



**IDENTIFY VULNERABILITIES,  
RESPOND, REMEDIATE AND  
RECOVER FROM A DATA  
BREACH:**

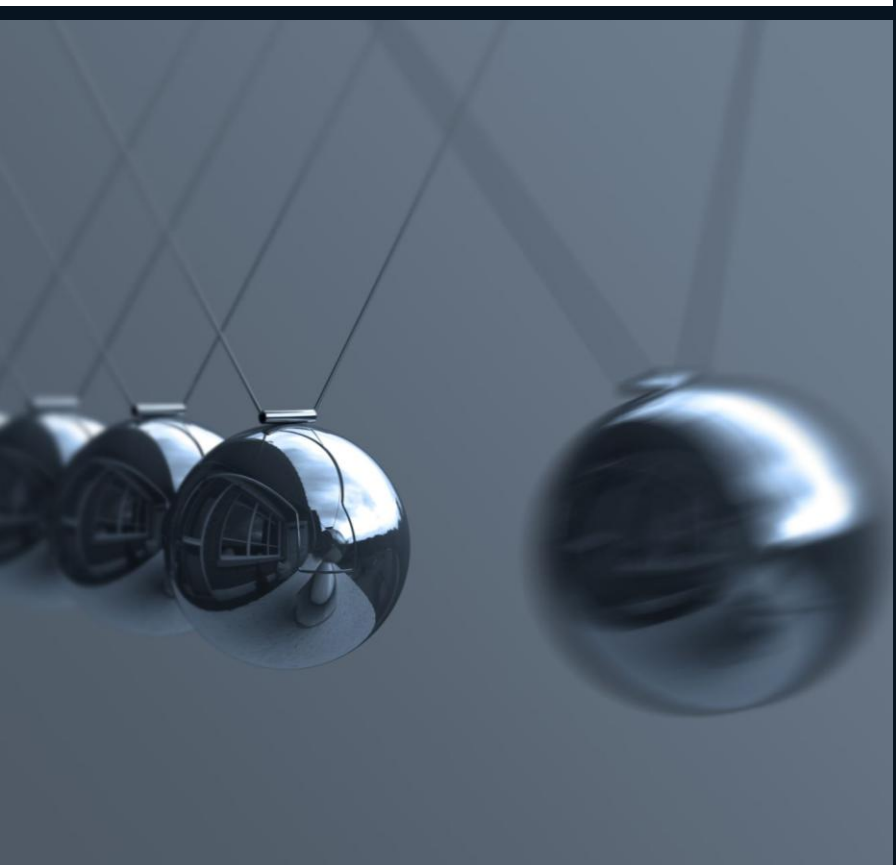
*using **Google** Cloud  
Security Command  
Center*

LOUIS.O

**Task 1. Analyze the  
data breach and  
gather information**

LOUIS.O

# Scenario: Cymbal Retail Data Breach



- Cymbal Retail runs 170 stores and an online platform in 28 countries, with \$15B revenue and 80,400 staff. Millions of transactions occur daily, so security and compliance are critical.
- Recently, the company suffered a major data breach. As a junior cloud security analyst, you will:
  - Identify vulnerabilities in Google Cloud Security Command Center
  - Shut down old VM & create new one from snapshot
  - Restrict public access to storage bucket & enforce uniform access
  - Limit firewall ports and fix firewall rules
  - Run compliance report to verify remediation
- **Goal:** Contain the breach, recover systems, remediate risks, and ensure compliance.

1. In the Google Cloud console, in the **Navigation menu** (☰), click **Security > Risk overview**. The Security Command Center Overview page opens.
2. Scroll down to **Active vulnerabilities**. This provides an overview of current security vulnerabilities or issues that need attention within the Google Cloud environment.
3. Select the **Findings By Resource Type** tab. The security findings or vulnerabilities based on the type of cloud resource affected (e.g., instances, buckets, databases) are organized. By reviewing active

# Sign-In To Account

The image shows a Google Cloud sign-in dialog box overlaid on a dashboard. The dialog contains the following elements:

- Account information: A profile icon with the letter 'S', the name 'student 3f2a64f4', and the email 'student-03-951b8559f126@qwiklabs.net'. A 'Switch account' link is to the right.
- Country selection: A dropdown menu currently showing 'Nigeria'. A red arrow labeled '1' points to this dropdown.
- Terms of Service: A checkbox with a blue checkmark is checked. The text reads: 'I agree to the [Google Cloud Platform Terms of Service](#), and the terms of service of [any applicable services and APIs](#)'. A red box highlights the checkbox.
- Agree and continue: A blue button labeled 'Agree and continue' is at the bottom right. A red box highlights this button, and a red arrow labeled '2' points from it to the 'Switch account' link.

The background dashboard includes a navigation sidebar with 'Cloud Hub', 'Cloud overview', 'Solutions', and 'Recently visited'. The main content area shows 'Google Cloud Platform status' (All services normal), 'Billing' (Estimated charges USD \$0.00), and 'Monitoring'.

### Project info

Project name  
qwiklabs-gcp-04-867c17bf76fa

Project number  
377021291057

Project ID  
qwiklabs-gcp-04-867c17bf76fa

[Add people to this project](#)

[Go to project settings](#)

### Resources

BigQuery  
Data warehouse/analytics

### Compute Engine

CPU (%)

● instance/cpu/utilization: 7.62%

[The data might not be complete due to potential unavailability of certain regions. Visit Cloud Hub for more accurate data.](#)

### Google Cloud Platform status

All services normal

[Go to Cloud status dashboard](#)

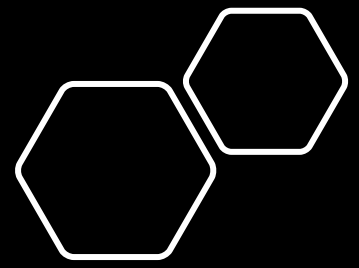
### Billing

Estimated charges USD \$0.00  
For the billing period Aug 1 – 20, 2025

[Take a tour of billing](#)

[View detailed charges](#)

### Monitoring



LOUIS.O

- Marketplace
- APIs & Services
- Vertex AI
- Compute Engine
- Kubernetes Engine
- Cloud Storage
- Security**
- BigQuery
- Monitoring
- Cloud Run

- Security Command Center
  - Risk Overview** → 2
  - Compliance
  - Assets
  - Findings
  - Sources
  - Posture Management
- Detections and Controls
  - Google SecOps
  - reCAPTCHA** → 1
  - Model Armor
  - Web Security Scanner
  - Cyber Insurance Hub
  - Binary Authorization
  - Advisory Notifications

[View all products](#)

Search

Google Cloud Platform status: All services normal

Go to Cloud status dashboard

Billing: Estimated charges for Aug 1 - 20, 2024

Take a tour of billing

View detailed charges

Monitoring

# Scroll down to “Active Vulnerabilities”

**Security**

**Risk overview** Overall, are you satisfied with SCC? [SETTINGS](#)

Security Command Center

- Risk Overview**
- Threats
- Vulnerabilities
- Compliance
- Assets
- Findings
- Sources
- Posture Management

Detections and Controls

- Marketplace
- Release Notes

Use Security Command Center's overview dashboard to find the most severely rated findings in your organization so you can prioritize fixes.

**i** This page displays results only for projects which have Security Command Center services enabled. Some services may not be enabled for all of your projects or clusters. Enable these services in settings.

[EDIT SETTINGS](#) [DISMISS](#)

**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](#)

### Active vulnerabilities

80 active vulnerabilities

Findings By Category

Findings By Resource Type

Findings By Project

Filter Categories

Severity ↓	Finding category	Total findings
!!!	<a href="#">Open RDP port</a>	1
!!!	<a href="#">Open SSH port</a>	1
!!!	<a href="#">Public bucket ACL</a>	1
!!!	<a href="#">Public IP address</a>	1
!!	<a href="#">Firewall rule logging disabled</a>	4
!!	<a href="#">Admin service account</a>	1
!!	<a href="#">Bucket policy only disabled</a>	1
!!	<a href="#">Compute Secure Boot disabled</a>	1
!!	<a href="#">Default service account used</a>	1
!!	<a href="#">Full API access</a>	1

LOUIS.O

Security Command Ce...

Risk Overview

Threats

Vulnerabilities

Compliance

Assets

Findings

Sources

Posture Management

Detections and Controls

Google SecOps

reCAPTCHA

Model Armor

Marketplace

Release Notes

<1

### Active vulnerabilities

80 active vulnerabilities

Findings By Category Findings By Resource Type Findings By Project

Filter Resource types

Resource Type ↑	Critical Findings	High Severity Findings	Medium Severity Findings	Low Severity Findings	Unspecified Severity Findings
<a href="#">Bucket</a>	0	1	1	1	0
<a href="#">compute.Instance</a>	0	1	3	0	0
<a href="#">Firewall</a>	0	2	4	0	0
<a href="#">resourcemanager.Project</a>	0	0	2	8	0
<a href="#">ServiceAccountKey</a>	0	0	1	0	0
<a href="#">Subnetwork</a>	0	0	0	56	0

### Identity and access findings

Top severity identity and access findings by category.

Severity ↓	Finding category	Cloud Provider	Total findings
!!!	<a href="#">Public bucket ACL</a>	Google	1

### AI Workload findings

Review violations to Secure AI policies, drift from security issues detected on AI resources

Vulnerabilities Policy Drift

Scroll down to PCI DSS3.2.1 and click "View details"

The screenshot shows the Google Cloud Security Command Center interface. At the top, the breadcrumb navigation includes 'Google Cloud', 'qwiklabs-gcp-04-867c17bf76fa', and 'Compliance'. The left sidebar lists various security tools, with 'Compliance' selected. The main content area is titled 'Compliance' and features a 'Monitor' tab. It displays four compliance frameworks with their respective passing percentages and 'View details' links. Red annotations include a box around the scrollbar, an arrow labeled '1' pointing to the 'Compliance' breadcrumb, and an arrow labeled '2' pointing to the 'View details' link for PCI DSS 3.2.1.

Compliance Framework	Passing Percentage	Action
100% passing	100%	<a href="#">View details</a>
100% passing	100%	<a href="#">View details</a>
PCI DSS 3.2.1	87%	<a href="#">View details</a>
PCI DSS 4.0	50%	<a href="#">View details</a>
SOC2 2017	56%	<a href="#">View details</a>

Google Cloud | qwiklabs-gcp-03-cab28d253fb9 | Search (/) for resources, docs, products, and

Security | Compliance detail

UTC+1 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Aug 12 Aug 13 Aug 14 Aug 15 Aug 16 Aug 17 Aug 18

Filter Enter property name or value

Control ↑	Status	Rule ?	Severity	Findings
▶ 1.1.4	✔ Compliant			0
▶ 1.1.5	✔ Compliant			0
▶ 1.2	✔ Compliant			0
▶ 1.2.1	✔ Compliant			0
▶ 1.2.2	✔ Compliant			0
▶ 1.3	✔ Compliant			0
▶ 1.3.2	✔ Compliant			0
▶ 1.3.4	✔ Compliant			0
▶ 1.3.7	✔ Compliant			0
▶ 2.1	✔ Compliant			0
▶ 2.2	✔ Compliant			0
▶ 2.2.2	✔ Compliant			0
▶ 2.3	✔ Compliant			0
▶ 2.4	✔ Compliant			0
▶ 3.5	✔ Compliant			0

Security Command Center

- Risk Overview
- Threats
- Vulnerabilities
- Compliance**
- Assets
- Findings
- Sources
- Posture Management

Detections and Controls

- Google SecOps
- reCAPTCHA
- Model Armor
- Web Security Scanner
- Marketplace

Google Cloud | qwiklabs-gcp-03-cab28d253fb9 | Search (/) for resources, docs, products, and

Security | Compliance detail

UTC+1 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Aug 12 Aug 13 Aug 14 Aug 15 Aug 16 Aug 17 Aug 18

Filter Enter property name or value

Control	Status	Rule ?	Severity	Findings
▶ 7.1.2	✘ Non-compliant			1
▶ 10.1	✘ Non-compliant			1
▶ 10.2	✘ Non-compliant			1
▶ 1.1.4	✔ Compliant			0
▶ 1.1.5	✔ Compliant			0
▶ 1.2	✔ Compliant			0
▶ 1.2.1	✔ Compliant			0
▶ 1.2.2	✔ Compliant			0
▶ 1.3	✔ Compliant			0
▶ 1.3.2	✔ Compliant			0
▶ 1.3.4	✔ Compliant			0
▶ 1.3.7	✔ Compliant			0
▶ 2.1	✔ Compliant			0
▶ 2.2	✔ Compliant			0
▶ 2.2.2	✔ Compliant			0
▶ 2.3	✔ Compliant			0
▶ 2.4	✔ Compliant			0

Security Command Center

- Risk Overview
- Threats
- Vulnerabilities
- Compliance**
- Assets
- Findings
- Sources
- Posture Management

Detections and Controls

- Google SecOps
- reCAPTCHA
- Model Armor
- Web Security Scanner
- Marketplace
- Release Notes



# In the Quick filters panel, scroll down and checkbox “Google Cloud Storage Bucket”

Google Cloud | qwiklabs-gcp-03-cab28d253fb9 | Search (/) for resources, docs, products, and more | Search

Security | Findings | You can now search for documentation, resource metadata, tutorials, and API keys | Feedback | Settings | Learn

Security Command Ce...  
Risk Overview  
Threats  
Vulnerabilities  
Compliance  
Assets  
Findings  
Sources  
Posture Management  
Detections and Controls  
Google SecOps  
reCAPTCHA  
Model Armor  
Web Security Scanner  
Marketplace  
Release Notes

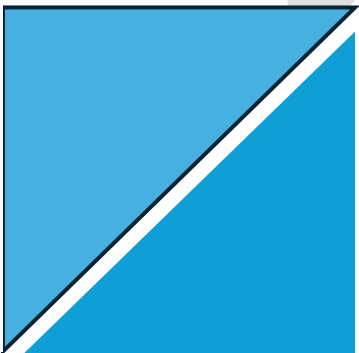
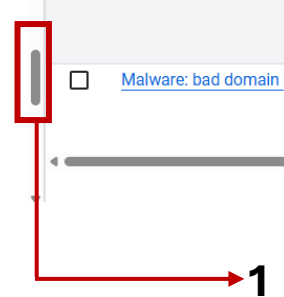
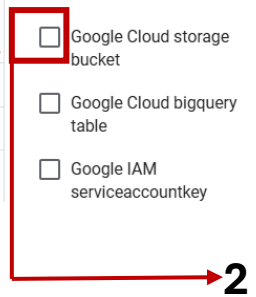
Filter findings on IP range  
You can now use the new inIpRange function to filter findings based on whether they contain or do not contain an IPv4 or IPv6 IP address within a specified CIDR range. For example: `contains(connections, inIpRange(source_ip, "192.0.2.0/24"))`. [Learn more](#)

Query preview  
`state="ACTIVE" AND NOT mute="MUTED"` | Edit query | Time range: Last 7 days

Quick filters | Clear all | Findings query results | Change active state | Set security marks | Mute options | Export | Columns

Quick filters	Findings query results
<input checked="" type="checkbox"/> resourcemanager project (11)	<input type="checkbox"/> Category
<input type="checkbox"/> Google compute firewall (6)	<input type="checkbox"/> <a href="#">Exfiltration: bigquery data extraction</a>   Severity: Low   Attack exposure score: -   Event time: Sep 3, 2025, 8:38:05 PM   Create time: Sep 3, 2025, 8:38:05 PM   Finding c
<input type="checkbox"/> Google compute instance (5)	<input type="checkbox"/> <a href="#">Discovery: service account self-investigation</a>   Severity: Low   Attack exposure score: -   Event time: Sep 3, 2025, 8:35:58 PM   Create time: Sep 3, 2025, 8:35:58 PM   Threat
<input type="checkbox"/> Google Cloud storage bucket (3)	<input type="checkbox"/> <a href="#">Malware: bad domain</a>   Severity: Low   Attack exposure score: -   Event time: Sep 3, 2025, 8:35:44 PM   Create time: Sep 3, 2025, 8:35:45 PM   Threat
<input type="checkbox"/> Google Cloud bigquery table (1)	
<input type="checkbox"/> Google IAM serviceaccountkey (1)	

Rows per page: 30 | 1 - 30 of 83



In the **Quick filters** panel, scroll down to **Resource Type** section select the checkbox for the **Google compute Instance** resource type and uncheck **Google Cloud storage bucket**

Google Cloud | qwiklabs-gcp-03-cab28d253fb9 | Search (/) for resources, docs, products, and more | Search

Security | Findings | You can now search for documentation, resource metadata, tutorials, and API keys | Feedback | Setting

### Filter findings on IP range

You can now use the new `inIpRange` function to filter findings based on whether they contain or do not contain an IPv4 or IPv6 IP address within a specified CIDR range. For example: `contains(connections, inIpRange(source_ip, "192.0.2.0/24"))`. [Learn more](#)

Query preview: `state="ACTIVE" AND NOT mute="MUTED" AND resource.type="google.cloud.storage.Bucket"` | Edit query | Time range: Last 7 days

Quick filters: Clear all | resourcemanager project (11) | Google compute firewall (6) |  Google compute instance (5) |  Google Cloud storage bucket (3) | Google Cloud bigquery table (1) | Google IAM serviceaccountkey (1)

### Findings query results

Change active state | Set security marks | Mute options | Export

Category	Severity	Attack exposure score	Event time	Create time	Finding
<input type="checkbox"/> <a href="#">Public bucket ACL</a>	High	—	Sep 3, 2025, 8:35:43 PM	Sep 3, 2025, 8:35:44 PM	Miscon
<input type="checkbox"/> <a href="#">Bucket logging disabled</a>	Low	—	Sep 3, 2025, 8:35:41 PM	Sep 3, 2025, 8:35:42 PM	Miscon
<input type="checkbox"/> <a href="#">Bucket policy only disabled</a>	Medium	—	Sep 3, 2025, 8:35:41 PM	Sep 3, 2025, 8:35:42 PM	Miscon

Rows per page: 30 | 1 - 3 of

- Security
- Security Command Ce...
- Risk Overview
- Threats
- Vulnerabilities
- Compliance
- Assets
- Findings**
- Sources
- Posture Management
- Detections and Controls
  - Google SecOps
  - reCAPTCHA
  - Model Armor
  - Web Security Scanner
- Marketplace
- Release Notes

Findings You can now search for documentation, resource metadata, tutorials, and API keys Feedback Settings Learn

### Filter findings on IP range

You can now use the new `inIpRange` function to filter findings based on whether they contain or do not contain an IPv4 or IPv6 IP address within a specified CIDR range. For example: `contains(connections, inIpRange(source_ip, "192.0.2.0/24"))`. [Learn more](#)

Query preview `state="ACTIVE" AND NOT mute="MUTED" AND resource.type="google.compute.Instance"` Edit query Time range: Last 7 days

- #### Quick filters
- resourcemanager project 11
  - Google compute firewall 6
  - Google compute instance 5
  - Google Cloud storage bucket 3
  - Google Cloud bigquery table 1
  - Google IAM serviceaccountkey 1

#### Findings query results

Category	Severity	Attack exposure score	Event time	Create time	Finding class
<input type="checkbox"/> <a href="#">Malware: bad domain</a>	Low	—	Sep 3, 2025, 8:35:44 PM	Sep 3, 2025, 8:35:45 PM	Threat
<input type="checkbox"/> <a href="#">Compute Secure Boot disabled</a>	Medium	—	Sep 3, 2025, 8:33:36 PM	Sep 3, 2025, 8:33:36 PM	Misconfiguration
<input type="checkbox"/> <a href="#">Default service account used</a>	Medium	—	Sep 3, 2025, 8:33:36 PM	Sep 3, 2025, 8:33:36 PM	Misconfiguration

In the **Quick filters** panel, scroll down to **Resource Type** section , uncheck **Google compute instance** and check **Google Compute firewall**,

In the **Quick filters** panel, scroll down to **Resource Type** section select the checkbox for the **Google compute firewall** resource type

The screenshot shows the Google Cloud Security console interface. The top navigation bar includes the Google Cloud logo, account ID (qwiklabs-gcp-03-cab28d253fb9), a search bar, and utility icons. The left sidebar contains navigation options like Security Command Center, Risk Overview, Threats, Vulnerabilities, Compliance, Assets, Findings, Sources, Posture Management, and Detections and Controls. The main content area is titled 'Findings' and features a 'Filter findings on IP range' notification. Below this is a 'Query preview' section with the query: `state="ACTIVE" AND NOT mute="MUTED" AND resource.type="google.compute.Firewall"`. The 'Quick filters' panel on the left lists various resource types, with 'Google compute firewall' selected. The 'Findings query results' table displays three findings, with the first one being 'Open SSH port' (High severity) and the others being 'Firewall rule logging disabled' (Medium severity). Red annotations with numbers 1, 2, and 3 highlight the 'Google compute firewall' checkbox, the 'Open SSH port' finding, and the search bar respectively.

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

Filter findings on IP range

You can now use the new `inIpRange` function to filter findings based on whether they contain or do not contain an IPv4 or IPv6 IP address within a specified CIDR range. For example: `contains(connections, inIpRange(source_ip, "192.0.2.0/24"))`. [Learn more](#)

Query preview  
`state="ACTIVE" AND NOT mute="MUTED" AND resource.type="google.compute.Firewall"`

Quick filters [Clear all](#) [K](#)

Category	Severity	Attack exposure score	Event time	Create time	Finding class
<input type="checkbox"/> Open SSH port	High	—	Sep 3, 2025, 8:33:16 PM	Sep 3, 2025, 8:33:17 PM	Misconfiguration
<input type="checkbox"/> Firewall rule logging disabled	Medium	—	Sep 3, 2025, 8:33:16 PM	Sep 3, 2025, 8:33:17 PM	Misconfiguration
<input type="checkbox"/> Firewall rule logging disabled	Medium	—	Sep 3, 2025, 8:33:16 PM	Sep 3, 2025, 8:33:16 PM	Misconfiguration

# **Task 2. Fix the Compute Engine Vulnerabilities**

LOUIS.O

The image shows a Google Cloud console interface with a navigation menu on the left and a main content area on the right. A red arrow labeled '1' points to the 'Compute Engine' menu item. A second red arrow labeled '2' points to the 'VM instances' sub-item in the dropdown menu that appears after clicking 'Compute Engine'. The 'VM instances' item is highlighted with a red box. Below the navigation menu, there is a blue button that says 'Click to view all products and pin them to the navigation'. The background content area shows a search bar at the top, a 'Feedback' and 'Settings' link, and a section titled 'accurate attack exposure scores'. Below this, there is a 'Findings query results' table with columns for 'Clear all', 'Export', 'Mute options', 'Columns', 'Set security marks', and 'Change ac'. The table contains three rows of findings, each with a checkbox, a description, a severity level, and two timestamps.

Clear all	Export	Mute options	Columns	Set security marks	Change ac
12	<input type="checkbox"/>	<a href="#">Firewall rule logging disabled</a>	medium	Aug 17, 2025, 11:12:22 AM	Aug 17, 2025, 11:12:23 AM
6	<input type="checkbox"/>	<a href="#">Firewall rule logging disabled</a>	Medium	Aug 17, 2025, 11:12:22 AM	Aug 17, 2025, 11:12:23 AM
4	<input type="checkbox"/>	<a href="#">Open SSH port</a>	High	Aug 17, 2025, 11:12:22 AM	Aug 17, 2025, 11:12:23 AM

Compute Engine VM instances [Create instance](#) [Import VM](#) [Refresh](#) [Learn](#)

- Overview
- Security risk overview
- Virtual machines
  - VM instances**
  - Instance templates
  - Sole-tenant nodes
  - Machine images
  - TPUs
  - Committed use discou...
  - Reservations
  - Migrate to Virtual Mach...
- Storage
  - Disks
  - Marketplace
  - Release Notes

Instances Observability Instance schedules

1  1 [Start / Resume](#) **Stop** [Suspend](#) [Reset](#) [Create a group based on this vm](#) [More actions](#)

Filter Enter property name or value

<input type="checkbox"/>	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External	Connect
<input type="checkbox"/>	✓	<a href="#">cc-app-01</a>	europa-west1-c			10.132.0.2 <a href="#">(nic0)</a>	34.79.16 <a href="#">(nic0)</a>	SSH

Related actions [Hide](#)

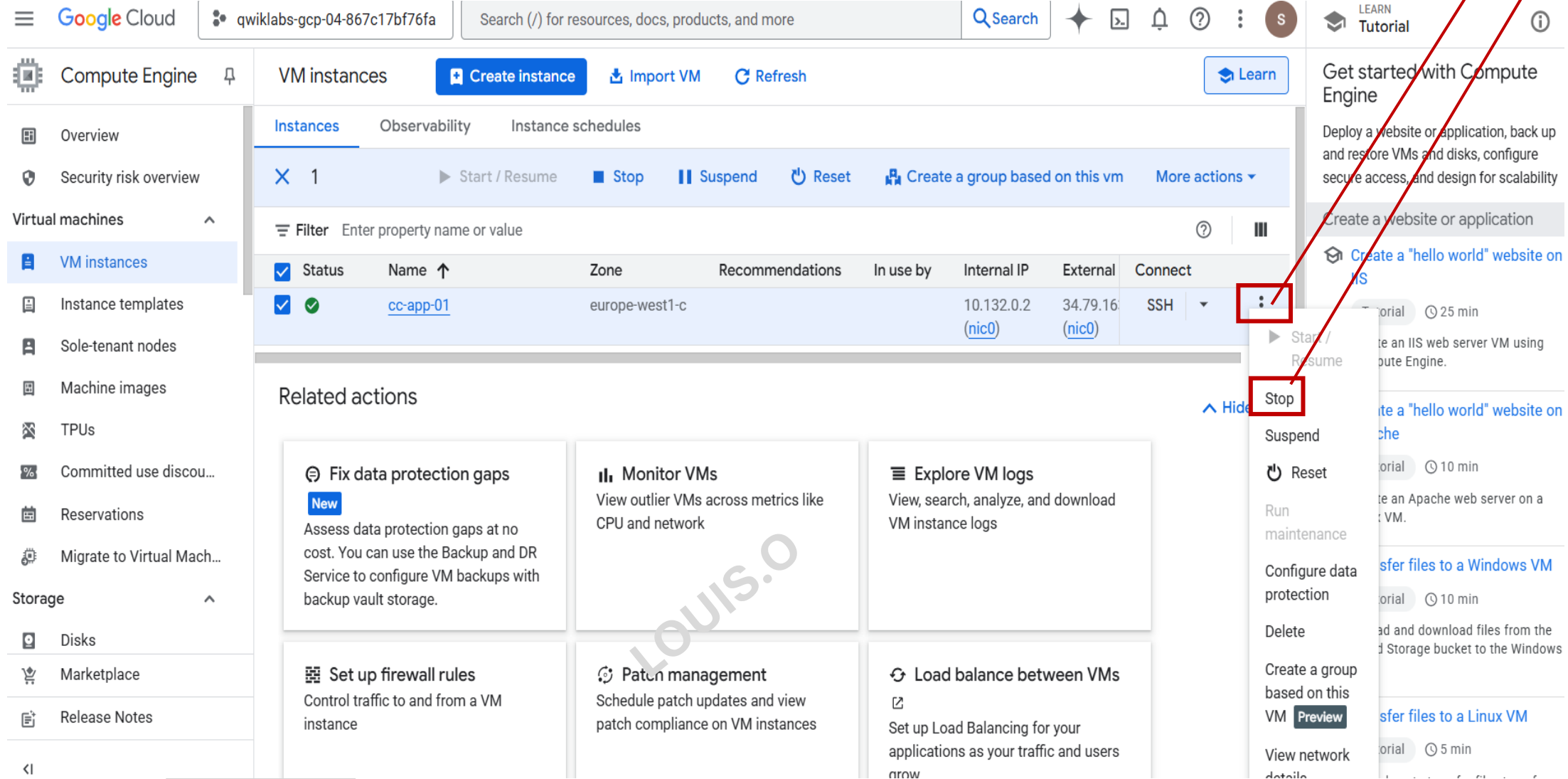
- Fix data protection gaps** New  
Assess data protection gaps at no cost. You can use the Backup and DR Service to configure VM backups with backup vault storage.
- Monitor VMs**  
View outlier VMs across metrics like CPU and network
- Explore VM logs**  
View, search, analyze, and download VM instance 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

2

1

LOUNGO

# Alternatively, you can click on the three dot to also stop the VM Instance



The screenshot shows the Google Cloud Platform interface for VM instances. A context menu is open for the instance 'cc-app-01', with the 'Stop' option highlighted. A large blue arrow on the left points down, and a red arrow on the right points from the 'Stop' option to the top right corner of the image.

Google Cloud | qwiklabs-gcp-04-867c17bf76fa | Search (/) for resources, docs, products, and more

Compute Engine | VM instances | Create instance | Import VM | Refresh | Learn

Instances | Observability | Instance schedules

1 | Start / Resume | Stop | Suspend | Reset | Create a group based on this vm | More actions

Filter | Enter property name or value

Status	Name	Zone	Recommendations	In use by	Internal IP	External	Connect
✓	cc-app-01	europe-west1-c			10.132.0.2 (nic0)	34.79.16 (nic0)	SSH

Related actions

- Fix data protection gaps (New) | Monitor VMs | Explore VM logs
- Set up firewall rules | Patch management | Load balance between VMs

Context menu options: Start / Resume, Stop, Suspend, Reset, Run maintenance, Configure data protection, Delete, Create a group based on this VM (Preview), View network details

- Overview
- Security risk overview
- Virtual machines
  - VM instances
  - Instance templates
  - Sole-tenant nodes
  - Machine images
  - TPUs
  - Committed use discou...
  - Reservations
  - Migrate to Virtual Mach...
- Storage
  - Disks
  - Marketplace
  - Release Notes

1 | Start / Resume | Stop | Suspend | Reset | Create a group based on this vm | More actions

Filter	Enter	Internal IP	External	Connect
<input checked="" type="checkbox"/> Status		10.132.0.2 <a href="#">(nic0)</a>	34.79.16 <a href="#">(nic0)</a>	SSH

### Stop cc-app-01?

You'll be billed only for these preserved resources:

- Persistent disks
- Static IP addresses

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

Skip graceful shutdown (if applicable) **Beta**

Cancel | **Stop**

### Related actions

- Fix data** New  
Assess data... cost. You c...  
Service to... backup vault storage.
- 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

# Create a New VM Instance From a Snapshot

Google Cloud | qwiklabs-gcp-04-867c17bf76fa | Search (/) for resources, docs, products, and more

Compute Engine | VM instances | **Create instance** | Import VM | Refresh

Instances | Observability | Instance schedules

1 | Start / Resume | Stop | Suspend | Reset | Create a group based on this vm | More actions

Filter | Enter property name or value

Status	Name	Zone	Recommendations	In use by	Internal IP	Connect
<input checked="" type="checkbox"/>	<a href="#">cc-app-01</a>	europe-west1-c			10.132.0.2 <a href="#">(nic0)</a>	SSH

Related actions

- Fix data protection gaps** (New)  
Assess data protection gaps at no cost. You can use the Backup and DR Service to configure VM backups with backup vault storage.
- 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
- Patch management**  
Schedule patch updates and view
- Load balance between VMs**

# In the **Name** field, type **cc-app-02** & scroll down to **Machine type section**

- Machine configuration  
e2-medium, europe-west1
- OS and storage  
Debian GNU/Linux 12 (bookworm)
- Data protection  
Snapshot schedules
- Networking  
1 network interface
- Observability  
Install Ops Agent
- Security
- Advanced

## Machine configuration


Name \*

Region \*

Zone \*

Region is permanent

Google will choose a zone on your behalf, maximizing VM obtainability. Zone is permanent.

 **New C4 machine types with Titanium SSD and Xeon 6 (Granite Rapids)** ×  
Generally Available

✓ Try new C4 machine types, including local SSD and bare metal variants, on the latest [Try now](#)

General purpose  Compute optimized  Memory optimized  Storage optimized  GPUs

Machine types for common workloads, optimized for cost and flexibility

Series ?	Description	vCPUs ?	Memory ?	CPU Platform
----------	-------------	---------	----------	--------------

# In the machine Type section select Shared-Core and select e2-medium, click OS and Storage

The screenshot shows the Google Cloud console interface for creating a VM instance. The left sidebar contains a navigation menu with the following items:

- Machine configuration (e2-medium, europe-west1)
- OS and storage (Debian GNU/Linux 12 (bookworm))
- Data protection (Snapshot schedules)
- Networking (1 network interface)
- Observability (Install Ops Agent)
- Security
- Advanced

The main content area displays a table of instance sizes. The 'E2' machine type is selected, and a dropdown menu is open showing the 'Shared-core' category with 'e2-medium' highlighted. Below the dropdown, the selected configuration is summarized:

Machine Type	Performance	vCPU	Memory	Processor
C3D	Consistently high performance	4 - 360	8 - 2,880 GB	AMD Genoa
<b>E2</b>	Low cost, day-to-day computing	0.25 - 32	1 - 128 GB	Intel Broadwe
N2	Balanced price & performance	2 - 128	2 - 864 GB	Intel Cascade

Filter: Instance sizes

- Shared-core
  - e2-medium** (1-2 vCPU (1 shared core), 4 GB memory)
  - e2-micro (0.25-2 vCPU (1 shared core), 1 GB memory)
  - e2-small (0.5-2 vCPU (1 shared core), 2 GB memory)
- Standard
- High memory
- High CPU

Summary: 1-2 vCPU (1 shared core), 4 GB memory

Buttons: Create, Cancel, Equivalent code

- Machine configuration  
e2-medium, europe-west1

- OS and storage**  
Debian GNU/Linux 12  
(bookworm)

- Data protection  
Snapshot schedules

- Networking  
1 network interface

- Observability  
Install Ops Agent

- Security

- Advanced

## Operating system and storage

Name	cc-app-02
Type	New balanced persistent disk
Size	10 GB
Snapshot schedule ?	default-schedule-1
License type ?	Free
Image	Debian GNU/Linux 12 (bookworm)

[Change](#)

## Additional disks

[+ Add new disk](#) [+ Attach existing disk](#) [+ Add local SSD](#)

## Container Deprecated ?

Deploy a container image to this VM instance

[Deploy container](#)

Create

Cancel

↔ Equivalent code

Click The Drop-Down, Select “cc-app01-snapshot” & “Select”, then scroll-down to **Identity and API Access**, the next slide.

### Boot disk

Select an image or snapshot to create a boot disk; or attach an existing disk. Can't find what you're looking for? Explore hundreds of VM solutions in [Marketplace](#)

[Public images](#) [Custom images](#) **Snapshots** [Archive Snapshots](#) [Existing Disks](#)

Operating system  
Debian

Version \*  
Debian GNU/Linux 12 (bookworm)

x86/64, amd64 built on 20250812

Boot disk type \*  
Balanced persistent disk

[Compare disk types](#)

Size (GB) \*  
10

Provision between 10 and 65536 GB

[Show advanced configuration](#)

**Select** Cancel

### Boot disk

Select an image or snapshot to create a boot disk; or attach an existing disk. Can't find what you're looking for? Explore hundreds of VM solutions in [Marketplace](#)

[Public images](#) [Custom images](#) **Snapshots** [Archive Snapshots](#) [Existing Disks](#)

Snapshot  
Filter |Type to filter

**cc-app01-snapshot**  
Created on Aug 20, 2025, 8:15:40 PM, cc-app-01

[Compare disk types](#)

Size (GB) \*  
10

Provision between 10 and 65536 GB

[Show advanced configuration](#)

**Select** Cancel

4

3

1

2

After step 1&2, Scroll-down and select the drop-down at the front of **Advance Options & Networking Section**

The screenshot shows the Google Cloud console interface for creating a VM instance. The page is titled "Create an instance" and includes a search bar at the top. The left sidebar contains a navigation menu with categories: Machine configuration, OS and storage, Data protection, Networking, Observability, Security, and Advanced. The "Security" section is currently selected and expanded, showing sub-sections: Identity and API access, Service accounts, Confidential VM service, and Shielded VM. The "Service accounts" section is open, displaying a list of service accounts. A red box highlights the "Qwiklabs User Service Account" entry. A red box also highlights a small dropdown arrow in the top right corner of the service account list. Four red arrows, numbered 1 through 4, point to specific elements: Arrow 1 points to the "Qwiklabs User Service Account" entry; Arrow 2 points to the dropdown arrow in the top right of the list; Arrow 3 points to the vertical scrollbar on the right side of the list; Arrow 4 points to the "Networking" section in the left sidebar. The "Networking" section in the sidebar is also highlighted with a red box. At the bottom of the page, there are buttons for "Create", "Cancel", and "Equivalent code".

Google Cloud

qwiklabs-gcp-04-867c17bf76fa

Search (/) for resources, docs, products, and more

Create an instance

Create VM from...

- Machine configuration  
e2-medium, europe-west1
- OS and storage  
cc-app01-snapshot
- Data protection  
Snapshot schedules
- Networking**  
1 network interface
- Observability
- Security**
- Advanced

### Security

#### Identity and API access

#### Service accounts

Service account

Filter Filter service accounts

- No service account
- Compute Engine default service account**  
377021291057-compute@developer.gserviceaccount.com
- Qwiklabs User Service Account**  
qwiklabs-gcp-04-867c17bf76fa@qwiklabs-gcp-04-867c17bf76fa.iam.gserviceaccount.com

#### Confidential VM service

Confidential Computing is disabled on this VM instance

Enable

#### Shielded VM

Select a shielded image to use shielded VM features.

Create Cancel Equivalent code

After entry “cc” scroll-down to **Network interfaces** section, click the drop-down & select **default** network

In the **External IPV4 address** Section Click the **Drop-down** Select **None** & **Create**

The screenshot shows the 'Create an instance' page in the Google Cloud console, specifically the 'Networking' section. The left sidebar lists various configuration categories: Machine configuration, OS and storage, Data protection, Networking (selected), Observability, Security, and Advanced. The main content area is titled 'Networking' and includes sections for Firewall, Network tags, Hostname, and IP forwarding. The 'Network tags' section shows a text input field containing 'cc'. Below this, the 'Edit network interface' section is visible, with a dropdown menu for 'Network' set to 'default' and a 'Subnetwork' dropdown set to 'default IPv4 (10.132.0.0/20)'. Red annotations include a box around the 'Network tags' field with an arrow pointing to '1', a box around the 'Network' dropdown with an arrow pointing to '2', and a box around the 'Subnetwork' dropdown with an arrow pointing to '3'. At the bottom, there are 'Create', 'Cancel', and 'Equivalent code' buttons.

The screenshot shows the 'Create an instance' page in the Google Cloud console, specifically the 'External IPV4 address' section. The left sidebar is similar to the previous screenshot, with 'Networking' selected. The main content area is titled 'External IPV4 address' and includes sections for IP stack type, Primary internal IPv4 address, Alias IP ranges, and External IPv4 address. The 'IP stack type' section has 'IPv4 (single-stack)' selected. The 'Primary internal IPv4 address' dropdown is set to 'Ephemeral (Automatic)'. The 'External IPv4 address' section has a dropdown menu open, showing options: 'None', 'Ephemeral', and 'Reserve static external IP address'. The 'None' option is highlighted. Red annotations include a box around the dropdown menu with an arrow pointing to '1', a box around the 'None' option with an arrow pointing to '2', and a box around the 'Reserve static external IP address' link with an arrow pointing to '3'. At the bottom, there are 'Create', 'Cancel', and 'Equivalent code' buttons.

Google Cloud | qwiklabs-gcp-00-6d8119cedc0a | Search (/) for resources, docs, products, and more

Create an instance | Create VM from...

- Machine configuration  
e2-medium, us-west1
- OS and storage  
cc-app01-snapshot
- Data protection  
Snapshot schedules
- Networking  
1 network interface
- Observability
- Security
- Advanced

### Security

#### Identity and API access

Service accounts

Service account

Compute Engine default service account

To access instances with this service account you need to add the Service Account User role: roles/iam.serviceAccountUser. [Learn more](#)

Access scopes

Allow default access

Allow full access to all Cloud APIs

Set access for each API

#### Confidential VM service

Confidential Computing is disabled on this VM instance

[Enable](#)

#### Shielded VM

Select a shielded image to use shielded VM features.

Turn on all settings for the most secure configuration.

[Create](#) [Cancel](#) [Equivalent code](#)

VM instance stopped

**1**

Google Cloud | qwiklabs-gcp-00-6d8119cedc0a | Search (/) for resources, docs, products, and more

Create an instance | Create VM from...

- Machine configuration  
e2-medium, us-west1
- OS and storage  
cc-app01-snapshot
- Data protection  
Snapshot schedules
- Networking  
1 network interface
- Observability
- Security
- Advanced

### Security

#### Identity and API access

Service accounts

Service account

Filter Filter service accounts

No service account

Qwiklabs User Service Account  
quiklabs-gcp-00-6d8119cedc0a@quiklabs-gcp-00-6d8119cedc0a.iam.gserviceaccount.com

Compute Engine default service account  
535457421436-compute@developer.gserviceaccount.com

#### Confidential VM service

Confidential Computing is disabled on this VM instance

[Enable](#)

#### Shielded VM

Select a shielded image to use shielded VM features.

Turn on all settings for the most secure configuration.

[Create](#) [Cancel](#) [Equivalent code](#)

VM instance stopped

**3**

**2**

# New Virtual Machine “cc-app02” has been Created from the “cc-app01” snapshot. Now stop the new VM

The screenshot shows the Google Cloud Platform interface for VM instances. The left sidebar contains navigation options like Overview, Security risk overview, and Virtual machines. The main content area shows a list of VM instances. The 'Stop' button is highlighted with a red box and an arrow labeled '2'. The checkbox for the instance 'cc-app-02' is highlighted with a red box and an arrow labeled '1'.

Status	Name	Zone	Recommendations	In use by	Internal IP	External	Connect
<input type="checkbox"/>	<a href="#">cc-app-01</a>	europa-west1-c			10.132.0.2 (nic0)		SSH
<input type="checkbox"/>	<a href="#">cc-app-02</a>	europa-west1-d			10.132.0.4 (nic0)		SSH

Related actions:

- Fix data protection gaps** (New): Assess data protection gaps at no cost. You can use the Backup and DR Service to configure VM backups with backup vault storage.
- 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.
- Patch management**: Schedule patch updates and view.
- Load balance between VMs**

Google Cloud qwiklabs-gcp-04-867c17bf76fa Search (/) for resources, docs, products, and more Search 3 ? S

Compute Engine VM instances Create instance Import VM Refresh Learn

Overview  
Security risk overview

Virtual machines ^

- VM instances
- Instance templates
- Sole-tenant nodes
- Machine images
- TPUs
- Committed use discou...
- Reservations
- Migrate to Virtual Mach...

Storage ^

- Disks
- Marketplace
- Release Notes

Instances Observability Instance schedules

1 Start / Resume Stop Suspend Reset Create a group based on this vm More actions

Filter Enter

Status

	Internal IP	External	Connect
<input type="checkbox"/>	10.132.0.2 <a href="#">(nic0)</a>		SSH <span>⌵</span> <span>⋮</span>
<input checked="" type="checkbox"/>	10.132.0.4 <a href="#">(nic0)</a>		SSH <span>⌵</span> <span>⋮</span>

Hide

Related actions

- Fix data protection gaps at no cost. You can use the Backup and DR Service to configure VM backups with backup vault storage. New
- 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

Explore VM logs  
Search, analyze, and download VM instance logs

Stop cc-app-02?

You'll be billed only for these preserved resources:

- Persistent disks
- Static IP addresses

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

Skip graceful shutdown (if applicable) Beta

Cancel Stop

Compute Engine

VM instances

Create instance

Import VM

Refresh

Learn

- Overview
- Security risk overview

Virtual machines

- VM instances
- Instance templates
- Sole-tenant nodes
- Machine images
- TPUs
- Committed use discou...
- Reservations
- Migrate to Virtual Mach...

Storage

- Disks
- Marketplace
- Release Notes

Instances Observability Instance schedules

1 Start / Resume Stop Suspend Reset Create a group based on this vm More actions

Filter Enter property name or value

Status	Name	Zone	Recommendations	In use by	Internal IP	External	Connect
<input type="checkbox"/>	<a href="#">cc-app-01</a>	europa-west1-c			10.132.0.2 <a href="#">(nic0)</a>		SSH
<input checked="" type="checkbox"/>	<a href="#">cc-app-02</a>	europa-west1-d			10.132.0.4 <a href="#">(nic0)</a>		SSH

Related actions

**Fix data protection gaps**  
**New**  
Assess data protection gaps at no cost. You can use the Backup and DR Service to configure VM backups with backup vault storage.

**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

- Start / Resume
- Stop
- Suspend
- Reset
- Run maintenance
- Configure data protection
- Delete
- Create a group based on this VM **Preview**
- View network details

- Overview
- Security risk overview

Virtual machines

- VM instances
- Instance templates
- Sole-tenant nodes
- Machine images
- TPUs
- Committed use discou...
- Reservations
- Migrate to Virtual Mach...

Storage

- Disks
- Marketplace
- Release Notes

Details Observability OS Info Screenshot

SSH Connect to serial console

Connecting to serial ports is disabled

Logs

- Logging
- Serial port 1 (console)

Show more

Basic information

Name	cc-app-02
Instance Id	1598572369470552387
Description	None
Type	Instance
Status	Stopped
Creation time	Aug 20, 2025, 11:09:50 PM UTC+01:00
Location	europa-west1-d

# Scroll down to **Security and Access** section, select **checkbox** and click **Save**

Google Cloud | qwiklabs-gcp-04-867c17bf76fa | Search (/) for resources, docs

Compute Engine | Edit cc-app-02 instance

### Basic information

Instance ID	1598572369470552387
Status	Stopped
Creation time	Aug 20, 2025, 11:09:50 PM UTC+01:00
Zone	europe-west1-d
Reservation	Automatically choose
Confidential VM service	Disabled

Rename

VM instance name \*  
cc-app-02

Tip: Reference the VM by its URI in API calls and gcloud CLI commands to make sure your project isn't affected by any name changes. [Learn more](#)

Remote access

Enable connecting to serial ports

Labels

[Manage labels](#)

[Save](#) [Cancel](#)

Google Cloud | qwiklabs-gcp-04-867c17bf76fa | Search (/) for resources, docs

Compute Engine | Edit cc-app-02 instance

### 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. [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

[Save](#) [Cancel](#)

- Overview
- Security risk overview
- Virtual machines
  - VM instances
  - Instance templates
  - Sole-tenant nodes
  - Machine images
  - TPUs
  - Committed use discou...
  - Reservations
  - Migrate to Virtual Mach...
- Storage
  - Disks
  - Marketplace
  - Release Notes

### 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 ?

Save Cancel

Click on the arrow until you get to VM Instance Interface to see the newly created VM

In the **Compute Engine** menu, select **VM Instance**, Select the checkbox for the **cc-app-02**, and click **Start/ Resume**

The screenshot shows the Google Cloud Compute Engine interface. The left sidebar contains the 'Compute Engine' menu with 'VM instances' selected. The main content area displays a table of VM instances. The 'Start / Resume' button for the selected instance 'cc-app-02' is highlighted with a red box and labeled '2'. The checkbox for 'cc-app-02' is highlighted with a red box and labeled '1'. A red arrow points from '1' to '2'.

Status	Name	Zone	Recommendations	In use by	Internal IP	External	Connect
<input type="checkbox"/>	<a href="#">cc-app-01</a>	eu-west1-c			10.132.0.2 <a href="#">(nic0)</a>		SSH
<input type="checkbox"/>	<a href="#">cc-app-02</a>	eu-west1-d			10.132.0.4 <a href="#">(nic0)</a>		SSH

Related actions

- Fix data protection gaps**  
Assess data protection gaps at no cost. You can use the Backup and DR Service to configure VM backups with backup vault storage.
- Monitor VMs**  
View outlier VMs across metrics like CPU and network.
- Explore VM logs**  
View, search, analyze, and download VM instance logs.

Google Cloud | qwiklabs-gcp-04-867c17bf76fa | Search (/) for resources, docs, products, and more

### Compute Engine

VM instances [Create instance](#) [Import VM](#) [Refresh](#)

Instances | Observability | Instance schedules

1 [Start / Resume](#) [Stop](#) [Suspend](#) [Reset](#) [Create a group based on this vm](#) [More actions](#)

Filter Enter property name or value

Status	Name	Zone	Recommendations	In use by	Internal IP	External	Connect
<input type="checkbox"/>	cc-app-01				10.132.0.2 <a href="#">(nic0)</a>		SSH
<input checked="" type="checkbox"/>	cc-app-02				10.132.0.4 <a href="#">(nic0)</a>		SSH

Related actions

- Fix data protection gaps**  
Assess data protection gaps at no cost. You can use the Backup and DR Service to configure VM backups with backup vault storage.
- Monitor VMs**  
View outlier VMs across metrics like CPU and network.
- Explore VM logs**  
View, search, analyze, and download VM instance logs.

**Start cc-app-02?**

You'll be charged for running this VM according to its configuration.

[Cancel](#) [Start](#)

# Click on the three dots and select delete, to delete the Compromised VM “cc-app-01”

The screenshot shows the Google Cloud Platform interface for VM instances. The left sidebar contains navigation options like Overview, Security risk overview, and VM instances. The main content area displays a table of VM instances. The instance 'cc-app-01' is highlighted, and its 'More actions' menu is open, showing options like Start / Resume, Stop, Suspend, Reset, and Delete. Red boxes and arrows highlight the three-dot menu icon (labeled '1') and the 'Delete' option (labeled '2').

Google Cloud | qwiklabs-gcp-04-867c17bf76fa | Search (/) for resources, docs, products, and more | Search

Compute Engine | VM instances | Create instance | Import VM | Refresh

Instances | Observability | Instance schedules

1 | Start / Resume | Stop | Suspend | Reset | Create a group based on this vm | More actions

Filter | Enter property name or value

Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External	Connect
<input checked="" type="checkbox"/>	<a href="#">cc-app-01</a>	europa-west1-c			10.132.0.2 ( <a href="#">nic0</a> )		SSH
<input type="checkbox"/>	<a href="#">cc-app-02</a>	europa-west1-d			10.132.0.4 ( <a href="#">nic0</a> )		SSH

Related actions

- Fix data protection gaps (New) | Monitor VMs | Explore VM logs

2 | Delete | Create a group based on this VM | Preview

- Compute Engine
- Overview
- Security risk overview
- Virtual machines
- VM instances
- Instance templates
- Sole-tenant nodes
- Machine images
- TPUs
- Committed use discou...
- Reservations
- Migrate to Virtual Mach...
- Storage
- Disks
- Marketplace

VM instances **Create instance** Import VM Refresh

Instances Observability Instance schedules

1 Start / Resume Stop Suspend Reset Create a group based on this vm More actions

Filter Enter

Status	Internal IP	External	Connect
<input checked="" type="checkbox"/>	10.132.0.2 ( <a href="#">nic0</a> )		SSH
<input type="checkbox"/>	10.132.0.4 ( <a href="#">nic0</a> )		SSH

### Delete cc-app-01?

Are you sure you want to delete instance **cc-app-01**?

This will delete boot disk **cc-app-01**

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

Skip graceful shutdown (if applicable) **Beta**

Cancel **Delete**

Related actions

- Fix data**  
Assess data protection gaps at no cost. You can use the Backup and DR Service to configure VM backups with backup vault storage.
- CPU and network
- Explore VM logs  
Search, analyze, and download VM instance logs

LOUIS.O



Compute Engine

VM instances

Create instance

Import VM

Refresh



Overview



Security risk overview

Virtual machines



VM instances



Instance templates



Sole-tenant nodes



Machine images



TPUs



Committed use discou...



Reservations



Migrate to Virtual Mach...

Storage



Disks



Storage Pools



Marketplace



Release Notes



Instances

Observability

Instance schedules

VM instances

Filter Enter property name or value

<input type="checkbox"/>	Status	Name <span>↑</span>	Zone	Recommendations	In use by	Internal IP	External IP	Connect
<input checked="" type="checkbox"/>	<span>✓</span>	<a href="#">cc-app-02</a>	us-west1-b			10.138.0.4 ( <a href="#">nic0</a> )		SSH <span>▾</span> <span>⋮</span>

Related actions



Fix data protection gaps

New

Assess data protection gaps at no cost. You can use the Backup and DR Service to configure VM backups with backup vault storage.



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

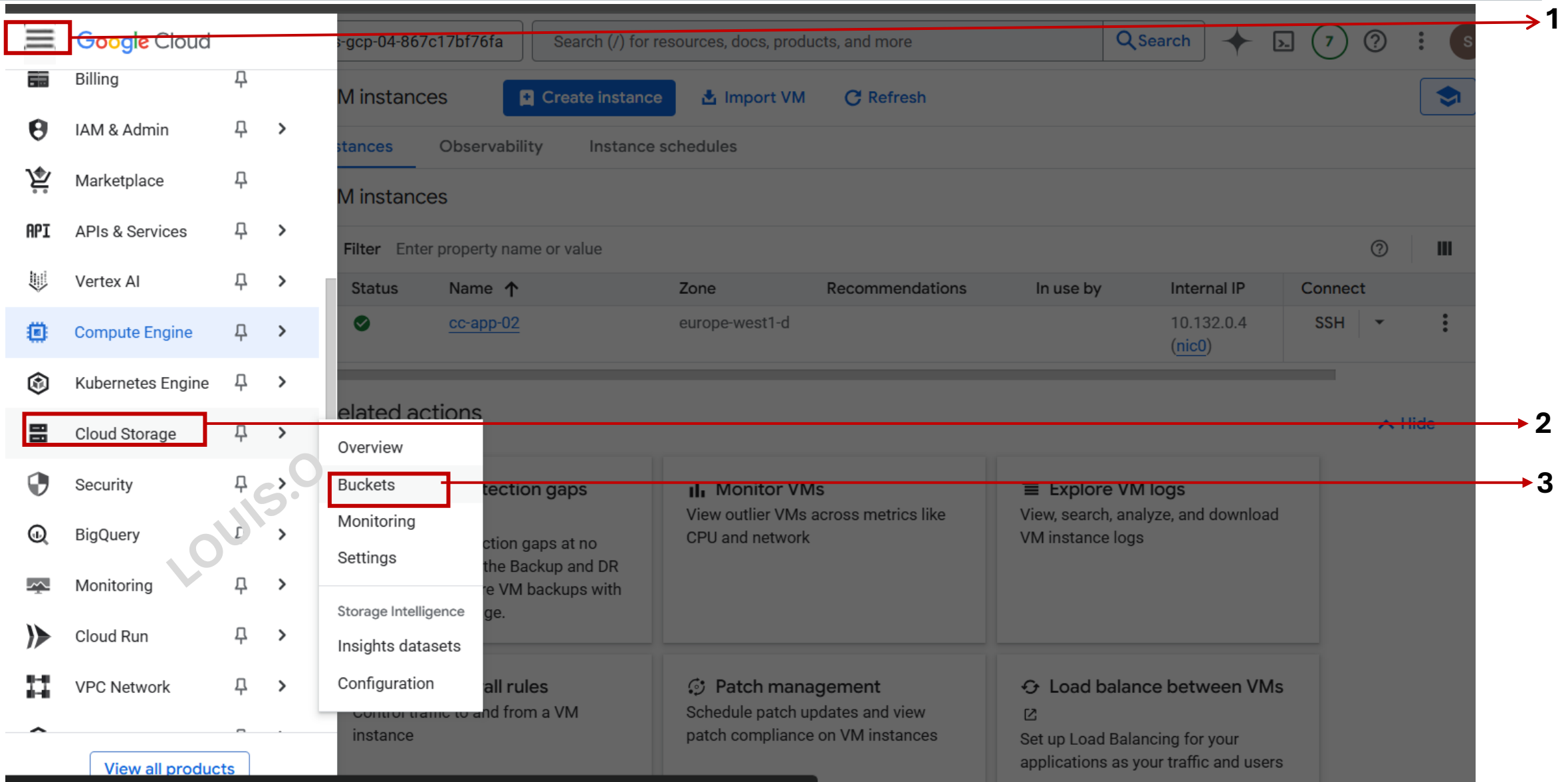
Instance deleted



# Task 3. Fix Cloud Storage Bucket Permissions

Louis

In the **Navigation menu** () , select **Cloud Storage > Buckets**. The Buckets page opens. Click the **qwiklabs-gcp-02-71bb6bc399\_bucket** storage bucket link. The Bucket details page opens



The screenshot shows the Google Cloud navigation menu with the following items:

- Billing
- IAM & Admin
- Marketplace
- APIs & Services
- Vertex AI
- Compute Engine
- Kubernetes Engine
- Cloud Storage
- Security
- BigQuery
- Monitoring
- Cloud Run
- VPC Network

The **Cloud Storage** menu item is highlighted with a red box. A red arrow labeled **1** points to the hamburger menu icon. A red arrow labeled **2** points to the **Cloud Storage** menu item. A red arrow labeled **3** points to the **Buckets** sub-menu item.

The background shows a table of VM instances:

Status	Name ↑	Zone	Recommendations	In use by	Internal IP	Connect
✓	<a href="#">cc-app-02</a>	europe-west1-d			10.132.0.4 ( <a href="#">nic0</a> )	SSH

Cloud Storage

Buckets [+ Create](#) [Refresh](#)

[Go to path](#)

- Overview
- Buckets**
- Monitoring
- Settings
- Storage Intelligence
  - Insights datasets
  - Configuration

Filter Filter buckets

<input type="checkbox"/>	Name ↑	Created	Location type	Location	Default storage class
<input type="checkbox"/>	<a href="#">qwiklabs-gcp-04-867c17bf76fa_bucket</a>	Aug 20, 2025, 8:17:11 PM	Region	europe-west1	Standard

LOUIS.O

Cloud Storage

Bucket details

Overview

Buckets

Monitoring

Settings

Storage Intelligence

Insights datasets

Configuration

qwiklabs-gcp-00-6d8119cedc0a\_bucket

**Public to internet:** This bucket is publicly accessible because allUsers or allAuthenticatedUsers have one or more permissions. Remove these principals

Location	Storage class	Public access	Protection
us-west1 (Oregon)	Standard	<b>Public to internet</b>	Soft Delete

- Objects
- Configuration
- Permissions**
- Protection
- Lifecycle
- Observability **New**
- Inventory Reports
- Operations

1

Public access

**Public to internet**

One or more bucket-level permissions grant access to everyone on the internet (**allUsers**) or anyone signed into a Google account (**allAuthenticatedUsers**). If this bucket should not be publicly accessible, remove these public permissions or prevent public access to this bucket. [Learn more](#)

2

[Prevent public access](#)

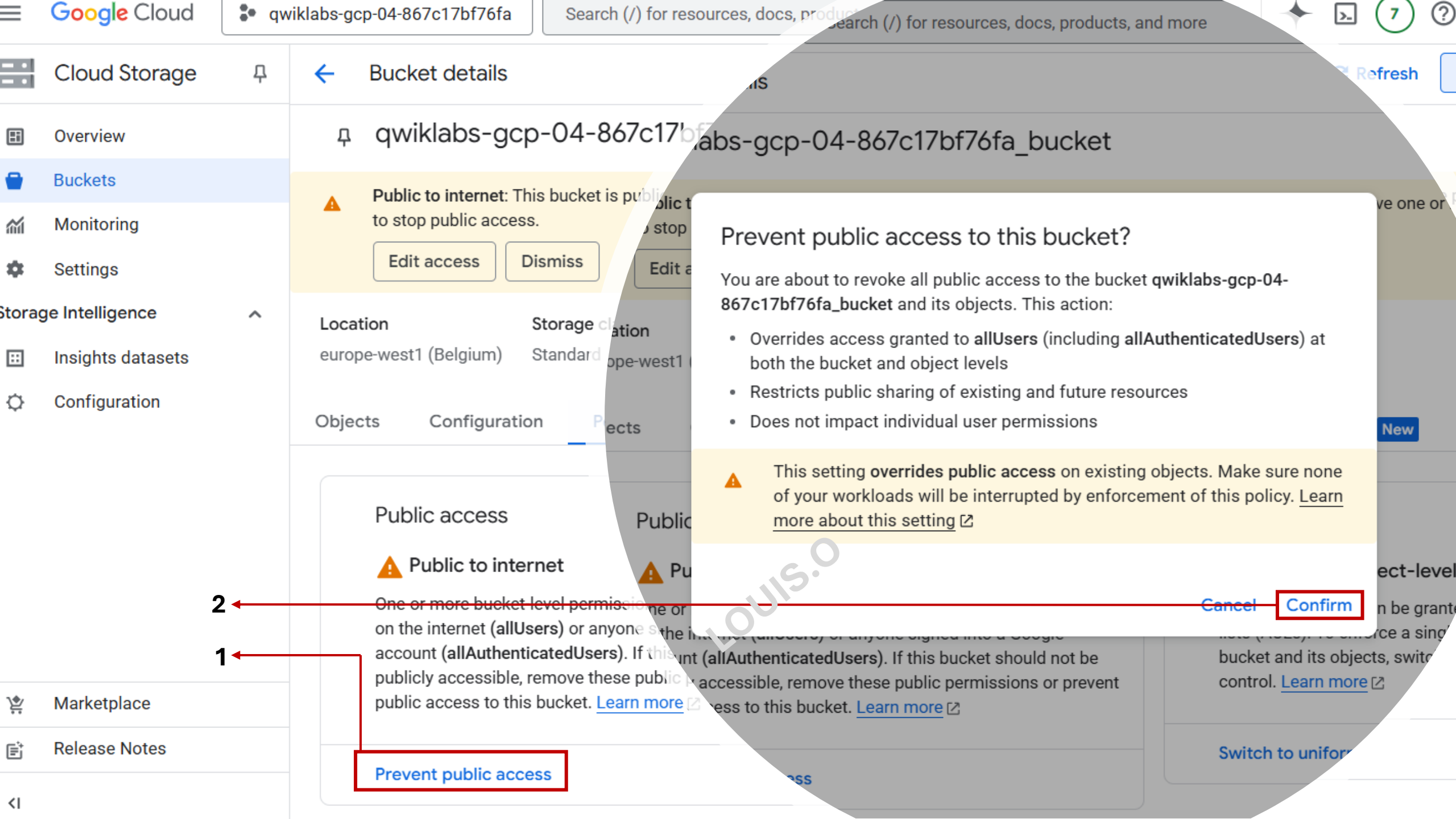
Access control

**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](#)

Marketplace



qwiklabs-gcp-04-867c17bf76fa\_bucket

**Public to internet:** This bucket is publicly accessible. To stop public access, click the Prevent public access button.

Edit access

Dismiss

Location: europe-west1 (Belgium)  
Storage class: Standard

Objects Configuration **Public access**

### Public access

#### **Public to internet**

One or more bucket level permissions on the internet (**allUsers**) or anyone signed into a Google account (**allAuthenticatedUsers**). If this bucket should not be publicly accessible, remove these public permissions or prevent public access to this bucket. [Learn more](#)

**Prevent public access**

### Prevent public access to this bucket?

You are about to revoke all public access to the bucket **qwiklabs-gcp-04-867c17bf76fa\_bucket** and its objects. This action:

- Overrides access granted to **allUsers** (including **allAuthenticatedUsers**) at both the bucket and object levels
- Restricts public sharing of existing and future resources
- Does not impact individual user permissions

**Warning:** This setting overrides public access on existing objects. Make sure none of your workloads will be interrupted by enforcement of this policy. [Learn more about this setting](#)

Cancel

**Confirm**

2

1

# Modify Storage bucket access by switching the access control to **UNIFORM** and remove Permissions for **All Users**

Cloud Storage Bucket details for `qwiklabs-gcp-04-867c17bf76fa_bucket`

Location: europe-west1 (Belgium) | Storage class: Standard | Public access: Not public | Protection: Soft Delete

Permissions tab selected. Sub-tabs: Objects, Configuration, **Permissions**, Protection, Lifecycle, Observability (New), Inventory Reports, Operations.

**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 section: [View by principals](#) | View | [Grant access](#)

Notification: Public access is prevented for this bucket

## Edit access control

Choose how to control object access in this bucket.

- Uniform**  
Ensure uniform access to all objects in the bucket by using only bucket-level permissions (IAM). This option becomes permanent after 90 days. [Learn more](#)
- Fine-grained**  
Specify access to individual objects by using object-level permissions (ACLs) in addition to your bucket-level permissions (IAM). [Learn more](#)

Cancel Save

1 2

Google Cloud | qwiklabs-gcp-04-867c17bf76fa | Search (/) for resources, docs, products, and more

Cloud Storage | Bucket details | Go to path | Refresh | Learn

### Edit access control

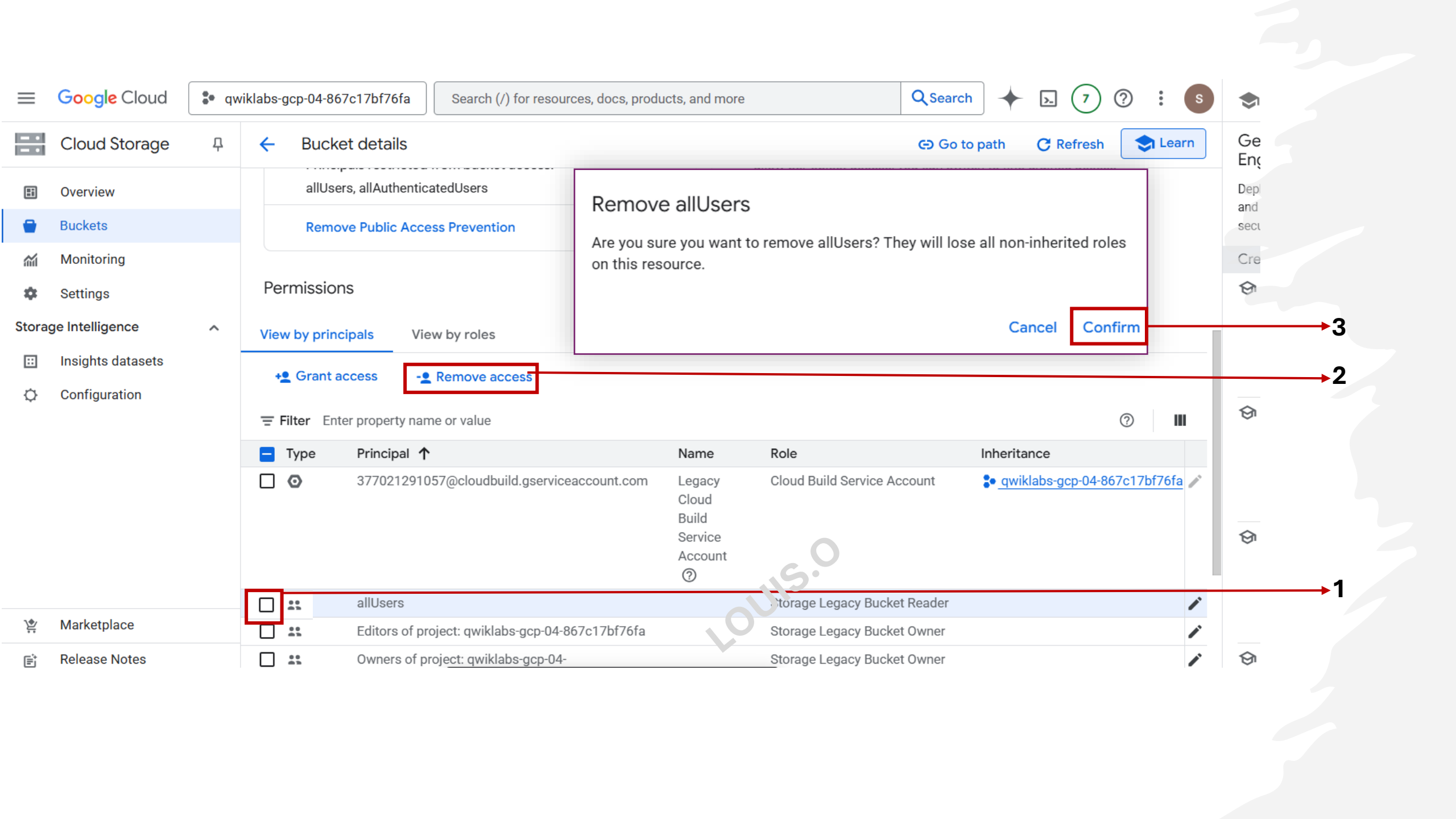
Choose how to control object access in this bucket.

- Uniform**  
Ensure uniform access to all objects in the bucket by using only bucket-level permissions (IAM). This option becomes permanent after 90 days. [Learn more](#)
- Fine-grained**  
Specify access to individual objects by using object-level permissions (ACLs) in addition to your bucket-level permissions (IAM). [Learn more](#)

**Warning:** Uniform access control removes object ACLs from this bucket. This will revoke object access for users who rely solely on ACLs for access unless you add their permissions to the bucket's IAM policy. [Learn more](#)

**Add project role ACLs to the bucket IAM policy**  
This ensures that users who rely on project owner, editor, and viewer roles to access the bucket's objects won't lose access.

1 → 2 →



- Overview
- Buckets**
- Monitoring
- Settings
- Storage Intelligence
  - Insights datasets
  - Configuration

allUsers, allAuthenticatedUsers  
[Remove Public Access Prevention](#)

### Remove allUsers

Are you sure you want to remove allUsers? They will lose all non-inherited roles on this resource.

Cancel **Confirm**

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"/>	377021291057@cloudbuild.gserviceaccount.com	Legacy Cloud Build Service Account	Cloud Build Service Account	qwiklabs-gcp-04-867c17bf76fa
<input type="checkbox"/>	allUsers		Storage Legacy Bucket Reader	
<input type="checkbox"/>	Editors of project: qwiklabs-gcp-04-867c17bf76fa		Storage Legacy Bucket Owner	
<input type="checkbox"/>	Owners of project: qwiklabs-gcp-04-		Storage Legacy Bucket Owner	

- Marketplace
- Release Notes

- Ge Eng
- Depl and sect
- Cre
- 
- 
- 
- 

3

2

1

# Task 4. Limit Firewall Ports Access

LOUIS.O

- Marketplace
- APIs & Services
- Vertex AI
- Compute Engine
- Kubernetes Engine
- Cloud Storage**
- Security
- BigQuery
- Monitoring
- Cloud Run
- VPC Network**
- SQL
- Google Maps Platf...

- VPC networks
- IP addresses
- Internal ranges
- Bring your own IP
- Firewall**
- Routes
- VPC network peering
- Shared VPC
- Serverless VPC access
- Packet mirroring
- VPC Flow Logs

### Bucket details

allUsers, allAuthenticatedUsers

within 90 days. [Learn more](#)

[Switch to fine-grained](#)

View by roles

Remove access

Name or value

	Name	Role
	057@cloudbuild.gserviceaccount.com	Legacy Cloud Build Service Account
		Account
Editors of project: qwiklabs-gcp-04-867c17bf76fa		Storage Legacy Bucket Owner
		Storage Legacy Object Owner
Owners of project: qwiklabs-gcp-04-867c17bf76fa		Storage Legacy Bucket Owner

- Cloud Armor
  - DDoS Dashboard
  - Cloud Armor policies
  - Adaptive Protection
  - Cloud Armor Service Tier
- Cloud IDS
  - IDS Dashboard
  - IDS Endpoints
  - IDS Threats
- Cloud NGFW
  - Dashboard
  - Firewall policies**
  - Threats
  - Firewall endpoints
- Secure Web Proxy

### Get started with real-time analytics

Use Network Intelligence Center for comprehensive monitoring and troubleshooting. [Learn more](#)

- ✓ Visualize your network resources
- ✓ Diagnose and prevent connectivity issues
- ✓ View packet loss and latency metrics
- ✓ Keep your firewall rules strict and efficient

[Try now](#) [Remind me later](#)

**⚠ You don't have required permissions:**

- `compute.organizations.listAssociations`

to view the firewall policies inherited by this project.

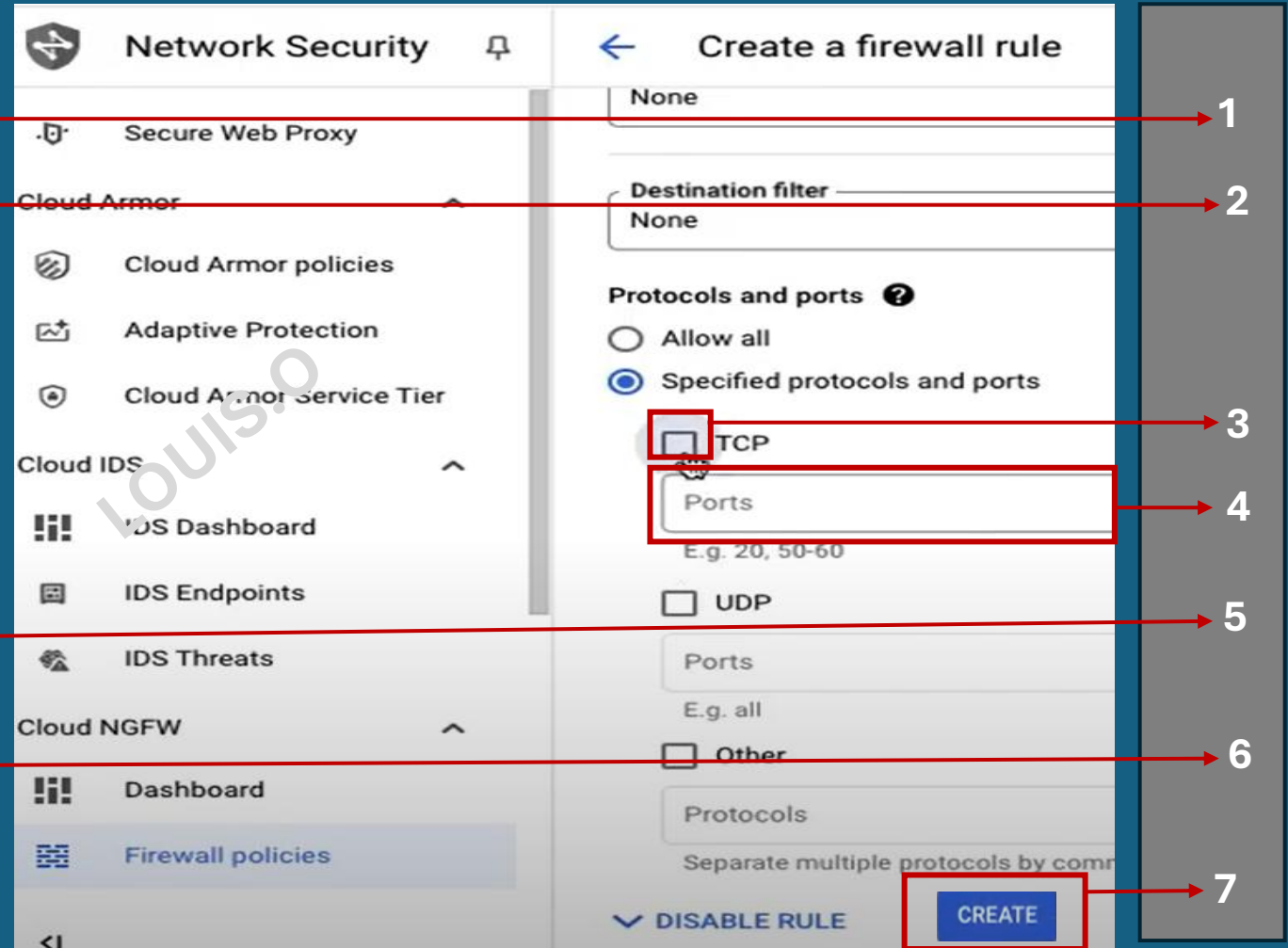
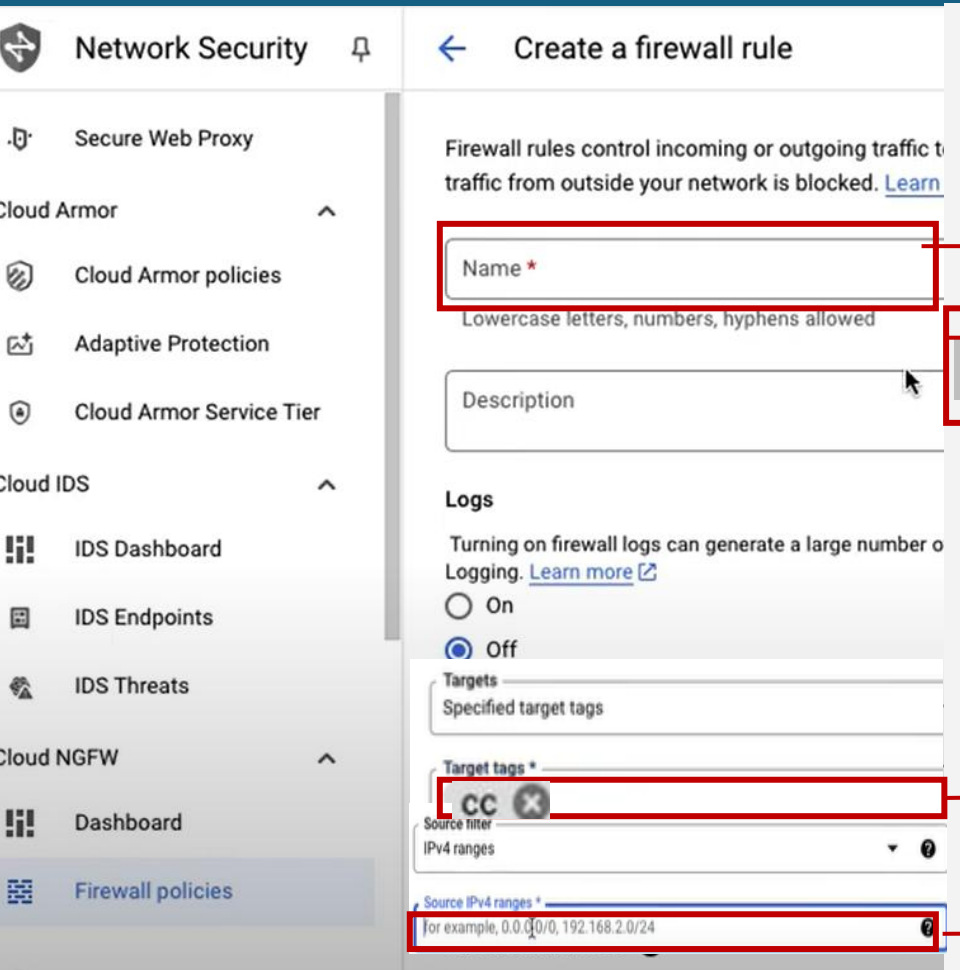
### VPC firewall rules

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

Note: App Engine firewalls are managed in the [App Engine Firewall rules section](#)



In the **NAME** field type-in “**limit-ports**”, **TARGET TAGS** type-in “**cc**”, Scroll down to **SOURCE FILTER** type-in **35.235.240.0/20**, checkbox TCP and type-in 22 in the field under TCP and Click **CREATE**



**NB:** In the Firewall Rule “**Restrict SSH access**” to only authorized IP from the source network **35.235.240.0/20** to compute instance with the target tag “**cc**”

# Task 5. Fix Firewall Configuration

LOUIS.O

**Challenge: Customize firewall rules & Enable Logging**

Delete the **default-allow-icmp**, **default-allow-rdp**, and **default-allow-ssh** firewall rules. These rules are overly broad and by deleting them, you'll allow for a more secure and controlled network environment.

By deleting these rules, you have restricted access to these protocols, limiting the potential for unauthorized access attempts and reducing the attack surface of your network.

The screenshot shows the Google Cloud Network Security console. The left sidebar contains navigation options for Network Security, Cloud Armor, Cloud IDS, and Cloud NGFW. The main content area is titled "Firewall policies" and includes buttons for "CREATE FIREWALL POLICY", "CREATE FIREWALL RULE", "REFRESH", "CONFIGURE LOGS", and "DELETE". A table lists several firewall rules. Red boxes and arrows highlight the "DELETE" button and the checkboxes for the rules "default-allow-icmp", "default-allow-rdp", and "default-allow-ssh". A success message at the bottom states "Successfully created firewall rule 'limit-ports'".

<input type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network	
<input type="checkbox"/>	<a href="#">limit-ports</a>	Ingress	cc	IP ranges:	tcp:22	Allow	1000	<a href="#">default</a>	▼
<input type="checkbox"/>	<a href="#">default-allow-icmp</a>	Ingress	Apply to all	IP ranges:	icmp	Allow	65534	<a href="#">default</a>	▼
<input type="checkbox"/>	<a href="#">default-allow-internal</a>	Ingress	Apply to all	IP ranges:	tcp:0-65535 udp:0-65535 icmp	Allow	65534	<a href="#">default</a>	▼
<input type="checkbox"/>	<a href="#">default-allow-rdp</a>	Ingress	Apply to all	IP ranges:	tcp:3389	Allow	65534	<a href="#">default</a>	▼
<input type="checkbox"/>	<a href="#">default-allow-ssh</a>	Ingress	Apply to all	IP ranges:	tcp:22	Allow	65534	<a href="#">default</a>	▼

**Network firewall policies**

Firewall policies let you group several firewall rules so that you can update them all at once, effectively controlled

Successfully created firewall rule "limit-ports".

Network Security

Firewall policies

+ Create firewall policy

+ Create firewall rule

Cloud Armor

DDoS Dashboard

Cloud Armor policies

Adaptive Protection

Cloud Armor Service Tier

Cloud IDS

IDS Dashboard

IDS Endpoints

IDS Threats

Cloud NGFW

Dashboard

Firewall policies

Threats

Firewall endpoints

Secure Web Proxy

SMTP port 25 disallowed in this project. [Learn more](#)

Refresh

Configure logs

Delete

Filter Enter property

<input type="checkbox"/>	Name	Type	Apply to	IP ranges	Protocols / ports	Action	Priority
<input type="checkbox"/>	<a href="#">limit-ports</a>	Ingress	Apply to all		tcp:22	Allow	100
<input checked="" type="checkbox"/>	<a href="#">default-allow-icmp</a>	Ingress	Apply to all		icmp	Allow	65535
<input type="checkbox"/>	<a href="#">default-allow-internal</a>	Ingress	Apply to all	IP ranges:	tcp:0-65535 udp:0-65535 icmp	Allow	65535
<input checked="" type="checkbox"/>	<a href="#">default-allow-rdp</a>	Ingress	Apply to all	IP ranges:	tcp:3389	Allow	65535
<input checked="" type="checkbox"/>	<a href="#">default-allow-ssh</a>	Ingress	Apply to all	IP ranges:	tcp:22	Allow	65535

Delete 3 firewall rules?

Are you sure you want to delete 3 firewall rules?

Cancel

Delete

Network firewall policies

Enable logging for the remaining firewall rules **limit-ports** (the rule created in a previous task) and **default-allow-internal**. Enabling logging allows you to track and analyze the traffic that is allowed by this rule, which is likely to be internal between instances within your VPC

The screenshot shows the AWS IAM console's Firewall policies page. The left sidebar contains navigation options for Network Security, Cloud Armor, Cloud IDS, and Cloud NGFW. The main content area displays a table of firewall rules. The 'limit-ports' rule is highlighted with a red box. Below the table, there is a section for 'Network firewall policies' with a description and a 'Refresh' button. At the bottom, a notification box indicates 'Firewall rules deleted'.

<input type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network	
<input type="checkbox"/>	limit-ports	Ingress	cc	IP ranges:	tcp:22	Allow	1000	default	▼
<input type="checkbox"/>	default-allow-internal	Ingress	Apply to all	IP ranges:	tcp:0-65535 udp:0-65535 icmp	Allow	65534	default	▼

**Network firewall policies**

Firewall policies let you group several firewall rules so that you can update them all at once, effectively controlled by Identity and Access Management (IAM) roles. [Learn more](#)

Policy name ↑

Policy name	Firewall rules	Description	Deployment scope	Associated with
No rows to display				

Firewall rules deleted

Network Security

Secure Web Proxy

Cloud Armor

- Cloud Armor policies
- Adaptive Protection
- Cloud Armor Service Tier

Cloud IDS

- IDS Dashboard
- IDS Endpoints
- IDS Threats

Cloud NGFW

- Dashboard
- Firewall policies

Firewall rule details

limit-ports

Logs

Off

[view in Logs Explorer](#)

Network default

Priority 1000

Direction Ingress

Action on match Allow

Targets

Target tags cc

EDIT

DELETE

Network Security

Secure Web Proxy

Cloud Armor

- Cloud Armor policies
- Adaptive Protection
- Cloud Armor Service Tier

Cloud IDS

- IDS Dashboard
- IDS Endpoints
- IDS Threats

Cloud NGFW

- Dashboard
- IDS Dashboard
- IDS Endpoints
- IDS Threats

Cloud NGFW

Firewall policies

limit-ports

Description

Logs

Turning on firewall logs can generate a large number of log entries. [Learn more](#)

On

Off

Network default

Priority \* 1000

Priority can be 0 - 65535

Direction Ingress

Ports

E.g. all

Other

Protocols

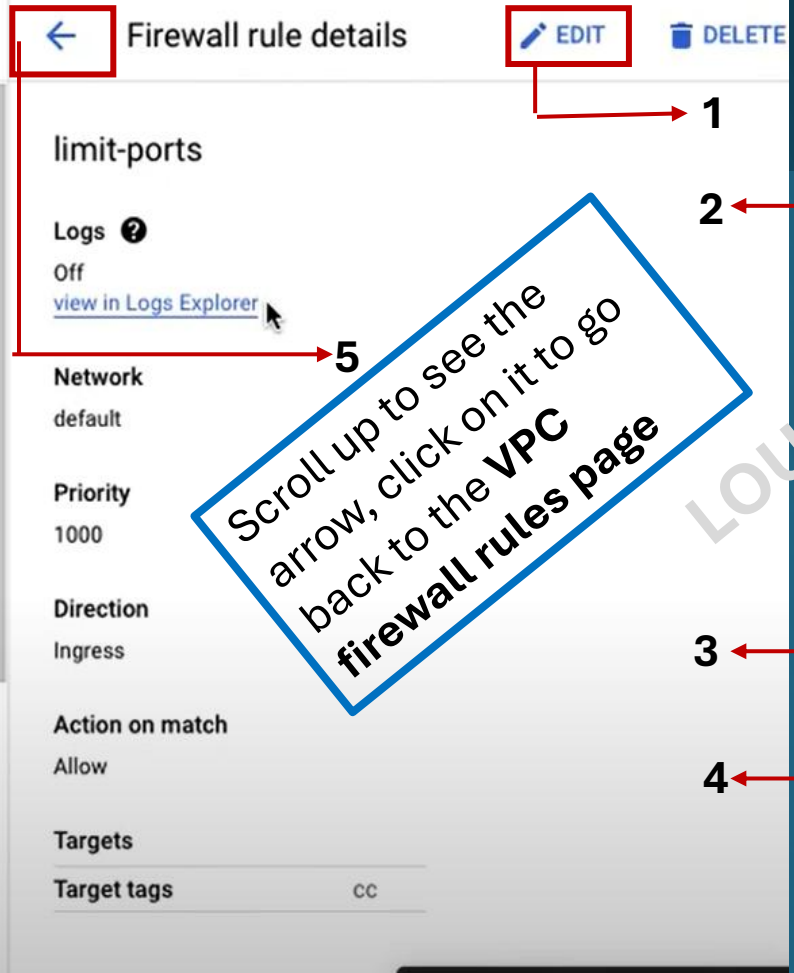
Separate multiple protocols

DISABLE RULE

SAVE

CANCEL

Scroll up to see the arrow, click on it to go back to the VPC firewall rules page



- Secure Web Proxy
- Cloud Armor
  - Cloud Armor policies
  - Adaptive Protection
  - Cloud Armor Service Tier
- Cloud IDS
  - IDS Dashboard
  - IDS Endpoints
  - IDS Threats
- Cloud NGFW
  - Dashboard
  - Firewall policies

### VPC firewall rules

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

Note: App Engine firewalls are managed in the [App Engine Firewall rules section](#).

**i** SMTP port 25 disallowed in this project. [Learn more](#)

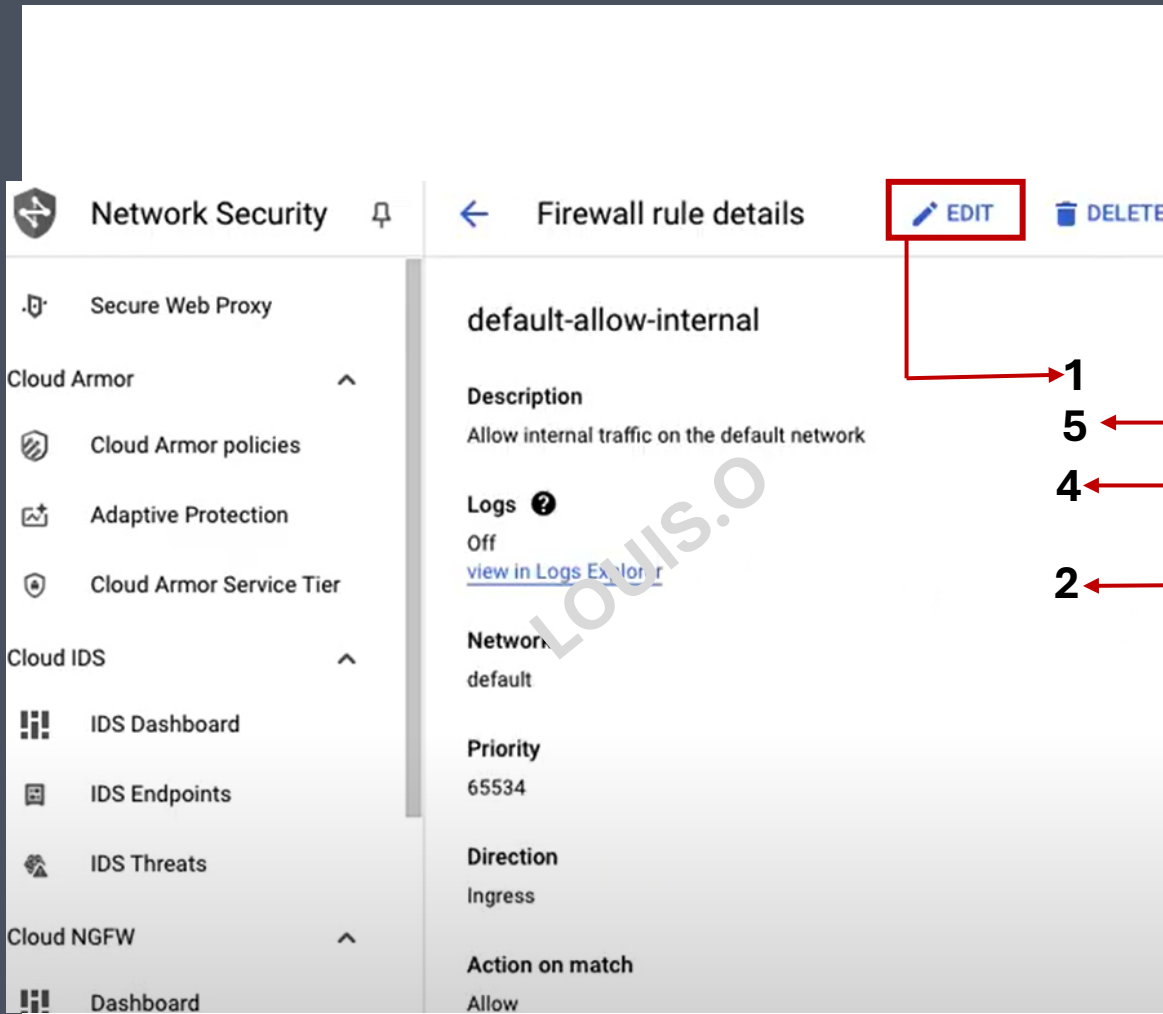
REFRESH CONFIGURE LOGS DELETE

Filter Enter property name or value

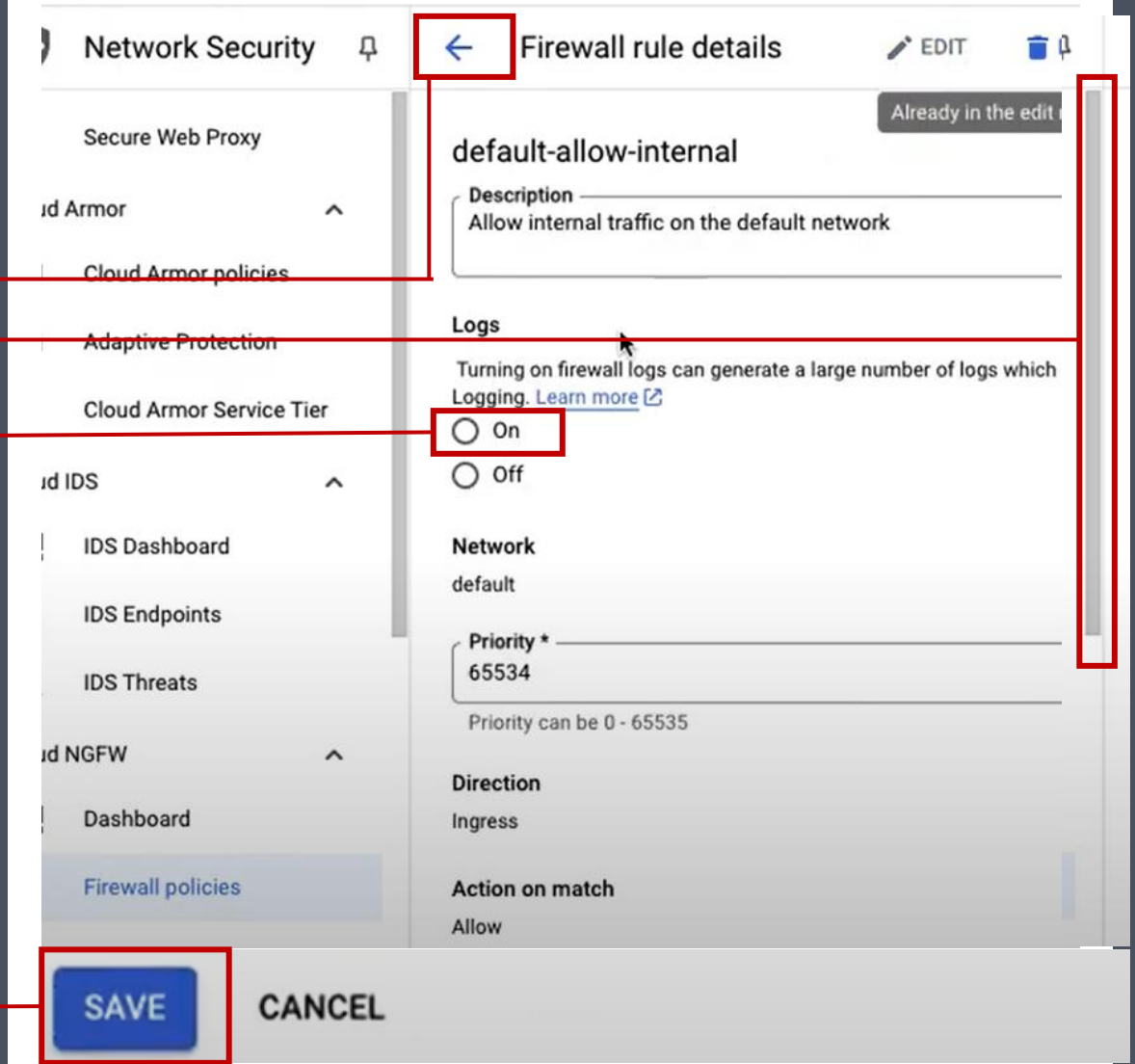
<input type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network	
<input type="checkbox"/>	<a href="#">limit-ports</a>	Ingress	cc	IP ranges:	tcp:22	Allow	1000	<a href="#">default</a>	▼
<input type="checkbox"/>	<a href="#">default-allow-internal</a>	Ingress	Apply to all	IP ranges:	tcp:0-65535 udp:0-65535 icmp	Allow	65534	<a href="#">default</a>	▼

### Network firewall policies

Firewall policies let you group several firewall rules so that you can update them all at once, effectively controlled by Identity and Access Management (IAM) roles. [Learn more](#)



Select **on** and **Save**, scroll- up and click the arrow



1

2

3

4

5

# Task 6. Verify Compliance

LOUIS.O

Google Cloud

SECURITY COMMAND CENTER

- IAM & Admin
- Marketplace
- Vertex AI
- Compute Engine
- Kubernetes Engine
- Cloud Storage
- BigQuery
- VPC network
- Cloud Run
- SQL
- Security**
- Google Maps Plat...

SECURITY COMMAND CENTER

- Risk Overview
- Threats
- Vulnerabilities
- Compliance**
- Assets
- Findings
- Sources
- Posture Management **NEW**

DETECTIONS AND CONTROLS

- Google SecOps
- reCAPTCHA Enterprise
- Web Security Scanner
- Risk Manager
- Binary Authorization
- Advisory Notifications
- Access Approval

Annotations: 1 points to the menu icon, 2 points to the Security menu item, and 3 points to the Compliance menu item.

Google Cloud

qwiklabs-gcp-04-867c17bf76fa

Compliance

Overall, are you satisfied with

Review your compliance with the security standards on this page. For more information about your compliance standard.

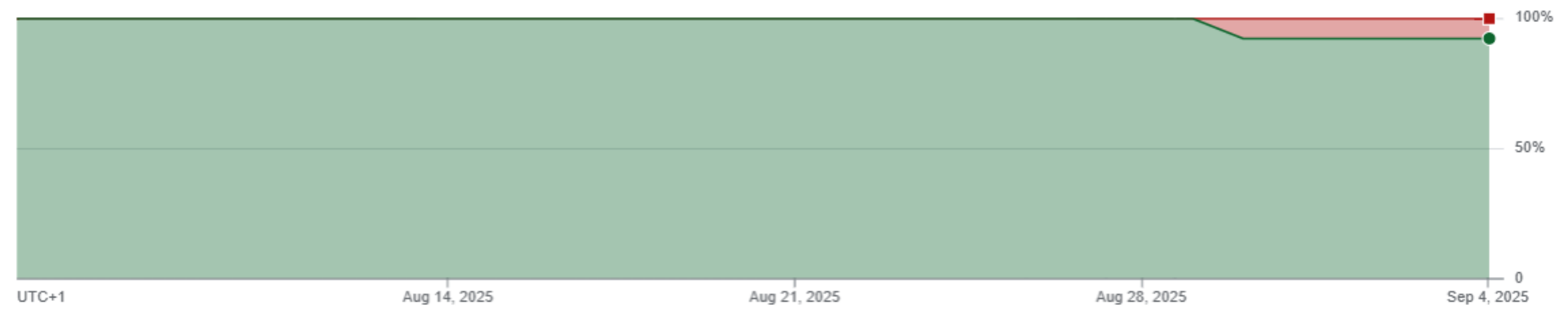
<b>NIST 800-53 R5</b> 68% passing <a href="#">View details</a>	<b>NIST CSF 1.0</b> 63% passing <a href="#">View</a>
<b>OWASP 2017</b> 100% passing <a href="#">View details</a>	<b>OWASP 2021</b> 100% passing <a href="#">View</a>
<b>PCI DSS 3.2.1</b> 90% passing <a href="#">View details</a>	<b>PCI DSS 4.0</b> 52% passing <a href="#">View</a>

- Security
- Security Command Ce...
- Risk Overview
- Threats
- Vulnerabilities
- Compliance**
- Assets
- Findings
- Sources
- Posture Management
- Detections and Controls
- Google SecOps
- reCAPTCHA
- Model Armor
- Web Security Scanner
- Marketplace
- Release Notes

### Compliance detail

Settings Learn

to view the state of your controls over time.



Filter Enter property name or value

Control ↑	Status	Rule ?	Severity	Findings	Resources scanned
▶ 1.1.4	✓ Compliant			0	
▶ 1.1.5	✓ Compliant			0	
▶ 1.2	✓ Compliant			0	
▶ 1.2.1	✓ Compliant			0	
▶ 1.2.2	✓ Compliant			0	
▶ 1.3	✓ Compliant			0	
▶ 1.3.2	✓ Compliant			0	
▶ 1.3.4	✓ Compliant			0	
▶ 1.3.7	✓ Compliant			0	

Successfully updated firewall rule "default-allow-internal".

Security Command Center ^

Risk Overview

Threats

Vulnerabilities

**Compliance**

Assets

Findings

Sources

Posture Management ...

Detections and Controls ^

Marketplace

70% of controls passed (35 out of 39) 31 total findings



Filter Enter property name or value

Rule	Severity	Findings	Controls
<a href="#">VPC Flow logs should be Enabled for every subnet in VPC Network</a>	Low	29	10.1 10.2
<a href="#">Basic roles (Owner, Writer, Reader) are too permissive and should not be used</a>	Medium	1	7.1.2
<a href="#">An egress deny rule should be set</a>	Low	1	7.2
<a href="#">All apps must have a valid firewall audit label. Check the app's firewall and add a label with the format `pci-dss-firewall-audit: "pci-dss-2022q1" where the suffix is {Year}q{Quarter}.</a>	Low	0	1.1.4
<a href="#">Every app in the cluster requires a `network-controls/date` annotation. Check the app's network-controls and add an `network-controls/date` annotation with the schema {YYYY-MM-DD}.</a>	Low	0	1.1.5 2.4
<a href="#">Cannot use a namespace in the cluster without a NetworkPolicy. Add a NetworkPolicy to your namespace.</a>	Low	0	1.2

# Conclusion

Great work!

You have helped the security team at Cymbal Bank to mitigate the impact of the data breach, address the identified vulnerabilities, and significantly enhanced the security posture of Cymbal Bank's Google Cloud environment.

First, you examined and analyzed the vulnerabilities and findings in Google Cloud Security Command Centre.

Next, you shut the old VM down and created a new VM from a snapshot taken before the malware infection.

Then, you fixed the cloud storage permissions by revoking public access to the storage bucket and switching to uniform bucket-level access control. You also removed all user permissions from the storage bucket.

Next, you fixed the firewall rules by deleting the default-allow-icmp, default-allow-rdp, and default-allow-ssh firewall rules, and enabling logging for the remaining firewall rules.

Finally, you run a compliance report to confirm that the vulnerability issues have been remediated.

Remember, as a security analyst it is crucial to maintain regular security audits and implement ongoing monitoring practices for continued protection against evolving threats and vulnerabilities.

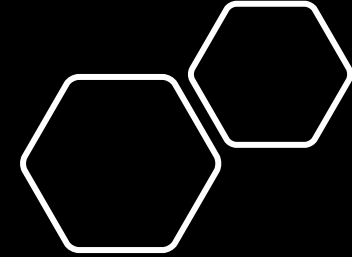


# Security Incident Report

LOUIS.O

# Cymbal

## Security Incident Report



### Table of contents

	Page
Executive summary	1
Investigation	1
Response and remediation	2
Containment and eradication measures	2
Recovery measures	2
Recommendations	3

### Executive summary

Cymbal Retail recently faced a major data breach caused by misconfigured cloud resources, outdated systems, and weak firewall rules. The incident highlighted how critical it is to secure cloud environments to protect sensitive data, maintain customer trust, and ensure compliance. The breach required urgent containment, system recovery, and remediation efforts to secure the environment and prevent future attacks.

## Investigation

A comprehensive investigation was conducted to determine the nature and extent of the compromise. The following findings were identified:

### **1. Malware infection:**

Forensic analysis confirmed the presence of malware on the compromised VM. The specific type and variant of the malware were identified through in-depth analysis, providing insights into the attacker's techniques and potential motivations.

### **2. Unauthorized access:**

Evidence revealed that the attacker gained unauthorized access to the compromised VM by exploiting open RDP and SFTP services. The access logs and network traffic analysis provided crucial insights into the attacker's entry point and their subsequent activities.

### **3. Privilege escalation:**

The forensic examination indicated that the attacker leveraged the compromised VM to escalate privileges and gain access to sensitive systems and resources. Through the exploitation of user and service account credentials, the attacker was able to move laterally within the network and target additional services, in particular gaining unauthorized access to BigQuery.

### **4. Data exfiltration:**

The forensic analysis confirmed the exfiltration of credit card information, including card numbers, usernames, and associated locations. The attacker utilized a storage bucket with public internet access to initiate and facilitate the exfiltration, exporting the compromised data for later remote retrieval. The findings provide valuable insights into the attack, enabling the incident response team to understand the attack vector, the attacker's actions, and the compromised data. These findings will serve as crucial evidence for further investigations, remediation efforts, and future cybersecurity enhancements.

# Response and remediation

To effectively remediate the incident, a series of actions were taken in alignment with industry best practices. The following outlines the containment, remediation, and recovery measures taken in response to the security incident.

## Containment and eradication measures:

These steps helped me to contain and eradication the breach.

1. I shut down old vulnerable VM and rebuilt from snapshot
2. I restricted public access to cloud storage buckets
3. I enforced uniform access controls on sensitive data
4. I limited firewall ports and corrected misconfigured rules
5. I ran compliance reports to verify remediation

## Recovery measures:

These steps ensured the compromised systems were recovered, secured and operations were restored.

1. Restored business services on a secure VM instance
2. Validated system integrity through security scans
3. Monitored logs in Google Cloud Security Command Center
4. Re-established compliance with regulatory requirements
5. Documented lessons learned to improve future response

## Recommendations:

This incident provided valuable lessons that can inform future cybersecurity practices and help prevent similar attacks. The following are recommendations that I suggested to be implemented to mitigate similar attacks from the future:

### **1. Strengthen Cloud Configuration Management**

- Enforce least privilege access, use automated tools (e.g., Google Cloud Security Command Center) to detect and remediate misconfigurations in real-time.

### **2. Implement Continuous Patch & Vulnerability Management**

- Regularly update VMs, applications, and firewalls with automated patching to reduce the attack surface.

### **3. Adopt Zero Trust Principles**

- Restrict access based on identity, device health, and context. Ensure multi-factor authentication for all users.

### **4. Enhance Monitoring & Incident Response Preparedness**

- Deploy centralized logging and SIEM integration for faster detection. Conduct regular tabletop exercises and red/blue team simulations to test readiness.

By implementing these measures, the security team successfully mitigated the incident, reduced the attack risks, removed the attacker's presence, and restored affected systems to a secure operational state.

Thank  
you!