GCP ACE:
Prep for ACE Journey Q2 2023
Ivan Vlad S.

1 Environment Setup

Overview

- Establish resource hierarchy
  > Organization level
  > Folder level
  > Project level
- Identify identity and access roles
  > Who --- Data analyst
  > Can do what --- view data and run queries
  > on which resource --- BigQuery datasets
- Operations Suite
  > Cloud monitoring and metrics
  > Scoping project - monitor metrics for multiple projects
  > Monitored projects
- Interacting with GCP
  > Console - web user interface
  > SDK and Cloud Shell - CLI
  > Mobile app - for iOS and Android
  > REST-based API - for custom apps
- Outcomes of this phase of the migration journey
  > Establishing resource hierarchy
  > Implementing org policies
  ★ > Aanaging projects and quotas
  > Aanaging users and groups
  > Applying access management
  > Setup billing and monitoring

Diagnostic Qs

- Best practice to manage role assignment by groups, not by individual users
- Billing acc can handle billing for more than 1 project
  A project and its resources can only be tied to 1 billing acc
- Can set up to 5 Cloud Monitoring channels to define email recipients that will receive budget alerts

- GCP resource hierarchy = ORG > Folder > Proj > Res
- Use gsutil to interact with Cloud Storage via SDK in Cloud Shell
- Basic roles are broad and don't use least priv, grant only the roles that someone needs through predefined and custom roles
- Editor = lowest level basic role that gives permissions to change resource state

2 Planning and Configuring a cloud solution

- Selecting Resources
  - > Planning and estimating pricing using Public Calculator
    > Planning and config for compute resources
    > Planning and config for data storage options
    > Planning and config for network resources
  - Gather/obtain customer app requirements and map to appropriate GCP service(s)
    > technical reqs: compute, data, network
    > functional reqs: need/ask/purpose of app
- Diagnostic Qs
  - Data storage pricing is based on amount of data and storage type; (min duration)
    > Standard - none
    > Nearline - 30 days
    > Coldline - 90 days
    > Archive - 365 days
  - BigQuery = GCP data warehouse. Analyzes historical data using SQL query engine
  - Cloud Run provides serverless container mgmt; lets you focus on code and you can deploy your solution quickly
  - K8s Engine gives full control of container orchestration and availability
  - HTTP/S = L7 load balancer
    SSL = L4 load balancer
  - Compute Engine gives full control over OS choice and config
  - Compute Engine = great option for quick migration of traditional apps. Can implement a solution in the cloud without changing your existing code

- To populate visual dashboards with historical time-based data, need to use BigQuery (SQL) or Cloud Bigtable (NoSQL)
- Cloud Functions = submit and execute small snippets of code the fire based on system events (like AWS Lambda)

3 Deploying & Implementing a cloud solution

- ★ Understand availability, concurrency, connectivity, and access options for services/solutions being deployed
- Deploy and implement:
  > Compute Engine resources
  > GKE resources
  > Cloud Run and Cloud Functions resources
  > data solutions
  > networking resources
  > using Cloud Marketplace
  > implementing resources using IaC
- Diagnostic Qs
  - BigQuery transfer service is simplest process to set up transfers between Cloud Storage and BigQuery. Only one command and it's free
  - VPC - custom mode network = control over regions you place subnets in and lets you specify IP ranges
  - Terraform Apply = sets up resources specified in config file
  - Instance OS - Proactive mode = institutes rolling update where surge is auto set to 1, minimizes resources
  - Cloud Run = serverless, exposes services as an endpoint, abstracts all infra
  - Cloud SQL: -availability-type : option allows you to specify zonal or regional availability; regional provides auto failover to a standby node in another region
  - Cloud Spanner = GCP globally available, horizontally scalable RDB

4 Ensuring Successful Ops of a Cloud Solution

- ★ Understand how to manage the resources used in an orgs cloud solutions
  - > Compute Engine resources
    > GKE resources
    > Cloud Run resources
    > storage and db solutions
    > network resources
    > monitoring and logging

- Diagnostic Qs
  - Storage:
    > MatchesStorageClass = required to look for objects with a standard storage type
    > CreatedBefore = specify date
  - CloudRun: Max instances controls costs, limits number of connections to a backing services
  - Managed Instance Group config:
    > Health Checks
    > number of instances
  - Understand basic GKE commands and objects
  - Understand basic gsutil commands and options
  - Understand basic gcloud commands for cloudshell and SDK

5 Configuring Access & Security

- Managing Access
  - IAM
  - Service Accounts
    > Create Acc
    > Assign perms
    > Attach to VM
  - Audit logs
- ensure ongoing access and security for cloud solutions
- Diagnostic Qs
  - Data Access logs are disabled by default except for BigQuery
  - Service Accounts = uses account identity and access key, it is used by apps to connect to services
  - Service Account keys used for accessing private data such as Pub/Sub info from external environment, e.g. mobile app