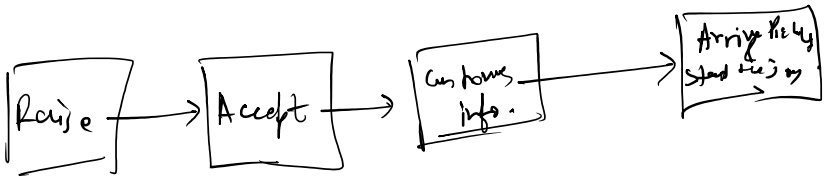
Auto → 15% ↓ 25%

(3.) Apache Kafka:-

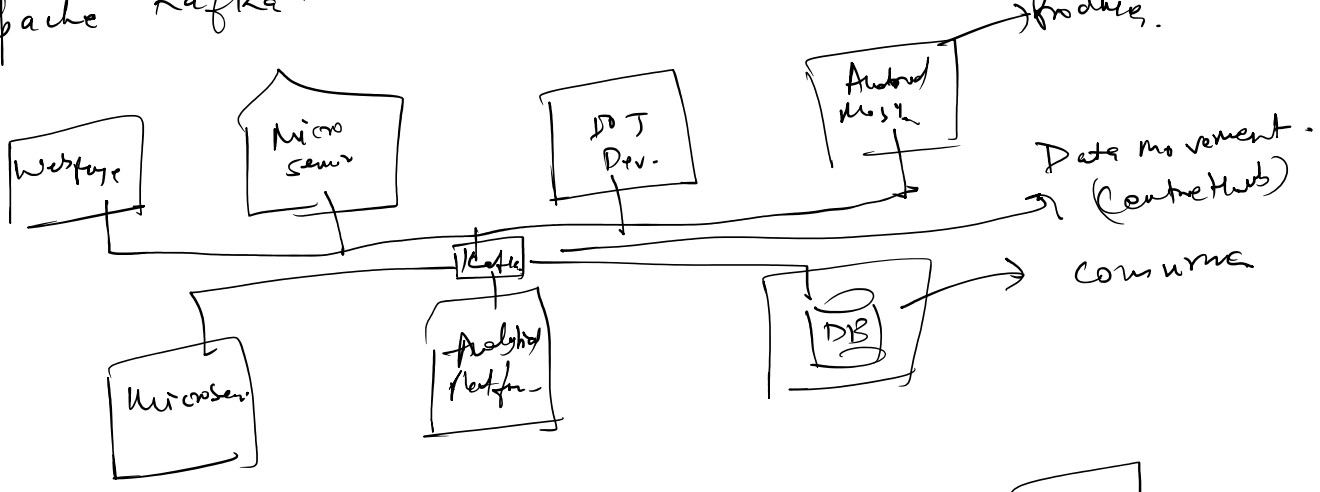
Event streaming



Multiple / Continuous flow of data packet from the source to destination.

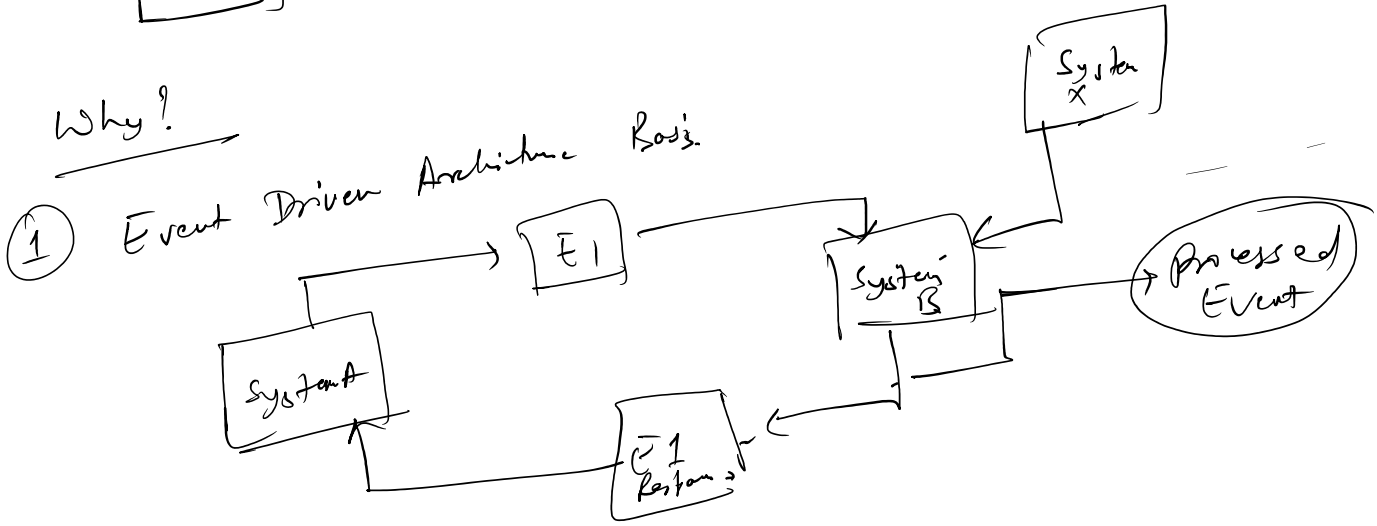


Apache Kafka – Distributed event streaming platform.



Why?

(1) Event Driven Architecture Basis.

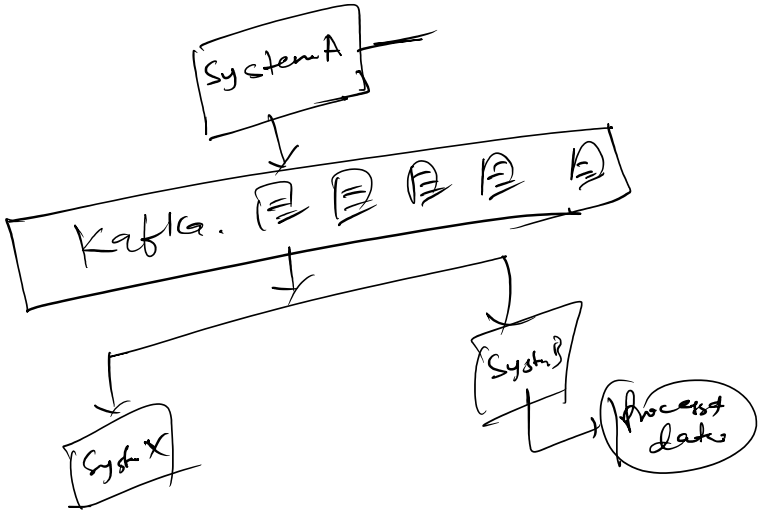


Pitfalls

(1) Tight coupling

(2) Reduced Scalability

(1) High [illegible]
(2) Reduced Scalability.
(3) Single point of failure.
(4) No message persistence.



Benefit :-

(1) High Throughput = Massive event stream.
(2) Fault Tolerance = resilience & high availability
(3) Scalability - Instant data & effortless Scale your infra.
(4) Real Time Processing - Enable instant data insight action with Kafka low latency Stream processing.