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 projects under an organisation doesn't change their linked billing project.
- Billing data -> export BQ -> visualize = Data Studio
- https://cloud.google.com/billing/docs/how-to/billing-access
- https://cloud.google.com/billing/docs/how-to/budgets
- 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

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.

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 occurs - On host maintenance=Migrate VM instance, Automatic restart=ON
- 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

FW

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

Cloud Storage

- Storage Admin
- Bucket public -> a signed URL
- failover
- save sensitive data
- lifecycle

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

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

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,
- your applications and VMs
- IAP controls access to App Engine apps and VMs
- 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 jobUser - query

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)

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

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
```

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

Stackdriver

- different projects, monitor a single report

BigTable

- time series database

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

LB/MIGs

- HTTP(s), SSL, TCP, Network TCP/UDP, Internal TCP/UDP, Internal HTTP(s)
- httpST, N, IH
- Traffic type: HTTP(s), TCP, UDP
- TCP, port 443, SSL offload -> SSL proxy
- SSL Proxy LB == non-HTTP(S) traffic.
- IPv6 - httpST(HTTP, SSL proxy, TCP proxy)
- Autoscaling policies: CPU utilization, Monitoring metrics, Queue-based workload, Load balancing capacity

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