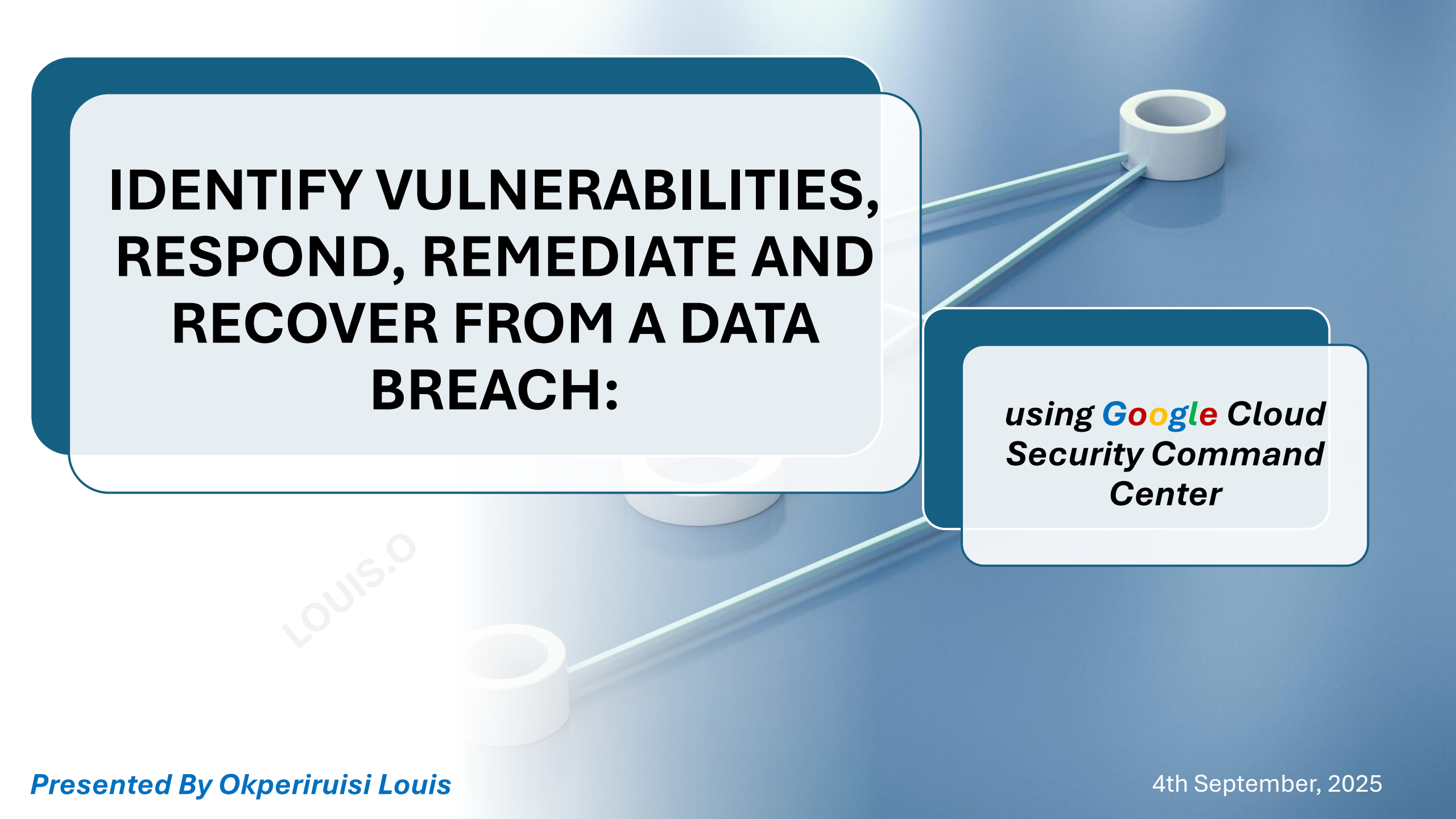
IDENTIFY VULNERABILITIES, RESPOND, REMEDIATE AND RECOVER FROM A DATA BREACH:

using Google Cloud Security Command Center

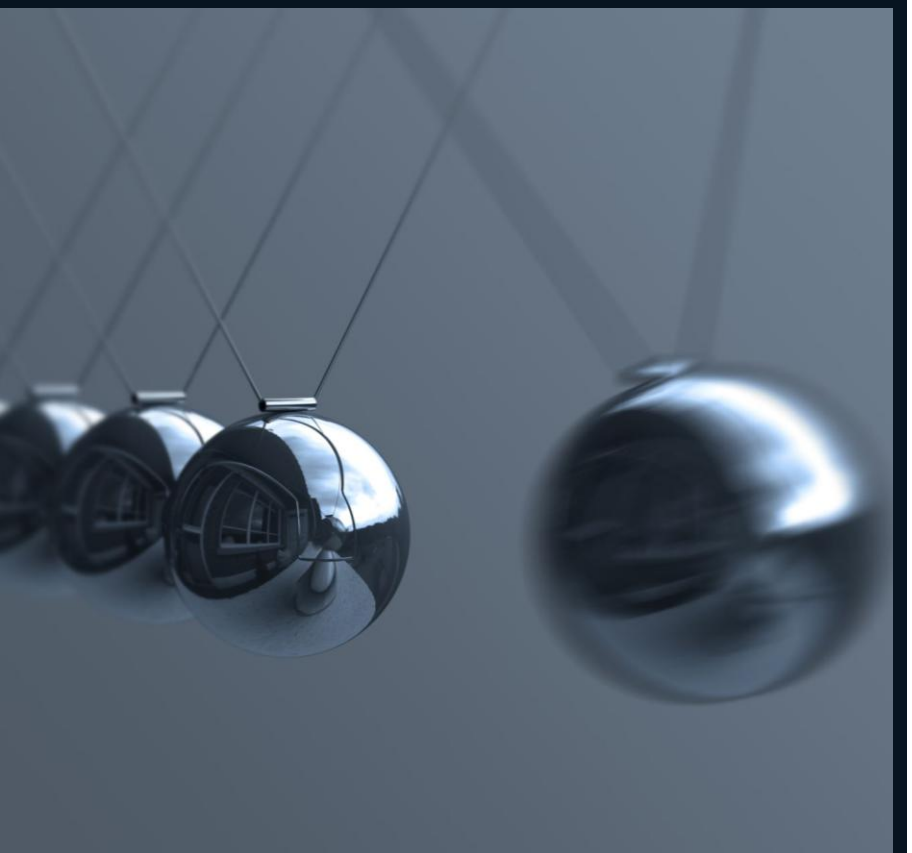


Presented By Okperiruisi Louis

4th September, 2025

Task 1. Analyze the data breach and gather information

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

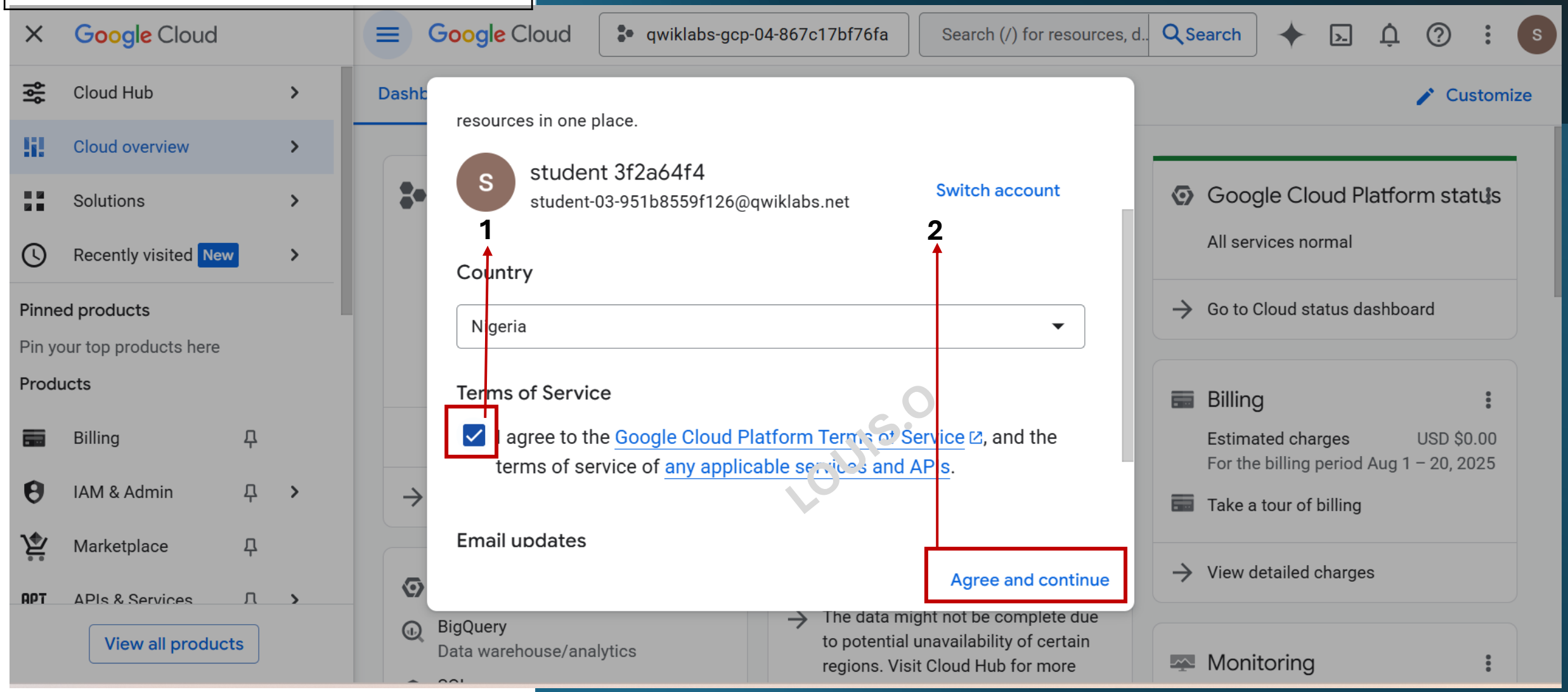
- **Goal:** Contain the breach, recover systems, remediate risks, and ensure compliance.

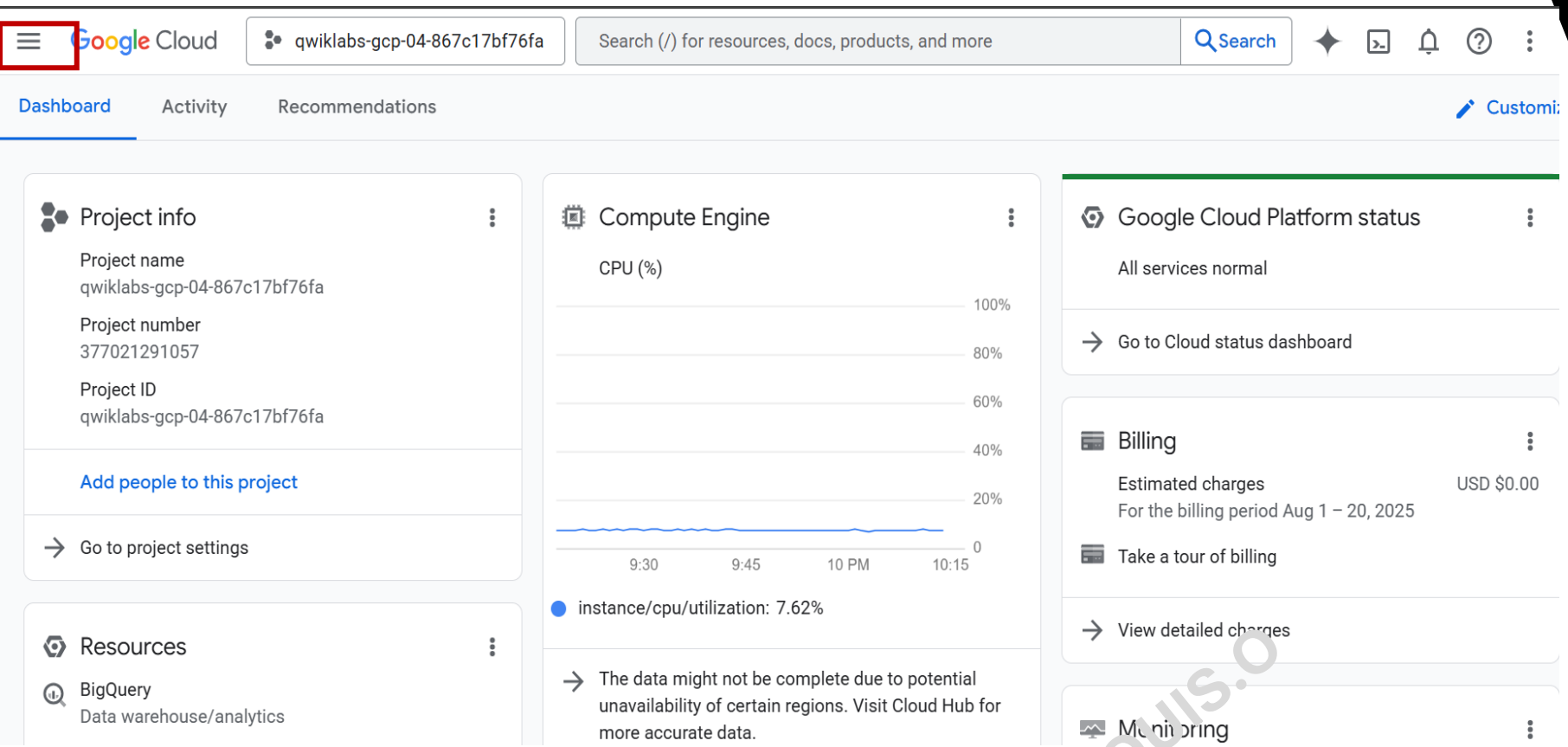
1. In the Google Cloud console, in the **Navigation menu** (☰), click **Security > Risk overview**. The Security Command Center Overview page opens.

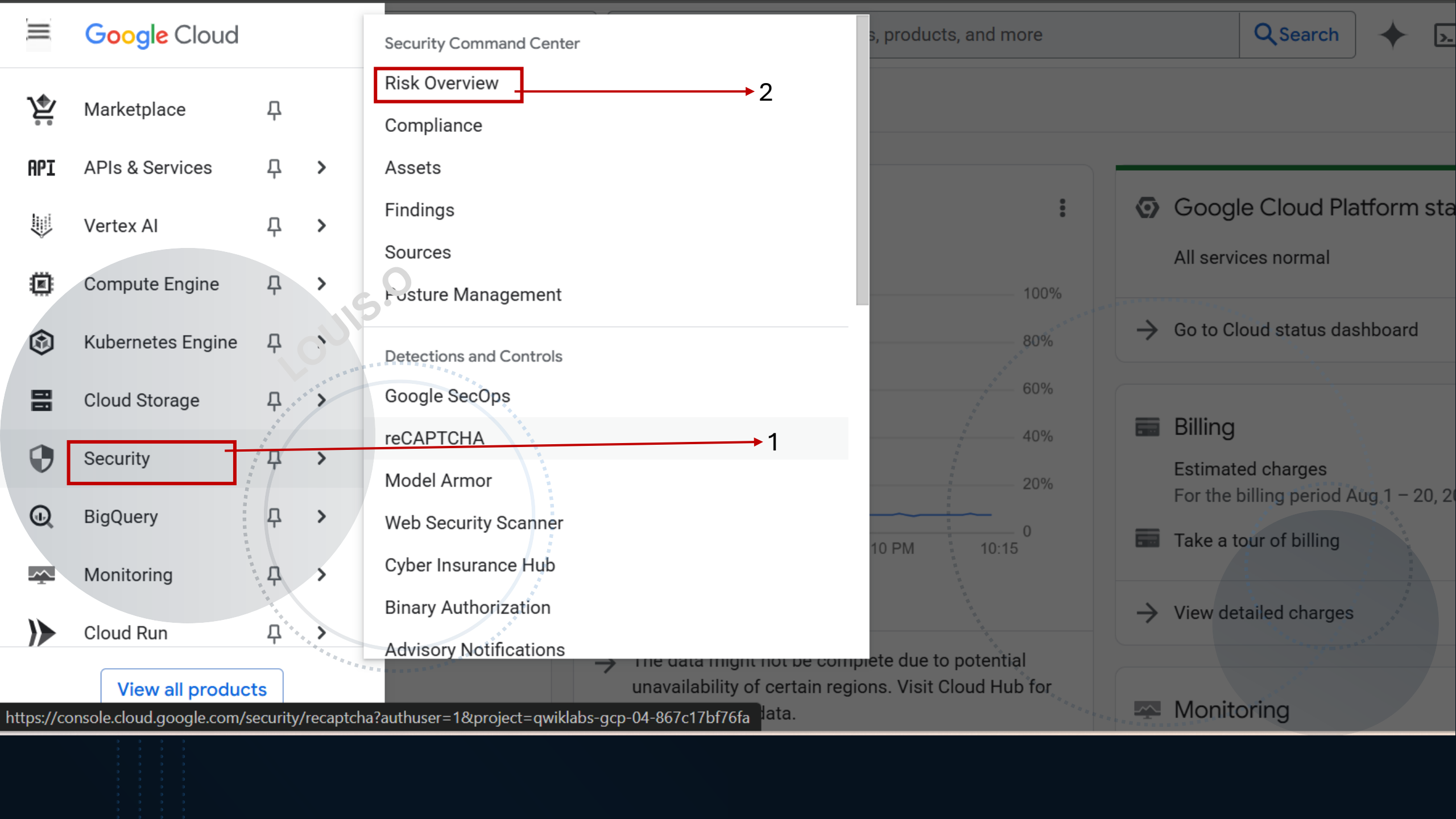
2. Scroll down to **Active vulnerabilities**. This provides an overview of current security vulnerabilities or issues that need attention within the Google Cloud environment.

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

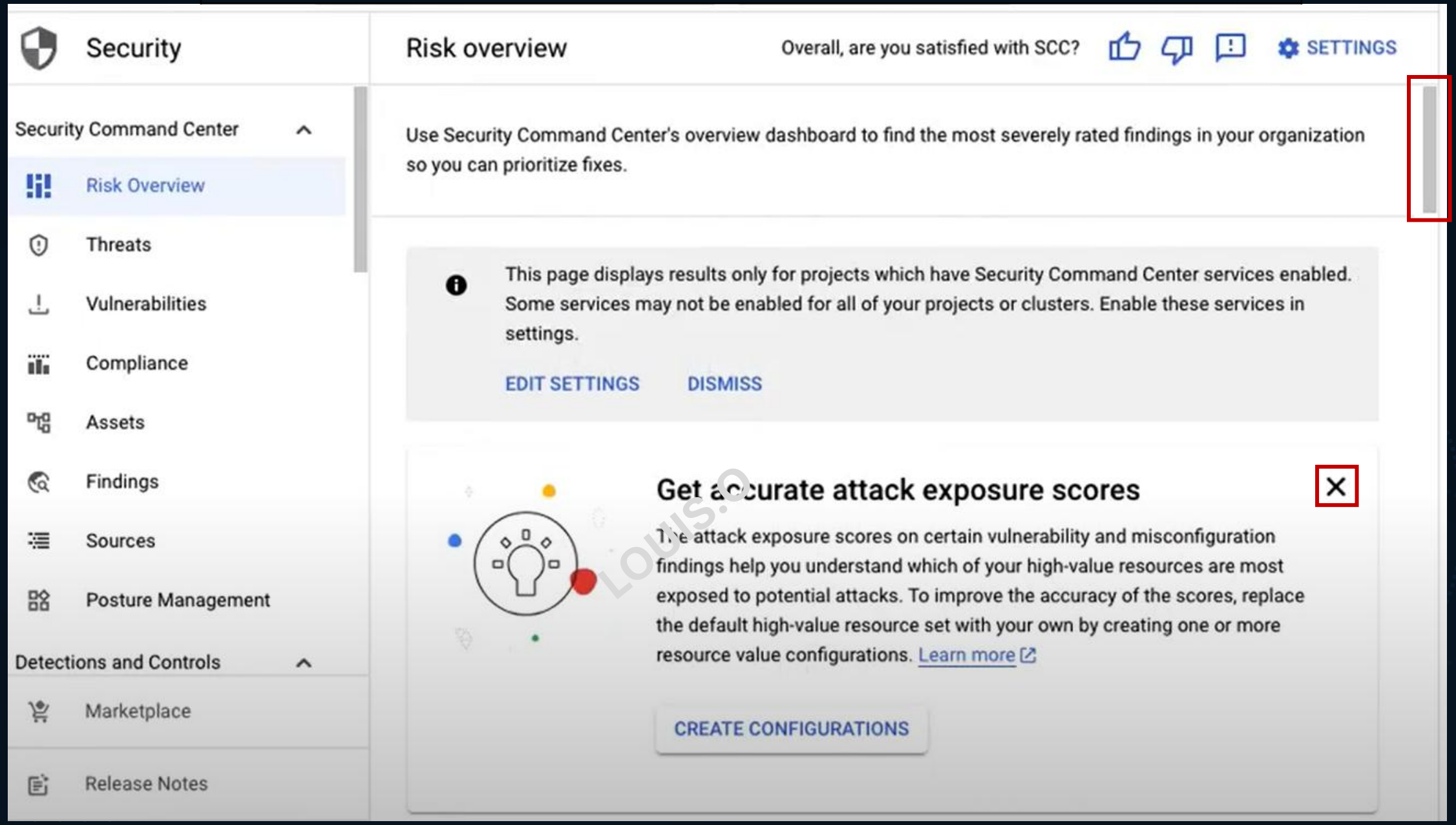
Sign-In To Account




Google Cloud
qwiklabs-gcp-04-867c17bf76fa
Search (/) for resources, docs, products, and more
Search
Dashboard
Activity
Recommendations
Customiz
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 (%)
100%
80%
60%
40%
20%
0
9:30
9:45
10 PM
10:15
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


Google Cloud
Marketplace
APIs & Services
Vertex AI
Compute Engine
Kubernetes Engine
Cloud Storage
Security
BigQuery
Monitoring
Cloud Run
View all products
Security Command Center
Risk Overview
Compliance
Assets
Findings
Sources
Posture Management
Detections and Controls
Google SecOps
reCAPTCHA
Model Armor
Web Security Scanner
Cyber Insurance Hub
Binary Authorization
Advisory Notifications
1
2
Search
Google Cloud Platform sta
All services normal
Go to Cloud status dashboard
Billing
Estimated charges
Take a tour of billing
View detailed charges
Monitoring
100%
80%
60%
40%
20%
0
10 PM
10:15
https://console.cloud.google.com/security/recaptcha?authuser=1&project=qwiklabs-gcp-04-867c17bf76fa

Scroll down to “Active Vulnerabilities”



Security Command Ce...
- Risk Overview
- Threats
- Vulnerabilities
- Compliance
- Assets
- Findings
- Sources
- Posture Management

Detections and Controls
- Google SecOps
- reCAPTCHA
- Model Armor

Marketplace

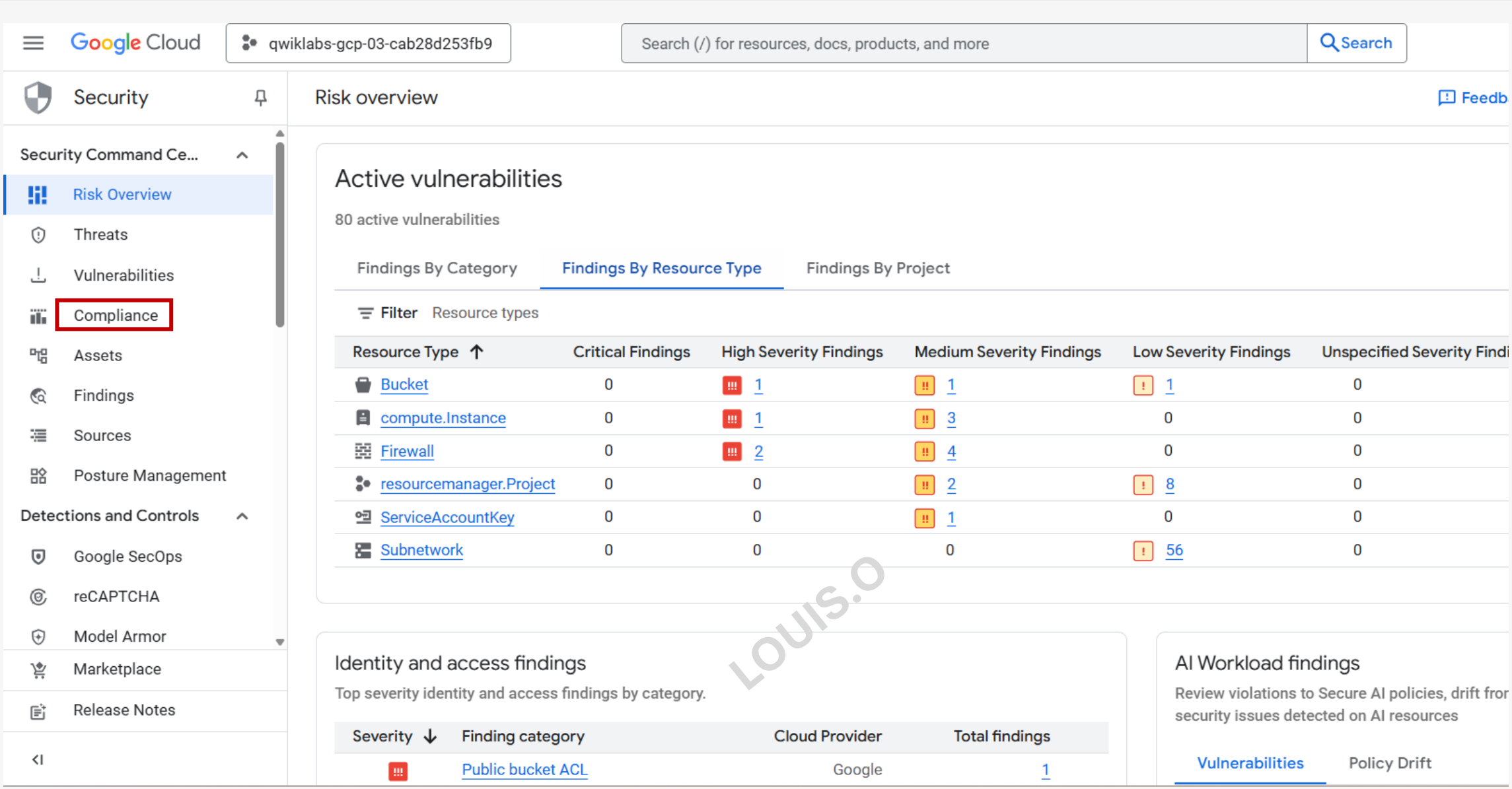
Active vulnerabilities

80 active vulnerabilities

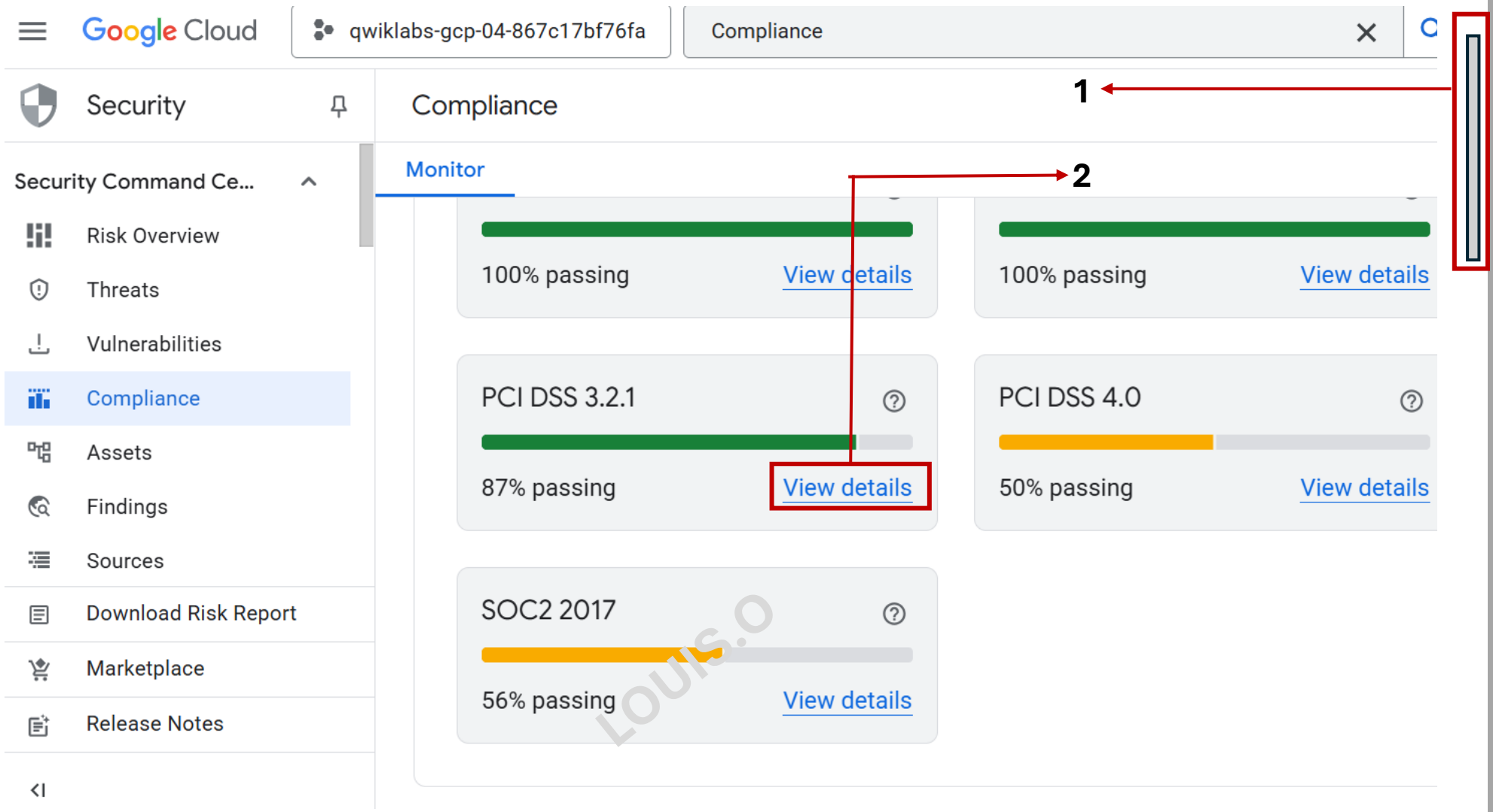
Findings By Category | Findings By Resource Type | Findings By Project

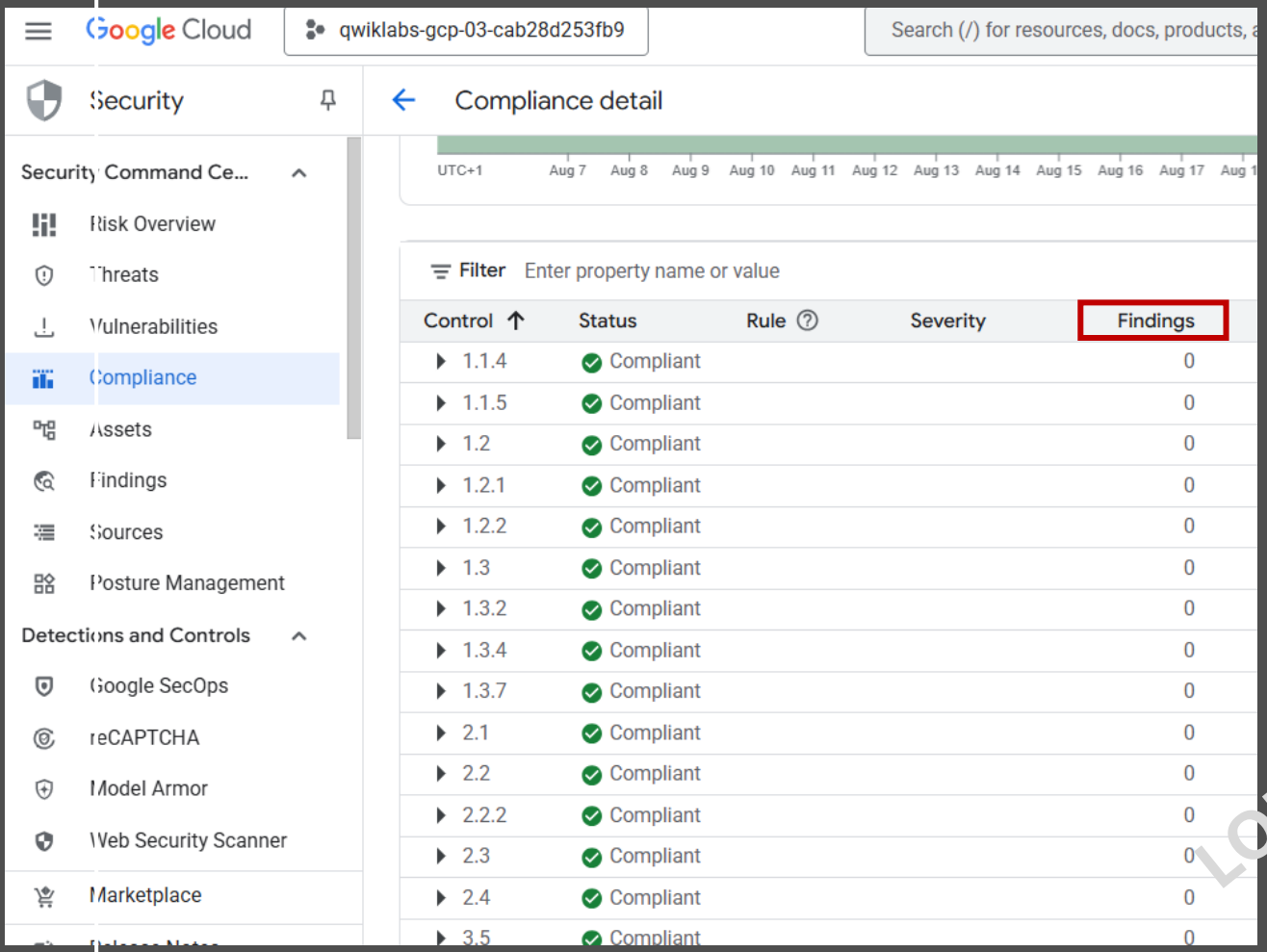
Filter Categories

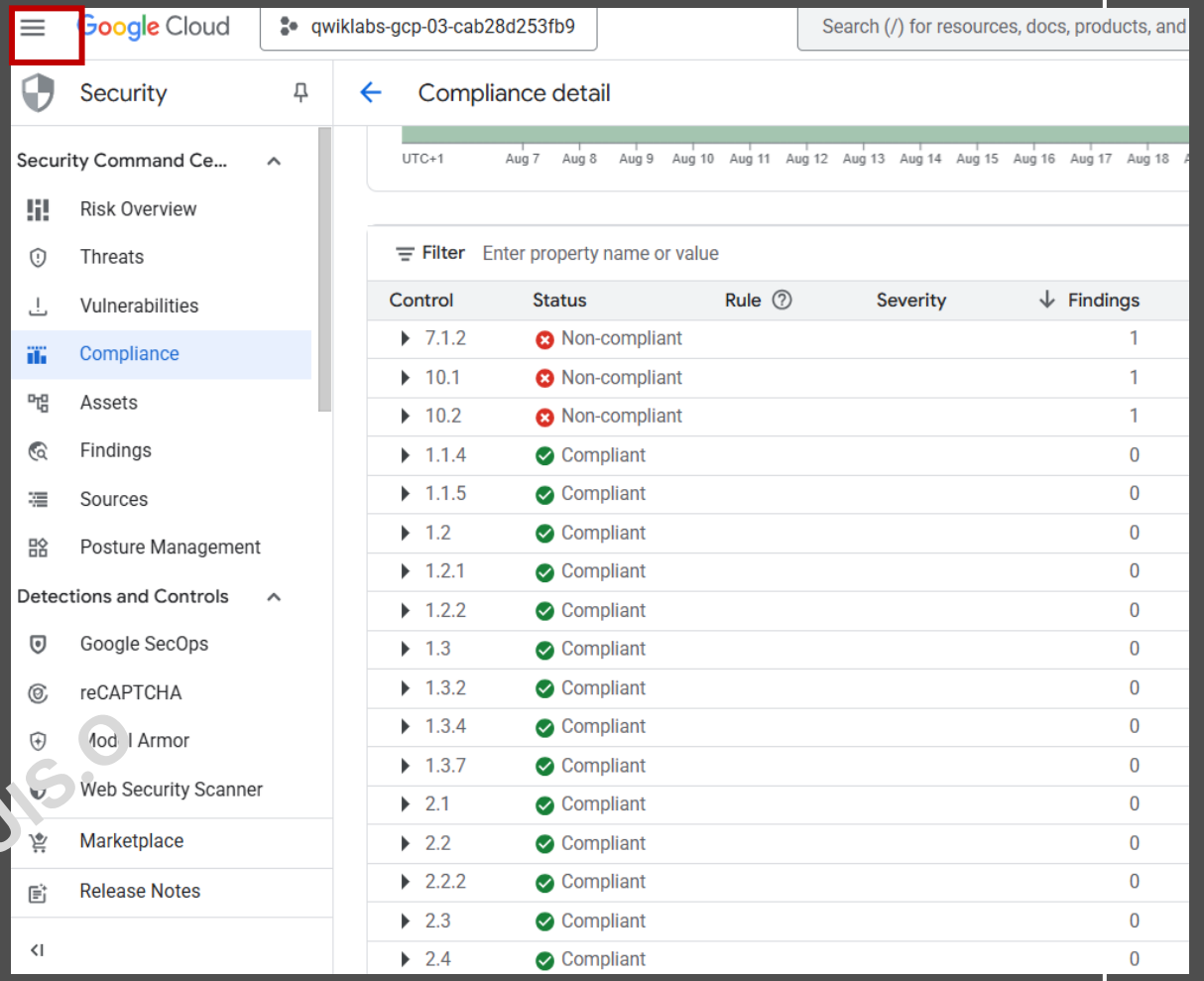
Severity	Finding category	Total findings
High	Open RDP port	1
High	Open SSH port	1
High	Public bucket ACL	1
High	Public IP address	1
Medium	Firewall rule logging disabled	4
Medium	Admin service account	1
Medium	Bucket policy only disabled	1
Medium	Compute Secure Boot disabled	1
Medium	Default service account used	1
Medium	Full API access	1


Google Cloud
qwiklabs-gcp-03-cab28d253fb9
Search (/) for resources, docs, products, and more
Search
Security
Risk overview
Feedb
Security Command Ce...
Risk Overview
Threats
Vulnerabilities
Compliance
Assets
Findings
Sources
Posture Management
Detections and Controls
Google SecOps
reCAPTCHA
Model Armor
Marketplace
Release Notes
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 Findi
Bucket 0 1 1 1 0
compute.Instance 0 1 3 0 0
Firewall 0 2 4 0 0
resourcemanager.Project 0 0 2 8 0
ServiceAccountKey 0 0 1 0 0
Subnetwork 0 0 0 56 0
Identity and access findings
Top severity identity and access findings by category.
Severity
Finding category
Cloud Provider
Total findings
Public bucket ACL Google 1
AI Workload findings
Review violations to Secure AI policies, drift fror
security issues detected on AI resources
Vulnerabilities
Policy Drift
LOUIS.O

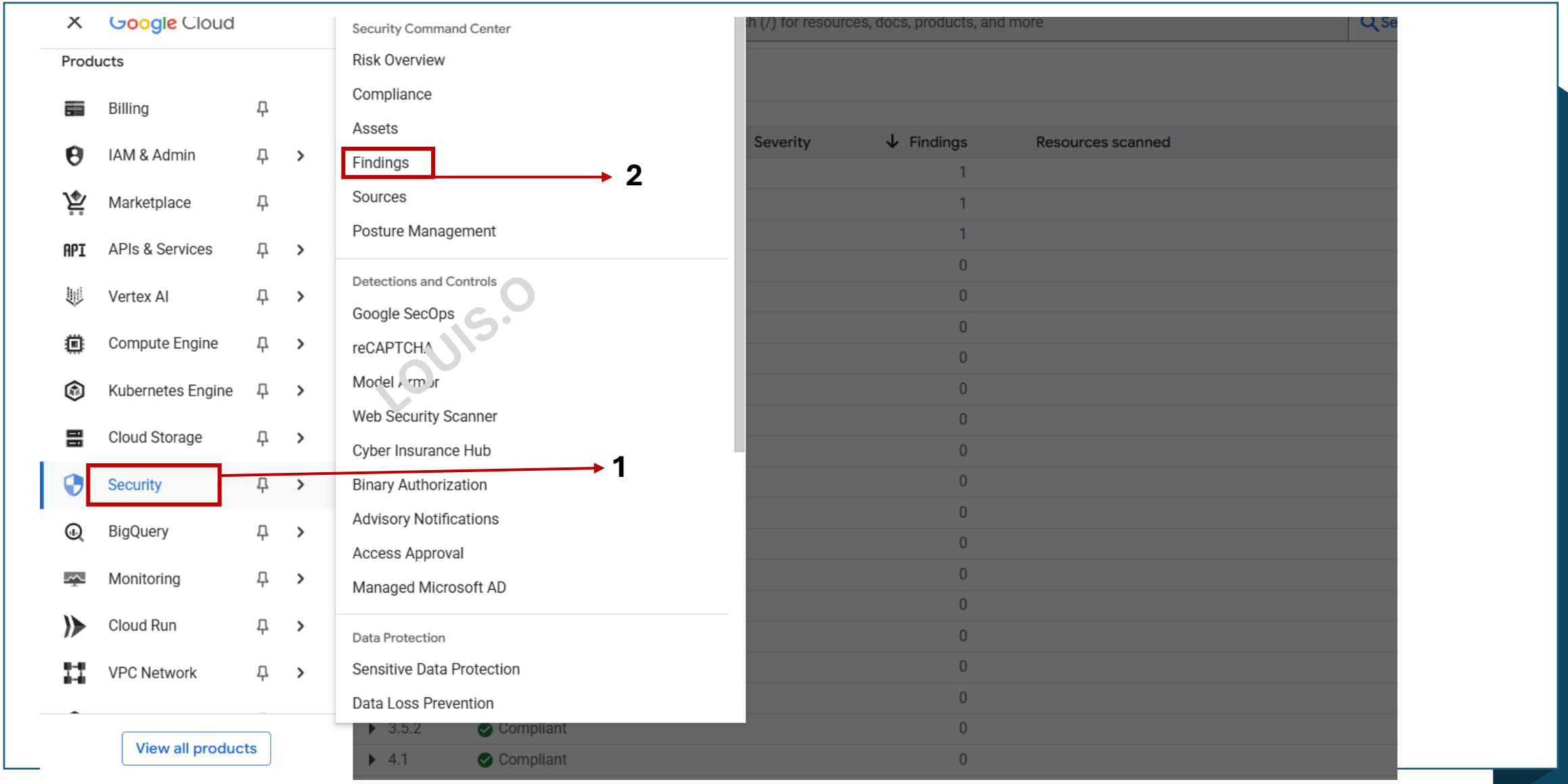
Scroll down to PCI DSS3.2.1 and click “View details”



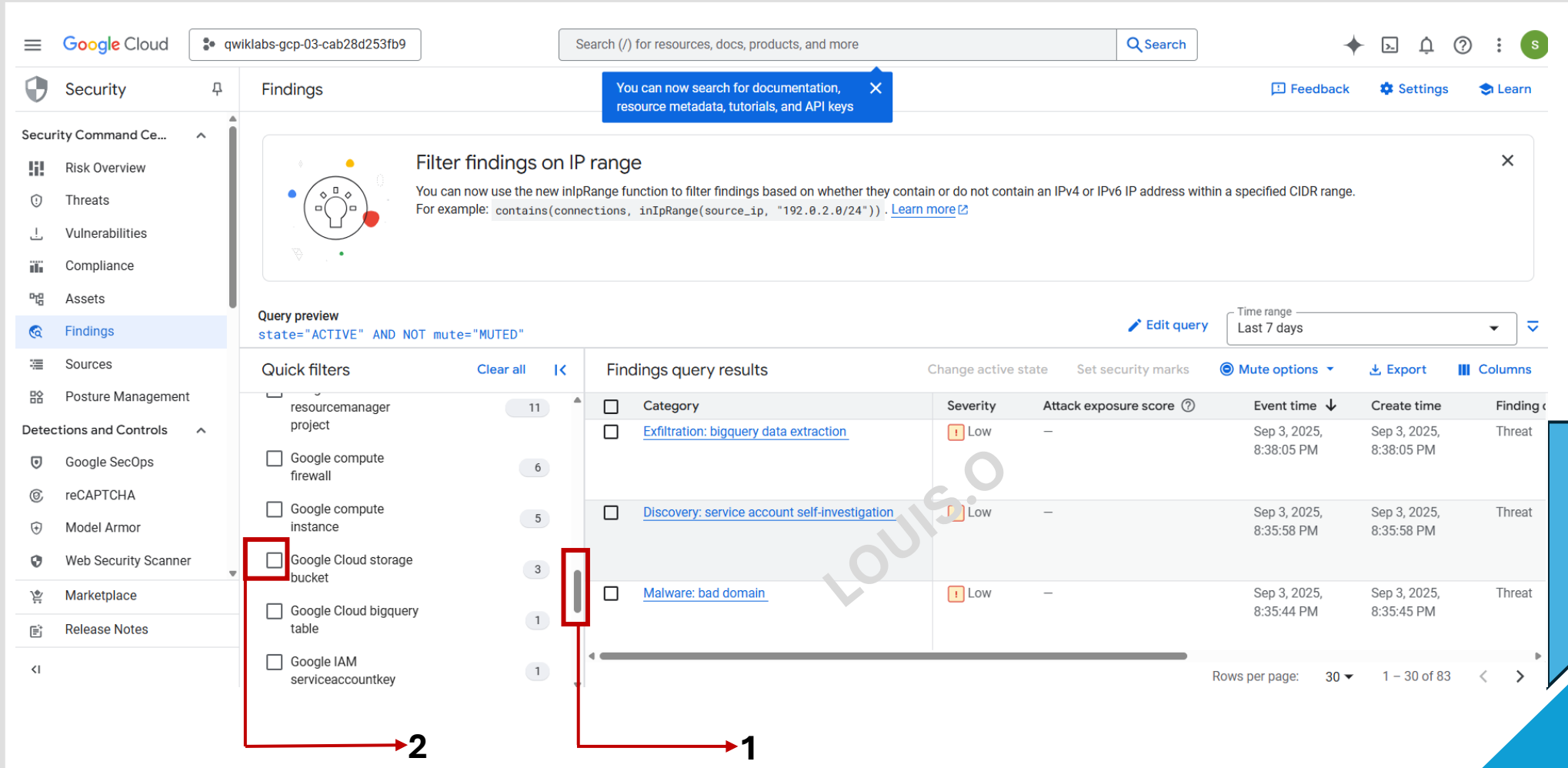

Google Cloud
qwiklabs-gcp-03-cab28d253fb9
Search (/) for resources, docs, products,
Security
Compliance detail
Security Command Ce...
Risk Overview
Threats
Vulnerabilities
Compliance
Assets
Findings
Sources
Posture Management
Detections and Controls
Google SecOps
reCAPTCHA
Model Armor
Web Security Scanner
Marketplace
UTC+1
Aug 7
Aug 8
Aug 9
Aug 10
Aug 11
Aug 12
Aug 13
Aug 14
Aug 15
Aug 16
Aug 17
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


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

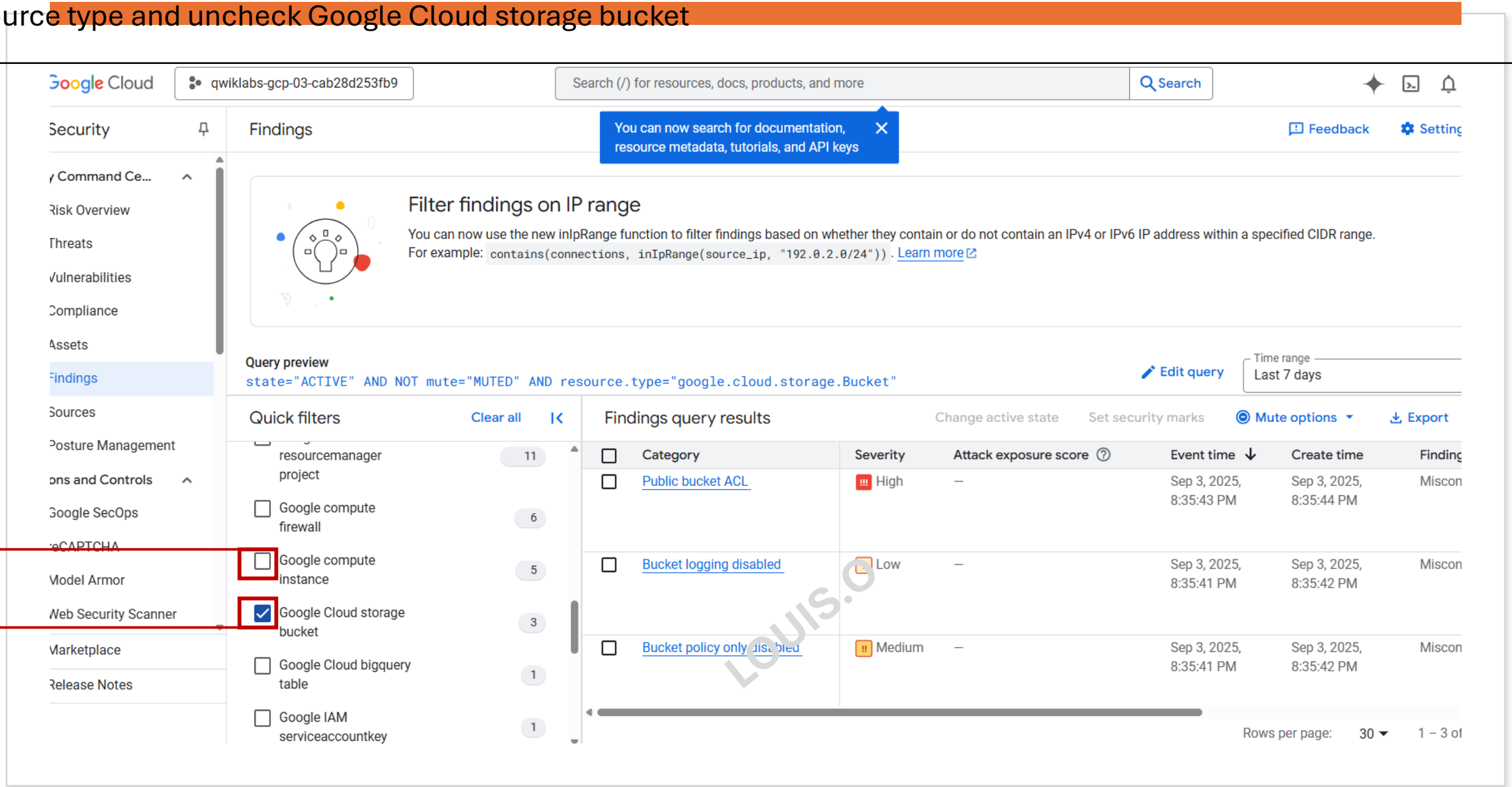
In the Google Cloud console, in the **Navigation menu** (☰), click **Security > Findings**. The **Findings** page opens.

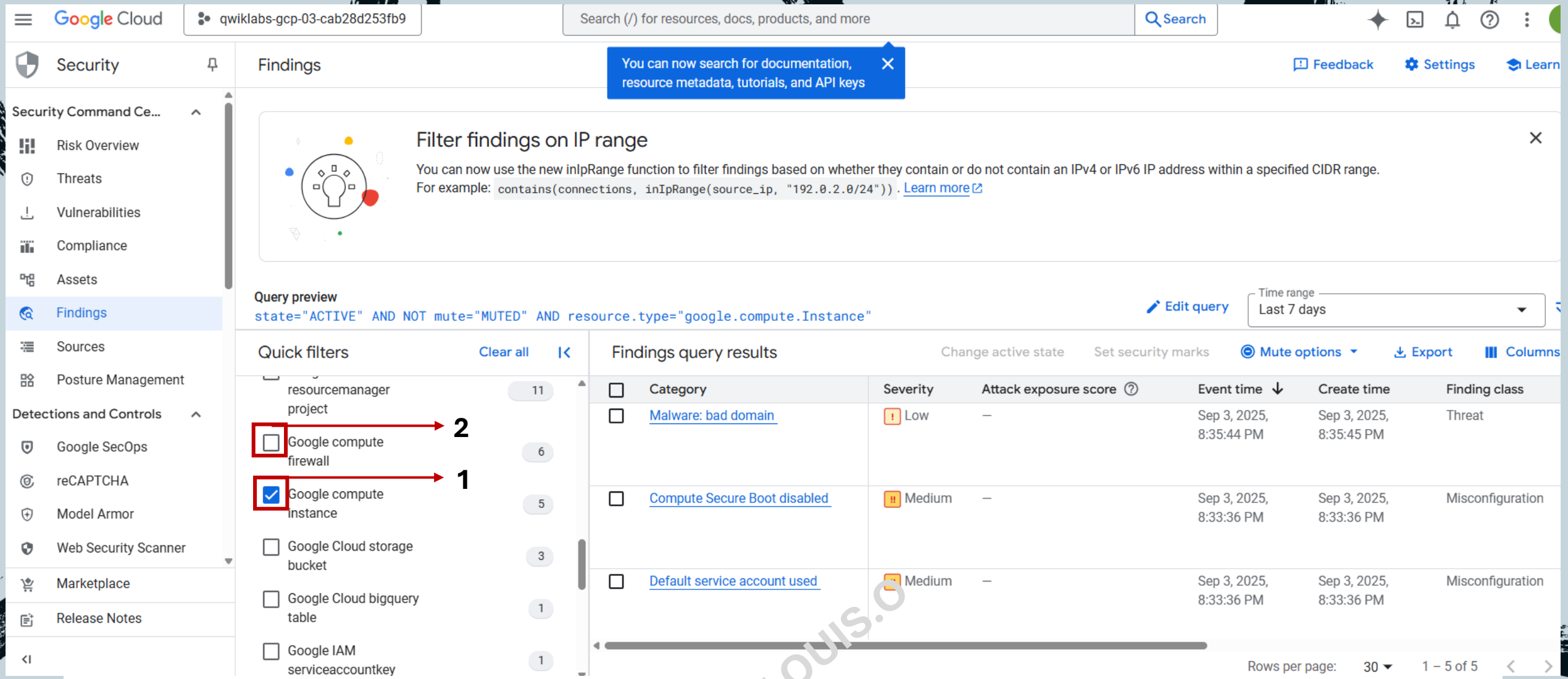


In the Quick filters panel, scroll down and checkbox “Google Cloud Storage Bucket”



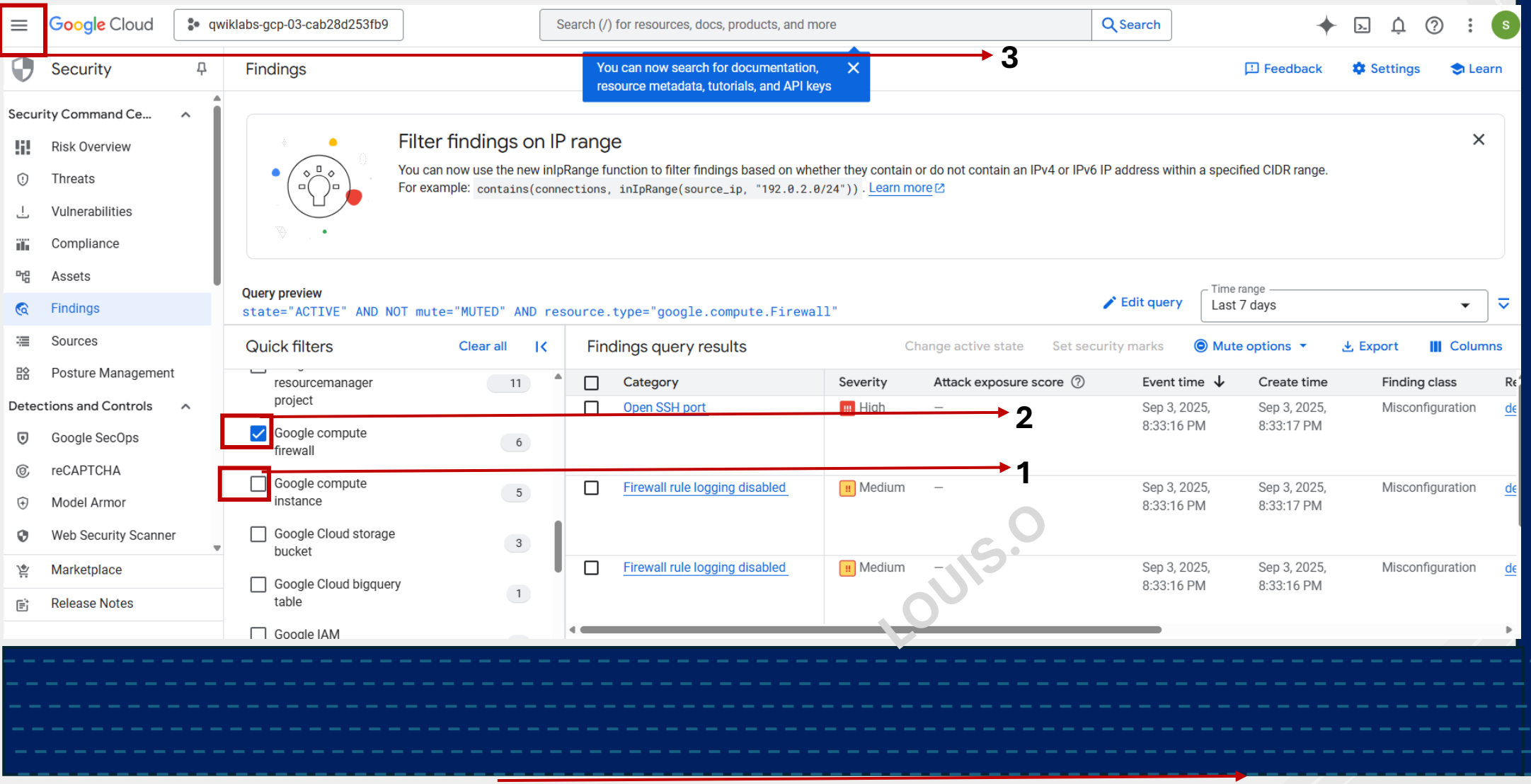
In the **Quick filters** panel, scroll down to **Resource Type** section select the checkbox for the **Google compute Instance** resource type and uncheck Google Cloud storage bucket



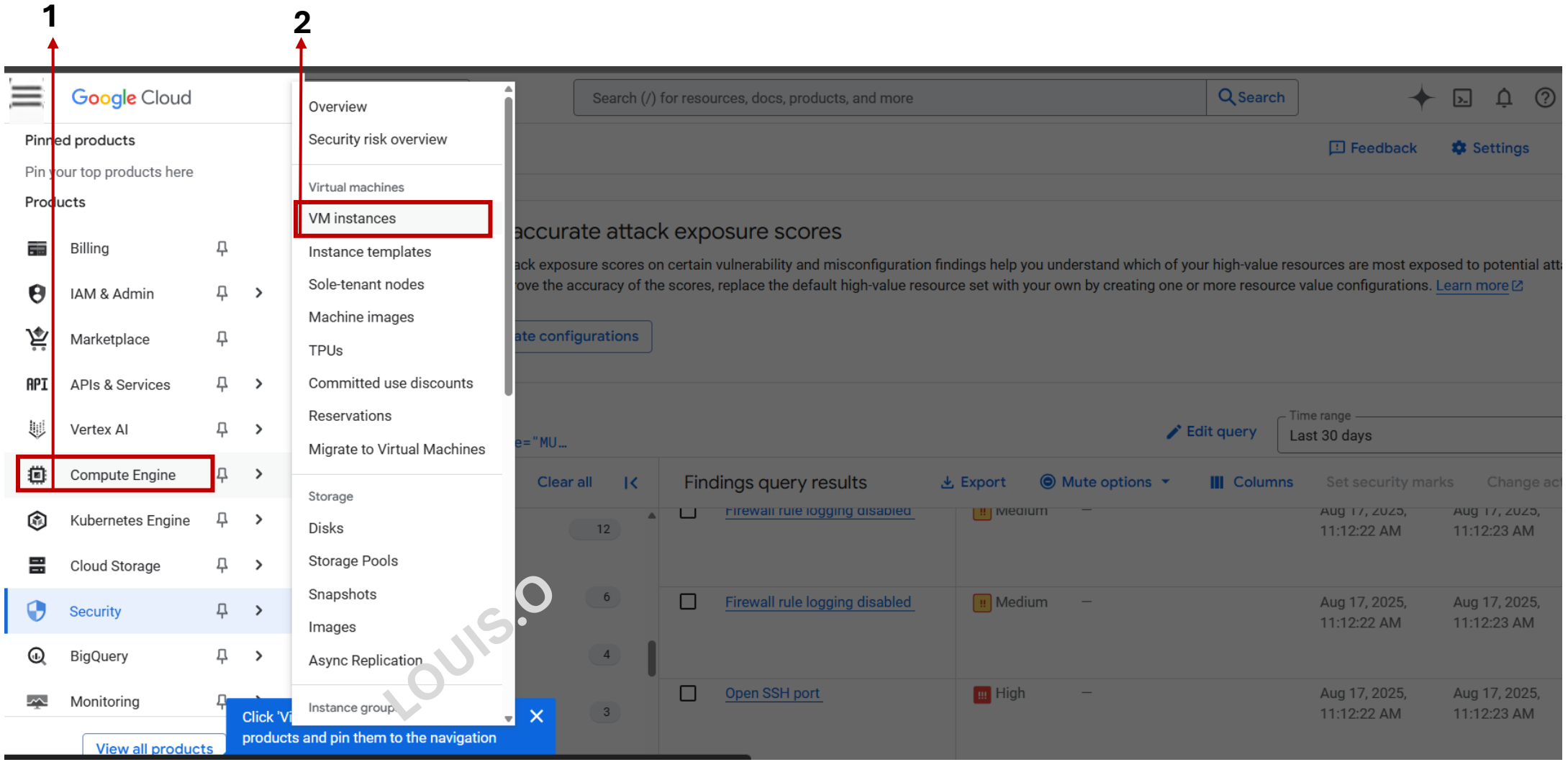


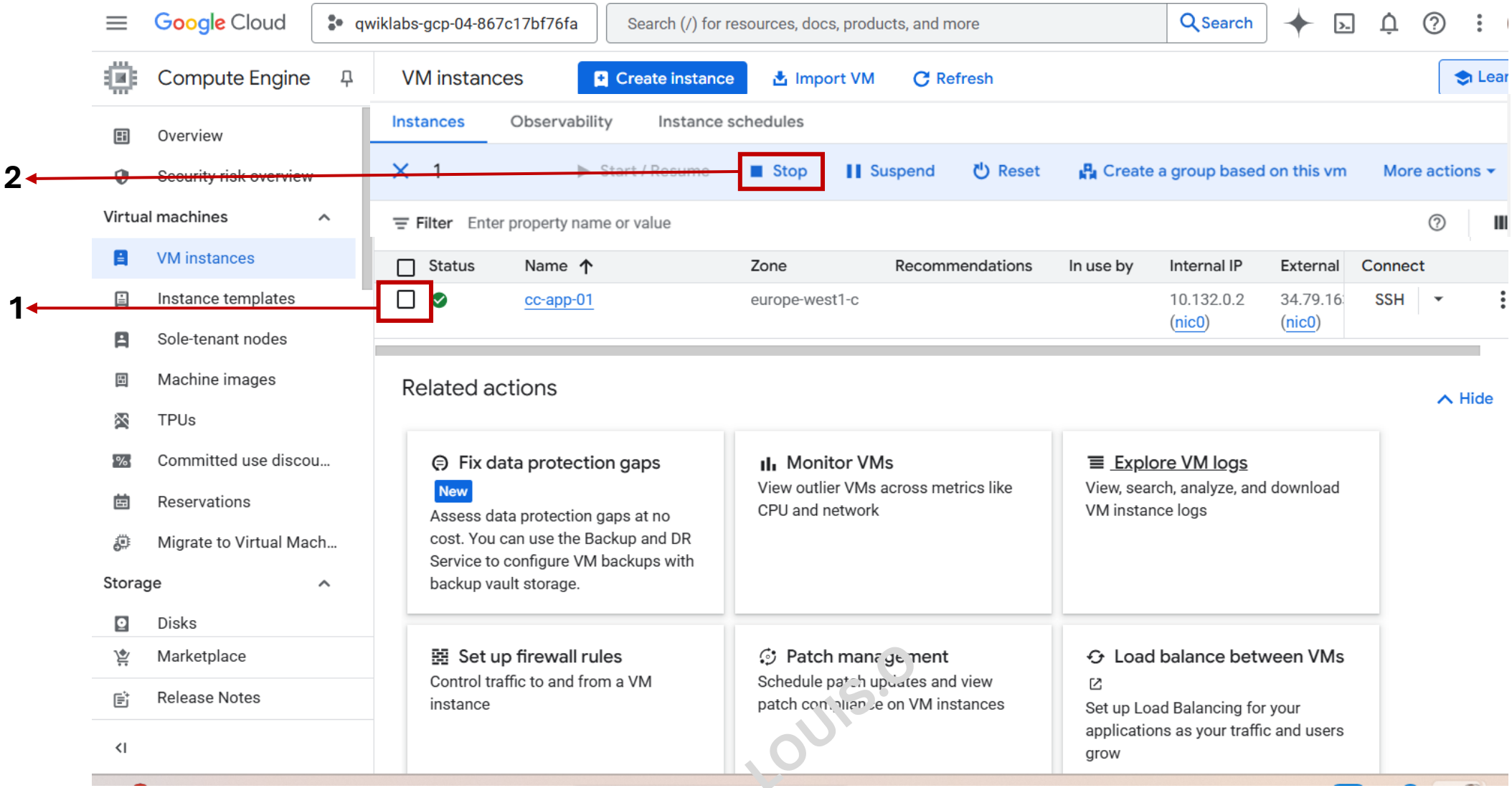
In the **Quick filters** panel, scroll down to **Resource Type** section , uncheck **Google compute instance and check Google Compute firewall,**

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

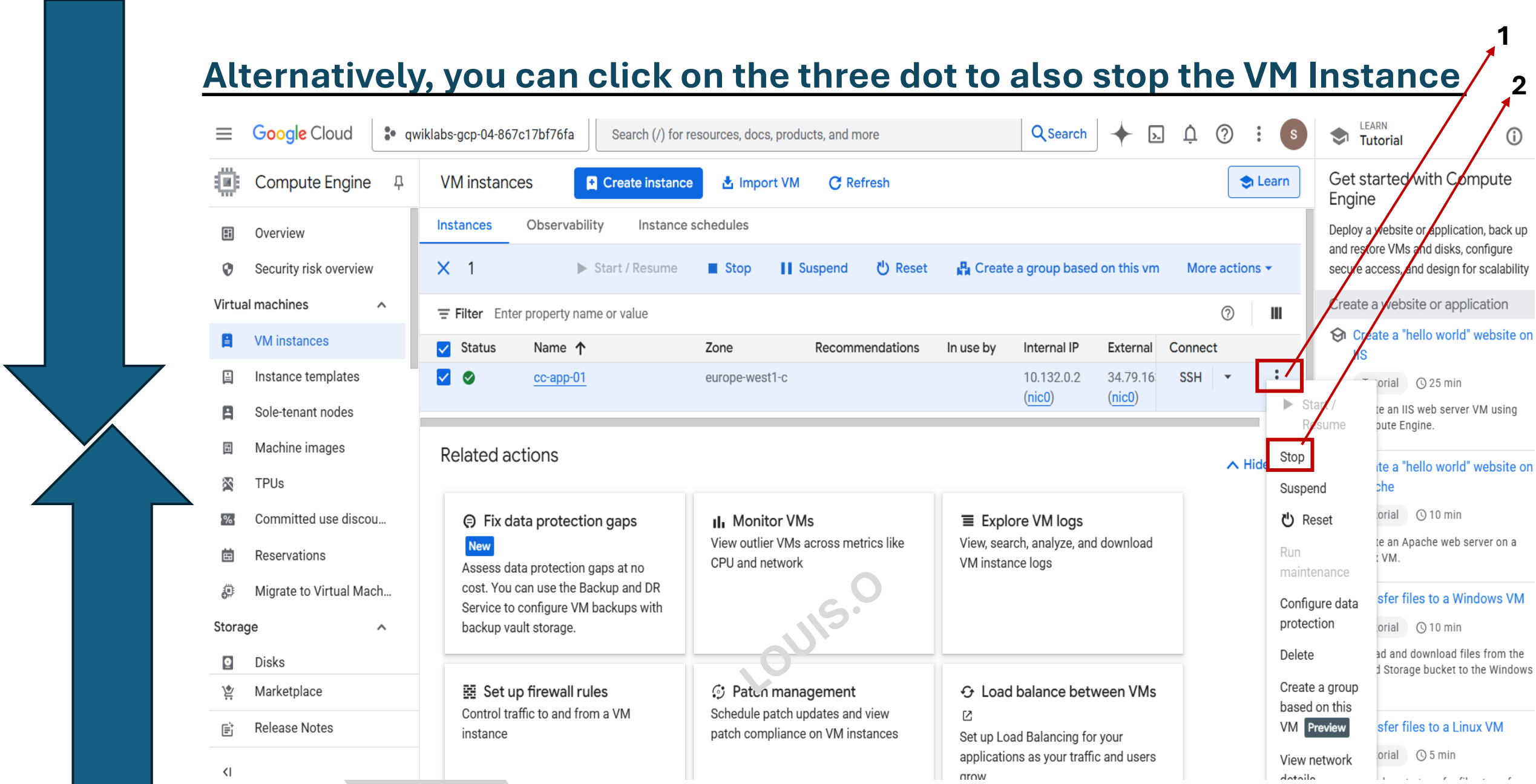


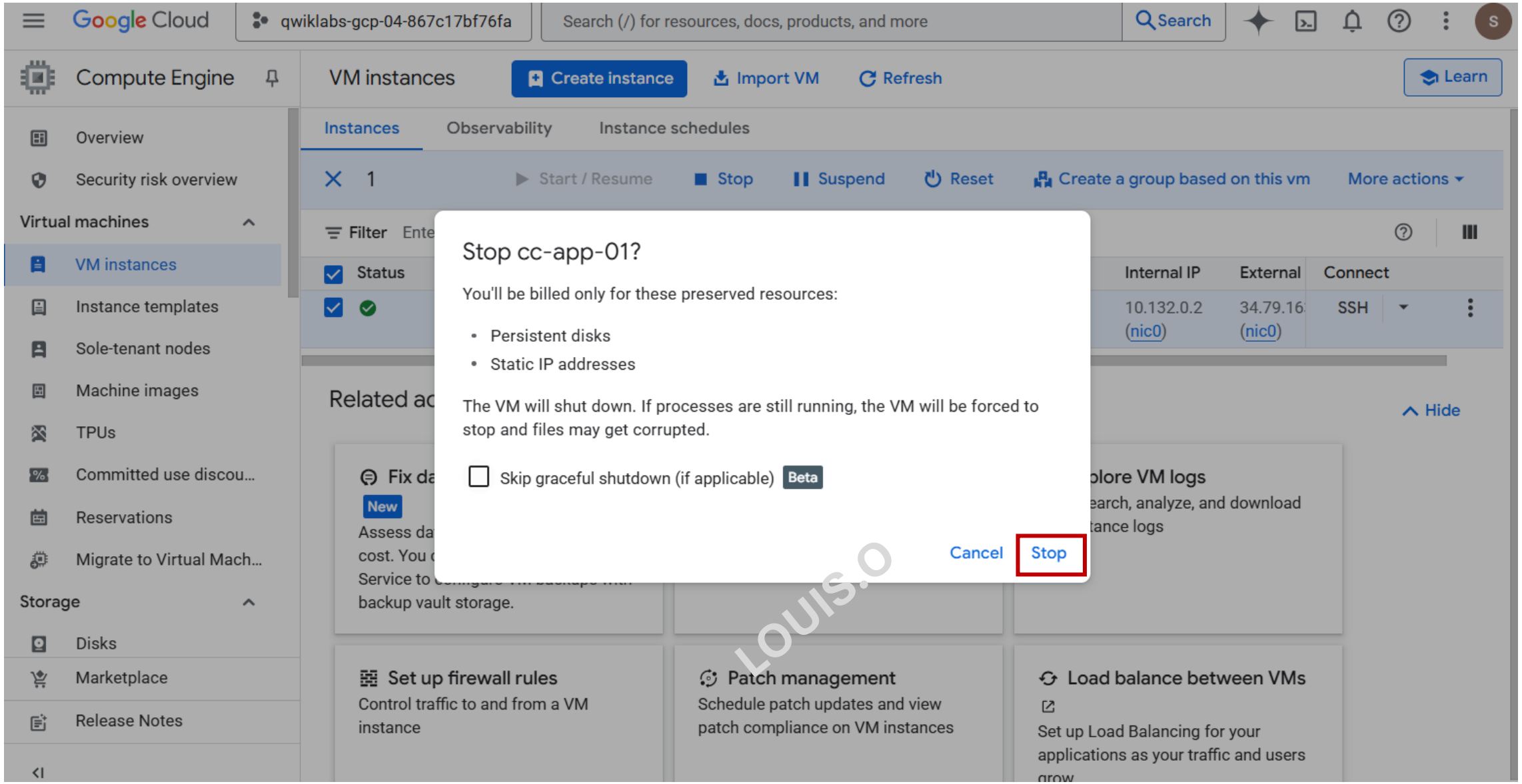
Task 2. Fix the Compute Engine Vulnerabilities


1
2
Google Cloud
Pinned products
Pin your top products here
Products
Billing
IAM & Admin
Marketplace
APIs & Services
Vertex AI
Compute Engine
Kubernetes Engine
Cloud Storage
Security
BigQuery
Monitoring
View all products
Overview
Security risk overview
Virtual machines
VM instances
Instance templates
Sole-tenant nodes
Machine images
TPUs
Committed use discounts
Reservations
Migrate to Virtual Machines
Storage
Disks
Storage Pools
Snapshots
Images
Async Replication
Instance group
products and pin them to the navigation
Search (/) for resources, docs, products, and more
Search
Feedback
Settings
accurate attack exposure scores
ck exposure scores on certain vulnerability and misconfiguration findings help you understand which of your high-value resources are most exposed to potential att
ove 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
ate configurations
Edit query
Time range
Last 30 days
Clear all
Findings query results
Export
Mute options
Columns
Set security marks
Firewall rule logging disabled
Medium
Aug 17, 2025, 11:12:22 AM
Aug 17, 2025, 11:12:23 AM
Open SSH port
High
12
6
4
3
LOUIS.O

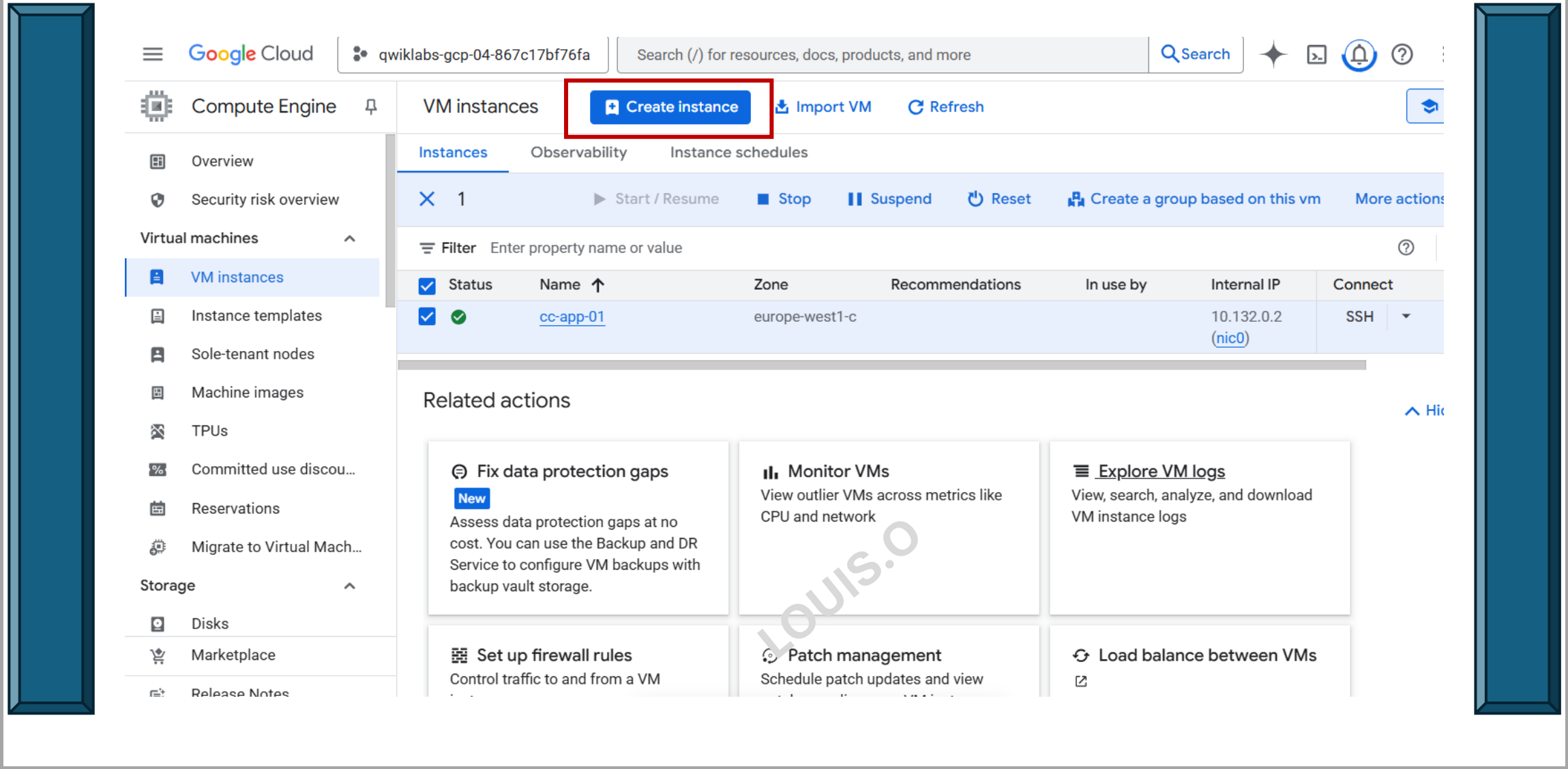

Google Cloud
qwiklabs-gcp-04-867c17bf76fa
Search (/) for resources, docs, products, and more
Search
Compute Engine
VM instances
Create instance
Import VM
Refresh
Overview
Security risk overview
Virtual machines
VM instances
Instance templates
Sole-tenant nodes
Machine images
TPUs
Committed use discou...
Reservations
Migrate to Virtual Mach...
Storage
Disks
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
cc-app-01
europe-west1-c
10.132.0.2 (nic0)
34.79.16
(nic0)
SSH
2
1
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

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




Google Cloud
qwiklabs-gcp-04-867c17bf76fa
Search (/) for resources, docs, products, and more
Search
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
Status
Internal IP
External
Connect
10.132.0.2 (nic0)
34.79.16 (nic0)
SSH
Related ac
Hide
Fix da
New
Assess da
cost. You
Service to
backup vault storage.
lore VM logs
earch, analyze, and download
tance 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
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
LOUIS.O

Create a New VM Instance From a Snapshot



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 *
instance-20250820-215346

Region *
europe-west1 (Belgium)
Region is permanent

Zone *
Any
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

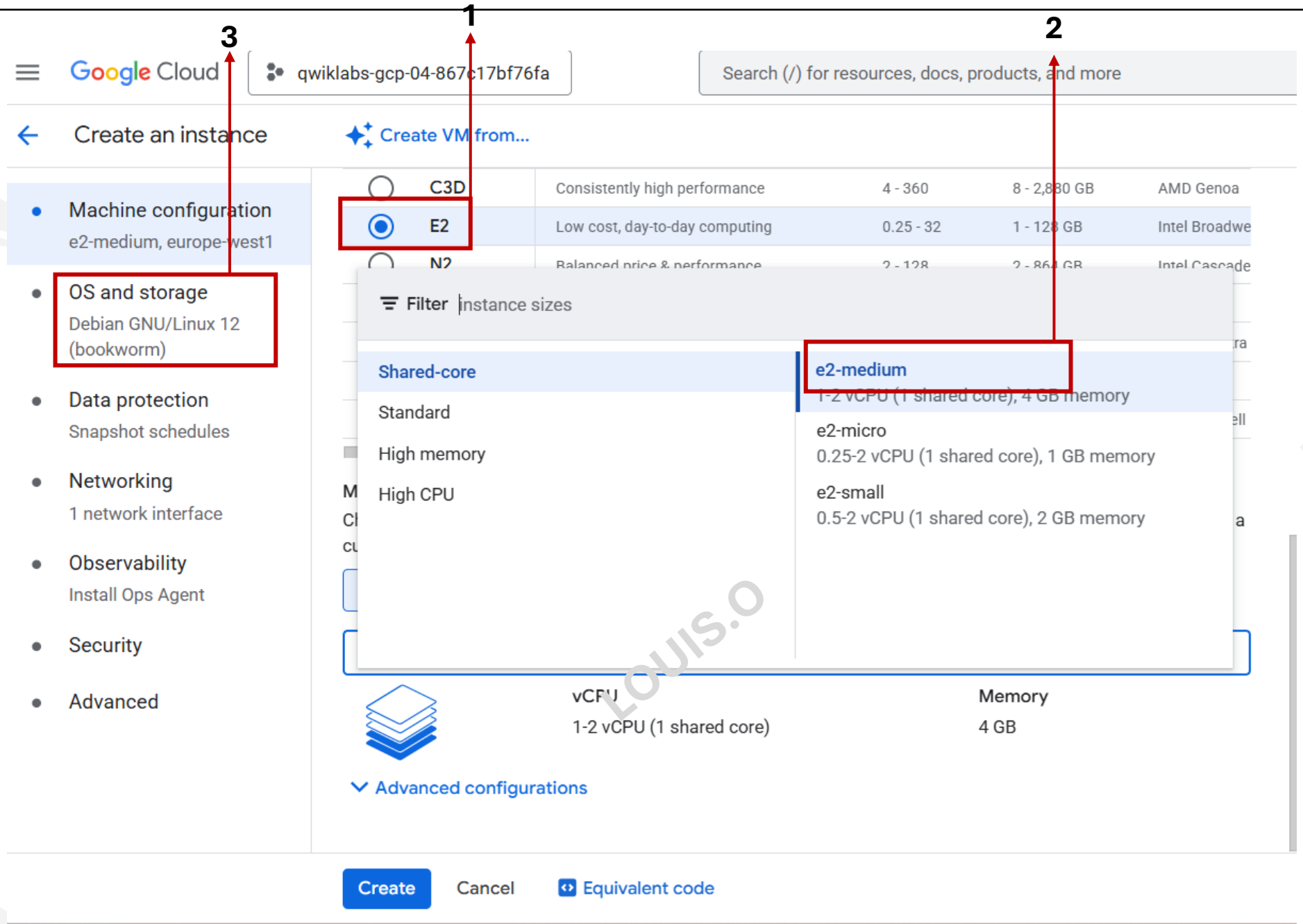
Try new C4 machine types, including local SSD and bare metal variants, on the latest — Try now

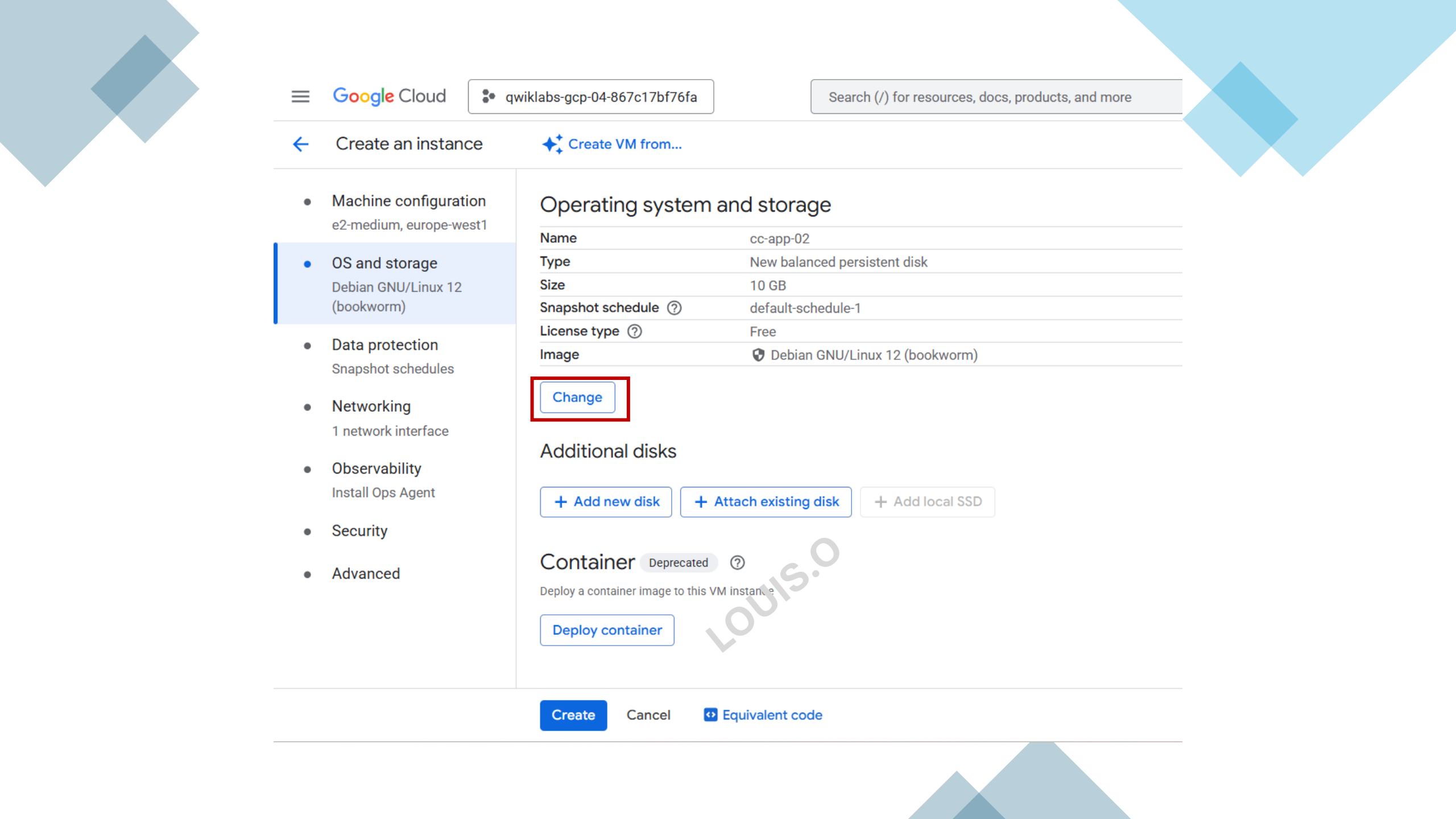
General purpose | Compute optimized | Memory optimized | Storage optimized | GPUs

Machine types for common workloads, optimized for cost and flexibility

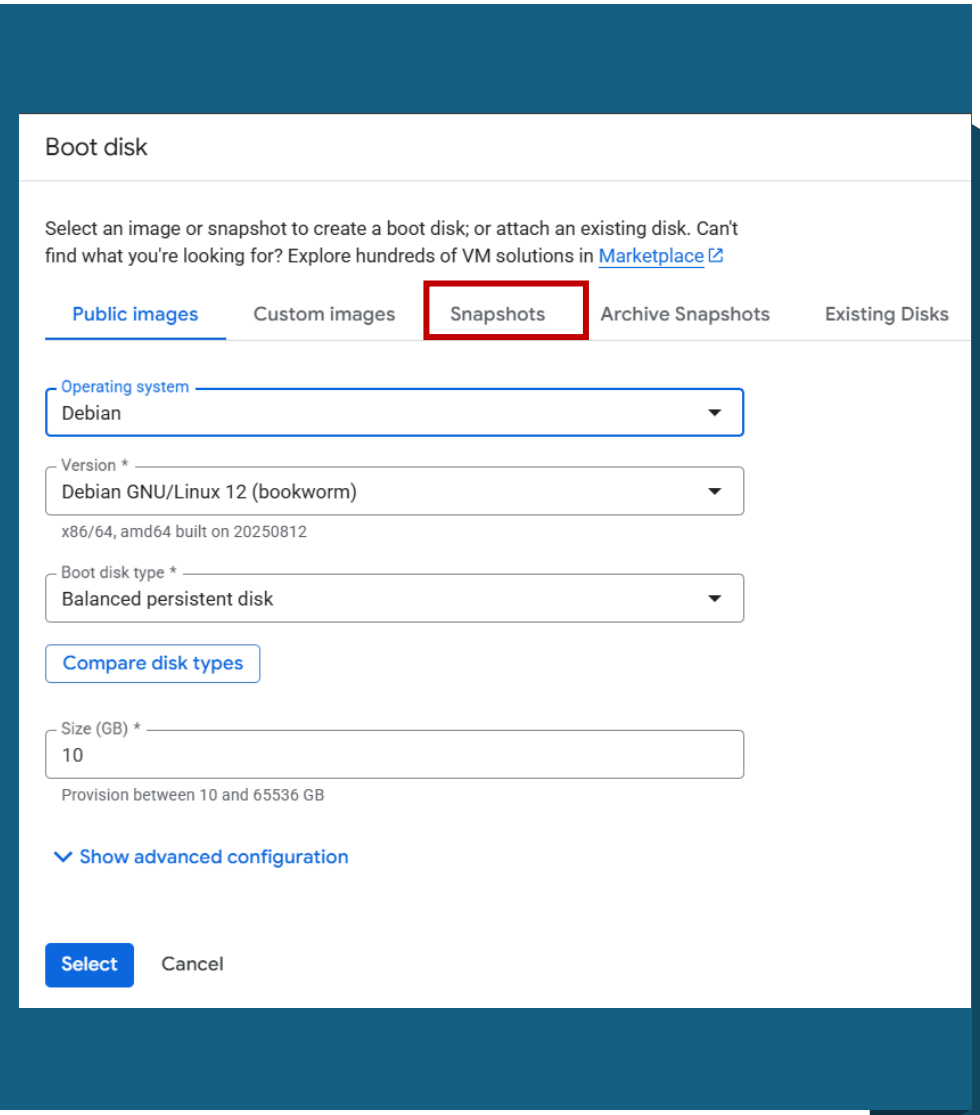
Series	Description	vCPUs	Memory	CPU Platfor

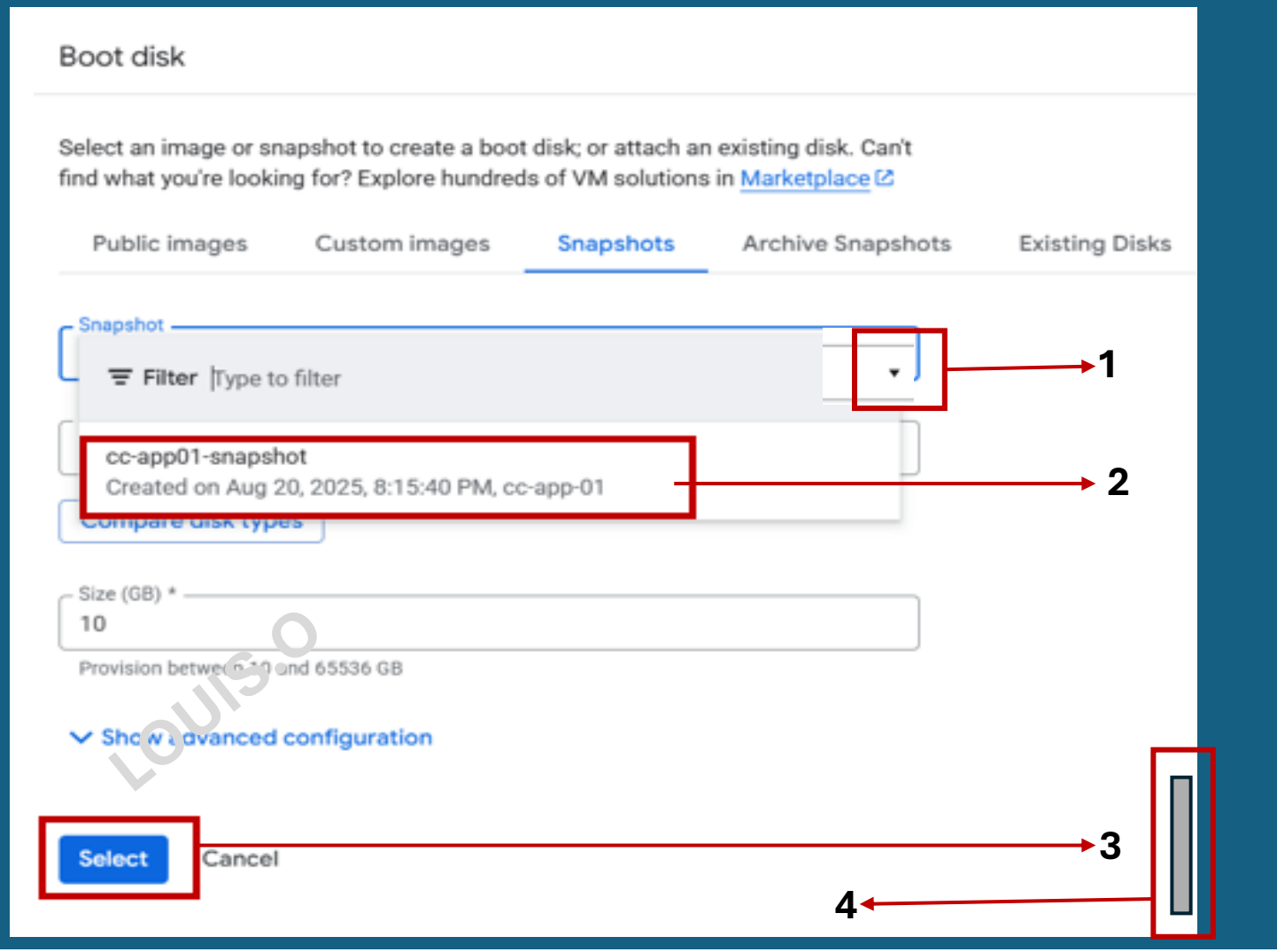
In the **machine Type section** select **Shared-Core** and select **e2-medium,** click **OS and Storage**



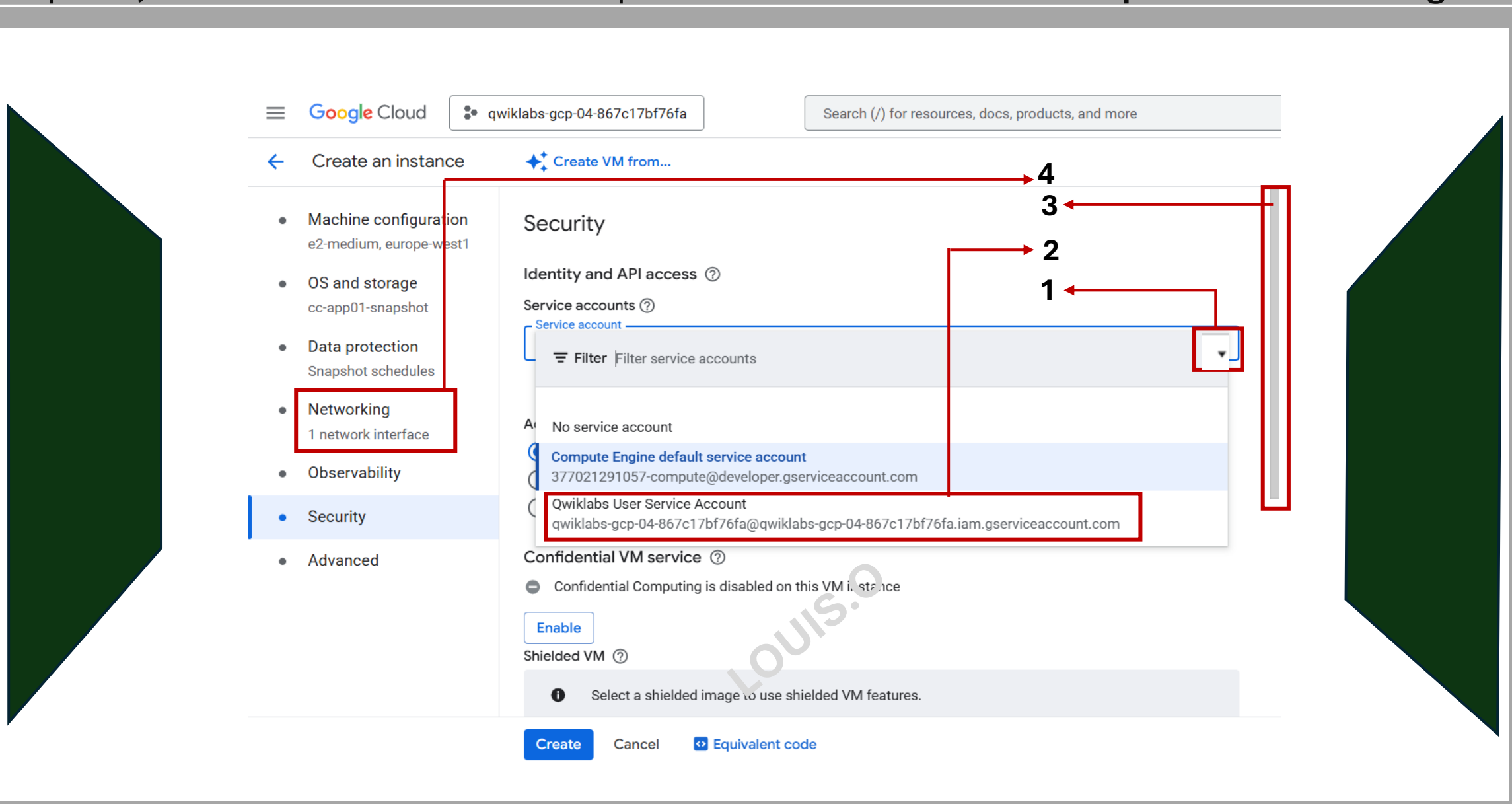

Google Cloud
qwiklabs-gcp-04-867c17bf76fa
Search (/) for resources, docs, products, and more
Create an instance
Create VM from...
Machine configuration
e2-medium, europe-west1
OS and storage
Debian GNU/Linux 12 (bookworm)
Data protection
Snapshot schedules
Networking
1 network interface
Observability
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
LOUIS.O
Create
Cancel
Equivalent code

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

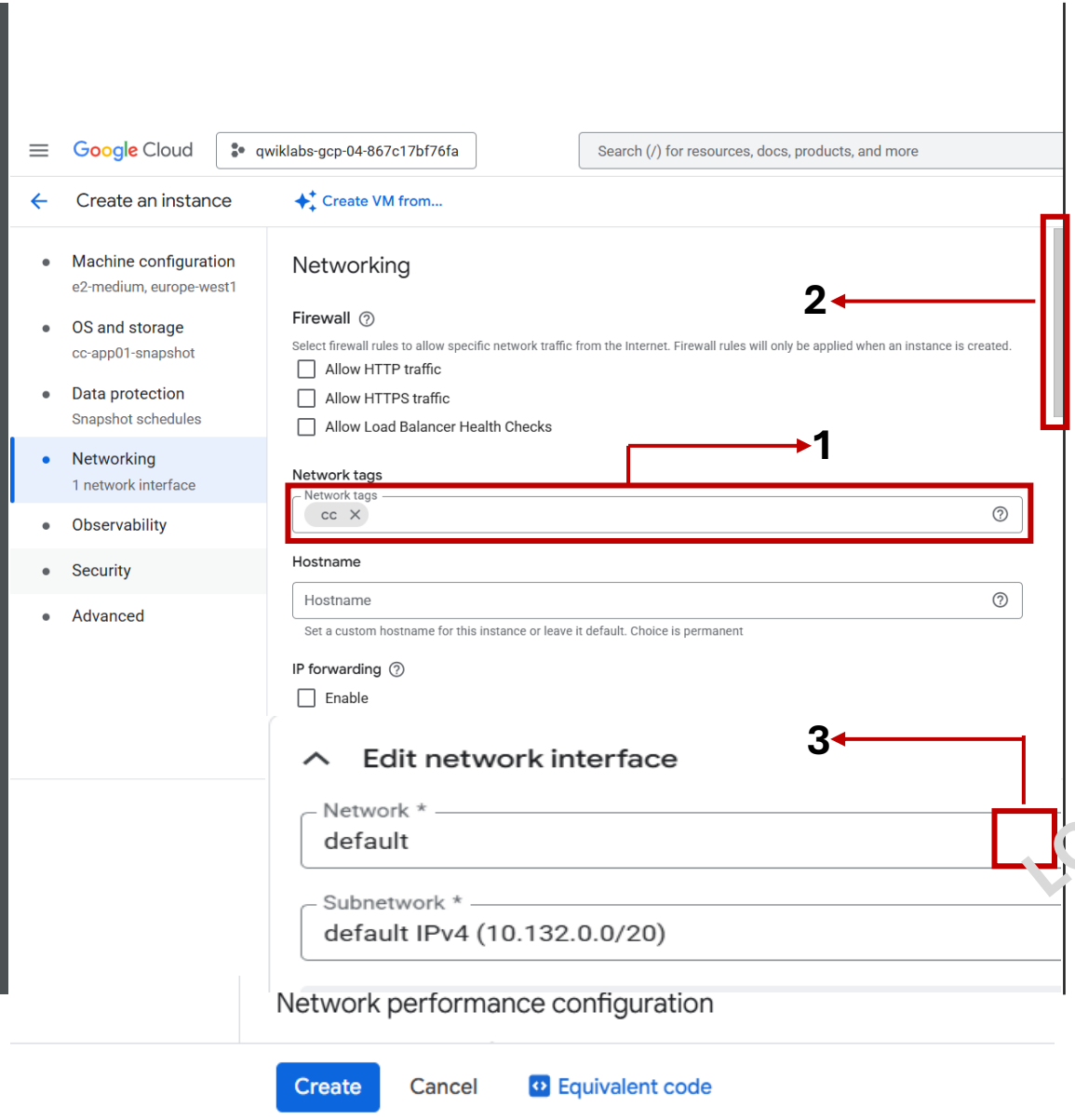




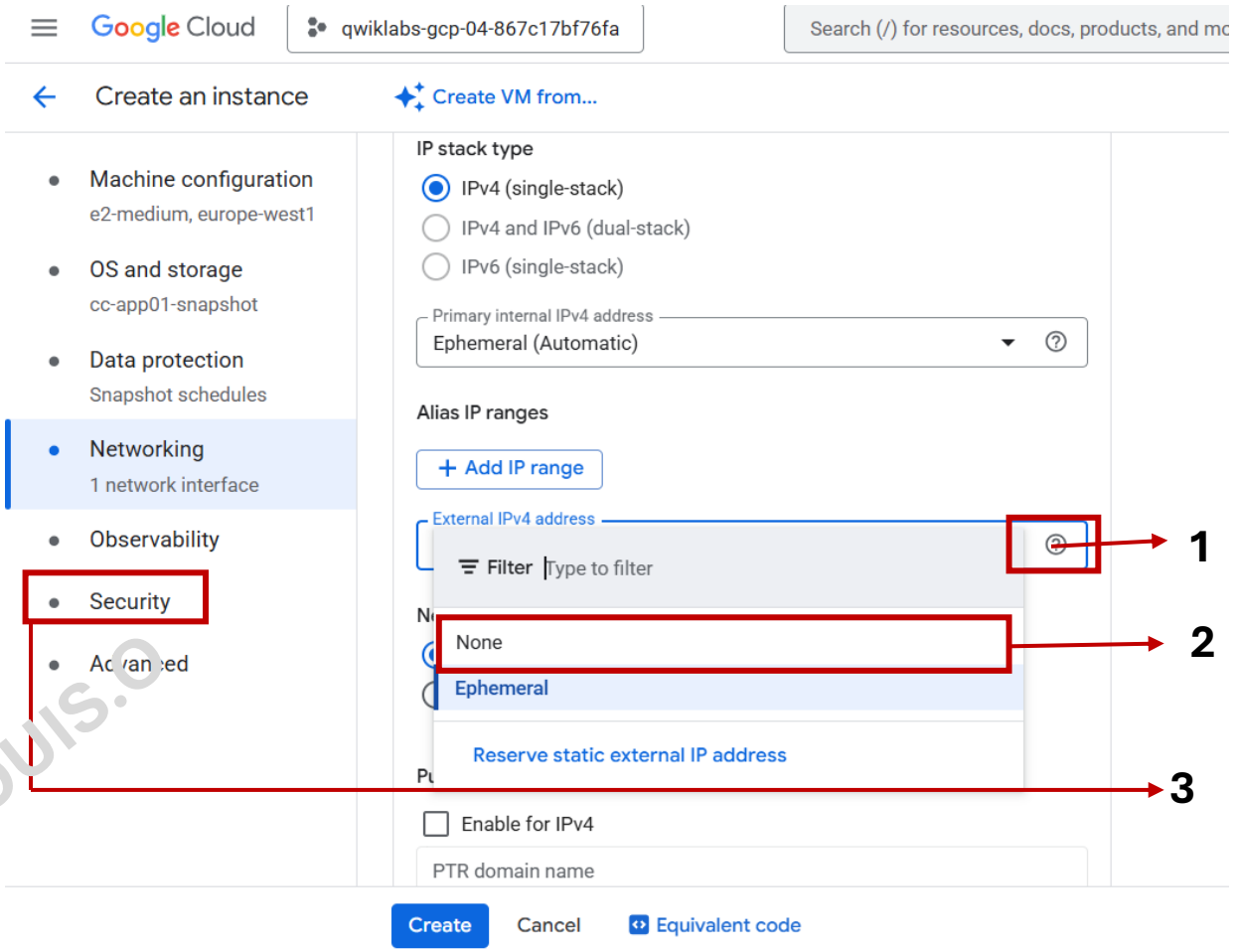
After step **1&2,** Scroll-down and select the drop-down at the front of **Advance Options** & **Networking Section**

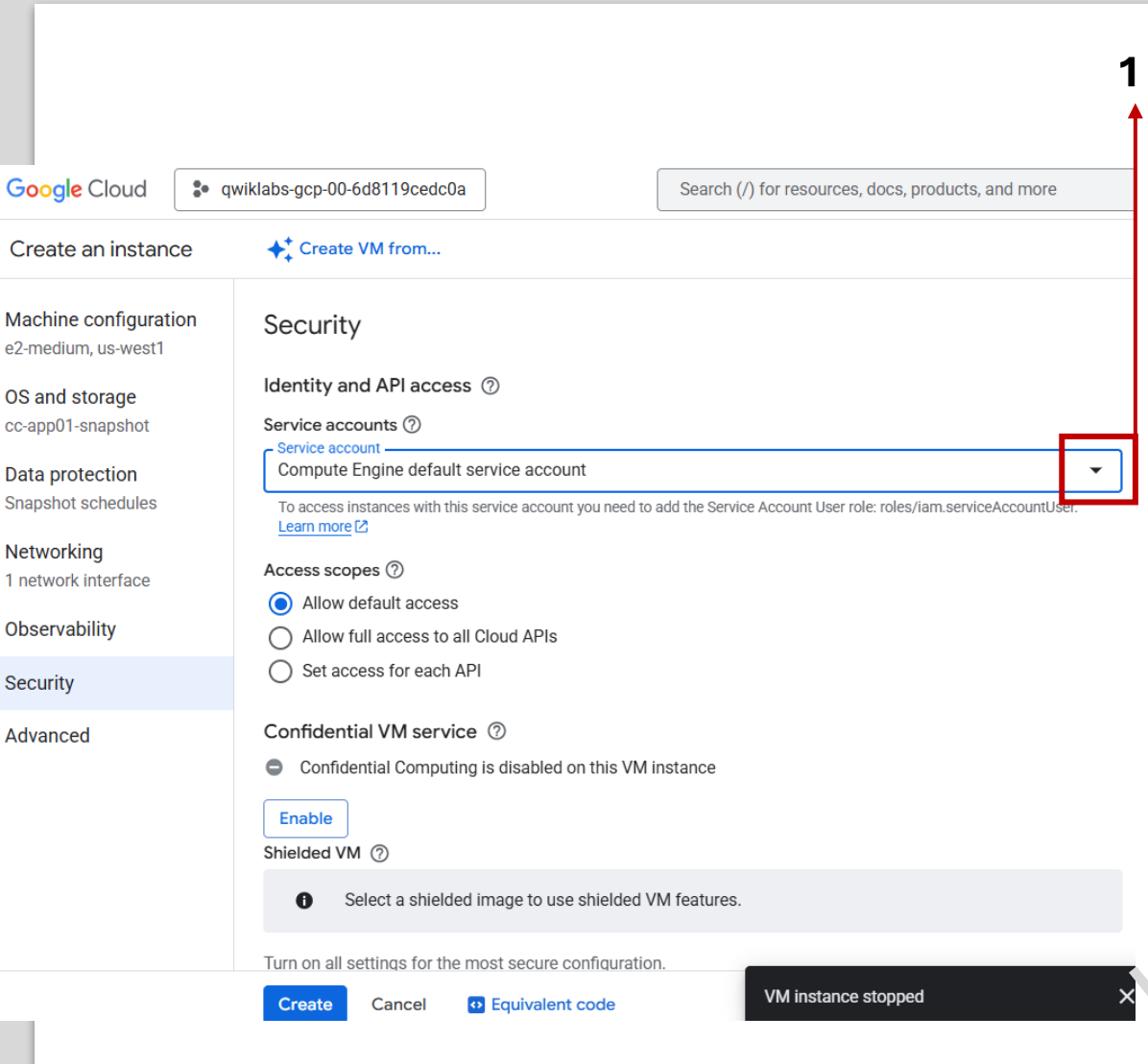


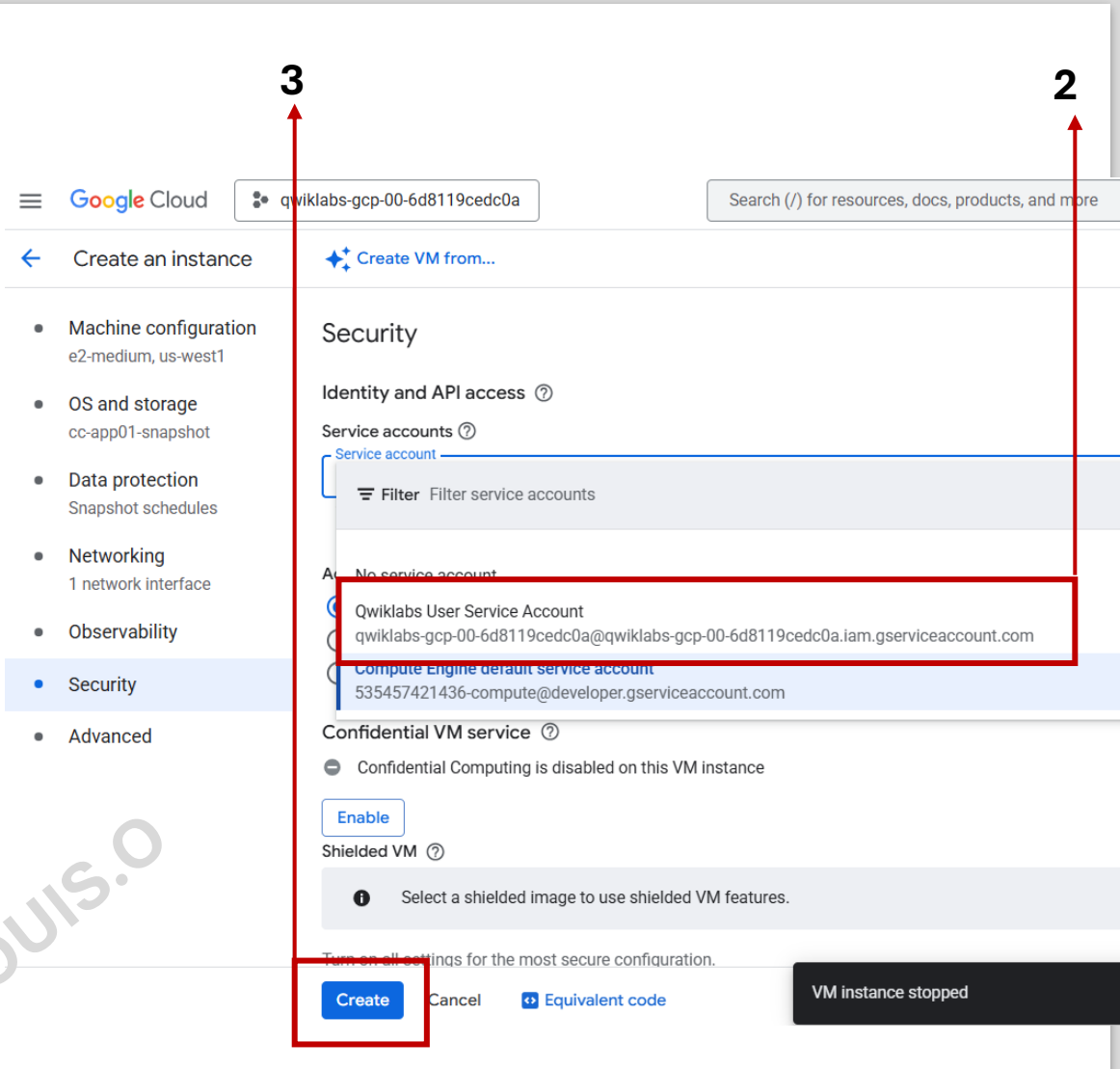
After entry “cc” scroll-down to **Network interfaces** section, click the drop-down & select **default** network



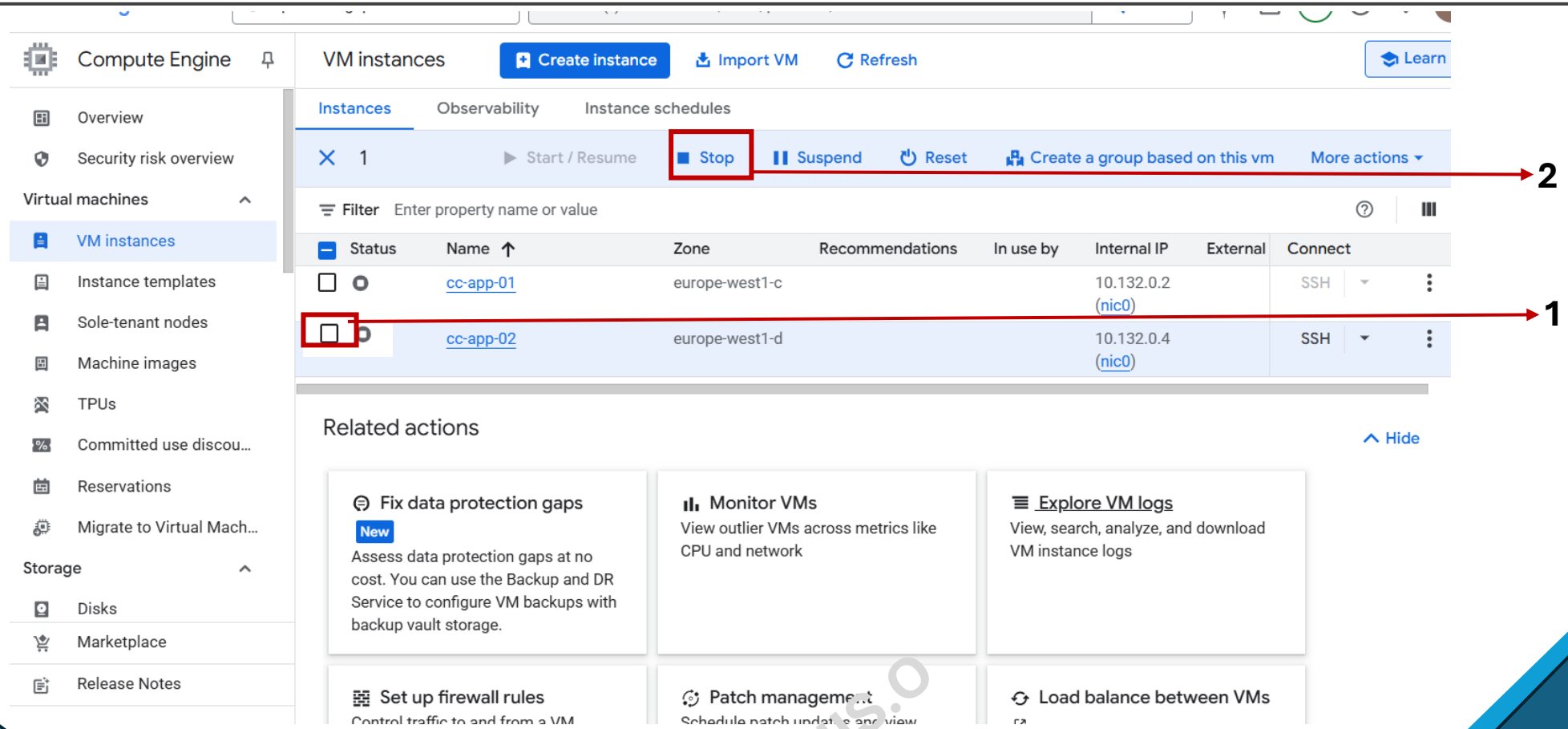
In the **External IPV4 address Section** Click the **Drop-down** Select **None** & **Create**

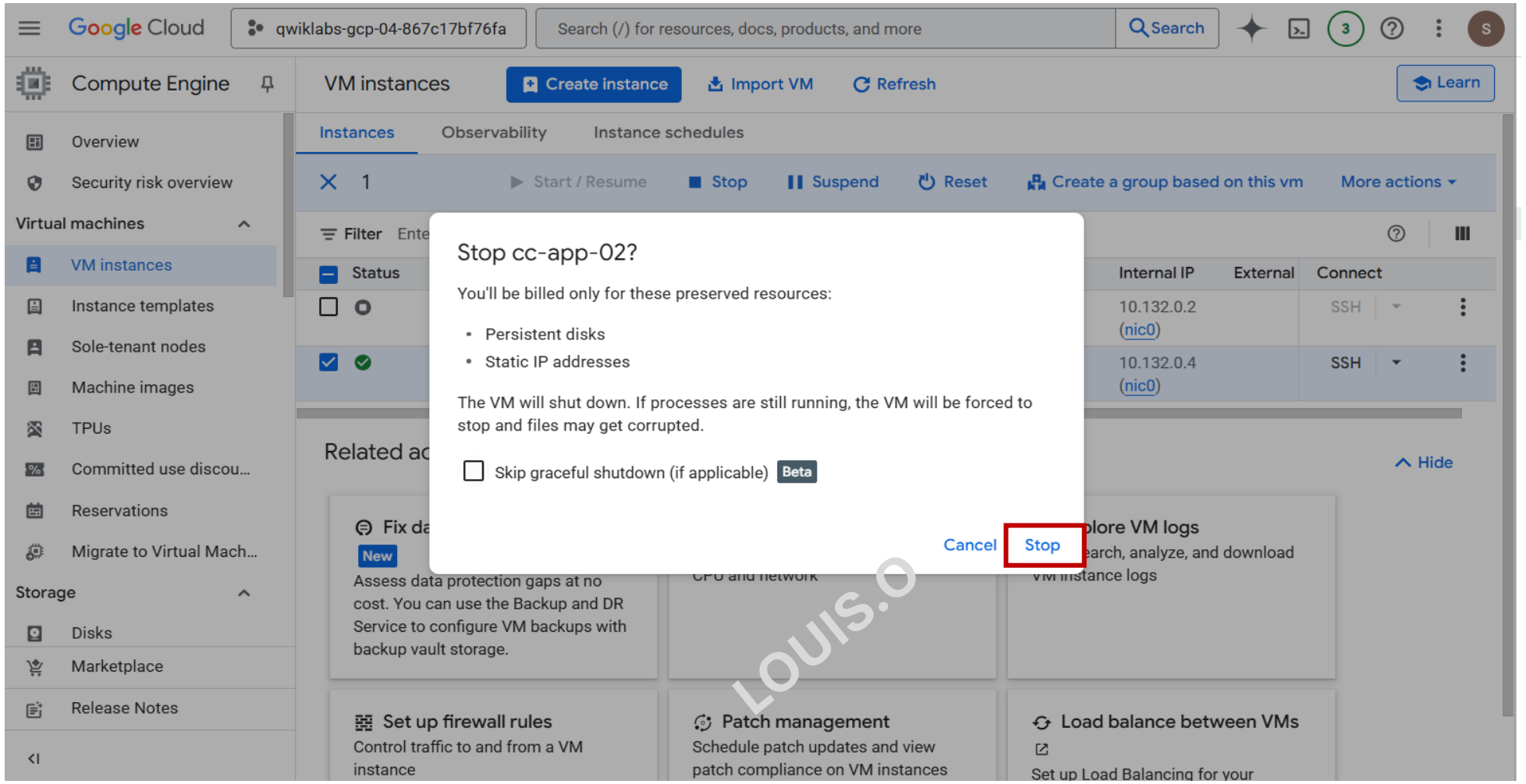


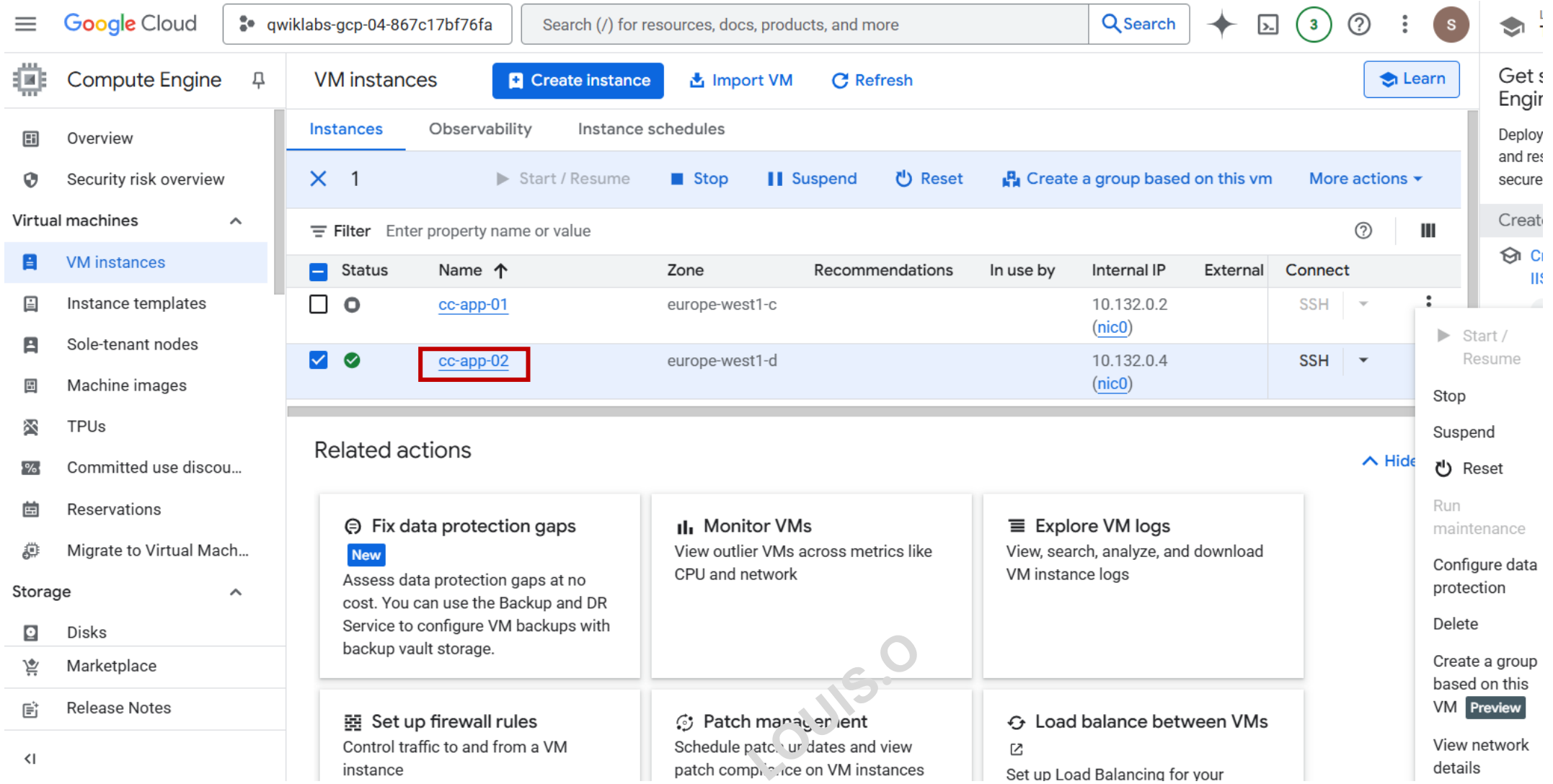

1
Google Cloud
qwiklabs-gcp-00-6d8119cedc0a
Search (/) for resources, docs, products, and more
Create an instance
Create VM from...
Machine configuration
e2-medium, us-west1
OS and storage
cc-app01-snapshot
Data protection
Snapshot schedules
Networking
1 network interface
Observability
Security
Advanced
Security
Identity and API access
Service accounts
Service account
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

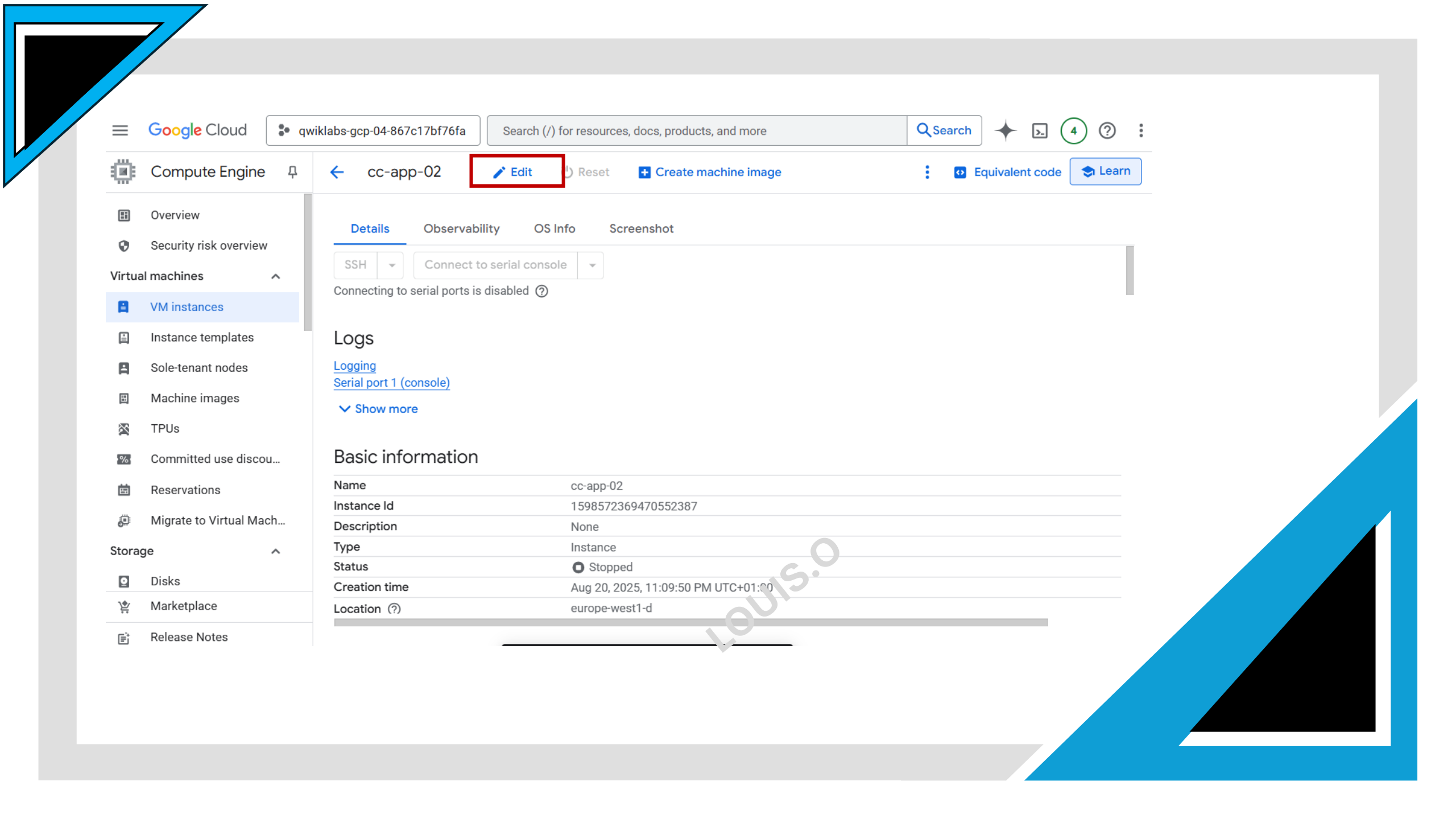

3
2
Google Cloud
qwiklabs-gcp-00-6d8119cedc0a
Search (/) for resources, docs, products, and more
Create an instance
Create VM from...
Machine configuration
e2-medium, us-west1
OS and storage
cc-app01-snapshot
Data protection
Snapshot schedules
Networking
1 network interface
Observability
Security
Advanced
Security
Identity and API access
Service accounts
Service account
Filter
Filter service accounts
No service account
Qwiklabs User Service Account
qwiklabs-gcp-00-6d8119cedc0a@qwiklabs-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.
Create
Cancel
Equivalent code
VM instance stopped

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

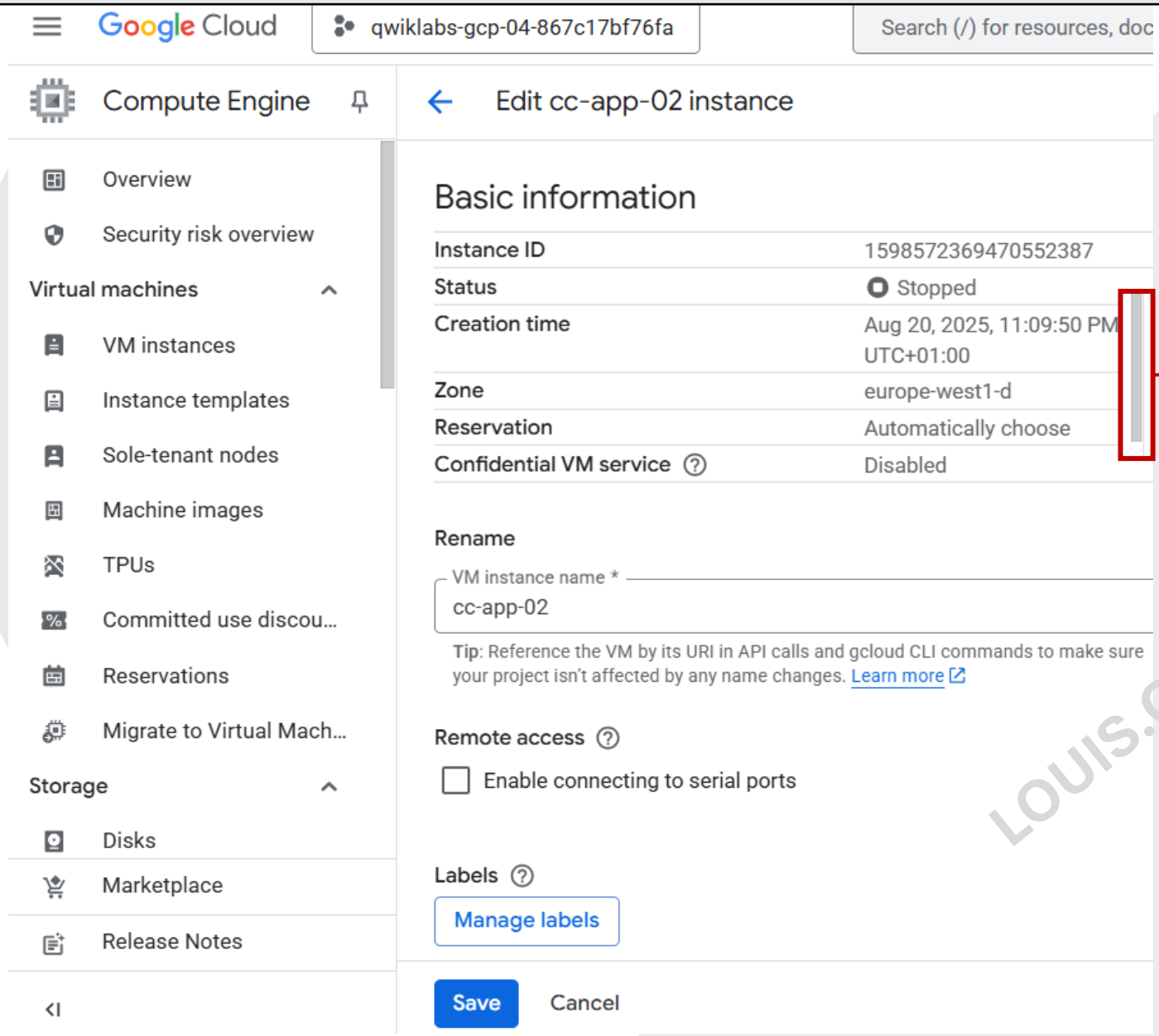


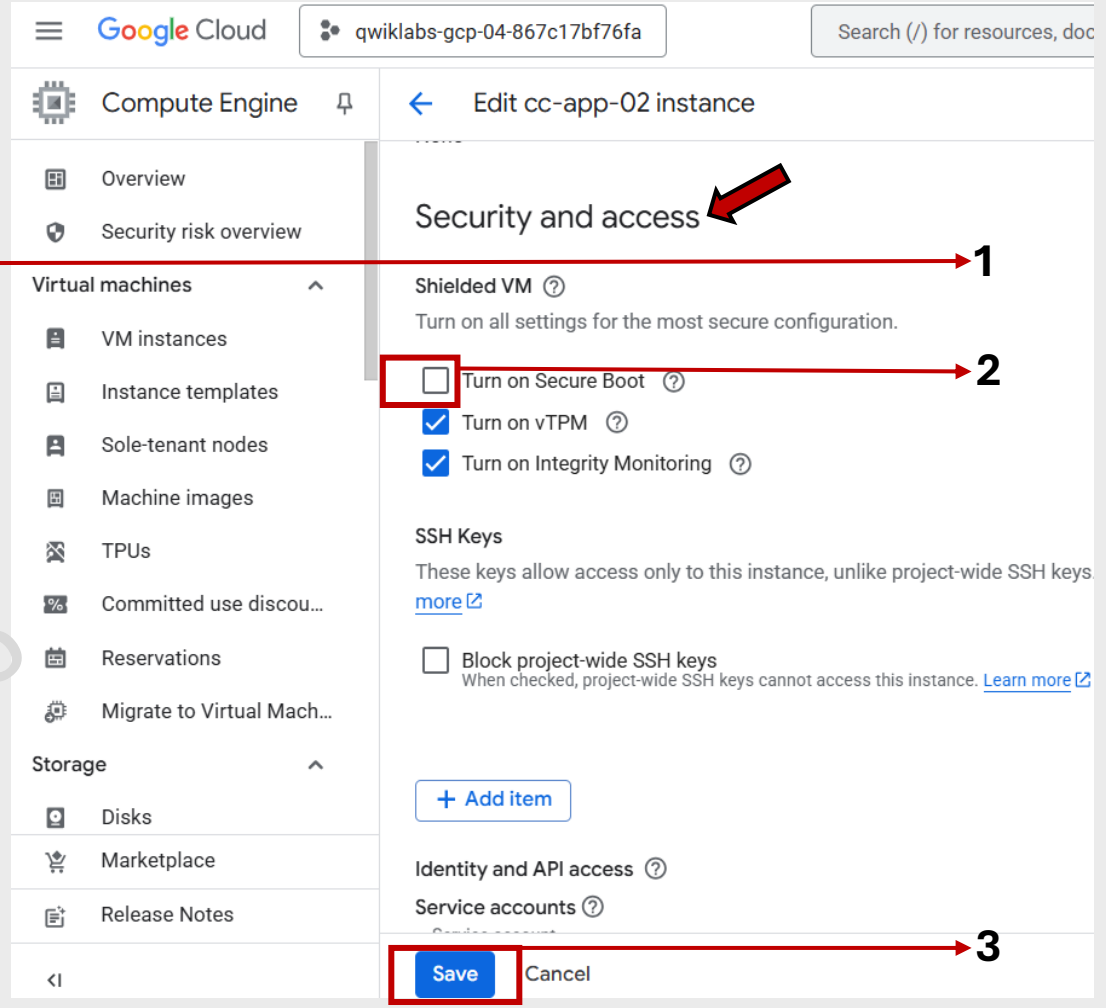

Google Cloud
qwiklabs-gcp-04-867c17bf76fa
Search (/) for resources, docs, products, and more
Search
Compute Engine
VM instances
Create instance
Import VM
Refresh
Learn
Overview
Security risk overview
Virtual machines
VM instances
Instance templates
Sole-tenant nodes
Machine images
TPUs
Committed use 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
Status
Internal IP
External
Connect
10.132.0.2 (nic0)
SSH
10.132.0.4 (nic0)
SSH
Hide
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
New
Assess data protection gaps at no cost. You can use the Backup and DR Service to configure VM backups with 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
LOUIS.O

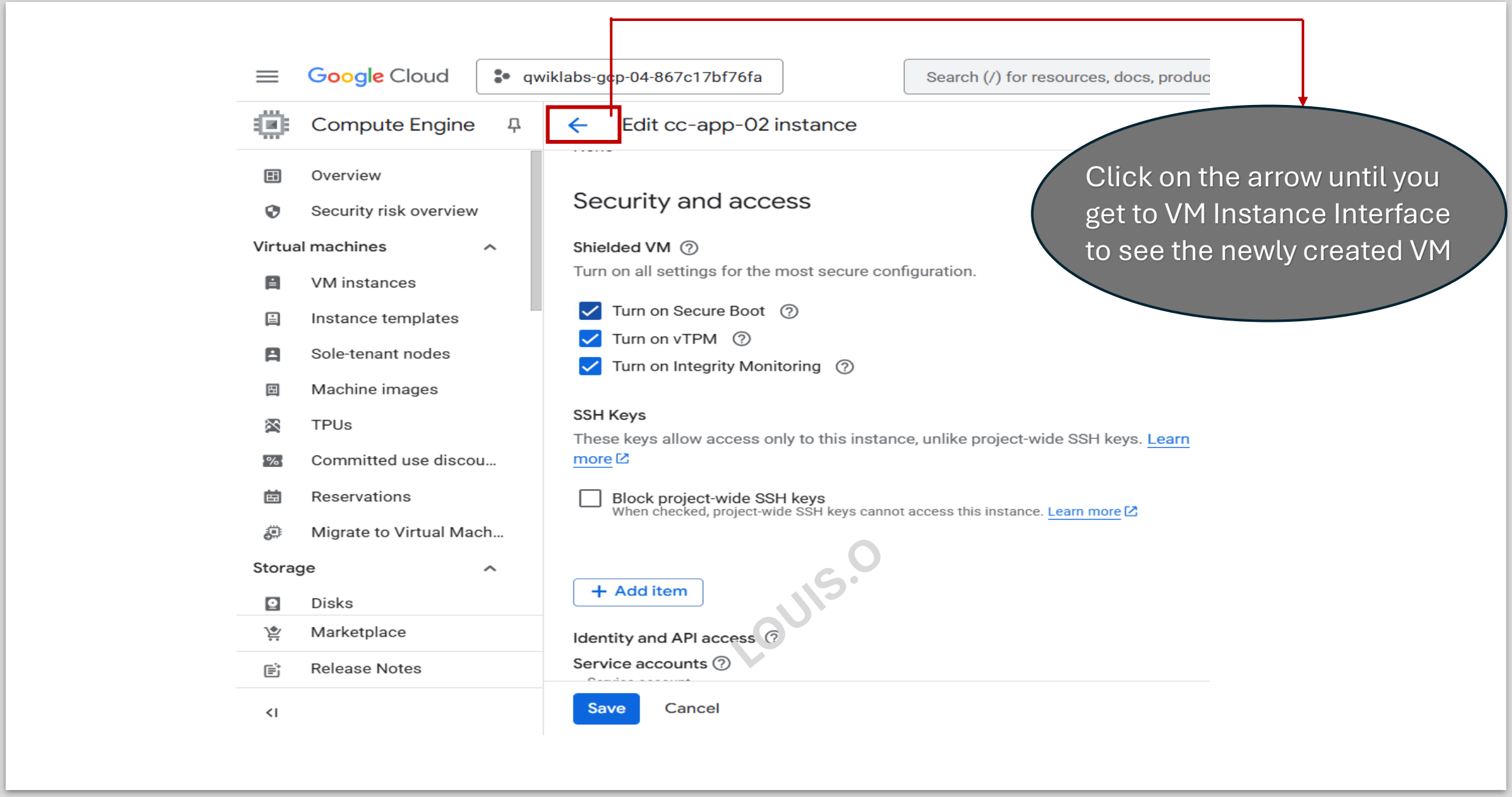

Google Cloud
qwiklabs-gcp-04-867c17bf76fa
Search (/) for resources, docs, products, and more
Search
Compute Engine
VM instances
Create instance
Import VM
Refresh
Learn
Overview
Security risk overview
Virtual machines
VM instances
Instance templates
Sole-tenant nodes
Machine images
TPUs
Committed use 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
cc-app-01
europe-west1-c
10.132.0.2 (nic0)
SSH
cc-app-02
europe-west1-d
10.132.0.4 (nic0)
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
Start / Resume
Stop
Suspend
Reset
Run maintenance
Configure data protection
Delete
Create a group based on this VM
Preview
View network details


Google Cloud
qwiklabs-gcp-04-867c17bf76fa
Search (/) for resources, docs, products, and more
Search
Compute Engine
cc-app-02
Edit
Reset
Create machine image
Equivalent code
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
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
europe-west1-d
LOUIS.O

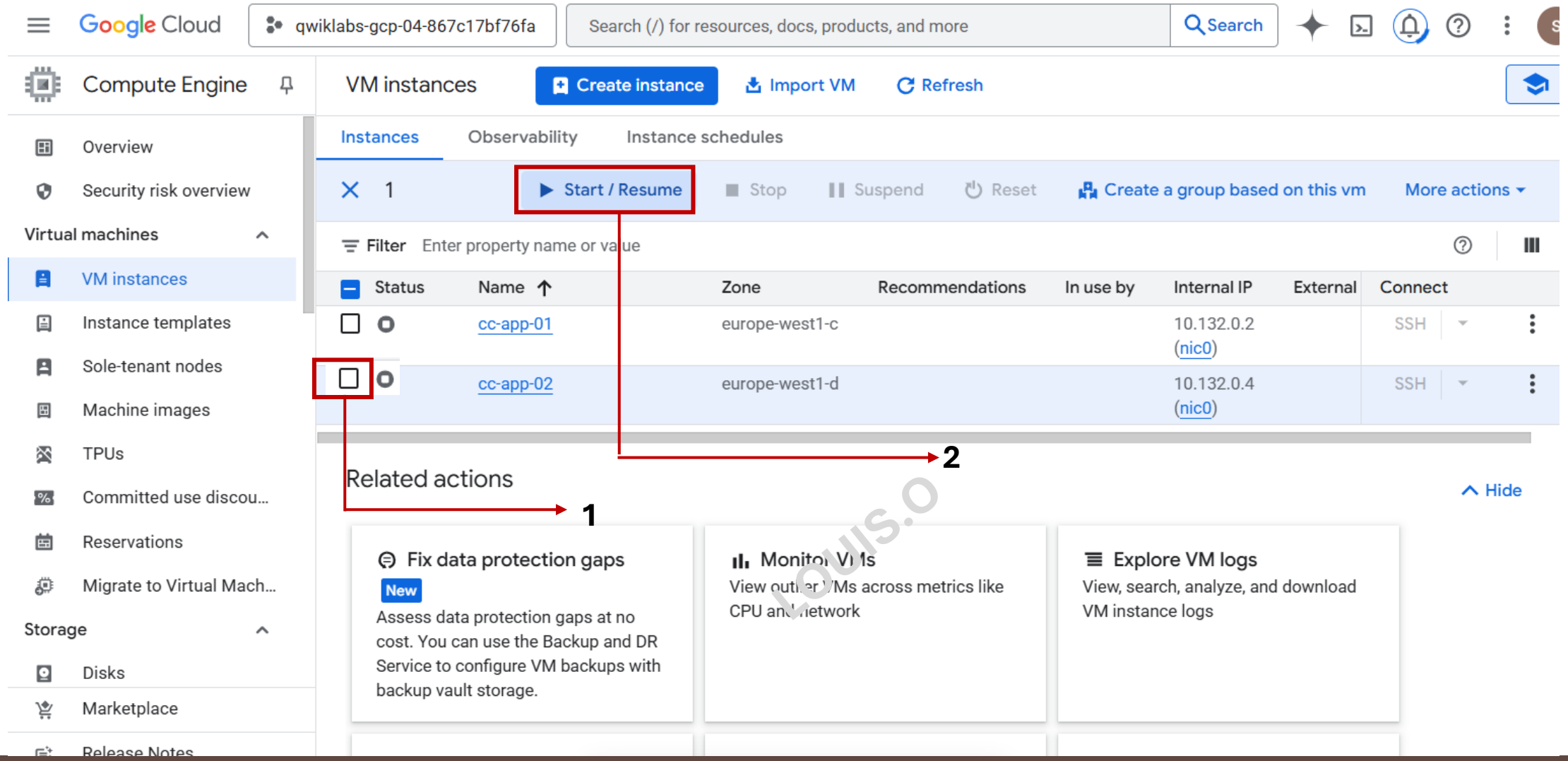
Scroll down to **Security and Access** section, select **checkbox** and click **Save**

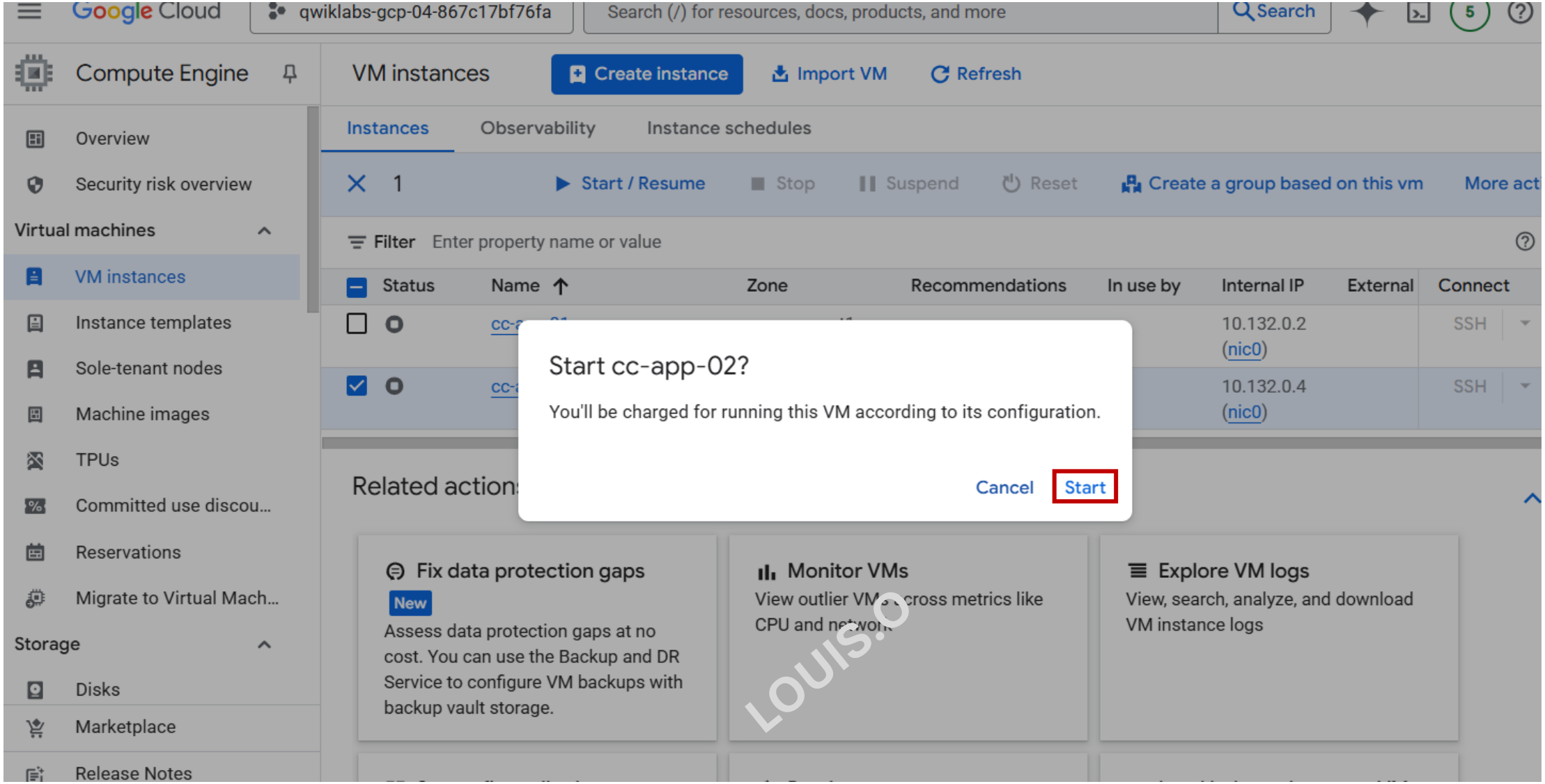




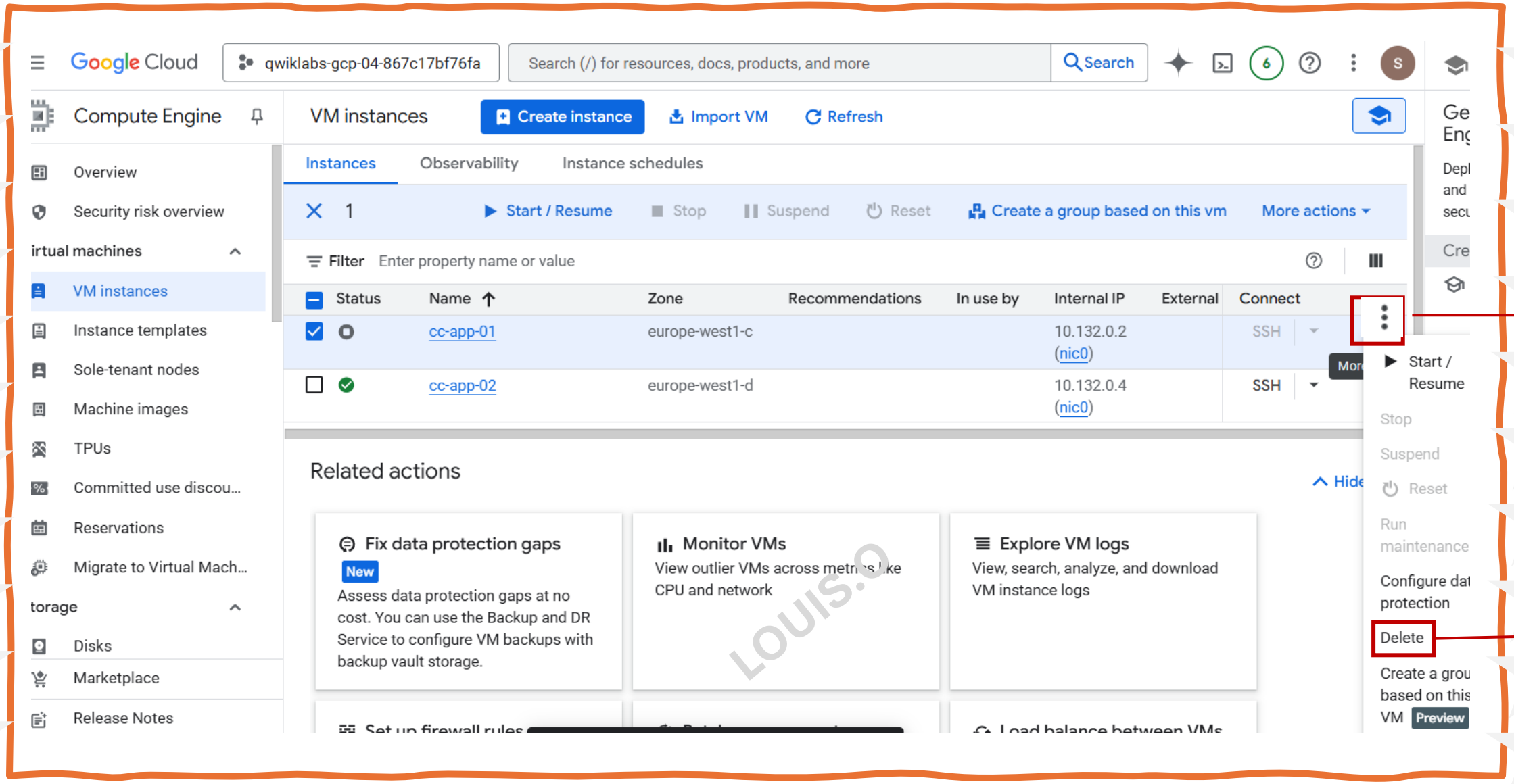

Google Cloud
qwiklabs-gcp-04-867c17bf76fa
Search (/) for resources, docs, produc
Compute Engine
Edit cc-app-02 instance
Overview
Security risk overview
Virtual machines
VM instances
Instance templates
Sole-tenant nodes
Machine images
TPUs
Committed use discou...
Reservations
Migrate to Virtual Mach...
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
LOUIS.O

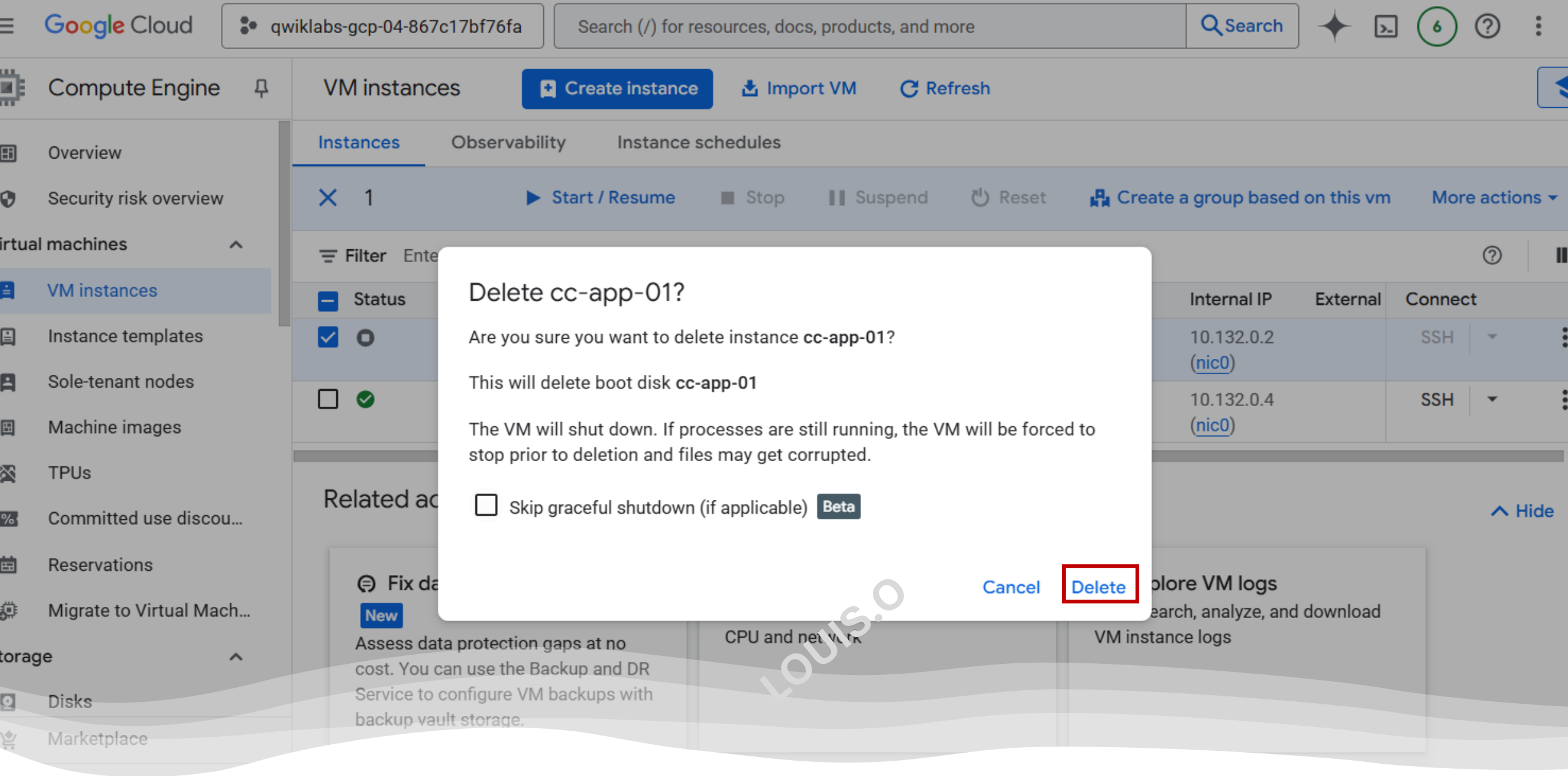
In the **Compute Engine** menu, select **VM Instance**, Select the checkbox for the **cc-app-02**, and click **Start/ Resume**

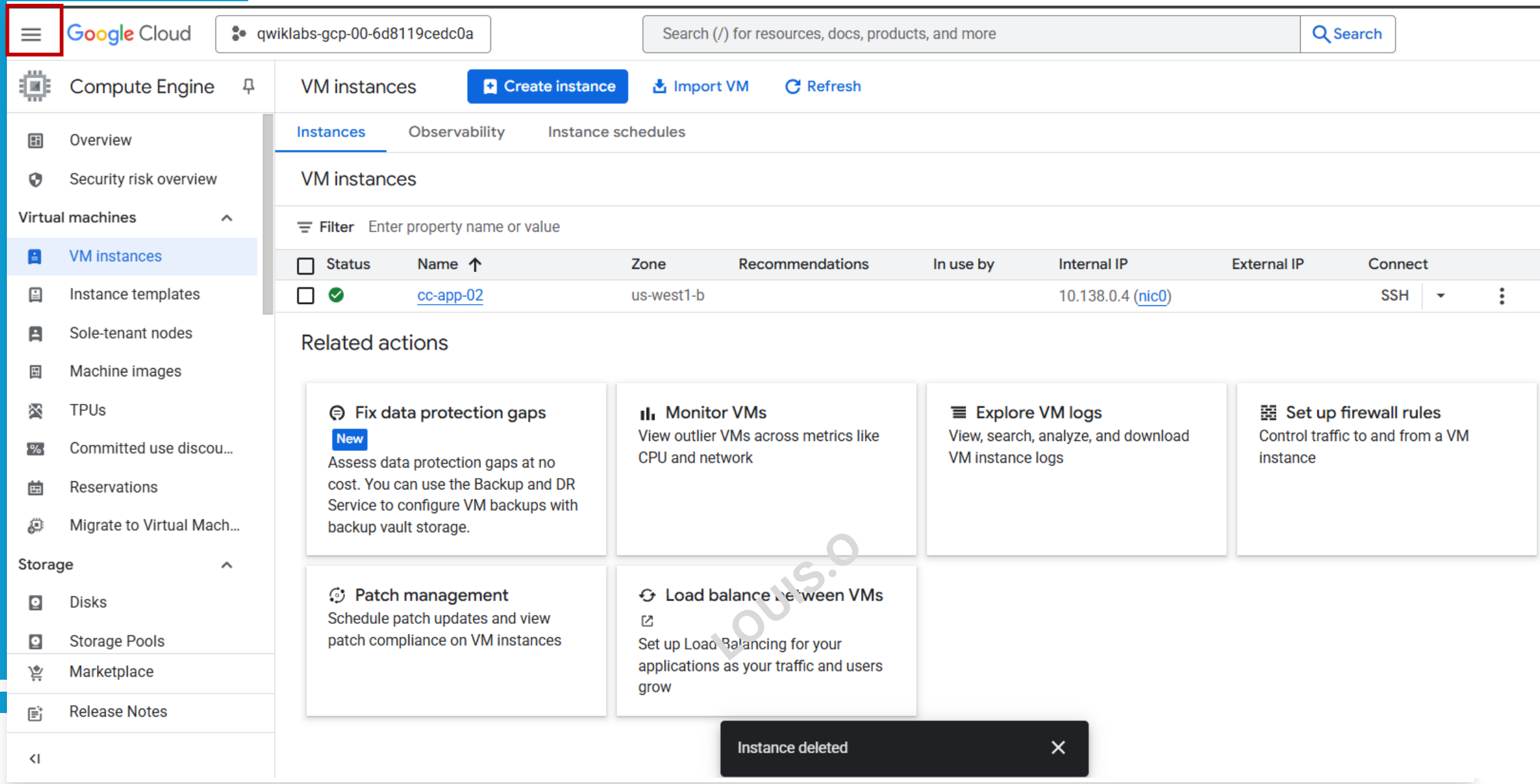



Google Cloud
qwiklabs-gcp-04-867c17bf76fa
Search (/) for resources, docs, products, and more
Search
Compute Engine
VM instances
Create instance
Import VM
Refresh
Overview
Security risk overview
Virtual machines
VM instances
Instance templates
Sole-tenant nodes
Machine images
TPUs
Committed use discou...
Reservations
Migrate to Virtual Mach...
Storage
Disks
Marketplace
Release Notes
Instances
Observability
Instance schedules
1
Start / Resume
Stop
Suspend
Reset
Create a group based on this vm
More act
Filter
Enter property name or value
Status
Name
Zone
Recommendations
In use by
Internal IP
External
Connect
10.132.0.2 (nic0)
SSH
10.132.0.4 (nic0)
SSH
Start cc-app-02?
You'll be charged for running this VM according to its configuration.
Cancel
Start
Related action
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

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

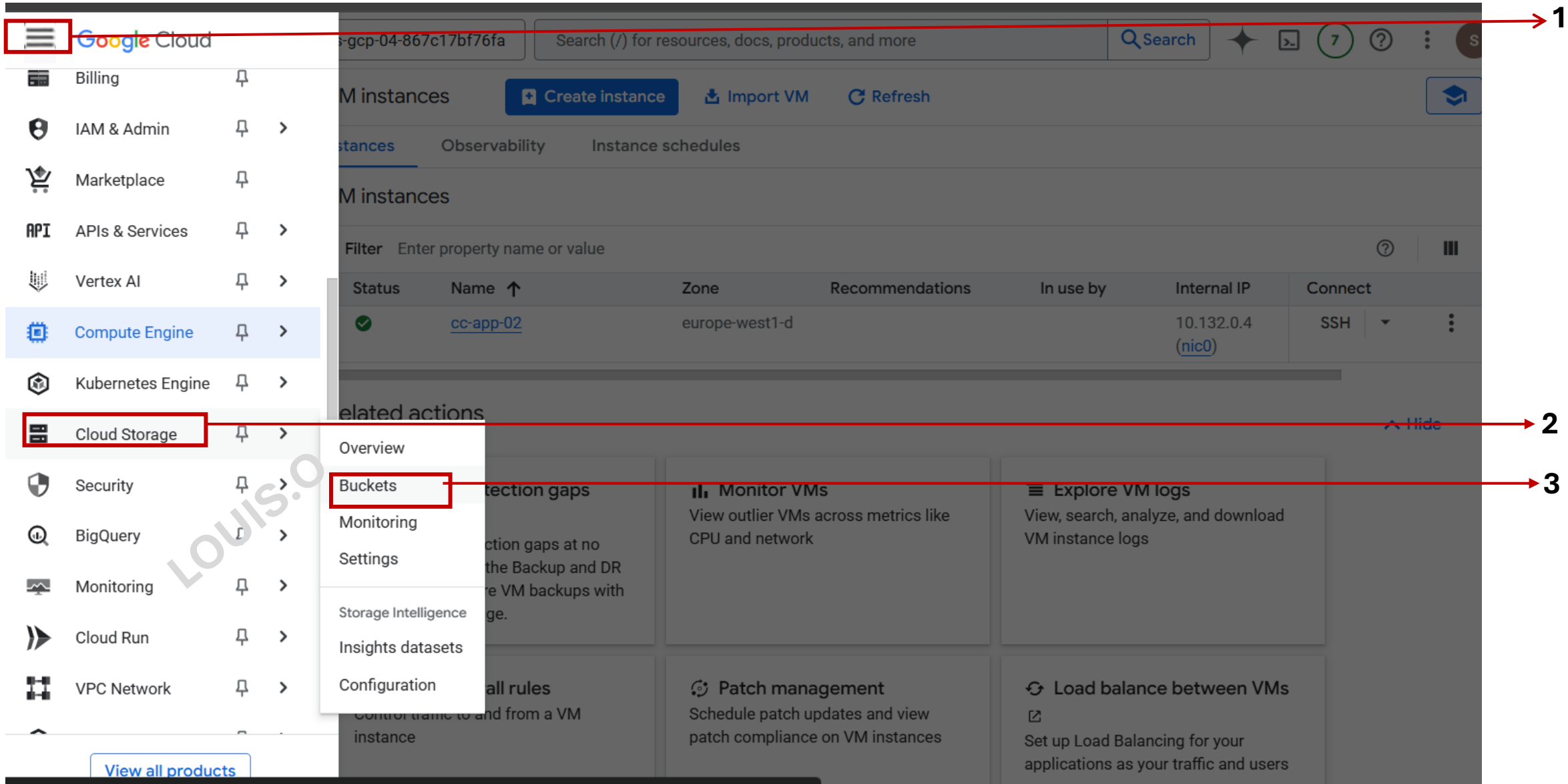


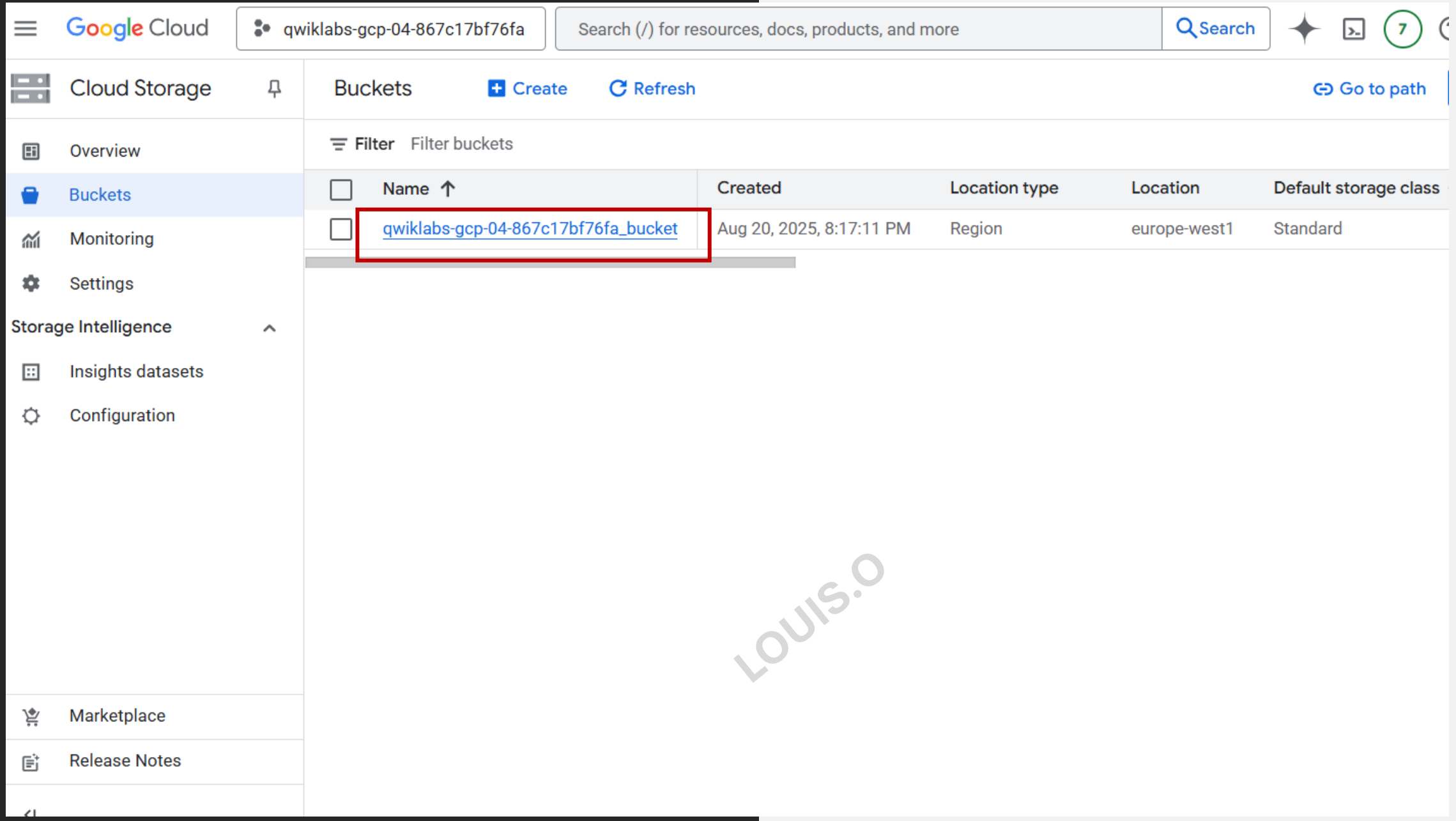

Google Cloud
qwiklabs-gcp-04-867c17bf76fa
Search (/) for resources, docs, products, and more
Search
Compute Engine
VM instances
Create instance
Import VM
Refresh
Instances
Observability
Instance schedules
Start / Resume
Stop
Suspend
Reset
Create a group based on this vm
More actions
Filter
Status
Internal IP
External
Connect
10.132.0.2 (nic0)
SSH
10.132.0.4 (nic0)
SSH
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
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 ac
Hide
Fix da
New
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 net
lore VM logs
earch, analyze, and download VM instance logs
LOUIS.O

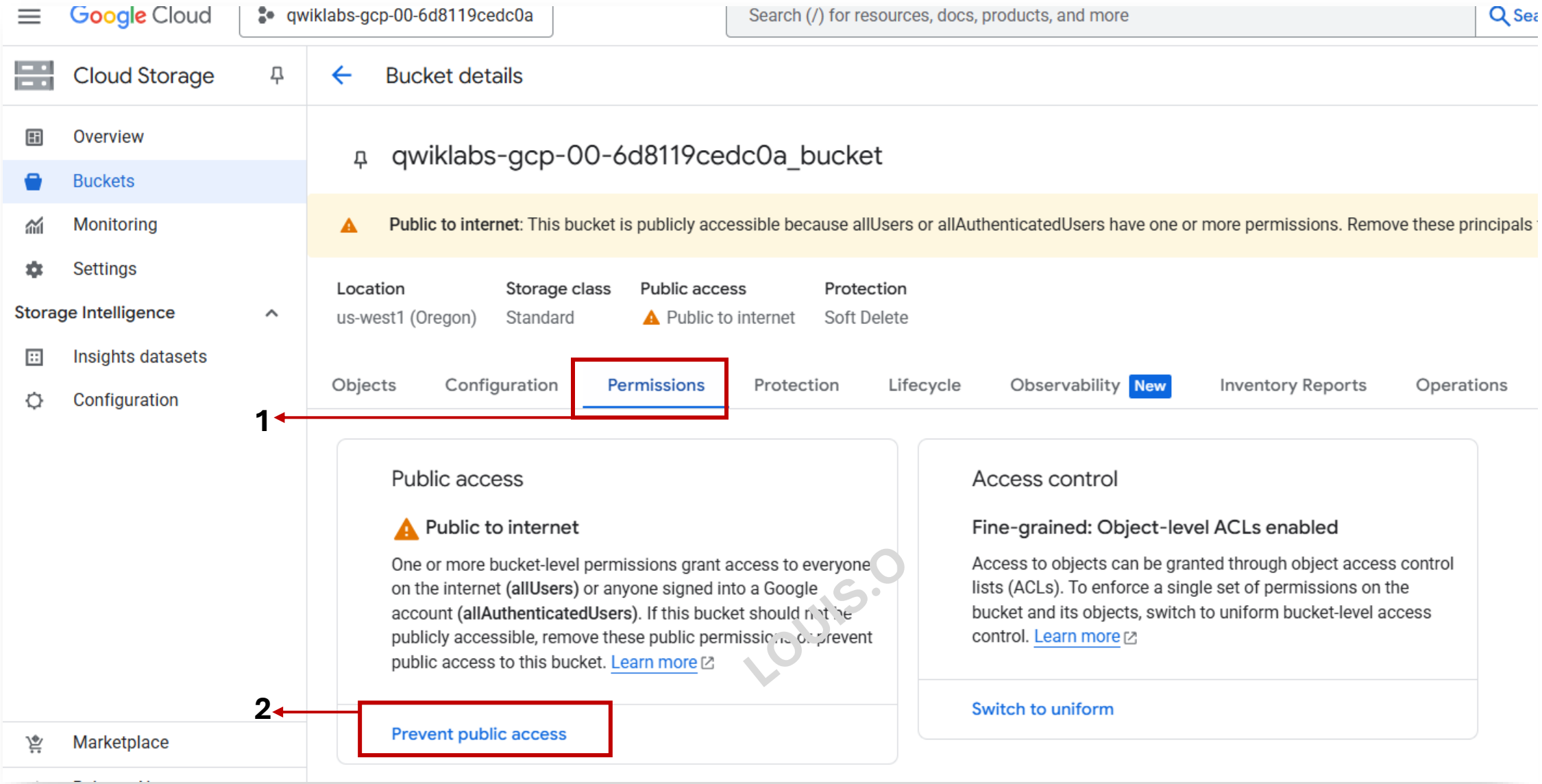

Google Cloud
qwiklabs-gcp-00-6d8119cedc0a
Search (/) for resources, docs, products, and more
Search
Compute Engine
VM instances
Create instance
Import VM
Refresh
Overview
Security risk overview
Virtual machines
VM instances
Instance templates
Sole-tenant nodes
Machine images
TPUs
Committed use discou...
Reservations
Migrate to Virtual Mach...
Storage
Disks
Storage Pools
Marketplace
Release Notes
Instances
Observability
Instance schedules
VM instances
Filter
Enter property name or value
Status
Name
Zone
Recommendations
In use by
Internal IP
External IP
Connect
cc-app-02
us-west1-b
10.138.0.4 (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 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

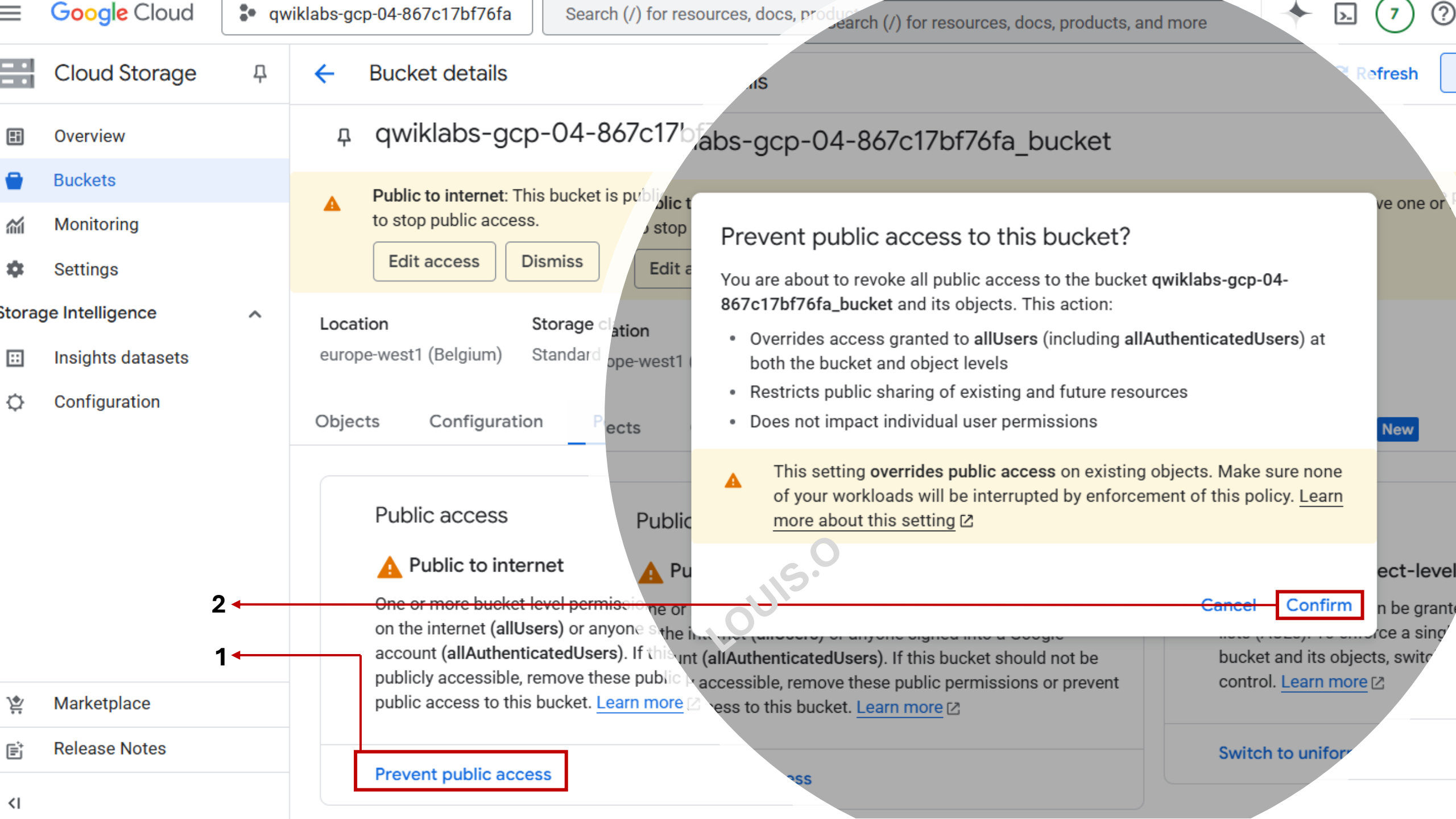
Task 3. Fix Cloud Storage Bucket Permissions

In the **Navigation menu (☰),** select **Cloud Storage >Buckets**. The Buckets page opens. Click the **qwiklabs-gcp-02-71bb6bcdc399_bucket** storage bucket link. The Bucket details page opens

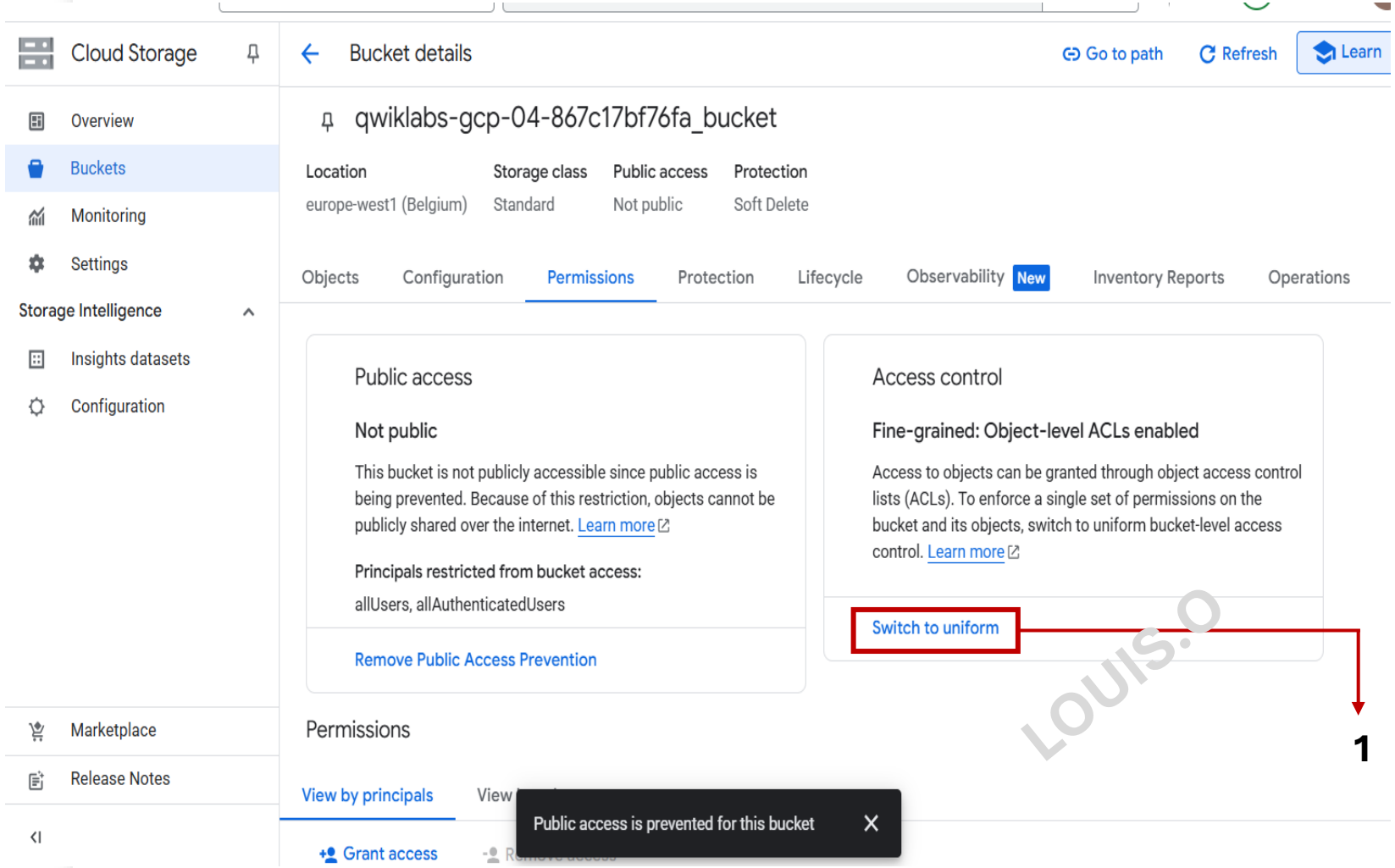


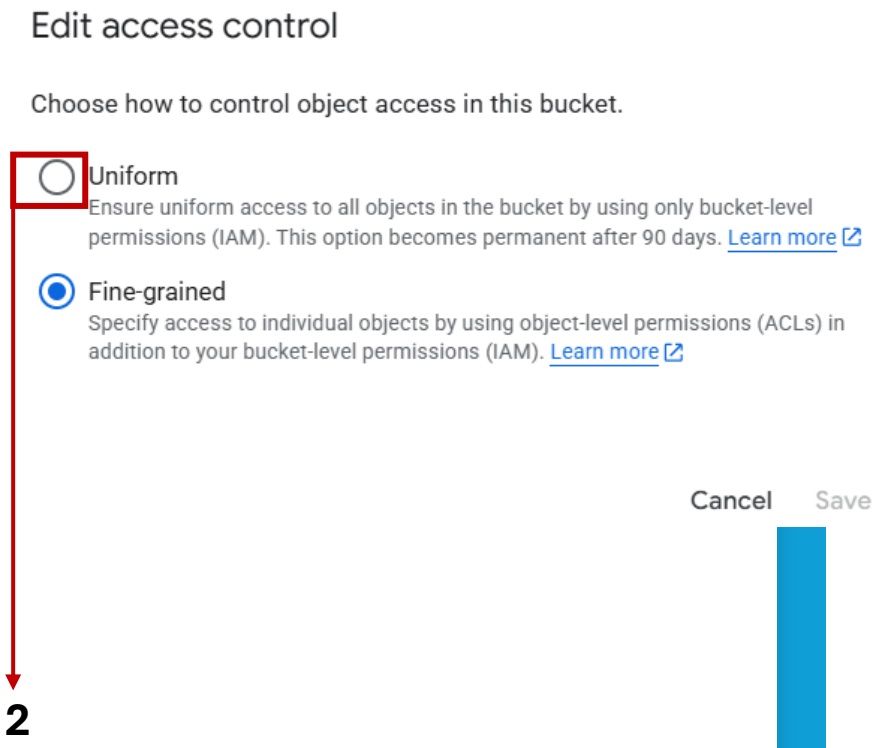

Google Cloud
qwiklabs-gcp-04-867c17bf76fa
Search (/) for resources, docs, products, and more
Search
7
Cloud Storage
Buckets
Create
Refresh
Go to path
Overview
Buckets
Monitoring
Settings
Storage Intelligence
Insights datasets
Configuration
Filter
Filter buckets
Name
Created
Location type
Location
Default storage class
qwiklabs-gcp-04-867c17bf76fa_bucket
Aug 20, 2025, 8:17:11 PM
Region
europe-west1
Standard
Marketplace
Release Notes
LOUIS.O

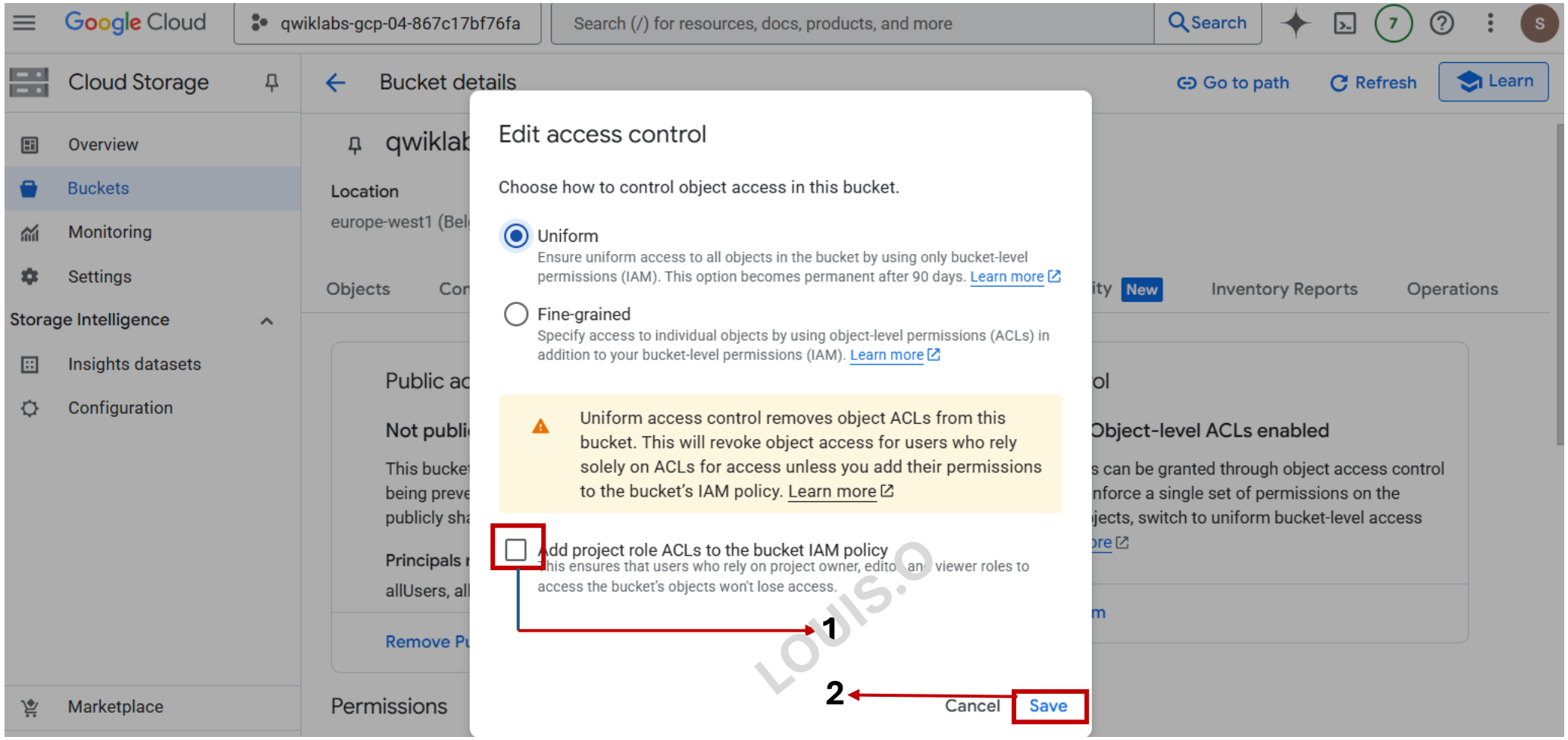

Google Cloud
qwiklabs-gcp-00-6d8119cedc0a
Search (/) for resources, docs, products, and more
Cloud Storage
Overview
Buckets
Monitoring
Settings
Storage Intelligence
Insights datasets
Configuration
Marketplace
Bucket details
qwiklabs-gcp-00-6d8119cedc0a_bucket
Public to internet: This bucket is publicly accessible because allUsers or allAuthenticatedUsers have one or more permissions. Remove these principals
Location
us-west1 (Oregon)
Storage class
Standard
Public access
Public to internet
Protection
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 to 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

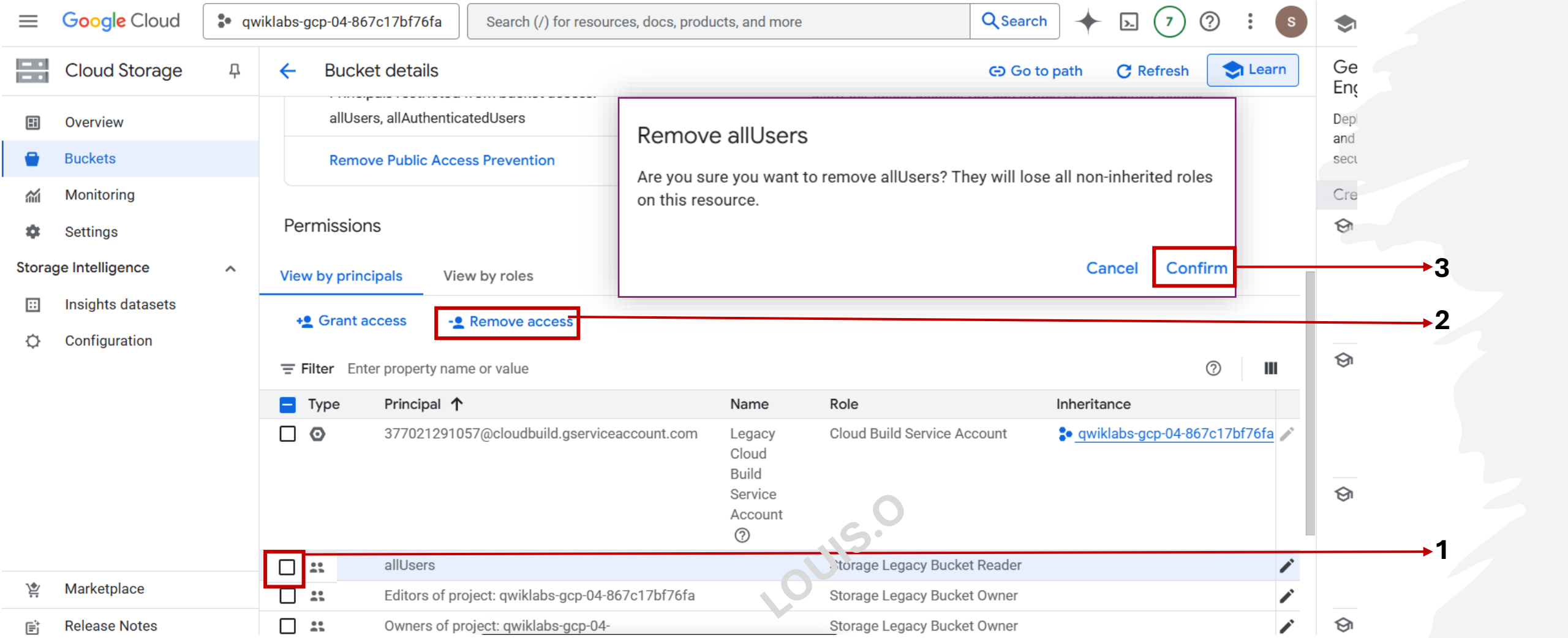

Google Cloud
qwiklabs-gcp-04-867c17bf76fa
Search (/) for resources, docs, products, and more
Cloud Storage
Bucket details
Refresh
Overview
Buckets
Monitoring
Settings
Storage Intelligence
Insights datasets
Configuration
Marketplace
Release Notes
qwiklabs-gcp-04-867c17bf76fa_bucket
Public to internet: This bucket is public to stop public access.
Edit access
Dismiss
Location
europe-west1 (Belgium)
Storage class
Standard
Objects
Configuration
Public access
Public to internet
One or more bucket level permissions grant access to 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
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
New
Switch to uniform
bucket and its objects, switch control. Learn more

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

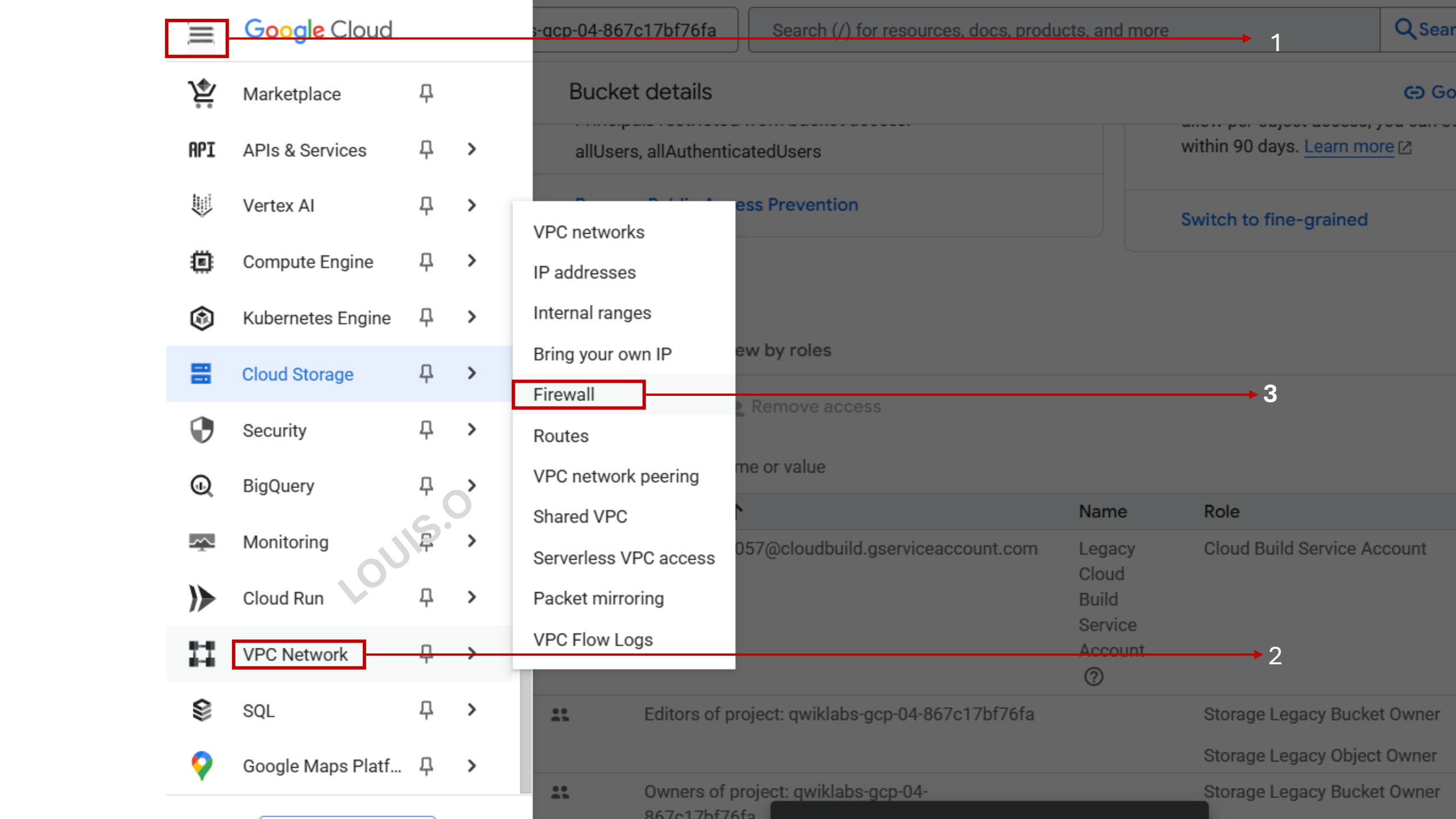


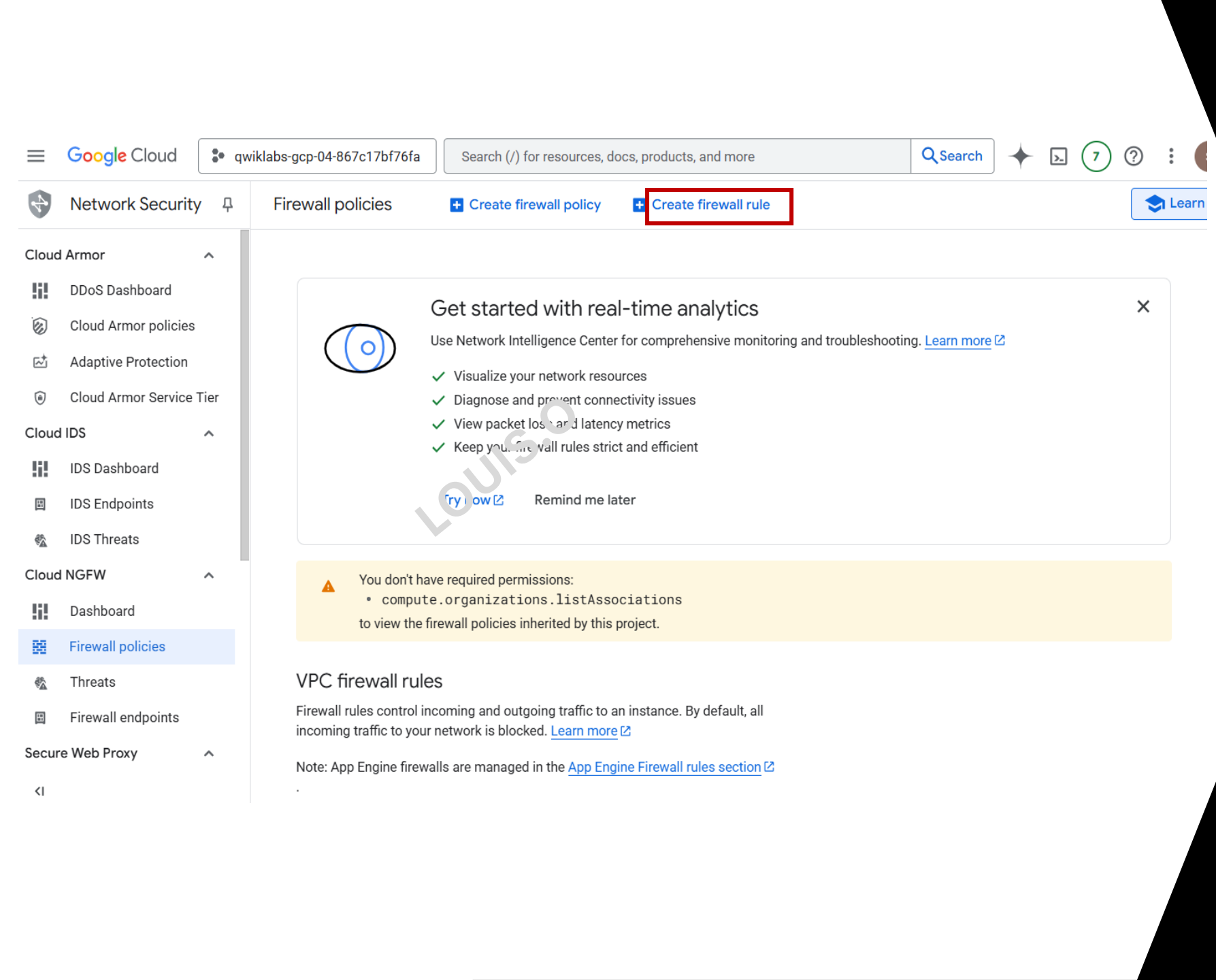



Google Cloud
qwiklabs-gcp-04-867c17bf76fa
Search (/) for resources, docs, products, and more
Search
Cloud Storage
Bucket details
Go to path
Refresh
Learn
Overview
Buckets
Monitoring
Settings
Storage Intelligence
Insights datasets
Configuration
Marketplace
Location
Objects
New
Inventory Reports
Operations
Permissions
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
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
Cancel
Save
Object-level ACLs enabled

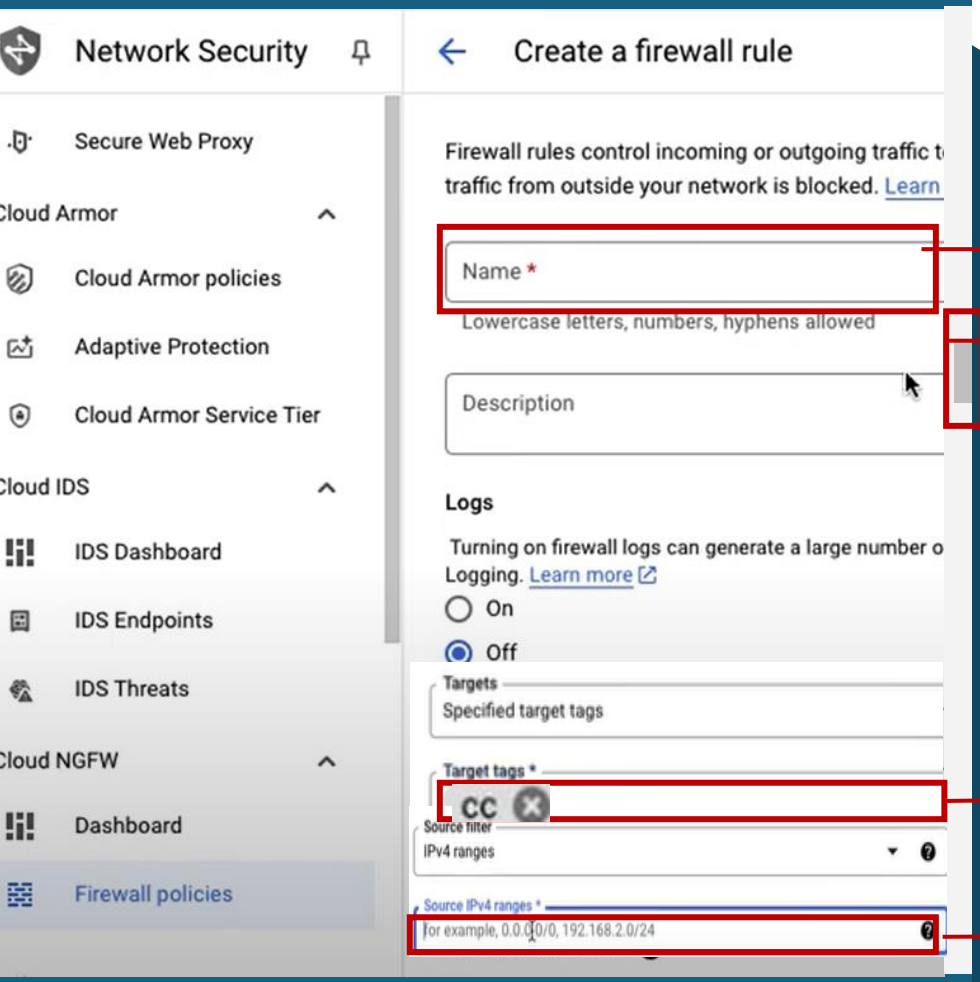

Google Cloud
qwiklabs-gcp-04-867c17bf76fa
Search (/) for resources, docs, products, and more
Search
Cloud Storage
Bucket details
Go to path
Refresh
Learn
Overview
Buckets
Monitoring
Settings
Storage Intelligence
Insights datasets
Configuration
Marketplace
Release Notes
allUsers, allAuthenticatedUsers
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
377021291057@cloudbuild.gserviceaccount.com
Legacy Cloud Build Service Account
Cloud Build Service Account
qwiklabs-gcp-04-867c17bf76fa
allUsers
Storage Legacy Bucket Reader
Editors of project: qwiklabs-gcp-04-867c17bf76fa
Storage Legacy Bucket Owner
Owners of project: qwiklabs-gcp-04-
Storage Legacy Bucket Owner
Remove allUsers
Are you sure you want to remove allUsers? They will lose all non-inherited roles on this resource.
Cancel
Confirm
1
2
3

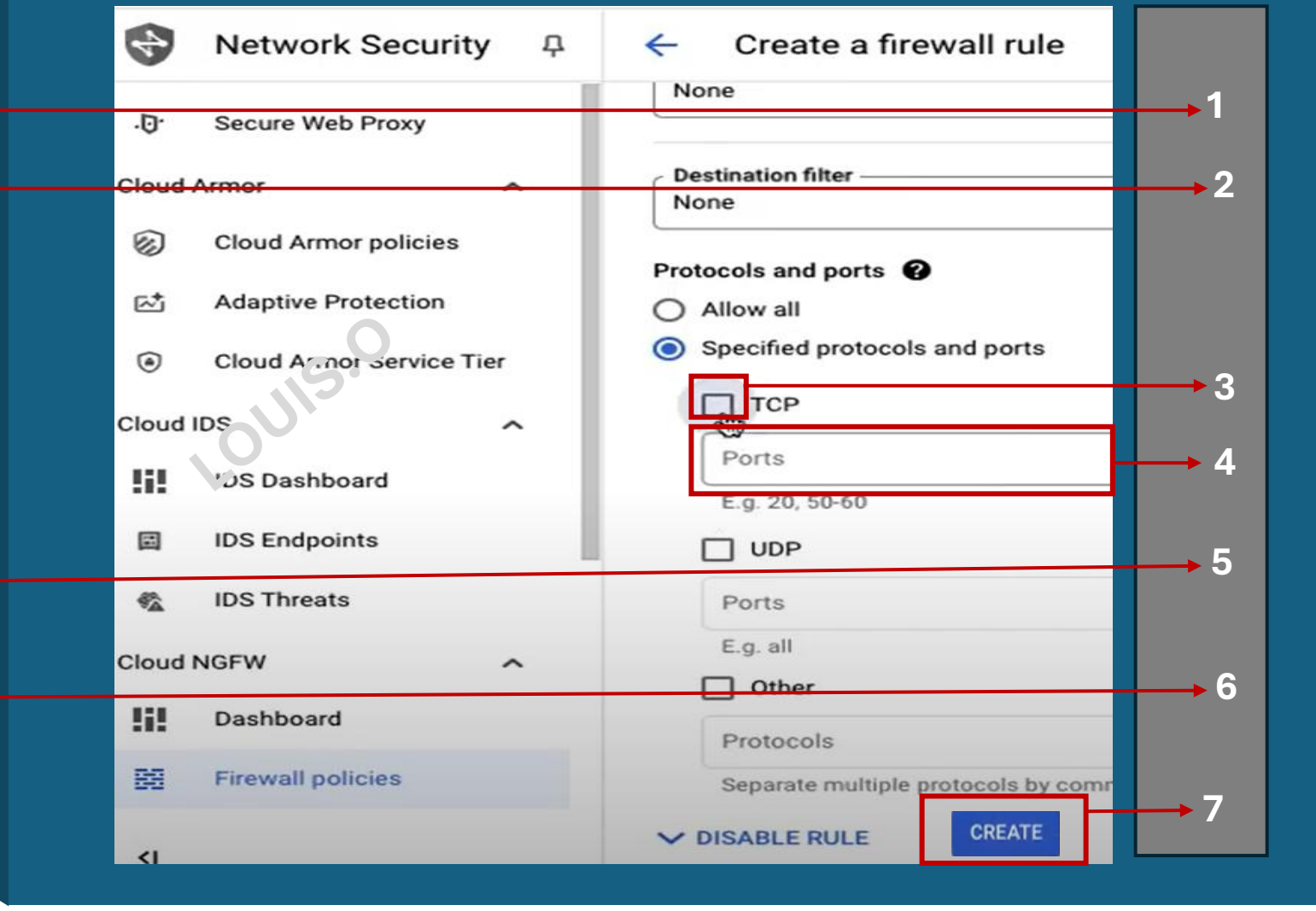
Task 4. Limit Firewall Ports Access


Google Cloud
Search (/) for resources, docs, products, and more
1
Bucket details
allUsers, allAuthenticatedUsers
within 90 days. Learn more
Switch to fine-grained
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
3
2
Remove access
Name
Role
057@cloudbuild.gserviceaccount.com
Legacy Cloud Build Service Account
Cloud Build Service Account
Editors of project: qwiklabs-gcp-04-867c17bf76fa
Storage Legacy Bucket Owner
Storage Legacy Object Owner
Owners of project: qwiklabs-gcp-04-
Storage Legacy Bucket Owner


Google Cloud
qwiklabs-gcp-04-867c17bf76fa
Search (/) for resources, docs, products, and more
Search
Network Security
Firewall policies
Create firewall policy
Create firewall rule
Learn
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
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 filed under TCP and Click **CREATE**





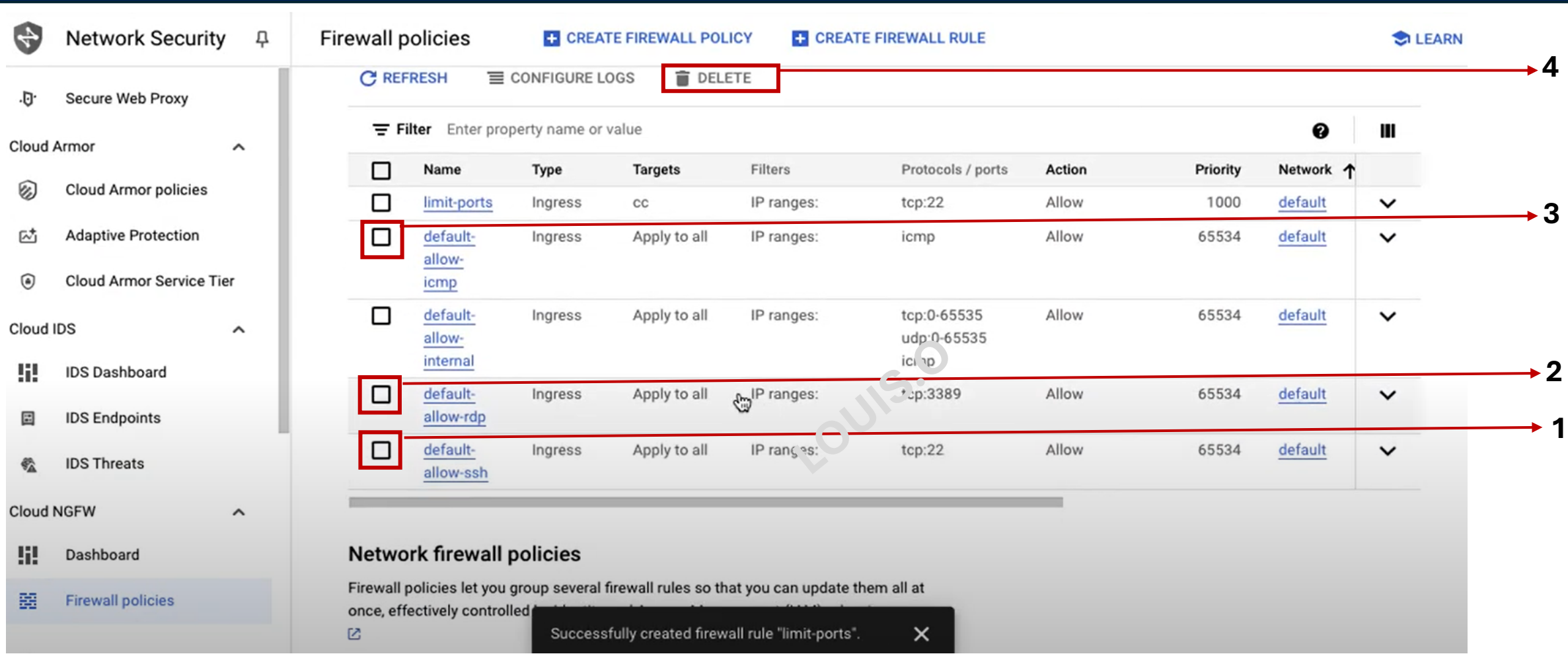
NB: In the Firewall Rule "**Restrict SSH access**" to only authorized IP from the source network **35.235.240.0/20** to compute instance with the target tag "**cc**"

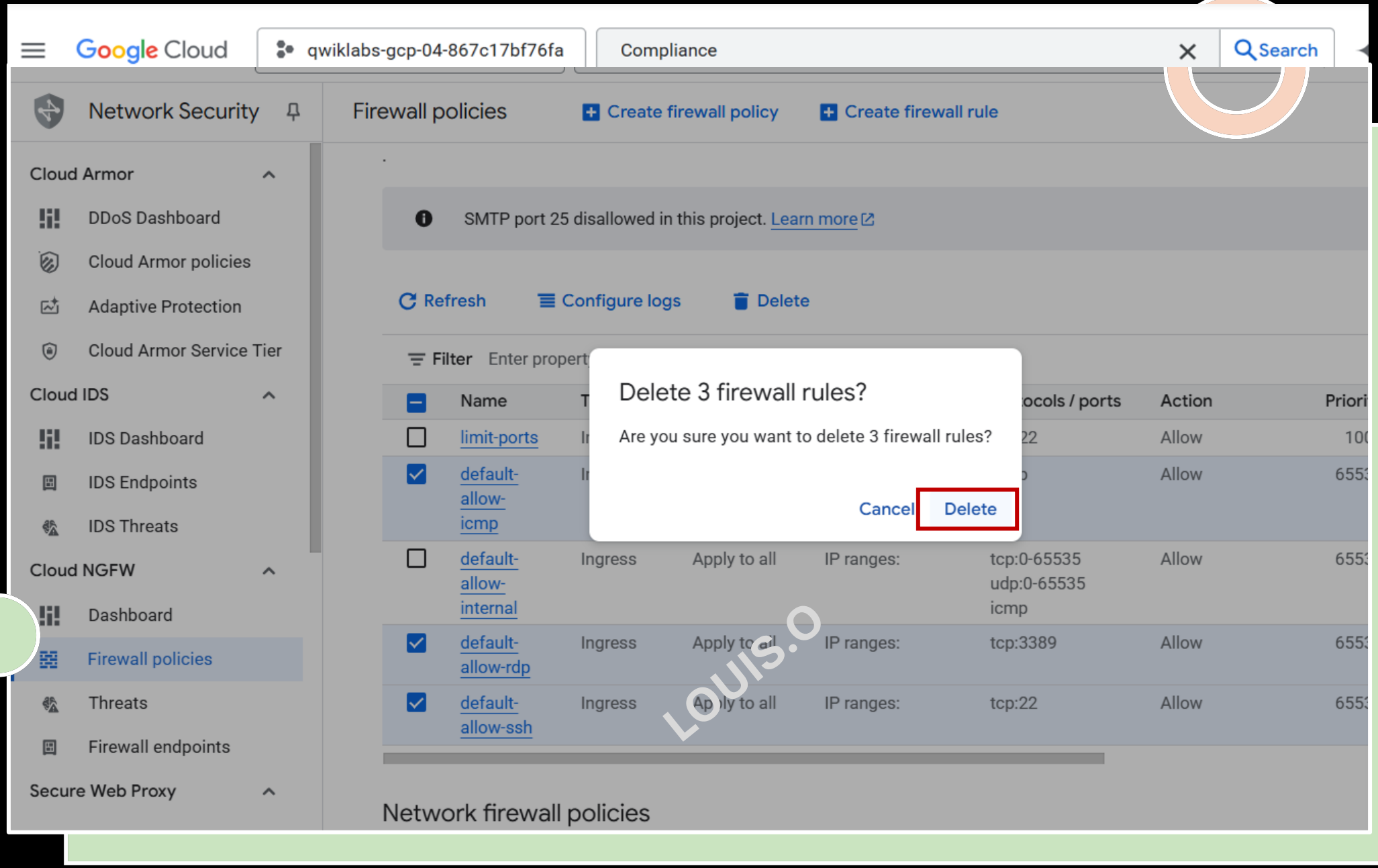
Task 5. Fix Firewall Configuration

Challenge: Customize firewall rules & Enable Logging

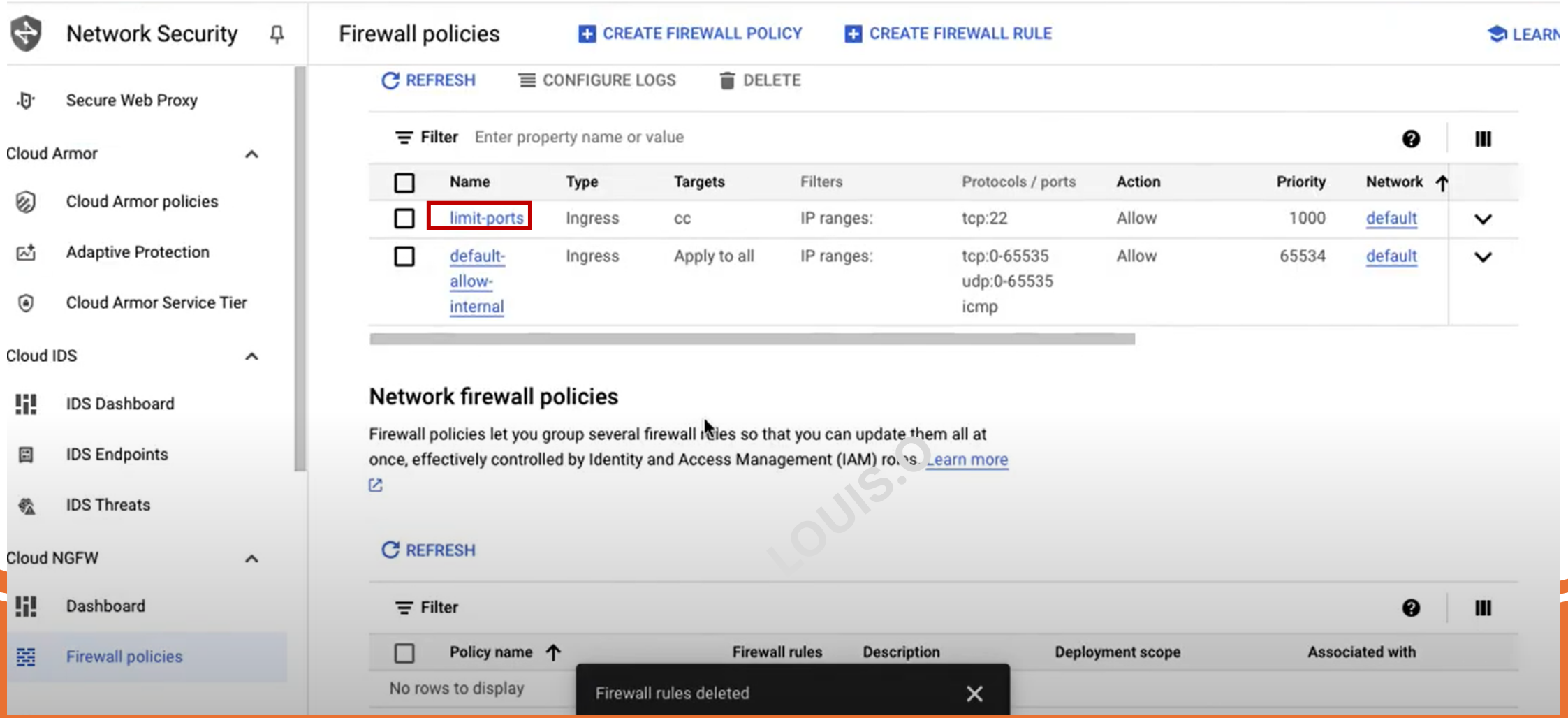
Delete the **default-allow-icmp**, **default-allow-rdp**, and **default-allow-ssh** firewall rules. These rules are overly broad and by deleting them, you'll allow for a more secure and controlled network environment.

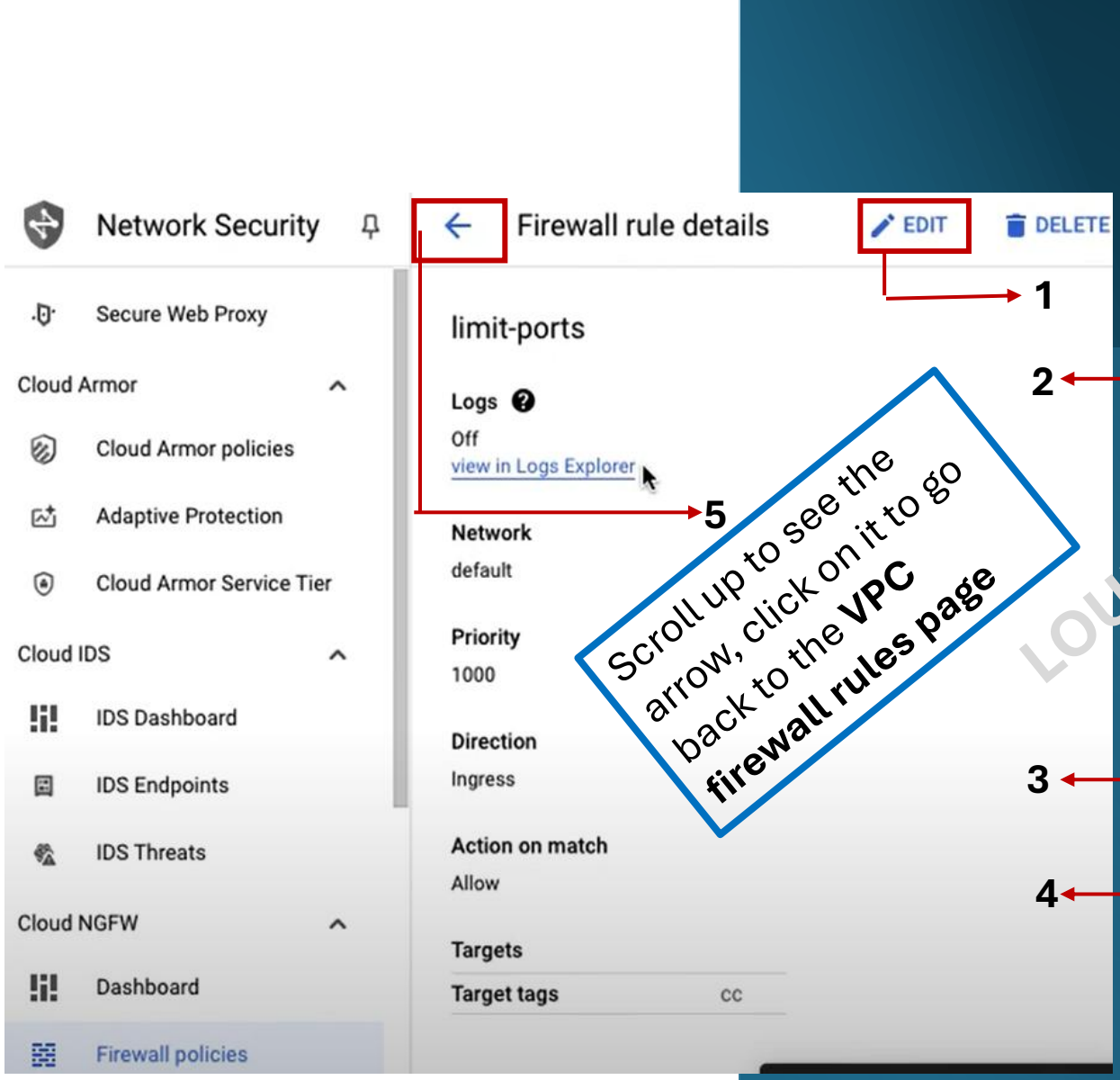
By deleting these rules, you have restricted access to these protocols, limiting the potential for unauthorized access attempts and reducing the attack surface of your network.

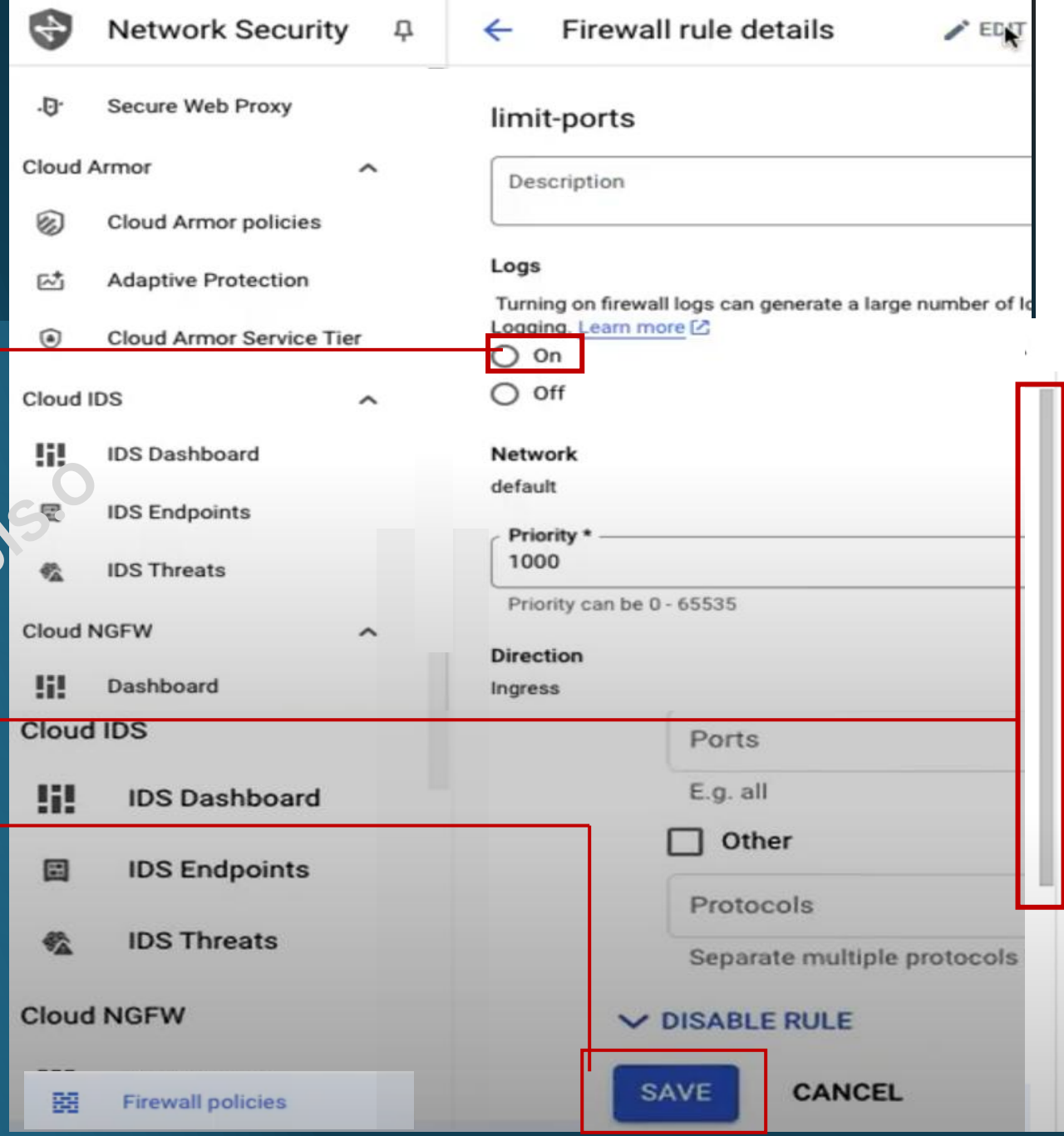


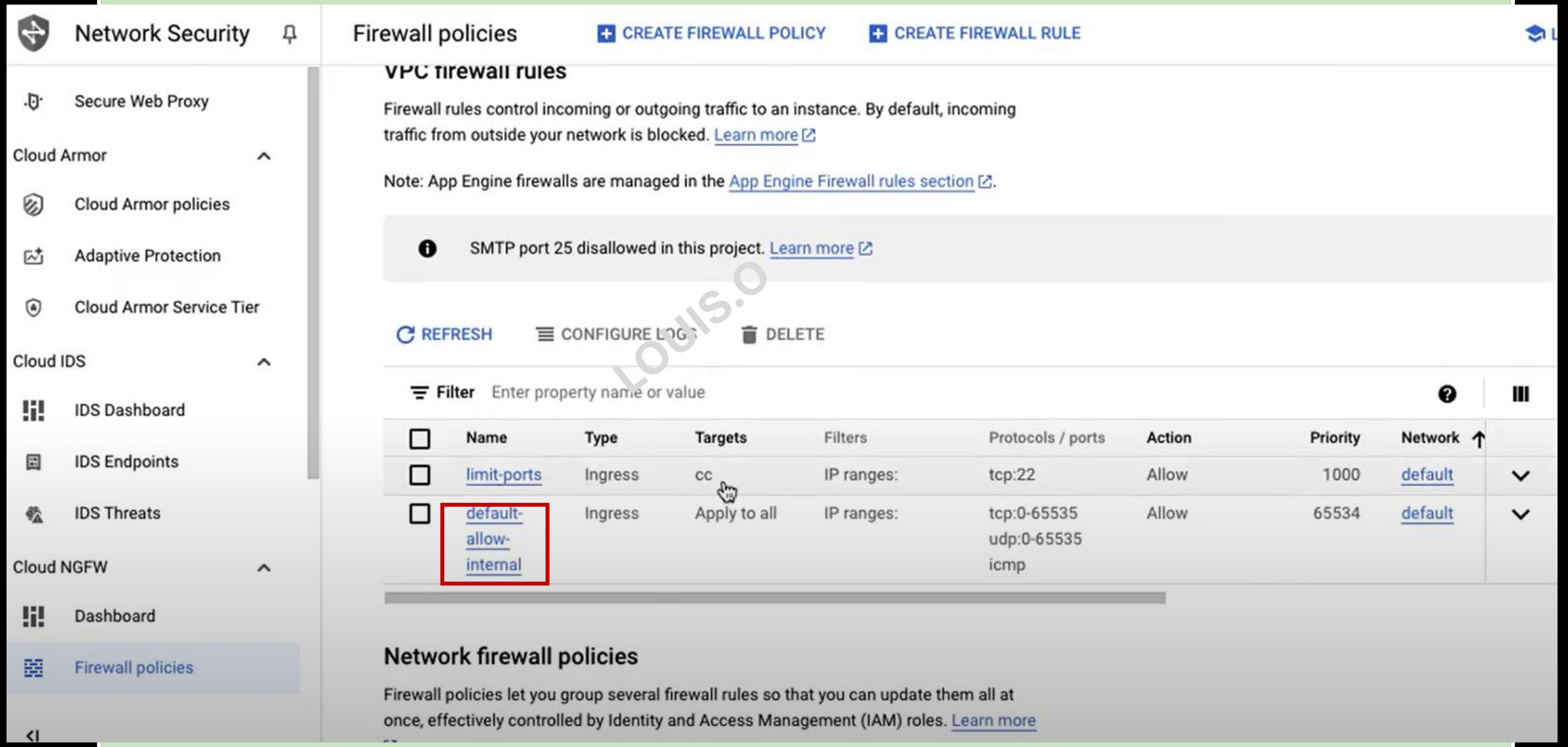

Google Cloud
qwiklabs-gcp-04-867c17bf76fa
Compliance
Search
Network Security
Firewall policies
Create firewall policy
Create firewall rule
Cloud Armor
DDoS Dashboard
Cloud Armor policies
Adaptive Protection
Cloud Armor Service Tier
Cloud IDS
IDS Dashboard
IDS Endpoints
IDS Threats
Cloud NGFW
Dashboard
Firewall policies
Threats
Firewall endpoints
Secure Web Proxy
SMTP port 25 disallowed in this project. Learn more
Refresh
Configure logs
Delete
Filter
Name
Action
limit-ports
Allow
default-allow-icmp
Allow
default-allow-internal
Ingress
Apply to all
IP ranges:
tcp:0-65535
udp:0-65535
icmp
Allow
default-allow-rdp
Ingress
IP ranges:
tcp:3389
Allow
default-allow-ssh
Ingress
IP ranges:
tcp:22
Allow
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

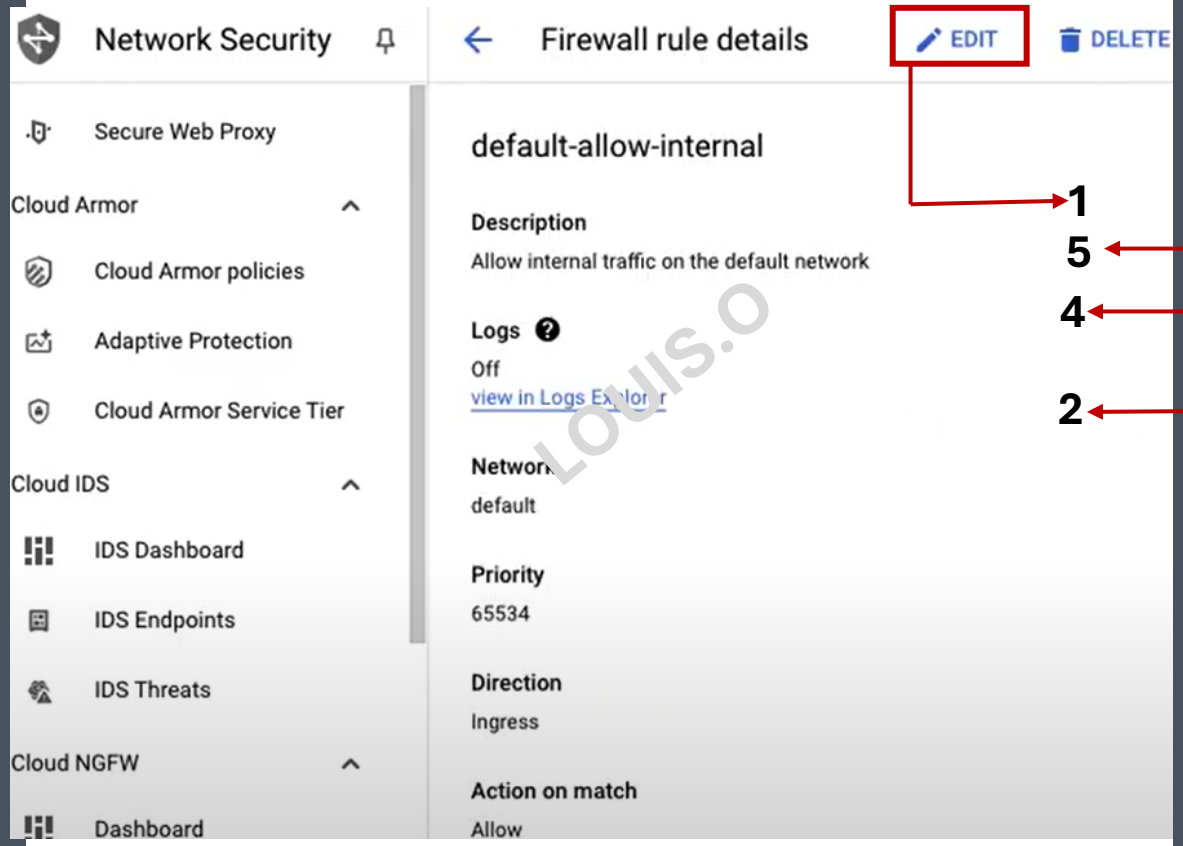


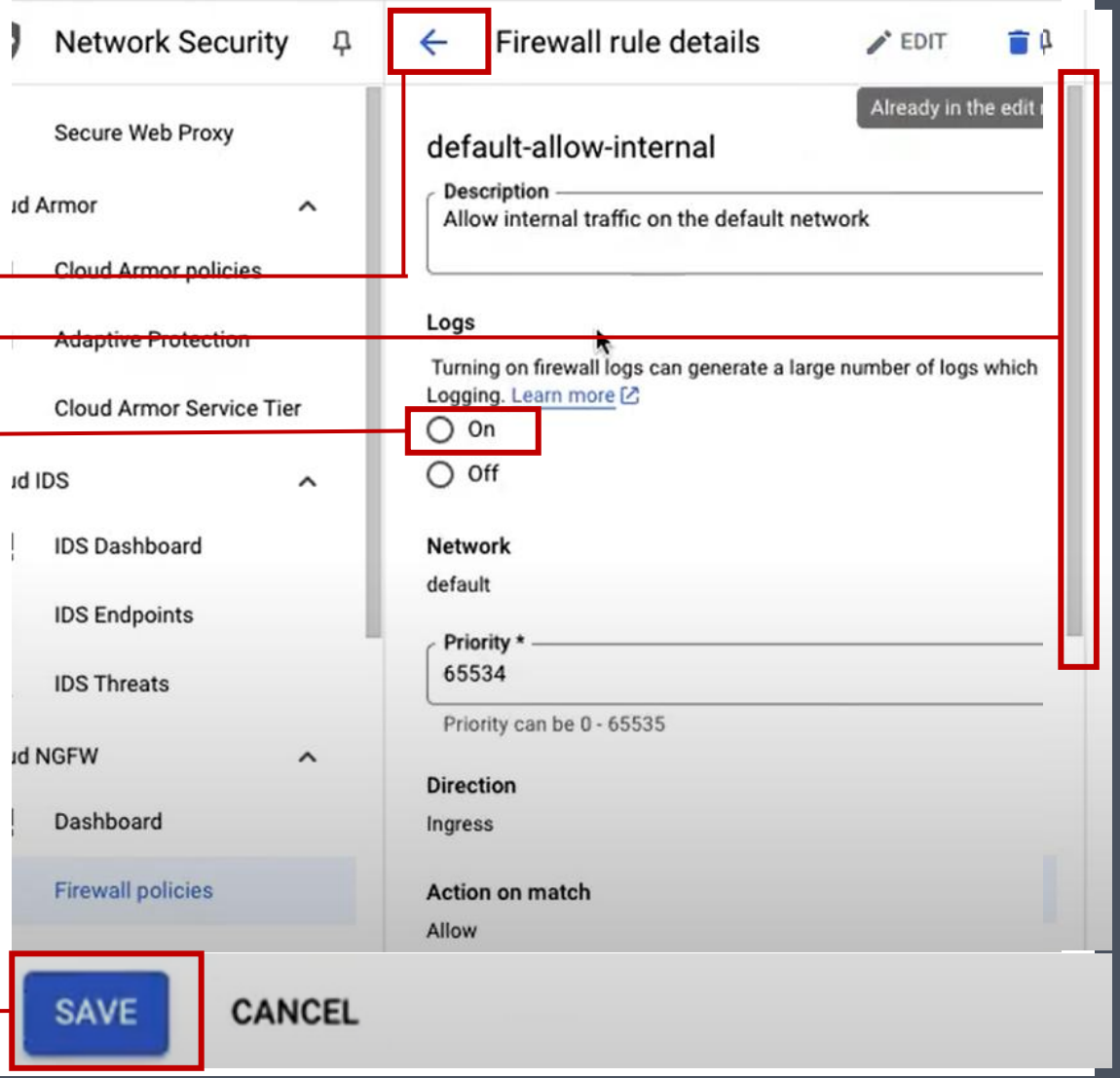

Network Security
Firewall rule details
EDIT
DELETE
Secure Web Proxy
Cloud Armor
Cloud Armor policies
Adaptive Protection
Cloud Armor Service Tier
Cloud IDS
IDS Dashboard
IDS Endpoints
IDS Threats
Cloud NGFW
Dashboard
Firewall policies
limit-ports
Logs
Off
view in Logs Explorer
Network
default
Priority
1000
Direction
Ingress
Action on match
Allow
Targets
Target tags
1
2
3
4
5
Scroll up to see the arrow, click on it to go back to the VPC firewall rules page


Network Security
Firewall rule details
EDIT
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
Cloud IDS
IDS Dashboard
IDS Endpoints
IDS Threats
Cloud NGFW
Firewall policies
limit-ports
Description
Logs
Turning on firewall logs can generate a large number of lo
Logging. 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

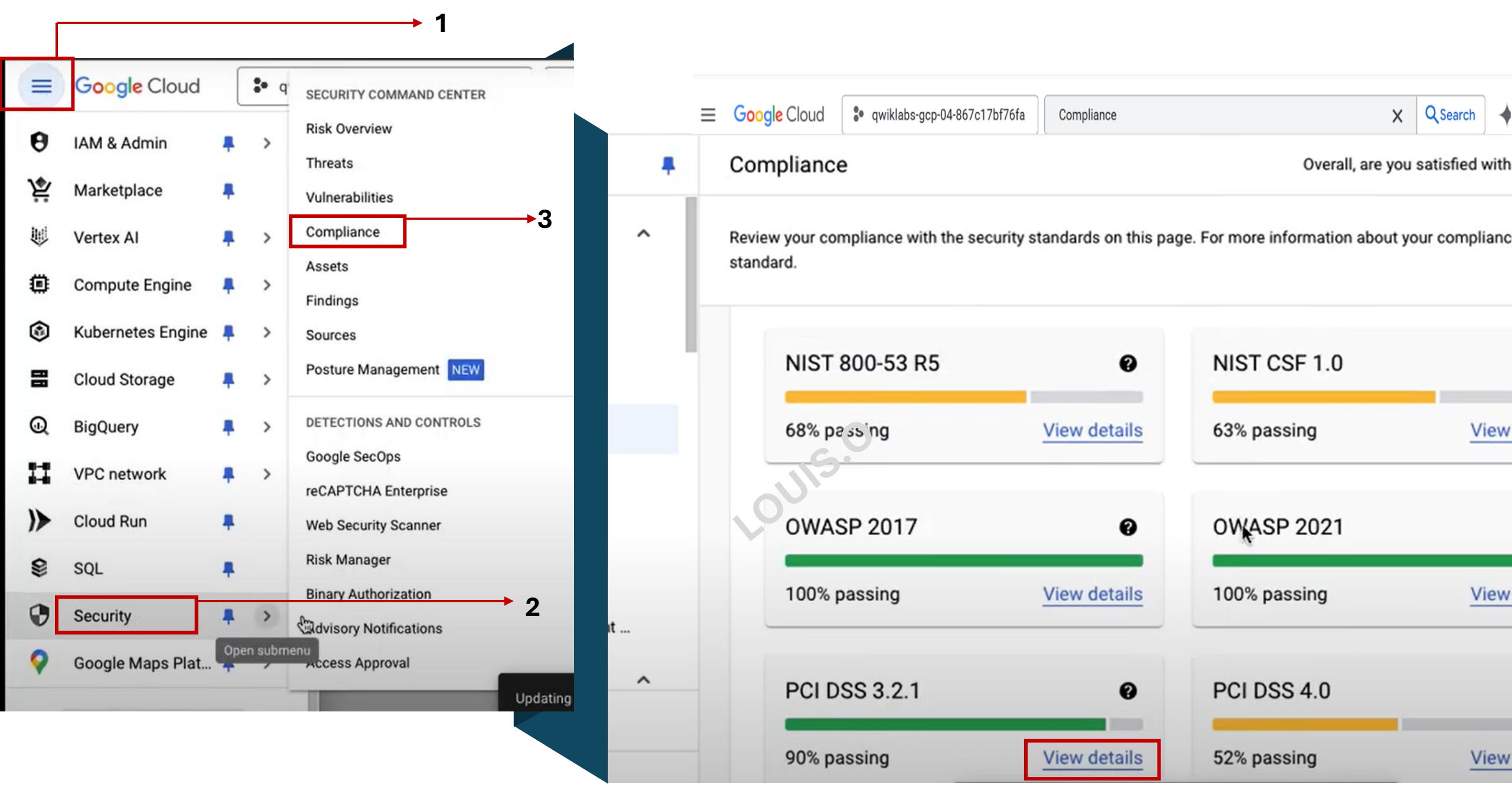

Network Security
Firewall policies
CREATE FIREWALL POLICY
CREATE FIREWALL RULE
Secure Web Proxy
Cloud Armor
Cloud Armor policies
Adaptive Protection
Cloud Armor Service Tier
Cloud IDS
IDS Dashboard
IDS Endpoints
IDS Threats
Cloud NGFW
Dashboard
Firewall policies
VPC firewall rules
Firewall rules control 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.
SMTP port 25 disallowed in this project. Learn more
REFRESH
CONFIGURE LOGS
DELETE
Filter
Enter property name or value
Name
Type
Targets
Filters
Protocols / ports
Action
Priority
Network
limit-ports
Ingress
cc
IP ranges:
tcp:22
Allow
1000
default
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

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



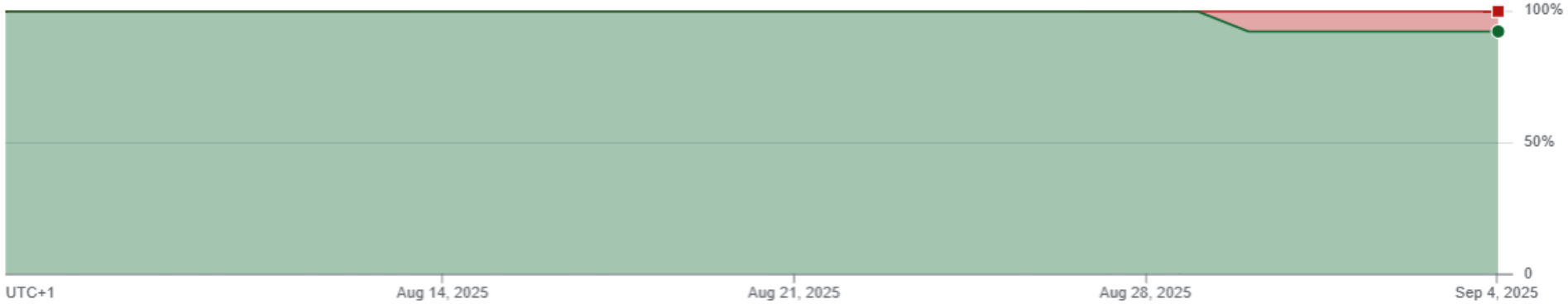


Task 6. Verify Compliance


1
Google Cloud
IAM & Admin
Marketplace
Vertex AI
Compute Engine
Kubernetes Engine
Cloud Storage
BigQuery
VPC network
Cloud Run
SQL
Security
Google Maps Plat...
Open submenu
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
Updating
2
3
Google Cloud
qwiklabs-gcp-04-867c17bf76fa
Compliance
Search
Compliance
Overall, are you satisfied with
Review your compliance with the security standards on this page. For more information about your compliance
standard.
NIST 800-53 R5
68% passing
View details
NIST CSF 1.0
63% passing
View
OWASP 2017
100% passing
View details
OWASP 2021
100% passing
View
PCI DSS 3.2.1
90% passing
View details
PCI DSS 4.0
52% passing
View

Compliance detail

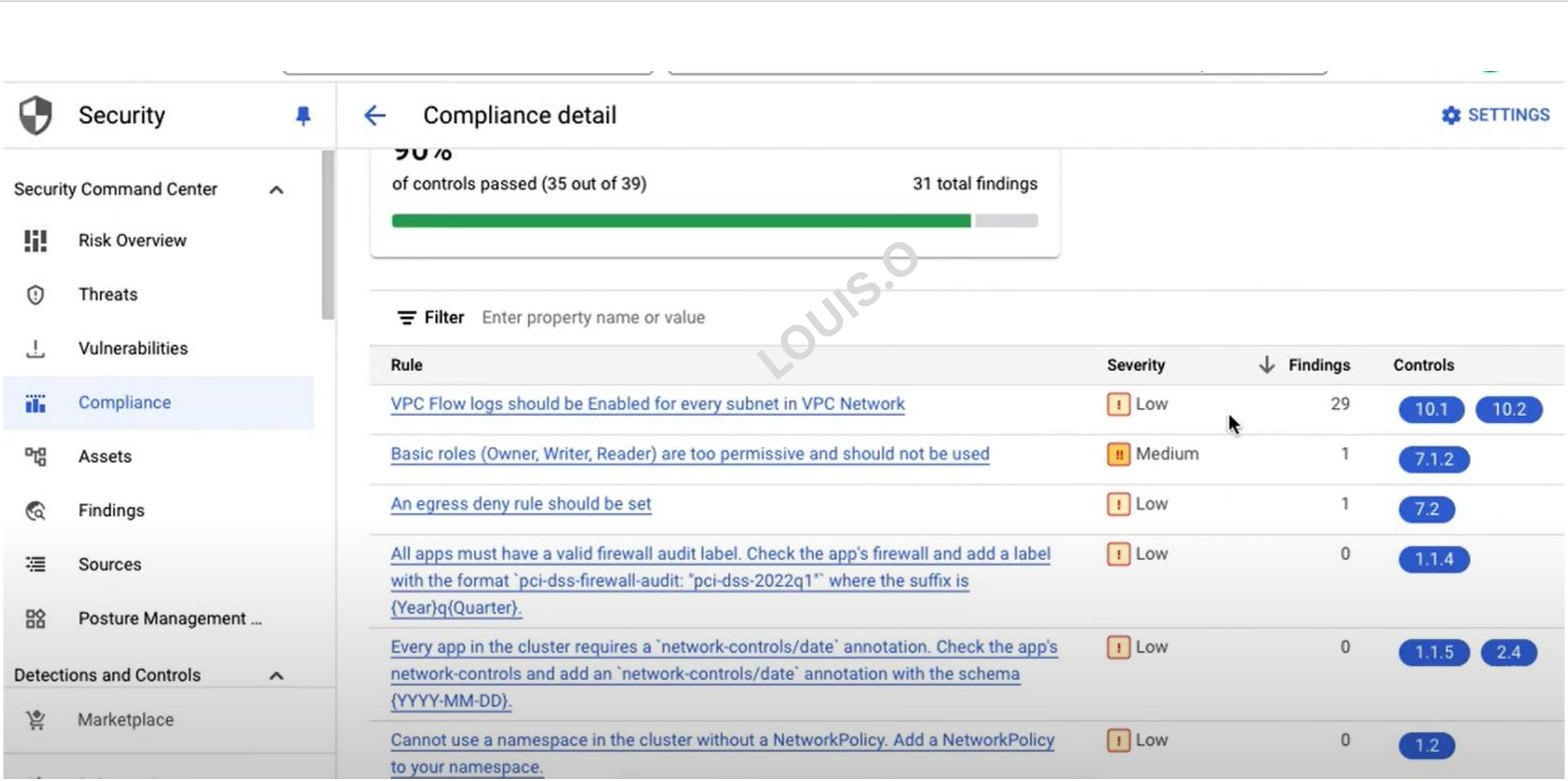
to view the state of your controls over time.



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
Compliance detail
SETTINGS
Security Command Center
Risk Overview
Threats
Vulnerabilities
Compliance
Assets
Findings
Sources
Posture Management ...
Detections and Controls
Marketplace
90%
of controls passed (35 out of 39)
31 total findings
Filter
Enter property name or value
Rule
Severity
Findings
Controls
VPC Flow logs should be Enabled for every subnet in VPC Network
Low
29
10.1
10.2
Basic roles (Owner, Writer, Reader) are too permissive and should not be used
Medium
1
7.1.2
An egress deny rule should be set
Low
1
7.2
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}.
Low
0
1.1.4
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}.
Low
0
1.1.5
2.4
Cannot use a namespace in the cluster without a NetworkPolicy. Add a NetworkPolicy to your namespace.
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

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 findir were identified:

1. **Malware infection:**

Forensic analysis confirmed the presence of malware on the compromised VM. The specific type and variant of the malwa 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 S services. The access logs and network traffic analysis provided crucial insights into the attacker's entry point and th subsequent activities.

3. **Privilege escalation:**

The forensic examination indicated that the attacker leveraged the compromised VM to escalate privileges and gain acce to sensitive systems and resources. Through the exploitation of user and service account credentials, the attacker was al 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 interr access to initiate and facilitate the exfiltration, exporting the compromised data for later remote retrieval. The findings provi valuable insights into the attack, enabling the incident response team to understand the attack vector, the attacker's actio and the compromised data. These findings will serve as crucial evidence for further investigations, remediation efforts, a future cybersecurity enhancements.

Response and remediation

To effectively remediate the incident, a series of actions were taken in alignment with industry best practices. The fo
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
The following are recommendations that I suggested to be implemented to mitigate similar attacks from
future:

1. **Strengthen Cloud Configuration Management**
   - Enforce least privilege access, use automated tools (e.g., Google Cloud Security Command Cent
     misconfigurations in real-time.
2. **Implement Continuous Patch & Vulnerability Management**
   - Regularly update VMs, applications, and firewalls with automated patching to reduce the attack s
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 ex
     red/blue team simulations to test readiness.

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


Thank
You!