Course 3_Lab 1: Create a role in Google Cloud IAM

Scenario

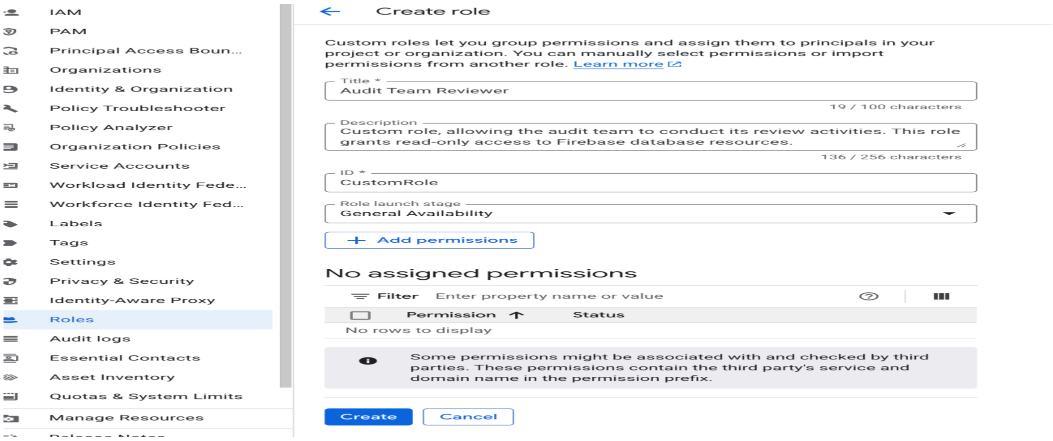
As part of its migration plan, Cymbal Bank is incrementally deploying its workflows to the cloud. One of these deployments includes a database which stores sensitive customer billing and invoice data. Before this database can be deployed, it needs to go through a comprehensive third-party audit. The 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.

Here's how you'll do this task: First, you'll create a role and assign the required permissions. Next, you'll assign the new role you have created to a user. Finally, you'll verify that the role you created has been granted.

Activity: In this lab, you'll learn how to create and manage Identity and Access Management (IAM) custom roles.

MY WORK:
Task 1: Create a Custom Role & add permissions

In this task, I was able to create a custom role using the Identity and Access Management (IAM) service. I was also able to add permissions within the role creation.



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
Custom role, allowing the audit team to conduct its review activities. This role grants read-only access to Firebase database resources.
136 / 256 characters

ID *
CustomRole

Role launch stage
General Availability

+ Add permissions

No assigned permissions

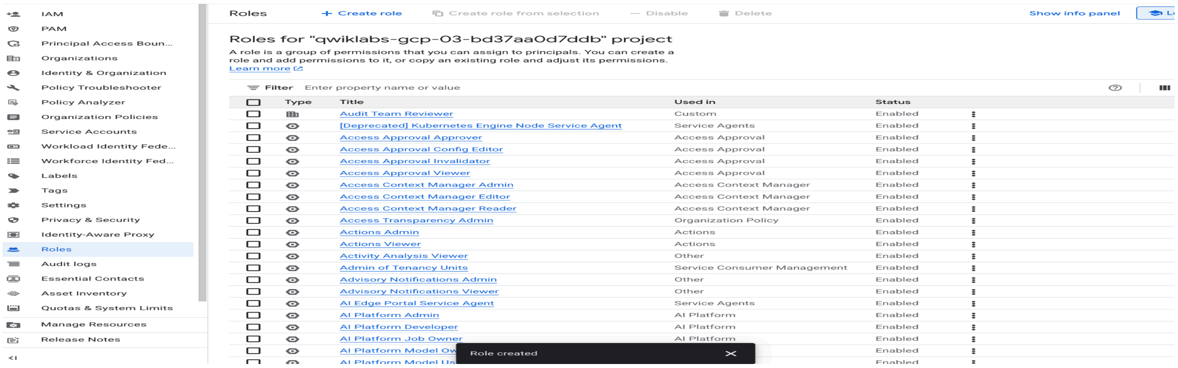
Filter Enter property name or value

☐	Permission ↑	Status

No rows to display

Some permissions might be associated with and checked by third parties. These permissions contain the third party's service and domain name in the permission prefix.

Create Cancel



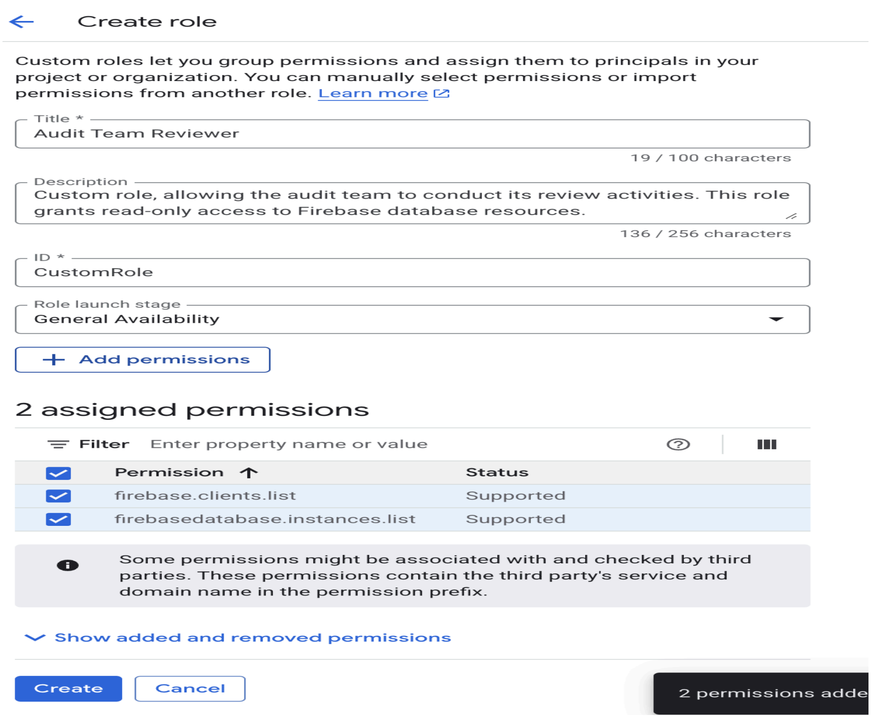
Roles for "qwiklabs-gcp-03-bd37aa0d7ddb" project

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
☐		Audit Team Reviewer	Custom	Enabled
☐		[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
☐		Actions Viewer	Actions	Enabled
☐		Activity Analysis Viewer	Other	Enabled
☐		Admin of Tenancy Units	Service Consumer Management	Enabled
☐		Advisory Notifications Admin	Other	Enabled
☐		Advisory Notifications Viewer	Other	Enabled
☐		AI Edge Portal Service Agent	Service Agents	Enabled
☐		AI Platform Admin	AI Platform	Enabled
☐		AI Platform Developer	AI Platform	Enabled
☐		AI Platform Job Owner	AI Platform	Enabled
☐		AI Platform Model Ow		Enabled
☐		AI Platform Model Us		Enabled

Role created



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
Custom role, allowing the audit team to conduct its review activities. This role grants read-only access to Firebase database resources.
136 / 256 characters

ID *
CustomRole

Role launch stage
General Availability

+ Add permissions

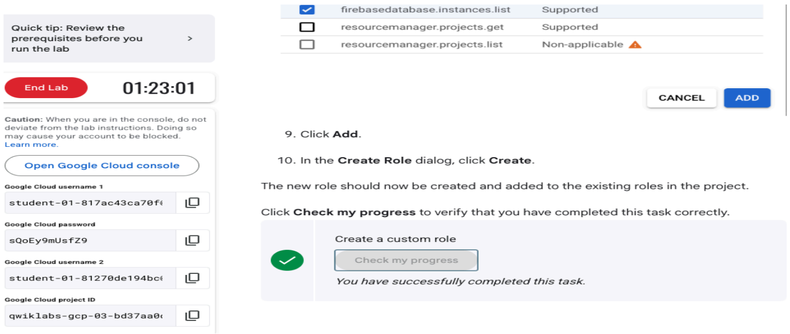
2 assigned permissions

Filter Enter property name or value

	Permission ↑	Status
☑	firebase.clients.list	Supported
☑	firebasedatabase.instances.list	Supported

Some permissions might be associated with and checked by third parties. These permissions contain the third party's service and domain name in the permission prefix.

Show added and removed permissions



Quick tip: Review the prerequisites before you run the lab

01:23:01

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Google Cloud username 1
student-01-817ac43ca70f(

Google Cloud password
sQoEy9mUsfZ9

Google Cloud username 2
student-01-81270de194bc(

Google Cloud project ID
qwiklabs-gcp-03-bd37aa0(

☑	firebasedatabase.instances.list	Supported
□	resourcemanager.projects.get	Supported
□	resourcemanager.projects.list	Non-applicable ⚠

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.

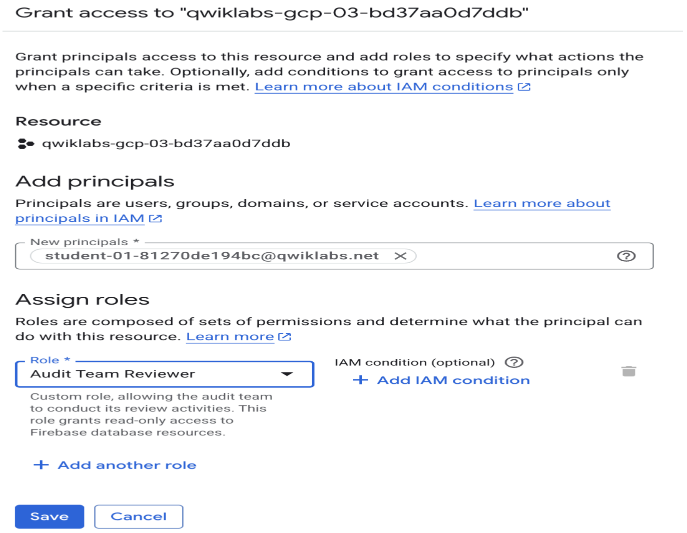
Click **Check my progress** to verify that you have completed this task correctly.

✓ Create a custom role

You have successfully completed this task.

Task 2: Grant a role to a user

For this task, I was able to grant the role created in the first task to a user account.



Grant access to "qwiklabs-gcp-03-bd37aa0d7ddb"

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-03-bd37aa0d7ddb

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

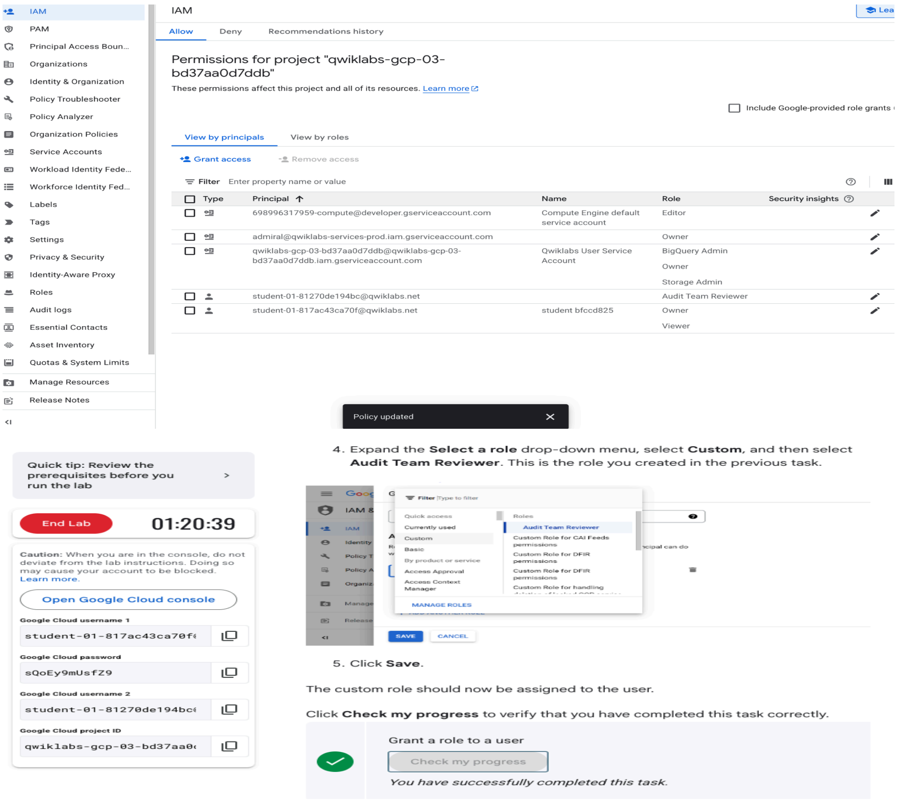
New principals *
student-01-81270de194bc@qwiklabs.net ✕

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

IAM condition (optional)
+ Add IAM condition

+ Add another role



IAM

Permissions for project "qwiklabs-gcp-03-bd37aa0d7ddb"

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 insights
□	698996317959-compute@developer.gserviceaccount.com	Compute Engine default service account	Editor	
□	admiral@qwiklabs-services-prod.iam.gserviceaccount.com		Owner	
□	qwiklabs-gcp-03-bd37aa0d7ddb@qwiklabs-gcp-03-bd37aa0d7ddb.iam.gserviceaccount.com	Qwiklabs User Service Account	BigQuery Admin Owner Storage Admin	
□	student-01-81270de194bc@qwiklabs.net		Audit Team Reviewer	
□	student-01-817ac43ca70f@qwiklabs.net	student bfccd825	Owner Viewer	

Policy updated ✕

Quick tip: Review the prerequisites before you run the lab >

01:20:39

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Google Cloud username 1: student-01-817ac43ca70f

Google Cloud password: sQoEy9mUsfZ9

Google Cloud username 2: student-01-81270de194bc

Google Cloud project ID: qwiklabs-gcp-03-bd37aa0

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.

5. Click **Save**.

The custom role should now be assigned to the user.

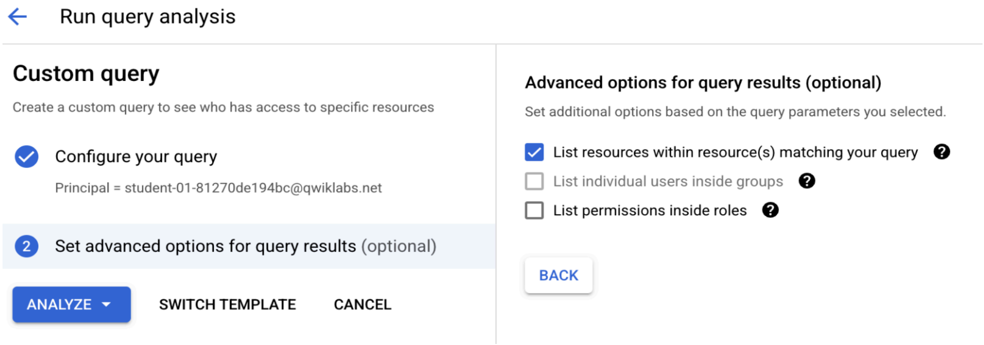
Click **Check my progress** to verify that you have completed this task correctly.

Grant a role to a user

You have successfully completed this task.

Task 3: Verify the Role

Using The Policy Analyzer tool in the Google Cloud Platform, I was able to verify that the role was created, by running a custom query.



Run query analysis

Custom query

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

Configure your query

Principal = student-01-81270de194bc@qwiklabs.net

2 Set advanced options for query results (optional)

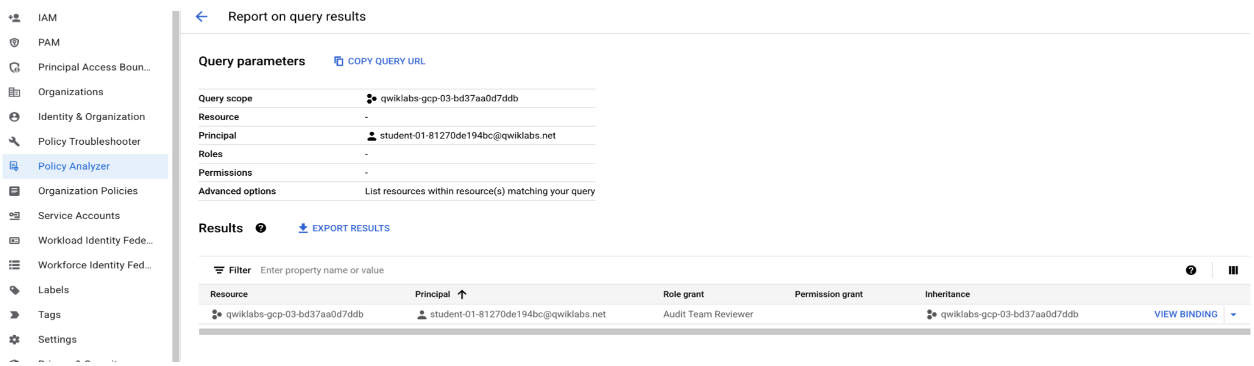
Advanced options for query results (optional)

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



Report on query results

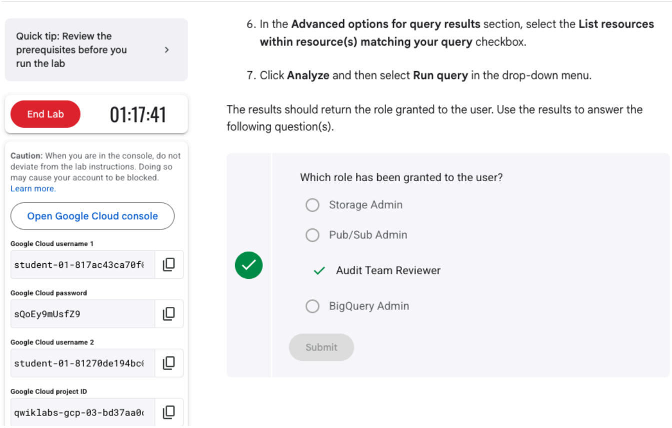
Query parameters

Query scope	qwiklabs-gcp-03-bd37aa0d7ddb
Resource	-
Principal	student-01-81270de194bc@qwiklabs.net
Roles	-
Permissions	-
Advanced options	List resources within resource(s) matching your query

Results

Filter Enter property name or value

Resource	Principal ↑	Role grant	Permission grant	Inheritance	
qwiklabs-gcp-03-bd37aa0d7ddb	student-01-81270de194bc@qwiklabs.net	Audit Team Reviewer		qwiklabs-gcp-03-bd37aa0d7ddb	VIEW BINDING



Quick tip: Review the prerequisites before you run the lab ›

End Lab 01:17:41

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Open Google Cloud console

Google Cloud username 1

student-01-817ac43ca70f

Google Cloud password

sQoEy9mUsfZ9

Google Cloud username 2

student-01-81270de194bc

Google Cloud project ID

qwiklabs-gcp-03-bd37aa0

6. In the **Advanced options for query results** section, select the **List resources within resource(s) matching your query** checkbox.

7. Click **Analyze** and then select **Run query** in the drop-down menu.

The results should return the role granted to the user. Use the results to answer the following question(s).

Which role has been granted to the user?

○ Storage Admin

○ Pub/Sub Admin

✓ Audit Team Reviewer

○ BigQuery Admin

Submit

My Assessment:

Overall, this lab did not present any tasks or steps that were impossible or presented any level of confusion. The lab emphasized the importance of concepts such as least privilege, access based controls, specifically RBAC (role-based access control), while providing hands-on learning with Google Services such as IAM, Policy Analyzer, creating permissions and roles. Understanding the difference between the different role launch stages when creating a role and why General Availability is important was helpful.