Create a role in Google Cloud IAM

Scenario

As part of its migration plan, Cymbal Bank is incrementally deploying its workflows to the cloud. One of these deployments includes a database which stores sensitive customer billing and invoice data. Before this database can be deployed, it needs to go through a comprehensive third-party audit. The auditors need access to this database to complete this audit. They need to be granted the appropriate permissions necessary to complete their job. Your team lead, Chloe, has tasked you with leveraging IAM to implement access control to this database for the audit group.

IAM is a fundamental component of cloud security, and it will play a pivotal role in your task. The members of the audit team will require designated roles with restricted access, exclusively for viewing and listing the database contents. Your task, as outlined by your team lead, entails the precise configuration of user access to align with these strict requirements.

Task 1. Create a custom role

Applying the principle of least privilege is integral to IAM. It ensures that users are only given the permissions they need to perform their tasks. Custom roles provide a way to tailor permissions to an organization's needs, making sure that users do not have broad and excessive permissions.

In this task, you'll create a custom role for the audit team at Cymbal. You'll then grant the custom role restricted access for viewing the database contents.

1. In the Google Cloud console, in the **Navigation menu** (☰), click **IAM & Admin** > **Roles**. The **Roles** page opens.
2. On the Explorer bar, located near the top of the **Roles** page, click **+ Create Role**.
3. In the **Create Role** dialog, specify the following settings and leave the remaining settings as their defaults:

Property	**Value (type or select)**
Title	Audit Team Reviewer
Description	Custom role, allowing the audit team to conduct its review activities. This role grants read-only access to Firebase database resources.

ID	CustomRole
Role launch stage	General Availability

Each custom role can be given a **role launch stage** which reflects the different phases of a role's development, testing, and deployment. These stages help users understand the current state of a role and its suitability for various use cases.

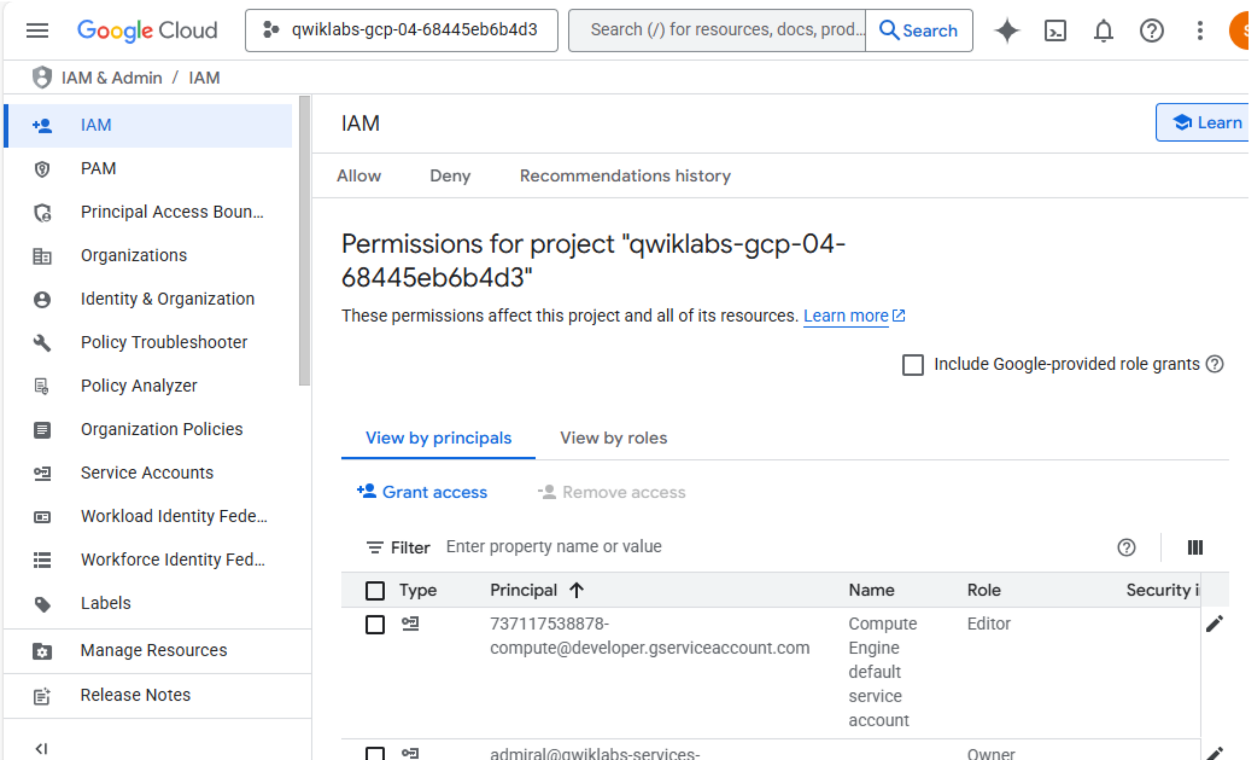
There are several launch stages in Google Cloud. The three primary role launch stages you should know about are:

Alpha: Roles in the Alpha stage are typically experimental and may undergo significant changes. They are not recommended for production environments. Users can provide feedback on alpha roles to influence their development.

Beta: Roles in the Beta stage are more mature than alpha roles but might still receive updates and improvements based on user feedback. They are considered suitable for certain non-production scenarios but may not be fully stable.

General Availability (GA): Roles that have reached General Availability have undergone thorough development, testing, and refinement. They are considered stable, reliable, and suitable for widespread use in production environments. GA roles have been extensively reviewed and are intended to provide consistent and dependable behavior.

4. Click the **+ Add permissions**. The **Add permissions** dialog box opens.
5. In the **Filter permissions by role** field, type **Firebase Realtime**.
6. In the results drop-down field, select the **Firebase Realtime Database Viewer** checkbox.
7. Click **OK**.
8. Under **Filter**, select the **firebase.clients.list** and **firebasedatabase.instances.list** checkboxes to add these permissions to the custom role.



IAM

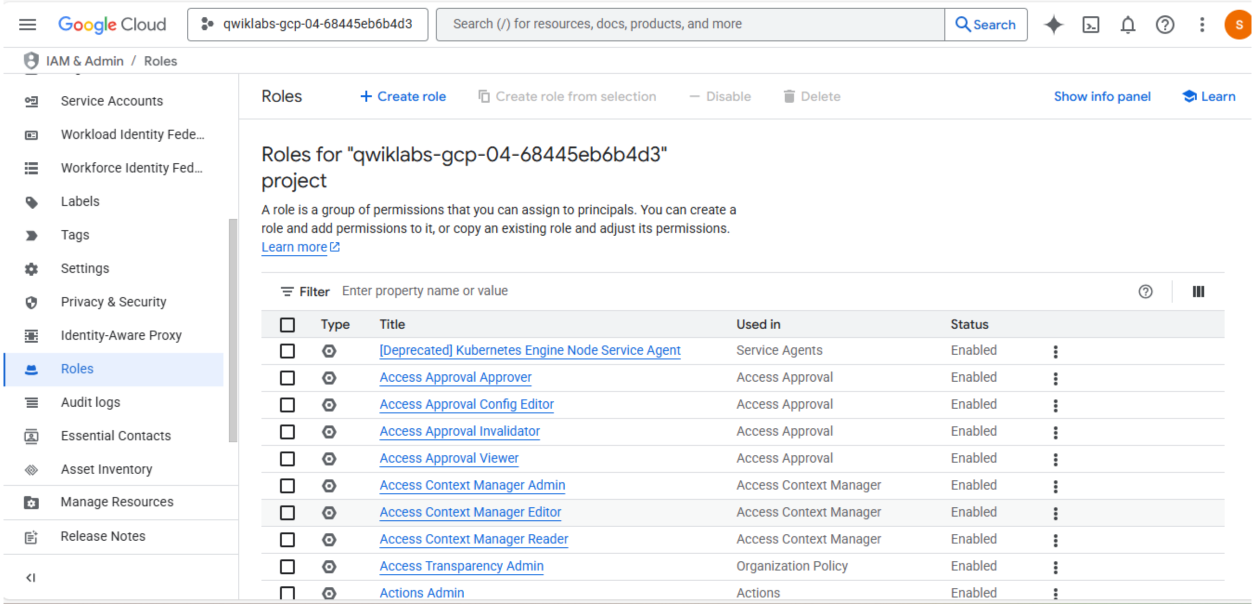
Permissions for project "qwiklabs-gcp-04-68445eb6b4d3"

These permissions affect this project and all of its resources. Learn more

□ Include Google-provided role grants

Filter Enter property name or value

□	Type	Principal ↑	Name	Role	Security i
□		737117538878-compute@developer.gserviceaccount.com	Compute Engine default service account	Editor	
□		admiral@qwiklabs-services-		Owner	



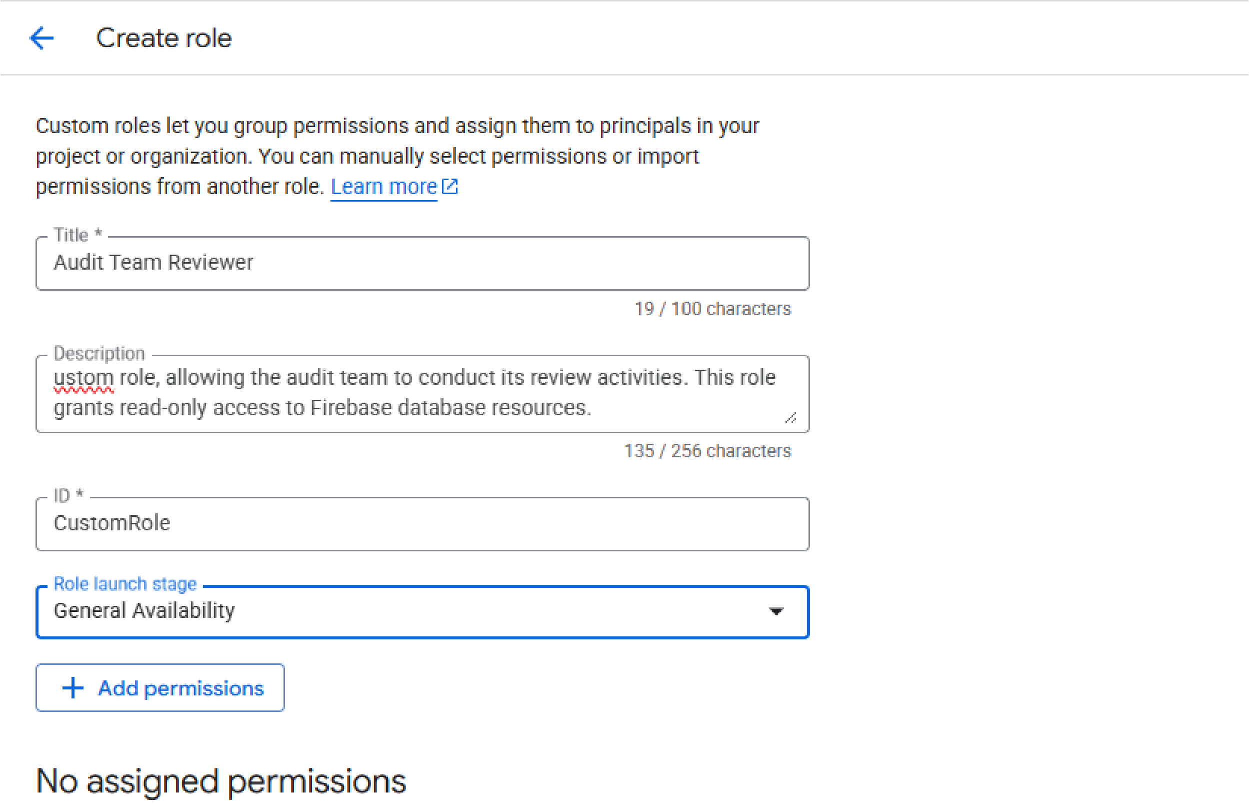
Roles

Roles for "qwiklabs-gcp-04-68445eb6b4d3" project

A role is a group of permissions that you can assign to principals. You can create a role and add permissions to it, or copy an existing role and adjust its permissions. Learn more

Filter Enter property name or value

□	Type	Title	Used in	Status
□		[Deprecated] Kubernetes Engine Node Service Agent	Service Agents	Enabled
□		Access Approval Approver	Access Approval	Enabled
□		Access Approval Config Editor	Access Approval	Enabled
□		Access Approval Invalidator	Access Approval	Enabled
□		Access Approval Viewer	Access Approval	Enabled
□		Access Context Manager Admin	Access Context Manager	Enabled
□		Access Context Manager Editor	Access Context Manager	Enabled
□		Access Context Manager Reader	Access Context Manager	Enabled
□		Access Transparency Admin	Organization Policy	Enabled
□		Actions Admin	Actions	Enabled



Create role

Custom roles let you group permissions and assign them to principals in your project or organization. You can manually select permissions or import permissions from another role. Learn more

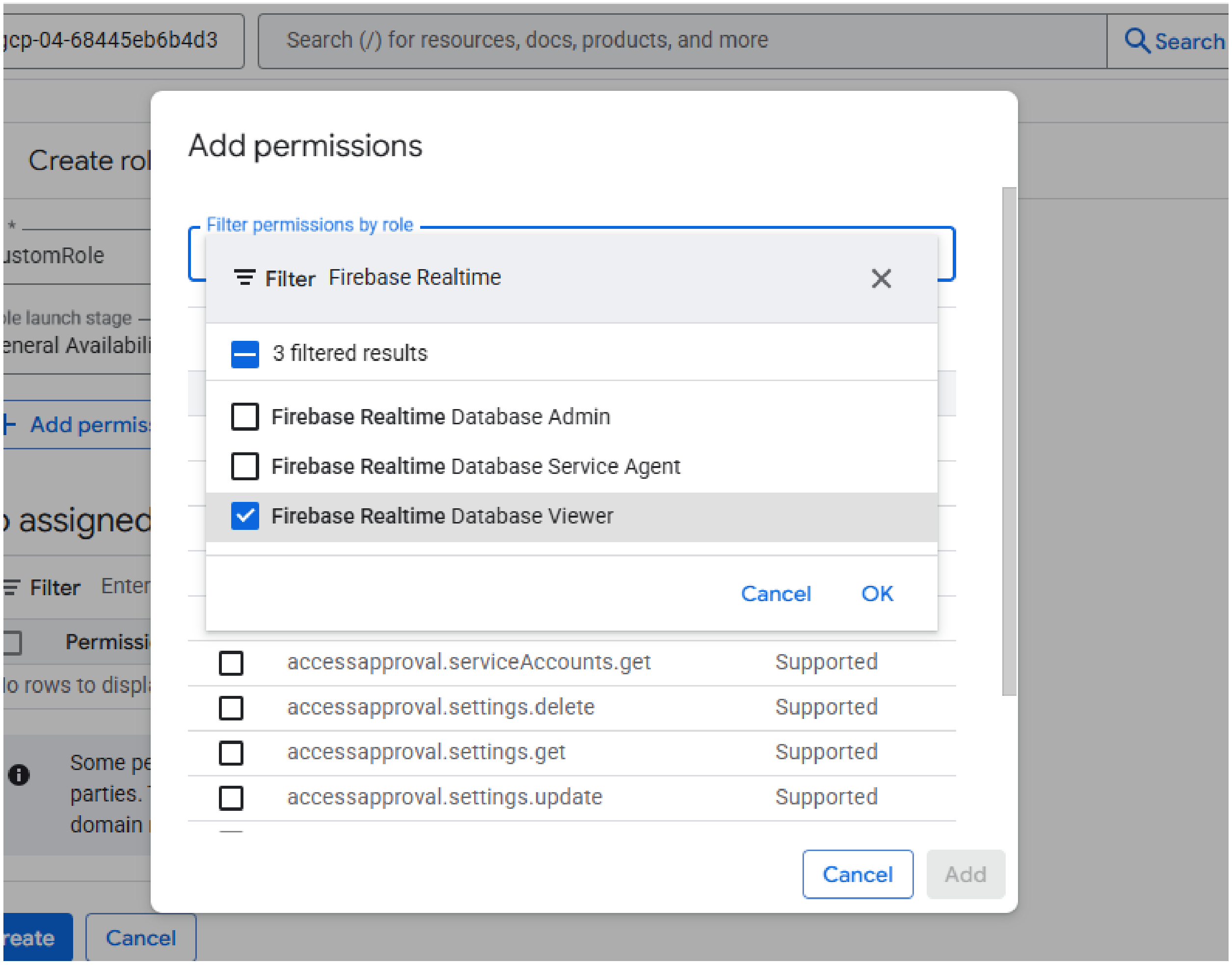
Title *
Audit Team Reviewer
19 / 100 characters

Description
ustom role, allowing the audit team to conduct its review activities. This role grants read-only access to Firebase database resources.
135 / 256 characters

ID *
CustomRole

Role launch stage
General Availability

No assigned permissions



Add permissions

Filter permissions by role

Filter Firebase Realtime

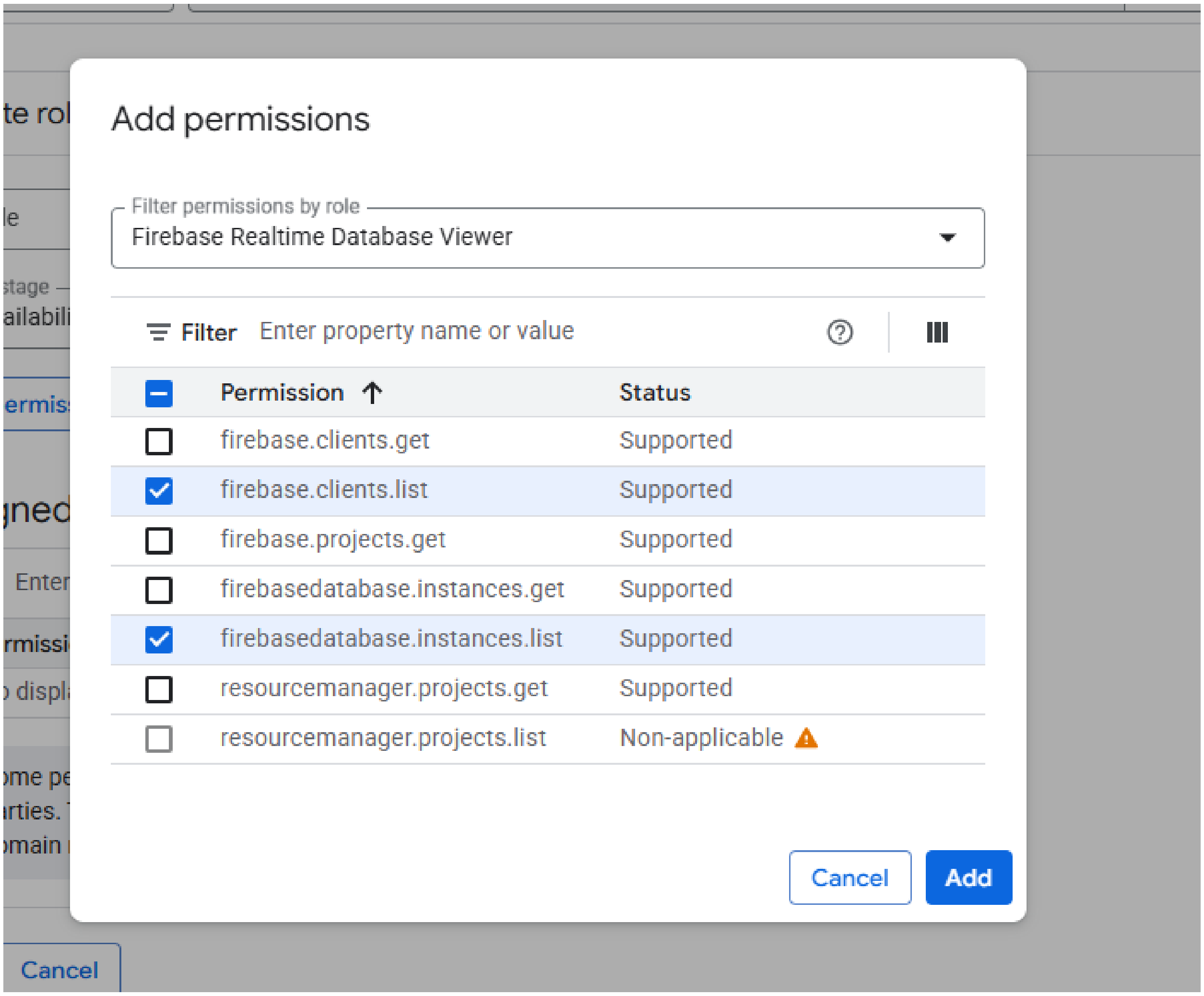
☐ 3 filtered results

☐ **Firebase Realtime** Database Admin

☐ **Firebase Realtime** Database Service Agent

☑ **Firebase Realtime** Database Viewer

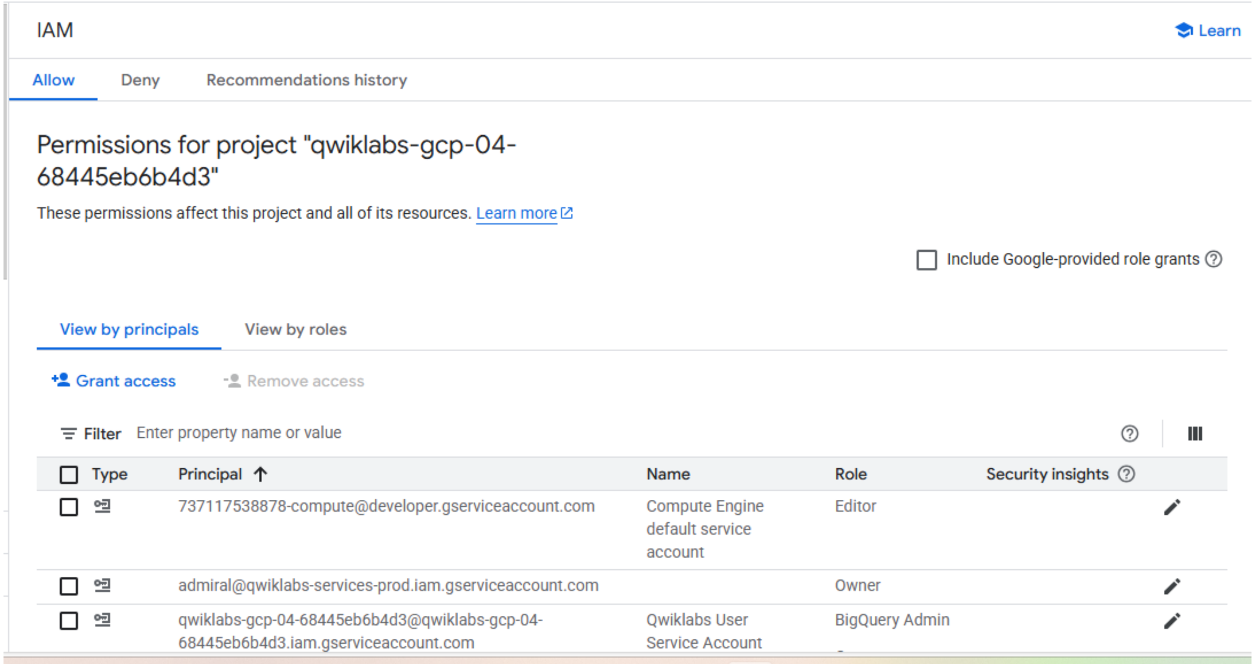
☐	accessapproval.serviceAccounts.get	Supported
☐	accessapproval.settings.delete	Supported
☐	accessapproval.settings.get	Supported
☐	accessapproval.settings.update	Supported



Add permissions

Filter permissions by role: Firebase Realtime Database Viewer

⊟	Permission ↑	Status
☐	firebase.clients.get	Supported
☑	firebase.clients.list	Supported
☐	firebase.projects.get	Supported
☐	firebasedatabase.instances.get	Supported
☑	firebasedatabase.instances.list	Supported
☐	resourcemanager.projects.get	Supported
☐	resourcemanager.projects.list	Non-applicable ⚠



IAM

Permissions for project "qwiklabs-gcp-04-68445eb6b4d3"

These permissions affect this project and all of its resources. Learn more

☐ Include Google-provided role grants

☐ Type	Principal ↑	Name	Role	Security insights
☐	737117538878-compute@developer.gserviceaccount.com	Compute Engine default service account	Editor	
☐	admiral@qwiklabs-services-prod.iam.gserviceaccount.com		Owner	
☐	qwiklabs-gcp-04-68445eb6b4d3@qwiklabs-gcp-04-68445eb6b4d3.iam.gserviceaccount.com	Qwiklabs User Service Account	BigQuery Admin	

9. Click **Add**.
10. In the **Create Role** dialog, click **Create**.

The new role should now be created and added to the existing roles in the project.

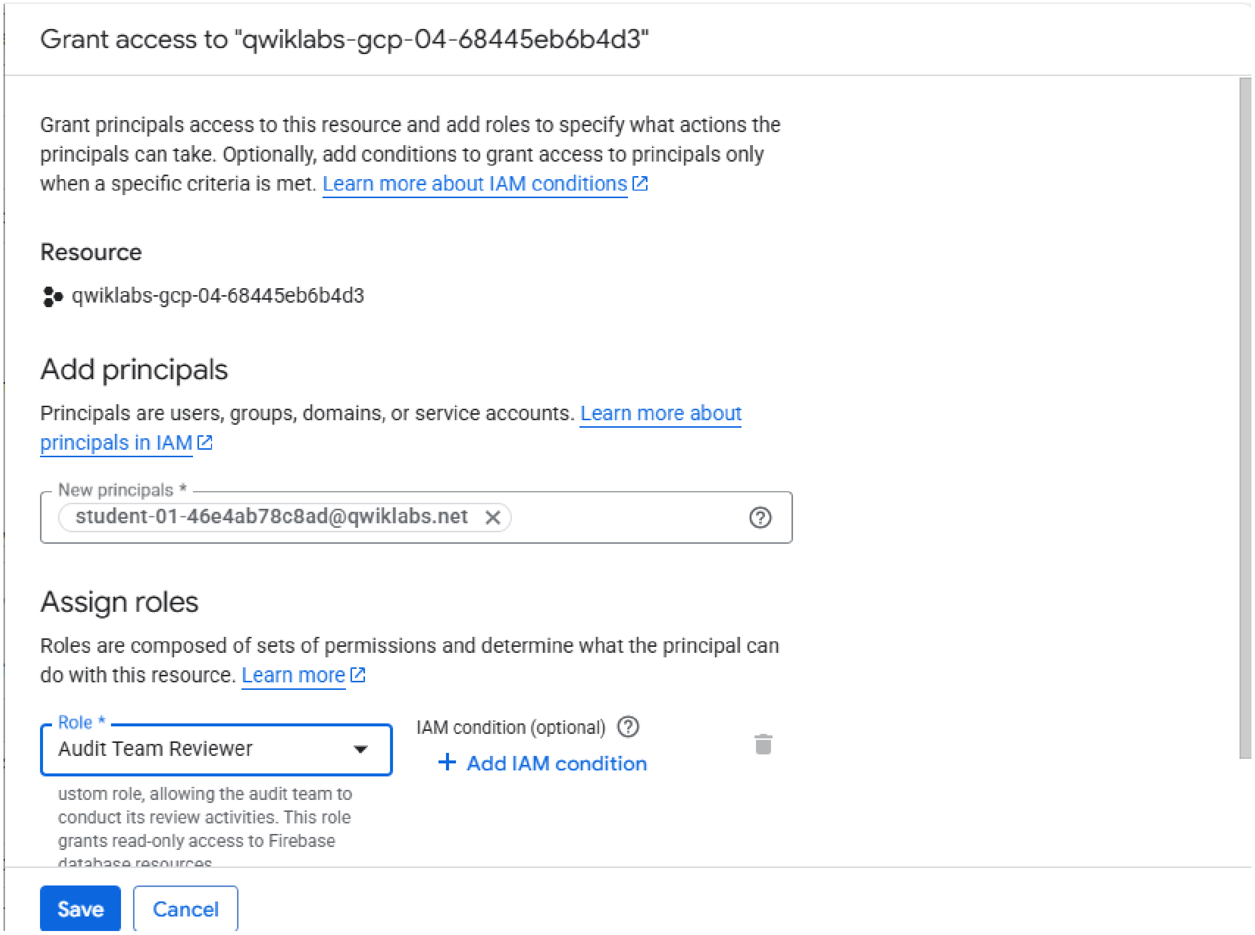
Task 2. Grant a role to a user

In this task, you'll assign the custom role you created in Task 1 to an existing user.

1. In the Google Cloud console, in the **Navigation menu** (☰), click **IAM & Admin** > **IAM**. The **IAM** page opens.
2. On the **View By Principals** tab, click **Grant access**. The **Grant access** dialog window will open.

The **Grant access** dialogue box is a crucial component of the IAM system in Google Cloud. It provides you with the ability to precisely define and manage these permissions for users, groups, and service accounts.

3. Copy the **Google Cloud usern**



Grant access to "qwiklabs-gcp-04-68445eb6b4d3"

Grant principals access to this resource and add roles to specify what actions the principals can take. Optionally, add conditions to grant access to principals only when a specific criteria is met. Learn more about IAM conditions

Resource

qwiklabs-gcp-04-68445eb6b4d3

Add principals

Principals are users, groups, domains, or service accounts. Learn more about principals in IAM

New principals *: student-01-46e4ab78c8ad@qwiklabs.net ✕

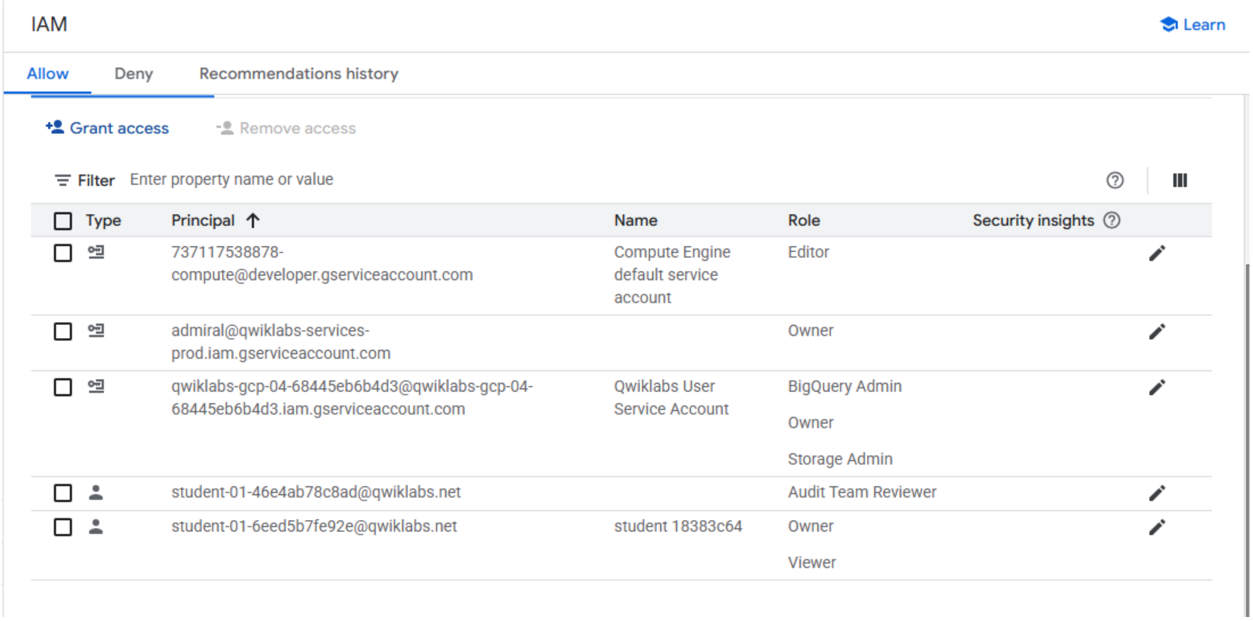
Assign roles

Roles are composed of sets of permissions and determine what the principal can do with this resource. Learn more

Role *: Audit Team Reviewer

ustom role, allowing the audit team to conduct its review activities. This role grants read-only access to Firebase database resources

4. Expand the **Select a role** drop-down menu, select **Custom**, and then select **Audit Team Reviewer**. This is the role you created in the previous task.



□	Type	Principal ↑	Name	Role	Security insights
□		737117538878-compute@developer.gserviceaccount.com	Compute Engine default service account	Editor	
□		admiral@qwiklabs-services-prod.iam.gserviceaccount.com		Owner	
□		qwiklabs-gcp-04-68445eb6b4d3@qwiklabs-gcp-04-68445eb6b4d3.iam.gserviceaccount.com	Qwiklabs User Service Account	BigQuery Admin Owner Storage Admin	
□		student-01-46e4ab78c8ad@qwiklabs.net		Audit Team Reviewer	
□		student-01-6eed5b7fe92e@qwiklabs.net	student 18383c64	Owner Viewer	

5. Click **Save**.

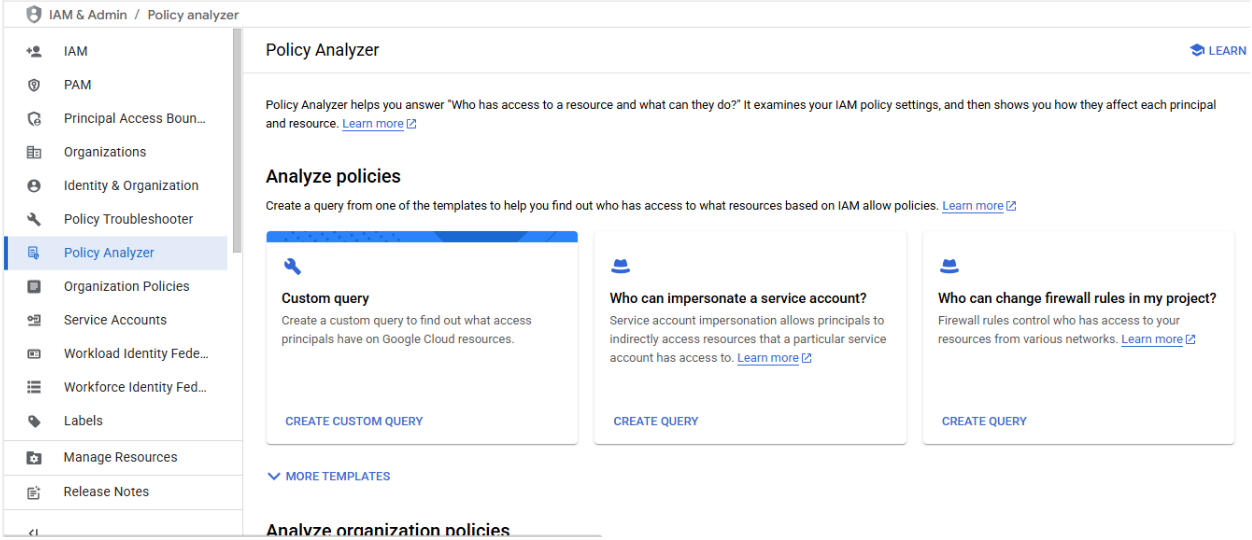
   The custom role should now be assigned to the user.

Task 3. Verify the role

So far, you've created a custom role with the appropriate permissions and granted the role to the user. Now, you'll need to check your work to verify that the user has been assigned the role you created. Ensuring that you've correctly configured settings is an integral in part of your workflow as a cloud security analyst.

In this task, you'll use Google Cloud's Policy Analyzer to create a query to check the roles granted to the user.

1. In the Google Cloud console, in the **Navigation menu** (☰), click **IAM & Admin** > **Policy Analyzer**. The **Policy Analyzer** page opens.
2. In the **Analyze policies** section, on the **Custom Query** tile, click **Create custom query**. A pop-up may appear at the top left Google Cloud menu () with the text “Click on the menu anytime to find solutions for your business”. Select **Got it** and proceed to the next step.
3. In the **Set the query parameters** section, expand the **Parameter 1** drop-down menu and select **Principal**.
4. Copy the **Google Cloud username 2: Username 2** and paste it into the **Principal** field.



Policy Analyzer

Policy Analyzer helps you answer "Who has access to a resource and what can they do?" It examines your IAM policy settings, and then shows you how they affect each principal and resource. Learn more

Analyze policies

Create a query from one of the templates to help you find out who has access to what resources based on IAM allow policies. Learn more

Custom query

Create a custom query to find out what access principals have on Google Cloud resources.

CREATE CUSTOM QUERY

Who can impersonate a service account?

Service account impersonation allows principals to indirectly access resources that a particular service account has access to. Learn more

CREATE QUERY

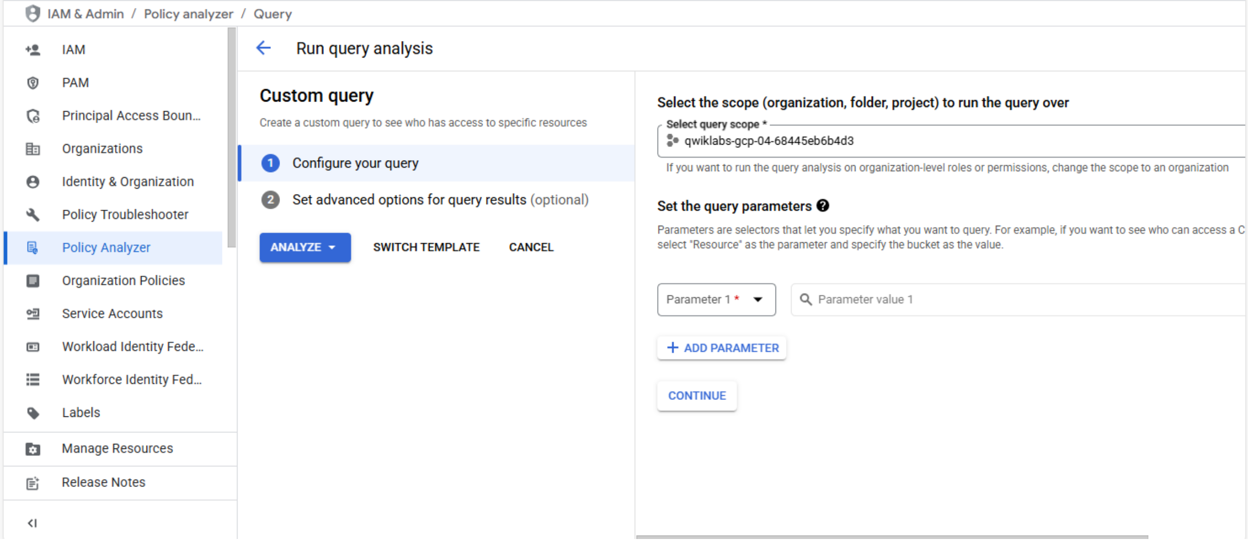
Who can change firewall rules in my project?

Firewall rules control who has access to your resources from various networks. Learn more

CREATE QUERY

MORE TEMPLATES

Analyze organization policies



Run query analysis

Custom query

Create a custom query to see who has access to specific resources

1 Configure your query

2 Set advanced options for query results (optional)

Select the scope (organization, folder, project) to run the query over

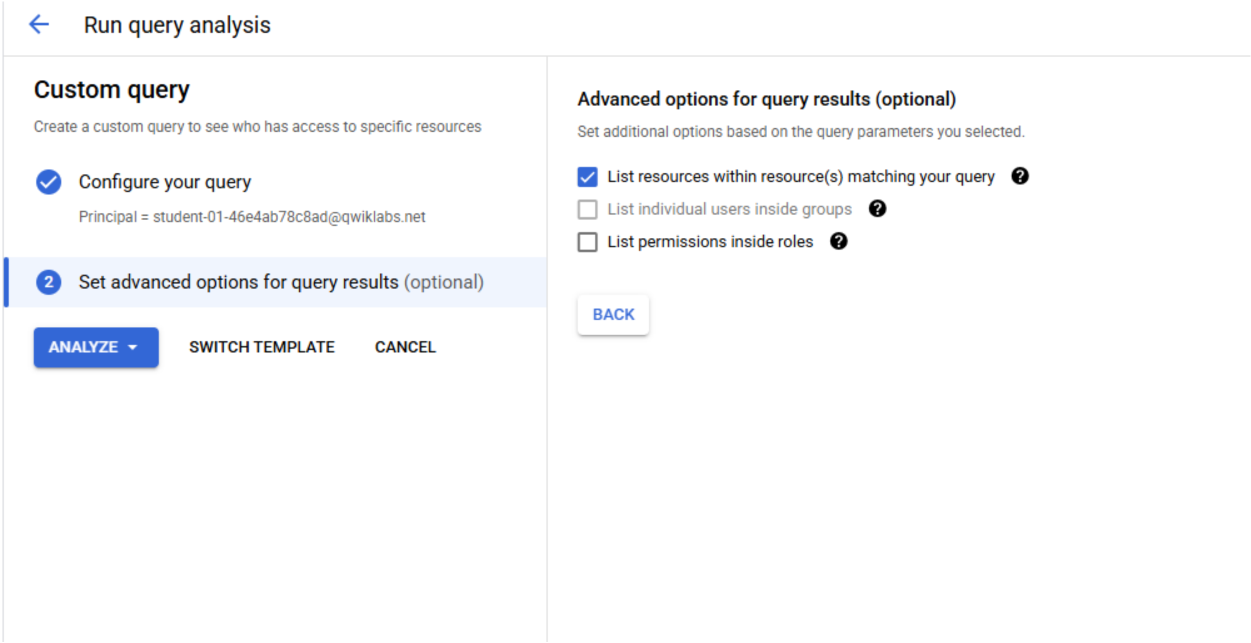
Select query scope * qwiklabs-gcp-04-68445eb6b4d3

If you want to run the query analysis on organization-level roles or permissions, change the scope to an organization

Set the query parameters

Parameters are selectors that let you specify what you want to query. For example, if you want to see who can access a C select "Resource" as the parameter and specify the bucket as the value.

Parameter 1 * | Parameter value 1



Run query analysis

Custom query

Create a custom query to see who has access to specific resources

✓ Configure your query

Principal = student-01-46e4ab78c8ad@qwiklabs.net

2 Set advanced options for query results (optional)

Advanced options for query results (optional)

Set additional options based on the query parameters you selected.

☑ List resources within resource(s) matching your query

□ List individual users inside groups

□ List permissions inside roles