ONE PAGE SUMMARY

IT & Software › Google Cloud Platform › Cloud IAM

Introduction to Cloud IAM

Master Cloud IAM for secure Google Cloud access management.

DEFINITION

> Cloud IAM (Identity and Access Management) helps you manage who can access your Google Cloud resources and what they can do with them.

KEY CONCEPTS

Roles

Roles define a set of permissions that determine what actions users can perform on resources.

Policies

Policies are rules that grant or restrict access to resources based on roles assigned to users.

Service Accounts

Service accounts are special accounts used by applications to interact with Google Cloud services securely.

Permissions

Permissions are the specific actions that can be performed on resources, such as read or write.

Principals

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

EXAMPLES

→ Assigning a user the 'Viewer' role to access Cloud Storage.

→ Creating a service account for a web application to access BigQuery.

→ Setting a policy that restricts access to sensitive data.

MEMORY TIPS

★ Remember 'R-P-P-S' for Roles, Policies, Permissions, and Service accounts.

★ Think of IAM as a 'lock and key' system for your cloud resources.

★ Use the acronym 'P-R-S' to recall Principals, Roles, and Service accounts.

COMMON MISTAKES

✗ Confusing roles with permissions; roles are collections of permissions.

✗ Neglecting to review IAM policies regularly for security.

✗ Over-assigning permissions, leading to potential security risks.

QUICK RECAP

Cloud IAM is essential for managing access to Google Cloud resources. It involves understanding roles, policies, permissions, and principals to ensure secure and efficient resource management.