1. Use IAM to do the following tasks:

* Create an owner role and try to launch an instance.
* Change this owner role to editor and try to delete the instance created earlier.
* Using pre-defined roles, try to create a user which can create or delete compute instances. (Do not use owner, editor, or viewer).
* Create a custom role, which can create and edit compute and storage instances.

So IAM stands for Identity and Access Control. Identity and Access Management (IAM) lets administrators authorize who can act on specific resources, giving you full control and visibility to manage Google Cloud resources centrally. For enterprises with complex organizational structures, hundreds of workgroups, and many projects, IAM provides a unified view into security policy across your entire organization, with built-in auditing to ease compliance processes. There are Multiple Feathers of IAM lets go through it quickly:

* Single access control interface: IAM provides a simple and consistent access control interface for all Google Cloud services. Learn one access control interface and apply that knowledge to all Google Cloud resources.
* Fine-grained control: Grant access to users at a resource level of granularity, rather than just project level. For example, you can create an IAM access control policy that grants the Subscriber role to a user for a particular Pub/Subtopic.
* Automated access control recommendations: Remove unwanted access to Google Cloud resources with smart access control recommendations. Using Recommender, you can automatically detect overly permissive access and right size them based on similar users in the organization and their access patterns.
* Context-aware access: Control access to resources based on contextual attributes like device security status, IP address, resource type, and date/time.
* Flexible roles: Prior to IAM, you could only grant Owner, Editor, or Viewer roles to users. A wide range of services and resources now surface additional IAM roles out of the box. For example, the Pub/Sub service exposes Publisher and Subscriber roles in addition to the Owner, Editor, and Viewer roles.
* Web, programmatic, and command-line access: Create and manage IAM policies using the Google Cloud Console, the IAM methods, and the gcloud command line tool.
* Built-in audit trail: To ease compliance processes for your organization, a full audit trail is made available to admins without any additional effort.
* Support for Cloud Identity: IAM supports standard Google Accounts. Create IAM policies granting permission to a Google group, a Google-hosted domain, a service account, or specific Google Account holders using Cloud Identity. Centrally manage users and groups through the Google Admin Console.
* Free of charge: IAM is offered at no additional charge for all Google Cloud customers. You will be charged only for use of other Google Cloud services. For information on the pricing of other Google Cloud services, see the Google Cloud Pricing Calculator.

So, let’s start our first task of creating OWNER role and launching an instance with OWNER role. Let’s move quickly to Menu->IAM & Admin. Click on Add and principle which mean the user id or Emil id of the employee to use, and Role is according to task. In my case principal is [has\*\*\*\*\*\*\*\*\*@\*\*\*\*\*\*\*\*.com](mailto:has*********@********.com) and Rols is Owner.Graphical user interface, application

Description automatically generatednow let’s create an instance with owner role (general instance without any specific configuration/minimal configuration). Graphical user interface, text, application, email

Description automatically generatednow change the IAM Role to “Editor” from “Owner” Graphical user interface, application

Description automatically generatedGraphical user interface, text, application, email

Description automatically generatednow try to delete instance: Graphical user interface, text, application, Word

Description automatically generatedand I can see I can delete the instanceGraphical user interface, text, application

Description automatically generated

Now time to work on 3rd task of the assignment and that is to create a user and assign a pre-define roles using IAM, so that he can manage the instances (create and delete). So now assume I have a user that is working in my orgnisation and I need to assign a task to manage the vm instances in my project so I need to assign the roles to that user and roles must be pre-defined (according to task). Predefined roles are created and maintained by Google. Google automatically updates their permissions as necessary, such as when Google Cloud adds new features or services.

Pre-define Roles – are the primitive or gorup of permission which is alreaddy defined in the drop down of Roles. All the roles classified according to the resources. for example for Compute engine we have multipal predefine roles are available like:

Compute Admin Compute Image User

Compute Instance Admin (beta)

Compute Instance Admin (v1)

Compute Load Balancer Admin

Compute Load Balancer Services User

Compute Network Admin

Compute Network User

Compute Network Viewer

Compute Organization Firewall Policy Admin

Compute Organization Firewall Policy User

Compute Organization Resource Admin

Compute Organization Security Policy Admin

Compute Organization Security Policy User

Compute OS Admin Login

Compute OS Login

Compute packet mirroring admin

Compute packet mirroring user

Compute Public IP Admin

Compute Security Admin

Compute Storage Admin

Compute Viewer

GuestPolicy Admin

GuestPolicy Editor

GuestPolicy Viewer

InstanceOSPoliciesCompliance Viewer

OS Inventory Viewer

OS VulnerabilityReport Viewer

OSPolicyAssignment Admin

OSPolicyAssignment Editor

OSPolicyAssignment Viewer

OSPolicyAssignmentReport Viewer

Patch Job Executor

Patch Job Viewer

PatchDeployment Admin

PatchDeployment Viewer

Likewise, we have Multiple Resources available in the GCP and according to the Cloud Resources we have multiple pre-define role for each resource as we have seen above.

According to the Task I have selected the “Compute Engine” Resource and “Compute Instance Admin V1” Role is select and according to role now user have full access over “VM Instance” he can now create and delete the VM InstancesGraphical user interface, application

Description automatically generatedGraphical user interface, text, application

Description automatically generated

Final Task of the Assignment is to create a Custom Role and assign to user so that User are able to manage the “Compute Engine Instances” and “Storage Instances”

Custom-Role – Custom roles help us to enforce the principle of least privilege, because they help to ensure that the principals in your organization have only the permissions that they need. Consider creating a custom role in the following situations:

* A principal needs a permission, but each predefined role that includes that permission also includes permissions that the principal does not need and should not have.
* We use role recommendations to replace overly permissive role grants with more appropriate role grants. In some cases, you might receive a recommendation to create a custom role.

Some IAM permissions are not supported in custom roles. To check whether a specific permission is supported.

Custom roles are user-defined and allow us to bundle one or more supported permissions to meet your specific needs. Custom roles are not maintained by Google; when new permissions, features, or services are added to Google Cloud, your custom roles will not be updated automatically.

When we create a custom role, we must choose an organization or project to create it in. we can then grant the custom role on the organization or project, as well as any resources within that organization or project.

To create a custom role we need to navigate through Menu->IAM and Admin->Roles and create a role fill the details that required and assign roles that need to perform tasks.

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated Graphical user interface, application

Description automatically generated Graphical user interface, text, application, email

Description automatically generated

PTO