Google Cloud Platform Identity and Access Management

Learning Objectives

- Overview of identity and access management
- Key components of IAM
- Members
- Permissions
- Roles

Demo: Exploring Members, Roles, and Permissions

- Service Accounts

Demo: Exploring Service Accounts

- Where do you use IAM?

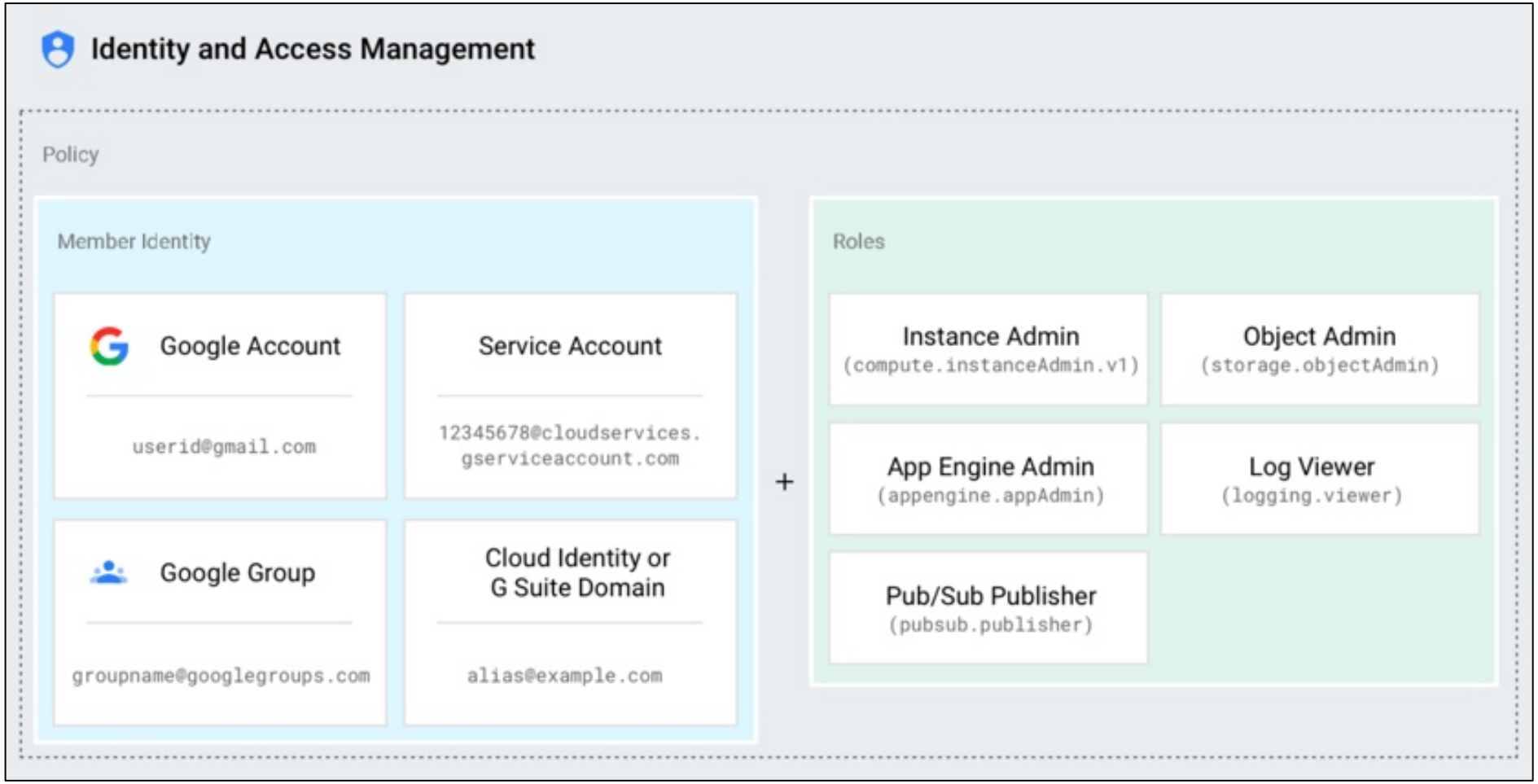
Overview of Cloud IAM

Overview of Cloud IAM

- IAM controls access by defining **who** (identity) has **what** access (role) for **which** resource

- Cloud IAM is based on the principle of least privilege
- An IAM policy binds identity to roles which contains permissions

Google Cloud IAM



Cloud IAM Identity

Cloud IAM Users/Members

- Google account
- Service account
- Google group
- G Suite domain
- Cloud Identity domain
- *allAuthenticatedUsers*
- *allUsers*

Cloud IAM Permissions

Cloud IAM Permissions

- Permissions determine the operations performed on a resource
- Correspond 1:1 with REST methods of GCP resources
- Each GCP resource exposes REST APIs to perform operations
- Permissions are directly mapped to each REST API
  - *Publisher.Publish() -> pubsub.topics.publish*
- Permissions cannot be assigned directly to members/users
- One or more permissions are assigned to an IAM Role

Cloud IAM Roles

Cloud IAM Roles

- **Primitive roles**
  - Owner
  - Editor
  - Viewer
- **Predefined roles**
  - *roles/pubsub.publisher*
  - *roles/compute.admin*
  - *roles/storage.objectAdmin*
- **Custom roles**
  - Collection of assorted set of permissions
  - Fine-grained access to resources

Cloud IAM – Key Elements

Key Elements of Cloud IAM

- **Resource** – Any GCP resource
  - *Projects*
  - *Cloud Storage Buckets*
  - *Compute Engine Instances*
- **Permissions** - Determines operations allowed on a resource
  - *<service>.<resource>.<verb>*
  - *pubsub.subscriptions.consume*
  - *compute.instances.insert*
- **Roles** – A collection of permissions
  - Compute.instanceAdmin
    - *compute.instances.start*
    - *compute.instances.stop*
    - *compute.instances.delete*
    - *….*
- **Users –** Represents an identity
  - *Google Account*
  - *Google Group*
  - *G Suite Domain*
  - **…**

Google Cloud IAM Service Accounts

Cloud IAM Service Accounts

- A special Google account that belongs to an application or VM
- Service account is identified by its unique email address
- Service accounts are associated with key-pairs used for authentication
- Two types of service accounts
  - User managed
  - Google managed
- Each service account is associated with one or more roles

When to use Cloud IAM?

Where do you use IAM?

- To share GCP resources with fine-grained control
- Selectively allow/deny permissions to individual resources
- Define custom roles that are specific to a team/organization
- Enable authentication of applications through service accounts

Google Cloud Platform Fundamentals

Resources for Google Cloud IAM

Key Links

- Cloud IAM
- Cloud Identity

References

- How IAM Works
- Understanding Roles
- Service Accounts