

# Identity and Access Management

IAM Resource Hierarchy: Organization => Project => Resources

## Organization Node

- Organization is created by Google Sales.
- Owner is established at creation (G Suite Super Admin).
- It is the root node for Google Cloud Resources.
- 2 organization roles:
  - Organization Admin: control over all cloud resources.
  - Organization Viewer: View access to all resources.
  - Project Creator: controls project creation.

## Cloud Platform Authorization

- Uses Google's credential system:
  - Manage accounts from G Suite (Google-hosted domains) or Google accounts (@gmail).
  - Sync existing credentials using Google Cloud Directory Sync.
  - Optionally implement single sign-on (SSO).
- Features:
  - Session activity tracking.
  - Session management tools.
  - Security alerts.
  - Suspicious activity detection.

## Google Cloud Directory Sync (GCDS)

- Sync GSuite accounts to match the user data in existing LDAP or Active Directory databases:
  - Syncs groups and memberships, not content or settings.
  - Supports sophisticated rules for custom mapping of users, groups, non-employee contacts, user profiles, aliases, and exceptions.
- One-way synchronization from LDAP to directory.
- Runs as a utility in your server environment.

## Single Sign-On (SSO)

- BYO authentication mechanism.
- Federate.
- Revoke access using your existing credential management.
- Google Apps Directory Sync integrates with LDAP.

## Best Practices

- Principle of least privilege.
- Use groups.
- Control who can change policies and group memberships.
- Audit policy changes: Audit logs record project-level permission changes.

## Project Roles

*Note: Add a new user to a Project by clicking on the account picture.*

Groups of permissions.

- Primitive Roles:
  - Owner: All rights including deleting project.
  - Editor: Deploy applications, modify code, configure services, and viewer rights.
  - Viewer: Read-only access.
  - Billing Administrator: Manage billing, add administrators, remove administrators.
- Curated Roles: Custom roles with individual permissions.

## Service Accounts

Allows you to delegate permissions to application to carryout server-to-server interactions.

- Name looks like an email address.
- Three different types:
  - User-created (custom).
  - Built-in (Compute Engine and App Engine default service accounts).
  - Google APIs service account (for Google internal processes).
- Authenticate with keys:
  - Google manages keys for App and Compute Engine.
  - You can manage keys for some resources.
- Can have roles assigned.
- Customizing Scopes for a VM:
  - Allows access to other Google Cloud Platform resources.
  - You can create an instance with customized scopes.
  - For user-created service accounts, use IAM roles instead.