https://www.skills.google/focuses/46415150?parent=lti_session

Tarefa 1: identifique vulnerabilidades com o Security Command Center (SCC)

Nesta tarefa, você vai usar o Security Command Center (SCC) para verificar o status de conformidade do seu projeto e identificar as vulnerabilidades de alto e médio risco que precisam ser corrigidas.

1. No **Menu de navegação** (☰) do console do Google Cloud, selecione **Segurança** > **Visão geral**. A página de visão geral do Security Command Center será aberta.
2. No menu **Security Command Center**, clique em **Vulnerabilidades**. A página "Vulnerabilidades" será aberta.

Existem muitas vulnerabilidades ativas listadas. Você pode usar o filtro para procurar as descobertas especificadas usando o **ID do módulo**. Você se concentrará nas descobertas a seguir ativas listadas para seu bucket de armazenamento:

- **ACL de bucket público (PUBLIC_BUCKET_ACL)**: indica que há uma entrada de lista de controle de acesso (ACL) para o bucket de armazenamento que é acessível publicamente. Isso significa que qualquer pessoa na Internet pode ler arquivos armazenados no bucket. Essa é uma vulnerabilidade de segurança de alto risco que precisa ter a correção priorizada.
- **Somente a política do bucket desativada (BUCKET_POLICY_ONLY_DISABLED)**: essa entrada indica que permissões uniformes no nível do bucket não estão ativadas em um bucket. O acesso uniforme no nível do bucket oferece uma maneira de controlar quem pode acessar buckets e objetos do Cloud Storage, simplificando a forma como você concede acesso aos recursos do Cloud Storage. Essa é uma vulnerabilidade de risco médio que também precisa ser corrigida.
- **Geração de registros de bucket desativada (BUCKET_LOGGING_DISABLED)**: essa entrada indica que há um bucket de armazenamento sem a geração de registros ativada. Essa é uma vulnerabilidade de baixo risco sem necessidade de correção neste cenário.

Observação*: se a entrada* ***ACL de bucket público*** *ou* ***Somente a política do bucket desativada*** *não estiverem listadas ou não exibirem nenhuma descoberta ativa, talvez seja necessário aguardar alguns minutos e atualizar a página. Aguarde até que essas vulnerabilidades exibam descobertas ativas antes de continuar.*

Em seguida, gere um relatório de conformidade que confirme os problemas de vulnerabilidade.

3. No menu **Security Command Center**, clique em **conformidade**. A página "conformidade" será aberta.

4. Na seção **Padrões de conformidade do Google Cloud**, clique em **Ver detalhes** no bloco **CIS Google Cloud Platform Foundation 2.0**. O relatório CIS Google Cloud Platform Foundation 2.0 será aberto.

5. Clique na coluna **Descobertas** para classificar as informações e mostrar as descobertas ativas no topo da lista.

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

checkCloud Storage buckets should not be anonymously or publicly accessible

VMs should not be assigned public IP addresses

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

checkBucket policy only should be Enabled

Tarefa 2: corrija as vulnerabilidades de segurança

Nesta tarefa, você vai corrigir as vulnerabilidades de segurança identificadas na etapa anterior. Em seguida, você vai verificar o status de segurança do bucket do Cloud Storage no relatório para confirmar se os problemas foram corrigidos.

1. No **Menu de navegação** (☰) do console do Google Cloud, selecione **Cloud Storage** > **Buckets**.

2. Na seção **Filtro**, clique no link do **nome** do bucket do seu projeto (BUCKET_NAME). A página de detalhes "Bucket" será aberta.

3. Clique na guia **Permissões**. A seção **Permissões** lista todas as permissões fornecidas para o bucket.

Para começar, remova o acesso público ao bucket do Cloud Storage.

4. Na seção **Permissões**, clique na guia **Visualizar por papéis**.

5. Abra o papel **Leitor de objetos do Storage** e marque a caixa de seleção para **allUsers.**

6. Clique em **Remover acesso**.

7. Vai aparecer um pop-up para você confirmar a remoção do acesso. Verifique se a opção **Remover todos os usuários do papel Leitor de objetos de armazenamento neste recurso** está selecionada e clique em **Remover**.

Depois, mude o controle de acesso para uniforme. Isso aplicará um conjunto único (uniforme) de permissões para o bucket e seus objetos.

8. No bloco **Controle de acesso**, clique em **Mudar para uniforme**.

9. Na caixa de diálogo **Editar controle de acesso**, selecione **Uniforme**.

10. Clique em **Salvar**.

Por fim, gere um relatório de conformidade para verificar se os problemas de vulnerabilidade foram corrigidos.

11. No **Menu de navegação** (☰) do console do Google Cloud, selecione **Segurança** > **conformidade**.

12. No bloco **CIS Google Cloud Platform Foundation 2.0**, clique em **Ver detalhes** para abrir o relatório novamente.

O número de descobertas ativas para as regras **Os buckets do Cloud Storage não podem ser acessíveis anonimamente ou publicamente** e **A política de bucket apenas precisa estar Ativada** agora precisa ser **0**. Isso indica que as vulnerabilidades **ACL de bucket público** e **Somente a política do bucket desativada** do bucket do Cloud Storage foram corrigidas.

Observação*: se as descobertas ativas das opções* ***ACL de bucket público*** *ou* ***Somente a política do bucket desativada*** *não aparecerem como* ***0*** *(zero) depois que você corrigir as vulnerabilidades, talvez seja necessário aguardar alguns minutos e atualizar a página.*

Clique em **Verificar meu progresso** para confirmar que você concluiu a tarefa corretamente.

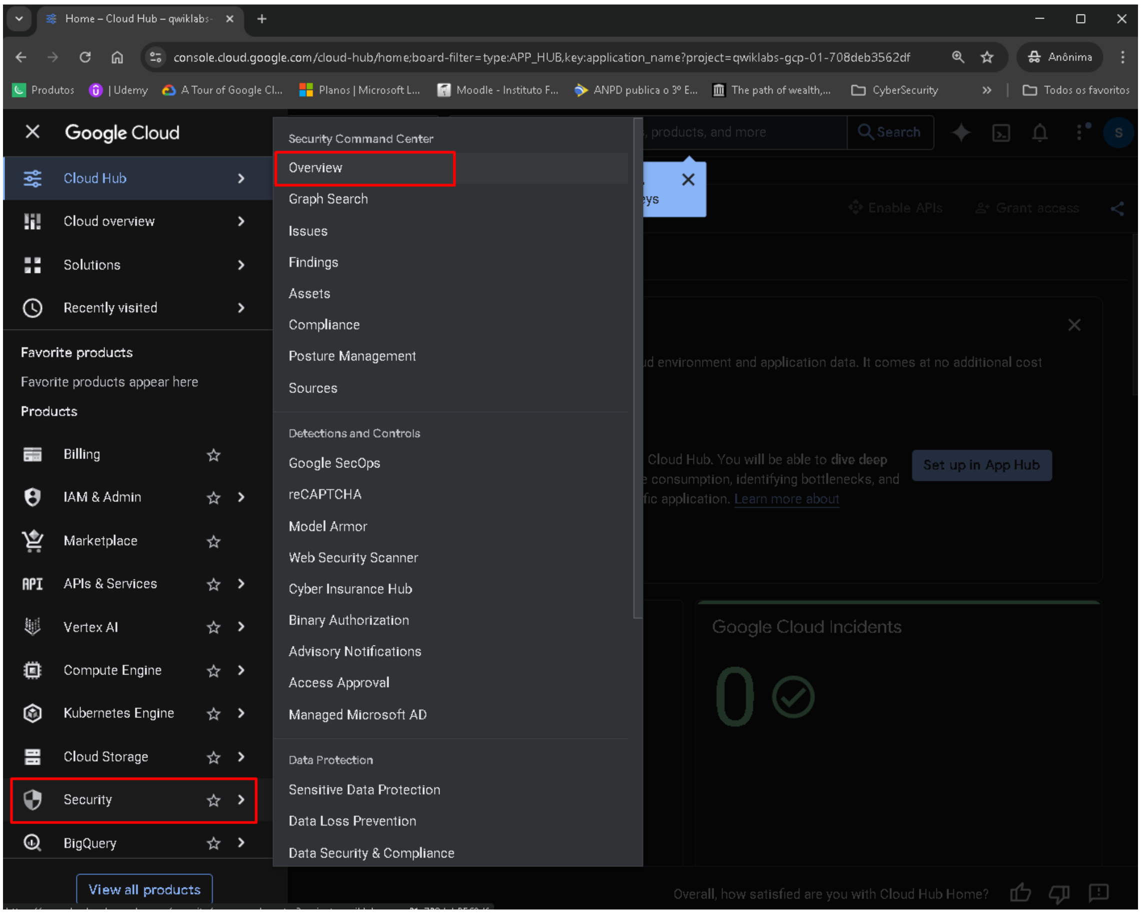
Corrigir as vulnerabilidades de segurança

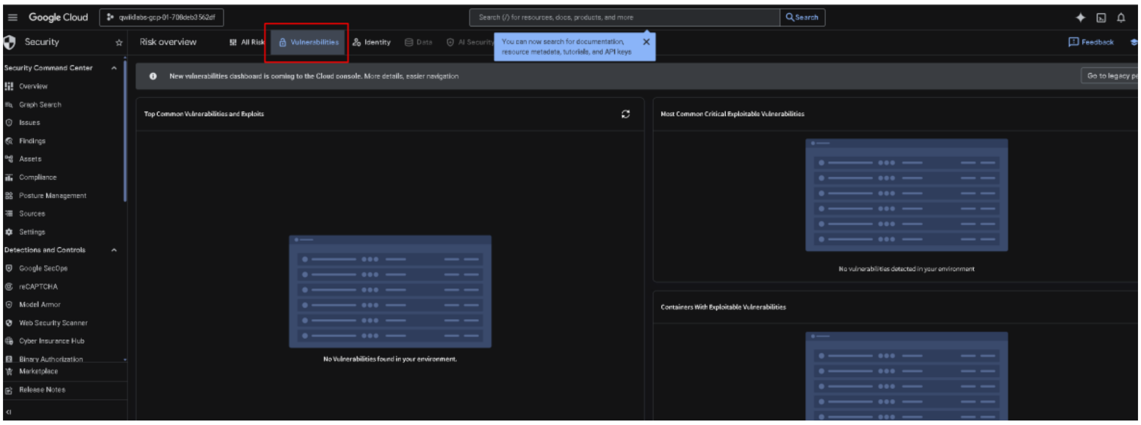
Conclusão

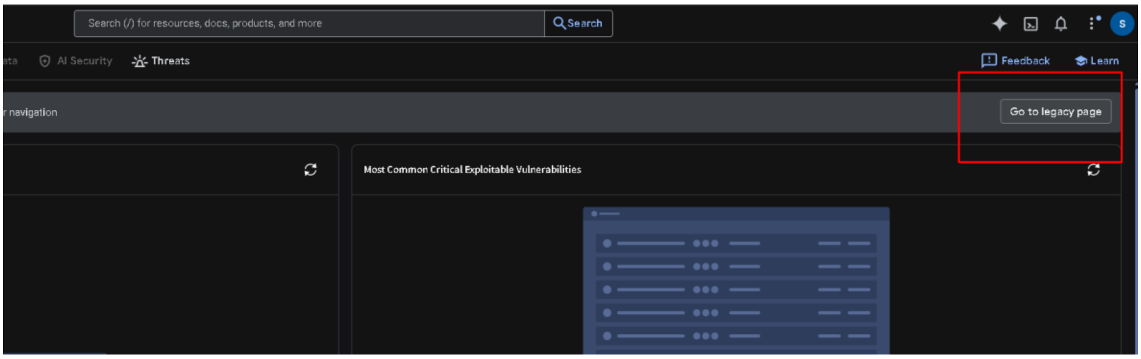
Bom trabalho!

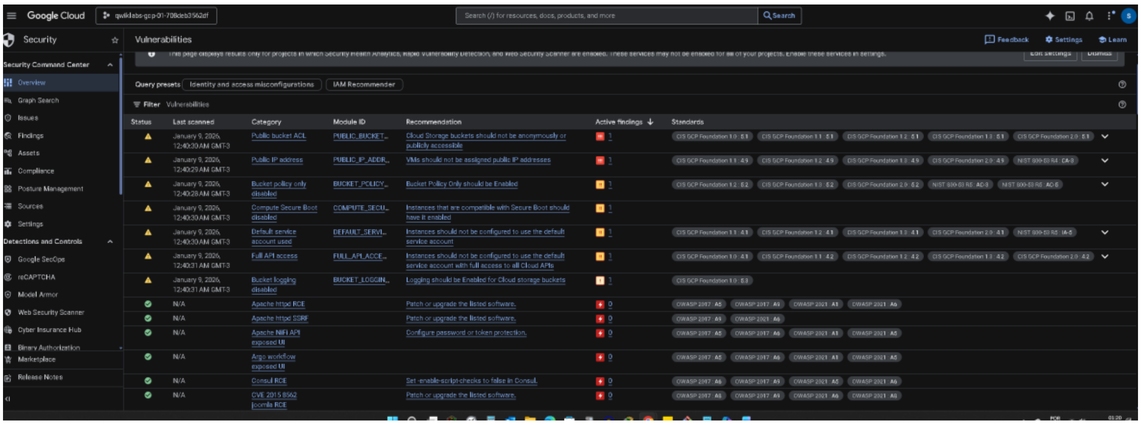
Ao longo deste laboratório, você adquiriu experiência prática na identificação e priorização de ameaças usando o Security Command Center. Você também corrigiu as vulnerabilidades identificadas no seu projeto e gerou um relatório para confirmar que as vulnerabilidades foram corrigidas.

Ao corrigir as vulnerabilidades e garantir o status de conformidade do bucket do Cloud Storage, você ajudou sua organização a evitar violações de dados, acesso não autorizado e perda de dados.



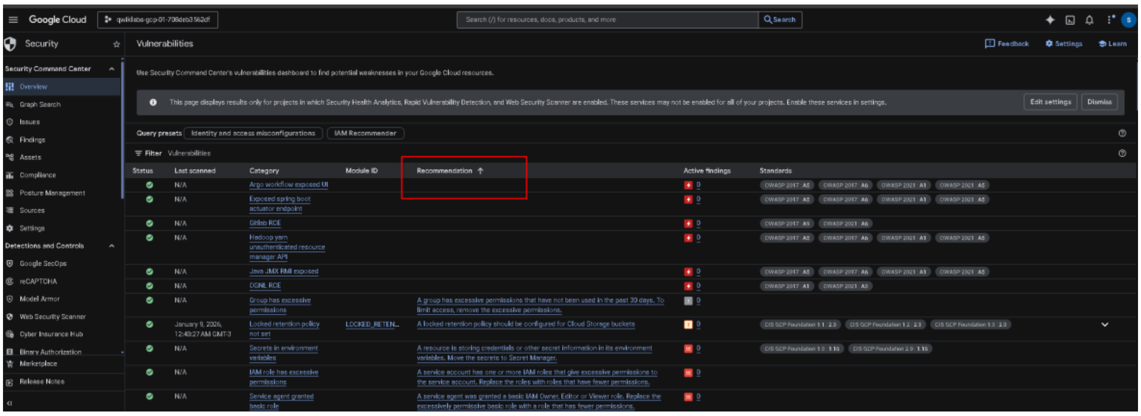

Google Cloud
qwiklabs-gcp-01-708deb3562df
Search (/) for resources, docs, products, and more
Search
Security
Risk overview
All Risk
Vulnerabilities
Identity
Data
AI Security
You can now search for documentation, resource metadata, tutorials, and API keys
Feedback
Security Command Center
Overview
Graph Search
Issues
Findings
Assets
Compliance
Posture Management
Sources
Settings
Detections and Controls
Google SecOps
reCAPTCHA
Model Armor
Web Security Scanner
Cyber Insurance Hub
Binary Authorization
Marketplace
Release Notes
New vulnerabilities dashboard is coming to the Cloud console. More details, easier navigation
Go to legacy pa
Top Common Vulnerabilities and Exploits
No Vulnerabilities found in your environment.
Most Common Critical Exploitable Vulnerabilities
No vulnerabilities detected in your environment
Containers With Exploitable Vulnerabilities


Search (/) for resources, docs, products, and more
Search
ata
AI Security
Threats
Feedback
Learn
r navigation
Go to legacy page
Most Common Critical Exploitable Vulnerabilities



This page displays results only for projects in which Security Health Analytics, Rapid Vulnerability Detection, and Web Security Scanner are enabled. These services may not be enabled for all of your projects. Enable these services in settings.

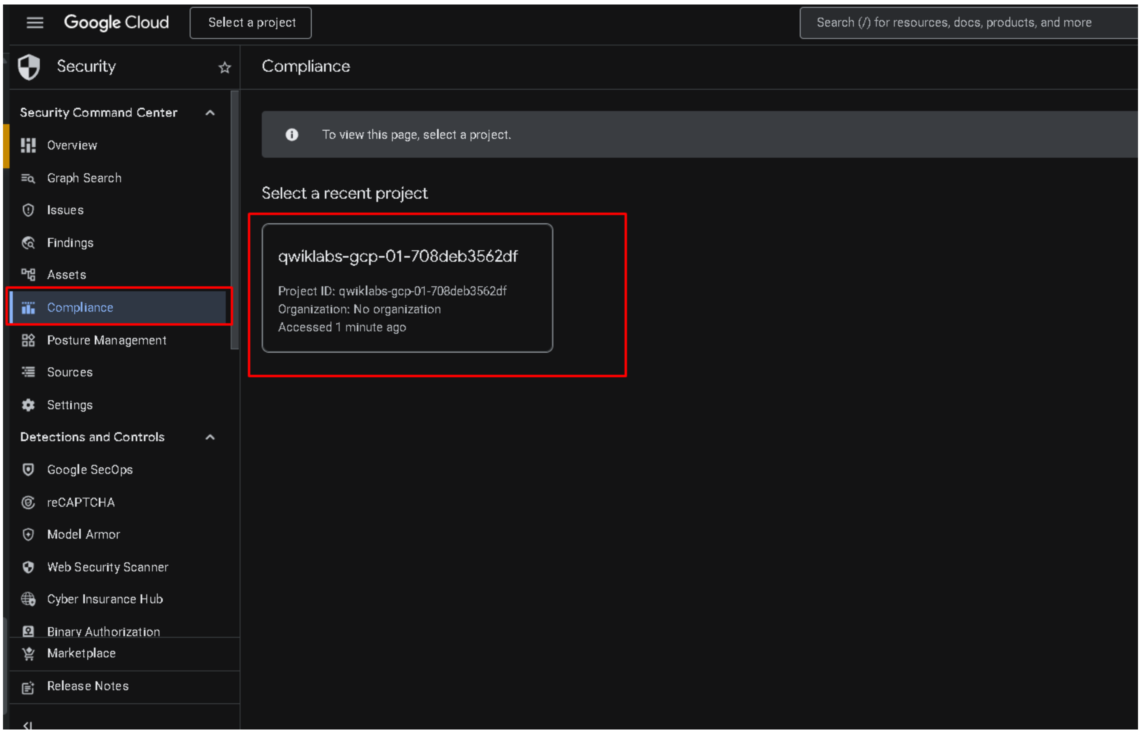
Status	Last scanned	Category	Module ID	Recommendation	Active findings ↓	Standards
▲	January 9, 2026, 12:40:30 AM GMT-3	Public bucket ACL	PUBLIC_BUCKET_...	Cloud Storage buckets should not be anonymously or publicly accessible	1	CIS GCP Foundation 1.0 : 5.1 CIS GCP Foundation 1.1 : 5.1 CIS GCP Foundation 1.2 : 5.1 CIS GCP Foundation 1.3 : 5.1 CIS GCP Foundation 2.0 : 5.1
▲	January 9, 2026, 12:40:29 AM GMT-3	Public IP address	PUBLIC_IP_ADDR_...	VMs should not be assigned public IP addresses	1	CIS GCP Foundation 1.1 : 4.9 CIS GCP Foundation 1.2 : 4.9 CIS GCP Foundation 1.3 : 4.9 CIS GCP Foundation 2.0 : 4.9 NIST 800-53 R4 : CA-3
▲	January 9, 2026, 12:40:28 AM GMT-3	Bucket policy only disabled	BUCKET_POLICY_...	Bucket Policy Only should be Enabled	1	CIS GCP Foundation 1.2 : 5.2 CIS GCP Foundation 1.3 : 5.2 CIS GCP Foundation 2.0 : 5.2 NIST 800-53 R5 : AC-3 NIST 800-53 R5 : AC-6
▲	January 9, 2026, 12:40:30 AM GMT-3	Compute Secure Boot disabled	COMPUTE_SECU_...	Instances that are compatible with Secure Boot should have it enabled	1	
▲	January 9, 2026, 12:40:30 AM GMT-3	Default service account used	DEFAULT_SERVI_...	Instances should not be configured to use the default service account	1	CIS GCP Foundation 1.1 : 4.1 CIS GCP Foundation 1.2 : 4.1 CIS GCP Foundation 1.3 : 4.1 CIS GCP Foundation 2.0 : 4.1 NIST 800-53 R5 : IA-5
▲	January 9, 2026, 12:40:31 AM GMT-3	Full API access	FULL_API_ACCE_...	Instances should not be configured to use the default service account with full access to all Cloud APIs	1	CIS GCP Foundation 1.0 : 4.1 CIS GCP Foundation 1.1 : 4.2 CIS GCP Foundation 1.2 : 4.2 CIS GCP Foundation 1.3 : 4.2 CIS GCP Foundation 2.0 : 4.2
▲	January 9, 2026, 12:40:31 AM GMT-3	Bucket logging disabled	BUCKET_LOGGIN_...	Logging should be Enabled for Cloud storage buckets	1	CIS GCP Foundation 1.0 : 5.3
✓	N/A	Apache httpd RCE		Patch or upgrade the listed software.	0	OWASP 2017 : A5 OWASP 2017 : A9 OWASP 2021 : A1 OWASP 2021 : A6
✓	N/A	Apache httpd SSRF		Patch or upgrade the listed software.	0	OWASP 2017 : A9 OWASP 2021 : A6
✓	N/A	Apache NiFi API exposed UI		Configure password or token protection.	0	OWASP 2017 : A5 OWASP 2017 : A6 OWASP 2021 : A1 OWASP 2021 : A5
✓	N/A	Argo workflow exposed UI			0	OWASP 2017 : A5 OWASP 2017 : A6 OWASP 2021 : A1 OWASP 2021 : A5
✓	N/A	Consul RCE		Set -enable-script-checks to false in Consul.	0	OWASP 2017 : A6 OWASP 2017 : A9 OWASP 2021 : A5 OWASP 2021 : A6
✓	N/A	CVE 2015 8562 Joomla RCE		Patch or upgrade the listed software.	0	OWASP 2017 : A6 OWASP 2017 : A9 OWASP 2021 : A6 OWASP 2021 : A8



Use Security Command Center's vulnerabilities dashboard to find potential weaknesses in your Google Cloud resources.

This page displays results only for projects in which Security Health Analytics, Rapid Vulnerability Detection, and Web Security Scanner are enabled. These services may not be enabled for all of your projects. Enable these services in settings.

Status	Last scanned	Category	Module ID	Recommendation ↑	Active findings	Standards
✓	N/A	Argo workflow exposed UI			0	OWASP 2017 : A5 OWASP 2017 : A6 OWASP 2021 : A1 OWASP 2021 : A5
✓	N/A	Exposed spring boot actuator endpoint			0	OWASP 2017 : A5 OWASP 2017 : A6 OWASP 2021 : A1 OWASP 2021 : A5
✓	N/A	Gitlab RCE			0	OWASP 2017 : A9 OWASP 2021 : A6
✓	N/A	Hadoop yarn unauthenticated resource manager API			0	OWASP 2017 : A5 OWASP 2017 : A6 OWASP 2021 : A1 OWASP 2021 : A5
✓	N/A	Java JMX RMI exposed			0	OWASP 2017 : A5 OWASP 2017 : A6 OWASP 2021 : A1 OWASP 2021 : A5
✓	N/A	OGNL RCE			0	OWASP 2017 : A1 OWASP 2021 : A3
✓	N/A	Group has excessive permissions		A group has excessive permissions that have not been used in the past 30 days. To limit access, remove the excessive permissions.	0	
✓	January 9, 2026, 12:40:27 AM GMT-3	Locked retention policy not set	LOCKED_RETEN_...	A locked retention policy should be configured for Cloud Storage buckets	0	CIS GCP Foundation 1.1 : 2.3 CIS GCP Foundation 1.2 : 2.3 CIS GCP Foundation 1.3 : 2.3
✓	N/A	Secrets in environment variables		A resource is storing credentials or other secret information in its environment variables. Move the secrets to Secret Manager.	0	CIS GCP Foundation 1.3 : 1.18 CIS GCP Foundation 2.0 : 1.18
✓	N/A	IAM role has excessive permissions		A service account has one or more IAM roles that give excessive permissions to the service account. Replace the roles with roles that have fewer permissions.	0	
✓	N/A	Service agent granted basic role		A service agent was granted a basic IAM Owner, Editor or Viewer role. Replace the excessively permissive basic role with a role that has fewer permissions.	0	



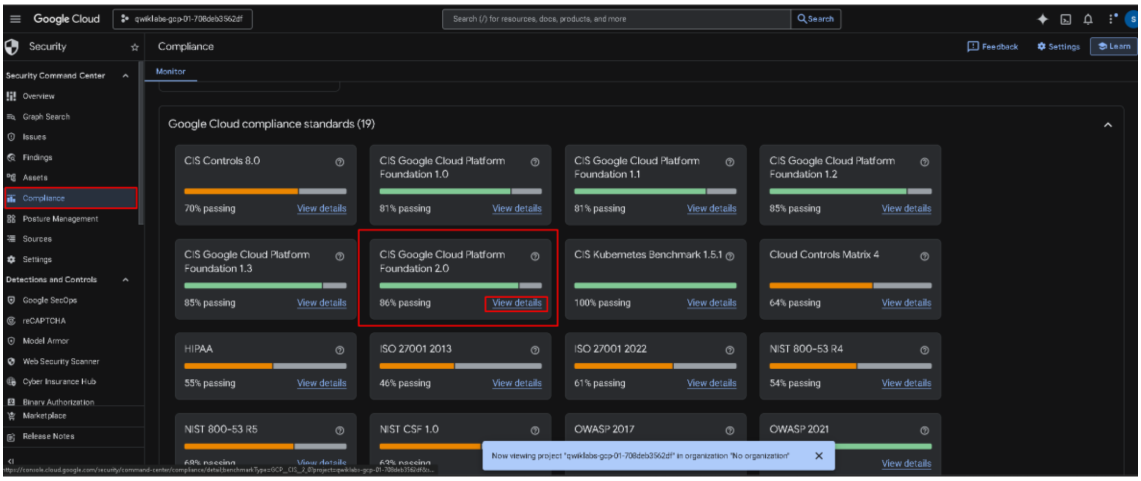
Compliance

To view this page, select a project.

Select a recent project

qwiklabs-gcp-01-708deb3562df

Project ID: qwiklabs-gcp-01-708deb3562df
Organization: No organization
Accessed 1 minute ago



Compliance

Google Cloud compliance standards (19)

CIS Controls 8.0
70% passing View details

CIS Google Cloud Platform Foundation 1.0
81% passing View details

CIS Google Cloud Platform Foundation 1.1
81% passing View details

CIS Google Cloud Platform Foundation 1.2
85% passing View details

CIS Google Cloud Platform Foundation 1.3
85% passing View details

CIS Google Cloud Platform Foundation 2.0
86% passing View details

CIS Kubernetes Benchmark 1.5.1
100% passing View details

Cloud Controls Matrix 4
64% passing View details

HIPAA
55% passing View details

ISO 27001 2013
46% passing View details

ISO 27001 2022
61% passing View details

NIST 800-53 R4
54% passing View details

NIST 800-53 R5
68% passing View details

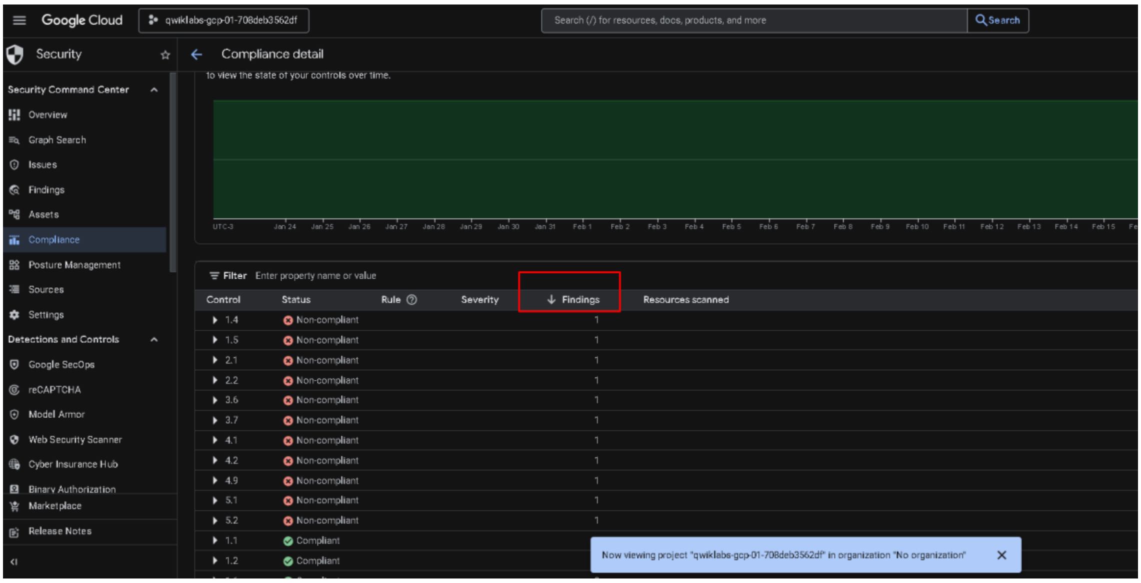
NIST CSF 1.0
63% passing

OWASP 2017

OWASP 2021
View details

Now viewing project "qwiklabs-gcp-01-708deb3562df" in organization "No organization"

https://console.cloud.google.com/security/command-center/compliance/detail;benchmarkType=GCP__CIS__2_0?project=qwiklabs-gcp-01-708deb3562df&s...

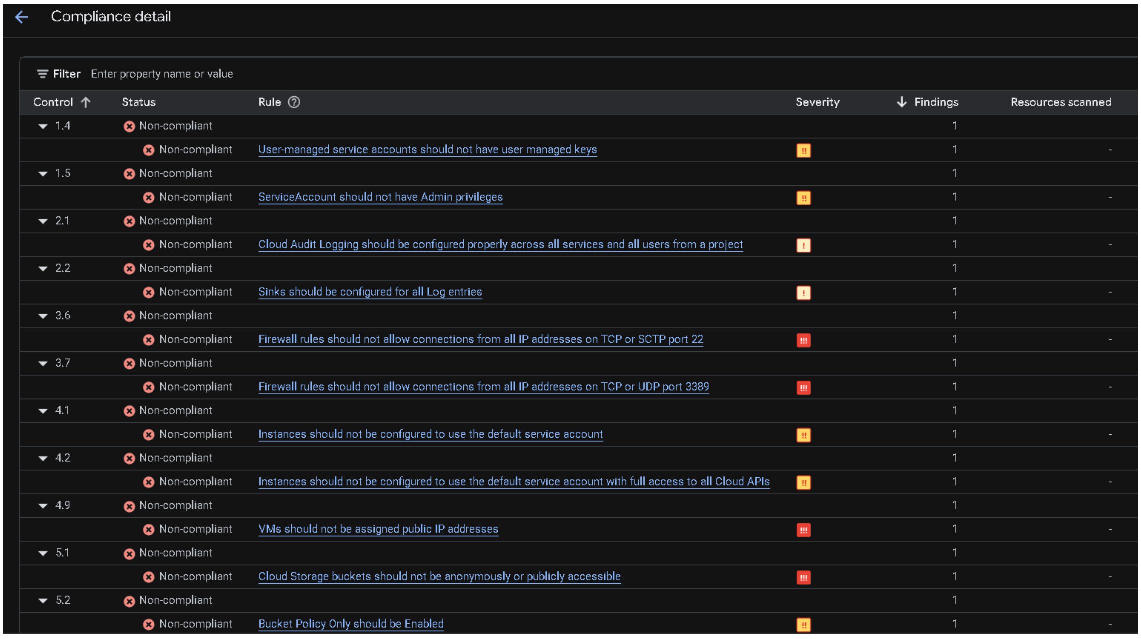


Compliance detail

to view the state of your controls over time.

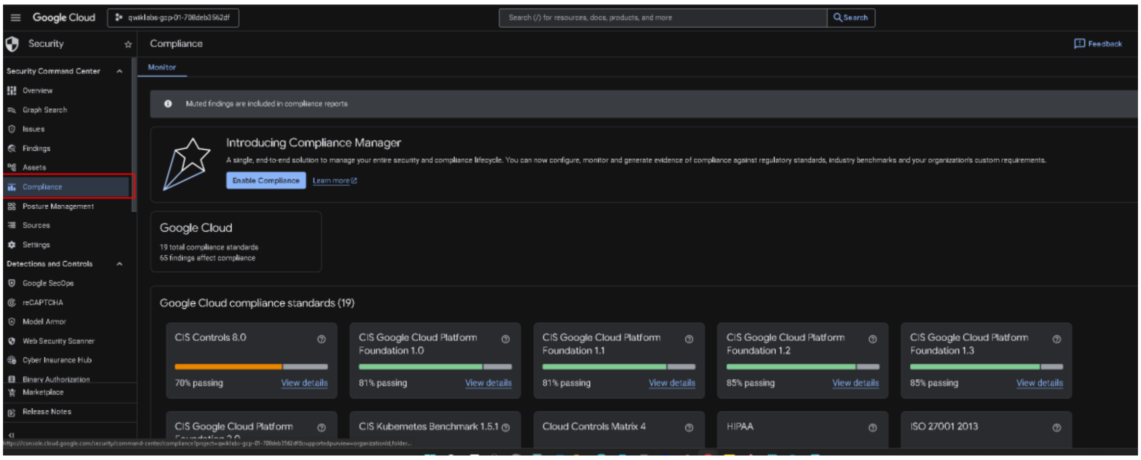
Control	Status	Rule	Severity	↓ Findings	Resources scanned
1.4	✖ Non-compliant			1	
1.5	✖ Non-compliant			1	
2.1	✖ Non-compliant			1	
2.2	✖ Non-compliant			1	
3.6	✖ Non-compliant			1	
3.7	✖ Non-compliant			1	
4.1	✖ Non-compliant			1	
4.2	✖ Non-compliant			1	
4.9	✖ Non-compliant			1	
5.1	✖ Non-compliant			1	
5.2	✖ Non-compliant			1	
1.1	✓ Compliant				
1.2	✓ Compliant				

Now viewing project "qwiklabs-gcp-01-708deb3562df" in organization "No organization"



Compliance detail

Control ↑	Status	Rule	Severity	↓ Findings	Resources scanned
1.4	✖ Non-compliant			1	
	✖ Non-compliant	User-managed service accounts should not have user managed keys	!!	1	-
1.5	✖ Non-compliant			1	
	✖ Non-compliant	ServiceAccount should not have Admin privileges	!!	1	-
2.1	✖ Non-compliant			1	
	✖ Non-compliant	Cloud Audit Logging should be configured properly across all services and all users from a project	!	1	-
2.2	✖ Non-compliant			1	
	✖ Non-compliant	Sinks should be configured for all Log entries	!	1	-
3.6	✖ Non-compliant			1	
	✖ Non-compliant	Firewall rules should not allow connections from all IP addresses on TCP or SCTP port 22	!!!	1	-
3.7	✖ Non-compliant			1	
	✖ Non-compliant	Firewall rules should not allow connections from all IP addresses on TCP or UDP port 3389	!!!	1	-
4.1	✖ Non-compliant			1	
	✖ Non-compliant	Instances should not be configured to use the default service account	!!	1	-
4.2	✖ Non-compliant			1	
	✖ Non-compliant	Instances should not be configured to use the default service account with full access to all Cloud APIs	!!	1	-
4.9	✖ Non-compliant			1	
	✖ Non-compliant	VMs should not be assigned public IP addresses	!!!	1	-
5.1	✖ Non-compliant			1	
	✖ Non-compliant	Cloud Storage buckets should not be anonymously or publicly accessible	!!!	1	-
5.2	✖ Non-compliant			1	
	✖ Non-compliant	Bucket Policy Only should be Enabled	!!	1	-



Muted findings are included in compliance reports

Introducing Compliance Manager

A single, end-to-end solution to manage your entire security and compliance lifecycle. You can now configure, monitor and generate evidence of compliance against regulatory standards, industry benchmarks and your organization's custom requirements.

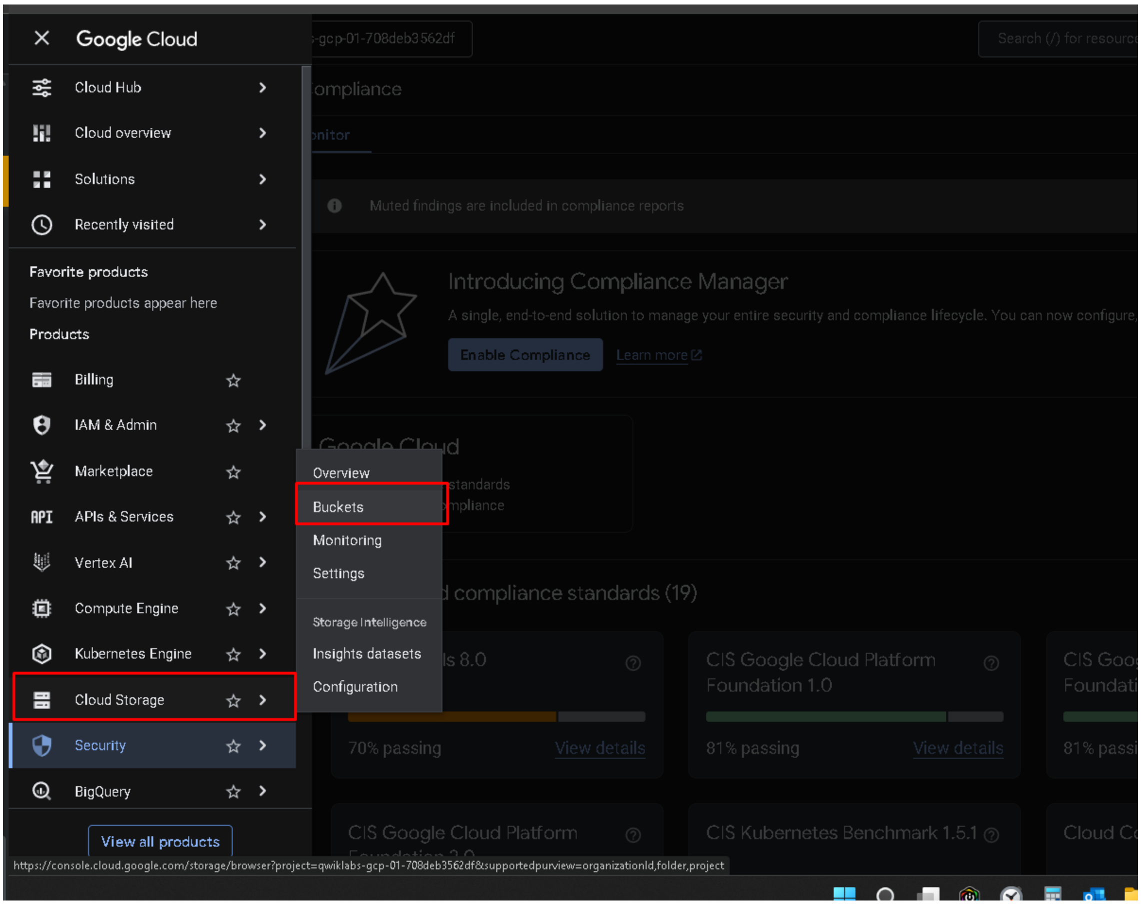
Google Cloud

19 total compliance standards
65 findings affect compliance

Google Cloud compliance standards (19)

Standard	Passing	
CIS Controls 8.0	70% passing	View details
CIS Google Cloud Platform Foundation 1.0	81% passing	View details
CIS Google Cloud Platform Foundation 1.1	81% passing	View details
CIS Google Cloud Platform Foundation 1.2	85% passing	View details
CIS Google Cloud Platform Foundation 1.3	85% passing	View details
CIS Google Cloud Platform Foundation 2.0		
CIS Kubernetes Benchmark 1.5.1		
Cloud Controls Matrix 4		
HIPAA		
ISO 27001 2013		

https://console.cloud.google.com/security/command-center/compliance?project=qwiklabs-gcp-01-708deb3562df&supportedpurview=organizationId,folder...



Muted findings are included in compliance reports

Introducing Compliance Manager

A single, end-to-end solution to manage your entire security and compliance lifecycle. You can now configure,

Google Cloud

standards
mpliance

d compliance standards (19)

ls 8.0 — 70% passing — View details

CIS Google Cloud Platform Foundation 1.0 — 81% passing — View details

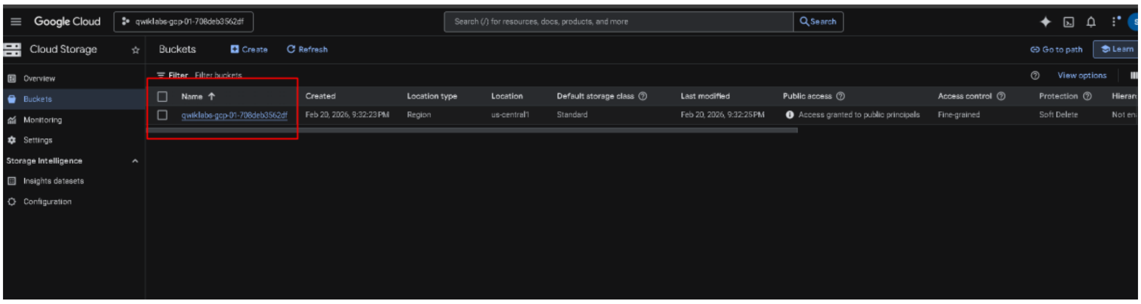
CIS Goo Foundati — 81% passi

CIS Google Cloud Platform Foundation 2.0

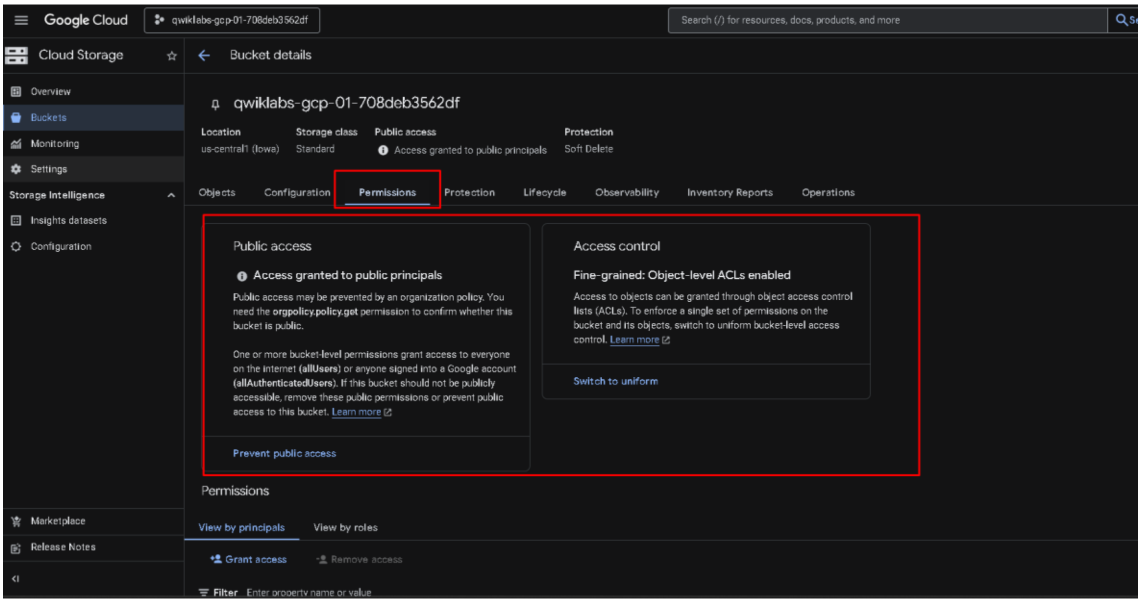
CIS Kubernetes Benchmark 1.5.1

Cloud C

https://console.cloud.google.com/storage/browser?project=qwiklabs-gcp-01-708deb3562df&supportedpurview=organizationId,folder,project



☐	Name ↑	Created	Location type	Location	Default storage class	Last modified	Public access	Access control	Protection	Hieran
☐	qwiklabs-gcp-01-708deb3562df	Feb 20, 2026, 9:32:23 PM	Region	us-central1	Standard	Feb 20, 2026, 9:32:25 PM	Access granted to public principals	Fine-grained	Soft Delete	Not en



qwiklabs-gcp-01-708deb3562df

Location	Storage class	Public access	Protection
us-central1 (Iowa)	Standard	Access granted to public principals	Soft Delete

Public access

Access granted to public principals

Public access may be prevented by an organization policy. You need the **orgpolicy.policy.get** permission to confirm whether this bucket is public.

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

Prevent public access

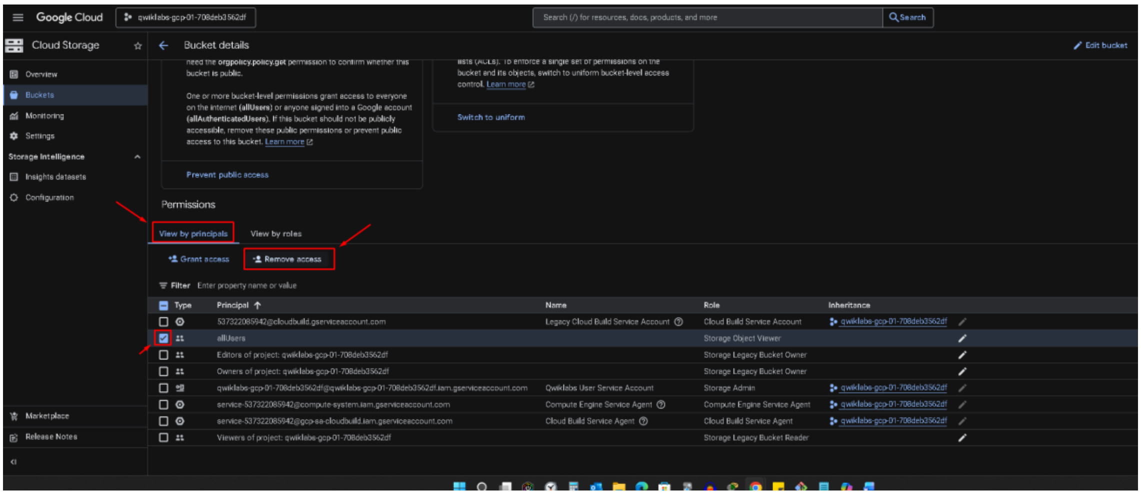
Access control

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

Permissions



need the **orgpolicy.policy.get** permission to confirm whether this bucket is public.

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

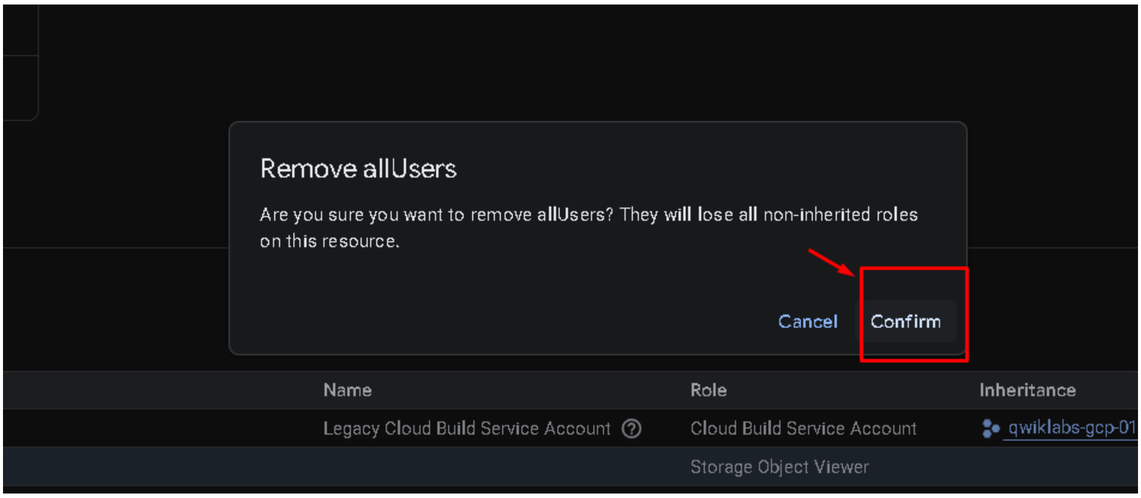
Prevent public access

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

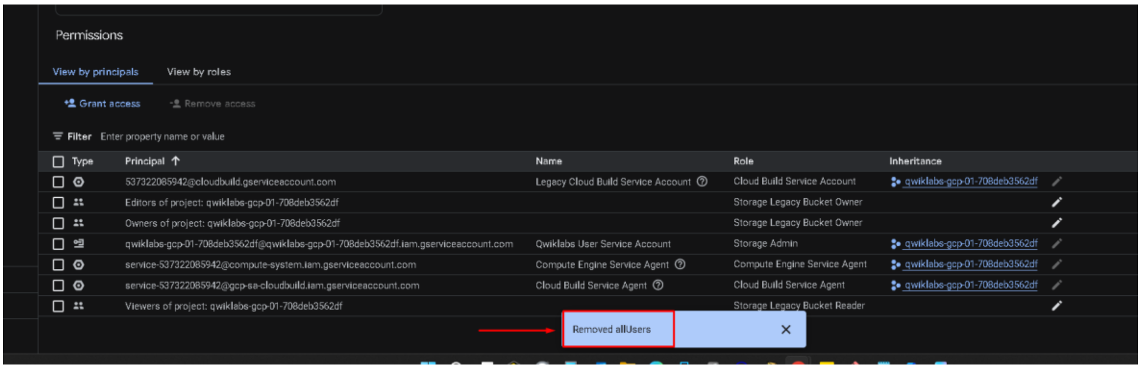
☐	Type	Principal ↑	Name	Role	Inheritance
☐		537322085942@cloudbuild.gserviceaccount.com	Legacy Cloud Build Service Account	Cloud Build Service Account	qwiklabs-gcp-01-708deb3562df
☑		allUsers		Storage Object Viewer	
☐		Editors of project: qwiklabs-gcp-01-708deb3562df		Storage Legacy Bucket Owner	
☐		Owners of project: qwiklabs-gcp-01-708deb3562df		Storage Legacy Bucket Owner	
☐		qwiklabs-gcp-01-708deb3562df@qwiklabs-gcp-01-708deb3562df.iam.gserviceaccount.com	Qwiklabs User Service Account	Storage Admin	qwiklabs-gcp-01-708deb3562df
☐		service-537322085942@compute-system.iam.gserviceaccount.com	Compute Engine Service Agent	Compute Engine Service Agent	qwiklabs-gcp-01-708deb3562df
☐		service-537322085942@gcp-sa-cloudbuild.iam.gserviceaccount.com	Cloud Build Service Agent	Cloud Build Service Agent	qwiklabs-gcp-01-708deb3562df
☐		Viewers of project: qwiklabs-gcp-01-708deb3562df		Storage Legacy Bucket Reader	



Remove allUsers

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

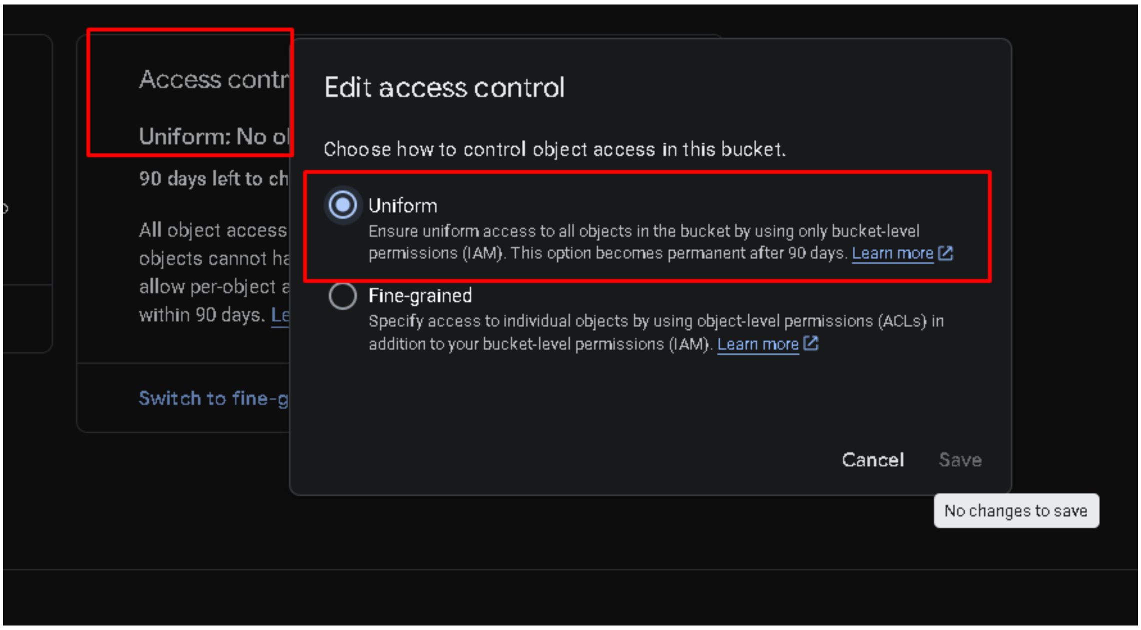
Name	Role	Inheritance
Legacy Cloud Build Service Account	Cloud Build Service Account	qwiklabs-gcp-01
	Storage Object Viewer	



Permissions

□ Type	Principal ↑	Name	Role	Inheritance
□	537322085942@cloudbuild.gserviceaccount.com	Legacy Cloud Build Service Account	Cloud Build Service Account	qwiklabs-gcp-01-708deb3562df
□	Editors of project: qwiklabs-gcp-01-708deb3562df		Storage Legacy Bucket Owner	
□	Owners of project: qwiklabs-gcp-01-708deb3562df		Storage Legacy Bucket Owner	
□	qwiklabs-gcp-01-708deb3562df@qwiklabs-gcp-01-708deb3562df.iam.gserviceaccount.com	Qwiklabs User Service Account	Storage Admin	qwiklabs-gcp-01-708deb3562df
□	service-537322085942@compute-system.iam.gserviceaccount.com	Compute Engine Service Agent	Compute Engine Service Agent	qwiklabs-gcp-01-708deb3562df
□	service-537322085942@gcp-sa-cloudbuild.iam.gserviceaccount.com	Cloud Build Service Agent	Cloud Build Service Agent	qwiklabs-gcp-01-708deb3562df
□	Viewers of project: qwiklabs-gcp-01-708deb3562df		Storage Legacy Bucket Reader	

Removed allUsers ✕



Access contr

Uniform: No ol

90 days left to ch

All object access
objects cannot ha
allow per-object a
within 90 days. Le

Switch to fine-g

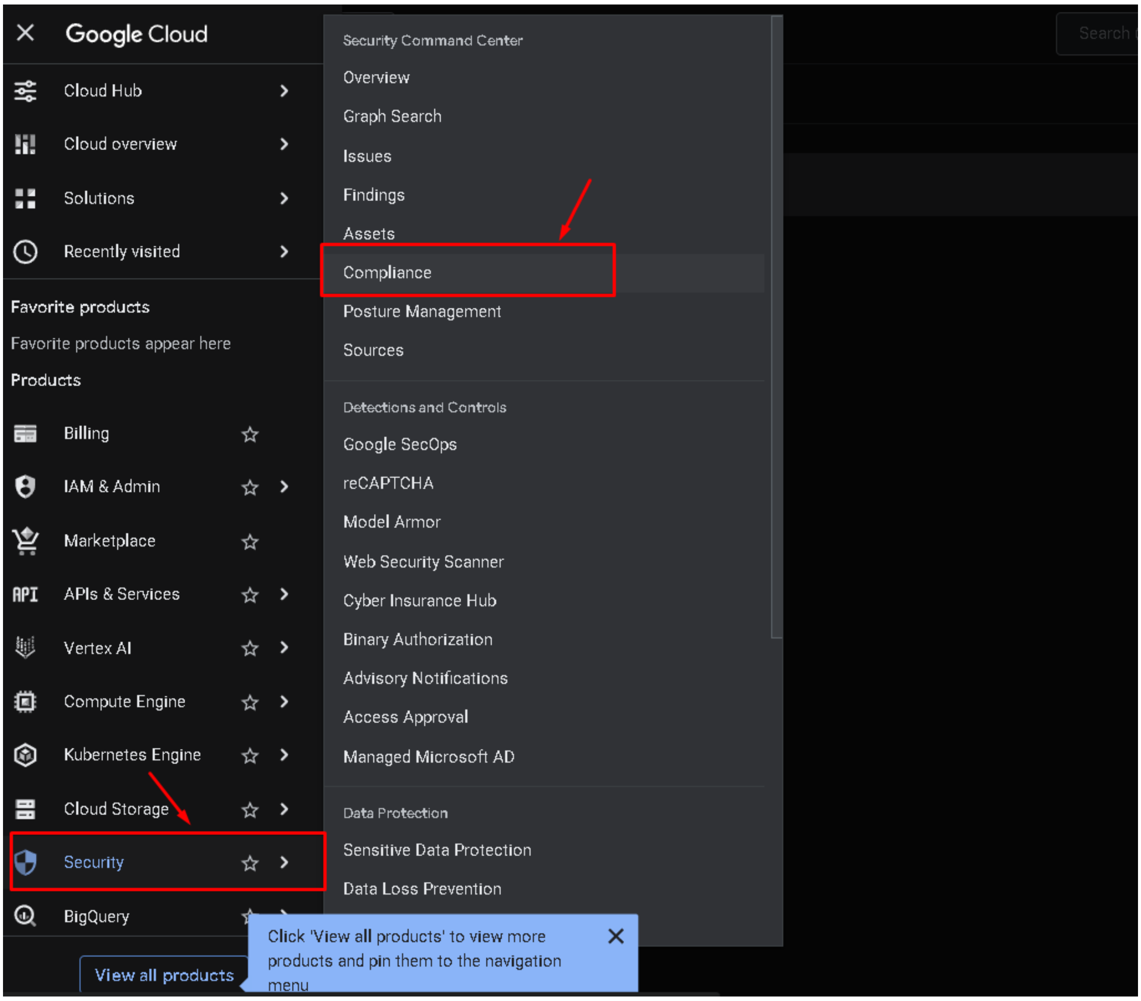
Edit access control

Choose how to control object access in this bucket.

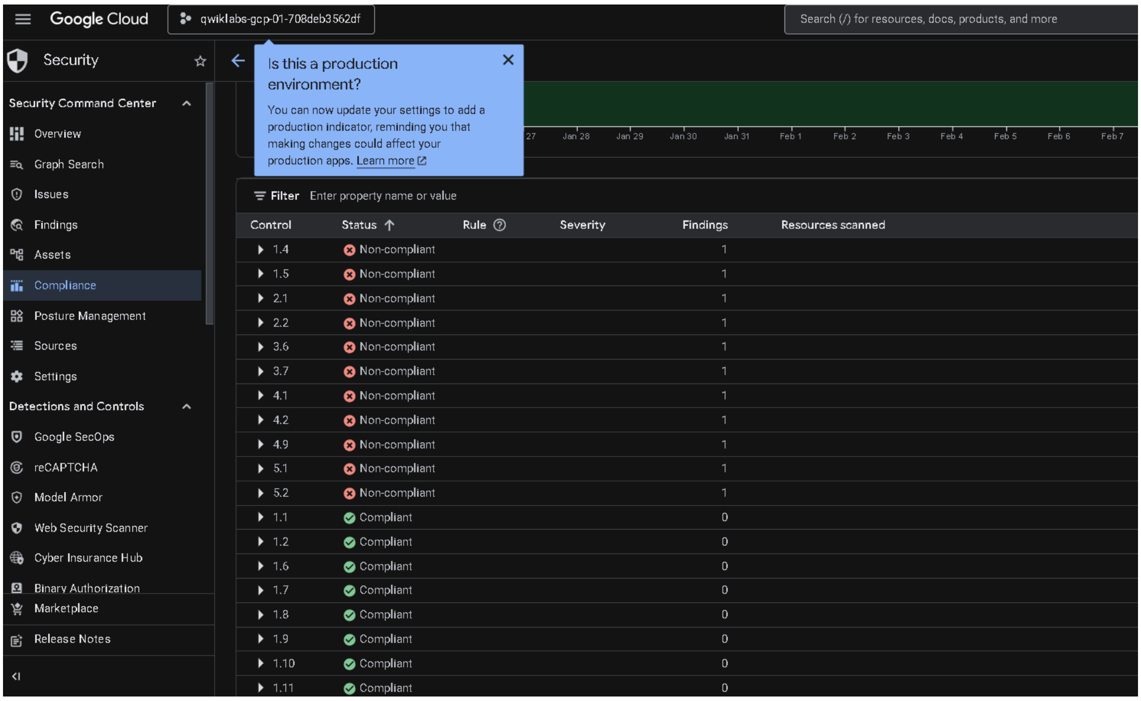
● Uniform
Ensure uniform access to all objects in the bucket by using only bucket-level permissions (IAM). This option becomes permanent after 90 days. Learn more

○ Fine-grained
Specify access to individual objects by using object-level permissions (ACLs) in addition to your bucket-level permissions (IAM). Learn more

No changes to save



Click 'View all products' to view more products and pin them to the navigation menu



Is this a production environment?

You can now update your settings to add a production indicator, reminding you that making changes could affect your production apps. Learn more

Control	Status	Rule	Severity	Findings	Resources scanned
1.4	Non-compliant			1	
1.5	Non-compliant			1	
2.1	Non-compliant			1	
2.2	Non-compliant			1	
3.6	Non-compliant			1	
3.7	Non-compliant			1	
4.1	Non-compliant			1	
4.2	Non-compliant			1	
4.9	Non-compliant			1	
5.1	Non-compliant			1	
5.2	Non-compliant			1	
1.1	Compliant			0	
1.2	Compliant			0	
1.6	Compliant			0	
1.7	Compliant			0	
1.8	Compliant			0	
1.9	Compliant			0	
1.10	Compliant			0	
1.11	Compliant			0	