REPORT ENTITLED:

GOOGLE CLOUD ACCESS CONTROL: PRACTICAL IMPLEMENTATION OF CUSTOM ROLES

BY

DAMOAH BASHIRU

DATE: 10TH MARCH 2025

ABSTRACT

This project demonstrates practical cloud security management on Google Cloud Platform (GCP) through Identity and Access Management (IAM). It focuses on creating and assigning a Custom Viewer role to enforce the principle of least privilege, ensuring users have read-only access to project resources. The workflow covers account creation, Qwiklabs Quickstart access, project setup, IAM policy analysis, and role verification using Cloud Shell. The project highlights hands-on skills in cloud access control, policy management, and secure role configuration, providing real-world insights into maintaining secure cloud environments

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Background of the Study

Cloud computing has become an integral part of modern IT infrastructure, enabling organizations to deploy, manage, and scale applications efficiently. Google Cloud Platform (GCP) is one of the leading cloud service providers, offering a wide range of services and tools for computing, storage, networking, and security.

As organizations increasingly adopt cloud technologies, managing access to resources becomes critical. Identity and Access Management (IAM) in GCP provides administrators with the ability to define who can access which resources and what actions they can perform. Proper configuration of IAM policies ensures that users have the minimum necessary permissions, reducing the risk of unauthorized access or accidental misconfiguration.

This project focuses on understanding and implementing IAM policies in GCP, with particular emphasis on creating a **Custom Viewer** role. This role allows read-only access to specific resources, demonstrating the principle of least privilege while maintaining secure operations.

1.2 Significance of the Study

The study is significant for several reasons:

- **Cloud Security Awareness:** Proper IAM configuration is essential for protecting cloud resources from unauthorized access and potential data breaches.
- **Hands-On Learning:** The project provides practical experience in setting up custom roles, assigning permissions, and verifying IAM policies.
- **Principle of Least Privilege:** Understanding and implementing custom roles reinforces best practices in cloud access management.
- **Real-World Application:** Skills acquired through this project are directly applicable to professional cloud administration and cybersecurity roles.

1.3 Objectives of the Report

The main objectives of this report are to:

1. Demonstrate the creation of a Google Cloud account and setup of a GCP project.
2. Access and analyze IAM policies using the GCP Console and Cloud Shell.
3. Create and assign a **Custom Viewer** role to a user, ensuring limited read-only access.
4. Verify and document the effective permissions associated with the custom role.
5. Highlight the importance of IAM policy management in securing cloud resources and applying the principle of least privilege.

CHAPTER 2

LITERATURE REVIEW

2.1 Cloud Computing and Google Cloud Platform

Cloud computing has transformed the way organizations deploy and manage IT resources. Google Cloud Platform (GCP) offers a comprehensive suite of services including computing, storage, networking, and security. The flexibility and scalability of cloud services make them attractive, but they also introduce challenges in access management and data security.

2.2 Identity and Access Management (IAM)

IAM is a critical component of cloud security. It enables administrators to control who has access to which resources and what operations they can perform. Proper IAM configuration ensures that only authorized users can access sensitive data or perform critical operations, reducing the risk of accidental or malicious misuse.

Key IAM concepts include:

- **Roles:** Collections of permissions that define what actions users can perform. Predefined roles include Viewer, Editor, and Owner.
- **Custom Roles:** Tailored roles that allow fine-grained control over permissions to adhere to the principle of least privilege.
- **Policies:** Define how roles are assigned to users, groups, or service accounts within a project.
- **Principals:** The users, groups, or service accounts to whom permissions are granted.

2.3 Importance of Custom Roles

While predefined roles provide broad access, they may grant more permissions than necessary. Custom roles, such as the **Custom Viewer** role, enable organizations to restrict access to read-only actions on specific resources. This reduces security risks and aligns with industry best practices for least-privilege access management.

2.4 Best Practices in Cloud Access Management

Effective cloud access management involves:

- **Applying Least Privilege:** Assigning only the permissions necessary for a user to perform their tasks.
- **Regularly Reviewing IAM Policies:** Auditing permissions to identify and remove excessive or unused access.
- **Using Service Accounts Appropriately:** Assigning roles to service accounts for automation rather than using personal accounts.
- **Monitoring and Logging:** Enabling Cloud Audit Logs to track changes in IAM policies and resource access.

2.5 Existing Research on IAM and Custom Roles

Studies in cloud security emphasize that misconfigured IAM policies are one of the most common causes of data breaches. Research shows that using custom roles and continuous monitoring significantly reduces the risk of unauthorized access. Proper training and awareness among administrators further enhance the effectiveness of IAM controls.

2.6 Summary

The literature review highlights the critical role of IAM in securing cloud environments. Custom roles, such as the Custom Viewer role, offer granular control over permissions and help implement the principle of least privilege. Regular auditing, monitoring, and adherence to best practices are essential for maintaining secure and well-managed cloud projects.

CHAPTER 3

FINDINGS AND ANALYSIS

3.1 Overview

This chapter presents a detailed walkthrough of the Google Cloud IAM Quickstart lab, including the creation and assignment of a Custom Viewer role. Each step is illustrated with a corresponding screenshot stored in the `images` folder to document the workflow and evidence of task completion.

3.2 Step-by-Step Lab Walkthrough (with evidence)

1. **Sign in or create Google Cloud account.**

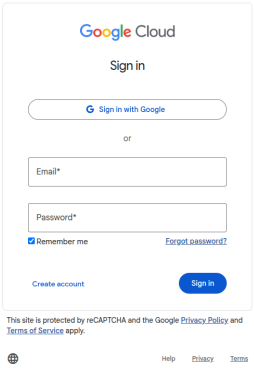

Figure 3.1 Step 1: Sign in or create Google Cloud account.

2. **Search for IAM on Google Cloud.**

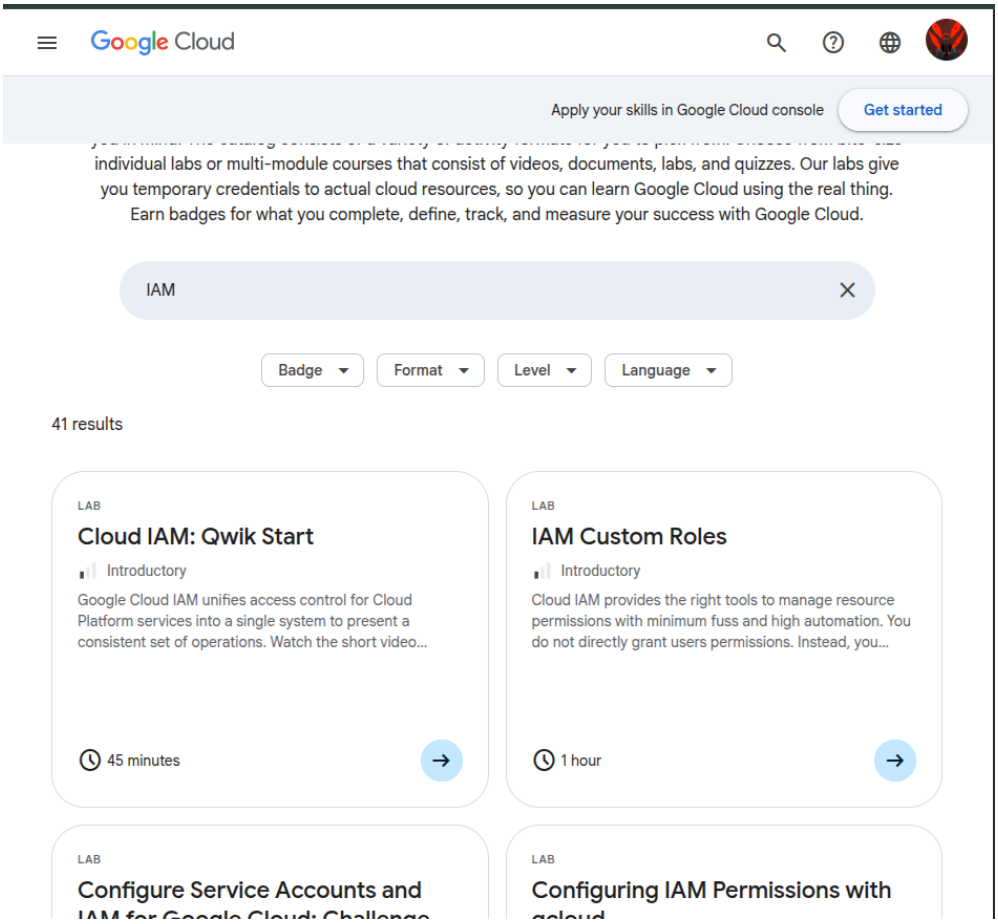

Figure 3.2 Step 2: Searching for IAM in the GCP console.

3. **Start the IAM Quickstart lab.**

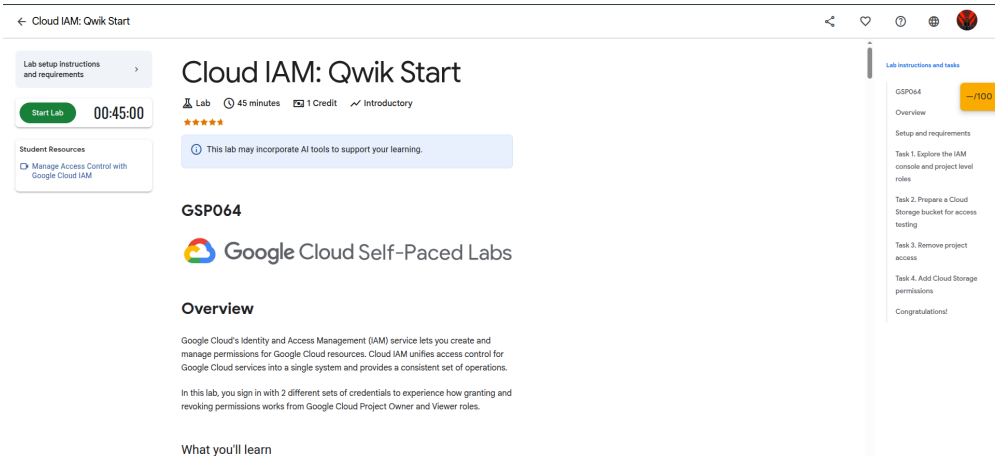

Figure 3.3 Step 3: Starting the IAM Quickstart lab.

4. **Retrieve user credentials generated by the lab.**

← Cloud IAM: Qwik Start

Lab setup instructions and requirements

Protect your account and progress. Always use a private browser window and lab credentials to run this lab.

End Lab 00:44:05

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

Username 1

student-04-38a13a2377a2

Username 2

student-04-1a3f3e31cb2a

Password

5. **Open Incognito and sign in to GCP with the lab user.**

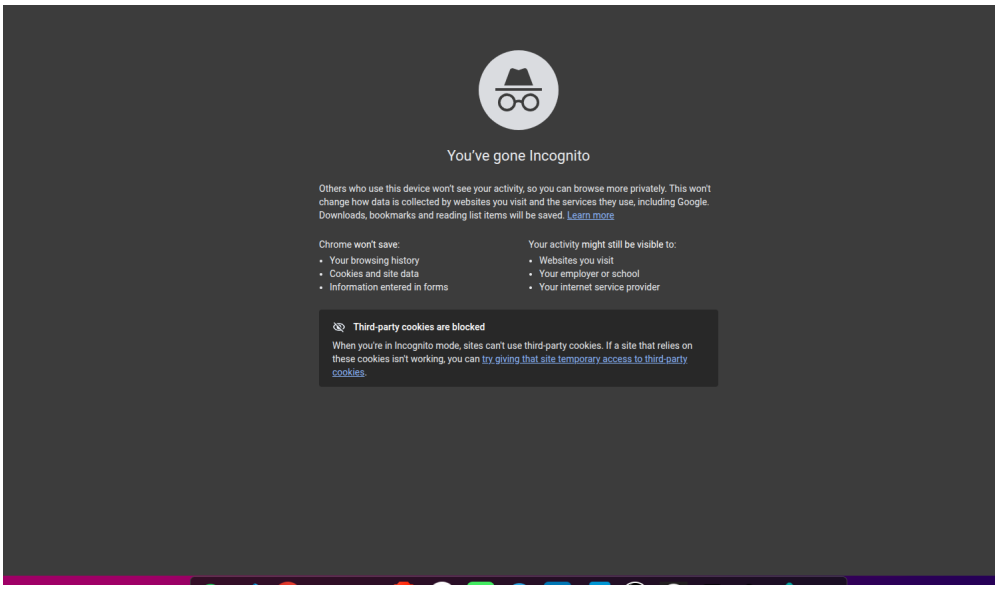

Figure 3.5 Step 5: Open Incognito browser.

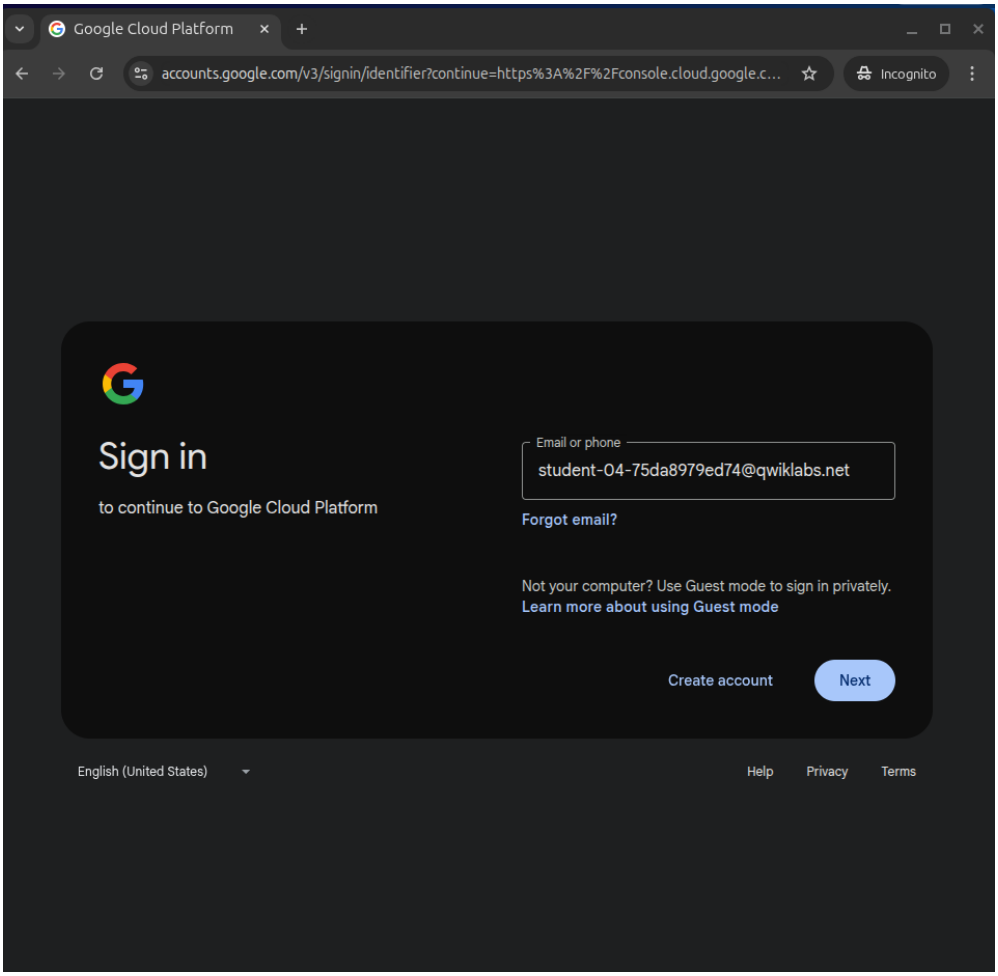

Figure 3.6 Step 6: Sign in with lab-generated user credentials.

6. **Navigate to IAM Quickstart lab dashboard.**

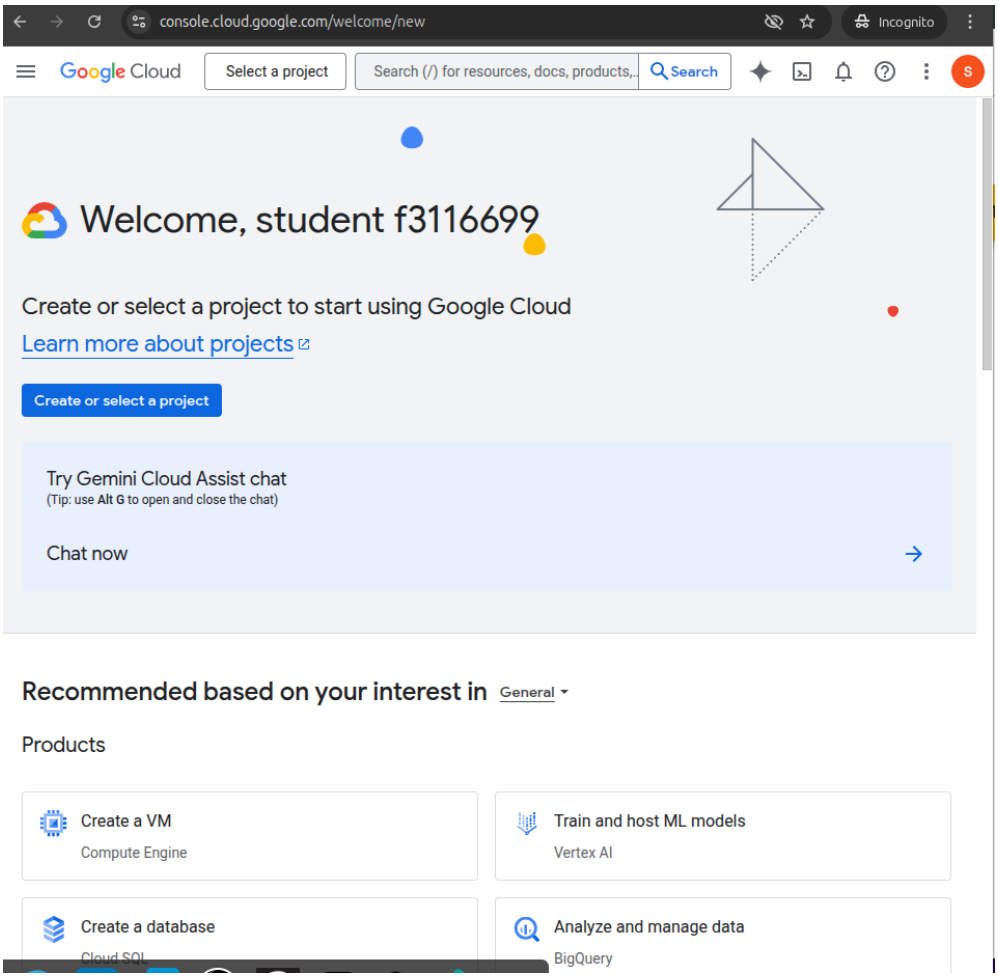

Figure 3.7 Step 7: Lab dashboard overview.

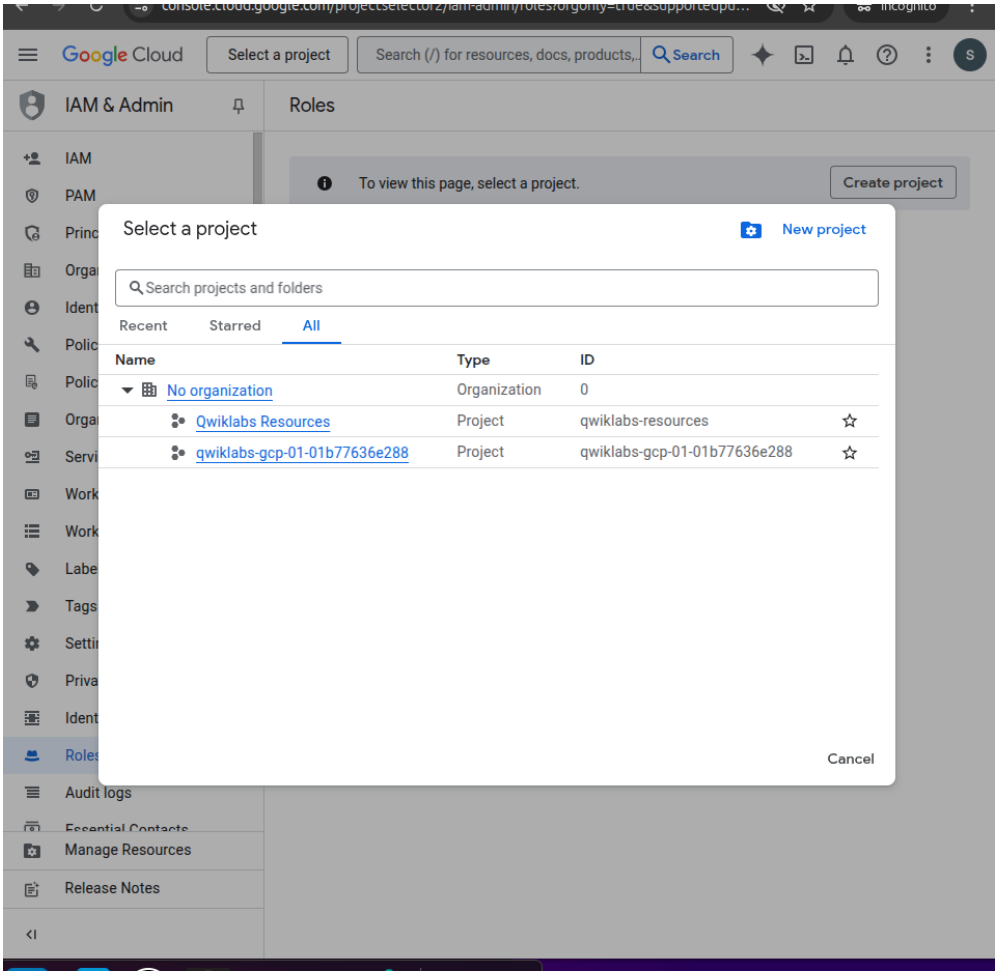

Figure 3.8 Step 8: Selecting the project for IAM tasks.

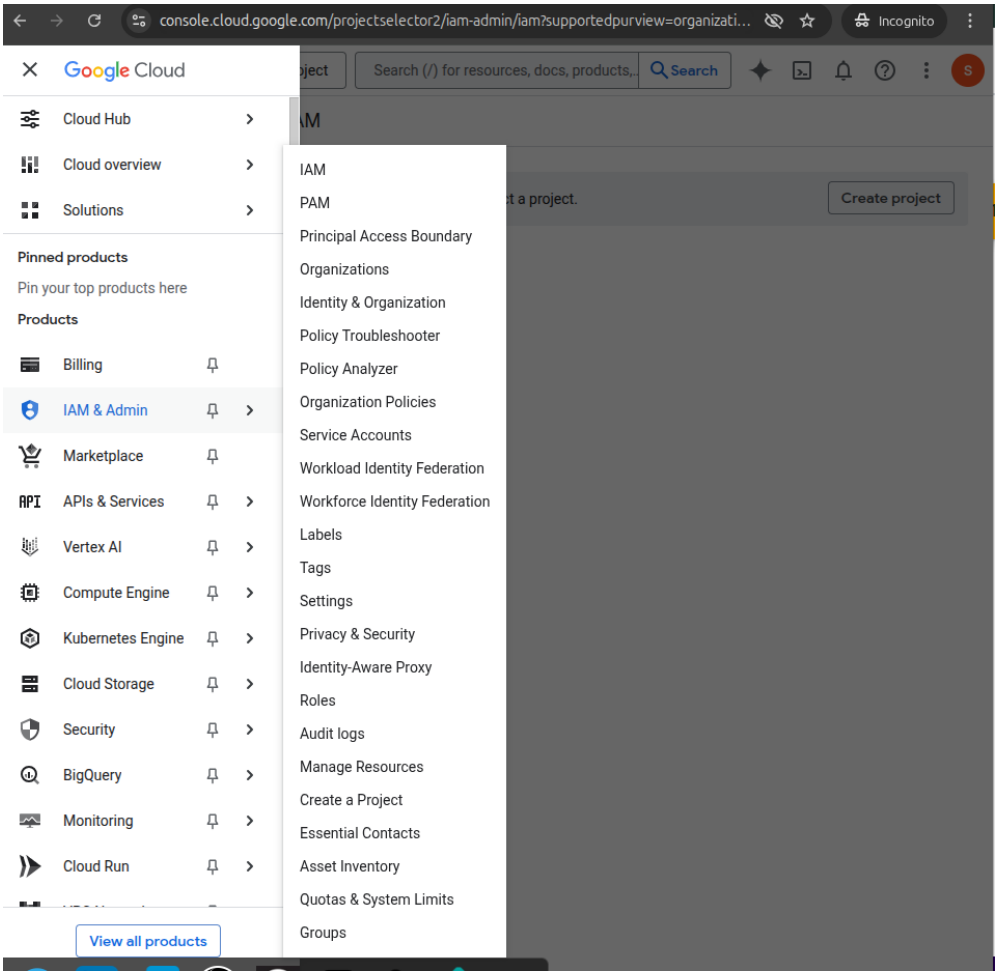

Figure 3.9 Step 9: Open IAM Admin from toggle menu.

7. **Create a Custom Viewer role.**

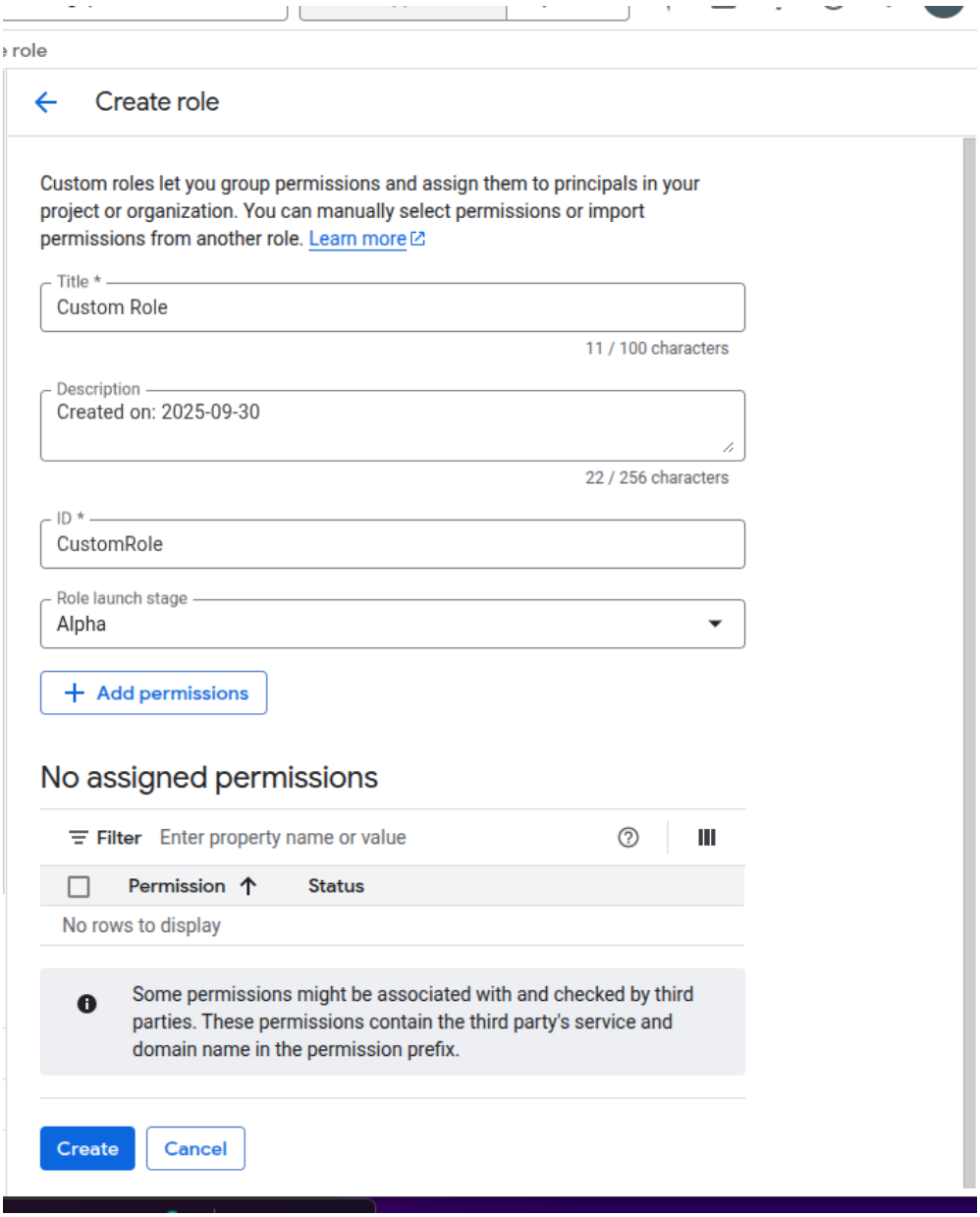

Figure 3.10 Step 10: Creating a custom role.

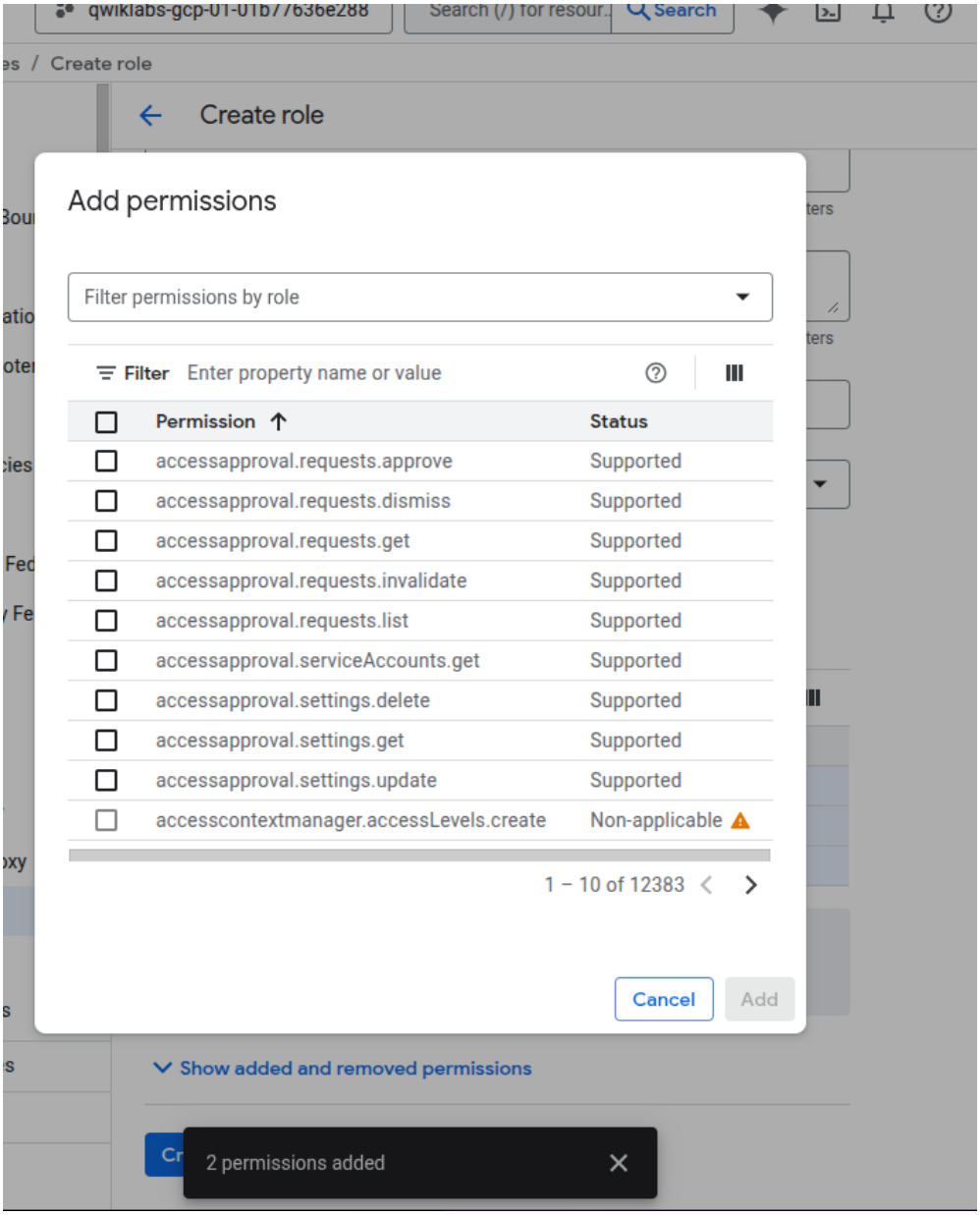

Figure 3.11 Step 11: Adding permissions to the custom role.

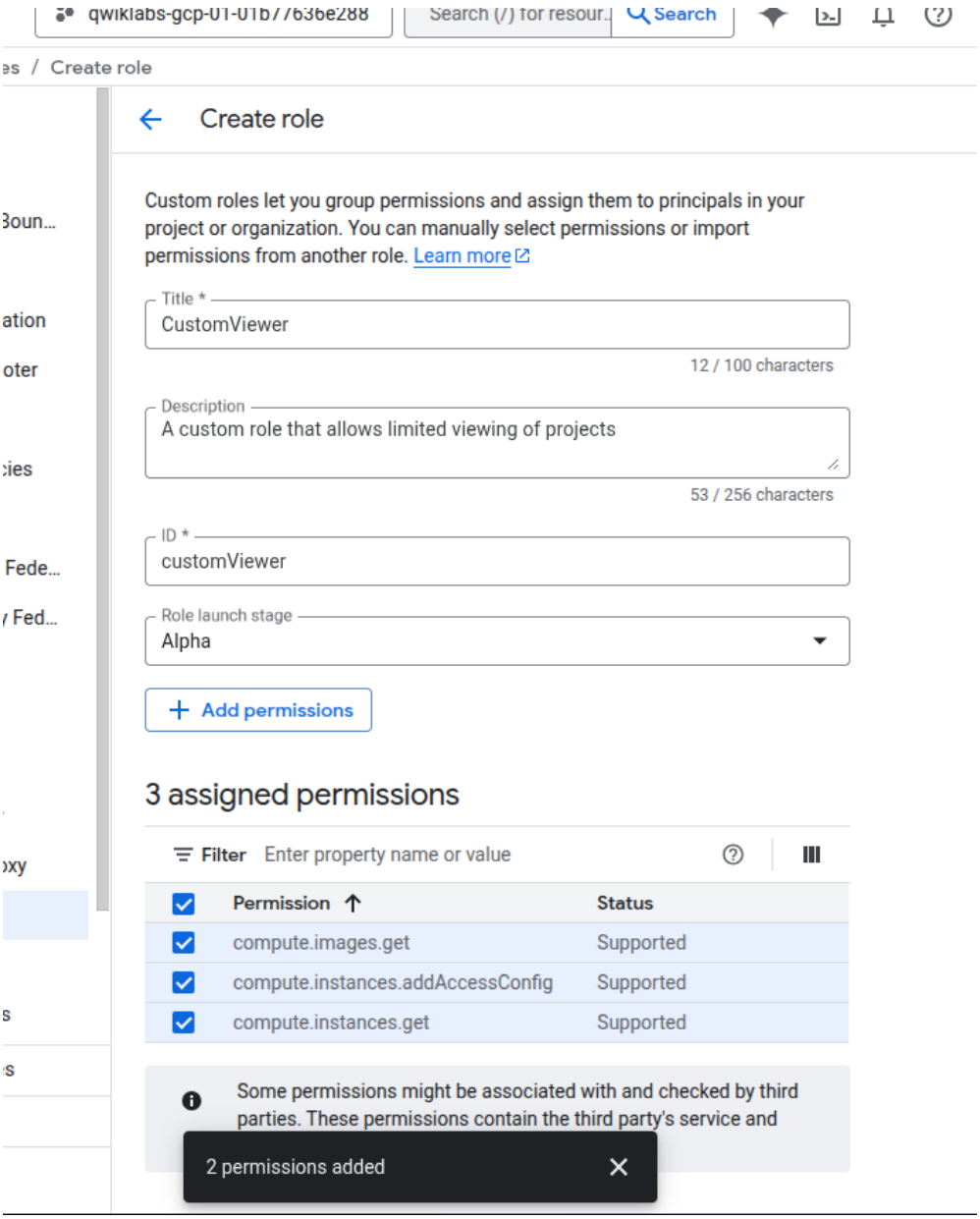

Figure 3.12 Step 12: Confirming permissions addition.

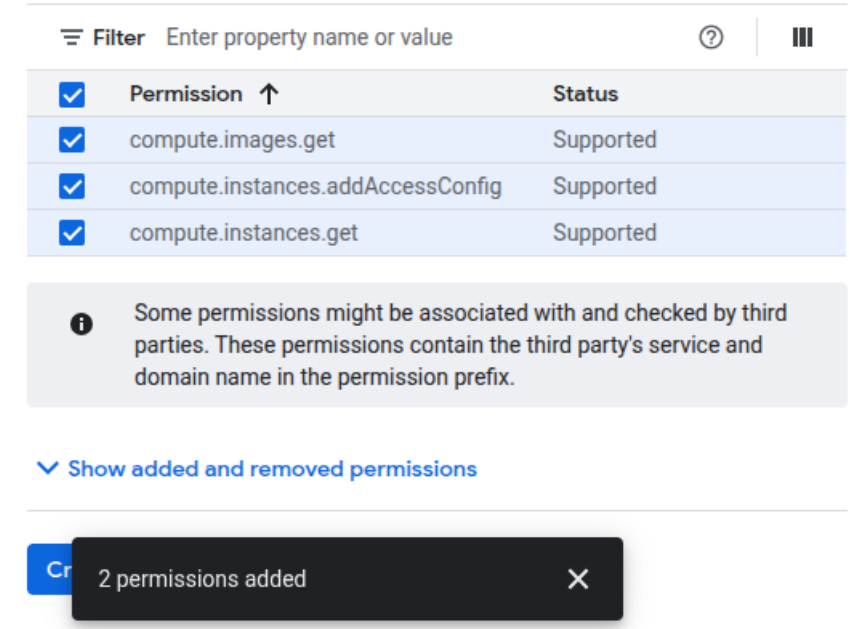

Figure 3.13 Step 13: Permissions successfully added.

8. **Assign the Custom Viewer role to a new principal.**

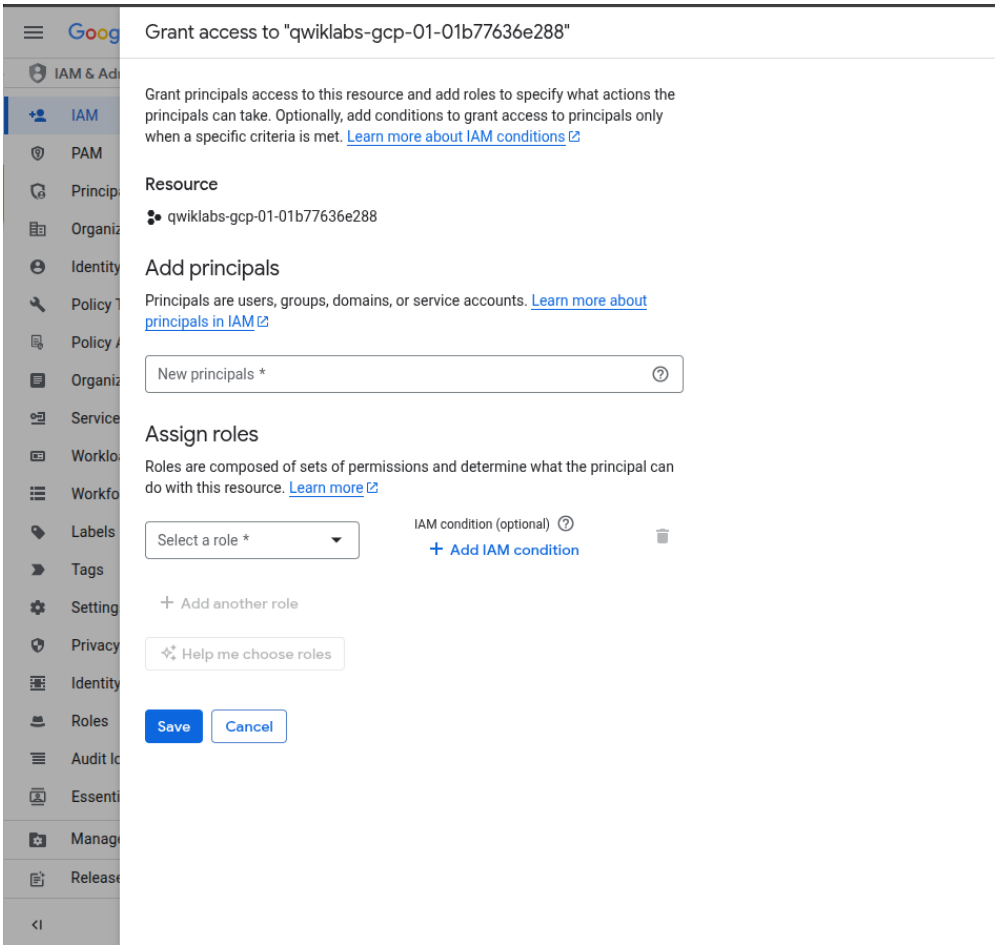

Figure 3.14 Step 14: Adding a new principal.

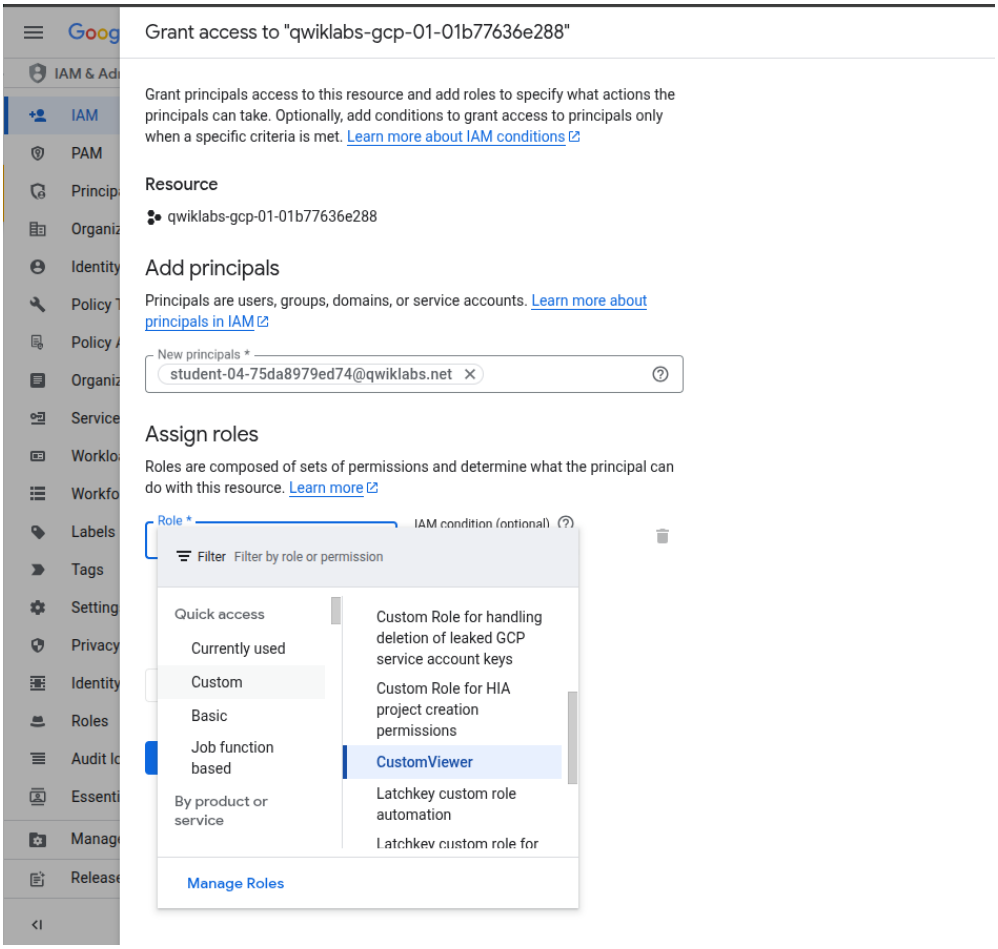

Figure 3.15 Step 15: Assigning the Custom Viewer role.

9. **Verify IAM policy and effective permissions.**

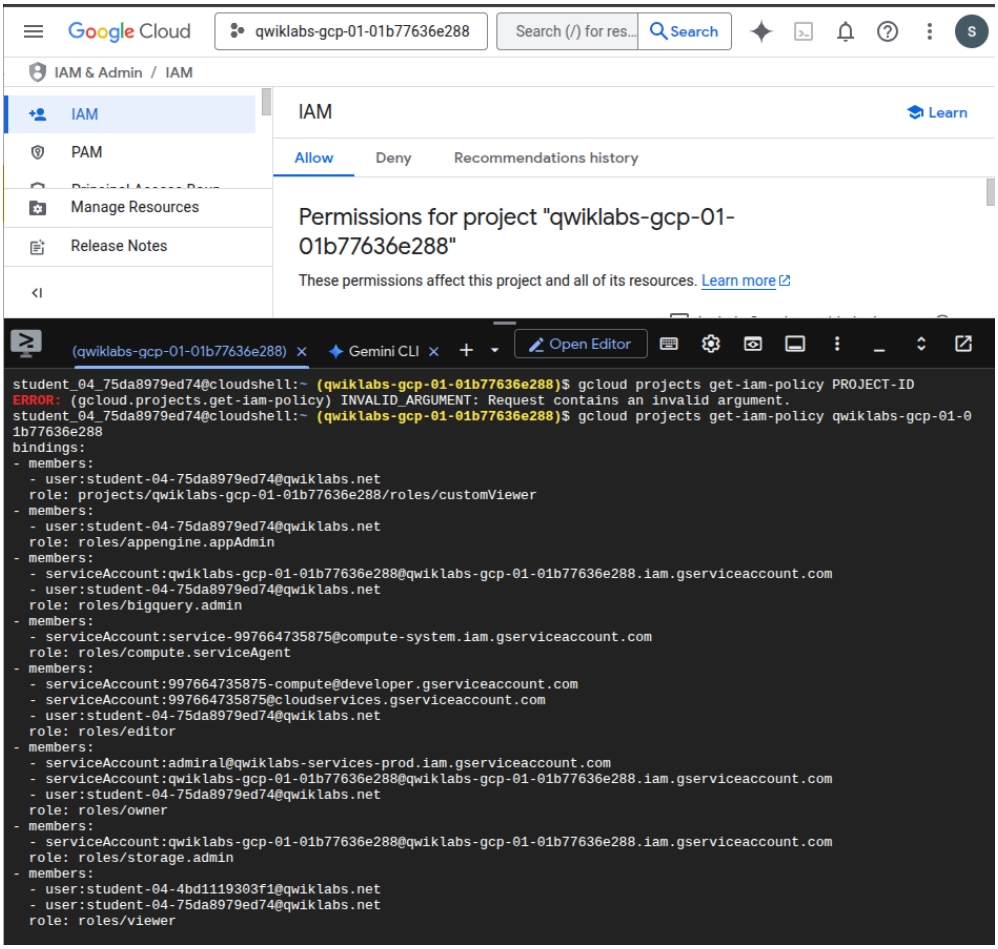

Figure 3.16 Step 16: Verifying IAM policy and effective permissions.

3.3 Analysis of Findings

- The lab demonstrated successful **Custom Viewer role creation and assignment**, illustrating proper implementation of the **principle of least privilege**.
- Verification of IAM policies confirmed **restricted read-only access**, preventing modification or deletion of project resources.
- The workflow emphasizes the importance of **auditing, monitoring, and role-based access management** for cloud security.

3.4 Practical Implications

Implementing custom IAM roles allows organizations to:

- Minimize risk from insider threats or human error.

- Provide temporary or restricted access for auditors or external consultants.
- Maintain compliance with internal security policies and regulatory requirements.

CHAPTER 4

DISCUSSION

4.1 Comparison with Literature

The hands-on implementation of IAM in GCP aligns with prior research on cloud security and access management. Studies highlight that misconfigured IAM policies are a leading cause of cloud security breaches. The lab demonstrated that using custom roles, like the Custom Viewer role, enforces the principle of least privilege, a best practice widely recommended in cloud security literature.

4.2 Strengths of the Analysis

The lab exercise successfully illustrated:

- Step-by-step creation and assignment of a **Custom Viewer role**, providing a practical understanding of IAM functionality.
- Verification of permissions using IAM policy tools and Cloud Shell, confirming that users have only the intended read-only access.
- The importance of **auditing and monitoring**, highlighting how IAM policies can be reviewed to ensure compliance and security.

4.3 Challenges and Limitations

While the lab provided practical exposure, certain limitations exist:

- Temporary lab accounts and environments do not fully simulate enterprise-scale complexities.
- The exercise focused on a single project and role type; real-world organizations manage multiple projects, service accounts, and complex role hierarchies.
- Cloud IAM policies can become complex, and errors in permission assignment may be hard to detect without automated auditing tools.

4.4 Implications

The exercise emphasizes that organizations must:

- Implement **least-privilege access** through custom roles to reduce risk of accidental or malicious changes.
- Continuously audit and monitor IAM policies to maintain secure access control.
- Train administrators and staff on best practices for IAM configuration and access management.

CHAPTER 5

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

The Google Cloud IAM Quickstart lab demonstrated how to create and assign a **Custom Viewer role** effectively. The exercise highlighted the importance of **role-based access control**, **principle of least privilege**, and proper verification of IAM policies. By following a structured workflow, the lab reinforced theoretical knowledge with hands-on practice, providing clear insights into cloud access management and secure operations.

5.2 Recommendations

- Organizations should design and implement **custom roles** for different user groups to ensure minimal necessary access.
- Regular audits of IAM policies should be conducted to identify and correct over-permissions or misconfigurations.
- Staff should receive **training on IAM best practices**, including role creation, permission assignment, and policy verification.
- Implement **monitoring and logging** mechanisms to track changes in IAM policies and resource access for accountability and security.

5.3 Future Research

Future work could explore:

- Developing automated tools for **IAM policy auditing** and anomaly detection in multi-project environments.
- Studying the effectiveness of **role-based access control** in preventing insider threats and accidental misconfigurations.
- Comparative analysis of **predefined vs. custom roles** across different cloud platforms to identify best practices.

- Integrating IAM policy management with **security information and event management (SIEM)** solutions for proactive monitoring.