Google Cloud Architect - Resource hiearchy

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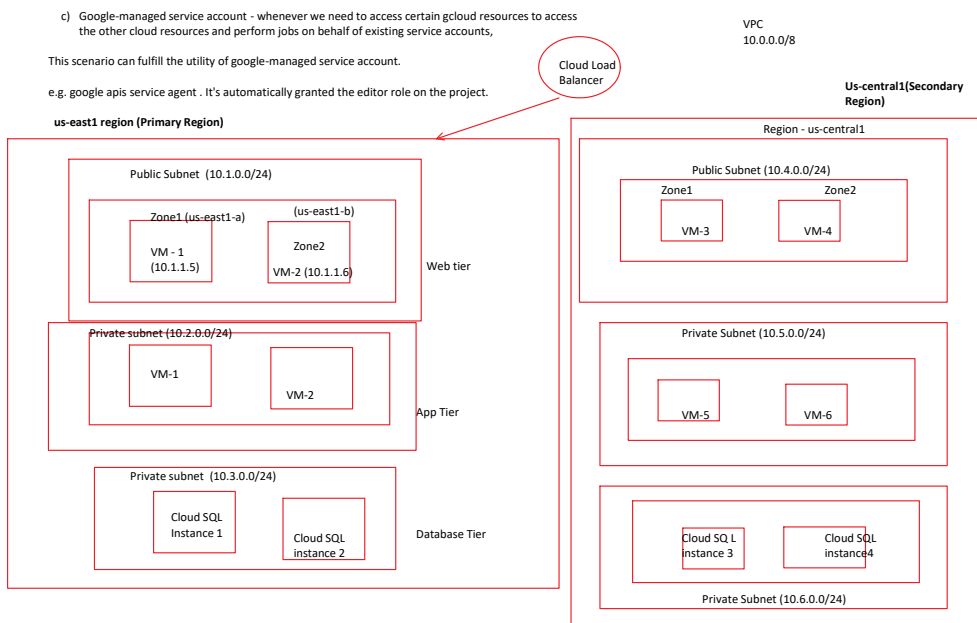
For compute engine, the default service account name:
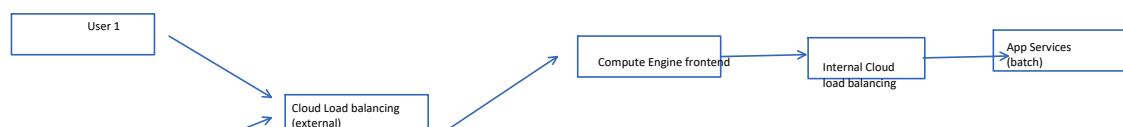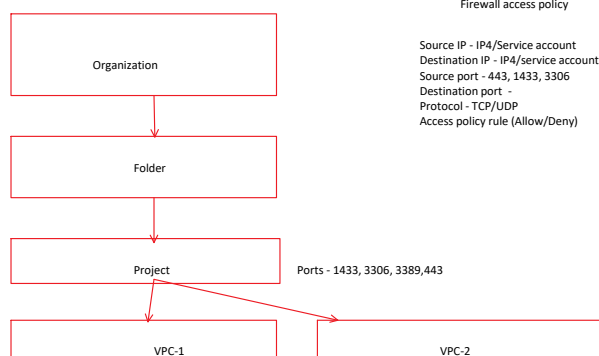"<project-number-compute@developer.gserviceaccount.com"

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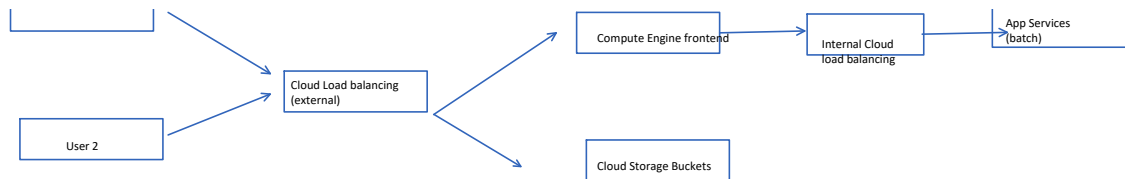
This scenario can fulfill the utility of google-managed service account.

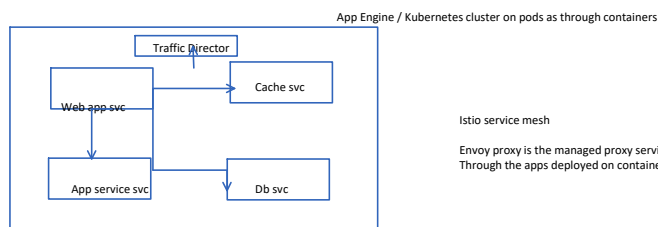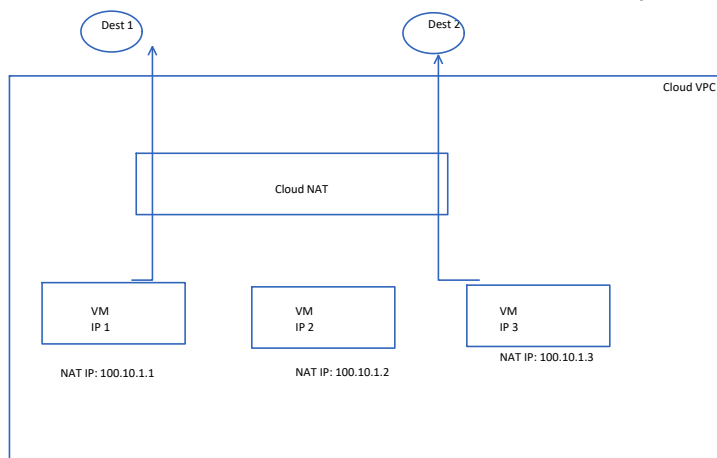e.g. google apis service agent . It's automatically granted the editor role on the project.

VPC
10.0.0.0/8

User 2 → Cloud Load balancing (external)

Cloud Load balancing (external) → Compute Engine frontend → Internal Cloud load balancing → App Services (batch)

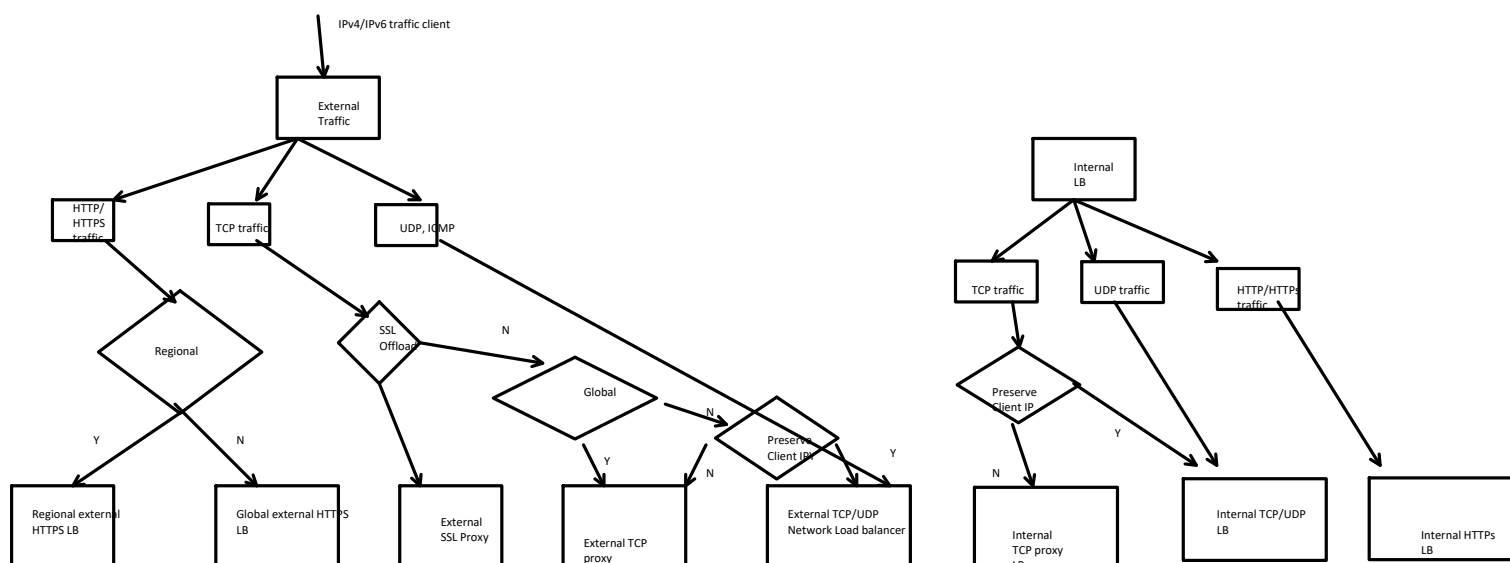Cloud Load balancing (external) → Cloud Storage Buckets

- 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

Dest 1   Dest 2

Cloud VPC

Cloud NAT

VM IP 1

VM IP 2

VM IP 3

NAT IP: 100.10.1.1

NAT IP: 100.10.1.2

NAT IP: 100.10.1.3

App Engine / Kubernetes cluster on pods as through containers

Traffic Director

Cache svc

Web app svc

App service svc

Db svc

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.

IPv4/IPv6 traffic client

External Traffic

HTTP/HTTPS traffic

TCP traffic

UDP, ICMP

Regional

SSL Offload

Global

N

Preserve Client IP

Y   N

Regional external HTTPS LB

Global external HTTPS LB

External SSL Proxy

External TCP proxy

External TCP/UDP Network Load balancer

Y   N

Y   N

Internal LB

TCP traffic

UDP traffic

HTTP/HTTPS traffic

Preserve Client IP

N   Y

Internal TCP proxy LB

Internal TCP/UDP LB

Internal HTTPs LB

Landing Zone

01 April 2023   13:24

Shared VPC

Data Analytics Project

Host Project

Cloud Router

Cloud NAT

Cloud Dataflow

BigQuery

Firewall Rules

App1 service project

Compute Engine 1

Compute Engine 2

Cloud Storage

GKE

On-prem Apps

Cloud Interconnect

AWS/Azure

Cloud VPN

- Identity provisioning
- Resource Hierarchy
- Network
- Security Controls
- Monitoring and logging
- Backup & DR
- Compliance
- Cost efficiency and control
- API management
- Cluster management

Security

Cloud Resource Manager

Org Policy Service

Identity

Cloud Identity

IAM

Cloud DNS (Private DNS)

Monitoring, auditing and troubleshooting

Monitoring

VPC Flow Logs

Cloud Audit Logs

Firewall Rules logging