CREATE A ROLE IN GOOGLE CLOUD IAM

PROJECT DESCRIPTION

In this lab activity, I learnt how to create and manage Identity and Access Management (IAM) custom roles.

SCENARIO

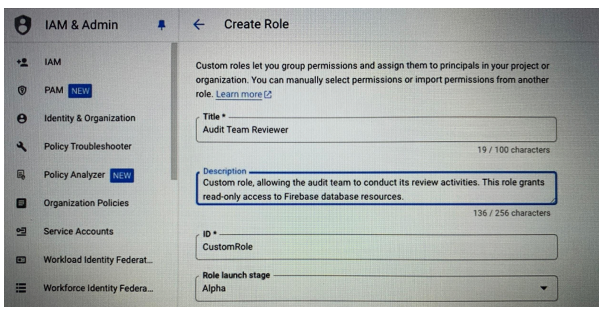
A database to be deployed needs to go through a comprehensive third party audit. I am tasked with leveraging IAM to implement access control to this database for the audit group. This task, entails the precise configuration of user access to align with these strict requirements.

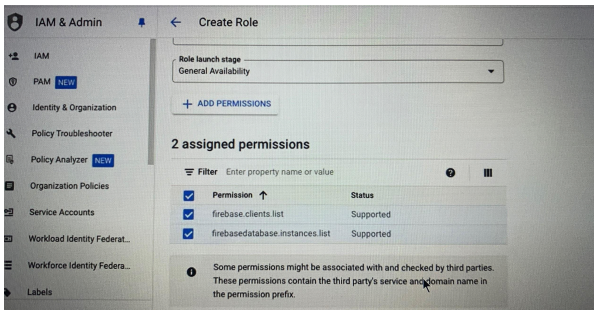
Here's how I did this;

First Step: Create a Custom Role

I created a custom role for the audit team. I then granted the custom role restricted access for viewing the database contents.

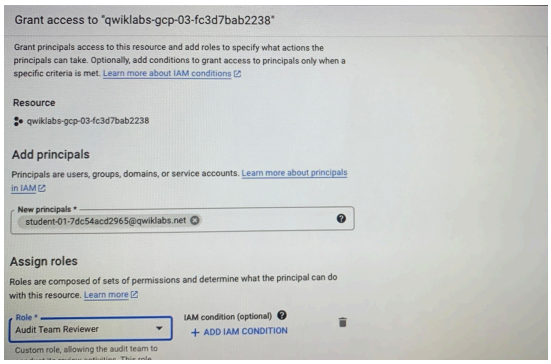
I also added permissions to the custom role as seen below.





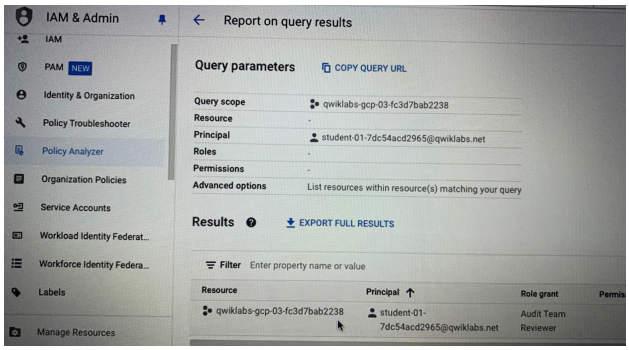
Second Step: Grant a Role to a User

I assigned the custom role I created in the first step to an existing user.



Final Step: Verify the Role

I used Google Cloud's Policy analyzer to create a query to check the roles granted to the user. After I ran the query, the results returned the role granted to the user which is **Audit Team Reviewer.**



CONCLUSION

Through this lab activity, I have successfully utilized IAM to create a custom role, grant access to a user for that role and verified the permissions within Google Cloud. The audit team can now begin their work on database audit using the custom role I created.

By using IAM services, I am well on my way to effectively managing access and permissions to storage resources.