## **Understanding IAM Custom Roles**

Cloud IAM also provides the ability to create customized Cloud IAM roles. You can create a custom Cloud IAM role with one or more permissions and then grant that custom role to users. Cloud IAM provides a UI and API for creating and managing custom roles.

**Key Point:** Custom roles enable you to enforce the principle of least privilege, ensuring that the user and service accounts in your organization have only the permissions essential to performing their intended functions.

## **To create a custom role using a YAML file**

Create your role definition YAML file by running:

nano role-definition.yaml

Add this custom role definition to the YAML file:

title: "Role Editor" description: "Edit access for App Versions" stage: "ALPHA" includedPermissions: - appengine.versions.create - appengine.versions.delete

Then save and close the file Execute the following gcloud command:

gcloud iam roles create editor --project $DEVSHELL\_PROJECT\_ID \ --file role-definition.yaml

## **Create a custom role using flags**

Execute the following gcloud command to create a new role using flags:

gcloud iam roles create viewer --project $DEVSHELL\_PROJECT\_ID \ --title "Role Viewer" --description "Custom role description." \ --permissions compute.instances.get,compute.instances.list --stage ALPHA