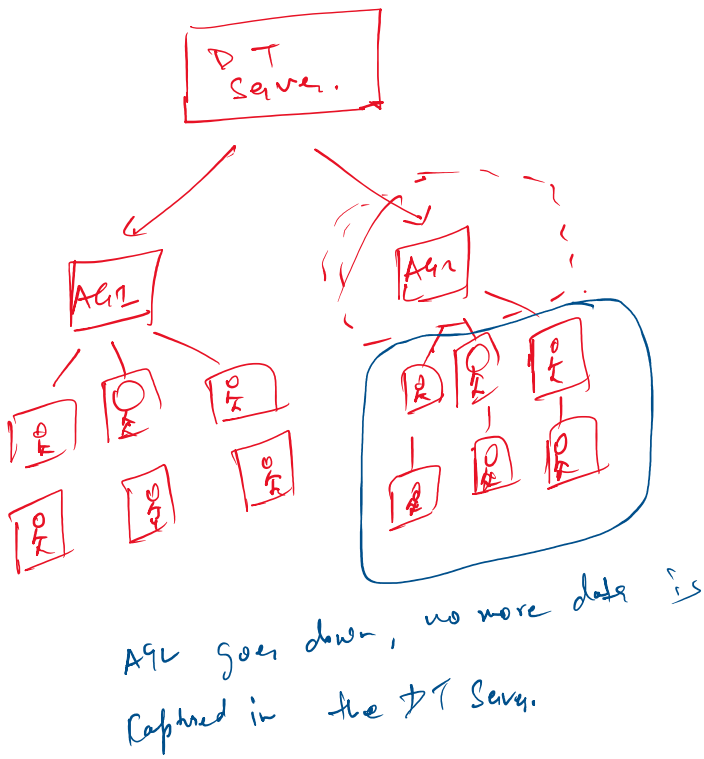


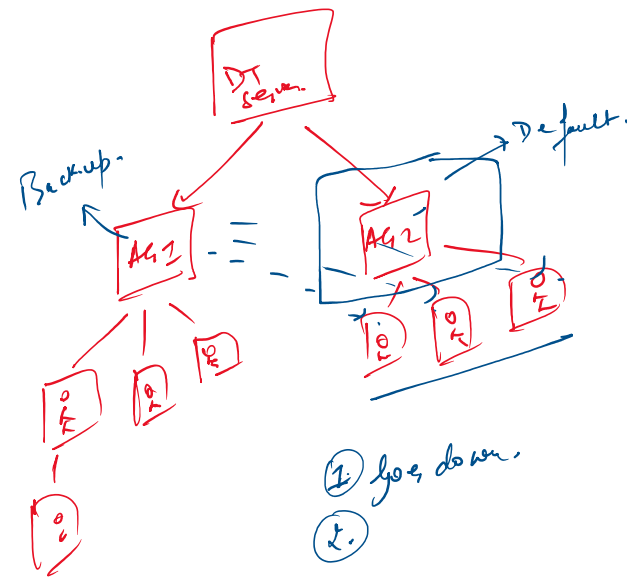
① Network zone!

- ① Architecture-
- ② Why?
- ③ How?

W/O Network zone.



With N/w zone

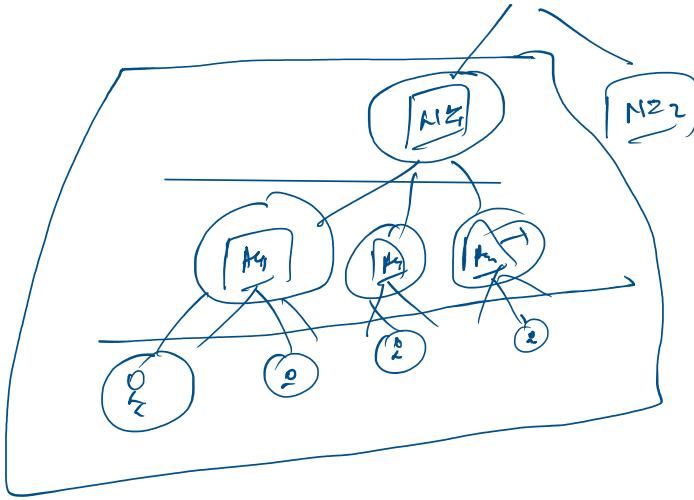


- ① Fallback mechanism.
- ② efficiency.
- ③ Scalability.

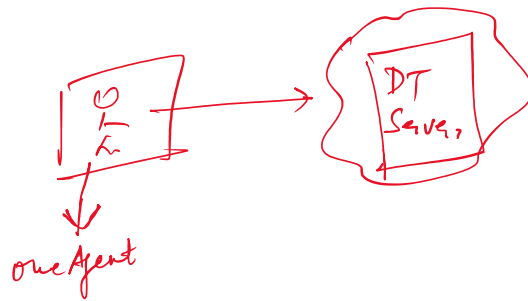
① Uninstall the existing AG in windows.

② /bin/ls DT --set-network-zone= AG2

→ Tag this AG with the n/w zone



② Host Group:-



③ License:- Two Model -

- ① Dynatrace Platform subscription (DPS)
- ② Classic Licensing,

① DPS:- Annual Platform commitment. (1 yrs or 3 yrs)
Rate Card (APM, DPM, RUM, logs, Traces, Synthetic etc.)
Usage is tracked on the hourly with budget visibility.

② Classic Licensing:- Unit method.

- ① Host Unit - One Agent Host
- ② DEM - RUM / Synthetic
- ③ TTV - Custom metric / logs / events / traces

- (2) DERI -
- (3) DDV - Custom metrics / logs / events / traces
- (4) ASU - App Sec.

(4) Default Retention in DT S ASU Grafal → Data Lake of Dynatrace

- (i) logs → 35 days. → built in default log buckets.
- (ii) Metrics → 15 months (default) - 10 yrs.
- (iii) Distributed trace (Grafal) - Default = 10 days → 10 yrs.
- (iv) Distributed traces (classic) - 10 days.
- (v) RUM - 35 days.
- (vi) Synthetic monitor = 35 days.
- (vii) Davis Problem = 14 months.
- (viii) One Agent / Active Gate Diagnostic = 30 days.

(5) Service → All the service will be auto captured.

Alert →
 Problem notification / vulnerability
 Anomaly detection task

(6) User & Role Management:

