

## 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:

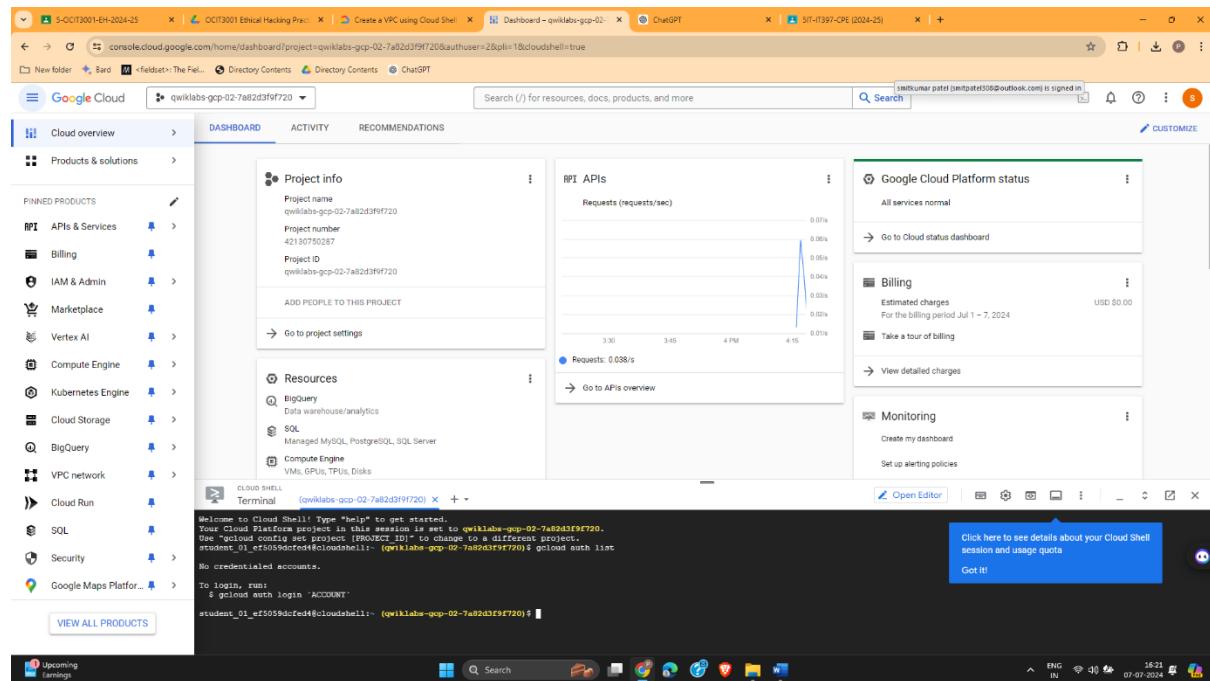


Figure 1: This figure shows the list of all authenticated Google Cloud accounts and indicates the currently active one.

```
student_01_ef5059dcfed4@cloudshell:~ (qwiklabs-gcp-02-7a82d3f9f720)$ gcloud compute networks create labnet --subnet-mode=custom
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.

What is the subnet mode of the labnet network you created?

- Auto
- None of these options
- Custom

**Submit**

Figure 5 MCQ which is in the lab section

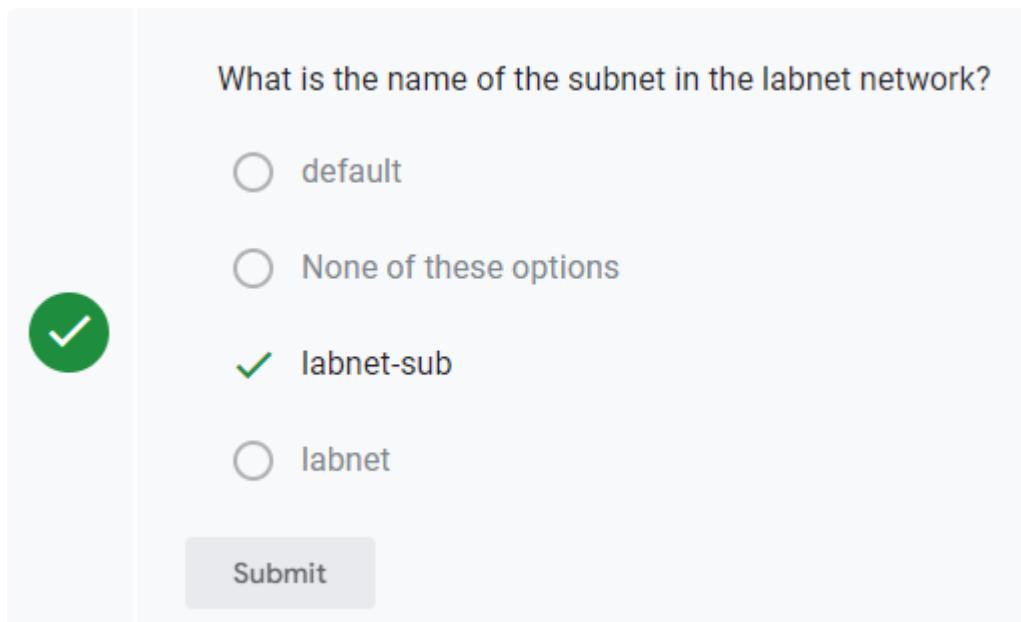


Figure 6 MCQ which is in the lab section

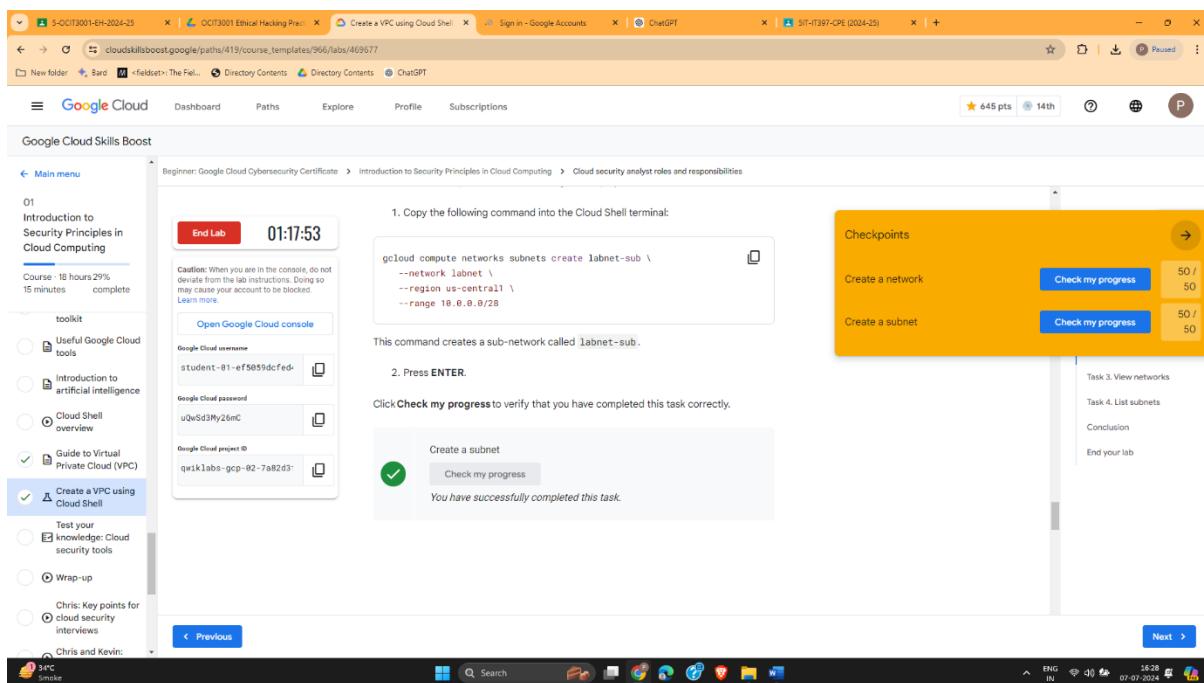


Figure 7 This figure shows the completion of my Google Cloud lab.

## 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 google: <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:

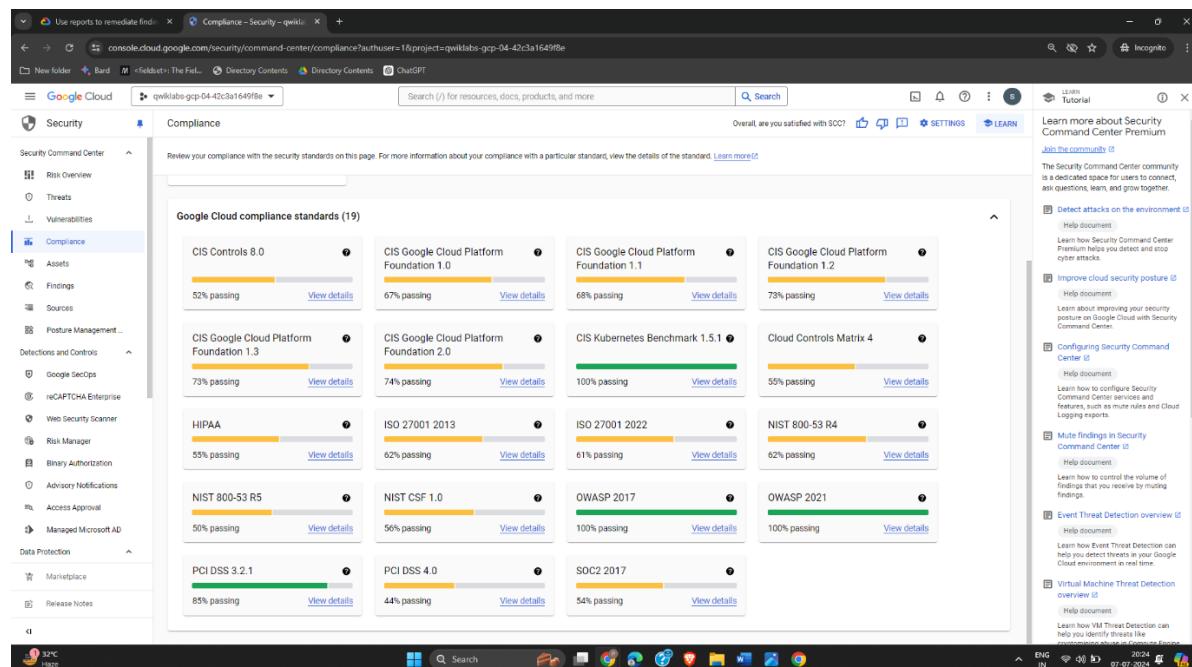


Figure 1 This figure shows that I click Compliance in the Security Command Center menu to open the Compliance page.

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.

**CIS Google Cloud Platform Foundation 2.0**  
Google Cloud

**74%**  
of controls passed (57 out of 77)      20 total findings

**Filter** Enter property name or value

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

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

Which of the following rules in the report have active findings for the Cloud Storage bucket? Select all that apply.

Bucket policy only should be Enabled

Cloud Storage buckets should not be anonymously or publicly accessible

Firewall rules should not allow connections from all IP addresses on TCP or SCTP port 22

VMs should not be assigned public IP addresses

**Submit**

Figure 4 MCQ IN LAB

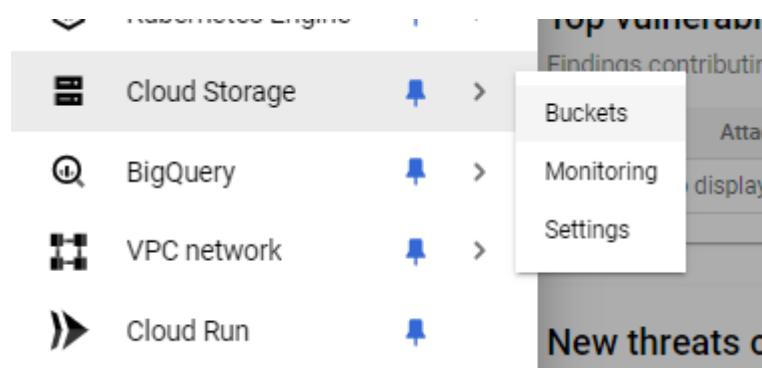


Figure 5 This figure shows that I navigate to Cloud Storage > Buckets from the Google Cloud console's Navigation menu.

Filter <a href="#">qwiklabs-gcp-04-42c3a1649f8e</a> Filter buckets									
Name	Created	Location type	Location	Default storage class	Last modified	Public access	Access control	Protection	Bucket retent
<a href="#">qwiklabs-gcp-04-42c3a1649f8e</a>	Jul 7, 2024, 7:15:47 PM	Region	us-east4	Standard	Jul 7, 2024, 7:15:49 PM	⚠️ Public to internet	Fine-grained	Soft Delete	None

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.

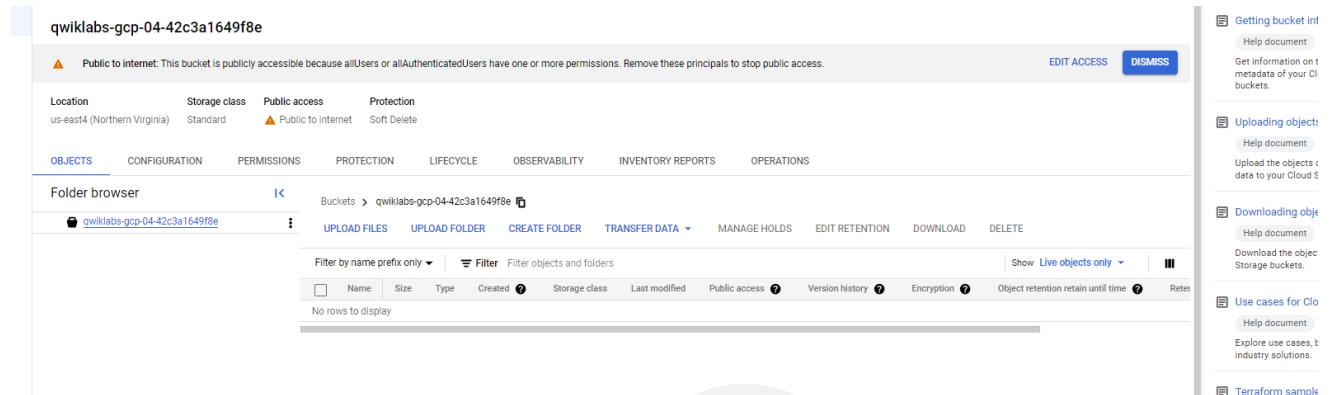


Figure 7 This figure shows that I click the Permissions tab to view all the permissions provided for the bucket.

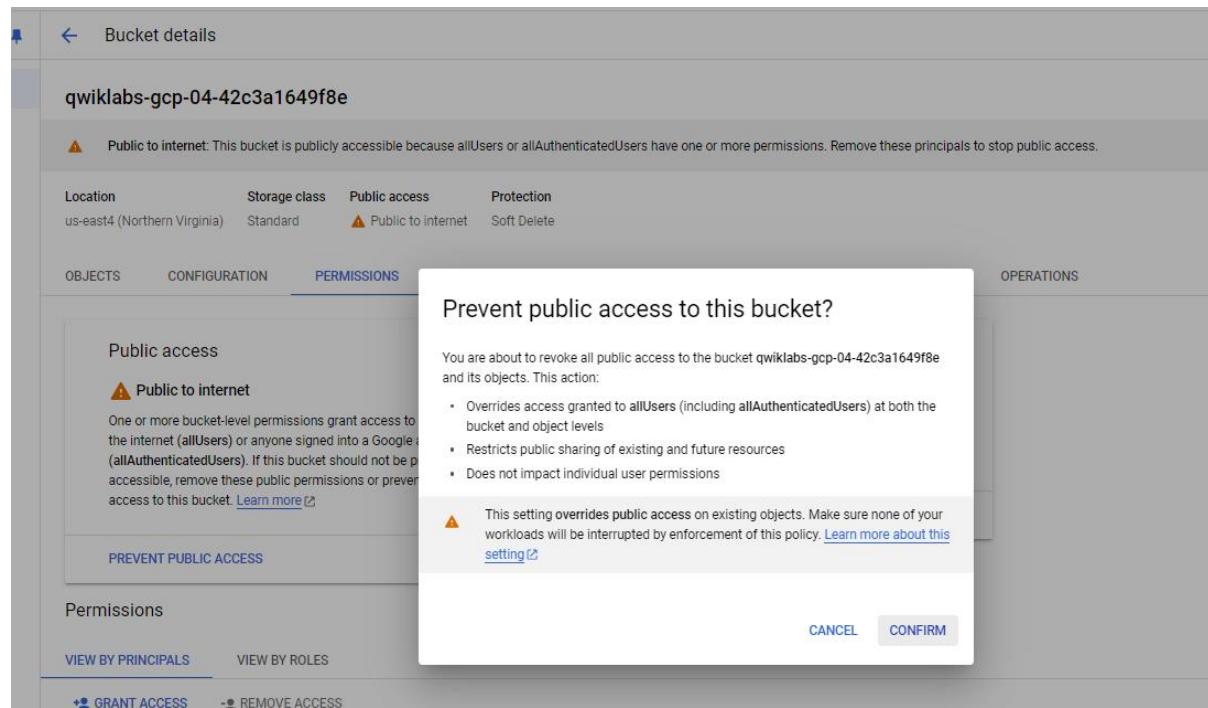


Figure 8 This figure shows that I remove the public access to the Cloud Storage bucket.

The screenshot shows the 'Permissions' section of the Google Cloud IAM interface. The 'VIEW BY ROLES' tab is active. Below it, there are two buttons: '+👤 GRANT ACCESS' and '-👤 REMOVE ACCESS'. A 'Filter' input field is present. A table lists roles and principals. The 'Storage Object Viewer' role is expanded, showing its members. The 'allUsers' member has a checked checkbox under 'REMOVE ACCESS'. A modal dialog titled 'Remove role from principal?' is displayed, asking if the user wants to remove the 'Storage Object Viewer' role from 'allUsers'. It contains two options: 'Remove allUsers from the role Storage Object Viewer on this resource.' (selected) and 'Remove allUsers from all roles on this resource. They may still have access via inherited roles.' At the bottom of the dialog are 'CANCEL' and 'REMOVE' buttons.

Role / Principal ↑	Name
<input type="checkbox"/> ▶ Cloud Build Service Account (1)	
<input type="checkbox"/> ▶ Cloud Build Service Agent (1)	
<input type="checkbox"/> ▶ Compute Engine Service Agent (1)	
<input type="checkbox"/> ▶ Storage Admin (1)	
<input type="checkbox"/> ▶ Storage Legacy Bucket Owner (2)	
<input type="checkbox"/> ▶ Storage Legacy Bucket Reader (1)	
<input type="checkbox"/> ▼ Storage Object Viewer (1)	
<input checked="" type="checkbox"/> allUsers	

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.

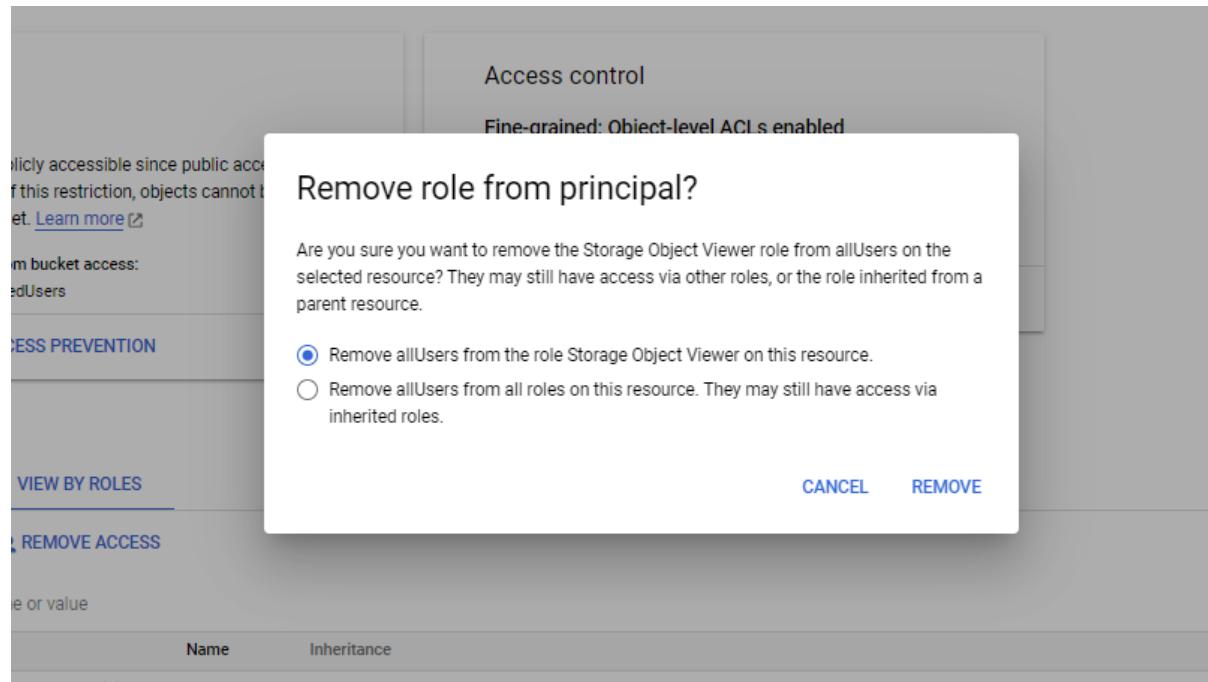


Figure 10 This figure shows that I confirm the removal of allUsers from the role Storage Object Viewer by ensuring the correct option is selected and clicking Remove.

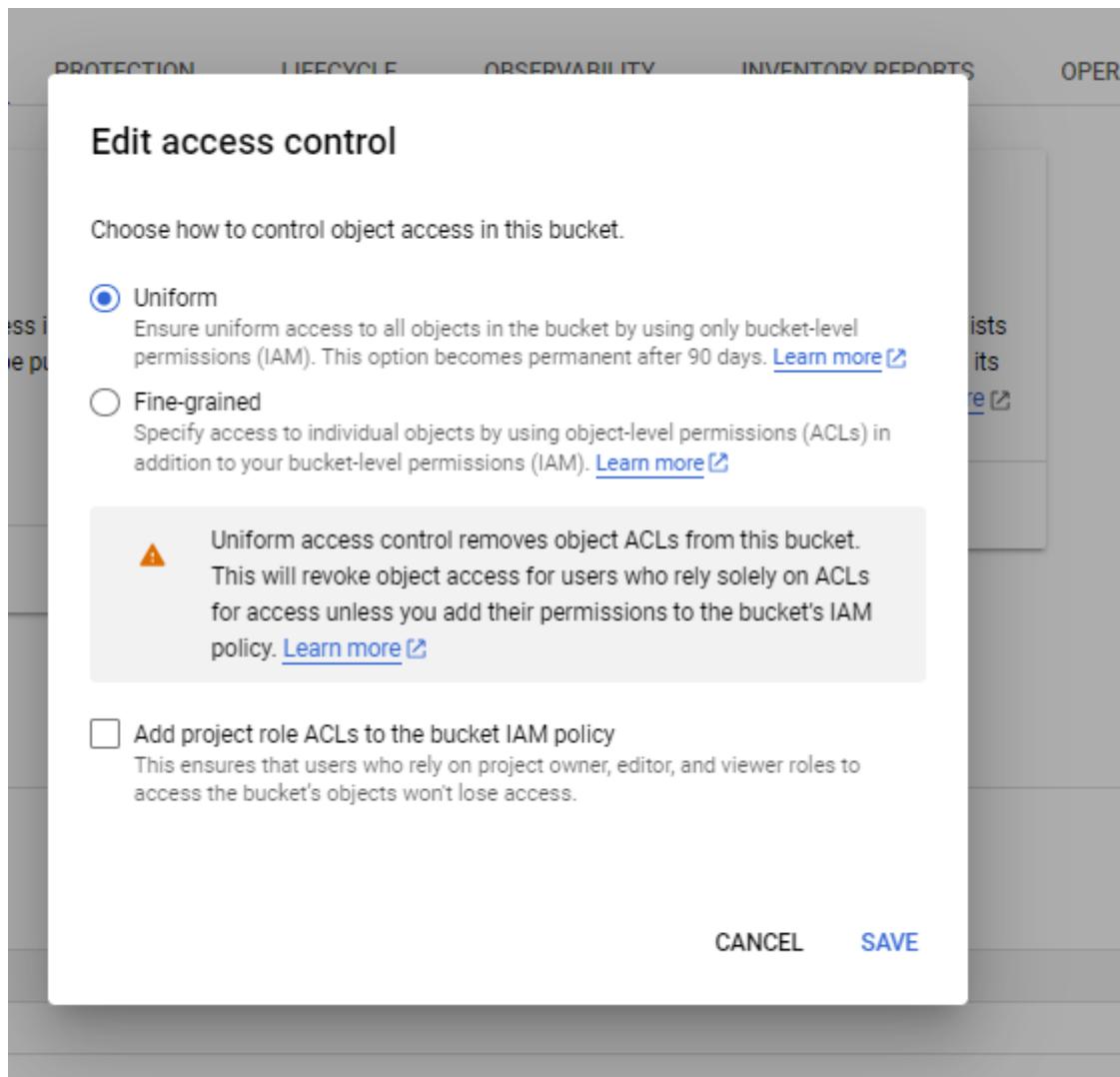


Figure 11 This figure shows that I select Uniform on the Edit access control dialog and click Save.

Muted findings are included in compliance reports

### CIS Google Cloud Platform Foundation 2.0

Google Cloud

**77%**  
of controls passed (59 out of 77)      18 total findings

Filter Enter property name or value

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.

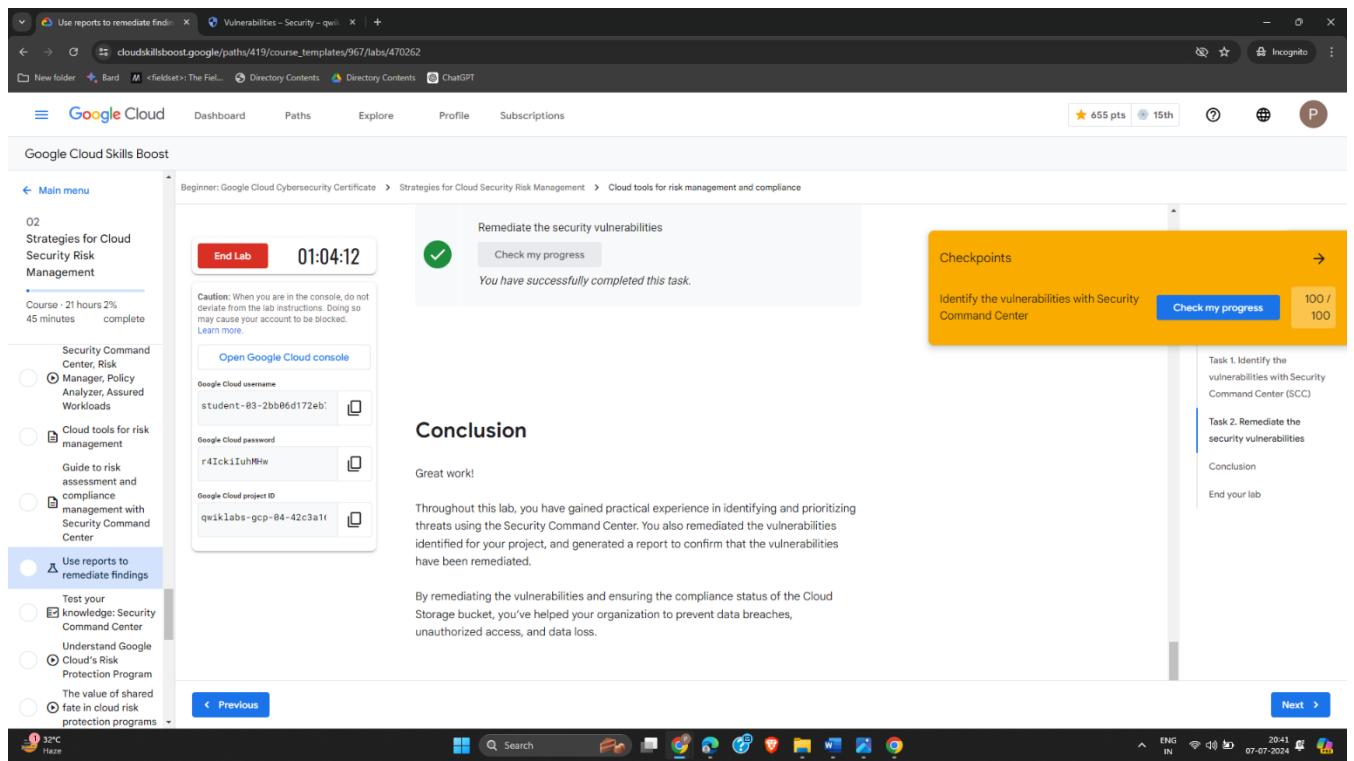


Figure 13 This figure shows the completion of my Google Cloud lab.

## 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:**

The screenshot shows the 'Create Role' dialog in the Google Cloud Platform (GCP) console. At the top, there is a dropdown menu showing 'qwiklabs-gcp-00-f4e74248d578' and a search bar. Below the title 'Create Role' is a descriptive text about custom roles. The form fields are as follows:

- Title \***: Audit Team Reviewer (19 / 100 characters)
- Description**: Created on: 2024-07-14 Custom role, allowing the audit team to conduct its review activities. This role grants read-only access to Firebase database resources. (160 / 256 characters)
- ID \***: CustomRole
- Role launch stage**: General Availability

Below the form is a section titled 'No assigned permissions' with a table header: **Filter** (with a placeholder 'Enter property name or value'), a question mark icon, and a help icon. The table has columns:  (checkbox), Permission (with an upward arrow), and Status. A message 'No rows to display' is shown. At the bottom of this section is a note: 'Some permissions might be associated with and checked by third parties. These permissions contain the third party's service and domain name in the permission prefix.' with an info icon.

At the very bottom are two buttons: **CREATE** (in blue) and **CANCEL**.

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

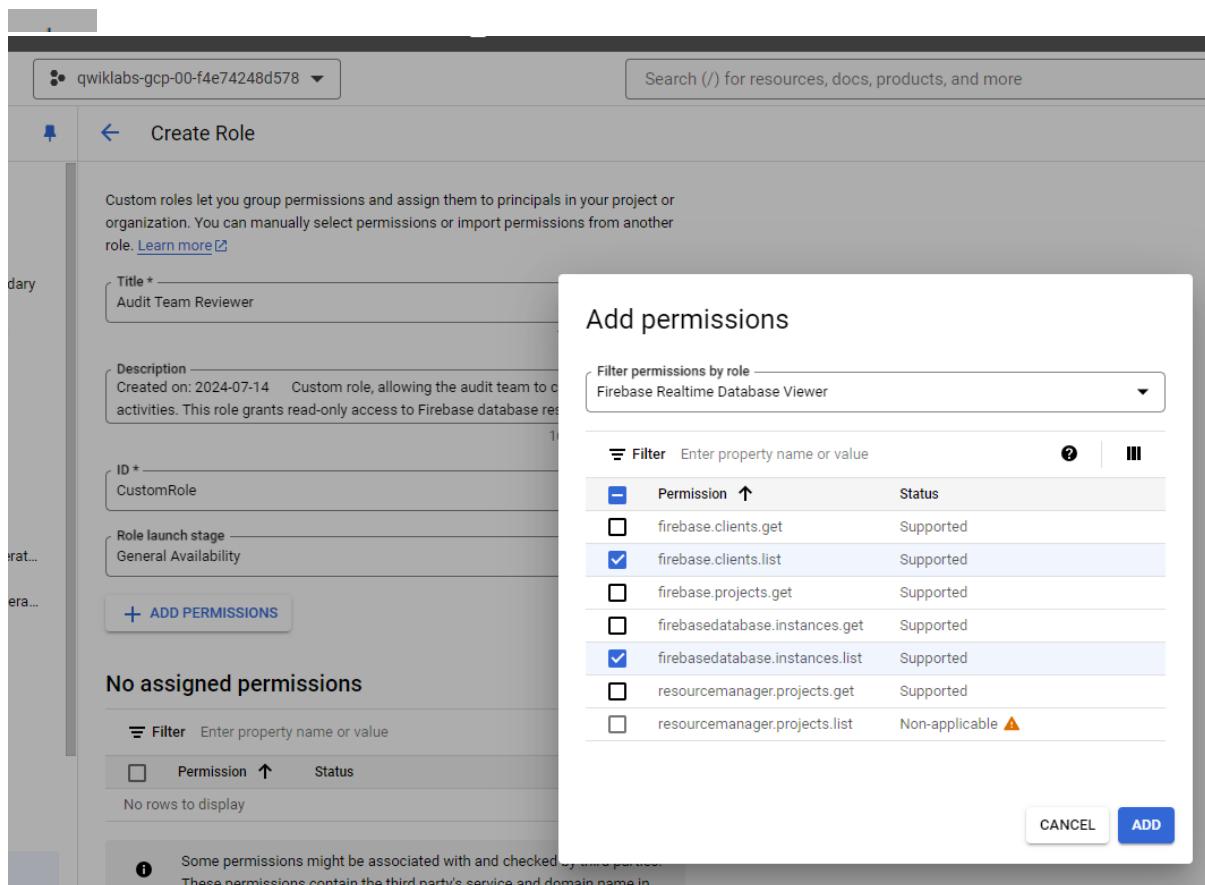


Figure 2 Screenshot of the Add permissions dialog with the Filter permissions by role field showing 'Firebase Realtime' and the Firebase Realtime Database Viewer checkbox selected and Add permissions dialog with the firebase.clients.list and firebasedatabase.instances.list checkboxes selected..

The screenshot shows the Google Cloud IAM interface for the project "qwiklabs-gcp-00-f4e74248d578". The left sidebar is titled "IAM & Admin" and includes options like PAM, Principal Access Boundary, Identity & Organization, Policy Troubleshooter, Policy Analyzer, Organization Policies, Service Accounts, Workload Identity Federation, Workforce Identity Federation, Labels, Tags, Settings, Privacy & Security, and Identity-Aware Proxy. The main panel is titled "IAM" and has tabs for "PERMISSIONS" (which is selected) and "RECOMMENDATIONS HISTORY". A sub-section titled "Permissions for project 'qwiklabs-gcp-00-f4e74248d578'" displays a message about permissions affecting all resources. Below this are two tabs: "VIEW BY PRINCIPALS" (selected) and "VIEW BY ROLES". Under "VIEW BY PRINCIPALS", there are "GRANT ACCESS" and "REMOVE ACCESS" buttons. A "Filter" input field is present. A table lists principals with their email addresses:

Type	Principal
<input type="checkbox"/>	198095636530-compute@developer.gserviceaccount.com
<input type="checkbox"/>	admiral@qwiklabs-services-prod.iam.gserviceaccount.com
<input type="checkbox"/>	qwiklabs-gcp-00-f4e74248d578@qwiklabs-gcp-00-f4e74248d578.iam.gserviceaccount.com
<input type="checkbox"/>	student-01-00f2a756dd24@qwiklabs.net

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

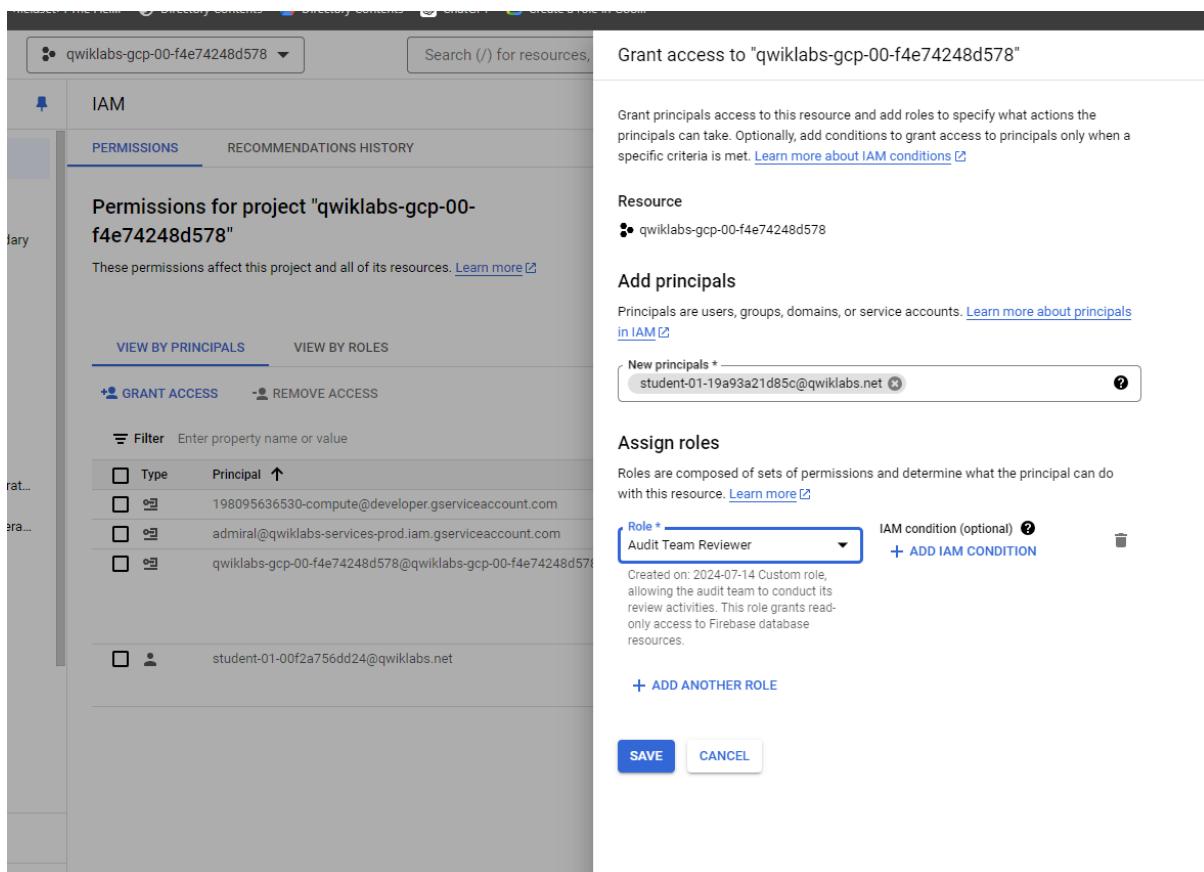


Figure 4 Screenshot of the Grant access dialog with the New principals field filled in with Google Cloud username 2 and the Select a role drop-down menu with Custom and Audit Team Reviewer selected.

The interface includes a timer at the top right (01:10:31), a red 'End Lab' button, and a 'Caution' message about not deviating from lab instructions. On the left, there's a 'Open Google Cloud console' button and a form for entering Google Cloud credentials: 'Google Cloud username 1' (student-01-00f2a756dd24), 'Google Cloud password' (SWdGv40jSj62), 'Google Cloud username 2' (student-01-19a93a21d85c), and 'Google Cloud project ID' (qwiklabs-gcp-00-f4e74248d578). On the right, a multiple-choice question asks 'Which role has been granted to the user?' with four options: 'BigQuery Admin' (radio button), 'Audit Team Reviewer' (radio button, checked with a green checkmark), 'Storage Admin' (radio button), and 'Pub/Sub Admin' (radio button). A 'Submit' button is at the bottom right of the MCQ section.

Figure 5 MCQ and credential

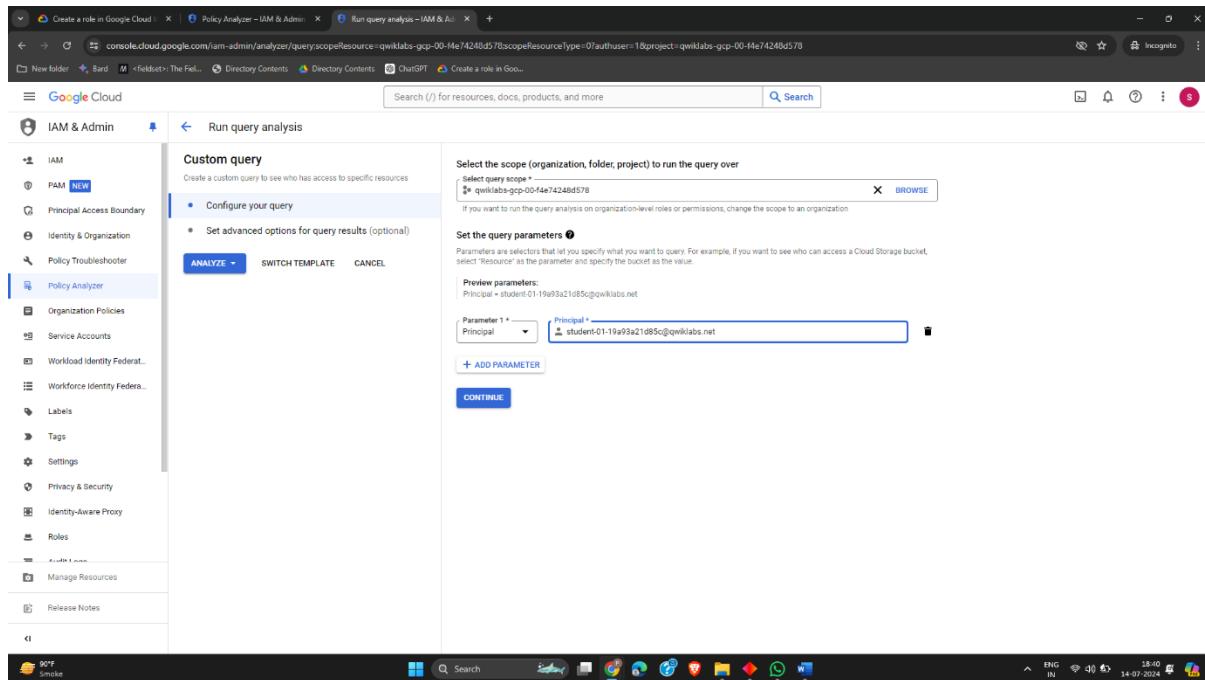


Figure 6 Screenshot of the Analyze policies section with the List resources within resource(s) matching your query checkbox selected and the Analyze button highlighted.

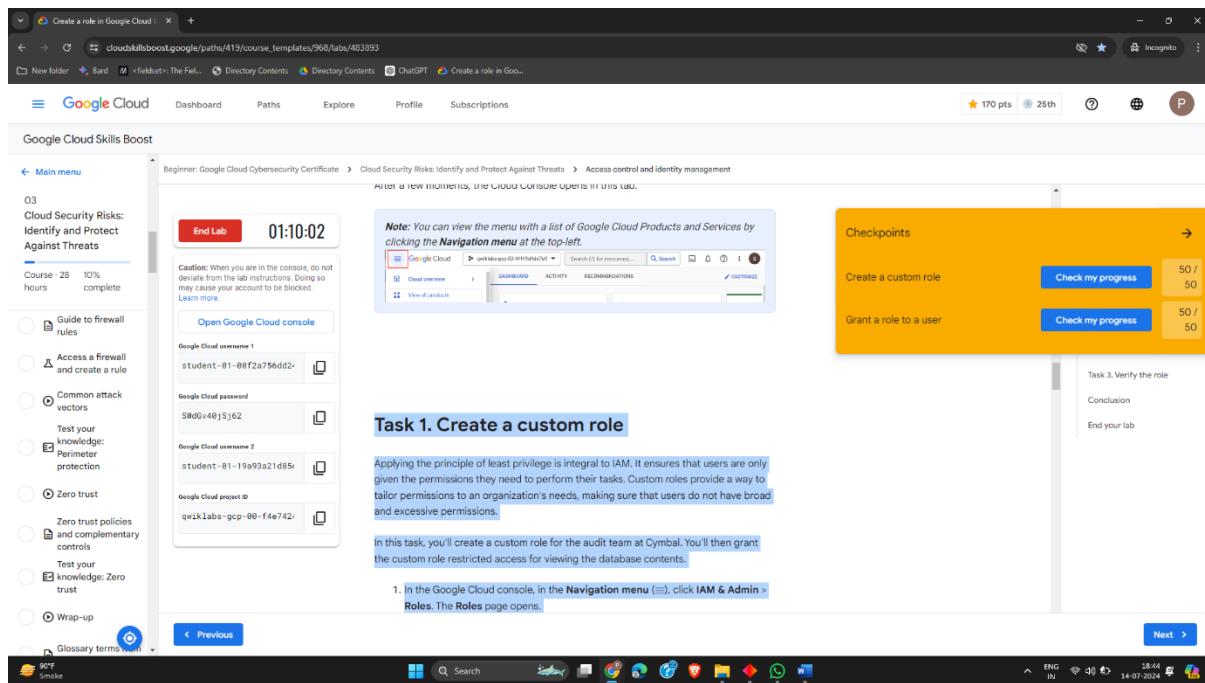


Figure 7 Screenshot of completing the task

## 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](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.

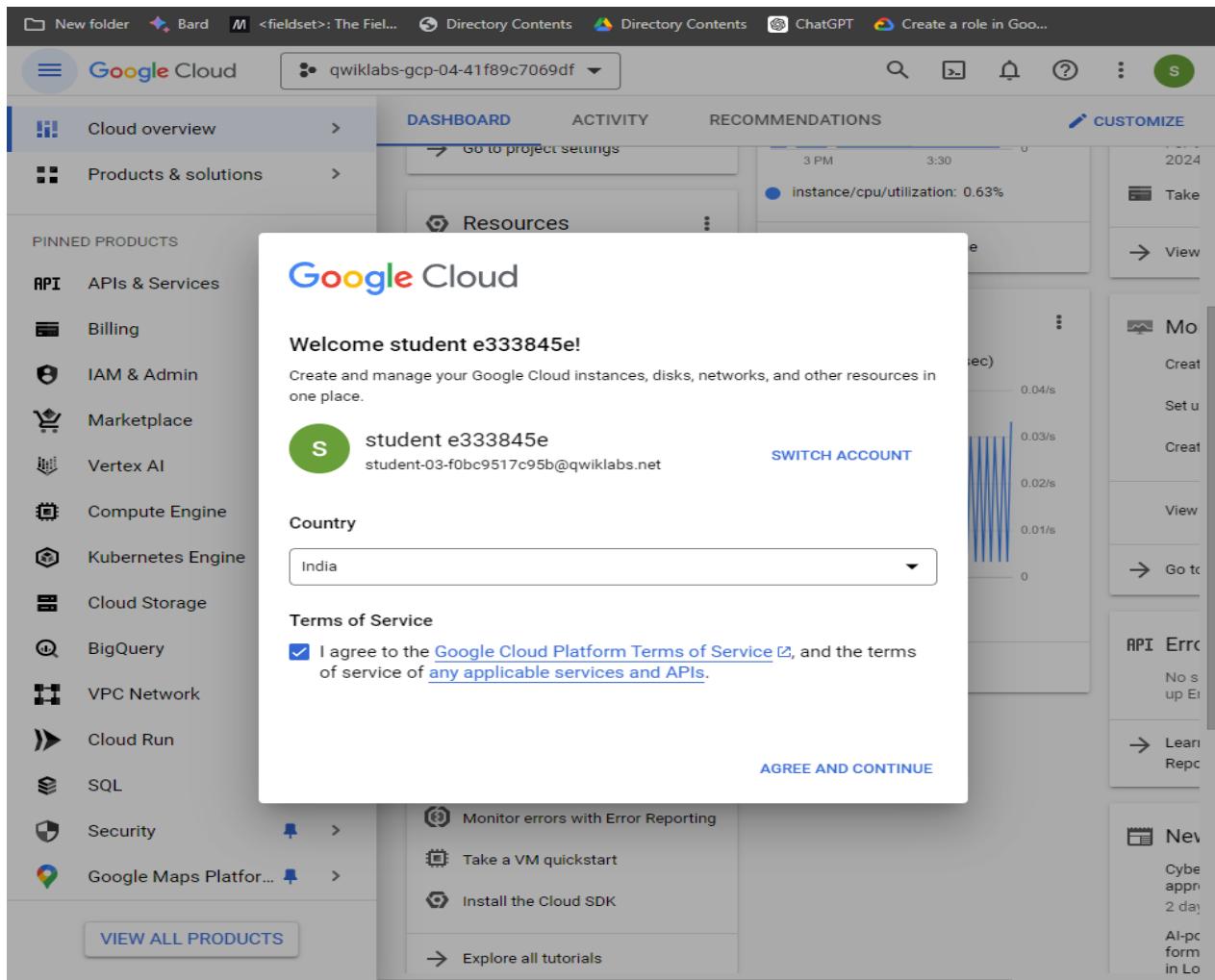
**OUTPUT:**

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

The screenshot shows the Google Cloud Network Security interface. On the left, there's a sidebar with various security components: Secure Web Proxy, Cloud Armor, Adaptive Protection, Cloud Armor Service Tier, Cloud IDS, Cloud NGFW, Firewall policies (which is selected and highlighted in blue), Threats, Firewall endpoints, Common components (Address groups, Security profiles, TLS inspection policies, SSL policies), and a section for Cloud Monitoring.

The main area is titled "Create a firewall rule". It contains several configuration fields:

- Name \***: allow-http-ssh (with a note: "Lowercase letters, numbers, hyphens allowed")
- Description**: (empty text area)
- Logs**: A note about logging costs, with options "On" (selected) and "Off".
- SHOW LOGS DETAILS** button
- Network \***: vpc-net
- Priority \***: 1000 (with a "COMPARE" link and a note: "Priority can be 0 - 65535")
- Direction of traffic**: Ingress (selected)
- Action on match**: Allow (selected)
- Targets**: Specified target tags (with a note: "Targets can be instances, groups, or subnets")
- Target tags \***: http-server (with a delete icon)

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

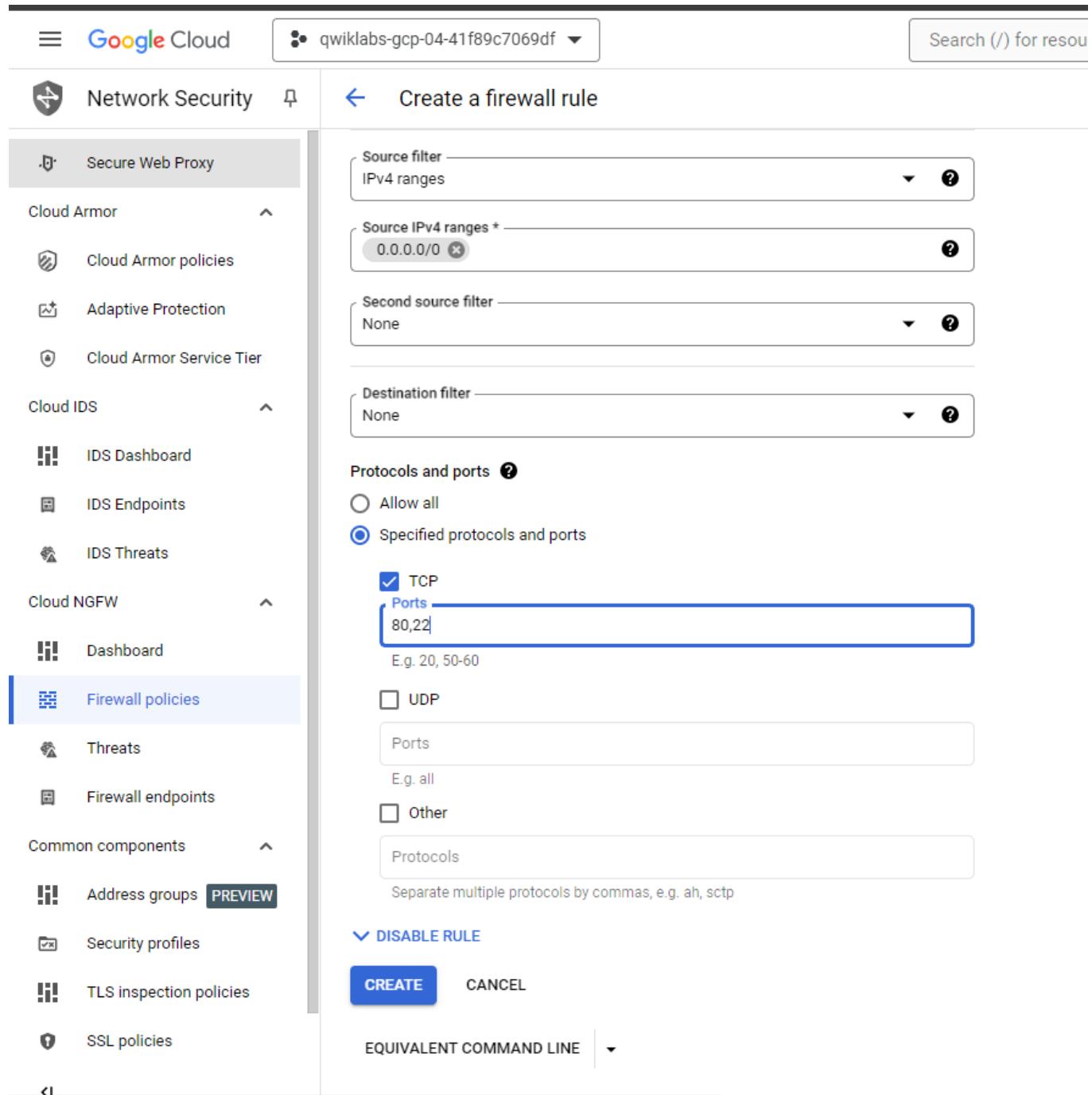


Figure 3 : Create a firewall rule dialog with specified settings.

**Left Panel (Google Cloud Form):**

- End Lab button
- 01:27:12 timer
- Caution message: "When you are in the console, do not delete from the lab instructions. Doing so may cause your account to be blocked." (with a "Learn more" link)
- Google Cloud username: student-03-f0bc9517c951
- Google Cloud password: raf7KcvitZot
- Google Cloud project ID: qwiklabs-gcp-04-41f89c

**Central Panel (whatismyip.com Screenshot):**

- In the Google Cloud console, click the Navigation menu (≡).
- Select Compute Engine > VM instances. The VM instances page opens.
- For web-server, click on the External IP link to access the server.
- (Alternatively, you can add the External IP value to [http://EXTERNAL\\_IP/](http://EXTERNAL_IP/) in a new browser window or tab.) A default web page should display.

**Right Panel (Checkpoints Summary):**

Action	Status	Progress
Create a firewall rule	Check my progress	25 / 25
Generate HTTP network traffic	Check my progress	0 / 25
Create a deny firewall rule	Check my progress	0 / 25
Analyze the firewall logs	Check my progress	0 / 25

Notes:

- server Flow Logs
- Task 4. Create a firewall rule to deny HTTP traffic
- Task 5. Analyze the firewall logs
- Conclusion
- End your lab

**Note:** Ensure that the IP address only contains numerals (IPv4) and is not

Figure 4 : Task 1 Completion Verification.

**Google Cloud Compute Engine VM Instances Page:**

- VM instances tab selected.
- INSTANCE FILTER: Status (Status), Name (Name ↑), Zone (Zone), Recommendations (Recommendations), In use by (In use by), Internal IP (Internal IP), External IP (External IP), Connect (Connect).
- Instance details for 'web-server':
 

Status: up	Name: web-server	Zone: us-east1-b	Internal IP: 10.1.3.2 (nic0)	External IP: 35.237.79.55 (nic0)	Connect: SSH
------------	------------------	------------------	------------------------------	----------------------------------	--------------
- Related actions:
  - Explore Backup and DR (NEW): Back up your VMs and set up disaster recovery.
  - Monitor VMs: View outlier VMs across metrics like CPU and network.
  - Explore VM logs: View, search, analyze, and download VM instance logs.
  - Set up firewall rules: Control traffic to and from a VM instance.
  - Patch management: Schedule patch updates and view patch compliance on VM instances.
  - Load balance between VMs: Set up Load Balancing for your applications as your traffic and users grow.

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

The screenshot shows a Google Cloud Skills Boost lab interface. On the left, there's a sidebar with 'End Lab' and a timer at 01:25:19. Below it are input fields for 'Google Cloud username' (student-03-f0bc9517c951), 'Google Cloud password' (raif7Kcv1tZot), and 'Google Cloud project ID' (qwiklabs-gcp-04-41f89c). A note cautions against deviating from lab instructions. In the center, a browser window shows whatismyip.com with the IP address 59. To the right, a yellow 'Checkpoints' panel lists five tasks: 'Create a firewall rule' (25/25), 'Generate HTTP network traffic' (25/25), 'Create a deny firewall rule' (0/25), and 'Analyze the firewall logs' (0/25). At the bottom, there are links for 'Task 4. Create a firewall rule to deny HTTP traffic', 'Task 5. Analyze the firewall logs', 'Conclusion', and 'End your lab'.

Figure 6 : Task 2 Completion Verification.

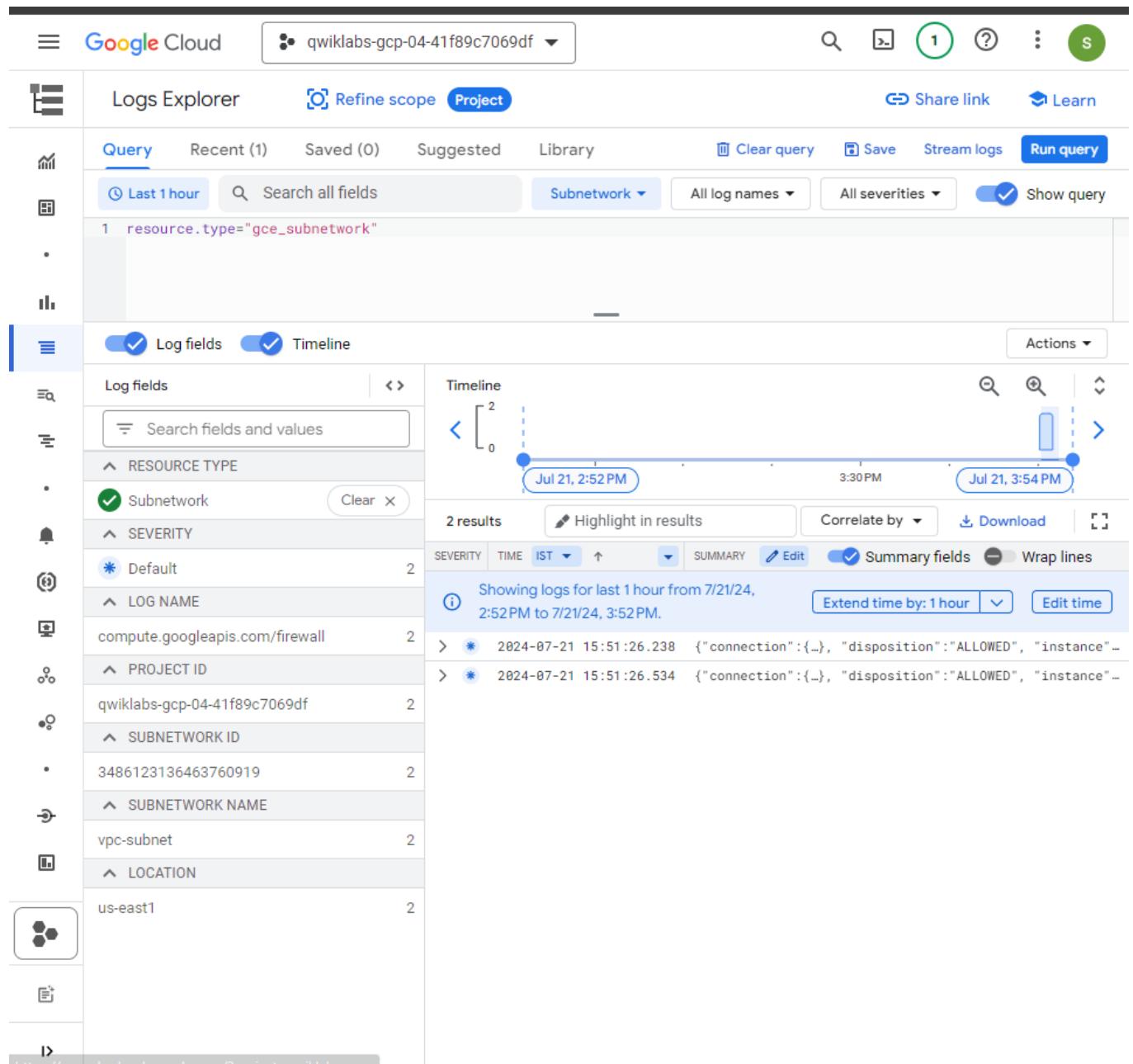


Figure 7 : Log fields pane showing the selection of `compute.googleapis.com/vpc_flows` for accessing VPC Flow logs.

The screenshot shows the 'Create a firewall rule' dialog in the Google Cloud Platform. The left sidebar lists various network-related icons. The main form fields are as follows:

- Name \***: deny-http (with a note: "Lowercase letters, numbers, hyphens allowed")
- Description**: (empty text area)
- Logs**:
  - Turning on firewall logs can generate a large number of logs which can increase costs in Logging. [Learn more](#)
  - On
  - Off
- SHOW LOGS DETAILS**:
  - Network \***: vpc-net
  - Priority \***: 1000 (with a note: "Priority can be 0 - 65535")
  - Direction of traffic**:  Ingress
  - Action on match**:  Deny
  - Targets**: Specified target tags
  - Target tags \***: http-server

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

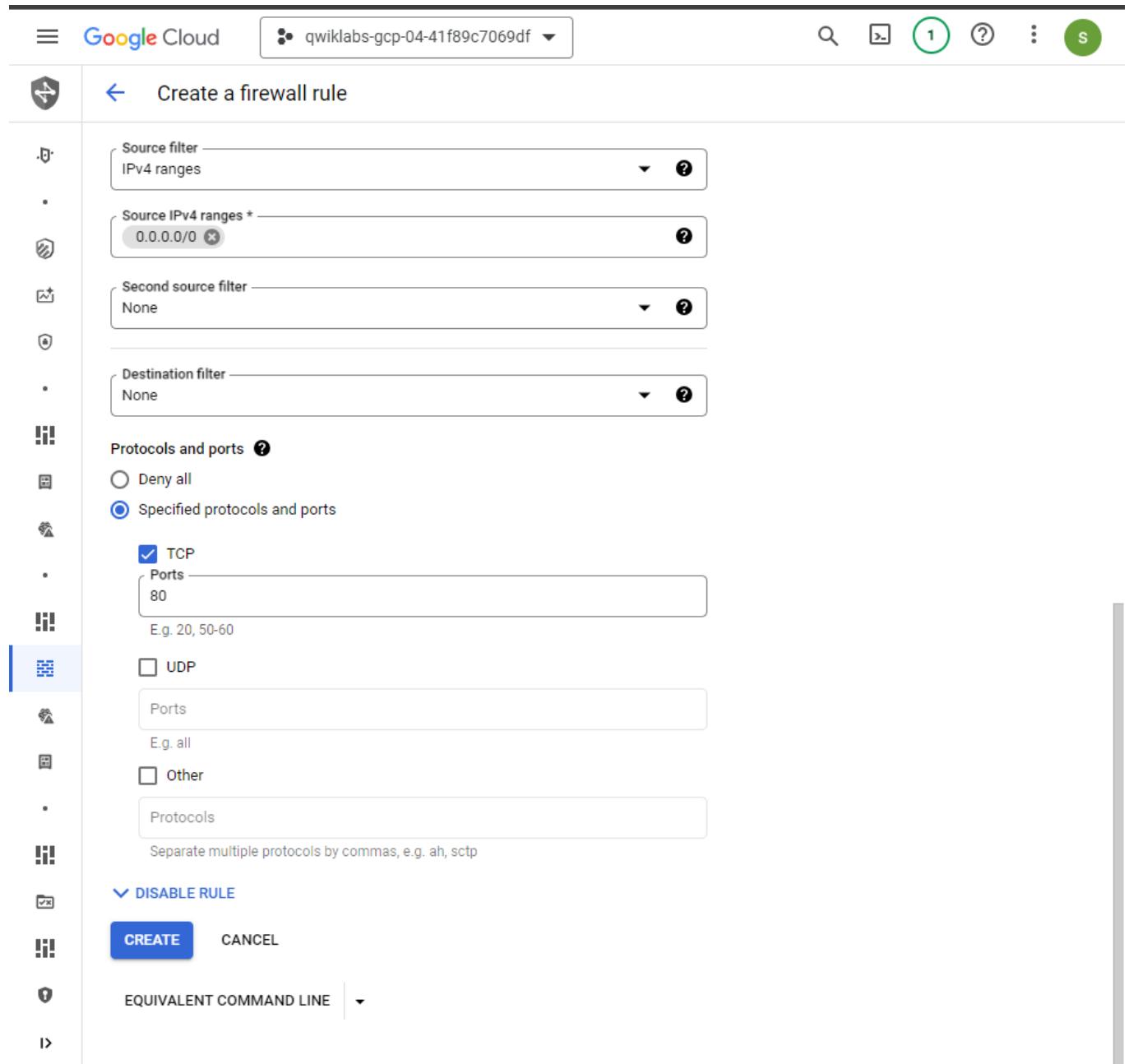


Figure 9 : Create a firewall rule dialog with the Create button highlighted to finalize the creation of the rule.

The screenshot shows a Google Cloud Skills Boost interface. On the left, there's a sidebar with 'End Lab' and a timer at 01:19:17. Below it are fields for 'Google Cloud username' (student-03-f0bc9517c951), 'Google Cloud password' (raf7Kcv1tZot), and 'Google Cloud project ID' (qwiklabs-gcp-04-41f89c). A 'Caution' message at the top of the sidebar advises against deviating from lab instructions. The main content area displays a log entry: "a random port number between 49152-65535." It asks, "After analyzing the details of this log entry, you should notice that the network traffic you generated (on HTTP port 80) was allowed due to the firewall rule **allow-http-ssh** you created previously. This rule allowed incoming traffic on ports 80 and 22." To the right is a multiple-choice question: "According to the log entries, what is the IP address of the web server?" with options 127.0.0.1, 0.0.0.0, 10.1.3.2 (selected), and 255.255.255.255. A 'Submit' button is at the bottom.

Figure 10 : MCQ

The screenshot shows the same Google Cloud Skills Boost interface. The sidebar now shows a timer at 01:19:07 and the same user information. The main content area displays a table of a firewall rule configuration:

Action on match	Deny
Targets	Specified target tags
Target tags	http-server
Source filter	IPv4 ranges
Source IPv4 ranges	0.0.0.0
In the Protocols and ports section	<ul style="list-style-type: none"> <li>Select Specified protocols and ports</li> <li>Select the TCP checkbox</li> <li>In the Ports field enter 80</li> </ul>

Below the table, step 5 says "Click Create." A note says "Click Check my progress to verify that you have completed this task correctly." A success message states "Create a firewall to deny HTTP traffic" and "Check my progress". A green checkmark icon is present. To the right, a "Checkpoints" sidebar lists tasks with progress bars: "Create a firewall rule" (25/25), "Generate HTTP network traffic" (25/25), "Create a deny firewall rule" (25/25), and "Analyze the firewall logs" (0/25). A vertical sidebar on the right shows "Task 4. Create a firewall rule to deny HTTP traffic" and "Task 5. Analyze the firewall logs". Buttons for "Conclusion" and "End your lab" are at the bottom.

Figure 11 : Task 3 Completion Verification.

The screenshot shows the Google Cloud VM instances page. At the top, there's a navigation bar with 'Google Cloud' and a dropdown for 'qwiklabs-gcp-04-41f89c7069df'. A search bar on the right says 'Search (/) for resources, docs, products, and more'. Below the navigation is a header with 'VM instances', 'CREATE INSTANCE', 'IMPORT VM', and 'REFRESH' buttons. Underneath are tabs for 'INSTANCES', 'OBSERVABILITY', and 'INSTANCE SCHEDULES'. The main area is titled 'VM instances' and shows a table with one row for a 'web-server' instance in 'us-east1-b' zone. The table columns include Status, Name, Zone, Recommendations, In use by, Internal IP, External IP, Connect, and a more options menu. Below the table are 'Related actions' cards for Backup and DR, Monitoring, VM logs, and Firewall rules.

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

The screenshot shows a web browser window with a dark theme. The address bar displays the IP address '35.237.79.55'. The main content area shows an error message: 'This site can't be reached' with the text '35.237.79.55 took too long to respond.' Below this, under 'Try:', are two items: 'Checking the connection' and 'Checking the proxy and the firewall'. At the bottom, the error code 'ERR\_CONNECTION\_TIMED\_OUT' is shown. There are 'Reload' and 'Details' buttons at the bottom right.

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

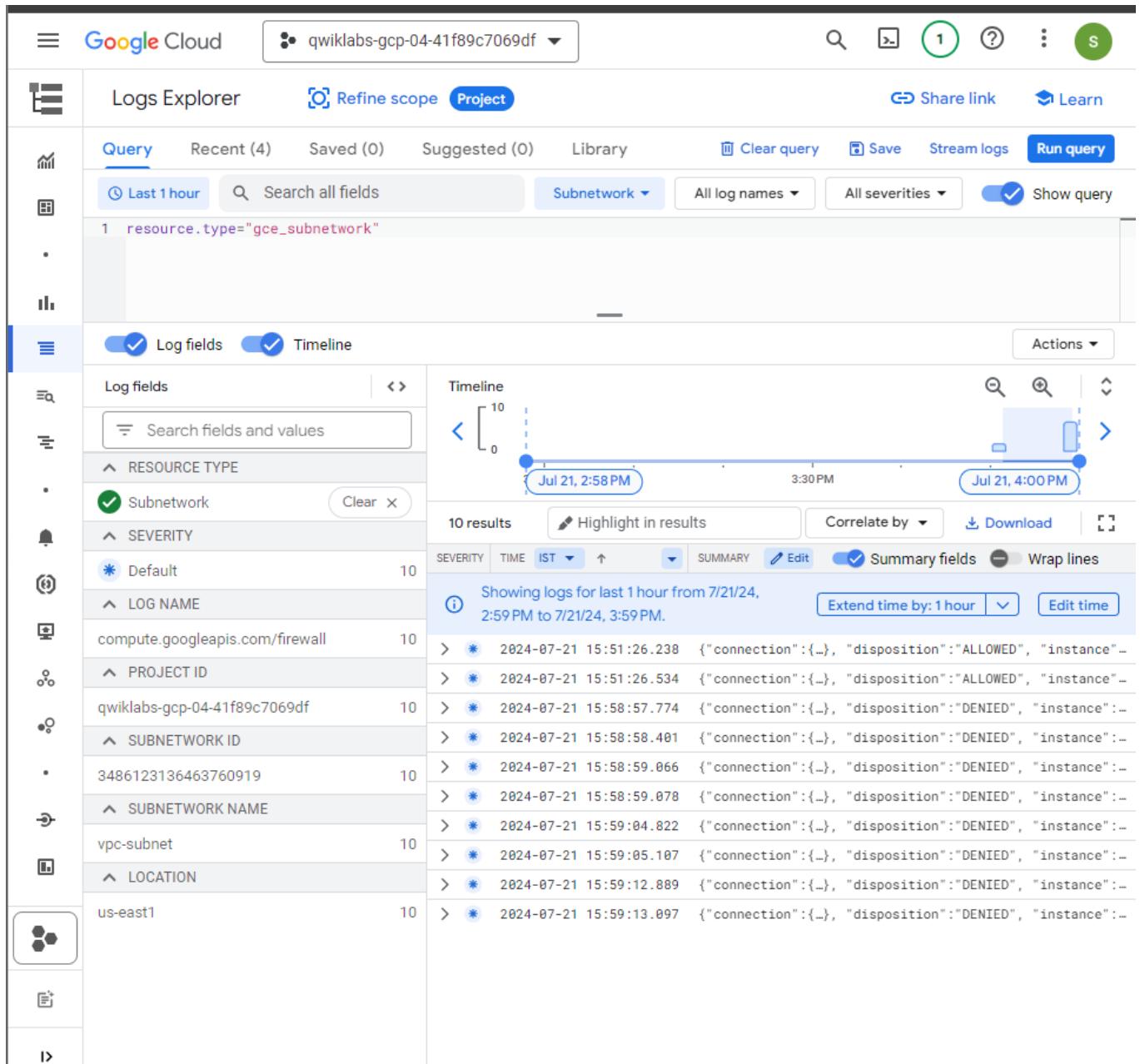


Figure 14 : Navigation menu in Google Cloud Console showing the path to select Logging > Logs Explorer.

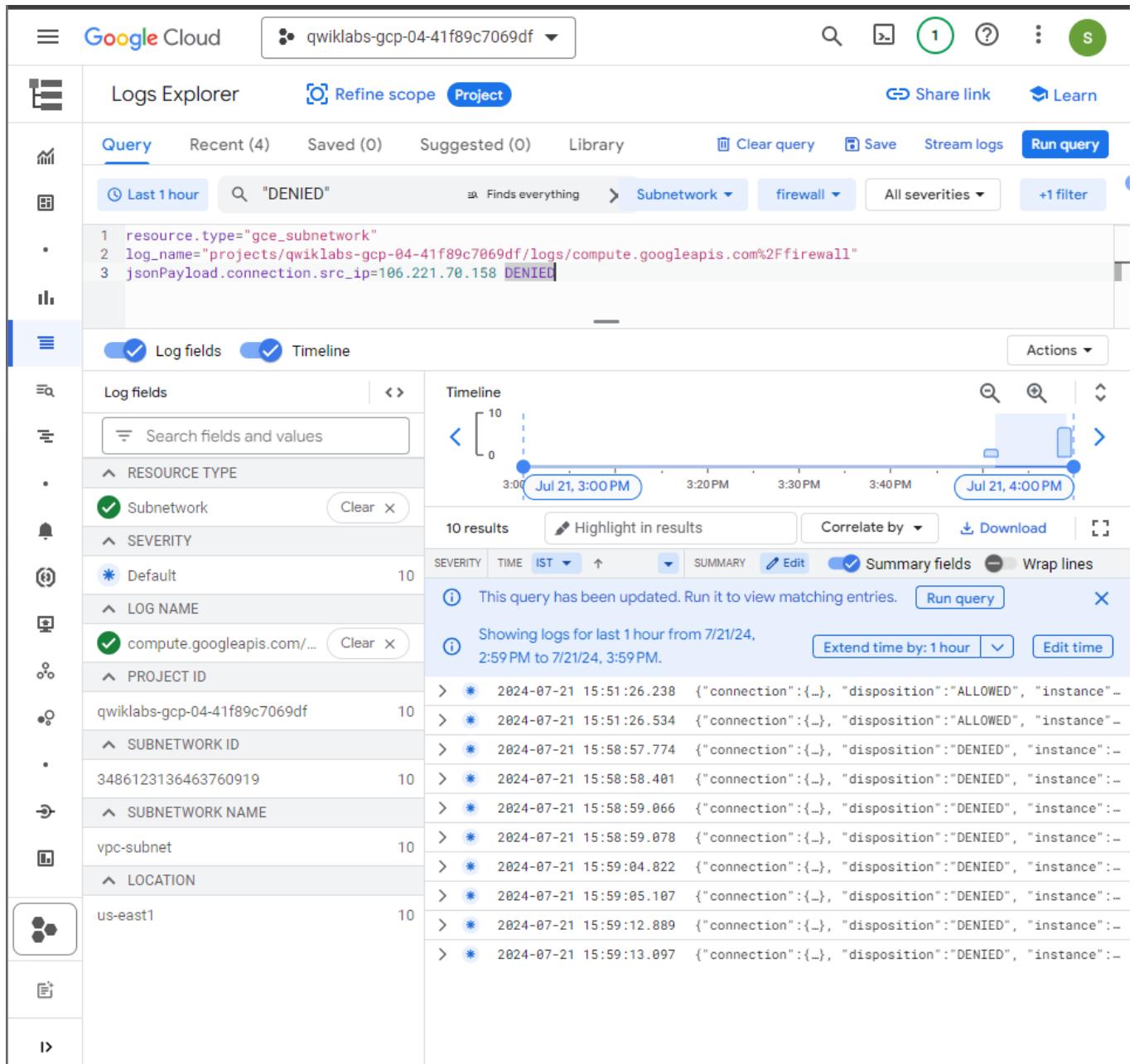


Figure 15 : Query builder in Logs Explorer with the query jsonPayload.connection.src\_ip=YOUR\_IP DENIED entered and executed

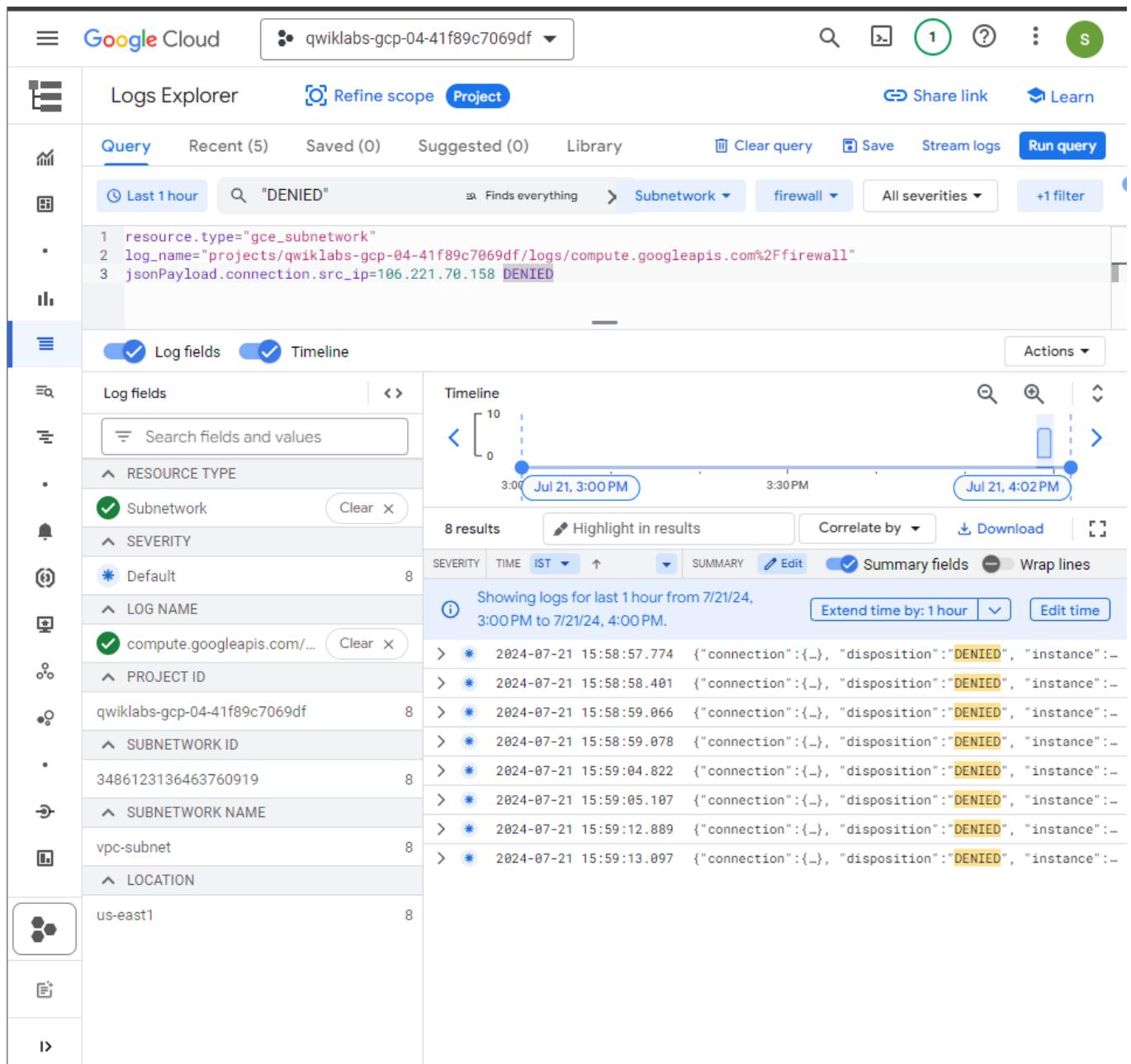


Figure 16 : . Query results pane displaying firewall log entries after running the query.

The screenshot shows a Google Cloud Skills Boost interface. On the left, there's a sidebar with 'Google Cloud' navigation and user info. The main area displays a task titled 'Cloud Security Risks: Identify and Protect Against Threats' under 'Access control and identity management'. A message says 'Every time you set up a deny rule, it was successfully triggered. This rule denied incoming network traffic on port 80.' Below this, a button says 'Click Check my progress to verify that you have completed this task correctly.' A green checkmark icon and the text 'You have successfully completed this task.' are shown. To the right, a 'Checkpoints' section lists four tasks with their status: 'Create a firewall rule' (25/25), 'Generate HTTP network traffic' (25/25), 'Create a deny firewall rule' (25/25), and 'Analyze the firewall logs' (25/25). A vertical sidebar on the right shows 'Task 4. Create a firewall rule to deny HTTP traffic' and 'Task 5. Analyze the firewall logs'.

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](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:

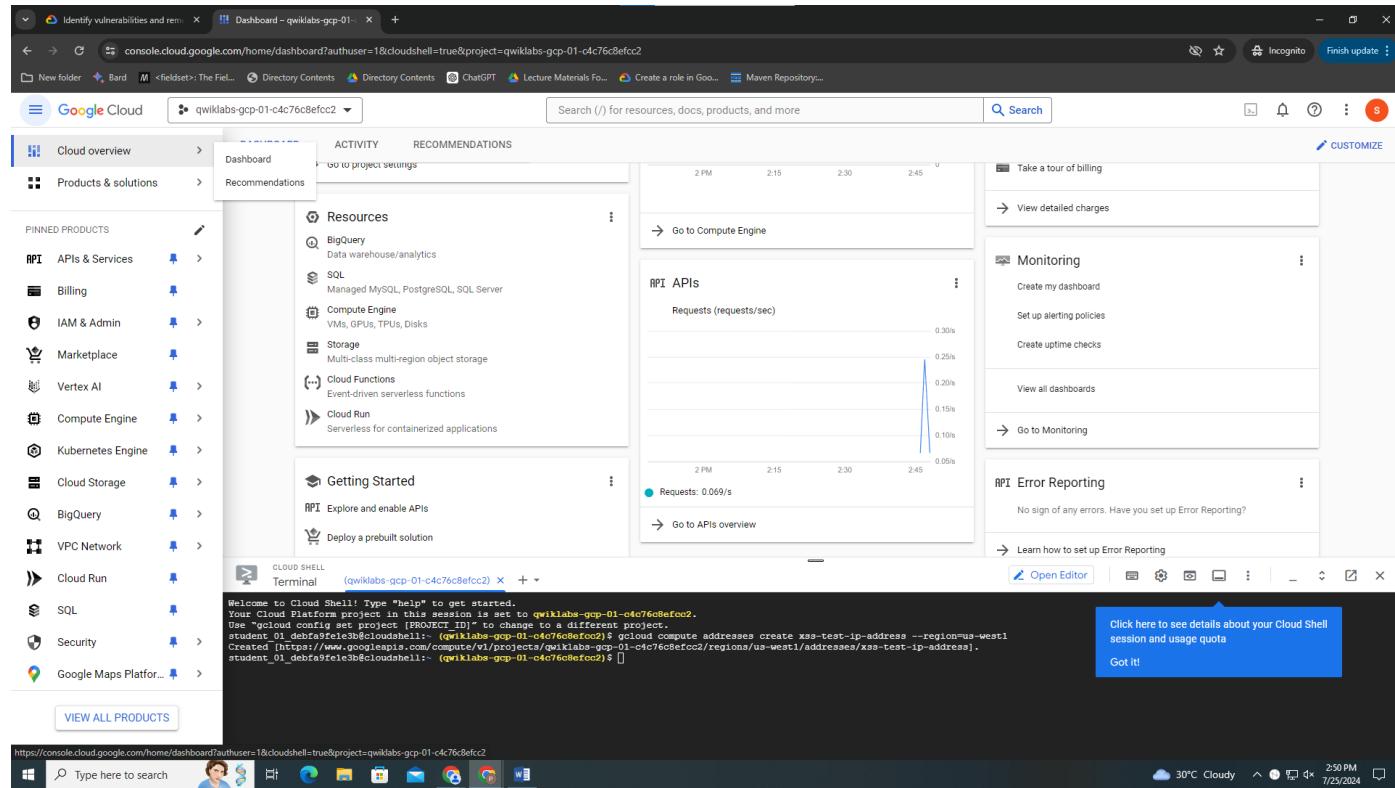


Figure 1 : Starting Google Cloud Skills Lab.

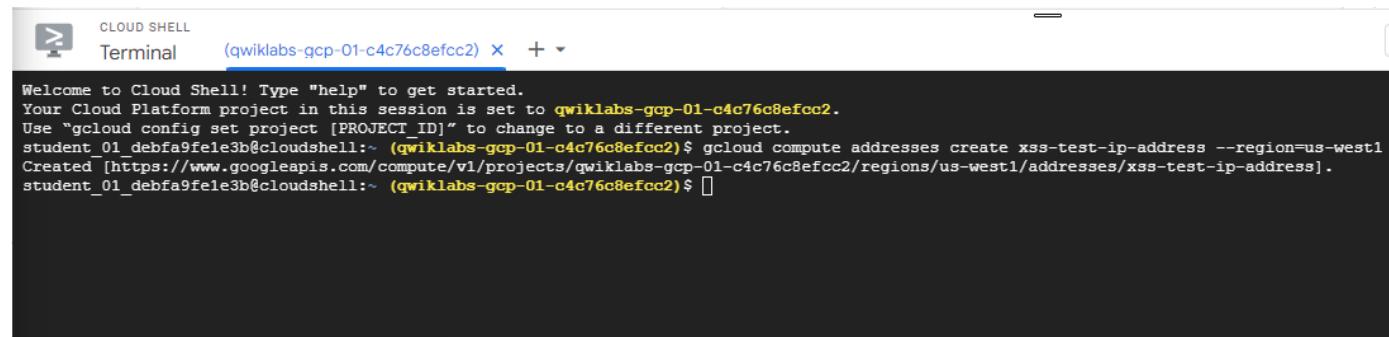


Figure 2 : Creating a static IP address

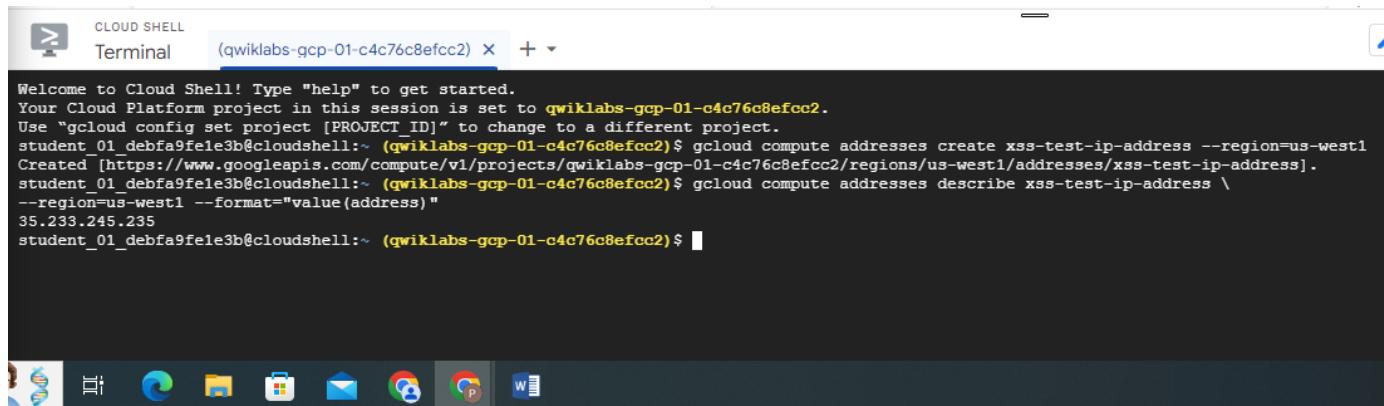


Figure 3 : Describing the static IP address in Cloud Shell.

```
student_01_debfa9fe1e3b@cloudshell:~ (qwiklabs-gcp-01-c4c76c8efcc2)$ gcloud compute instances create xss-test-vm-instance --address=xss-test-ip-address \
--no-scopes --machine-type=e2-micro --zone=us-west1-a \
--metadata=startup-script='apt-get update; apt-get install -y python3-flask'

Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-01-c4c76c8efcc2/zones/us-west1-a/instances/xss-test-vm-instance].
NAME: xss-test-vm-instance
ZONE: us-west1-a
MACHINE_TYPE: e2-micro
PREEMPTIBLE:
INTERNAL_IP: 10.138.0.3
EXTERNAL_IP: 35.233.245.235
STATUS: RUNNING
student_01_debfa9fe1e3b@cloudshell:~ (qwiklabs-gcp-01-c4c76c8efcc2)$
student_01_debfa9fe1e3b@cloudshell:~ (qwiklabs-gcp-01-c4c76c8efcc2)$
```

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

```
Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-01-c4c76c8efcc2/zones/us-west1-a/instances/xss-test-vm-instance]
NAME: xss-test-vm-instance
ZONE: us-west1-a
MACHINE_TYPE: e2-micro
PREEMPTIBLE:
INTERNAL_IP: 10.138.0.3
EXTERNAL_IP: 35.233.245.235
STATUS: RUNNING
```

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

```
student_01_debfa9fe1e3b@cloudshell:~ (gwiklabs-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/gwiklabs-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:~ (gwiklabs-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/gwiklabs-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

	Status	Name	Zone	Recommendations	In use by	Internal IP	External IP	Connect
<input type="checkbox"/>	<span>✓</span>	lab-vm	us-west1-a			10.138.0.2 (nic0)	35.203.147.215 (nic0)	SSH
<input type="checkbox"/>	<span>✓</span>	xss-test-vm-instance	us-west1-a			10.138.0.3 (nic0)	35.233.245.235 (nic0)	SSH

Figure 8 : Select Compute Engine > VM instances.

<input type="checkbox"/>	Status	Name	Zone	Recommendations	In use by	Internal IP	External IP	Connect
<input type="checkbox"/>	<span>✓</span>	lab-vm	us-west1-a			10.138.0.2 (nic0)	35.203.147.215 (nic0)	SSH
<input type="checkbox"/>	<span>✓</span>	xss-test-vm-instance	us-west1-a			10.138.0.3 (nic0)	35.233.245.235 (nic0)	SSH

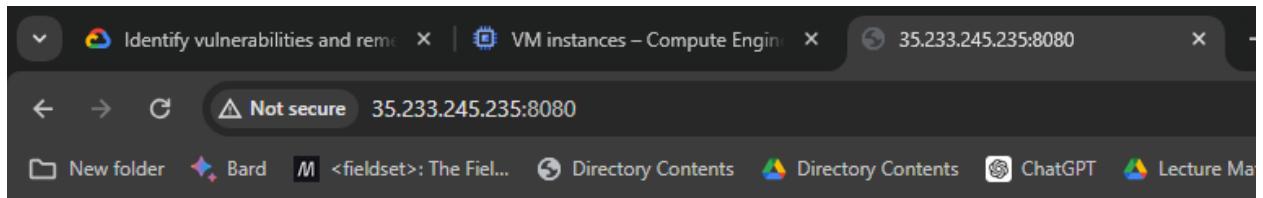
Figure 9 : VM instance name xss-test-vm- instance

The screenshot shows a terminal window titled "SSH-in-browser" with two tabs open. The left tab shows the command `gsutil cp gs://cloud-training/GCPSEC-ScannerAppEngine/flask\_code.tar . && tar xvf flask\_code.tar` being run, with output indicating files are being copied from Google Cloud Storage to the current directory. The right tab shows the same command. A modal dialog box is overlaid on the terminal, containing the message: "Please consider adding the IAP-secured Tunnel User IAM role (iap.tunnellInstances.accessVialAP) to start using Cloud IAP for TCP forwarding for better performance." An "X" button is visible in the bottom right corner of the modal.

Figure 10 : Downloading and extracting the vulnerable web application files

The screenshot shows a terminal window with the command `python3 app.py` being run. The output indicates that a Flask app named "app" is serving on port 8080 in production mode. It includes a warning about using it in production and a note that it's a development server.

Figure 11 : Running the vulnerable application



This is a demo application for Cymabl Bank's corporate banking portal.

Enter your financial institution name below and click POST.

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

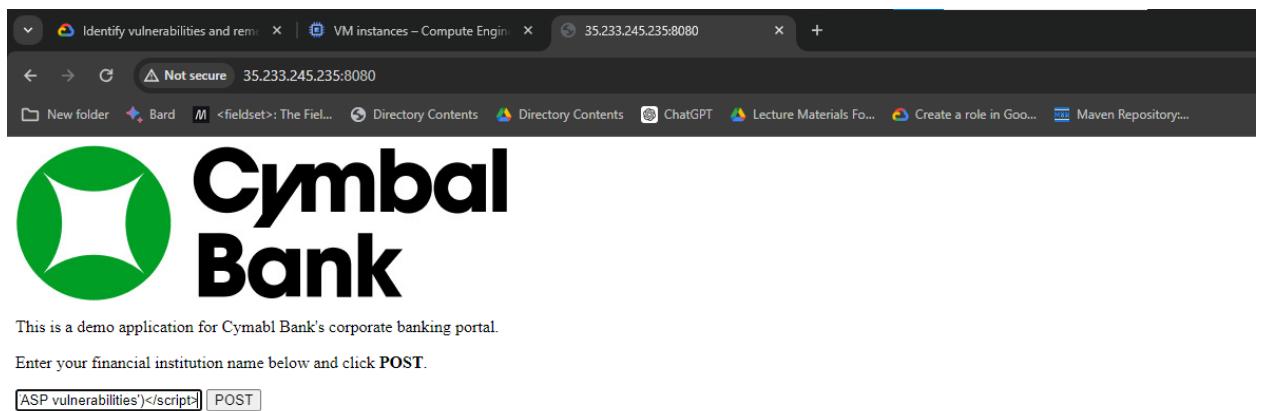


Figure 13 : Injecting an XSS script <script>alert('This is an XSS Injection to demonstrate one of OWASP vulnerabilities')</script> into the web form.

```
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.

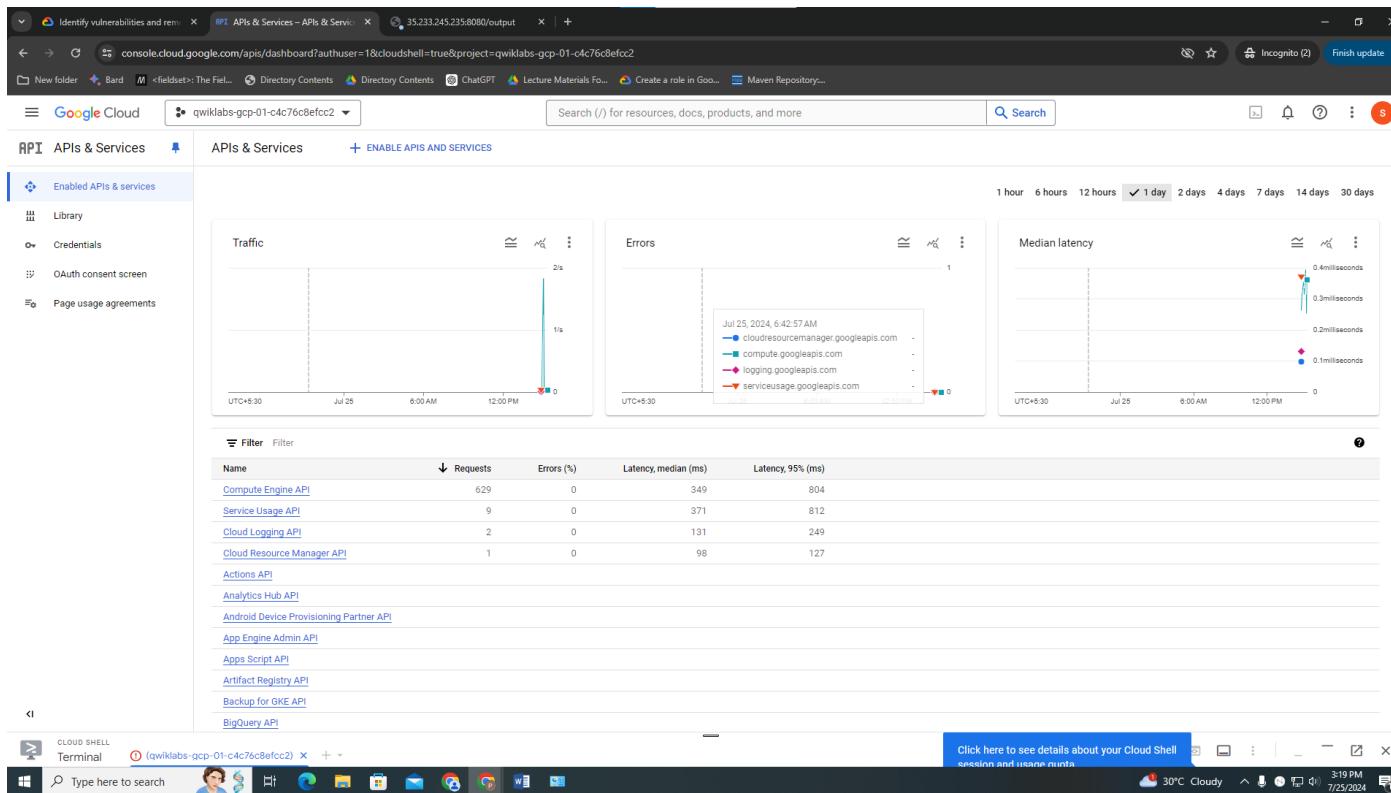


Figure 15 : Select APIs & Services > Enabled APIs and services. The APIs & Services page displays.

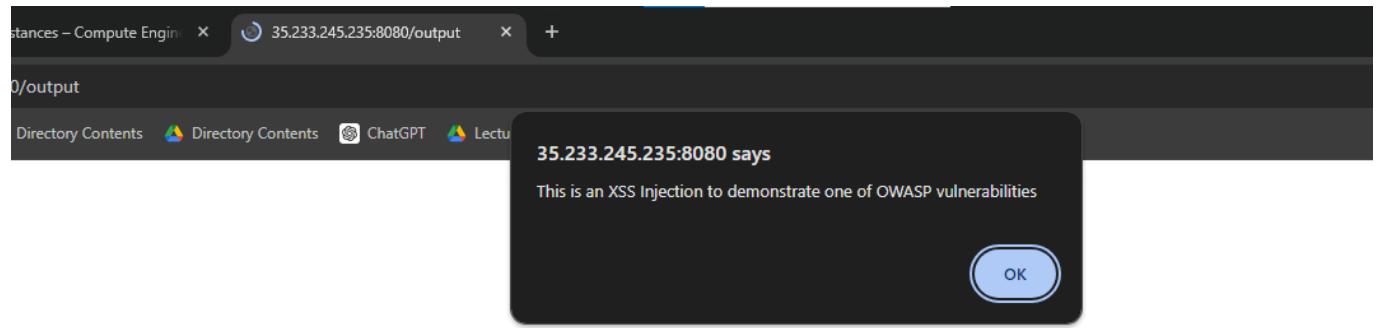


Figure 16 : XSS vulnerability demonstration with alert message.

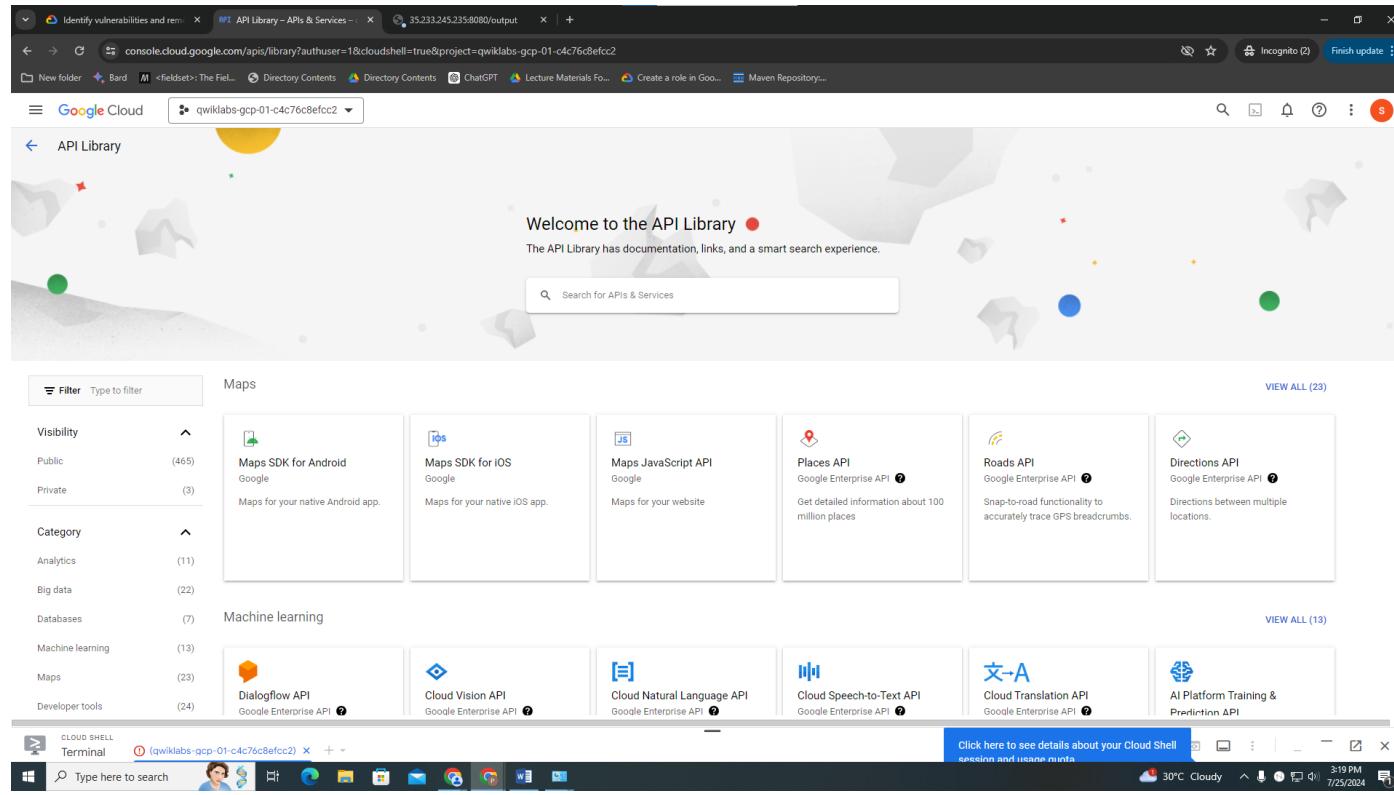


Figure 17 : In the search field, type **Web Security Scanner**, and press **ENTER**.

The screenshot shows a search results page for "Web Security Scanner" in the Google Cloud search interface. At the top, there's a dropdown menu showing "qwiklabs-gcp-01-c4c76c8efcc2". Below it is a search bar with the query "Web Security Scanner". The results section indicates "1 result" and shows a card for the "Web Security Scanner API". The card includes the API name, provider ("Google Enterprise API"), a brief description ("Scans your Compute and App Engine apps for common web vulnerabilities."), and a circular icon with a play button symbol.

Figure 18

The screenshot shows the "Product details" page for the "Web Security Scanner API" in the Google Cloud console. The header includes the Google Cloud logo and the project name "qwiklabs-gcp-01-c4c76c8efcc2". The main content area features a large circular icon with a play button symbol, the API name "Web Security Scanner API", its provider "Google Enterprise API", and a brief description "Scans your Compute and App Engine apps for common web vulnerabilities.". Below this are two buttons: "ENABLE" (in blue) and "TRY THIS API" (with a link icon). A call-to-action button "Click to enable this API" is also present. At the bottom, there are navigation links for "OVERVIEW" (underlined), "DOCUMENTATION", and "RELATED PRODUCTS".

Figure 19 : Select Web Security Scanner API.

The screenshot shows the 'API/Service Details' page for the 'Web Security Scanner API'. At the top, there's a 'DISABLE API' button and a search bar with the placeholder 'You can now search for documentation, resource metadata, tutorials, and API keys'. Below the header, the service name is listed as 'websecurityscanner.googleapis.com', 'Type' as 'Public API', and 'Status' as 'Enabled'. There are 'Documentation' and 'TRY IN API EXPLORER' links. The main content area includes tabs for 'METRICS', 'QUOTAS & SYSTEM LIMITS', and 'CREDENTIALS'. Under 'METRICS', there are filters for 'Select Graphs' (4 Graphs), 'Versions' (v1, v1alpha, and v1beta), 'Credentials' (Compute Engine default s...), and 'Methods' (41 options selected). A chart titled 'Traffic by response code' shows no data available for the selected time frame (Jul 8, 2024, 11:54:50 AM). Below the chart is a section for 'Errors by API method'.

Figure 20 : Enabling the Web Security Scanner API.

The screenshot shows the 'Cloud Web Security Scanner' interface. The left sidebar has sections like 'Security Command Center' (Risk Overview, Threats, Vulnerabilities, Compliance, Assets, Findings, Sources, Posture Management...), 'Detections and Controls' (Google SecOps, reCAPTCHA Enterprise, Web Security Scanner, Risk Manager, Binary Authorization, Marketplace, Release Notes), and 'CLOUD SHELL' (Terminal). The main panel is titled 'Scan configs' and includes buttons for '+ NEW SCAN' and 'DELETE'. A search bar at the top right says 'You can now search for documentation, resource metadata, tutorials, and API keys'. The status bar at the bottom shows 'Click here to see details about your Cloud Shell session and usage quota'.

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

The screenshot shows the Google Cloud Web Security Scanner interface. On the left, there is a sidebar with various security-related options like Security Command Center, Risk Overview, Threats, Vulnerabilities, Compliance, Assets, Findings, Sources, Posture Management, Google SecOps, reCAPTCHA Enterprise, Web Security Scanner (which is selected and highlighted in blue), Risk Manager, Binary Authorization, Advisory Notifications, Marketplace, and Release Notes. The main content area is titled "Create a new scan". It has fields for "Name" (set to "Cross-Site Scripting scan"), "Starting URLs" (set to "http://35.233.245.235:8080"), "Excluded URLs" (with dropdowns for Authentication set to "None" and Schedule set to "Never"), and "Export options" (with a checked checkbox for "Export to Security Command Center"). There are also "Run scans from a pre-defined set of source IPs" and "PREVIEW" buttons.

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>.

The screenshot shows the Cloud Web Security Scanner interface. At the top, there are navigation links: 'Cloud Web Security Scanner' (with a back arrow), 'RUN' (blue button), 'EDIT' (pencil icon), and 'DELETE' (trash icon). Below this, the title 'Cross-Site Scripting scan' is displayed. A message says 'You have not run this scan yet' with a 'RUN SCAN' button. The 'DETAILS' tab is selected, showing configuration details:

Starting URLs	http://35.233.245.235:8080
Authentication	None
User agent	Chrome on Linux
Maximum scan speed (QPS)	15
Risk level	Normal
Ignore HTTP status errors	No

Below the details, the 'RESULTS' tab is selected, showing the scan progress: 'Waiting in queue'. The 'URLS CRAWLED' and 'DETAILS' tabs are also visible.

At the bottom, under 'RESULTS', a section titled 'Cross-site scripting (3)' lists vulnerabilities:

- Unescaped or unsanitized input to your application was detected. Learn about [XSS bugs](#). To reproduce this vulnerability, follow the link below and note that a popup occurs. This means some user input to your application is not escaped or sanitized. If you have difficulty reproducing the exploit yourself, follow [these instructions](#).
- http://35.233.245.235:8080/
- http://35.233.245.235:8080/
- http://35.233.245.235:8080/

Figure 23 : Running the security scan on the application.

```

ssh.cloud.google.com/v2/ssh/projects/qwiklabs-gcp-01-c4c76c8efcc2/zones/us-west1-a/instances/xss-test-vm-instance?authuser=1&hl=en_US&projectNumber=3295800021208&nonAdminProxySessionReason...
ssh.cloud.google.com/v2/ssh/projects/qwiklabs-gcp-01-c4c76c8efcc2/zones/us-west1-a/instances/xss-test-vm-instance?authuser=1&hl=en_US&projectNumber=3295800021208&nonAdminPro...
SSH-in-browser
GNU nano 5.4                                         app.py
# Copyright 2023 Google LLC
#
# Licensed under the Apache License, Version 2.0 (the "License");
# you may not use this file except in compliance with the License.
# You may obtain a copy of the License at
#
#     http://www.apache.org/licenses/LICENSE-2.0
#
# Unless required by applicable law or agreed to in writing, software
# distributed under the License is distributed on an "AS IS" BASIS,
# WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
# See the License for the specific language governing permissions and
# limitations under the License.
import flask
app = flask.Flask(__name__)
input_string = ""

html_escape_table = {
    "&": "&amp;",
    "'": "&quot;",
    ">": "&apos;",
    ">": "&gt;",
    "<": "&lt;",
}

@app.route('/', methods=["GET", "POST"])
def input():
    global input_string
    if flask.request.method == "GET":
        return flask.render_template("input.html")
    else:
        input_string = flask.request.form.get("input")
        return flask.redirect("output")

@app.route('/output')
def output():
    # output_string = "".join([html_escape_table.get(c, c) for c in input_string])
    output_string = input_string
    return flask.render_template("output.html", output=output_string)

if __name__ == '__main__':
    app.run(host='0.0.0.0', port=8080)

```

File menu: Help, Write Out, Where Is, Cut, Paste, Execute, Location, Undo, Redo, Set Mark, Copy, To Bracket, Where Was.

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

```

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)

```

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

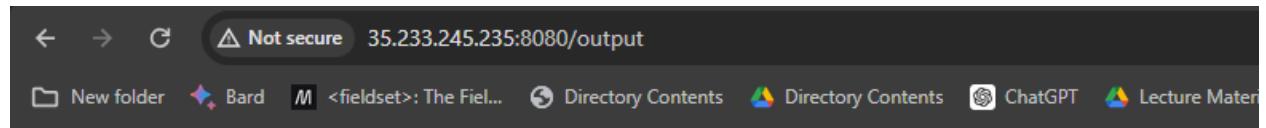
Scan date	URLs crawled	Duration	Vulnerabilities found	Next scheduled scan
Jul 25, 3:57 PM	4	1 min 41 sec	0	

RESULTS URLS CRAWLED DETAILS

No vulnerabilities found.

Cloud Web Security Scanner is continuously updated, so check back and re-run this scan to look for new vulnerabilities.

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



The screenshot shows a browser window with the URL `35.233.245.235:8080/output`. The page content is a single line of HTML code: `<script>alert('This is an XSS Injection to demonstrate one of OWASP vulnerabilities')</script>`. The browser's address bar indicates "Not secure". Below the address bar, there are several browser extensions or toolbars visible.

```

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

***  

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 -  

56.249.83.111 -- [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.

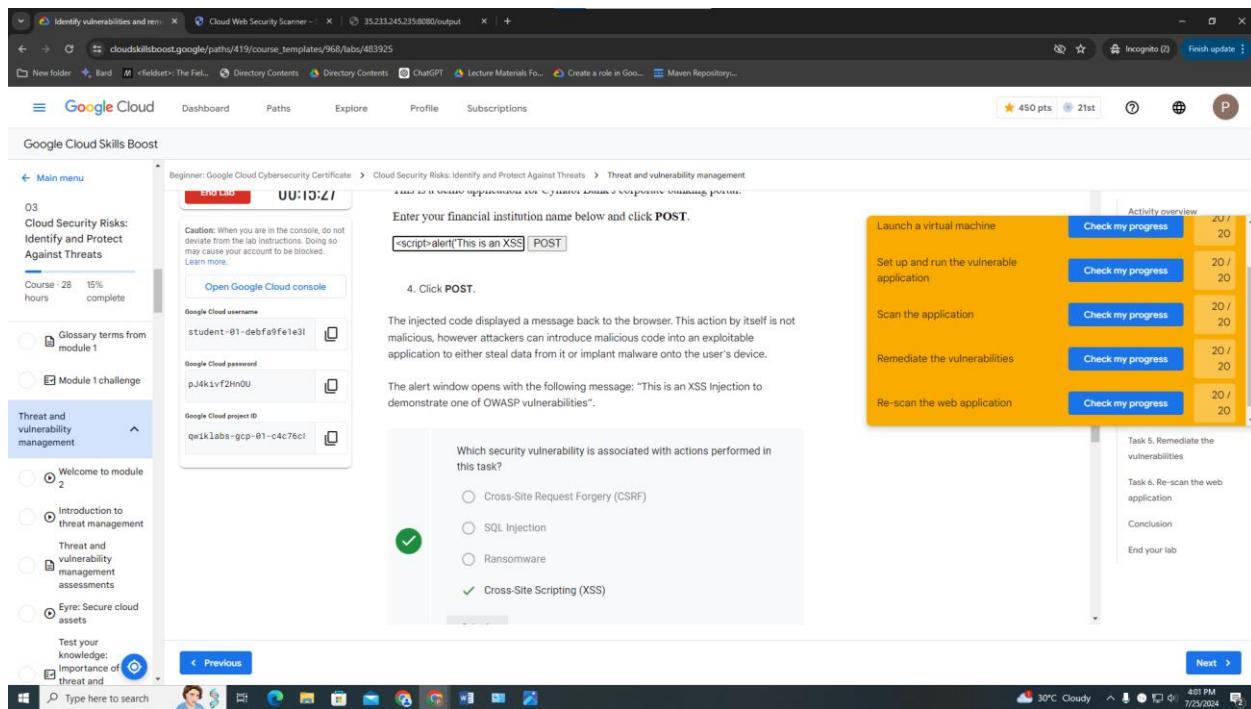


Figure 29 : Earning all points and ending the lab.

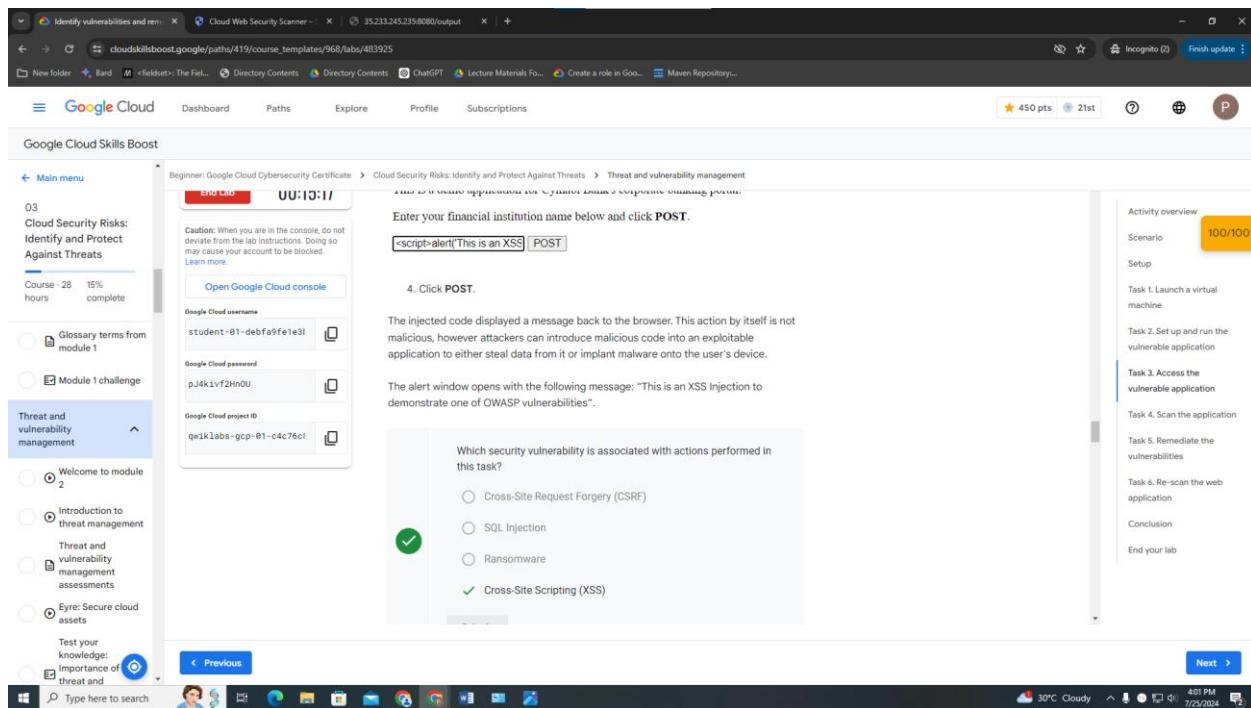


Figure 30 : MCQ

## 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:

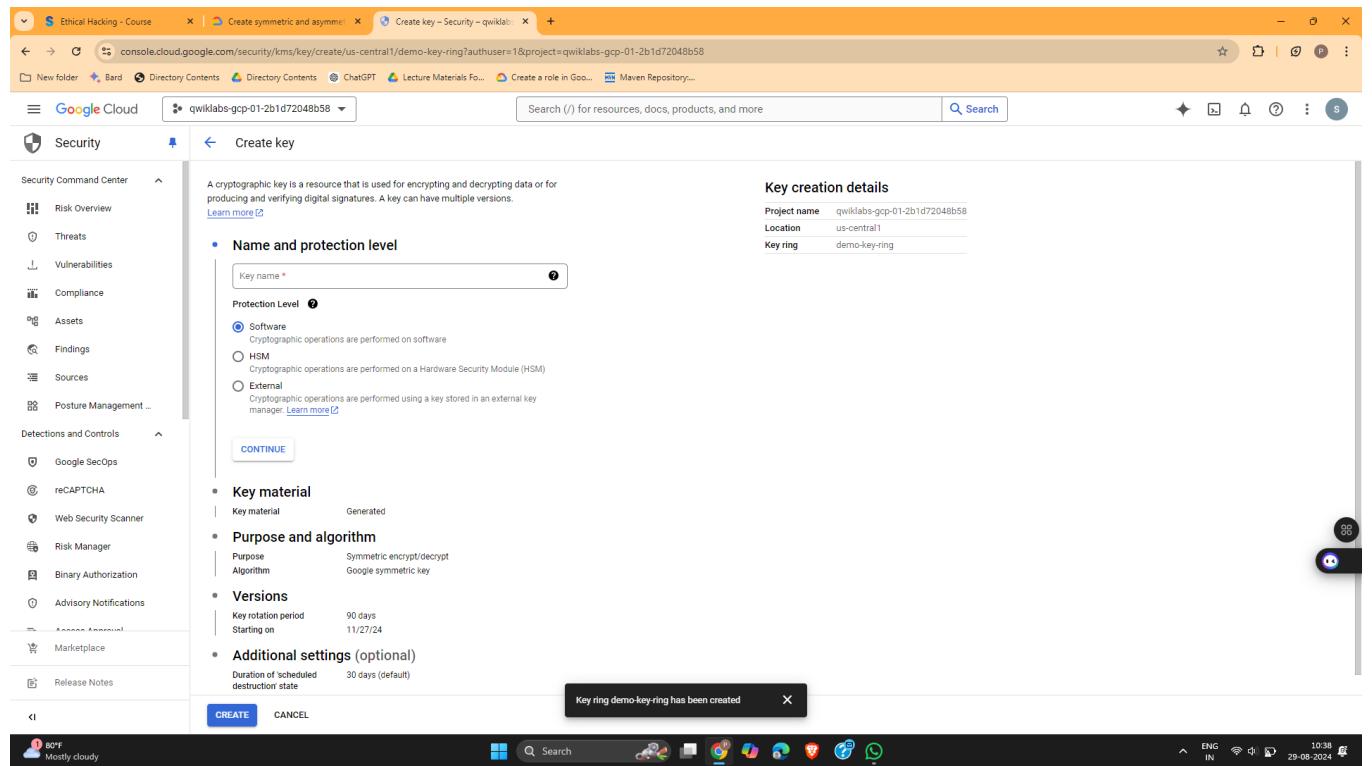


Figure 1 : This figure shows the "Create Key Ring" page in the Google Cloud console, where the user is entering the name demo-key-ring and selecting the region for the key ring.

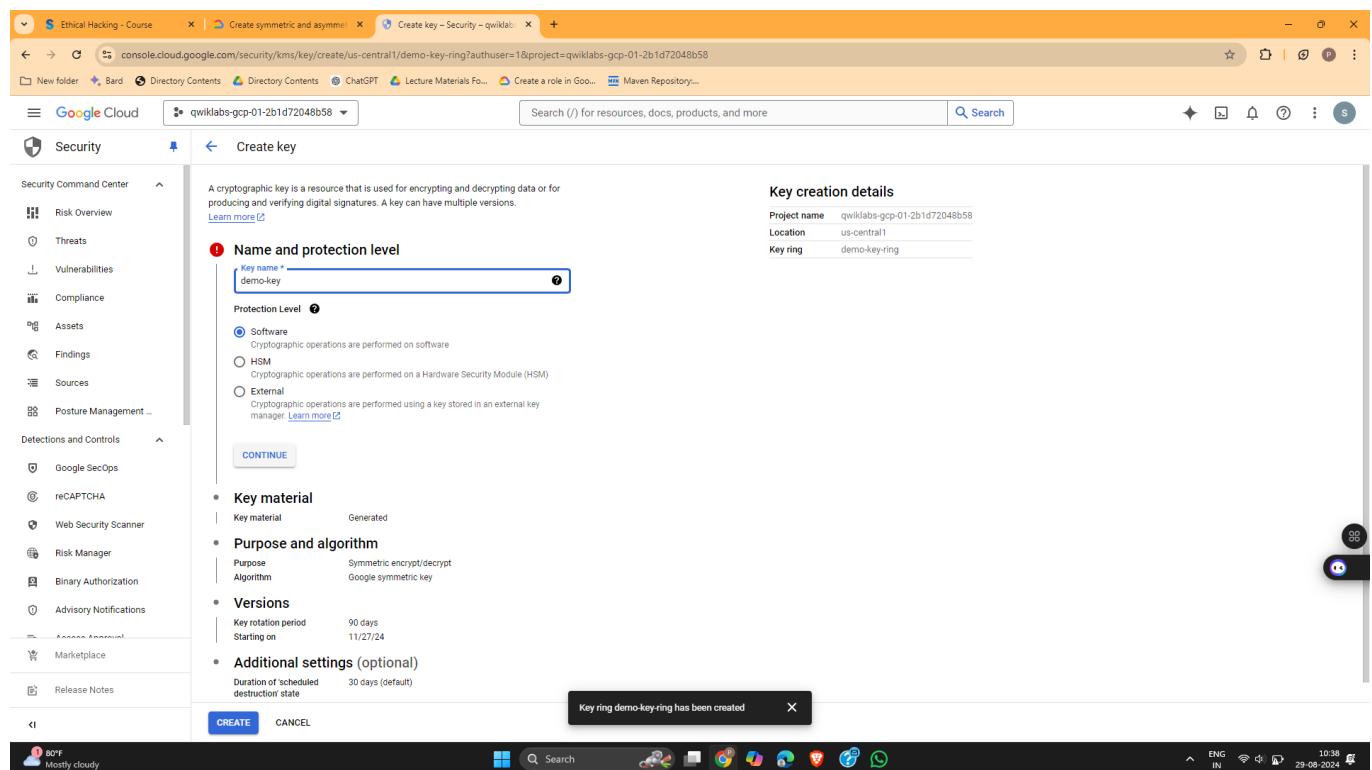


Figure 2 : This figure shows the "Key Details" form, where the user specifies the key name as demo-key and sets the protection level to "Software".

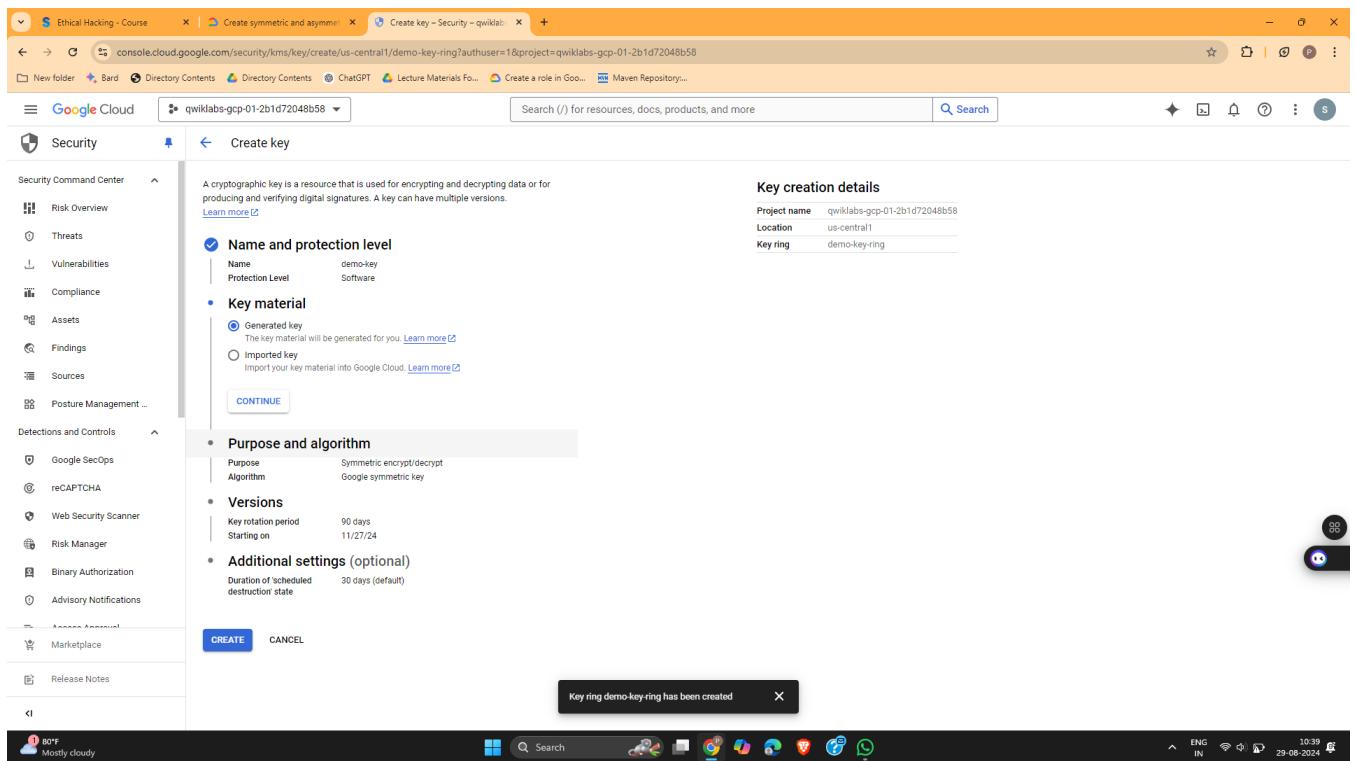


Figure 3 : This figure illustrates the options selected for the symmetric key material generation, including "Generated key"

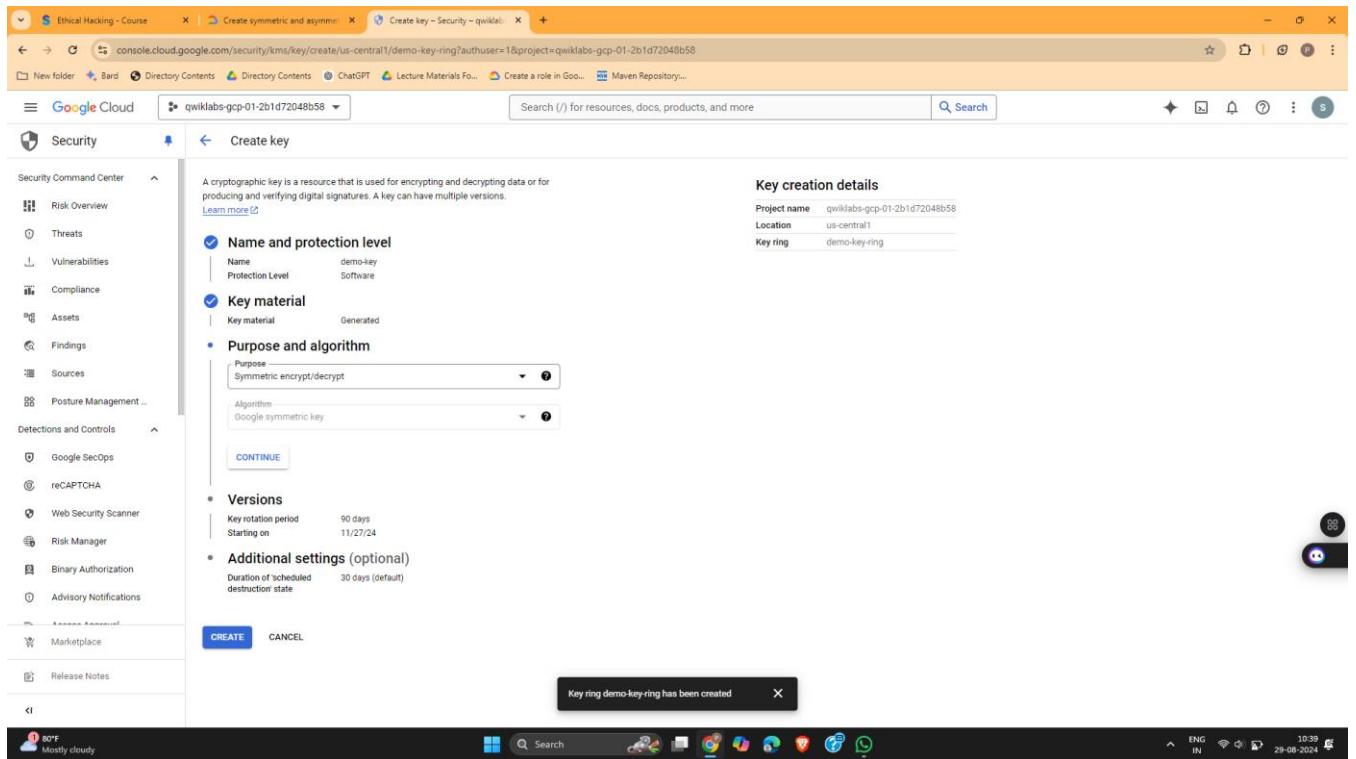


Figure 4 : This figure illustrates the options selected for the purpose set to "Symmetric encrypt/decrypt".

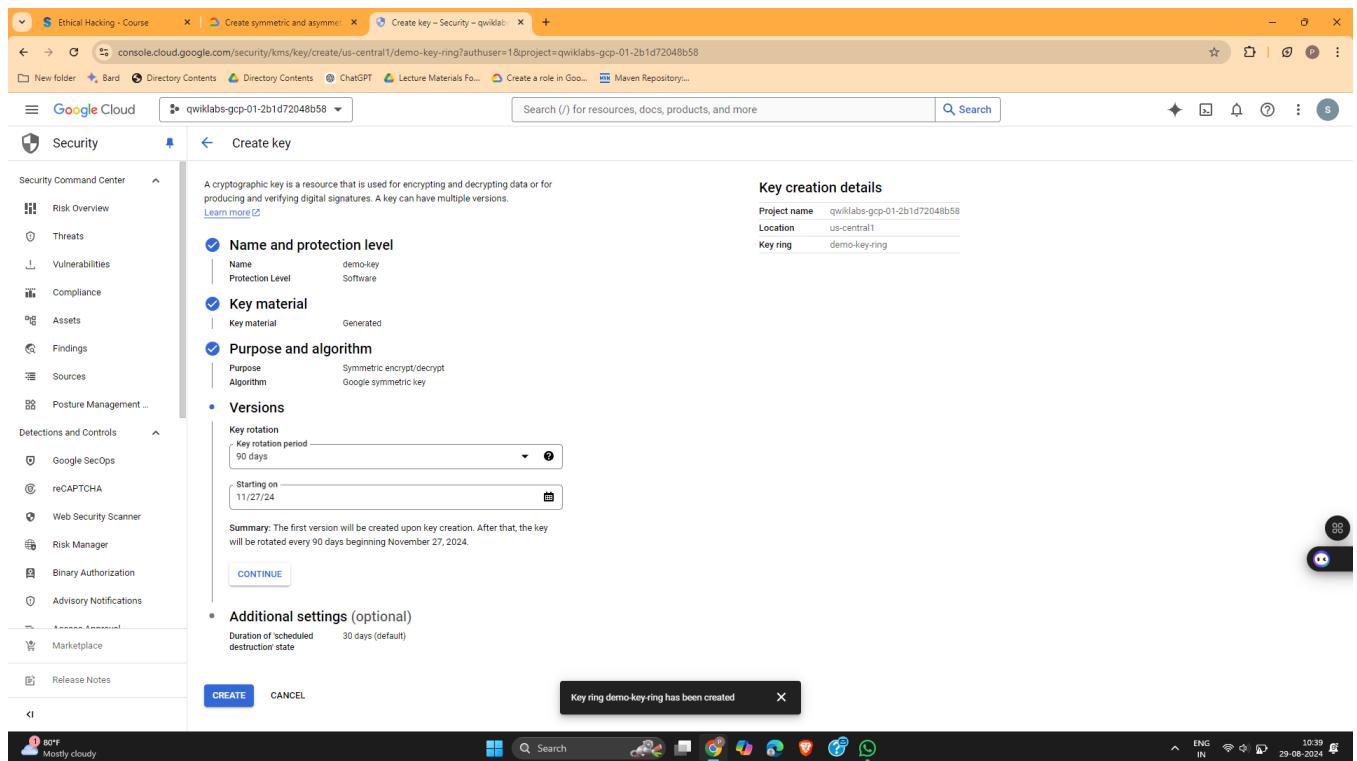


Figure 5 This figure shows the configuration of the key rotation period set to 90 days for the symmetric key.

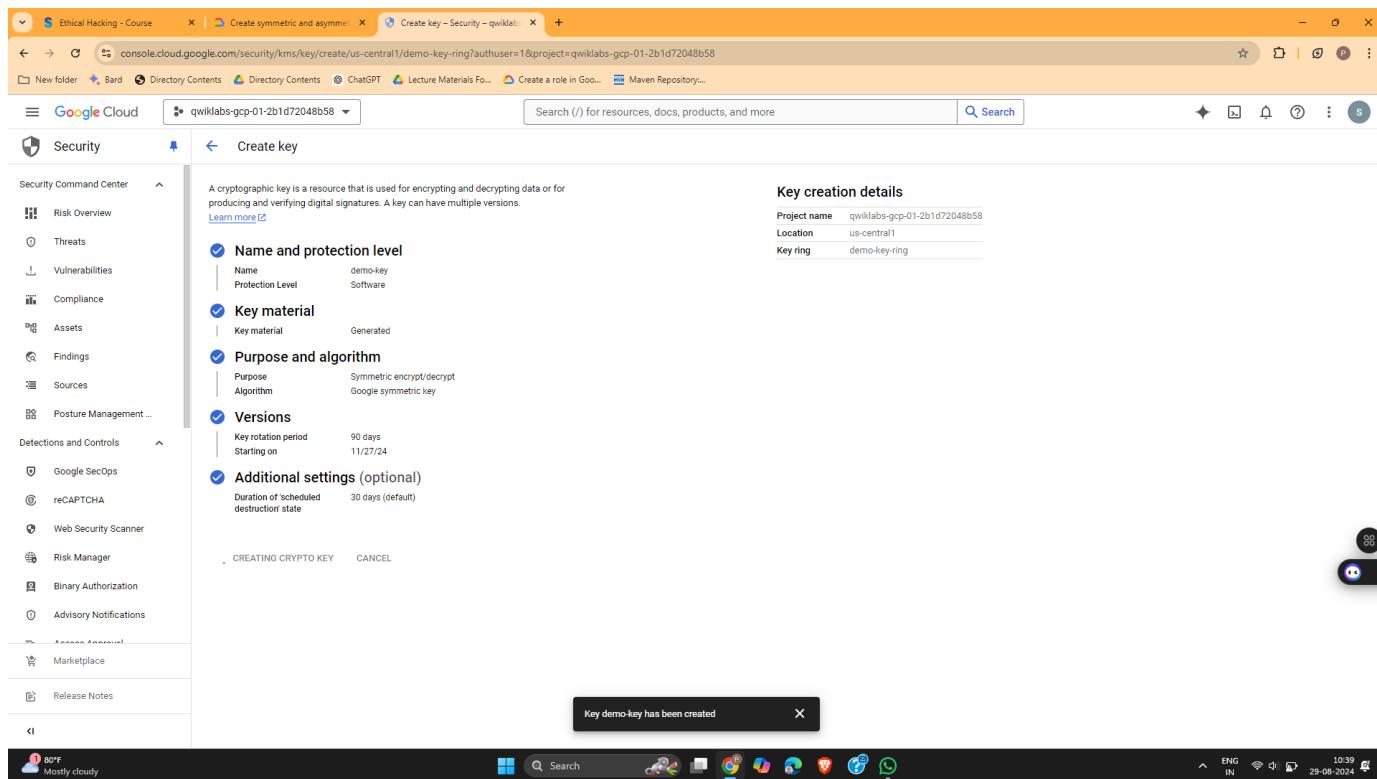


Figure 6 : This figure shows the confirmation message indicating the successful creation of the symmetric key in Google Cloud.

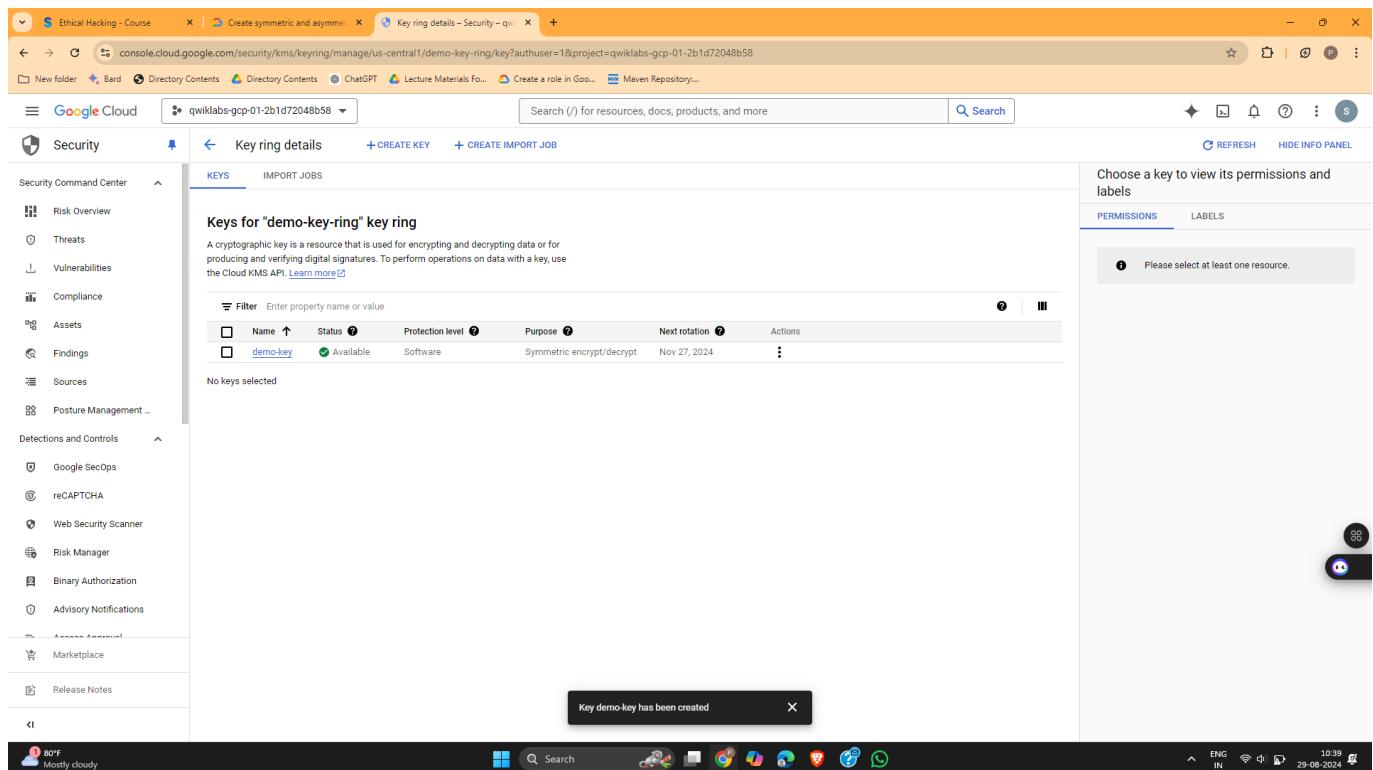


Figure 7 : This figure shows the confirmation message indicating the successful creation of the symmetric key in Google Cloud.

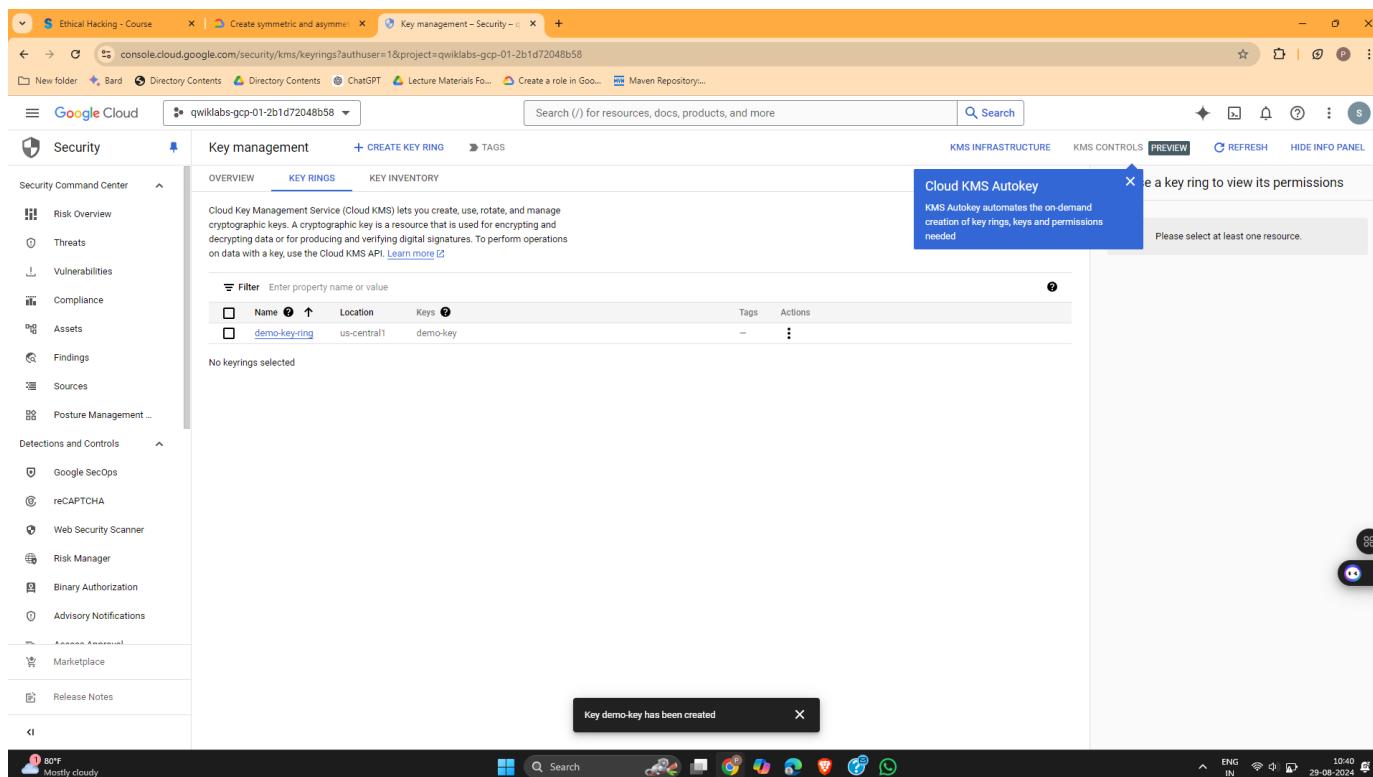


Figure 8 : This figure depicts the navigation process to the "Create Key" page within the demo-key-ring section in Google Cloud Key Management.

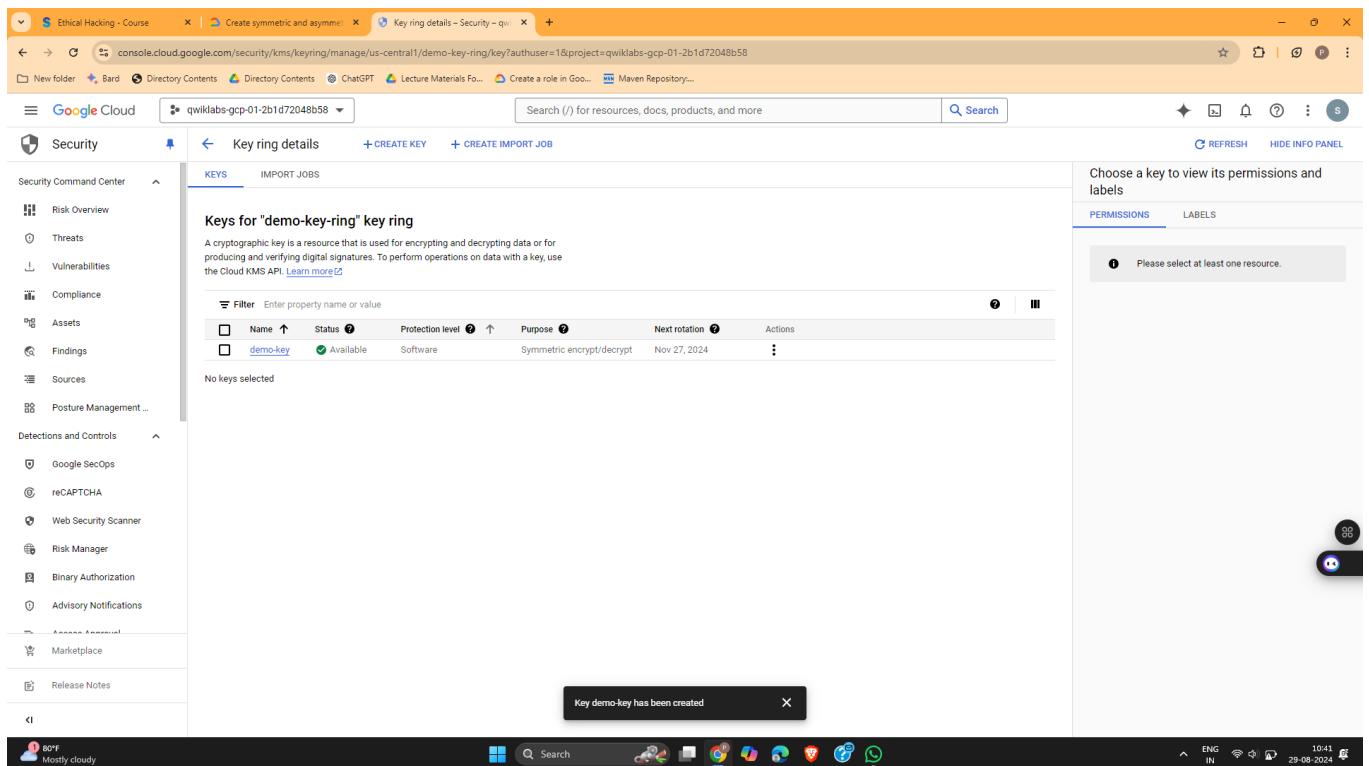


Figure 9 : This figure depicts the navigation process to the "Create Key" page within the demo-key-ring section in Google Cloud Key Management.

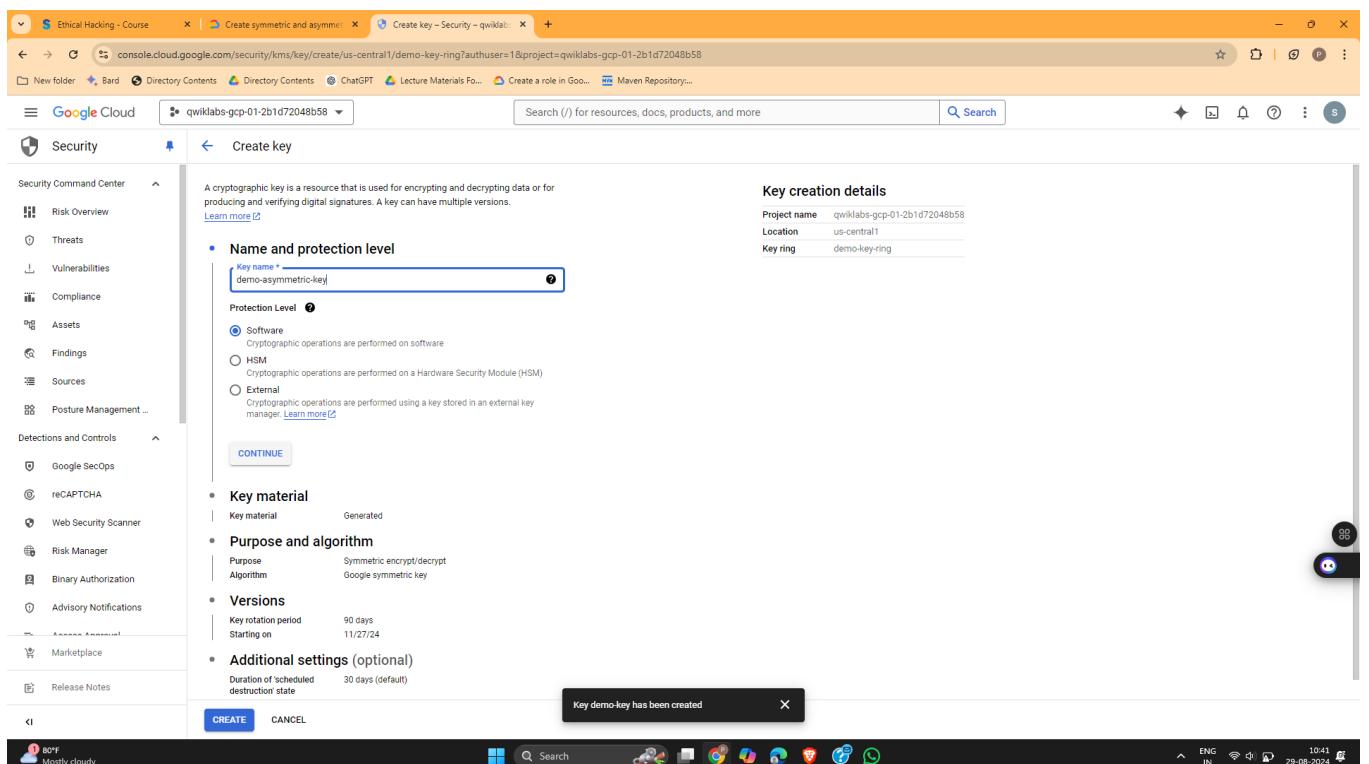


Figure 10 : This figure shows the form where the user enters the key name demo-asymmetric-key and selects the protection level as "Software".

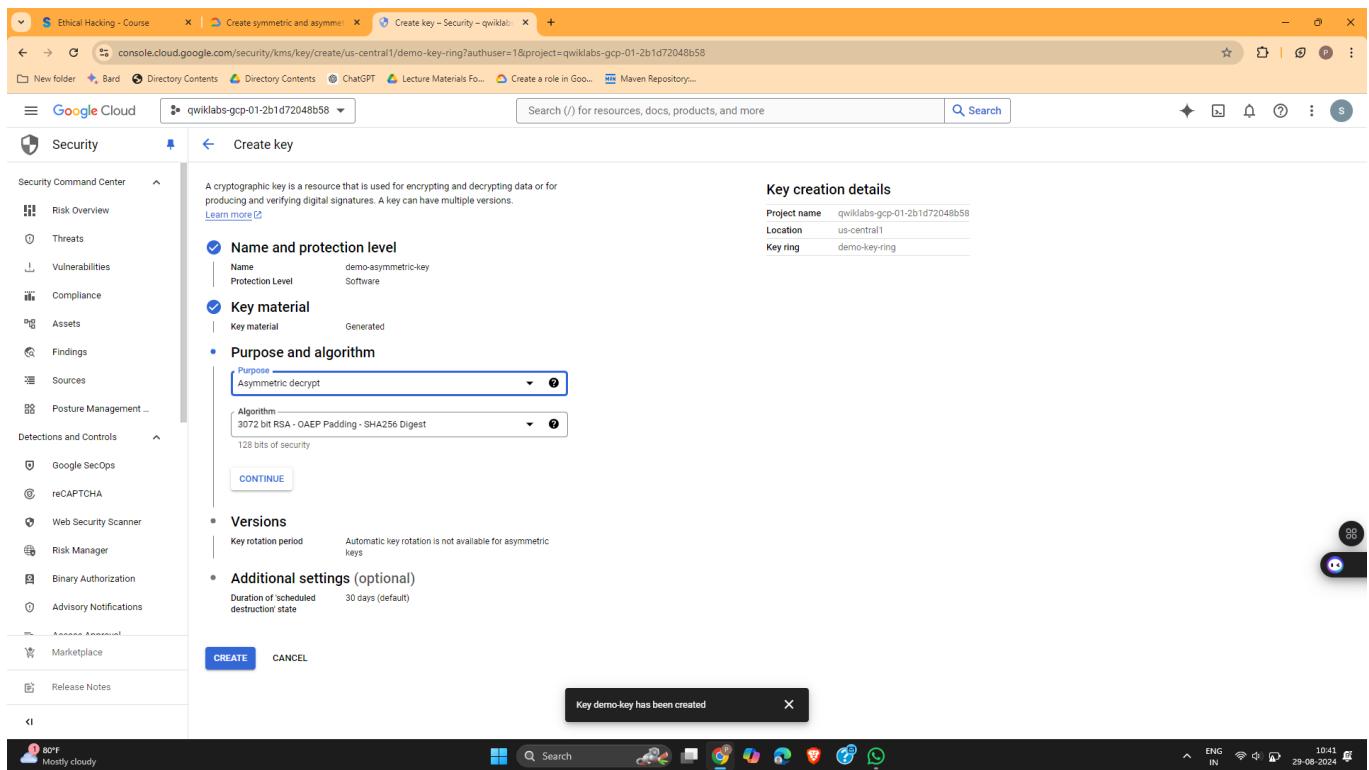


Figure 11 : This figure illustrates the selection of the key material as "Generated key" and the purpose set to "Asymmetric decrypt".

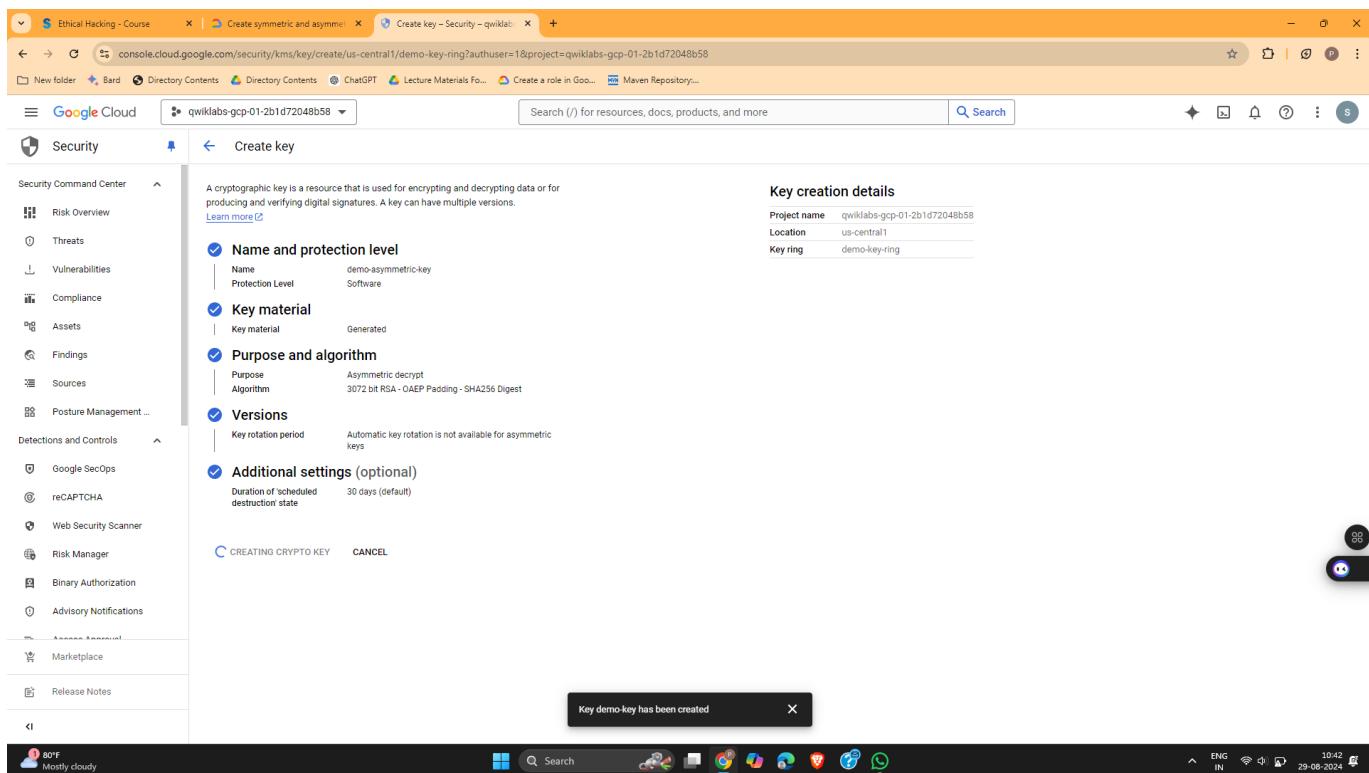


Figure 12 : This figure shows the "Create" button clicked to complete the process of creating the asymmetric key in Google Cloud.

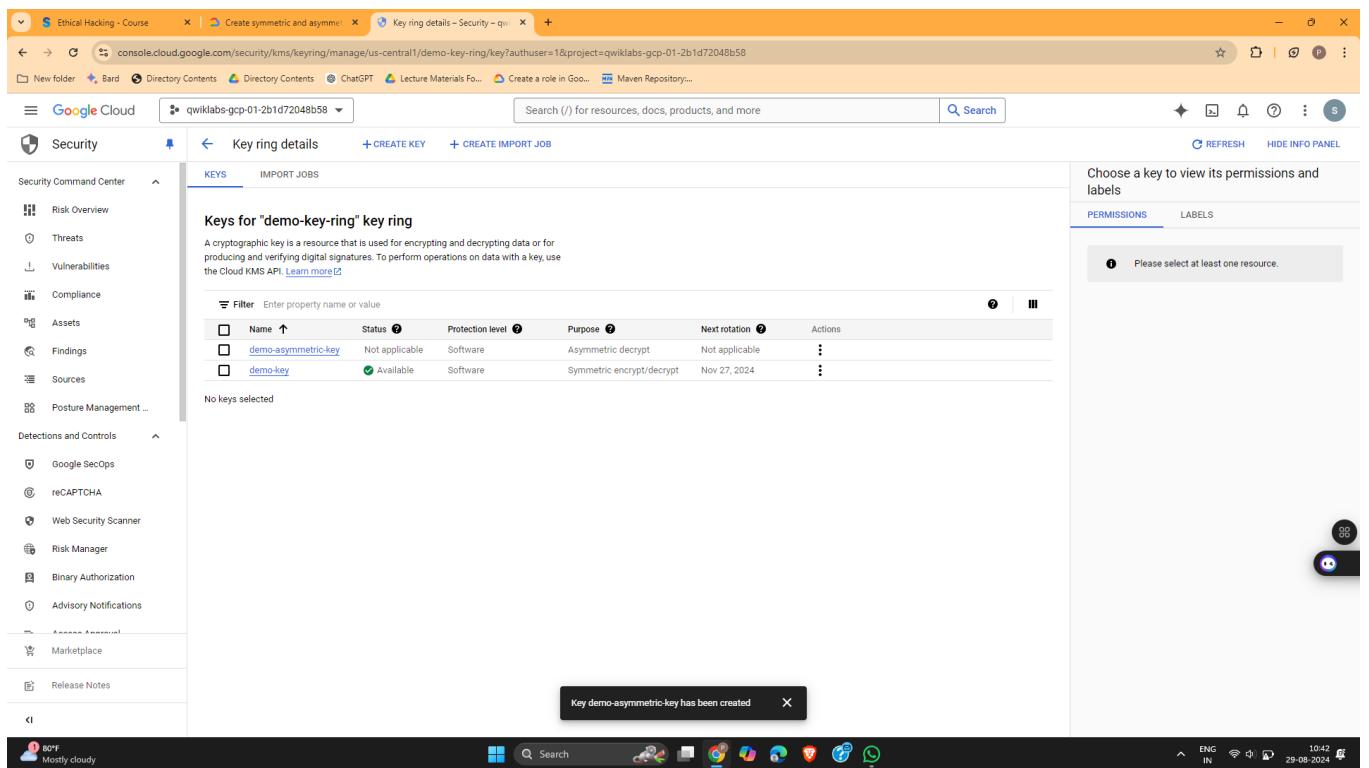


Figure 13 : This figure displays the confirmation screen indicating that the asymmetric key has been successfully created, ready for use.

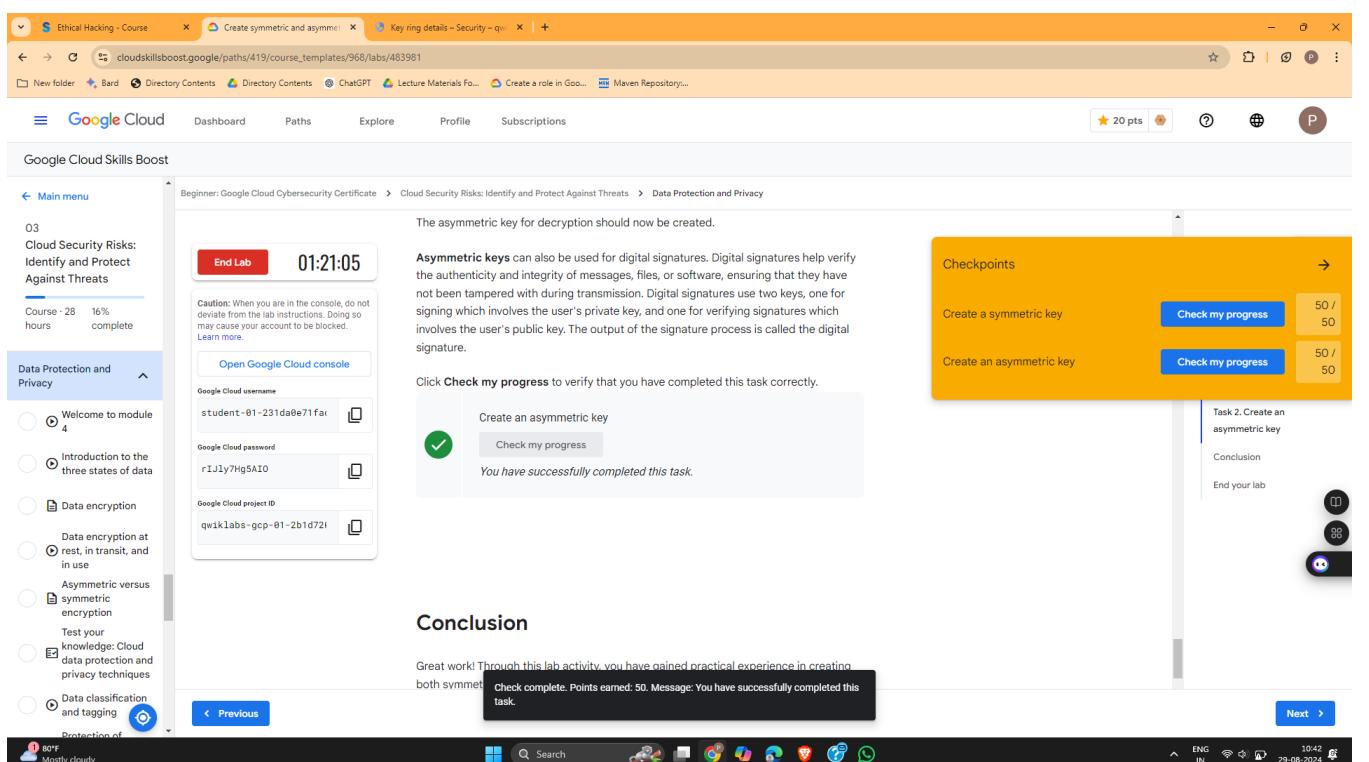


Figure 14 : This figure displays the confirmation screen for lab completion.

## 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=PLBlnK6fEyqRhBsP45jUdcqBivf25hyVkJU>

## 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.

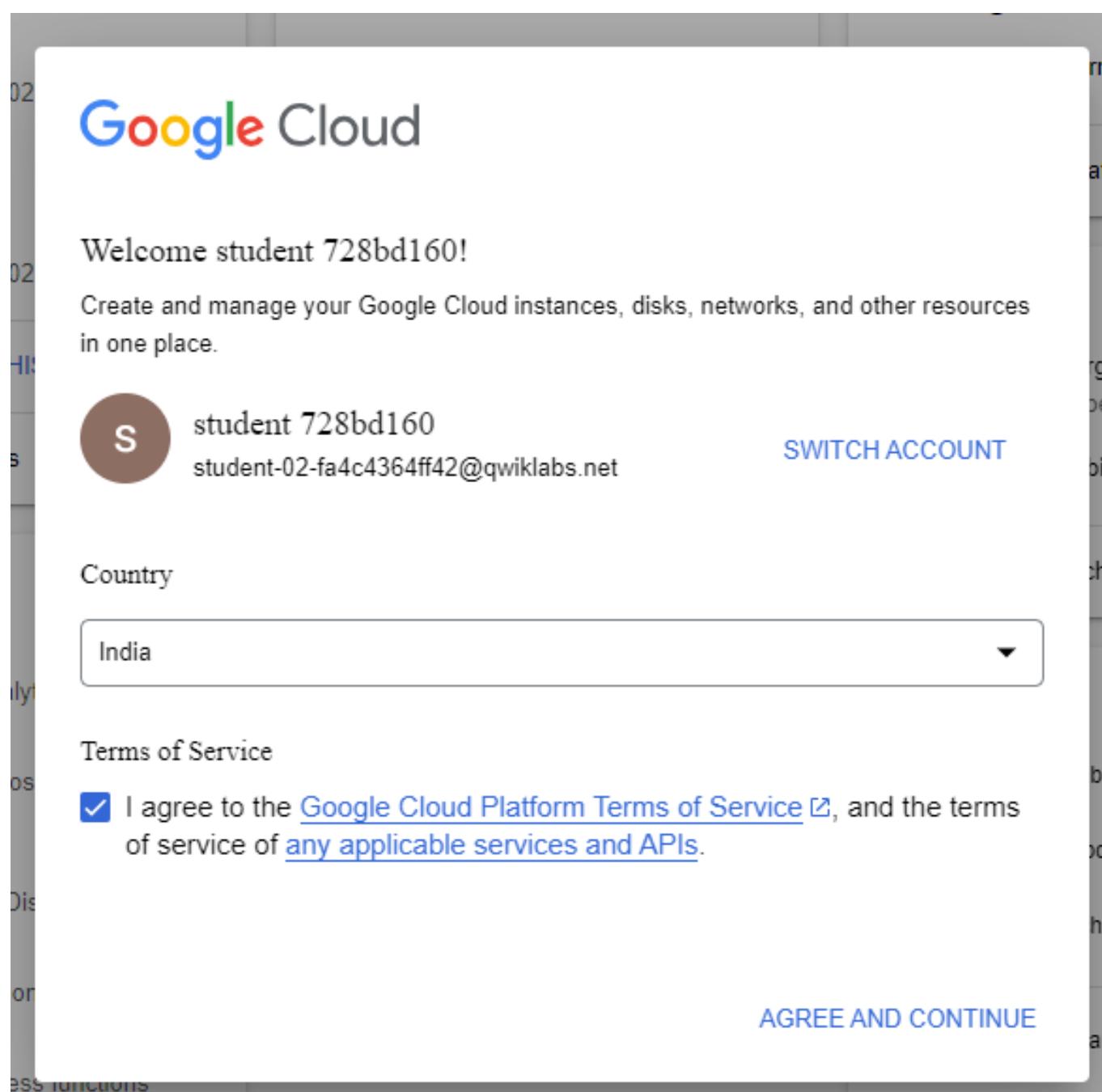
**OUTPUT:**

Figure 1: Credentials Page

The screenshot shows the Google Cloud IAM console interface. The left sidebar is titled "IAM & Admin" and contains the following menu items:

- IAM** (selected)
- PAM
- Principal Access Boundary
- Identity & Organization
- Policy Troubleshooter
- Policy Analyzer **NEW**
- Organization Policies
- Service Accounts
- Workload Identity Federation
- Workforce Identity Federation
- Labels
- Tags
- Settings
- Privacy & Security
- Identity-Aware Proxy
- Roles
- Audit Logs
- Manage Resources
- Release Notes

The main content area is titled "IAM" and "PERMISSIONS". It displays the permissions for the project "qwiklabs-gcp-04-df3028b0afbd". The table lists the principals and their names:

Type	Principal	Name
Compute Engine default service account	10427300012-compute@developer.gserviceaccount.com	Compute Engine default service account
Qwiklabs User Service Account	admiral@qwiklabs-services-prod.iam.gserviceaccount.com	
Qwiklabs User Service Account	qwiklabs-gcp-04-df3028b0afbd@qwiklabs-gcp-04-df3028b0afbd.iam.gserviceaccount.com	Qwiklabs User Service Account
User	student-00-da7df6d082d9@qwiklabs.net	
User	student-02-fa4c4364ff42@qwiklabs.net	student 728bd160

At the bottom of the interface, there is a weather widget showing "80°F Partly sunny" and a navigation bar with icons for Home, Search, and other Google services.

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

Grant access to "qwiklabs-gcp-04-df3028b0afbd"

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

Resource

- qwiklabs-gcp-04-df3028b0afbd

Add principals

Principals are users, groups, domains, or service accounts. [Learn more about principals in IAM](#)

New principals \*  ? X

Assign roles

Roles are composed of sets of permissions and determine what the principal can do with this resource. [Learn more](#)

Role \*  ? ▼

IAM condition (optional) ? + ADD IAM CONDITION trash

Full access to most Google Cloud resources. See the list of included permissions.

[+ ADD ANOTHER ROLE](#)

SAVE CANCEL

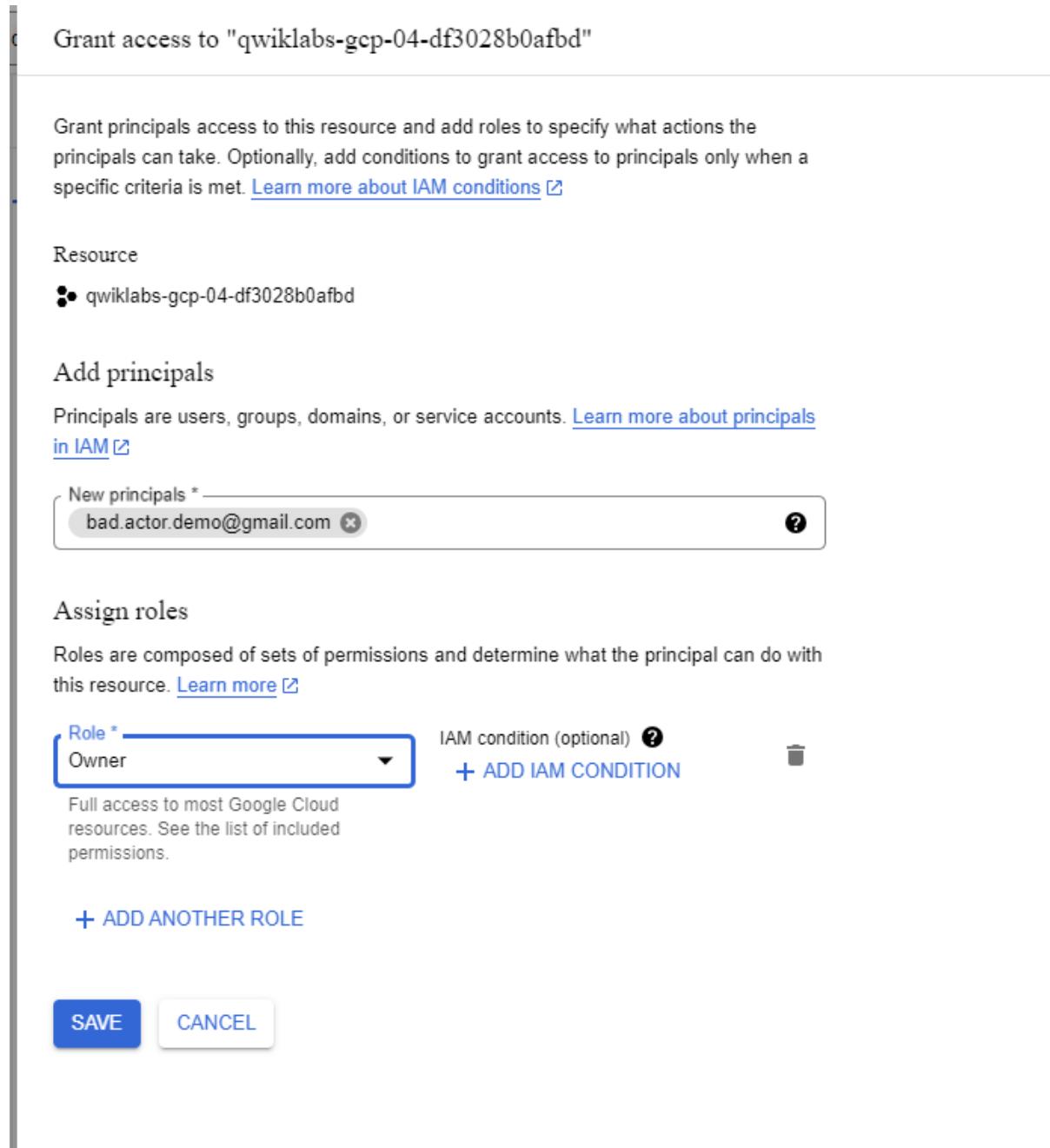


Figure 3 : Adding the external user (bad.actor.demo@gmail.com) as an owner of the project in Google Cloud IAM.

Findings – Security – qwiklabs-gcp-04-df3028b0afbd

console.cloud.google.com/security/command-center/findingsv2;filter=state%3D"ACTIVE"%0AAND%20NOT%20mute%3D"MUTED";timeRange=P7D?project=qwiklabs-gcp-04-df3028b0afbd

Google Cloud Search (I) for resources, docs, products, and more

**Security**

**Findings**

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. You can set a resource-based policy to automatically mute specific findings or resource sets. [Learn more](#)

**CREATE CONFIGURATIONS**

Query preview  
state="ACTIVE" AND NOT mute="MUTED"

Category	Severity	Attack exposure score
Persistence: IAM anomalous grant	High	—
Non org IAM member	High	—
Org policy location restriction	Medium	—
Org policy location restriction	Medium	—
Org policy location restriction	Medium	—

Policy updated

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

The screenshot shows the Google Cloud Security Command Center interface. On the left, there's a sidebar with various navigation options like Risk Overview, Threats, Vulnerabilities, Compliance, Assets, Findings, Sources, and Posture Management. The 'Findings' option is selected. The main area displays a table of findings results. At the top of the table, there are filters for 'State' (with 'Show inactive' and 'Show muted' checkboxes) and 'Category'. One category is selected: 'Persistence: IAM anomalous grant'. The table columns include Category, Severity, Attack exposure score, Event time, Create time, and Finding class. There are five entries listed:

Category	Severity	Attack exposure score	Event time	Create time	Finding class
Persistence: IAM anomalous grant	High	—	Sep 8, 2024, 9:04:45 AM	Sep 8, 2024, 9:04:45 AM	Threat
Non org IAM member	High	—	Sep 8, 2024, 9:04:38 AM	Sep 8, 2024, 9:04:38 AM	Misconfiguration
Org policy location restriction	Medium	—	Sep 8, 2024, 4:56:50 AM	Sep 8, 2024, 8:35:20 AM	Misconfiguration
Org policy location restriction	Medium	—	Sep 8, 2024, 4:56:50 AM	Sep 8, 2024, 8:37:47 AM	Misconfiguration
Org policy location restriction	Medium	—	Sep 8, 2024, 4:56:50 AM	Sep 8, 2024, 8:37:06 AM	Misconfiguration

At the bottom of the interface, there are various links for learning and help, as well as system status indicators like weather and network connection.

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.

**Persistence: IAM anomalous grant**

You can now search for documentation, resource metadata, tutorials, and API keys

**SUMMARY**   **SOURCE PROPERTIES (8)**   **JSON**

**What was detected**

State	Active	state
Severity	High	severity
Event time	September 8, 2024 at 9:04:45 AM GMT+5	event_time
Create time	September 8, 2024 at 9:04:45 AM GMT+5	create_time
Principal email	student-02-fa4c4364ff42@qwiklabs.net	access.principal_email
Caller IP	2401:4900:7c0c:bd53:55f:d7f:c39c:d60	access.caller_ip
Caller IP geo region code	IN	access.caller_ip_geo.region_code
User agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36,gzip(gfe),gzip(gfe)	access.user_agent
Service name	cloudresourcemanager.googleapis.com	access.service_name
Method name	InsertProjectOwnershipInvite	access.method_name

**Affected resource**

Resource display name	qwiklabs-gcp-04-df3028b0afbd	resource.display_name
Resource full name	//clouresourcemanager.googleapis.com/projects/104273300012	resource.name
Resource type	google.cloud.resourcemanagement.Project	resource.type
Project full name	//clouresourcemanager.googleapis.com/projects/104273300012	resource.gcp_metadata.project
Resource path	Navy Projects > gcp_low_extra > gcp_low_extra_navy-04 > qwiklabs-gcp-04-df3028b0afbd	
Cloud provider	Google Cloud	resource.cloudProvider
Security contacts	None	contacts.security
Technical contacts	None	contacts.technical

**Security marks**

No marks

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

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

▼ properties	{ "sensitiveRoleGrant": { "principalEmail": "student-02-fa4c4364ff42@qwiklabs.net", "members": [ "user:bad.actor.demo@gmail.com" ] } }
▼ sensitiveRoleGrant	{ "principalEmail": "student-02-fa4c4364ff42@qwiklabs.net", "members": [ "user:bad.actor.demo@gmail.com" ] }
principalEmail	student-02-fa4c4364ff42@qwiklabs.net
▼ members	[ "user:bad.actor.demo@gmail.com", "user:bad.actor.demo@gmail.com" ]
0	user:bad.actor.demo@gmail.com

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

Which user was granted the owner role in the earliest Persistence: IAM Anomalous Grant finding record?

A Compute Engine service account

None of these options

The external user  
bad.actor.demo@gmail.com

A user belonging to the qwiklabs.net organization

**Submit**

Figure 9 : MCQ

Which user was granted the owner role in the Persistence: IAM Anomalous Grant finding with the latest event time?

The default Compute Engine service account

None of these options

A student user belonging to the qwiklabs.net organization

The external  
bad.actor.demo@gmail.com user

**Submit**

Figure 10 : MCQ

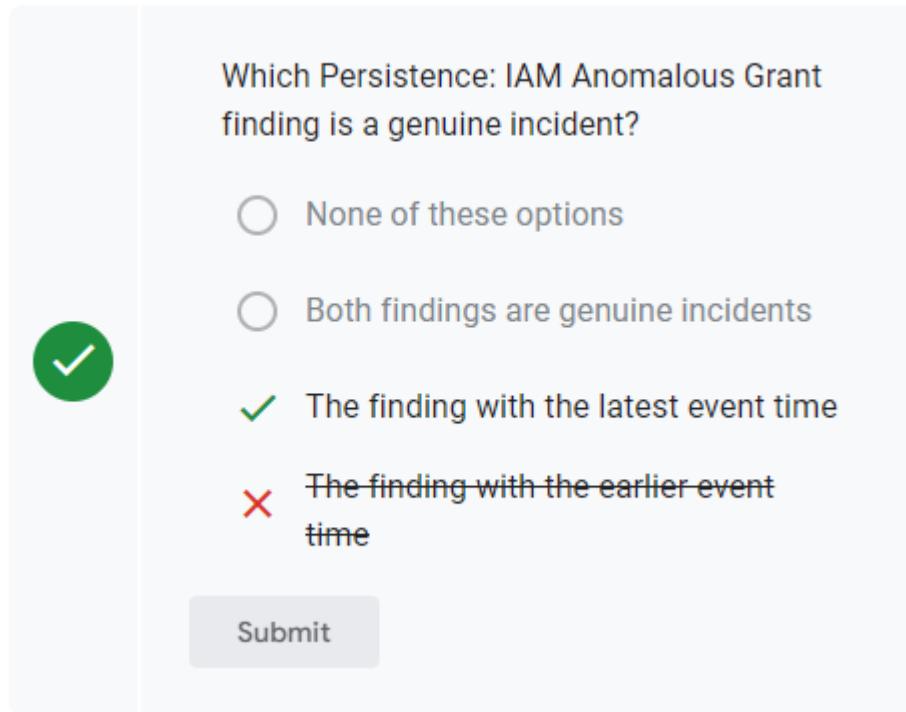


Figure 11 : MCQ

The screenshot shows the Google Cloud Logs Explorer interface. The search query is "logging". The results list several log entries related to IAM permission changes, such as "iam.assetService.SearchAllResources" and "iam.log". The timeline shows events from Sep 8, 8:34 AM to Sep 8, 9:36 AM. The results table has columns for Severity, Time, ID, and Log. The log entries are as follows:

ID	Severity	Time	Log
629	INFO	2024-09-08 09:33:59.638	cloudasset.googleapis.com ..._iamAssetService.SearchAllResources ...
551	INFO	2024-09-08 09:34:00.419	cloudasset.googleapis.com ..._iamAssetService.SearchAllResources ...
351	INFO	2024-09-08 09:34:00.550	cloudasset.googleapis.com ..._iamAssetService.SearchAllResources ...
32	INFO	2024-09-08 09:34:01.202	cloudasset.googleapis.com ..._iamAssetService.SearchAllResources ...
31	INFO	2024-09-08 09:34:03.311	cloudasset.googleapis.com ..._iamAssetService.SearchAllResources ...
23	INFO	2024-09-08 09:34:03.413	cloudasset.googleapis.com ..._iamAssetService.SearchAllResources ...
7	INFO	2024-09-08 09:34:03.413	cloudasset.googleapis.com ..._iamAssetService.SearchAllResources ...
2	INFO	2024-09-08 09:34:03.534	cloudasset.googleapis.com ..._iamAssetService.SearchAllResources ...
2	INFO	2024-09-08 09:34:03.565	cloudasset.googleapis.com ..._iamAssetService.SearchAllResources ...
2	INFO	2024-09-08 09:34:08.489	compute.googleapis.com ..._v1.compute.instances.aggregatedList ...
1	INFO	2024-09-08 09:34:08.879	compute.googleapis.com ..._v1.compute.instances.aggregatedList ...
1	INFO	2024-09-08 09:34:09.307	cloudail.googleapis.com ..._cloudail.instances.list ...
1	INFO	2024-09-08 09:34:09.470	monitoring.googleapis.com ..._log.v3.MetricService.ListTimeSeries ...
1	INFO	2024-09-08 09:34:09.510	monitoring.googleapis.com ..._log.v3.MetricService.ListTimeSeries ...
3	INFO	2024-09-08 09:34:09.571	monitoring.googleapis.com ..._log.v3.MetricService.ListTimeSeries ...
3	INFO	2024-09-08 09:34:09.519	monitoring.googleapis.com ..._log.v3.MetricService.ListTimeSeries ...
3	INFO	2024-09-08 09:34:10.313	cloudBilling.googleapis.com ..._GetResourceBillingInfo ...
111	INFO	2024-09-08 09:34:10.313	monitoring.googleapis.com ..._log.v3.MetricService.ListTimeSeries ...

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

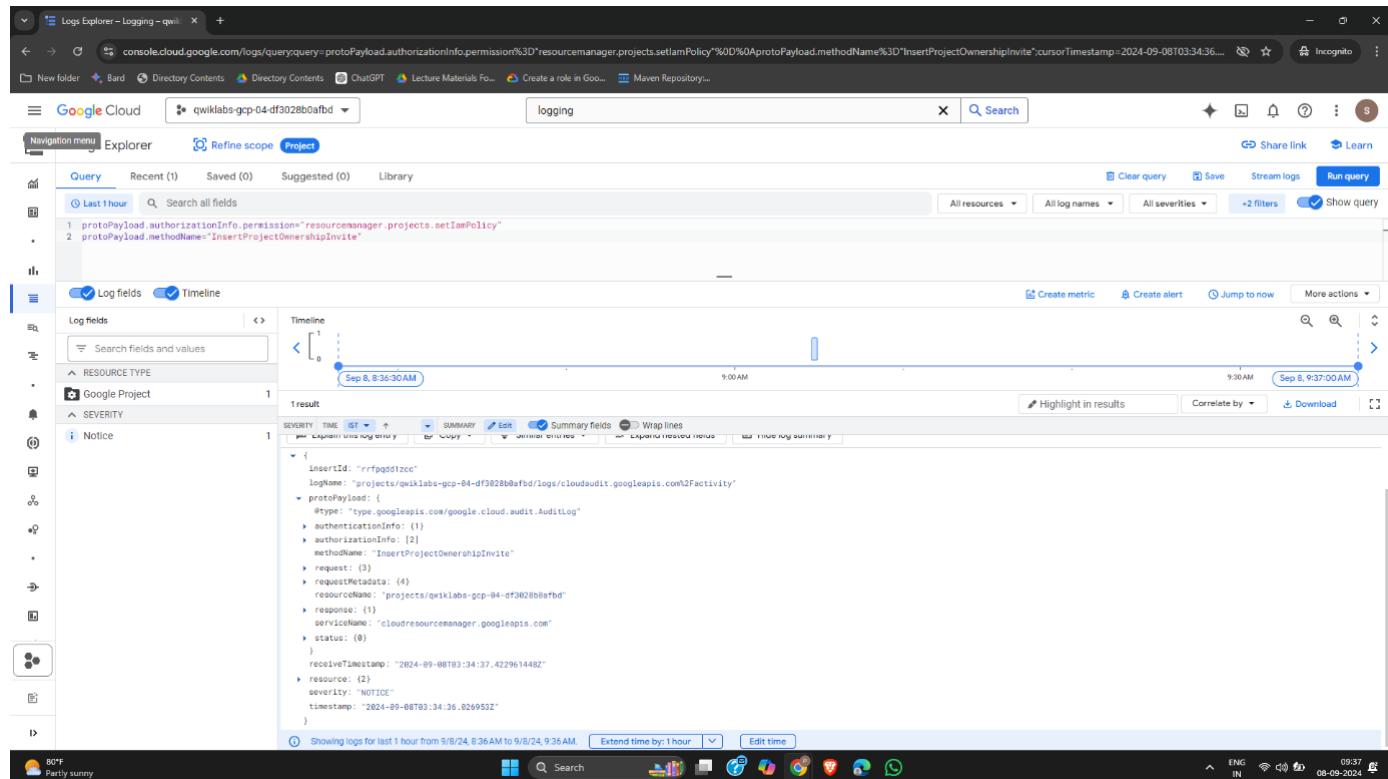


Figure 13 : Examining log entries related to the anomalous IAM grant in Cloud Logging, showing the requester and granted permissions and Detailed view of the anomalous request event showing authentication info and the user who made the request.

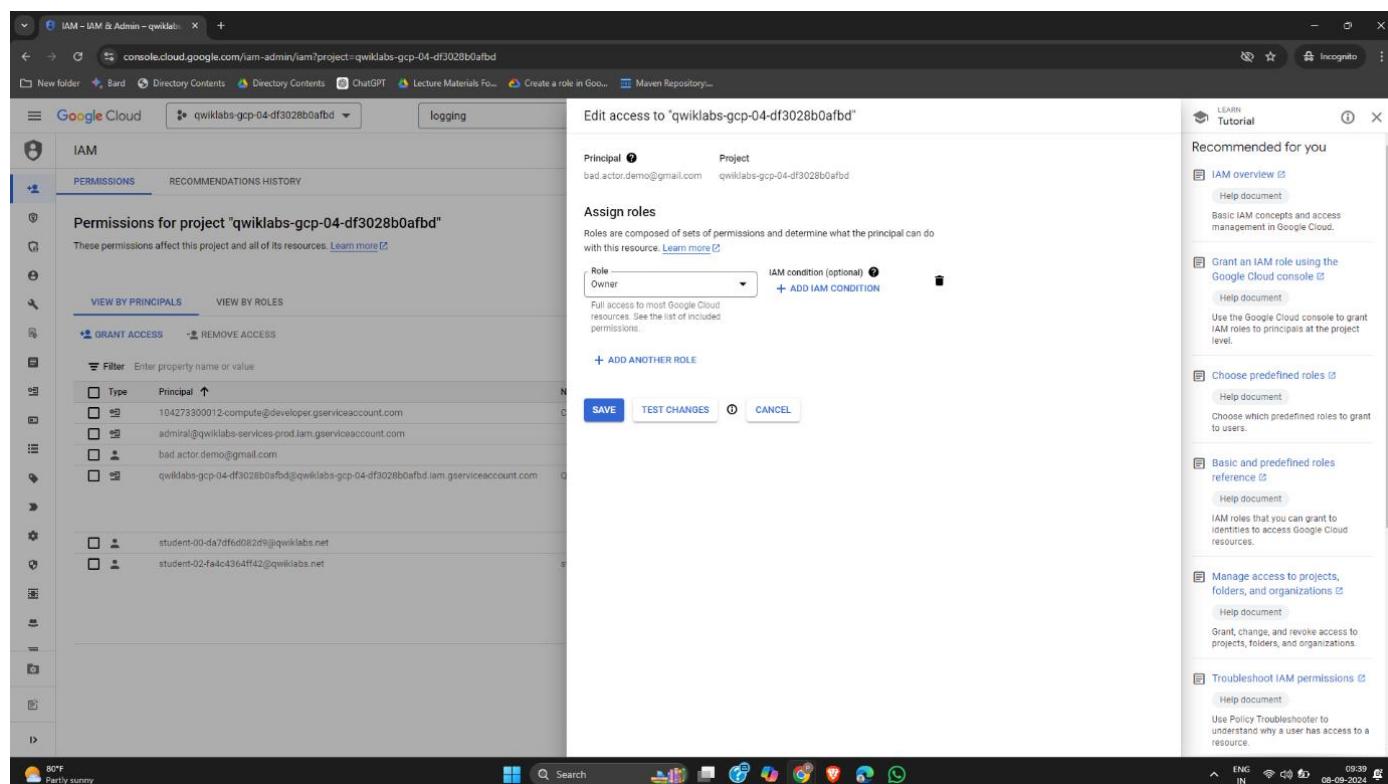


Figure 14 : Removing the project owner role from the external user bad.actor.demo@gmail.com in the IAM console to remediate the malicious finding.

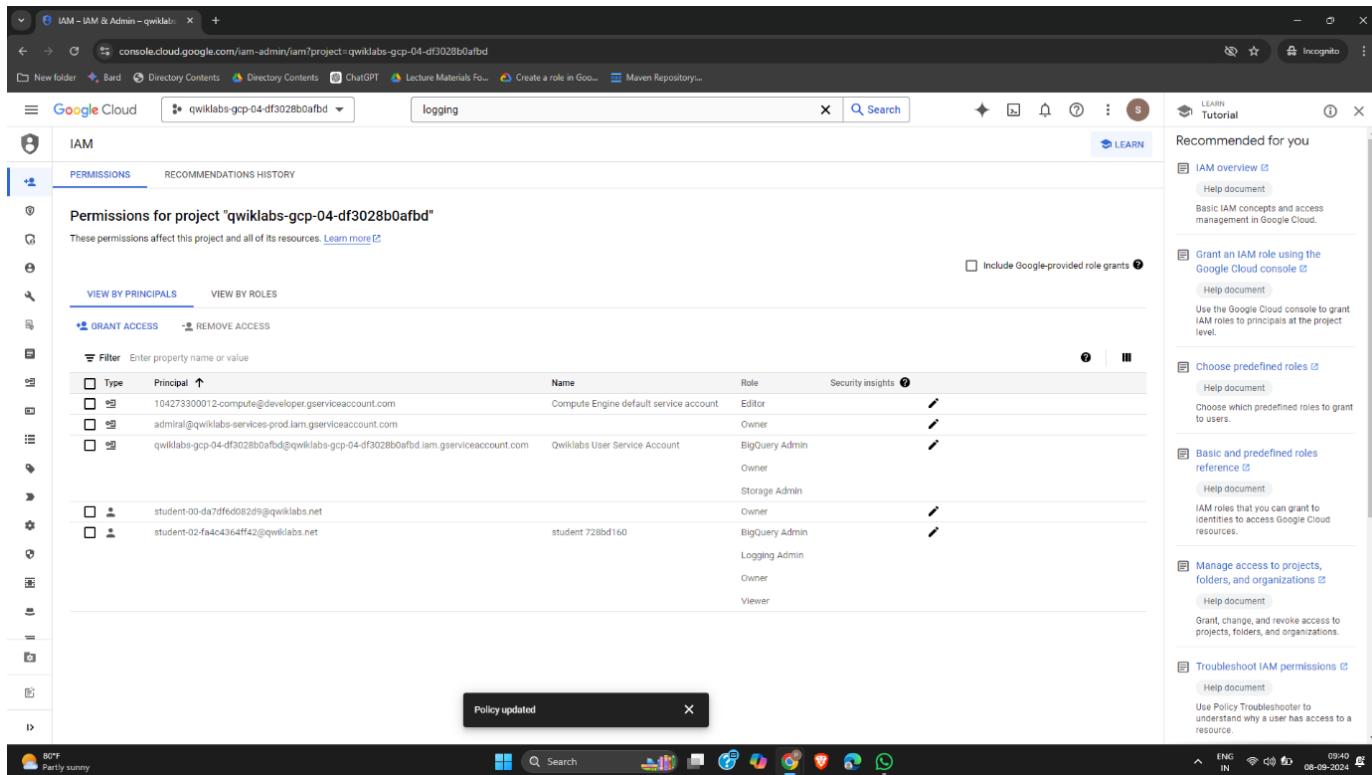


Figure 15 : Confirmation of the IAM role removal and successful remediation of the security incident in Google Cloud IAM.

## 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

The screenshot shows the Google Cloud IAM & Admin Service accounts page for the project "qwiklabs-gcp-02-be9536c706f8". The left sidebar is collapsed. The main area displays a table of service accounts:

Email	Status	Name	Description	Key ID	Key creation date	OAuth 2 Client ID	Actions
<a href="#">72642292873-compute@developer.gserviceaccount.com</a>	Enabled	Compute Engine default service account	No keys			11463581670563562983	⋮
<a href="#">qwiklabs-gcp-02-be9536c706f8@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com</a>	Enabled	Qwiklabs User Service Account	068d724c85f60a4bcc8b3af22016a6c5b3d050d2	Sep 10, 2024	10321946856318912874	⋮	
<a href="#">hank-test-sa@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com</a>	Enabled	Test Service Account for Hank Byrne	89154bb63d9f58055e9fbdd1f4e6ae699974a7	Sep 12, 2024	10059459212561229536	⋮	

The screenshot shows the "Create service account" dialog in the Google Cloud IAM & Admin interface. The left sidebar is collapsed. The dialog has two main sections: "Service account details" and "Grant users access to this service account (optional)".

**Service account details**

- Grant this service account access to project (optional)**
- Grant users access to this service account (optional)**

**Permissions**

Show inherited roles in table

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)

**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**

**Policy updated**



The screenshot shows the Google Cloud IAM & Admin interface. On the left, a sidebar lists various sections like IAM, PAM, and Service Accounts. The main area is titled 'test-account' under the 'Keys' tab. It displays a single key entry:

Type	Status	Key	Creation date	Expiration date
SSH	Active	a9b6f3b1b481d526156989c49161fc7d3c909da9	Sep 12, 2024	Jan 1, 10000

A message at the bottom states: "No change - principal already exists on the policy". The system bar at the bottom shows a battery level of 5.80% and the date/time as 12-09-2024.

The screenshot shows a file browser interface. A file named 'test-account' is selected, with details: Type: JSON Source File, Date modified: 12-09-2024 17:27, Size: 2.34 KB.

The screenshot shows a Cloud Shell terminal window. The user has run the command 'gcloud config set project PROJECT\_ID' to change the project to 'qwiklabs-gcp-02-be9536c706f8'. The terminal output shows the creation of a new key:

```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project ID 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)$ [REDACTED]
```

A message box in the top right says: "Click here to see details about your Cloud Shell session and usage quota". The system bar at the bottom shows a battery level of 17.31% and the date/time as 12-09-2024.

The screenshot shows a second Cloud Shell terminal window with identical content to the first one. It shows the creation of a service account key in the 'qwiklabs-gcp-02-be9536c706f8' project. The terminal output is the same as above.

A message box in the top right says: "Click here to see details about your Cloud Shell session and usage quota". The system bar at the bottom shows a battery level of 17.31% and the date/time as 12-09-2024.

```

student_02_93faf25036ea@cloudshell: ~(qwiklabs-gcp-02-be9536c706f8)$ gcloud auth list
Credentialed Accounts
ACTIVE:
ACCOUNT: student-02-93faf25036ea@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_93faf25036ea@cloudshell: ~(qwiklabs-gcp-02-be9536c706f8)$
  
```

```

To set the active account, run:
$ gcloud config set account "ACCOUNT"
student_02_93faf25036ea@cloudshell: ~(qwiklabs-gcp-02-be9536c706f8)$ export STUDENT2=student-02-20b-e2bb9401b@qwiklabs.net
student_02_93faf25036ea@cloudshell: ~$ gcloud config set account $STUDENT2 --role roles/editor
Updating IAM policy for project [qwiklabs-gcp-02-be9536c706f8].
auditConfigs:
- auditLogConfig:
  - logType: DATA_WRITE
  - logType: DATA_READ
  - logType: ADMIN_READ
  - services: allServices
bindings:
- members:
  - serviceAccounts:qwiklabs-gcp-02-be9536c706f8@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com
  - role: roles/bigquery.admin
- members:
  - serviceAccount:service-7242228273@cloudbuild.gserviceaccount.com
  - role: roles/cloudBuild.build
- members:
  - serviceAccount:service-7242228273@gcp-sa-cloudBuild.iam.gserviceaccount.com
  - role: roles/cloudBuild.serviceAgent
- members:
  - roles:
    - roles/compute.osAdmin
    - roles/compute.osViewer
  - serviceAccount:service-7242228273@compute-system.iam.gserviceaccount.com
  - role: roles/compute.serviceAgent
- members:
  - roles:
    - roles/container.containerEngine
    - roles/container.containerEngineRobot
  - serviceAccount:service-7242228273@container-engine-robot.iam.gserviceaccount.com
  - role: roles/container.serviceAgent
- members:
  - roles:
    - roles/compute.osAdmin
    - roles/compute.osViewer
  - serviceAccount:service-7242228273@compute-developer.gserviceaccount.com
  - serviceAccount:service-7242228273@compute-developer.gserviceaccount.com
  - user:bhd.actor_demo@gmail.com
- members:
  - serviceAccount:service-7242228273@cloudservices.gserviceaccount.com
  - user:student-02-93faf25036ea@qwiklabs.net
  - user:student-02-93faf25036ea@qwiklabs.net
  - role: roles/editor
members:
- serviceAccount:service-7242228273@compute-developer.gserviceaccount.com
- serviceAccount:service-7242228273@notebooks.iam.gserviceaccount.com
- serviceAccount:service-7242228273@notebooks.iam.gserviceaccount.com
- serviceAccount:admin@qwiklabs-services-prod.iam.gserviceaccount.com
- serviceAccount:task-test-asd@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com
- serviceAccount:task-test-abc@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com
- serviceAccount:test-account@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com
  - member: student-02-93faf25036ea@qwiklabs.net
  - role: roles/owner
  - members:
    - serviceAccount:task-test-asd@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com
    - serviceAccount:task-test-abc@qwiklabs-gcp-02-be9536c706f8.iam.gserviceaccount.com
    - role: roles/storage.admin
  - members:
    - user:student-02-93faf25036ea@qwiklabs.net
  
```

The screenshot shows the Google Cloud Platform dashboard for project "qwiklabs-gcp-02-be9536c706f8". The left sidebar lists pinned products like APIs & Services, Billing, IAM & Admin, Marketplace, Vertex AI, Compute Engine, Kubernetes Engine, Cloud Storage, BigQuery, VPC Network, Cloud Run, SQL, Security, and Google Maps Platform. The main area displays "Project info" with details like project name, number, and ID. It also shows "Compute Engine" metrics for CPU utilization (0.13%) and API requests over time. A "Getting Started" section for APIs is present.

The screenshot shows the Google Cloud Security Command Center findings page. It features a "Get accurate attack exposure scores" section and a "Findings query results" table. The table lists findings such as "Persistence: IAM anomalous grant" (High severity, threat), "Discovery: service account self-investigation" (Low severity, threat), "Primitive roles used" (Medium severity, misconfig), and "User managed service account key" (Medium severity, misconfig). The left sidebar includes sections for Security Command Center, Risk Overview, Threats, Vulnerabilities, Compliance, Assets, and Findings. A right sidebar provides links to learn more about security command center findings, threats, vulnerabilities, and more.

**Findings**

**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 muted="MUTED"

**Quick filters** **CLEAR ALL** **EDIT QUERY** **Time range** Last 7 days **EXPORT** **COLUMNS**

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
<b>User managed service account key</b>	Medium	—	Sep 12, 2024, 5:27:17 PM	Sep 12, 2024, 5:27:17 PM	Miscor
Admin service account	Medium	0	Sep 12, 2024, 5:25:17 PM	Sep 10, 2024, 11:21:01 PM	Miscor
Persistence: IAM anomalous grant	High	—	Sep 12, 2024, 3:39:17 PM	Sep 12, 2024, 3:39:17 PM	Threat

Rows per page: 30 | 1 - 30 of 54

**LEARN** **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

**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
Google	Active	a9b6f3b1b481d526156989c49161fc7d3c909da9	Sep 12, 2024	Jan 1, 10000

<https://console.cloud.google.com/iam-admin/serviceaccounts/details/117795094062525820/keys/aut...>

Finance headline: US Core inflati...

The screenshot shows the Google Cloud IAM & Admin console. On the left, there's a sidebar with various navigation options like IAM, PAM, Principal Access Boundary, Identity & Organization, Policy Troubleshooter, Policy Analyzer (which is highlighted in blue), Organization Policies, Service Accounts, Workload Identity Federations, Labels, Tags, Settings, Privacy & Security, Identity-Aware Proxy, Roles, and Manage Resources. The main area is titled 'test-account' under 'IAM & Admin'. It shows a 'Keys' tab selected. A modal window titled 'Delete key ID' is open, asking if you want to delete a specific key. The key details shown are: Type: RSA, Status: Active, Key ID: a9b6f301b481d526156989c49161fc7d3c909da9. There are 'Delete' and 'Cancel' buttons at the bottom of the modal.

The screenshot shows a Google Cloud Skills Boost lab conclusion page. At the top, it says 'End Lab' and '01:07:22'. Below that, there's a note: 'Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.' To the right, there's a yellow box containing a summary of completed tasks with their status: '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), and 'Delete the key' (Check my progress, 25/25). Further down, there are links for 'Task 3. Trigger the false positive finding', 'Task 4. Sign in as the second user', 'Task 5. View the threat finding in SCC', 'Task 6. Fix the finding', 'Conclusion', and 'End your lab'. At the bottom, there are 'Previous' and 'Next' buttons, and the system status bar shows 'ENG IN' and the date '12-09-2024'.

The screenshot shows a Google Cloud Skills Boost lab interface. On the left, there's a sidebar with navigation links like 'Dashboard', 'Paths', 'Explore', 'Profile', and 'Subscriptions'. A central panel displays a 'Conclusion' section with a timer showing '01:07:09'. Below the timer, there's a message about staying in the console and a link to 'Open Google Cloud console'. There are also fields for 'Google Cloud username 1' (student-02-93faf258366) and 'Google Cloud password' (kK7nabQhjP3f). A 'Google Cloud project ID' field contains 'quwiklabs-gcp-02-be9536'. To the right, a large yellow box contains four actions: 'Create a service account', 'Create a JSON authentication key for your service account', 'Assign excessive permissions to trigger threat detection', and 'Delete the key'. At the bottom, there's a 'Sign Out' button and links for 'Privacy · Terms', 'Task 5. View the threat finding in SCC', 'Task 6. Fix the finding', 'Conclusion', and 'End your lab'. The top of the screen shows a browser window with multiple tabs related to Google Cloud and IAM.

## 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:

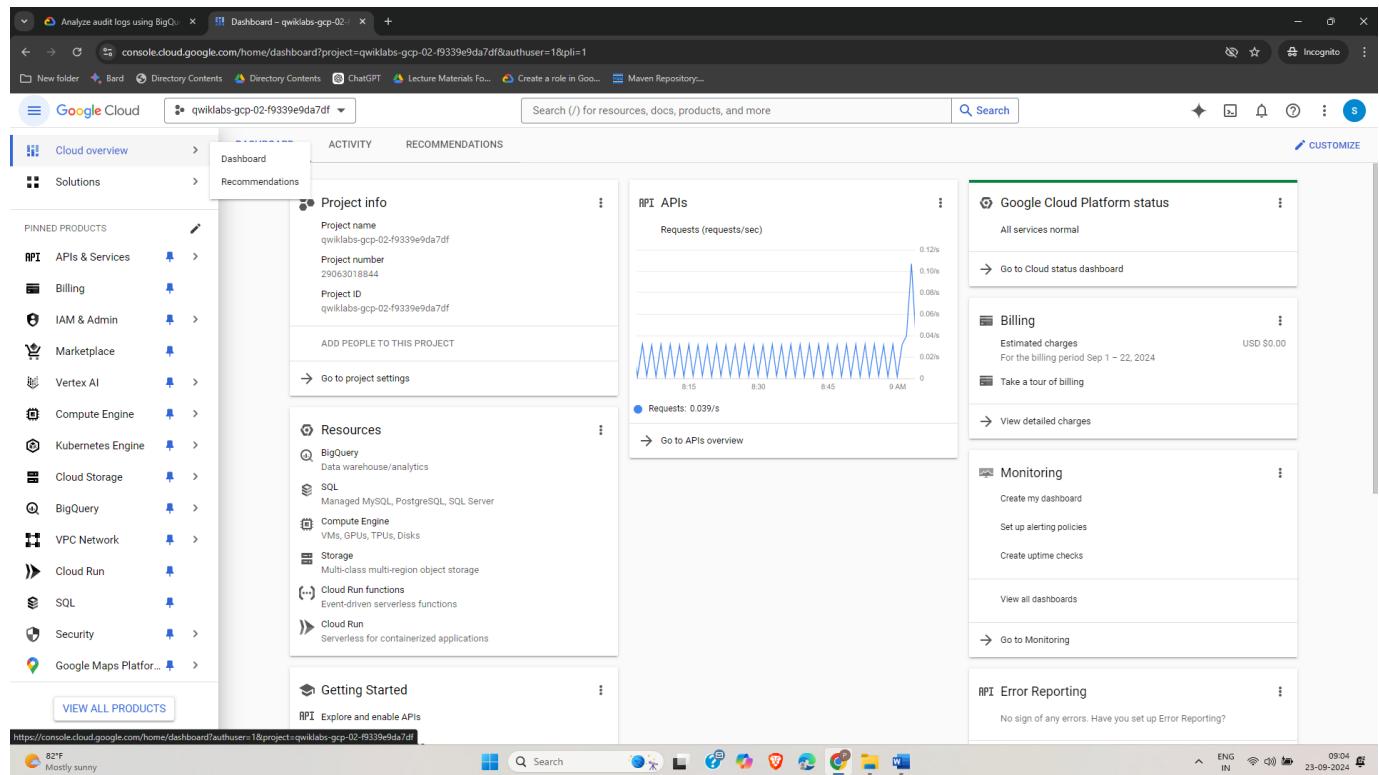


Figure 1 : Successful login using credentials for Username 1.

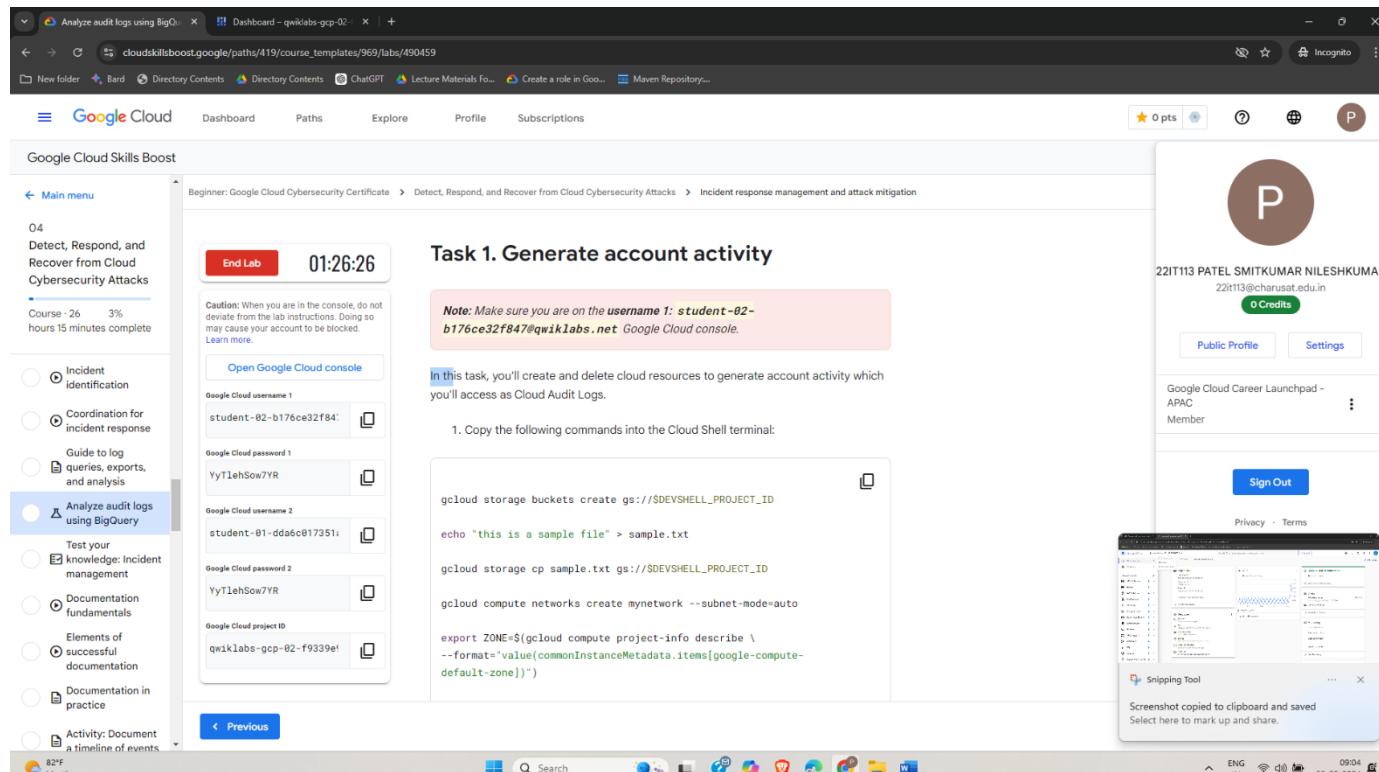


Figure 2 : The initial reference screen after logging in.

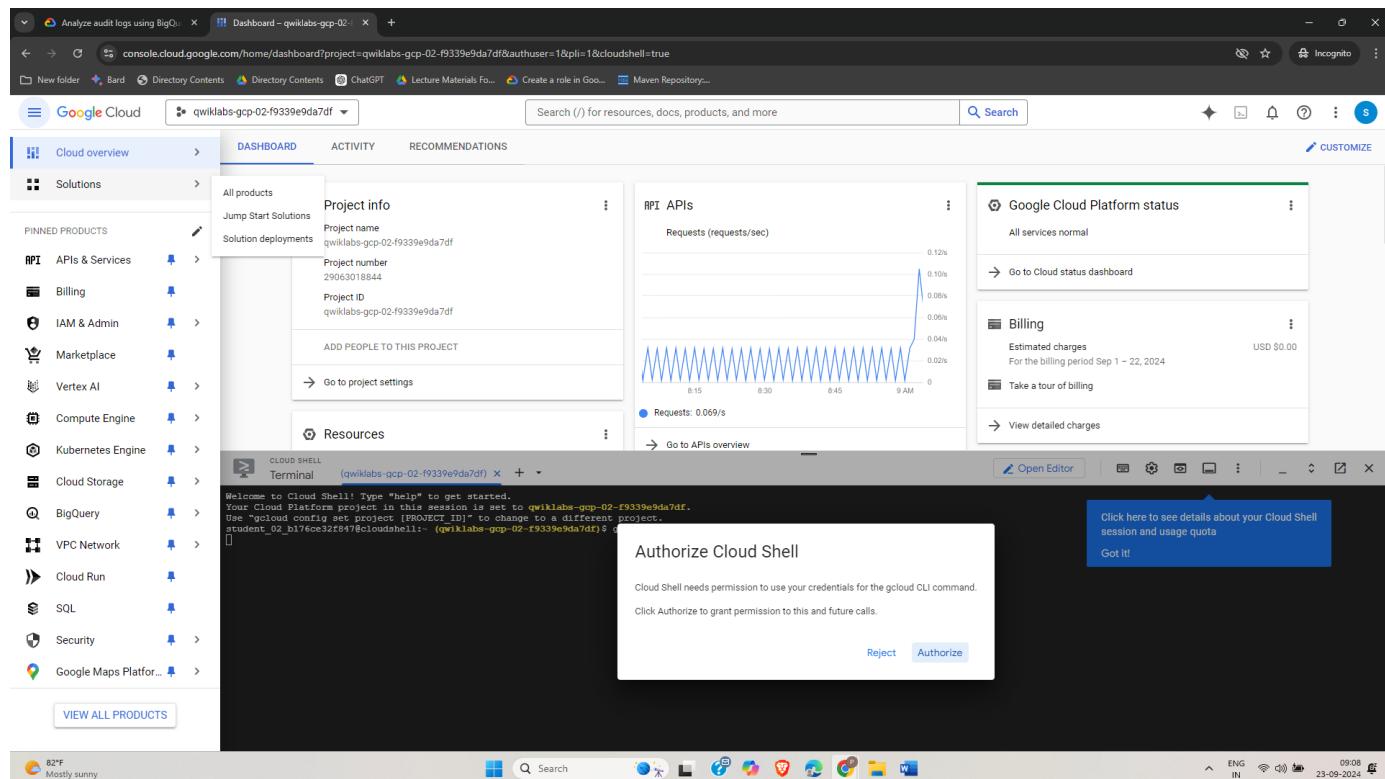


Figure 3 : Authorization request within Cloud Shell for accessing resources.

```
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.

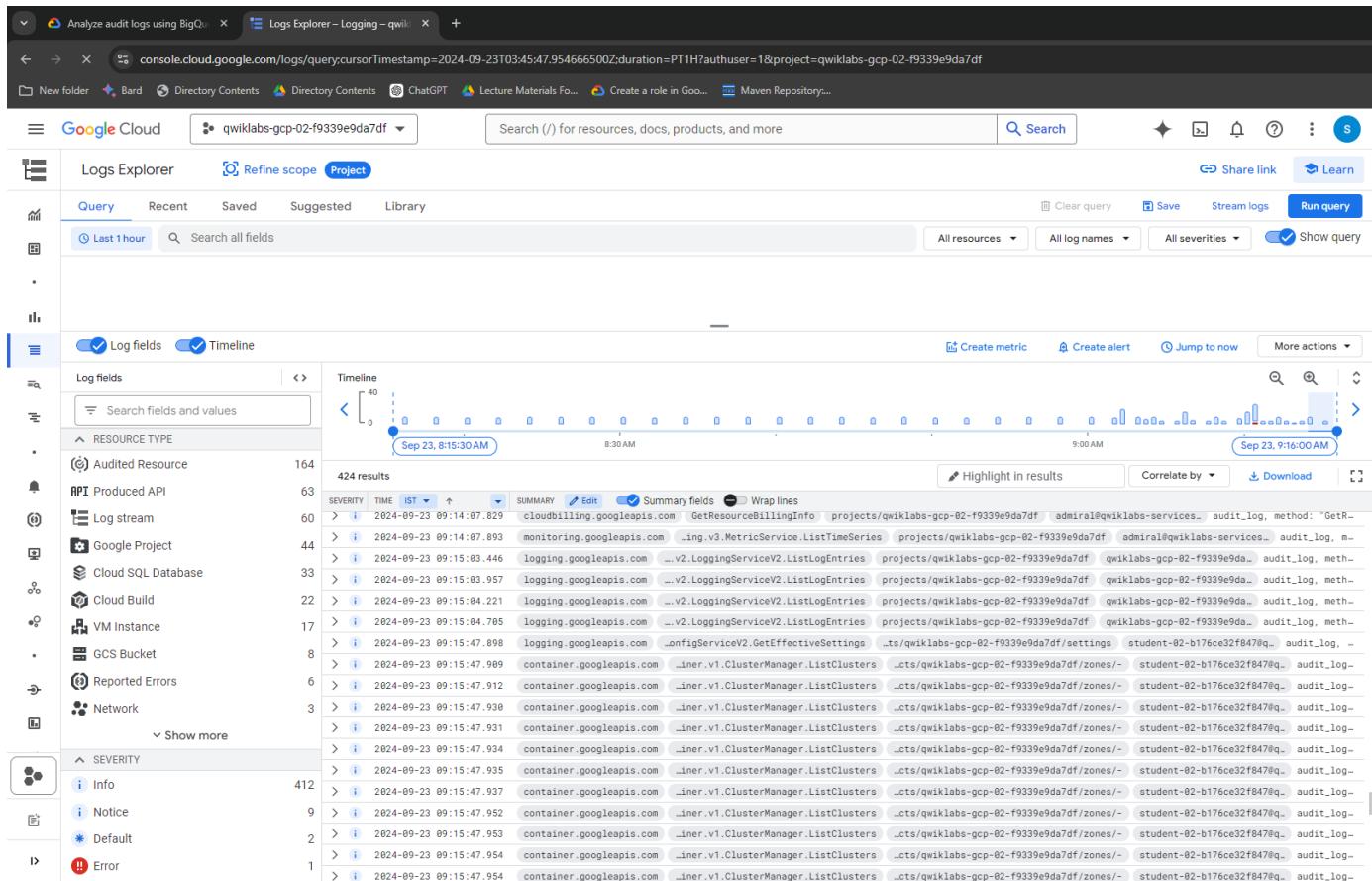


Figure 6 : Navigating to Cloud Logging using the Cloud Logging Explorer.

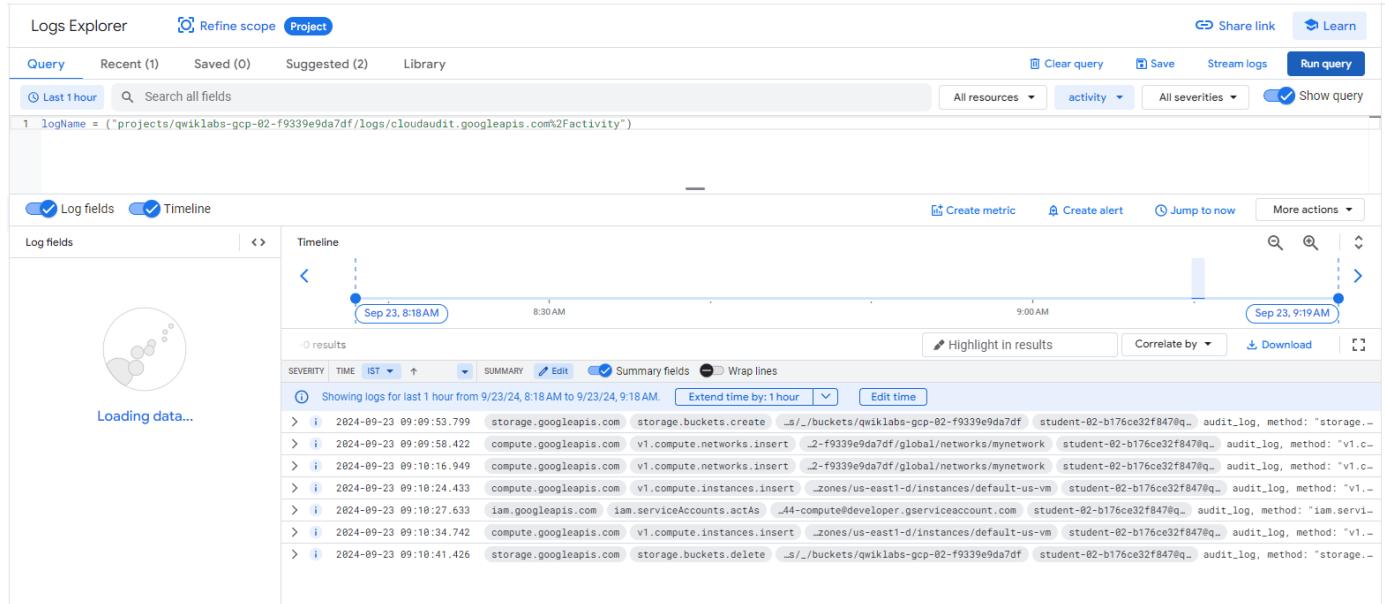


Figure 7 : Running a query in the Query Editor to find log activity.

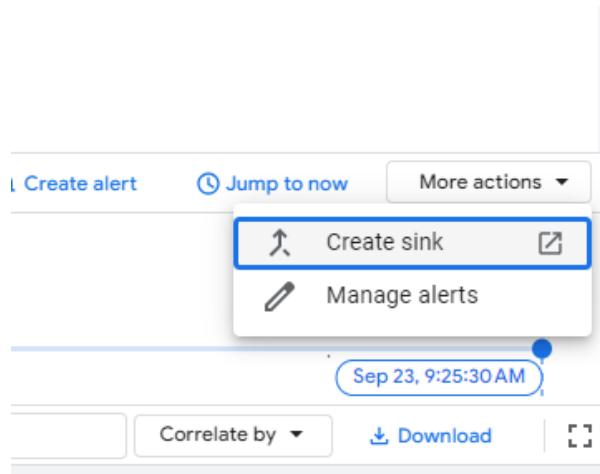


Figure 8 : Proceeding to create a log sink for audit log export.

### ① Sink details

Provide a name and description for logs routing sink

Sink name \*  
AuditLogsExport

Sink description

[Next](#)

Figure 9 : Inputting a name for the log sink.

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

## 2 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.

Select sink service \* –  
BigQuery dataset

Select BigQuery dataset \* –  
auditlogs\_dataset

Use partitioned tables [?](#)

[Next](#)

Figure 11 : Successfully creating the auditlog\_dataset in BigQuery.

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

Build inclusion filter Preview logs 

Press Alt+F1 for accessibility options.

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

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	BigQuery dataset
Destination	bigrquery.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.

The screenshot shows the Google Cloud Log Router interface. At the top, there's a navigation bar with tabs like 'Analyze audit logs using BigQ...', 'Logs Explorer - Logging - qwik...', and 'Log Router - Logging - qwik...'. Below the navigation bar, the main area has a sidebar with icons for 'Log Router Volume' (1.51 MB), 'Log Buckets only', 'Volume by destination type' (chart), 'Create alerting policy', and 'Billable Volume from other projects' (0 B). The main content area is titled 'Log Router Sinks' and lists three sinks:

Enabled	Type	Name	Description	Destination	Volume	Created	Last updated
<input checked="" type="checkbox"/>	Logging bucket	_Default		logging.googleapis.com/projects/qwiklabs-gcp-02-f9339e9da7df/locations/global/buckets/_Default	1.51 MB	2024-09-23 09:30:47.404 IST	2024-09-23 09:30:47.404 IST
<input checked="" type="checkbox"/>	Logging bucket	_Required		logging.googleapis.com/projects/qwiklabs-gcp-02-f9339e9da7df/locations/global/buckets/_Required	150.04 KB	2024-09-23 09:30:47.404 IST	2024-09-23 09:30:47.404 IST
<input checked="" type="checkbox"/>	BigQuery dataset	AuditLogsExport		bigrquery.googleapis.com/projects/qwiklabs-gcp-02-f9339e9da7df/datasets/auditlogs_dataset	0 B	2024-09-23 09:30:47.404 IST	2024-09-23 09:30:47.404 IST

At the bottom, there's a system tray showing weather (83°F, mostly sunny), network status, and system date/time (23-09-2024, 09:32).

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

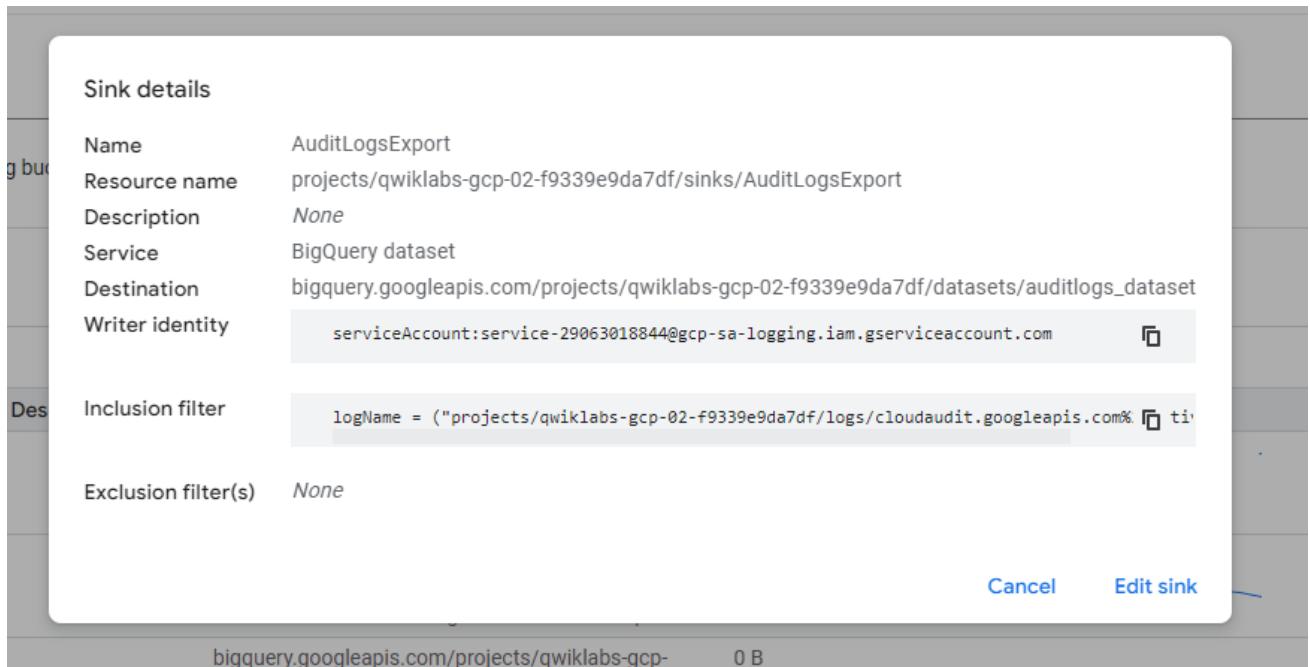


Figure 15 : Viewing the created sink in Log Routing.

```

CLOUD SHELL
Terminal (qwiklabs-gcp-02-f9339e9da7df) X + ▾

Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to qwiklabs-gcp-02-f9339e9da7df.
Use "gcloud config set project [PROJECT_ID]" to change to a different project.
student_02_b176ce32f847@cloudshell:~ (qwiklabs-gcp-02-f9339e9da7df)$
gcloud storage buckets create gs://$DEVSHELL_PROJECT_ID

gcloud storage buckets create gs://$DEVSHELL_PROJECT_ID-test
echo "this is another sample file" > sample2.txt
gcloud storage cp sample.txt gs://$DEVSHELL_PROJECT_ID-test
export ZONE=$(gcloud compute project-info describe \
--format="value(commonInstanceMetadata.items[google-compute-default-zone])")

gcloud compute instances delete --zone=$ZONE \
--delete-disks=all default-us-vm
Creating gs://qwiklabs-gcp-02-f9339e9da7df/...
Creating gs://qwiklabs-gcp-02-f9339e9da7df-test/...
Copying file://sample.txt to gs://qwiklabs-gcp-02-f9339e9da7df-test/sample.txt
Completed files 1/1 | 22.0B/22.0B
The following instances will be deleted. Any attached disks configured to be auto-deleted will be deleted unless they are attached
irreversible and any data on the disk will be lost.
- [default-us-vm] in [us-east1-d]

Do you want to continue (Y/n)? Y

Deleted [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-02-f9339e9da7df/zones/us-east1-d/instances/default-us-vm].
student_02_b176ce32f847@cloudshell:~ (qwiklabs-gcp-02-f9339e9da7df)$
student_02_b176ce32f847@cloudshell:~ (qwiklabs-gcp-02-f9339e9da7df)$

```

Figure 16 : Creating and deleting a simple storage bucket.

```

student_02_b176ce32f847@cloudshell:~ (qwiklabs-gcp-02-f9339e9da7df)$
student_02_b176ce32f847@cloudshell:~ (qwiklabs-gcp-02-f9339e9da7df)$ gcloud storage rm --recursive gs://$DEVSHELL_PROJECT_ID
gcloud storage rm --recursive gs://$DEVSHELL_PROJECT_ID-test
Removing objects:
Completed 0
Removing buckets:
Removing gs://qwiklabs-gcp-02-f9339e9da7df/...
Completed 1/1
Removing objects:
Removing gs://qwiklabs-gcp-02-f9339e9da7df-test/sample.txt#1727064404731339...
Completed 1/1
Removing buckets:
Removing gs://qwiklabs-gcp-02-f9339e9da7df-test/...
Completed 1/1
student_02_b176ce32f847@cloudshell:~ (qwiklabs-gcp-02-f9339e9da7df)$

```

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

```

Your Cloud Platform project in this session is set to lqwiklabs-gcp-02-f9339e9da7df.
Use "gcloud config set project PROJECT_ID" to change to a different project.
Switched to project lqwiklabs-gcp-02-f9339e9da7df
gcloud storage buckets create gs://$DEVSHELL_PROJECT_ID

gcloud storage buckets create gs://$DEVSHELL_PROJECT_ID-test
echo "this is another sample file" > sample2.txt
gcloud storage cp sample.txt gs://$DEVSHELL_PROJECT_ID-test
export ZONE=$(_gcloud compute project-info describe \
--format="value(commonInstanceMetadata.items[google-compute-default-zone]")

gcloud compute instances delete --zone=$ZONE \
--delete-disk=all default-us-vm
Creating gs://lqwiklabs-gcp-02-f9339e9da7df...
Completed file 1/1 [22.08/22.08]
Copying file:/sample.txt to gs://lqwiklabs-gcp-02-f9339e9da7df/test/sample.txt
Completed file 1/1 [22.08/22.08]

The following disk(s) will be deleted: Any attached disks configured to be auto-deleted will be deleted unless they are attached to any other instances or the '--keep-disks' flag is given and specifies them for keeping. Deleting a disk is irreversible and any data on the disk will be lost.
- [default-us-vm] in [us-east1-d]

Do you want to continue (Y/n)? Y

Deleted [https://www.googleapis.com/compute/v1/projects/lqwiklabs-gcp-02-f9339e9da7df/zones/us-east1-d/instances/default-us-vm].
gsutil rm -r gs://lqwiklabs-gcp-02-f9339e9da7df
student_02_b1f6cc32f847@cloudshell: ~(lqwiklabs-gcp-02-f9339e9da7df)$ gcloud storage rm --recursive gs://$DEVSHELL_PROJECT_ID-test

gcloud storage rm --recursive gs://$DEVSHELL_PROJECT_ID-test
Removing objects:
  Composing...
  Removing buckets:
    Removing gs://lqwiklabs-gcp-02-f9339e9da7df/...
      Completed 1/1
    Removing gs://lqwiklabs-gcp-02-f9339e9da7df-test/...
      Completed 1/1
    Removing buckets:
      Removing gs://lqwiklabs-gcp-02-f9339e9da7df-test/...
        Completed 1/1
      student_02_b1f6cc32f847@cloudshell: ~(lqwiklabs-gcp-02-f9339e9da7df)$
  
```

Figure 18 : Logging out of the Username 1 account.

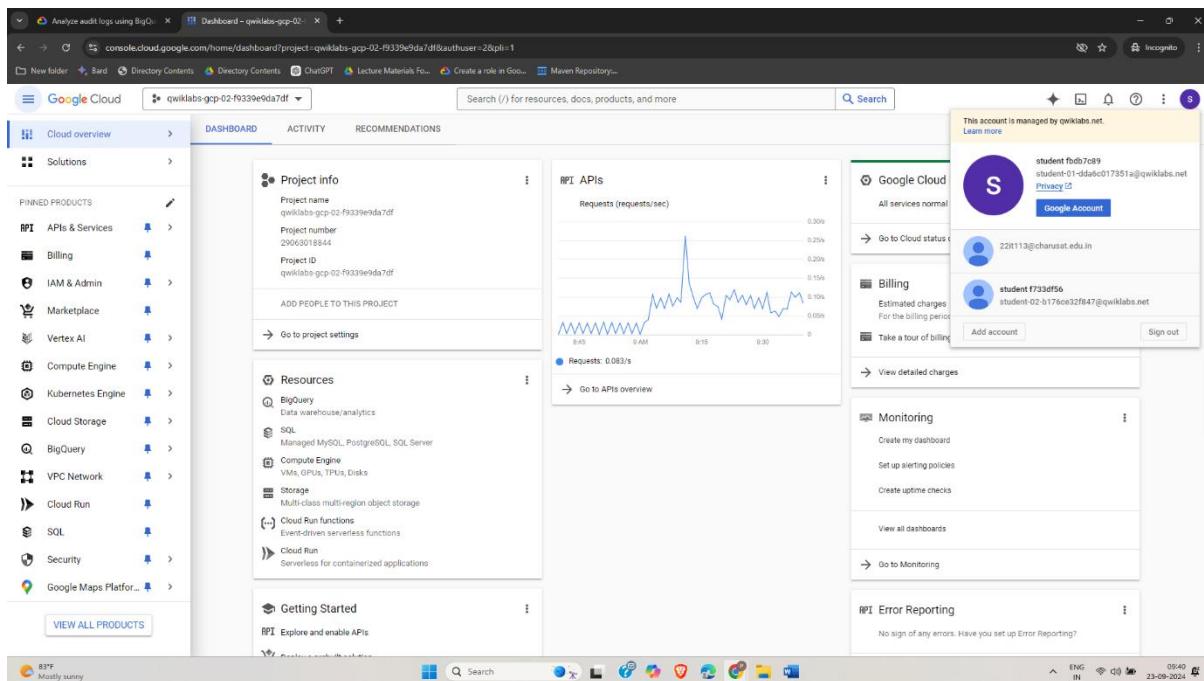


Figure 19 : Logging in with credentials for Username 2.

The screenshot shows the Google Cloud Logs Explorer interface. A search query is entered: `logName = ('projects/qwiklabs-gcp-02-f9339e9da7df/logs/cloudaudit.googleapis.com%2Factivity')`. The results pane displays 1,365 log entries from September 23, 2024, between 09:39:49 and 09:42:00. The logs are categorized by severity (Info, Notice, Error, Default) and resource type (GKE Cluster Operations, Log stream, Audited Resource, API Produced API, Google Project, Cloud SQL Database, Cloud Build, GCS Bucket, VM Instance, Reported Errors). One specific log entry is highlighted:

```

2024-09-23 09:40:13.828 storage.googleapis.com storage.buckets.delete .../buckets/qwiklabs-gcp-02-f9339e9da7df student-02-b176ce32f847eq_ audit_log, method: "storage.buckets.delete", principal_email: "student-02-...
2024-09-23 09:40:13.842 storage.googleapis.com storage.buckets.delete .../buckets/qwiklabs-gcp-02-f9339e9da7df student-02-b176ce32f847eq_ audit_log, method: "storage.buckets.delete", principal_email: "student-02-...
2024-09-23 09:40:13.361 storage.googleapis.com storage.buckets.delete .../buckets/qwiklabs-gcp-02-f9339e9da7df-test student-02-b176ce32f847eq_ audit_log, method: "storage.buckets.delete", principal_email: "student-02-...

```

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

The screenshot shows the Google Cloud Logs Explorer interface with a query: `storage.googleapis.com storage.buckets.delete`. The results pane displays 3 log entries from September 23, 2024, between 09:10:41 and 09:48:13. The logs are categorized by severity (Info, Notice, Error, Default) and resource type (GKE Cluster Operations, Log stream, Audited Resource, API Produced API, Google Project, Cloud SQL Database, Cloud Build, GCS Bucket, VM Instance, Reported Errors). One specific log entry is highlighted:

```

2024-09-23 09:10:41.426 storage.googleapis.com storage.buckets.delete .../buckets/qwiklabs-gcp-02-f9339e9da7df student-02-b176ce32f847eq_ audit_log, method: "storage.buckets.delete", principal_email: "student-02-...
2024-09-23 09:38:13.842 storage.googleapis.com storage.buckets.delete .../buckets/qwiklabs-gcp-02-f9339e9da7df student-02-b176ce32f847eq_ audit_log, method: "storage.buckets.delete", principal_email: "student-02-...
2024-09-23 09:38:13.361 storage.googleapis.com storage.buckets.delete .../buckets/qwiklabs-gcp-02-f9339e9da7df-test student-02-b176ce32f847eq_ audit_log, method: "storage.buckets.delete", principal_email: "student-02-...

```

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

The screenshot shows the Google Cloud Logs Explorer interface with a query: `storage.googleapis.com storage.buckets.delete`. The results pane displays 3 log entries from September 23, 2024, between 09:10:41 and 09:48:13. The logs are categorized by severity (Info, Notice, Error, Default) and resource type (GKE Cluster Operations, Log stream, Audited Resource, API Produced API, Google Project, Cloud SQL Database, Cloud Build, GCS Bucket, VM Instance, Reported Errors). One specific log entry is highlighted, showing the principal\_email:

```

2024-09-23 09:10:41.426 storage.googleapis.com storage.buckets.delete .../buckets/qwiklabs-gcp-02-f9339e9da7df student-02-b176ce32f847eq_ audit_log, method: "storage.buckets.delete", principal_email: "student-02-...
2024-09-23 09:38:13.842 storage.googleapis.com storage.buckets.delete .../buckets/qwiklabs-gcp-02-f9339e9da7df student-02-b176ce32f847eq_ audit_log, method: "storage.buckets.delete", principal_email: "student-02-...
2024-09-23 09:38:13.361 storage.googleapis.com storage.buckets.delete .../buckets/qwiklabs-gcp-02-f9339e9da7df-test student-02-b176ce32f847eq_ audit_log, method: "storage.buckets.delete", principal_email: "student-02-...

```

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

The screenshot shows the Google Cloud Query Editor interface. A log entry is displayed in the editor:

```

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.

3 results

SEVERITY	TIME	IST	↑	↓	SUMMARY	Edit	Summary fields	Wrap lines
<pre>insertId: "zjzz24ed7lyo" logName: "projects/qwiklabs-gcp-02-f9339e9da7df/logs/claudaudit.googleapis.com%2Factivity" protoPayload: {   @type: "type.googleapis.com/google.cloud.audit.AuditLog"   authenticationInfo: {     principalEmail: "student-02-b176ce32f847@qwiklabs.net"   }   authorizationInfo: [2]   methodName: "storage.buckets.delete"   requestMetadata: {4}   resourceLocation: {1}   resourceName: "projects/_/buckets/qwiklabs-gcp-02-f9339e9da7df"   serviceName: "storage.googleapis.com"</pre>								

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

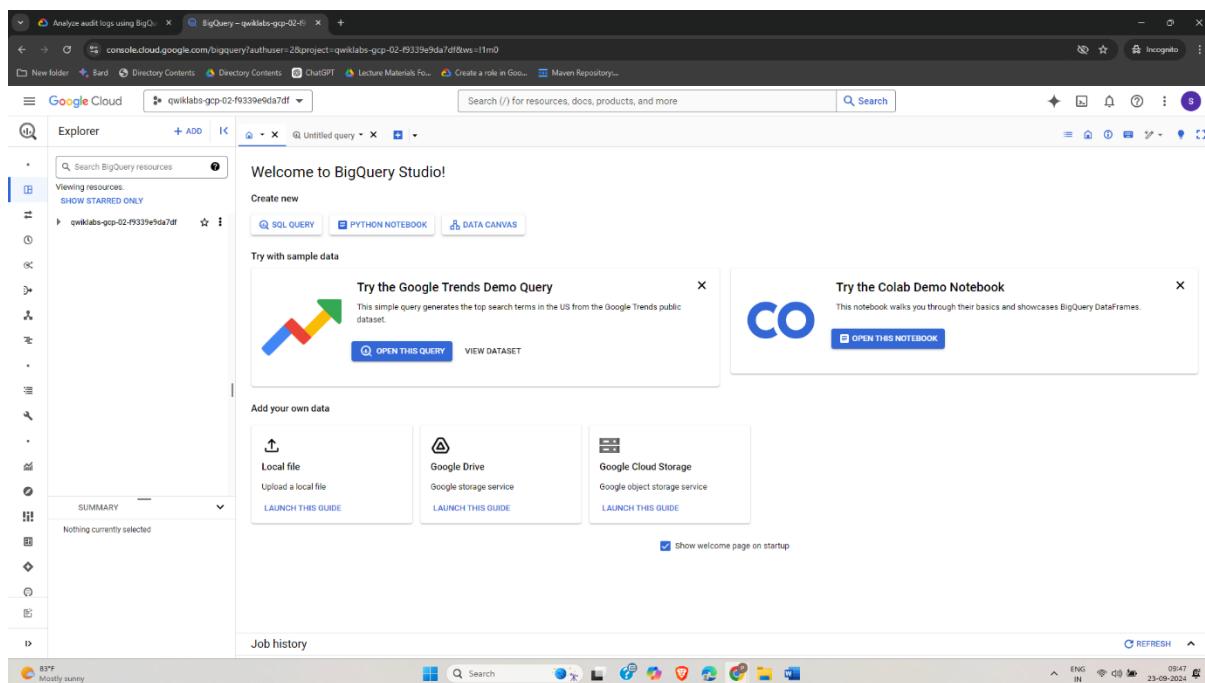


Figure 25 : Navigating to BigQuery Studio.

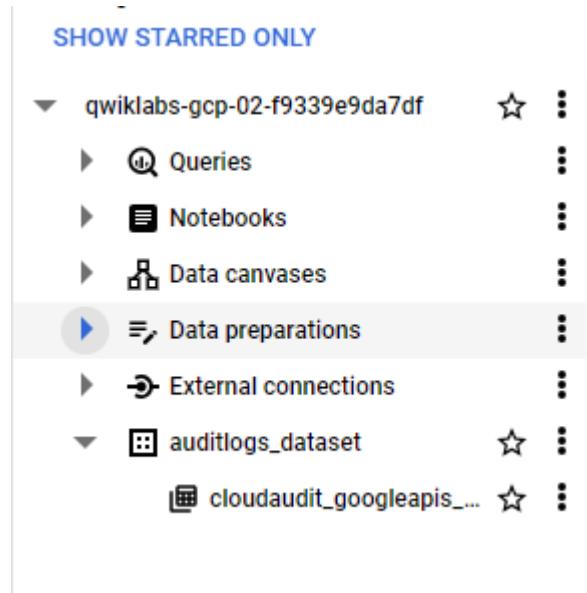


Figure 26 : Opening the side dialog box to display the project ID.

The screenshot shows the 'auditlogs\_dataset' page in the BigQuery interface. The top navigation bar includes tabs for 'Untitled query', 'auditlogs...set', and 'auditlogs\_dataset'. The main content area displays 'Dataset info' with details like Dataset ID (qwiklabs-gcp-02-f9339e9da7df.auditlogs\_dataset), Created (Sep 23, 2024, 9:28:55 AM UTC+5:30), and Last modified (Sep 23, 2024, 9:30:49 AM UTC+5:30). On the right, a sidebar titled 'SHARING' is open, showing options for 'Permissions' (Authorize Views, Authorize Routines, Authorize Datasets), 'Manage Subscriptions', and 'Publish as Listing'. A 'CREATE TABLE' button is also present at the top right of the main content area.

Figure 27 : Accessing the auditlog\_dataset and reviewing sharing permissions.

## Share permissions for "auditlogs\_dataset"

Edit or delete roles below, or select "Add Principal" to grant new access.

[+ ADD PRINCIPAL](#)

Show inherited roles in table  
Display roles inherited from the parent resources in the table below

Role / Principal	Inheritance	?
▶ BigQuery Admin (3)		
▼ BigQuery Data Editor (2)		
⋮ Editors of project: qwiklabs-gcp-02-f9339e9da7df		
⋮ service-29063018844@gcp-sa-logging.iam.gserviceaccount.com		
▶ BigQuery Data Owner (2)		
▶ BigQuery Data Viewer (1)		
▶ Cloud Logging Service Agent (1)		
▶ Editor (4)		
▶ Kubernetes Engine Service Agent (1)		
▶ Owner (2)		
▶ Viewer (2)		

CLOSE

Figure 28 : Observing the tables associated with audit logs.

⋮ service-29063018844@gcp-sa-logging.iam.gserviceaccount.com

Figure 29 : Reviewing the sharing settings and log services.

The screenshot shows the BigQuery schema browser interface. At the top, there are tabs for SCHEMA, DETAILS, PREVIEW, TABLE EXPLORER, INSIGHTS, LINEAGE, DATA PROFILE, and DATA QUALITY. The PREVIEW tab is selected. Below the tabs is a search bar labeled "Filter Enter property name or value". A table lists the schema with columns: Field name, Type, Mode, Key, Collation, Default Value, Policy Tags, and Description. The schema includes fields like logName (STRING), resource (RECORD), timestamp (TIMESTAMP), severity (STRING), insertId (STRING), httpRequest (RECORD), operation (RECORD), trace (STRING), spanId (STRING), traceSampled (BOOLEAN), sourceLocation (RECORD), split (RECORD), errorGroups (RECORD), and labels (RECORD). At the bottom of the table are buttons for EDIT SCHEMA and VIEW ROW ACCESS POLICIES.

Figure 30 : Viewing the claudaudit\_googleapis\_com\_activity\_20240923 service.

The screenshot shows the Google Cloud BigQuery interface. The URL in the browser is console.cloud.google.com/bigquery?authuser=2&project=qwiklabs-gcp-02-f9339e9da7df&ws=!1m5!1m4!4m3!1sqwiklabs-gcp-02-f9339e9da7df!2sauditlogs\_dataset!3scloudaudit\_googleapis\_com\_activity\_20240923. The main area shows the Google Cloud Explorer sidebar on the left and the BigQuery interface on the right. The BigQuery interface has tabs for Untitled query, RUN, SAVE, DOWNLOAD, SHARE, SCHEDULE, OPEN IN, and MORE. The query editor contains the following SQL code:

```

1 SELECT
2   timestamp,
3   resource.labels.instance_id,
4   protopayload_auditlog.authenticationInfo.principalEmail,
5   protopayload_auditlog.resourceName,
6   protopayload_auditlog.methodName
7 FROM
8   `auditlogs_dataset.cloudaudit_googleapis_com_activity_*`
9 WHERE
10  PARSE_DATE('%Y%m%d', _TABLE_SUFFIX) BETWEEN
11  DATE_SUB(CURRENT_DATE(), INTERVAL 7 DAY) AND
12  CURRENT_DATE()
13  AND resource.type = "gce_instance"
14  AND operation.first IS TRUE
15  AND protopayload_auditlog.methodName = "v1.compute.instances.delete"
16  ORDER BY
17   timestamp,
18   resource.labels.instance_id
19 LIMIT
20  1000;

```

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

The screenshot shows the BigQuery interface with an 'Untitled query' tab. The query retrieves data from the 'auditlogs\_dataset.cloudaudit\_googleapis\_com\_activity\_\*' table. It filters for events between 7 days ago and today, where the resource type is 'gce\_instance', the operation is 'first', and the method name is 'v1.compute.instances.delete'. The results are ordered by timestamp. The results table has columns: Row, timestamp, instance\_id, principalEmail, resourceName, and methodName. One row is shown: timestamp 2024-09-23 04:06:54.074092 UTC, instance\_id 1613083242936491462, principalEmail student-02-b176ce32f847@qw..., resourceName projects/qwiklabs-gcp-02-f9339e9da7df/zones/us-east1-d/instances/default-us-vm, methodName v1.compute.instances.delete.

```

1 SELECT
2   timestamp,
3   resource.labels.instance_id,
4   protopayload_auditlog.authenticationInfo.principalEmail,
5   protopayload_auditlog.resourceName,
6   protopayload_auditlog.methodName
7 FROM
8   `auditlogs_dataset.cloudaudit_googleapis_com_activity_*`
9 WHERE
10   PARSE_DATE('%Y%m%d', _TABLE_SUFFIX) BETWEEN
11   DATE_SUB(CURRENT_DATE(), INTERVAL 7 DAY) AND
12   CURRENT_DATE()
13   AND resource.type = "gce_instance"
14   AND operation.first IS TRUE
15   AND protopayload_auditlog.methodName = "v1.compute.instances.delete"
16 ORDER BY
  
```

**Query results**

Row	timestamp	instance_id	principalEmail	resourceName	methodName
1	2024-09-23 04:06:54.074092 UTC	1613083242936491462	student-02-b176ce32f847@qw...	projects/qwiklabs-gcp-02-f9339e9da7df/zones/us-east1-d/instances/default-us-vm	v1.compute.instances.delete

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

The screenshot shows the BigQuery interface with an 'Untitled query' tab. The query retrieves data from the 'auditlogs\_dataset.cloudaudit\_googleapis\_com\_activity\_\*' table. It filters for events between 7 days ago and today, where the resource type is 'gcs\_bucket', and the method name is 'storage.buckets.delete'. The results are ordered by timestamp. The results table has columns: Row, timestamp, bucket\_name, principalEmail, resourceName, and methodName. Two rows are shown: timestamp 2024-09-23 04:08:14.842856 UTC, bucket\_name qwiklabs-gcp-02-f9339e9da7df, principalEmail student-02-b176ce32f847@qw..., resourceName projects/\_buckets/qwiklabs-g..., methodName storage.buckets.delete; timestamp 2024-09-23 04:08:20.361517 UTC, bucket\_name qwiklabs-gcp-02-f9339e9da7df, principalEmail student-02-b176ce32f847@qw..., resourceName projects/\_buckets/qwiklabs-g..., methodName storage.buckets.delete.

```

1 SELECT
2   timestamp,
3   resource.labels.bucket_name,
4   protopayload_auditlog.authenticationInfo.principalEmail,
5   protopayload_auditlog.resourceName,
6   protopayload_auditlog.methodName
7 FROM
8   `auditlogs_dataset.cloudaudit_googleapis_com_activity_*`
9 WHERE
10   PARSE_DATE('%Y%m%d', _TABLE_SUFFIX) BETWEEN
11   DATE_SUB(CURRENT_DATE(), INTERVAL 7 DAY) AND
12   CURRENT_DATE()
13   AND resource.type = "gcs_bucket"
14   AND protopayload_auditlog.methodName = "storage.buckets.delete"
15 ORDER BY
16   timestamp,
17   resource.labels.instance_id
18 LIMIT
19   1000;
  
```

**Query results**

Row	timestamp	bucket_name	principalEmail	resourceName	methodName
1	2024-09-23 04:08:14.842856 UTC	qwiklabs-gcp-02-f9339e9da7df	student-02-b176ce32f847@qw...	projects/_buckets/qwiklabs-g...	storage.buckets.delete
2	2024-09-23 04:08:20.361517 UTC	qwiklabs-gcp-02-f9339e9da7df	student-02-b176ce32f847@qw...	projects/_buckets/qwiklabs-g...	storage.buckets.delete

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

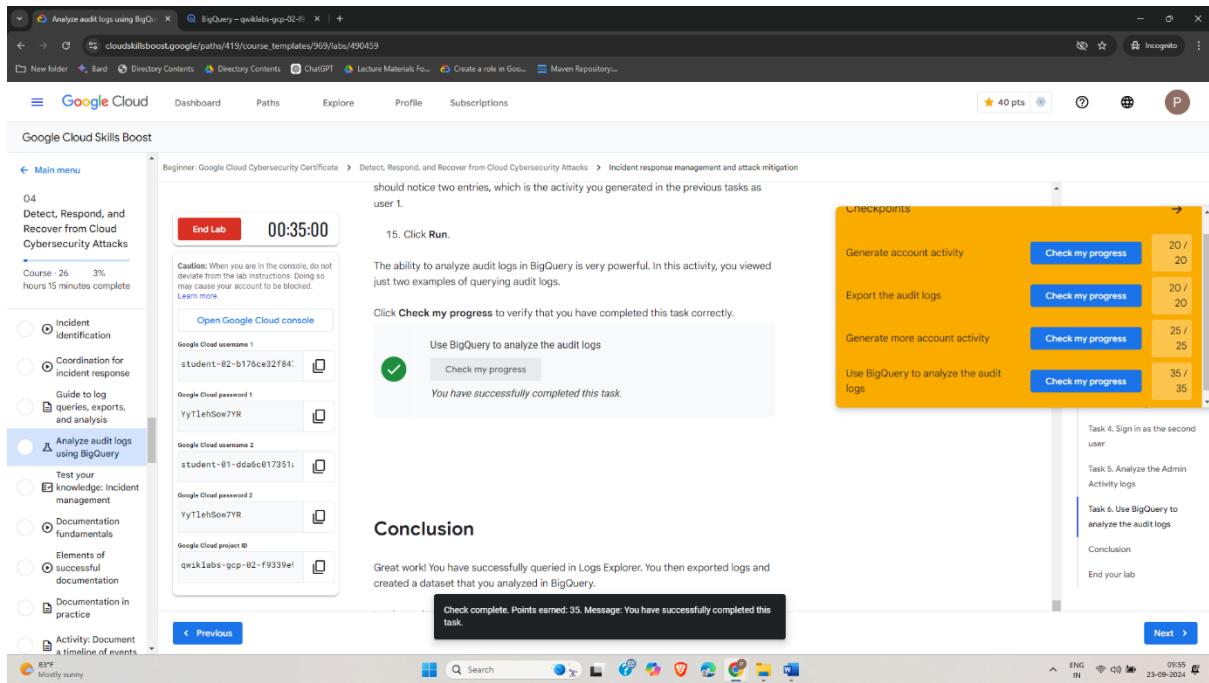


Figure 34 : Successfully completing the lab session.

## 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:

The screenshot shows the Google Cloud Skills Boost interface for a lab titled "Recover VMs with Google Backup and DR Service". The sidebar on the left lists completed tasks under "04 Detect, Respond, and Recover from Cloud Cybersecurity Attacks". The main content area shows a "Conclusion" section with a timer at 01:29:28, a success message ("Great work! You successfully used Google Backup and DR Service to create a backup template and then applied it to two Compute Engine instances."), and a summary of completed tasks. A right sidebar shows user profile information (22IT113 PATEL SMITKUMAR NILESHKUMAR) and a task list for "Task 5. Restore a Compute Engine instance" and "Task 6. Restore a Compute Engine instance to an alternate project".

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

The screenshot shows the Google Cloud Backup and DR service console. The main interface includes sections for "Management", "Analysis", and "Discover". The "Management" section shows an "Overview" of backup vaults. The "Discover" section provides links to "Manage user access", "Understand pricing", and "Explore concepts". A sidebar on the right lists "Recommended for you" resources and "Help document" links for various backup and DR topics.

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

The screenshot shows the Google Cloud Backup and DR management console. At the top, there's a navigation bar with 'Cloud' and a dropdown menu showing 'qwiklabs-gcp-01-966649512f5c'. A search bar on the right says 'Search (/) for resources, docs, products'. Below the navigation bar, a sidebar on the left lists 'Cloud DR', 'Management console', 'Logs', 'Metrics', 'Sources', and 'Cloud console'. The main area has a title 'Log in to the management console' with a sub-instruction: 'This is where you can perform your backup and restore activities, like protecting your applications and managing backups, users, and policies.' It shows a location 'us-east1' and a status 'Ready' with a green checkmark. There are buttons for 'SHOW API CREDENTIALS' and 'LOG IN TO THE MANAGEMENT CONSOLE'.

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

The screenshot shows the Google Cloud Backup and DR management console dashboard. The top navigation bar includes 'Management console – Backup', 'Dashboard – Google Cloud Back...', and a '+' button. Below the navigation bar, there's a toolbar with links like 'New folder', 'Bard', 'Directory Contents', 'ChatGPT', 'Lecture Materials Fo...', 'Create a role in Goo...', and 'Maven Repository'. The main header says 'Google Cloud Backup and DR' and 'Dashboard'. The dashboard displays project information ('Project: qwiklabs-gcp-01-966649512f5c' and 'Region: us-east1'). On the left, there's a sidebar with 'Google Cloud Backup and DR', 'Dashboard', 'Back Up & Recover', 'App Manager', 'Backup Plans', 'Manage', 'Reports', and 'Monitor'. The main content area has sections for 'Applications' (with counts for Managed(0), Unmanaged(0), and Unscheduled(0)) and 'Job Status' (with counts for Current Jobs, Past Jobs, and Job Types: Running(0), Queued(0), Succeeded(0), Failed(0), and Not Run(0)). A dropdown menu on the right lists 'Appliances', 'Hosts', 'Storage Pools', 'Credentials', 'Appliance Updates', and 'Certificates'. At the bottom, there are buttons for 'JOB TYPES' and 'APPLIA'.

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.

**FILTER BY**

- Appliance Name: Search by appliance name
- IP Address: Search by IP Address
- Update Status: Out Of Support, Pending

	NAME	APPLIANCE ID	CONNECTIVITY	IP	MACHINE TYPE	LAST SYNC
<input type="checkbox"/>	qwiklabs-appliance	142947360532		10.142.0.3	e2-standard-4	2024-1

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

**FILTER BY**

- Template Name: Search by template name

**Backup Plans**

- Templates
- Profiles
- Dynamic Protection Tags New

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

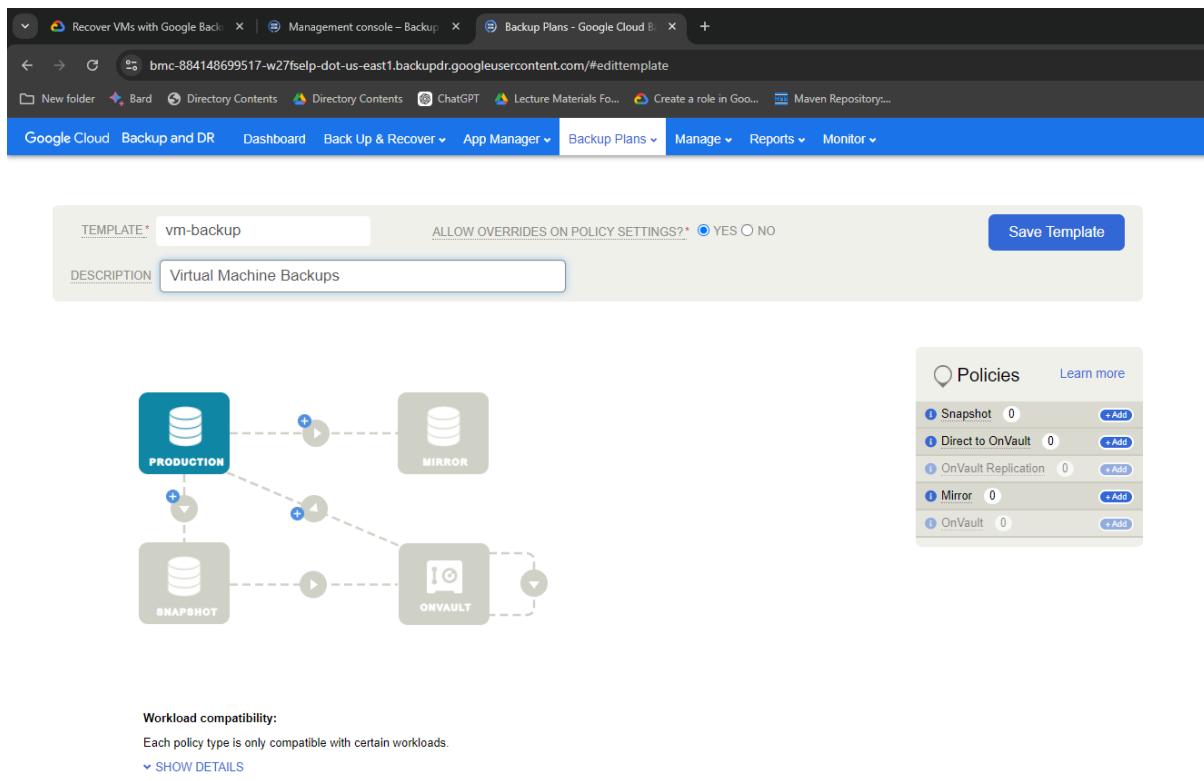


Figure 7 : Creating a backup template with name and description Demonstrates the process of creating a backup template with essential information.

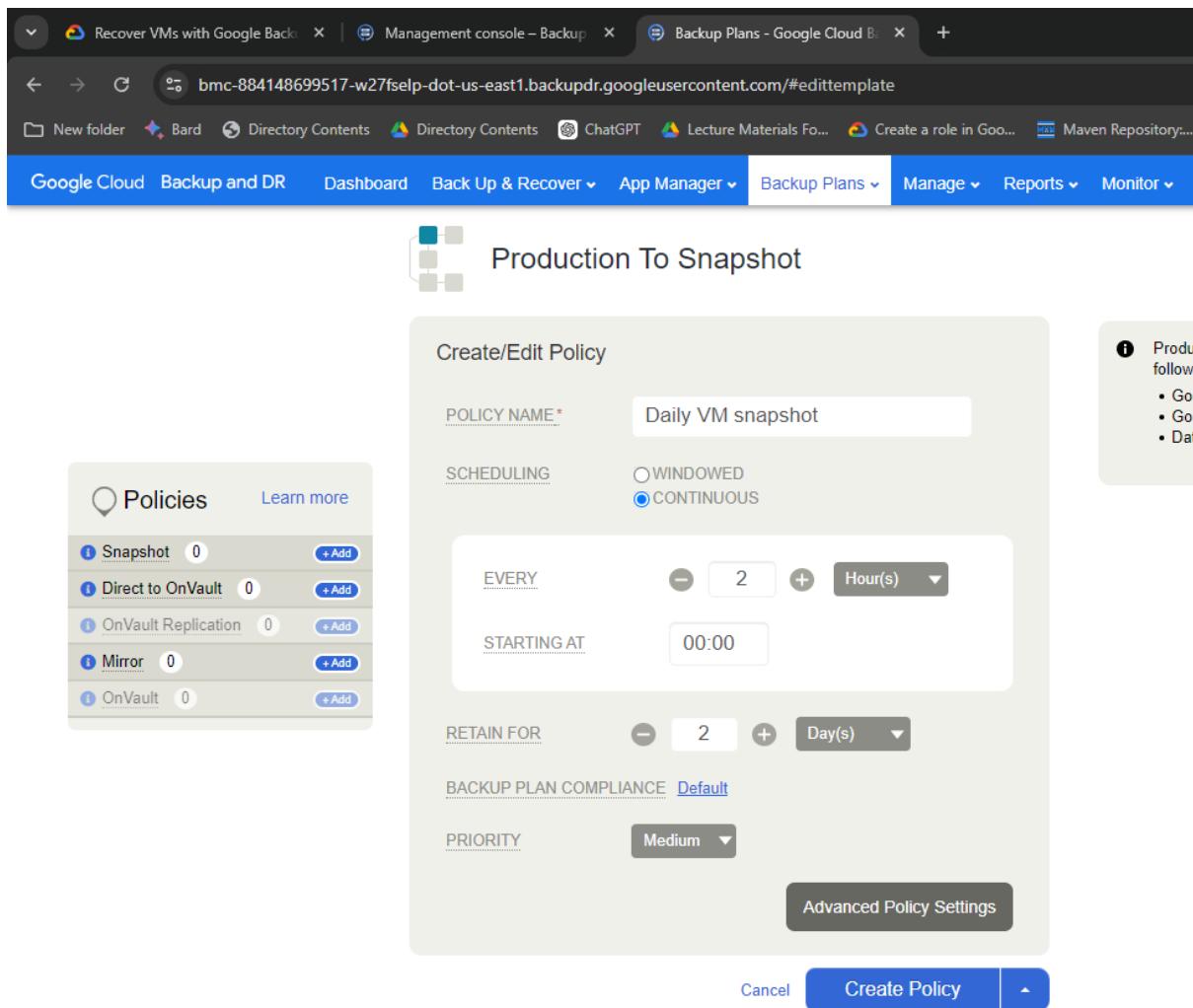


Figure 8 : Creating a policy for snapshots Setting up a policy to manage snapshot frequency and retention.

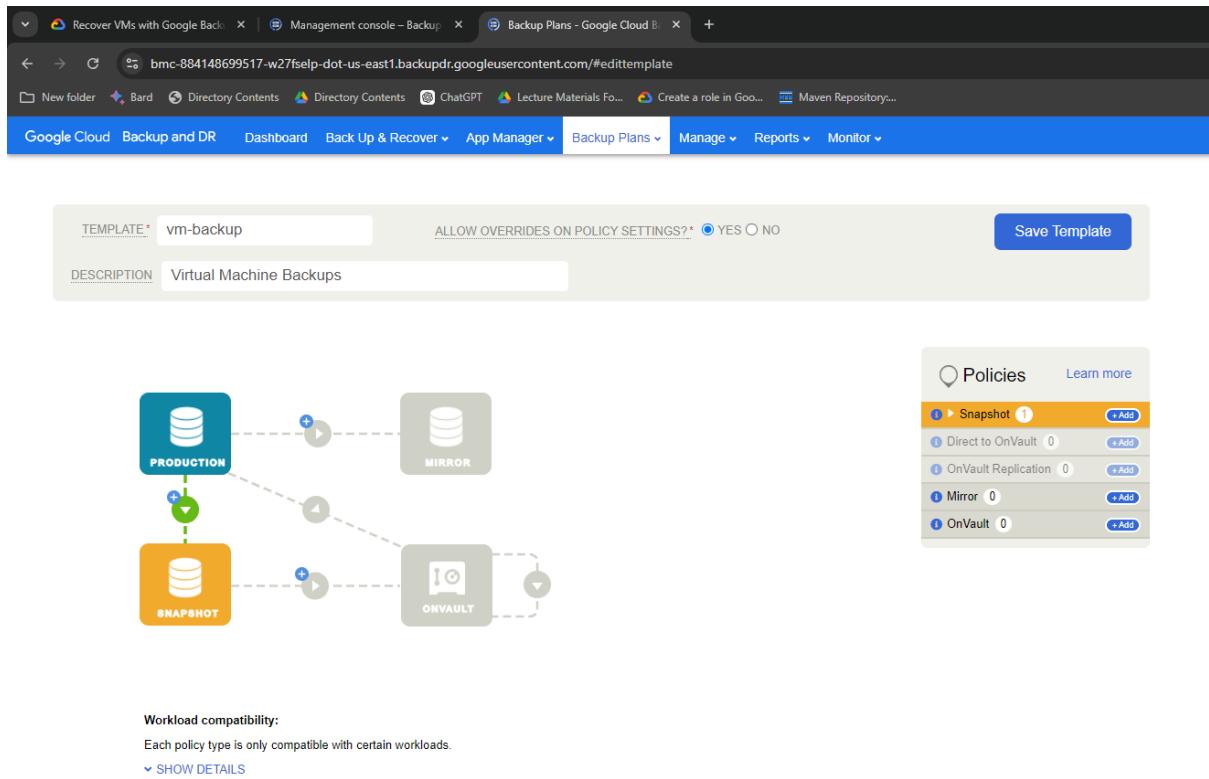


Figure 9 : Saving the template Confirmation of the backup template creation.

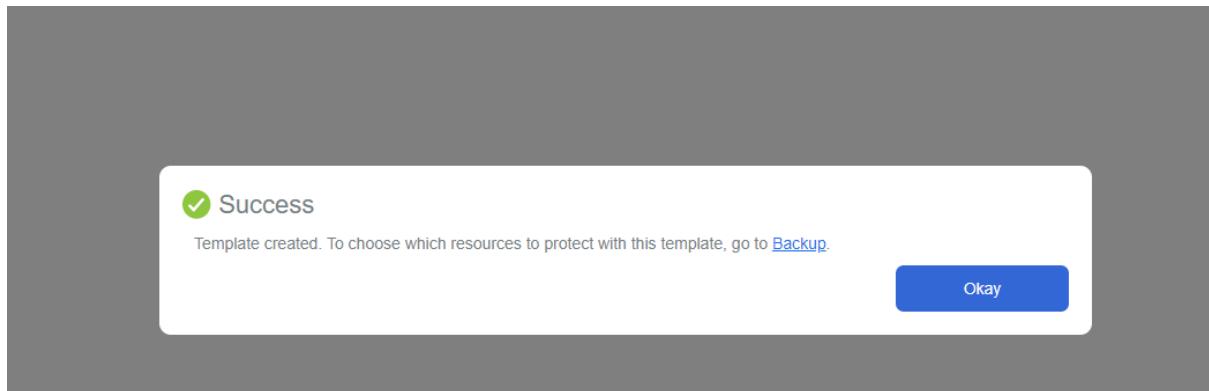


Figure 10 : Successful creation of the template Shows the final confirmation after the backup template has been created.

Service Account User				
<input type="checkbox"/>	admiral@qwiklabs-services-prod.iam.gserviceaccount.com		Owner	
<input type="checkbox"/>	backup@qwiklabs-gcp-01-966649512f5c.iam.gserviceaccount.com	Service account for backup and recovery appliance.	Backup and DR Cloud Storage Operator Backup and DR Compute Engine Operator Logs Writer Service Account User	qwiklabs-appliance-e4b59b-cloud-storage-metadata
<input type="checkbox"/>	qwiklabs-gcp-01-966649512f5c@qwiklabs-gcp-01-966649512f5c.iam.gserviceaccount.com	Qwiklabs User Service	BigQuery Admin Owner	

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

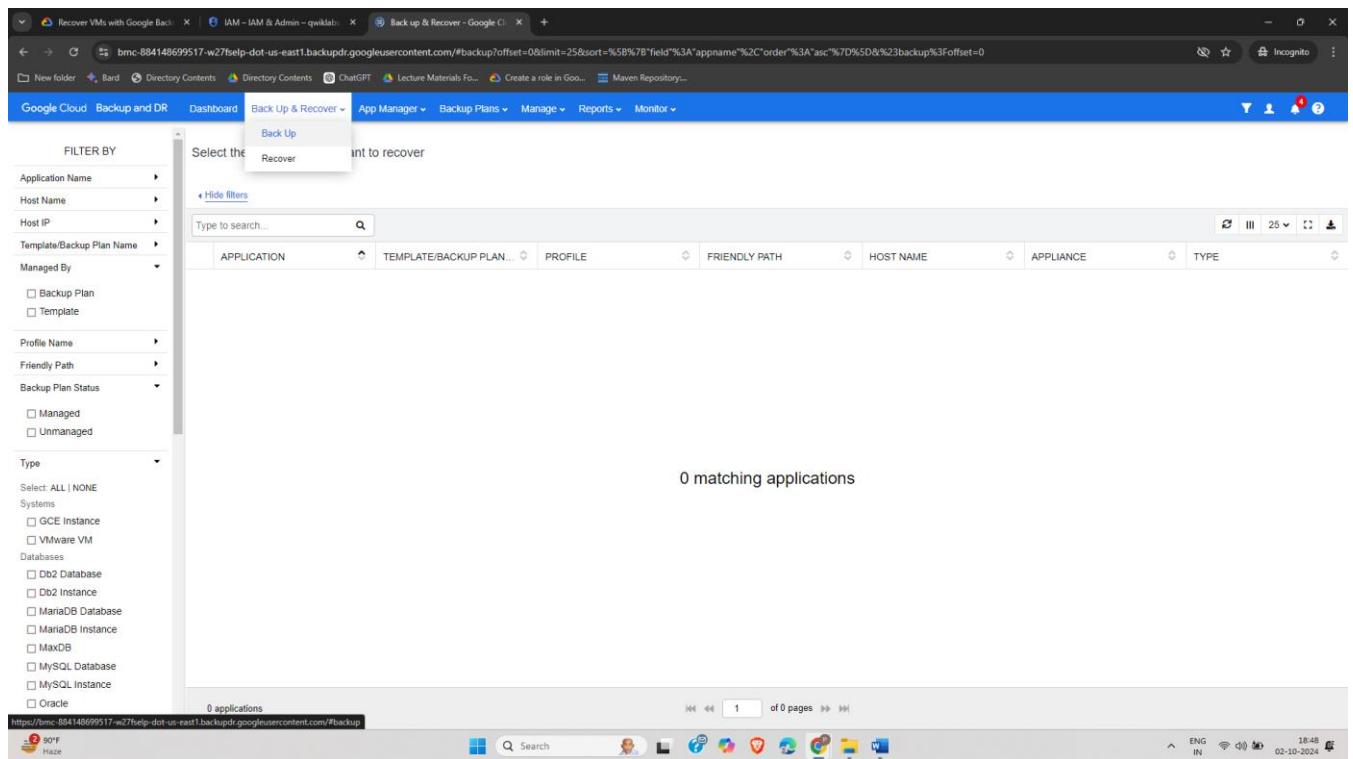


Figure 12 : Navigating to the backup section Accessing the backup configuration section.

The screenshot shows the Google Cloud Backup and DR interface. At the top, there are three tabs: "Recover VMs with Google Back..." (closed), "Management console – Backup" (closed), and "Back up & Recover - Google Cl..." (active). Below the tabs, the URL is [bmc-884148699517-w27fse1.backupdr.googleusercontent.com/#backup](https://bmc-884148699517-w27fse1.backupdr.googleusercontent.com/#backup). The main navigation bar includes "Google Cloud", "Backup and DR", "Dashboard", "Back Up & Recover" (selected), "App Manager", "Backup Plans", "Manage", and "Reports".  
  
The main content area is titled "Select the type of ap" (application) and includes a "Tip: Hover on the icon for more information. To learn how".  
  
The interface is divided into two sections:

- Servers & Applications (Agents required):** This section contains icons for Db2, MariaDB, MySQL, SAP HANA, SAP IQ, and SAP MaxDB.
- Google Cloud:** This section contains icons for VMware Engine and Compute Engine.

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

Enable backups for Compute Engine VM instances?

1 Discover    2 Select    3 Manage    4 Finish

[NEW] Begin using [Dynamic Protection Tags](#) to automate protection of your Compute Engine VMs going forward to avoid manual protection using this workflow.

Select the service account that should back up the VM.

Note: The service account should have “**Backup and DR Compute Engine Operator**” role in the project that contains the Compute Engine instances.

Search... 

CREDENTIAL	SERVICE ACCOUNT	APPLIANCE
backup	backup@qwiklabs-gcp-01-966649512f5c.iam.gserviceaccount.com	qwiklabs-appliance

[CANCEL](#) [NEXT](#)

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

Enable backups for Compute Engine VM instances?

1 Discover    2 Select    3 Manage    4 Finish

Select a filter to see VM instances based on their state. You can select one or more VM instances in different states to apply an action in the next page.

Project ID:  Zone:

[SEARCH](#)

[Don't see your project ID here?](#)

NAME	ID	ZONE	INTERNAL IP	EXTERNAL IP	PROJECT NAME
<input type="checkbox"/> lab-vm	4887293587572747125	us-east1-d	10.142.0.2	34.139.217.142	qwiklabs-gcp-01-966...
<input type="checkbox"/> qwiklabs-appliance	8115071049362662758	us-east1-d	10.142.0.3		qwiklabs-gcp-01-966...

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

Select a filter to see VM instances based on their state. You can select one or more VM instances in different states to apply an action in the next page.

Project ID:  Zone:

[SEARCH](#)

[Don't see your project ID here?](#)

NAME	ID	ZONE	INTERNAL IP	EXTERNAL IP	PROJECT NAME
<input checked="" type="checkbox"/> lab-vm	4887293587572747125	us-east1-d	10.142.0.2	34.139.217.142	qwiklabs-gcp-01-966...
<input type="checkbox"/> qwiklabs-appliance	8115071049362662758	us-east1-d	10.142.0.3		qwiklabs-gcp-01-966...

CANCEL    PREVIOUS    **NEXT**

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

Select one or more VM instances, then choose an action.

Action: **Backup template:**

INSTANCE NAME	GROUP	TEMPLATE/BACKUP PL...	PROFILE	VOLUME OPTIONS	PREVIEW
<input checked="" type="checkbox"/> lab-vm	None	None	None	<input type="button" value="Capture All Volumes"/>	<input type="button"/> <input type="button"/> <input type="button"/>

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

Enable backups for Compute Engine VM instances?

1 Discover    2 Select    3 Manage    4 Finish

Summary of changes

- 1 Instance will have a backup template applied

**Note:** Backup and DR will automatically create a Cloud Storage bucket with Standard storage to store VM metadata. Metadata will be charged at standard storage rates.

INSTANCE NAME	APPLIANCE	ACTION	STATUS
lab-vm	qwiklabs-appliance	Apply a backup template	--

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

**Jobs**

[Cloud Monitoring](#) and [Cloud Logging](#)

Type to search...

<input type="checkbox"/>	JOB	STATUS	HOST	APPLICATION	APPLIANCE	QUEUED	STARTED
<input type="checkbox"/>	Job_0009841	<span style="color: green;">Running: 82%</span>	lab-vm	lab-vm	qwiklabs-a...	2024-10-02...	2024-10-02...

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

Type to search...

<input type="checkbox"/>	JOB	STATUS	HOST	APPLICATION	APPLIANCE	QUEUED	STARTED	ENDED	DURATION	TYPE
<input type="checkbox"/>	Job_0009841	<span style="color: green;">Succeeded</span>	lab-vm	lab-vm	qwiklabs-a...	2024-10-02...	2024-10-02...	2024-10-02...	00:01:40	snapshot

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

APPLICATION	TEMPLATE/BACKUP PLAN...	PROFILE	FRIENDLY PATH	HOST NAME	APPLIANCE
lab-vm	vm-backup	backup_Profile	us-east1-d.default.default:qwiki...	lab-vm	qwiklabs-appliance

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

IMAGE NAME	CONSISTENC...	IMAGE TYPE	SIZE (GB)	LABEL	IMMUTABILITY D...	EXPIRATION	ACTIVE MOUNTS	RECOVERY RAN...	SENSITIVE DATA	APPLIANCE
Image_0009841	2024-10-02 19:07...	snapshot	100.00			2024-10-04 19:08...	0	No	qwiklabs-appliance	

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

IMAGE NAME	CONSISTENC...	IMAGE TYPE	SIZE (GB)	LABEL	IMMUTABILITY D...	EXPIRATION	ACTIVE MOUNTS	RECOVERY RAN...	SENSITIVE DATA	APPLIANCE
Image_0009841	2024-10-02 19:07...	snapshot	100.00			2024-10-04 19:08...	0	No	qwiklabs-appliance	

1 backups

Mount

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

The screenshot shows a browser window with three tabs: 'Recover VMs with Google Back...', 'Management console - Backup', and 'Application Manager - Google'. The main content is a 'Mount' configuration dialog for a backup snapshot named 'Image\_0009841'. The dialog has two radio button options: 'MOUNT TO EXISTING GCE INSTANCE' (unchecked) and 'MOUNT AS NEW GCE INSTANCE' (checked). A note below states: 'Note: A network egress charge applies if you recover the instance in a region that's different from the region of the selected backup.' Below this are fields for 'CLOUD CREDENTIALS NAME\*' (set to 'backup'), 'PROJECT NAME\*' (set to 'qwiklabs-gcp-01-966649512f5c'), 'REGION\*' (set to 'us-east1'), and 'ZONE\*' (set to 'us-east1-d'). The 'INSTANCE NAME\*' field is set to 'lab-vm-recovered'. Other settings include 'SOLE TENANCY' (None), 'MACHINE TYPE\*' (e2-medium(2 vCPU, 4.00GB memory)), and 'USE DEFAULT COMPUTE ENGINE SA' (disabled). A 'NETWORK TAGS' field with a search bar is also present. At the bottom left is a blue 'Mount' button.

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

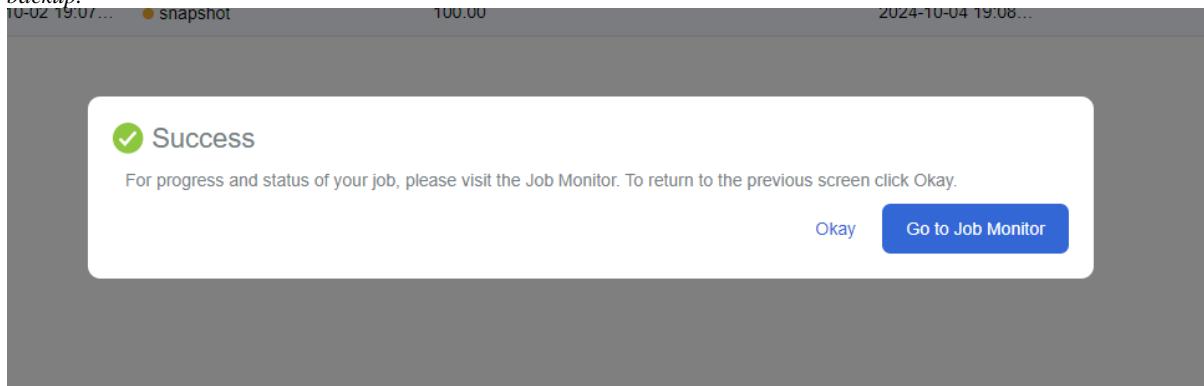


Figure 25 : Completing the mounting process Final steps of the mounting process for the new instance.

The screenshot shows the 'Jobs' section of the Google Cloud Backup and DR interface. The top navigation bar includes 'Google Cloud', 'Backup and DR', 'Dashboard', 'Back Up & Recover', 'App Manager', 'Backup Plans', 'Manage', 'Reports', and 'Monitor'. The 'Monitor' tab is active. On the left, there are filters for 'Job Name', 'Host', 'Target Host', and 'Application'. The main area displays a table of jobs:

JOB	STATUS	HOST	APPLICATION	APPLIANCE	QUEUED	STARTED	ENDED
Job_0009988	Succeeded	lab-vm	lab-vm	qwiklabs-a...	2024-10-02...	2024-10-02...	2024-10-02...
Job_0009841	Succeeded	lab-vm	lab-vm	qwiklabs-a...	2024-10-02...	2024-10-02...	2024-10-02...

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

Filter Enter property name or value							
Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect
<input type="checkbox"/>	lab-vm	us-east1-d			10.142.0.2 (nic0)	34.139.217.142 (nic0)	SSH ▾
<input type="checkbox"/>	lab-vm-recovered	us-east1-d			10.142.0.4 (nic0)		SSH ▾
<input type="checkbox"/>	qwiklabs-appliance	us-east1-d			10.142.0.3 (nic0)		SSH ▾

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

The screenshot shows the Google Cloud IAM & Admin interface. A modal window titled "Permissions for 966649512f5c" is open, displaying a list of resources and users with their respective roles. The resources include "qwiklabs-resources" and two "qwiklabs-gcp" projects. The users listed are "admin prod" and "backups". The interface includes tabs for "ALLOW" and "DENY", a search bar, and a sidebar with various IAM-related options like PAM, Principal Access Boundary, Policy Troubleshooter, and Policy Analyzer.

Name	Type	Role
qwiklabs-resources	Resource	Owner
qwiklabs-gcp-01-966649512f5c	Project	Storage Admin
qwiklabs-gcp-02-0ased580d8e0	Project	BigQuery Admin
student-01-6bf394d2cbea@qwiklabs.net	User	Storage Admin

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

Create a role in Goo... Maven Repository...

### Grant access to "qwiklabs-gcp-02-0a5ed580d8e0"

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

**Resource**

• qwiklabs-gcp-02-0a5ed580d8e0

**Add principals**

Principals are users, groups, domains, or service accounts. [Learn more about principals in IAM](#)

New principals \*

**Assign roles**

Roles are composed of sets of permissions and determine what the principal can do with this resource. [Learn more](#)

**Role \***  **IAM condition (optional)** [+ ADD IAM CONDITION](#)

Allows a Backup and DR service account to discover, back up, and restore Compute Engine VM instances.

**Role**  **IAM condition (optional)** [+ ADD IAM CONDITION](#)

Allows a Backup and DR service account to store and manage data (backups or metadata) in Cloud Storage.

[+ ADD ANOTHER ROLE](#)

**SAVE** **CANCEL**

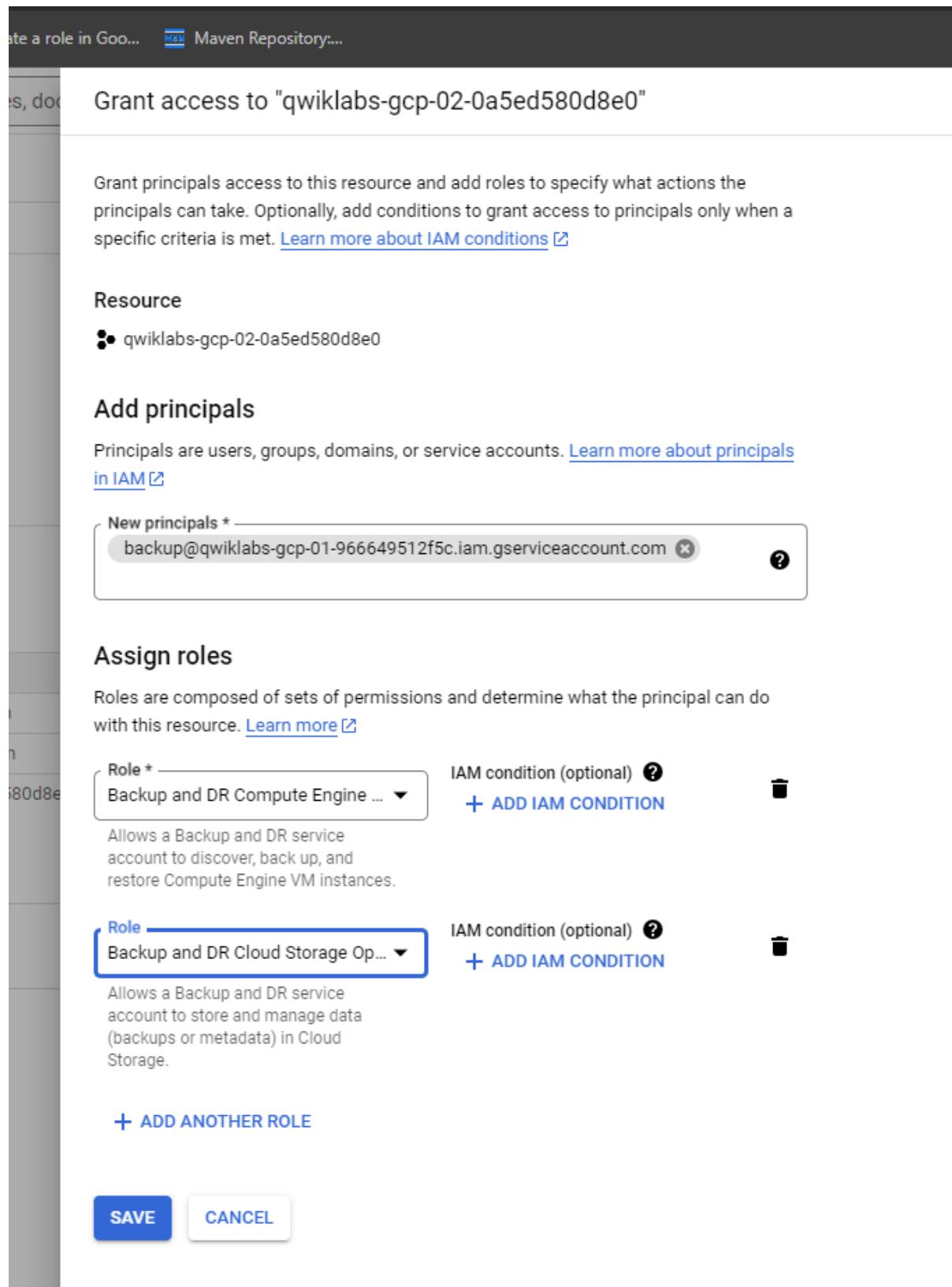


Figure 29 : Adding a new principal for backup access Assigning necessary roles and permissions for backup operations.

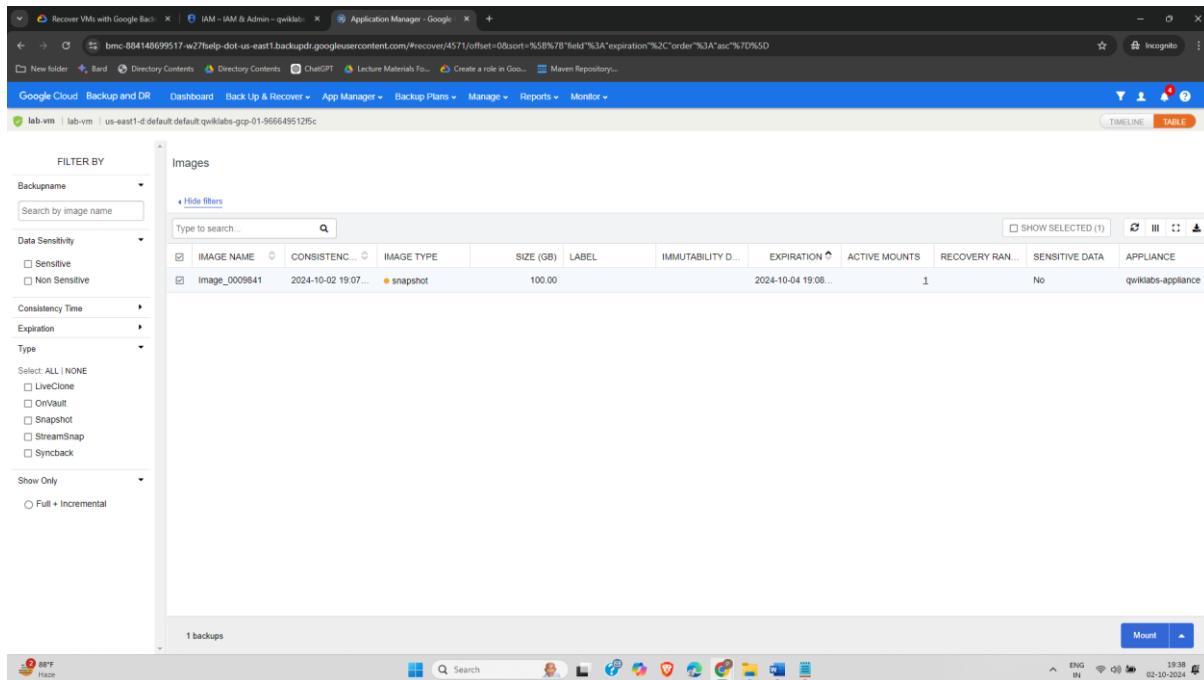


Figure 30 : Navigating to the VM instance and viewing the image Accessing the VM instance and viewing the backup image.

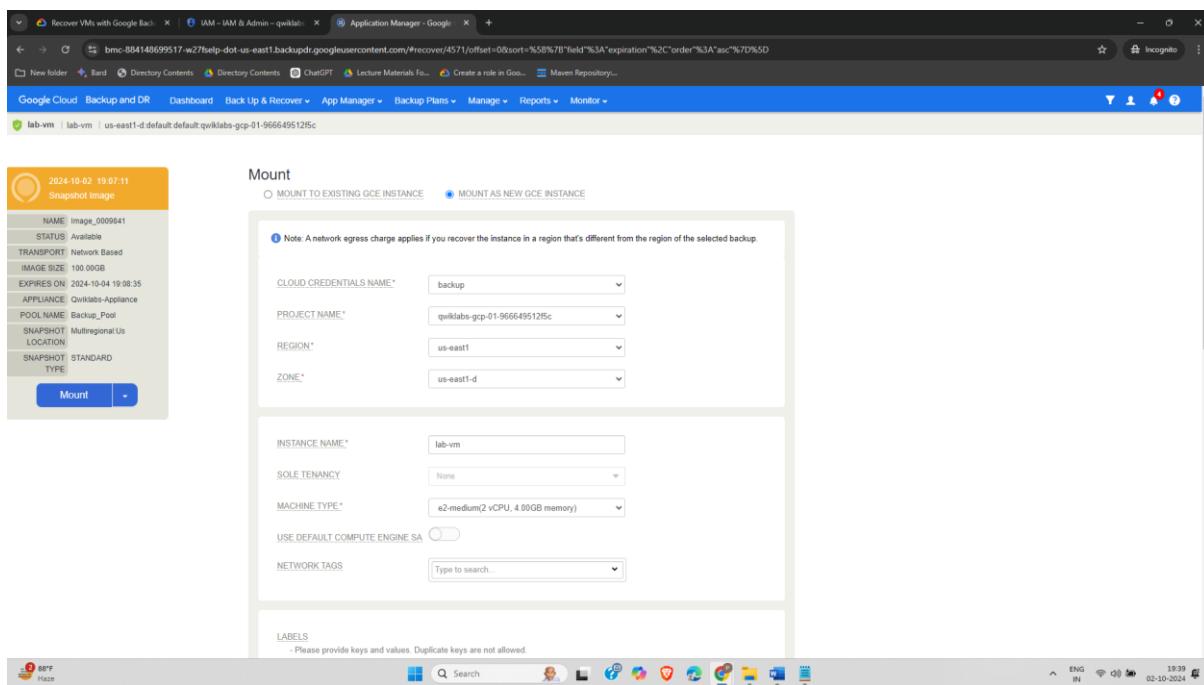


Figure 31 : Mounting the new image with a new GCE instance Mounting another backup image to create a new Compute Engine instance.

**Mount**

MOUNT TO EXISTING GCE INSTANCE  MOUNT AS NEW GCE INSTANCE

**Note:** A network egress charge applies if you recover the instance in a region that's different from the region of the selected backup.

CLOUD CREDENTIALS NAME*	backup
PROJECT NAME*	qwiklabs-gcp-02-0a5ed580d8e0
REGION*	us-east1
ZONE*	us-east1-d
INSTANCE NAME*	lab-vm-project2.
SOLE TENANCY	None
MACHINE TYPE*	e2-medium(2 vCPU, 4.00GB memory)
USE DEFAULT COMPUTE ENGINE SA	<input type="checkbox"/>
NETWORK TAGS	Type to search...

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

**JODS**

[Cloud Monitoring](#) and [Cloud Logging](#) are now integrated with the Backup and DR

Hide filters  Status: Running  Status: Succeeded

Type to search...

	JOB	STATUS	HOST	APPLICATION	APPLIANCE	QUEUED	STARTED	ENDED	DURATION	TYPE
<input type="checkbox"/>	Job_0010273	<span style="color: green;">●</span> Succeeded	lab-vm	lab-vm	qwiklabs-a...	2024-10-02...	2024-10-02...		00:02:09	mount
<input type="checkbox"/>	Job_0009988	<span style="color: green;">●</span> Succeeded	lab-vm	lab-vm	qwiklabs-a...	2024-10-02...	2024-10-02...	2024-10-02...	00:01:50	mount
<input type="checkbox"/>	Job_0009841	<span style="color: green;">●</span> Succeeded	lab-vm	lab-vm	qwiklabs-a...	2024-10-02...	2024-10-02...	2024-10-02...	00:01:40	snapst

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

The screenshot shows the Google Cloud VM instances page. At the top, there's a search bar and a dropdown for the project 'qwiklabs-gcp-02-0a5ed580d8e0'. Below the header, there are tabs for 'INSTANCES', 'OBSERVABILITY', and 'INSTANCE SCHEDULES'. The 'INSTANCES' tab is selected, displaying a table with one row for 'lab-vm-project2'. The table columns include Status (green checkmark), Name (link to 'lab-vm-project2'), Zone (us-east1-d), Recommendations, In use by, and Internal IP (10.142.0.2). Below the table, there's a section titled 'Related actions' with three cards: 'Explore Backup and DR' (NEW), 'Monitor VMs', and 'Load balance between VMs'.

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

The screenshot shows the Google Cloud Skills Boost interface. On the left, there's a sidebar with a navigation tree and a progress bar for a course. The main area shows a task titled 'Beginner: Google Cloud Cybersecurity Certificate' under 'Detect, Respond, and Recover from Cloud Cybersecurity Attacks'. The task details a step to 'Mount' a Compute Engine instance. A note says 'Note: Before you set the default service account as a Principal in a different project, you must add the default service account as a Principal in the target project.' A 'Check my progress' button is shown with a green checkmark and the message 'You have successfully completed this task.' To the right, there's a 'Checkpoints' section with several tasks listed, each with a 'Check my progress' button. The tasks include 'Create a backup plan template', 'Discover and add Compute Engine instances to the management console', 'Restore a Compute Engine instance', and 'Restore a Compute Engine instance to an alternate project'. A vertical sidebar on the right lists 'Task 4. Discover and add Compute Engine instances to the management console', 'Task 5. Restore a Compute Engine instance', and 'Task 6. Restore a Compute Engine instance'.

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 Cymbol Retail. Cymbol 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.

Cymbol 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:

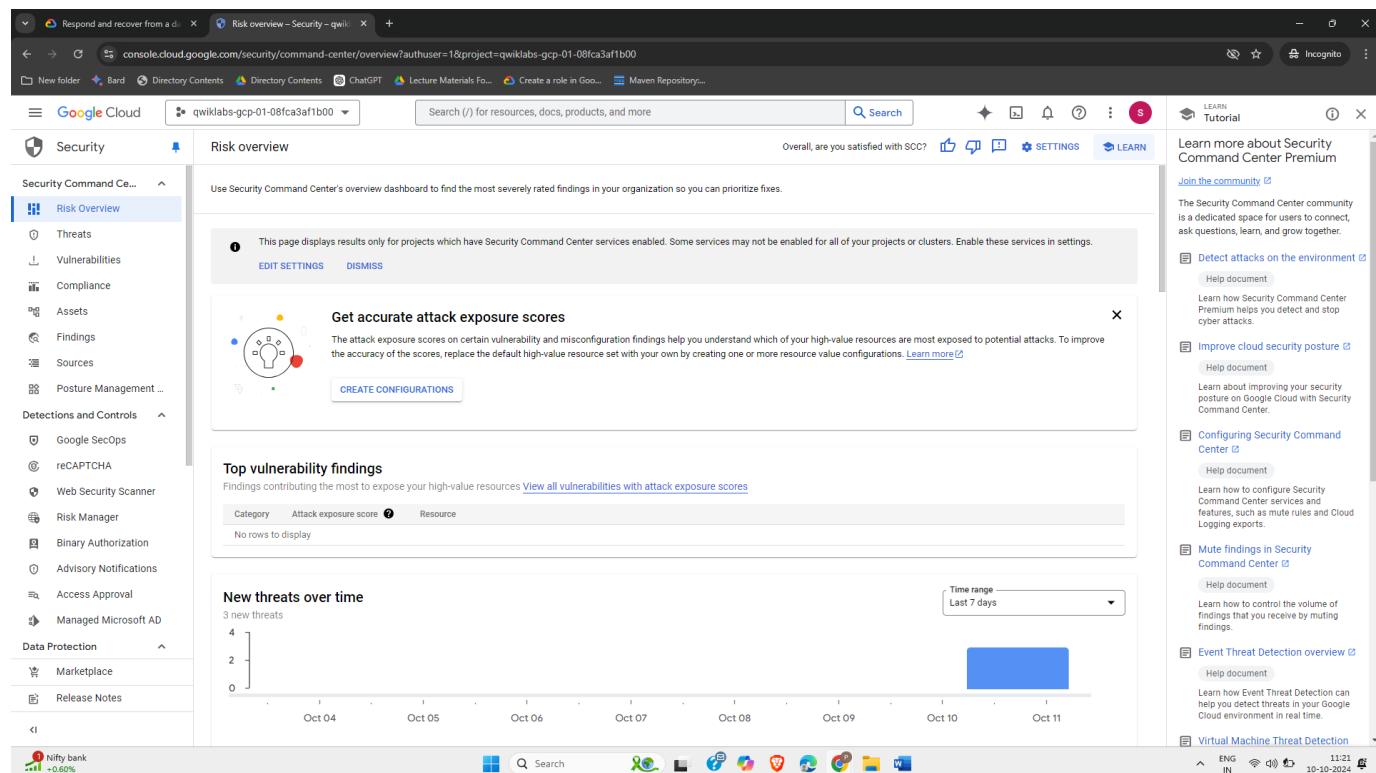


Figure 1 : Navigating to the Google Cloud Security Command Center's dashboard to assess security risks and vulnerabilities.

Findings by Category		Findings by Resource Type		Findings by Project	
		Critical Findings	High Severity Findings	Medium Severity Findings	Low Severity Findings
	<a href="#">Bucket</a>	0	1	1	1
	<a href="#">compute.instance</a>	0	1	3	0
	<a href="#">compute.Project</a>	0	0	1	0
	<a href="#">Firewall</a>	0	2	4	0
	<a href="#">Network</a>	0	0	2	0
	<a href="#">resourcemanager.Project</a>	0	0	2	9
	<a href="#">ServiceAccountKey</a>	0	0	1	0
	<a href="#">Subnetwork</a>	0	0	0	58

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

The screenshot shows the Google Cloud Security Command Center Compliance page. On the left, there's a sidebar with navigation links for Security, Risk Overview, Threats, Vulnerabilities, and Compliance (which is currently selected). The main content area is titled 'Compliance' and contains a section titled 'Google Cloud compliance standards (19)'. It lists several compliance standards with their passing percentages and 'View details' links:

- CIS Controls 8.0: 59% passing
- CIS Google Cloud Platform Foundation 1.0: 71% passing
- CIS Google Cloud Platform Foundation 1.1: 73% passing
- CIS Google Cloud Platform Foundation 1.2: 78% passing
- CIS Google Cloud Platform Foundation 1.3: 78% passing
- CIS Google Cloud Platform Foundation 2.0: 79% passing
- CIS Kubernetes Benchmark 1.5.1: 100% passing
- Cloud Controls Matrix 4: 64% passing
- HIPAA: 82% passing
- ISO 27001 2013: 62% passing
- ISO 27001 2022: 74% passing
- NIST 800-53 R4: 62% passing

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

The screenshot shows the Google Cloud Security Command Center interface. On the left, there's a sidebar with various security categories like Security Command Center, Risk Overview, Threats, Vulnerabilities, and Compliance (which is selected). The main area displays a chart titled "PCI DSS 3.2.1 controls over time" showing a timeline from UTC-5:30 to Oct 10, 2024. Below the chart is a table of findings:

Control	Status	Rule	Severity	Findings
10.1	Non-compliant		High	34
10.2	Non-compliant		High	34
1.2.1	Non-compliant		Medium	2
7.1.2	Non-compliant		Medium	1
7.2	Non-compliant		Medium	1
1.1.4	Compliant		Low	0

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

The screenshot shows the Google Cloud Event Threat Detection interface. At the top, there's a query preview: "state='ACTIVE' AND NOT mute='MUTED' AND resource.type='google.cloud.storage.Bucket'". Below it is a "Quick filters" section with checkboxes for various Google Cloud services, and a "Findings query results" table. The table has columns: Category, Severity, Attack exposure score, Event time, Create time, Finding class, and Resource. There are four entries:

Category	Severity	Attack exposure score	Event time	Create time	Finding class	Resource
Public bucket ACL	High	—	Oct 10, 2024, 7:11:06 AM	Oct 10, 2024, 7:11:06 AM	Misconfiguration	qwik[08fc]
Bucket policy only disabled	Medium	—	Oct 10, 2024, 7:11:05 AM	Oct 10, 2024, 7:11:06 AM	Misconfiguration	qwik[08fc]
Bucket logging disabled	Low	—	Oct 10, 2024, 7:11:05 AM	Oct 10, 2024, 7:11:06 AM	Misconfiguration	qwik[08fc]

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

**Public bucket ACL**

**SUMMARY**   **SOURCE PROPERTIES (11)**   **JSON**

**What was detected**

Description	This bucket is public and can be accessed by anyone on the internet. <code>allUsers</code> represents anyone on the Internet, and <code>allAuthenticatedUsers</code> represents anyone who is authenticated with a Google account; neither is constrained to users within your organization.	
State	Active	state
Severity	High	severity
Event time	October 10, 2024 at 7:11:06 AM GMT+5	event_time
Create time	October 10, 2024 at 7:11:06 AM GMT+5	create_time

**Affected resource**

Resource display name	qwiklabs-gcp-01-08fca3af1b00_bucket	resource.display_name
Resource full name	//storage.googleapis.com/qwiklabs-gcp-01-08fca3af1b00_bucket	resource.name
Resource type	google.cloud.storage.Bucket	resource.type
Project full name	//cloudresourcemanager.googleapis.com/projects/4130877743	resource.gcp_metadata.project
Resource path	Navy Projects > gcp_low_extra > gcp_low_extra_navy-01 > qwiklabs-gcp-01-08fca3af1b00	
Cloud provider	Google Cloud	resource.cloudProvider
Security contacts	None	contacts.security
Technical contacts	None	contacts.technical

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

Control ↑	Status	Rule ?	Severity
▼ 10.1	✗ Non-compliant		
	✗ Non-compliant	VPC Flow logs should be Enabled for every subnet in VPC Network	!
	✗ Non-compliant	Firewall rule logging should be enabled so you can audit network access	!!
	✗ Non-compliant	Cloud Audit Logging should be configured properly across all services and all users from a project	!!
	✓ Compliant	Stackdriver Monitoring should be Enabled on Kubernetes Engine Clusters	!
▼ 10.2	✗ Non-compliant		
	✗ Non-compliant	VPC Flow logs should be Enabled for every subnet in VPC Network	!
	✗ Non-compliant	Firewall rule logging should be enabled so you can audit network access	!!
	✗ Non-compliant	Cloud Audit Logging should be configured properly across all services and all users from a project	!!
	✓ Compliant	Stackdriver Monitoring should be Enabled on Kubernetes Engine Clusters	!
▼ 1.2.1	✗ Non-compliant		
	✗ Non-compliant	Firewall rules should not allow connections from all IP addresses on TCP or UDP port 3389	!!
	✗ Non-compliant	Firewall rules should not allow connections from all IP addresses on TCP or SCTP port 22	!!

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

Category	Severity	Attack exposure score ?	Event time ↓	Create time	Finding class
Public bucket ACL	High	—	Oct 10, 2024, 7:11:06 AM	Oct 10, 2024, 7:11:06 AM	Misconfiguration
Malware bad domain	Low	—	Oct 10, 2024	Oct 10, 2024	Threat

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

<input type="checkbox"/> <a href="#">Open SSH port</a>	<span style="color: red;">■</span> High	0	Oct 8, 2024, 10:26:39 AM	Oct 8, 2024, 10:26:39 AM	Misconfiguration
--	---	---	-----------------------------	-----------------------------	------------------

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

<input type="checkbox"/> <a href="#">Public IP address</a> <input type="checkbox"/>	<span style="color: red;">■</span> High	-	Oct 10, 2024, 7:09:53 AM	Oct 10, 2024, 7:09:53 AM	Misconfiguration
---	---	---	-----------------------------	-----------------------------	------------------

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

<input type="checkbox"/> <a href="#">Open RDP port</a>	<span style="color: red;">■</span> High	0	Oct 8, 2024, 10:26:39 AM	Oct 8, 2024, 10:26:39 AM	Misconfiguration
--	---	---	-----------------------------	-----------------------------	------------------

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

The screenshot shows the Google Cloud Compute Engine interface. On the left, there's a sidebar with navigation links like Google Cloud, VM instances, Virtual machines, Storage, Instance groups, and VM Manager. The main area is titled 'VM instances' and shows a list of instances. One instance, 'cc-app-01', is selected and highlighted. A modal dialog box is open over the list, titled 'Stop cc-app-01?'. It contains the following text:

You'll be billed only for these preserved resources:

- Persistent disks
- Static IP addresses

The VM will gracefully shut down. If processes are still running, the VM will be forced to stop and files may get corrupted.

At the bottom of the modal are two buttons: 'CANCEL' and 'STOP'.

On the right side of the screen, there's a sidebar with various tutorials and documentation links, such as 'Get started with Compute Engine', 'Create a website or application', 'Create a "hello world" website on IIS', 'Create an Apache web server on a Linux VM', 'Transfer files to a Windows VM', 'Transfer files to a Linux VM', 'Enable ingress traffic', 'Back up and restore a VM', and 'Back up a disk'.

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.

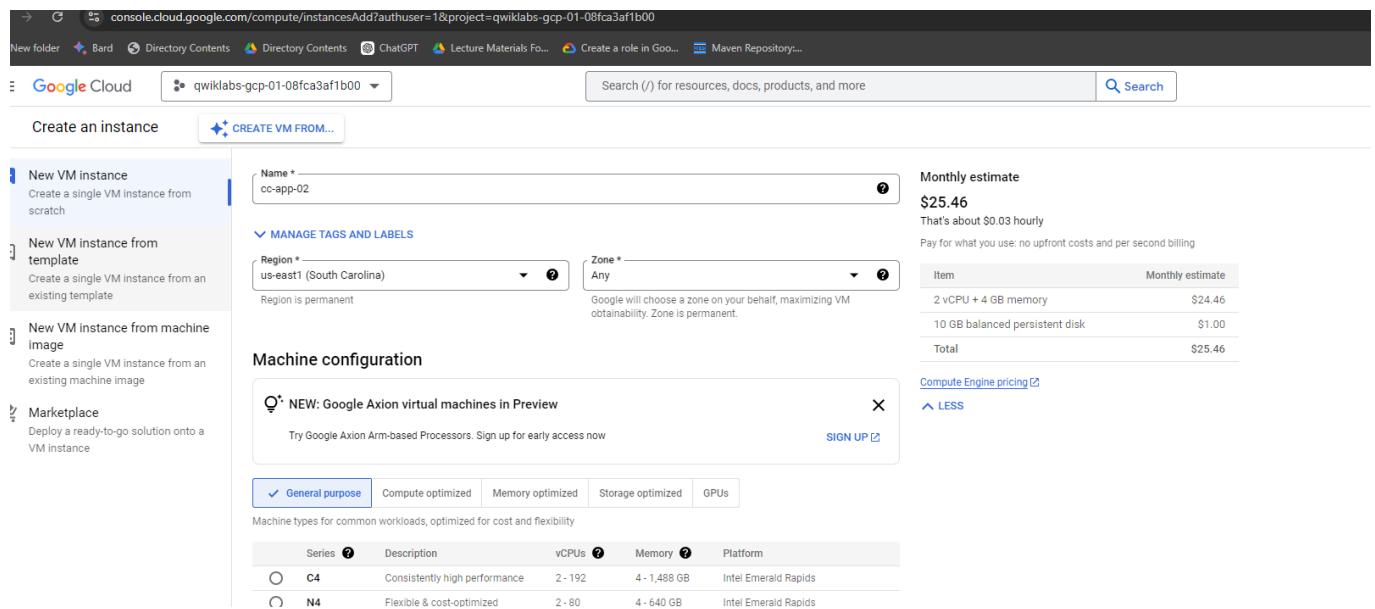


Figure 13 : Creating a new instance named cc-app-02 from the cc-app01-snapshot, ensuring the new instance uses secure boot options..

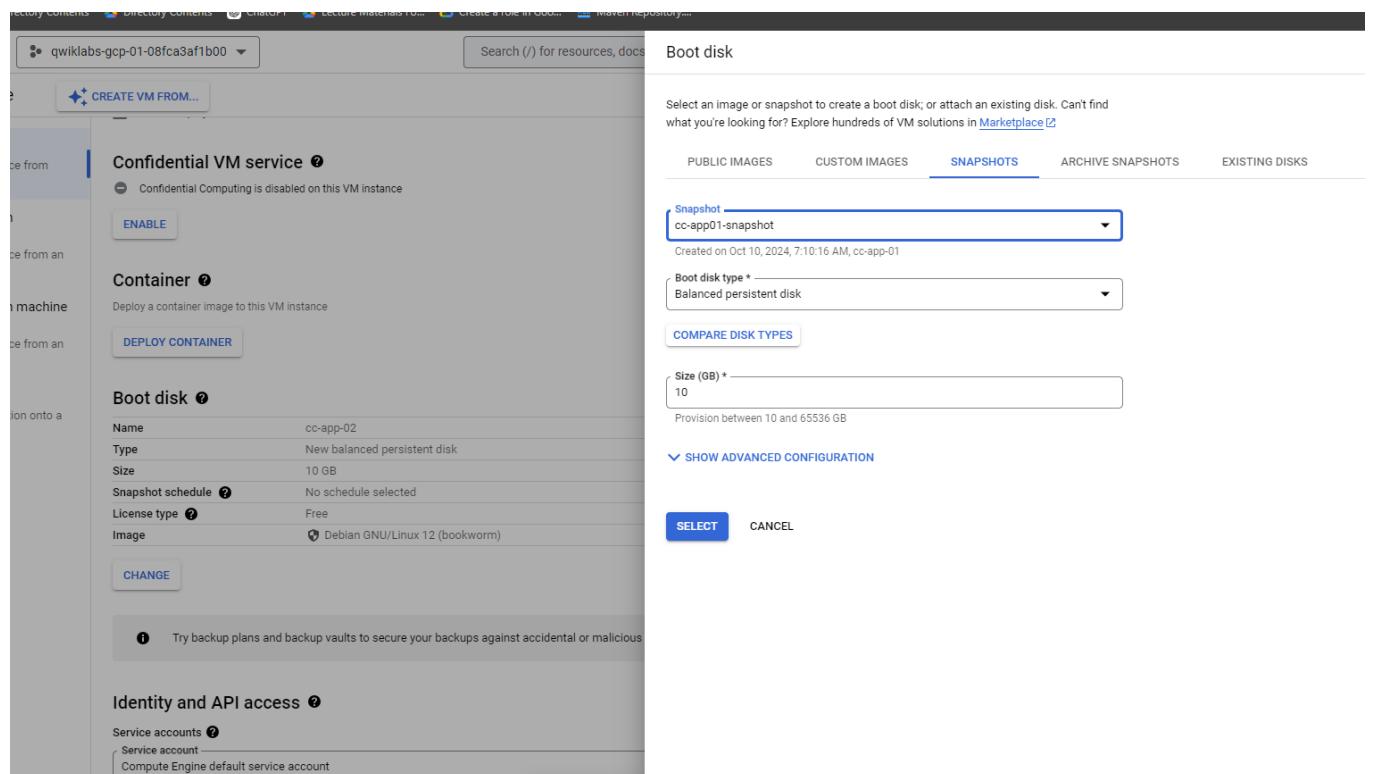


Figure 14 : Selecting the snapshot from the cc-app01-snapshot to replicate the environment while remediating security issues.

The screenshot shows the 'Advanced options' section of a VM configuration. Under 'Networking', there is a 'Network tags' field containing 'cc' with a delete button. Below it is a 'Hostname' field with a question mark icon. A note says 'Set a custom hostname for this instance or leave it default. Choice is permanent.' Under 'IP forwarding', there is an 'Enable' checkbox. In the 'Network performance configuration' section, there is a 'Network interface card' dropdown menu currently set to '-'.

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

## Identity and API access ?

### Service accounts ?

#### Service account

Qwiklabs User Service Account

Requires the Service Account User role (roles/iam.serviceAccountUser) to be set for users who want to access VMs with this service account. [Learn more](#)

### Access scopes ?

Allow default access

Allow full access to all Cloud APIs

Set access for each API

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

^ Edit network interface trash bin icon

Network \*  down arrow icon ?

Subnetwork \*  down arrow icon ?

**i** To use IPv6, you need an IPv6 subnet range. [LEARN MORE](#) checkbox icon

IP stack type  
 IPv4 (single-stack)  
 IPv4 and IPv6 (dual-stack)

Primary internal IPv4 address  down arrow icon ?

Alias IP ranges + ADD IP RANGE

External IPv4 address  down arrow icon ?

DONE

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

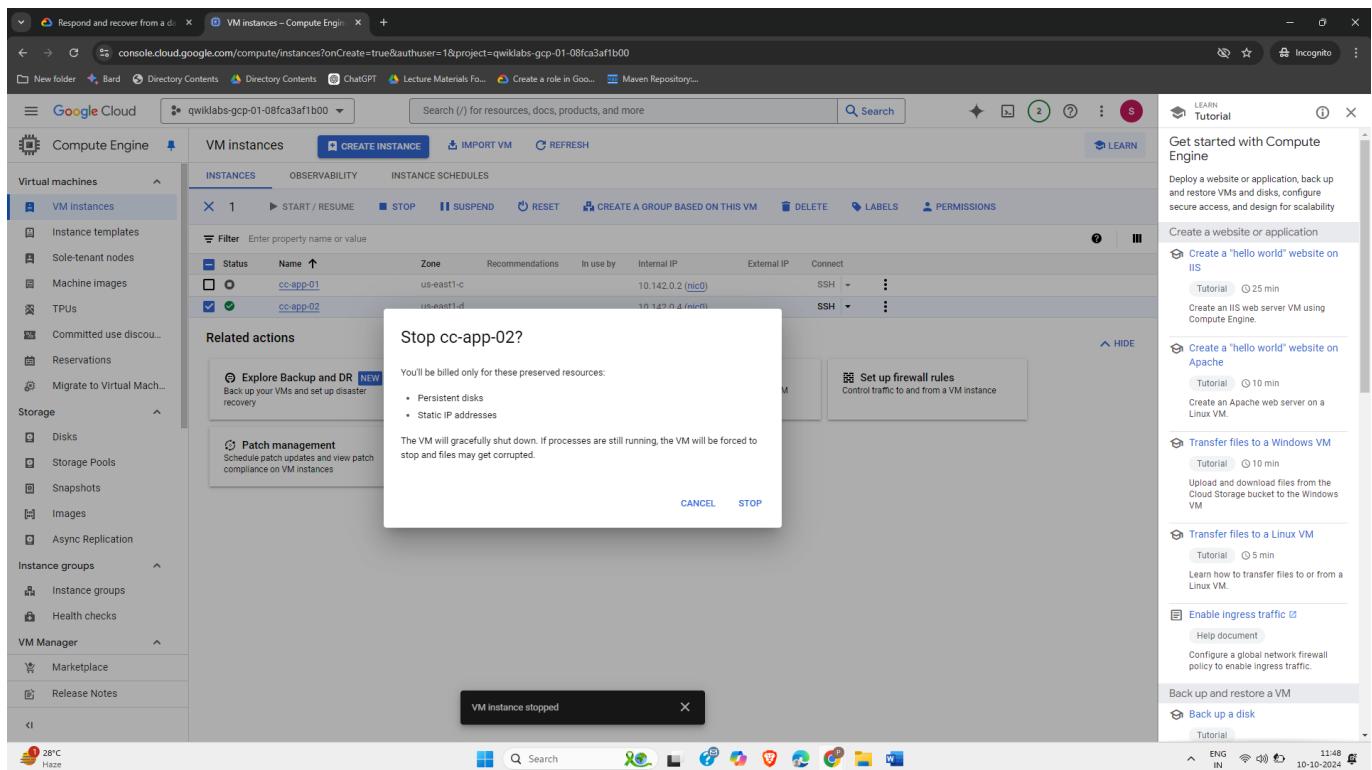


Figure 18 : Stopping the cc-app-02 VM temporarily for additional security configuration and applying the correct firewall rules.

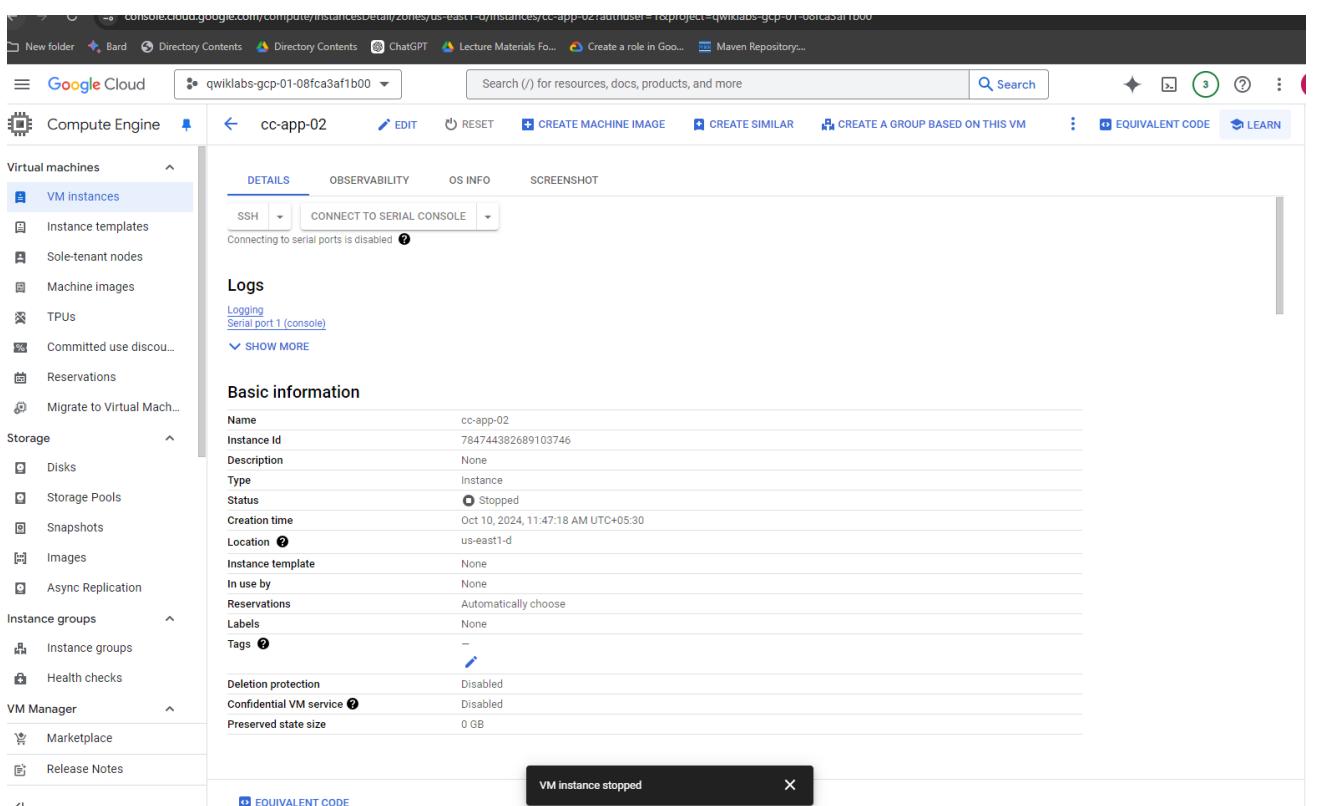


Figure 19 : Editing security settings for the cc-app-02 VM, ensuring that Secure Boot is enabled for compliance with security best practices.

## Security and access

### Shielded VM ?

Turn on all settings for the most secure configuration.

- Turn on Secure Boot ?
- Turn on vTPM ?
- Turn on Integrity Monitoring ?

### SSH Keys

These keys allow access only to this instance, unlike project-wide SSH keys. [Learn more](#)



- Block project-wide SSH keys

When checked, project-wide SSH keys cannot access this instance. [Learn more](#)

+ ADD ITEM

### Identity and API access ?

#### Service accounts ?

Service account

Qwiklabs User Service Account

▼

Requires the Service Account User role (roles/iam.serviceAccountUser) to be set for users who want to access VMs with this service account. [Learn more](#)

#### Access scopes ?

- Allow default access
- Allow full access to all Cloud APIs
- Set access for each API

## Management

VM instance stopped

SAVE

CANCEL

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

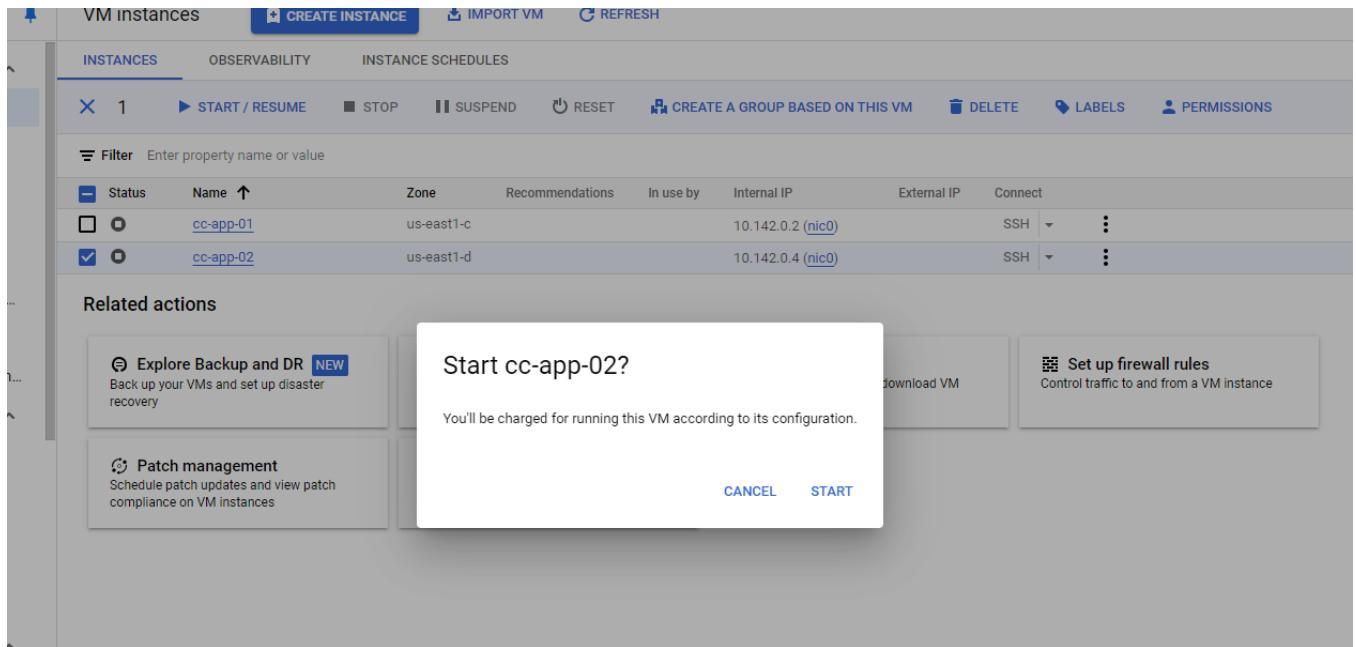


Figure 21 : Starting the cc-app-02 VM instance after ensuring all security protocols are in place.

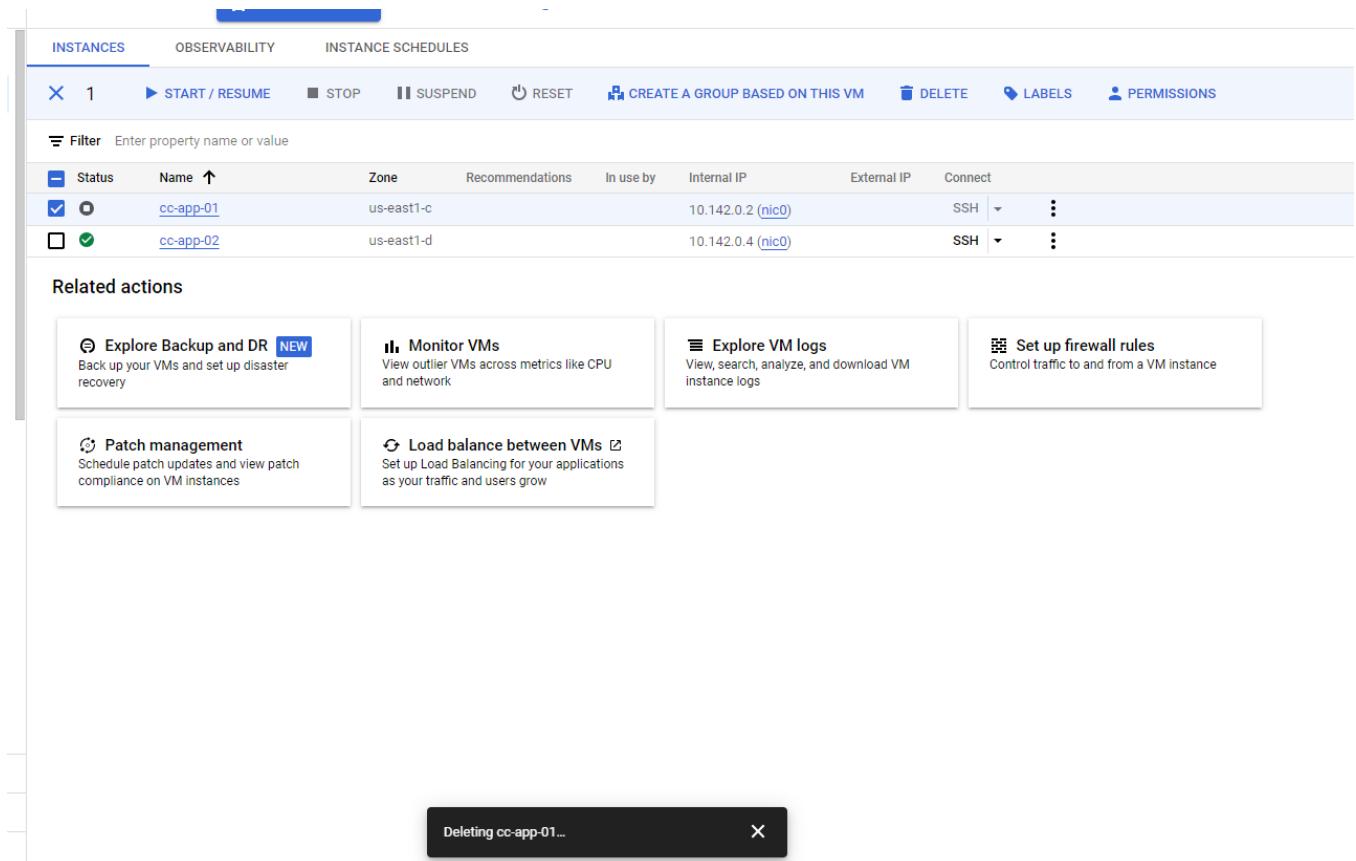


Figure 22 : Deleting the compromised cc-app-01 VM to eliminate the threat and prevent further exploitation.

Filter buckets							
Name	Created	Location type	Location	Default storage class	Last modified	Public access	Access control
qwiklabs-gcp-01-08fc3af1b00_bucket	Oct 10, 2024, 7:11:04 AM	Region	us-east1	Standard	Oct 10, 2024, 7:11:05 AM	Public to internet	Fine-grained

Figure 23 : Navigating to the project\_id\_bucket storage bucket where sensitive data was compromised and needs to be secured.

The screenshot shows the Google Cloud Storage console interface. On the left, there's a sidebar with 'Google Cloud' navigation, 'Cloud Storage' selected, and sub-options like 'Overview', 'Buckets' (which is currently active), 'Monitoring', and 'Settings'. The main area displays 'Bucket details' for 'qwiklabs-gcp-01-08fc3af1b00\_bucket'. Key information shown includes the location (us-east1), storage class (Standard), and public access status (Public to Internet). A warning message states: 'Public to internet: This bucket is publicly accessible because allUsers or allAuthenticatedUsers have one or more permissions. Remove these principals to stop public access.' Below this, there are tabs for 'OBJECTS', 'CONFIGURATION', 'PERMISSIONS', 'PROTECTION', 'LIFECYCLE', 'OBSERVABILITY', 'INVENTORY REPORTS', and 'OPERATIONS'. Under the 'OBJECTS' tab, a 'Folder browser' shows a single object named 'myfile.csv'. The object details are: Name: myfile.csv, Size: 11.2 KB, Type: application/octet-stream, Created: Oct 10, 2024, 7:13:18 AM, Storage class: Standard, Last modified: Oct 10, 2024, 7:13:18 AM. At the bottom of the page, a modal window displays the message 'Instance deleted'.

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

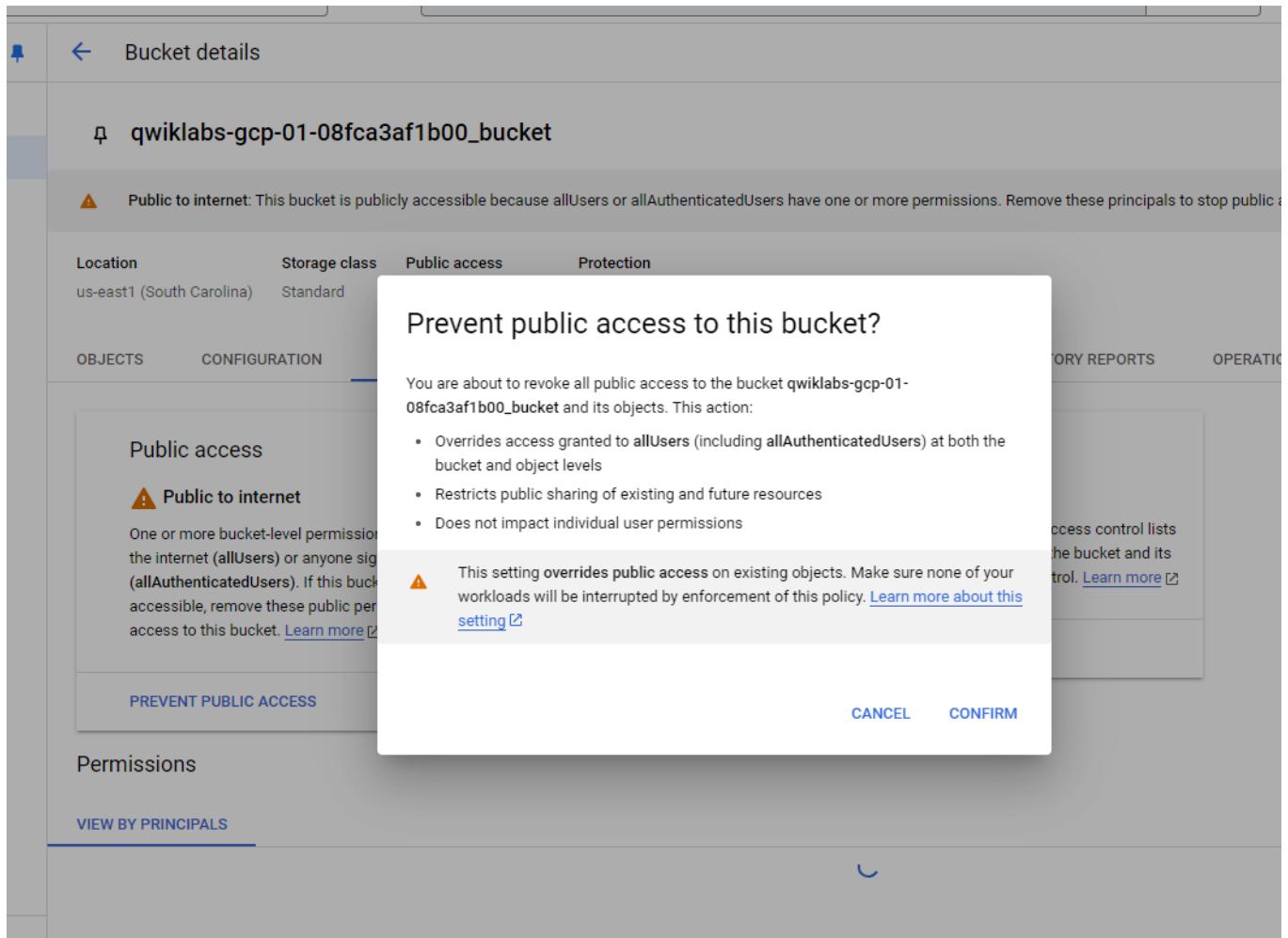


Figure 25 : Revoking public access to the storage bucket by selecting the "Prevent public access" option to safeguard the data.

### qwiklabs-gcp-01-08fca3af1b00\_bucket

Location	Storage class	Public access	Protection
us-east1 (South Carolina)	Standard	Not public	Soft Delete

**PERMISSIONS**

**Public access**

**Not public**

This bucket is not publicly accessible since public access is being prevented. Because of this restriction, objects cannot be publicly shared over the internet. [Learn more](#)

**Principals restricted from bucket access:**  
allUsers, allAuthenticatedUsers

[REMOVE PUBLIC ACCESS PREVENTION](#)

**Access control**

**Fine-grained: Object-level ACLs enabled**

Access to objects can be granted through object access control lists (ACLs). To enforce a single set of permissions on the bucket and its objects, switch to uniform bucket-level access control. [Learn more](#)

[SWITCH TO UNIFORM](#)

**Permissions**

[VIEW BY PRINCIPALS](#)
[VIEW BY ROLES](#)

[+👤 GRANT ACCESS](#)
[-👤 REMOVE ACCESS](#)

Filter Enter property name or value

Type	Principal ↑	Name	Role	Inheritance
<input type="checkbox"/>	4130877743@cloudbuild.gserviceaccount.com	Legacy Cloud Build Service Account	Cloud Build Service Account	
<input type="checkbox"/>	allUsers		Storage Legacy Bucket Reader	
<input type="checkbox"/>	Editors of project: qwiklabs-gcp-01-08fca3af1b00	Public access is prevented for this bucket	X	Storage Legacy Bucket Owner

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

[REMOVE PUBLIC ACCESS PREVENTION](#)

**Permissions**

[VIEW BY PRINCIPALS](#)
[VIEW BY ROLES](#)

[+👤 GRANT ACCESS](#)
[-👤 REMOVE ACCESS](#)

Filter Enter property name or value

Type	Principal ↑	Name	Role	Inheritance
<input type="checkbox"/>	4130877743@cloudbuild.gserviceaccount.com	Legacy Cloud Build Service Account	Cloud Build Service Account	
<input checked="" type="checkbox"/>	allUsers		Storage Legacy Bucket Reader	
<input type="checkbox"/>	Editors of project: qwiklabs-gcp-01-08fca3af1b00		Storage Legacy Bucket Owner	

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

The screenshot shows the Google Cloud Network Security Firewall policies interface. On the left sidebar, under 'Cloud NGFW', 'Firewall policies' is selected. The main area displays a table of existing firewall rules:

	Name	Type	Targets	Filters	Protocols / ports	Action
<input type="checkbox"/>	<a href="#">default-allow-icmp</a>	Ingress	Apply to all	IP ranges:	icmp	Allow
<input type="checkbox"/>	<a href="#">default-allow-internal</a>	Ingress	Apply to all	IP ranges:	tcp:0-65535 udp:0-65535 icmp	Allow
<input type="checkbox"/>	<a href="#">default-allow-rdp</a>	Ingress	Apply to all	IP ranges:	tcp:3389	Allow
<input type="checkbox"/>	<a href="#">default-allow-ssh</a>	Ingress	Apply to all	IP ranges:	tcp:22	Allow

A note at the top right states: "Note: App Engine firewalls are managed in the [App Engine Firewall rules section](#)". A warning message in a box says: "SMTP port 25 disallowed in this project. [Learn more](#)".

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

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

**Name \***  ?

Lowercase letters, numbers, hyphens allowed

**Description**

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

Deny

Targets  
Specified target tags

Target tags \*  
cc

Source filter  
IPv4 ranges

Source IPv4 ranges \*  
35.235.240.0/20

Second source filter  
None

Destination filter  
None

Protocols and ports

Allow all

Specified protocols and ports

TCP

Ports  
22

E.g. 20, 50-60

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'.

<input type="button" value="REFRESH"/> <input type="button" value="CONFIGURE LOGS"/> <input type="button" value="DELETE"/>											
<input type="button" value="Filter"/> Enter property name or value											
	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network <input type="button" value="UP"/>	Logs	Hit count <input type="button" value="?"/>	Last hit <input type="button" value="?"/>
<input type="checkbox"/>	limit-ports	Ingress	cc	IP ranges:	tcp:22	Allow	1000	<u>default</u>	Off	-	-
<input checked="" type="checkbox"/>	default-allow-icmp	Ingress	Apply to all	IP ranges:	icmp	Allow	65534	<u>default</u>	Off	-	-
<input type="checkbox"/>	default-allow-internal	Ingress	Apply to all	IP ranges:	tcp:0-65535 udp:0-65535 icmp	Allow	65534	<u>default</u>	Off	-	-
<input checked="" type="checkbox"/>	default-allow-rdp	Ingress	Apply to all	IP ranges:	tcp:3389	Allow	65534	<u>default</u>	Off	-	-
<input checked="" type="checkbox"/>	default-allow-ssh	Ingress	Apply to all	IP ranges:	tcp:22	Allow	65534	<u>default</u>	Off	-	-

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

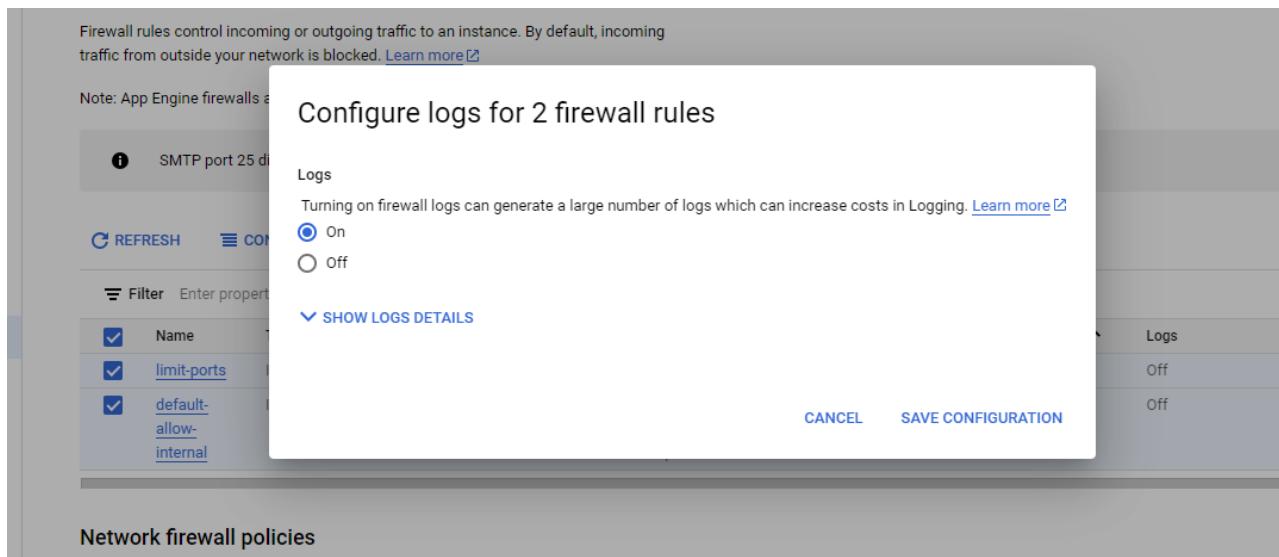


Figure 32 : Enabling logging for custom firewall rules to track network traffic and ensure compliance with security best practices.

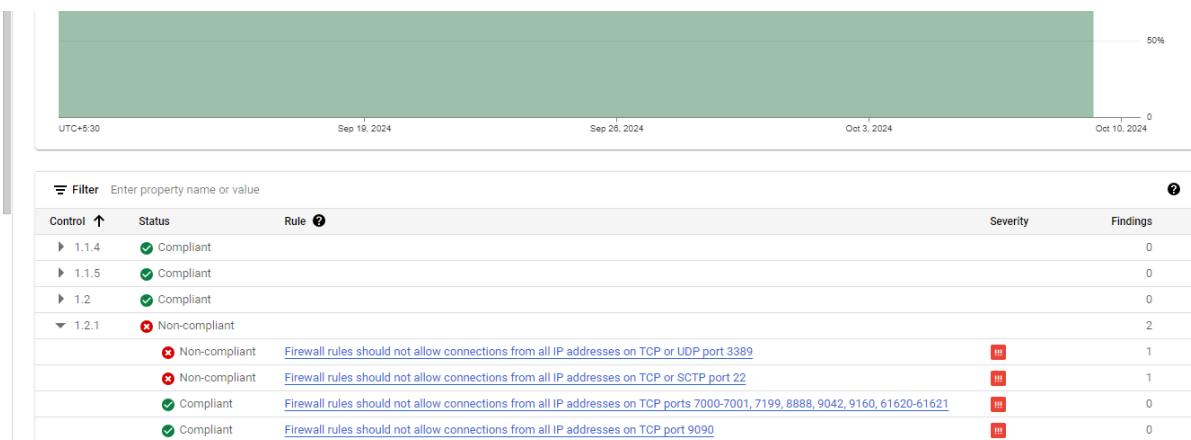


Figure 33 : Reviewing the updated compliance status in Google Cloud Security Command Center to verify that all findings have been addressed.

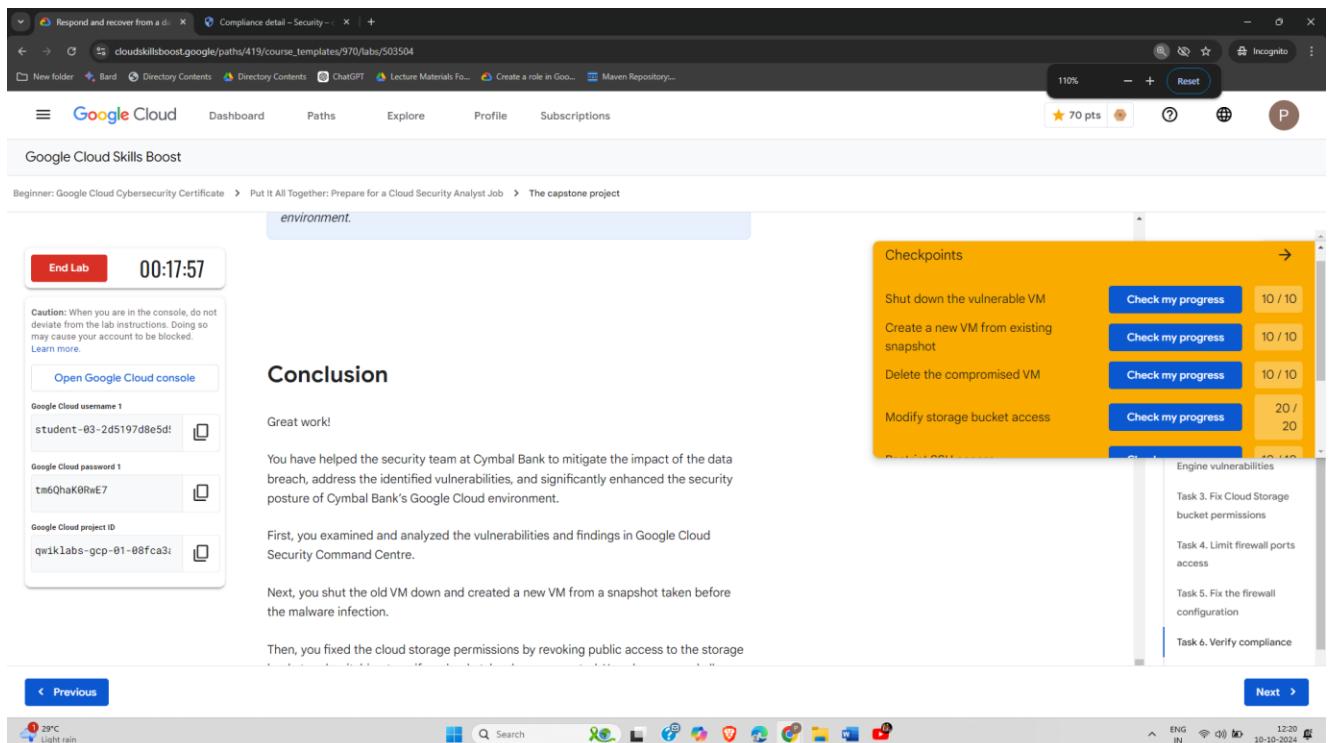


Figure 34 : completing the lab and verifying that all tasks, including remediation and compliance checks, were successful.

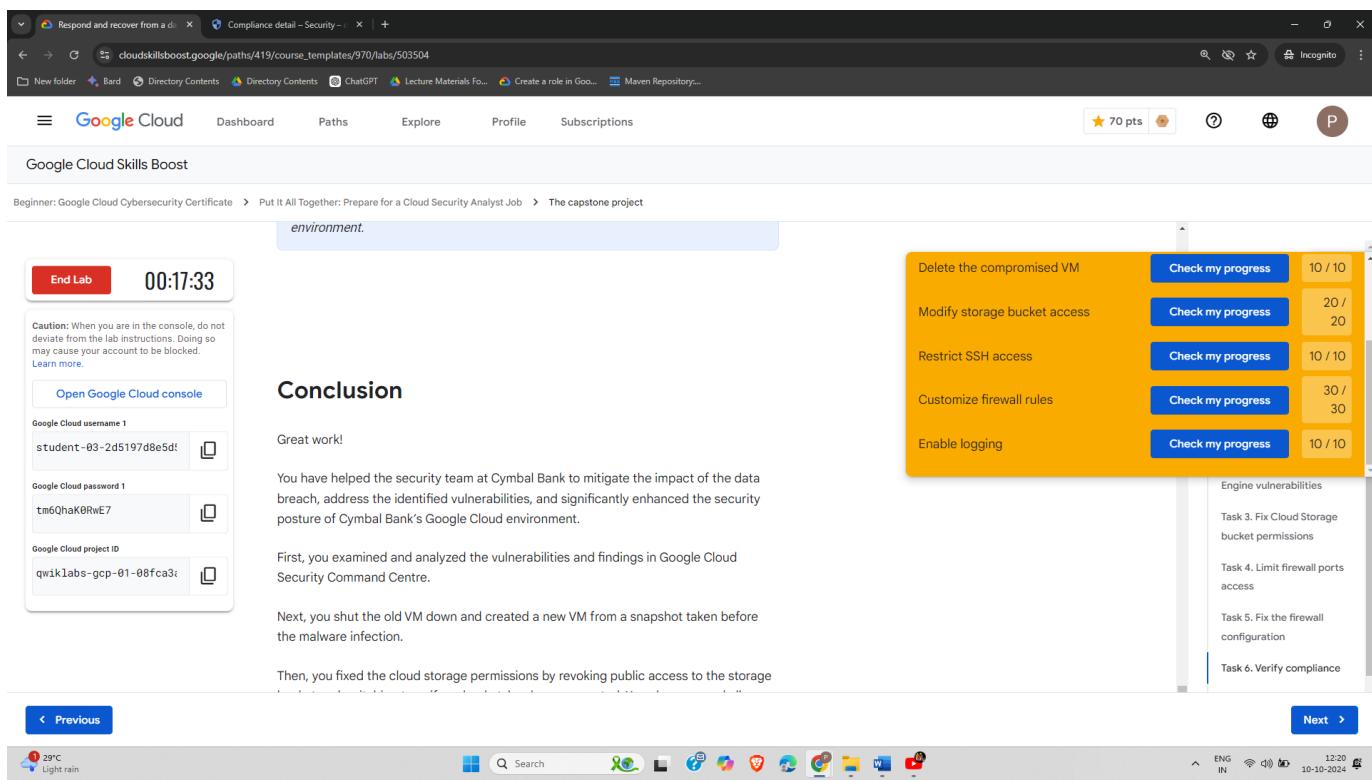


Figure 35 : completing the lab and verifying that all tasks, including remediation and compliance checks, were successful.

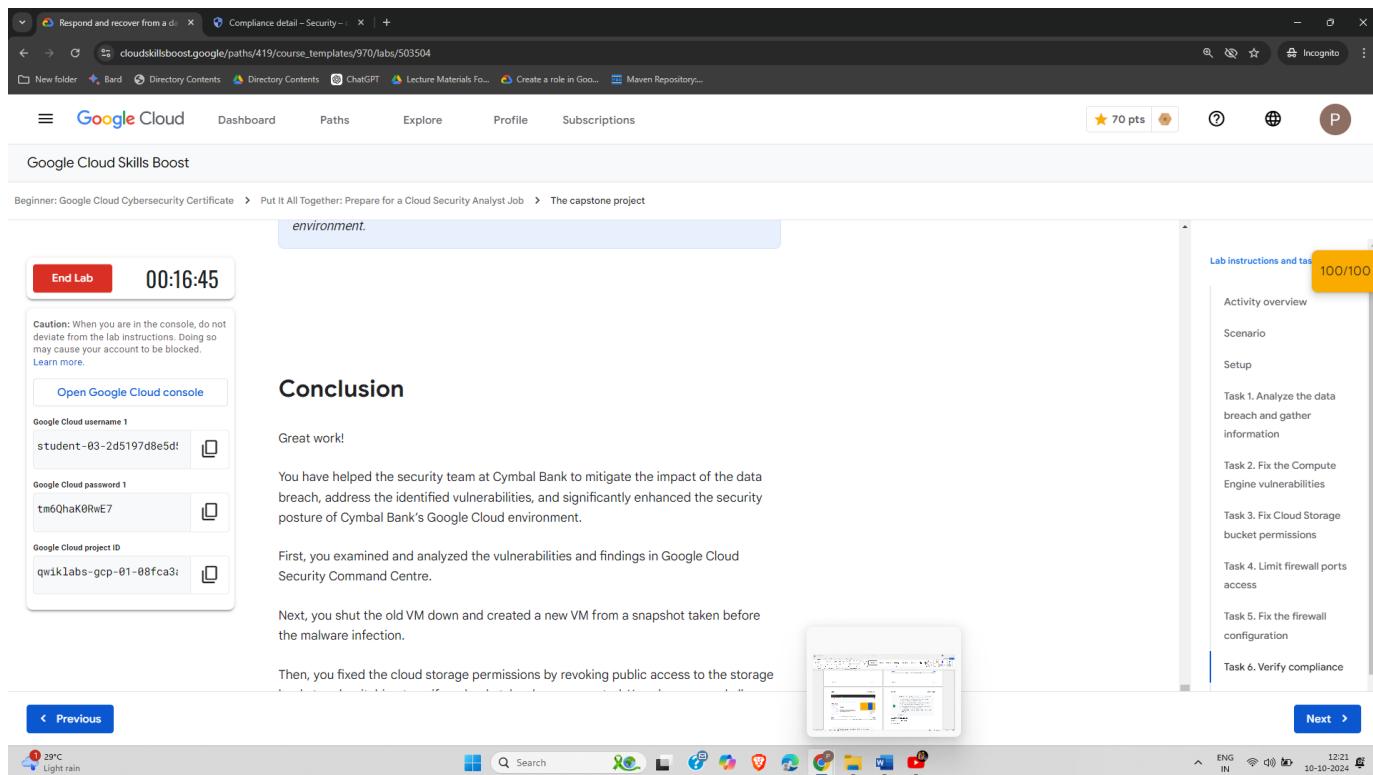


Figure 36 : completing the lab and verifying that all tasks, including remediation and compliance checks, were successful.

Which three resource types are listed with high severity findings?

Network, Firewall, and Bucket

Bucket, Subnetwork, and ServiceAccountKey

Network, Subnetwork, and compute.Instance

Bucket, compute.Instance, and Firewall

**Submit**

Figure 37 : MCQ

Which of the following findings are listed as high severity findings?

Public IP address, Default service account used, Full API access, and Firewall rule logging disabled

Bucket policy only disabled, Bucket logging disabled, Malware bad domain, and Compute secure boot disabled

Firewall rule logging disabled, Compute secure boot disabled, Public IP address, and Bucket logging disabled

Public bucket ACL, Public IP address, Open SSH port, and Open RDP port

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](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/>