GCP Services

Organising GCP Resources
- Resource Hirearchy
  - Domain (cloud level)
    - Organisation
      - Billing Account
      - Folders
        - Projects
          - Resources
  - Payments Profile
- Billing Accounts
  - Managing Budget, Alerts and Exports
- Corporte Directory Federation
- Organisation Policy Service
- Resource Hirearchy and IAM policy

Hybrid Cloud
- Cloud VPN
  - HA VPN
  - Classic VPN
- Cloud Interconnect
  - Dedicated Interconnect
  - Partner Interconnect
- Direct Peering (**NOT RECOMMENDED**)

Managed Services
- IAAS
  - Server
    - Compute Engine
- PAAS
  - Server
    - App Engine
- CAAS
  - Server
    - GKE
  - Serverless
    - App Engine Flexible
    - Cloud Run
- FAAS
  - Serverless
    - Cloud Functions

Discounts
- Sustained
- Committed

Cloud DataProc
- managed **Spark and Hadoop service**
- **data analysis platform**
- alternative: **BigQuery**

Cloud DataFlow
- **pipelines**
- **streaming** & batch use cases
- **serverless**
- **auto scaling**

Cloud DNS
- **global DNS**
- set up your DNS routing of your website

Market Place / Cloud Launcher
- Central repo of easily deployable apps and datasets

Deployment Manager
- **automate provisions of your infra**
- version control for your envs

Pricing Calculator
- estimate the cost of your gcp solution

Gcloud Operations Suite / Stackdriver
- Cloud Logging
  - Audit & Security logs
    - Cloud Audit Logs
      - Access Transparency logs
      - Admin activity logs
      - Data access logs
      - System event audit logs
      - Policy denied audit logs
  - Collection
  - Controlling & Routing
    - Types of log buckets
      - _Required
      - Default
  - **Export -** (create sinks)
    - **Use cases:**
      - Troubleshoot using VM logs
      - Export VM logs to BigQuery for querying using SQL like queries
      - You want to retain audit logs for external auditors at minimum
- Cloud Trace
- Cloud Monitoring
  - Workspace
  - Virtual Machines
- Cloud Debugger
- Cloud Profiler
- Error Reporting

VPC
- VPC Subnets
- Types
  - Auto mode VPC n/w
  - Custom mode VPC n/w (**Recommended for PROD**)
- CIDR
- Firewall Rules
  - Ingress
  - Egress
- Shared VPC
- VPC Peering

Databases
- Relational
  - OLAP - Analytics
    - **BigQuery (bq) - GLOBAL**
      - data warehouse
      - automatically expire data
      - expensive
  - OLTP - Transactional
    - **Cloud SQL - REGIONAL**
    - **Cloud Spanner - GLOBAL**
    - **Cloud SQL:**
      - **Point in time recovery: binary logging**
      - Export data from console UI
      - **High availabilty and failover:**
        - Standby with automatic failover.
        - Pre reqs: automated backup , **binary-logging**
      - **High availabilty** setup **CANNOT** be used as **Read Replica**

      Cloud Spanner:
      - **Expensive**
      - Data Export: use cloud console, **DataFlow** to automate export. **No gcloud export option**
      -
  - Import and Export
- Not Serverless
- Non relational
  - **DataStore/FireStore - REGIONAL**
  - **Cloud BigTable (cbt) - GLOBAL**
    - **DataStore/FireStore:**
      - NoSQL doc DB with SQL like queries
      - Export Data data only from gcloud (**NOT from cloud console**)

      Cloud BigTable:
      - **cbt command line tool**
      - **CANNOT export data using cloud console or gcloud**
        - either use a java application or use **HBASE commands**
      - **wide column DB**
      - **IOT Streams, graph data, real-time analytics**
  - **Memory Store**
  - Import and Export

Summary:
- BigQuery, Datastore, firebase doesnt need a VM config, where as **CloudSQL, BigTable need VM Config** (they use compute Engine VMs)
- **Relational DB:**
  - Small Local DB - Cloud SQL
  - Highly scalable global DB - Cloud Spanner
  - Datawarehouse - BigQuery)
- **NoSQL DB:**
  - Transactional DB for few TBs of data - Cloud DataStore
  - Huge Volumes of IOT or stream analytics data - BigTable

IAM
- Roles
  - Basic
    - Viewer
    - Editor
    - Owner
  - Predefined Roles (Recommended)
  - Custom Roles
- Policy
- Service Accounts (Recommended)
  - Default
  - **User Managed (Recommended)**
  - Google managed Service accounts
  - Use cases
    - VM to Cloud Storage
    - On Prem to Cloud Storage (long lived)
    - On Prem to Gcloud APIs(short lived)
- Access Control Lists
  - Uniform
  - Fine grained
- Best Practices
  - **Principle of Least Privilege**
  - **Seperation of duties**
  - **Constant Monitoring**
  - **Use Groups when Possible**

Remember:
- Roles: set of permissions
- Policy: assign permissions to members (assign role to a member)
- Don't use basic roles in prod
- **Service accounts:**
  - Default service account has Editor role by default (**Not recommended**)
- **ACL:**
  - **IAM** for common permissions to all objects in the bucket
  - **ACL** custom access to individual objects
  - use **Uniform** access when all users have same level of access across all objects in a bucket
- **Cloud Storage - SignedURL**
  - Allow user a limited access time
- **Cloud Storage - Static Website**
  - bucket name same as website name
  - add **allUsers** and grant **Storage Object Viewer**
  - **allow public access**

Compute Engine
- Image & Machine Types
  - **Custom Image**
    - Hardened Images
  - **Machine Image**
    - disk backups, instance cloning, replication
- IP Address
  - **Static IP address**
- **Instance Templates**
- **Instance Groups**
  - **Managed Instance Group**
    - **Releases**
      - Rolling updates
      - Canary Deployments
  - Unmanaged (Not recommended)
- **Virtual Machines / Instances**
  - Temporary VMs
    - Preemptible VM
    - Spot VM

MIG Features:
- Auto Healing
- Auto Scaling
- Load Balancer to distribute load

Remember:
- Live Migration
- Availability Policy
  - On host maintance - Migrate and Terminate
  - Automatic Restart
- You will be billed if the storage is attached even if compute engine instance is turned off
- IAAS

Kubernetes Engine
- **Kubernetes**
  - Deployment
  - **Service**
    - **ClusterIP**
    - Load Balancer
    - **NodePort**
  - **Pods**
    - **Pod Status**
      - **Pending**/Running/Succeeded/Failed/Unknown/**Waiting**
        - Ephemeral IP
        - One or more containers
        - N/w, storage, IP address, Ports, Vols (are shared b/w pods)
  - Replica Set
  - **Secrets**
  - Config Map
- **Cluster**
  - Master Node (Control Plane)
    - API Server
    - **Scheduler**
    - Control Manager
    - etcd
  - Worker Nodes
    - kubelet
  - **Types of Clusters**
    - Zonal
    - Regional
    - Private
    - Alpha
  - Node pools
    - nodeSelector
  - deployment.yaml
  - **Clusters**
    - **Standard**
    - **AutoPilot**
- **Container Registry (gcr)**

Remember:
- Replicate master nodes across zones - HA
- Supports **Stateful** deployments
  - **StatefulSet**
- **DaemonSet -** background job - logs, metrics
- **GKE cluster management** : '**gcloud container clusters**'
- **GKE workload management:** '**kubectl**'
- **Features - K8s:**
  - Auto Scaling
  - Service Discovery
  - Load Balancer
  - Self Healing
  - 0 downtime deployments
  - **HPA**
  - **VPA**

App Engine - REGIONAL
- Environments
  - **Standard**
    - Go for standard if you want to scale down to 0
  - **Flexible**
- Application Component Hirearchy
  - **Application - One Per Project**
  - Services(s) - Multiple micro services
  - Versions - associated with config and code
- Scaling Instances
  - Automatic - auto scale based on load
  - Basic - adhoc workloads
  - Manual
- Request Routing
  - With URLs
  - dispatch.yaml
  - Cloud load balancing
- **Traffic Splitting**
  - IP Splitting
  - Cookie Splitting
  - Random
- Cron Job - cron.yaml
- queue.yaml

Remember:
- Automatic Load balancing & Auto Scaling
- Manages Platform Updates & Application
- Health Monitoring
- Application Versioning
- Traffic Splitting
- App Engine Flexible can be CAAS but is expensive compared to Cloud Run.
- **One app per project**
- PAAS

Load Balancing
- SSL/TLS Termination/ Offloading
- **External**
  - **HTTP/HTTPS Traffic**
    - External HTTP(S) Loadbalancer (Global)
    - Regional External loadbalancer
  - **TCP Traffic**
    - **TCP Proxy (Global)**
    - **SSL Offload ?**
      - **SSL Proxy**
  - UDP Traffic
  - ESP/ICMP traffic
  - → **External N/w loadbalancing**
- **Internal**
  - TCP Traffic
    - Internal TCP/UDP Loadbalancing
  - UDP Traffic
  - HTPP/HTTPS
    - Internal HTTP(S) loadbalancing

Cloud Functions
- gen1
- gen2
  - Concurrency
  - Longer req timeout
  - Multiple fn revisions
  - Traffic splitting
  - EventArc
  - Larger Instance sizes

Remember:
- Serverless
- Pay only for what you use
- Horizontally Scaled
- Responds to Events
- Auto Scaling
- '**gcloud functions**'

Cloud Run
- Anthos

Remember:
- Serverless
- Pay per use
- Anthos - Run k8s clusters anywhere

KMS
- Google managed key
- Customer managed key
- Customer supplied key

Storage
- **Block Storage**
  - **Persistent disks - N/w Storage**
    - Standard
    - Balanced
    - SSD
    - **Snapshots - incremental**
      - incremental
      - snapshot from disk > snapshot from image
      - disk from image > disk from snapshot
      - snapshot scheduling
    - Options
      - Regional
      - Zonal
  - **Local SSDs - Physically attached - Ephemeral storage**
- **File Storage**
  - **FileStore**
    - high performance
    - fileshare, media workflows, content management
- **Object Storage**
  - **Cloud Storage - gsutil**
    - **Storage Classes**
      - Standard
      - Nearline
      - Coldline
      - Archive
    - Uploading and downloading objects
    - **Object Versioning**
    - **Object Lifecycle management**
      - Actions
        - setStorageClass
        - Deletion
    - Encryption
      - Server side
        - Google managed encryption key
        - Customer managed encryption key
      - Client side (optional)
    - **Signed URL**
    - **Static Website**

Remember:
- **key-value**
- objects are stored in buckets
- **supports all file types**
- partial update on objects is not allowed
- **bucket names are globally unique**
- **Object versioning prevents accidental deletion &** provides history
- **Object life cycle management:**
  - **change from one storage class to another**

Pub/Sub
- Use cases
  - **Event Ingestion**
  - **Delivery of streaming analytics pipelines**

Created by: Savitha Gollamudi

Presented with xmind