PRACTICAL: 1

AIM:

A Virtual Private Cloud (VPC) network is a private cloud hosted within a public cloud, enabling organizations to use the public cloud's resources while being completely isolated from other cloud users. A VPC provides networking functionality to Compute Engine virtual machine (VM) instances, Kubernetes Engine containers, and other Google Cloud services. Each Google Cloud project by default has a default VPC network, which provides each region with an automatically-created subnet network. In this experiment, you'll learn how to use Cloud Shell to create a custom VPC network with subnets. Create a VPC using Cloud Shell.

THEORY:

Bucket: A virtual container that holds objects

Cloud computing refers to the practice of using on-demand computing resources as services hosted over the internet.

In cloud computing, an ***instance*** is a server resource that runs workloads in the cloud.

Ephemerality is the concept that things only exist for a short amount of time.

Virtualization is technology that creates a virtual version of physical infrastructure, such as servers, storage, and networks.

VMs contain their own operating systems, like Windows and Linux, and use only a portion of the underlying computer's compute power.

Virtualization uses ***hypervisors*** to manage the relationship between physical and virtual resources.

A ***hypervisor*** is the abstraction layer that sits between the physical computer and the VM.

The ***standard*** storage class is best for hot data, or data that you need to access frequently, and for short periods of time

Nearline storage is best for data that you only need to access up to once a month. Nearline is more cost effective than standard storage, and a good option for backing up your data.

Coldline storage is very cost effective because the data being stored is at rest for long periods of time

Archival storage is best for archiving or backing up data for disaster recovery purposes. This includes data that is accessed very infrequently, or once a year.

Container: A software package that holds only the components necessary to execute a particular application

Data center: A physical building that stores servers, computer systems, and associated components

Latency: The time it takes for data to travel from one location to another .

Multicloud: A strategy of using more than one cloud service provider

Multi-tenant environment: An environment in which cloud infrastructure and resources are shared among users

On-premises: Information technology infrastructure that's physically located in an organization's own data center or office

Private cloud: A cloud model in which all cloud resources are dedicated to a single user or organization, and are created, managed, and owned within on-premises data centers

Public cloud: A cloud model that delivers computing, storage, and network resources through the internet, allowing users to share on-demand resources

Redundancy: The practice of having multiple copies of data in different locations to avoid a single point of failure

Zone: The collective number of data centers in an area

Region: A group of zones Repository: A centralized place to store, download, and share data

Resiliency: The ability to prepare for, respond to, and recover from disruptions

Single-tenant environment: An environment in which cloud infrastructure and resources are dedicated to a single user

Structured data: Data organized in a certain format, like rows and columns

Unstructured data: Data that is not organized in any easily identifiable way

Virtual private cloud (VPC): A private cloud hosted within a public cloud, enabling organizations to use the public cloud's resources, while being completely isolated from other cloud users

DevSecOps: A culture that consists of guidelines, best practices, and tools that development, operation, and security teams use to collaborate

GitOps: A framework that applies version control, collaboration, compliance, and CI/CD best practices to automate cloud infrastructure

Infrastructure as code (IaC): The practice of automating and managing infrastructure using reusable scripts

CODE:

- gcloud auth list

The gcloud auth list command lists all authenticated Google Cloud accounts and indicates the currently active one.

- gcloud compute networks create labnet --subnet-mode=custom

Use the gcloud compute networks create labnet --subnet-mode=custom command to create a custom VPC network for setting up your test environment in Google Cloud.

- gcloud compute networks subnets create labnet-sub \
  --network labnet \
  --region "REGION" \
  --range 10.0.0.0/28

Use the gcloud compute networks subnets create labnet-sub --network labnet --region "REGION" --range 10.0.0.0/28 command to create a subnet named labnet-sub within the labnet VPC network in the specified region, with the IP range 10.0.0.0/28.

- gcloud compute networks list

This command will list all the networks in your Google Cloud project.

OUTPUT:

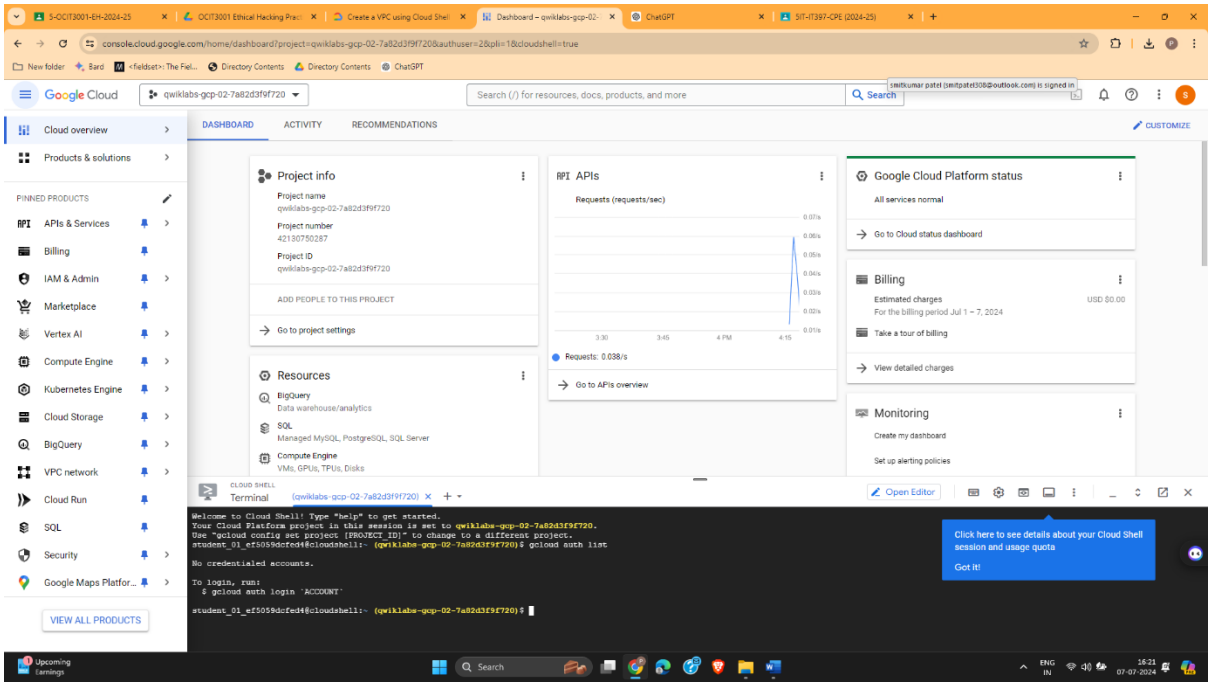


Figure 1: This figure shows the list of all authenticated Google Cloud accounts and indicates the currently active one.

```
student_01_ef5059dcfed4@cloudshell:~ (qwiklabs-gcp-02-7a82d3f9f720)$ gcloud compute networks create labnet --subnet-mode=cust
Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-02-7a82d3f9f720/global/networks/labnet].
NAME: labnet
SUBNET_MODE: CUSTOM
BGP_ROUTING_MODE: REGIONAL
IPV4_RANGE:
GATEWAY_IPV4:

Instances on this network will not be reachable until firewall rules
are created. As an example, you can allow all internal traffic between
instances as well as SSH, RDP, and ICMP by running:

$ gcloud compute firewall-rules create <FIREWALL_NAME> --network labnet --allow tcp,udp,icmp --source-ranges <IP_RANGE>
$ gcloud compute firewall-rules create <FIREWALL_NAME> --network labnet --allow tcp:22,tcp:3389,icmp
```

Figure 2 : This figure shows the creation of a custom VPC network named 'labnet' for setting up your test environment in Google Cloud.

```
student_01_ef5059dcfed4@cloudshell:~ (qwiklabs-gcp-02-7a82d3f9f720)$ gcloud compute networks subnets create labnet-sub \
   --network labnet \
   --region us-central1 \
   --range 10.0.0.0/28
Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-02-7a82d3f9f720/regions/us-central1/subnetworks/labnet-sub].
NAME: labnet-sub
REGION: us-central1
NETWORK: labnet
RANGE: 10.0.0.0/28
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:
student_01_ef5059dcfed4@cloudshell:~ (qwiklabs-gcp-02-7a82d3f9f720)$
```

Figure 3 : This figure shows the creation of a subnet named 'labnet-sub' within the 'labnet' VPC network in the specified region, with the IP range 10.0.0.0/28.

```
student_01_ef5059dcfed4@cloudshell:~ (qwiklabs-gcp-02-7a82d3f9f720)$ gcloud compute networks subnets list --network=labnet
NAME: labnet-sub
REGION: us-central1
NETWORK: labnet
RANGE: 10.0.0.0/28
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:
student_01_ef5059dcfed4@cloudshell:~ (qwiklabs-gcp-02-7a82d3f9f720)$
```

Figure 4: This figure shows the list of all networks in your Google Cloud project.

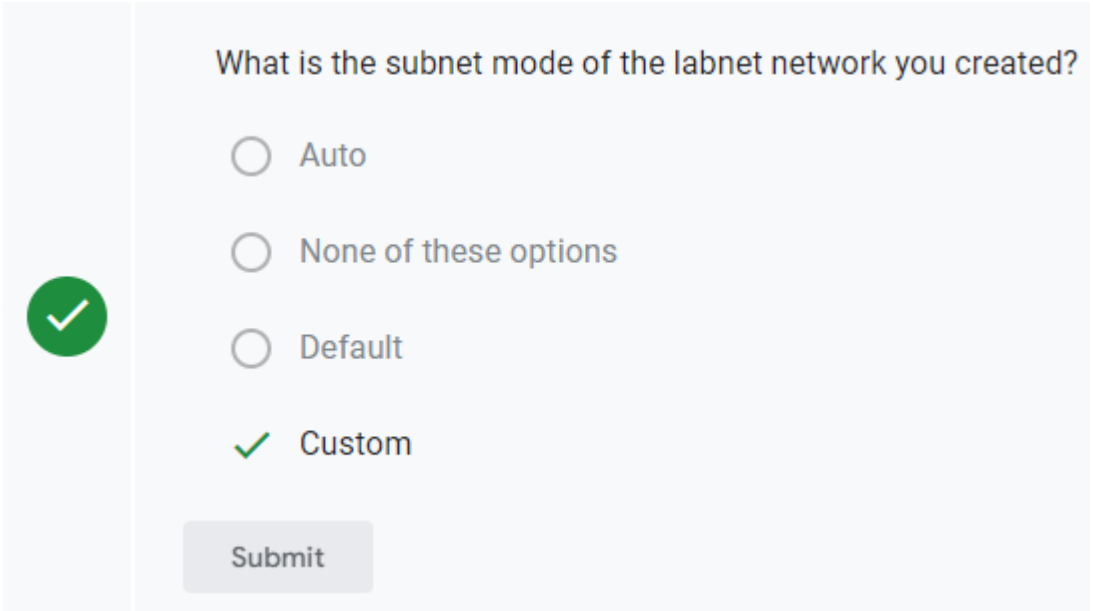


Figure 5 MCQ which is in the lab section

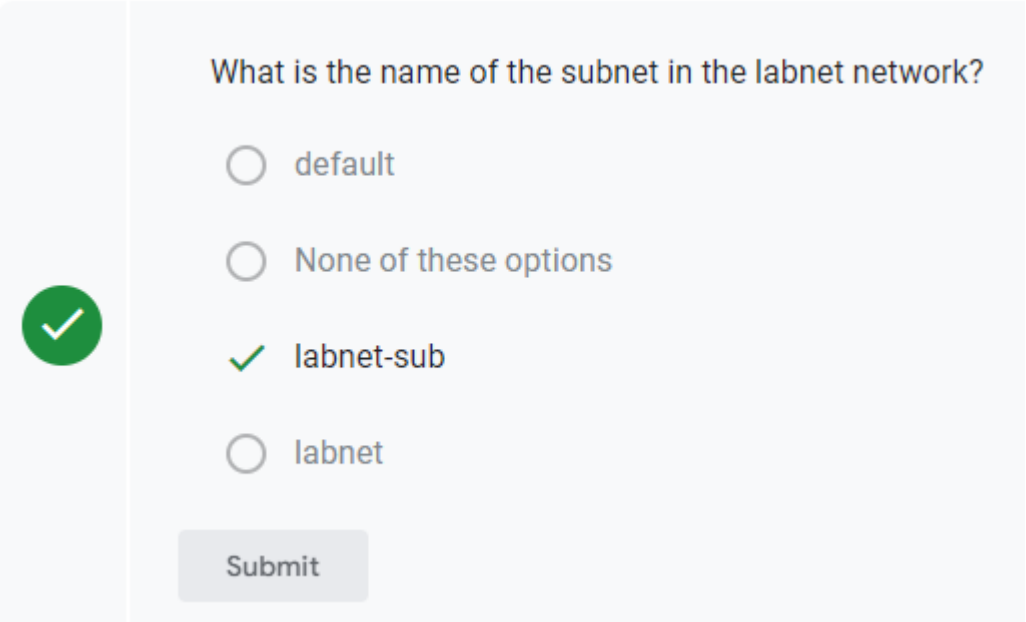


Figure 6 MCQ which is in the lab section

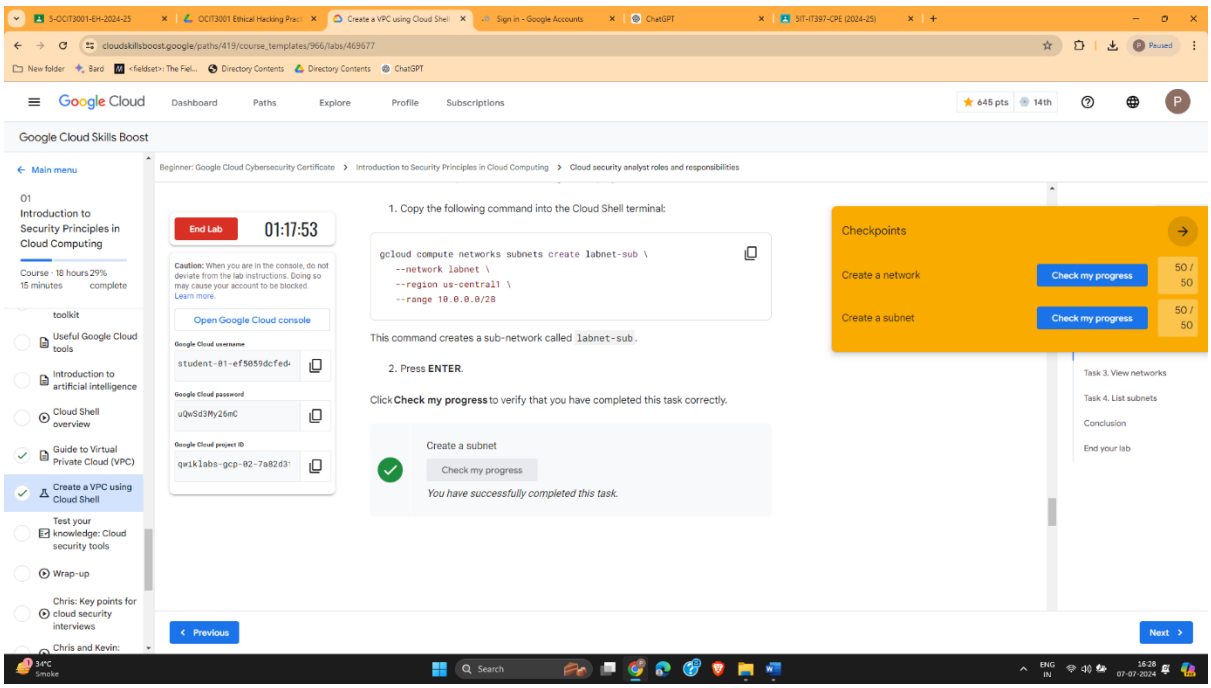


Figure 7 This figure shows the completion of my Google Cloud lab.

LATEST APPLICATIONS:

Cloud-Native Application Deployment: Deploy containerized applications and manage microservices with secure, isolated environments using custom VPCs and subnets.
Data Analytics and Machine Learning: Create isolated networks for data privacy and optimize configurations for high-performance computing.
Hybrid and Multi-Cloud Strategies: Enable secure interconnectivity between on-premises data centers and Google Cloud, and manage multi-cloud integrations.
DevOps and CI/CD: Set up dedicated networks for different CI/CD stages and integrate with IaC tools for automated network resource management.

LEARNING OUTCOME:

During this practical session, I gained valuable insights into key cloud computing concepts. We concluded by emphasizing the critical role networks play in IT infrastructure.

Setting up and configuring Virtual Private Cloud (VPC) networks in a cloud environment can be straightforward, involving just a few clicks or command-line instructions.

However, it's crucial to meticulously configure VPCs to adhere to an organization's security standards, employing measures such as firewall rules, network segmentation, and other security controls.

REFERENCES:

1. cloud shell of goole: https://youtu.be/NWosqZY1r10

PRACTICAL: 2

AIM:

Reports are essential for helping remediate findings, especially for cybersecurity, compliance, and quality assurance. These reports often highlight vulnerabilities, issues, or non-compliance with established standards. By analyzing these reports, you can identify areas for improvement and gather data-driven evidence to make informed decisions. Concrete data enables efficient prioritization and resource allocation to address the identified issues. Consequently, addressing the findings outlined in reports helps mitigate potential risks and vulnerabilities that could otherwise be exploited. This is especially critical in cybersecurity, where unaddressed issues can lead to data breaches or system compromises. As a security analyst, you are responsible for evaluating controls against established standards to ensure that an organization's security posture is effective, compliant, and aligned with industry best practices. This evaluation process is crucial for helping with risk management, compliance, and continuous security improvement, ultimately helping organizations protect sensitive data, systems, and their overall reputation. In this experiment, you'll use the Security Command Center interface to identify and remediate threats and vulnerabilities and confirm that the issues have been resolved.

THEORY:

Google Cloud Security Command Center (SCC):

Overview: Google Cloud SCC is a security and risk management platform that helps you prevent, detect, and respond to threats. It provides a centralized view of your cloud assets, vulnerabilities, and threats.

Components: SCC consists of assets, findings, and security marks. Assets are resources in your Google Cloud project, findings are potential security issues, and security marks are labels for categorizing assets and findings.

Creating and Managing VPC Networks:

VPC (Virtual Private Cloud): A VPC is a private network space within Google Cloud where you can deploy your resources.

Subnets: Subnets divide your VPC network into smaller segments. You can control IP address ranges and regions for each subnet.

Network Security:

Firewall Rules: Firewall rules control traffic to and from your instances. They can be applied to specific instances or network tags.

IAM (Identity and Access Management): IAM manages who can do what on Google Cloud. It provides granular access control to resources.

Monitoring and Logging:

Stackdriver: Stackdriver is Google Cloud's monitoring and logging service. It helps you track the performance and health of your applications and infrastructure.

Audit Logs: These logs provide a record of actions taken on your Google Cloud resources. They are essential for security and compliance.

Threat Detection and Response:

Vulnerability Scanning: Identify security weaknesses in your applications and infrastructure.

Incident Response: Steps to take when a security threat is detected, including containment, eradication, and recovery.

Compliance and Best Practices:

Standards and Frameworks: Familiarity with common security standards such as ISO 27001, NIST, and GDPR.

Best Practices: Implementing industry best practices for cloud security, such as the Principle of Least Privilege, encryption, and regular audits.

Infrastructure as code (IaC): The practice of automating and managing infrastructure using reusable scripts

Non-compliance: The failure to follow standards and regulations that are set by internal standards and policy, or external laws and regulations

Policy as code (PaC): The use of code to define, manage, and automate policies, rules, and conditions using a high-level programming language

OUTPUT:

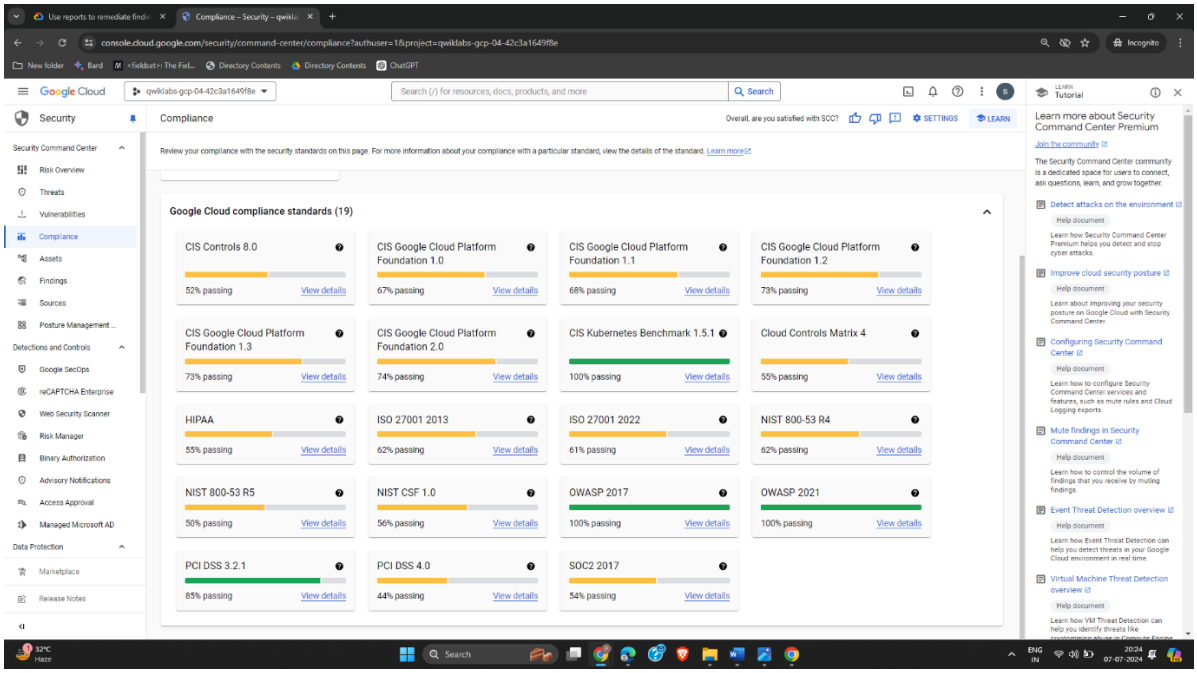
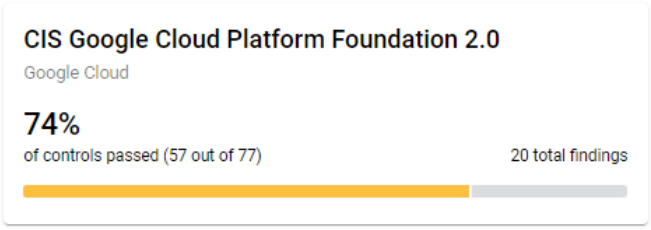


Figure 1 This figure shows that I click Compliance in the Security Command Center menu to open the Compliance page.

Status	Last scanned	Category	Module ID	Recommendation	Active findings
⚠	July 7, 2024 at 5:59:44 PM GMT+5	Public IP address	PUBLIC_IP_A...	VMs should not be assigned public IP addresses	1
⚠	July 7, 2024 at 5:59:44 PM GMT+5	Compute secure boot disabled	COMPUTE_S...	Instances that are compatible with Secure Boot should have it enabled	1
⚠	July 7, 2024 at 5:59:52 PM GMT+5	Default service account used	DEFAULT_SE...	Instances should not be configured to use the default service account	1
⚠	July 7, 2024 at 5:59:45 PM GMT+5	Full API access	FULL_API_AC...	Instances should not be configured to use the default service account with full	1

Figure 2 This figure shows that I click on Vulnerabilities in the Security Command Center menu to open the Vulnerabilities page.



Filter Enter property name or value

Rule	Severity	Findings	Controls
Corporate login credentials should be used instead of Gmail accounts	High	0	1.1
Multi-factor authentication should be enabled for all users in your org unit	High	0	1.2
User-managed service accounts should not have user managed keys	Medium	1	1.4
ServiceAccount should not have Admin privileges	Medium	1	1.5
The iam.serviceAccountUser and iam.serviceAccountTokenCreator roles should not be assigned to a user at the project level	Medium	0	1.6
Service account keys should be rotated every 90 days or less	Medium	0	1.7
Separation of duties should be enforced while assigning service account related roles to users	Medium	0	1.8
Cloud KMS cryptokeys should not be publicly accessible by anyone on the internet	High	0	1.9
Encryption keys should be rotated within a period of 90 days	Medium	0	1.10
Users should not have "Owner" permissions on a project that has cryptographic keys	Medium	0	1.11

Figure 3 This figure shows that I click View details in the CIS Google Cloud Platform Foundation 2.0 tile to open the report.

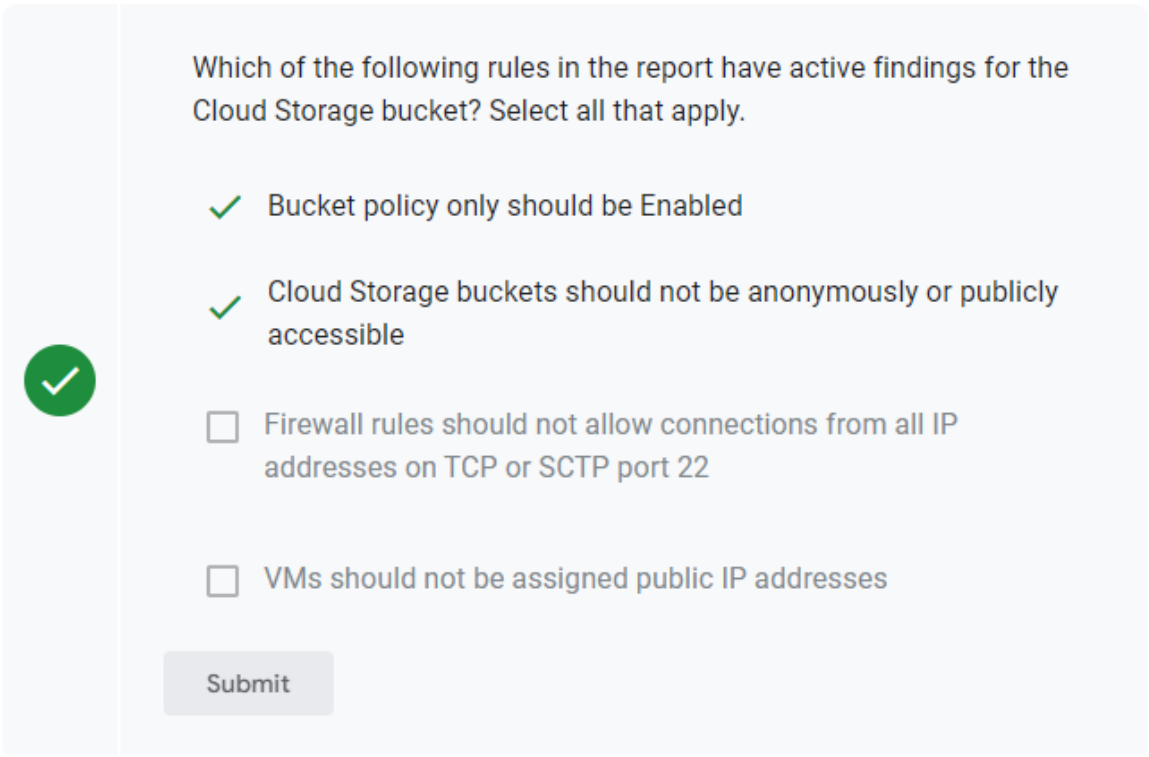


Figure 4 MCQ IN LAB

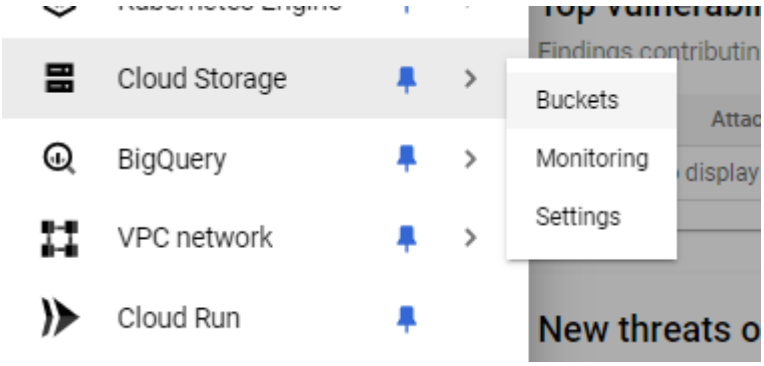


Figure 5 This figure shows that I navigate to Cloud Storage > Buckets from the Google Cloud console's Navigation menu.

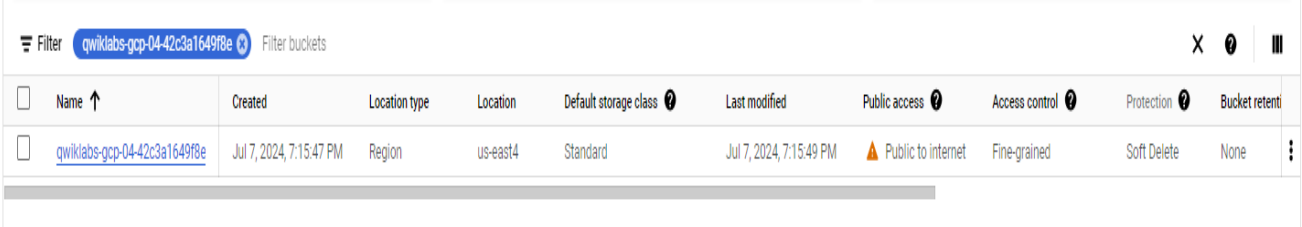


Figure 6 This figure shows that I click the Name link of the bucket for my project under the Filter section to open the Bucket details page.

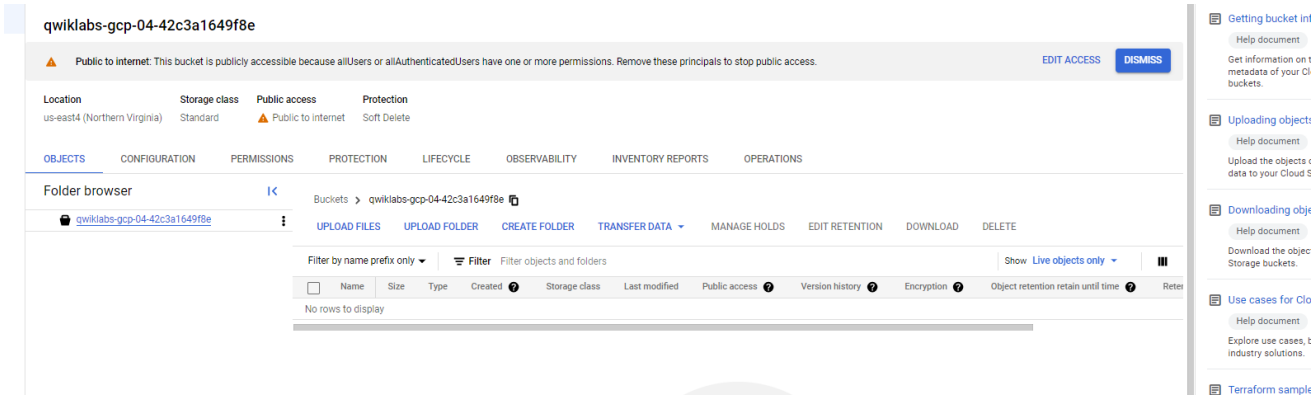


Figure 7 This figure shows that I click the Permissions tab to view all the permissions provided for the bucket.

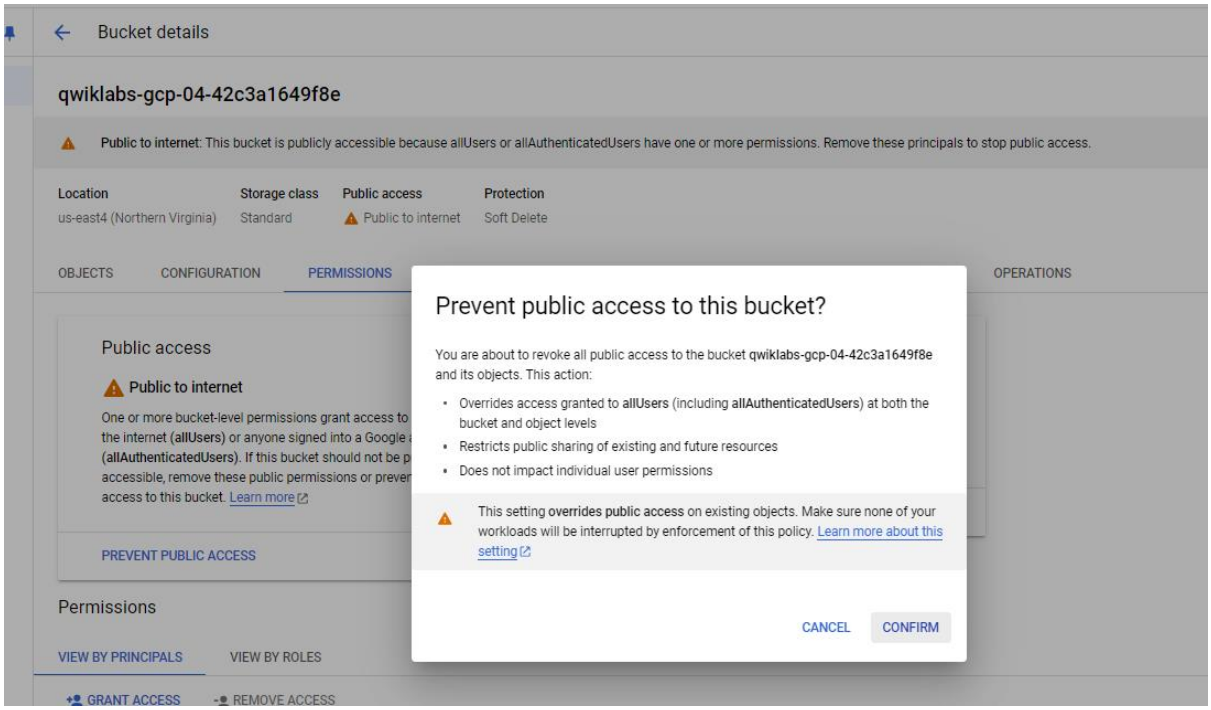


Figure 8 This figure shows that I remove the public access to the Cloud Storage bucket.

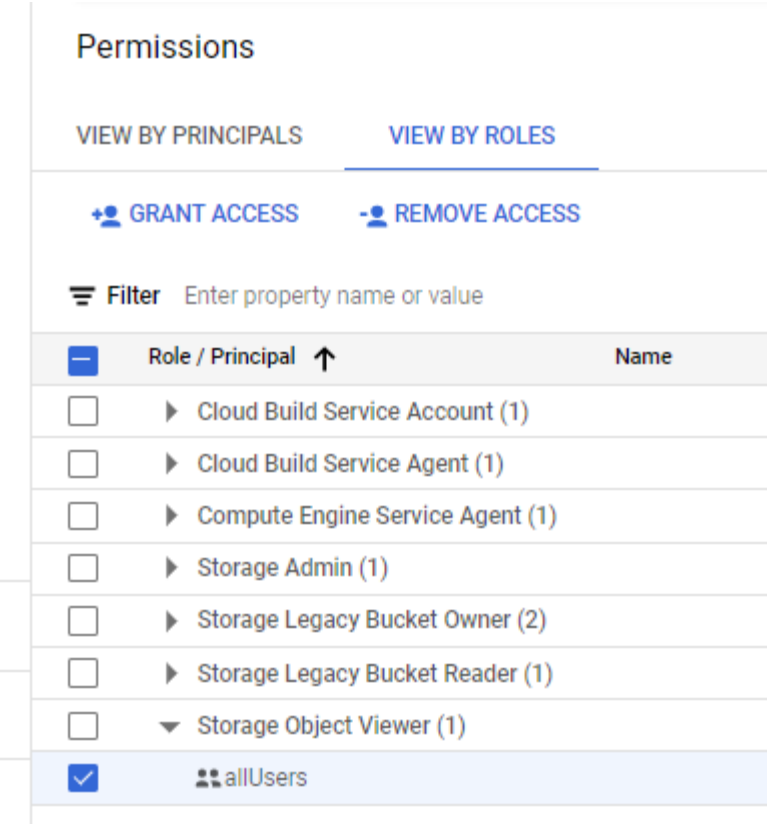


Figure 9 This figure shows that I click the View by Roles tab, expand the Storage Object Viewer role, select the checkbox for allUsers, and click Remove Access.

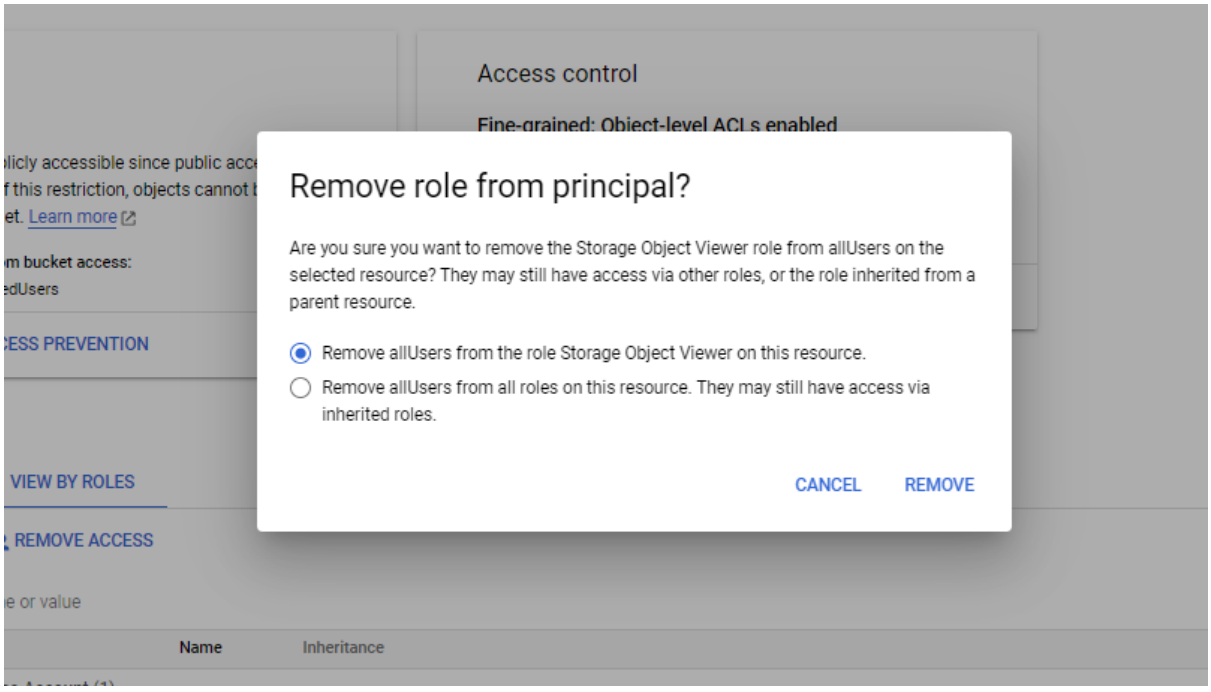


Figure 10 This figure shows that I confirm the removal of allUsers from the role Storage Object Viewer by ensuring the correct option is selected and clicking Remove.

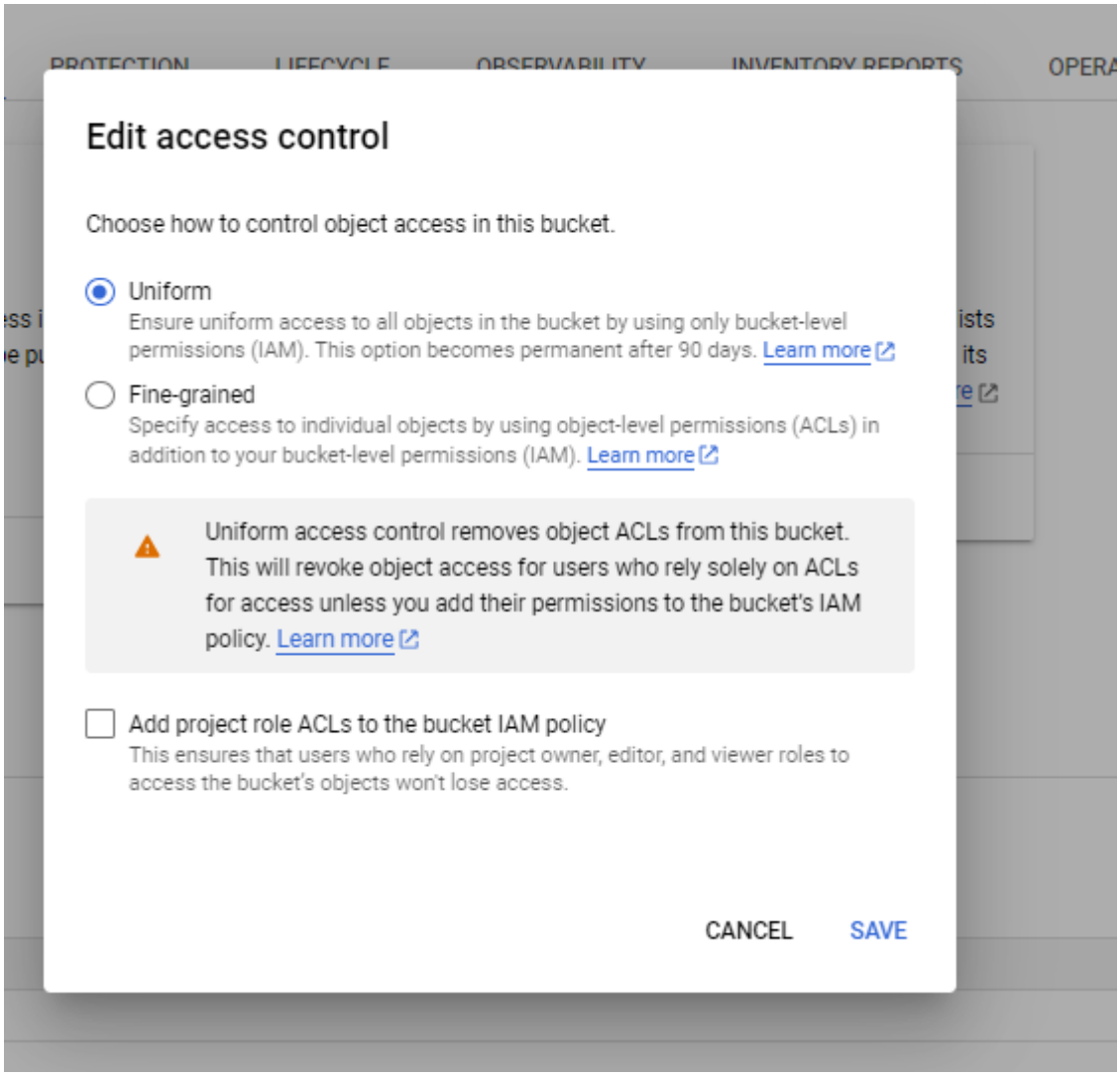


Figure 11 This figure shows that I select Uniform on the Edit access control dialog and click Save.

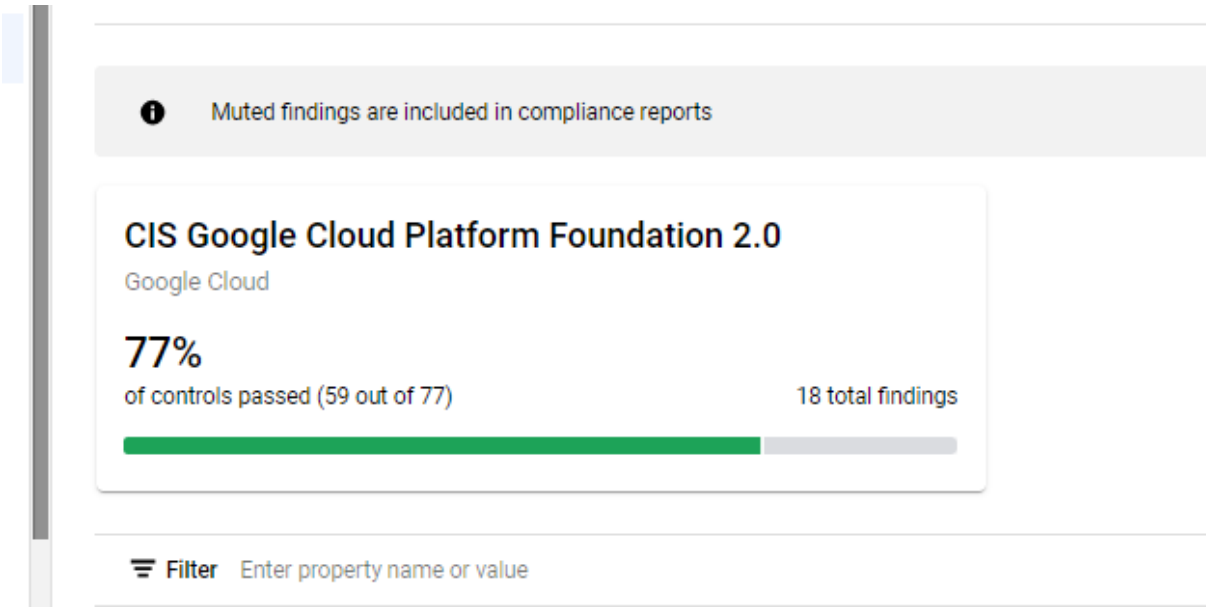


Figure 12 This figure shows that I click View details in the CIS Google Cloud Platform Foundation 2.0 tile to view the compliance report again.

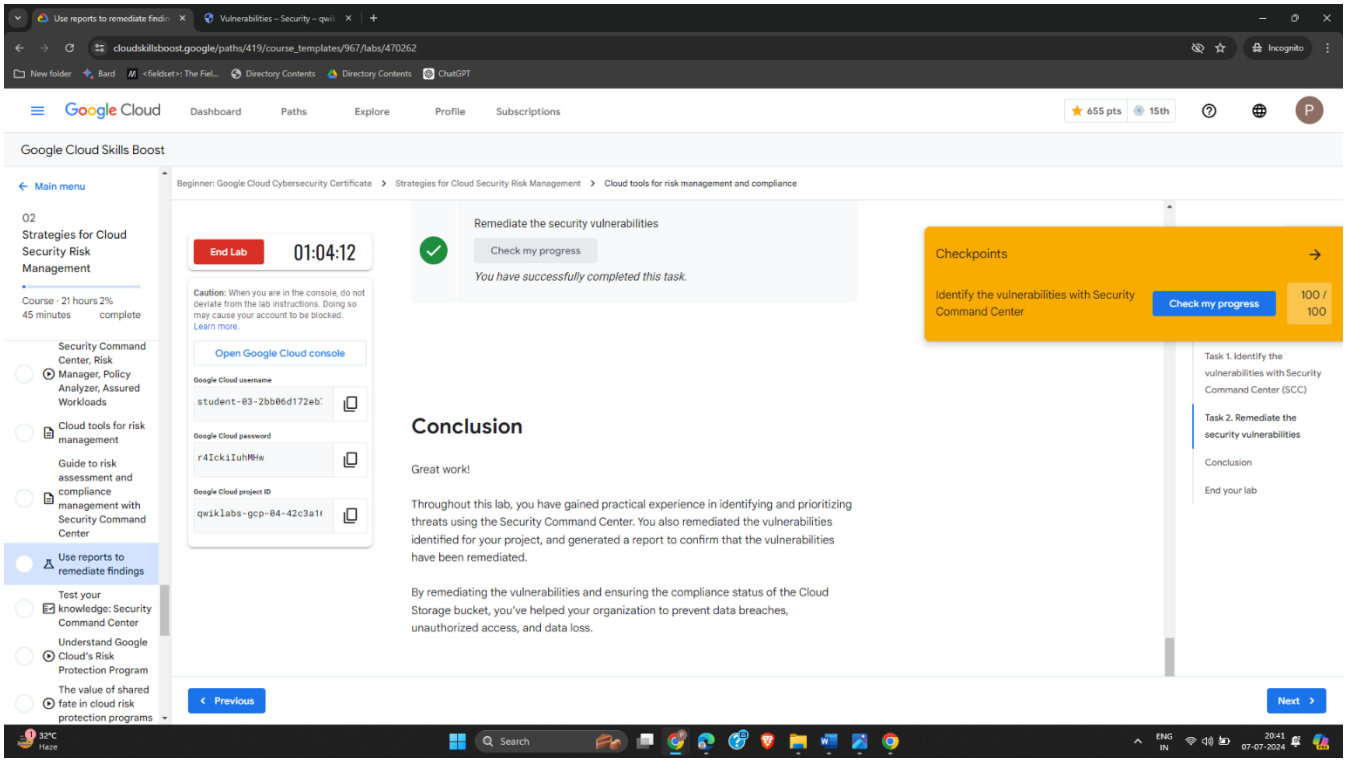


Figure 13 This figure shows the completion of my Google Cloud lab.

LATEST APPLICATIONS:

Enhanced Security Posture: Organizations use SCC to monitor and manage security threats and vulnerabilities, ensuring compliance and protecting data (e.g., a financial institution protecting customer data).

Risk Management: SCC helps identify and mitigate risks before exploitation, preventing breaches (e.g., an e-commerce platform addressing vulnerabilities).

Incident Response: SCC enables quick detection and response to security incidents, minimizing damage (e.g., a healthcare provider ensuring HIPAA compliance).

Compliance: SCC ensures organizations meet industry standards and regulatory requirements (e.g., a multinational corporation complying with GDPR and CCPA).

LEARNING OUTCOME:

By completing this lab, I will learn to navigate and utilize the Google Cloud Security Command Center (SCC), gaining insights into its key features like asset inventory, findings, and security marks.

I'll develop skills in identifying and remediating threats and vulnerabilities, enhancing my incident response and vulnerability management capabilities.

Additionally, I'll understand the importance of compliance and best practices in cloud security, learning to evaluate controls against established standards to ensure a robust security posture.

REFERENCES:

1 Security Command Center: https://youtu.be/mdmAlNpabkU

2 Risk Manager: https://youtu.be/n-bMYx71lRQ

PRACTICAL: 3

AIM:

IAM, or Identity and Access Management, is a collection of processes and technologies that help organizations manage digital identities in their environment. With IAM, access control is managed by defining the identity of users and their roles in relation to available resources. Resource access permissions are not granted directly to individual users. Instead, users are assigned to roles that are then given to authenticated principals. While the term "members" was used in the past, IAM now refers to these individuals as principals, although some APIs still use the previous terminology. There are three types of IAM roles in Google Cloud: Basic roles: Roles historically available in the Google Cloud console. These roles are Owner, Editor, and Viewer. Predefined roles: Roles that give finer-grained access control than the basic roles. For example, the predefined role Pub/Sub Publisher (roles/pubsub. publisher) provides access to only publish messages to a Pub/Sub topic. Custom roles: Roles that you create to tailor permissions to the needs of organization when predefined roles don't meet your needs. In this experiment, you'll learn how to create and manage Identity and Access Management (IAM) custom roles.

THEORY:

Identity and Access Management (IAM)

Overview

Identity and Access Management (IAM) is a collection of processes and technologies that help organizations manage digital identities within their environment. IAM ensures that the right individuals have appropriate access to technology resources. This involves defining identities, managing roles, and ensuring secure access to resources.

Key Components

1. **Role-Based Access Control (RBAC)**
    - **Definition**: A method of controlling access to resources based on user roles.
    - **Purpose**: Ensures users only have permissions necessary for their job functions.
    - **Benefits**: Streamlines permission management and enhances security by reducing the risk of unauthorized access.
2. **Single Sign-On (SSO)**
    - **Definition**: A technology that allows users to access multiple applications using a single set of credentials.
    - **Purpose**: Simplifies the authentication process and minimizes password fatigue.
    - **Benefits**: Enhances user experience and reduces the risk of credential-related security issues.
3. **Multifactor Authentication (MFA)**
    - **Definition**: A security measure requiring users to verify their identity in two or more ways to access a system.
    - **Purpose**: Adds an extra layer of security by requiring multiple methods of authentication.

   - **Examples**: Password combined with a fingerprint scan or a one-time code sent to a phone.
4. **Authentication, Authorization, and Auditing (Triple A Framework)**
   - **Authentication**: Verifying who someone is.
   - **Authorization**: Granting access to specific resources based on roles.
   - **Auditing**: Recording and reviewing system activity to ensure compliance and identify potential security breaches.

Auditing

- **Purpose**: Ensure deviations from expected behavior are identified and addressed.
- **Types**: Compliance audits, security audits, and operational audits.

Credential and Secrets Management

- **Best Practices**:
  - Use centralized secret management tools.
  - Apply strong encryption methods.
  - Regularly rotate API keys, passwords, and certificates.

Non-Interactive Access

- **Definition**: Accounts used for automated processes.
- **Risks**: If not properly managed, these accounts can be entry points for malicious actors.
- **Mitigation**: Regularly review and audit these accounts, rotate keys, and limit privileges.

Security Protocols

- **mTLS (Mutual Transport Layer Security)**
  - Provides mutual authentication and encryption between servers.
  - Ensures secure and private communication.
- **OAuth (Open Authorization)**
  - Allows users to grant applications access to their information without sharing passwords.
- **OpenID**
  - Used for single sign-on functionality.
  - Simplifies login processes and reduces password fatigue.

IAM Roles in Google Cloud

- **Basic Roles**: Owner, Editor, Viewer.
- **Predefined Roles**: Roles with finer-grained access control (e.g., Pub/Sub Publisher).
- **Custom Roles**: Tailored roles to meet specific organizational needs.

OUTPUT:

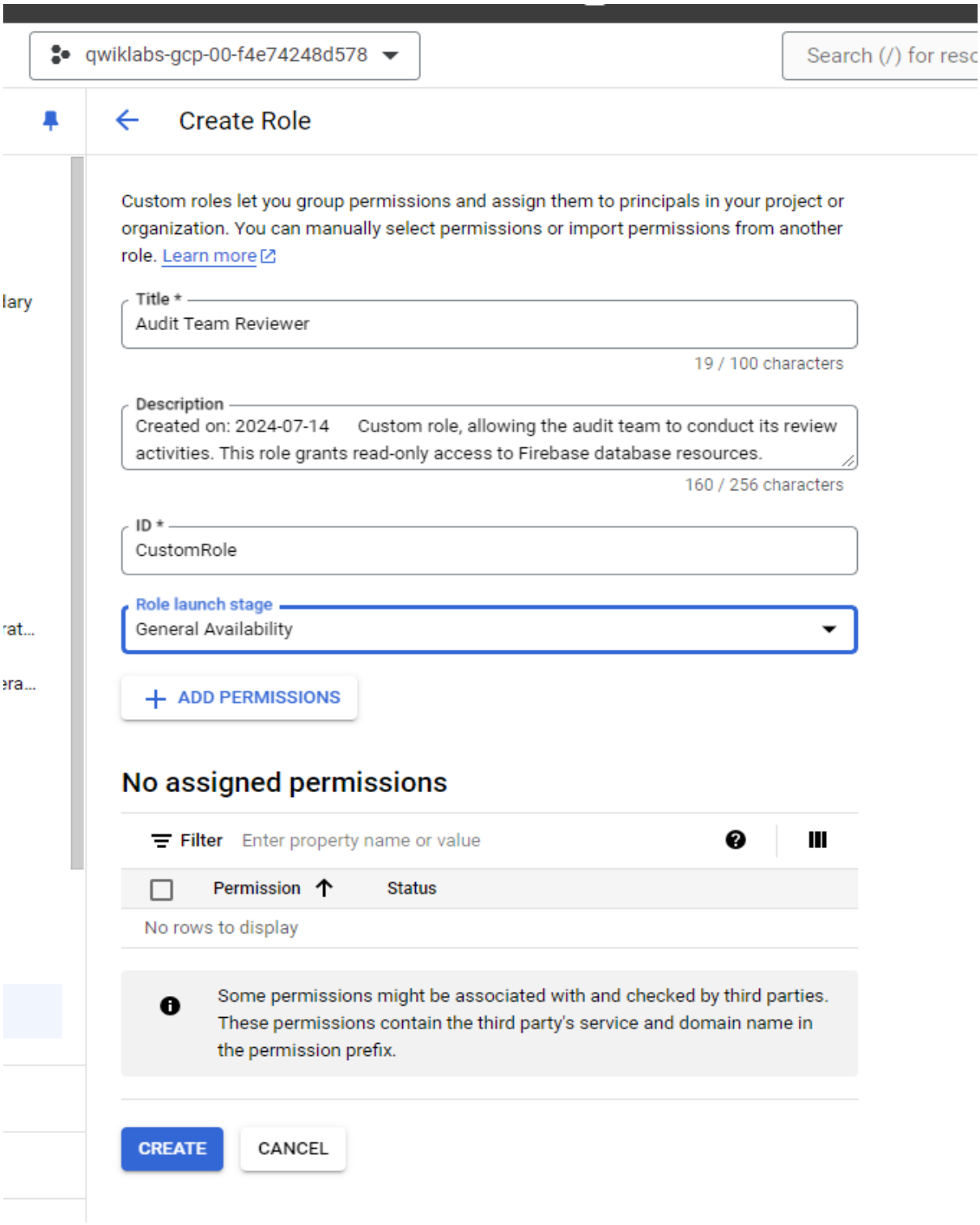


Figure 1 Screenshot of the Create Role dialog with the Title, Description, ID, and Role launch stage fields filled in.

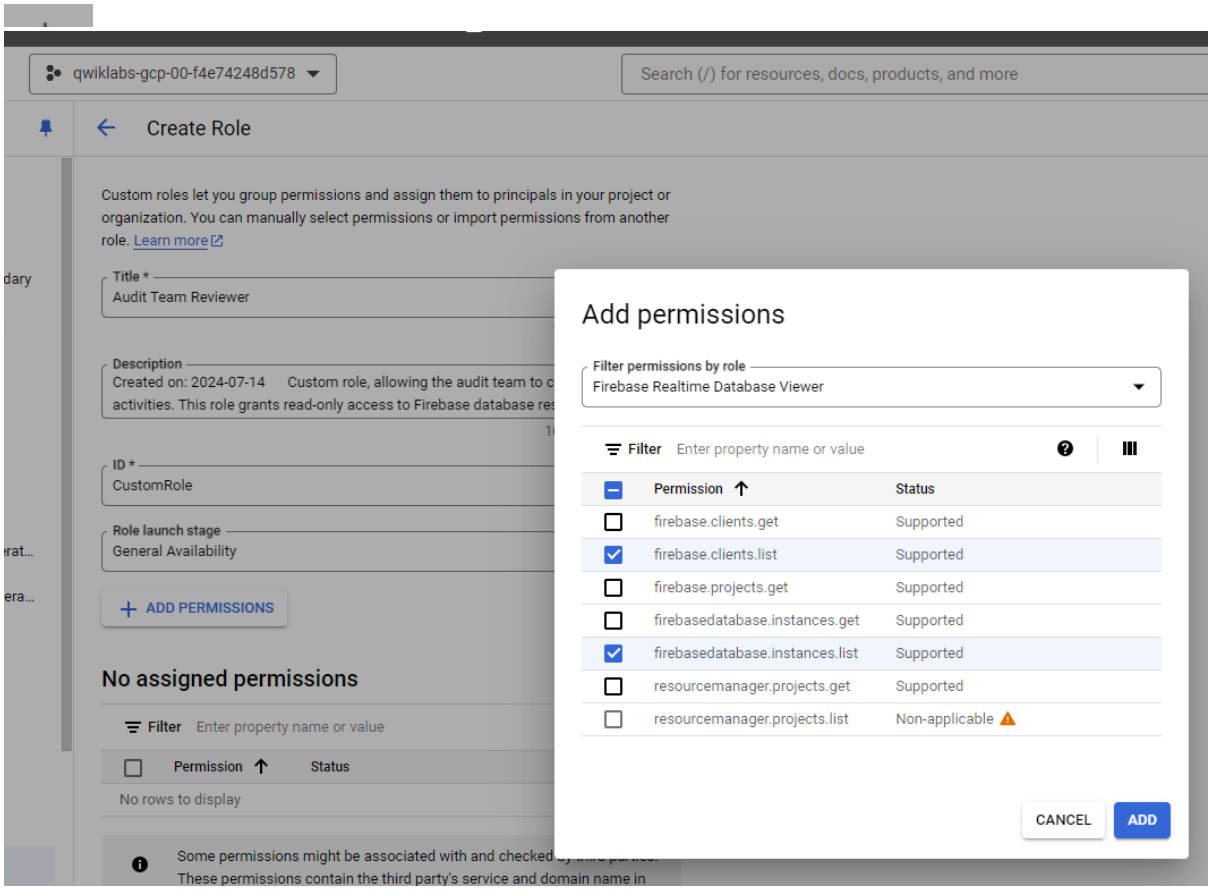


Figure 2 Screenshot of the Add permissions dialog with the Filter permissions by role field showing 'Firebase Realtime' and the Firebase Realtime Database Viewer checkbox selected and Add permissions dialog with the firebase.clients.list and firebasedatabase.instances.list checkboxes selected..

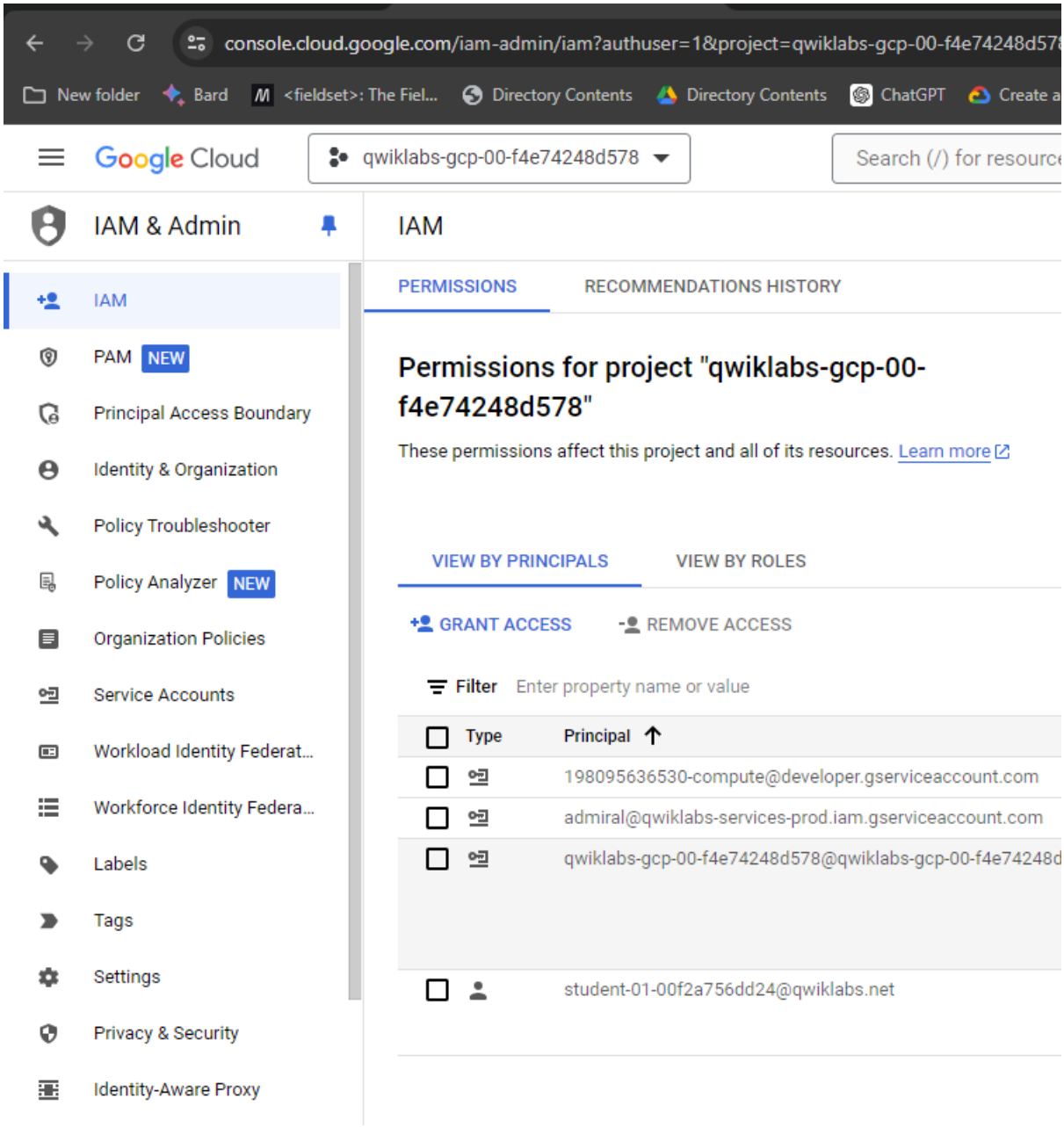


Figure 3 Screenshot of the IAM page with the View By Principals tab and the Grant access button highlighted.

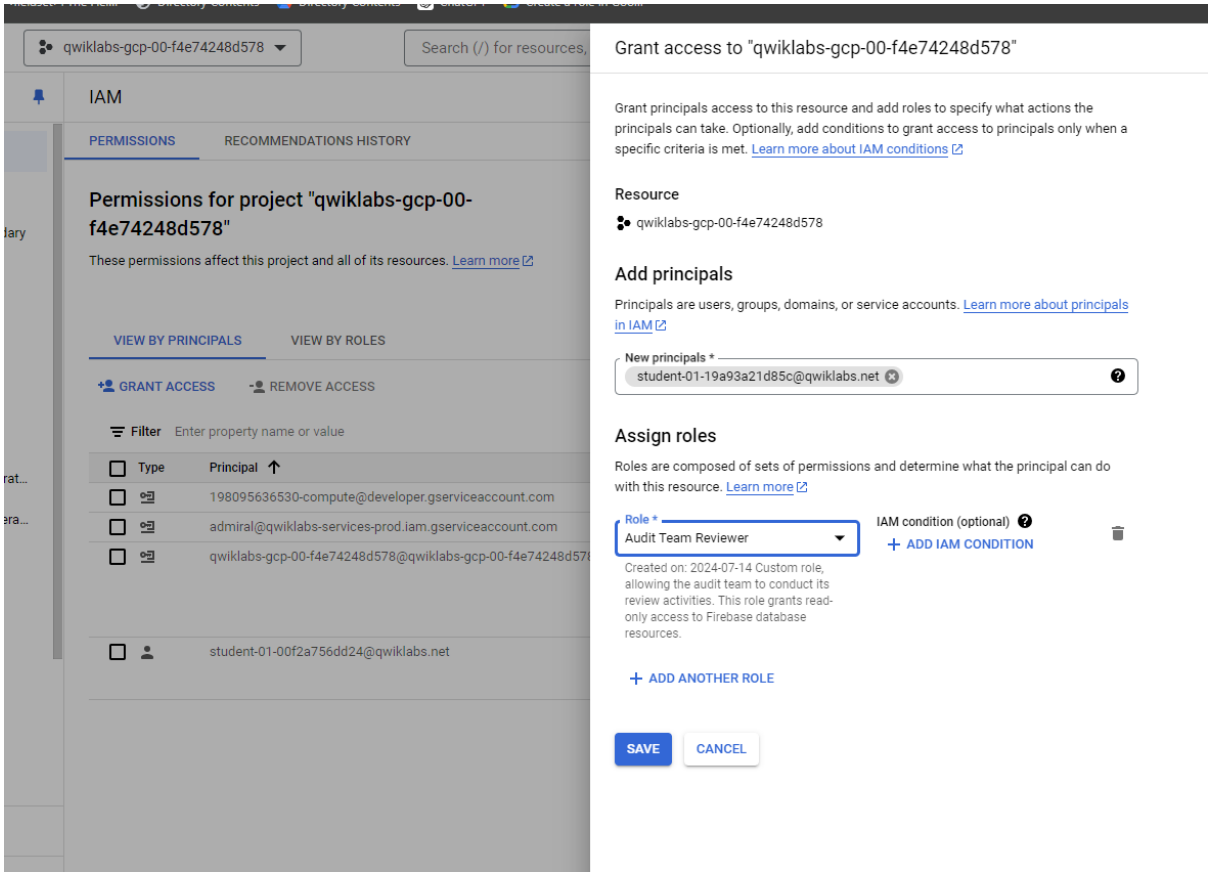


Figure 4 Screenshot of the Grant access dialog with the New principals field filled in with Google Cloud username 2 and the Select a role drop-down menu with Custom and Audit Team Reviewer selected.

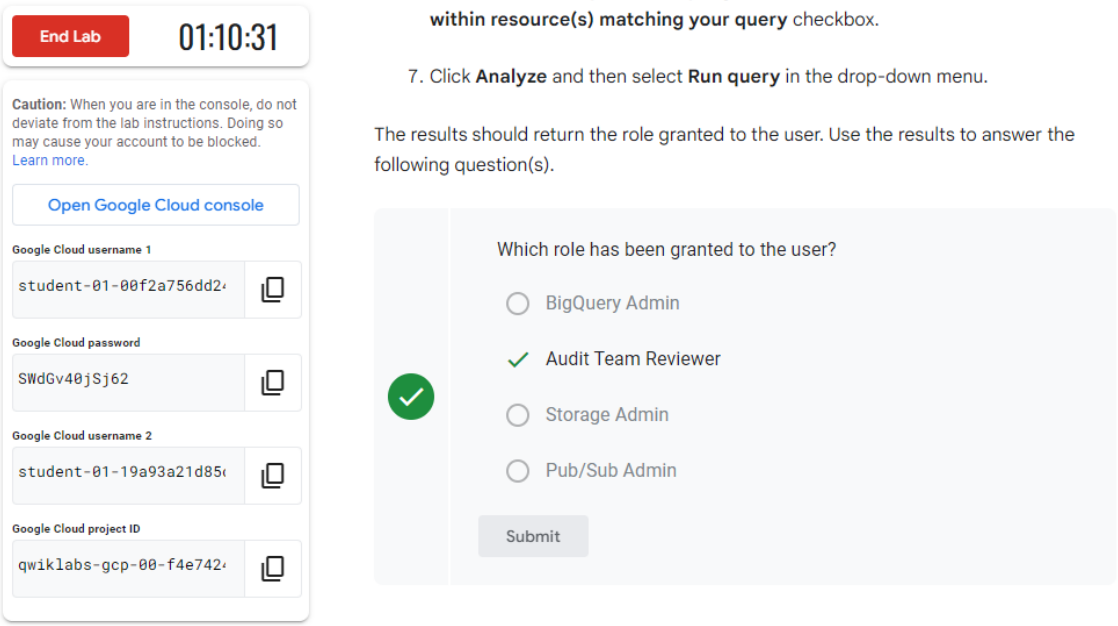


Figure 5 MCQ and credential

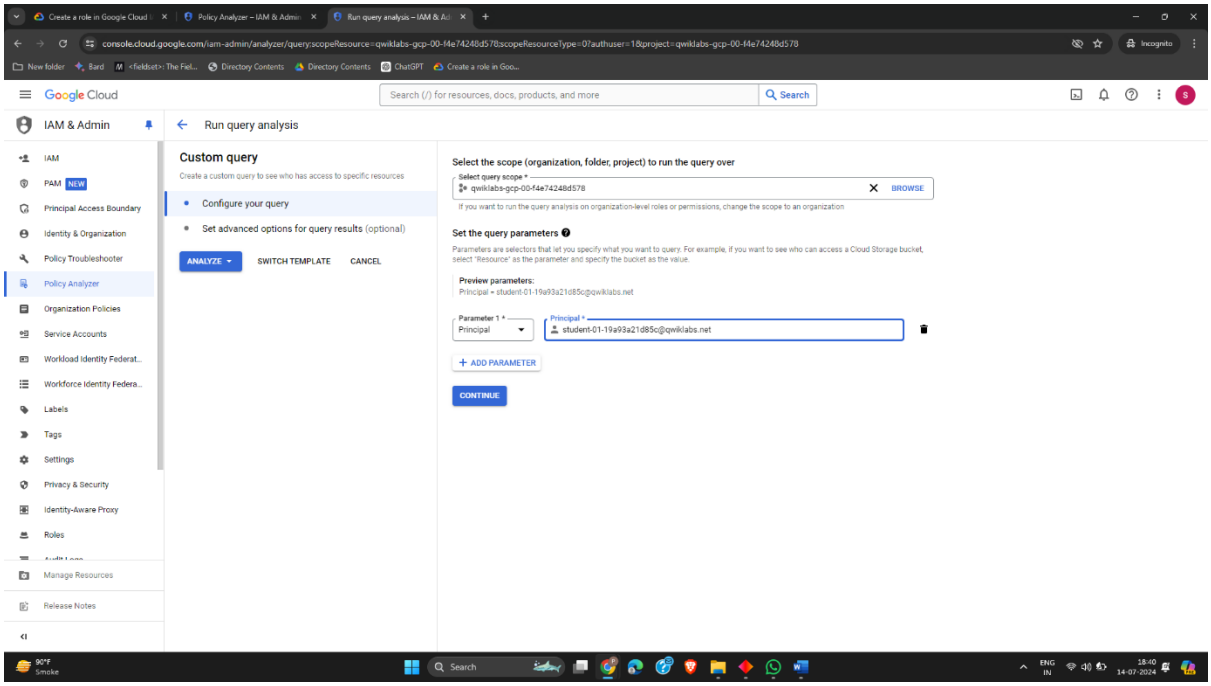


Figure 6 Screenshot of the Analyze policies section with the List resources within resource(s) matching your query checkbox selected and the Analyze button highlighted.

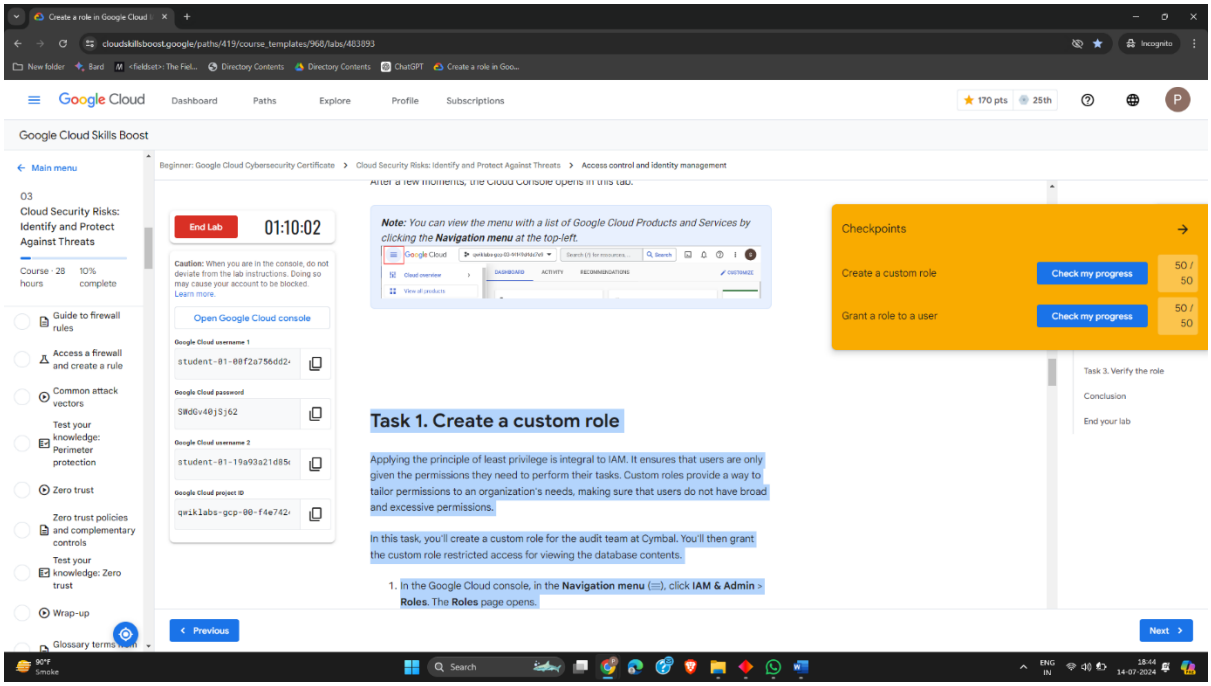


Figure 7 Screenshot of completing the task

LATEST APPLICATIONS:

1. **Implementing RBAC in an Organization**
   - Define roles based on job functions.
   - Assign permissions to roles rather than individuals.

- Regularly review and update roles to reflect changes in job functions.

2. **Deploying SSO Across Enterprise Applications**
   - Integrate SSO with enterprise applications to reduce the number of logins.
   - Improve user experience and security by centralizing authentication.
3. **Enhancing Security with MFA**
   - Require MFA for accessing sensitive systems and data.
   - Implement MFA using combinations like passwords and biometric scans.
4. **Auditing and Compliance**
   - Conduct regular compliance audits to ensure adherence to laws and regulations.
   - Perform security audits to assess and enhance the security posture of systems.
5. **Managing Credentials and Secrets**
   - Use tools like HashiCorp Vault for centralized secret management.
   - Encrypt and rotate credentials regularly to minimize security risks.
6. **Securing Non-Interactive Access**
   - Audit and manage service accounts used for automated processes.
   - Limit privileges and rotate keys to prevent unauthorized access.
7. **Using Security Protocols**
   - Implement mTLS for secure server-to-server communication.
   - Use OAuth for secure authorization without sharing credentials.
   - Utilize OpenID for streamlined single sign-on across multiple services.

LEARNING OUTCOME:

By Understanding and Implementing IAM, One Can:

1. **Improve Security Posture**: By enforcing RBAC, MFA, and auditing practices, organizations can significantly enhance their security.
2. **Enhance User Experience**: SSO and OpenID simplify login processes, reducing the burden on users and improving productivity.
3. **Ensure Compliance**: Regular audits help organizations comply with legal and regulatory requirements.
4. **Efficiently Manage Access**: Centralized management of roles, credentials, and secrets ensures efficient and secure access control.
5. **Mitigate Risks**: Proper management of non-interactive access and security protocols helps prevent unauthorized access and potential breaches.

REFERENCES:

Triple A Framework: https://youtu.be/Ty_zDOZyRdM

IAM : https://youtu.be/mUd6l74zJ-0

PRACTICAL: 4

AIM:

The assets within a cloud environment need to be protected from unauthorized access. To address this, security professionals use perimeter protection which refers to the security measures implemented to defend the edge of a network or system against unauthorized access and cyber threats. One type of perimeter protection includes using firewalls to manage and secure network traffic entering and leaving a cloud environment. Firewalls help protect trusted internal networks (like a company's private network) from untrusted external networks (such as the Internet). Firewalls examine both incoming and outgoing network traffic based on predefined rules to either allow or block specific data packets. This is crucial for helping maintain application security, traffic control, compliance, and policy enforcement. In this experiment, you'll access a firewall and create rules to test the security of a server and make modifications as necessary.

THEORY:

Firewalls: A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the Internet. Firewalls can block or allow traffic based on various criteria, including IP addresses, port numbers, and protocols, to prevent unauthorized access and protect sensitive data.

Logs: Logs are records of events that occur within an information system or network. They provide a detailed account of activities such as user logins, file access, network traffic, and system errors. Logs are essential for monitoring and auditing purposes, helping to detect security incidents, troubleshoot issues, and ensure compliance with regulatory requirements. Analyzing logs can reveal patterns and anomalies that indicate potential security threats or operational inefficiencies.

Discretionary Access Control (DAC): A security model where the owner of the data or resource has the discretion to grant or revoke access to other users.

Mandatory Access Control (MAC): A strict security model in which access is granted based on predefined security policies.

Role-Based Access Control (RBAC): A method of controlling access to resources based on the roles assigned to users.

Attribute-Based Access Control (ABAC): A security model where access is granted based on attributes like user, resource, and environment.

- In a cloud environment, ABAC works by creating policies that define the conditions under which access is granted or denied.
- These policies can be based on a variety of attributes, like the user's job title, the sensitivity level of the data, or even the current day and time.
- Implementing ABAC in a cloud environment typically involves setting up a Policy Decision Point (PDP) and a Policy Enforcement Point (PEP).
    - The PDP evaluates policies and makes access decisions.
    - The PEP enforces those decisions by granting or denying access to the resources.

Best Practices for Implementing Access Controls in Cloud Environments:

- **Apply the Principle of Least Privilege:** Grant users the minimum levels of access – or permissions – they need to perform their job functions. This reduces the risk of accidental or malicious misuse of privileges.
- **Separate Duties:** Distribute tasks and privileges among multiple users to ensure no single user has enough access to misuse the system on their own. This separation of duties helps in mitigating the risk of insider threats.
- **Regularly Audit:** Conduct regular audits and reviews of access controls and user permissions to ensure they are appropriate and comply with security policies. Regular audits help identify and rectify any unauthorized access or anomalies.

OUTPUT:

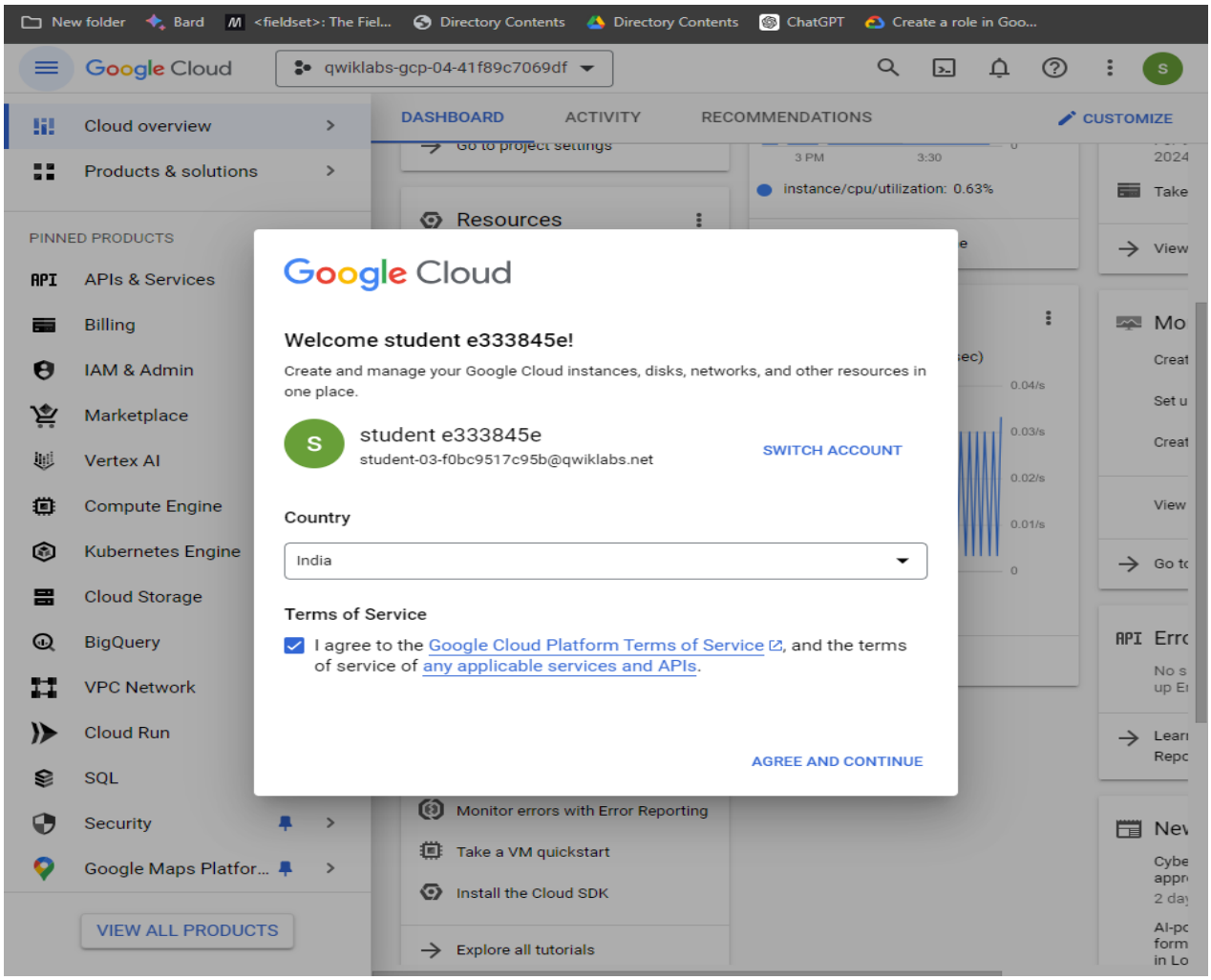


Figure 1 : Lab Details panel showing the time remaining, Google Cloud console button, and temporary credentials.

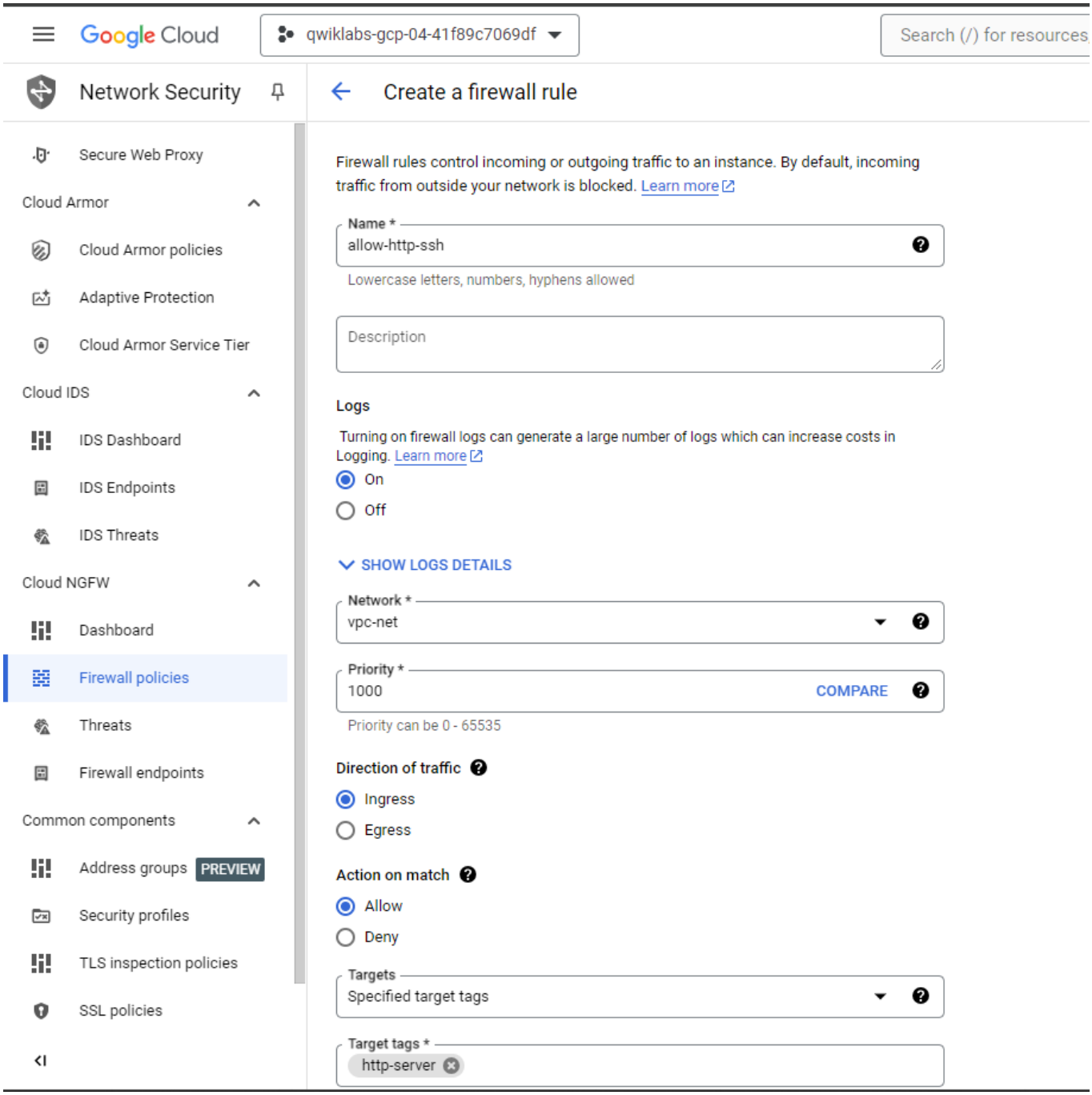


Figure 2 : Create a firewall rule dialog with specified settings.

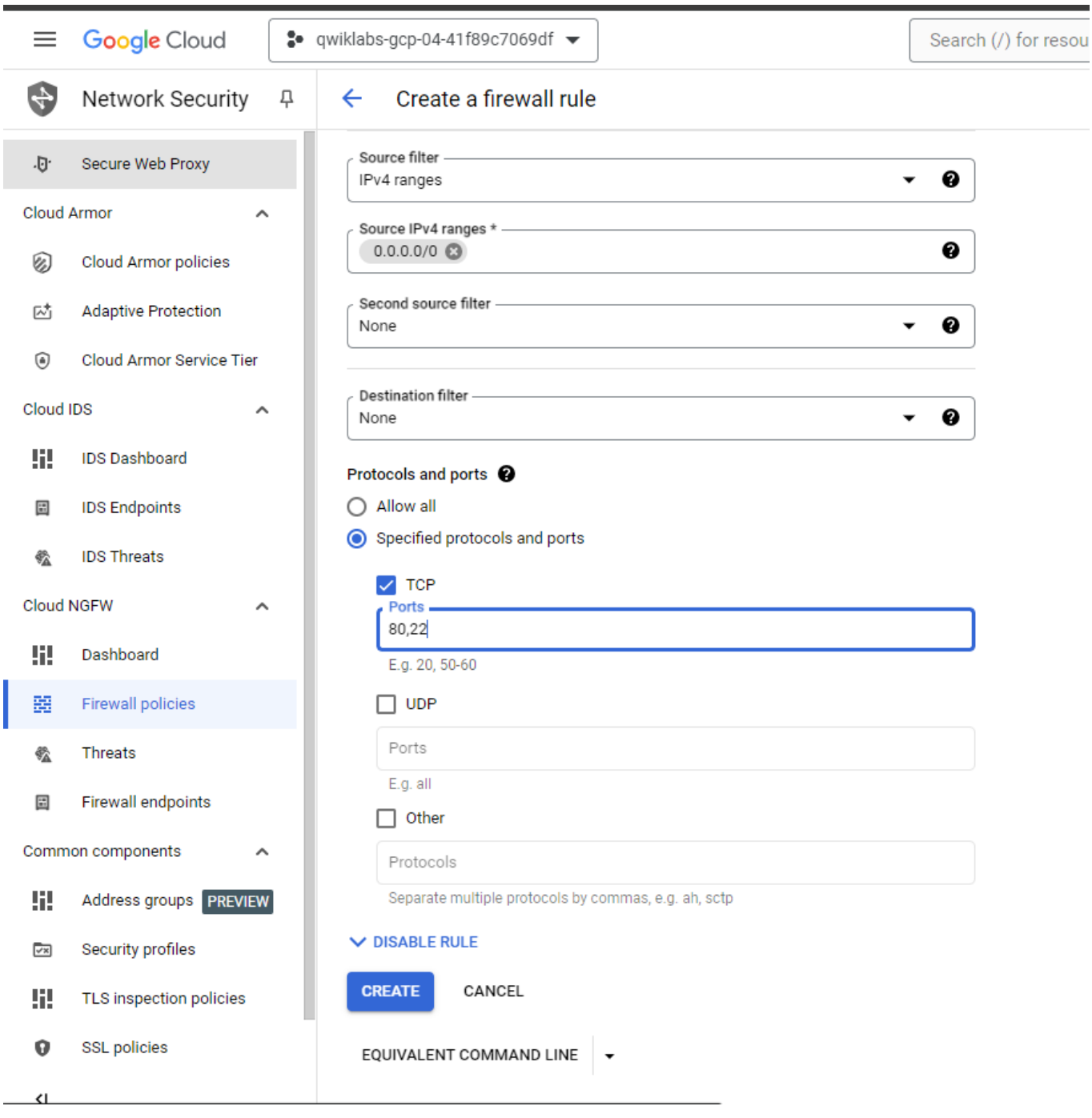


Figure 3 : Create a firewall rule dialog with specified settings.

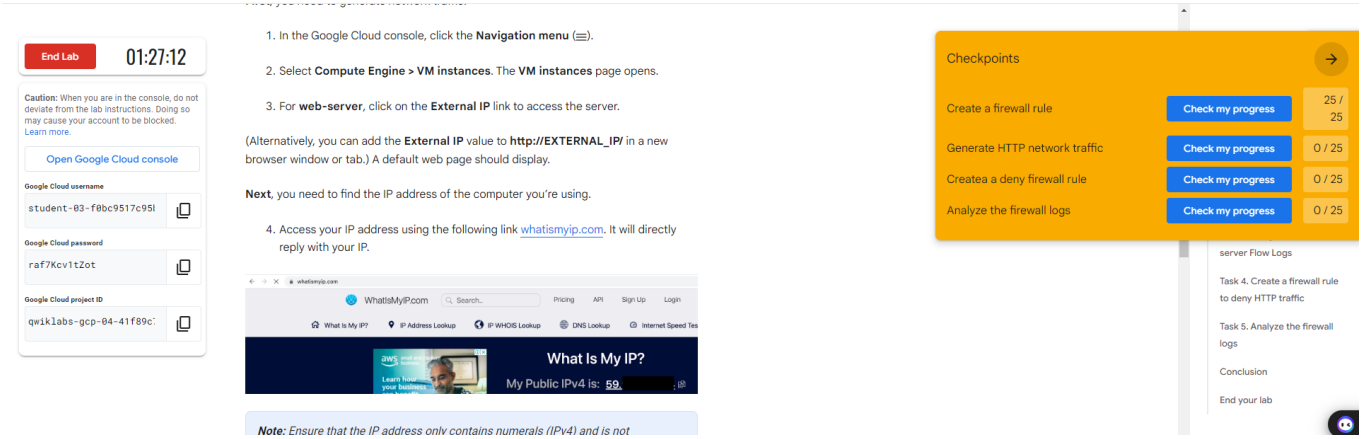


Figure 4 : : Task 1 Completion Verification.

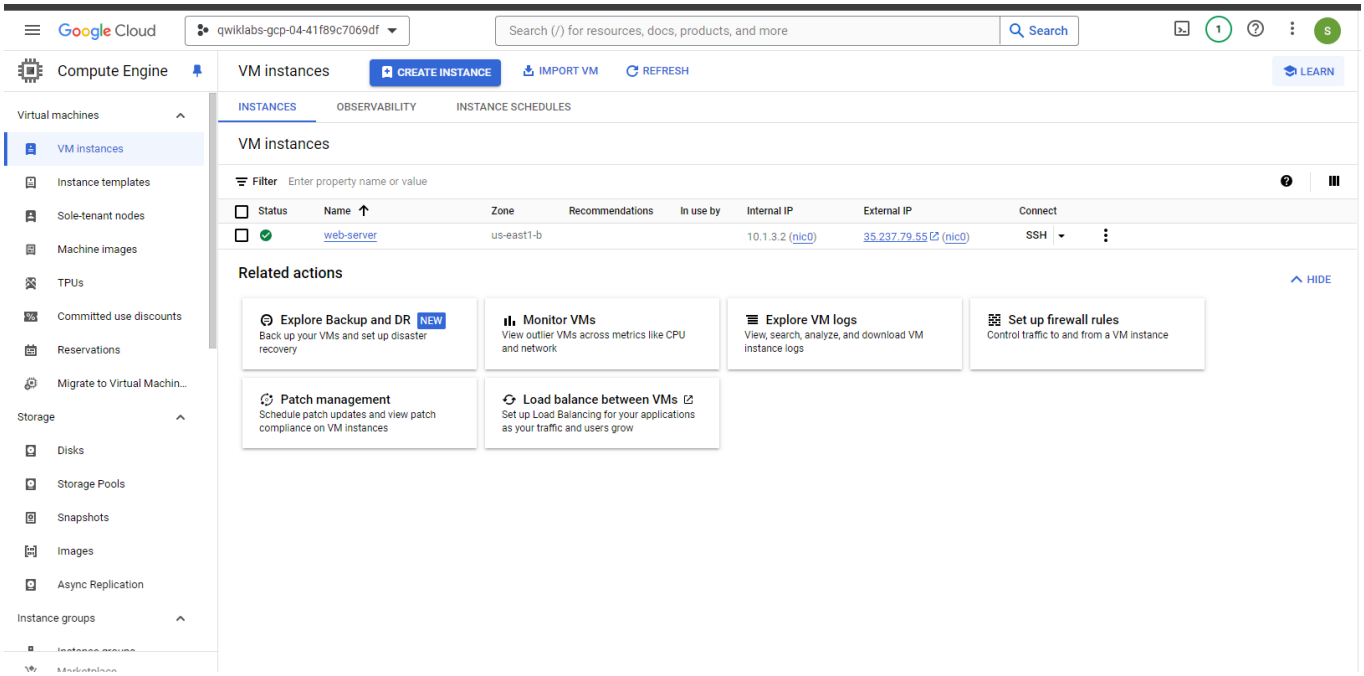


Figure 5: Generate network traffic by accessing the web server's external IP.

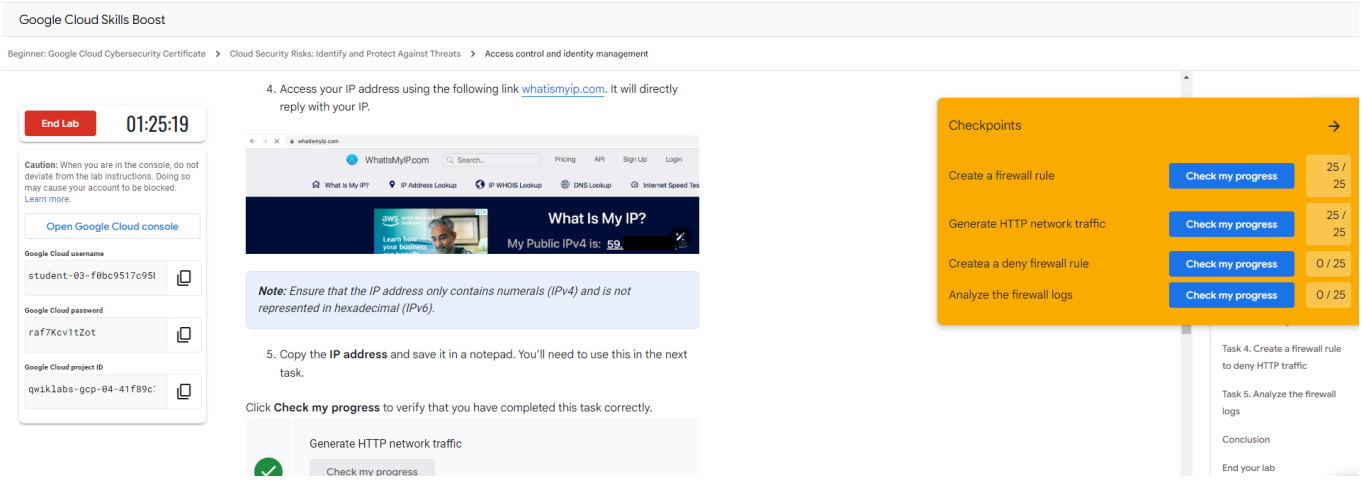


Figure 6 : : Task 2 Completion Verification.

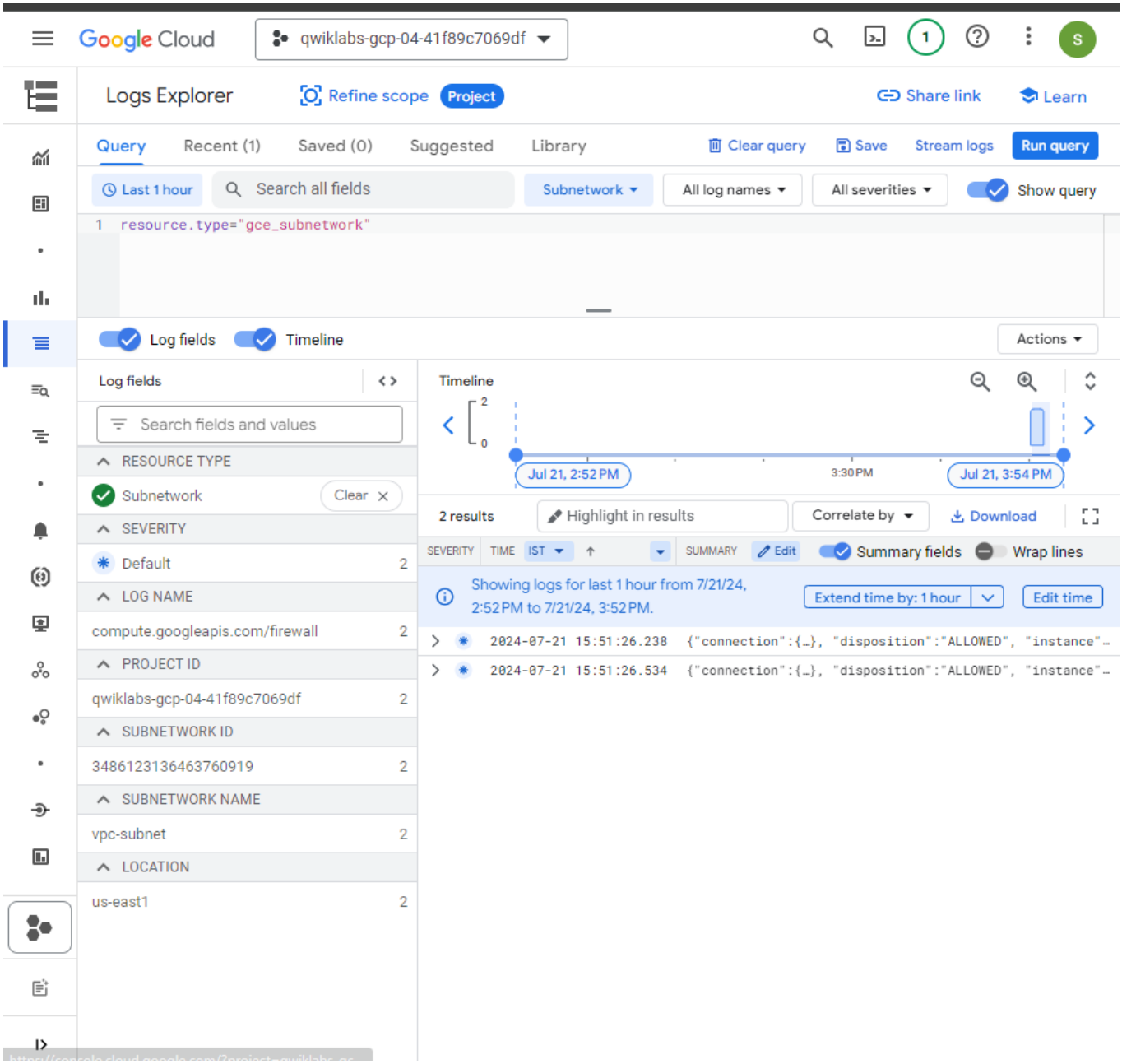


Figure 7 : Log fields pane showing the selection of compute.googleapis.com/vpc_flows for accessing VPC Flow logs.

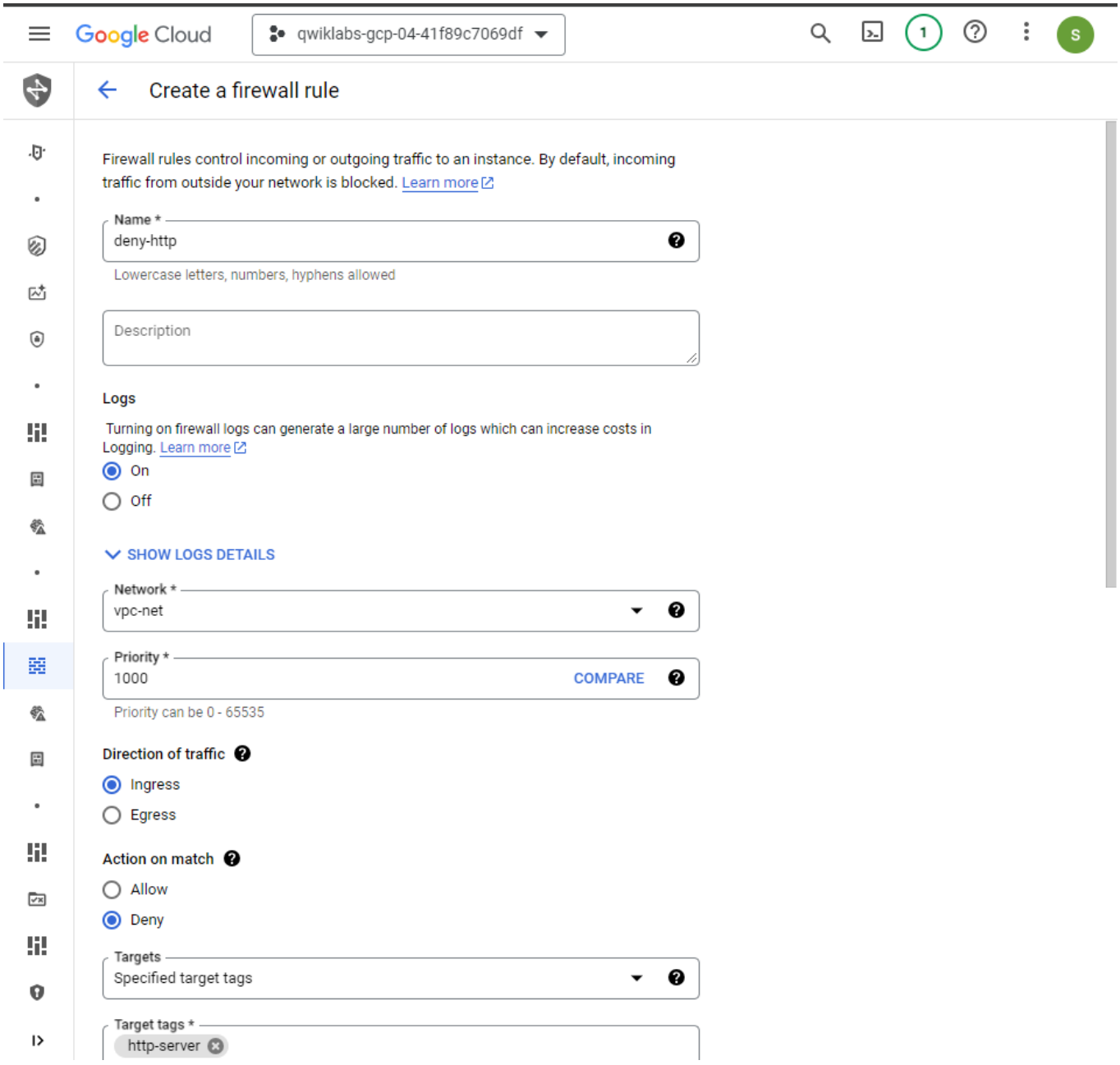


Figure 8 : Create a firewall rule dialog with the specified settings.

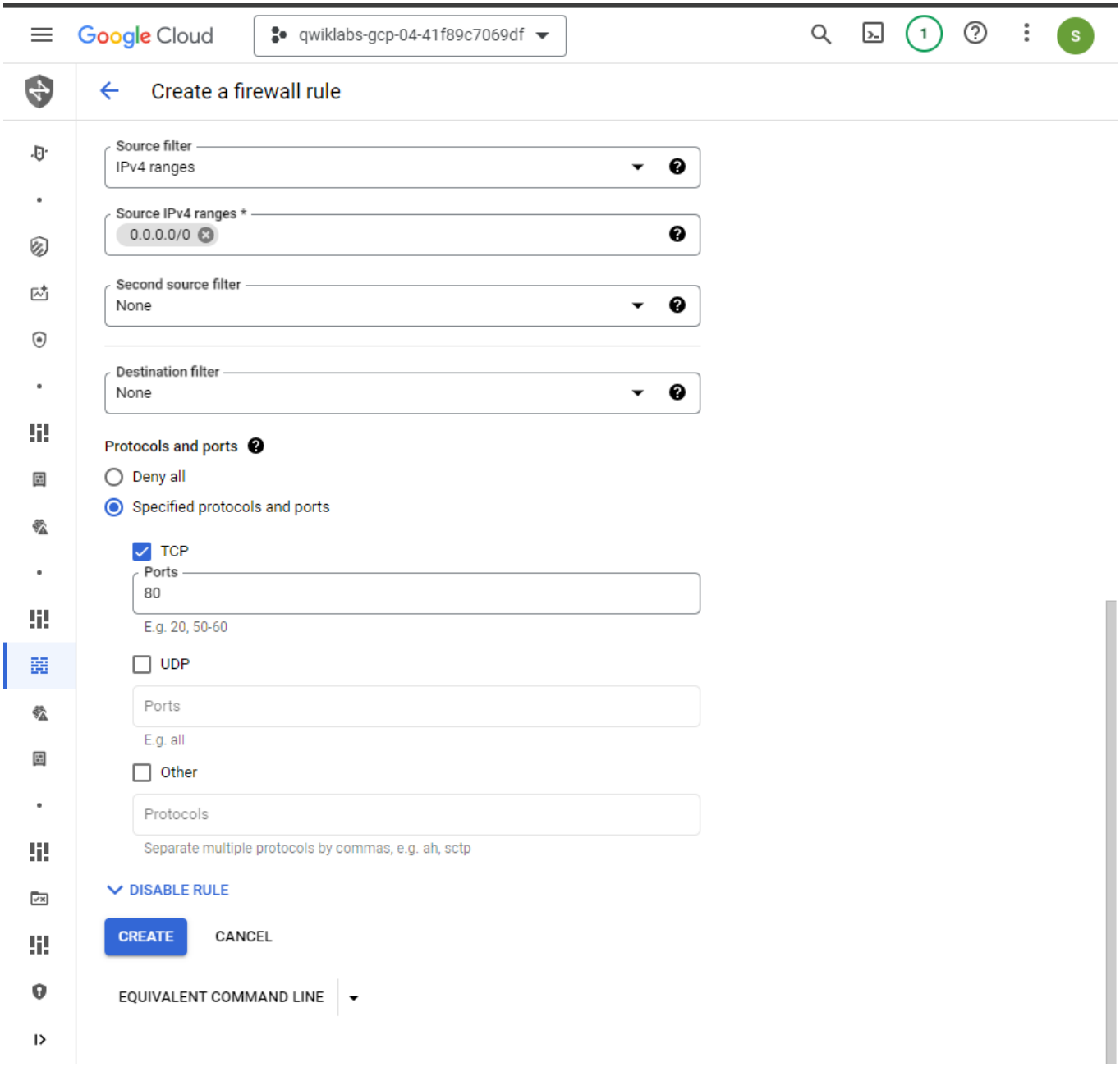


Figure 9 : Create a firewall rule dialog with the Create button highlighted to finalize the creation of the rule.

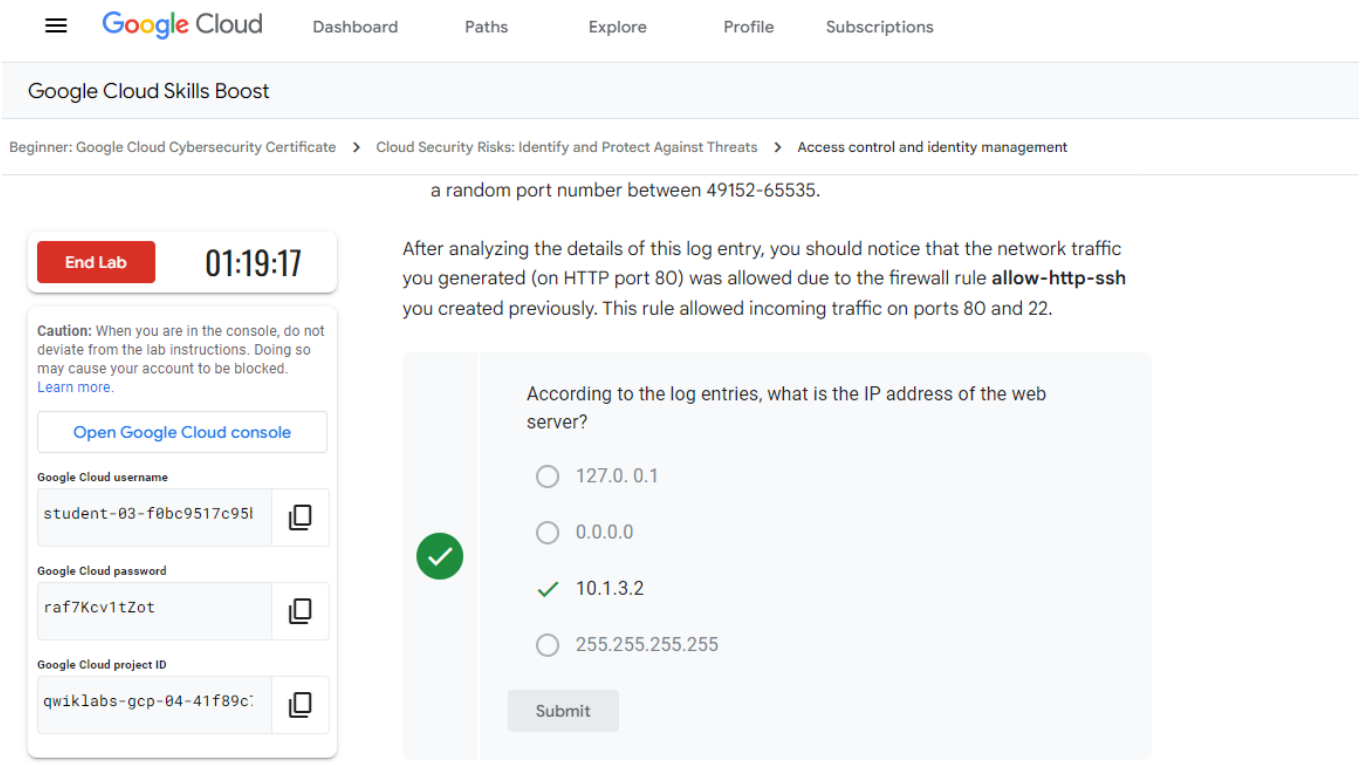


Figure 10 : MCQ

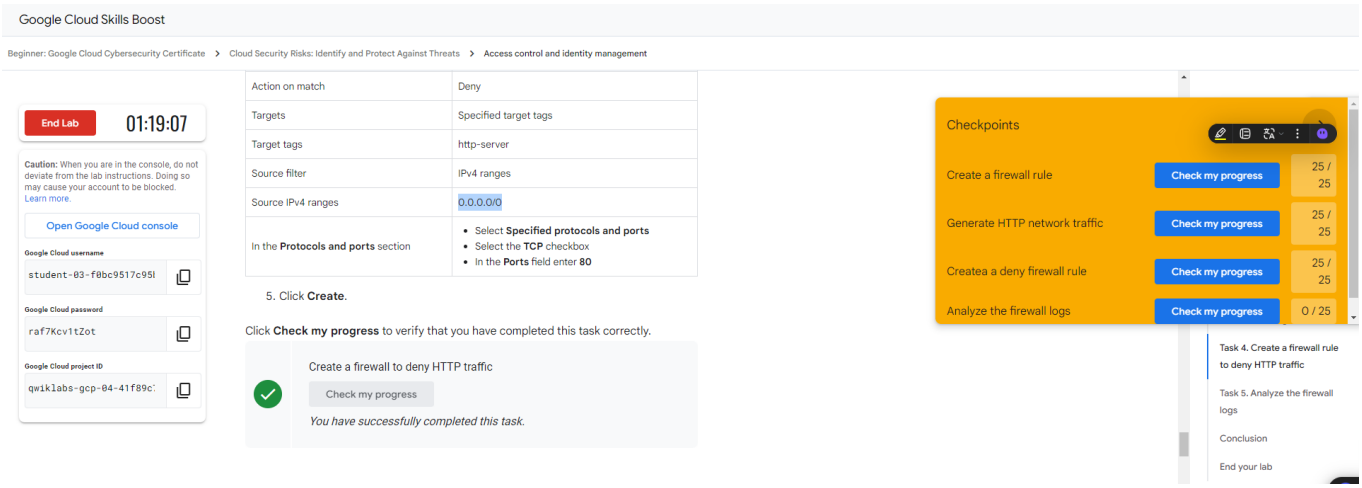


Figure 11 : Task 3 Completion Verification.

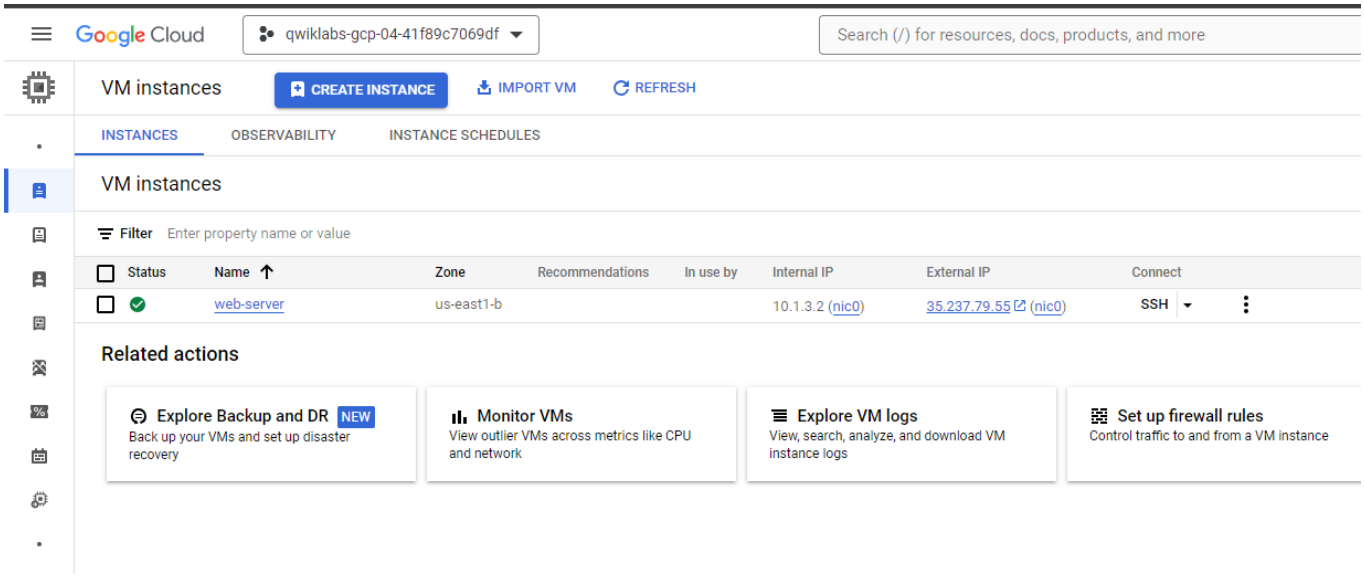


Figure 12 : VM instances page in Google Cloud Console with the External IP link for the web server highlighted.

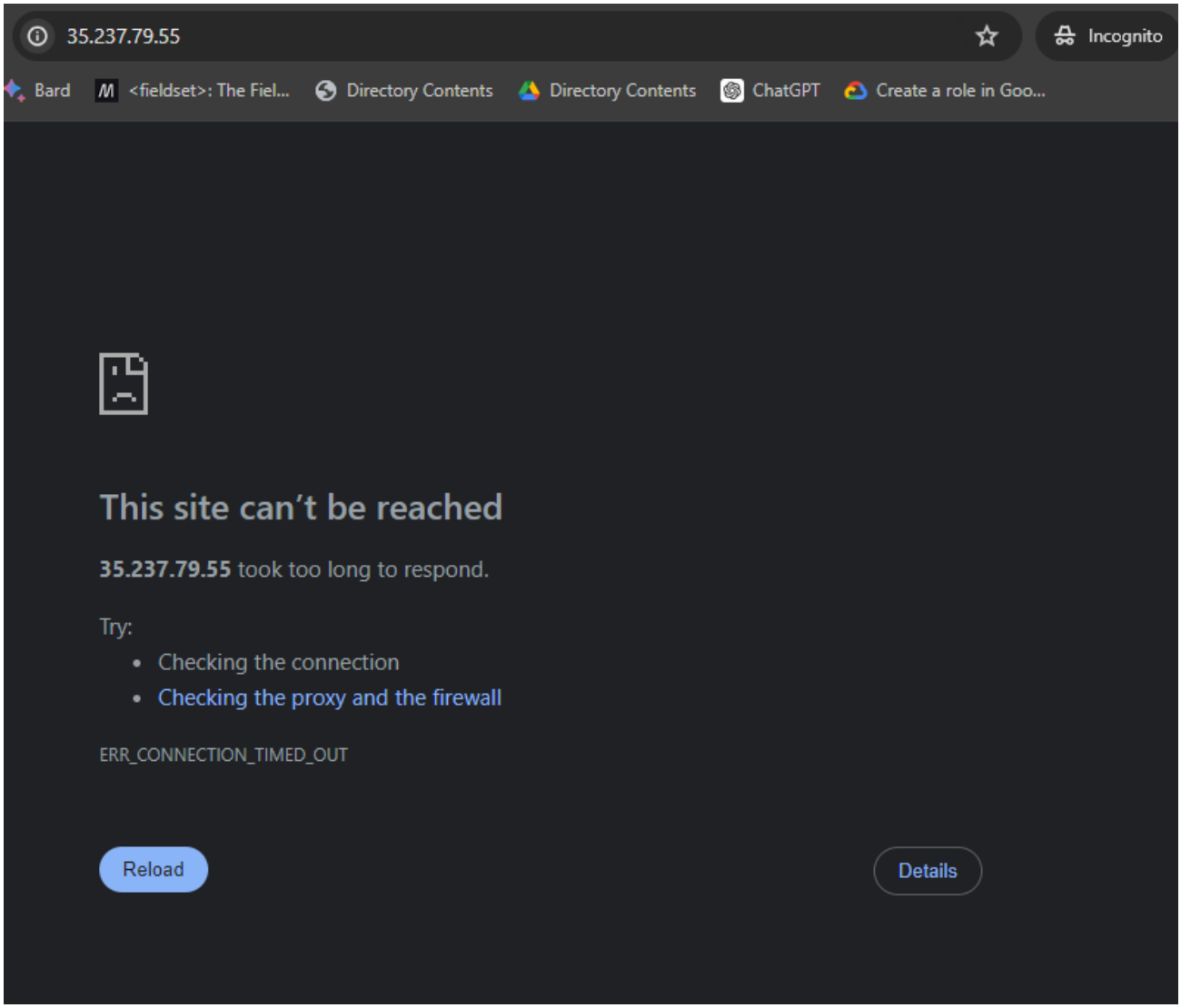


Figure 13 : Web browser displaying a site connection error message when attempting to access the web server.

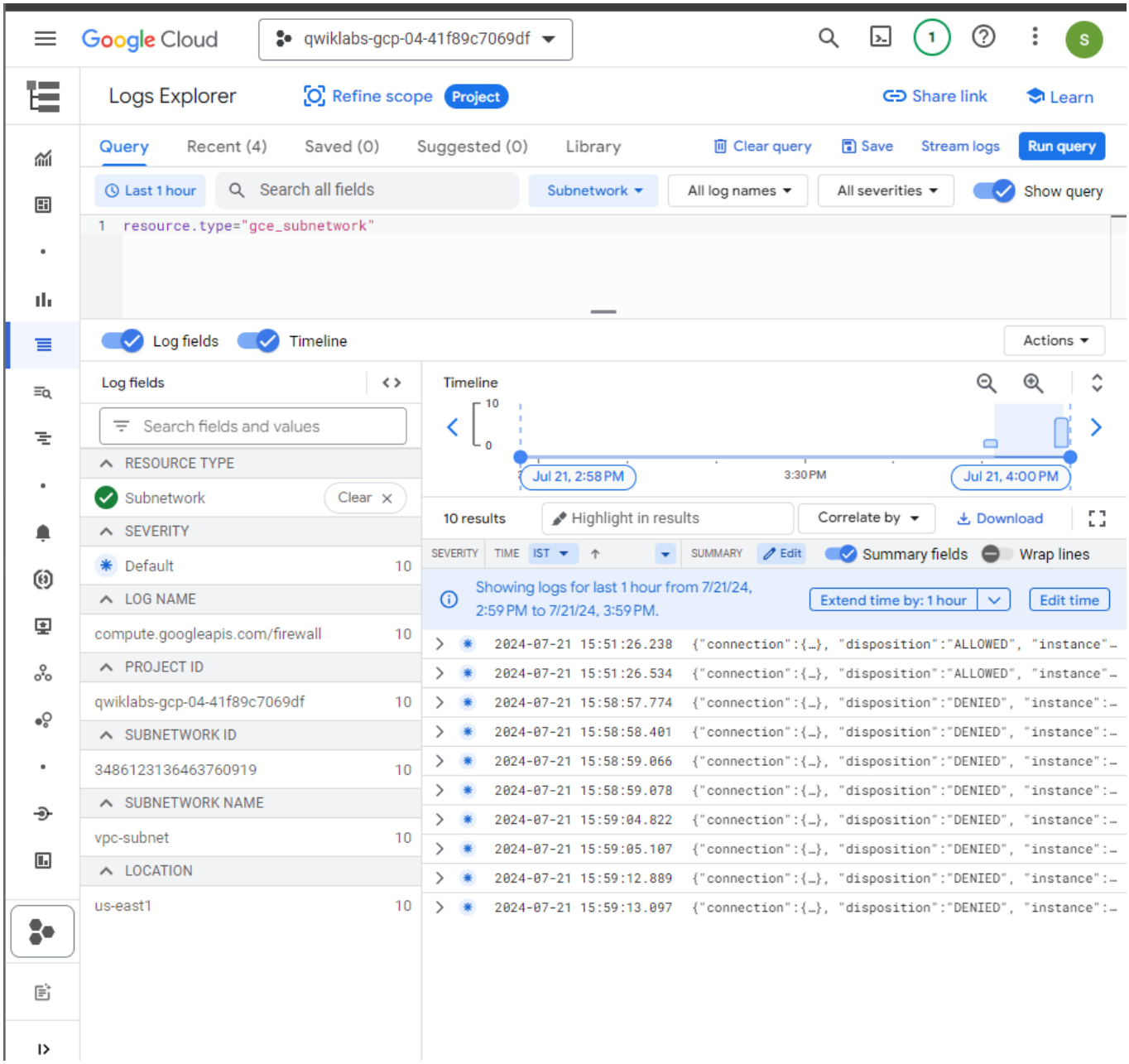


Figure 14 : Navigation menu in Google Cloud Console showing the path to select Logging > Logs Explorer.

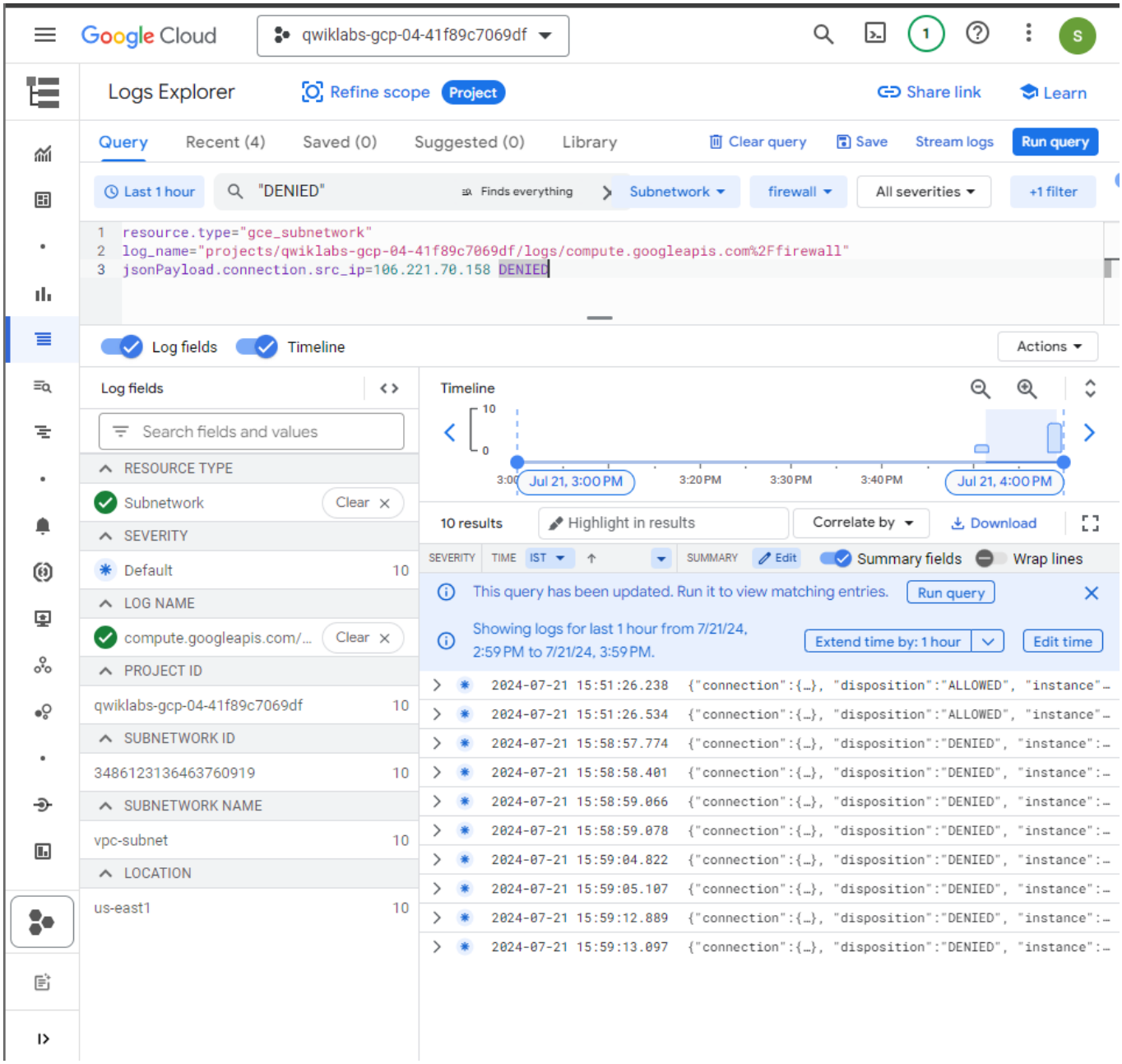


Figure 15 : Query builder in Logs Explorer with the query jsonPayload.connection.src_ip=YOUR_IP DENIED entered and executed

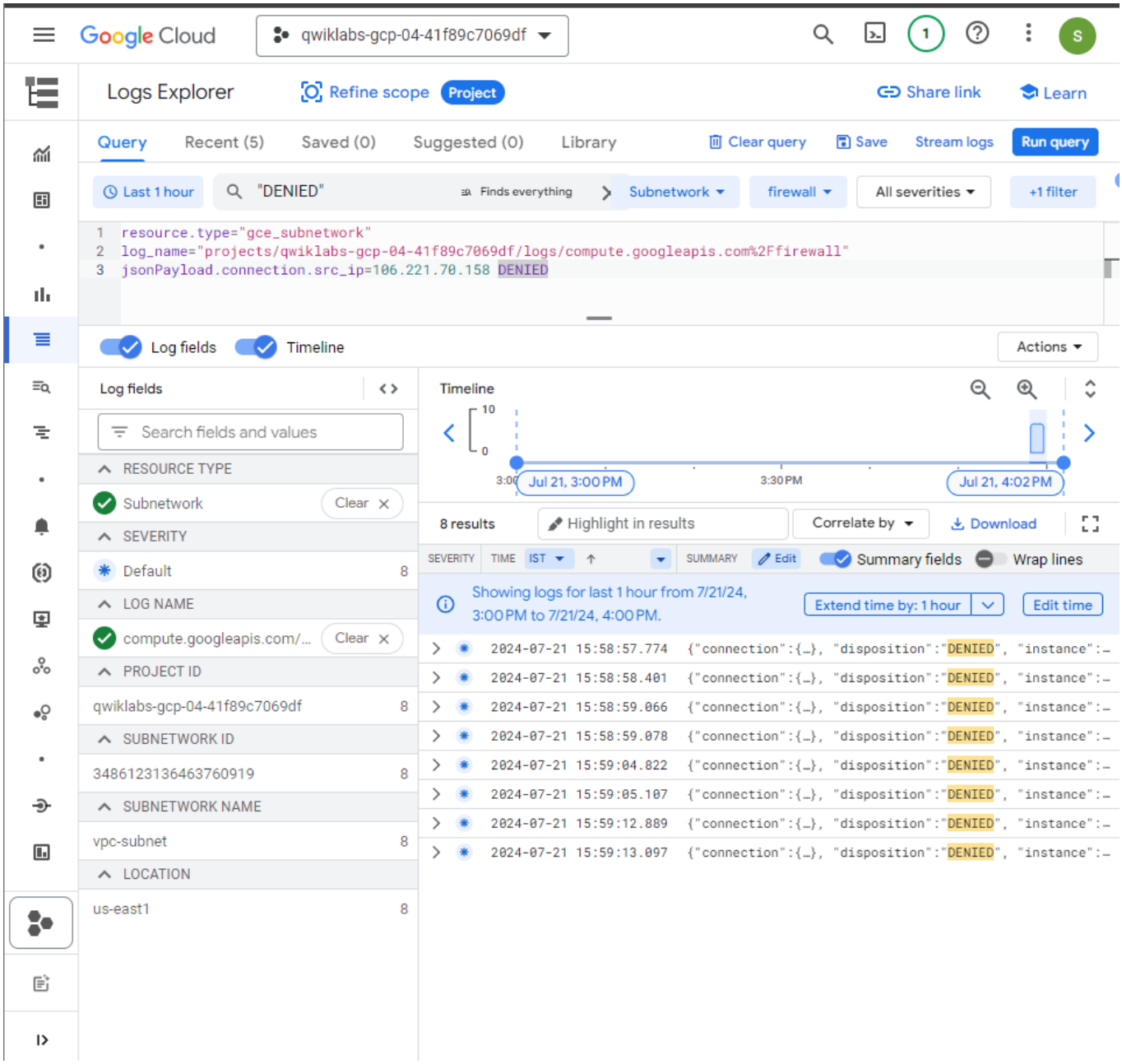


Figure 16 : . Query results pane displaying firewall log entries after running the query.

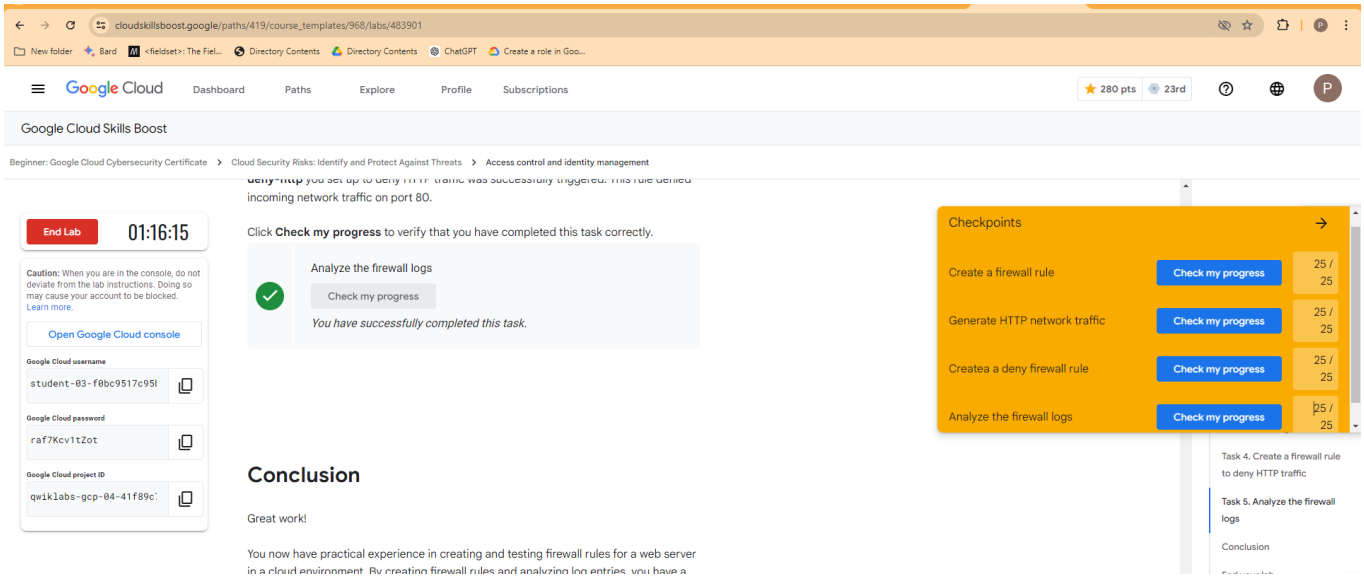


Figure 17 : Task 4 Completion Verification.

LATEST APPLICATIONS:

Zero Trust Architecture: Implementing a zero-trust model where no entity inside or outside the network is trusted by default, and continuous verification is required.

Microsegmentation: Dividing a cloud environment into smaller segments to reduce the attack surface and improve security management.

Next-Generation Firewalls (NGFWs): Advanced firewalls that provide deeper inspection capabilities, including application-level monitoring, intrusion prevention, and threat intelligence integration.

Cloud Access Security Brokers (CASBs): Security solutions that sit between cloud service users and cloud applications to monitor and enforce security policies.

Security Information and Event Management (SIEM): Tools that provide real-time analysis of security alerts generated by network hardware and applications.

LEARNING OUTCOME:

- Understand the importance of perimeter protection in securing cloud environments.
- Gain hands-on experience in configuring and managing firewall rules to protect a cloud-based server.
- Learn the differences and applications of various access control models (DAC, MAC, RBAC, ABAC) in cloud security.

 Develop skills to implement and enforce security policies using ABAC with PDP and PEP in a cloud environment.

 Explore the latest trends and tools in cloud security, such as zero trust architecture, microsegmentation, NGFWs, CASBs, and SIEM.

 Apply best practices for implementing access controls, including the principle of least privilege, separation of duties, and regular audits.

 Understand the role of logs in monitoring and auditing security events and maintaining compliance.

REFERENCES:

1. Access control: https://youtu.be/xXAYK-9vDJg
2. Trust boundaries: https://www.linkedin.com/posts/hassan-shahin007_what-are-trust-boundaries-trust-boundaries-activity-7096223279123767296-bsSW
3. firewall rules: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/8-firewall-best-practices-for-securing-the-network/

PRACTICAL: 5

AIM:

Identifying vulnerabilities and implementing remediation techniques is crucial for helping ensure the security and stability of various systems and applications. Many applications and systems handle sensitive information, such as personally identifiable information, financial records, or intellectual property. Identifying vulnerabilities helps protect this sensitive data from unauthorized access and potential breaches. Addressing vulnerabilities early in the development process is generally more cost-effective than dealing with security breaches later. The cost of remediating a vulnerability is often much higher than the cost of preventing it in the first place. As a security analyst, regularly scanning for vulnerabilities can help identify and address weaknesses before malicious attacks, thus mitigating potential threats proactively. It provides insight into an application's attack surface, helping enable you to understand potential avenues of exploitation and prioritize critical areas for improvement. In this experiment, you'll not only learn how to set up and run a vulnerable application but scan it for vulnerabilities.

THEORY:

In this practical, you will focus on identifying vulnerabilities in a web application and implementing remediation techniques. The theory behind this practical includes understanding the types of vulnerabilities commonly found in web applications and the tools used to identify them.

1. **Types of Vulnerabilities:**
    - **SQL Injection:** Exploiting vulnerabilities in an application's database layer by injecting malicious SQL queries.
    - **Cross-Site Scripting (XSS):** Injecting malicious scripts into web pages viewed by other users.
    - **Cross-Site Request Forgery (CSRF):** Forcing a user to execute unwanted actions on a web application where they are authenticated.
    - **Insecure Direct Object References:** Exposing internal objects through a URL, allowing attackers to access unauthorized data.

- **Security Misconfigurations:** Using default configurations or incomplete configurations that lead to security risks.

2. **Vulnerability Scanning Tools:**
    - **OWASP ZAP (Zed Attack Proxy):** A free and open-source security tool that helps find security vulnerabilities in web applications.
    - **Nmap:** A network scanning tool used to discover hosts and services on a computer network.
    - **Nessus:** A vulnerability scanner that detects vulnerabilities, misconfigurations, and compliance violations in physical, virtual, and cloud systems.
    - **Burp Suite:** A comprehensive platform for performing security testing of web applications.
3. **Remediation Techniques:**
    - **Input Validation:** Ensuring that all input is validated before being processed by the application.
    - **Parameterized Queries:** Using parameterized queries to prevent SQL injection attacks.
    - **Output Encoding:** Encoding output to prevent XSS attacks.
    - **Security Headers:** Implementing HTTP security headers like Content Security Policy (CSP), X-Content-Type-Options, and X-Frame-Options.
    - **Access Controls:** Implementing proper access controls to ensure users can only access data they are authorized to view.
    - **Patch Management:** Regularly updating and patching software to fix known vulnerabilities.

CODE:

```
gcloud compute addresses create xss-test-ip-address --region="REGION"
```

Description: Creates a static IP address named xss-test-ip-address in the specified region.

gcloud compute addresses describe xss-test-ip-address --region="REGION" --format="value(address)"

Description: Describes the static IP address and outputs the value of the address.

gcloud compute instances create xss-test-vm-instance --address=xss-test-ip-address --no-service-account --no-scopes --machine-type=e2-micro --zone="ZONE" --metadata=startup-script='apt-get update; apt-get install -y python3-flask'

Description: Creates a VM instance named xss-test-vm-instance using the specified static IP address and machine type, with a startup script to install Python Flask.

gcloud compute firewall-rules create enable-wss-scan --direction=INGRESS --priority=1000 --network=default --action=ALLOW --rules=tcp:8080 --source-ranges=0.0.0.0/0

Description: Creates a firewall rule to allow ingress traffic on port 8080 from any IP address.

gsutil cp gs://cloud-training/GCPSEC-ScannerAppEngine/flask_code.tar . && tar xvf flask_code.tar

Description: Copies the application files from a Google Cloud Storage bucket and extracts them.

gcloud services enable websecurityscanner.googleapis.com

Description: Enables the Web Security Scanner API in Google Cloud.

gcloud websecurityscanner scan-configs run <SCAN_CONFIG_ID>

Description: Re-runs the Web Security Scanner on the updated application.

OUTPUT:

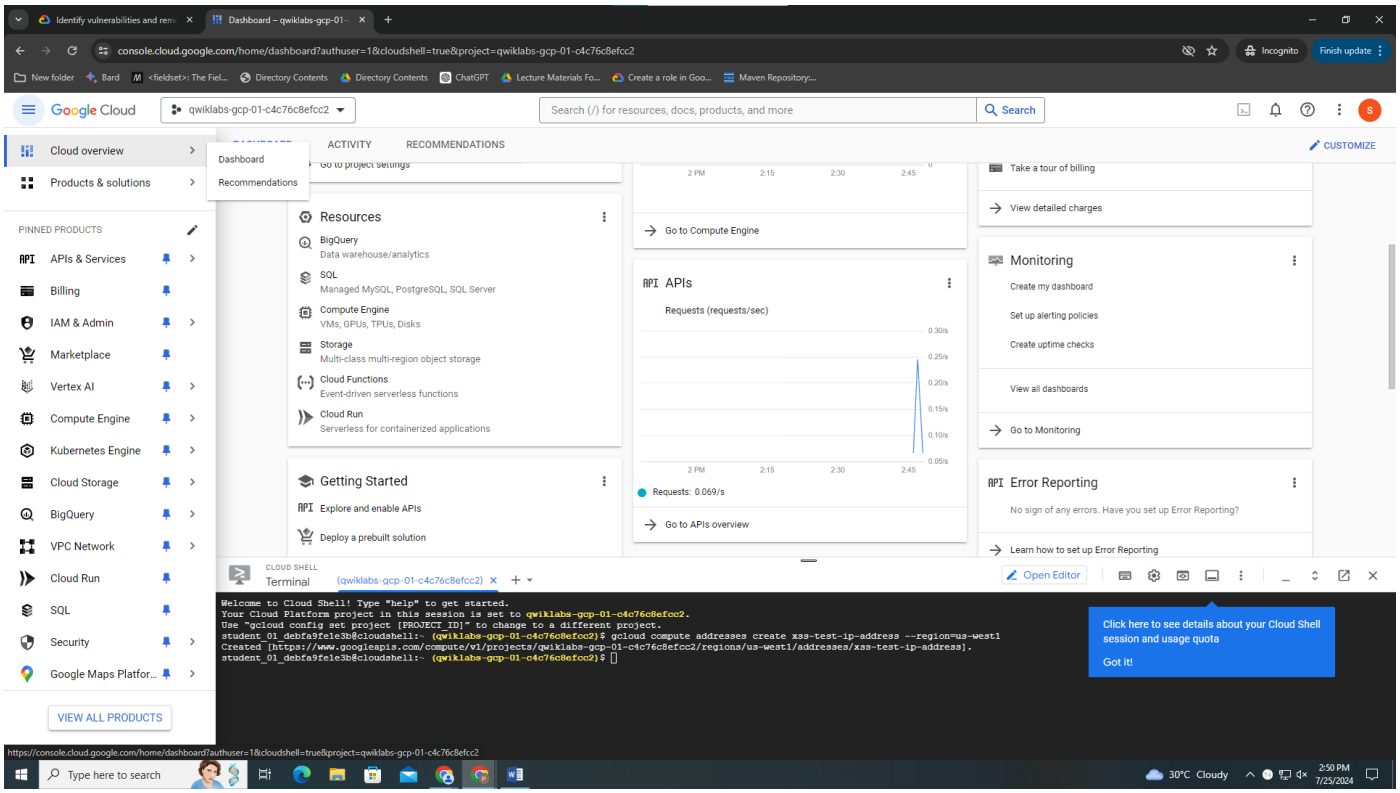


Figure 1 : Starting Google Cloud Skills Lab.

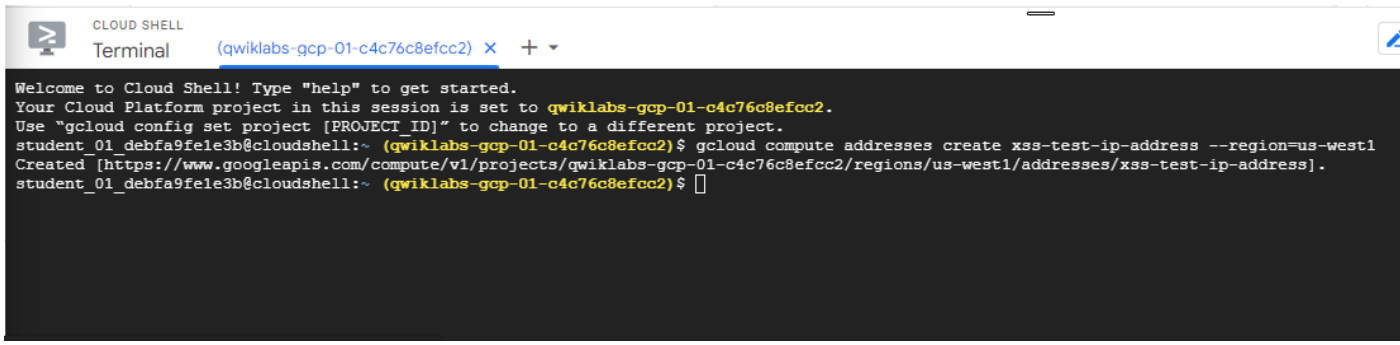


Figure 2 : Creating a static IP address

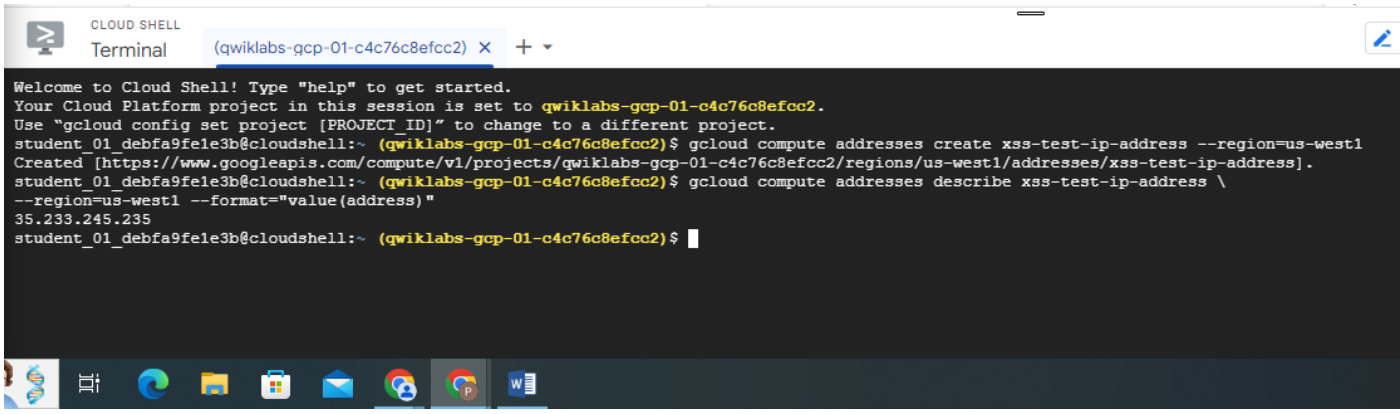


Figure 3 : Describing the static IP address in Cloud Shell.

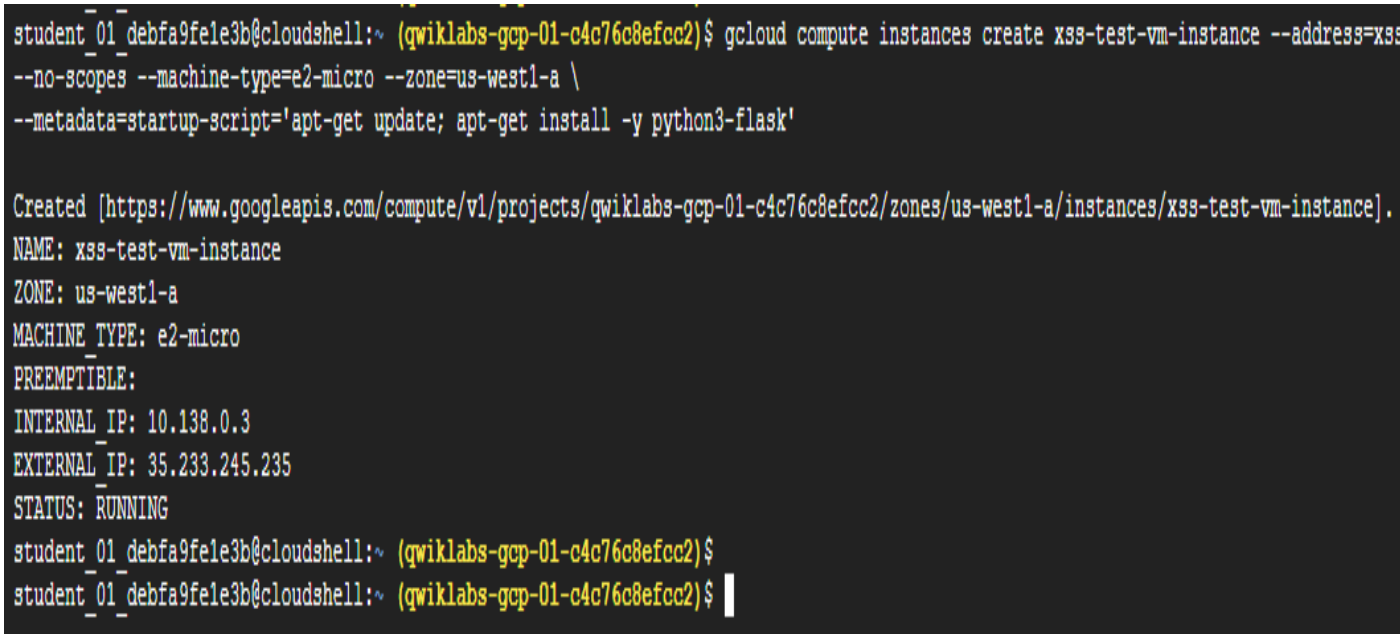


Figure 4 : Installing Python Flask on the VM instance and Creating a VM instance with a static IP address.

Figure 5 : A VM instance with a static IP address.

```
student_01_debfa9fe1e3b@cloudshell:~ (qwiklabs-gcp-01-c4c76c8efcc2)$ gcloud compute firewall-rules create enable-wss-scan \
--direction=INGRESS --priority=1000 \
--network=default --action=ALLOW \
--rules=tcp:8080 --source-ranges=0.0.0.0/0
Creating firewall...working..Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-01-c4c76c8efcc2/global/firewalls/enable-wss-scan].
Creating firewall...done.
NAME: enable-wss-scan
NETWORK: default
DIRECTION: INGRESS
PRIORITY: 1000
ALLOW: tcp:8080
DENY:
DISABLED: False
student_01_debfa9fe1e3b@cloudshell:~ (qwiklabs-gcp-01-c4c76c8efcc2)$
```

Figure 6 : Creating a firewall rule to allow Web Security Scanner access.

```
Creating firewall...working..Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-01-c4c76c8efcc2/global/firewalls/enable-wss-scan]
Creating firewall...done.
NAME: enable-wss-scan
NETWORK: default
DIRECTION: INGRESS
PRIORITY: 1000
ALLOW: tcp:8080
DENY:
DISABLED: False
```

Figure 7 : A firewall rule

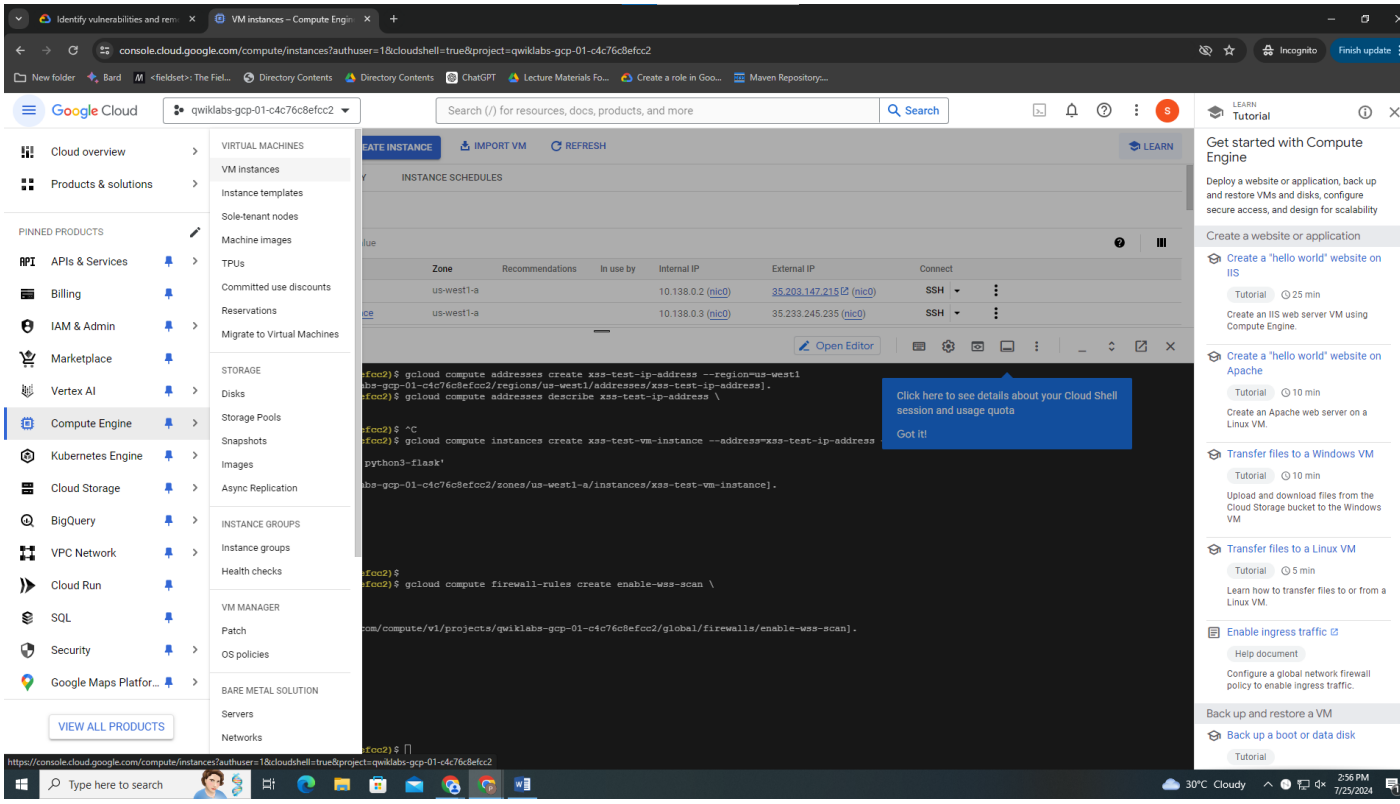


Figure 8 : Select Compute Engine > VM instances.

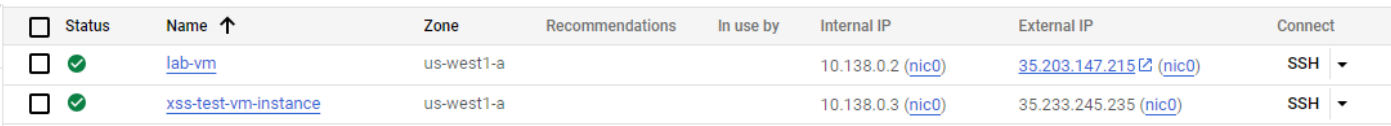


Figure 9 : VM instance name xss-test-vm- instance

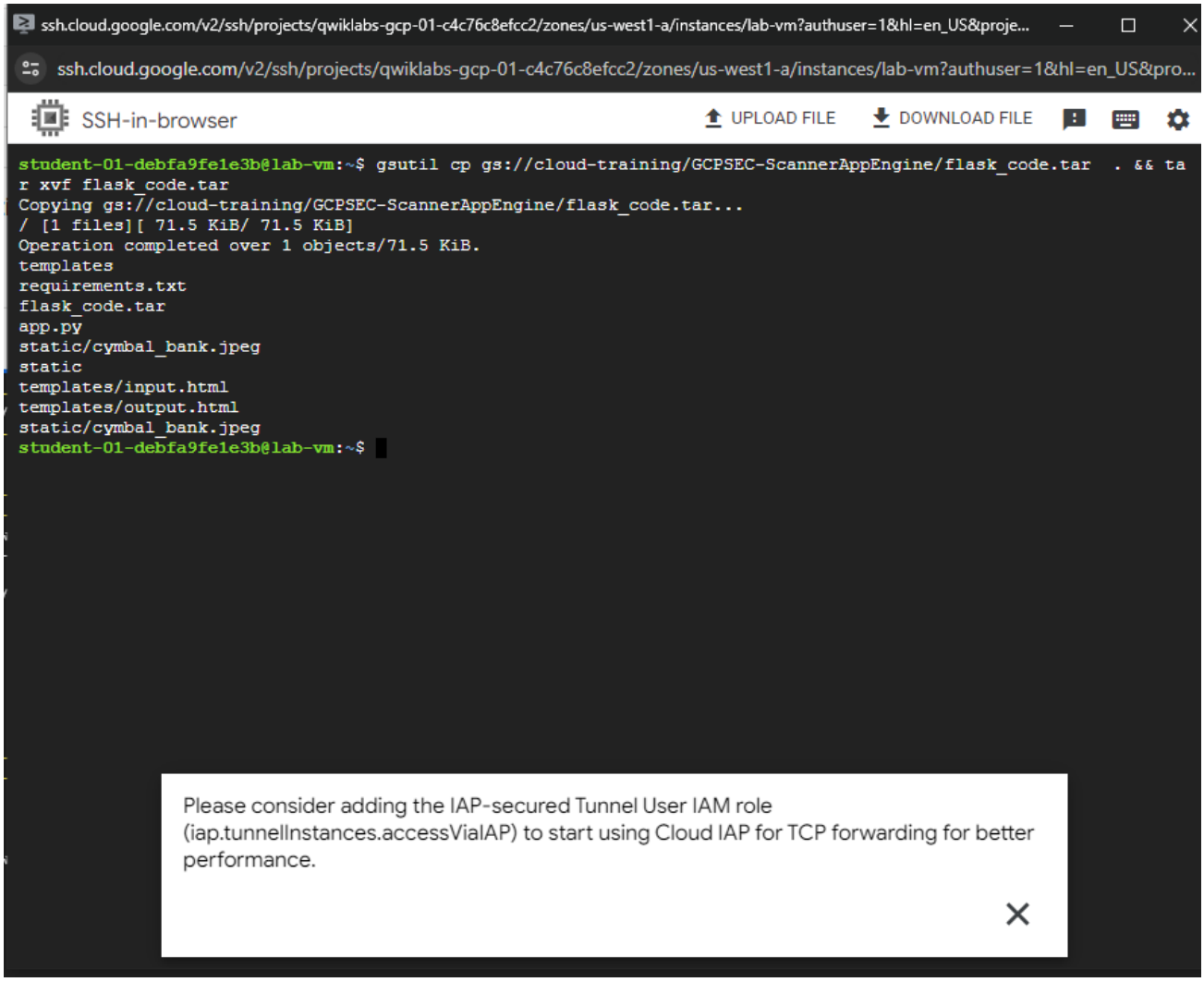


Figure 10 : Downloading and extracting the vulnerable web application files

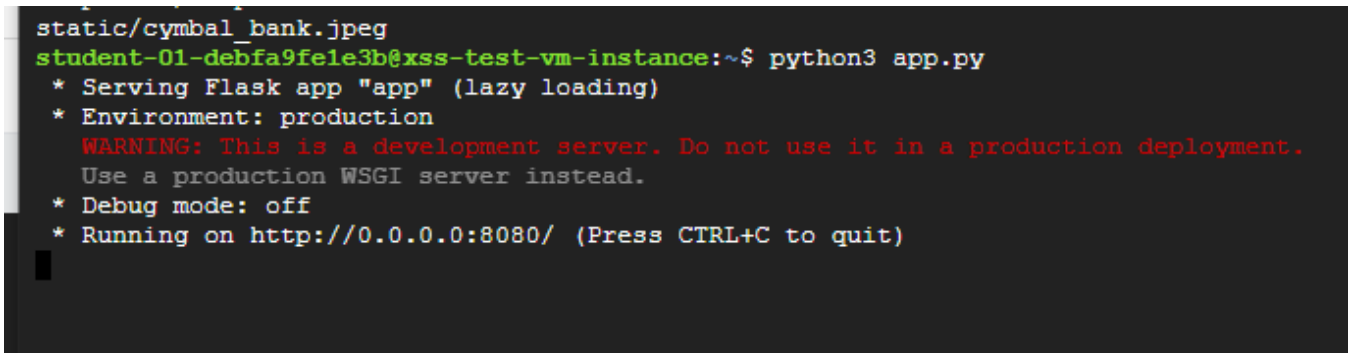


Figure 11 : Running the vulnerable application

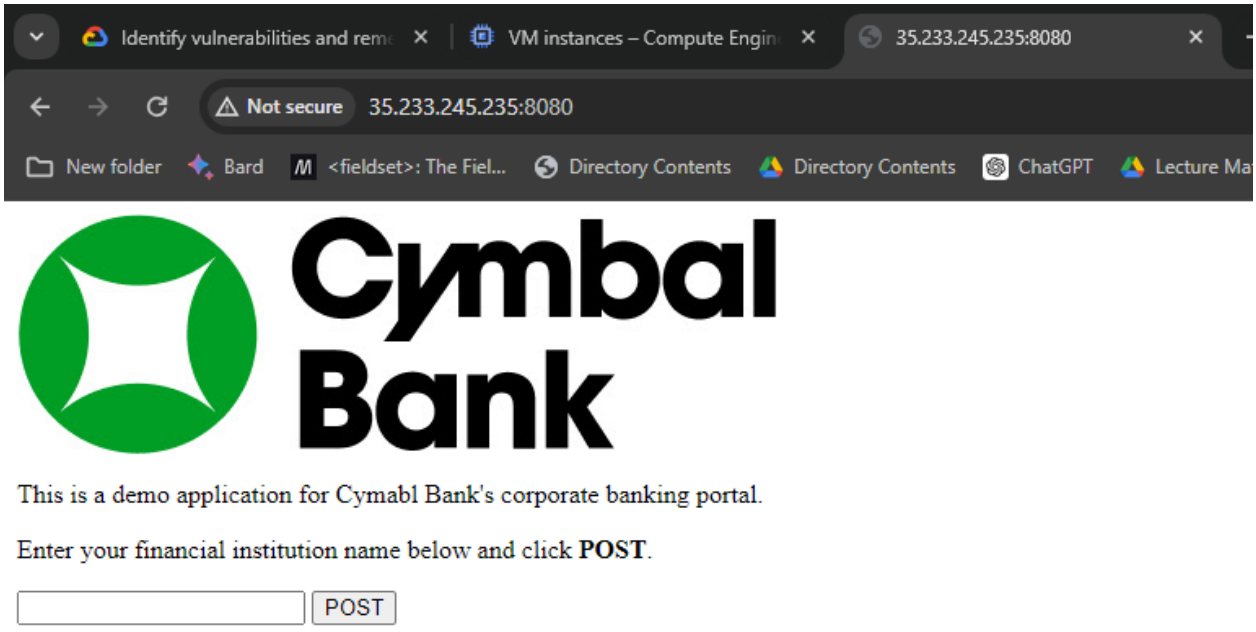


Figure 12 : Accessing the vulnerable application through a web browser.

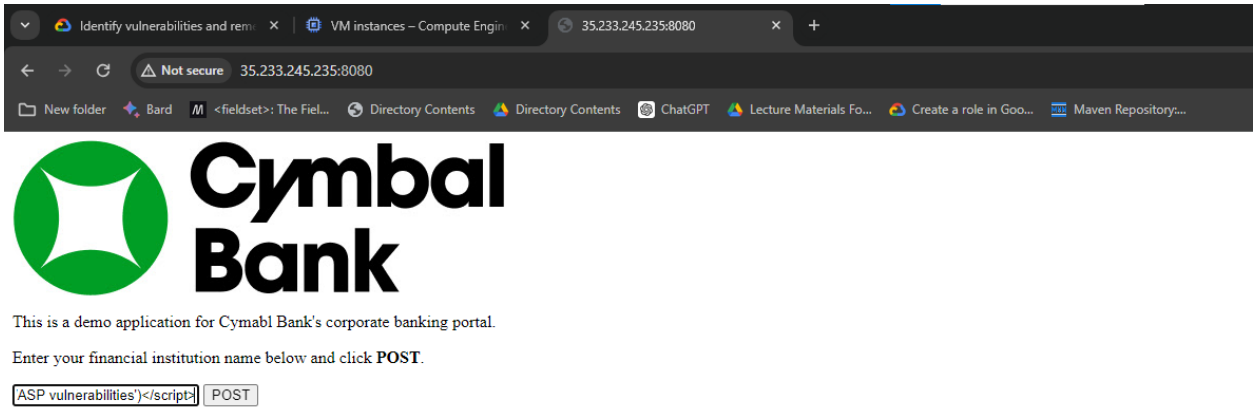


Figure 13 : Injecting an XSS script <script>alert('This is an XSS Injection to demonstrate one of OWASP vulnerabilities')</script> into the web form.

```
student-01-debfa9fe1e3b@xss-test-vm-instance:~$ python3 app.py
 * Serving Flask app "app" (lazy loading)
 * Environment: production
   WARNING: This is a development server. Do not use it in a production deployment.
   Use a production WSGI server instead.
 * Debug mode: off
 * Running on http://0.0.0.0:8080/ (Press CTRL+C to quit)
136.233.130.144 - - [25/Jul/2024 09:46:15] "GET / HTTP/1.1" 200 -
117.239.83.193 - - [25/Jul/2024 09:46:15] "GET /static/cymbal_bank.jpeg HTTP/1.1" 200 -
136.233.130.144 - - [25/Jul/2024 09:46:17] "GET /favicon.ico HTTP/1.1" 404 -
136.233.130.144 - - [25/Jul/2024 09:46:53] "POST / HTTP/1.1" 302 -
117.239.83.193 - - [25/Jul/2024 09:46:53] "GET /output HTTP/1.1" 200 -
136.233.130.144 - - [25/Jul/2024 09:47:12] "GET / HTTP/1.1" 200 -
117.239.83.193 - - [25/Jul/2024 09:47:14] "POST / HTTP/1.1" 302 -
136.233.130.144 - - [25/Jul/2024 09:47:15] "GET /output HTTP/1.1" 200 -
```

Figure 14 : Viewing scan logs in the SSH window.

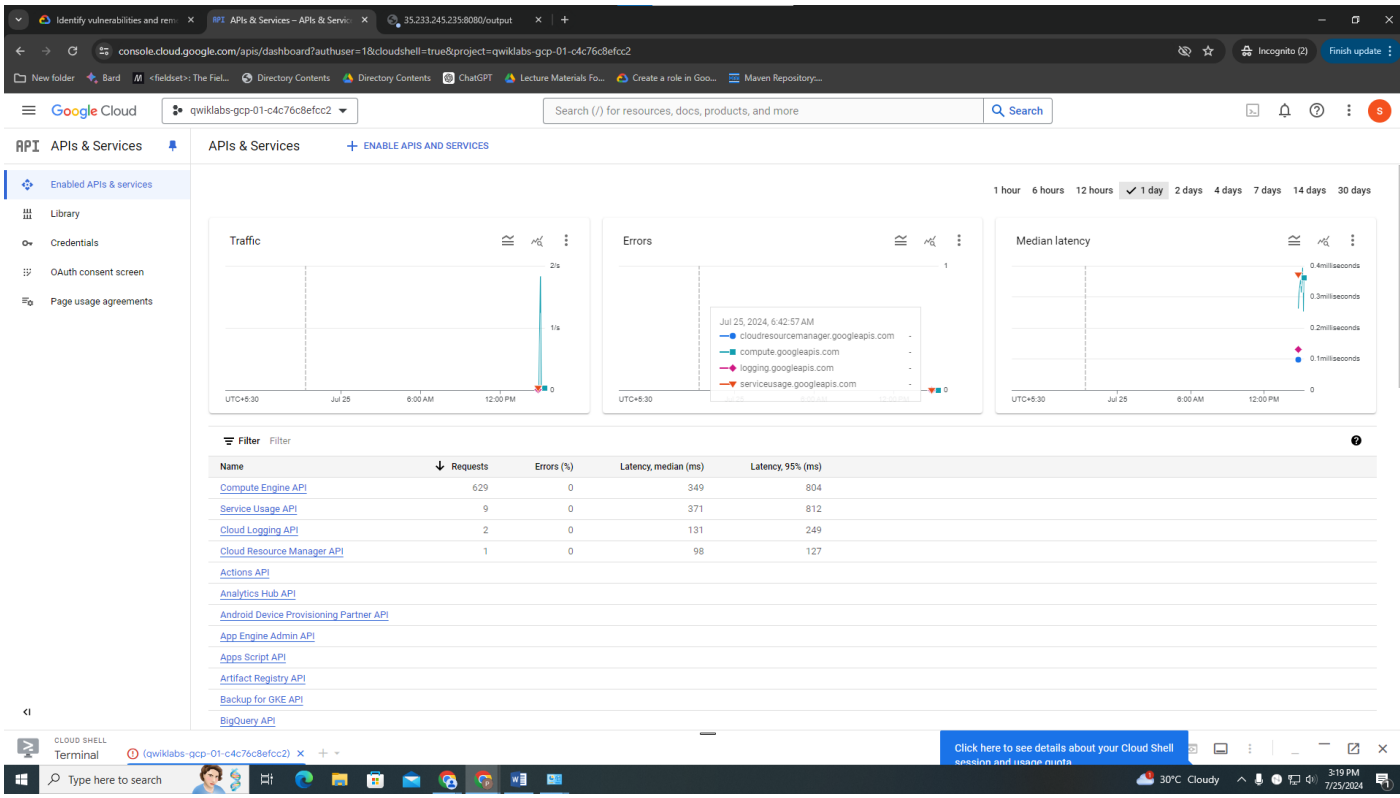


Figure 15 : Select APIs & Services > Enabled APIs and services. The APIs & Services page displays.

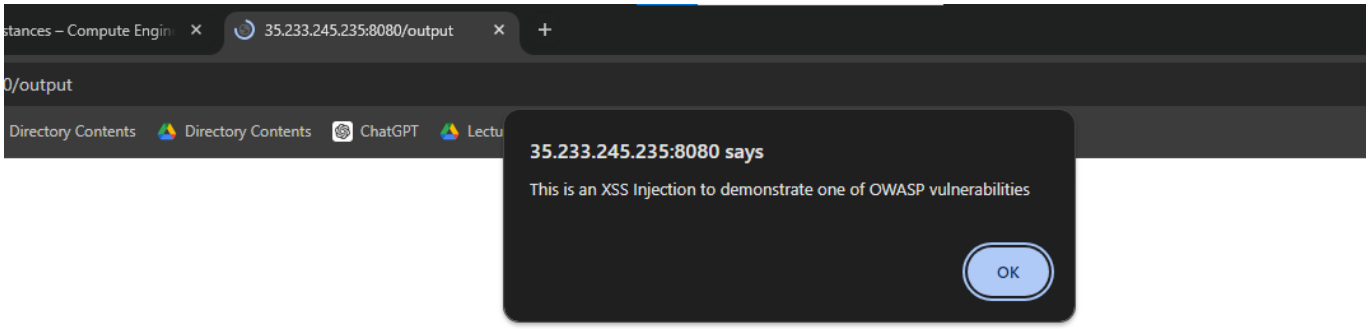


Figure 16 : XSS vulnerability demonstration with alert message.

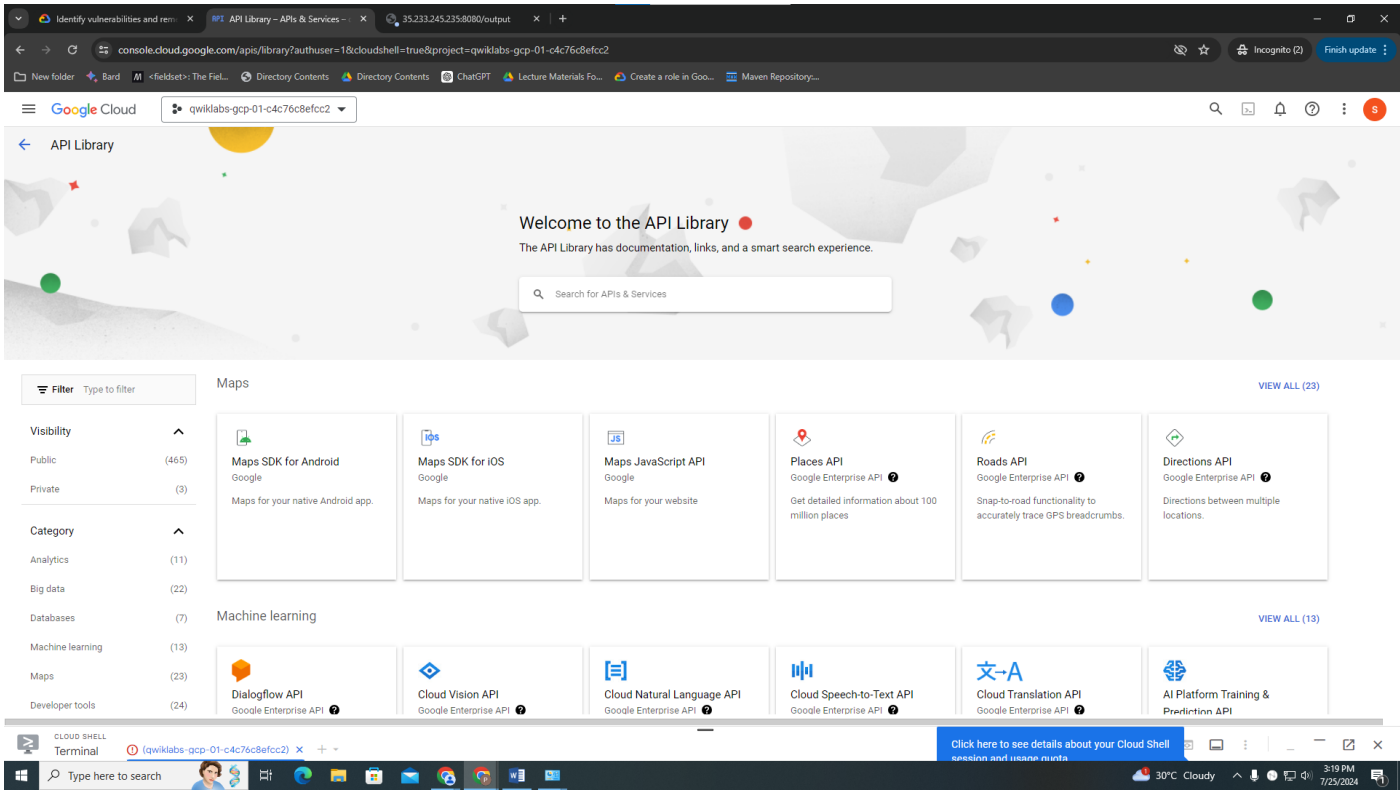


*Figure 17 : In the search field, type **Web Security Scanner**, and press **ENTER**.*

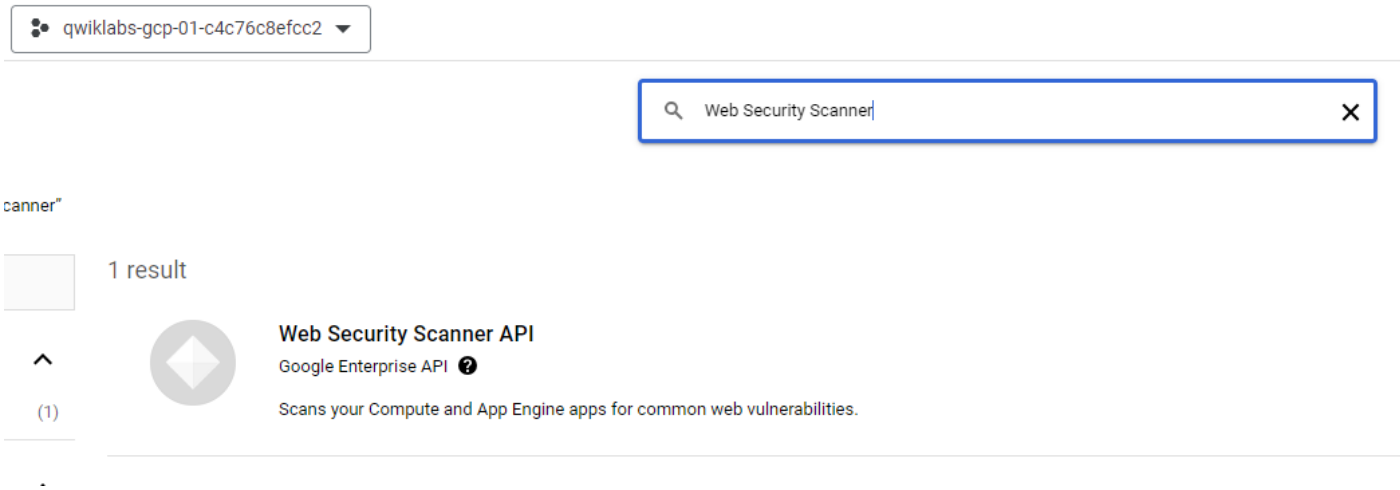


Figure 18

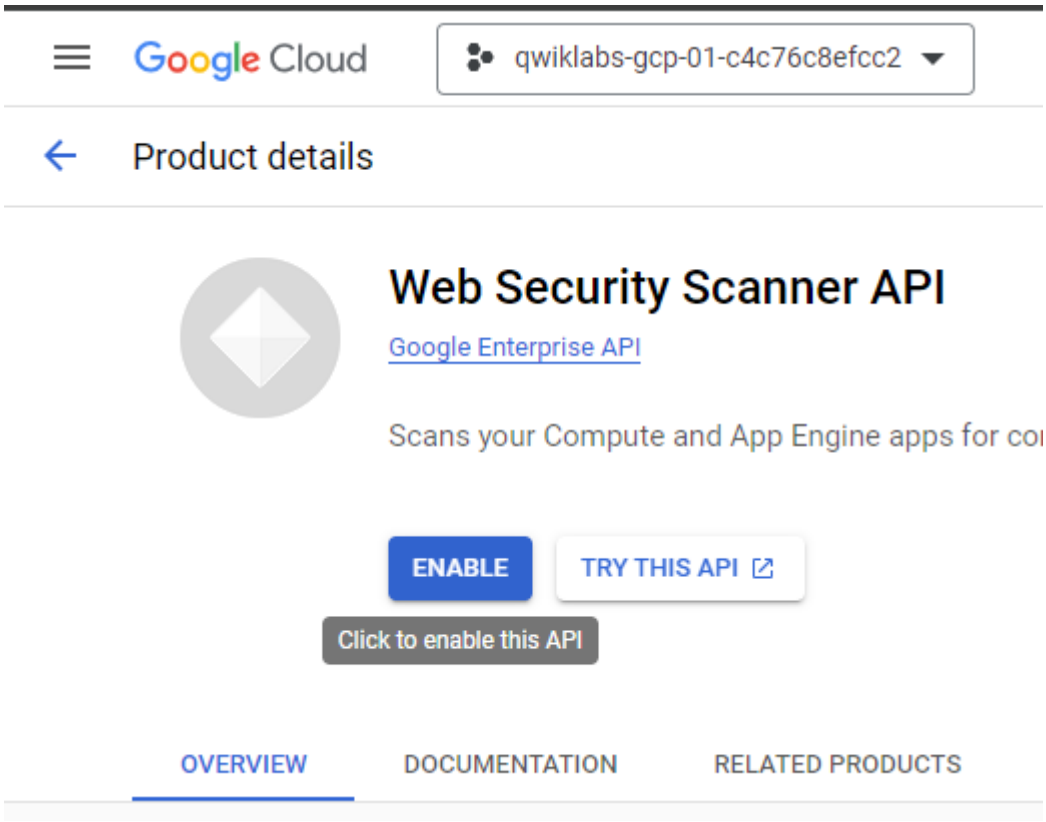


*Figure 19 : Select **Web Security Scanner API**.*

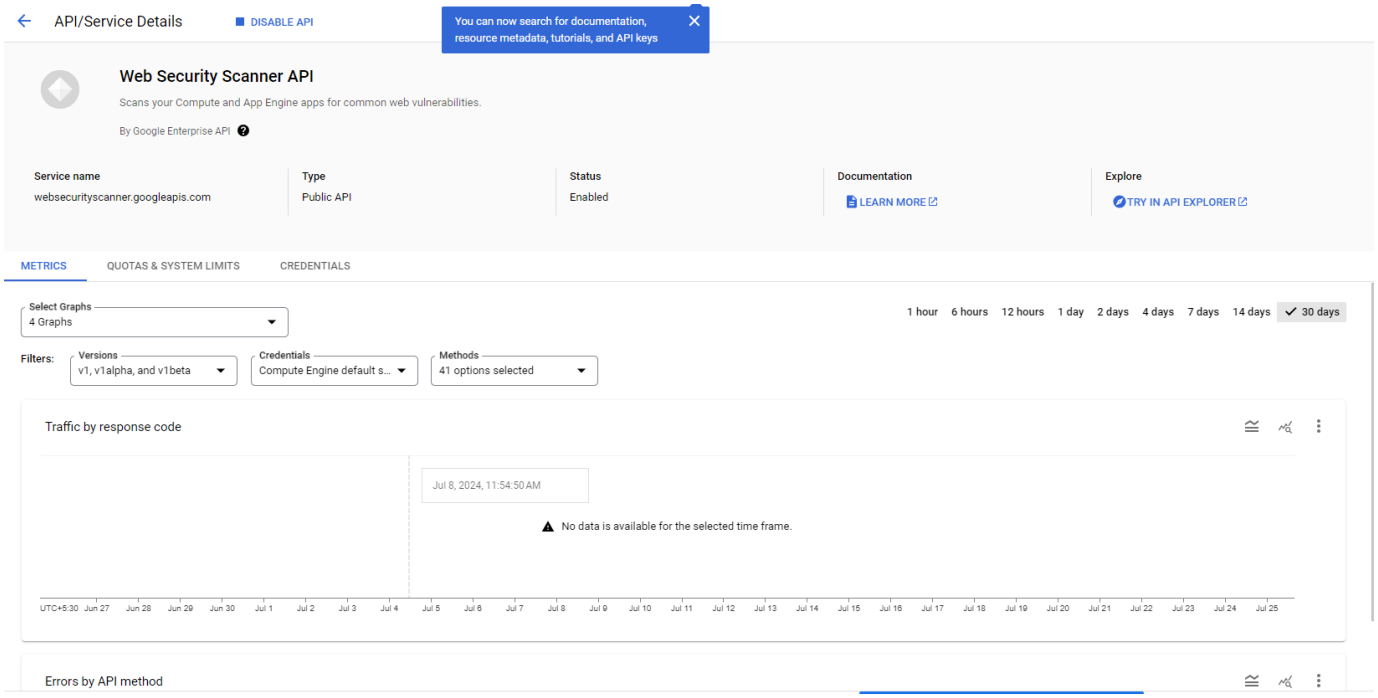


Figure 20 : Enabling the Web Security Scanner API.

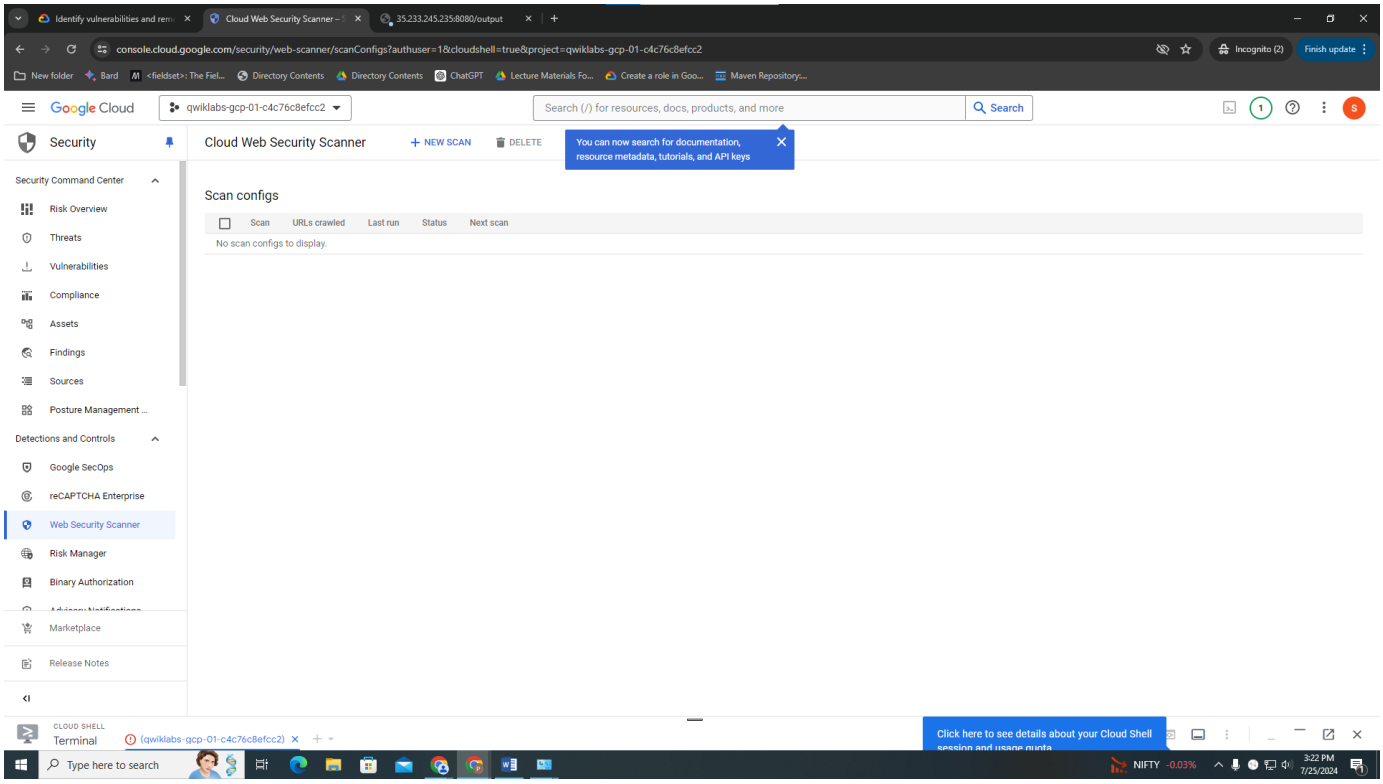


*Figure 21 : In the **Cloud Web Security Scanner** toolbar, click **+ New scan**.*

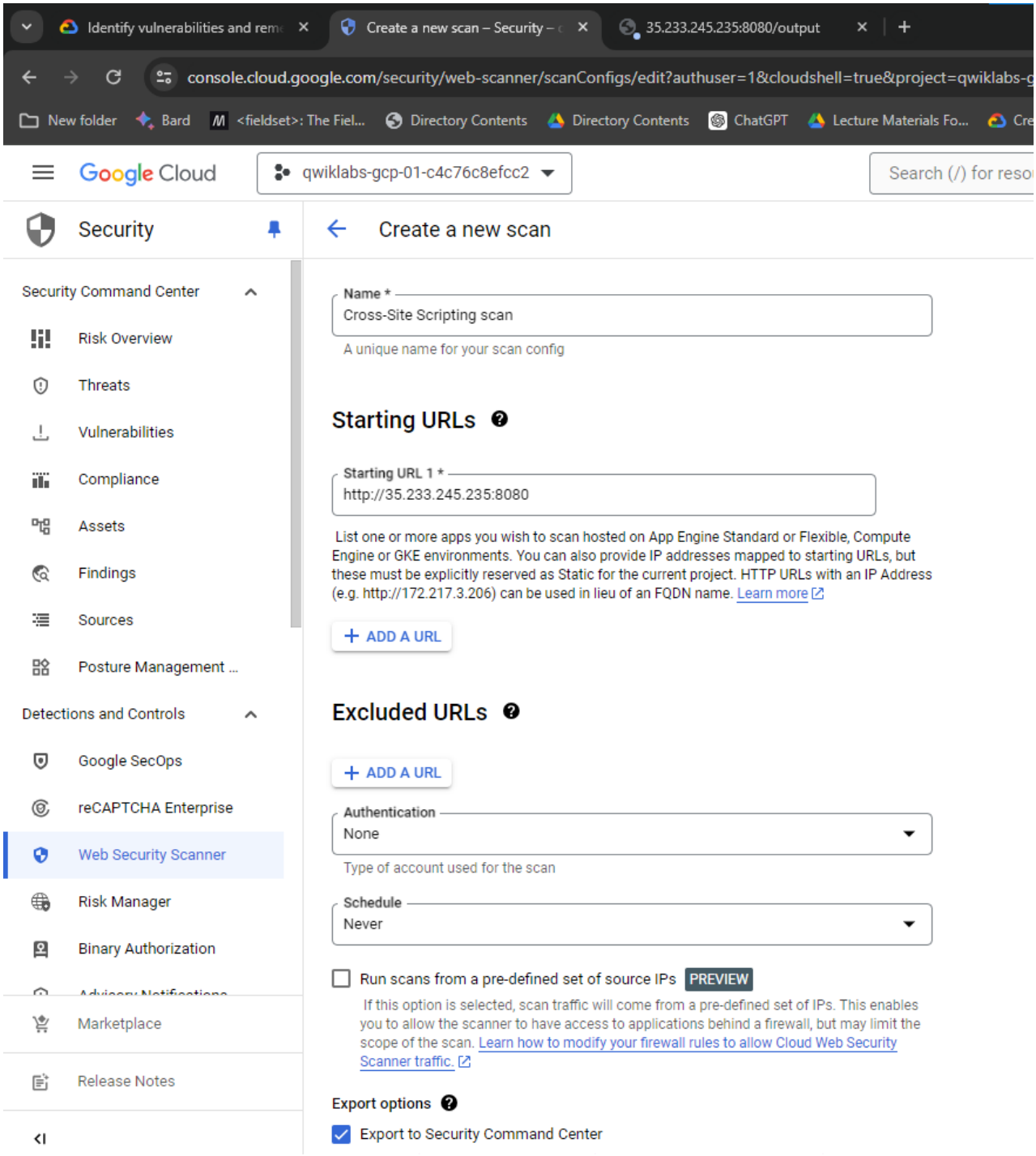


Figure 22 : Creating a new scan configuration in Web Security Scanner and Setting the starting URL for the scan with http://35.233.245.235:8080.

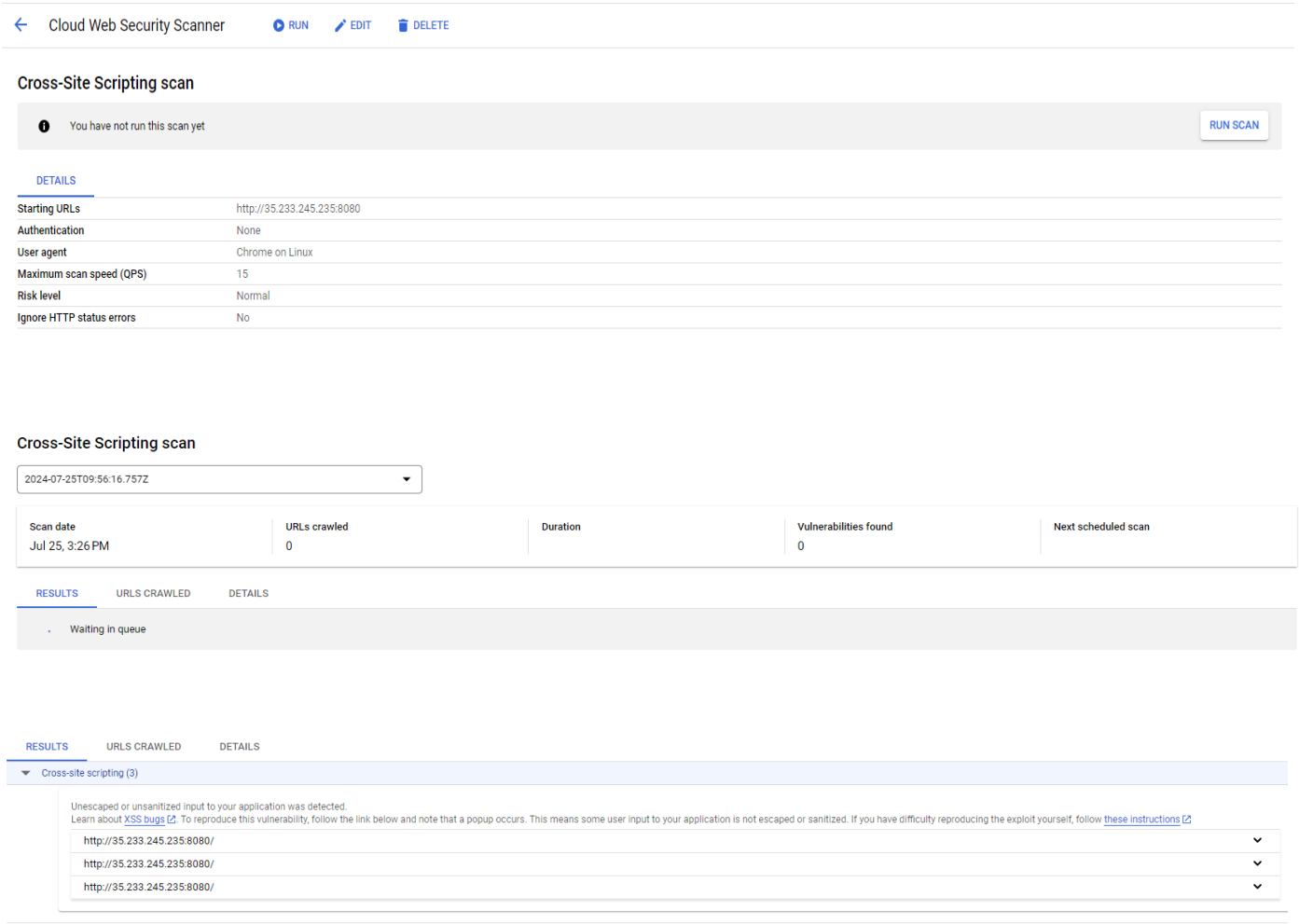


Figure 23 : Running the security scan on the application.

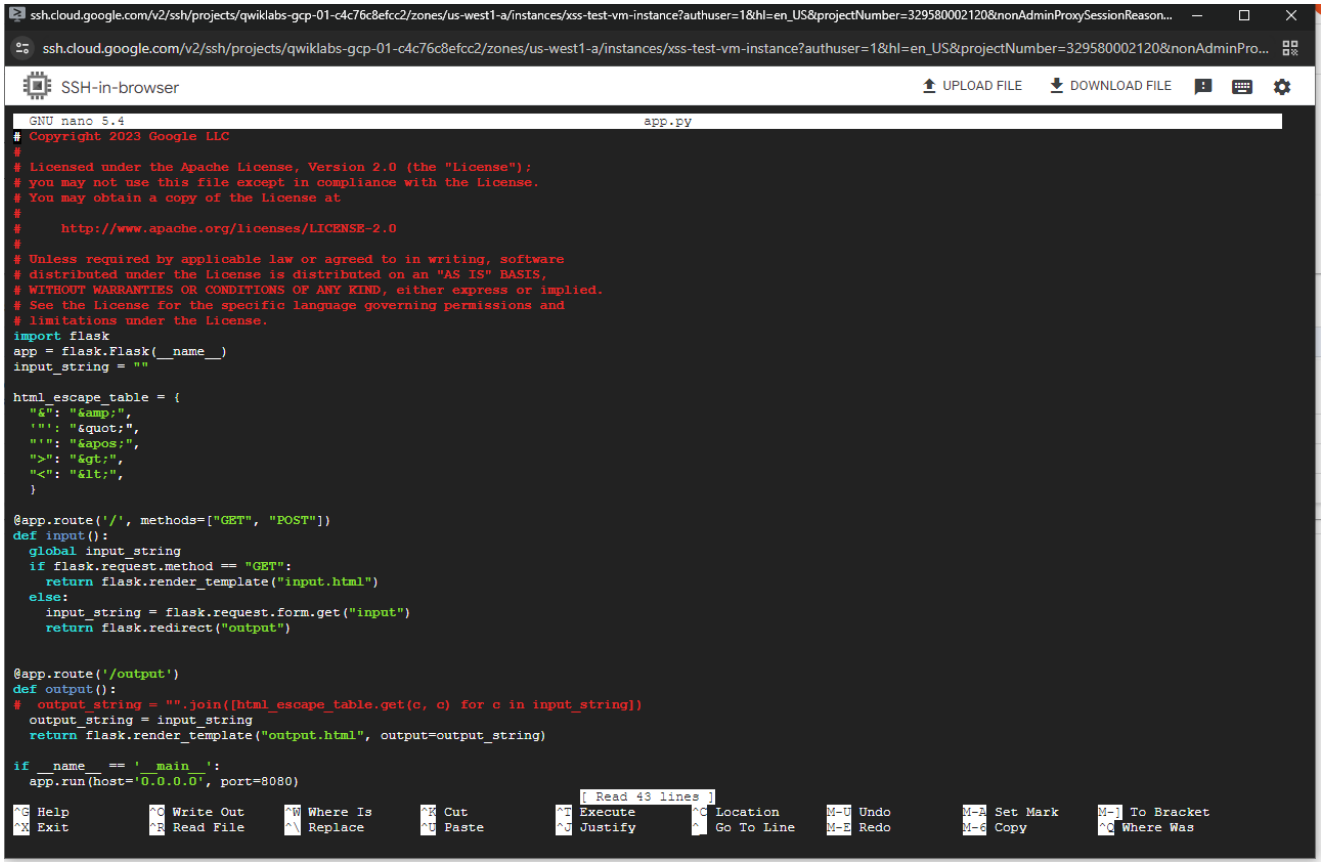


Figure 24 : Editing the application code to fix XSS vulnerabilities.

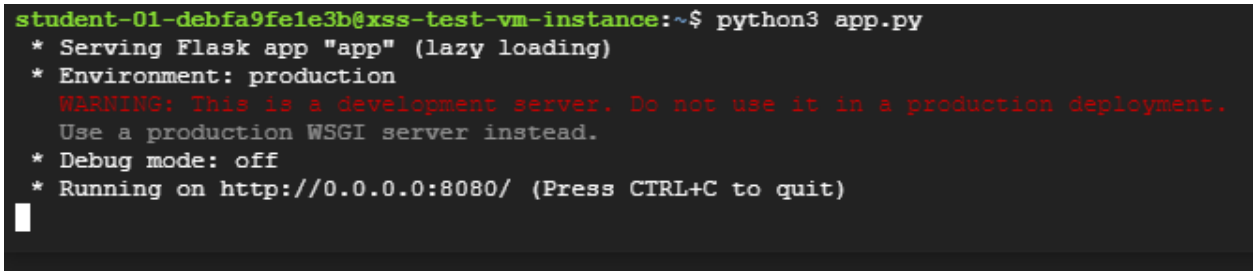


Figure 25 : Re-running the application with the updated code.

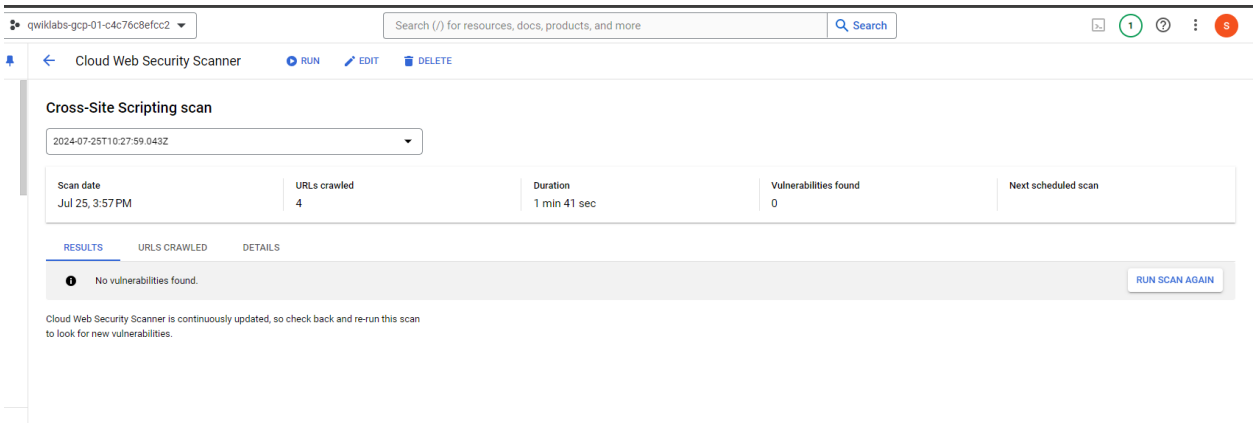
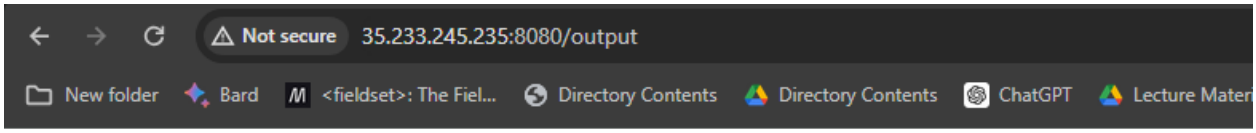


Figure 26 : Re-scanning the application to verify no vulnerabilities.



<script>alert('This is an XSS Injection to demonstrate one of OWASP vulnerabilities')</script>

Figure 27 : Demonstration of a secure web form without XSS vulnerabilities.

```
74.125.210.174 - - [25/Jul/2024 10:29:17] "GET / HTTP/1.1" 200 -
74.125.210.174 - - [25/Jul/2024 10:29:17] "GET /.svn/wc.db HTTP/1.1" 404 -
74.125.210.173 - - [25/Jul/2024 10:29:17] "GET /.git/config HTTP/1.1" 404 -
[2024-07-25 10:29:18,204] ERROR in app: Exception on /output [GET]
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/flask/app.py", line 2447, in wsgi_app
    response = self.full_dispatch_request()
  File "/usr/lib/python3/dist-packages/flask/app.py", line 1952, in full_dispatch_request
    rv = self.handle_user_exception(e)
  File "/usr/lib/python3/dist-packages/flask/app.py", line 1821, in handle_user_exception
    reraise(exc_type, exc_value, tb)
  File "/usr/lib/python3/dist-packages/flask/_compat.py", line 39, in reraise
    raise value
  File "/usr/lib/python3/dist-packages/flask/app.py", line 1950, in full_dispatch_request
    rv = self.dispatch_request()
  File "/usr/lib/python3/dist-packages/flask/app.py", line 1936, in dispatch_request
    return self.view_functions[rule.endpoint](**req.view_args)
  File "/home/student-01-debfa9fe1e3b/app.py", line 38, in output
    output_string = "".join([html_escape_table.get(c, c) for c in input_string])
TypeError: 'NoneType' object is not iterable
74.125.210.173 - - [25/Jul/2024 10:29:18] "GET /output HTTP/1.1" 500 -
66.249.83.111 - - [25/Jul/2024 10:29:18] "GET /.git/config HTTP/1.1" 404 -
74.125.210.173 - - [25/Jul/2024 10:29:18] "GET /output/.git/config HTTP/1.1" 404 -
74.125.210.174 - - [25/Jul/2024 10:29:18] "GET /.svn/wc.db HTTP/1.1" 404 -
74.125.210.173 - - [25/Jul/2024 10:29:18] "GET /output/.svn/wc.db HTTP/1.1" 404 -
74.125.215.46 - - [25/Jul/2024 10:29:20] "POST / HTTP/1.1" 302 -
74.125.215.45 - - [25/Jul/2024 10:29:20] "GET /output HTTP/1.1" 200 -
74.125.215.45 - - [25/Jul/2024 10:29:21] "POST / HTTP/1.1" 302 -
74.125.215.45 - - [25/Jul/2024 10:29:21] "GET /output HTTP/1.1" 200 -
74.125.215.46 - - [25/Jul/2024 10:29:22] "POST / HTTP/1.1" 302 -
74.125.215.46 - - [25/Jul/2024 10:29:23] "GET /output HTTP/1.1" 200 -
74.125.215.32 - - [25/Jul/2024 10:29:24] "POST / HTTP/1.1" 302 -
74.125.215.45 - - [25/Jul/2024 10:29:24] "GET /output HTTP/1.1" 200 -
74.125.215.32 - - [25/Jul/2024 10:29:24] "POST / HTTP/1.1" 302 -
74.125.215.45 - - [25/Jul/2024 10:29:24] "GET /output HTTP/1.1" 200 -
74.125.215.32 - - [25/Jul/2024 10:29:26] "POST / HTTP/1.1" 302 -
74.125.215.46 - - [25/Jul/2024 10:29:26] "GET /output HTTP/1.1" 200 -
74.125.215.46 - - [25/Jul/2024 10:29:27] "GET / HTTP/1.1" 200 -
74.125.215.32 - - [25/Jul/2024 10:29:27] "GET /static/cymbal_bank.jpeg HTTP/1.1" 200 -
74.125.215.32 - - [25/Jul/2024 10:29:28] "GET / HTTP/1.1" 200 -
74.125.215.45 - - [25/Jul/2024 10:29:29] "GET /static/cymbal_bank.jpeg HTTP/1.1" 200 -
74.125.215.45 - - [25/Jul/2024 10:29:29] "GET / HTTP/1.1" 200 -
74.125.215.32 - - [25/Jul/2024 10:29:29] "GET /static/cymbal_bank.jpeg HTTP/1.1" 200 -
74.125.215.45 - - [25/Jul/2024 10:29:30] "GET / HTTP/1.1" 200 -
74.125.215.32 - - [25/Jul/2024 10:29:30] "GET /static/cymbal_bank.jpeg HTTP/1.1" 200 -
74.125.215.45 - - [25/Jul/2024 10:29:32] "GET /output HTTP/1.1" 200 -
74.125.215.32 - - [25/Jul/2024 10:29:33] "GET /output HTTP/1.1" 200 -
74.125.215.45 - - [25/Jul/2024 10:29:36] "GET /output HTTP/1.1" 200 -
74.125.215.32 - - [25/Jul/2024 10:29:37] "GET /output HTTP/1.1" 200 -
117.239.83.193 - - [25/Jul/2024 10:30:32] "POST / HTTP/1.1" 302 -
117.239.83.193 - - [25/Jul/2024 10:30:32] "GET /output HTTP/1.1" 200 -
```

Figure 28 : Viewing the re-scan results indicating no vulnerabilities.

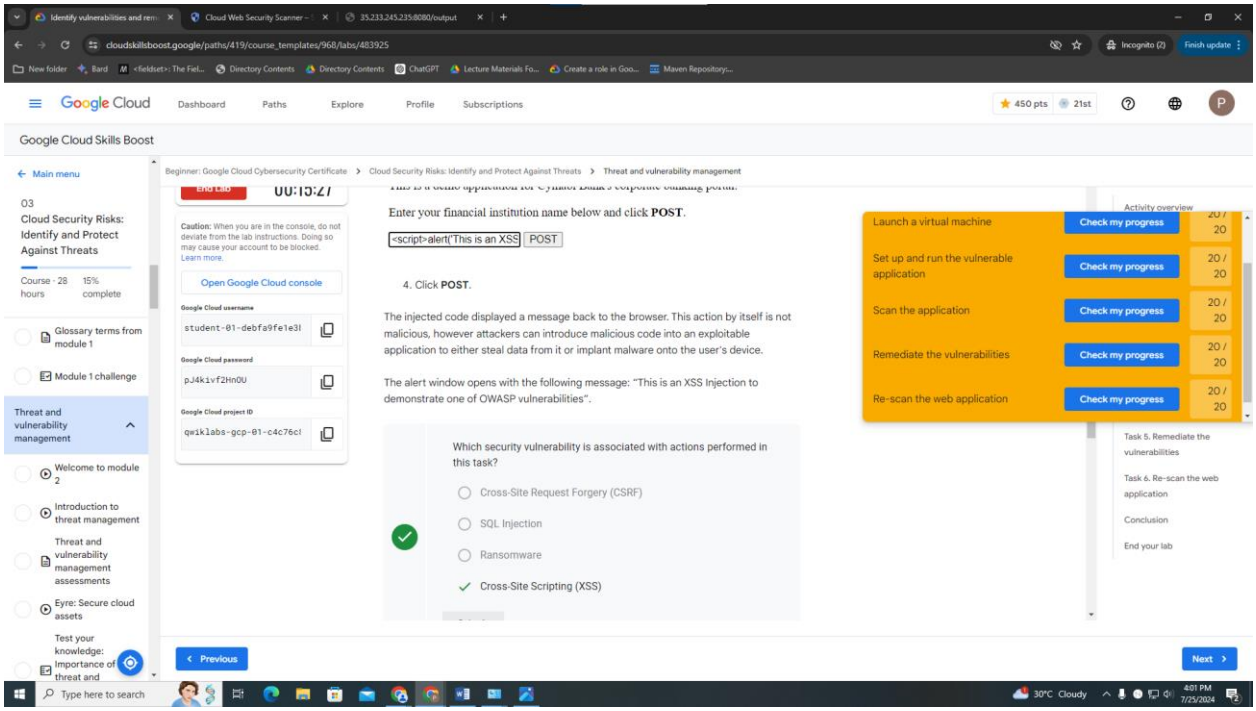


Figure 29 : Earning all points and ending the lab.

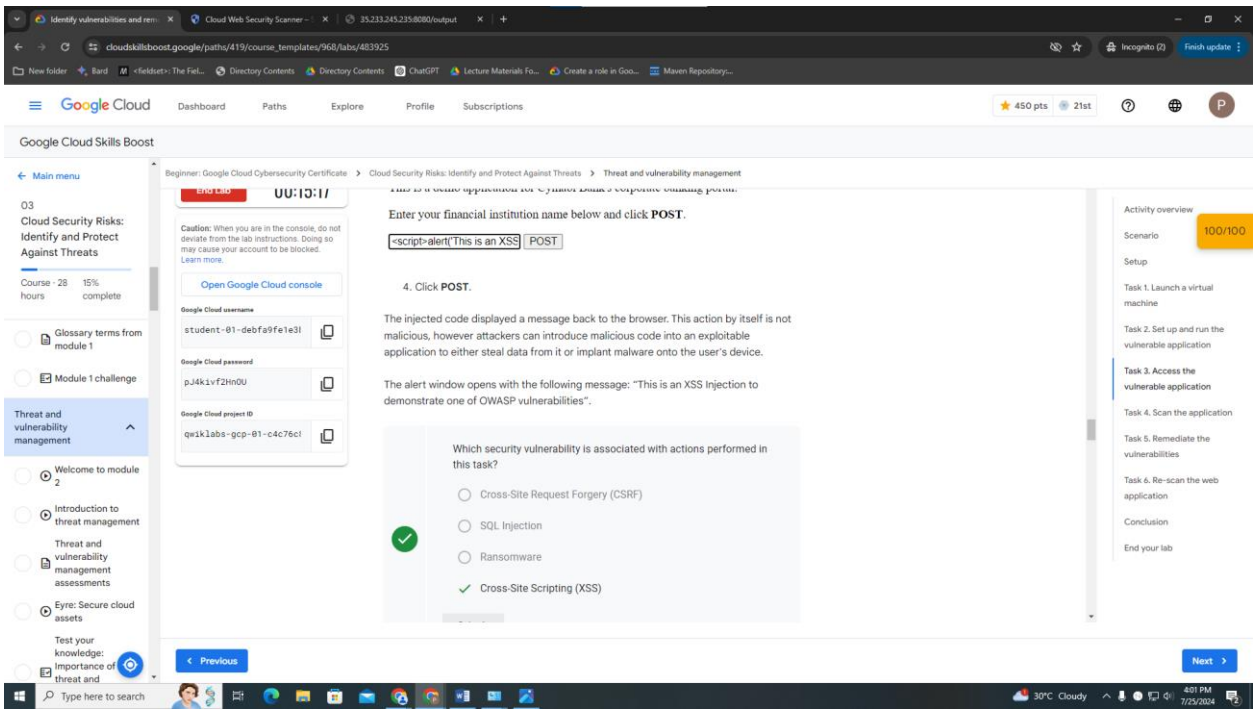


Figure 30 : MCQ

LATEST APPLICATIONS:

Cloud Security: Utilizing cloud-based tools and services to identify and remediate security vulnerabilities in web applications, ensuring data protection and compliance.

DevSecOps: Integrating security practices within the DevOps workflow to continuously monitor and address security issues throughout the development lifecycle.

Web Application Security: Implementing robust security measures in web applications to prevent common vulnerabilities like XSS, SQL injection, and CSRF.

LEARNING OUTCOME:

By completing this practical, you will gain hands-on experience with identifying and remediating web application vulnerabilities using Google Cloud tools. You will learn how to:

1. Set up and configure a vulnerable web application in Google Cloud.
2. Use vulnerability scanning tools to detect security issues.
3. Implement remediation techniques to secure the application.
4. Understand the importance of regular vulnerability assessments in maintaining application security.

REFERENCES:

OWASP (Open Web Application Security Project) : https://owasp.org

Google Cloud Documentation : https://cloud.google.com/docs

Nmap: Network Mapper : https://nmap.org

Nessus: Vulnerability Scanner : https://www.tenable.com/products/nessus

Burp Suite: Web Vulnerability Scanner : https://portswigger.net/burp

PRACTICAL: 7

AIM:

Encryption is a critical component for protecting data in cloud environments. Security professionals use cryptography to transform information into a form that unintended readers can't understand. Symmetric and asymmetric keys are cryptographic tools used to secure data and enable secure communication over networks. Each type of key has its own distinct differences and can be deployed for different situations. Symmetric Keys: Symmetric key cryptography uses a single key to encrypt and decrypt data. The same key is used by both the sender and the recipient which is why it's called symmetric. Symmetric key cryptography is efficient and fast. Asymmetric Keys: Asymmetric key cryptography (also known as public-key cryptography) uses a pair of keys: a public key and a private key. One of the keys is used to encrypt data, while the other key decrypts data. These keys are mathematically related but cannot be derived from each other. Asymmetric cryptography is known for its slow performance. This is due to the use of these two mathematically related keys which are longer than those used in symmetric encryption. In practice, many secure communication systems use a combination of symmetric and asymmetric cryptography to achieve both efficiency and security. For example, the Hypertext Transfer Protocol Secure (HTTPS) protocol uses asymmetric cryptography for the initial handshake to establish a secure connection, and then switches to symmetric encryption for the actual data transfer. One of the major problems with symmetric key cryptography involves key distribution. How do you ensure the secure exchange of keys without having the key be compromised or stolen? Asymmetric key cryptography solves this problem by using a public and private key pair. However ,it is computationally more expensive, so it's commonly used for initial key exchange and digital signatures, while symmetric keys are used for the bulk encryption of data. In this experiment, you'll create both a symmetric key and an asymmetric key to address a request for more space to securely store data.

THEORY:

Cryptography Overview: Cryptography is the science of securing communication and data through the use of mathematical techniques. It is an essential tool for protecting sensitive information in digital systems, ensuring that data remains confidential, authentic, and intact during transmission and storage. Cryptography is widely used in various applications, including secure communications, digital signatures, data protection, and authentication.

Symmetric Key Cryptography: Symmetric key cryptography, also known as secret-key cryptography, involves the use of a single key for both encryption and decryption. The same key is shared between the communicating parties, and it must be kept secret from unauthorized entities. The simplicity of using one key makes symmetric encryption fast and efficient, making it ideal for encrypting large volumes of data. However, the challenge lies in securely distributing and managing the key, as it must be shared between parties without being compromised.

Asymmetric Key Cryptography: Asymmetric key cryptography, also known as public-key cryptography, uses a pair of keys: a public key and a private key. The public key is freely distributed and can be used by anyone to encrypt data, while the private key is kept secret by the owner and is used to decrypt the data. This method eliminates the need for secure key distribution, as only the private key must be protected. Asymmetric cryptography is widely used for secure key exchanges, digital signatures, and ensuring the authenticity of messages. However, it is computationally more intensive than symmetric cryptography and is typically used in conjunction with symmetric encryption for efficiency.

Practical Implementation: In modern systems, a combination of symmetric and asymmetric cryptography is often used to leverage the strengths of both. For example, in secure communication protocols like HTTPS, asymmetric encryption is used to securely exchange a symmetric key, which is then used for encrypting the actual data being transmitted. This approach provides both the security of asymmetric cryptography and the efficiency of symmetric cryptography, making it a robust solution for securing data in transit and at rest.

OUTPUT:

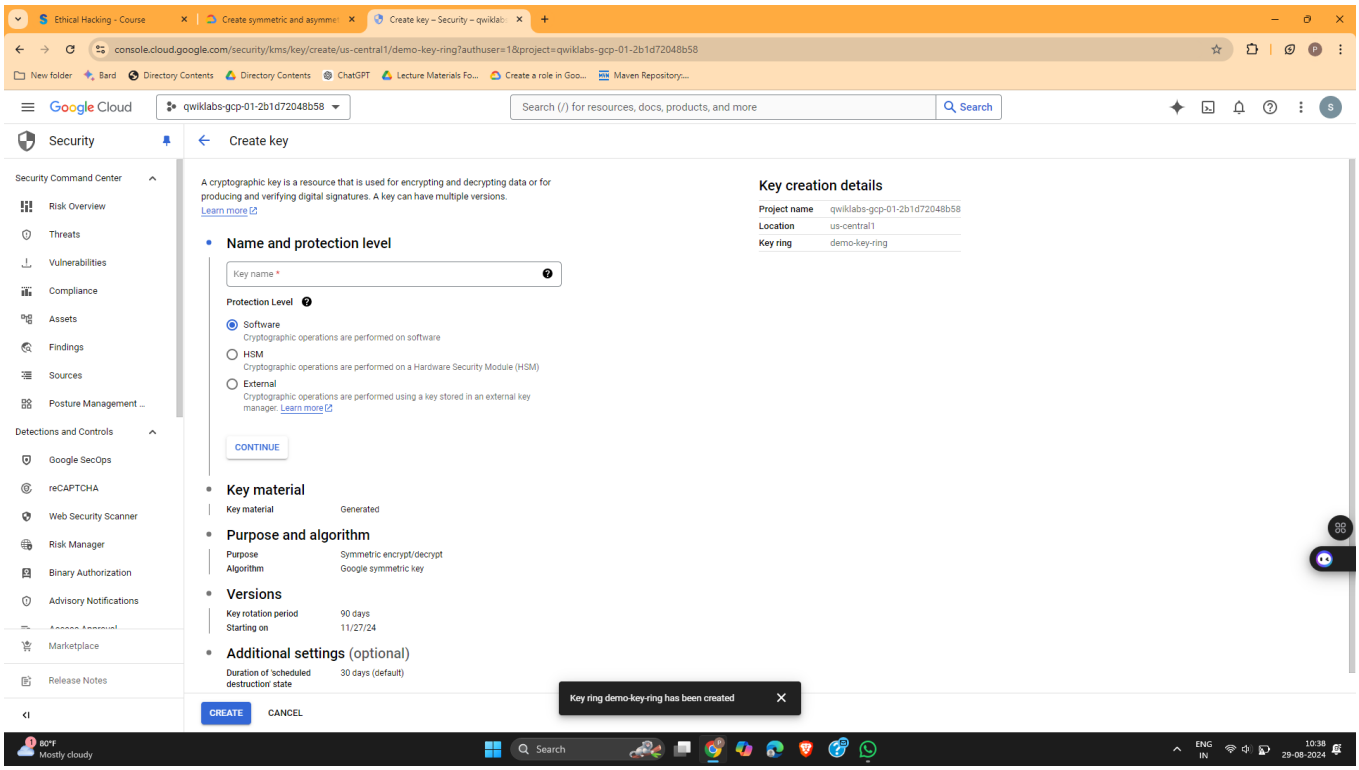


Figure 1 : This figure shows the "Create Key Ring" page in the Google Cloud console, where the user is entering the name demo-key-ring and selecting the region for the key ring.

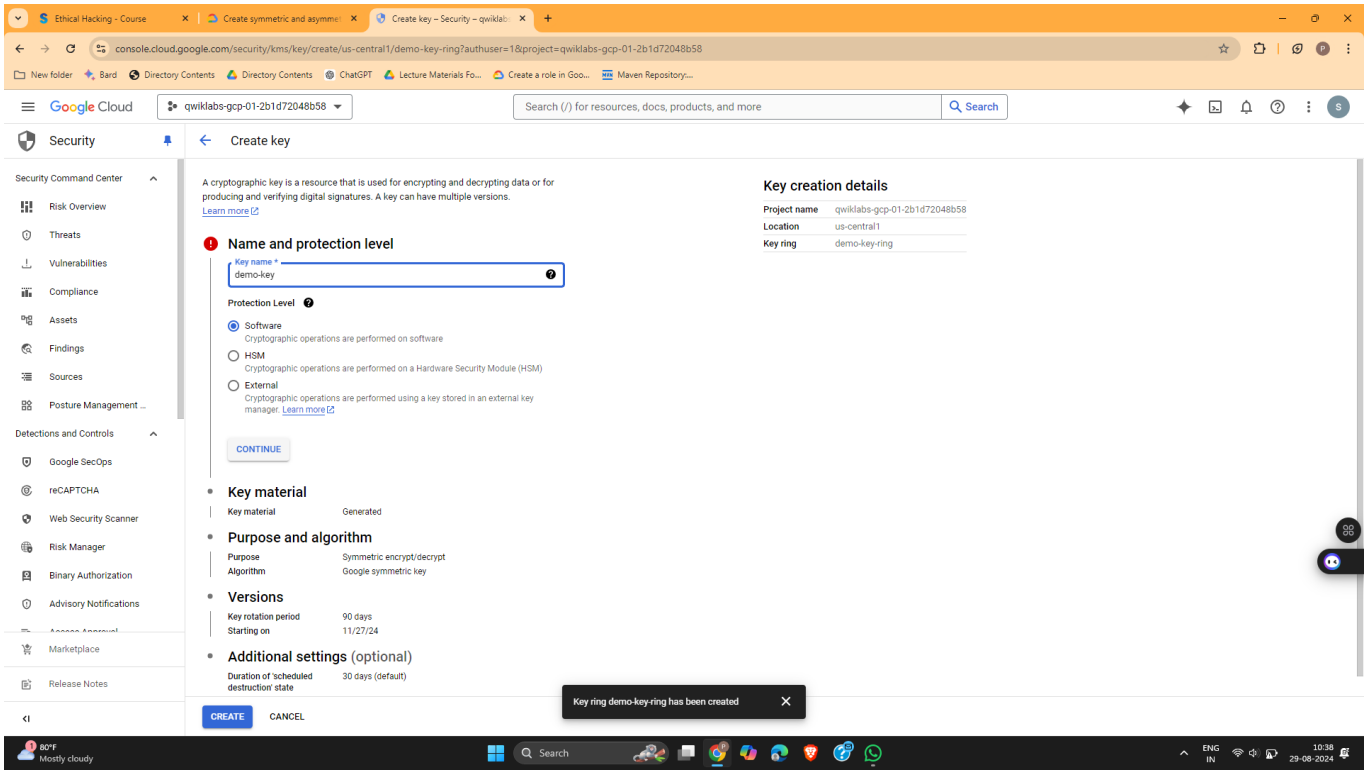


Figure 2 : This figure shows the "Key Details" form, where the user specifies the key name as demo-key and sets the protection level to "Software".

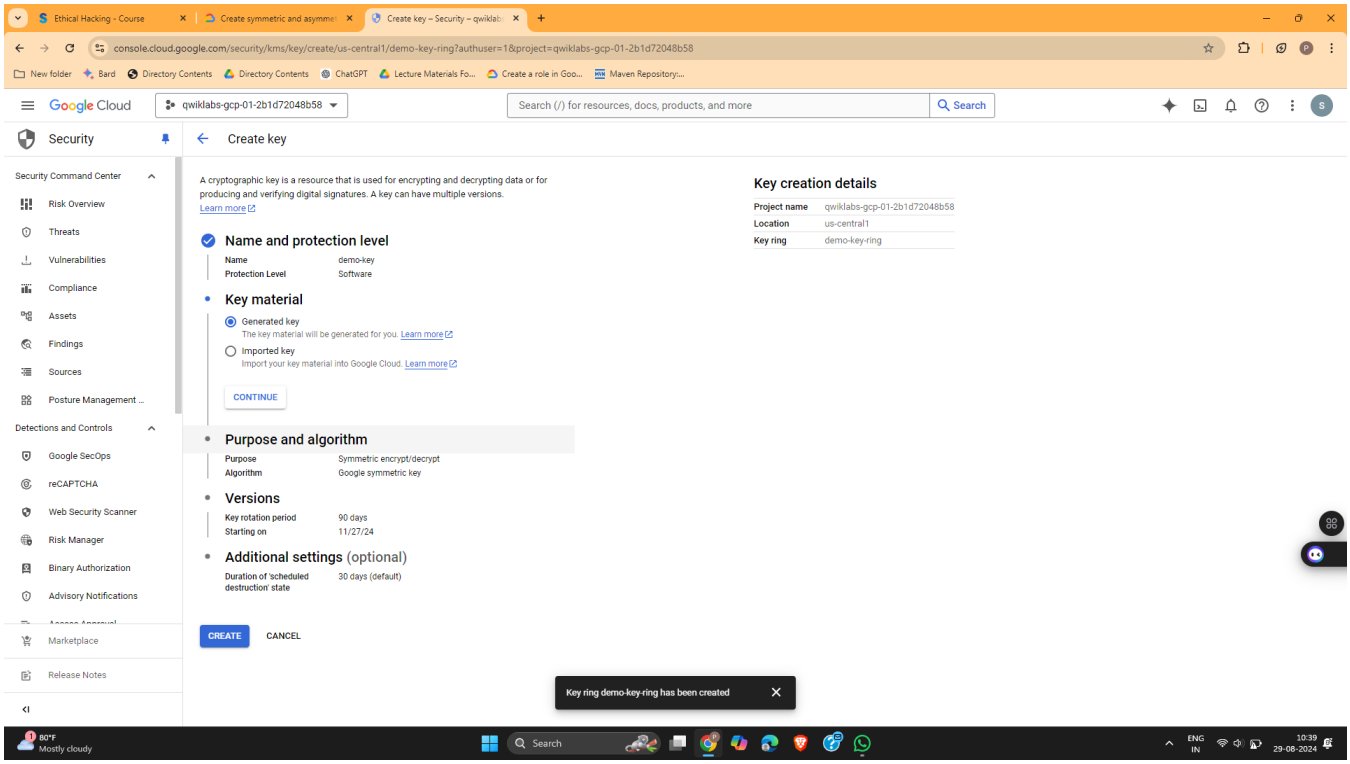


Figure 3 : This figure illustrates the options selected for the symmetric key material generation, including "Generated key"

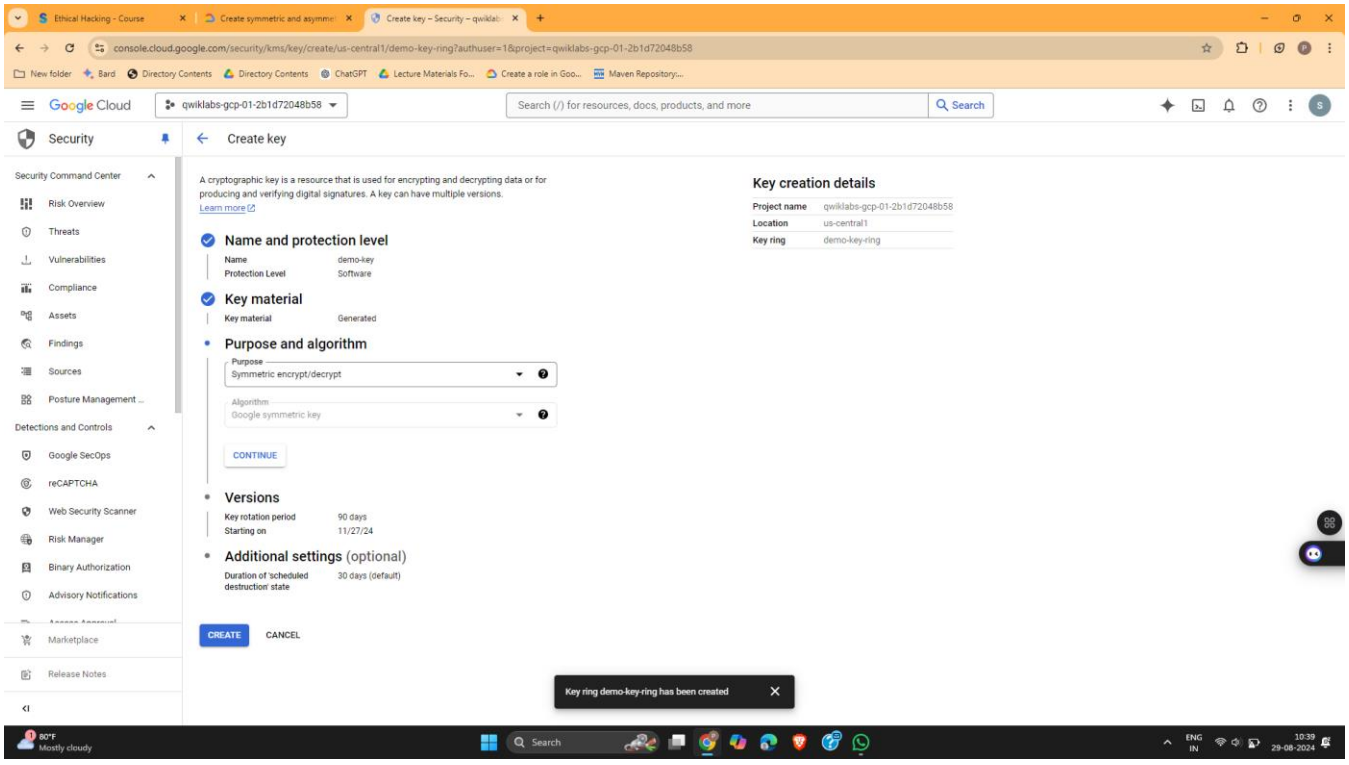


Figure 4 : This figure illustrates the options selected for the purpose set to "Symmetric encrypt/decrypt".

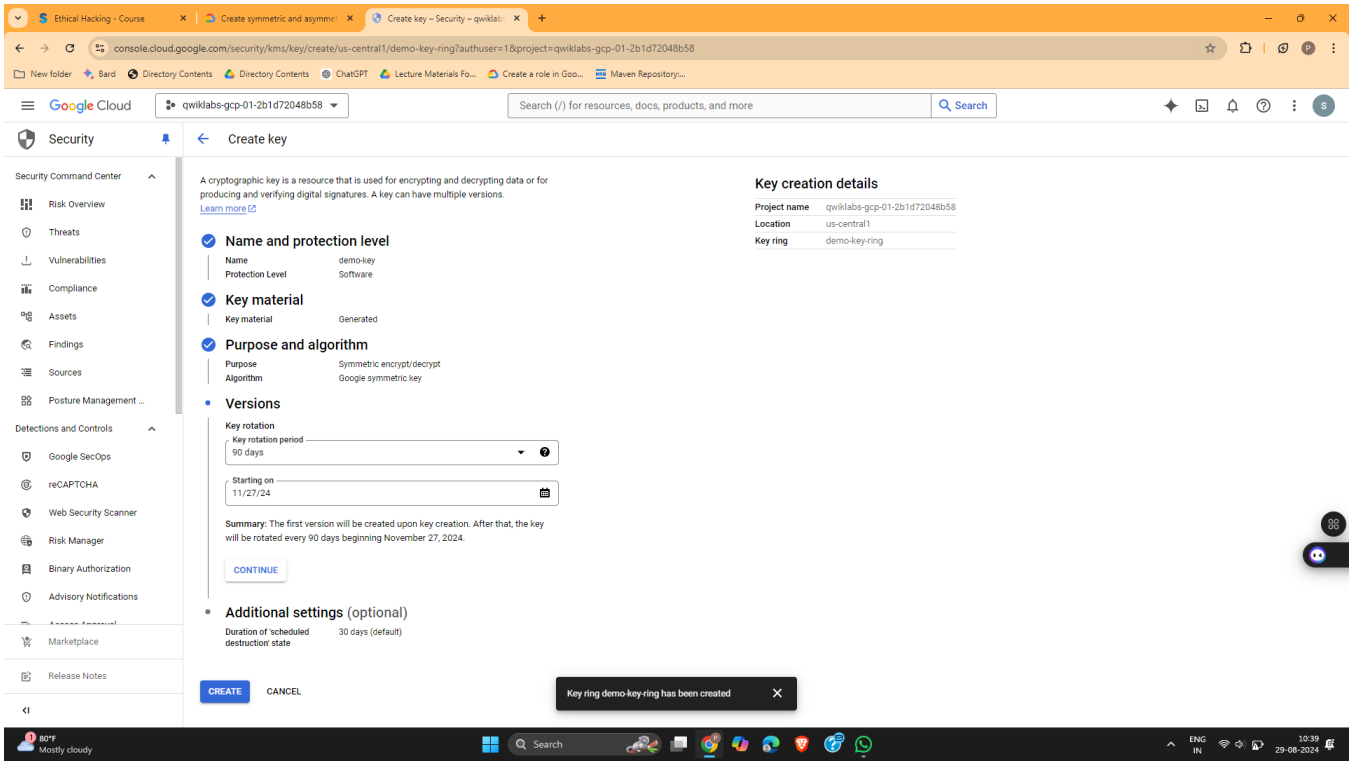


Figure 5 This figure shows the configuration of the key rotation period set to 90 days for the symmetric key.

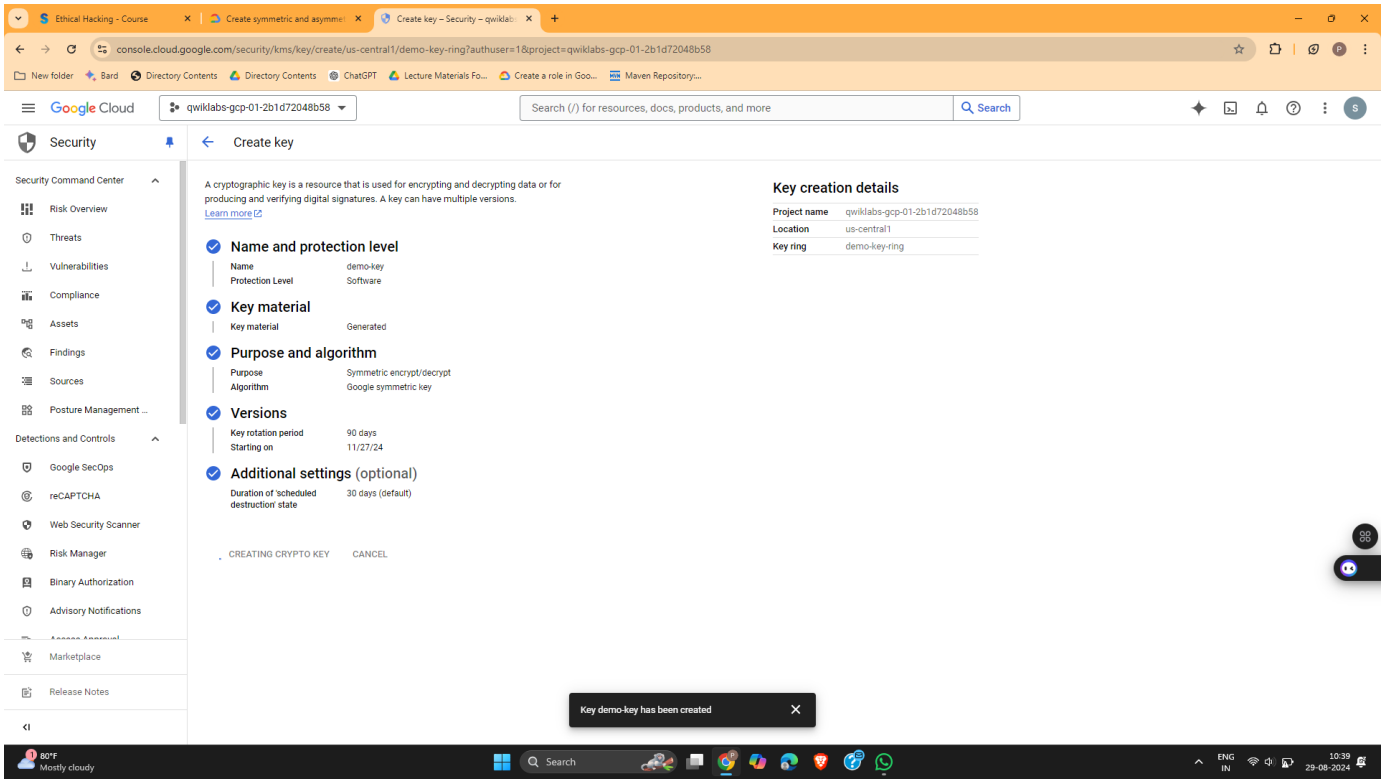


Figure 6 : This figure shows the confirmation message indicating the successful creation of the symmetric key in Google Cloud.

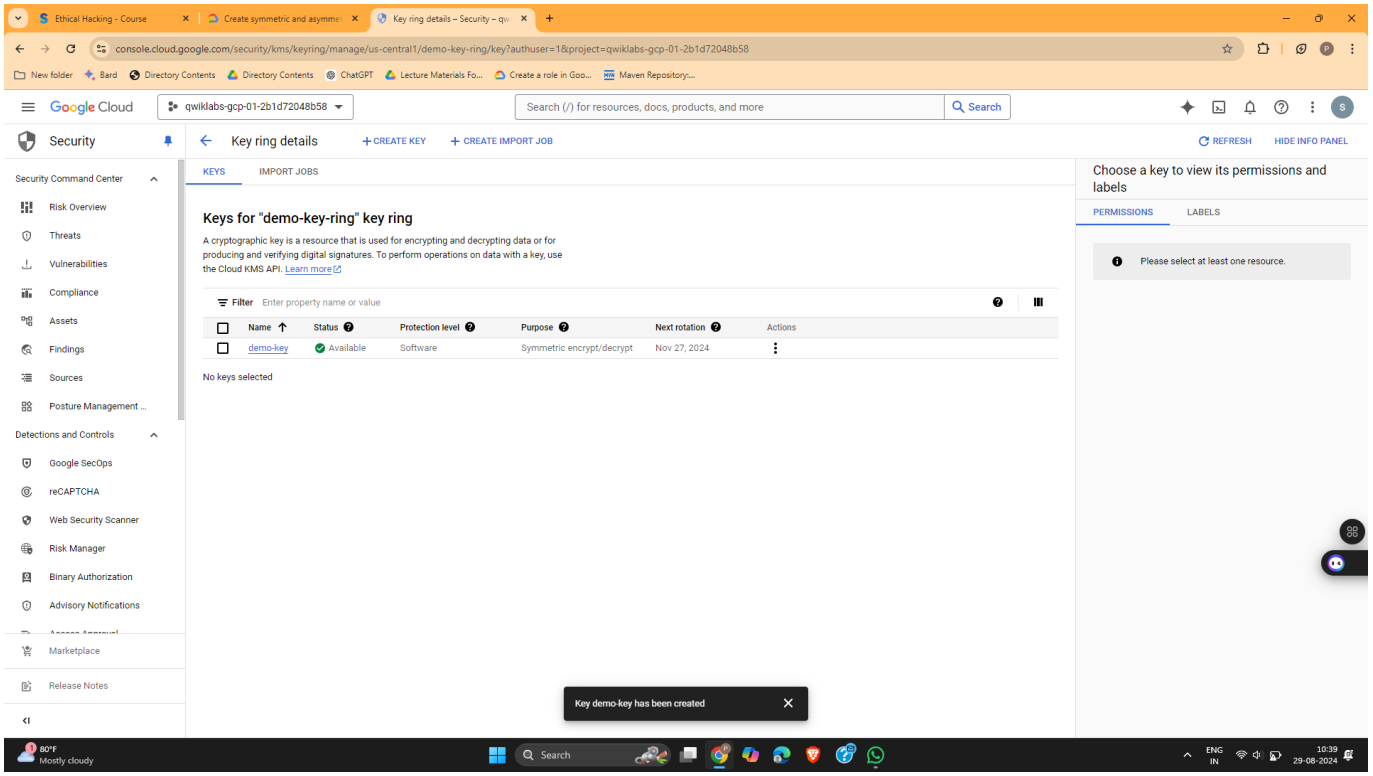


Figure 7 : This figure shows the confirmation message indicating the successful creation of the symmetric key in Google Cloud.

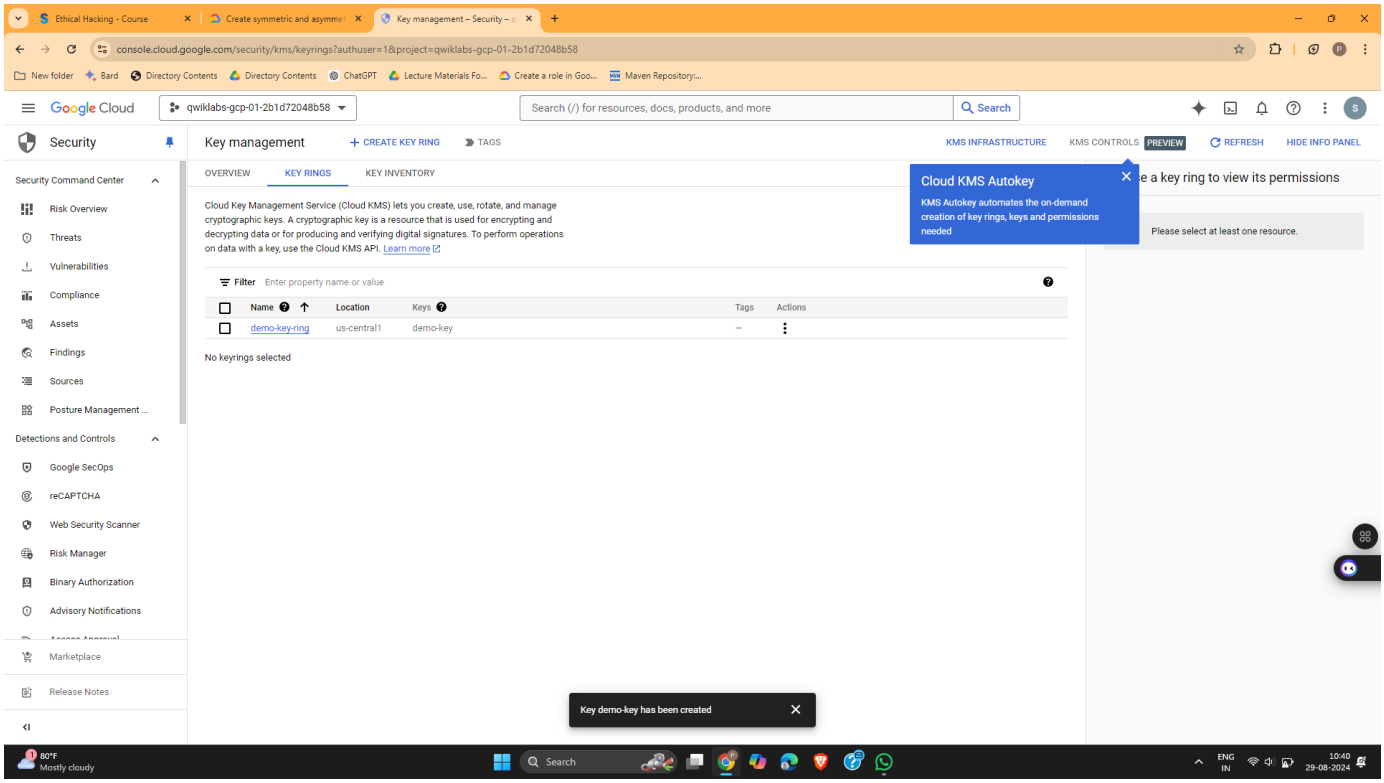


Figure 8 : This figure depicts the navigation process to the "Create Key" page within the demo-key-ring section in Google Cloud Key Management.

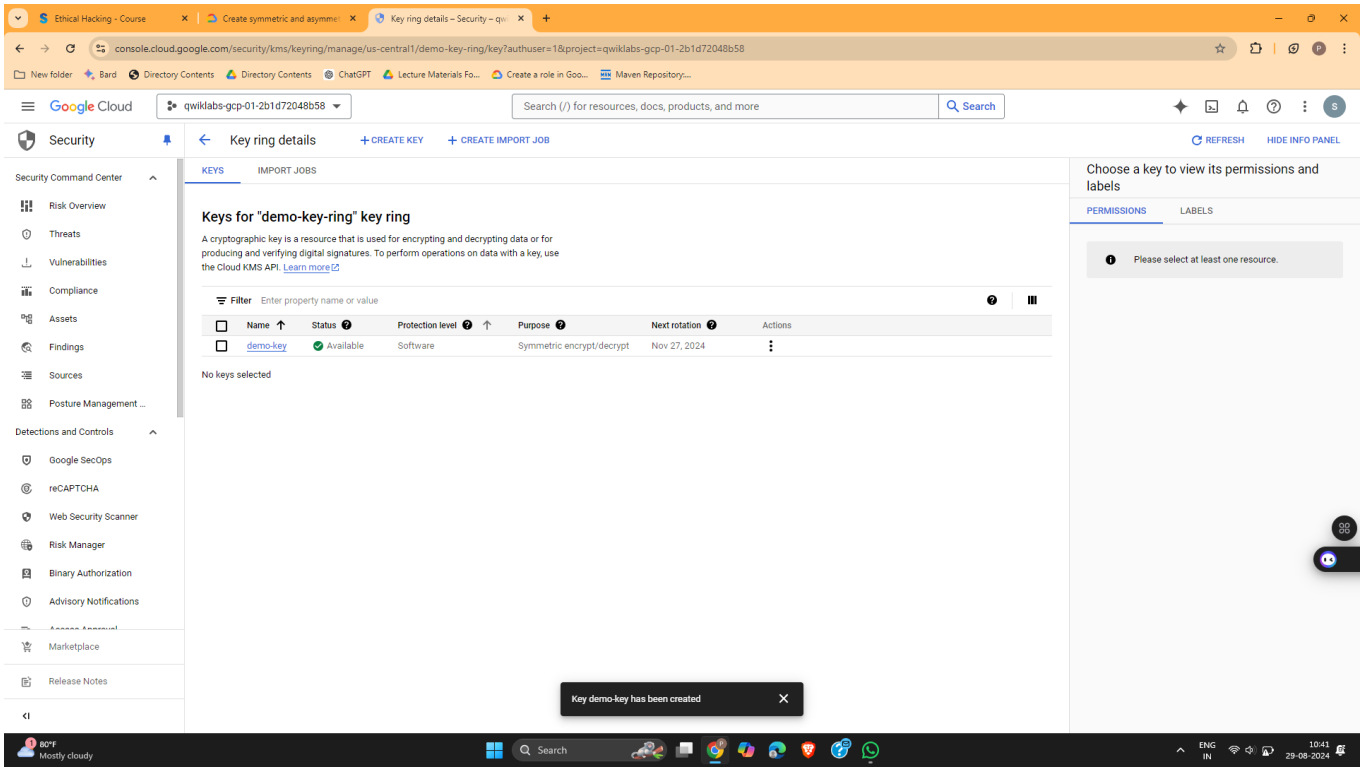


Figure 9 : This figure depicts the navigation process to the "Create Key" page within the demo-key-ring section in Google Cloud Key Management.

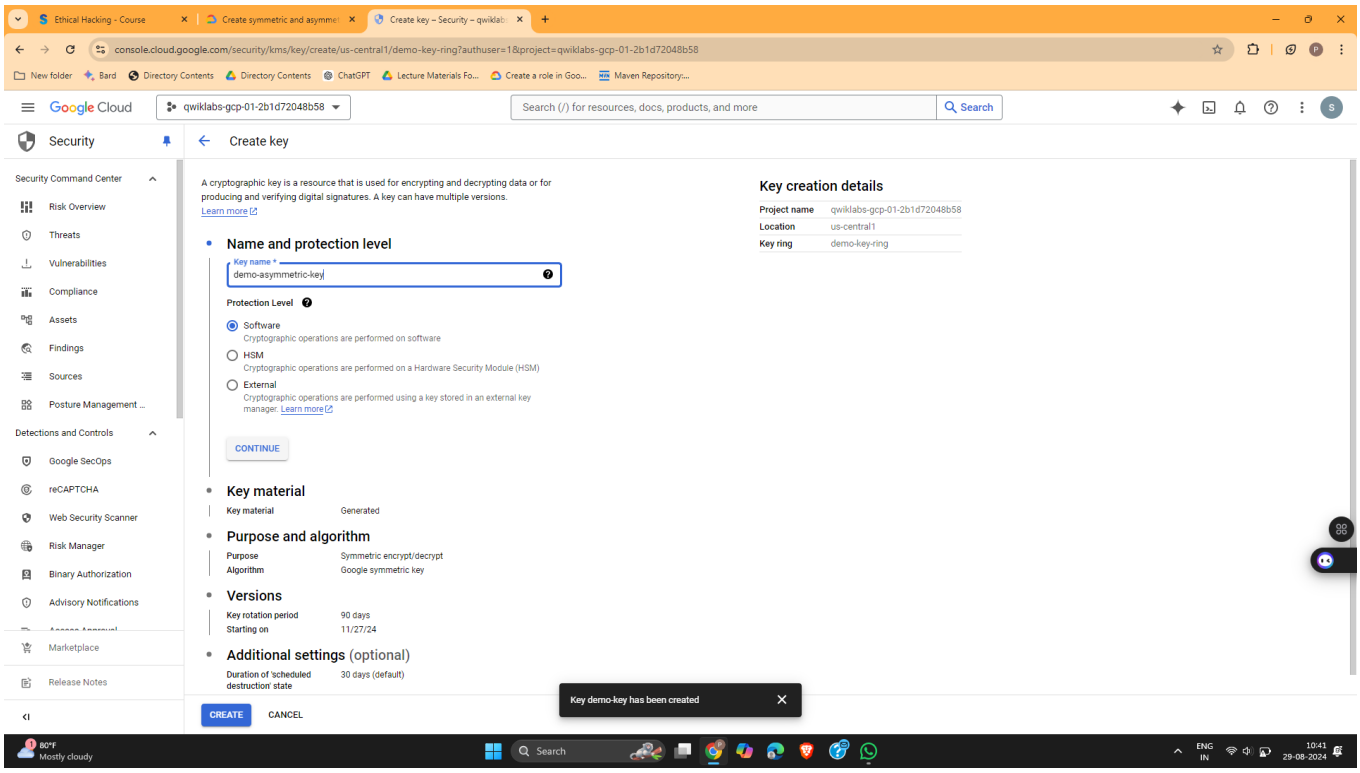


Figure 10 : This figure shows the form where the user enters the key name demo-asymmetric-key and selects the protection level as "Software".

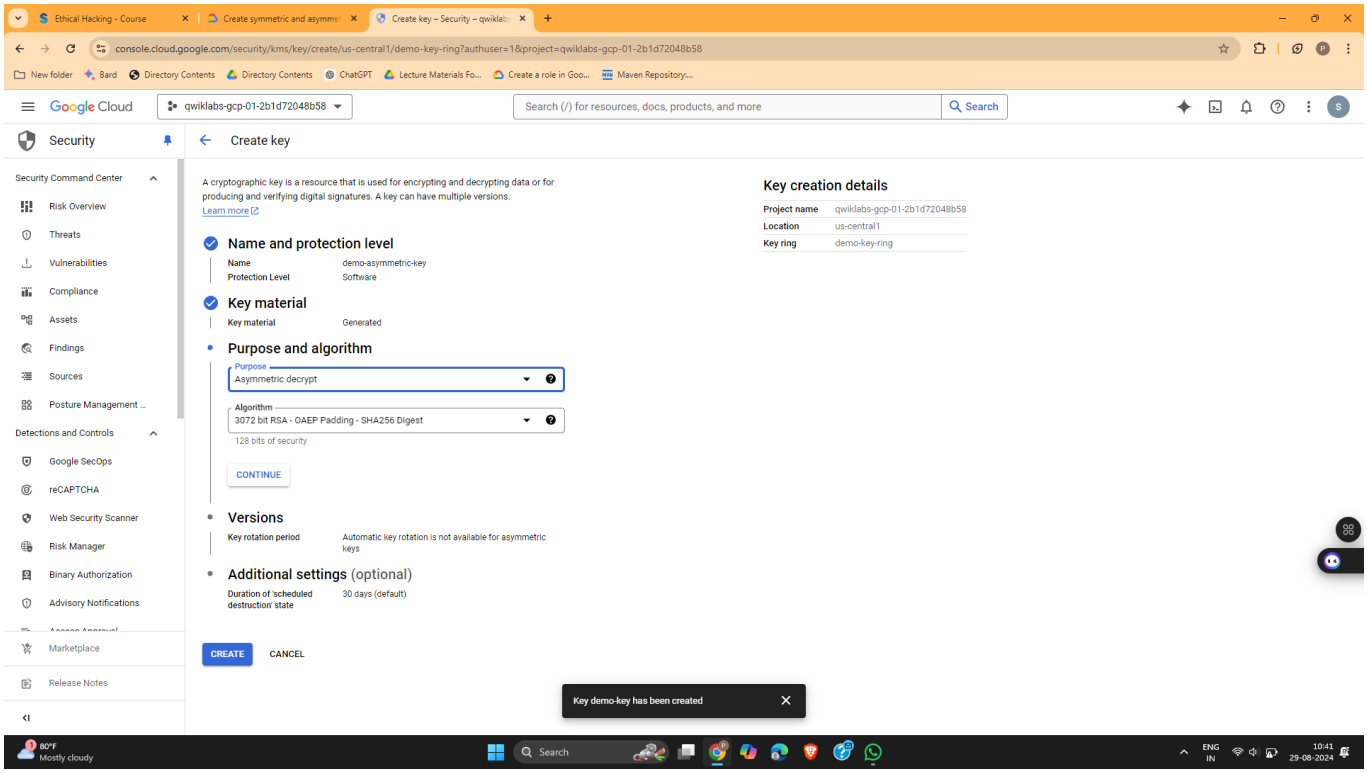


Figure 11 : This figure illustrates the selection of the key material as "Generated key" and the purpose set to "Asymmetric decrypt".

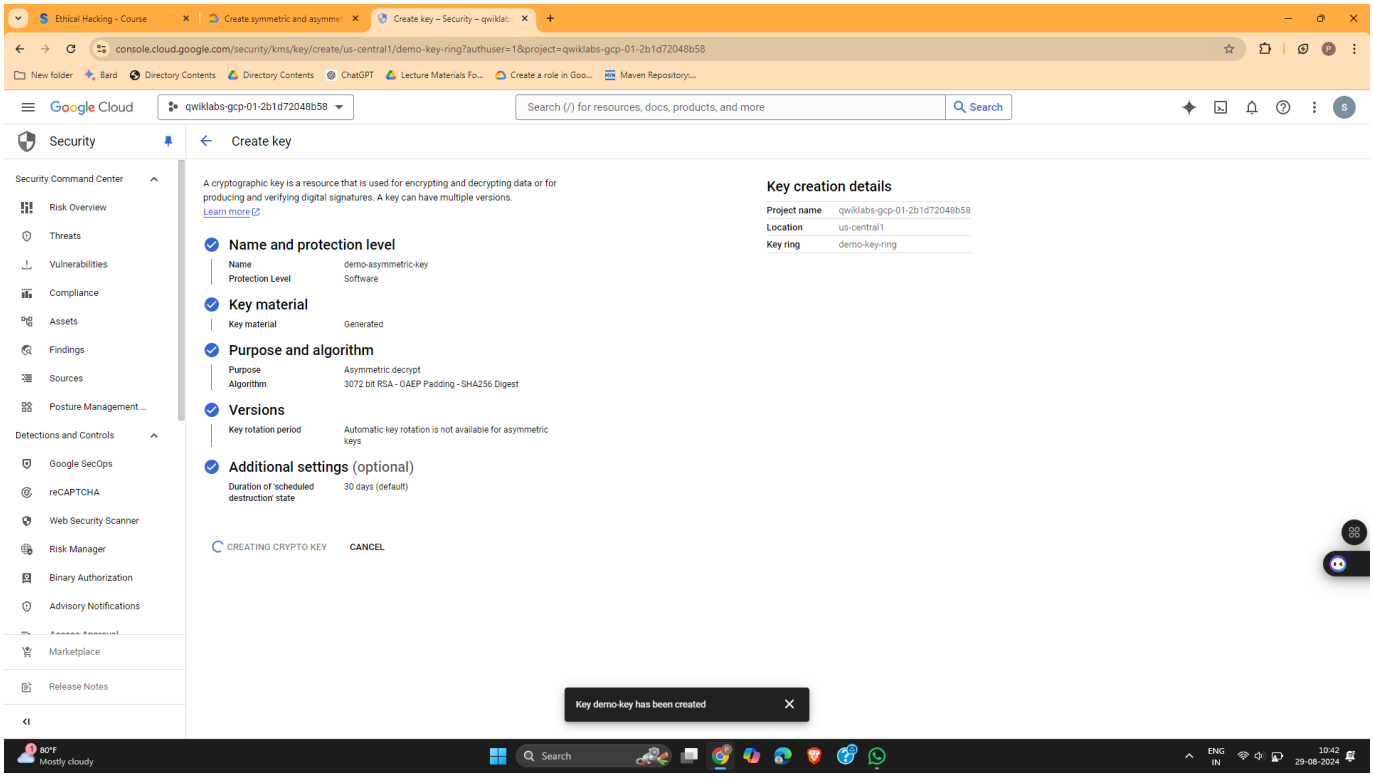


Figure 12 : This figure shows the "Create" button clicked to complete the process of creating the asymmetric key in Google Cloud.

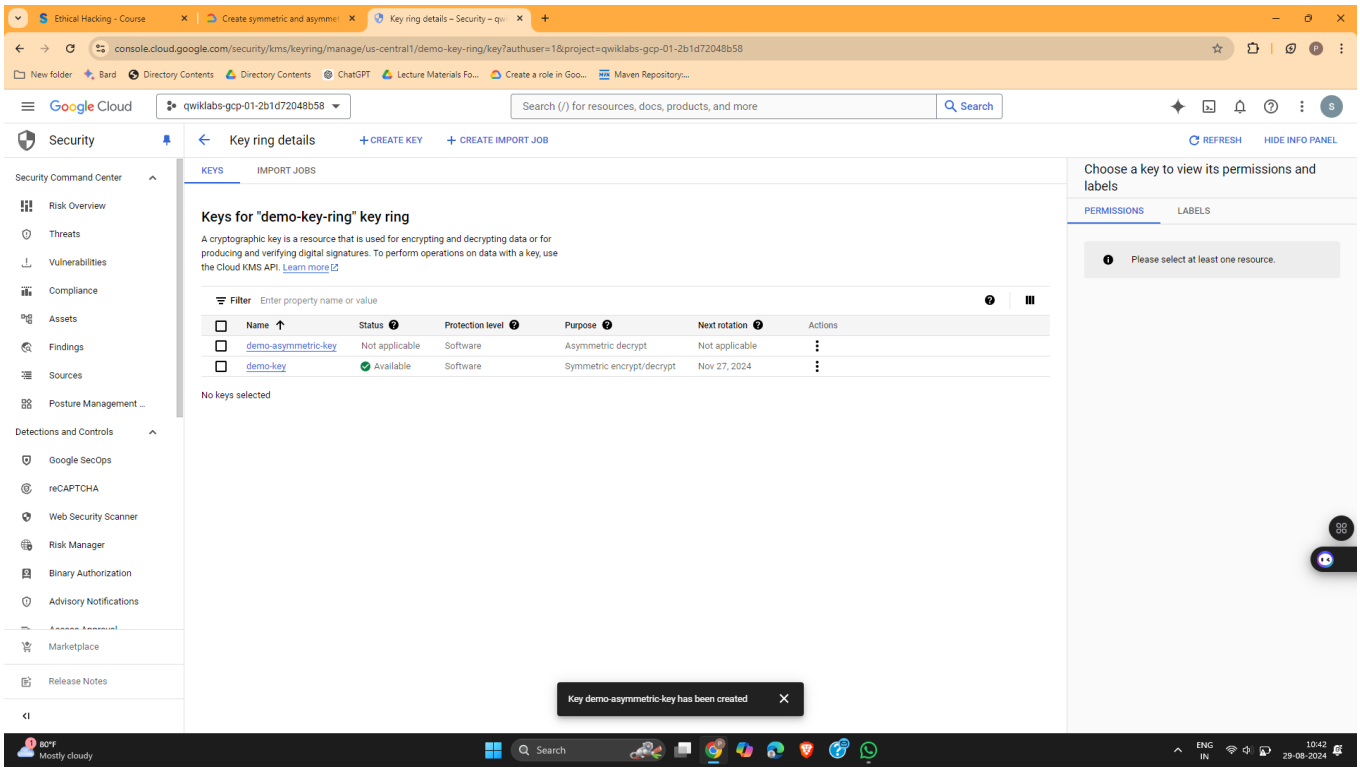


Figure 13 : This figure displays the confirmation screen indicating that the asymmetric key has been successfully created, ready for use.

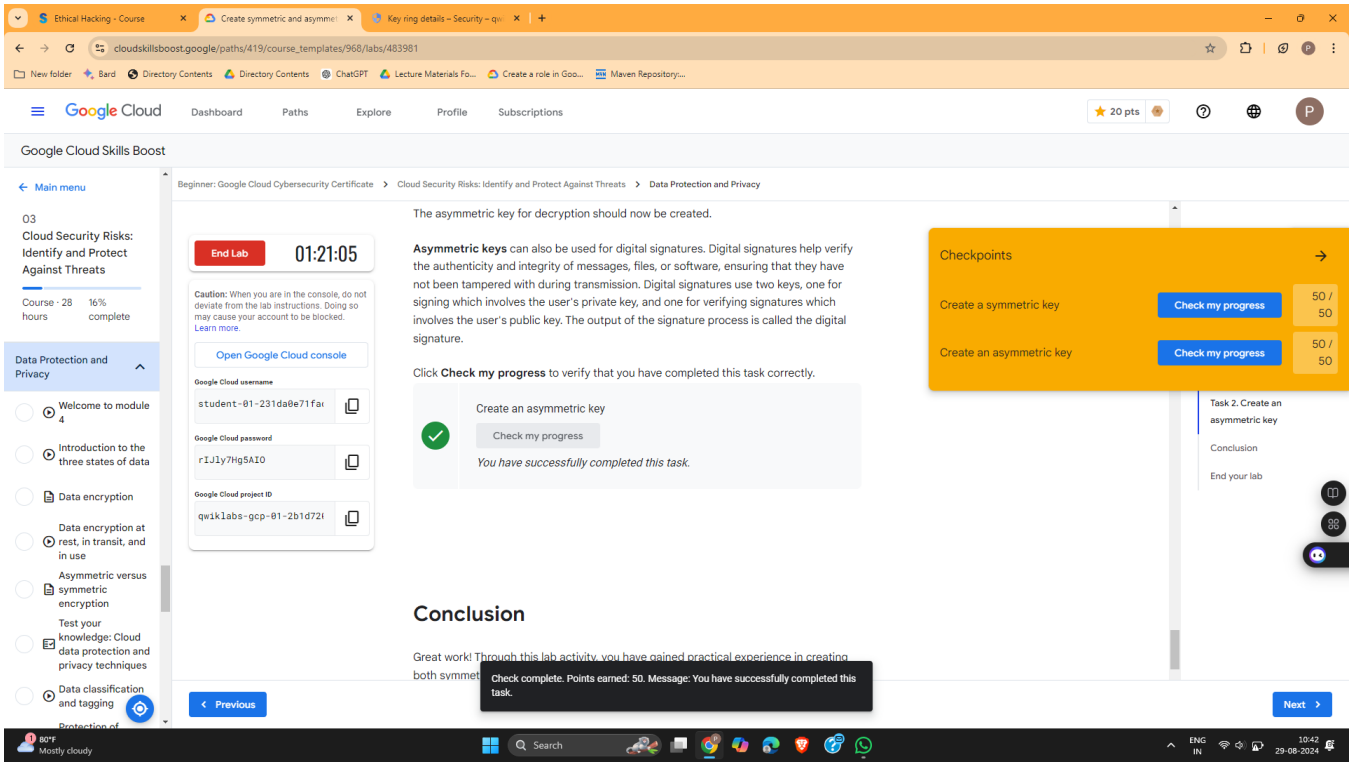


Figure 14 : This figure displays the confirmation screen for lab completion.

LATEST APPLICATIONS:

 Data Protection: Ensuring data confidentiality, integrity, and availability in cloud storage and transmission.

 Secure Communication: Used in protocols like HTTPS for secure key exchange and data encryption.

 Digital Signatures: Verifying the authenticity and integrity of digital documents and messages.

LEARNING OUTCOME:

By the end of this lab, you will understand the fundamental differences between symmetric and asymmetric cryptography, how to create and manage these keys using a cloud key management system, and their practical applications in securing data.

REFERENCES:

Basic concepts of cryptography: https://www.youtube.com/watch?v=JoeiLuFNBc4&list=PLBlnK6fEyqRhBsP45jUdcqBivf25hyVkU

PRACTICAL: 8

AIM:

Event Threat Detection is one of Security Command Center's (SCC) services. Event Threat Detection is a log-based threat analysis that continuously monitors Google Cloud logs for potential threats. When Event Threat Detection identifies suspicious activity, it generates a finding that you can investigate. In this experiment, you'll analyze findings in the Google Cloud Security Command Center and examine related events in Cloud Logging.

THEORY:

Event Threat Detection is a critical service provided by Google Cloud's Security Command Center (SCC). Its primary purpose is to continuously analyze cloud logs to detect potential security threats, such as unauthorized access or configuration changes that could compromise cloud resources. Event Threat Detection helps security teams quickly identify, investigate, and remediate malicious activity, reducing the risk of data breaches or system disruptions.

1. **Google Cloud IAM (Identity and Access Management)**: IAM is a tool used to manage access control for Google Cloud resources. It defines who (users) has what level of access to which resources in a cloud environment. This fine-grained access control allows administrators to grant appropriate permissions to users and groups while limiting access to sensitive information.

2. **IAM Roles and Permissions**: Google Cloud provides pre-defined roles such as Viewer, Editor, and Owner, each granting specific levels of permissions. Anomalous activity, such as granting the owner role to an external or unauthorized user, can be a security risk. Event Threat Detection can flag such activity as suspicious.

3. **Security Command Center (SCC)**: SCC is Google's centralized security and risk management platform for monitoring and improving the security posture of your cloud resources. SCC helps identify security misconfigurations, threats, and vulnerabilities by providing real-time alerts and insights into security risks.

4. **Cloud Logging**: Cloud Logging is a fully managed service for real-time log data and analysis. It allows administrators to collect and store logs from Google Cloud resources, making it easier to troubleshoot issues and monitor suspicious activity. In this lab, you will use Cloud Logging to filter IAM logs and investigate events related to security findings.

5. **Incident vs. Normal Activity**: In security, not all alerts represent true security threats. Some findings may result from benign user activity, while others indicate genuine malicious behavior. In this lab, you will distinguish between normal and anomalous activity by analyzing logs and understanding the source of suspicious actions.

OUTPUT:

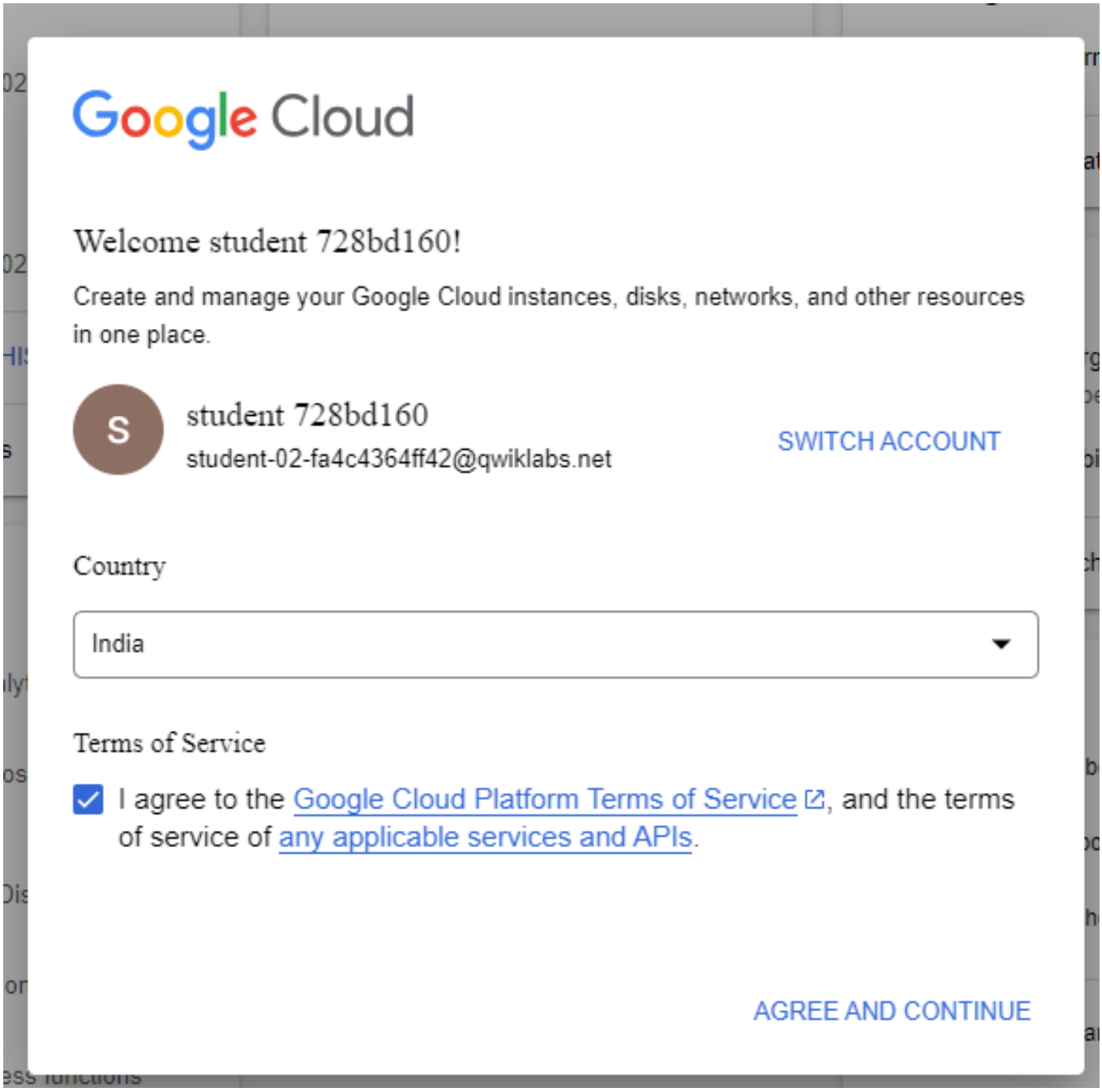


Figure 1: Credentials Page

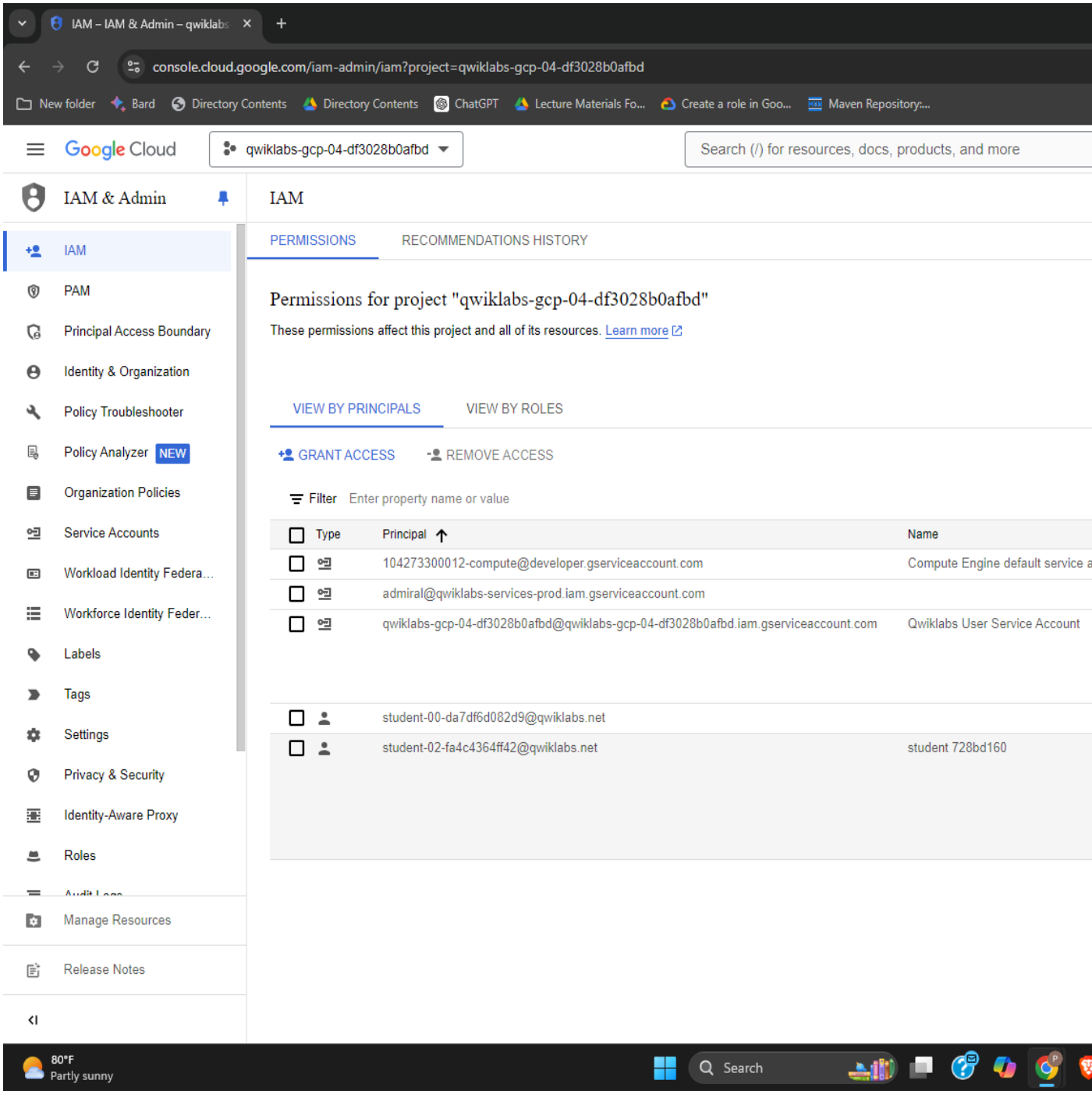


Figure 2 : Viewing IAM Principals in the Google Cloud IAM console before adding new permissions.

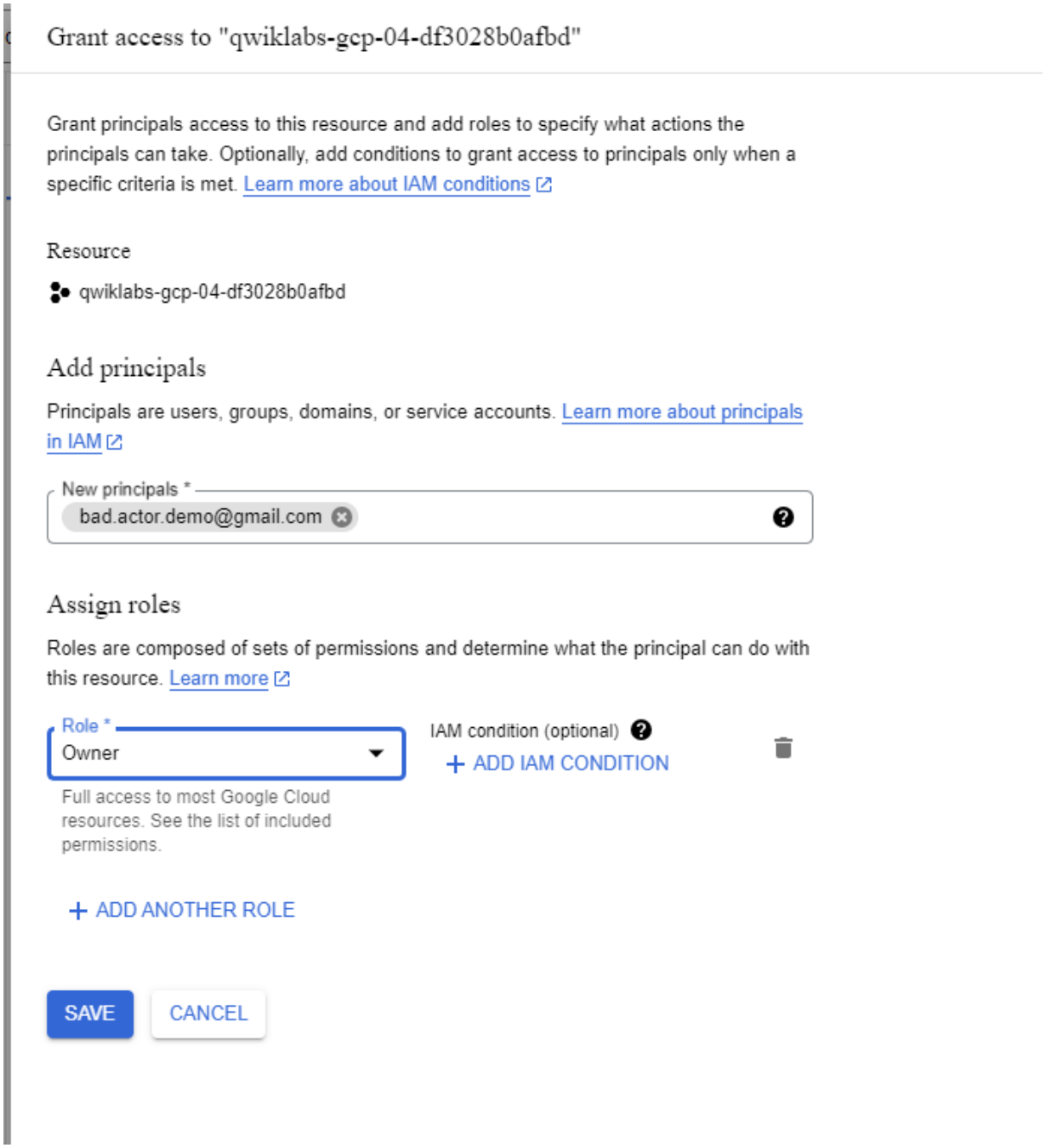


Figure 3 : Adding the external user (bad.actor.demo@gmail.com) as an owner of the project in Google Cloud IAM.

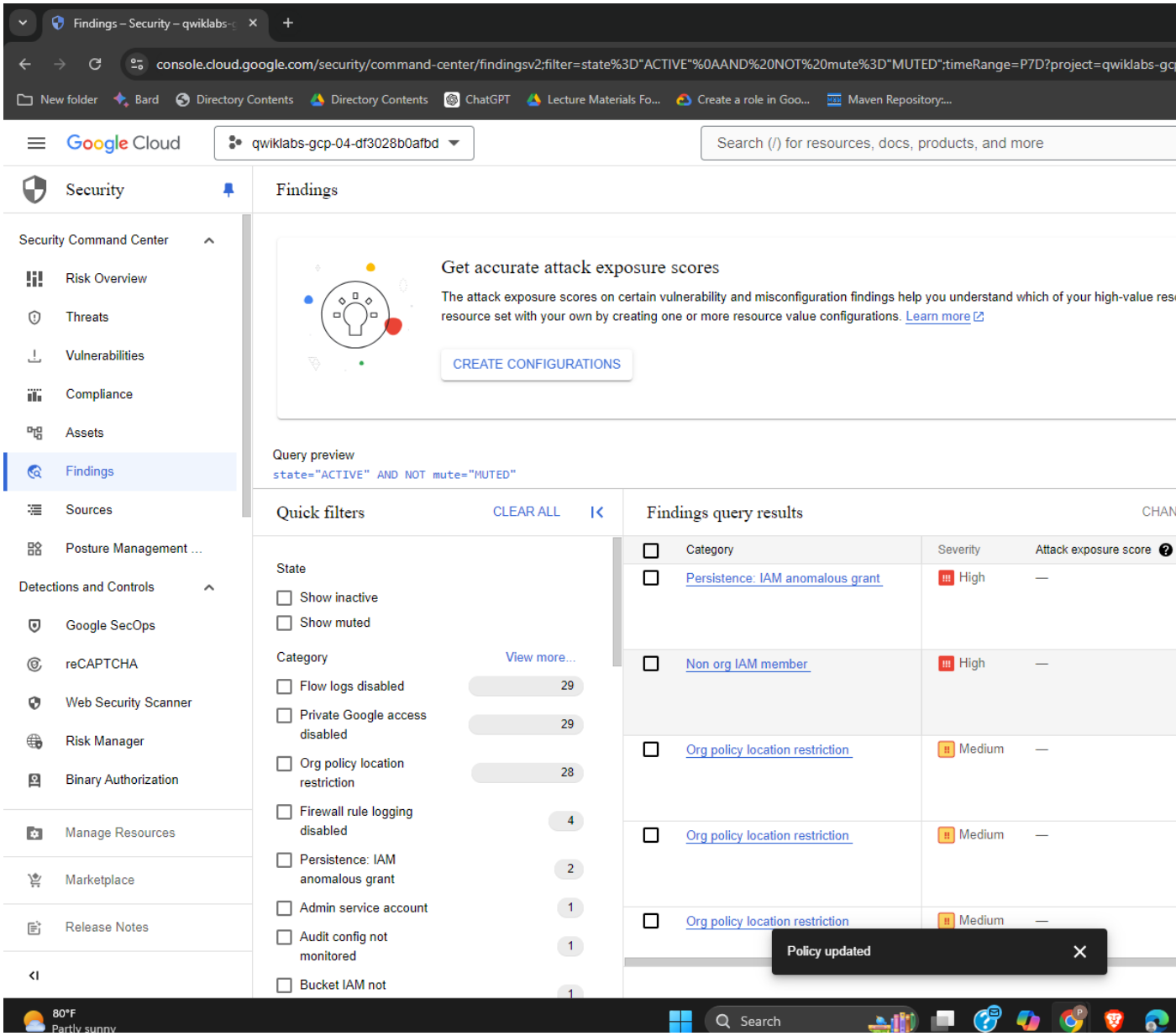


Figure 4 : Event Threat Detection findings in Google Cloud Security Command Center showing two high-severity IAM findings.

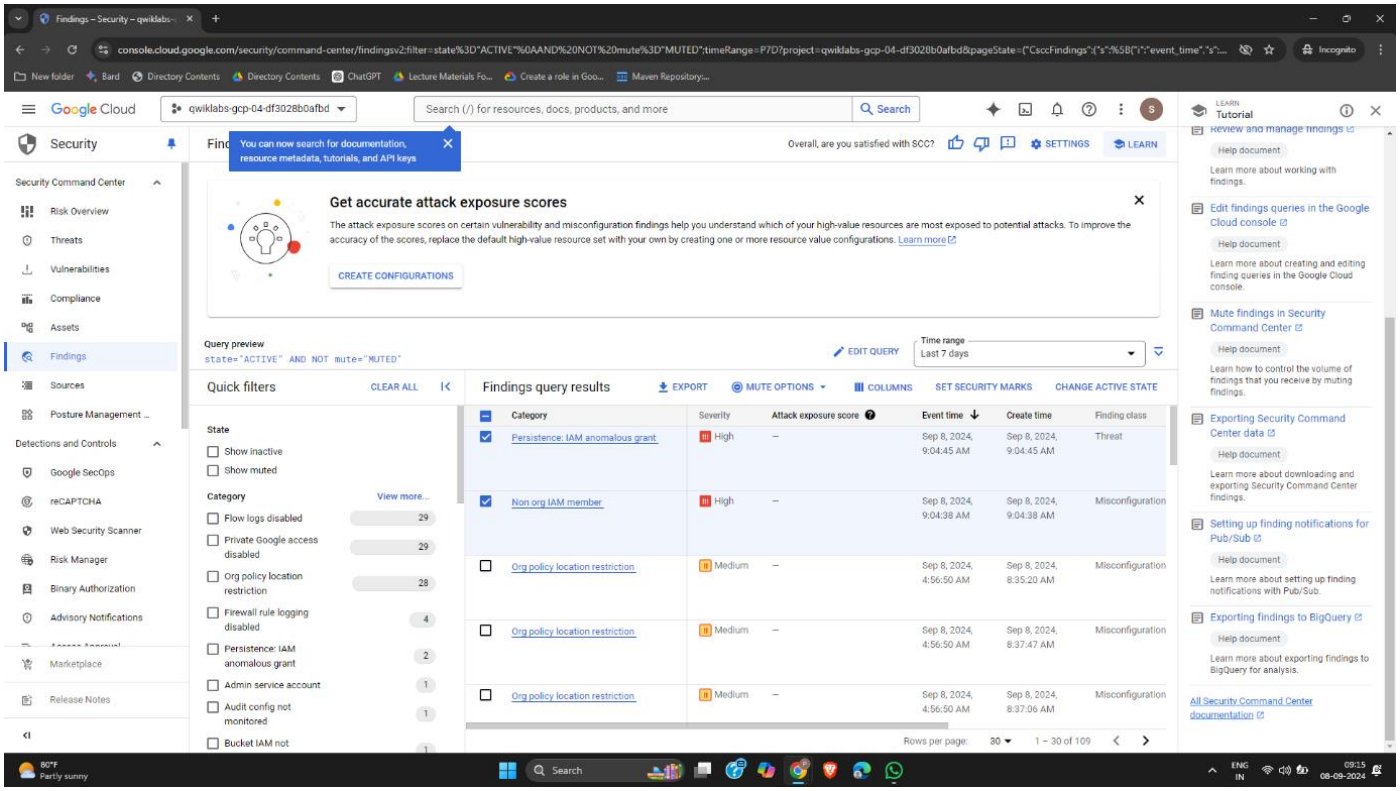


Figure 5 : Filtering Security Command Center findings by the IAM anomalous grant category And Analyzing the details of the earliest Persistence: IAM Anomalous Grant finding in the Security Command Center.

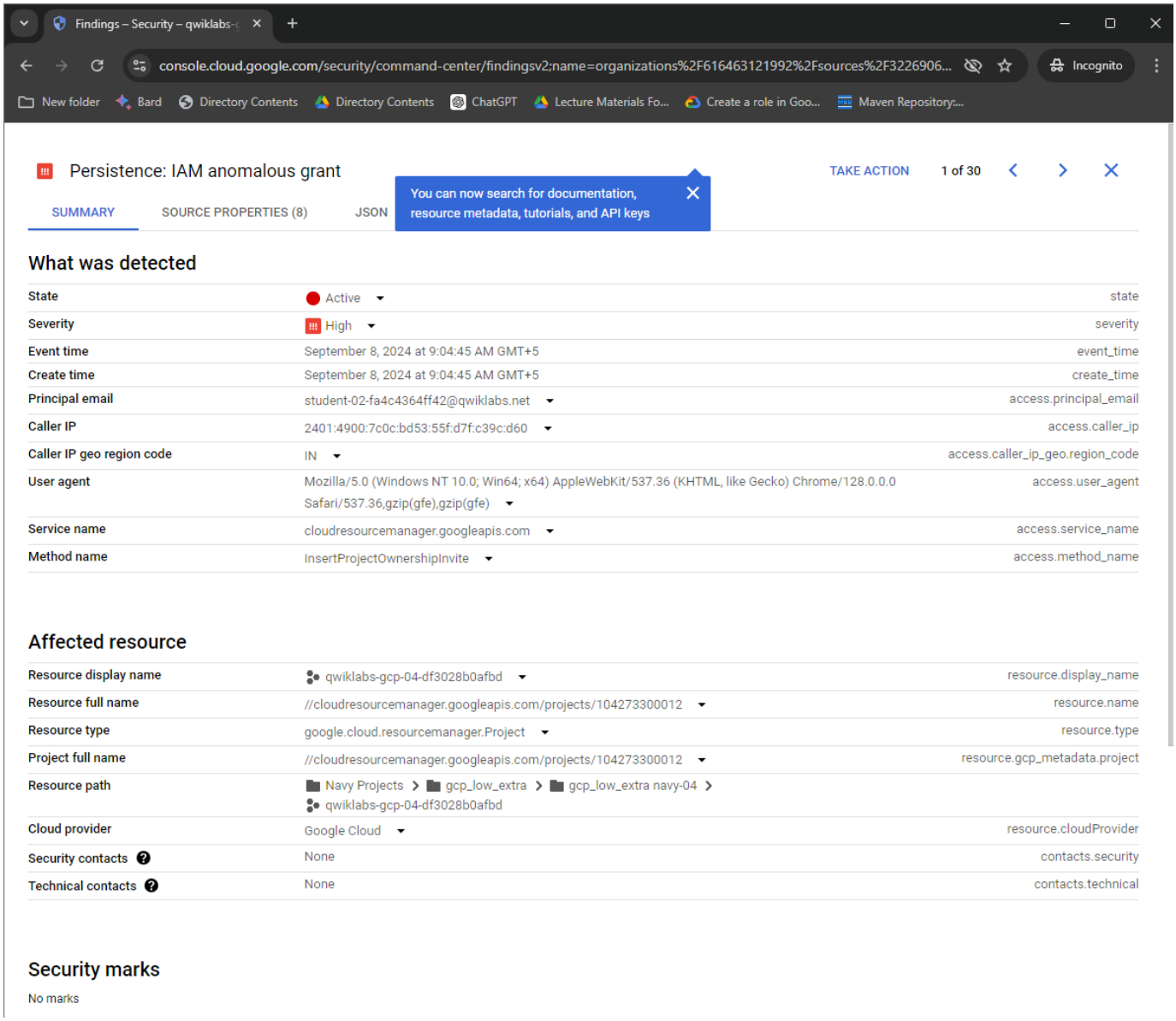


Figure 6 : Viewing the details of the latest Persistence: IAM Anomalous Grant finding involving the external user bad.actor.demo@gmail.com.

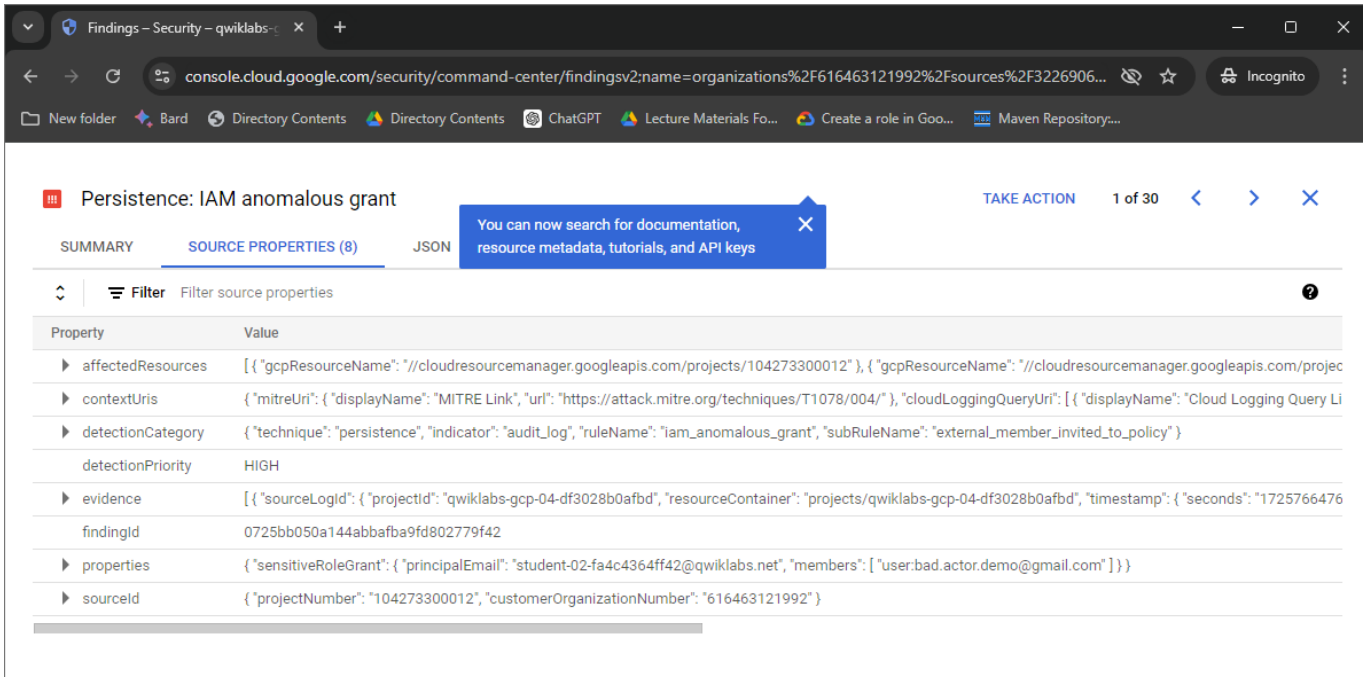


Figure 7 : Identifying the malicious finding by analyzing the principal and members associated with the grant.

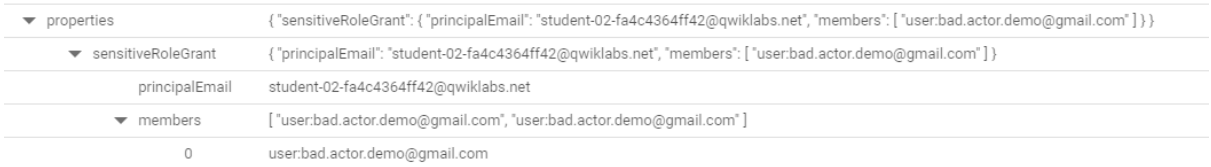


Figure 8 : Identifying the malicious finding by analyzing the principal and members associated with the grant.

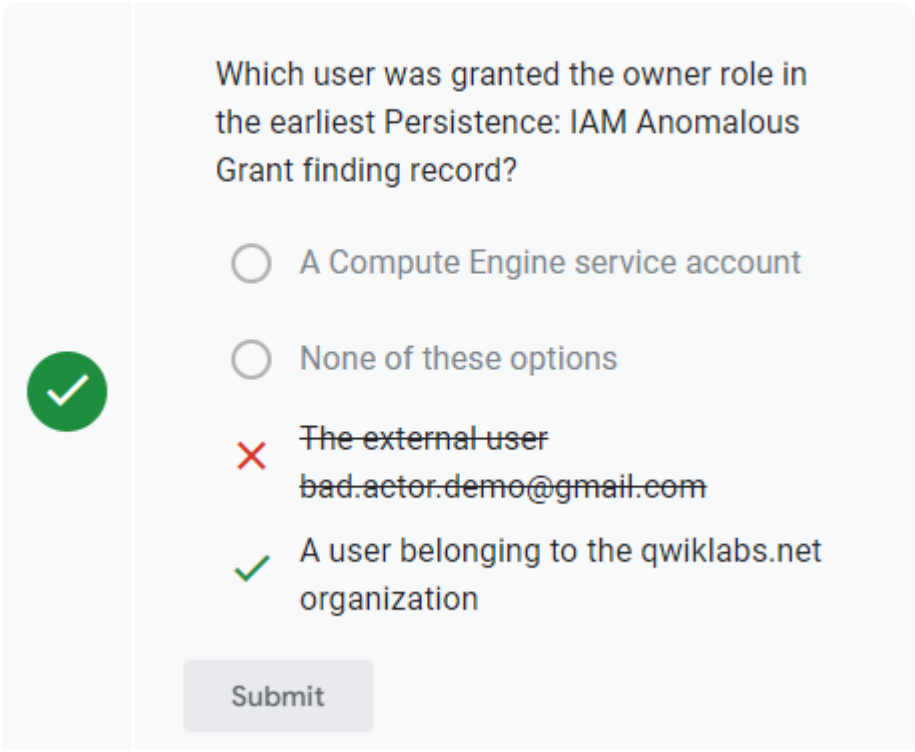


Figure 9 : MCQ

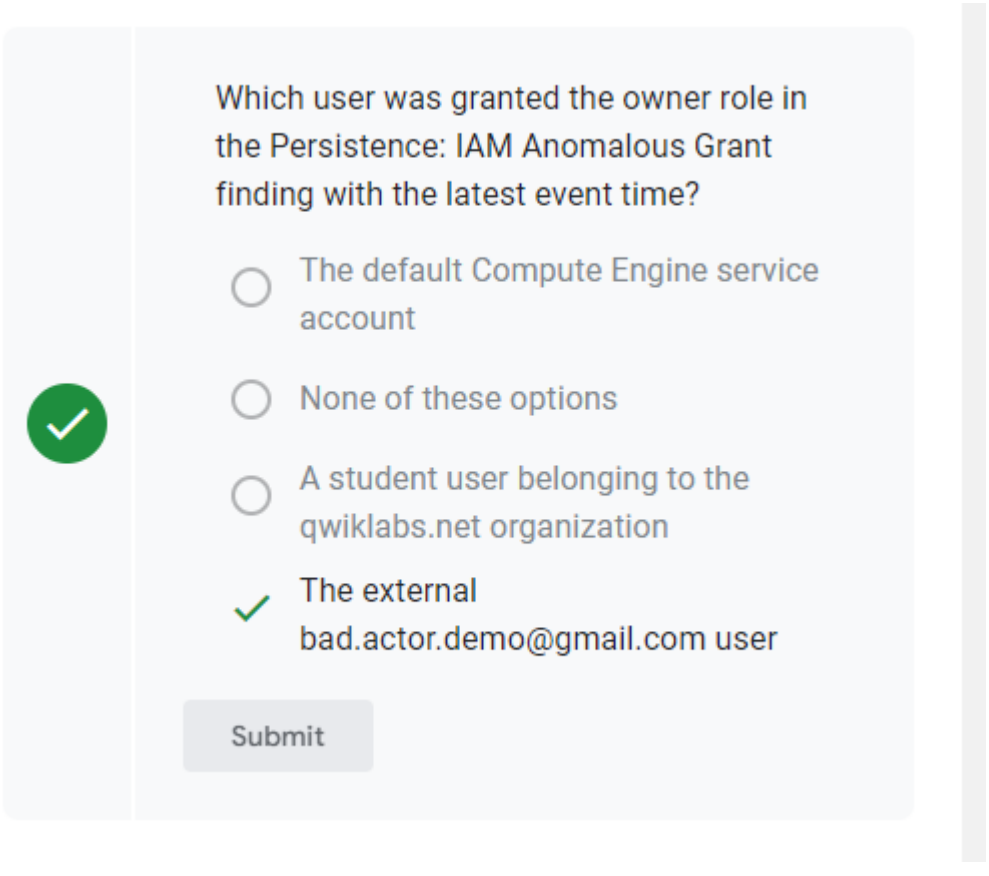


Figure 10 : MCQ

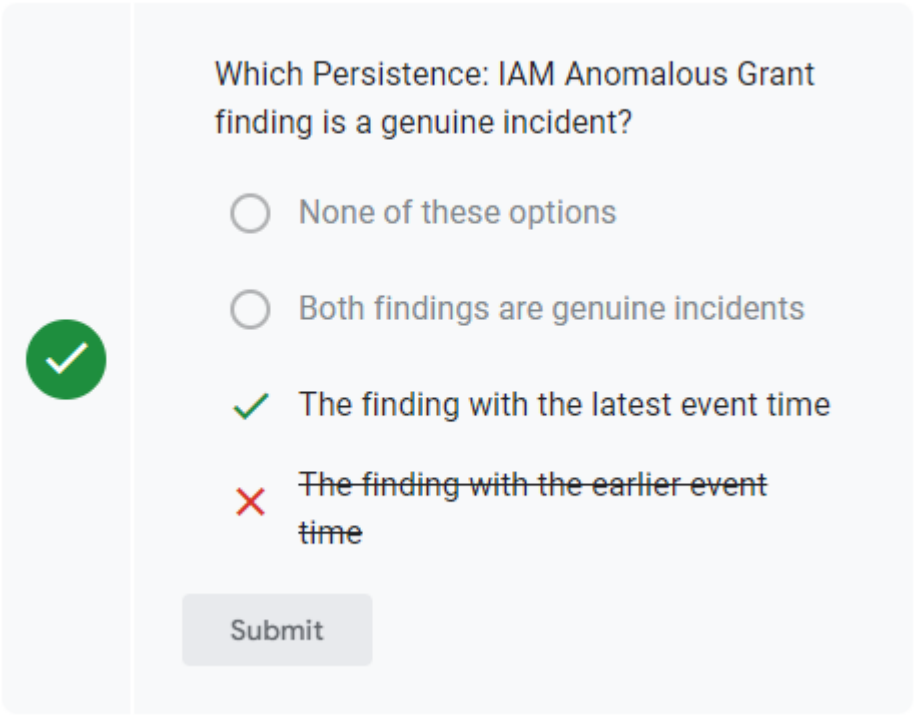


Figure 11 : MCQ

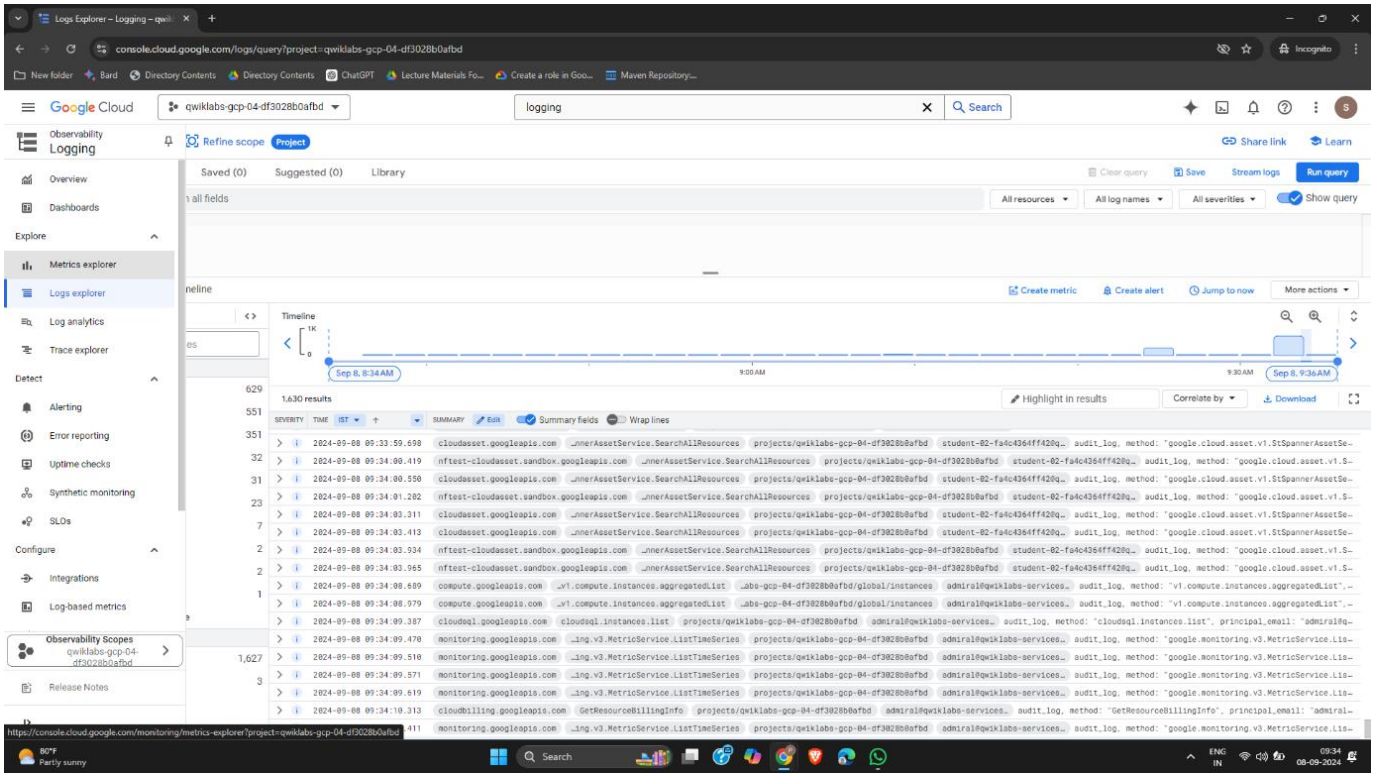


Figure 12 : Using Cloud Logging to search for IAM permission changes using a custom query in Logs Explorer.

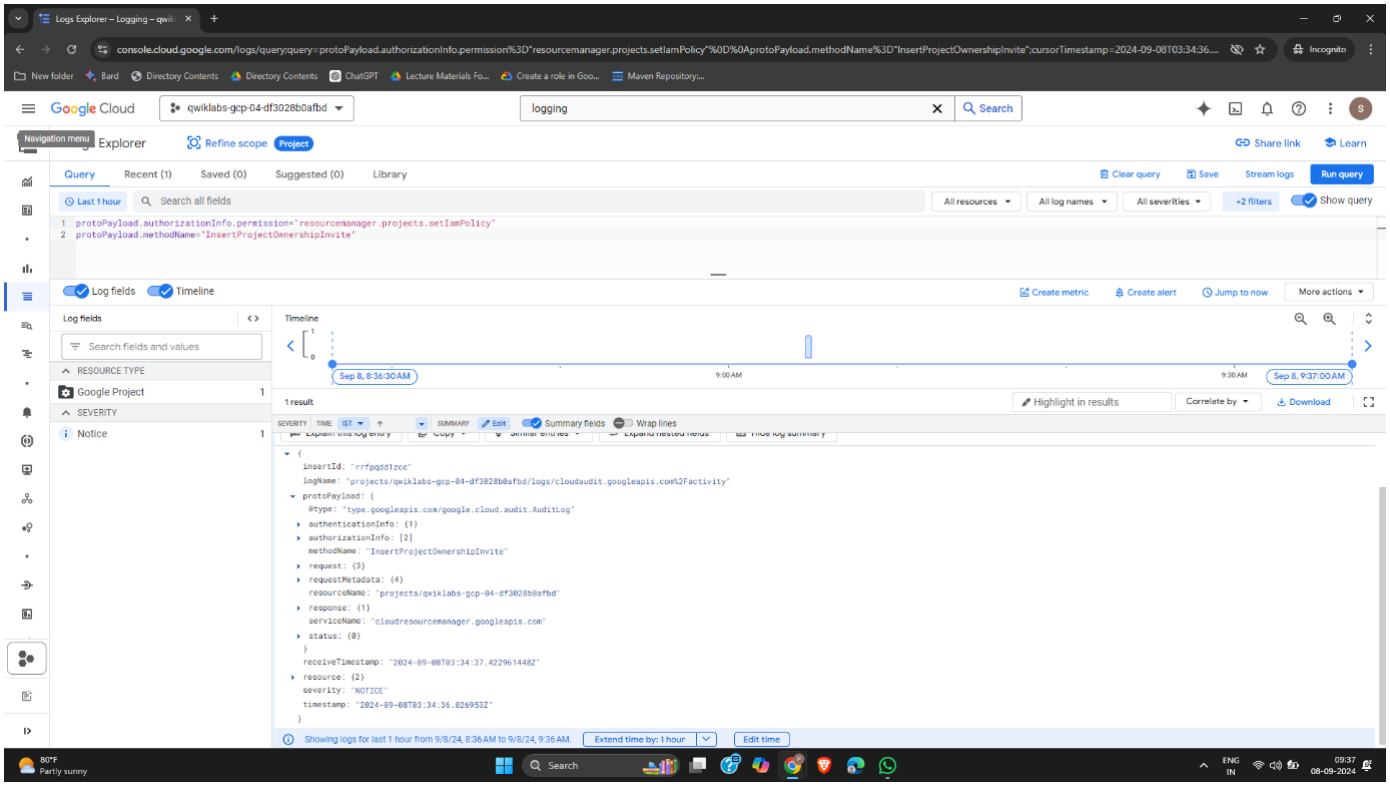


Figure 13 : Examining log entries related to the anomalous IAM grant in Cloud Logging, showing the requester and granted permissions and Detailed view of the anomalous request event showing authentication info and the user who made the request.

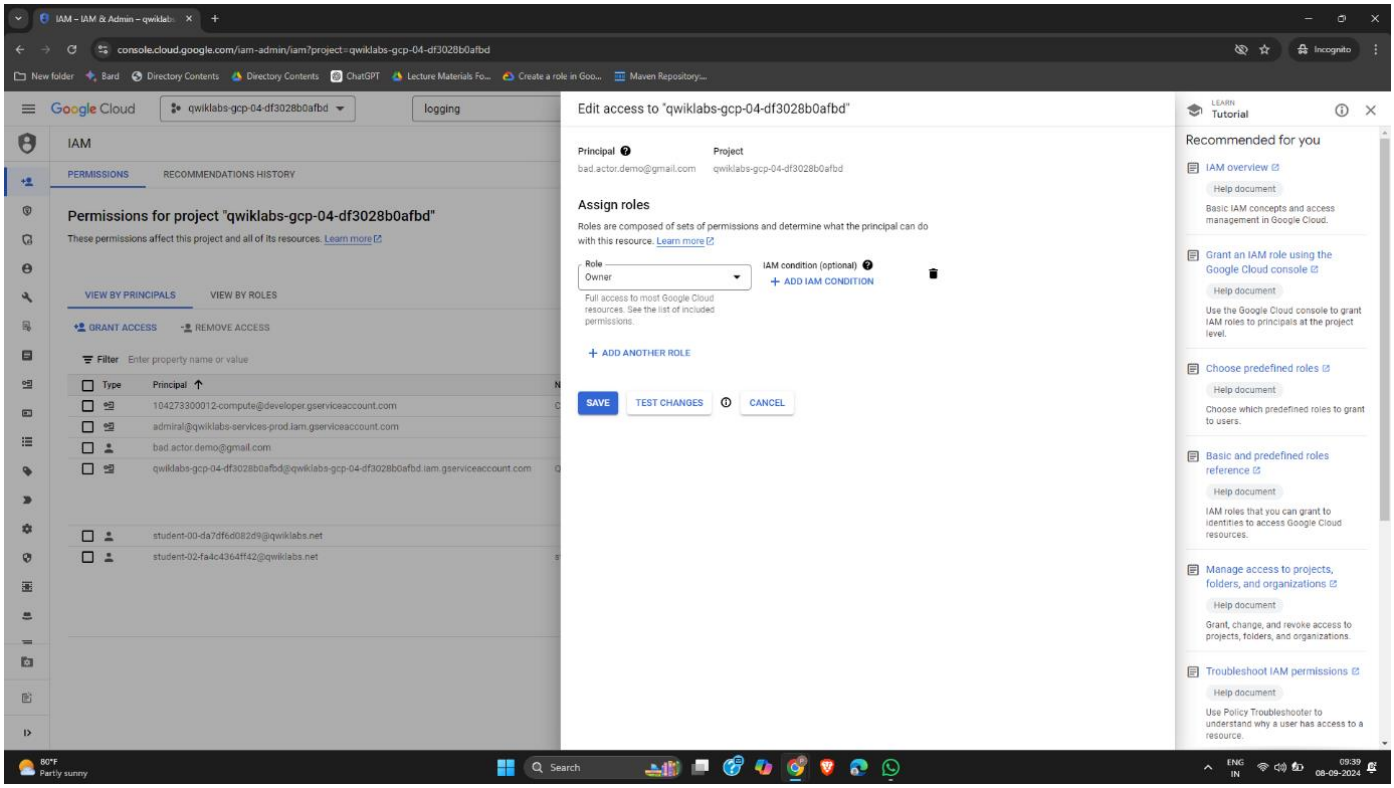


Figure 14 : Removing the project owner role from the external user bad.actor.demo@gmail.com in the IAM console to remediate the malicious finding.

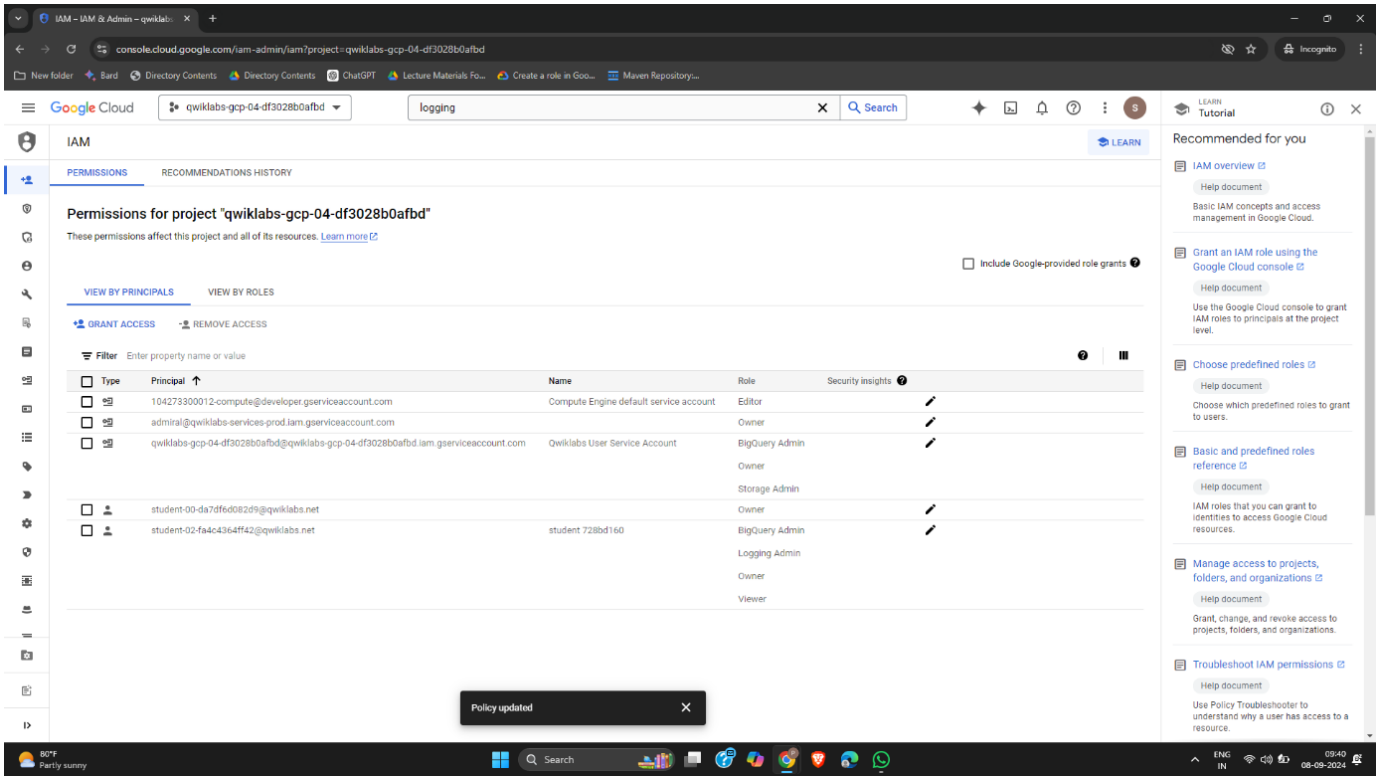


Figure 15 : Confirmation of the IAM role removal and successful remediation of the security incident in Google Cloud IAM.

LATEST APPLICATIONS:

- ✓ **Event Threat Detection** is actively used in modern cloud environments to monitor real-time activities, ensure compliance, and prevent unauthorized access to sensitive resources.
- ✓ **IAM Management** is an integral part of securing cloud infrastructure, as it allows organizations to apply the principle of least privilege.
- ✓ **Cloud Logging and Analysis** is widely used for auditing purposes and incident response to detect and remediate security threat.

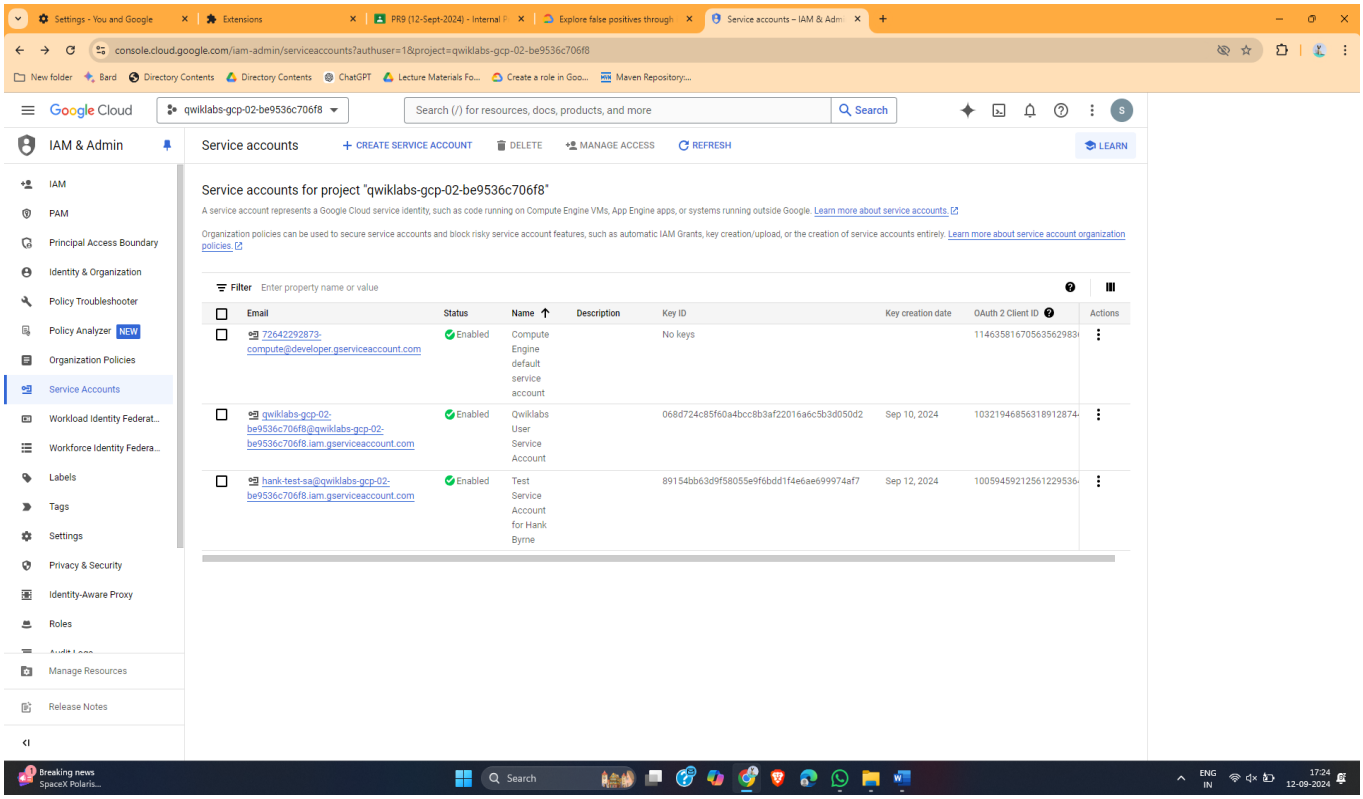
LEARNING OUTCOME:

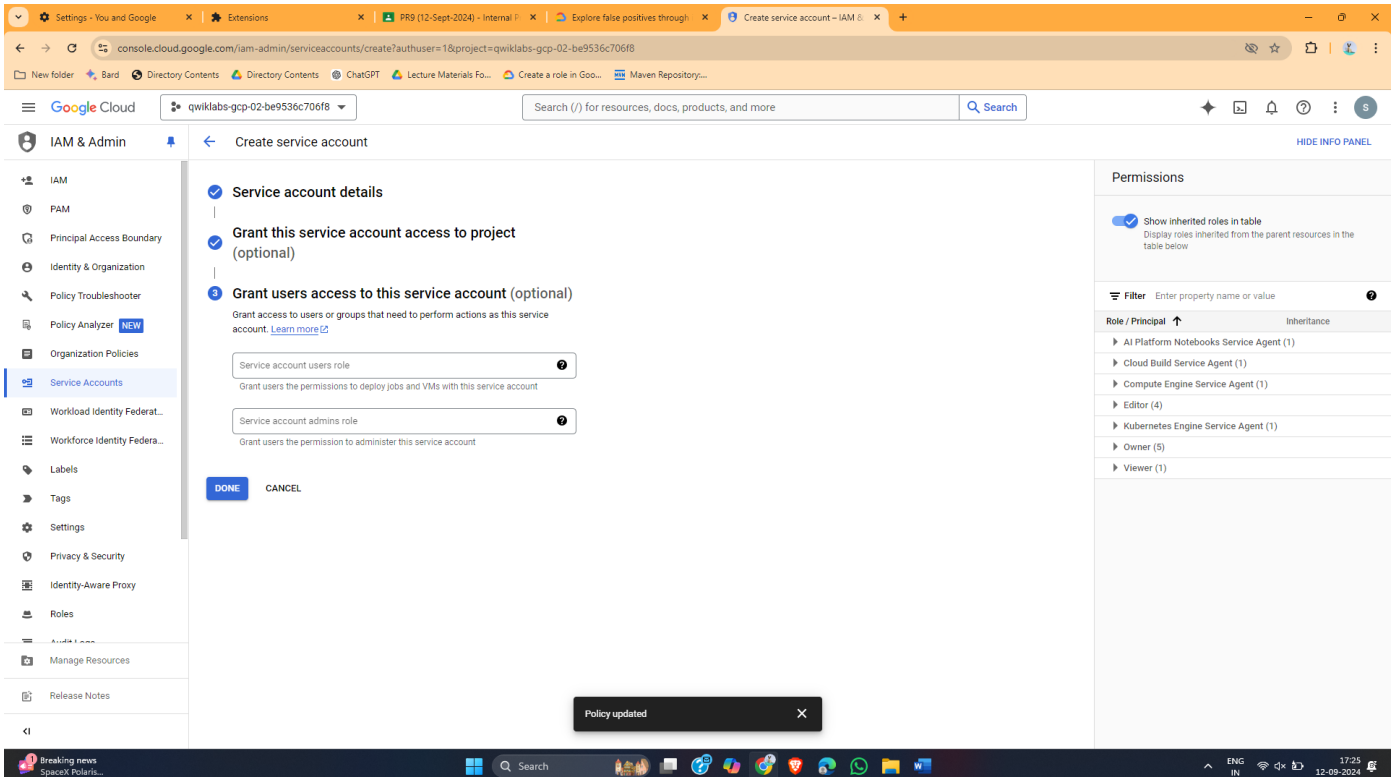
- ✓ Understand how to grant, review, and revoke IAM permissions in Google Cloud.
- ✓ Gain practical experience in identifying suspicious activities using Security Command Center.
- ✓ Learn to differentiate between normal user activity and potential security incidents.
- ✓ Use Cloud Logging to track and investigate IAM permission changes and security events.
- ✓ Remediate a malicious finding by removing unauthorized access.

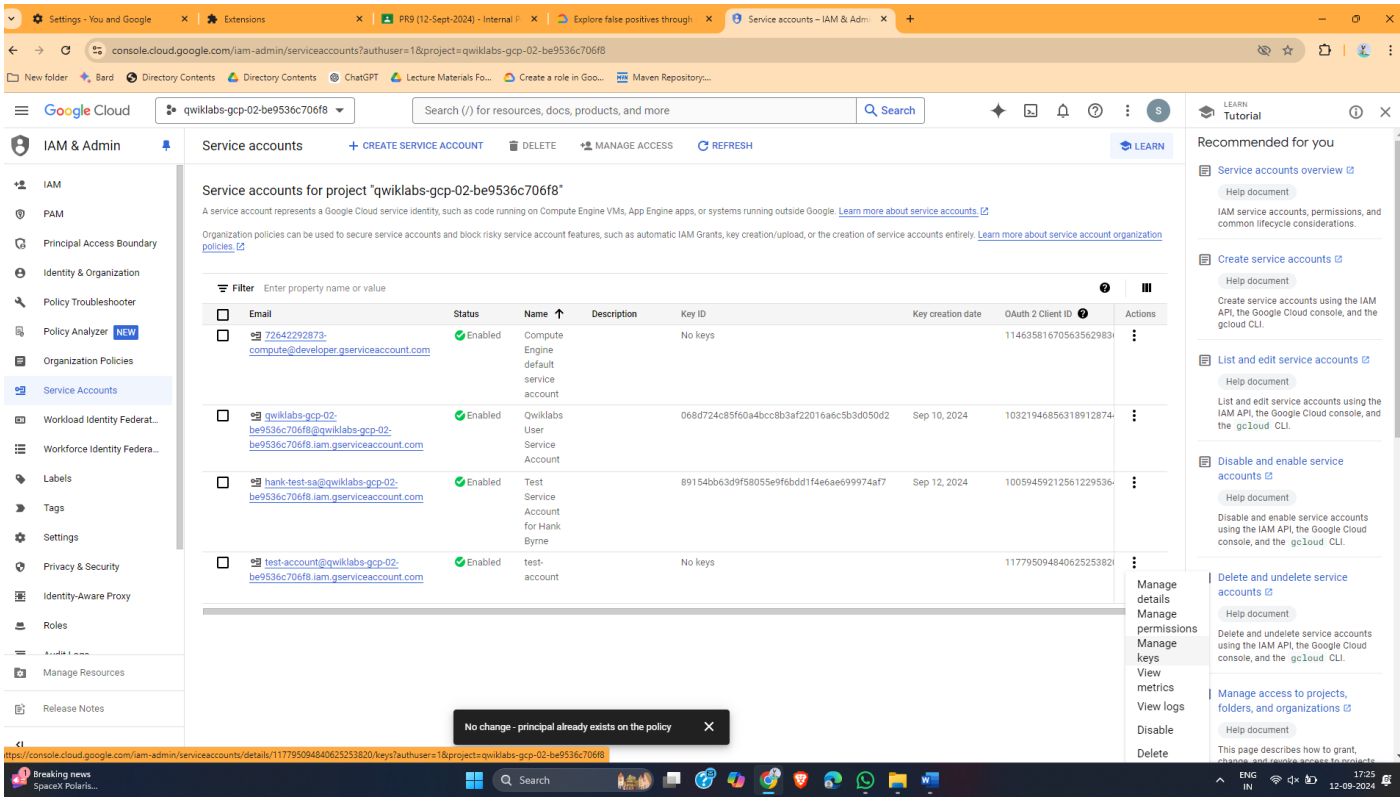
REFERENCES:

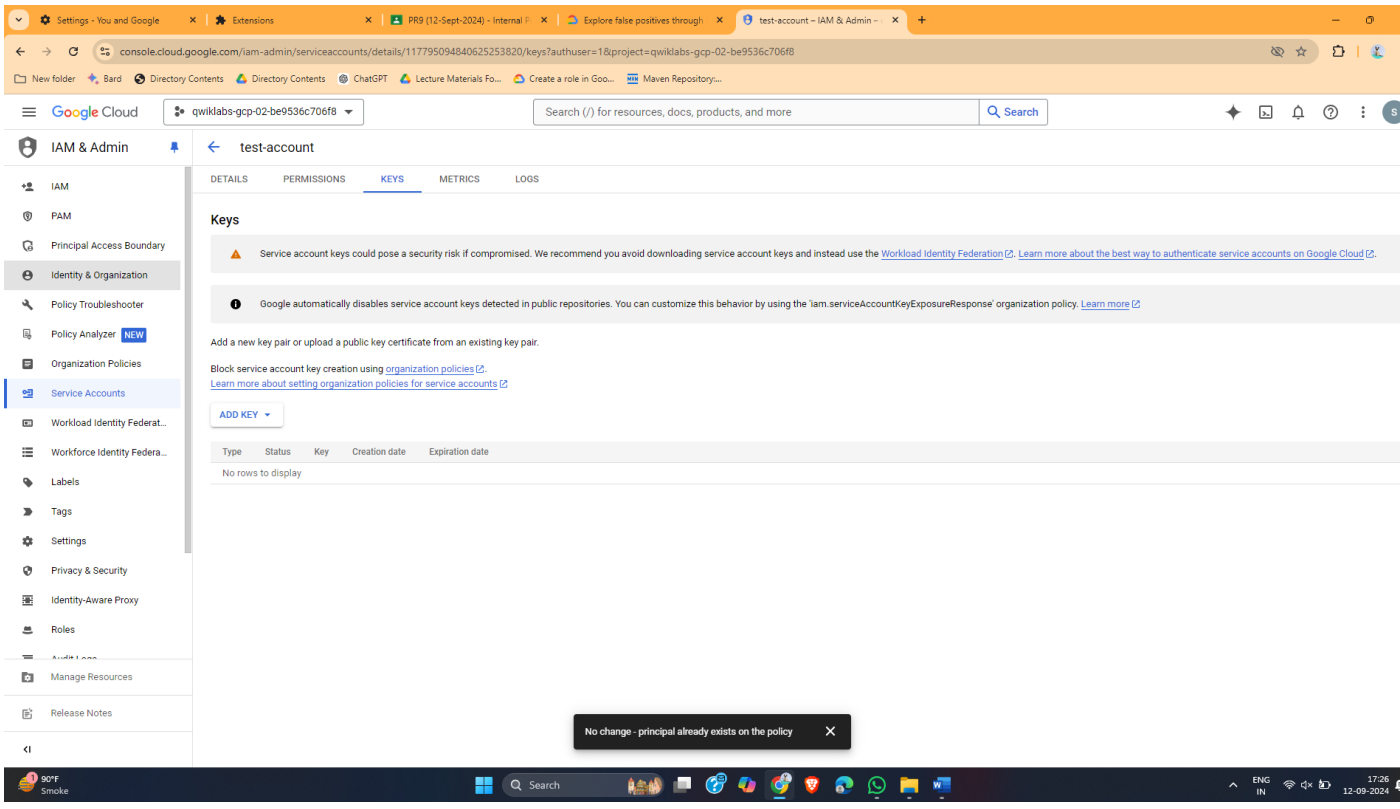
- **Google Cloud Documentation**: IAM Roles and Permissions, Security Command Center, and Cloud Logging.
- **Google Cloud Labs**: Event Threat Detection using Security Command Center.
- **NIST**: https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0

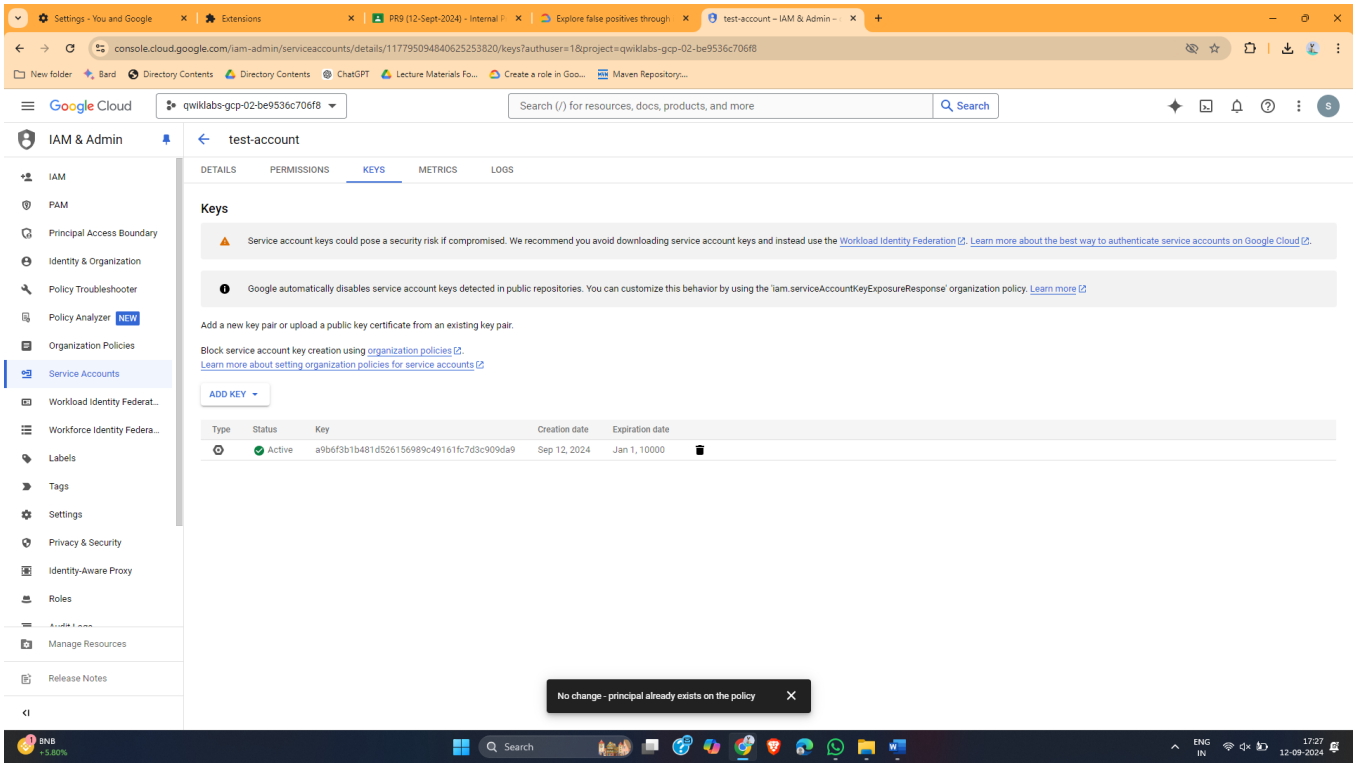
PRACTICAL: 9

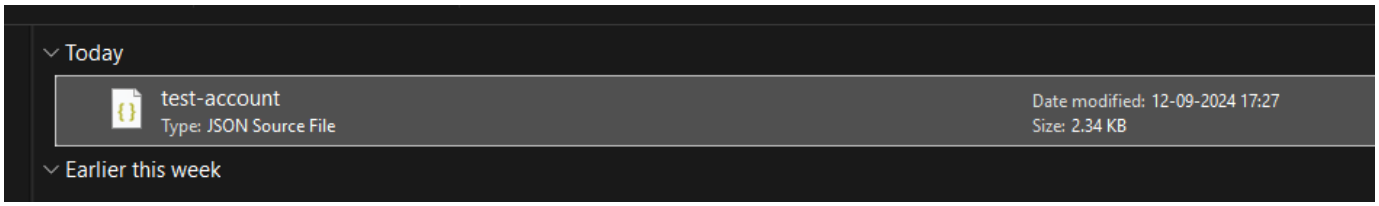

Google Cloud
qwiklabs-gcp-02-be9536c706f8
Search (/) for resources, docs, products, and more
Search
IAM & Admin
Service accounts
+ CREATE SERVICE ACCOUNT
DELETE
MANAGE ACCESS
REFRESH
LEARN
Service accounts for project "qwiklabs-gcp-02-be9536c706f8"
A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more about service accounts.
Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. Learn more about service account organization policies.
Filter Enter property name or value
Email
Status
Name
Description
Key ID
Key creation date
OAuth 2 Client ID
Actions
72642292873-compute@developer.gserviceaccount.com
Enabled
Compute Engine default service account
No keys
qwiklabs-gcp-02-be9536c706f8@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com
Enabled
Qwiklabs User Service Account
068d724c85f60a4bcc8b3af22016a6c5b3d050d2
Sep 10, 2024
hank-test-sa@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com
Enabled
Test Service Account for Hank Byrne
89154bb63d9f58055e9f6bdd1f4e6ae699974af7
Sep 12, 2024
IAM
PAM
Principal Access Boundary
Identity & Organization
Policy Troubleshooter
Policy Analyzer
NEW
Organization Policies
Service Accounts
Workload Identity Federat...
Workforce Identity Federa...
Labels
Tags
Settings
Privacy & Security
Identity-Aware Proxy
Roles
Manage Resources
Release Notes

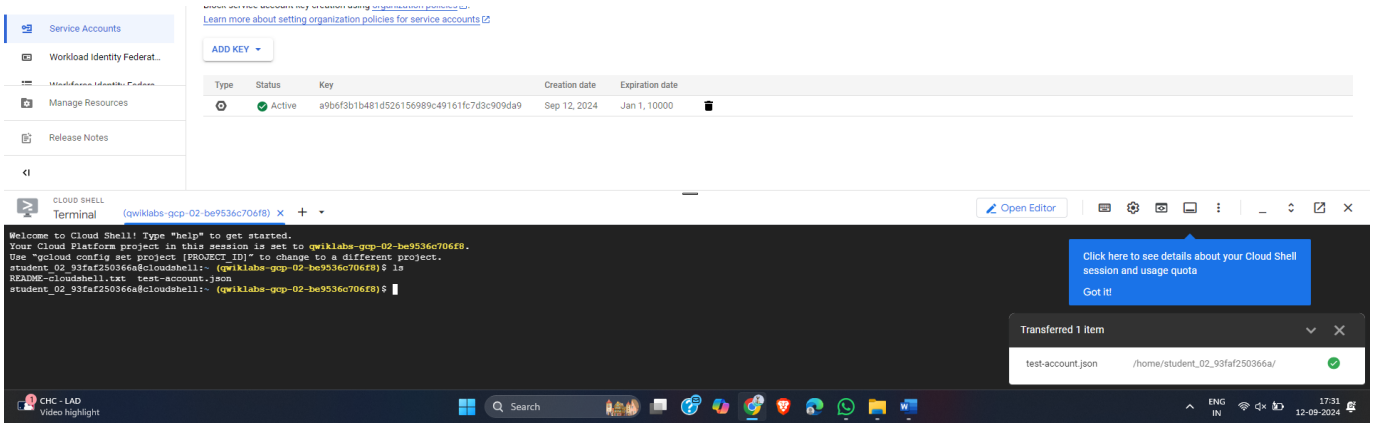

Google Cloud
qwiklabs-gcp-02-be9536c706f8
Search (/) for resources, docs, products, and more
Search
IAM & Admin
Create service account
HIDE INFO PANEL
Service account details
Grant this service account access to project (optional)
Grant users access to this service account (optional)
Grant access to users or groups that need to perform actions as this service account. Learn more
Service account users role
Grant users the permissions to deploy jobs and VMs with this service account
Service account admins role
Grant users the permission to administer this service account
DONE
CANCEL
Permissions
Show inherited roles in table
Display roles inherited from the parent resources in the table below
Filter Enter property name or value
Role / Principal
Inheritance
AI Platform Notebooks Service Agent (1)
Cloud Build Service Agent (1)
Compute Engine Service Agent (1)
Editor (4)
Kubernetes Engine Service Agent (1)
Owner (5)
Viewer (1)
Policy updated
IAM
PAM
Principal Access Boundary
Identity & Organization
Policy Troubleshooter
Policy Analyzer
NEW
Organization Policies
Service Accounts
Workload Identity Federat...
Workforce Identity Federa...
Labels
Tags
Settings
Privacy & Security
Identity-Aware Proxy
Roles
Manage Resources
Release Notes

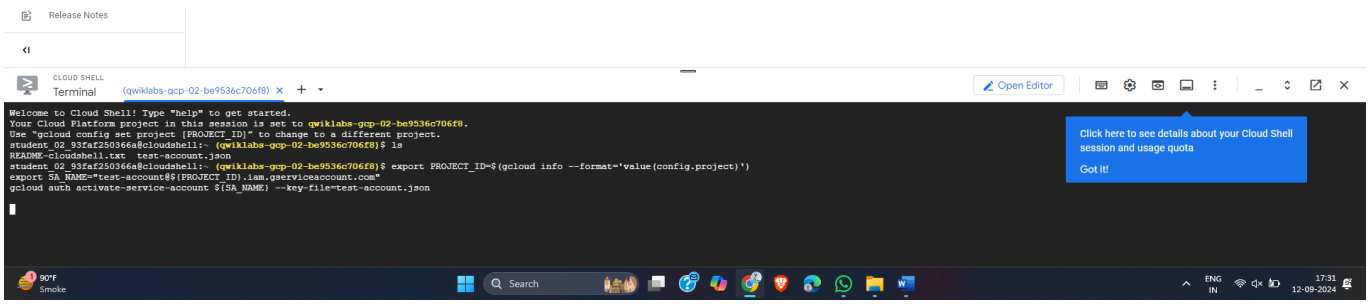

Service accounts – IAM & Admin
console.cloud.google.com/iam-admin/serviceaccounts?authuser=1&project=qwiklabs-gcp-02-be9536c706f8
Google Cloud
qwiklabs-gcp-02-be9536c706f8
Search (/) for resources, docs, products, and more
IAM & Admin
Service accounts
+ CREATE SERVICE ACCOUNT
DELETE
MANAGE ACCESS
REFRESH
LEARN
Service accounts for project "qwiklabs-gcp-02-be9536c706f8"
A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more about service accounts
Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. Learn more about service account organization policies
Filter Enter property name or value
Email
Status
Name
Description
Key ID
Key creation date
OAuth 2 Client ID
Actions
72642292873-compute@developer.gserviceaccount.com
Enabled
Compute Engine default service account
No keys
qwiklabs-gcp-02-be9536c706f8@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com
Enabled
Qwiklabs User Service Account
068d724c85f60a4bcc8b3af22016a6c5b3d050d2
Sep 10, 2024
hank-test-sa@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com
Enabled
Test Service Account for Hank Byrne
89154bb63d9f58055e9f6bdd1f4e6ae699974af7
Sep 12, 2024
test-account@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com
Enabled
test-account
No keys
Manage details
Manage permissions
Manage keys
View metrics
View logs
Disable
Delete
No change - principal already exists on the policy
Recommended for you
Service accounts overview
Create service accounts
List and edit service accounts
Disable and enable service accounts
Delete and undelete service accounts
Manage access to projects, folders, and organizations

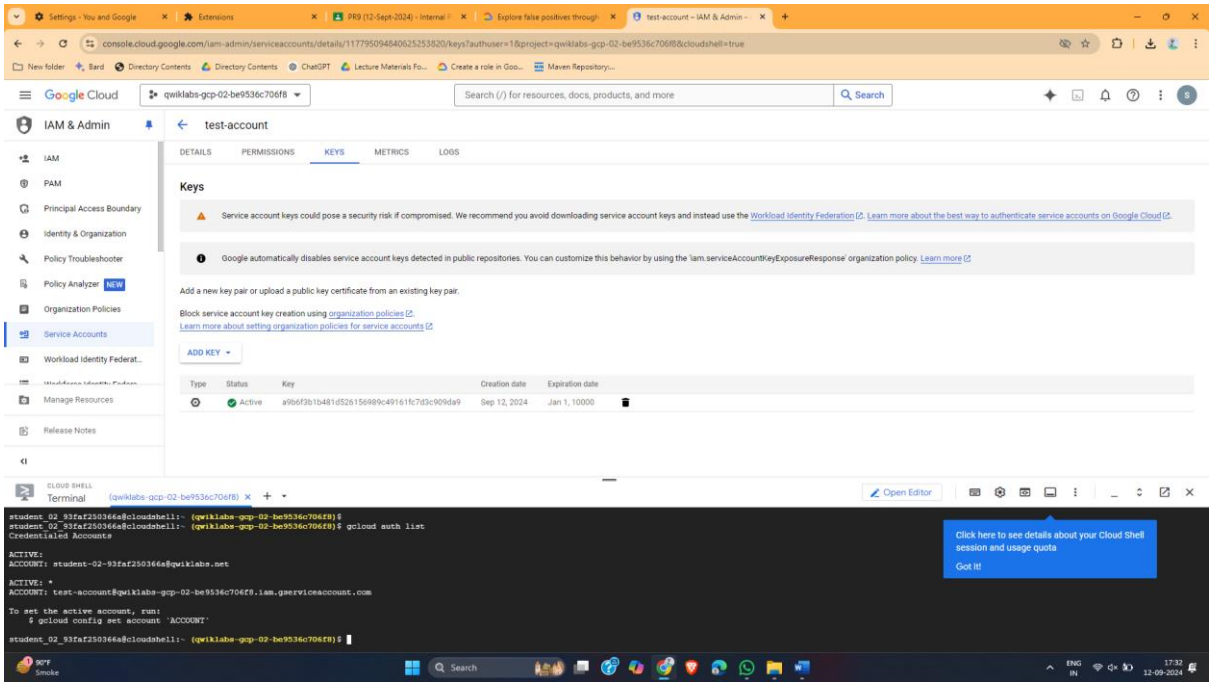

test-account – IAM & Admin
console.cloud.google.com/iam-admin/serviceaccounts/details/117795094840625253820/keys?authuser=1&project=qwiklabs-gcp-02-be9536c706f8
Google Cloud
qwiklabs-gcp-02-be9536c706f8
Search (/) for resources, docs, products, and more
IAM & Admin
test-account
DETAILS
PERMISSIONS
KEYS
METRICS
LOGS
Keys
Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use the Workload Identity Federation. Learn more about the best way to authenticate service accounts on Google Cloud.
Google automatically disables service account keys detected in public repositories. You can customize this behavior by using the 'iam.serviceAccountKeyExposureResponse' organization policy. Learn more
Add a new key pair or upload a public key certificate from an existing key pair.
Block service account key creation using organization policies.
Learn more about setting organization policies for service accounts
ADD KEY
Type
Status
Key
Creation date
Expiration date
No rows to display
No change - principal already exists on the policy

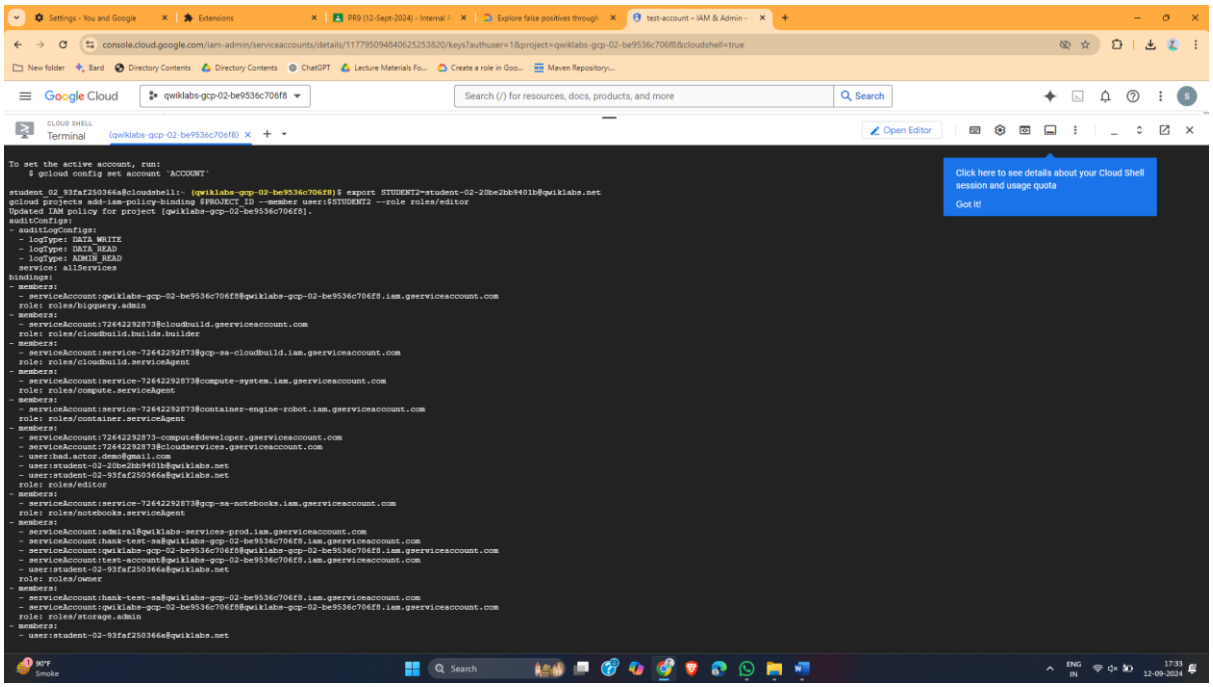

Google Cloud
qwiklabs-gcp-02-be9536c706f8
Search (/) for resources, docs, products, and more
Search
IAM & Admin
test-account
DETAILS
PERMISSIONS
KEYS
METRICS
LOGS
Keys
Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use the Workload Identity Federation. Learn more about the best way to authenticate service accounts on Google Cloud.
Google automatically disables service account keys detected in public repositories. You can customize this behavior by using the 'iam.serviceAccountKeyExposureResponse' organization policy. Learn more
Add a new key pair or upload a public key certificate from an existing key pair.
Block service account key creation using organization policies.
Learn more about setting organization policies for service accounts
ADD KEY
Type
Status
Key
Creation date
Expiration date
Active
a9b6f3b1b481d526156989c49161fc7d3c909da9
Sep 12, 2024
Jan 1, 10000
No change - principal already exists on the policy

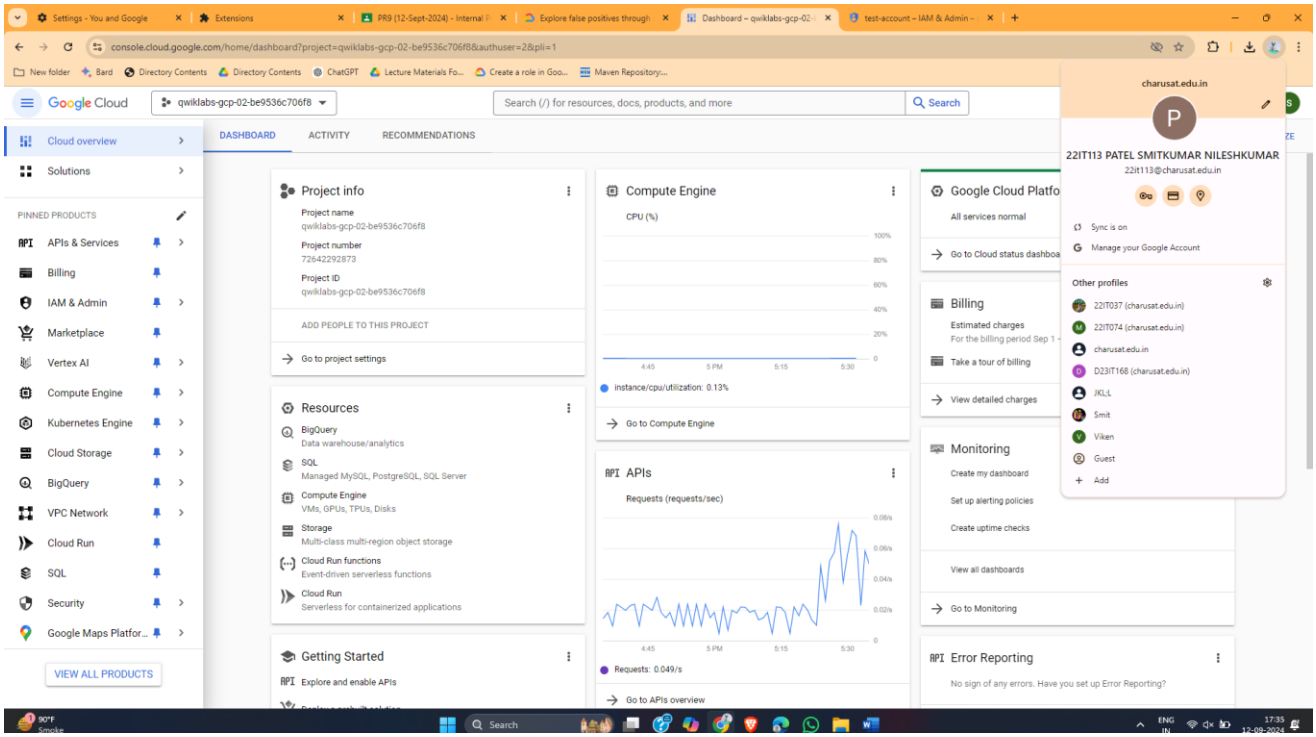

Today
test-account
Type: JSON Source File
Date modified: 12-09-2024 17:27
Size: 2.34 KB
Earlier this week

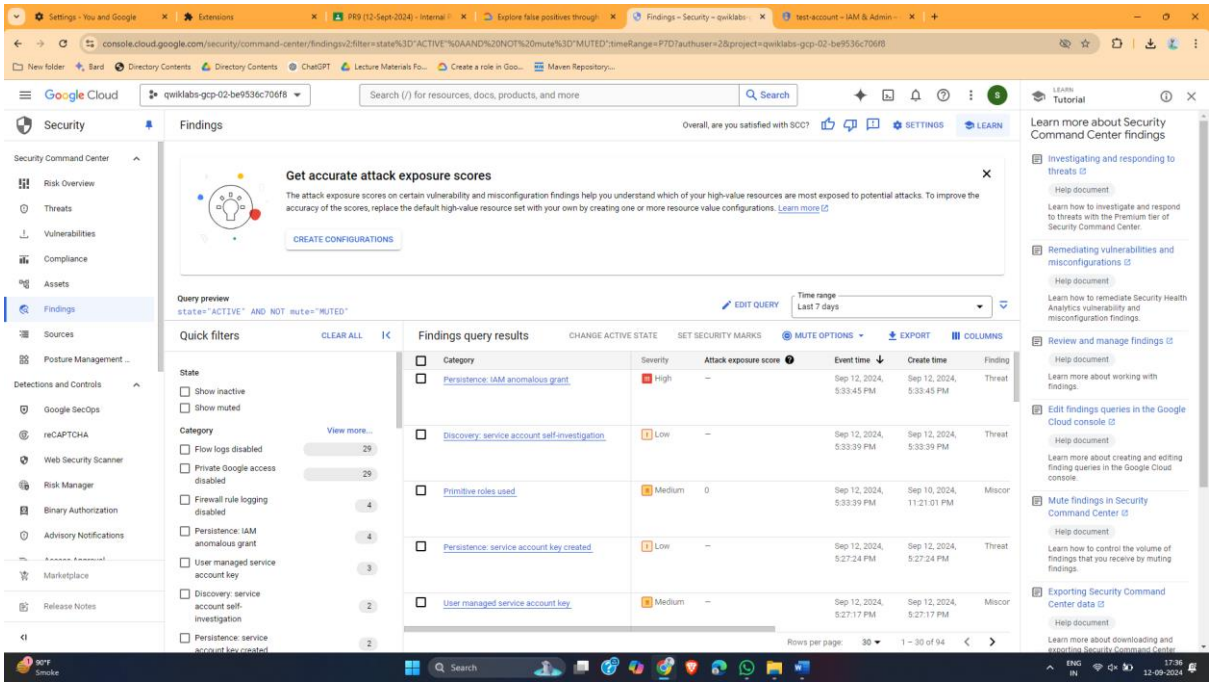

Service Accounts
Workload Identity Federat...
Manage Resources
Release Notes
Learn more about setting organization policies for service accounts
ADD KEY
Type
Status
Key
Creation date
Expiration date
Active
a9b6f3b1b481d526156989c49161fc7d3c909da9
Sep 12, 2024
Jan 1, 10000
CLOUD SHELL
Terminal
(qwiklabs-gcp-02-be9536c706f8)
Open Editor
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to qwiklabs-gcp-02-be9536c706f8.
Use "gcloud config set project [PROJECT_ID]" to change to a different project.
student_02_93faf250366a@cloudshell:~ (qwiklabs-gcp-02-be9536c706f8)$ ls
README-cloudshell.txt test-account.json
student_02_93faf250366a@cloudshell:~ (qwiklabs-gcp-02-be9536c706f8)$
Click here to see details about your Cloud Shell session and usage quota
Got it!
Transferred 1 item
test-account.json
/home/student_02_93faf250366a/

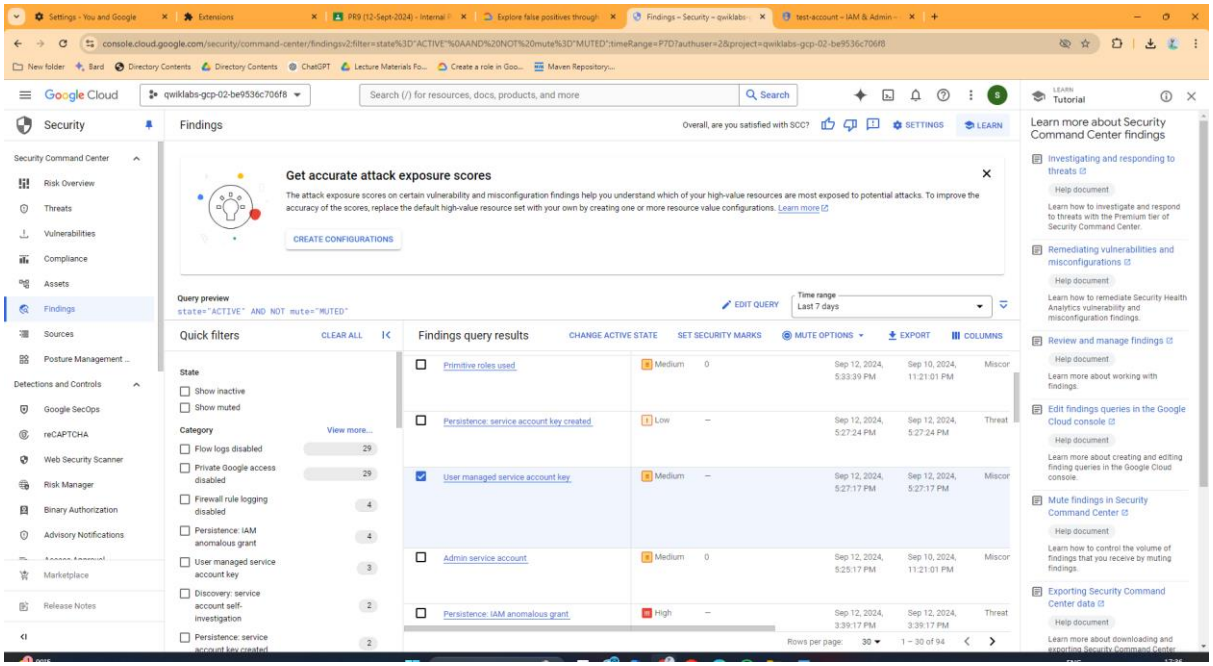

Release Notes
CLOUD SHELL
Terminal
(qwiklabs-gcp-02-be9536c706f8)
Open Editor
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to qwiklabs-gcp-02-be9536c706f8.
Use "gcloud config set project [PROJECT_ID]" to change to a different project.
student_02_93faf250366a@cloudshell:~ (qwiklabs-gcp-02-be9536c706f8)$ ls
README-cloudshell.txt test-account.json
student_02_93faf250366a@cloudshell:~ (qwiklabs-gcp-02-be9536c706f8)$ export PROJECT_ID=$(gcloud info --format='value(config.project)')
export SA_NAME="test-account@${PROJECT_ID}.iam.gserviceaccount.com"
gcloud auth activate-service-account ${SA_NAME} --key-file=test-account.json
Click here to see details about your Cloud Shell session and usage quota
Got it!

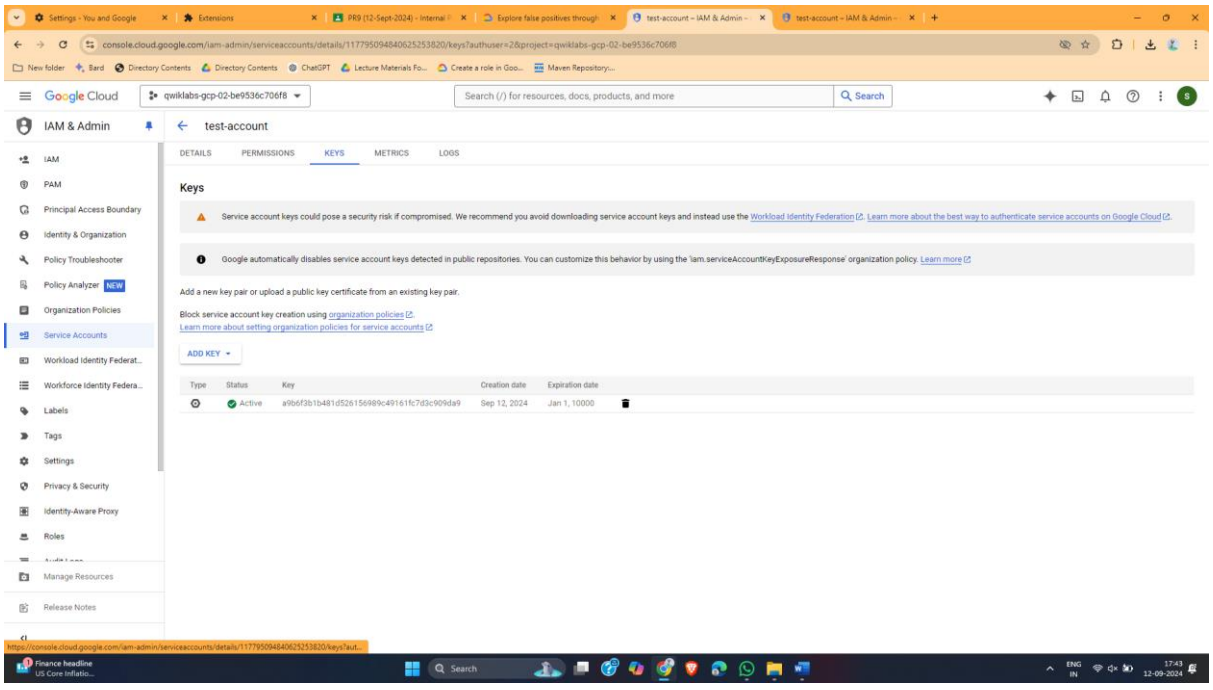

Google Cloud
qwiklabs-gcp-02-be9536c706f8
Search (/) for resources, docs, products, and more
Search
IAM & Admin
test-account
DETAILS
PERMISSIONS
KEYS
METRICS
LOGS
Keys
Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use the Workload Identity Federation. Learn more about the best way to authenticate service accounts on Google Cloud.
Google automatically disables service account keys detected in public repositories. You can customize this behavior by using the 'iam.serviceAccountKeyExposureResponse' organization policy. Learn more
Add a new key pair or upload a public key certificate from an existing key pair.
Block service account key creation using organization policies
Learn more about setting organization policies for service accounts
ADD KEY
Type
Status
Key
Creation date
Expiration date
Active
Sep 12, 2024
Jan 1, 10000
Terminal
Open Editor
Click here to see details about your Cloud Shell session and usage quota
Got it!
student_02_93faf250366a@cloudshell:~ (qwiklabs-gcp-02-be9536c706f8)$
student_02_93faf250366a@cloudshell:~ (qwiklabs-gcp-02-be9536c706f8)$ gcloud auth list
Credentialed Accounts
ACTIVE:
ACCOUNT: student-02-93faf250366a@qwiklabs.net
ACTIVE: *
ACCOUNT: test-account@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com
To set the active account, run:
$ gcloud config set account `ACCOUNT`
student_02_93faf250366a@cloudshell:~ (qwiklabs-gcp-02-be9536c706f8)$

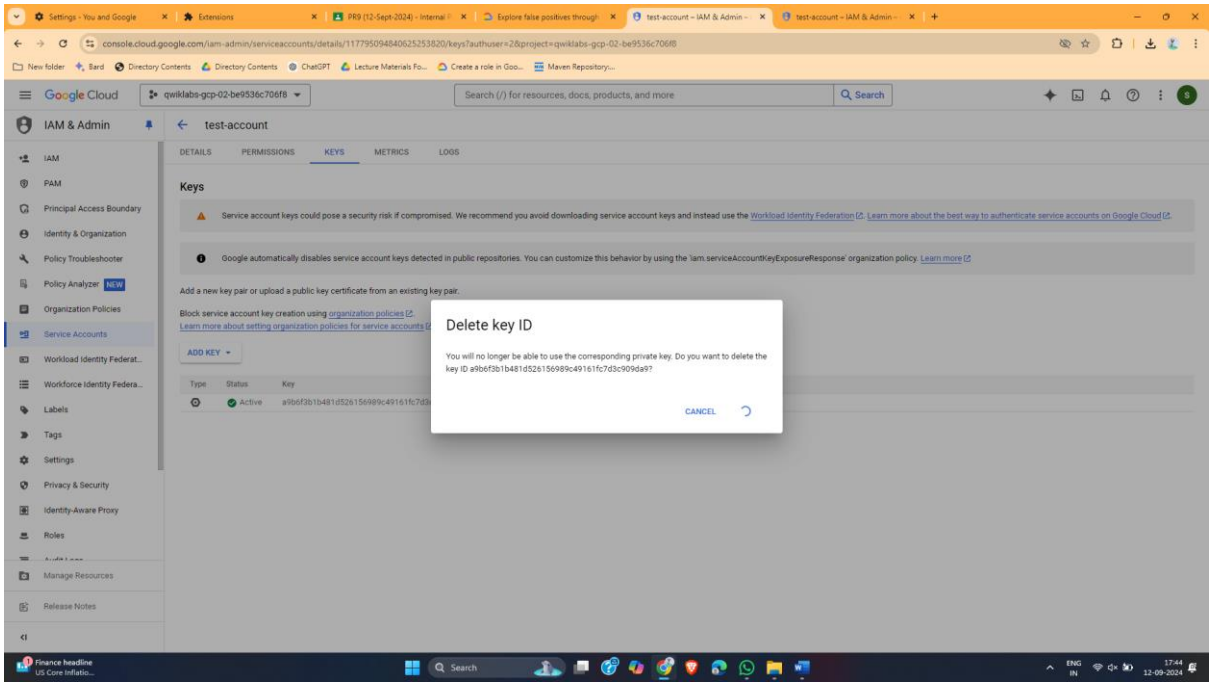

Google Cloud
qwiklabs-gcp-02-be9536c706f8
Search (/) for resources, docs, products, and more
Search
Terminal
Open Editor
Click here to see details about your Cloud Shell session and usage quota
Got it!
To set the active account, run:
$ gcloud config set account `ACCOUNT`
student_02_93faf250366a@cloudshell:~ (qwiklabs-gcp-02-be9536c706f8)$ export STUDENT2=student-02-20be2bb9401b@qwiklabs.net
gcloud projects add-iam-policy-binding $PROJECT_ID --member user:$STUDENT2 --role roles/editor
Updated IAM policy for project [qwiklabs-gcp-02-be9536c706f8].
auditConfigs:
- auditLogConfigs:
- logType: DATA_WRITE
- logType: DATA_READ
- logType: ADMIN_READ
service: allServices
bindings:
- members:
- serviceAccount:qwiklabs-gcp-02-be9536c706f8@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com
role: roles/bigquery.admin
- members:
- serviceAccount:726422928?3@cloudbuild.gserviceaccount.com
role: roles/cloudbuild.builds.builder
- members:
- serviceAccount:service-726422928?3@gcp-sa-cloudbuild.iam.gserviceaccount.com
role: roles/cloudbuild.serviceAgent
- members:
- serviceAccount:service-726422928?3@compute-system.iam.gserviceaccount.com
role: roles/compute.serviceAgent
- members:
- serviceAccount:service-726422928?3@container-engine-robot.iam.gserviceaccount.com
role: roles/container.serviceAgent
- members:
- serviceAccount:726422928?3-compute@developer.gserviceaccount.com
- serviceAccount:726422928?3@cloudservices.gserviceaccount.com
- user:bad.actor.demo@gmail.com
- user:student-02-20be2bb9401b@qwiklabs.net
- user:student-02-93faf250366a@qwiklabs.net
role: roles/editor
- members:
- serviceAccount:service-726422928?3@gcp-sa-notebooks.iam.gserviceaccount.com
role: roles/notebooks.serviceAgent
- members:
- serviceAccount:admiral@qwiklabs-services-prod.iam.gserviceaccount.com
- serviceAccount:hank-test-sa@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com
- serviceAccount:qwiklabs-gcp-02-be9536c706f8@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com
- serviceAccount:test-account@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com
- user:student-02-93faf250366a@qwiklabs.net
role: roles/owner
- members:
- serviceAccount:hank-test-sa@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com
- serviceAccount:qwiklabs-gcp-02-be9536c706f8@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com
role: roles/storage.admin
- members:
- user:student-02-93faf250366a@qwiklabs.net

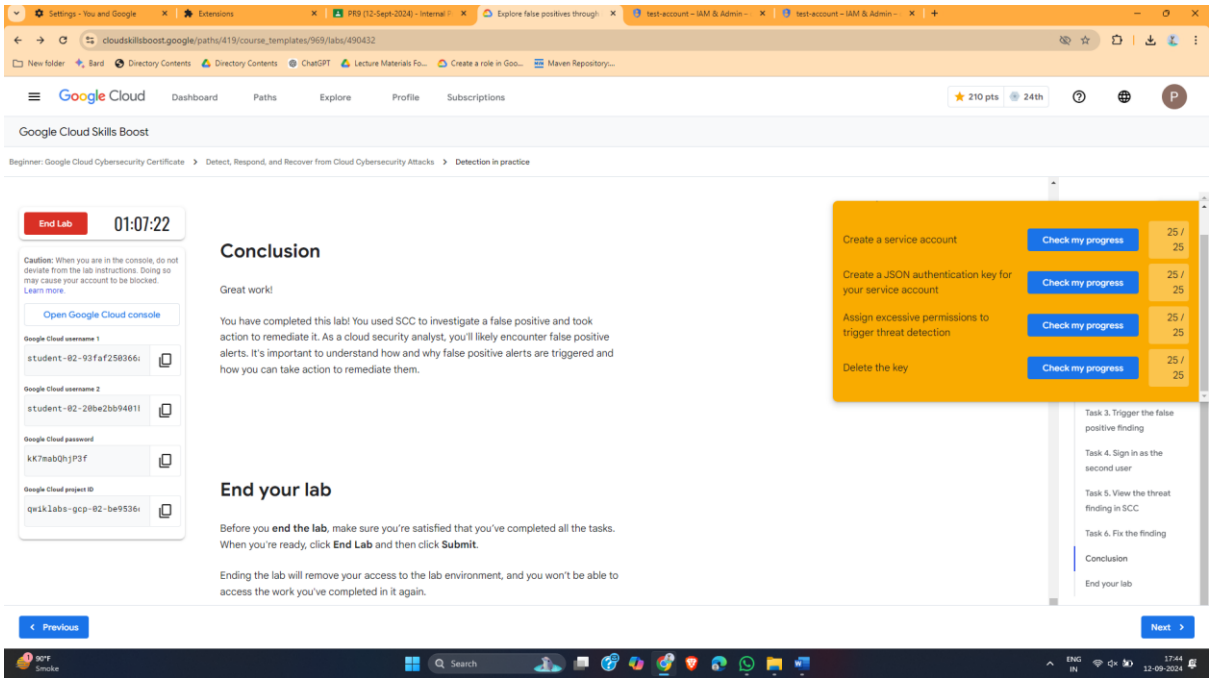

Google Cloud
qwiklabs-gcp-02-be9536c706f8
Search (/) for resources, docs, products, and more
Search
DASHBOARD
ACTIVITY
RECOMMENDATIONS
Cloud overview
Solutions
PINNED PRODUCTS
APIs & Services
Billing
IAM & Admin
Marketplace
Vertex AI
Compute Engine
Kubernetes Engine
Cloud Storage
BigQuery
VPC Network
Cloud Run
SQL
Security
Google Maps Platfor...
VIEW ALL PRODUCTS
Project info
Project name
qwiklabs-gcp-02-be9536c706f8
Project number
72642292873
Project ID
qwiklabs-gcp-02-be9536c706f8
ADD PEOPLE TO THIS PROJECT
Go to project settings
Resources
BigQuery
Data warehouse/analytics
SQL
Managed MySQL, PostgreSQL, SQL Server
Compute Engine
VMs, GPUs, TPUs, Disks
Storage
Multi-class multi-region object storage
Cloud Run functions
Event-driven serverless functions
Cloud Run
Serverless for containerized applications
Getting Started
Explore and enable APIs
Compute Engine
CPU (%)
instance/cpu/utilization: 0.13%
Go to Compute Engine
APIs
Requests (requests/sec)
Requests: 0.049/s
Go to APIs overview
Google Cloud Platfo
All services normal
Go to Cloud status dashboa
Billing
Estimated charges
For the billing period Sep 1 -
Take a tour of billing
View detailed charges
Monitoring
Create my dashboard
Set up alerting policies
Create uptime checks
View all dashboards
Go to Monitoring
Error Reporting
No sign of any errors. Have you set up Error Reporting?
charusat.edu.in
22IT113 PATEL SMITKUMAR NILESHKUMAR
22it113@charusat.edu.in
Sync is on
Manage your Google Account
Other profiles
22IT037 (charusat.edu.in)
22IT074 (charusat.edu.in)
charusat.edu.in
D23IT168 (charusat.edu.in)
JKLL
Smit
Viken
Guest
Add

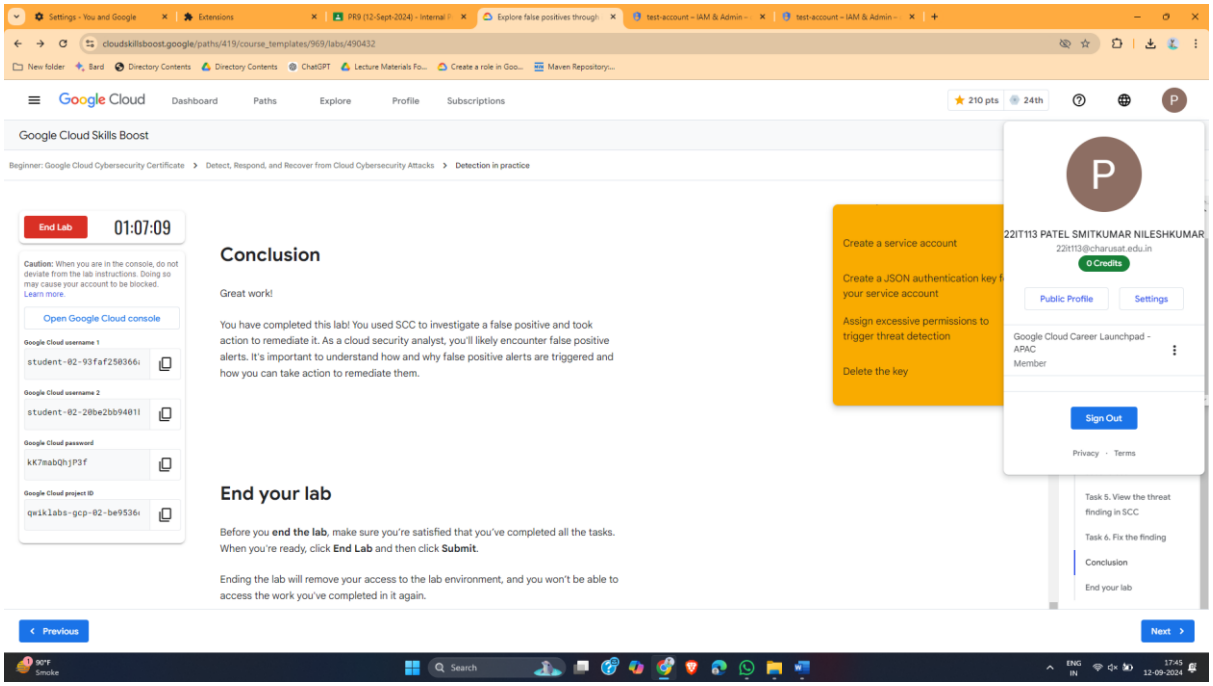

Google Cloud
qwiklabs-gcp-02-be9536c706f8
Search (/) for resources, docs, products, and more
Search
Security
Findings
Security Command Center
Risk Overview
Threats
Vulnerabilities
Compliance
Assets
Findings
Sources
Posture Management ...
Detections and Controls
Google SecOps
reCAPTCHA
Web Security Scanner
Risk Manager
Binary Authorization
Advisory Notifications
Marketplace
Release Notes
Overall, are you satisfied with SCC?
SETTINGS
LEARN
Get accurate attack exposure scores
The attack exposure scores on certain vulnerability and misconfiguration findings help you understand which of your high-value resources are most exposed to potential attacks. To improve the accuracy of the scores, replace the default high-value resource set with your own by creating one or more resource value configurations. Learn more
CREATE CONFIGURATIONS
Query preview
state="ACTIVE" AND NOT mute="MUTED"
EDIT QUERY
Time range
Last 7 days
Quick filters
CLEAR ALL
State
Show inactive
Show muted
Category
View more...
Flow logs disabled 29
Private Google access disabled 29
Firewall rule logging disabled 4
Persistence: IAM anomalous grant 4
User managed service account key 3
Discovery: service account self-investigation 2
Persistence: service account key created 2
Findings query results
CHANGE ACTIVE STATE
SET SECURITY MARKS
MUTE OPTIONS
EXPORT
COLUMNS
Category
Severity
Attack exposure score
Event time
Create time
Finding
Persistence: IAM anomalous grant
High
Sep 12, 2024, 5:33:45 PM
Sep 12, 2024, 5:33:45 PM
Threat
Discovery: service account self-investigation
Low
Sep 12, 2024, 5:33:39 PM
Sep 12, 2024, 5:33:39 PM
Threat
Primitive roles used
Medium
0
Sep 12, 2024, 5:33:39 PM
Sep 10, 2024, 11:21:01 PM
Miscor
Persistence: service account key created
Low
Sep 12, 2024, 5:27:24 PM
Sep 12, 2024, 5:27:24 PM
Threat
User managed service account key
Medium
Sep 12, 2024, 5:27:17 PM
Sep 12, 2024, 5:27:17 PM
Miscor
Rows per page: 30
1 – 30 of 94
Tutorial
Learn more about Security Command Center findings
Investigating and responding to threats
Help document
Learn how to investigate and respond to threats with the Premium tier of Security Command Center.
Remediating vulnerabilities and misconfigurations
Help document
Learn how to remediate Security Health Analytics vulnerability and misconfiguration findings.
Review and manage findings
Help document
Learn more about working with findings.
Edit findings queries in the Google Cloud console
Help document
Learn more about creating and editing finding queries in the Google Cloud console.
Mute findings in Security Command Center
Help document
Learn how to control the volume of findings that you receive by muting findings.
Exporting Security Command Center data
Help document
Learn more about downloading and exporting Security Command Center


Google Cloud
Security
Findings
Get accurate attack exposure scores
CREATE CONFIGURATIONS
Quick filters
Findings query results
Learn more about Security Command Center findings


Google Cloud
IAM & Admin
test-account
DETAILS
PERMISSIONS
KEYS
METRICS
LOGS
Keys
ADD KEY


Google Cloud
IAM & Admin
test-account
DETAILS
PERMISSIONS
KEYS
METRICS
LOGS
Keys
Delete key ID
You will no longer be able to use the corresponding private key. Do you want to delete the key ID a9b6f3b1b481d526156989c49161fc7d3c909da9?
CANCEL


Google Cloud
Dashboard
Paths
Explore
Profile
Subscriptions
Google Cloud Skills Boost
End Lab
01:07:22
Conclusion
Great work!
You have completed this lab! You used SCC to investigate a false positive and took action to remediate it. As a cloud security analyst, you'll likely encounter false positive alerts. It's important to understand how and why false positive alerts are triggered and how you can take action to remediate them.
End your lab
Before you end the lab, make sure you're satisfied that you've completed all the tasks. When you're ready, click End Lab and then click Submit.
Ending the lab will remove your access to the lab environment, and you won't be able to access the work you've completed in it again.
Create a service account
Check my progress
25 / 25
Create a JSON authentication key for your service account
Check my progress
25 / 25
Assign excessive permissions to trigger threat detection
Check my progress
25 / 25
Delete the key
Check my progress
25 / 25
Previous
Next


Google Cloud
Dashboard
Paths
Explore
Profile
Subscriptions
Google Cloud Skills Boost
End Lab
01:07:09
Open Google Cloud console
Conclusion
Great work!
You have completed this lab! You used SCC to investigate a false positive and took action to remediate it. As a cloud security analyst, you'll likely encounter false positive alerts. It's important to understand how and why false positive alerts are triggered and how you can take action to remediate them.
End your lab
Before you end the lab, make sure you're satisfied that you've completed all the tasks. When you're ready, click End Lab and then click Submit.
Ending the lab will remove your access to the lab environment, and you won't be able to access the work you've completed in it again.
Create a service account
Assign excessive permissions to trigger threat detection
Delete the key
22IT113 PATEL SMITKUMAR NILESHKUMAR
0 Credits
Public Profile
Settings
Sign Out
Task 5. View the threat finding in SCC
Task 6. Fix the finding
Conclusion
End your lab
Previous
Next

PRACTICAL: 10

AIM:

Google Cloud services write audit logs that record administrative activities and access within your Google Cloud resources. Audit log entries help you answer the questions "who did what, where, and when" within your Google Cloud projects. Enabling audit logs helps your security, auditing, and compliance entities monitor Google Cloud data and systems for possible vulnerabilities or external data misuse. In this experiment, you'll investigate audit logs to identify patterns of suspicious activity involving cloud resources.

THEORY:

Google Cloud audit logs are essential for maintaining security, monitoring, and auditing activities across cloud projects. These logs capture detailed information about who performed which actions, when, and where within your Google Cloud environment. They help ensure compliance with regulatory standards by logging administrative actions and access to cloud resources. This data becomes critical when investigating suspicious activities, identifying vulnerabilities, and responding to security breaches.

Google Cloud provides two types of audit logs:

1. **Admin Activity logs**: Capture information about modifications made to the configuration or metadata of cloud resources, such as creating or deleting resources.
2. **Data Access logs**: Track access to data within Google Cloud services.

This practical exercise involves navigating Google Cloud's audit logs to investigate and analyze patterns of suspicious activity within your cloud resources. Through these logs, you'll explore how to monitor, filter, and analyze administrative and data access activities to identify potential misuse of resources.

OUTPUT:

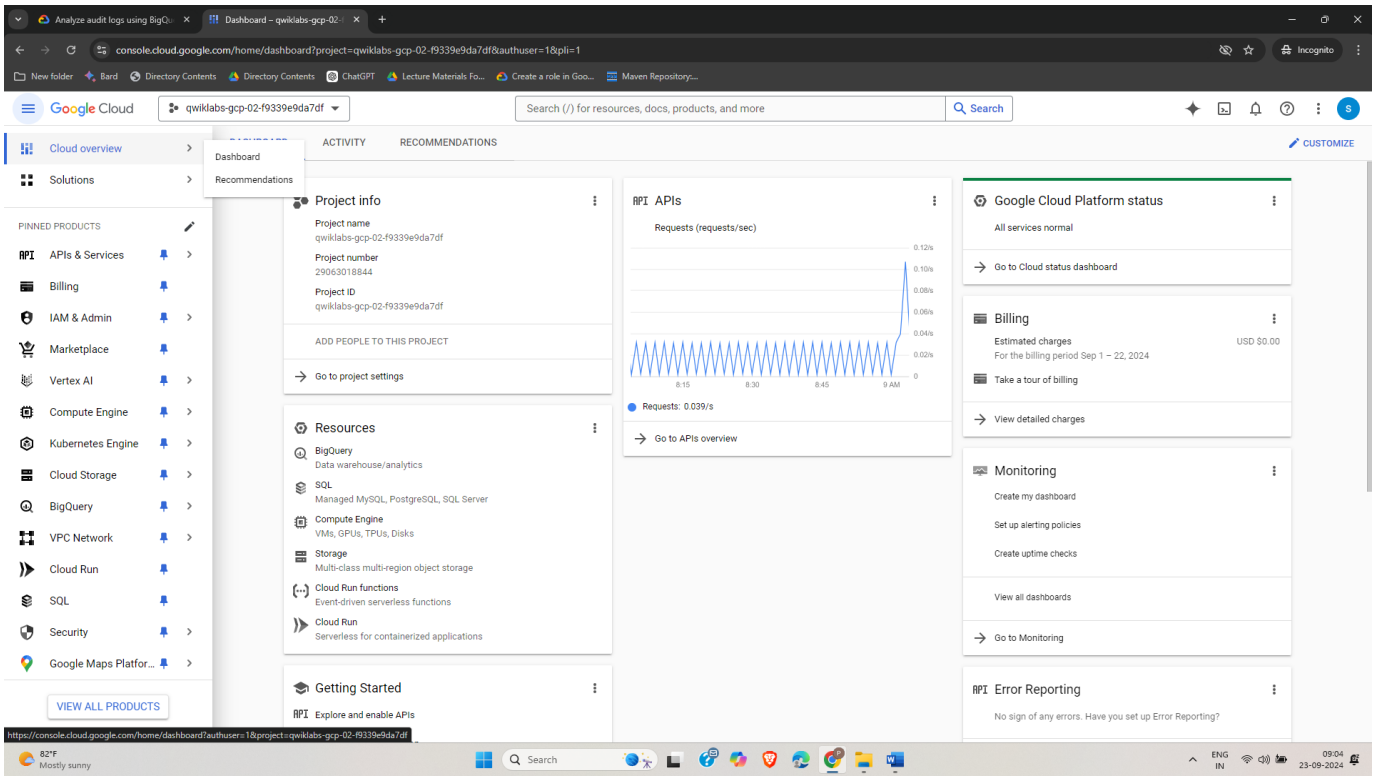


Figure 1 : Successful login using credentials for Username 1.

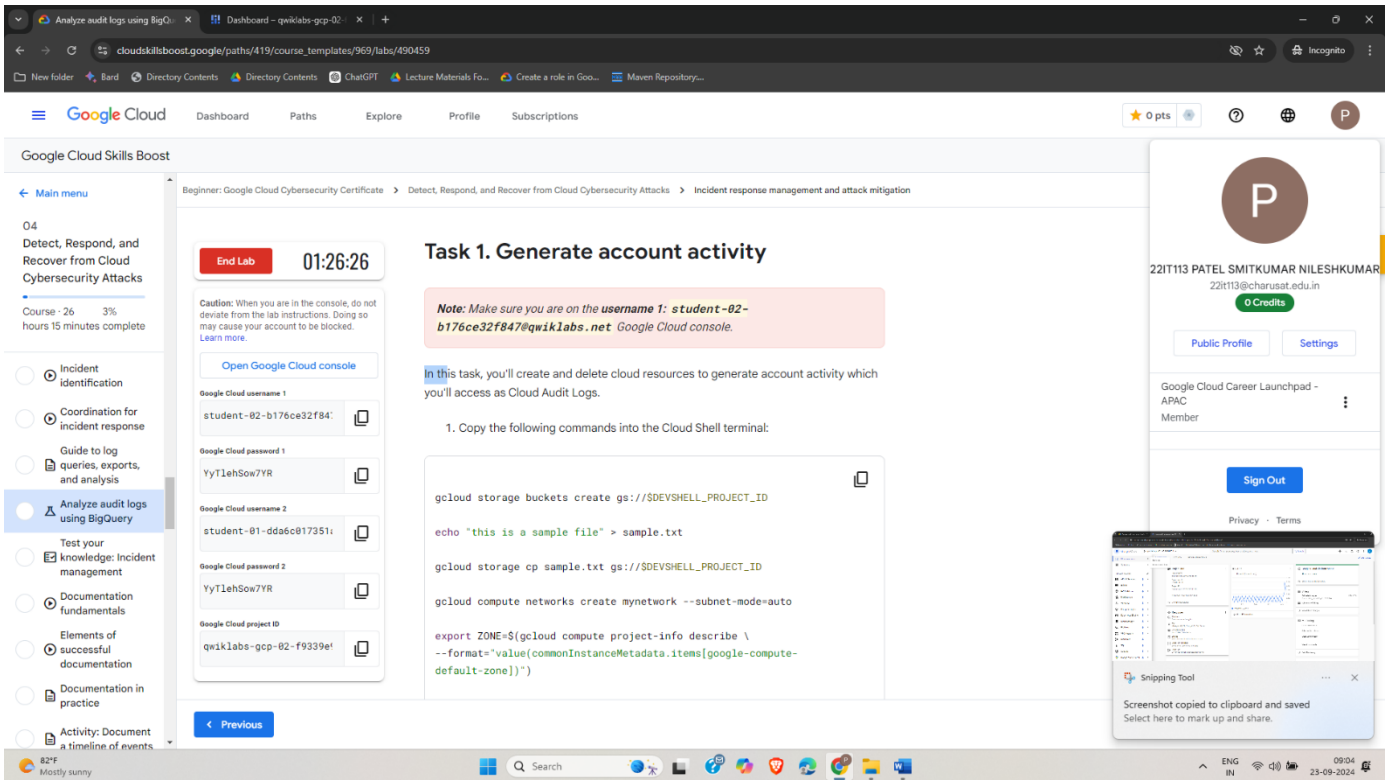


Figure 2 : The initial reference screen after logging in.

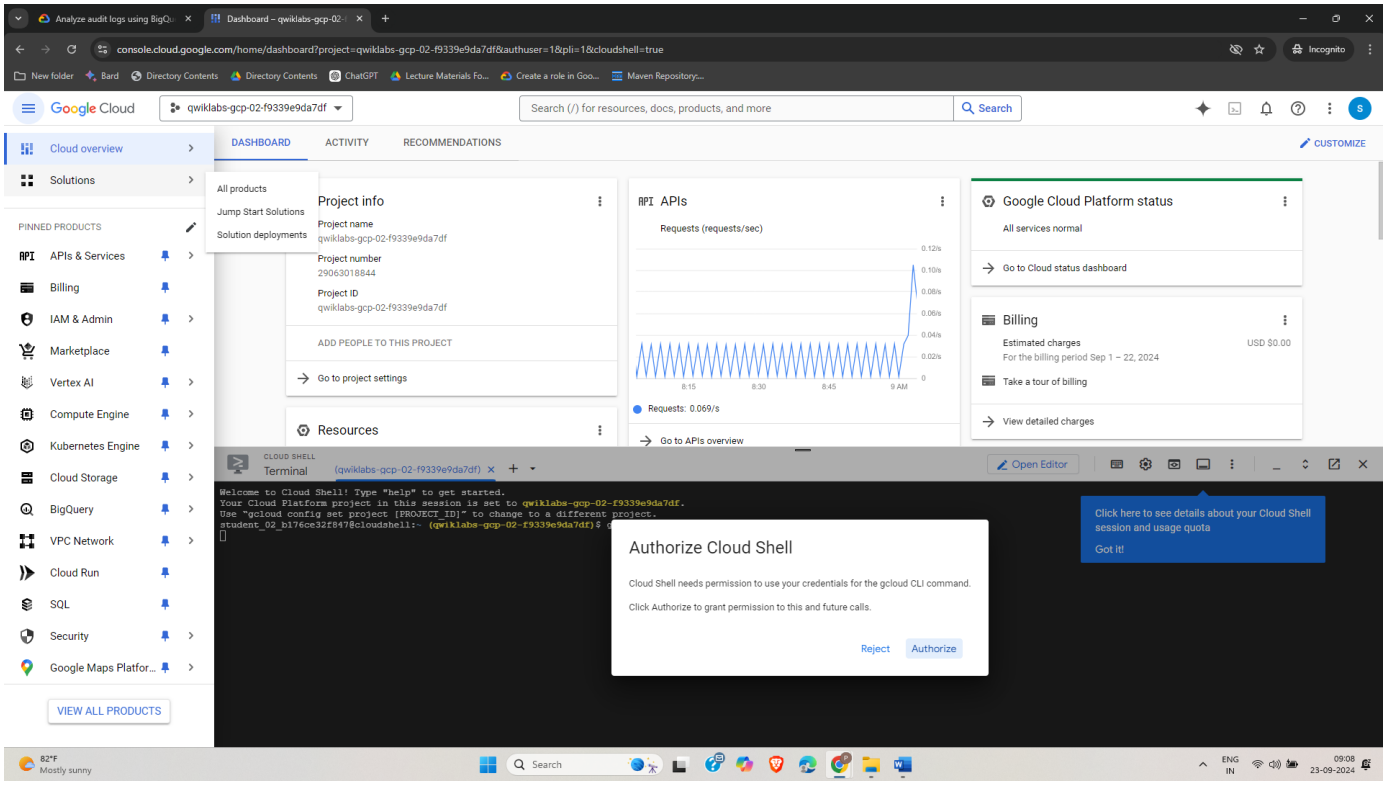


Figure 3 : Authorization request within Cloud Shell for accessing resources.

```
student_02_b176ce32f847@cloudshell:~ (qwiklabs-gcp-02-f9339e9da7df)$ gcloud auth list
Credentialed Accounts

ACTIVE: *
ACCOUNT: student-02-b176ce32f847@qwiklabs.net

To set the active account, run:
    $ gcloud config set account `ACCOUNT`

student_02_b176ce32f847@cloudshell:~ (qwiklabs-gcp-02-f9339e9da7df)$ gcloud config list project
[core]
project = qwiklabs-gcp-02-f9339e9da7df

Your active configuration is: [cloudshell-5255]
student_02_b176ce32f847@cloudshell:~ (qwiklabs-gcp-02-f9339e9da7df)$
```

Figure 4 : Displaying configuration values set as project variables.

```
Your active configuration is: [cloudshell-5255]
student_02_b176ce32f847@cloudshell:~ (qwiklabs-gcp-02-f9339e9da7df)$
gcloud storage buckets create gs://$DEVSHELL_PROJECT_ID

echo "this is a sample file" > sample.txt

gcloud storage cp sample.txt gs://$DEVSHELL_PROJECT_ID

gcloud compute networks create mynetwork --subnet-mode=auto

export ZONE=$(gcloud compute project-info describe \
--format="value(commonInstanceMetadata.items[google-compute-default-zone])")

gcloud compute instances create default-us-vm \
--machine-type=e2-micro \
--zone=$ZONE --network=mynetwork

gcloud storage rm --recursive gs://$DEVSHELL_PROJECT_ID
Creating gs://qwiklabs-gcp-02-f9339e9da7df/...
Copying file://sample.txt to gs://qwiklabs-gcp-02-f9339e9da7df/sample.txt
  Completed files 1/1 | 22.0B/22.0B
Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-02-f9339e9da7df/global/networks/mynetwork].
NAME: mynetwork
SUBNET_MODE: AUTO
BGP_ROUTING_MODE: REGIONAL
IPV4_RANGE:
GATEWAY_IPV4:

Instances on this network will not be reachable until firewall rules
are created. As an example, you can allow all internal traffic between
instances as well as SSH, RDP, and ICMP by running:

$ gcloud compute firewall-rules create <FIREWALL_NAME> --network mynetwork --allow tcp,udp,icmp --source-ranges <IP_RANGE>
$ gcloud compute firewall-rules create <FIREWALL_NAME> --network mynetwork --allow tcp:22,tcp:3389,icmp

Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-02-f9339e9da7df/zones/us-east1-d/instances/default-us-vm].
NAME: default-us-vm
ZONE: us-east1-d
MACHINE_TYPE: e2-micro
PREEMPTIBLE:
INTERNAL_IP: 10.142.0.2
EXTERNAL_IP: 34.73.110.4
STATUS: RUNNING
Removing objects:
Removing gs://qwiklabs-gcp-02-f9339e9da7df/sample.txt#1727062796373328...
  Completed 1/1
Removing buckets:
Removing gs://qwiklabs-gcp-02-f9339e9da7df/...
  Completed 1/1
student_02_b176ce32f847@cloudshell:~ (qwiklabs-gcp-02-f9339e9da7df)$
```

Figure 5 : Running a command to generate logs by creating and deleting cloud resources.

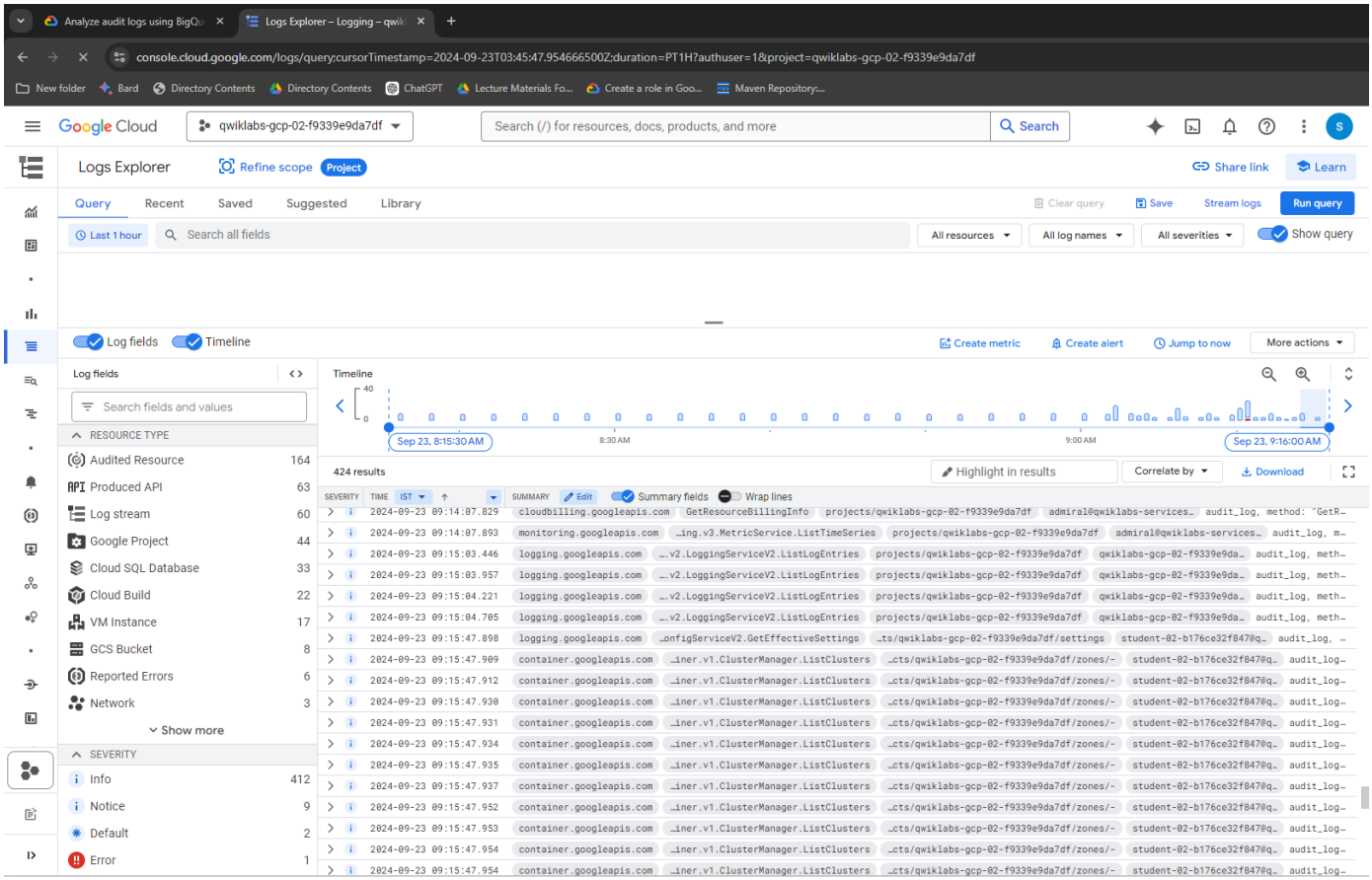


Figure 6 : Navigating to Cloud Logging using the Cloud Logging Explorer.

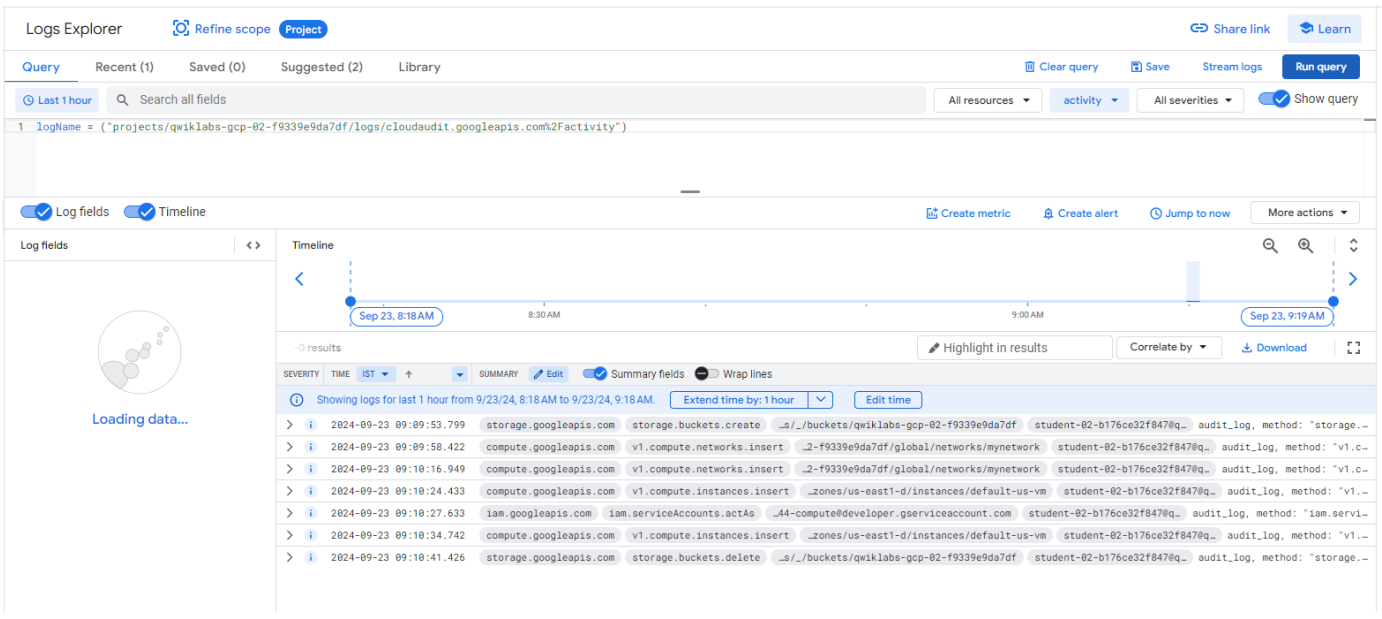


Figure 7 : Running a query in the Query Editor to find log activity.

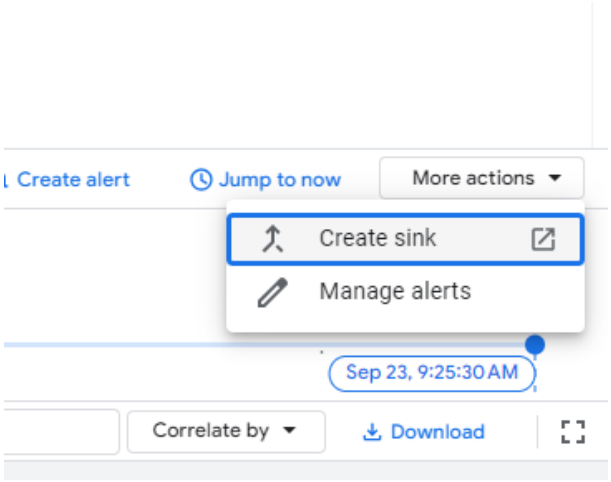


Figure 8 : Proceeding to create a log sink for audit log export.

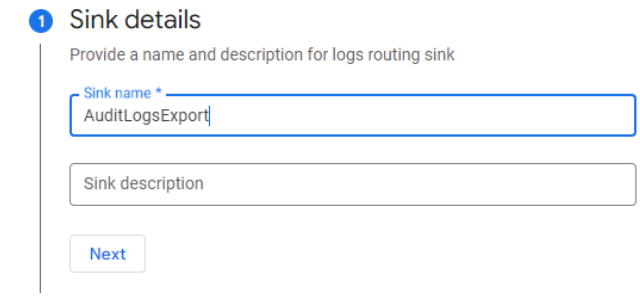


Figure 9 : Inputing a name for the log sink.

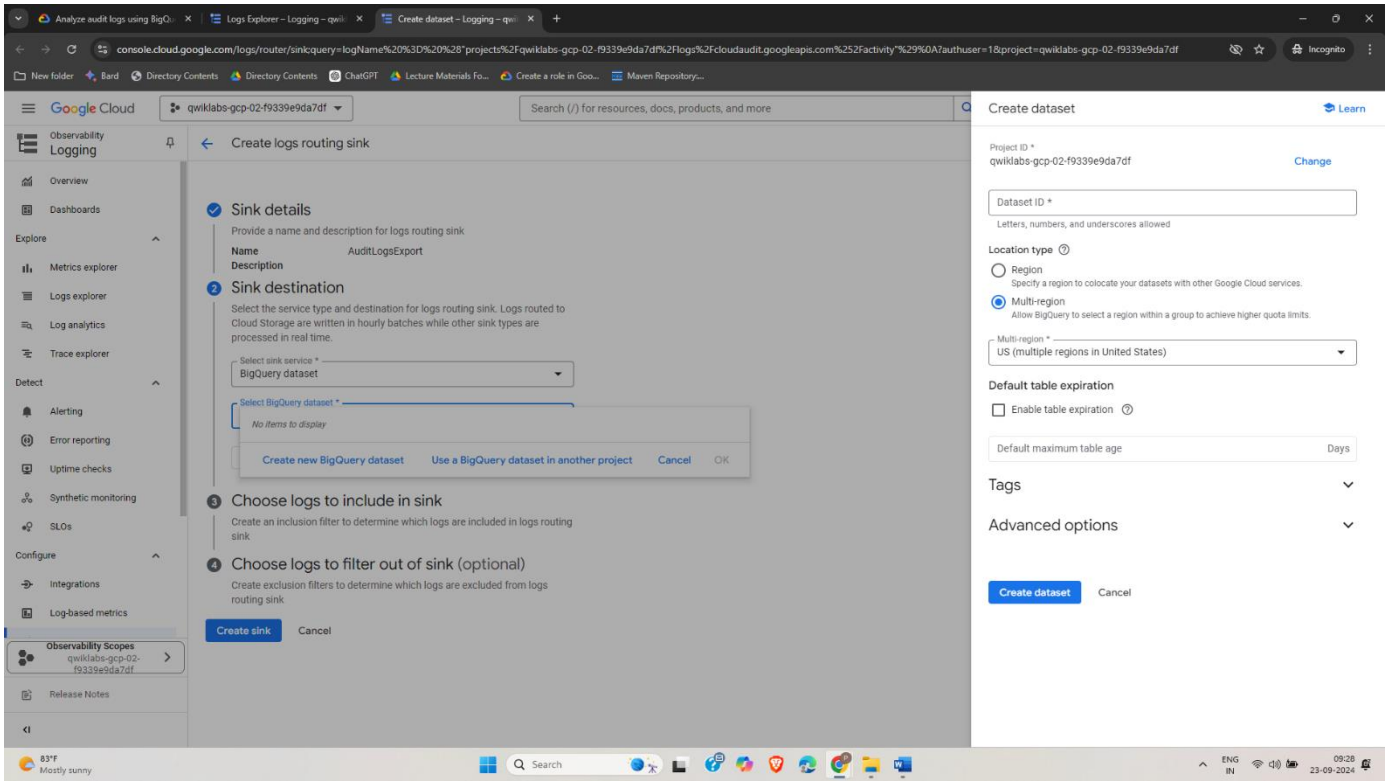


Figure 10 : Selecting BigQuery as the destination for the audit log export and creating a dataset.

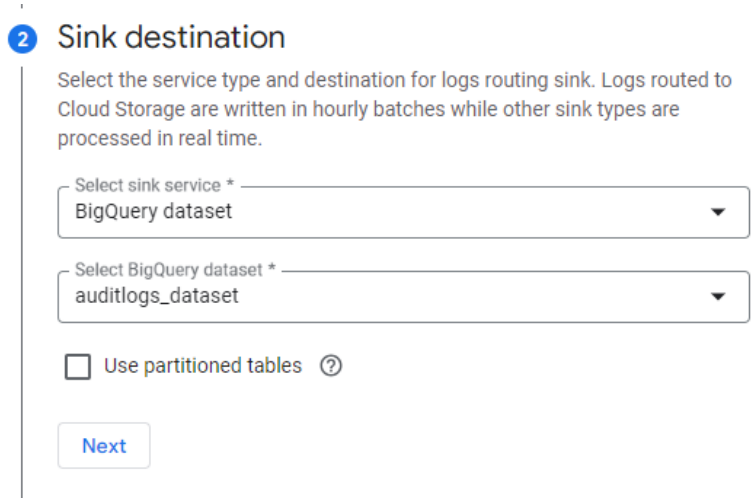


Figure 11 : Successfully creating the auditlog_dataset in BigQuery.

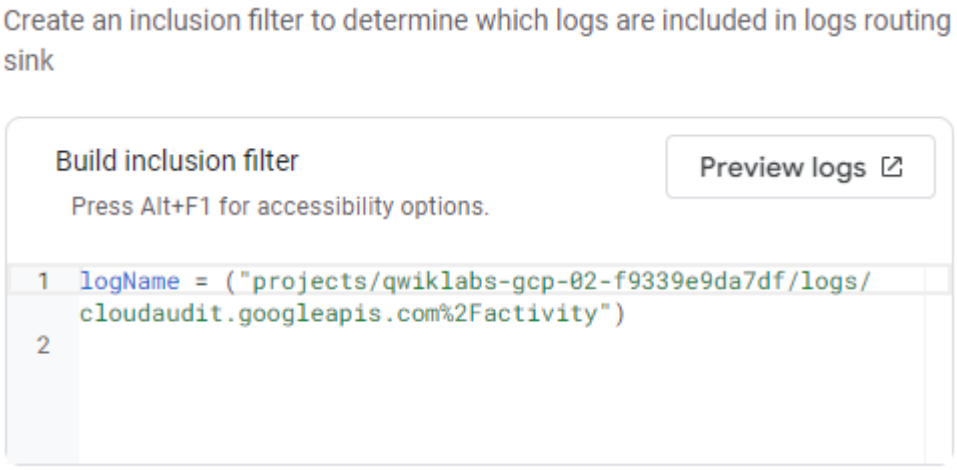


Figure 12 : Viewing build functions for processing audit logs.

Sink details

Provide a name and description for logs routing sink

Name AuditLogsExport

Description

Sink destination

Select the service type and destination for logs routing sink. Logs routed to Cloud Storage are written in hourly batches while other sink types are processed in real time.

Service Destination BigQuery dataset

bigquery.googleapis.com/projects/qwiklabs-gcp-02-f9339e9da7df/datasets/auditlogs_dataset

Partitioned No

Choose logs to include in sink

Create an inclusion filter to determine which logs are included in logs routing sink

Inclusion filter

```
logName = ("projects/qwiklabs-gcp-02-f9339e9da7df/logs/cloudaudit.googleapis.com%2Factivity")
```

Choose logs to filter out of sink (optional)

Create exclusion filters to determine which logs are excluded from logs routing sink

Processing... Cancel

Figure 13 : Completing the log sink creation process.

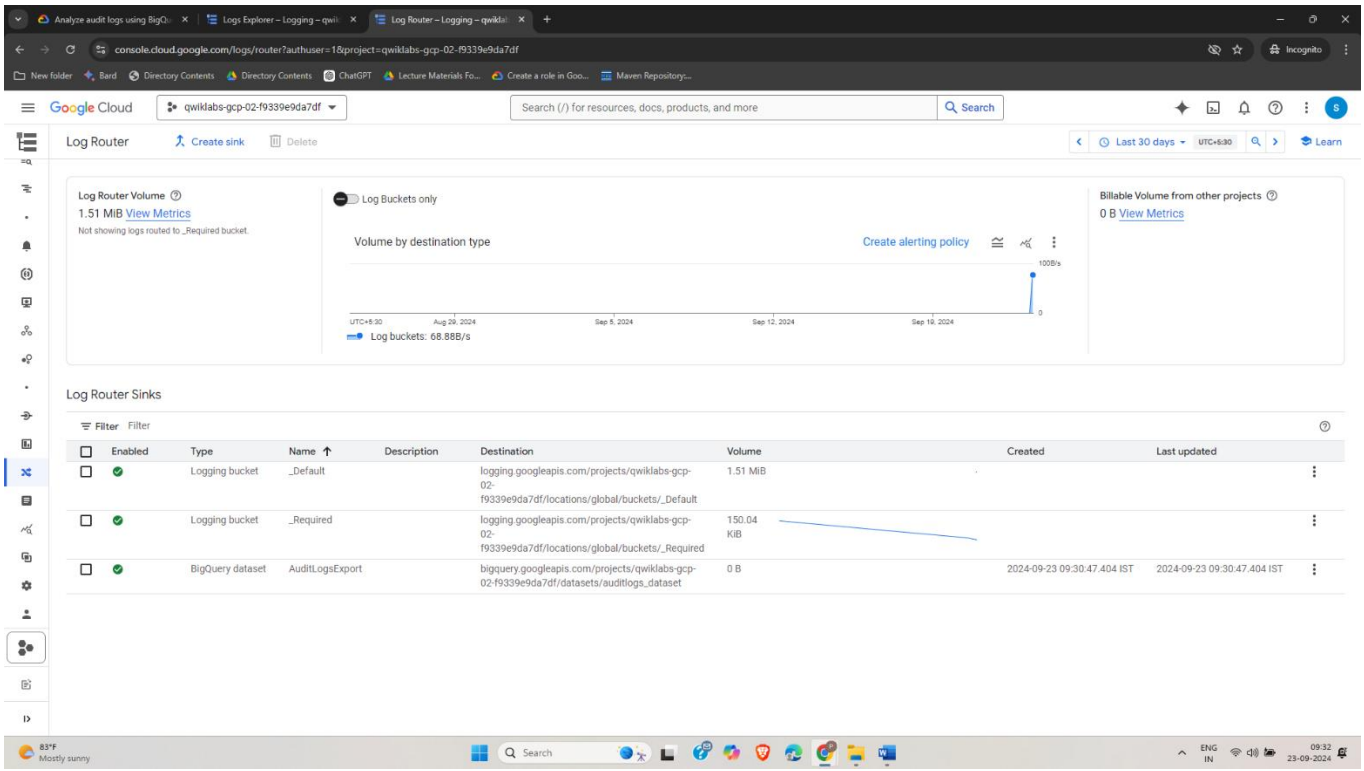


Figure 14 : Navigating to the Log Routing page for viewing sinks.

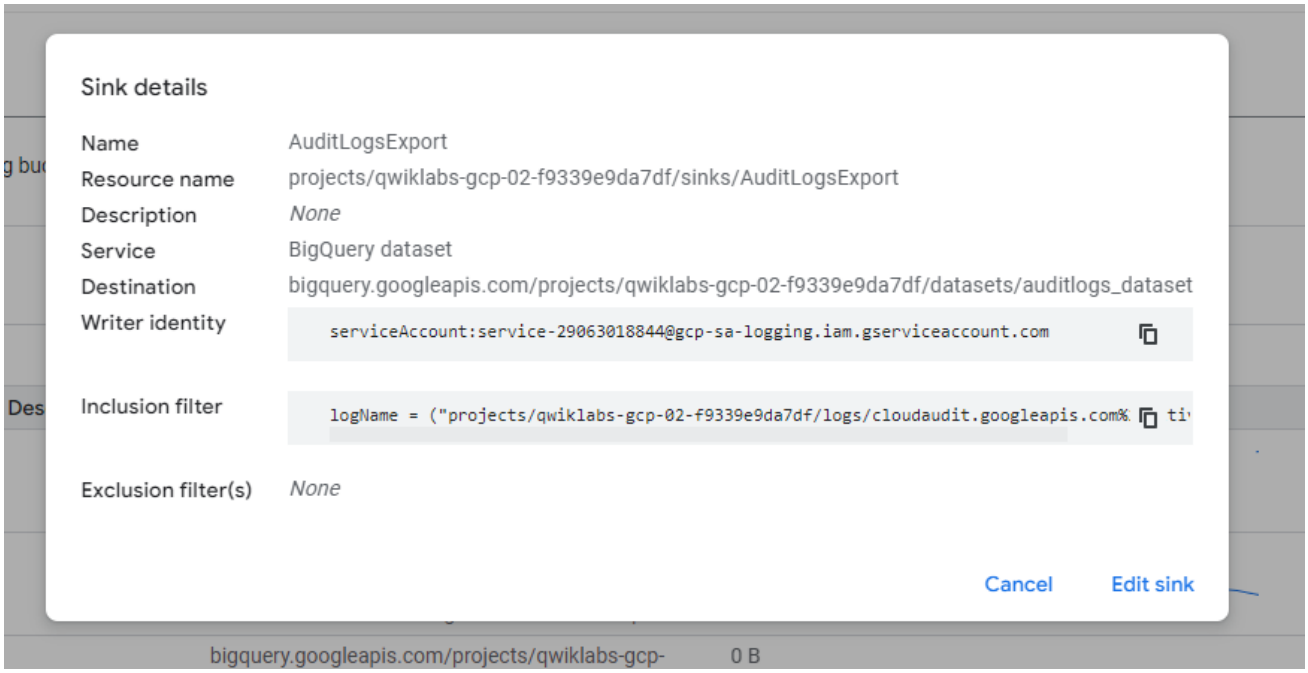


Figure 15 : Viewing the created sink in Log Routing.

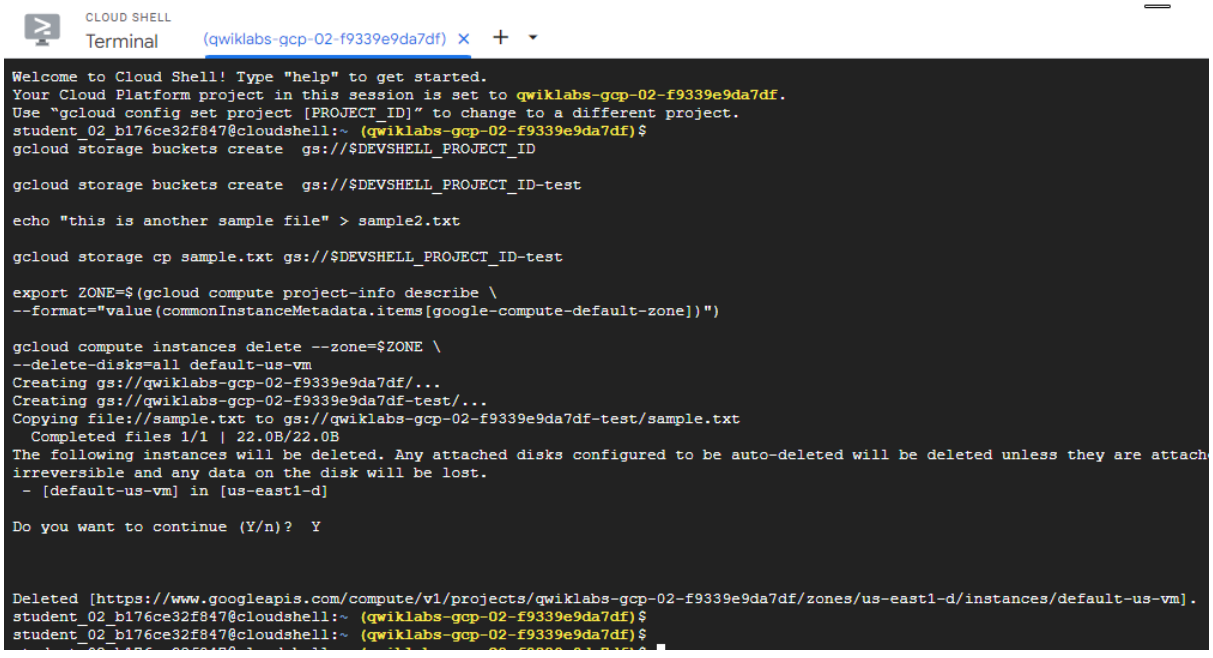


Figure 16 : Creating and deleting a simple storage bucket.

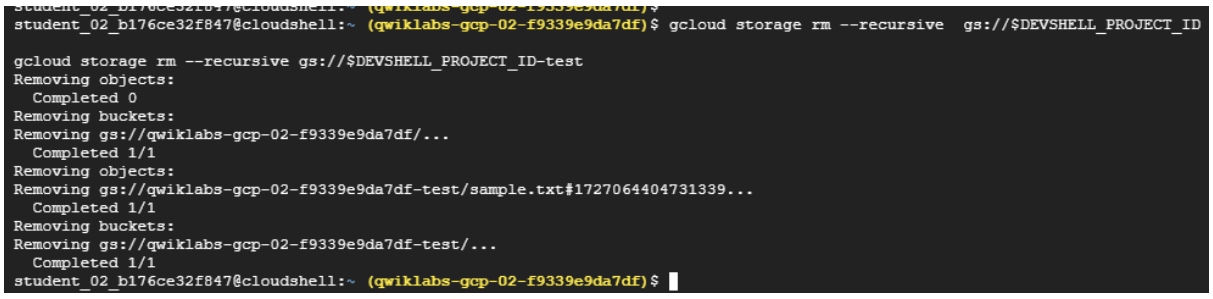


Figure 17 : Completely removing the storage bucket from the cloud project.

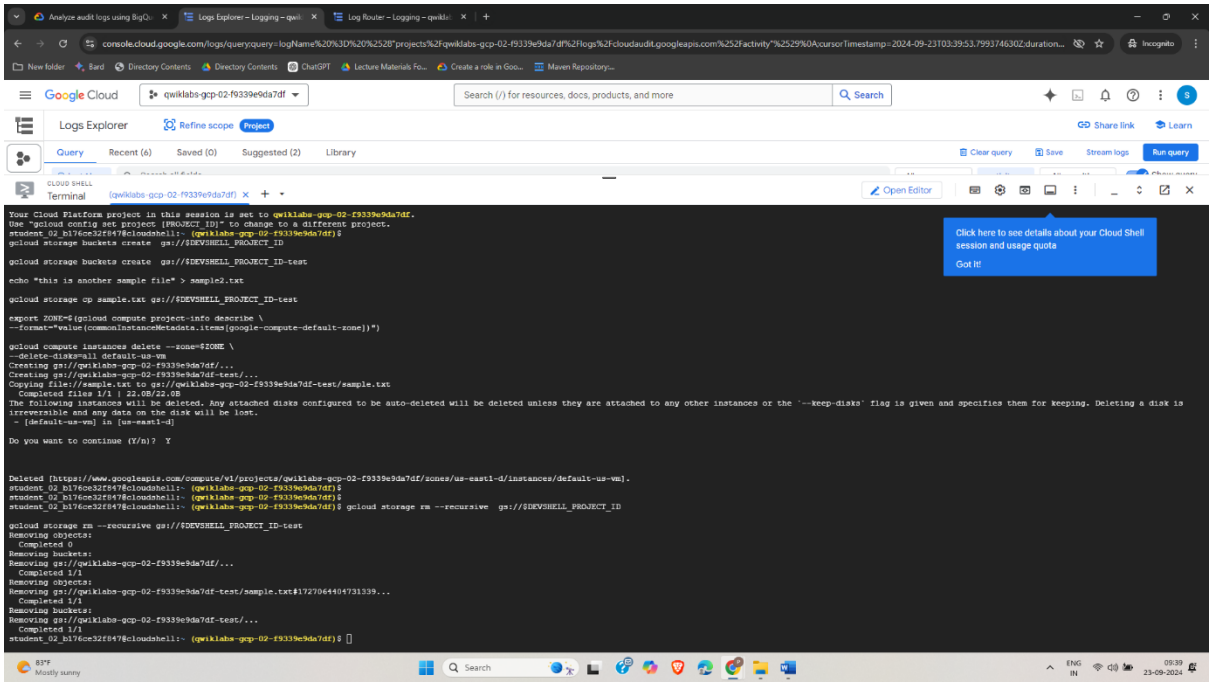


Figure 18 : Logging out of the Username 1 account.

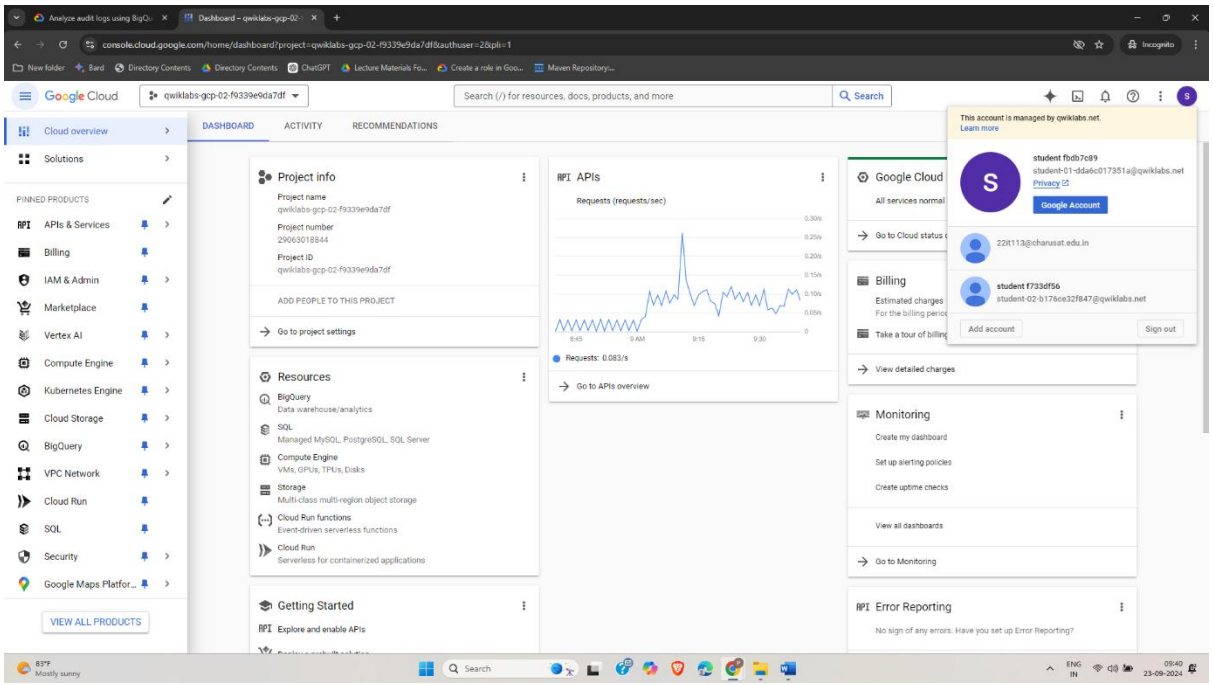


Figure 19 : Logging in with credentials for Username 2.

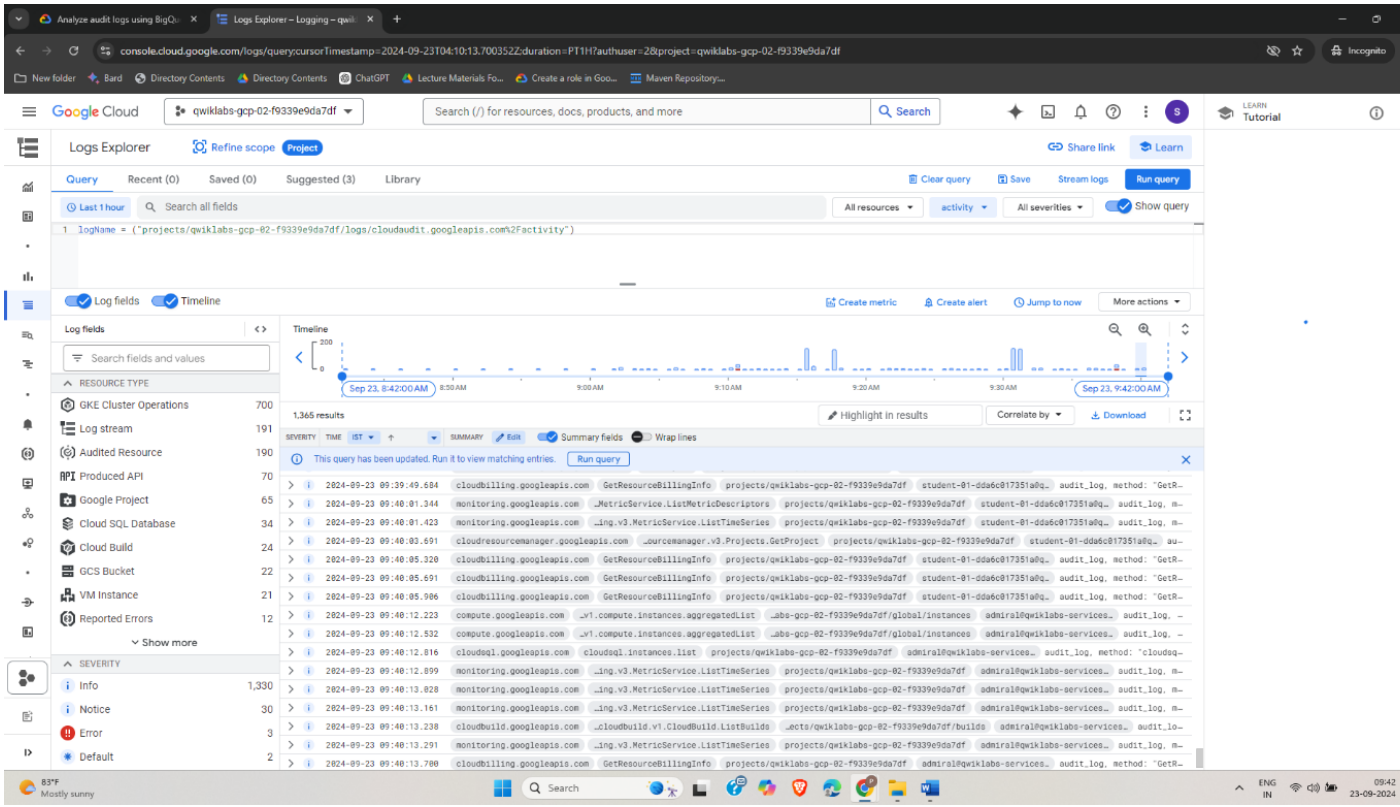


Figure 20 : Finding the log entry for storage.bucket.delete in the log list.

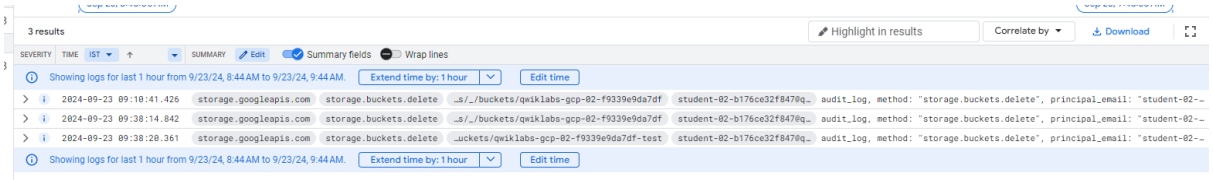


Figure 21 : Running a query to find similar logs for better analysis.

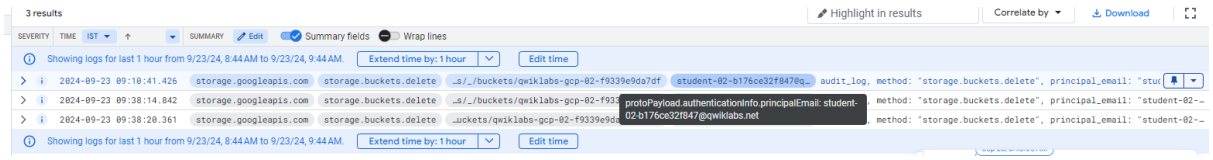


Figure 22 : Viewing the principal email for an action directly from the log entry.

```
logName = ("projects/qwiklabs-gcp-02-f9339e9da7df/logs/cloudaudit.googleapis.com%2Factivity")
protoPayload.methodName="storage.buckets.delete"
protoPayload.serviceName="storage.googleapis.com"
```

Figure 23 : Automatically adding the query in the Query Editor.

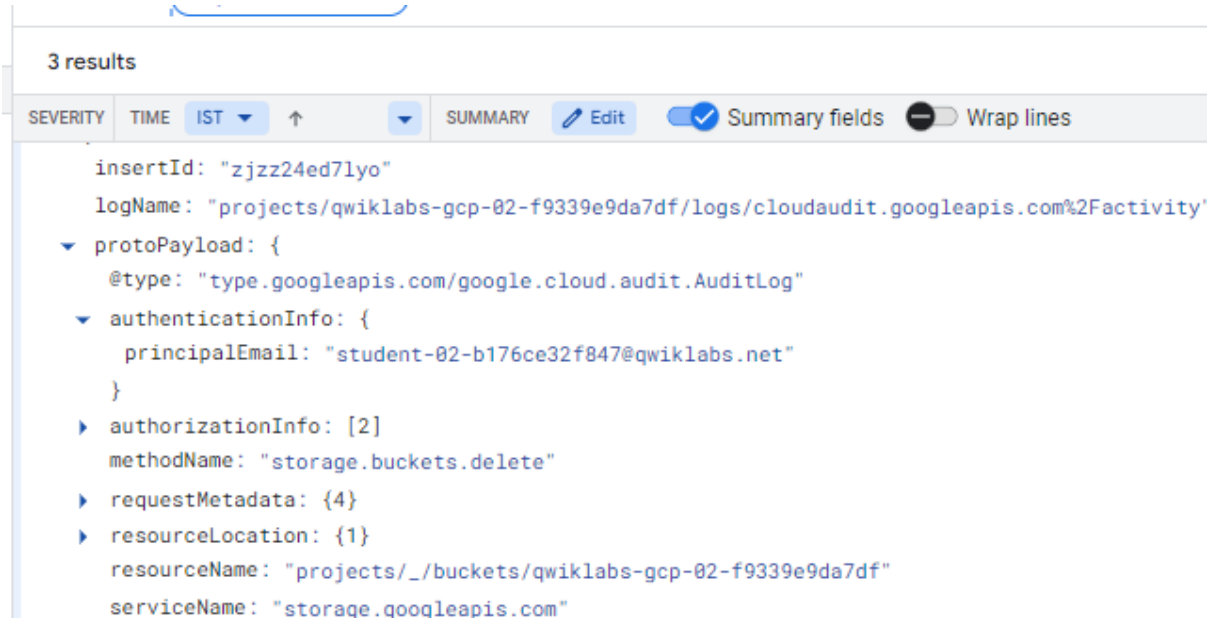


Figure 24 : Opening the authenticationInfo section of the log, which contains the principalEmail.

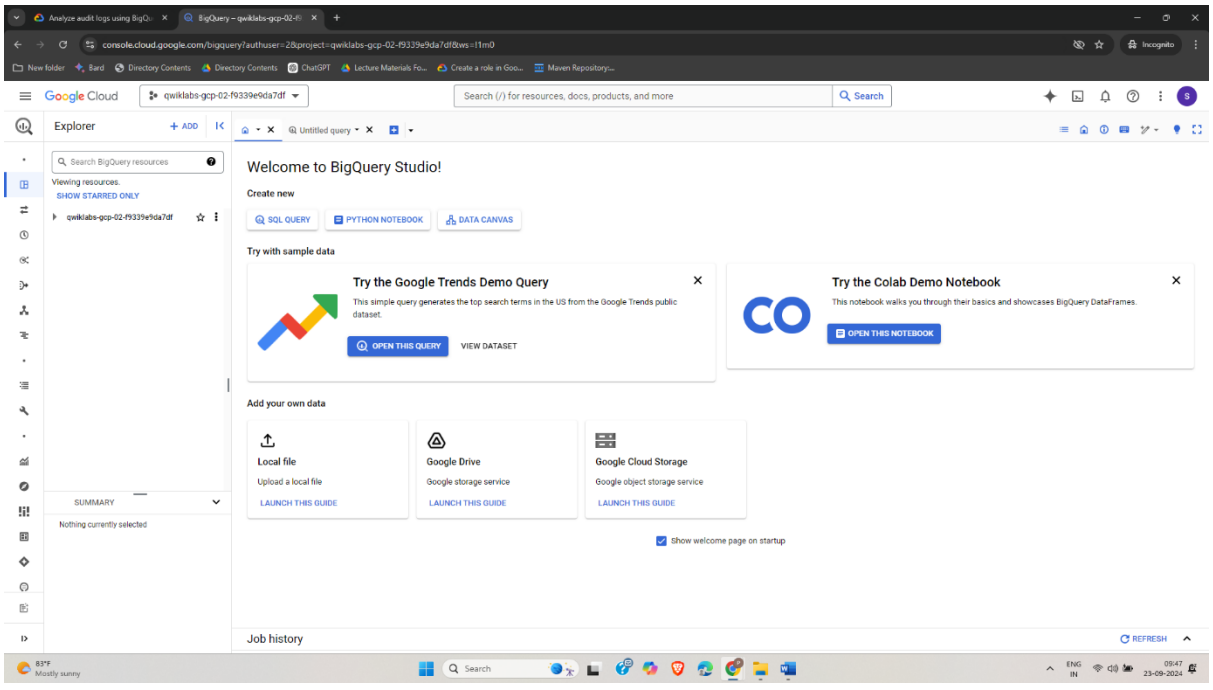


Figure 25 : Navigating to BigQuery Studio.

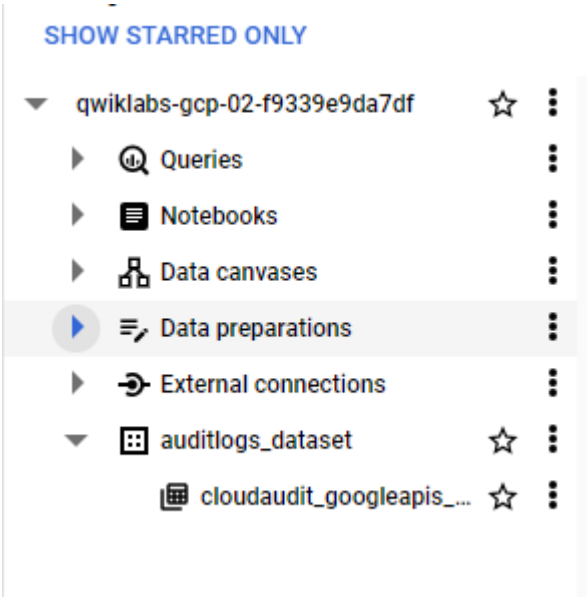


Figure 26 : Opening the side dialog box to display the project ID.

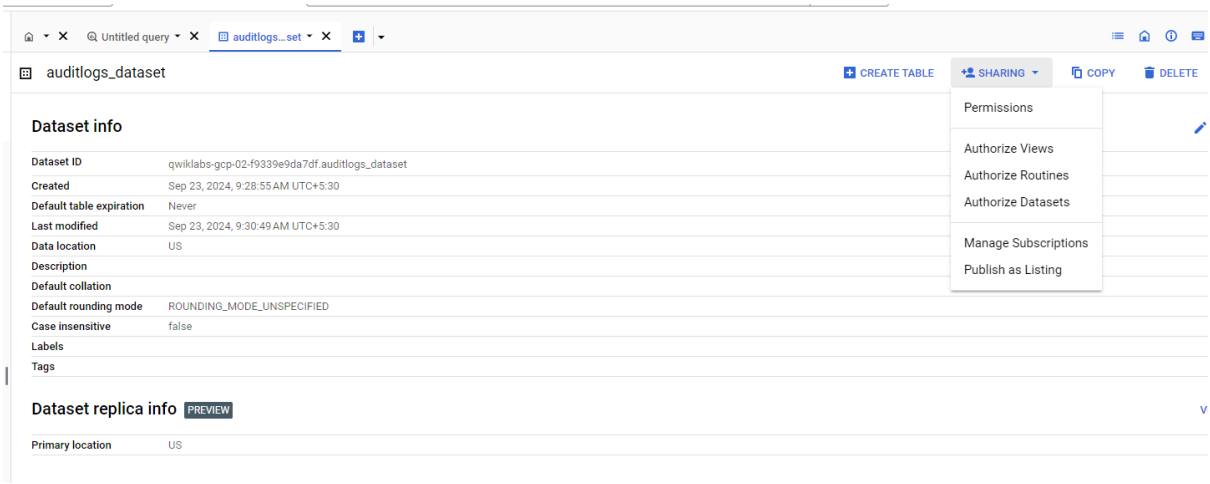


Figure 27 : Accessing the auditlog_dataset and reviewing sharing permissions.

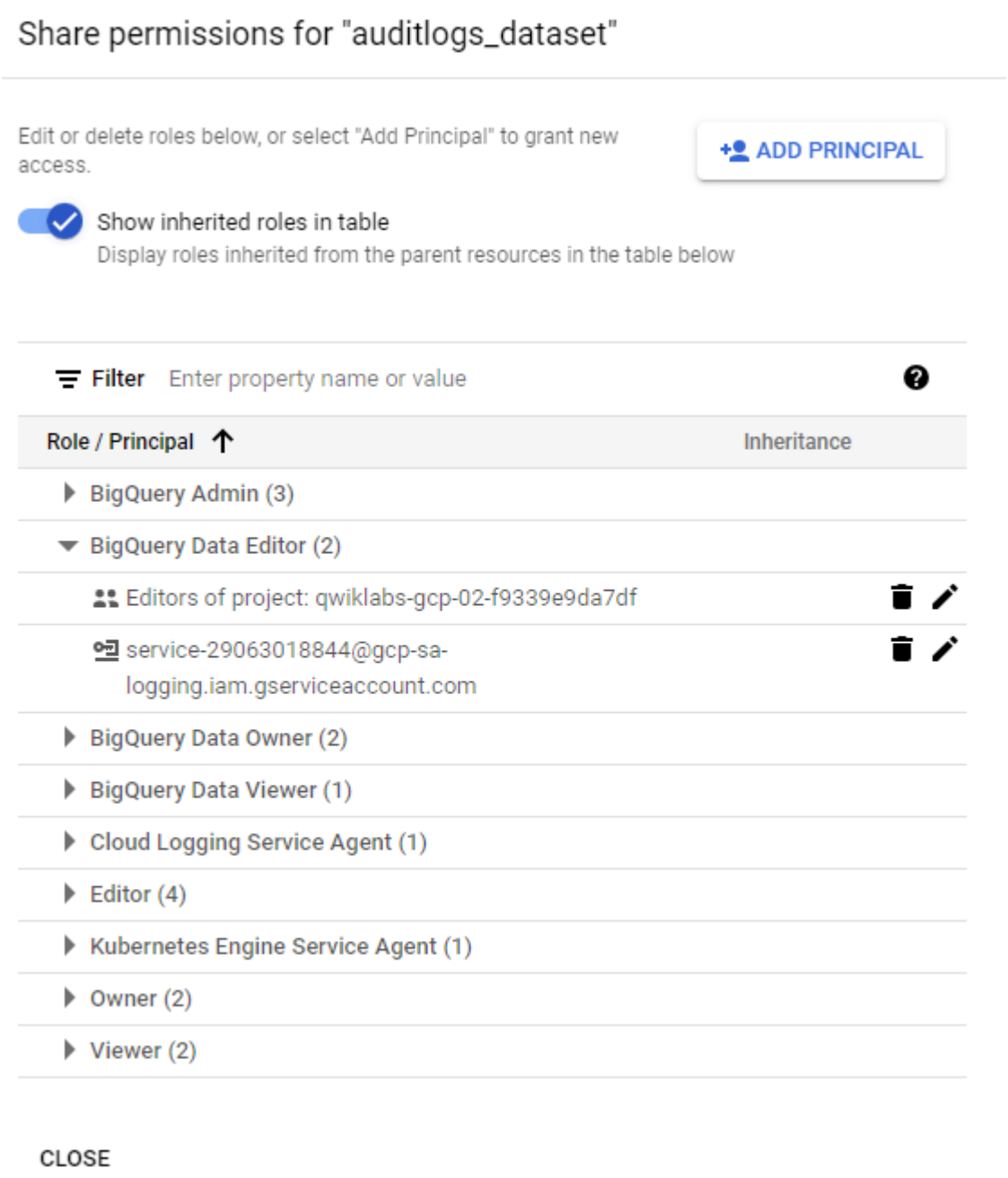


Figure 28 : Observing the tables associated with audit logs.

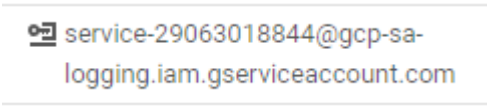


Figure 29 : Reviewing the sharing settings and log services.

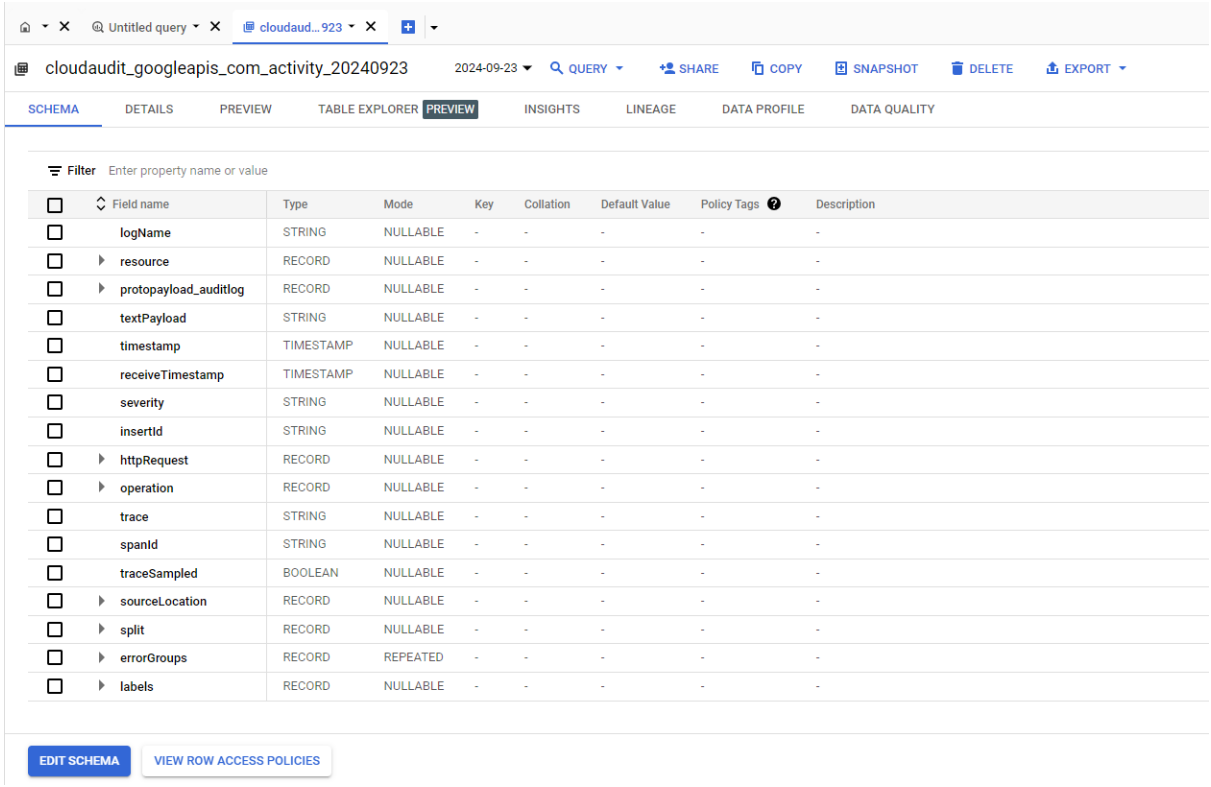


Figure 30 : Viewing the cloudaudit_googleapis_com_activity_20240923 service.

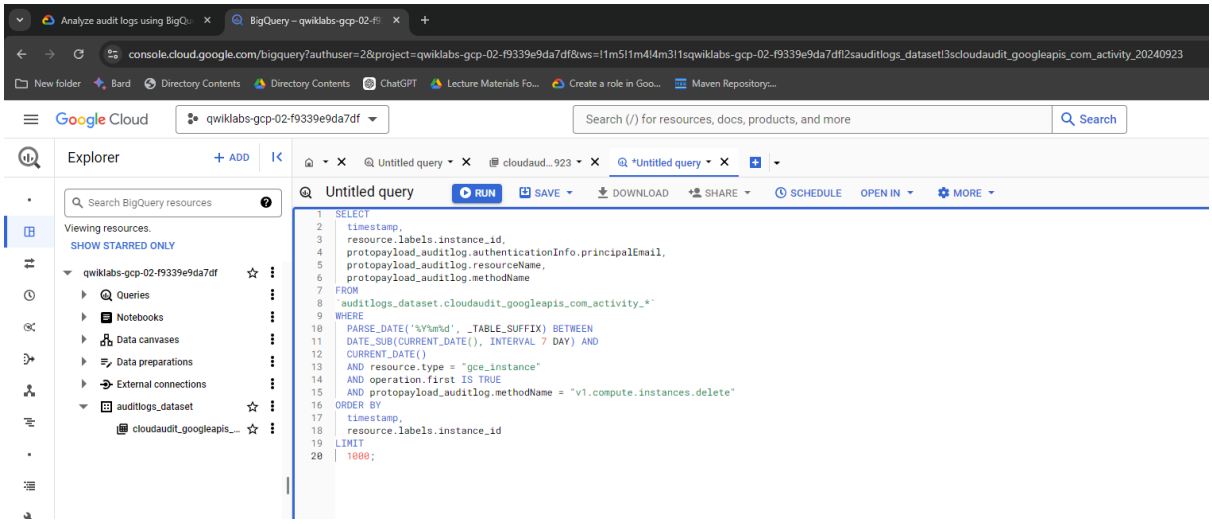


Figure 31 : Running a query to find activities related to instance creation and deletion by User 1.

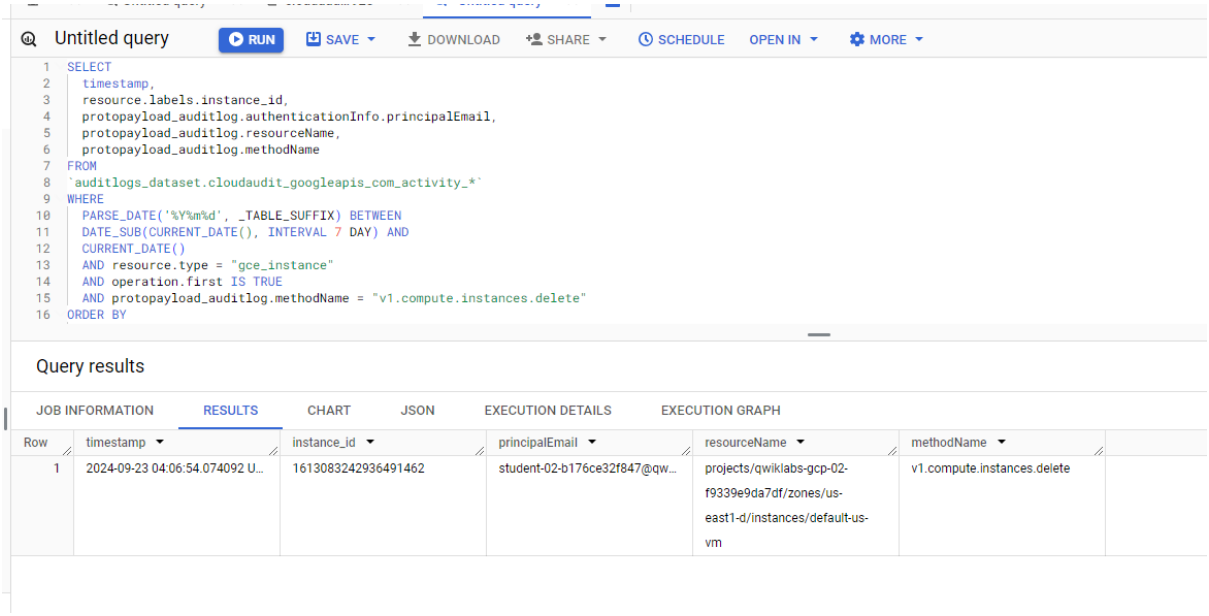


Figure 32 : Displaying the result of the first query related to instance activity by User 1.

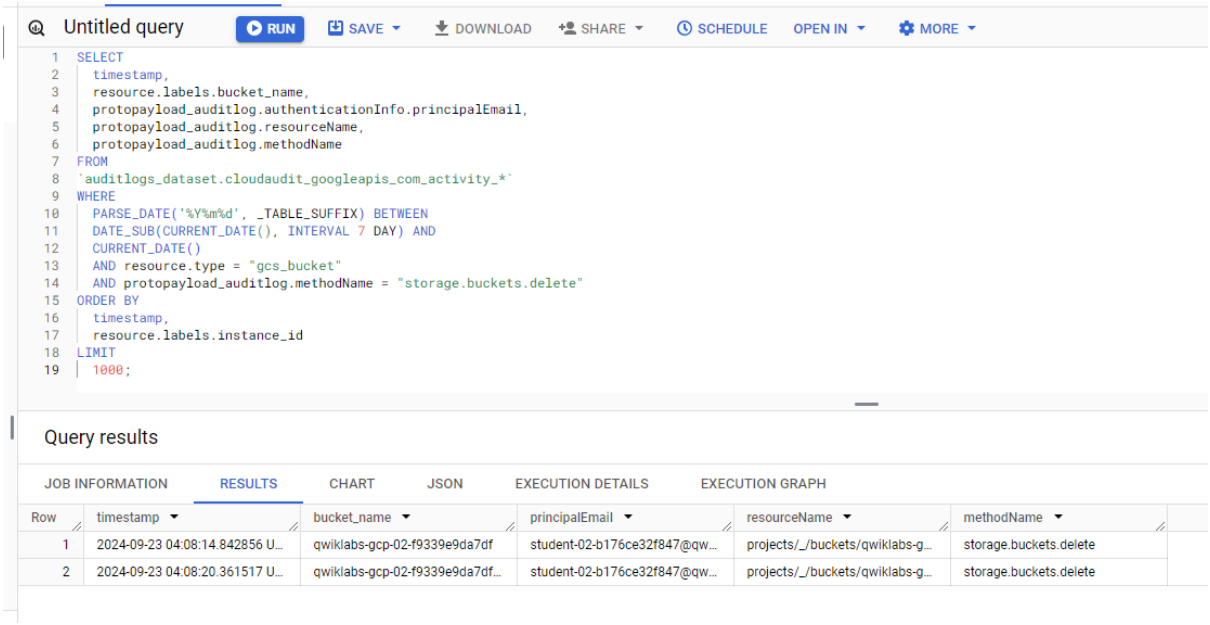


Figure 33 : Running a second query to find bucket-related activity (creation/deletion) by User 1 and displaying the results.

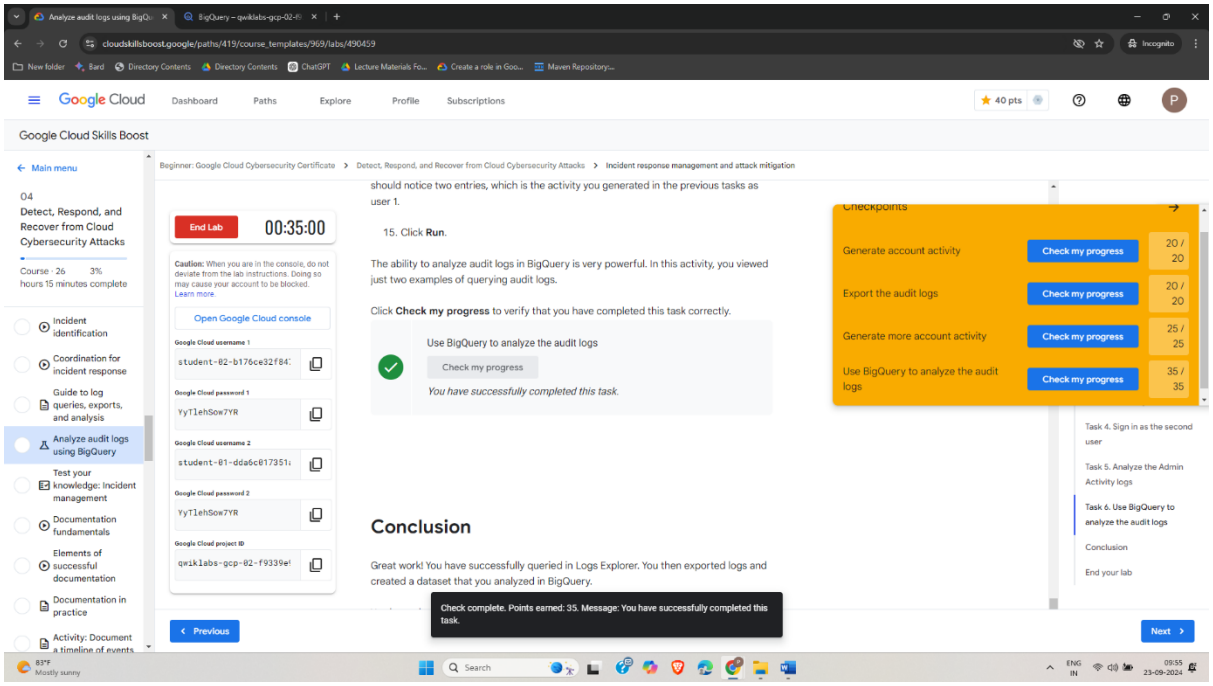


Figure 34 : Successfully completing the lab session.

LATEST APPLICATIONS:

Recent updates to Google Cloud's logging services make it easier to manage audit logs by exporting logs to external services such as BigQuery and Cloud Storage. These applications allow organizations to analyze logs more effectively, set up real-time alerts for suspicious activity, and store logs for long-term retention and compliance purposes.

LEARNING OUTCOME:

Through this lab, I learned how to:

- Navigate and filter Google Cloud audit logs.
- Analyze administrative activities to monitor resource usage.
- Create BigQuery datasets and log sinks to export and store audit logs.
- Write and execute queries in the Google Cloud Logging Explorer to detect unusual or suspicious activities.
- Manage cloud resources by creating and deleting buckets and other resources.

REFERENCES:

 Google Cloud Documentation on Audit Logs: https://cloud.google.com/logging/docs/audit

 BigQuery Documentation for Querying Logs: https://cloud.google.com/bigquery

PRACTICAL: 11

AIM:

Business continuity and disaster recovery planning is critical for sustaining business operations while recovering from a significant security incident, natural disaster, or disruption. Google Cloud Backup and DR Service is a cloud-based backup and disaster recovery solution that enables the backup and recovery of data , to support quick resumption of critical business operations. After Backup and DR performs an initial full backup, your data (general applications, VMware VMs, Compute Engine VMs, databases, and file systems) is backed up incrementally, updating and storing any data that has changed since the last backup.The initial configuration of the Backup and DR service includes the deployment of a management appliance that can take up to 45 minutes to complete. This task has been carried out for you prior to the lab startup. Once the Backup and DR Service are enabled, you can explore the Backup and DR management console and protect workloads.This lab guides you through the steps of discovering and protecting a Compute Engine instance, and finally mounting a fully-functional new Compute Engine instance from the backup image to a new location.

THEORY:

In this practical, we explore the Google Cloud Backup and DR service, focusing on its core functionalities:

- **Backup Management**: Google Cloud Backup and DR supports various workloads including VMs (Compute Engine, VMware), databases, and file systems. Backups are incremental after an initial full backup, ensuring that only changes are backed up.
- **Management Appliance**: Before using the Backup and DR service, a management appliance is deployed, which acts as the interface to manage backups.
- **Backup Templates and Policies**: The service allows for creating custom backup templates and policies, which define the frequency, retention, and recovery options for different workloads.
- **Disaster Recovery**: Recovery is straightforward by restoring backups to new instances, allowing for seamless business continuity in case of an incident.

OUTPUT:

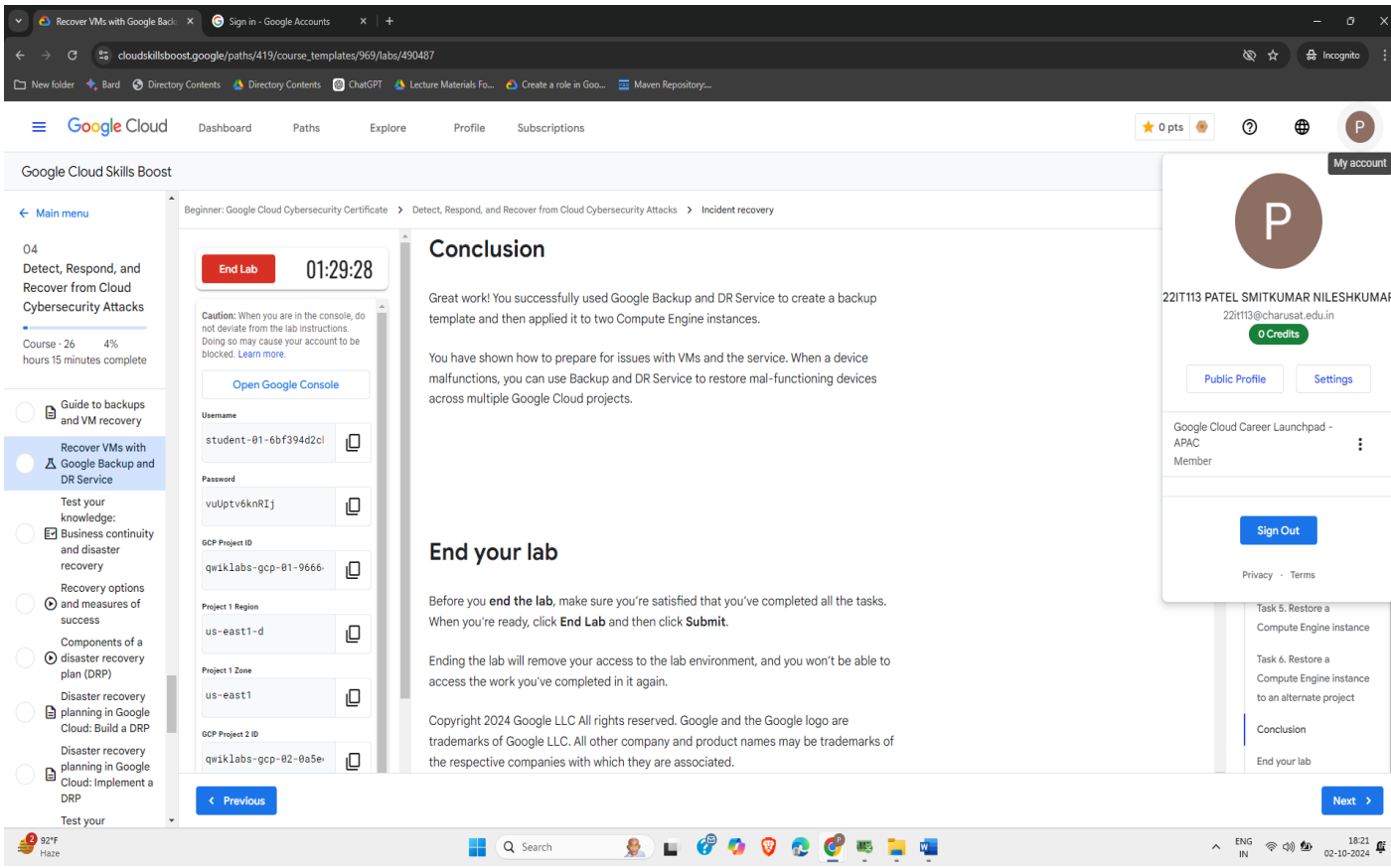


Figure 1 : Starting the lab . Shows the initial lab interface with environment setup completed.

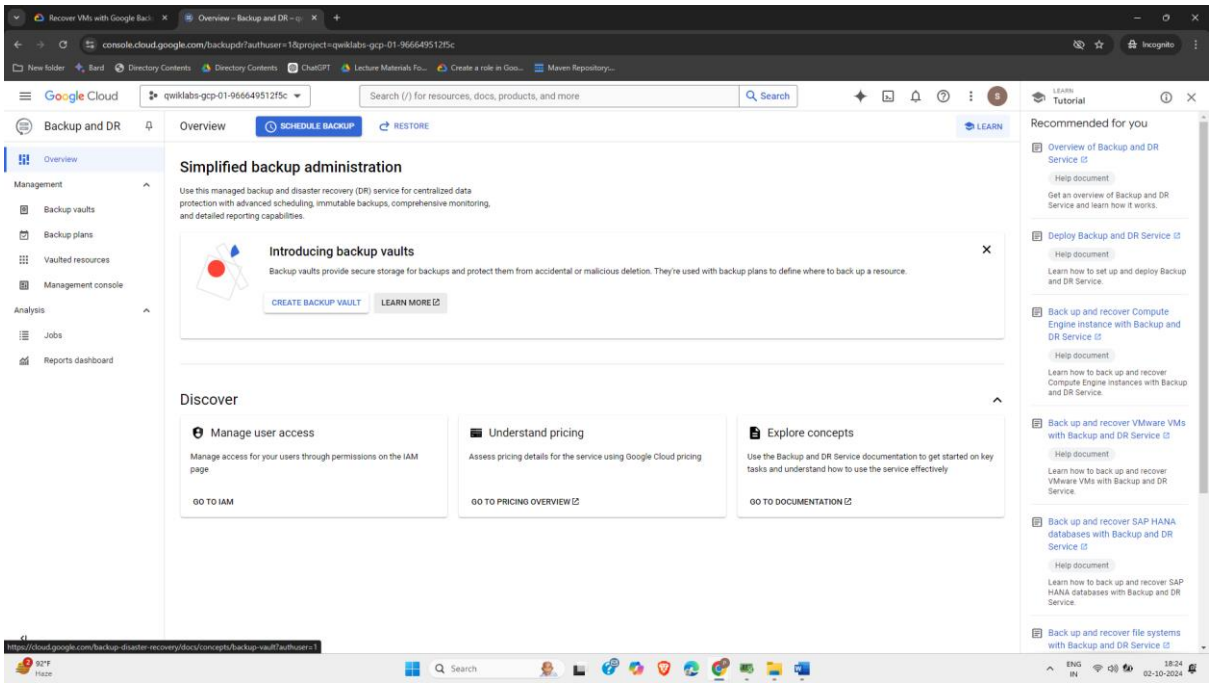


Figure 2 : Navigating to Backup and DR Navigating to the Backup and DR service console from the Google Cloud Console.

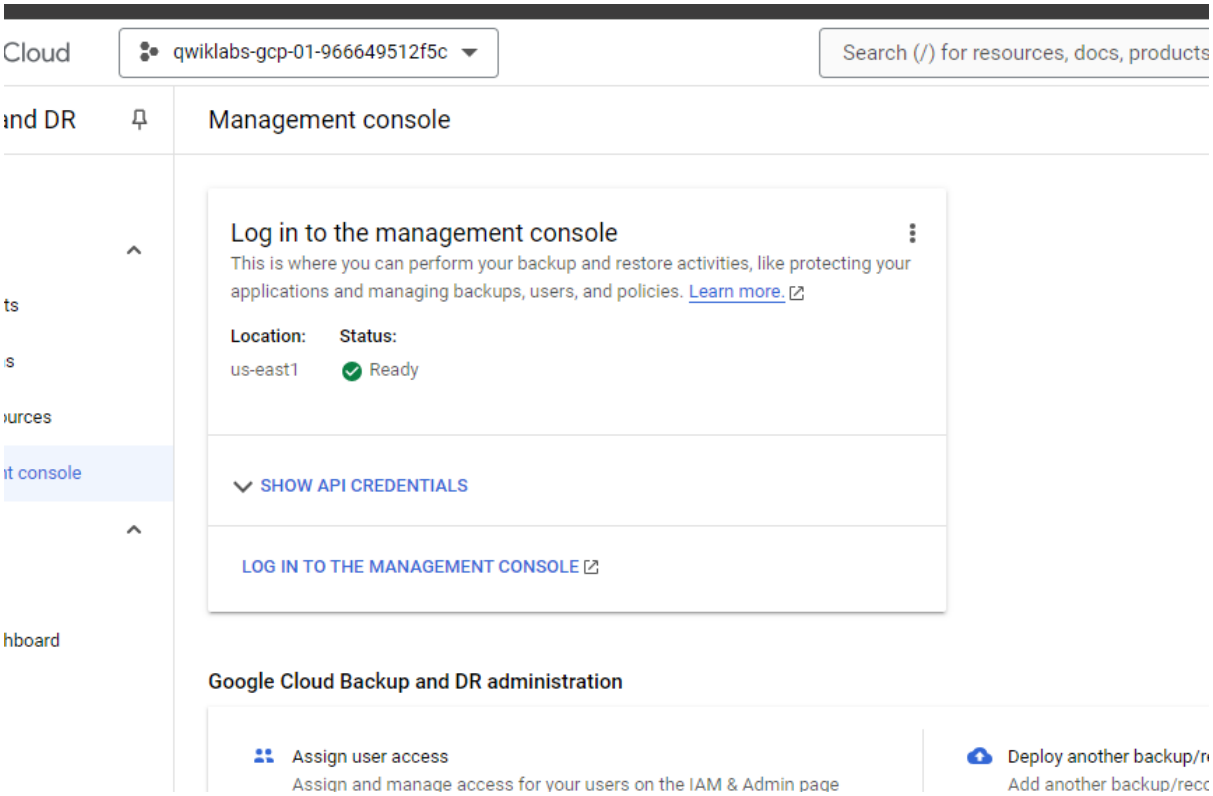


Figure 3 : Login to management console. Login to the Backup and DR management console to configure backup settings.

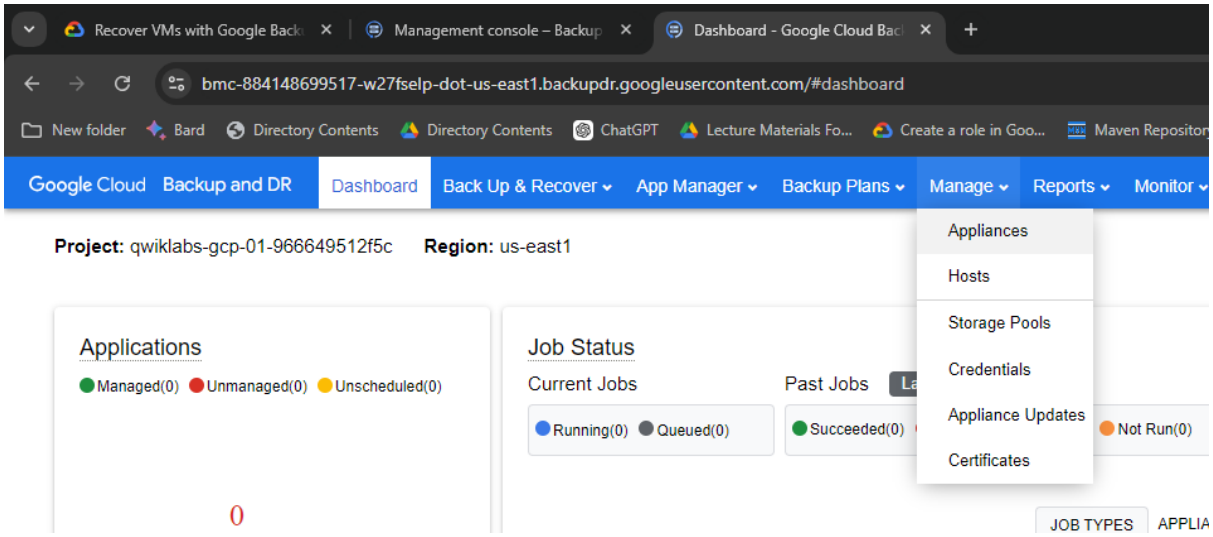


Figure 4 : Logging into the console using a student account and navigating to the appliance section Shows the process of accessing the appliance section for Backup and DR configuration.

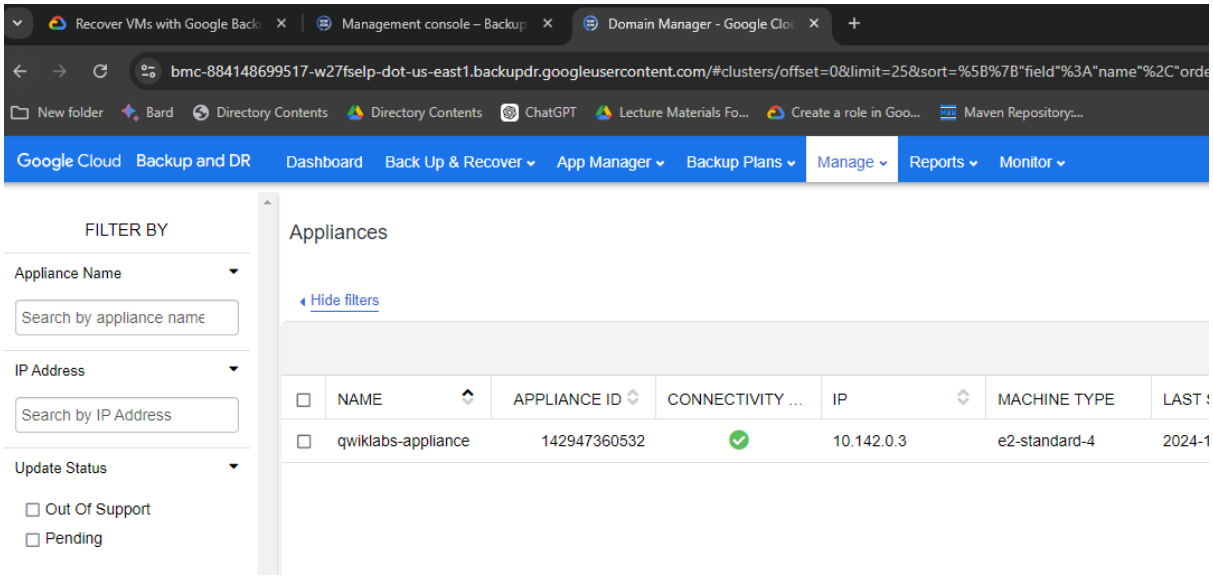


Figure 5 : Connectivity status with green checkIndicates successful installation of the management and backup servers.

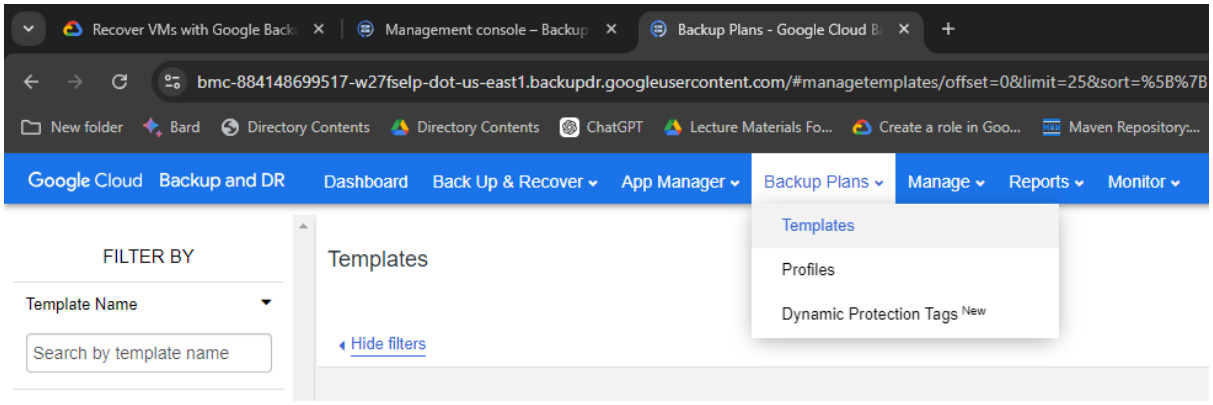


Figure 6 : Connectivity status with green check Indicates successful installation of the management and backup servers.

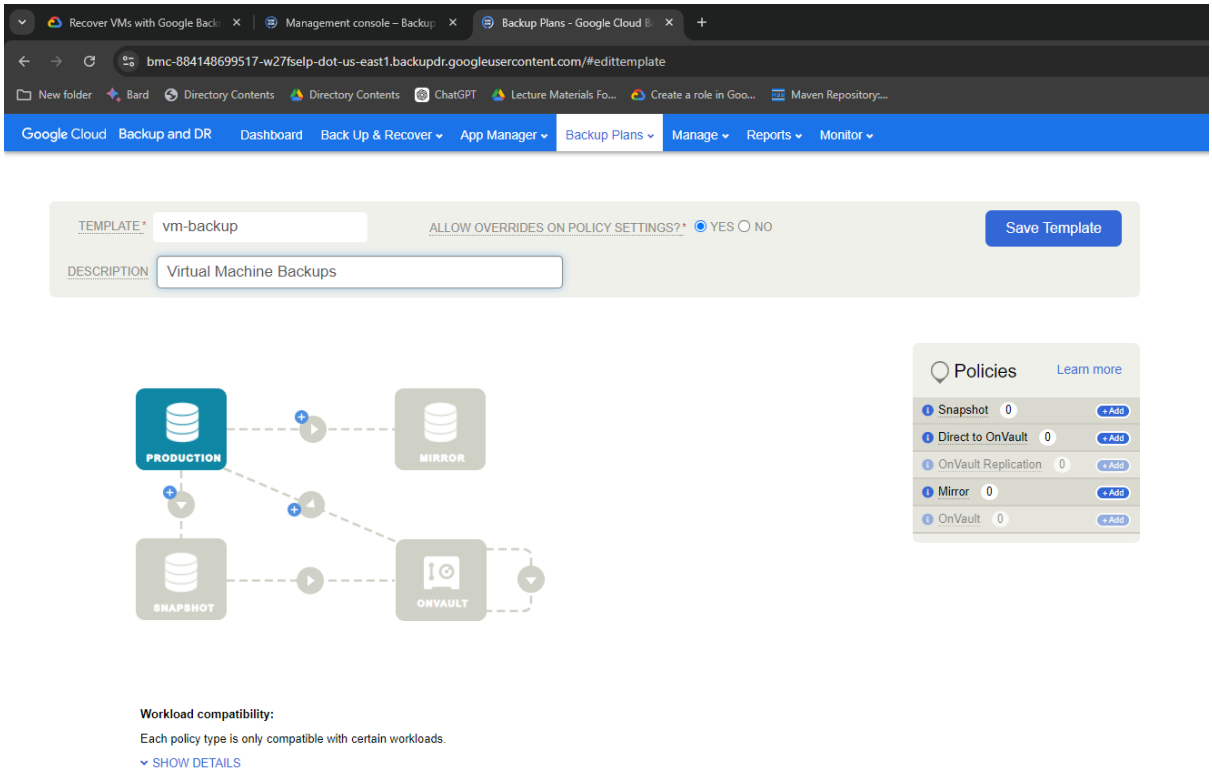


Figure 7 : Creating a backup template with name and description Demonstrates the process of creating a backup template with essential information.

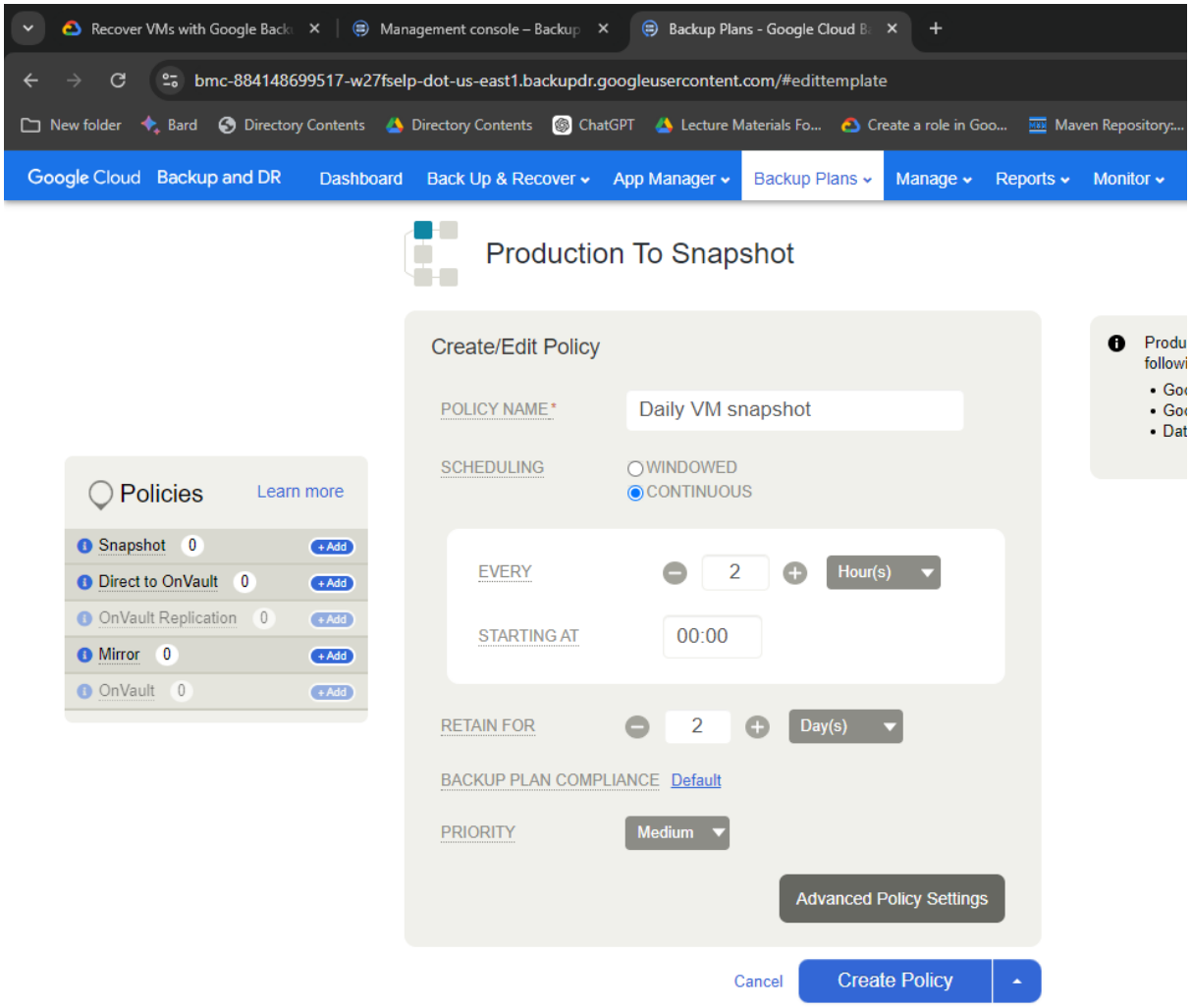


Figure 8 : Creating a policy for snapshots Setting up a policy to manage snapshot frequency and retention.

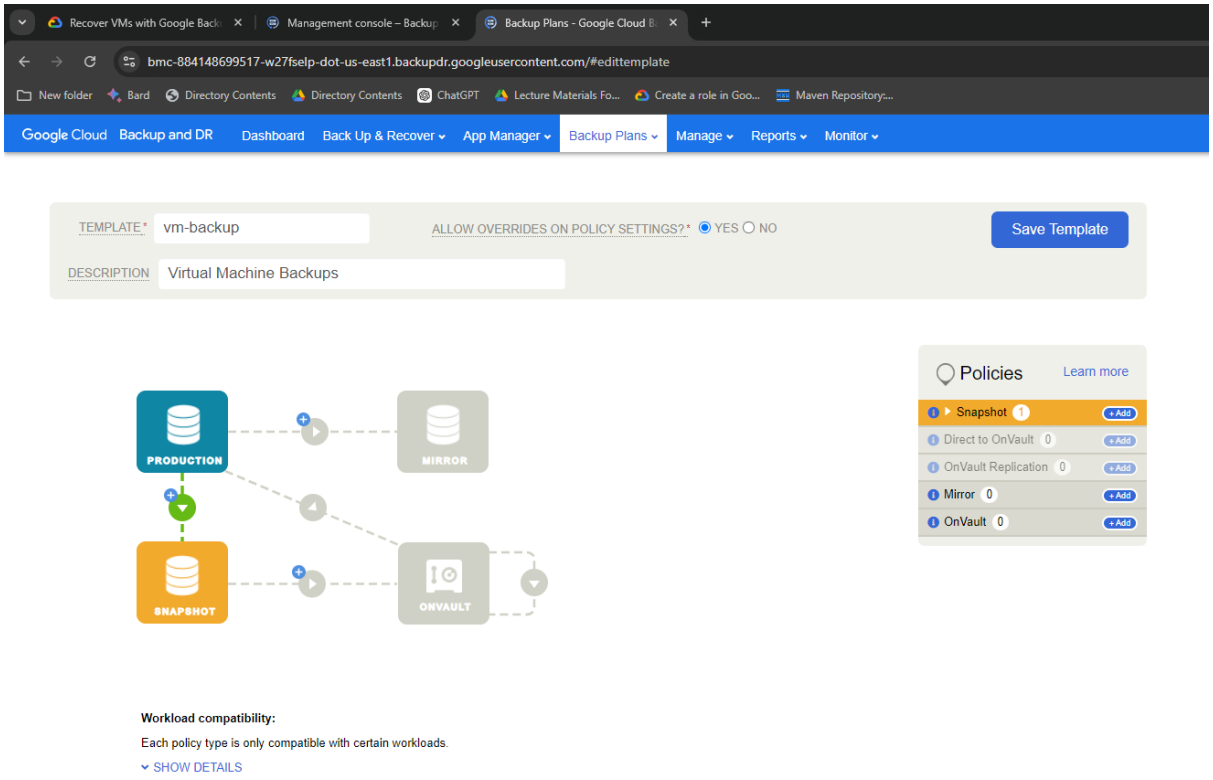


Figure 9 : Saving the template Confirmation of the backup template creation.

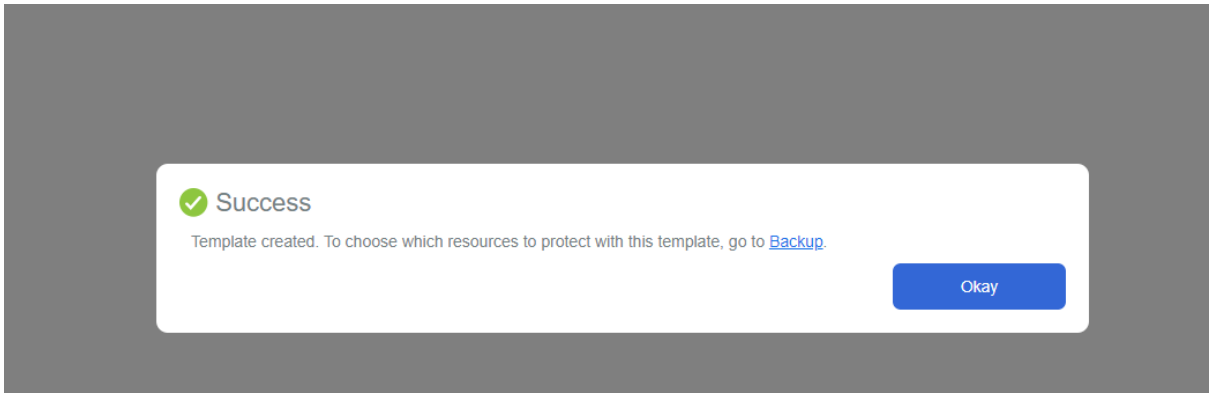


Figure 10 : Successful creation of the template Shows the final confirmation after the backup template has been created.

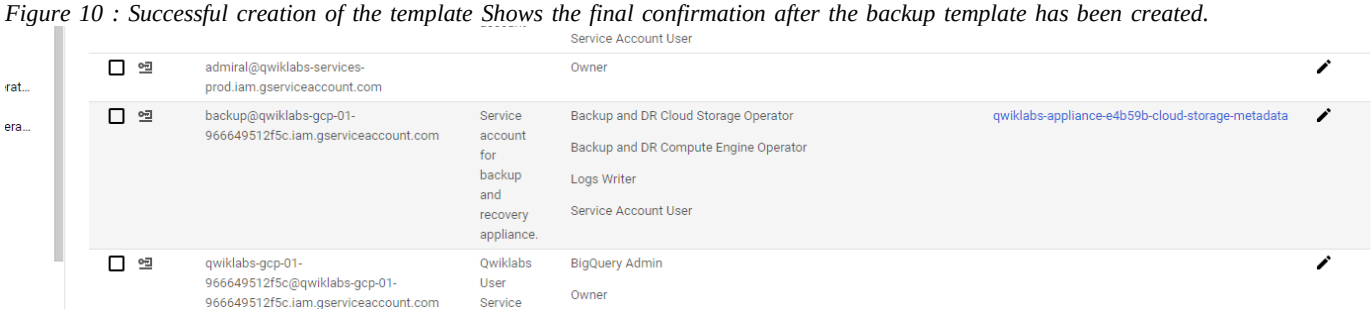


Figure 11 : Validating backup and recovery appliance service account permissions Ensures the service account has proper permissions to perform backups.

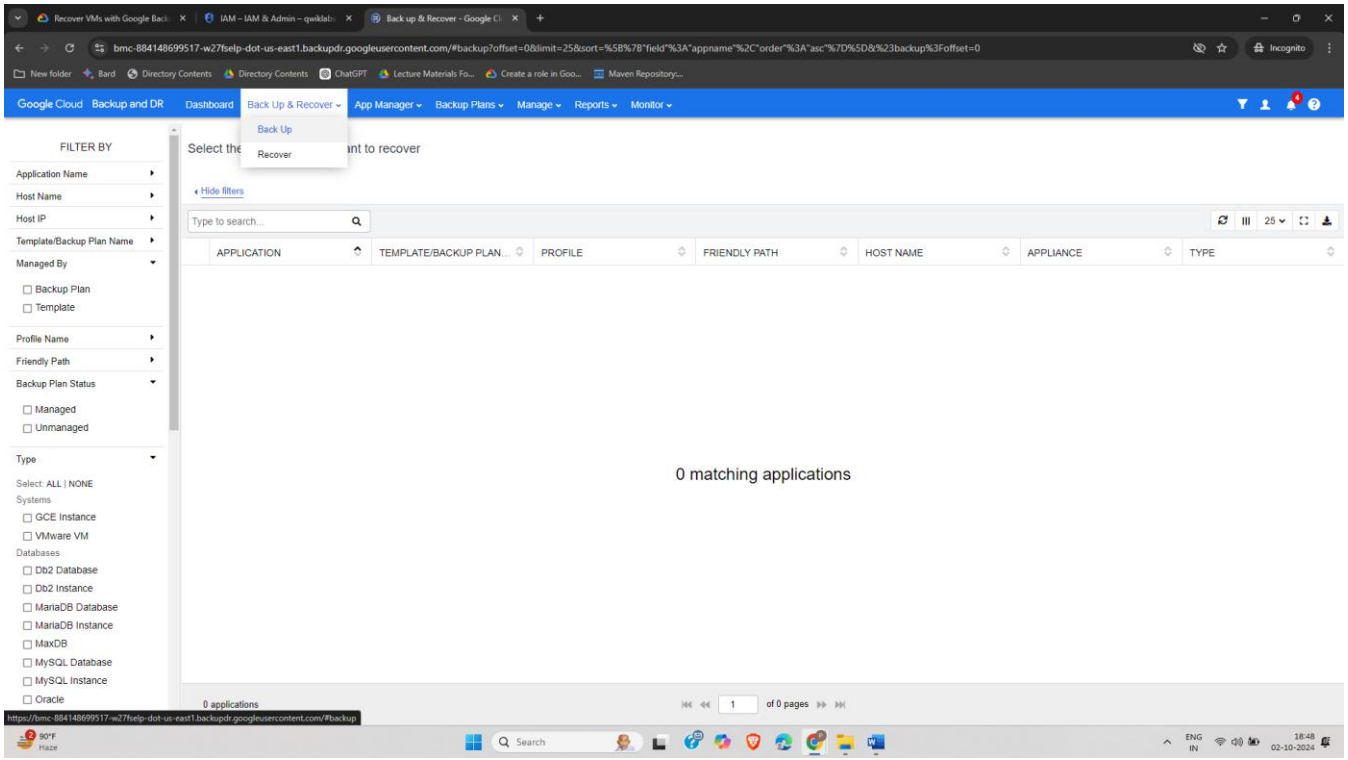


Figure 12 : Navigating to the backup section Accessing the backup configuration section.

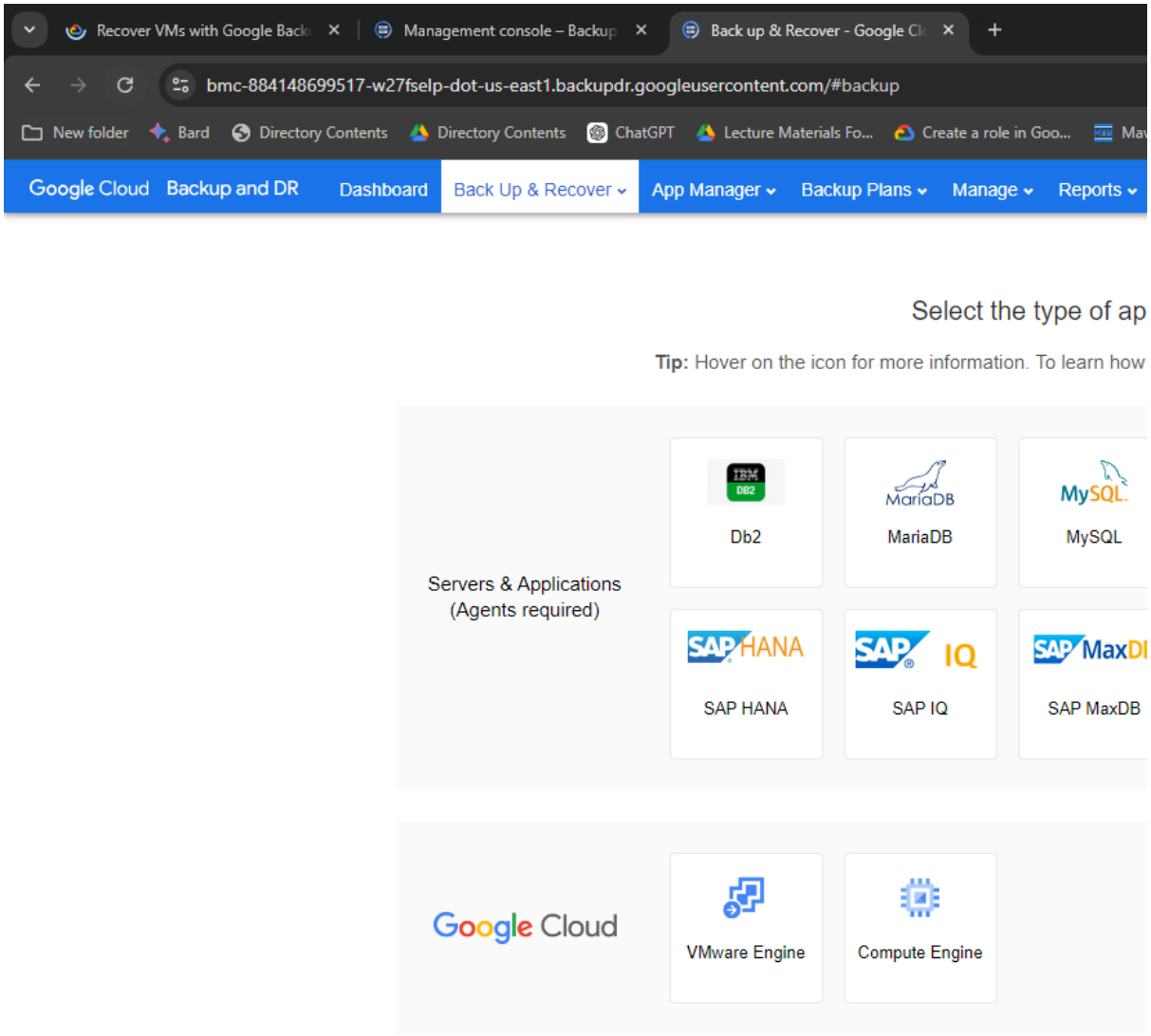


Figure 13 Navigating through backup options Exploring additional backup options available for workloads.

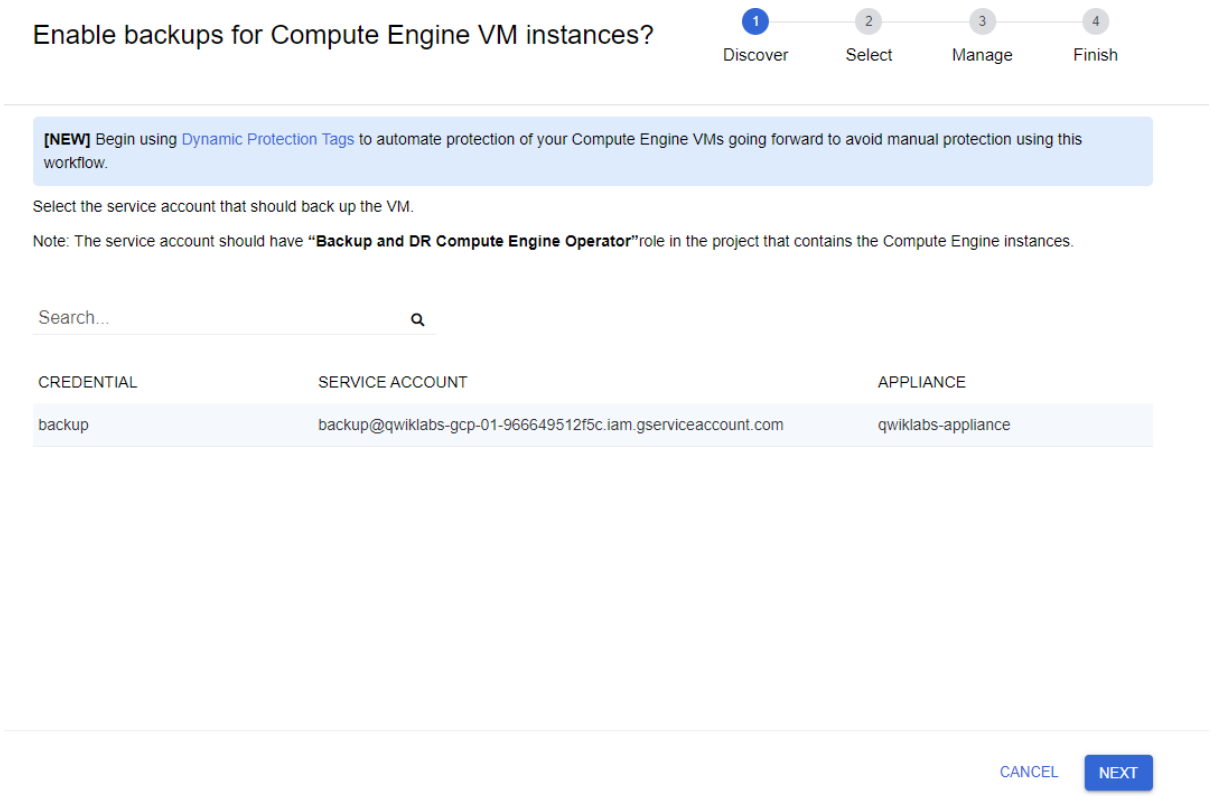


Figure 14 : Selecting a backup instance Shows the process of selecting a specific instance for backup.

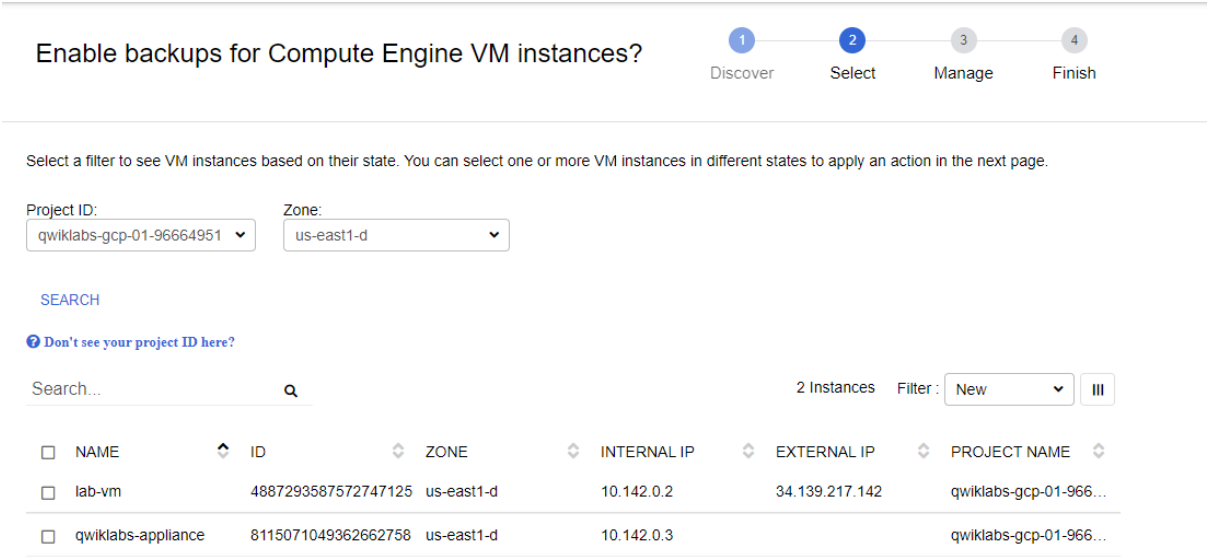


Figure 15 : Searching and finding two projects Demonstrating the ability to search across multiple projects for backups.

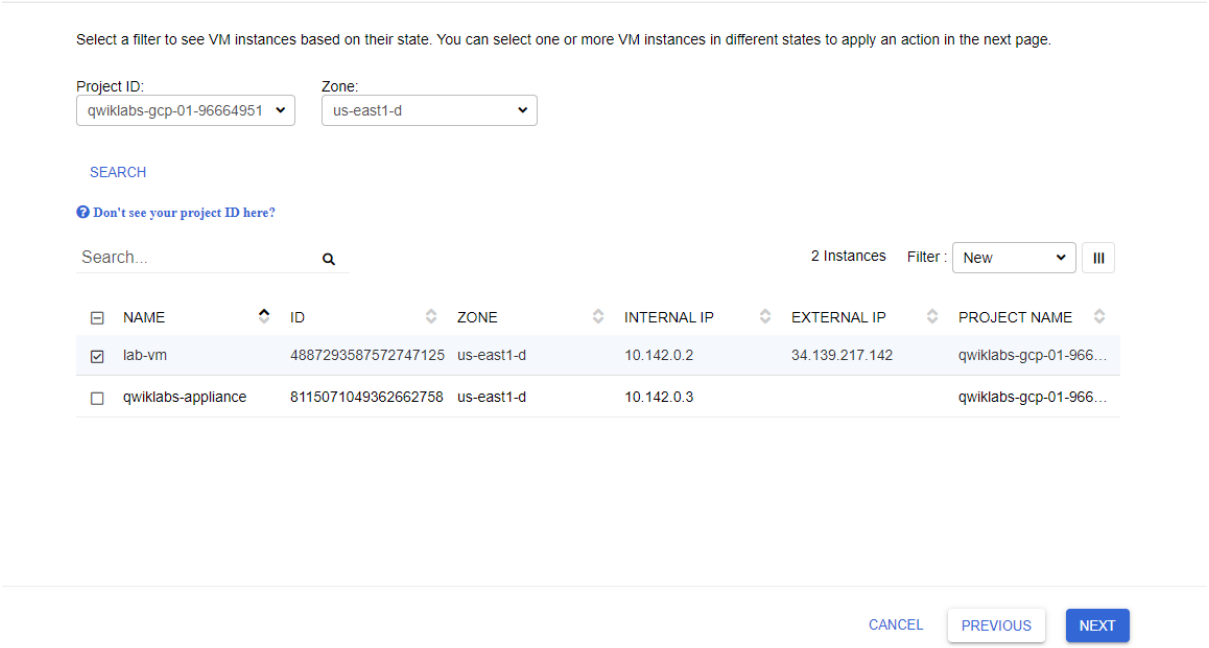


Figure 16 : Lab VM selection and clicking next Selecting the specific lab VM to backup and proceeding with the setup.

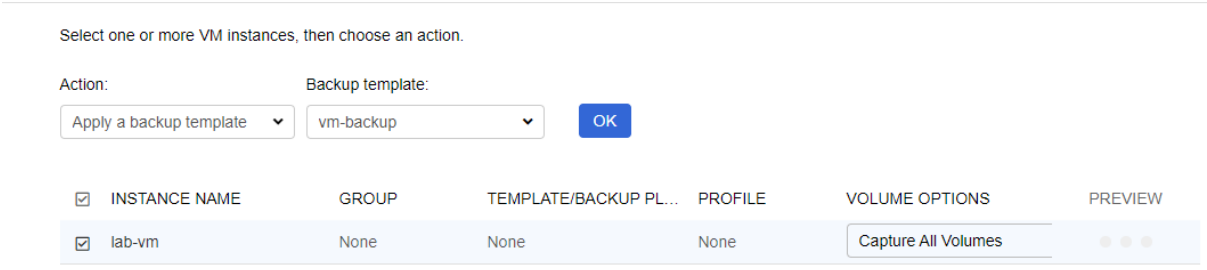


Figure 17 : Assigning the VM backup template to the project Shows the VM being assigned to the backup template created earlier.

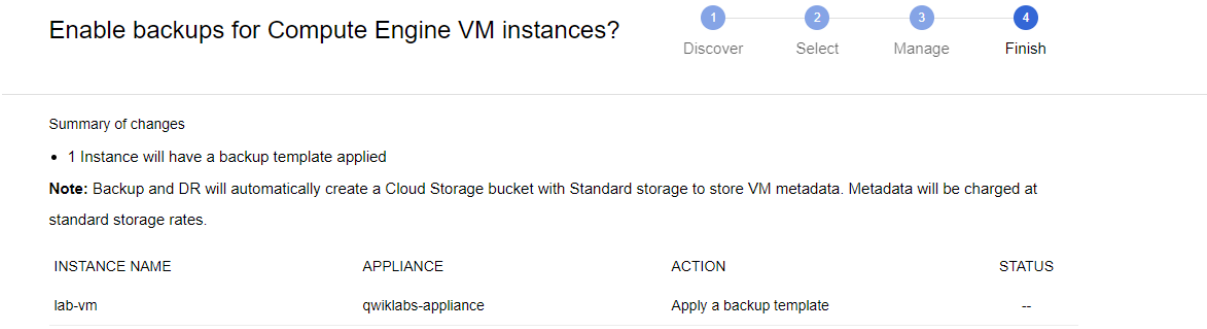


Figure 18 : Summary of backup assignment Displays the summary of the backup configuration before finalizing.

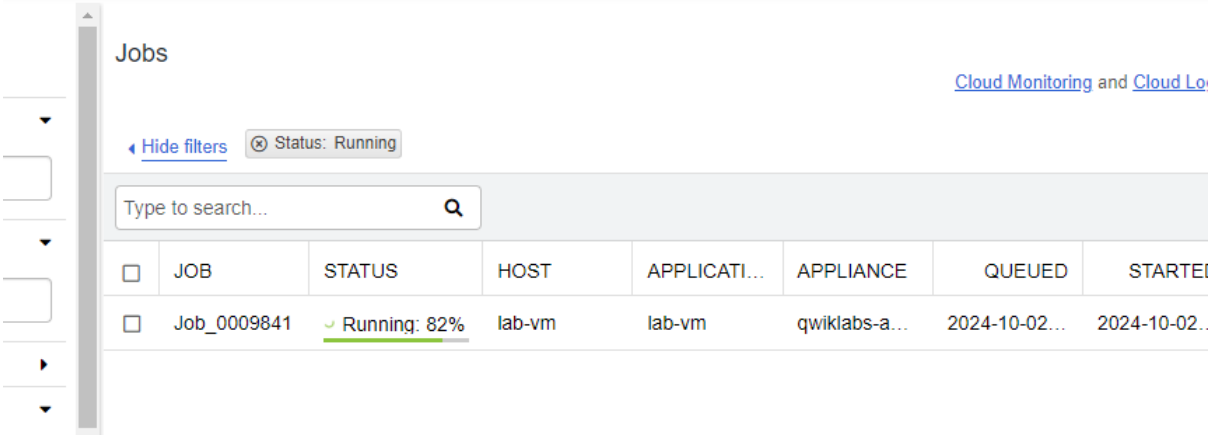


Figure 19 : Navigating to monitor jobs, finding the running job Accessing the monitoring section to track backup progress.

Figure 20 : Finding the job after it succeeded Shows the job completion status once the backup is successfully created.

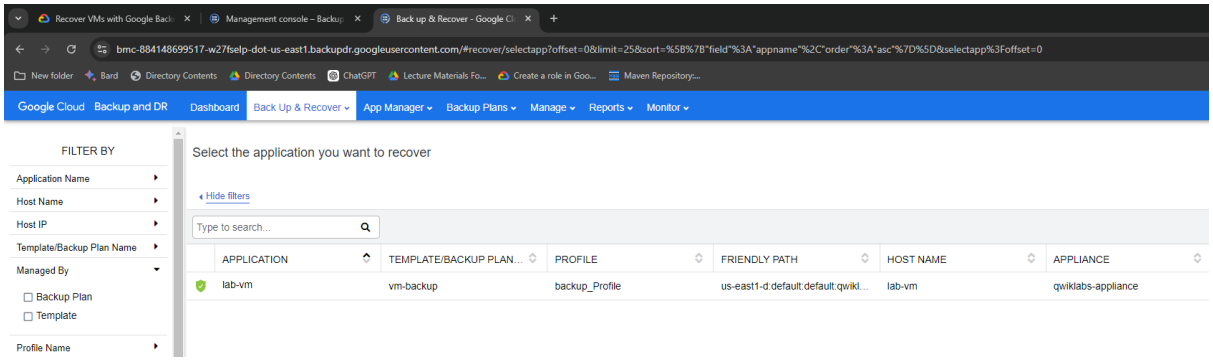


Figure 21 : Backup and recovery instance Verifying the existence of the backup instance in the system.

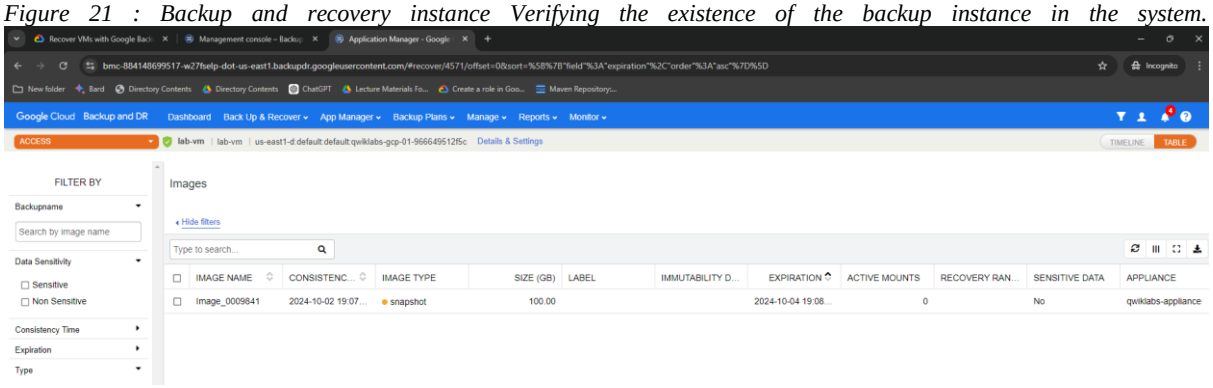


Figure 22 : Clicking on table to find the instance image Shows the table view with the backup image for recovery.

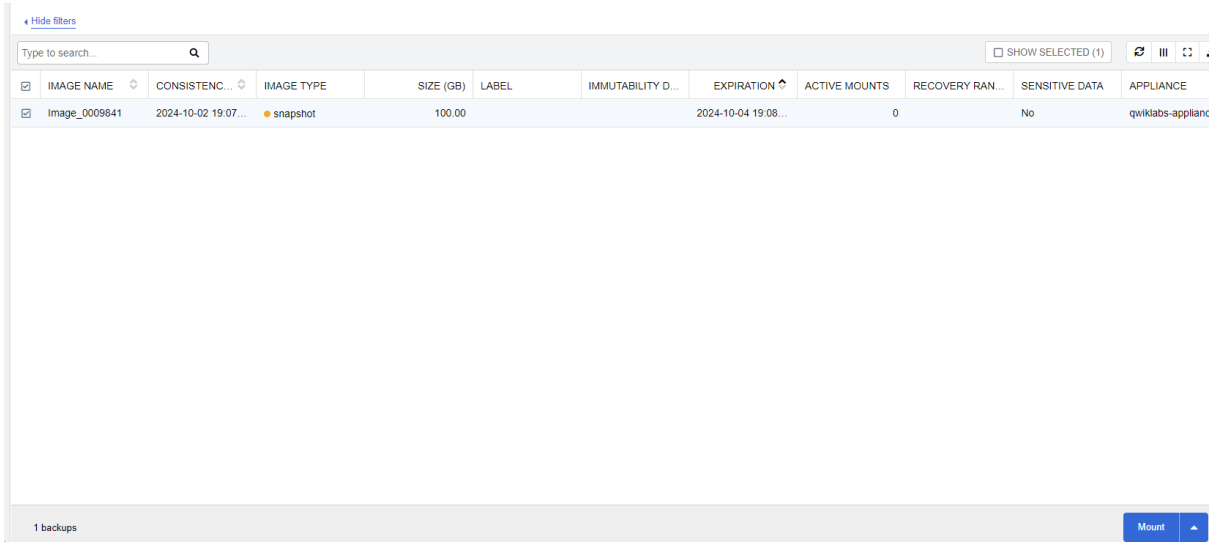


Figure 23 : Clicking on mount Mounting the backup image to create a new Compute Engine instance.

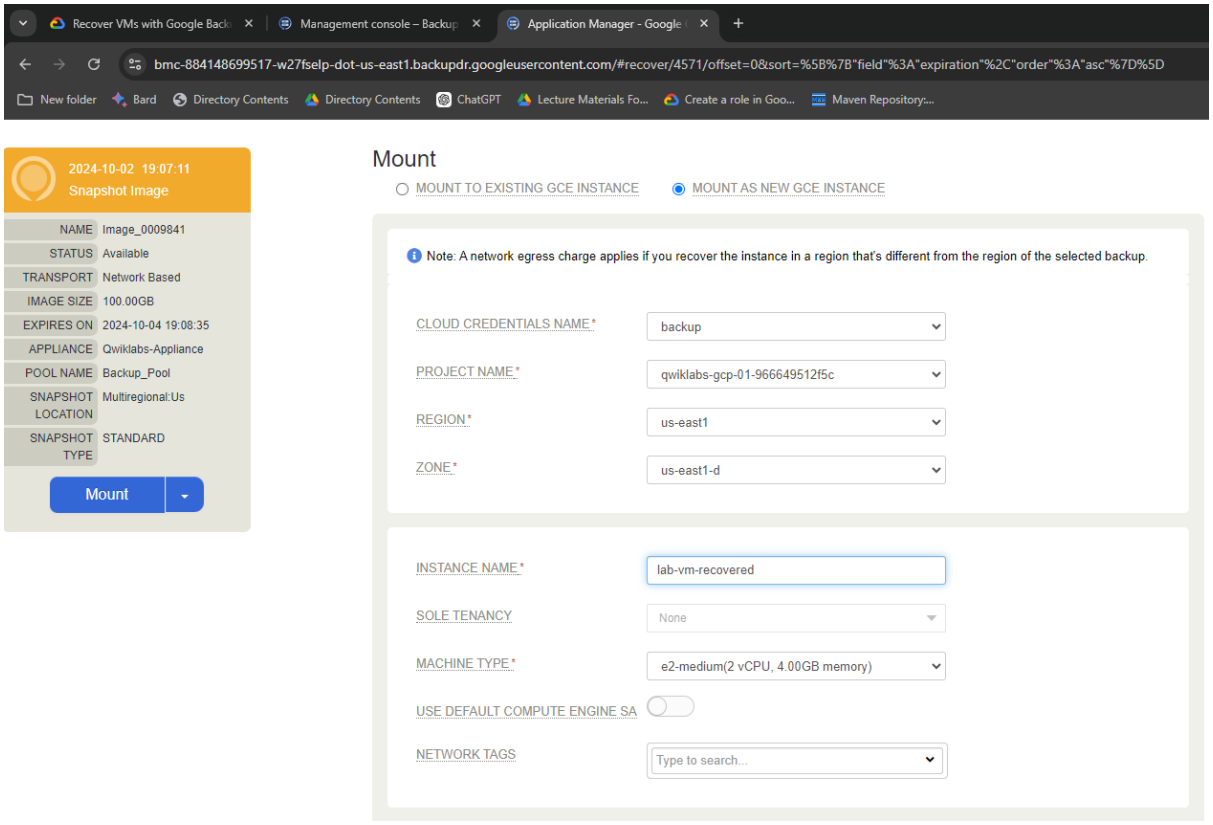


Figure 24 : Configuring the new GCE instance Setting up the configuration for the new Compute Engine instance from the backup.

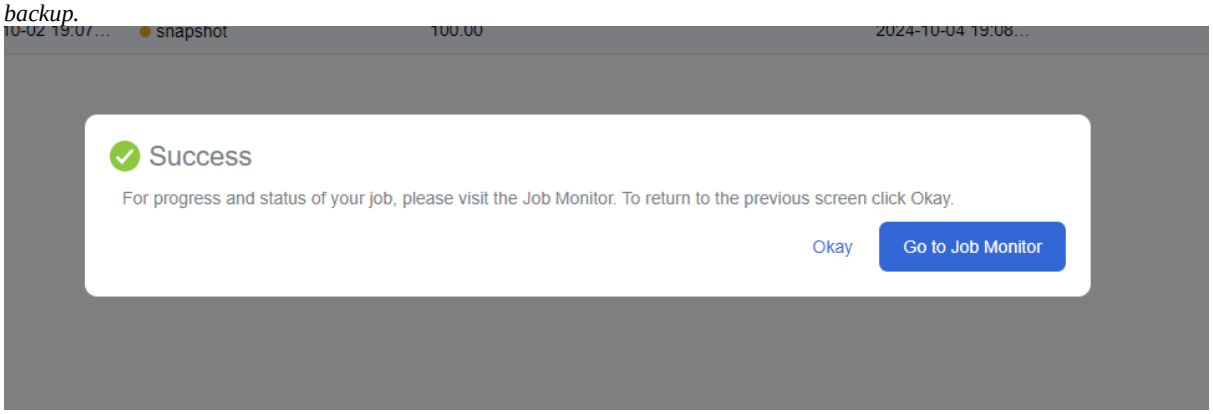


Figure 25 : Completing the mounting process Final steps of the mounting process for the new instance.

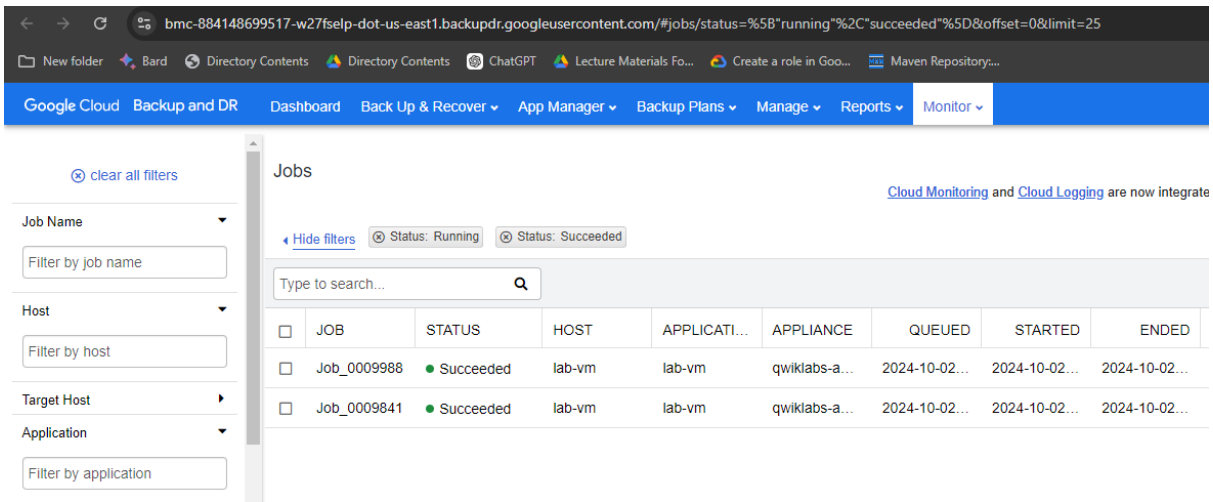


Figure 26 : New job completed Confirmation that the new instance has been successfully created.

Figure 27 : Viewing three VM instances Verifying that the new VM instance is now part of the system.

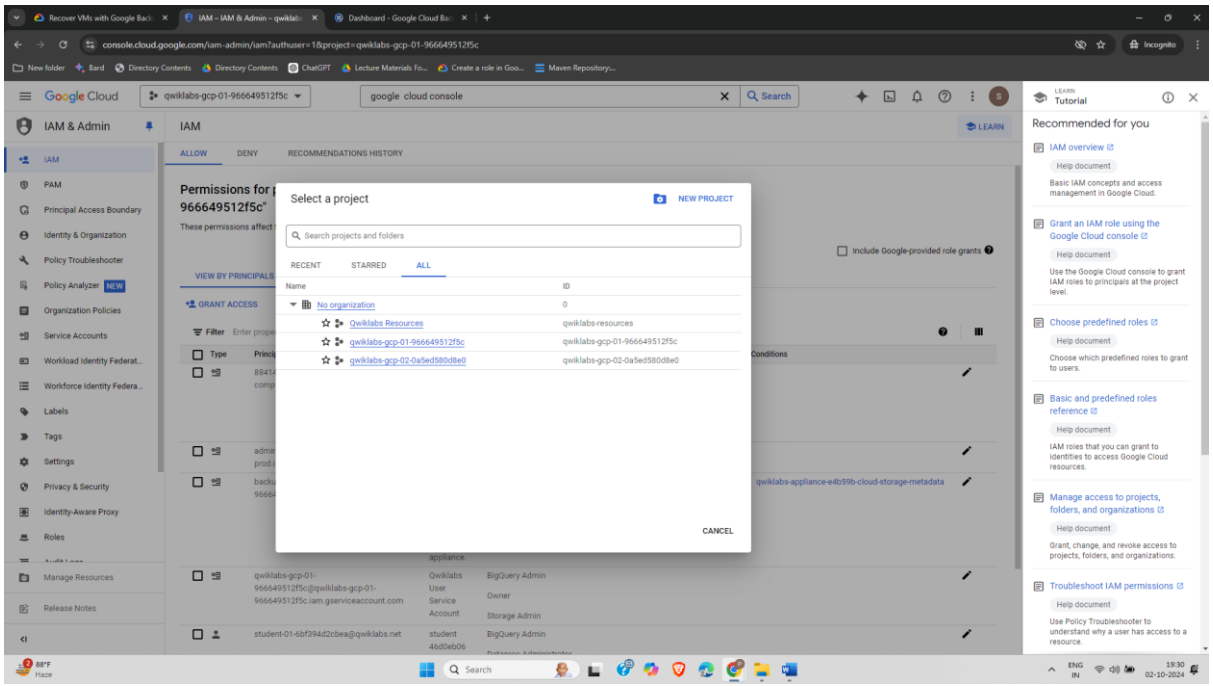


Figure 28 : Granting access in another project Setting up permissions for Backup and DR service in a different project.

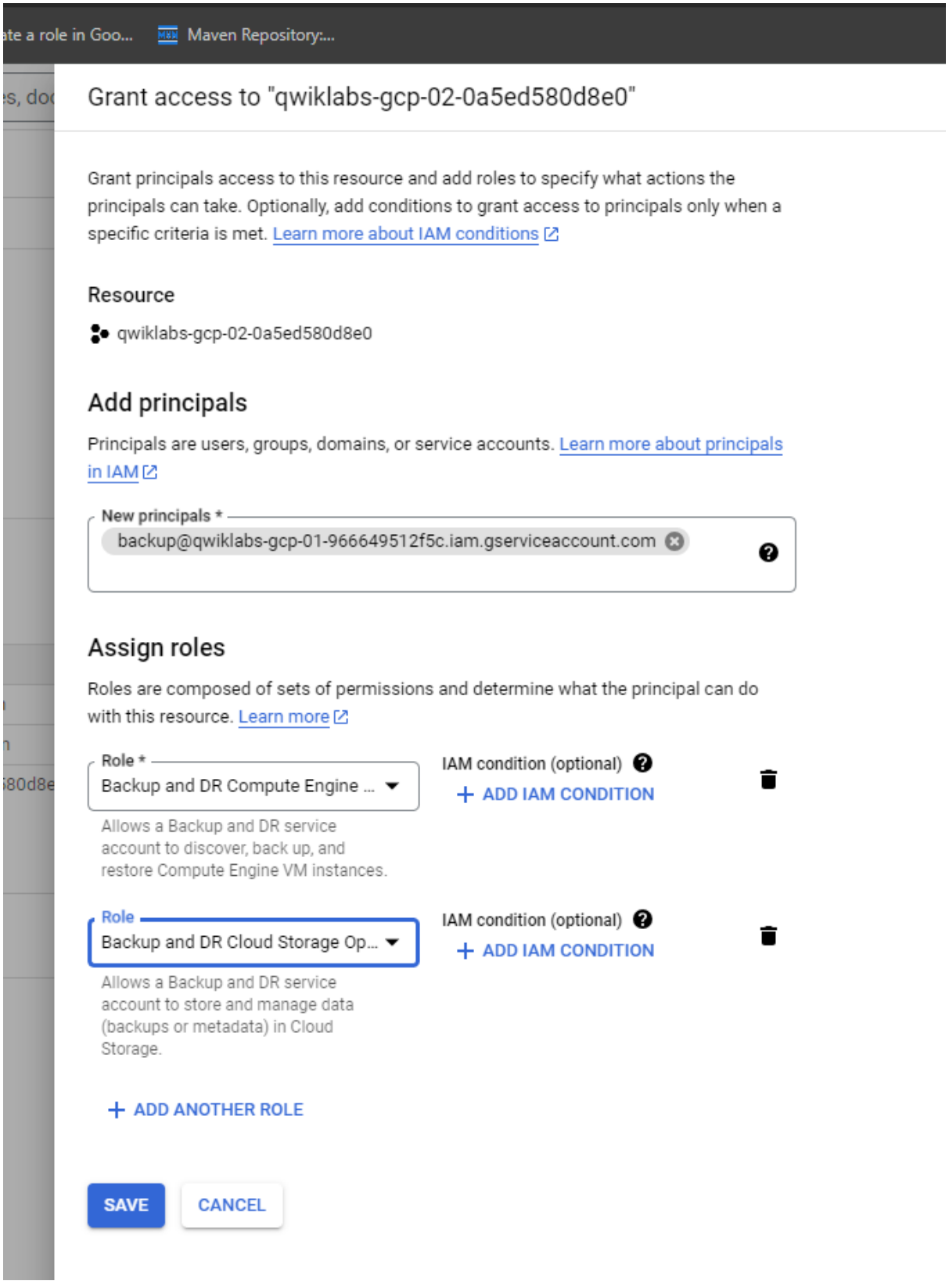


Figure 29 : Adding a new principal for backup access Assigning necessary roles and permissions for backup operations.

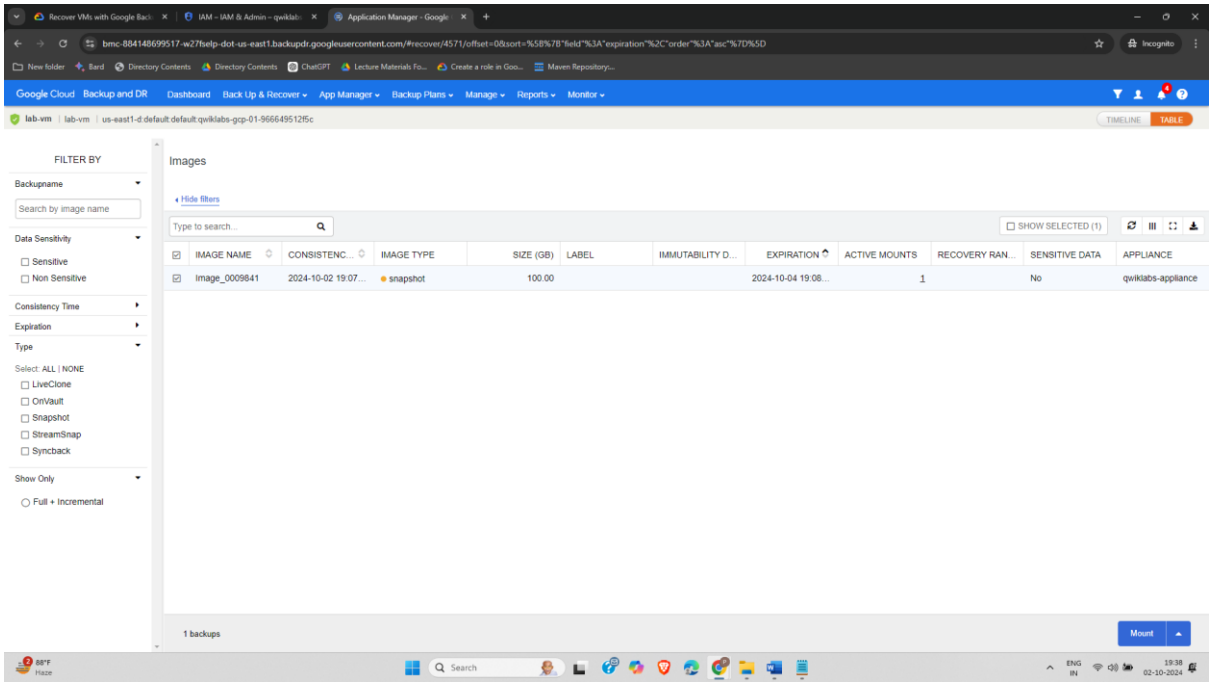


Figure 30 : Navigating to the VM instance and viewing the image Accessing the VM instance and viewing the backup image.

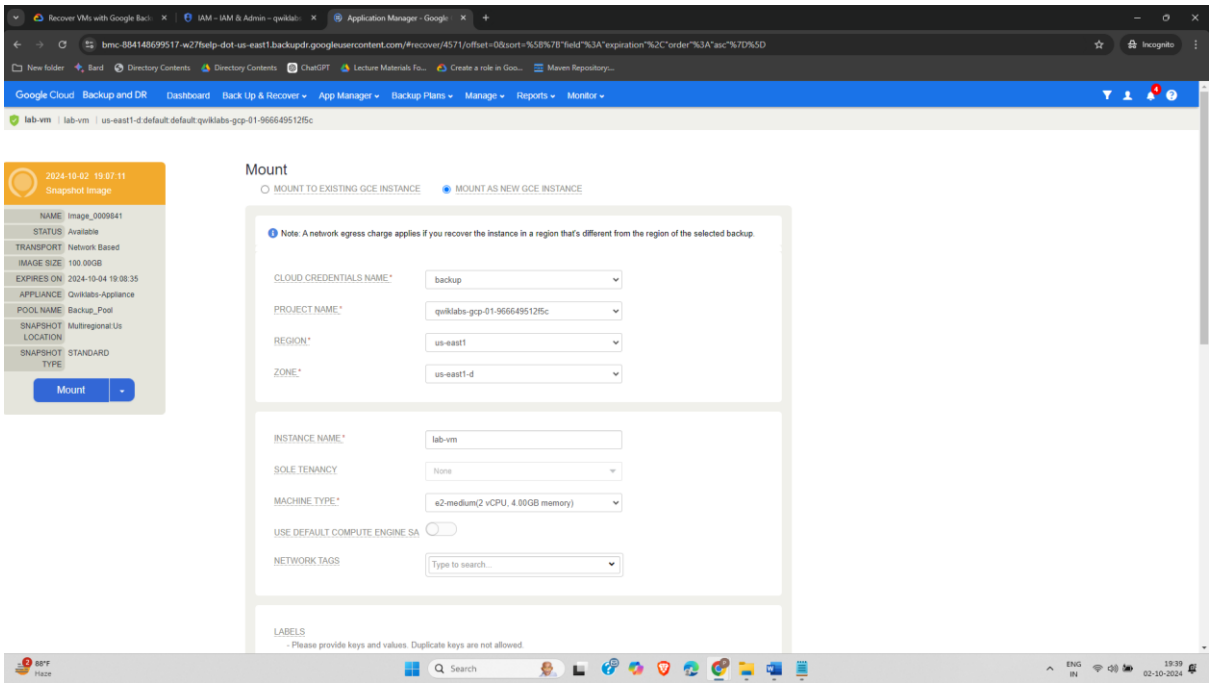


Figure 31 : Mounting the new image with a new GCE instance Mounting another backup image to create a new Compute Engine instance.

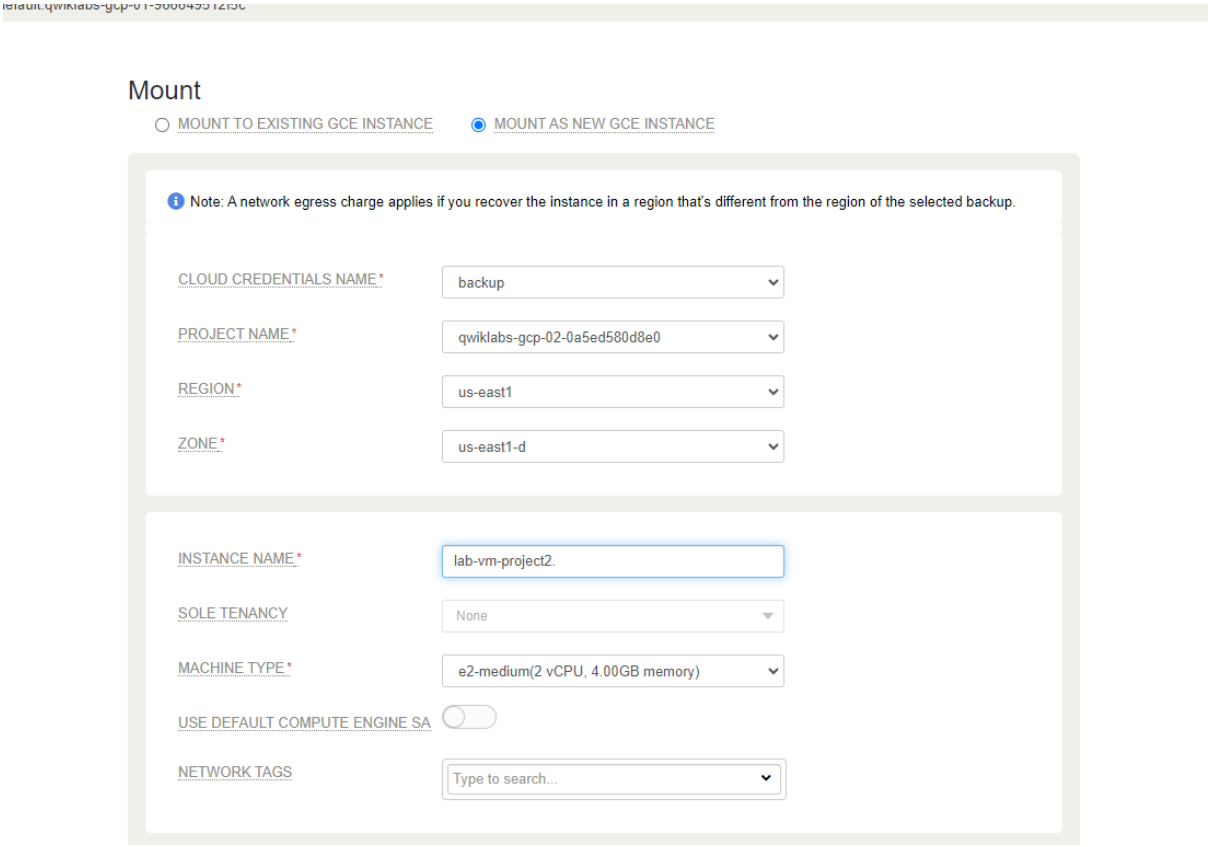


Figure 32 : Configuring project and instance name Final configuration steps for the project and instance details.

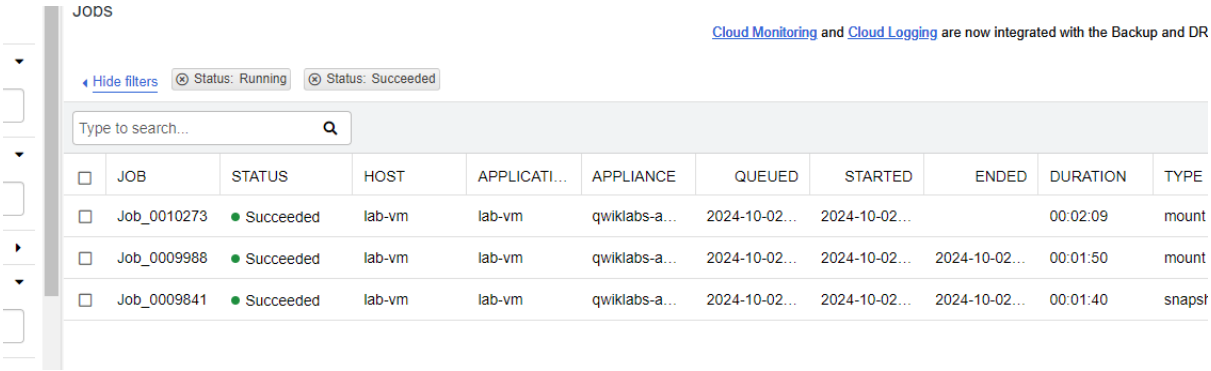


Figure 33 : Job succeeded, new VM instance created Confirmation of successful creation of the new VM instance.

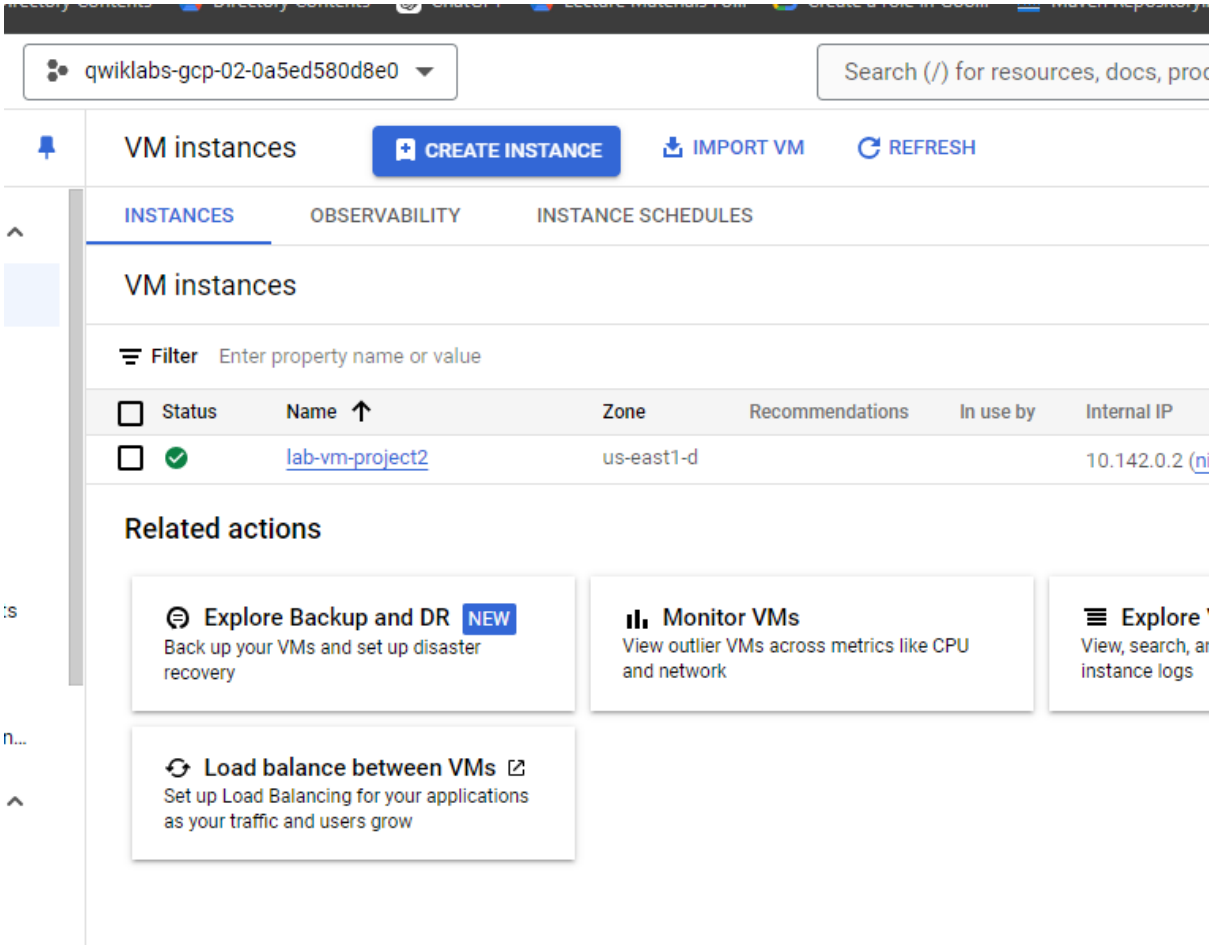


Figure 34 : Viewing the new instance in Project 2 The new instance is now available in the second project.

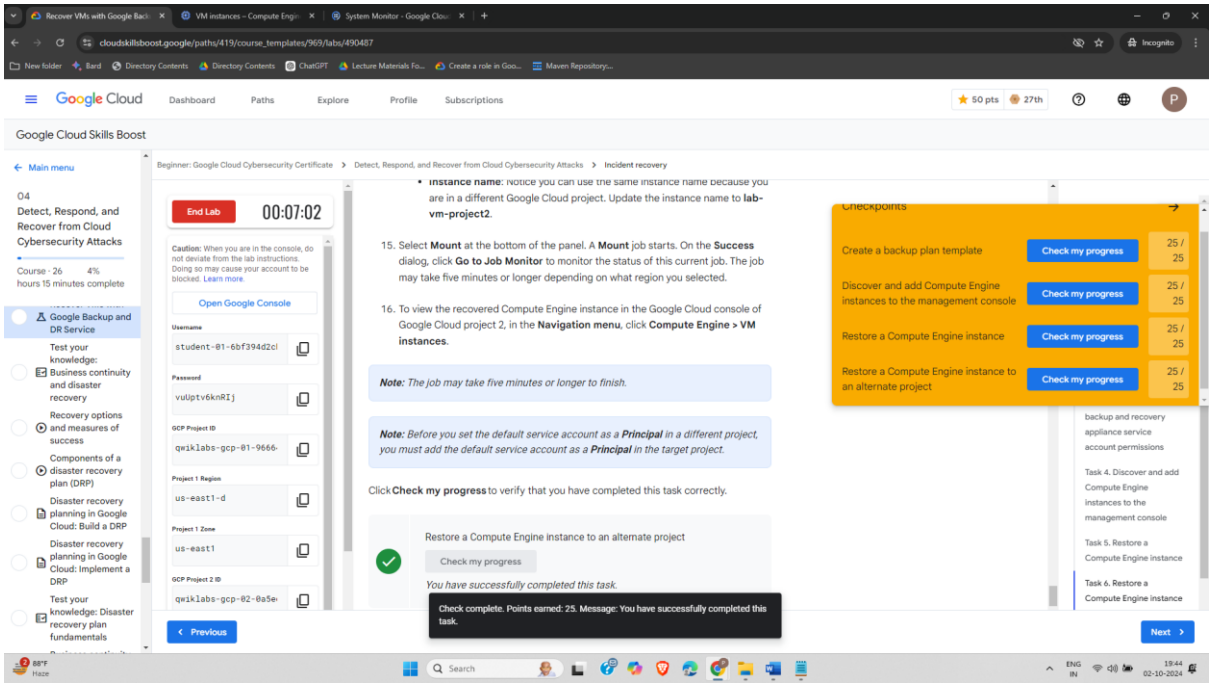


Figure 35 : Task completion Final step indicating the successful completion of the lab task.

LATEST APPLICATIONS:

This lab exercise is an example of how businesses can efficiently back up and restore critical data to ensure business continuity in case of disaster. It applies to scenarios where enterprises need fast and reliable recovery options for their virtual machines, databases, or file systems.

LEARNING OUTCOME:

Through this lab, we learned how to configure Google Cloud Backup and DR Service, create backup templates and policies, perform backups for Compute Engine instances, and recover instances using the mounted backup images. We also explored monitoring tools for tracking the status of backup jobs.

REFERENCES:

- Google Cloud Documentation: Backup and DR Service
- Lab Guides: Practical implementation of cloud-based disaster recovery solutions

PRACTICAL: 12

AIM:

For the last year, you've been working as a junior cloud security analyst at Cymbal Retail. Cymbal Retail is a market powerhouse currently operating 170 physical stores and an online platform across 28 countries. They reported $15 billion in revenue in 2022, and currently employ 80,400 employees across the world.

Cymbal Retail boasts a vast customer base with a multitude of transactions happening daily on their online platform. The organization is committed to the safety and security of its customers, employees, and its assets, ensuring that its operations meet internal and external regulatory compliance expectations in all the countries it operates in.

Recently, the company has experienced a massive data breach. As a junior member of the security team, you'll help support the security team through the lifecycle of this security incident. You'll begin by identifying the vulnerabilities related to the breach, isolate and contain the breach to prevent further unauthorized access, recover the compromised systems, remediate any outstanding compliance related issues, and verify compliance with frameworks.

Here's how you'll do this task: **First** you'll examine the vulnerabilities and findings in Google Cloud Security Command Center. **Next**, you'll shut the old VM down, and create a new VM from a snapshot. **Then**, you'll evoke public access to the storage bucket and switch to uniform bucket-level access control. **Next**, you'll limit the firewall ports access and fix the firewall rules. **Finally**, you'll run a report to verify the remediation of the vulnerabilities.

THEORY:

In cloud computing environments, ensuring data security is critical to protecting sensitive information and maintaining compliance with regulatory standards. Cloud providers offer a range of tools and services to help organizations secure their infrastructure and mitigate risks, such as unauthorized access, data breaches, and misconfigurations.

Key elements of cloud security include:

1. **Vulnerability Management**: Identifying and addressing weaknesses in the system is vital to preventing security breaches. Vulnerability scanners and security command centers provide continuous monitoring of cloud resources to detect issues such as open ports, insecure configurations, and exposed data storage.

2. **Access Control**: Proper access control mechanisms, such as identity and access management (IAM), are essential to restricting who can access various resources. Fine-grained permissions ensure that only authorized users and applications can interact with sensitive data and systems.

3. **Firewall and Network Security**: Configuring firewalls to restrict access to critical services, such as SSH and RDP, is a fundamental aspect of securing cloud networks. Firewalls block unauthorized traffic and allow only trusted IP addresses to interact with services, reducing the attack surface.

4. **Data Protection**: Publicly exposed cloud storage buckets are a common vulnerability that can lead to data breaches. By enforcing bucket-level permissions, restricting public access, and ensuring data encryption, organizations can protect their sensitive information from unauthorized access.

5. **Compliance**: Many organizations must adhere to specific regulatory frameworks, such as PCI DSS, HIPAA, or GDPR, depending on their industry and geographic location. Compliance involves regularly auditing systems, applying best practices, and remediating any issues to meet these requirements.

6. **Incident Response**: In the event of a security breach, it is essential to follow a structured incident response process. This includes identifying the root cause of the breach, isolating affected systems, recovering compromised assets, and implementing measures to prevent future incidents.

OUTPUT:

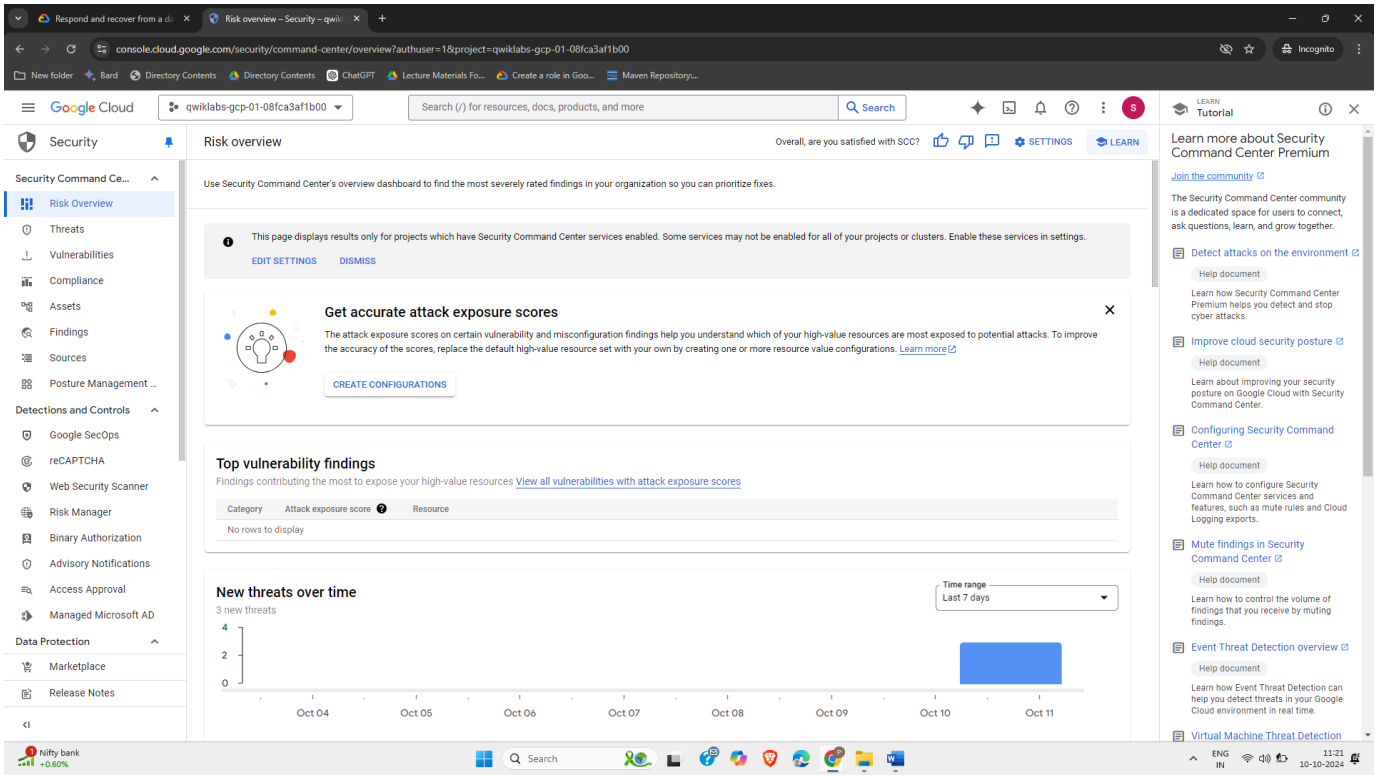


Figure 1 : Navigating to the Google Cloud Security Command Center's dashboard to assess security risks and vulnerabilities.

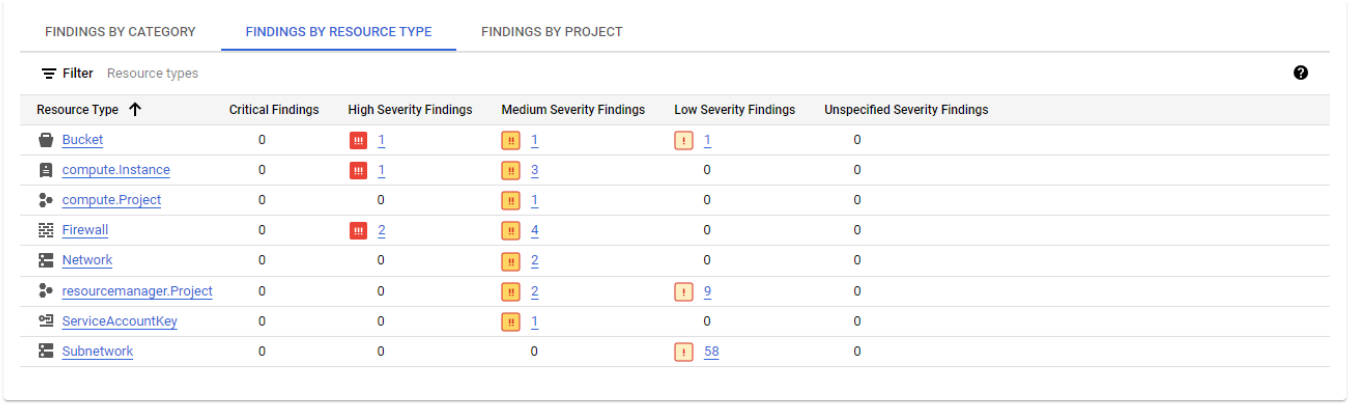


Figure 2 : Viewing active vulnerabilities by scrolling to the "Findings By Resource Type" tab to categorize vulnerabilities based on resource type.

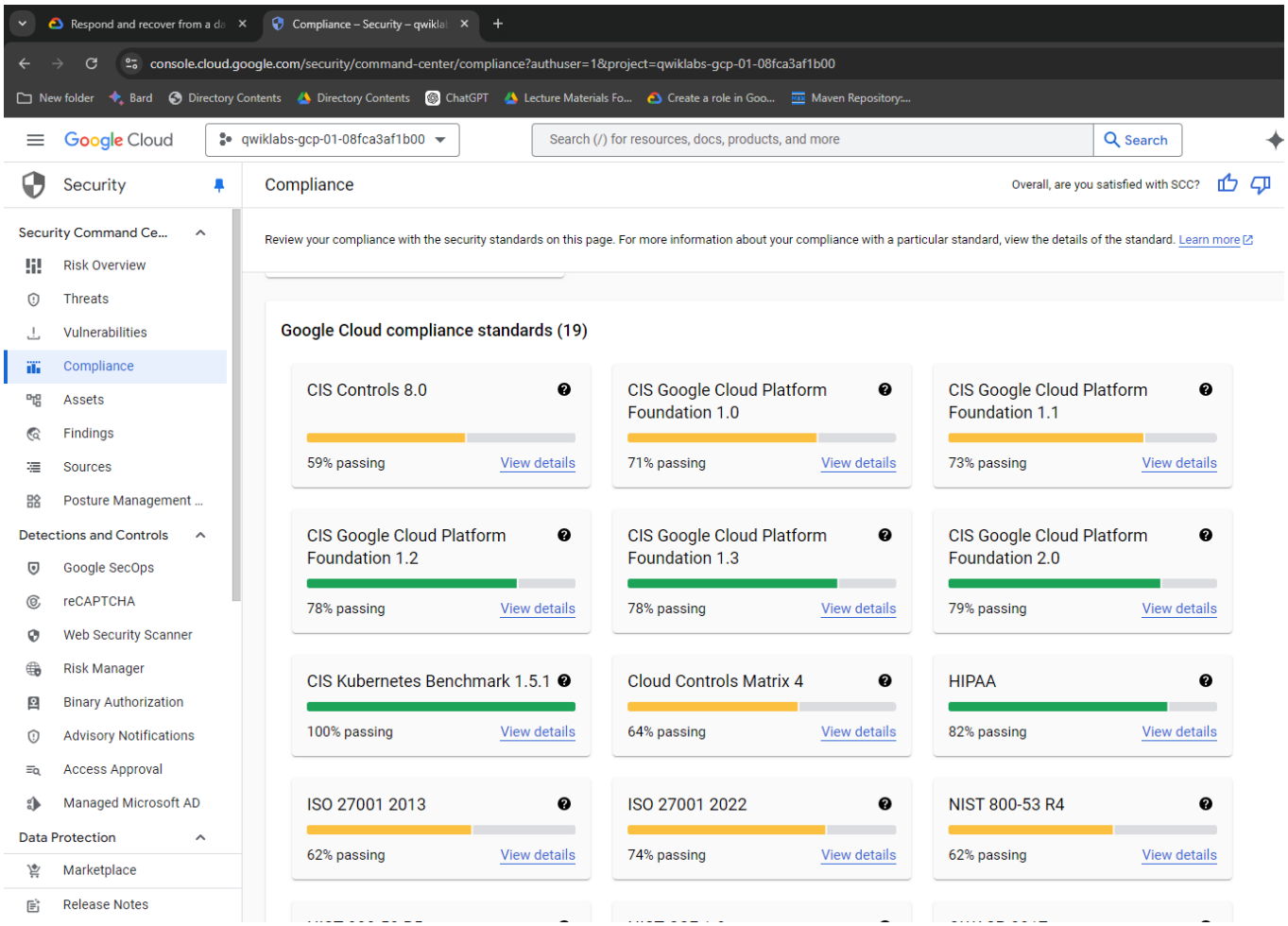


Figure 3 : Clicking on the PCI DSS 3.2.1 compliance tile in the compliance standards section to generate the corresponding report.

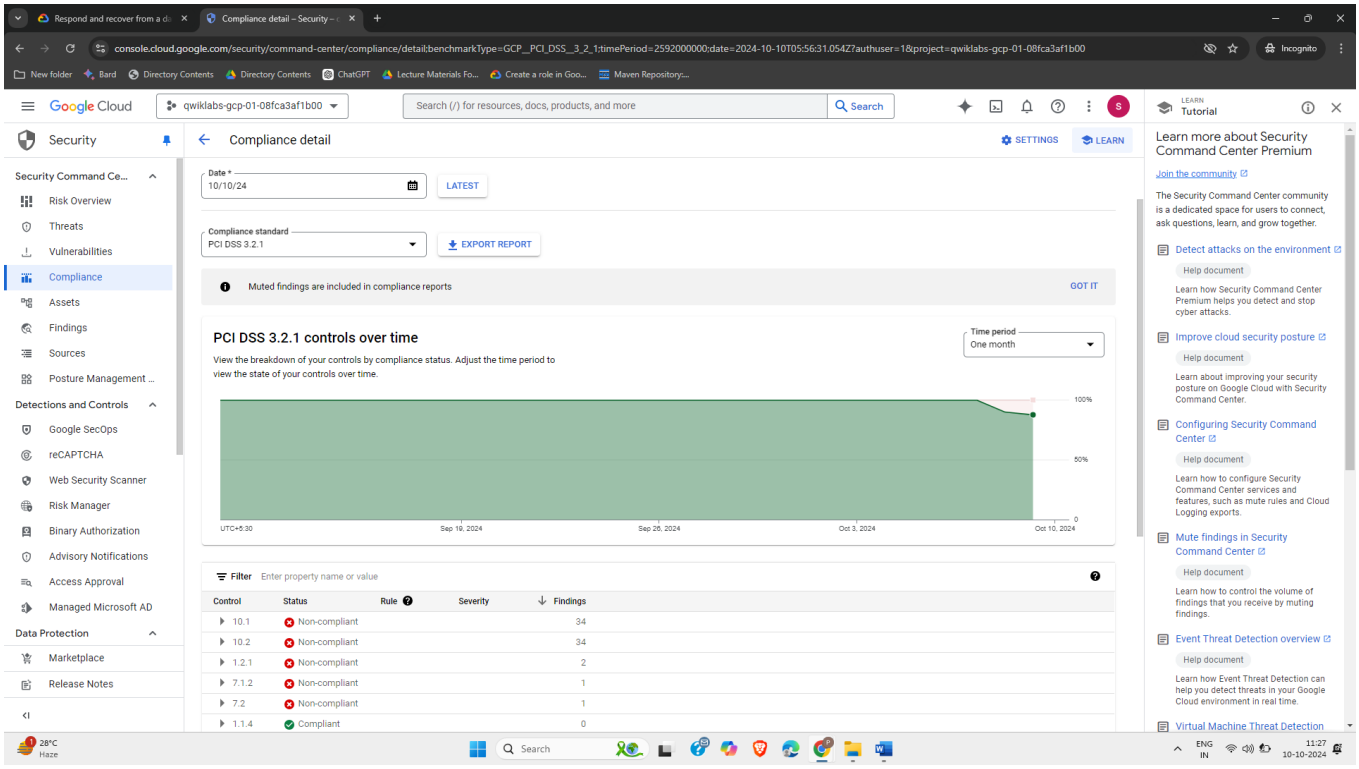


Figure 4 : Sorting findings by clicking on the Findings column, displaying active findings at the top for easy reference.

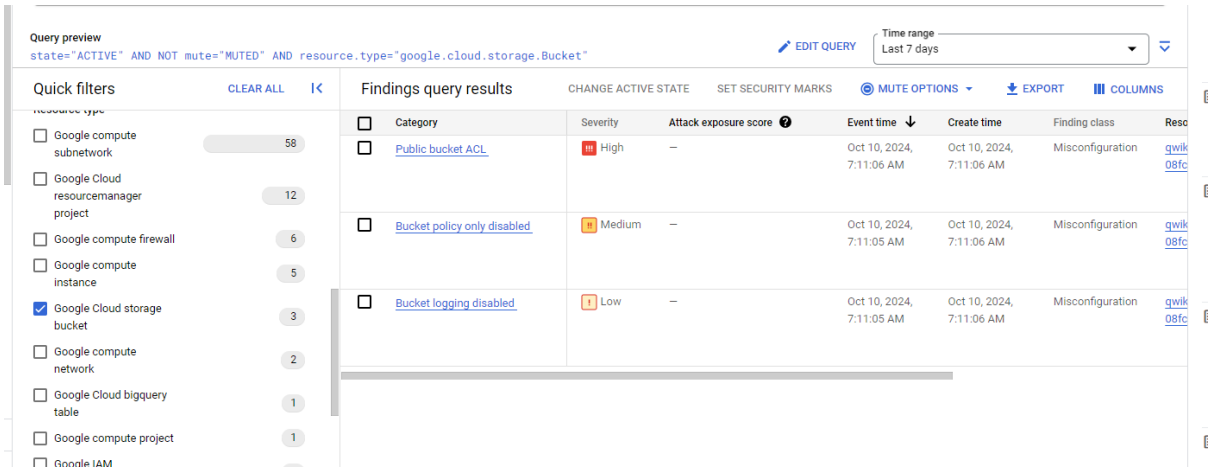


Figure 5 : Filtering by Google Cloud storage buckets, then switching filters to display findings related to Google Compute instances for a focused analysis.

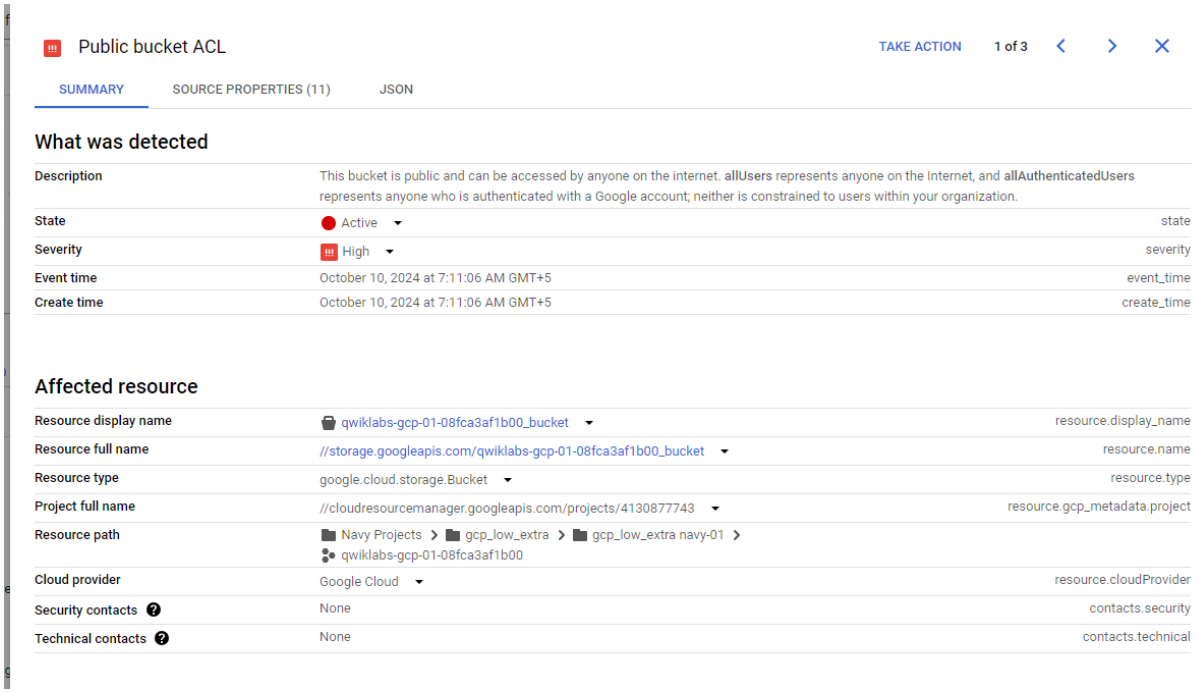


Figure 6 : Examining a public bucket ACL configuration, identifying its non-compliance with security protocols.

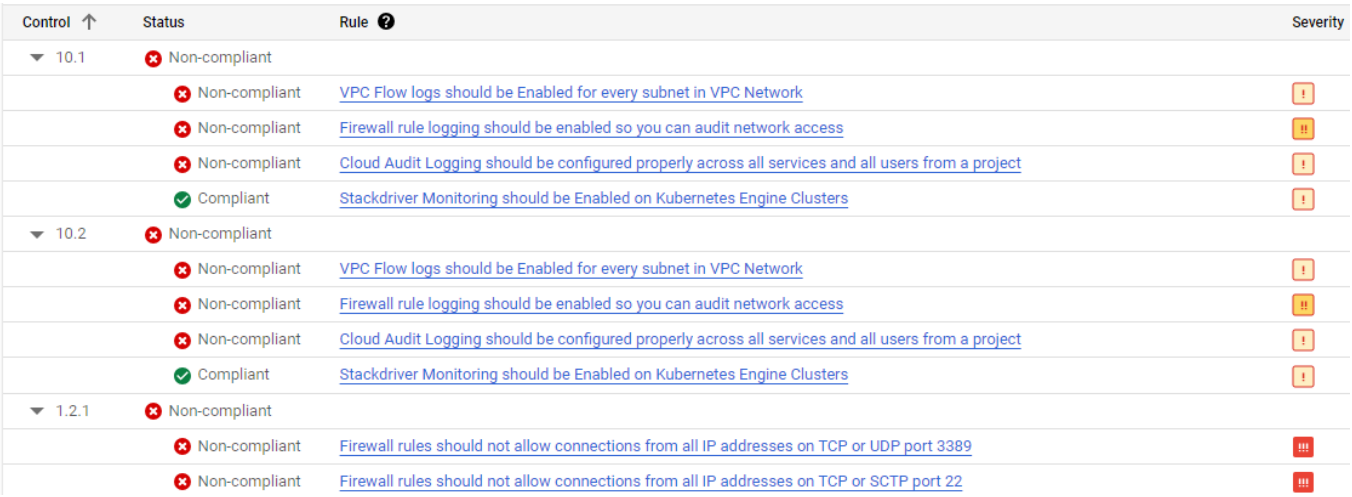


Figure 7 : Identifying non-compliant resources with high-risk configurations that need to be remediated to meet security standards.

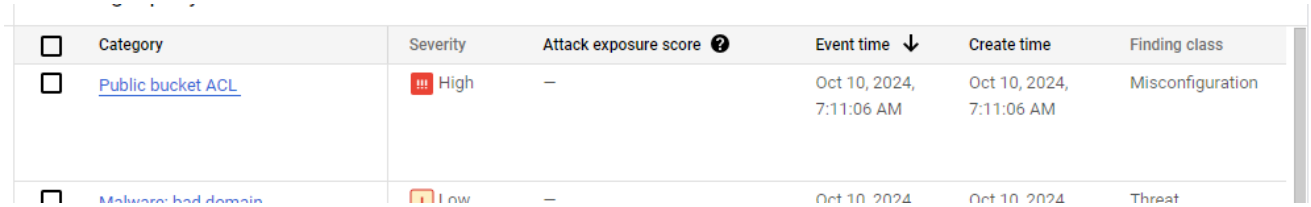


Figure 8 : Displaying a high-severity finding related to an open and publicly accessible Google Cloud Storage bucket ACL.

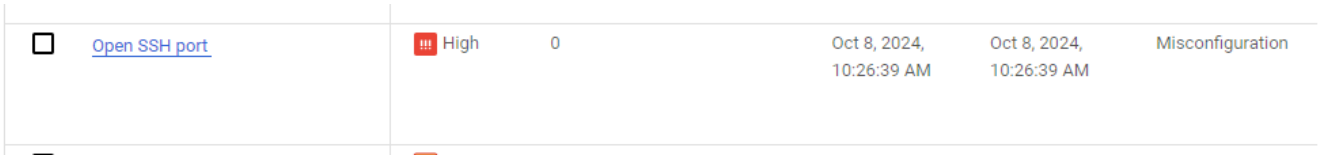


Figure 9 : Displaying a high-severity finding for an open SSH port on a vulnerable virtual machine, requiring immediate attention.

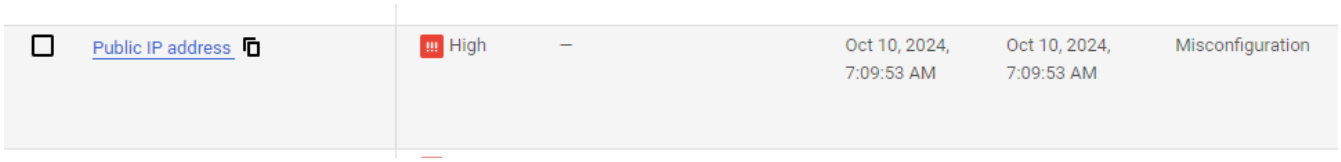


Figure 10 : High-severity findings showing a public IP address configuration, presenting a potential attack vector for the breach.

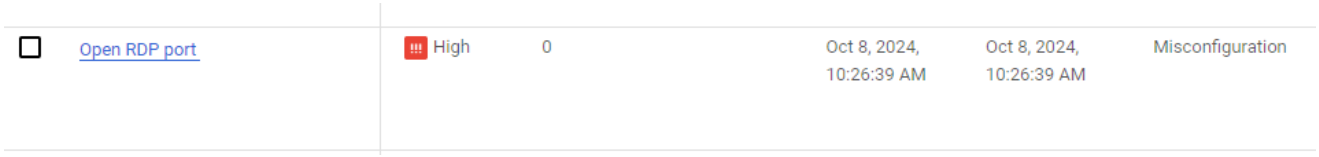


Figure 11 : Findings showing an open RDP port, which is a critical vulnerability on the compromised system.

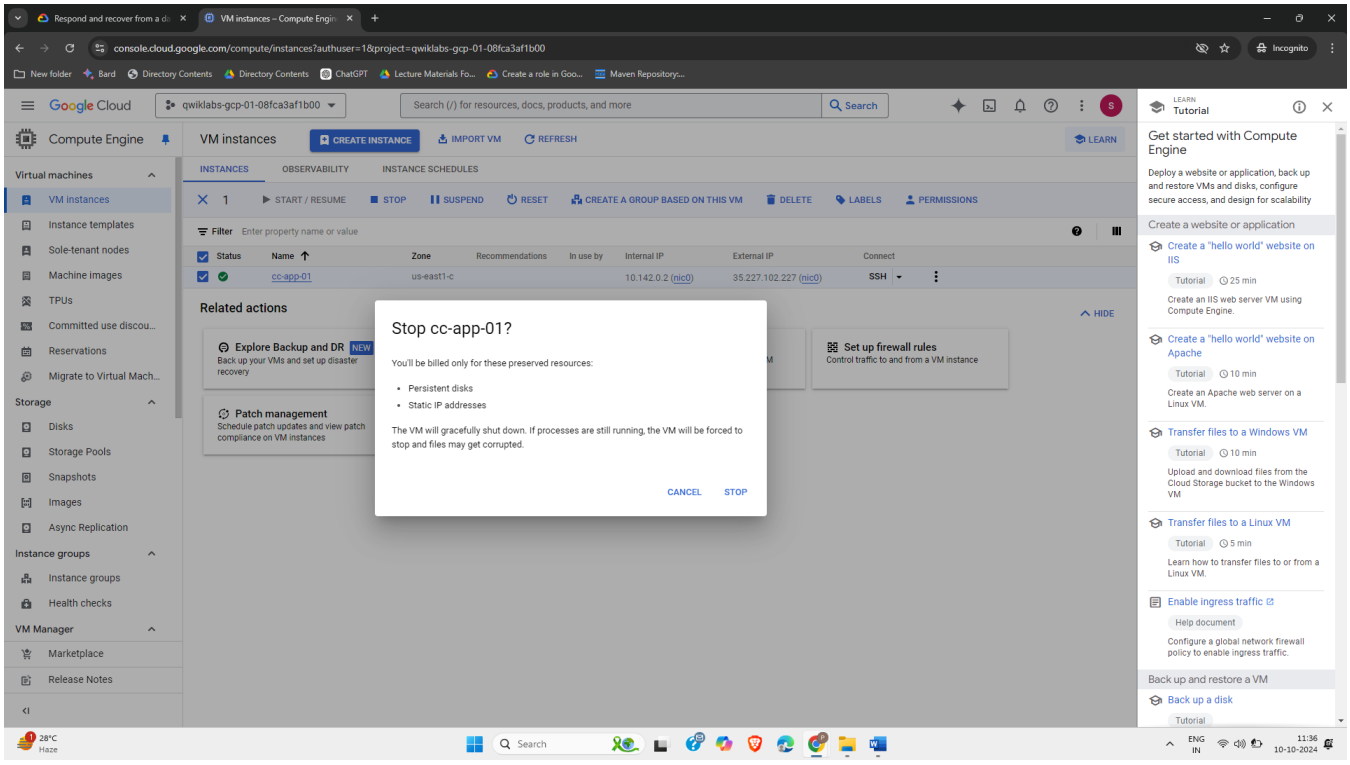


Figure 12 : Identifying the vulnerable VM instance, cc-app-01, on the Compute Engine > VM instances page. This VM needs to be stopped to prevent further compromise.

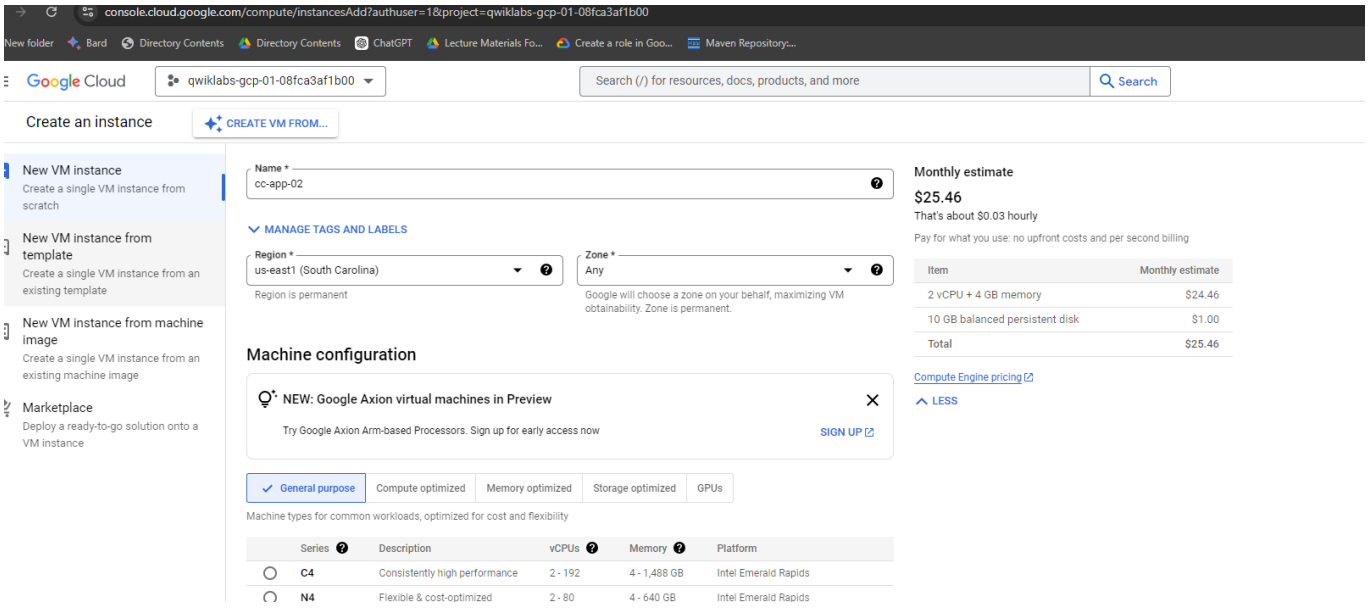


Figure 13 : Creating a new instance named cc-app-02 from the cc-app01-snapshot, ensuring the new instance uses secure boot options..

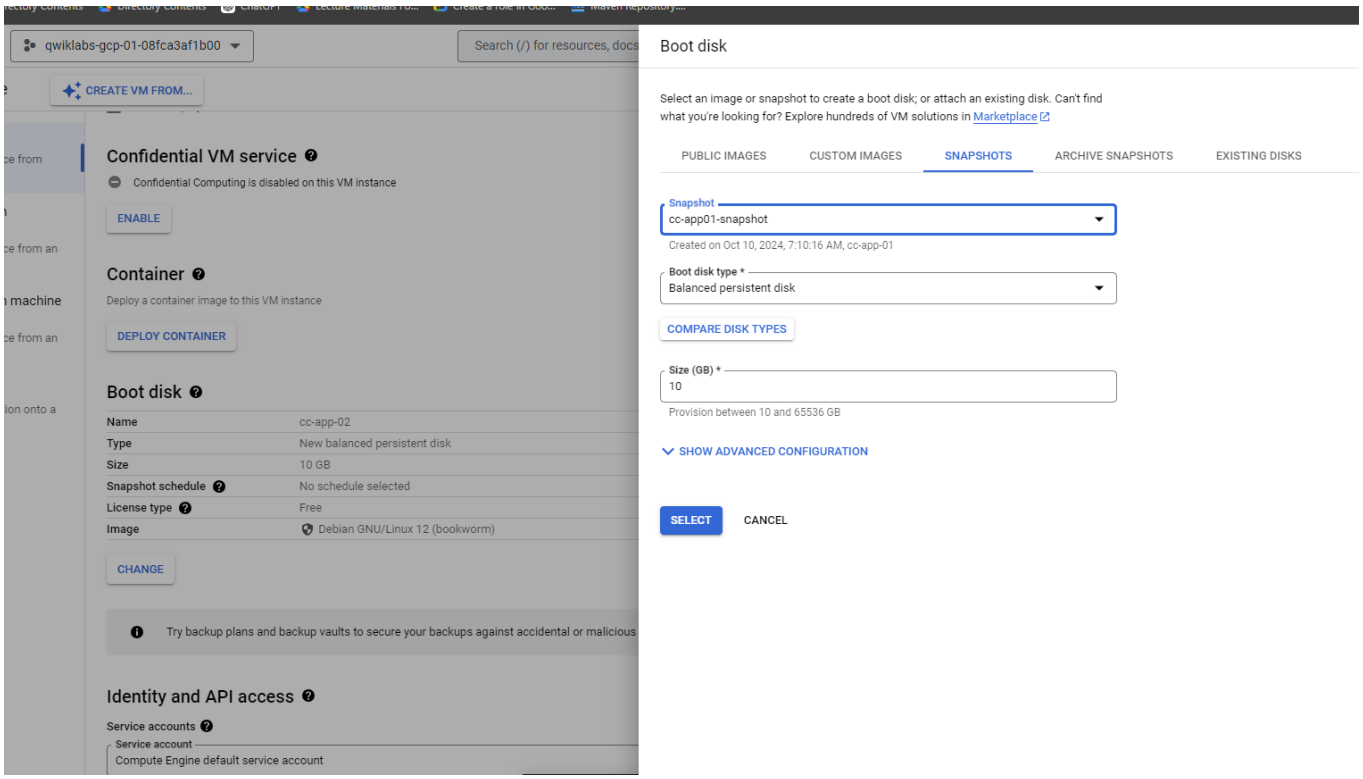


Figure 14 : Selecting the snapshot from the cc-app01-snapshot to replicate the environment while remediating security issues.

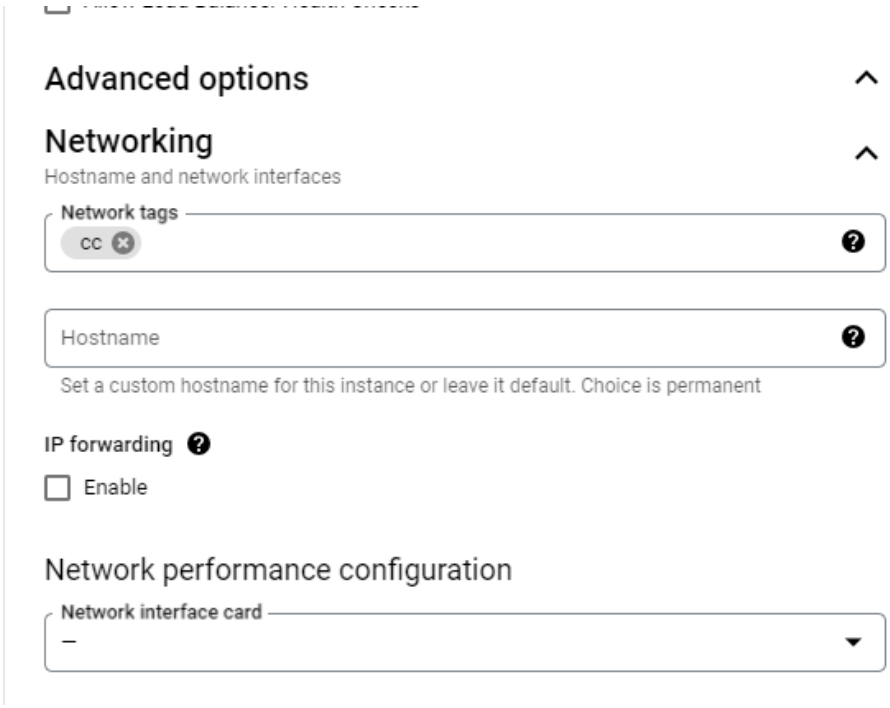


Figure 15 : Adding network tags (cc) for the new VM to apply specific firewall rules that restrict unauthorized access.

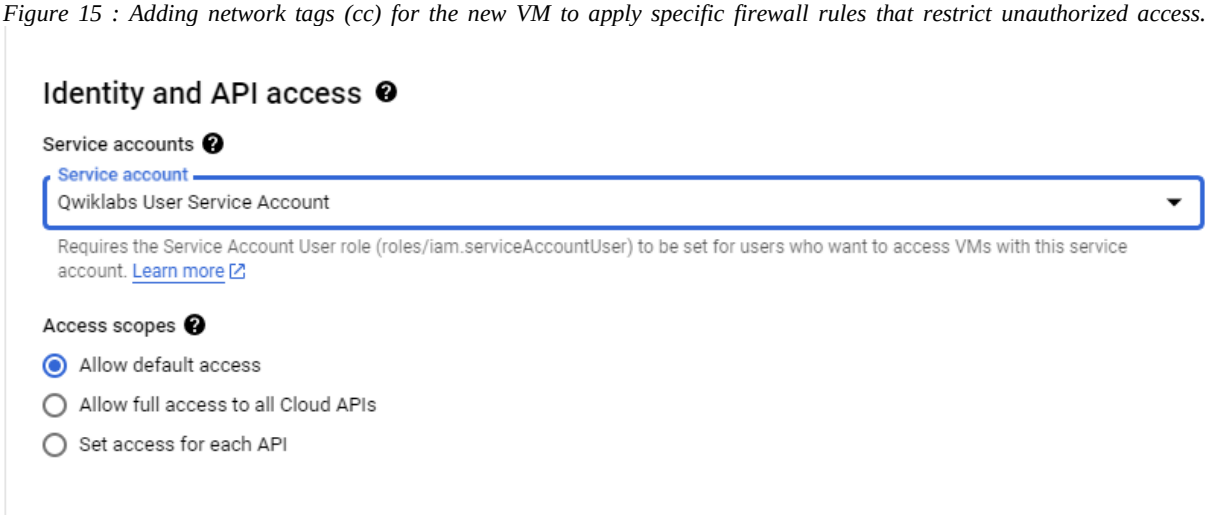


Figure 16: Assigning a service account (Qwiklabs User Service Account) to the new VM for controlled access and permission management.

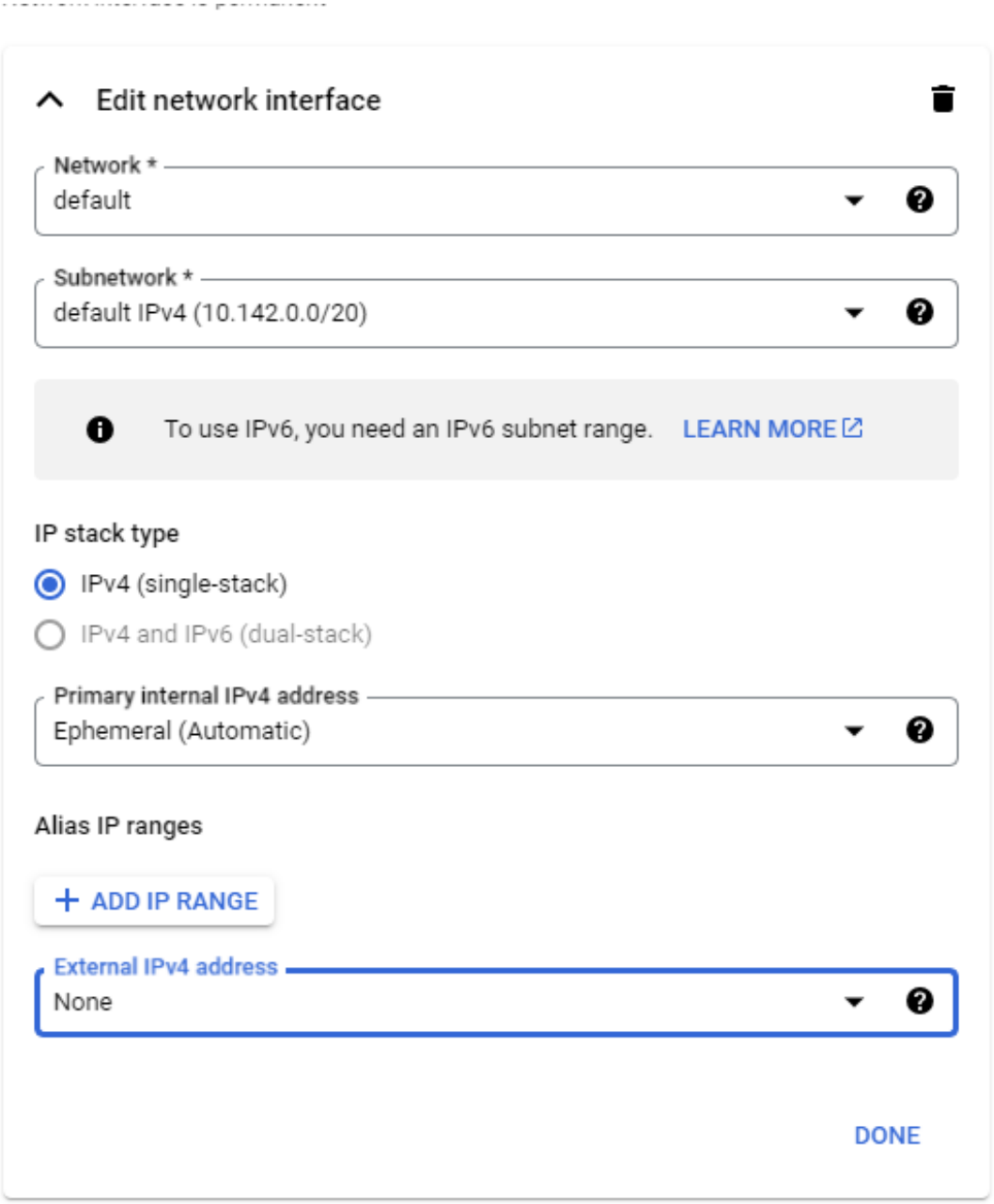


Figure 17 : Configuring the external IP address settings for cc-app-02, ensuring there is no public-facing IP to reduce exposure..

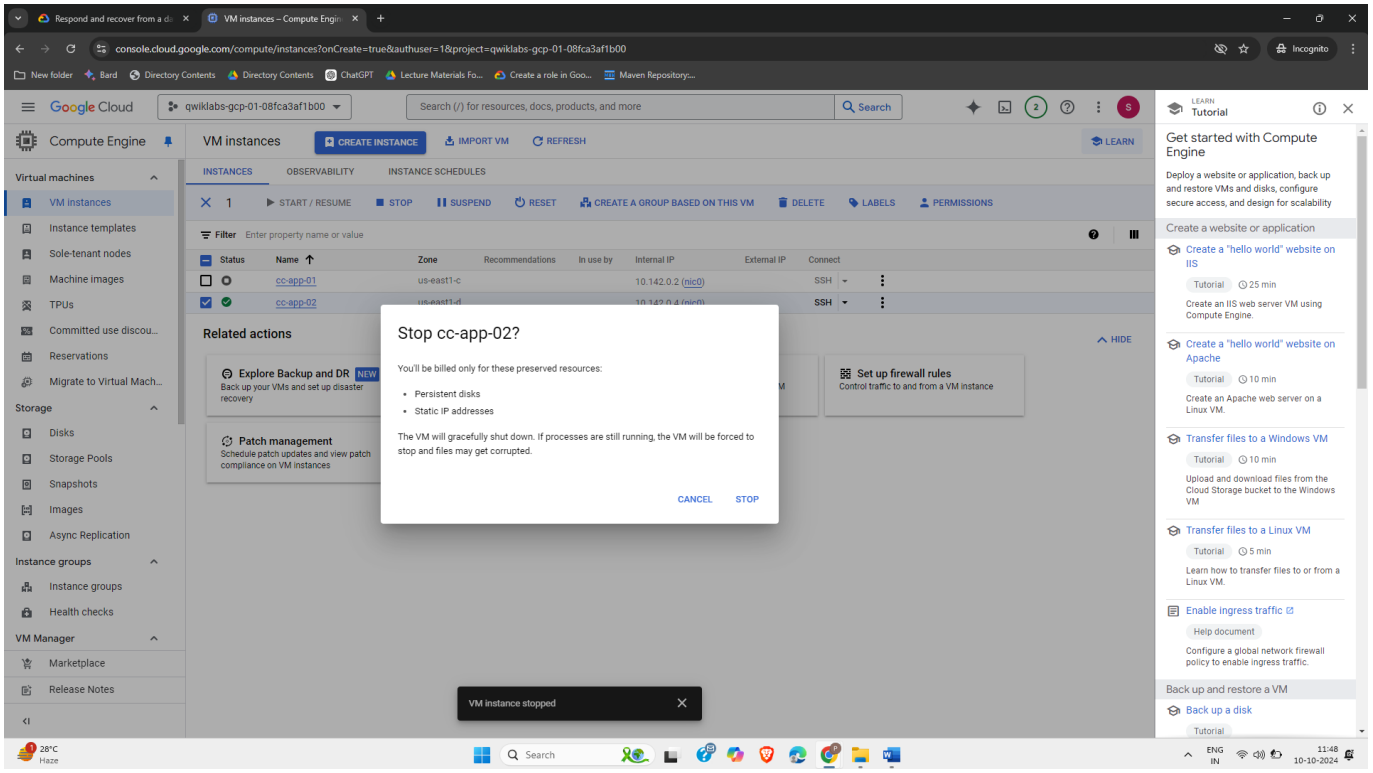


Figure 18 : Stopping the cc-app-02 VM temporarily for additional security configuration and applying the correct firewall rules.

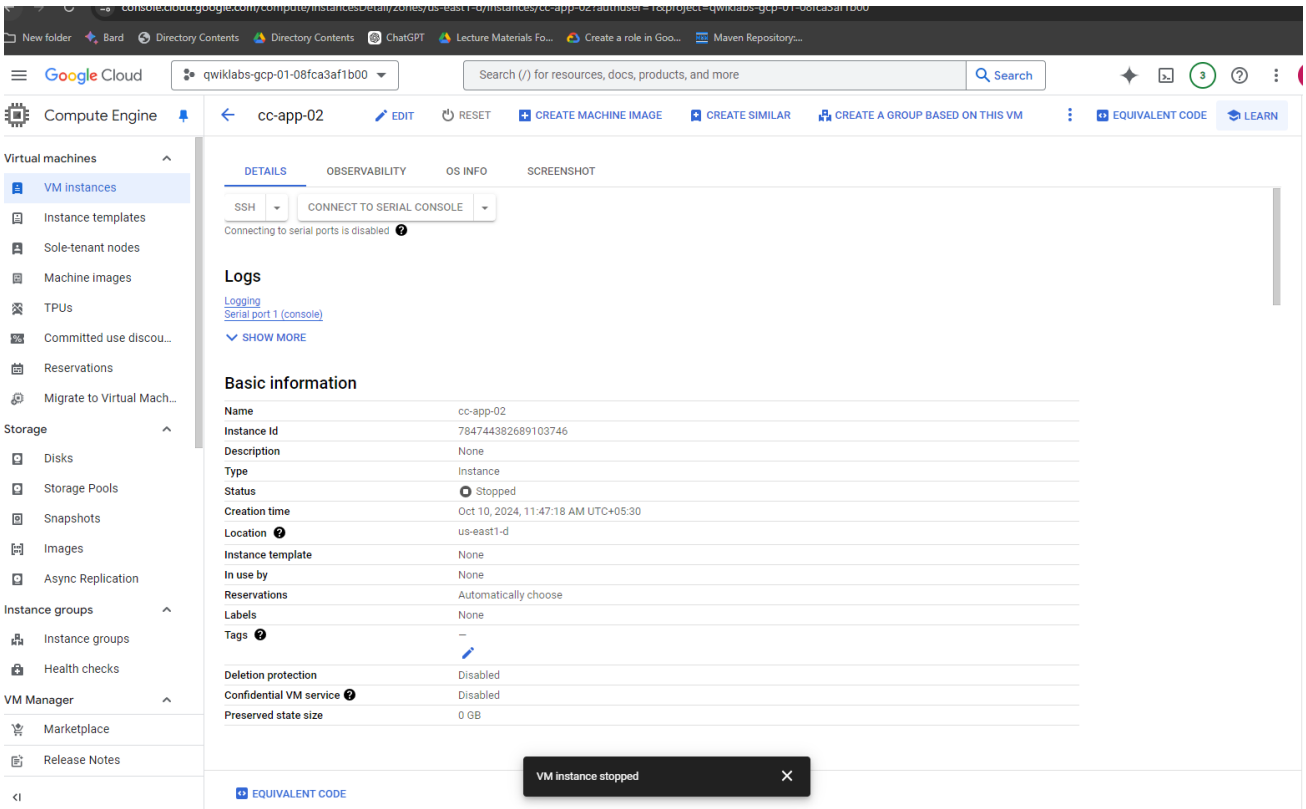


Figure 19 : Editing security settings for the cc-app-02 VM, ensuring that Secure Boot is enabled for compliance with security best practices.

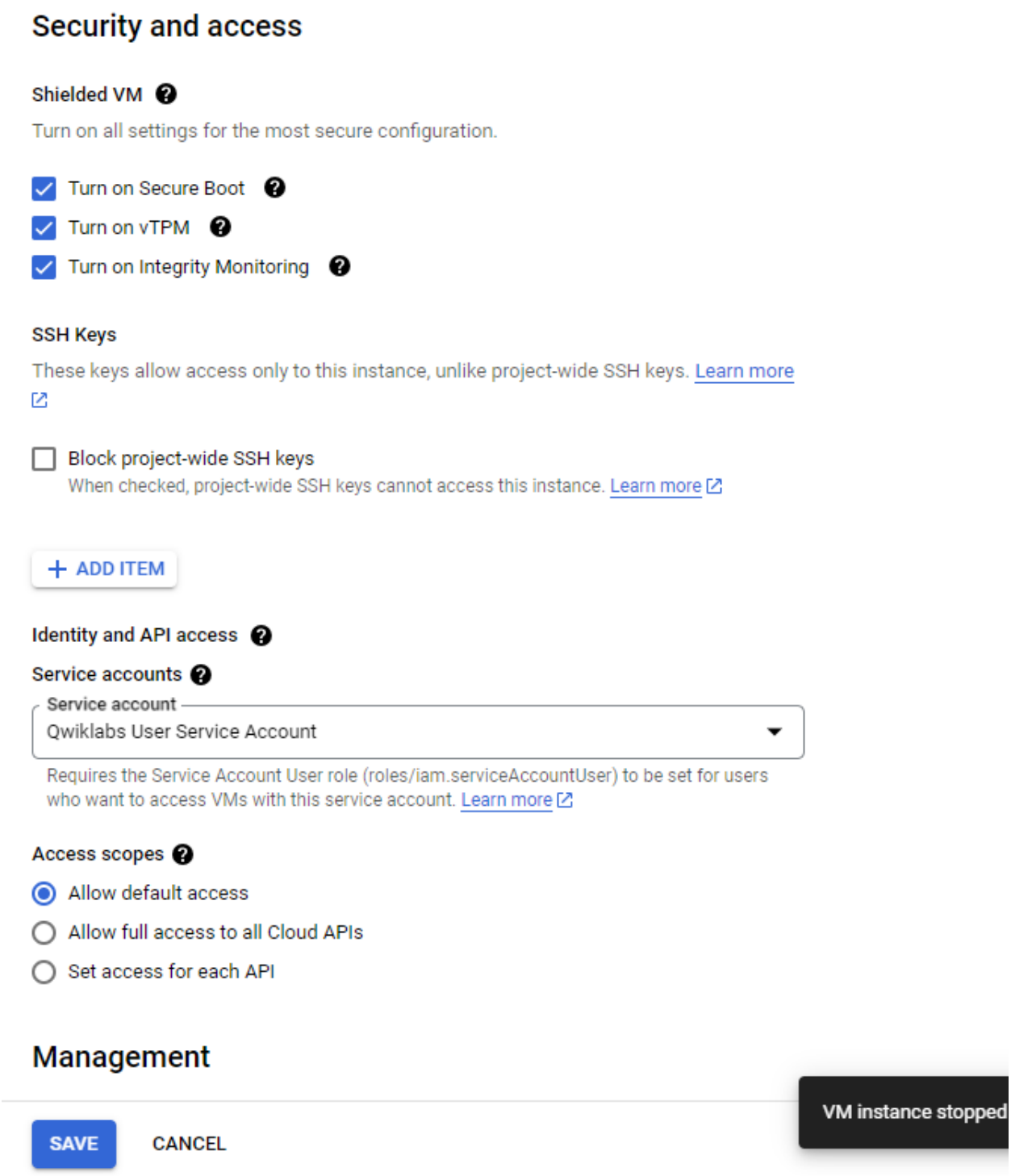


Figure 20 : Applying Shielded VM settings, enabling secure boot for the cc-app-02 instance, and ensuring the machine is protected from malicious rootkits.

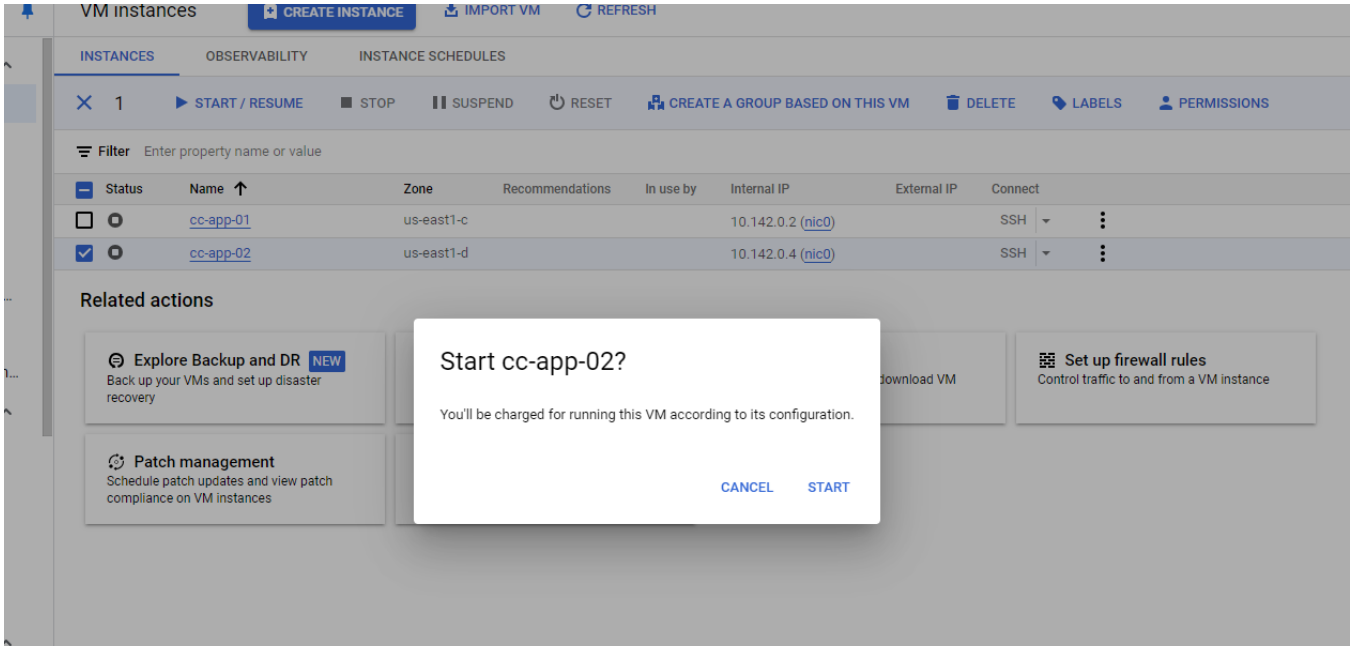


Figure 21 : Starting the cc-app-02 VM instance after ensuring all security protocols are in place.

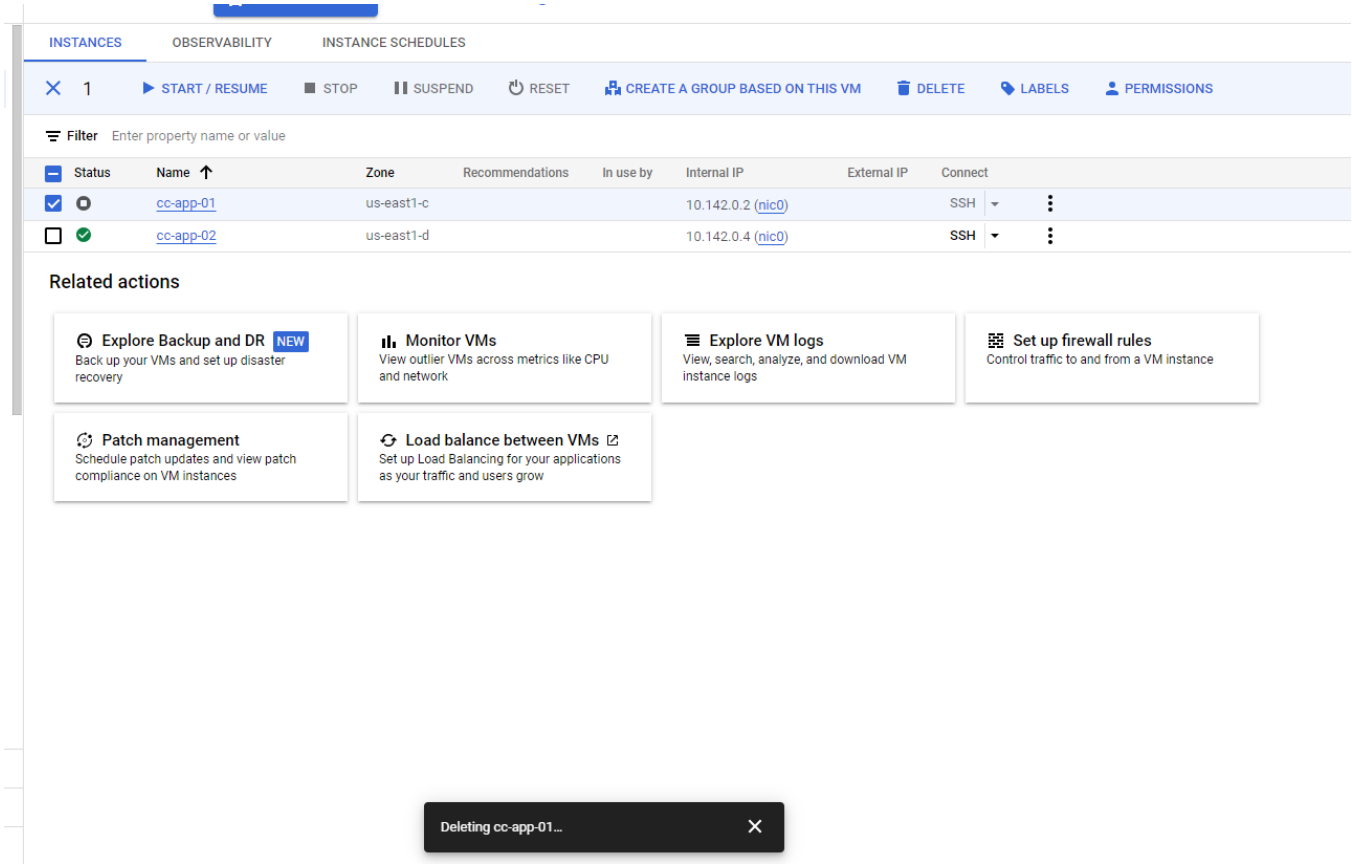


Figure 22 : Deleting the compromised cc-app-01 VM to eliminate the threat and prevent further exploitation.

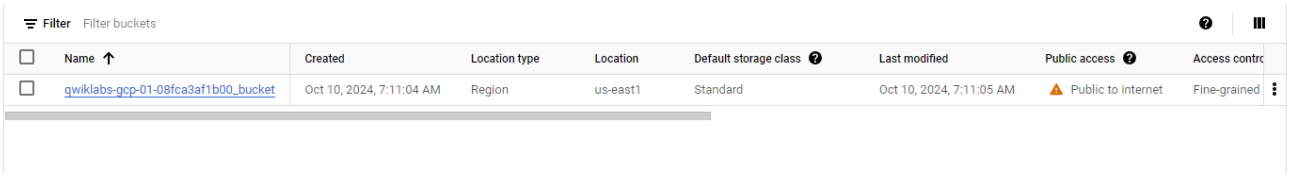


Figure 23 : Navigating to the project_id_bucket storage bucket where sensitive data was compromised and needs to be secured.

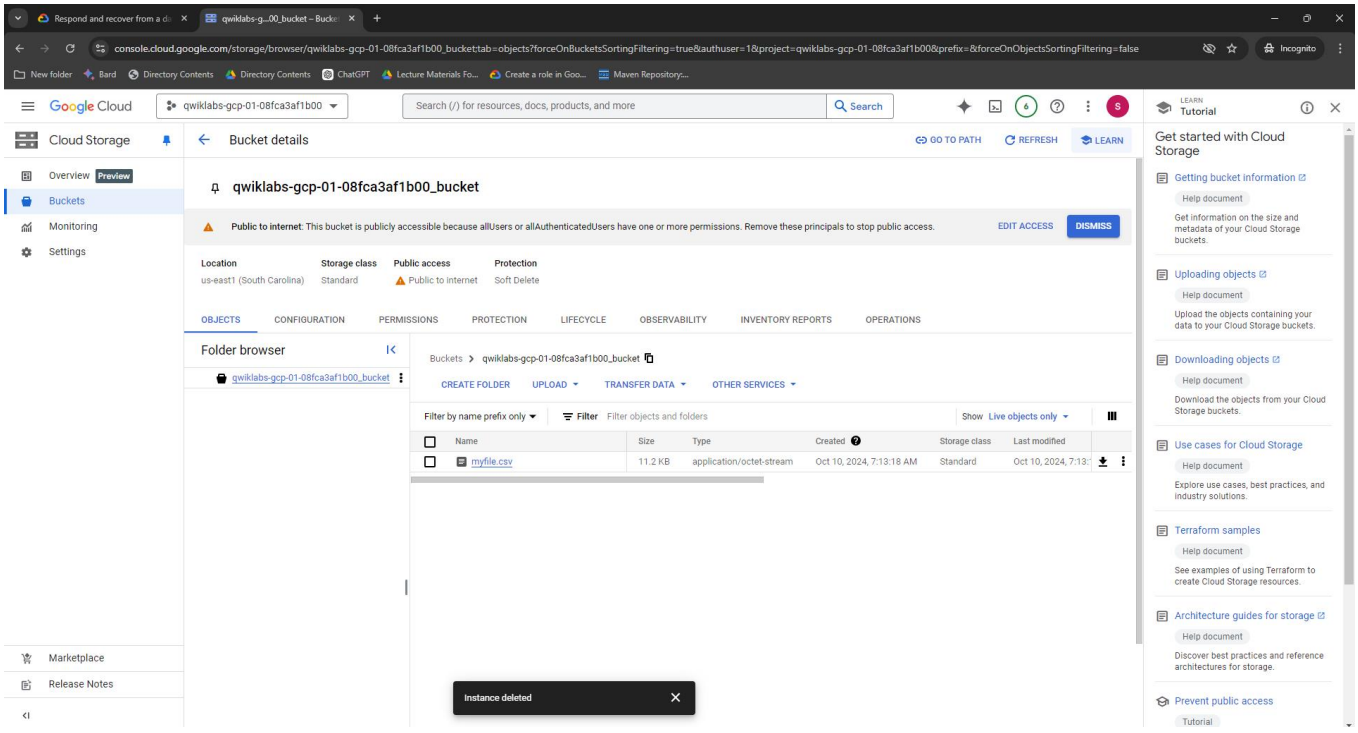


Figure 24 : Identifying the public file, myfile.csv, in the storage bucket, which contains compromised sensitive information, and beginning the remediation process.

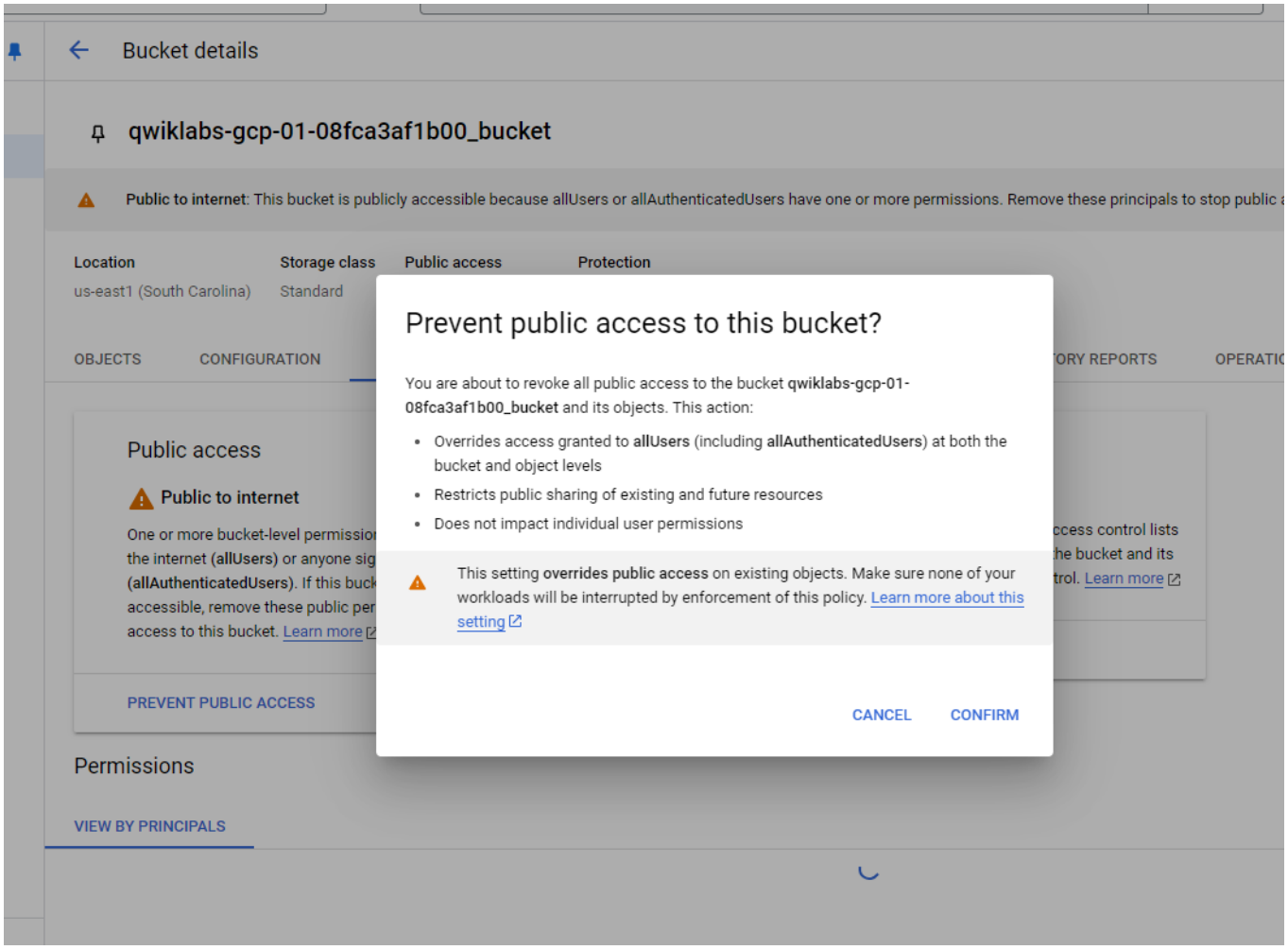


Figure 25 : Revoking public access to the storage bucket by selecting the "Prevent public access" option to safeguard the data.

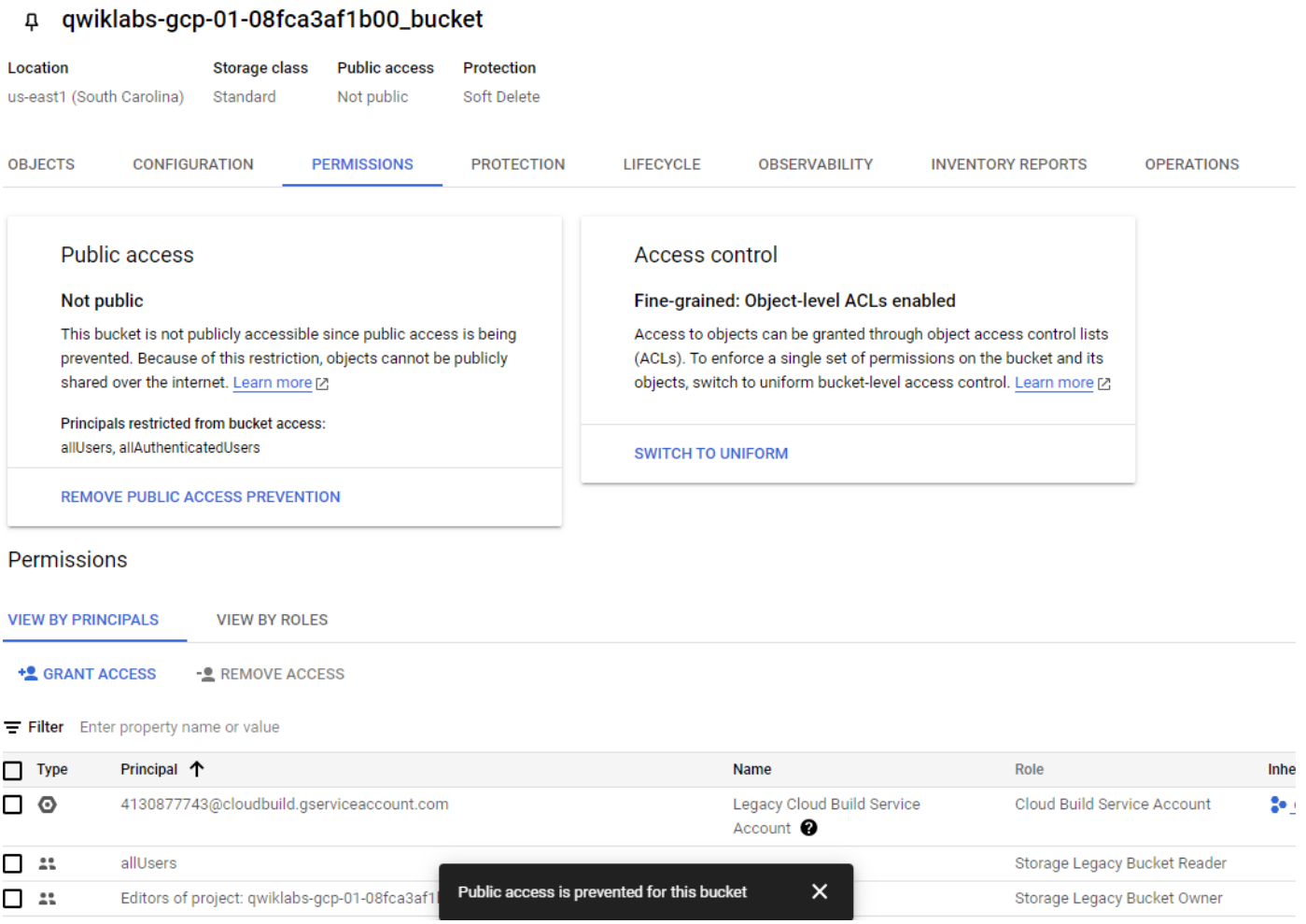


Figure 26 : Removing permissions for the allUsers principal from the bucket, enforcing strict access controls at the bucket level.

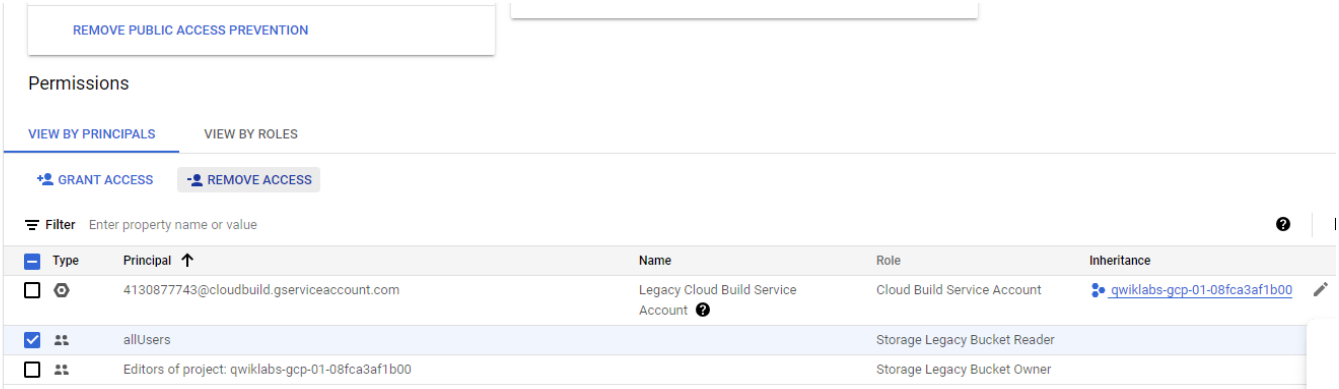


Figure 27 : Deleting the allUsers principal from the storage bucket, preventing unauthorized users from accessing bucket content.

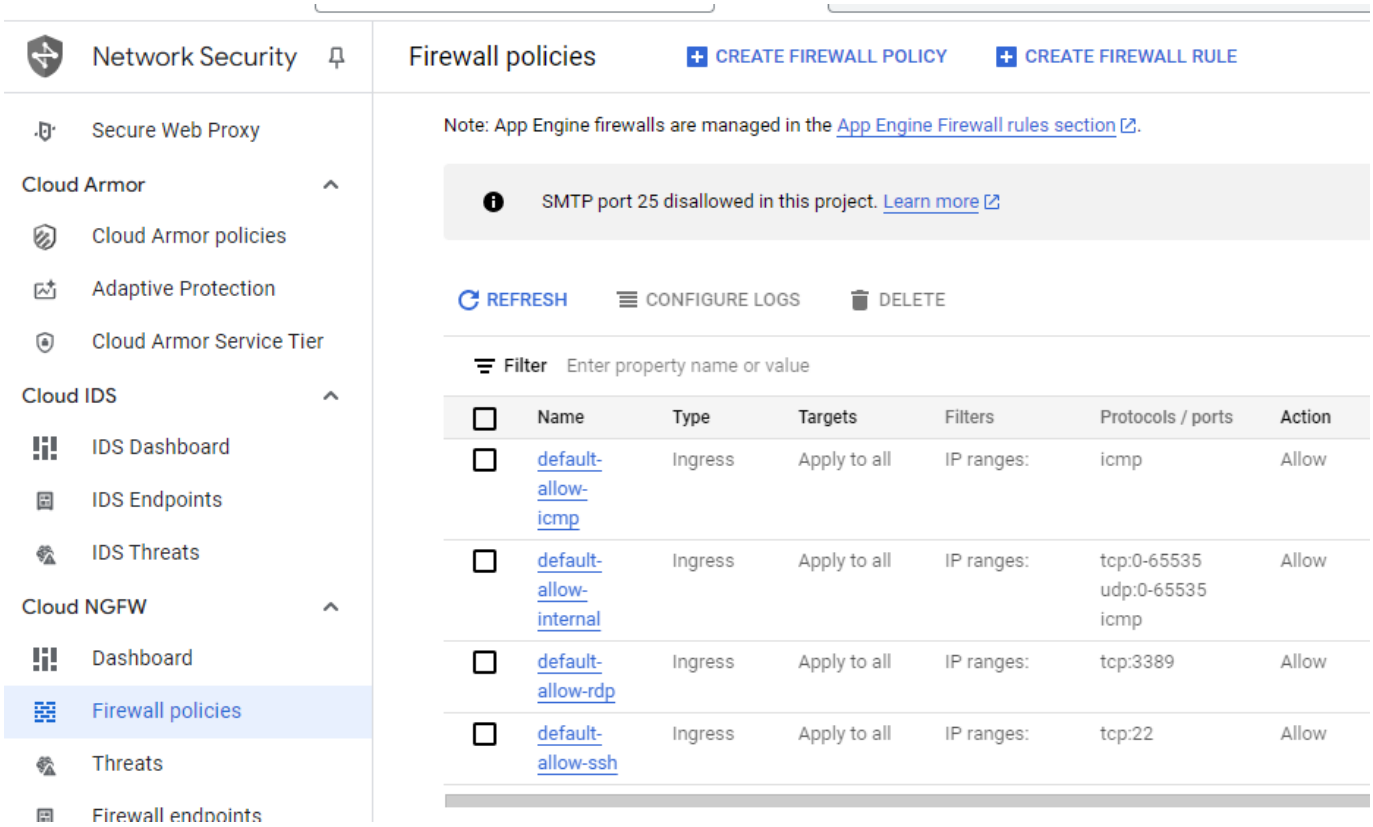


Figure 28 : Creating a new firewall rule to restrict access to authorized IP addresses and limit exposure of critical service..

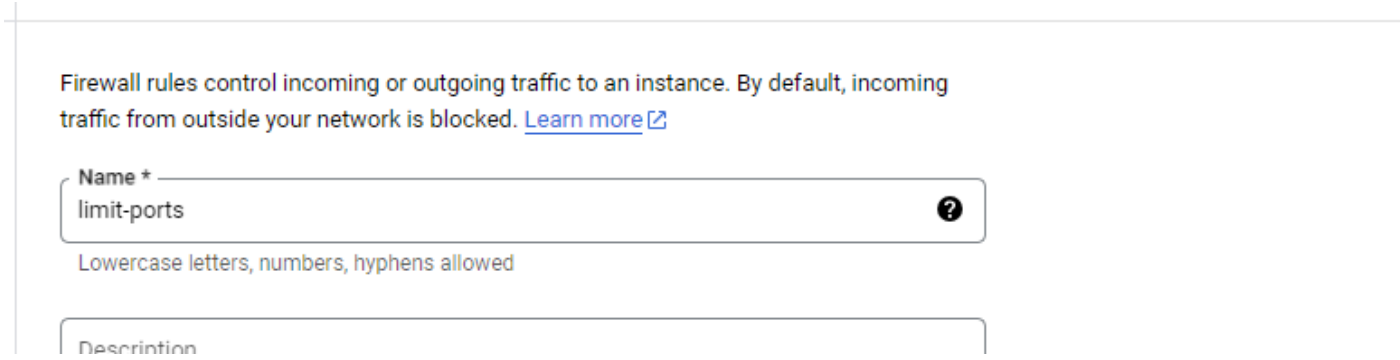


Figure 29 : Naming the firewall rule for easier identification and management in future compliance checks and audits.

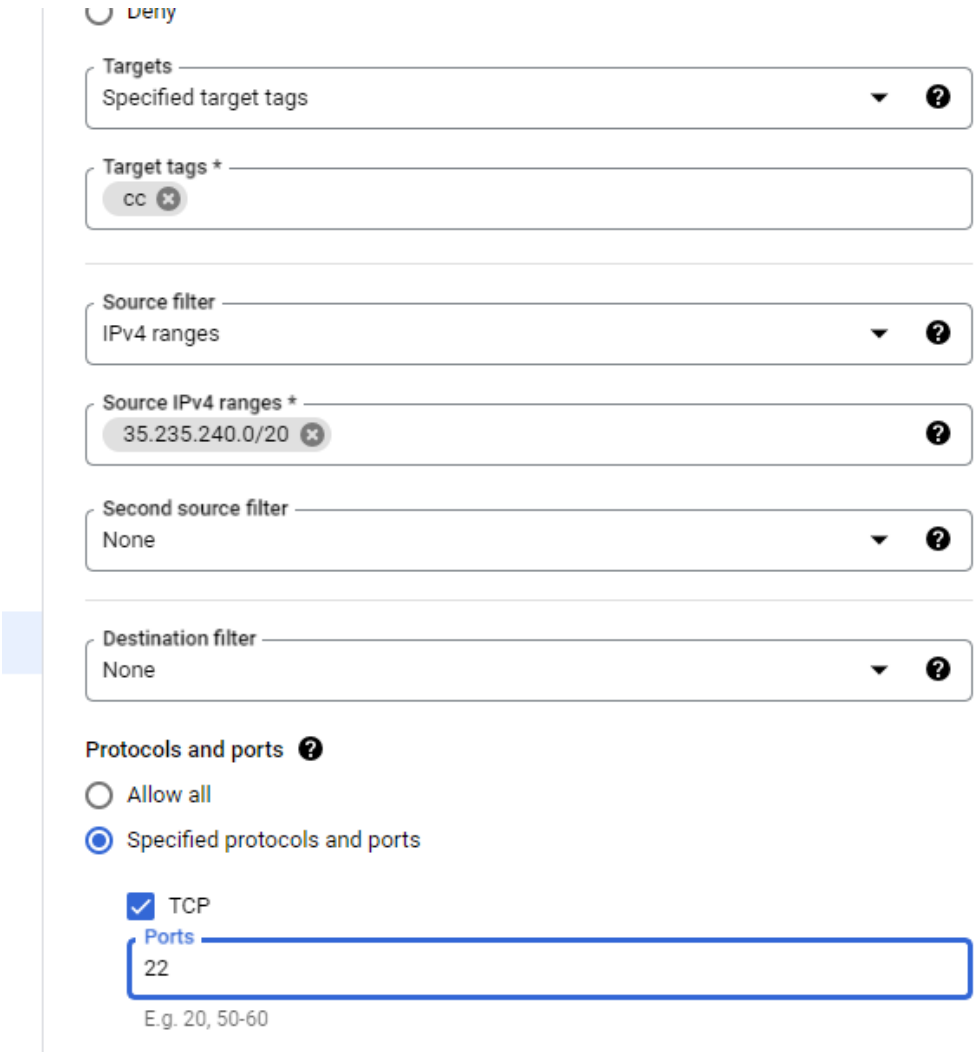


Figure 30 : Restricting SSH access to authorized IPs within the 35.235.240.0/20 range and applying it to instances with the tag 'cc'.

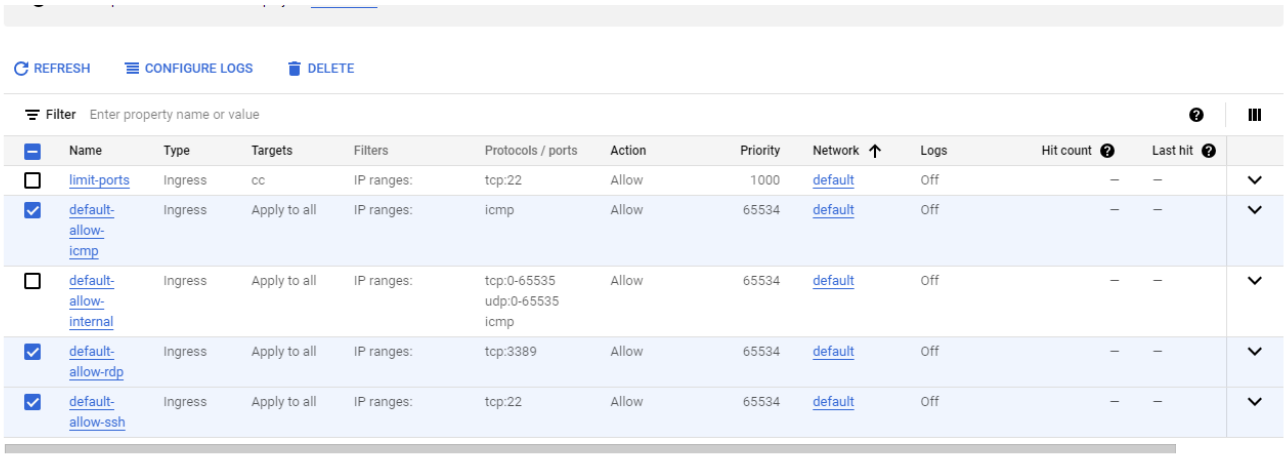


Figure 31 : Deleting the default-allow-icmp, default-allow-rdp, and default-allow-ssh firewall rules to close open ports that can be exploited..

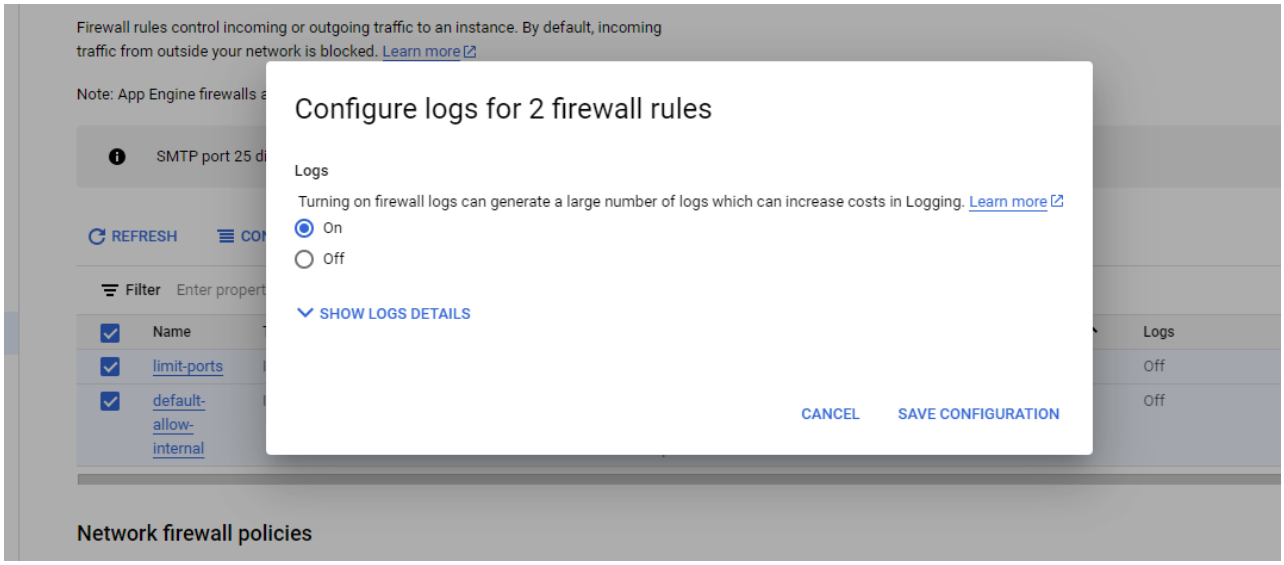


Figure 32 : Enabling logging for custom firewall rules to track network traffic and ensure compliance with security best practices.

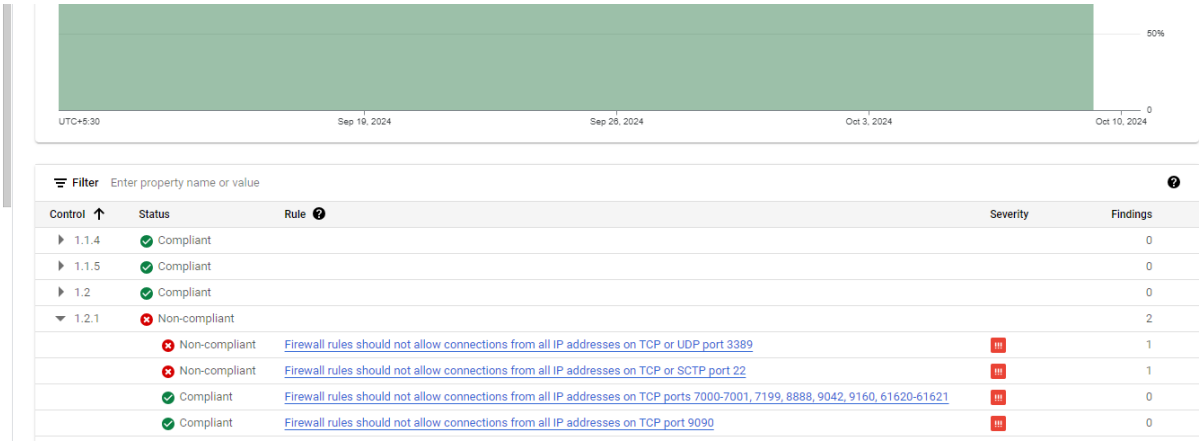


Figure 33 : Reviewing the updated compliance status in Google Cloud Security Command Center to verify that all findings have been addressed.

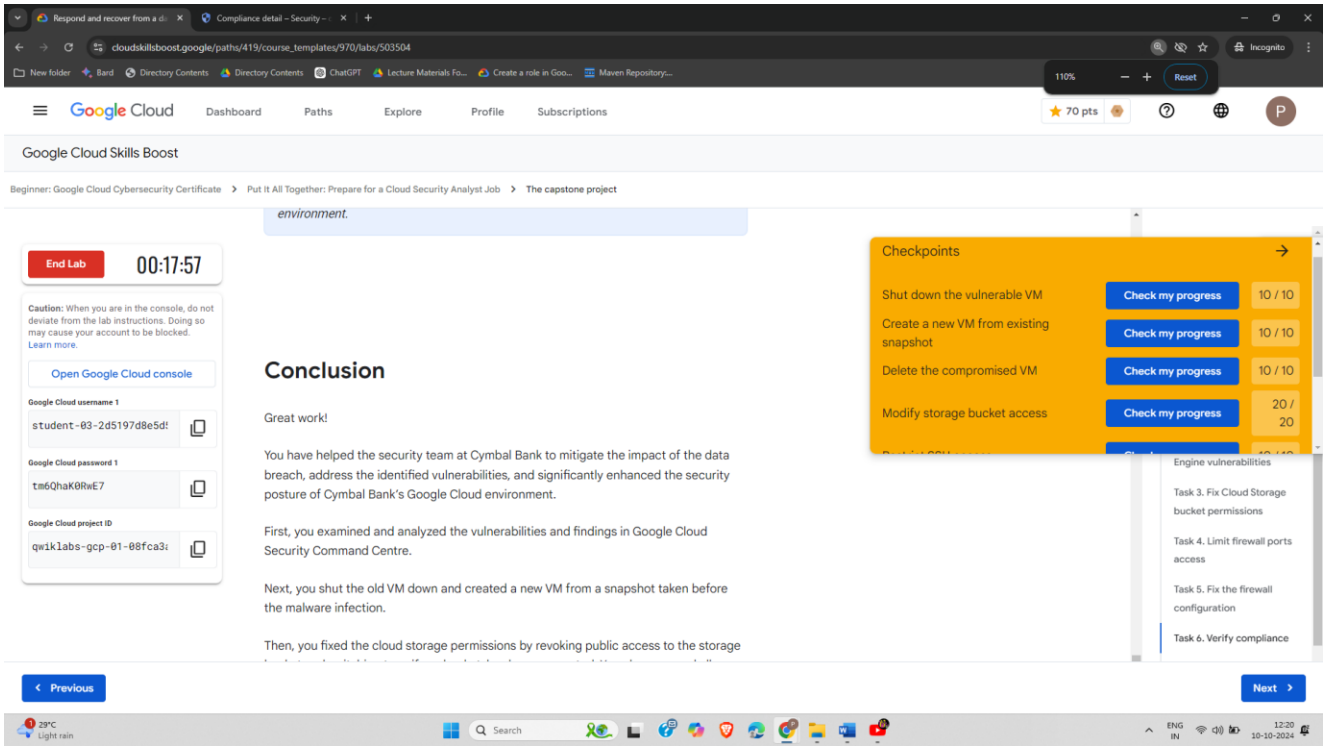


Figure 34 : completing the lab and verifying that all tasks, including remediation and compliance checks, were successful.

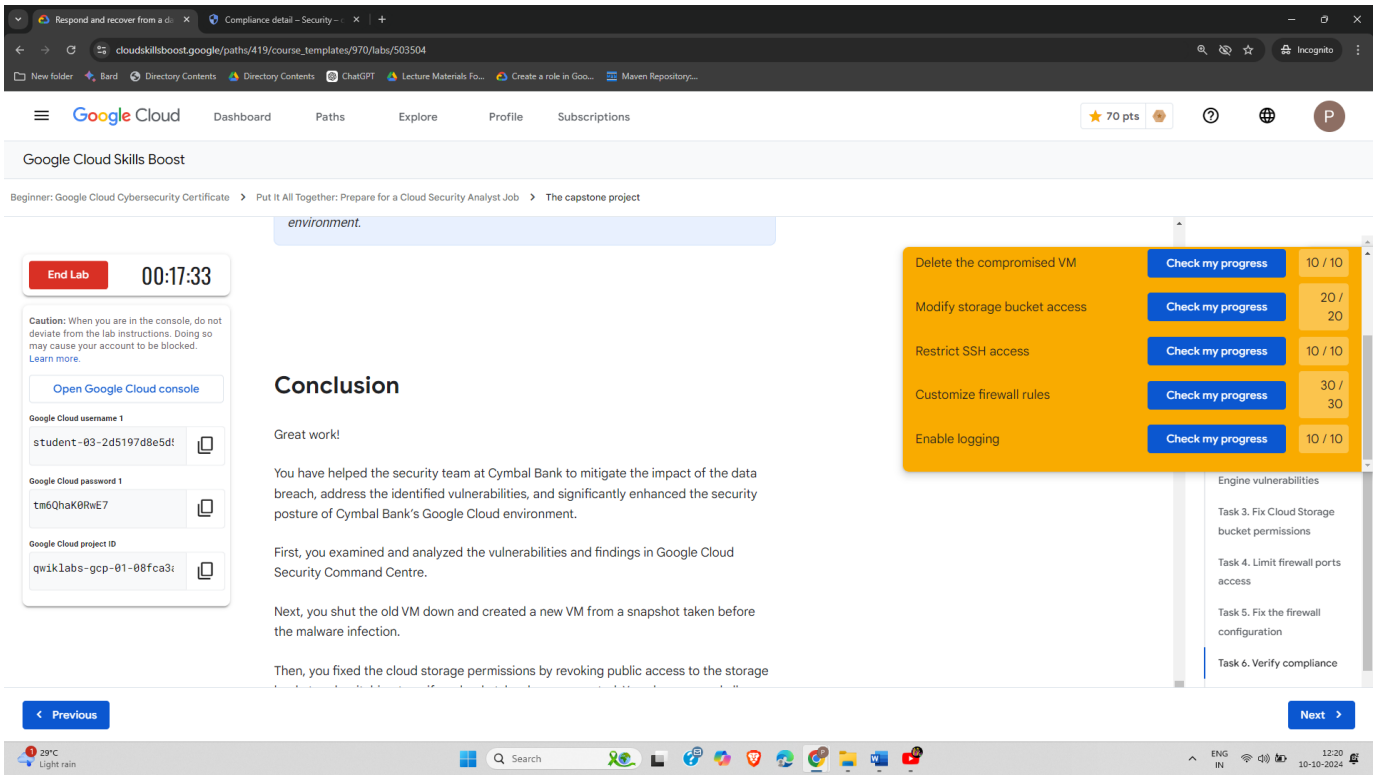


Figure 35 : completing the lab and verifying that all tasks, including remediation and compliance checks, were successful.

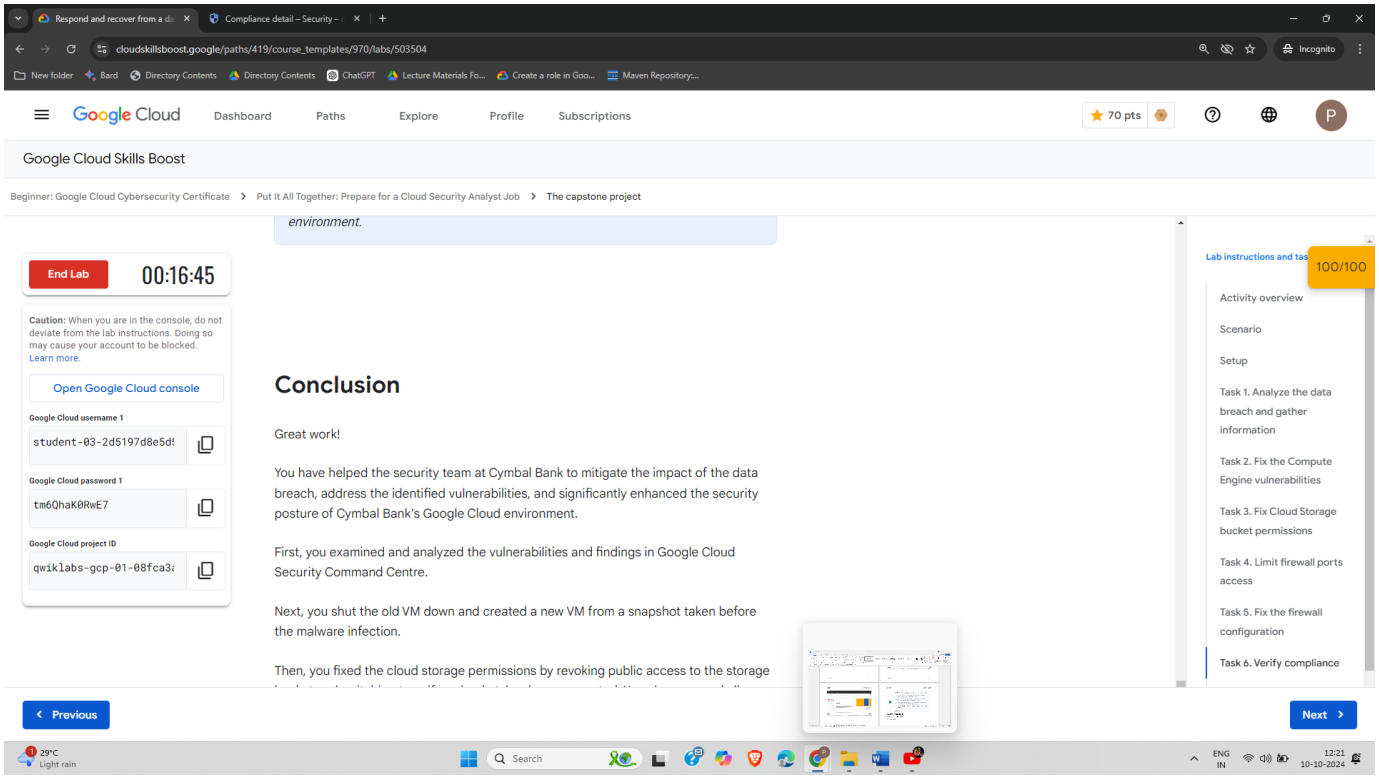


Figure 36 : completing the lab and verifying that all tasks, including remediation and compliance checks, were successful.

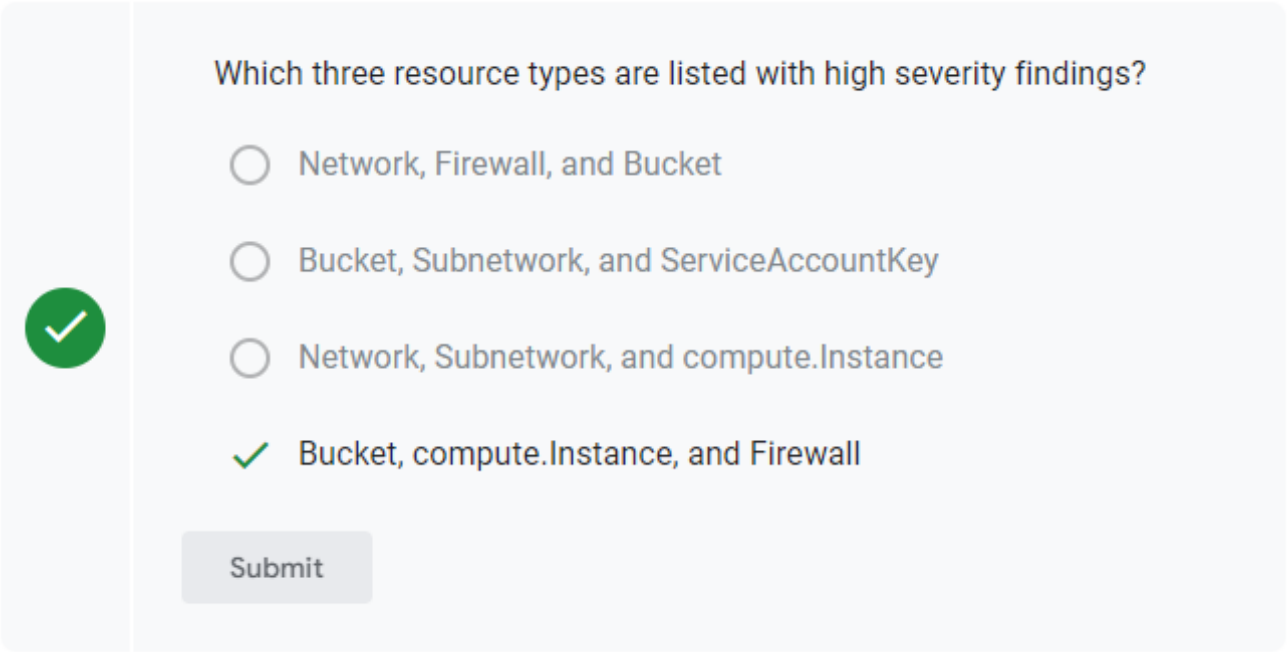


Figure 37 : MCQ

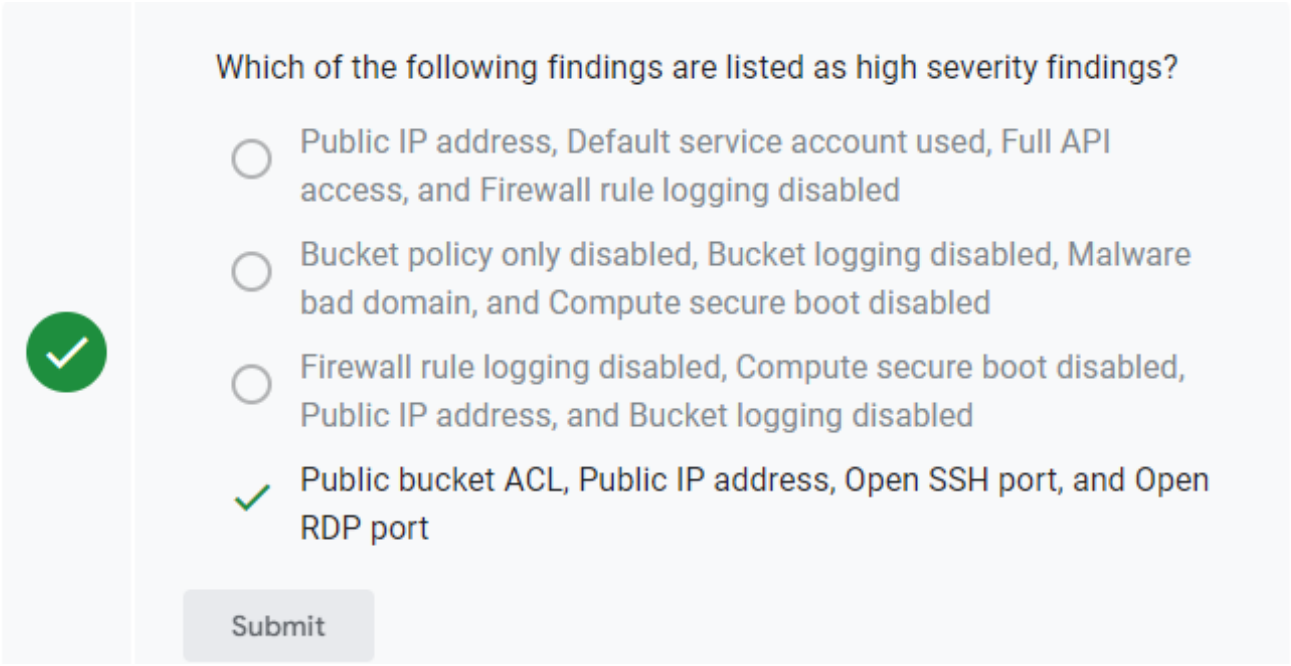


Figure 38 : MCQ

LATEST APPLICATIONS:

- Vulnerability detection and remediation using Google Cloud Security Command Center.
- Secure VM and network configuration through firewall rules and restricted access.
- Ensuring compliance with PCI DSS standards after a security breach.

LEARNING OUTCOME:

This practical demonstrated the process of detecting vulnerabilities, isolating compromised systems, and implementing security measures to safeguard cloud resources. The task also emphasized the importance of compliance with industry standards like PCI DSS to ensure organizational security.

REFERENCES:

- Google Cloud Security Command Center Documentation : https://cloud.google.com/security-command-center/docs
- PCI DSS 3.2.1 Compliance Standards :

https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf

- Firewall Configuration Best Practices :

https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/8-firewall-best-practices-for-securing-the-network/