Google Cloud Architect - Resource hiearchy

10 October 2022 17:36

Region - GCP locations are composed of regions and zones.

These regions are available across the globe where the resources can be hosted. Each region in GCP can have three or more zones.

Zone <region>.<zone>
Each zone consists of physical data centers with independent power, cooling and networking support connected to each other over virtual wan or high-bandwidth network.

e.g. us-west-1 region depicts the GCP west coast region.

Zones - us-west1-a, us-west1-b, us-west1-c

a) Handling failure - to minimize the risk of correlated and cascading failures caused by physical infrastructure like power, cooling or networking.
b) Decreased network latency - to overcome the network latency, effective cost benefits

Role Components

a) Title
b) Name (identifier will be in the following format)
- Pre-defined role: roles/SERVICE.ROLE (roles/cloudsql.reader)
- Project-level custom roles: projects/PROJECT_ID/roles/ROLE
- Organization-level custom roles: organization/Org_id/roles/ROLE
c) ID
d) Description
e) Stage (Alpha, beta, GA)
f) Permissions - access policies associated with a particular user or resource. Principles include the details like project id, project number.
g) Etag - AA== for basic and pre-defined roles , updating the custom role, the etags for the custom role changes.

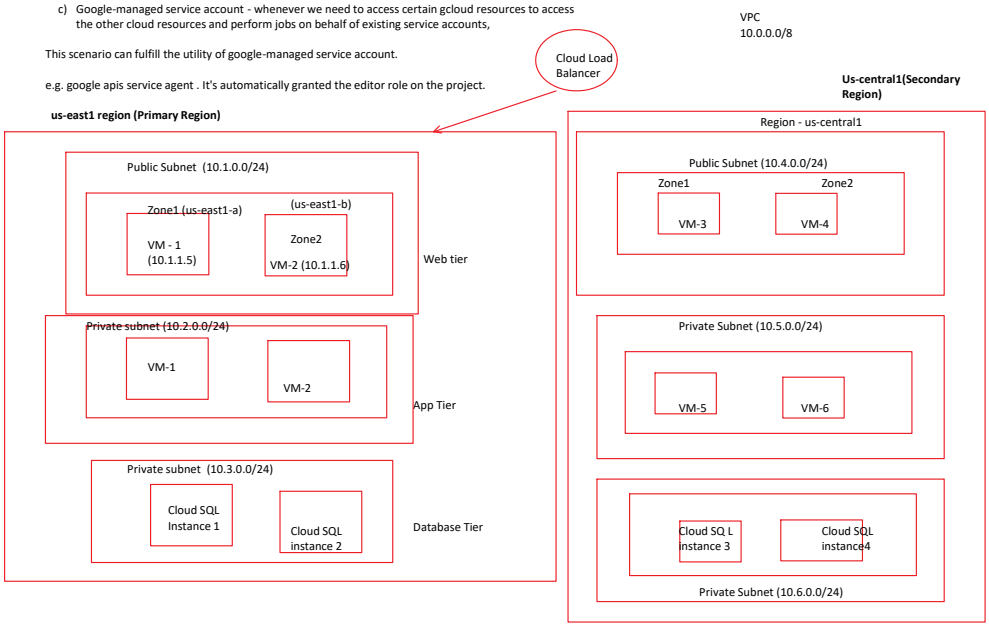
a) User-managed Service accounts - by default there're 100 user-managed service account can be provisioned in a project.
b) Default Service Account - initiated by gcloud itself, when we enable the api for the corresponding gcloud resource, use gcloud services, it has been created user -managed service accounts which can enable the service to deploy the jobs that can access other gcloud resources. These accounts are called as default service accounts.

For compute engine, the default service account name:
"<project-number-compute@developer.gserviceaccount.com"

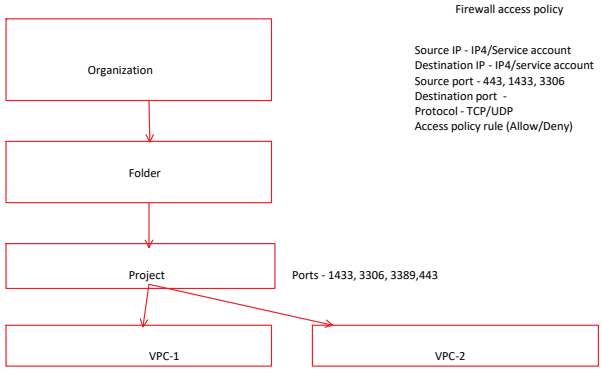
c) Google-managed service account - whenever we need to access certain gcloud resources to access the other cloud resources and perform jobs on behalf of existing service accounts,

This scenario can fulfill the utility of google-managed service account.

e.g. google apis service agent . It's automatically granted the editor role on the project.

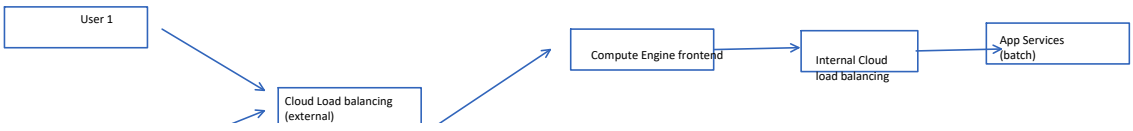


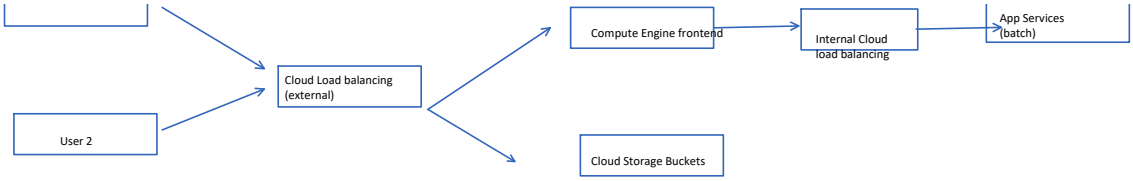
SYN ACK packet - TCP datagrams



Firewall access policy

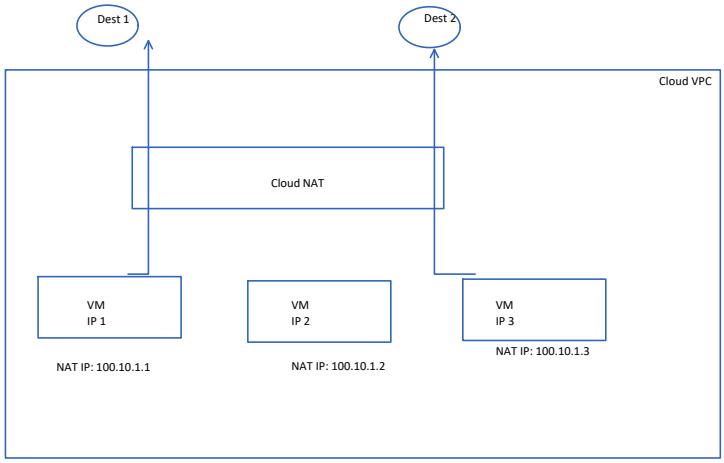
Source IP - IP4/Service account
Destination IP - IP4/service account
Source port - 443, 1433, 3306
Destination port -
Protocol - TCP/UDP
Access policy rule (Allow/Deny)



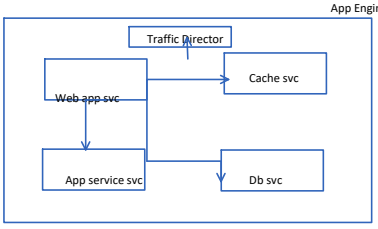


- Global External HTTPs Load Balancing
- Global HTTPs load balancing (classic)
- External SSL proxy load balancing
- External TCP proxy load balancer

- Regional External HTTPs Load Balancing
- Internal HTTPS load balancing
- Internal TCP proxy Load balancer
- Internal TCP/UDP Load Balancer
- External TCP/UDP Network Load balancing



App Engine / Kubernetes cluster on pods as through containers



Istio service mesh

Envoy proxy is the managed proxy service utilized service mesh network traffic routing
Through the apps deployed on containers in Kubernetes cluster.

https://www.cloudskillsboost.google/course_sessions/2516302/video/349763