

ONE PAGE SUMMARY

IT & Software > Google Cloud Platform > Cloud IAM

Introduction to Cloud IAM

Mastering Cloud IAM for Secure Google Cloud Access

DEFINITION

Cloud IAM (Identity and Access Management) is a service that helps manage who can access resources in Google Cloud. It allows you to control permissions and roles for users and services.

KEY CONCEPTS

Roles

Roles define a set of permissions that can be assigned to users or groups.

Policies

Policies are rules that determine who has access to specific resources and what actions they can perform.

Service Accounts

Service accounts are special accounts used by applications or virtual machines to interact with Google Cloud services.

Permissions

Permissions are specific actions that can be performed on resources, such as viewing or editing.

Principals

Principals are the users, groups, or service accounts that are granted access to resources.

EXAMPLES

- Granting a user the 'Viewer' role for a specific project.
- Creating a service account for an application to access Cloud Storage.
- Setting up a policy to restrict access to sensitive data.

MEMORY TIPS

- ★ Remember 'R-P-P-P' for Roles, Policies, Permissions, and Principals.
- ★ Think of IAM as a 'lock and key' system for cloud resources.
- ★ Use 'Service Account = App Identity' to recall service accounts' purpose.

COMMON MISTAKES

- ✗ Assigning overly broad roles that expose sensitive data.
- ✗ Neglecting to review and update permissions regularly.
- ✗ Confusing service accounts with user accounts.

QUICK RECAP

Cloud IAM is essential for managing access to Google Cloud resources. Understanding roles, policies, and permissions is crucial for secure cloud operations.