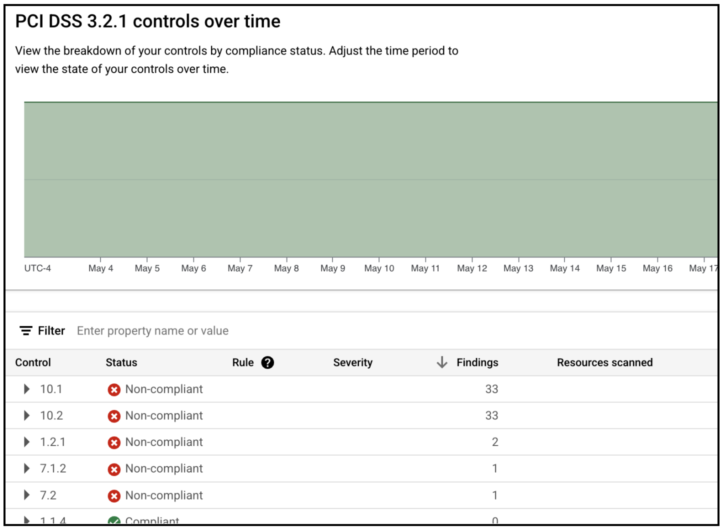
Course 5_Lab 1: Capstone: Respond and Recover from a Data Breach

Task 1: Analyze the data breach and gather information

In this task, I analyzed the resource types that were not in compliance with PCI DSS 3.2.1.

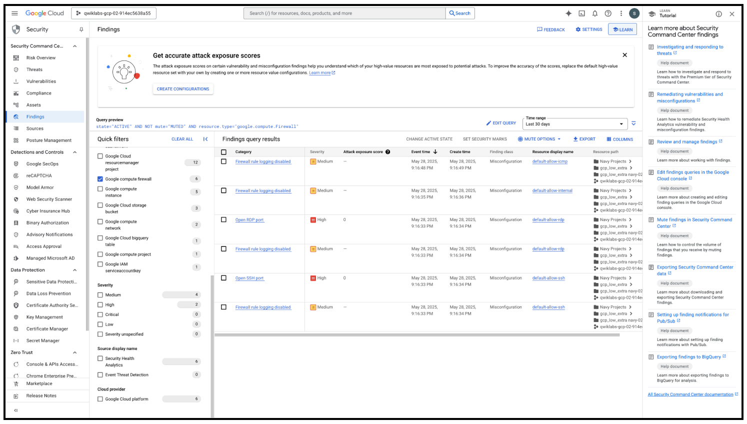


PCI DSS 3.2.1 controls over time

View the breakdown of your controls by compliance status. Adjust the time period to view the state of your controls over time.

Filter Enter property name or value

Control	Status	Rule	Severity	Findings	Resources scanned
10.1	☒ Non-compliant			33	
10.2	☒ Non-compliant			33	
1.2.1	☒ Non-compliant			2	
7.1.2	☒ Non-compliant			1	
7.2	☒ Non-compliant			1	
1.1.4	✓ Compliant			0	



Get accurate attack exposure scores

The attack exposure scores on certain vulnerability and misconfiguration findings help you understand which of your high-value resources are most exposed to potential attacks. To improve the accuracy of the scores, replace the default high-value resource set with your own by creating one or more resource value configurations. Learn more

CREATE CONFIGURATIONS

Query preview

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

EDIT QUERY · Time range: Last 30 days

Quick filters (CLEAR ALL)

- ☐ Google Cloud resourcemanager project 12
- ☑ Google compute firewall 6
- ☐ Google compute instance 5
- ☐ Google Cloud storage bucket 3
- ☐ Google compute network 2
- ☐ Google Cloud bigquery table 1
- ☐ Google compute project 1
- ☐ Google IAM serviceaccountkey 1

Severity

- ☐ Medium 4
- ☐ High 2
- ☐ Critical 0
- ☐ Low 0
- ☐ Severity unspecified 0

Source display name

- ☐ Security Health Analytics 6
- ☐ Event Threat Detection 0

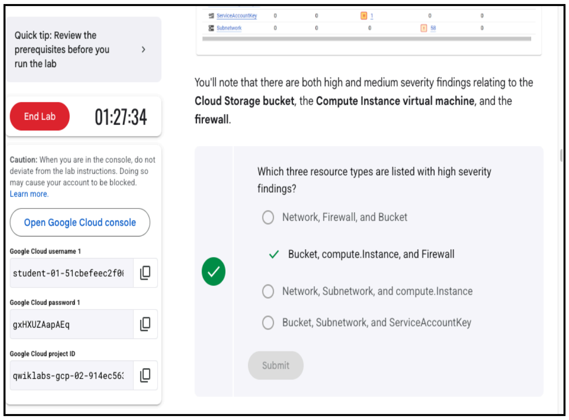
Cloud provider

- ☐ Google Cloud platform 6

Findings query results

CHANGE ACTIVE STATE · SET SECURITY MARKS · MUTE OPTIONS · EXPORT · COLUMNS

☐	Category	Severity	Attack exposure score	Event time	Create time	Finding class	Resource display name	Resource path
☐	Firewall rule logging disabled	Medium	–	May 28, 2025, 9:16:48 PM	May 28, 2025, 9:16:49 PM	Misconfiguration	default-allow-icmp	Navy Projects gcp_low_extra gcp_low_extra navy-02 qwiklabs-gcp-02-914e
☐	Firewall rule logging disabled	Medium	–	May 28, 2025, 9:16:35 PM	May 28, 2025, 9:16:36 PM	Misconfiguration	default-allow-internal	Navy Projects gcp_low_extra gcp_low_extra navy-02 qwiklabs-gcp-02-914e
☐	Open RDP port	High	0	May 28, 2025, 9:16:33 PM	May 28, 2025, 9:16:34 PM	Misconfiguration	default-allow-rdp	Navy Projects gcp_low_extra gcp_low_extra navy-02 qwiklabs-gcp-02-914e
☐	Firewall rule logging disabled	Medium	–	May 28, 2025, 9:16:33 PM	May 28, 2025, 9:16:34 PM	Misconfiguration	default-allow-rdp	Navy Projects gcp_low_extra gcp_low_extra navy-02 qwiklabs-gcp-02-914e
☐	Open SSH port	High	0	May 28, 2025, 9:16:33 PM	May 28, 2025, 9:16:34 PM	Misconfiguration	default-allow-ssh	Navy Projects gcp_low_extra gcp_low_extra navy-02 qwiklabs-gcp-02-914e
☐	Firewall rule logging disabled	Medium	–	May 28, 2025, 9:16:33 PM	May 28, 2025, 9:16:34 PM	Misconfiguration	default-allow-ssh	Navy Projects gcp_low_extra gcp_low_extra navy-02 qwiklabs-gcp-02-914e



Quick tip: Review the prerequisites before you run the lab

End Lab 01:27:34

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Open Google Cloud console

Google Cloud username 1: student-01-51cbefeec2f0

Google Cloud password 1: gxHXUZAapAEq

Google Cloud project ID: qwiklabs-gcp-02-914ec56:

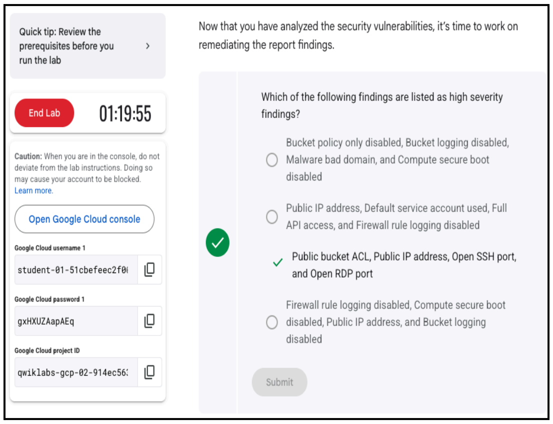
ServiceAccountKey	0	0	1	0	0
Subnetwork	0	0	0	58	0

You'll note that there are both high and medium severity findings relating to the **Cloud Storage bucket**, the **Compute Instance virtual machine**, and the **firewall**.

Which three resource types are listed with high severity findings?

- ○ Network, Firewall, and Bucket
- ✓ Bucket, compute.Instance, and Firewall
- ○ Network, Subnetwork, and compute.Instance
- ○ Bucket, Subnetwork, and ServiceAccountKey

Submit



Quick tip: Review the prerequisites before you run the lab

End Lab 01:19:55

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Open Google Cloud console

Google Cloud username 1: student-01-51cbefeec2f0

Google Cloud password 1: gxHXUZAapAEq

Google Cloud project ID: qwiklabs-gcp-02-914ec56:

Now that you have analyzed the security vulnerabilities, it's time to work on remediating the report findings.

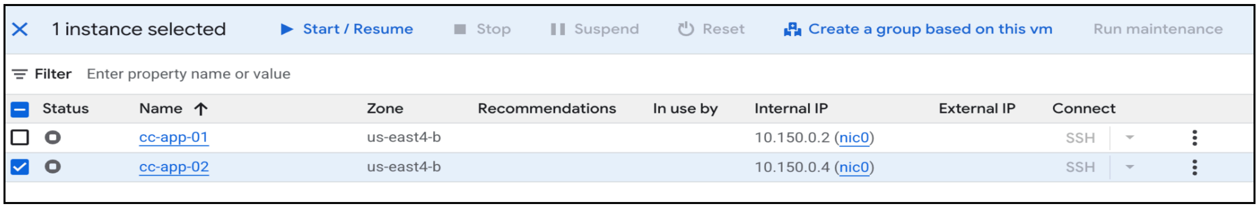
Which of the following findings are listed as high severity findings?

- ○ Bucket policy only disabled, Bucket logging disabled, Malware bad domain, and Compute secure boot disabled
- ○ Public IP address, Default service account used, Full API access, and Firewall rule logging disabled
- ✓ Public bucket ACL, Public IP address, Open SSH port, and Open RDP port
- ○ Firewall rule logging disabled, Compute secure boot disabled, Public IP address, and Bucket logging disabled

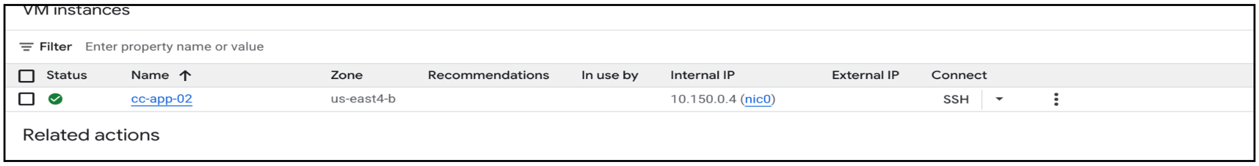
Submit

Task 2: Fix the compute engine vulnerabilities

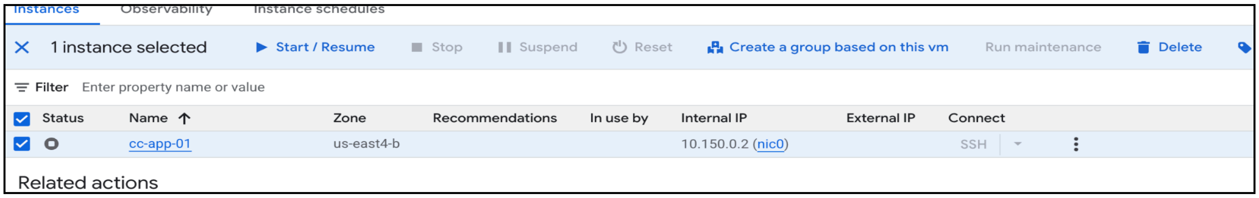
In this task, I focused on fixing the compute engine vulnerabilities. I stopped the instance containing the vulnerability, created a new instance from a snapshot previously created by Google for the purposes of this lab, and finally deleted the instance out of compliance.



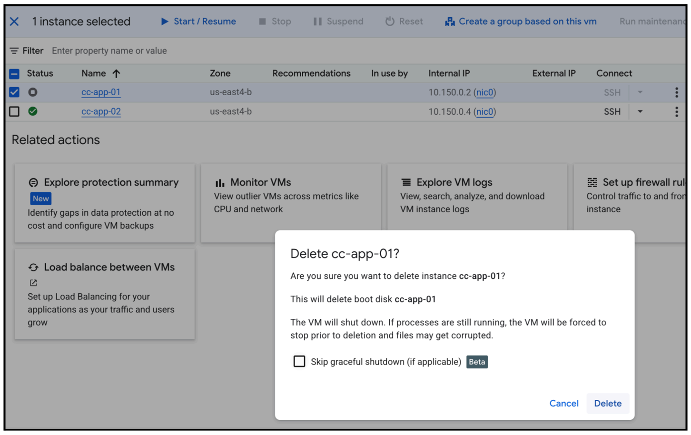
☐	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect
☐	○	cc-app-01	us-east4-b			10.150.0.2 (nic0)		SSH
☑	○	cc-app-02	us-east4-b			10.150.0.4 (nic0)		SSH



☐	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect
☐	✓	cc-app-02	us-east4-b			10.150.0.4 (nic0)		SSH



☑	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect
☑	○	cc-app-01	us-east4-b			10.150.0.2 (nic0)		SSH


1 instance selected
Start / Resume
Stop
Suspend
Reset
Create a group based on this vm
Run maintenanc
Filter
Enter property name or value

☐	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect
☑	○	cc-app-01	us-east4-b			10.150.0.2 (nic0)		SSH
☐	✓	cc-app-02	us-east4-b			10.150.0.4 (nic0)		SSH

Related actions
Explore protection summary
New
Identify gaps in data protection at no cost and configure VM backups
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 rul
Control traffic to and fron instance
Load balance between VMs
Set up Load Balancing for your applications as your traffic and users grow

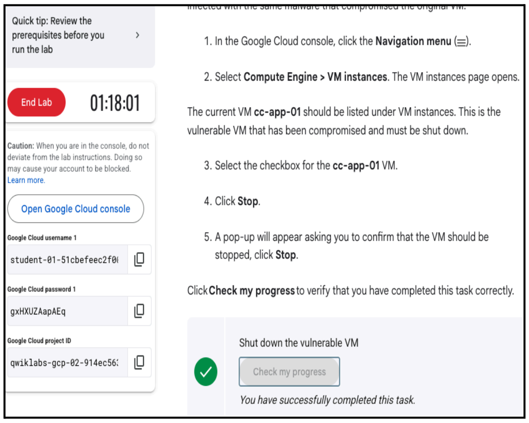
Delete cc-app-01?

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


Quick tip: Review the prerequisites before you run the lab
End Lab
01:18:01

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Open Google Cloud console

Google Cloud username 1: student-01-51cbefeec2f0(

Google Cloud password 1: gxHXUZAapAEq

Google Cloud project ID: qwiklabs-gcp-02-914ec56:

infected with the same malware that compromised the original VM.

1. In the Google Cloud console, click the **Navigation menu** (☰).
2. Select **Compute Engine > VM instances**. The VM instances page opens.

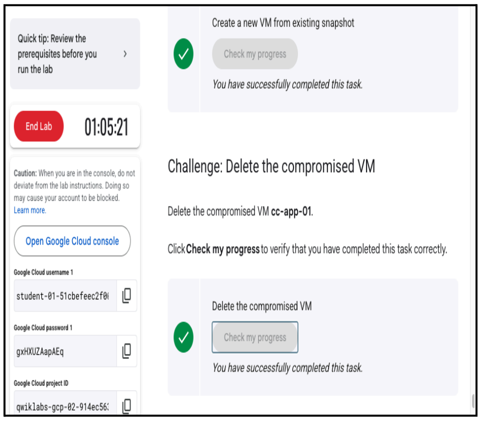
The current VM **cc-app-01** should be listed under VM instances. This is the vulnerable VM that has been compromised and must be shut down.

3. Select the checkbox for the **cc-app-01** VM.
4. Click **Stop**.
5. A pop-up will appear asking you to confirm that the VM should be stopped, click **Stop**.

Click **Check my progress** to verify that you have completed this task correctly.

✓ Shut down the vulnerable VM

You have successfully completed this task.


Quick tip: Review the prerequisites before you run the lab
End Lab
01:05:21

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Open Google Cloud console

Google Cloud username 1: student-01-51cbefeec2f0(

Google Cloud password 1: gxHXUZAapAEq

Google Cloud project ID: qwiklabs-gcp-02-914ec56:

✓ Create a new VM from existing snapshot

You have successfully completed this task.

Challenge: Delete the compromised VM

Delete the compromised VM **cc-app-01**.

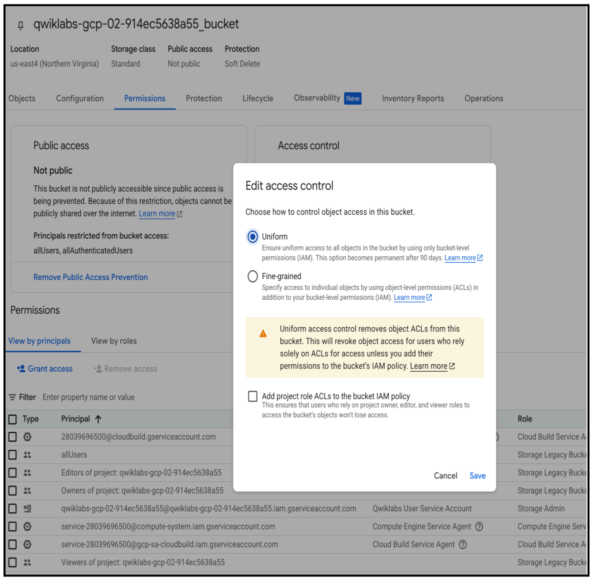
Click **Check my progress** to verify that you have completed this task correctly.

✓ Delete the compromised VM

You have successfully completed this task.

Task 3: Fix cloud storage bucket permissions

This task focused on remediating the issue within the cloud storage bucket. Removing public access and updating the access control reduces the risk of a data breach.



qwiklabs-gcp-02-914ec5638a55_bucket

Location	Storage class	Public access	Protection
us-east4 (Northern Virginia)	Standard	Not public	Soft Delete

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

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

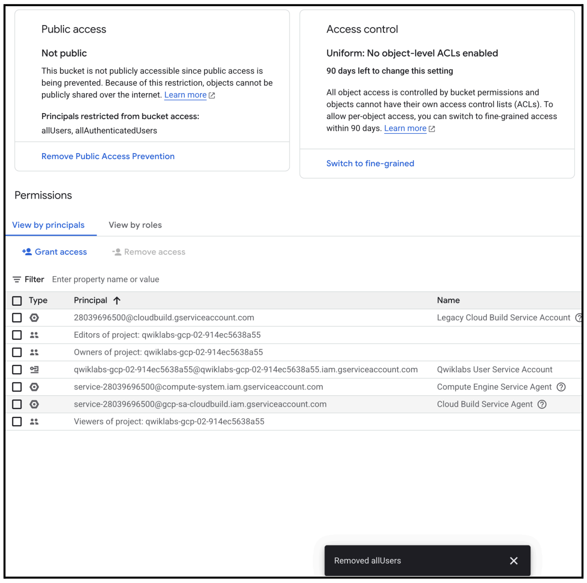
Uniform access control removes object ACLs from this bucket. This will revoke object access for users who rely solely on ACLs for access unless you add their permissions to the bucket's IAM policy. Learn more

□ 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.

Permissions

Filter Enter property name or value

Type	Principal ↑		Role
□	28039696500@cloudbuild.gserviceaccount.com		Cloud Build Service A
□	allUsers		Storage Legacy Bucke
□	Editors of project: qwiklabs-gcp-02-914ec5638a55		Storage Legacy Bucke
□	Owners of project: qwiklabs-gcp-02-914ec5638a55		Storage Legacy Bucke
□	qwiklabs-gcp-02-914ec5638a55@qwiklabs-gcp-02-914ec5638a55.iam.gserviceaccount.com	Qwiklabs User Service Account	Storage Admin
□	service-28039696500@compute-system.iam.gserviceaccount.com	Compute Engine Service Agent	Compute Engine Serv
□	service-28039696500@gcp-sa-cloudbuild.iam.gserviceaccount.com	Cloud Build Service Agent	Cloud Build Service A
□	Viewers of project: qwiklabs-gcp-02-914ec5638a55		Storage Legacy Bucke



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

Uniform: No object-level ACLs enabled

90 days left to change this setting

All object access is controlled by bucket permissions and objects cannot have their own access control lists (ACLs). To allow per-object access, you can switch to fine-grained access within 90 days. Learn more

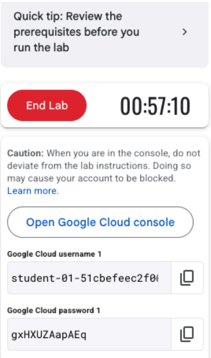
Switch to fine-grained

Permissions

Filter Enter property name or value

Type	Principal ↑	Name
□	28039696500@cloudbuild.gserviceaccount.com	Legacy Cloud Build Service Account
□	Editors of project: qwiklabs-gcp-02-914ec5638a55	
□	Owners of project: qwiklabs-gcp-02-914ec5638a55	
□	qwiklabs-gcp-02-914ec5638a55@qwiklabs-gcp-02-914ec5638a55.iam.gserviceaccount.com	Qwiklabs User Service Account
□	service-28039696500@compute-system.iam.gserviceaccount.com	Compute Engine Service Agent
□	service-28039696500@gcp-sa-cloudbuild.iam.gserviceaccount.com	Cloud Build Service Agent
□	Viewers of project: qwiklabs-gcp-02-914ec5638a55	

Removed allUsers ✕



Quick tip: Review the prerequisites before you run the lab ›

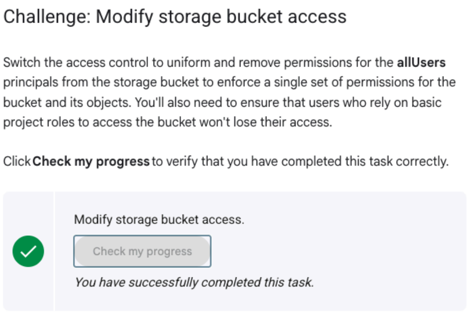
Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Google Cloud username 1

student-01-51cbefeec2f0(

Google Cloud password 1

gxHXUZAapAEq



Challenge: Modify storage bucket access

Switch the access control to uniform and remove permissions for the **allUsers** principals from the storage bucket to enforce a single set of permissions for the bucket and its objects. You'll also need to ensure that users who rely on basic project roles to access the bucket won't lose their access.

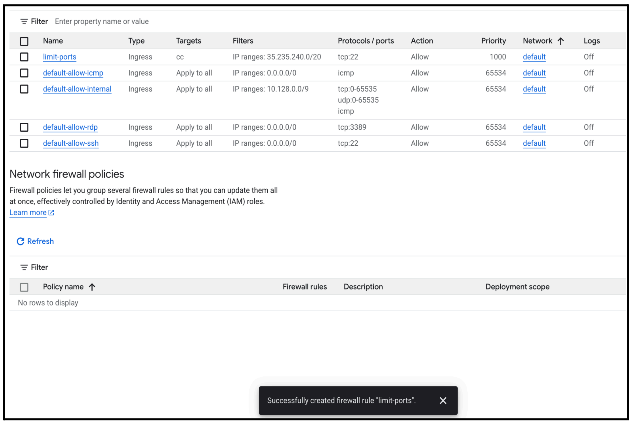
Click **Check my progress** to verify that you have completed this task correctly.

✓ Modify storage bucket access.

You have successfully completed this task.

Task 4: Limit firewall ports access

In this lab, I created a firewall rule and restricted access to only authorized IP addresses from the source network provided by Google.



Filter Enter property name or value

□	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network ↑	Logs
□	limit-ports	Ingress	cc	IP ranges: 35.235.240.0/20	tcp:22	Allow	1000	default	Off
□	default-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65534	default	Off
□	default-allow-internal	Ingress	Apply to all	IP ranges: 10.128.0.0/9	tcp:0-65535 udp:0-65535 icmp	Allow	65534	default	Off
□	default-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65534	default	Off
□	default-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65534	default	Off

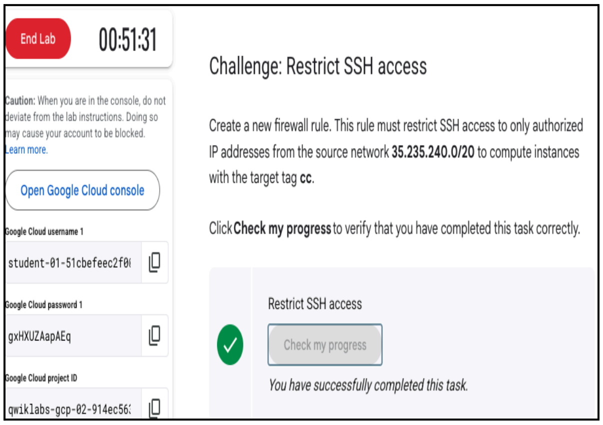
Network firewall policies

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

Filter

□	Policy name ↑	Firewall rules	Description	Deployment scope
No rows to display				

Successfully created firewall rule "limit-ports". ✕



Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Google Cloud username 1

student-01-51cbefeec2f0(

Google Cloud password 1

gxHXUZAapAEq

Google Cloud project ID

qwiklabs-gcp-02-914ec56:

Challenge: Restrict SSH access

Create a new firewall rule. This rule must restrict SSH access to only authorized IP addresses from the source network **35.235.240.0/20** to compute instances with the target tag **cc**.

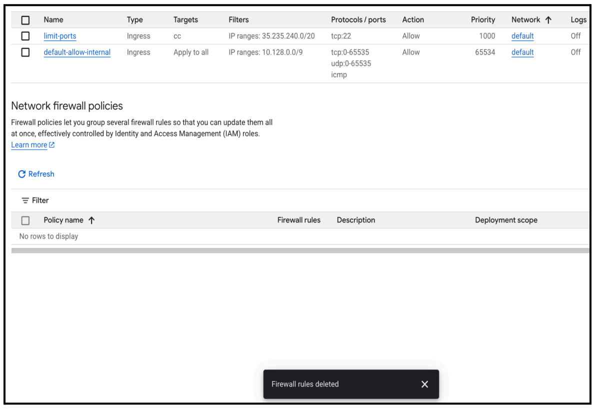
Click **Check my progress** to verify that you have completed this task correctly.

✓ Restrict SSH access

You have successfully completed this task.

Task 5: Fix the firewall configuration

In this task I customized the firewall rules, enabled logging, and deleted the firewall rules that were overly broad, allowing for a more secure and controlled network environment.



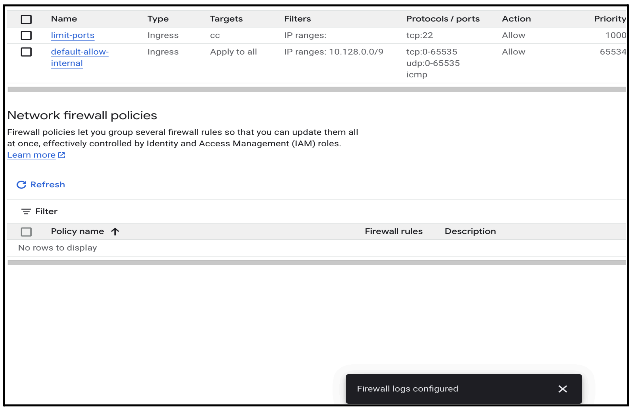
☐	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network ↑	Logs
☐	limit-ports	Ingress	cc	IP ranges: 35.235.240.0/20	tcp:22	Allow	1000	default	Off
☐	default-allow-internal	Ingress	Apply to all	IP ranges: 10.128.0.0/9	tcp:0-65535 udp:0-65535 icmp	Allow	65534	default	Off

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 ↑	Firewall rules	Description	Deployment scope
No rows to display				

Firewall rules deleted ✕



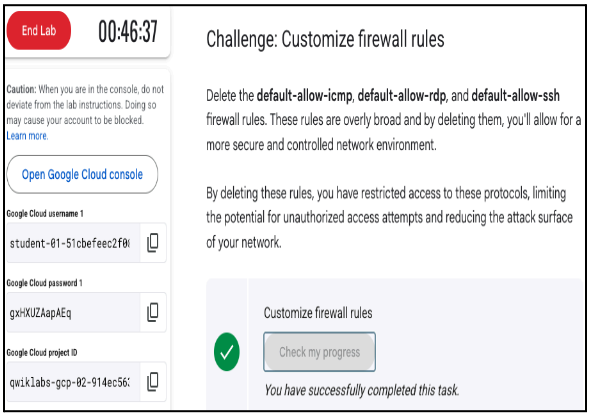
☐	Name	Type	Targets	Filters	Protocols / ports	Action	Priority
☐	limit-ports	Ingress	cc	IP ranges:	tcp:22	Allow	1000
☐	default-allow-internal	Ingress	Apply to all	IP ranges: 10.128.0.0/9	tcp:0-65535 udp:0-65535 icmp	Allow	65534

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 ↑	Firewall rules	Description
No rows to display			

Firewall logs configured ✕



00:46:37

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Google Cloud username 1
student-01-51cbefeec2f0

Google Cloud password 1
gxHXUZAapAEq

Google Cloud project ID
qwiklabs-gcp-02-914ec56

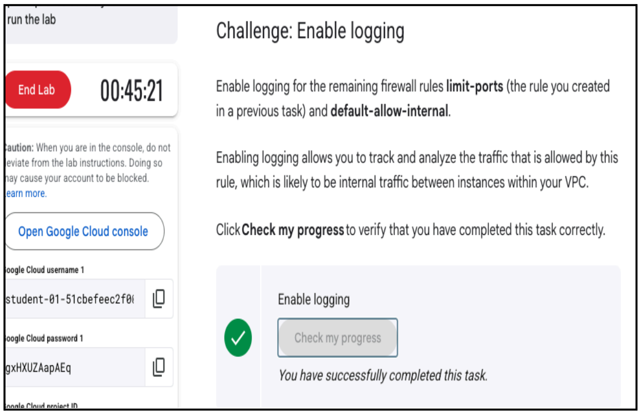
Challenge: Customize firewall rules

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.

✓ Customize firewall rules

You have successfully completed this task.



run the lab

00:45:21

aution: When you are in the console, do not eviate from the lab instructions. Doing so ay cause your account to be blocked. earn more.

oogle Cloud username 1
student-01-51cbefeec2f0

oogle Cloud password 1
gxHXUZAapAEq

oogle Cloud project ID

Challenge: Enable logging

Enable logging for the remaining firewall rules **limit-ports** (the rule you 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 traffic between instances within your VPC.

Click **Check my progress** to verify that you have completed this task correctly.

✓ Enable logging

You have successfully completed this task.

Task 6: Verify Compliance

The lab assessment returned a perfect score. Vulnerabilities identified in the PCI DSS 3.2.1 report required for this lab were remediated.

My Assessment:

This capstone lab presented a number of tasks that implemented challenges based on previous labs. In labs from other courses of this certificate program, step by step instructions were provided, however in the capstone these instructions did not exist forcing a more independent sense of completing the tasks.

Overall, I gained a wealth of knowledge in this specific program, including aspects of cybersecurity that I didn't think I would be prepared for upon entering the workforce. I was able to mitigate risks, remediate vulnerabilities, analyze logs, create firewalls, understand IDR, security frameworks, as well as create compliance reports, and other learning tools that enhanced my cybersecurity knowledge, specifically within Google Cloud.