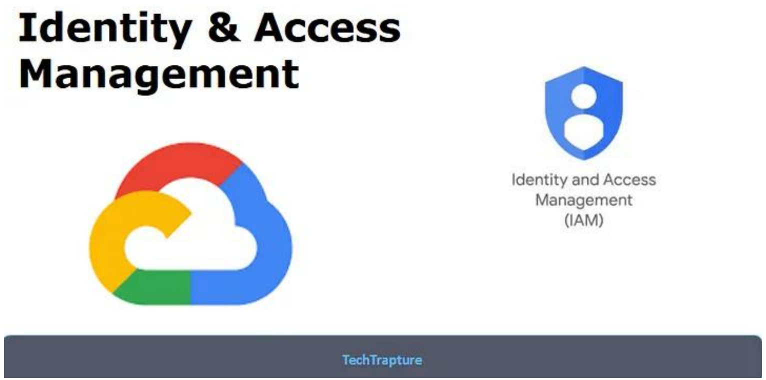
IAM Overview

Manage who can access what in Google Cloud.


Identity & Access Management
Identity and Access Management (IAM)
TechTrapture

IAM Dashboard

Central place to manage identities & roles.

Key Components

- Identity
- Roles
- Permissions

Identity

In Google Cloud IAM, an identity or principal refers to the entity that requires access to resources.

- Google Accounts
- Service accounts
- Google groups
- Google Workspace accounts
- Cloud Identity domains

Roles

A role in Google IAM defines a set of permissions associated with an identity.

- Basic Roles
- Predefined Roles
- Custom Roles

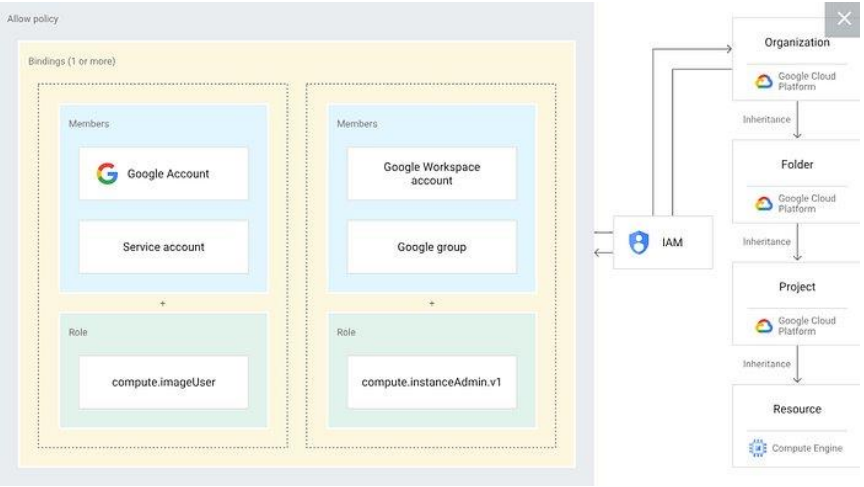
Permissions

Permissions define specific actions that can be performed on resources.

- **storage.objects.create** allows the creation of objects in Cloud Storage.
- **compute.instances.start** allows starting a virtual machine.

How IAM Works

- IAM checks allow policy before access.



Least Privilege

Give only required permissions.

Access Boundaries

Limit identities to specific resources.

PAM

Temporary elevated access for critical tasks.

Best Practices

Use predefined roles, review access, enable MFA.