

Day_3

Yogeshwaran. S

Solution:

IAM policy operations:

- **Reading** the existing policy
- **Modifying** the policy
- **Writing** the entire policy

So the default policy will be always empty however when a user creates a new project, the IAM policy for the project automatically has a role binding that grants the Owner role.

Types of roles:

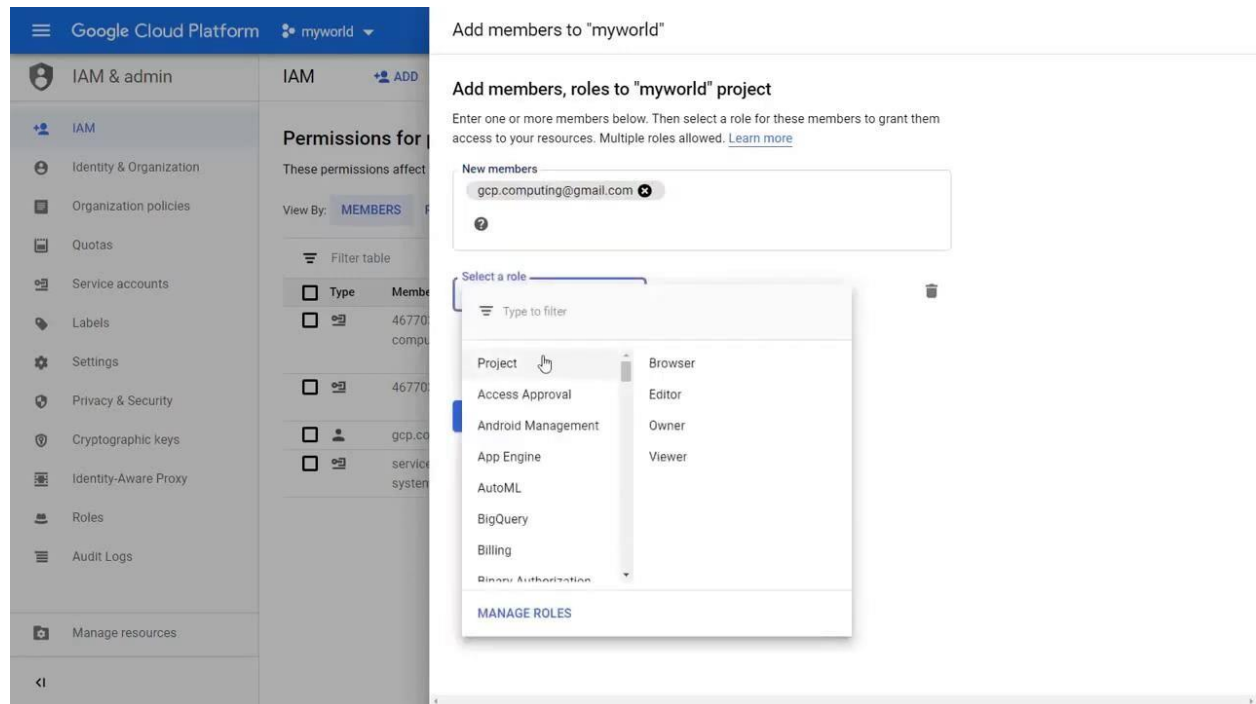
- Primitive Roles – owner, editor, viewer
- Predefined Roles - More granular level access
- Custom Roles – As per user requirement

So Robert has to create a viewer role that only viewing the data(read-only action), and another role is admin role and we can be called as an editor role that contains all viewer permissions and can change the things (modify GCP resources)

Service account:

- One service to connect another without human intervention
- User to authenticate from one service to another

Step 1: Add an admin role



After entering the new member's identification(after completing the process, that member will get a varication mail from GCP then that member will have the assigned role) user can create a new role by searching it from the dropdown menu and also selected the role categories from the browser, editor and owner and viewer

Step 2 : Check the roles assigned

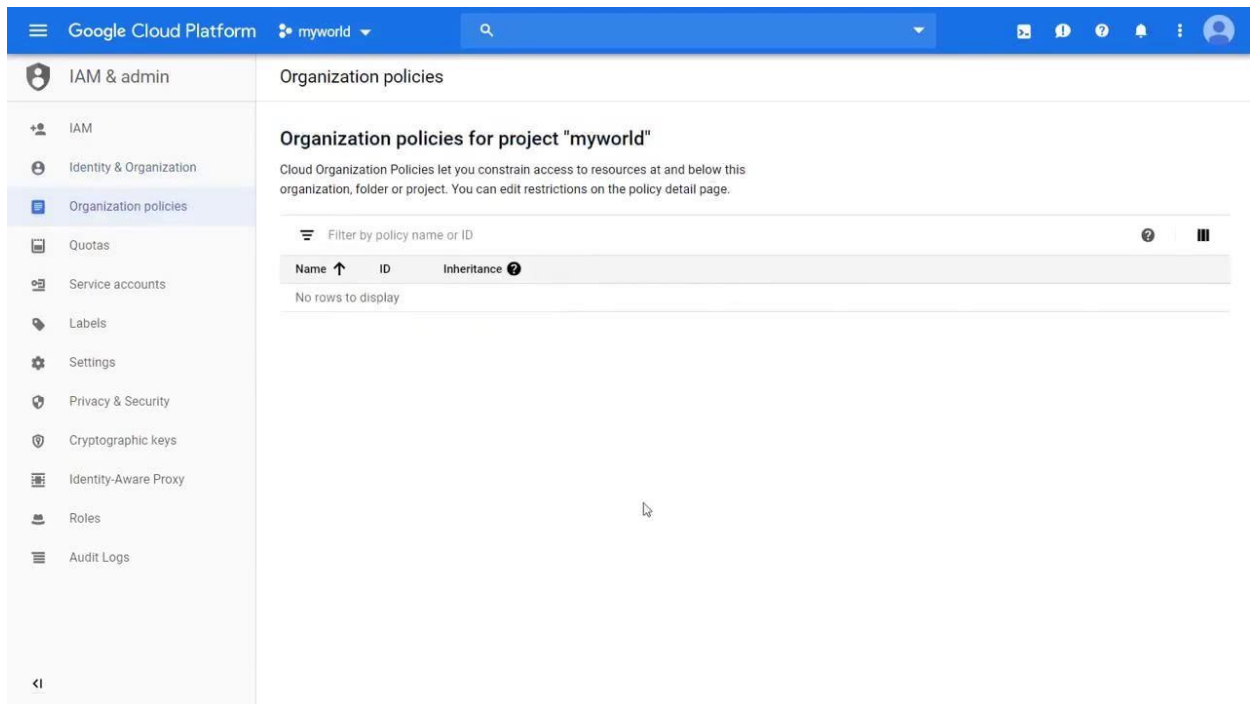
The screenshot shows the Google Cloud Platform interface for the project "myworld". The left sidebar lists various IAM & admin tools, with "IAM" selected. The main content area displays "Permissions for project 'myworld'", explaining that these permissions affect the project and all its resources. Below this, there are tabs for "MEMBERS" and "ROLES". The "MEMBERS" tab is active, showing a table of roles and members. The table has columns for "Role / Member", "Name", and "Inheritance". The members listed are:

Role / Member	Name	Inheritance
Compute Engine Service Agent (1)		
Editor (2)		
Owner (1)		
Storage Admin (1)		

Step 4: create organization level policies

The screenshot shows the Google Cloud Platform interface for the project "myworld", specifically the "Identity & Organization" section. The left sidebar lists various Identity & Organization tools, with "Identity & Organization" selected. The main content area displays "Identity", with sections for "Cloud Identity" and "Admin Console". The "Cloud Identity" section includes a "Sign up" button. The "Admin Console" section includes a "Manage users" button and a "Manage groups" button.

Here user can create an admin level policies if he is handling one or more organization at the one time



here user can see the policies listed here(I tried to create but can't able to understand the complete concept)

Step 5: group permission

Google Cloud Platform

myworld

IAM & admin

IAM

Identity & Organization

Organization policies

Quotas

Service accounts

Labels

Settings

Privacy & Security

Cryptographic keys

Identity-Aware Proxy

Roles

Audit Logs

Manage resources

Roles

+ CREATE ROLE

CREATE ROLE FROM SELECTION

DISABLE

DELETE

SHOW INFO PANEL

Roles for "myworld" project

A role is a group of permissions that you can assign to members. You can create a role and add permissions to it, or copy an existing role and adjust its permissions. [Learn more](#)

Filter table

Type	Title	Used in	Status
<input type="checkbox"/>	Access Approval Approver	Access Approval	Enabled
<input type="checkbox"/>	Access Approval Config Editor	Access Approval	Enabled
<input type="checkbox"/>	Access Approval Viewer	Access Approval	Enabled
<input type="checkbox"/>	Access Context Manager Admin	Other	Enabled
<input type="checkbox"/>	Access Context Manager Editor	Other	Enabled
<input type="checkbox"/>	Access Context Manager Reader	Other	Enabled
<input type="checkbox"/>	Access Transparency Admin	Organization Policy	Enabled
<input type="checkbox"/>	Admin	Cloud Talent Solution	Enabled
<input type="checkbox"/>	Admin of Tenancy Units	Service Consumer Management	Enabled
<input type="checkbox"/>	Android Management User	Android Management	Enabled
<input type="checkbox"/>	API Keys Admin	Service Usage	Enabled
<input type="checkbox"/>	API Keys Viewer	Service Usage	Enabled
<input type="checkbox"/>	App Engine Admin	App Engine	Enabled
<input type="checkbox"/>	App Engine Code Viewer	App Engine	Enabled

In roles column, user can create a new role and

Google Cloud Platform

myworld

IAM & admin

IAM

Identity & Organization

Organization policies

Quotas

Service accounts

Labels

Settings

Privacy & Security

Cryptographic keys

Identity-Aware Proxy

Roles

Audit Logs

Manage resources

← Create

Custom roles organization, role. [Learn more](#)

Title * Custom Role

Description Created on:

ID * CustomRole

Role launch s Alpha

+ ADD PERMISSIONS

No assign

Filter

No rows to

Add permissions

Filter permissions by role

Filter table

Permission ↑	Status
<input type="checkbox"/> accessapproval.requests.approve	Supported
<input type="checkbox"/> accessapproval.requests.dismiss	Supported
<input checked="" type="checkbox"/> accessapproval.requests.get	Supported
<input type="checkbox"/> accessapproval.requests.list	Supported
<input type="checkbox"/> accessapproval.settings.get	Supported
<input type="checkbox"/> accessapproval.settings.update	Supported
<input type="checkbox"/> accesscontextmanager.accessLevels.create	Non-applicable ⚠
<input type="checkbox"/> accesscontextmanager.accessLevels.delete	Non-applicable ⚠
<input type="checkbox"/> accesscontextmanager.accessLevels.get	Non-applicable ⚠
<input type="checkbox"/> accesscontextmanager.accessLevels.list	Non-applicable ⚠

1 - 10 of 2200 < >

CANCEL ADD

Customize and group some role for one user and that user has customized access control