BackUp Policies in otsuka:

These backup policies are crucial for ensuring data protection, disaster recovery, and business continuity

In Otsuka we are following TAG based backup policies.

Tags are key-value pairs that help categorize and manage AWS resources, so that we can streamline the backup process for specific sets of resources.

currently we have 4 backup policies .as follow

**Bronze**> every day once backup

**Gold**> every 4 hrs backup

**Silver**>every 12 hrs backup

**Platinum**> every 4 hrs backup and keeping the copy in secondary location(primary us-east1, secondary us-west-2 this is for prod servers for most of the prod servers we enabled dr in secondary location )

noramlly we have DR in every year,for every axp applications. when ever we performDR, those list of application server should enable the platinum, because the DR test perform on secondary site, so before proceding to DR we need to confirm weather platinum backup policy assinged or not .we need to restore and update dns, and update url in dns server also. windows team wl manage this.

external DNS managed by network team and internal DNS managed by windows team.

we used to get the email alert when ever there is a failure in backups. ICC team will create the Incident with the list of failures based on the failure report ops team work for the reason for failure.

and backups data moving to cloud s3 buckets, so end point backup is s3.

use case: most of the cases resourse limit exeeded we need to work on increase the limit.

external dns managed by network team and internal dns managed by windows team.

and backup level we used to get the email alert for the failed report, so icc teamwl create the incident TT with list of failures, based on the that ops team work for the reason for failure.

ex: most of the cases resourse limit exeeded we need to work on increase the limit.

some times, when deploy new server we enable the platinum, will initiate the backup to the secondary location , which doesnt have the access. so we used to get the failures.



---------------------

**Network**:

coming to Network part, we Have 2 Availability zones we created, az1 and az2, it is internal az1, and az2, and external we used the dmz network, total 4 subnets we createing every account.

The primary purpose of a DMZ is to add an additional layer of security to the organization's local network.

we shld not use aws public ip, if it happens rapid 7 may trigger the aleret and it will goes to management .