Google Certified

Associate Cloud Engineer

Batch-2011 | Moon International Karachi Pakistan

khawarhere@gmail.com

Lesson Plan

6. IAM: Security

    6.1. What is Security

        6.1.1. AuthN, AuthZ, Accounting

        6.1.2. AAA in GCP

    6.2. IAM Resources

        6.2.1. Project, Folder, Organizations

    6.3. Permissions And Roles

   6.4. Members and Groups

    6.5. Policies

6.1   What is Security

Information security, sometimes shortened to infosec, is the practice of protecting information by mitigating information risks. It is part of information risk management. It typically involves preventing or at least reducing the probability of unauthorized/inappropriate access, use, disclosure, disruption, deletion/destruction, corruption, modification, inspection, recording or devaluation

6.2   IAM Resources

- Resources:
  - Something we create in GCP
- Project:
  - Container for a set of related resources
- Folders
  - Contains any number of Projects and Folders
- Organization
  - Tied to G Suite or Cloud identity

4
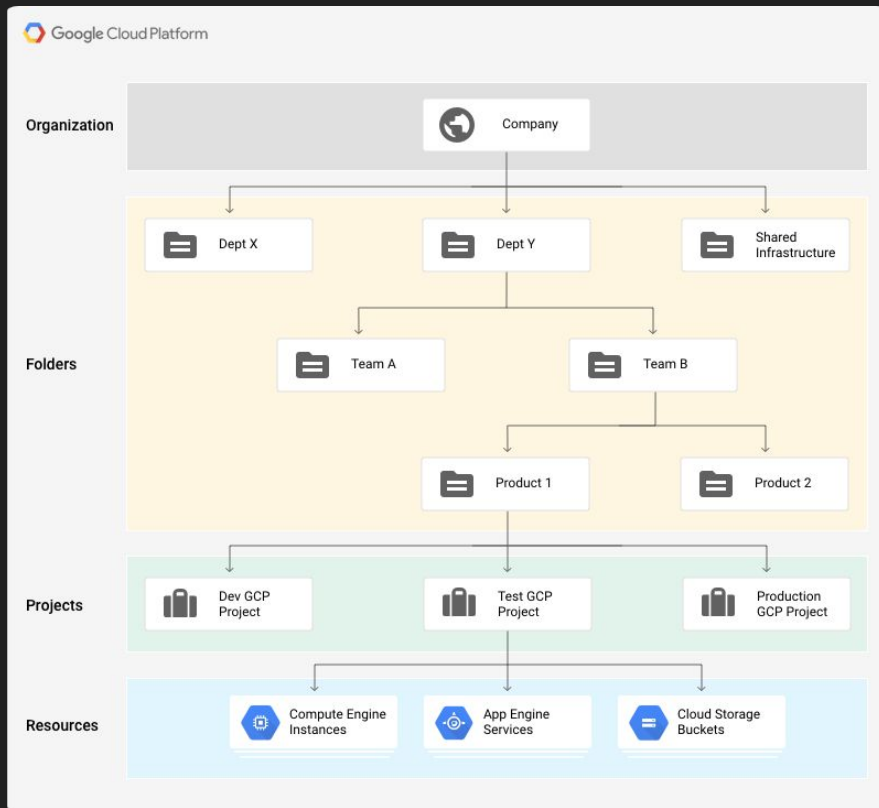
6.3   Permissions

- Permission allow you to perform certain action

- Follows the pattern : Service.Resource.Verb

- Usually corresponds to REST API methods.

- Example:

  - pubsub.subscription.consume

  - pubsub.topics.publish

6.4   Role

- A [Role](#) is a collection of Permissions to use or manage GCP resources
  - **Primitive roles**: Which include the Owner, Editor, and Viewer roles that existed prior to the introduction of Cloud IAM
  - **Predefined roles**: which provide granular access for a specific service and are managed by GCP
  - **Custom roles**: which provide granular access according to a user-specified list of permissions.

6.5　　Members and Groups

- Member: A member can be a Google Account.

- Member can be:

  - user: Specific Google account

  - serviceAccount: Service account for apps and services

  - group: Google group of users and service accounts.

  - domain: Whole domain managed by G Suit or cloud identity.

  - allAuthenticatedUsers: Any Google account or service account

  - allUsers: Anyone on the internet (public)

- Group: Named collection of Google accounts and service accounts.

6.6   Policies

- Policies: Binds Members to Roles for some scope of resources.
    - Who can do what to which things.
    - Attached to some level in the Resource Hierarchy
- Usually take 60s to apply changes.

```
# gcloud projects add-iam-policy-binding PROJECT_ID
--member=MEMBER --role=ROLE [GCLOUD_WIDE_FLAG …]
```

```
# gcloud beta compute instances add-iam-policy-binding myvm2 --member
user:me@example.com
```