Data Loss Prevention API

- automatically detect a sensitive data and mask. Los Angeles[LOCATION], HIROKO[PERSON_NAME],

Private Google Access

- VM that only have internal IP addresses (no external IP addresses) can use Private Google Access.
- They can reach the external IP addresses of Google APIs and services.
- VM + internal IP
- No effect public IP
- Private Google Access -> Internal IP -> can access an external Google services
- subnet-a, Private Google Access ON, 10.240.0.2 ---> Can access
- subnet-a, Private Google Access ON, 10.240.0.3 + public IP ---> CAN access
- subnet-b, Private Google Access OFF, 192.168.1.2 ---> CANNOT access
- subnet-b, Private Google Access OFF, 192.168.1.3 + public IP ---> CAN access
- https://cloud.google.com/vpc/docs/private-google-access#example

Cloud VPN

- Virtual Private Network(VPN), Virtual Private Cloud(VPC)
- on-prem + VPC = Cloud VPN
- VPC: two subnets(us-east1, us-west1) => communicate internal IP with routing, Cloud gateway, on-prem gateway, two tunnels
- Cloud VPN = static or dynamic routes=> set up Cloud Router with BGP(border gateway protocol)
- Cloud VPN gateway with dynamic routing ---> HA VPN Border Gateway Protocol (BGP).
- The highest level of availability, use HA VPN whenever possible.

Billing

Role	Description
Billing Account Creator	create a new Cloud Billing Account
Billing Account Creator	Use Billing Account Creator's role for initial billing setup or to allow creation of additional billing accounts.
Project Billing Manager	link/unlink the project to/from a billing.
Project Billing Manager	attach the project to the billing account, but does not grant any rights over resources.
Billing Account User	Create new projects linked to the billing account

Role	Description
Billing Account Administrator	Owner, can link/unlink, but cannot create billing accounts, create alert

- A billing account is assosicated with org.
- Billing alert - Avoid surprises on your bill, who -> Billing Account Administrator, Billing Account Costs Manager
- Moving a project from one organization resource to another won't impact billing, and charges will continue against the old billing account. []
- Billing data -> export BQ -> visualize = Data Studio
- Q: You need to create a new billing account and then link it with an existing Google Cloud Platform project. What should you do?
- A: Billing Account Admin can NOT create a billing account,link/unlink is Project Billing Manager

links:

1. Overview of Cloud Billing roles in IAM
2. Create a budget
3. Change the billing account for a project

microservices

- microservices, automation

Machine Family

- M1 machine type: "M" Memory-optimized - M, Compute-optimized - C, cost-optimized: E, Balanced price/performance: N
- Local SSD - When you stop a VM, all data on the local SSD is discarded.
- Unlike Persistent Disks, Local SSDs are physically attached to the server on VM.

Cloud SQL

- Backup(Data Protection) 1)automate backup is everyday setup only. 2) point-in-time(on-demand)
- Transactional and a single physical location = Cloud SQL.
- Region: us-central1, Single zone - in case of outage, no failover no recommended.
- Region: us-central1, dMultiple zones Automatic failover to another zone - recommended.

Spanner

- Spanner, CPU utilization, Cloud Monitoring, scaling
- Spanner is used for global scaling.
- primary key -> automatically created
- Secondary Index -> it more efficient to look up

- CREATE INDEX SongsBySongName ON Songs(SongName)

VM

- SSH connection/VM: **enable-osLogin=true** with roles/compute.osLogin or roles/compute.osAdminLogin.
- https://medium.com/infrastructure-adventures/centralized-ssh-login-to-google-compute-engine-instances-d00f8654f379
- RDP: Windows login, reset password, download RDP client
- Network tags: it makes FW enable in a vm.
- batch job, preemptible vm
- (maintenance)Maintenance occurs - On host maintenance=Migrate VM instance, Automatic restart=ON
- (maintenance) Live Migration - The reason A is not correct is because live migration simply moves an existing VM between hosts, no attributes or properties are changed otherwise. Hence, you cannot live migrate from 1 VM type to another.
- Stop VM when increasing the memeory 4GB -> 8GB
- disk - persistant disc Local SSD
- MIGs - port 4443 HTTPS
- MIGs - autoscaling- CPU, max/min,
- Authentication - best practice
- each VM that needs to call a Google API should run as a service account with the minimum permissions necessary.(Create new SA)
- how to login using Cloud Identity Proxy for VM Access a paticular instance
- "without allowing other instances" , the other instances are created with default compute engine service account. So you must create a new independant service account
- Q: multiple VMs without public IP, you want to access all VMs without having to configure specific access on the existing and new instances-->
- A: You can connect to Linux instances that don't have an external IP address by tunneling SSH traffic through IAP.[1]

1. Tunneling SSH connections

MIGs

- gradually deploy - maxUnavailable(How many instanes can be offline), maxSurge(How many extra instances to temporarily create)
- gcloud compute instance-groups managed rolling-action start-update INSTANCE_GROUP_NAME --version=template=INSTANCE_TEMPLATE_NAME
- Autoscaling policies: CPU utilization, Monitoring metrics, Queue-based workload, Load balancing capacity

LB

- HTTP LB --> global, HTTP or Port(80/8080), HTTPs on port 443, URL maps
- SSL Proxy LB --> global, encrypted, non-HTTP(s) traffic, TCP with SSL offload.
- TCP proxy LB --> glocal, unencrypted, non-HTTP traffic, TCP.
- Network LB --> regional, non-proxied LB, Traffic: UDP, TCP/UDP ports.
- Internal TCP/UDP --> regional, private LB, VM in same region, TCP/UDP traffic

> Q61:You have an instance group that you want to load balance. You want the load balancer to terminate the client SSL session. The instance group is used to serve a public web application over HTTPS.

- A: Configure an HTTP(S) load balancer -> global, HTTP or Port(80, 8080), HTTPs port 443, URL map**
- B: Configure an internal TCP load balancer. -> regional, private LB, TCP/UDP
- C: Configure an external SSL proxy load balancer.-> global, encrypted, non-HTTP(s)
- D: Configure an external TCP proxy load balancer. ->global, unencrypted, non-HTTP traffi

> Q148: You have an application that receives SSL-encrypted TCP traffic on port 443. Clients for this application are located all over the world. You want to minimize latency for the clients. Which load balancing option should you use?

- A: HTTPS Load Balancer -> global, HTTP or port - 80, 8080, HTTPS on 443, url map
- B: Network Load Balancer ->regional, non-proxied LB, UDP, TCP/SSL ports
- C: SSL Proxy Load Balancer --> global, encrypted, non-HTTP(s), TCP.**
- D: Internal TCP/UDP Load Balancer. -> regional, private LB, VM in same region, TCP/UDP traffic

> Q188: Your company developed a mobile game that is deployed on Google Cloud. Gamers are connecting to the game with their personal phones over the Internet. The game sends UDP packets to update the servers about the gamers actions while they are playing in multiplayer mode. Your game backend can scale over multiple virtual machines (VMs), and you want to expose the VMs over a single IP address. What should you do?

- A: Configure an SSL Proxy load balancer in front of the application servers.-> global, encrypted, non-HTTP(s)
- B: Configure an Internal UDP load balancer in front of the application servers.-> regional, private LB, VM in same region. TCP/UDP
- C: Configure an External HTTP(s) load balancer in front of the application servers.-> global, HTTP 80/8080, HTTPS 443, URL map
- D: Configure an External Network load balancer in front of the application servers. -> UDP, TCP/UDP ports,**

FW

- Request -> egress, Response -> ingress.
- egress is leaving

Cloud Storage

- Storage Admin
- Bucket public -> a signed URL
- failover
- save sensitive data
- lifecycle
- enable them to write data into a particular Cloud Storage bucket --> Storage Object Creator

Role	Description
Storage Object Creator	Allows users to create objects. Does not give permission to view, delete, or replace objects.
Storage Object Viewer	view objects
Storage Object Admin	Grants full control over objects
Storage Admin	Grants full control of buckets and objects.

- IAM roles for Cloud Storage

Audit log

Role	Audit Log Name
Logging.viewer	Admin Activity
Logging.viewer	Policy Denied
Logging.viewer	System Event
Logging.privateLogViewer	Data Access

- Has all permissions of Logging.privateLogViewer
- Data access audit log - disable as a default
- Audit Logs: Querying Logs, Pricing and Retention

```
For Admin Activity audit logs, select activity.
For Data Access audit logs, select data_access.
```

```
For System Event audit logs, select system_event.
For Policy Denied audit logs, select policy.
```

- Q: You are storing sensitive information in a Cloud Storage bucket. For legal reasons, you need to be able to record all requests that read any of the stored data. You want to make sure you comply with these requirements. What should you do?
- A: Enable Data Access audit logs for the Cloud Storage API.

IAM

- 4 Members: Google Account, SA, Google Group, Google Workspace /Cloud Identity

Member	Email
Google Account	userid@gmail.com
SA	12345678@cloudservices.gserviceaccount.com
Google Group	groupname@googlegroups.com
Google Workspace /Cloud Identity	test@example.com

- Cloud Identity - verify thrid party authentication
- G Suite = Google Workspace
- use predefined roles and create groups to control access to multiple users

SA

- To use a service account outside of Google Cloud, such as on other platforms or on-premises, you must first establish the identity of the service account. Public/private key pairs provide a secure way of accomplishing this goal.
- https://cloud.google.com/iam/docs/creating-managing-service-account-keys#iam-service-account-keys-create-rest

IAP(Identity-Aware Proxy)

- Identity Aware Proxy API(IAP)- https://cloud.google.com/iap/docs/external-identities
- Proxy(=dairi)
- external identities with Identity-Aware Proxy (IAP) instead of Google accounts.
- external identity: email/password, OAuth (Google, Facebook, Twitter, GitHub, Microsoft, etc.
- This is useful if your application is already using an external authentication system,
- IAP controls access to App Engine apps and VMs

- Q: Your company runs its Linux workloads on Compute Engine instances. Your company will be working with a new operations partner that does not use Google Accounts. You need to grant access to the instances to your operations partner so they can maintain the installed tooling.
- A:Enable Cloud IAP for the Compute Engine instances, and add the operations partner as a Cloud IAP Tunnel User.

1. Youtube - #GCP #IAP
2. https://cloud.google.com/architecture/identity/migrating-consumer-accounts

VPC

- auto or custom mode
- auto mode - one subnet from each region is automatically created within it.
- custom mode: you have to create a subnet
- VPC and the 2 subnets -> custom

BigQuery

- dry-run select * from coffee.coffee_dataset -->304538 bytes of data
- External table (source: Cloud Storage)
- BigQuery Job User((roles/bigquery.jobUser)) - can run query[1]

1. https://cloud.google.com/bigquery/docs/access-control#bigquery.jobUser

App Engine

- You specify the scaling type in your app's app.yaml.
- app.yaml: runtime, URL, scaling
- gradually deploy - a rolling-action start-update with maxSurge
- --split
- version in a same project

Deployment Manager

- gcloud deployment-manager deployments update my-deployment --config=new_config.yaml
- gcloud deployment-manager deployments update example-deployment
  --config configuration-file.yaml
  --preview
- **--preview**:Preview the requested create without actually instantiating the underlying resources. (default=False)
- A type provider exposes all of the resources of a third-party API to Deployment Manager as base types that you can use in your configurations. These types must be directly served by a **RESTful API** that supports Create, Read, Update, and Delete (CRUD).

Stackdriver

- different projects, monitor a single report

BigTable

- time series database

App Engine

- Important: Each Cloud project can contain only a single App Engine application, and once created you cannot change the location of your App Engine application.[1]

1. https://cloud.google.com/appengine/docs/flexible/managing-projects-apps-billing#create

Pub/Sub

- Q: You have created a **code snippet** that should be triggered **whenever a new file** is uploaded to a Cloud Storage bucket. You want to deploy this code snippet. What should you do?

Cross projects

- Q: You manage an App Engine Service that aggregates and visualizes data from BigQuery. The application is deployed with the default App Engine Service account. The data that needs to be visualized resides in a different project managed by another team. You do not have access to this project, but you want your application to be able to read data from the BigQuery dataset. What should you do?
- A: Ask the other team to grant your default App Engine Service account the role of BigQuery Data Viewer.

gcloud commands

- (Subnet) gcloud compute networks subnets expand-ip-range SUBNET --region=us-central1 --prefix-length=16
- (GKE) gcloud container node-pools create node-pool-1 --cluster=example-cluster --preemptible
- (VM) gcloud compute instances create [INSTANCE_NAME] --deletion-protection
- (Config) gcloud config configurations create my-config
- (Config) gcloud config set compute/region us-west4
- (Config) gcloud config set compute/zone us-west4-b
- gcloud compute regions list
- gcloud compute zones list
- gcloud config unset compute/zone
- gcloud config unset compute/region

- (Config) gcloud config list -> view project id
- (IAM) gcloud projects get-iam-policy react-app-demo
- (IAM) gcloud iam roles copy --source="roles/spanner.databaseAdmin" --destination=CustomSpannerDbAdmin --dest-project=PROJECT_ID
- (IAM) gcloud iam roles describe roles/spanner.databaseUser
- (IAM) gcloud iam roles list
- (IAM) gcloud iam service-accounts list
- (Cloud Function) gcloud functions deploy Hello --http-trigger
- (Cloud Function) gcloud functions deploy Hello --trigger-topic=mytopic

GKE

- Cluster -> Nodes(VM) -> Pod(container), Pod(container), Pod(container) [1]
- a cluster consists of at least one control plane and multiple worker machines called nodes.[1]
- Cluster type: Autopilot and Standard
- To deploy your app to the GKE cluster you created, you need two Kubernetes objects.[3]

Kubernetes objects	Description
Deployment	to define your app.
Service	to define how to access your app

- A deployment is responsible for keeping a set of pods running.[4]
- A service is responsible for enabling network access to a set of pods.[4]
- ClusterIP < NP < LB
- replicas

DaemonSets

- A DaemonSet ensures that all (or some) Nodes run a copy of a Pod.
- "Every Node" is the keyword here, which is what DaemonSet is used for
- DaemonSets attempt to adhere to a one-Pod-per-node model
- B is right: https://kubernetes.io/docs/concepts/workloads/controllers/daemonset/ Some typical uses of a DaemonSet are:
- running a cluster storage daemon on every node
- running a logs collection daemon on every node
- running a node monitoring daemon on every node

Reasons for a Pod Status Pending:[7]

- Troubleshooting Reason #1: Not enough CPU
- Troubleshooting Reason #2: Not enough memory
- Troubleshooting Reason #3: Not enough CPU and memory

```
kubectl get pods
$ kubectl get pods
NAME                                                    READY   STATUS
```

```
RESTARTS   AGE
echoserver-657f6fb8f5-wmgj5        0/1     Pending            0
1d
```

```
kubectl describe pod echoserver-657f6fb8f5-wmgj5
kubectl get nodes
kubectl describe node gke-gar-3-pool-1-9781becc-bdb3
```

GKE Sandbox

- GKE Sandbox on your cluster to isolate untrusted workloads in sandboxes on the node. GKE Sandbox is built using gVisor, an open source project.[8]
- click Security and select the Enable sandbox with gVisor checkbox.

Commands

- kubectl create deployment hello-server --image=us-docker.pkg.dev/google-samples/containers/gke/hello-app:1.0
- gcloud container clusters create-auto hello-cluster --region=us-central1
- kubectl config use-context black
- kubectl config view
- gcloud container clusters describe CLUSTER_NAME
- gcloud container clusters list
- gcloud config set container/cluster CLUSTER_NAME

GKE Links:

1. Standard cluster architecture
2. Quickstart-1
3. Quickstart-2
4. Kubernetes Service vs Deployment
5. Commands for Cluster
6. ClusterIP-NodePort-LB
7. https://managedkube.com/kubernetes/k8sbot/troubleshooting/pending/pod/2019/02/22/pending-pod.html
8. https://cloud.google.com/kubernetes-engine/docs/how-to/sandbox-pods?hl=en