1.9. Criar um papel no Google Cloud IAM.pdf

https://www.skills.google/focuses/46423428?parent=lti_session

Tarefa 1: criar um papel personalizado

Aplicar o princípio de privilégio mínimo é fundamental para o IAM. Ele garante que os usuários recebam apenas as permissões necessárias para executar as tarefas deles. Papéis personalizados fornecem uma maneira de adaptar as permissões às necessidades de uma organização, garantindo que elas não sejam amplas e excessivas para os usuários.

Nesta tarefa, você vai criar um papel personalizado para a equipe de auditoria da Cymbal. Em seguida, você vai conceder ao papel personalizado acesso restrito para visualizar o conteúdo do banco de dados.

1. No console do Google Cloud, no **menu de navegação** (☰), clique em **IAM e administrador** > **Papéis**. A página **Papéis** é aberta.
2. Na barra Explorador, próxima à parte de cima da página **Papéis**, clique em **+ Criar papel**.
3. Na caixa de diálogo **Criar papel**, especifique as configurações a seguir e deixe todas as configurações restantes como padrão:

Propriedade	Valor (digite ou selecione)
Cargo	Audit Team Reviewer
Descrição	Papel personalizado que permite que a equipe de auditoria conduza atividades de revisão. Esse papel concede acesso somente leitura aos recursos de bancos de dados do Firebase.
ID	CustomRole
Etapa da criação do papel	Disponibilidade geral

Cada papel personalizado pode receber uma **etapa da criação do papel** que reflete as diferentes fases de desenvolvimento, teste e implantação de um papel.

Essas etapas ajudam os usuários a entender o estado atual de um papel e a adequação dele para vários casos de uso.

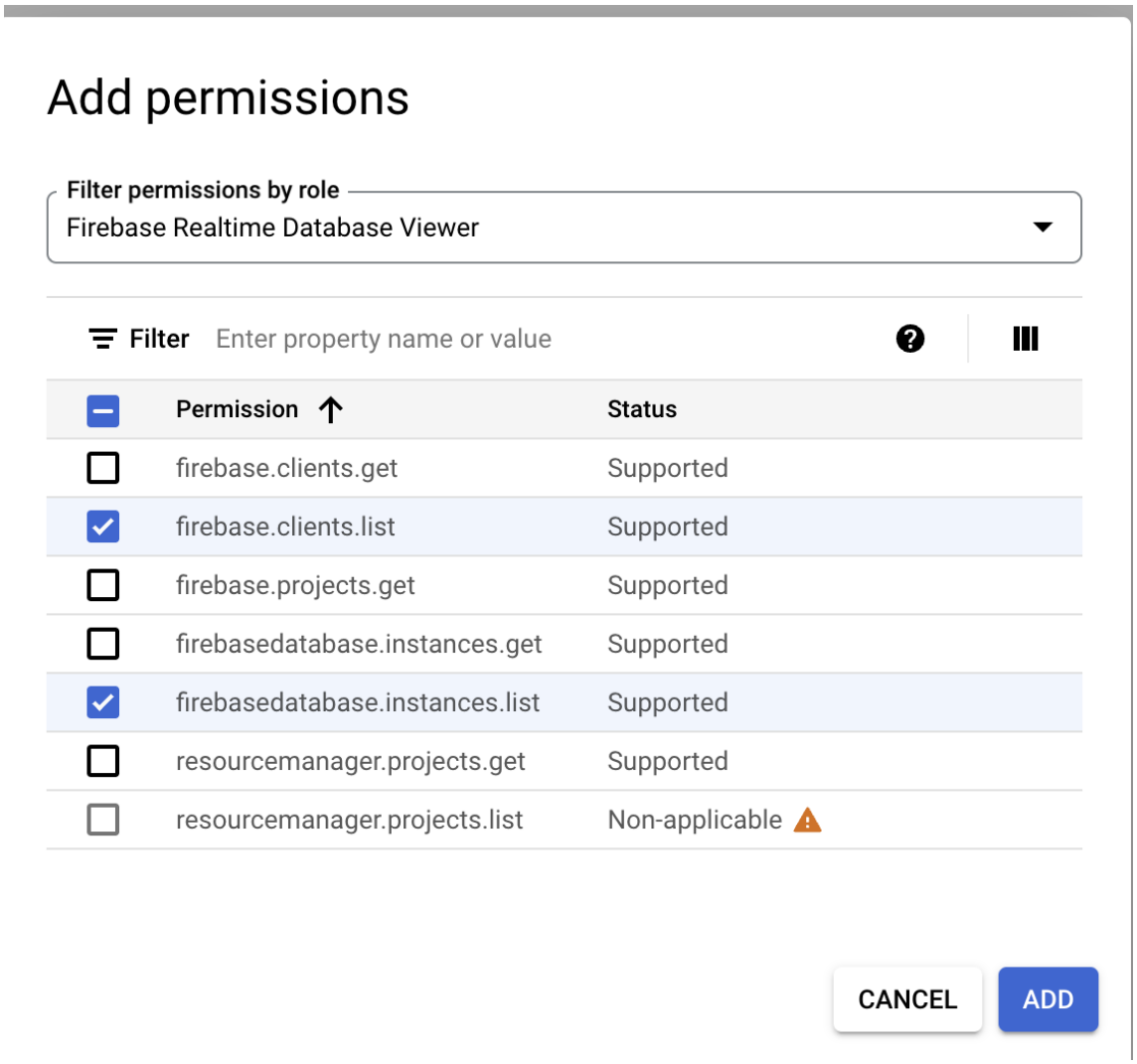
Há diversas etapas de lançamento no Google Cloud. As três etapas principais de lançamento de papéis que você precisa saber são:

Alfa: papéis na etapa Alfa geralmente são experimentais e podem sofrer mudanças significativas. Eles não são recomendados para ambientes de produção. Os usuários podem fornecer feedback sobre as funções alfa para influenciar o desenvolvimento delas.

Beta: papéis na etapa Beta são mais maduros do que aqueles na Alfa, mas ainda podem passar por atualizações e melhorias com base no feedback do usuário. Eles são considerados adequados para certos cenários de não produção, mas podem não ser totalmente estáveis.

Disponibilidade geral (GA): os papéis que alcançam a disponibilidade geral já concluíram as fases de desenvolvimento, teste e refinamento. Eles são considerados estáveis, confiáveis e adequados para uso generalizado em ambientes de produção. Os papéis de GA foram revisados de forma ampla e têm como objetivo apresentar um comportamento consistente e confiável.

4. Clique em **+ Adicionar permissões**. A caixa de diálogo **Adicionar permissões** é aberta.
5. No campo **Filtrar permissões por papel**, digite **Firebase Realtime**.
6. No campo de menu suspenso de resultados, marque a caixa de seleção **Leitor do Firebase Realtime Database**.
7. Clique em **OK**.
8. Em **Filtro**, marque as caixas de verificação **firebase.clients.list** e **firebasedatabase.instances.list** para adicionar essas permissões ao papel personalizado.



9. Clique em **Adicionar**.
10. Na caixa de diálogo **Criar papel**, clique em **Criar**.

Agora o novo papel foi criado e adicionado aos papéis do projeto.

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

Criar um papel personalizado

Tarefa 2: atribuir um papel a um usuário

Nesta tarefa, você vai atribuir um papel personalizado criado na Tarefa 1 a um usuário.

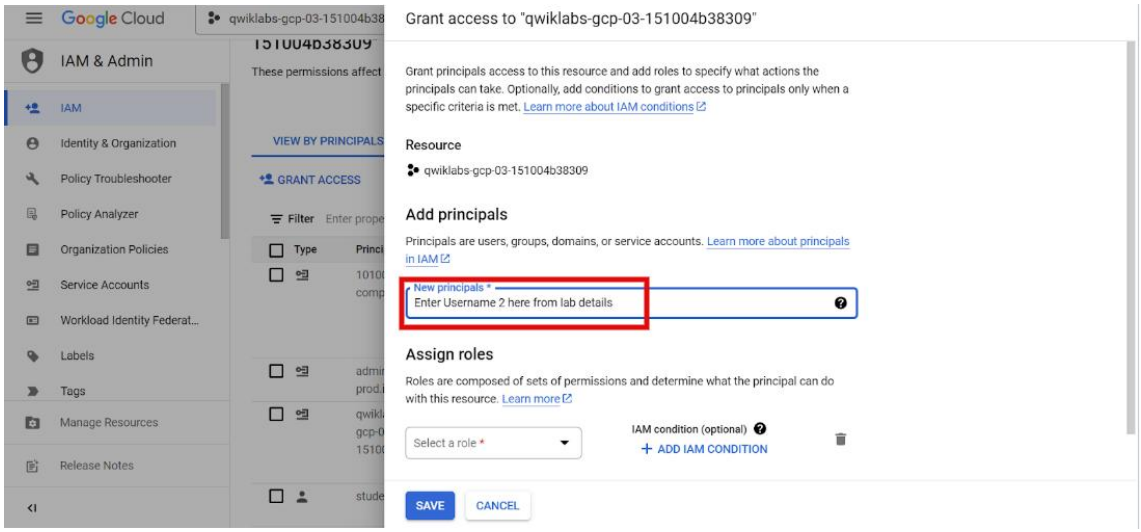
***Observação**: neste laboratório, você vai atribuir o novo papel ao **nome de usuário 2 do Google Cloud** fornecido no painel **Detalhes do laboratório**.*

1. No console do Google Cloud, no **menu de navegação** (☰), clique em **IAM e administrador** > **IAM**. A página **IAM** será aberta.

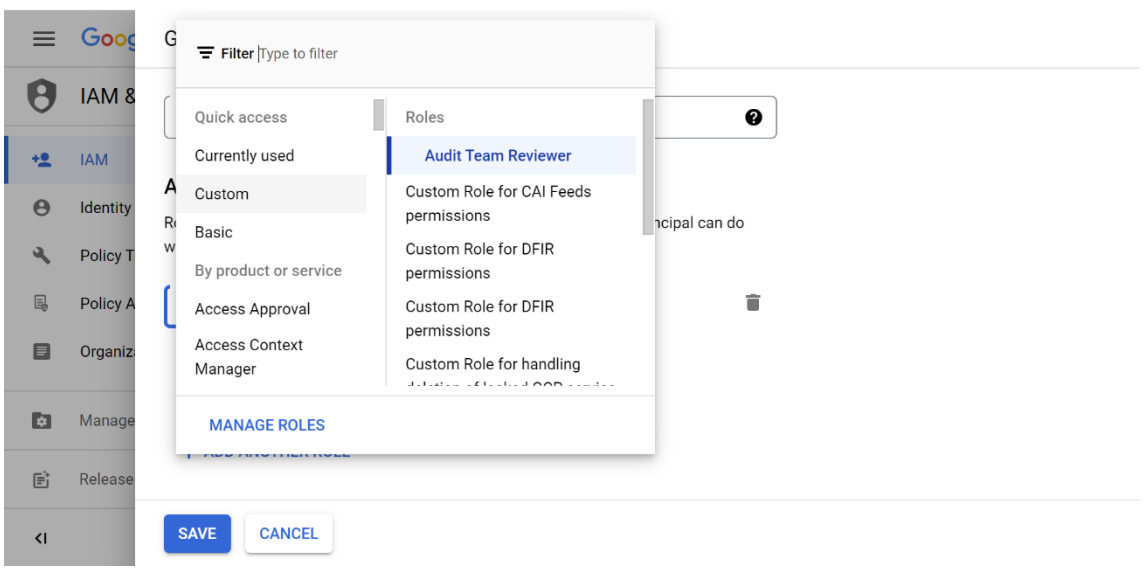
2. Na guia **Visualizar por principais**, clique em **Permitir acesso**. A janela de diálogo **Permitir acesso** será aberta.

A caixa de diálogo **Permitir acesso** é um componente crucial do sistema IAM no Google Cloud. Nela é possível definir e gerenciar com precisão as permissões para usuários, grupos e contas de serviço.

3. Copie **nome de usuário 2 do Google Cloud: Username 2** e cole no campo **Novos principais**.



4. Expanda o menu suspenso **Selecionar papel**, clique em **Personalizado** e depois em **Revisor da equipe de auditoria**. Esse é o papel que você criou na tarefa anterior.



5. Clique em **Salvar**.

Agora o papel personalizado foi atribuído ao usuário.

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

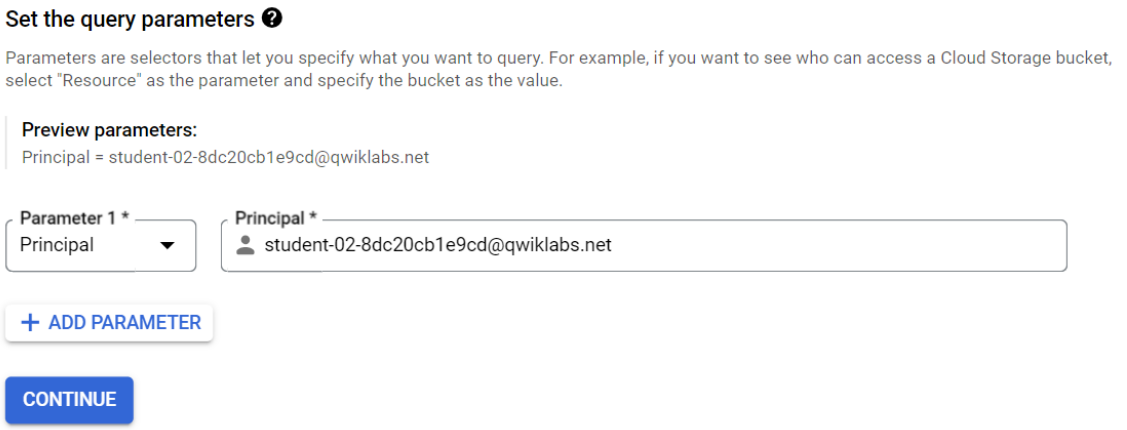
Atribuir um papel a um usuário

Tarefa 3: verificar o papel

Você já criou um papel personalizado com as permissões apropriadas e o atribuiu a um usuário. Agora você vai conferir seu próprio trabalho para verificar se o usuário recebeu o papel criado. Garantir que as configurações foram definidas corretamente é uma parte integral do fluxo de trabalho dos analistas de segurança na nuvem.

Nesta tarefa, você vai usar a ferramenta Análise de políticas do Google Cloud para criar uma consulta e verificar os papéis atribuídos ao usuário.

1. No console do Google Cloud, no **menu de navegação** (☰), clique em **IAM e administrador** > **Análise de políticas**. A página **Análise de políticas** é aberta.
2. Na seção **Analisar políticas**, no bloco **Consulta personalizada**, clique em **Criar consulta personalizada**. Um pop-up pode aparecer no canto superior esquerdo do menu do Google Cloud (☰) com o texto "Clique no menu a qualquer momento para encontrar soluções para sua empresa". Clique em **Entendi** e prossiga para a próxima etapa.
3. Na seção **Definir os parâmetros de consulta**, expanda o menu suspenso **Parâmetro 1** e selecione **Principal**.
4. Copie **nome de usuário 2 do Google Cloud: Username 2** e cole no campo **Principal**.



5. Clique em **Continuar**.

6. Na seção **Opções avançadas para resultados de consulta**, marque a caixa de seleção **Listar recursos nos recursos correspondentes à consulta**.
7. Clique em **Analisar** e depois selecione **Executar consulta** no menu suspenso.

Os resultados devem retornar o papel atribuído ao usuário. Use-os para responder a(s) pergunta(s) abaixo.

Which role has been granted to the user?

Pub/Sub Admin

checkAudit Team Reviewer

BigQuery Admin

Storage Admin

Conclusão

Bom trabalho! Você utilizou o IAM para criar um papel personalizado, conceder acesso a um usuário para o papel e verificar as permissões no Google Cloud. A equipe de auditoria do Cymbal Bank já pode começar a trabalhar na auditoria do banco de dados usando o papel personalizado que você criou.

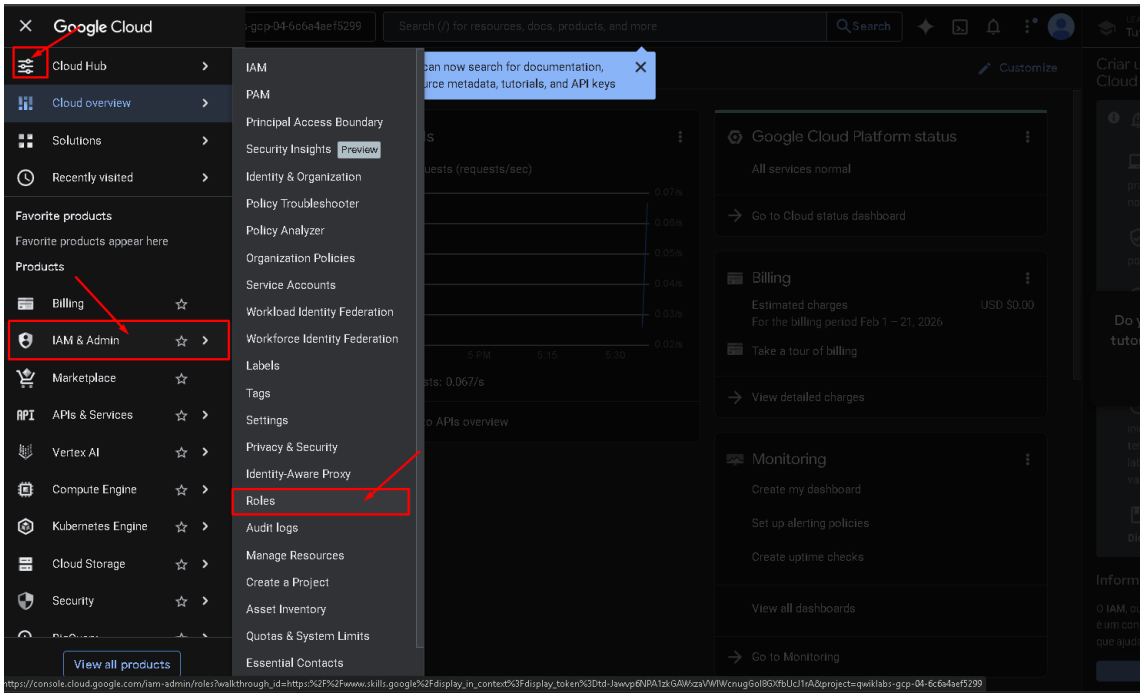
O IAM define quem tem acesso a quais recursos com base nos papéis. Ele é fundamental para gerenciar identidades digitais no ambiente de uma organização e será uma parte fundamental do seu trabalho como analista de segurança em nuvem.

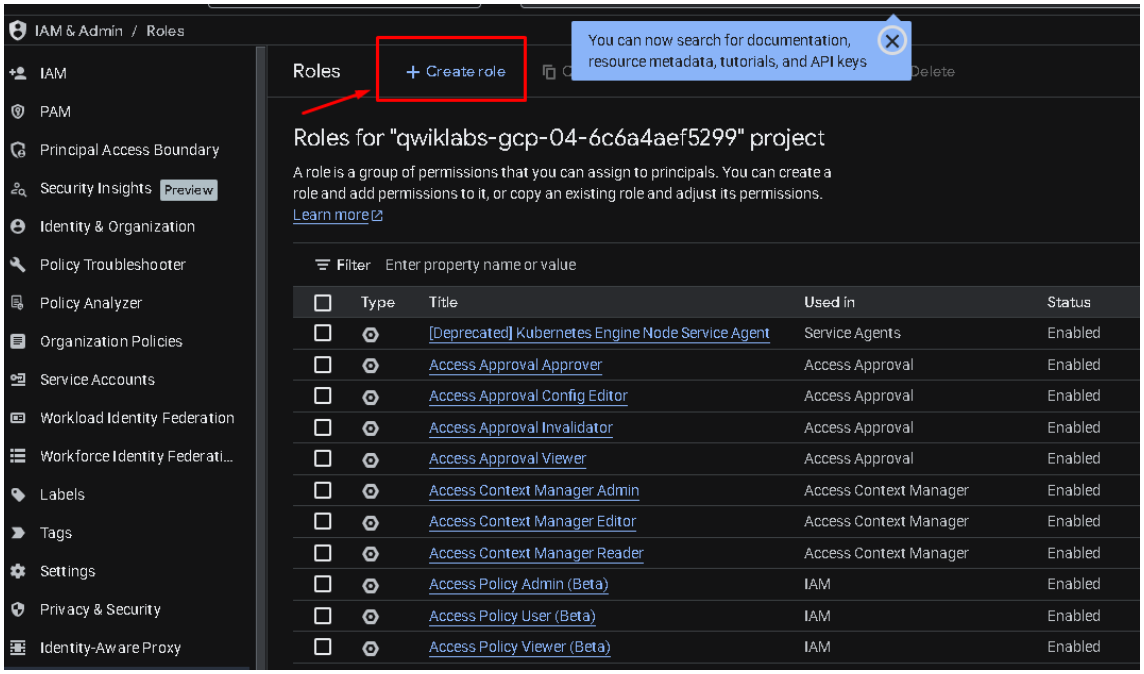
Usando os serviços do IAM, você vai estar no caminho certo para gerenciar efetivamente o acesso e as permissões aos recursos de armazenamento.

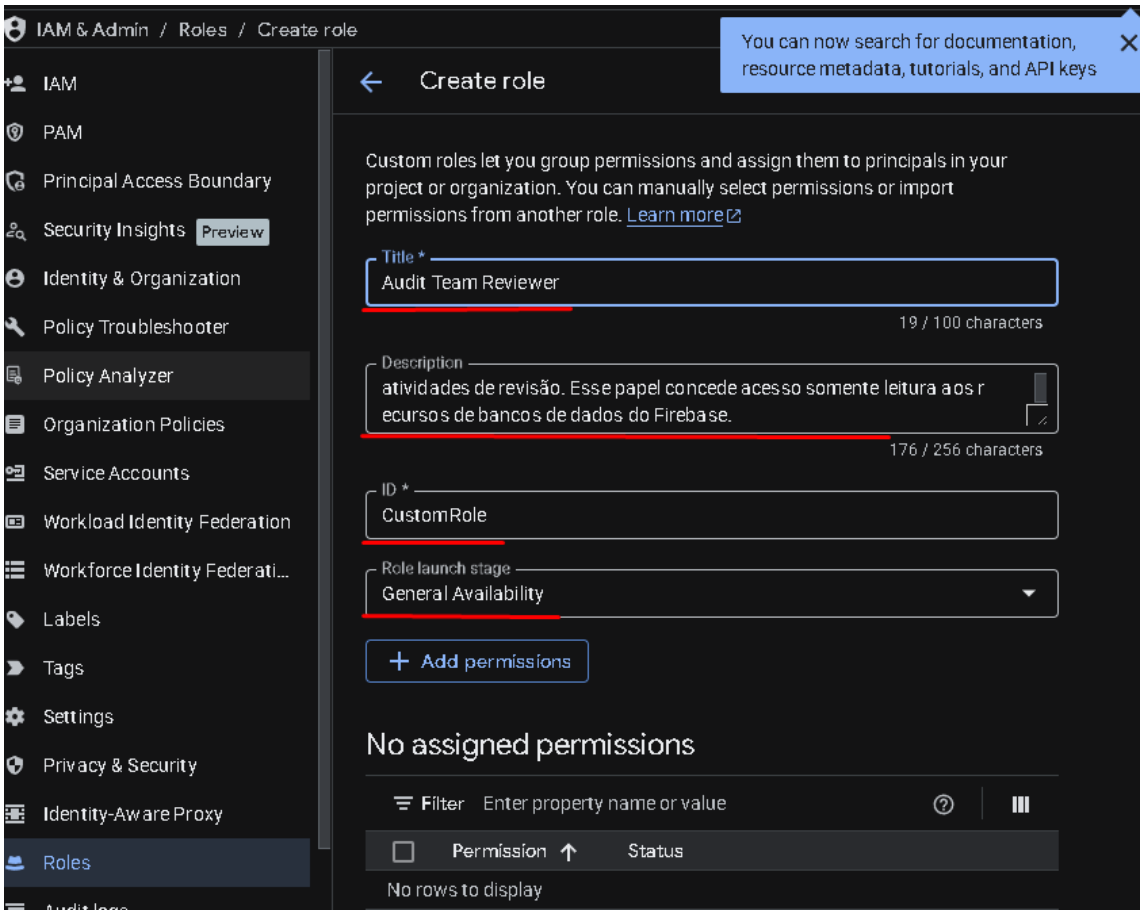
Finalize o laboratório

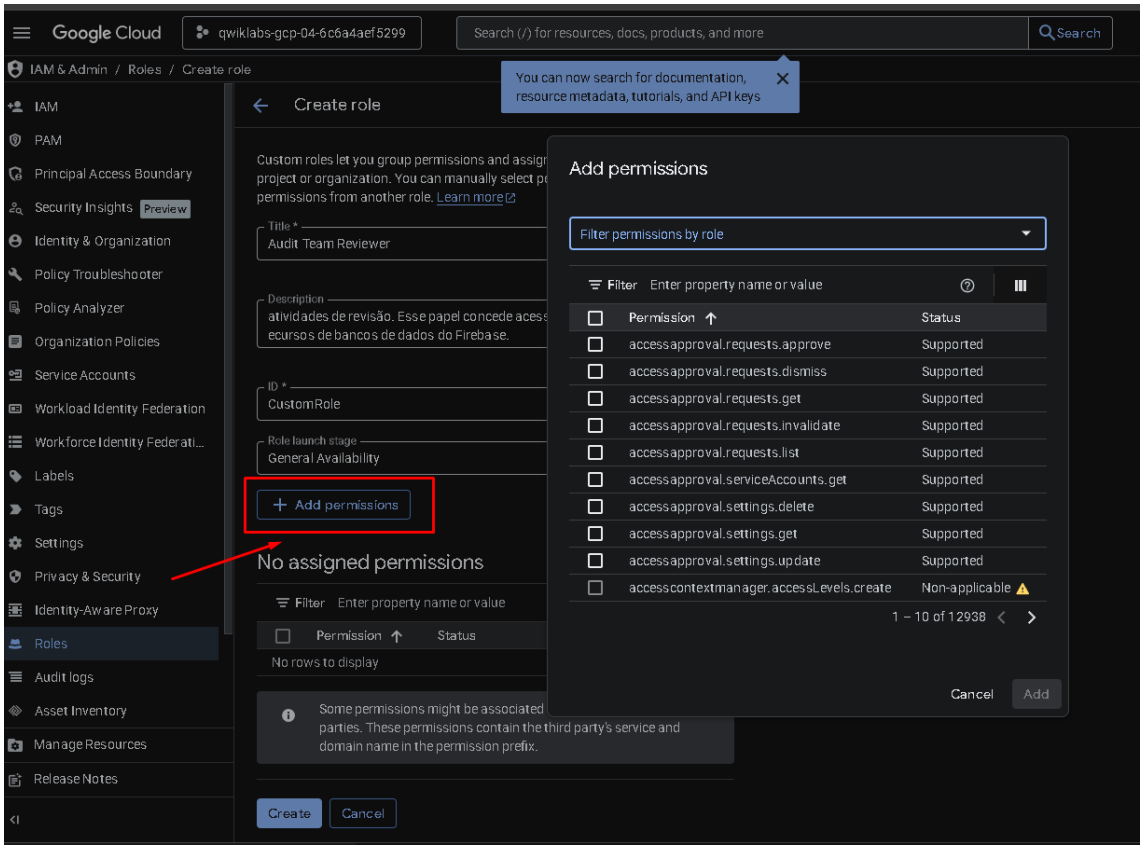
Antes de **encerrar o laboratório**, certifique-se de que você concluiu todas as tarefas. Quando tudo estiver pronto, clique em **Terminar o laboratório** e depois em **Enviar**.

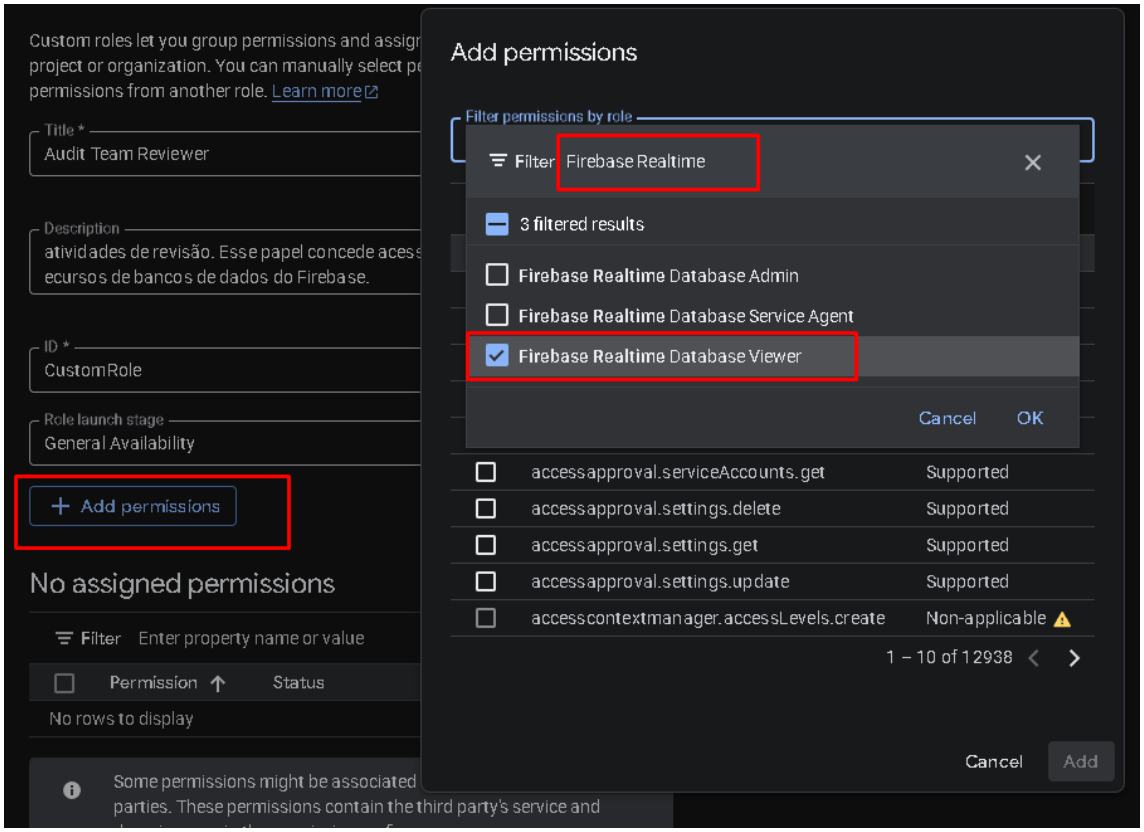
Depois que você finalizar um laboratório, não será mais possível acessar o ambiente do laboratório nem o trabalho que você concluiu nele.

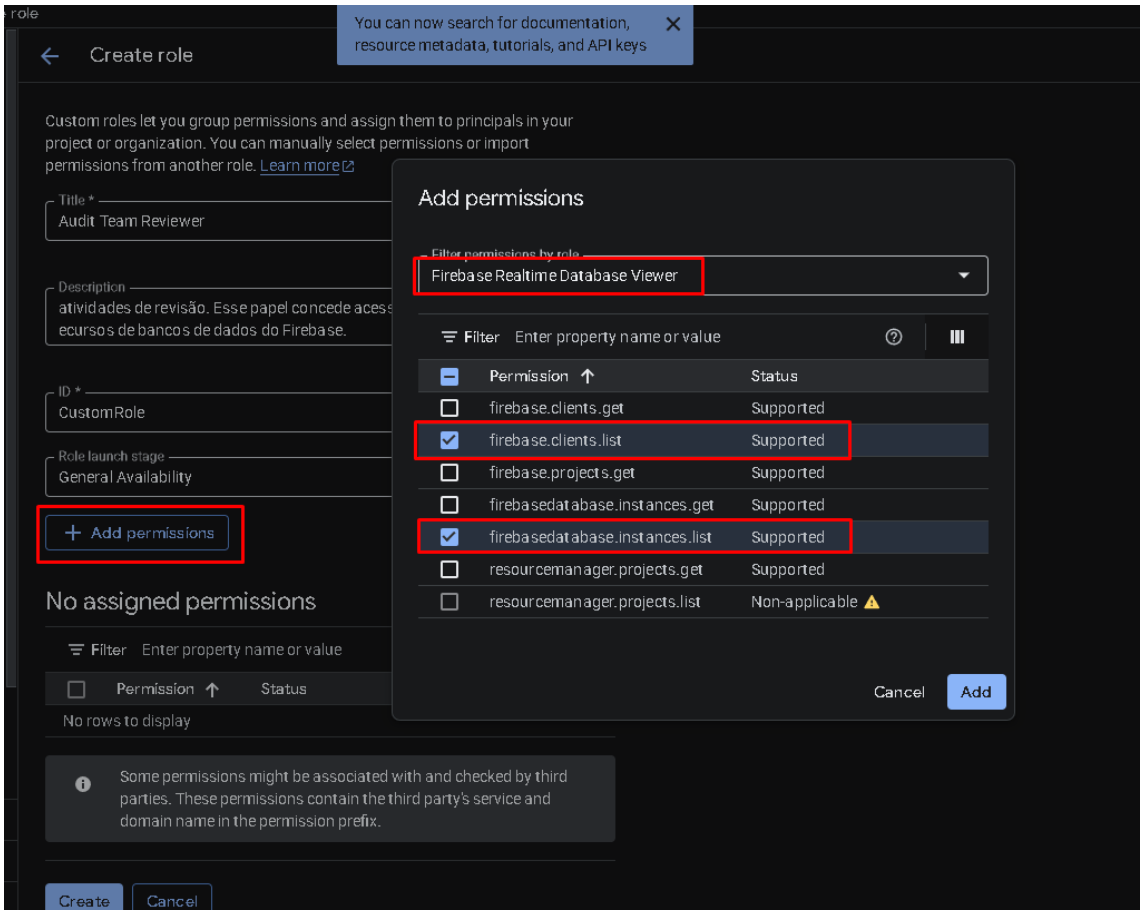

Google Cloud
Cloud Hub
Cloud overview
Solutions
Recently visited
Favorite products
Favorite products appear here
Products
Billing
IAM & Admin
Marketplace
APIs & Services
Vertex AI
Compute Engine
Kubernetes Engine
Cloud Storage
Security
View all products
IAM
PAM
Principal Access Boundary
Security Insights
Preview
Identity & Organization
Policy Troubleshooter
Policy Analyzer
Organization Policies
Service Accounts
Workload Identity Federation
Workforce Identity Federation
Labels
Tags
Settings
Privacy & Security
Identity-Aware Proxy
Roles
Audit logs
Manage Resources
Create a Project
Asset Inventory
Quotas & System Limits
Essential Contacts
Google Cloud Platform status
All services normal
Billing
Monitoring
Create my dashboard
Set up alerting policies
Create uptime checks
View all dashboards
Go to Monitoring

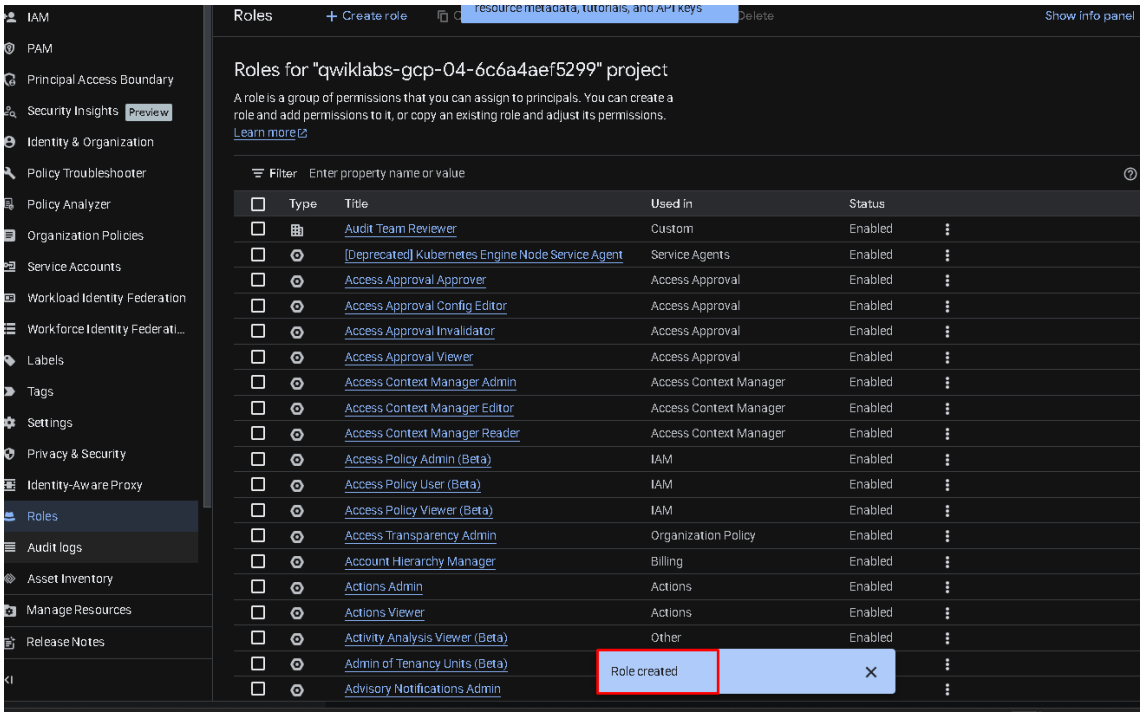

IAM & Admin / Roles
You can now search for documentation, resource metadata, tutorials, and API keys
Roles
+ Create role
Roles for "qwiklabs-gcp-04-6c6a4aef5299" project
A role is a group of permissions that you can assign to principals. You can create a role and add permissions to it, or copy an existing role and adjust its permissions.
Learn more
Filter
Enter property name or value
Type
Title
Used in
Status
[Deprecated] Kubernetes Engine Node Service Agent
Service Agents
Enabled
Access Approval Approver
Access Approval
Access Approval Config Editor
Access Approval Invalidator
Access Approval Viewer
Access Context Manager Admin
Access Context Manager
Access Context Manager Editor
Access Context Manager Reader
Access Policy Admin (Beta)
IAM
Access Policy User (Beta)
Access Policy Viewer (Beta)

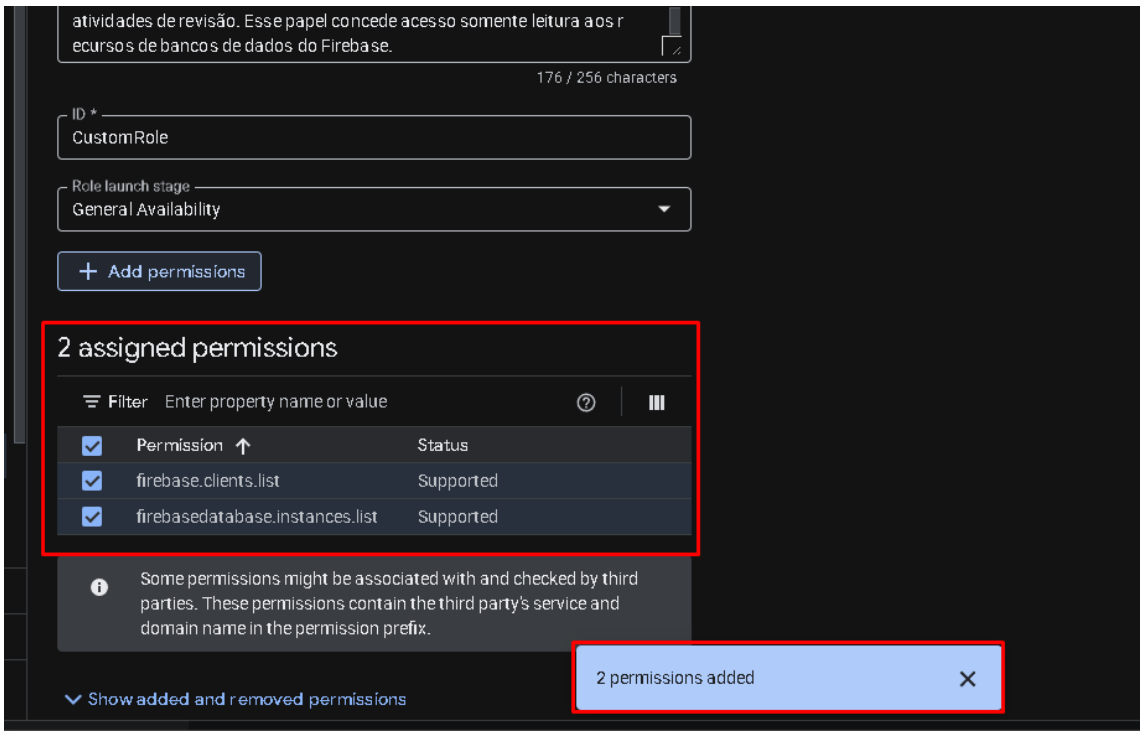

IAM & Admin / Roles / Create role
You can now search for documentation, resource metadata, tutorials, and API keys
IAM
PAM
Principal Access Boundary
Security Insights Preview
Identity & Organization
Policy Troubleshooter
Policy Analyzer
Organization Policies
Service Accounts
Workload Identity Federation
Workforce Identity Federati...
Labels
Tags
Settings
Privacy & Security
Identity-Aware Proxy
Roles
Create role
Custom roles let you group permissions and assign them to principals in your project or organization. You can manually select permissions or import permissions from another role. Learn more
Title *
Audit Team Reviewer
19 / 100 characters
Description
atividades de revisão. Esse papel concede acesso somente leitura aos r ecursos de bancos de dados do Firebase.
176 / 256 characters
ID *
CustomRole
Role launch stage
General Availability
Add permissions
No assigned permissions
Filter Enter property name or value
Permission
Status
No rows to display

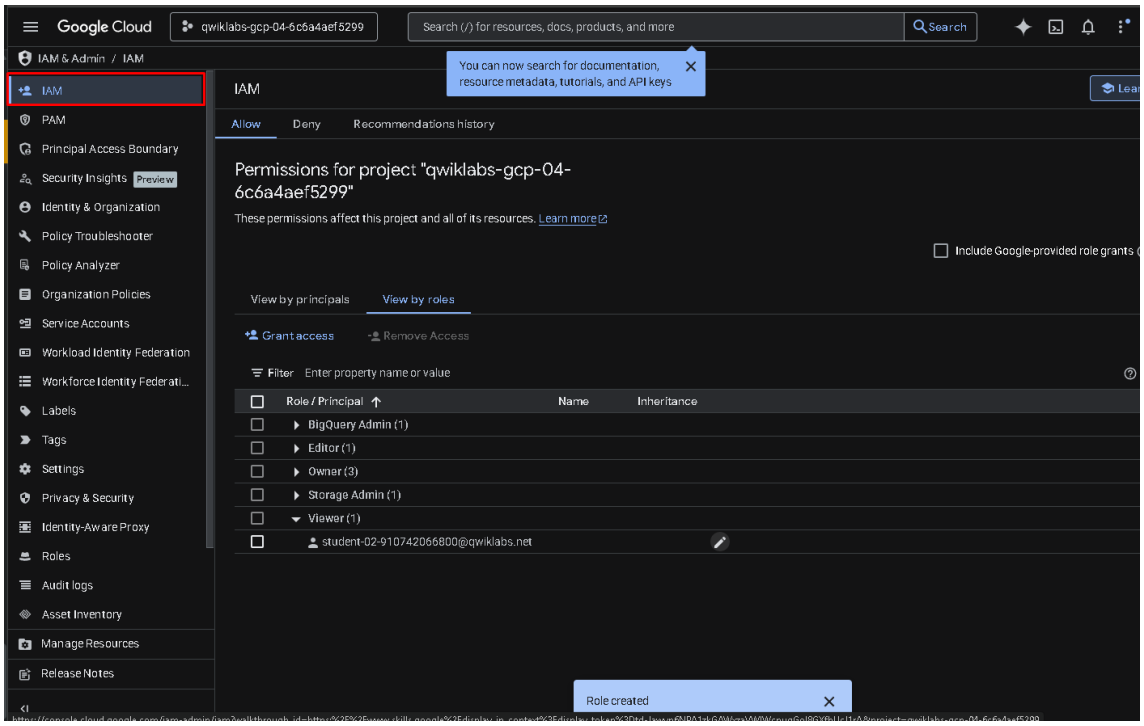

Google Cloud
qwiklabs-gcp-04-6c6a4aef5299
Search (/) for resources, docs, products, and more
Search
IAM & Admin / Roles / Create role
You can now search for documentation, resource metadata, tutorials, and API keys
Create role
Add permissions
Filter permissions by role
Filter Enter property name or value
Permission
Status
accessapproval.requests.approve Supported
accessapproval.requests.dismiss Supported
accessapproval.requests.get Supported
accessapproval.requests.invalidate Supported
accessapproval.requests.list Supported
accessapproval.serviceAccounts.get Supported
accessapproval.settings.delete Supported
accessapproval.settings.get Supported
accessapproval.settings.update Supported
accesscontextmanager.accessLevels.create Non-applicable
1 – 10 of 12938
Cancel
Add
Title *
Audit Team Reviewer
Description
Role launch stage
General Availability
Add permissions
No assigned permissions
No rows to display
Some permissions might be associated parties. These permissions contain the third party's service and domain name in the permission prefix.
Create
Cancel
Audit logs
Asset Inventory
Manage Resources
Release Notes

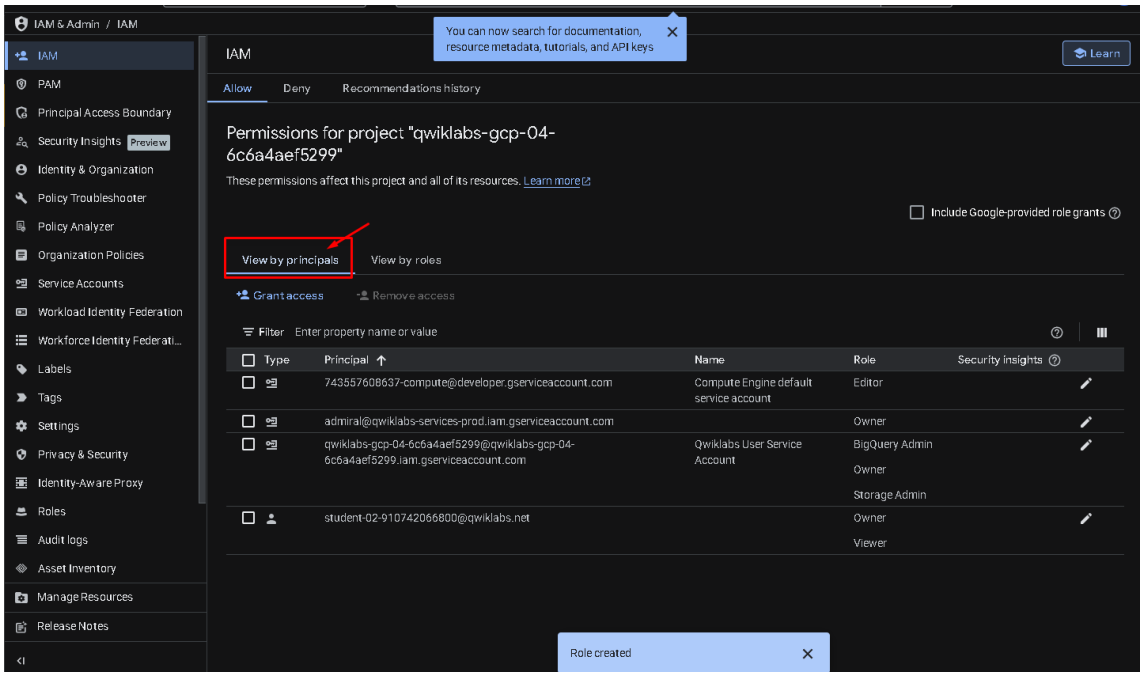

Custom roles let you group permissions and assigr
project or organization. You can manually select pe
permissions from another role. Learn more
Title *
Audit Team Reviewer
Description
atividades de revisão. Esse papel concede aces
ecursos de bancos de dados do Firebase.
ID *
CustomRole
Role launch stage
General Availability
Add permissions
No assigned permissions
Filter Enter property name or value
Permission
Status
No rows to display
Some permissions might be associated
parties. These permissions contain the third party's service and
Add permissions
Filter permissions by role
Filter Firebase Realtime
3 filtered results
Firebase Realtime Database Admin
Firebase Realtime Database Service Agent
Firebase Realtime Database Viewer
Cancel
OK
accessapproval.serviceAccounts.get Supported
accessapproval.settings.delete Supported
accessapproval.settings.get Supported
accessapproval.settings.update Supported
accesscontextmanager.accessLevels.create Non-applicable
1 – 10 of 12938
Cancel
Add

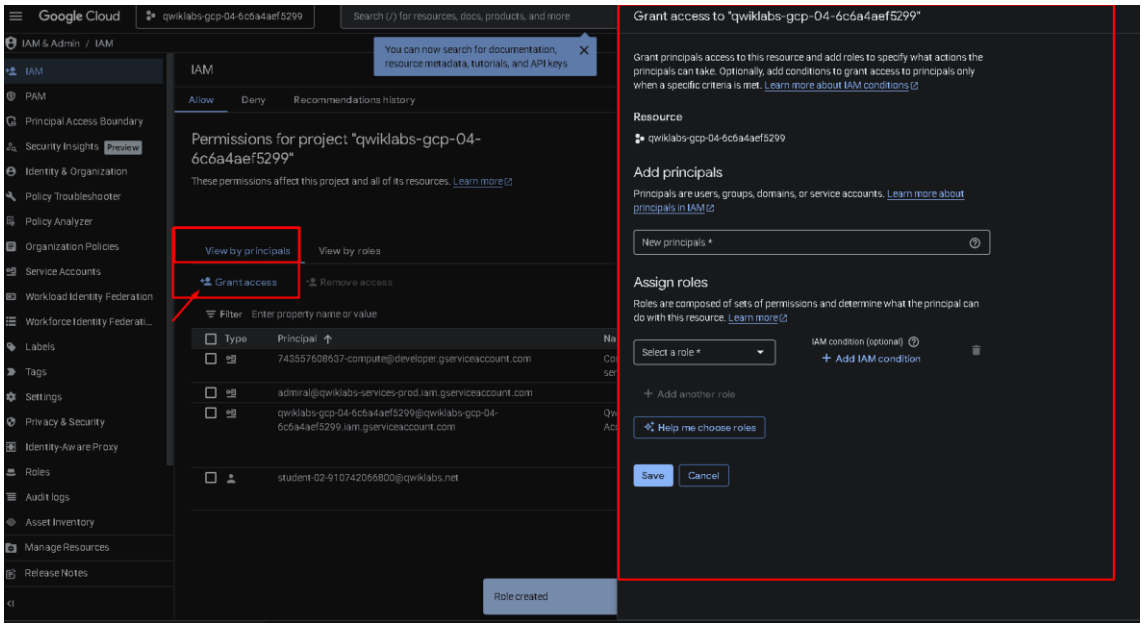

role
You can now search for documentation, resource metadata, tutorials, and API keys
Create role
Custom roles let you group permissions and assign them to principals in your project or organization. You can manually select permissions or import permissions from another role. Learn more
Title *
Audit Team Reviewer
Description
atividades de revisão. Esse papel concede aces
ecursos de bancos de dados do Firebase.
ID *
CustomRole
Role launch stage
General Availability
Add permissions
No assigned permissions
Filter Enter property name or value
Permission
Status
No rows to display
Some permissions might be associated with and checked by third parties. These permissions contain the third party's service and domain name in the permission prefix.
Create
Cancel
Add permissions
Filter permissions by role
Firebase Realtime Database Viewer
Filter Enter property name or value
Permission
Status
firebase.clients.get Supported
firebase.clients.list Supported
firebase.projects.get Supported
firebasedatabase.instances.get Supported
firebasedatabase.instances.list Supported
resourcemanager.projects.get Supported
resourcemanager.projects.list Non-applicable
Cancel
Add

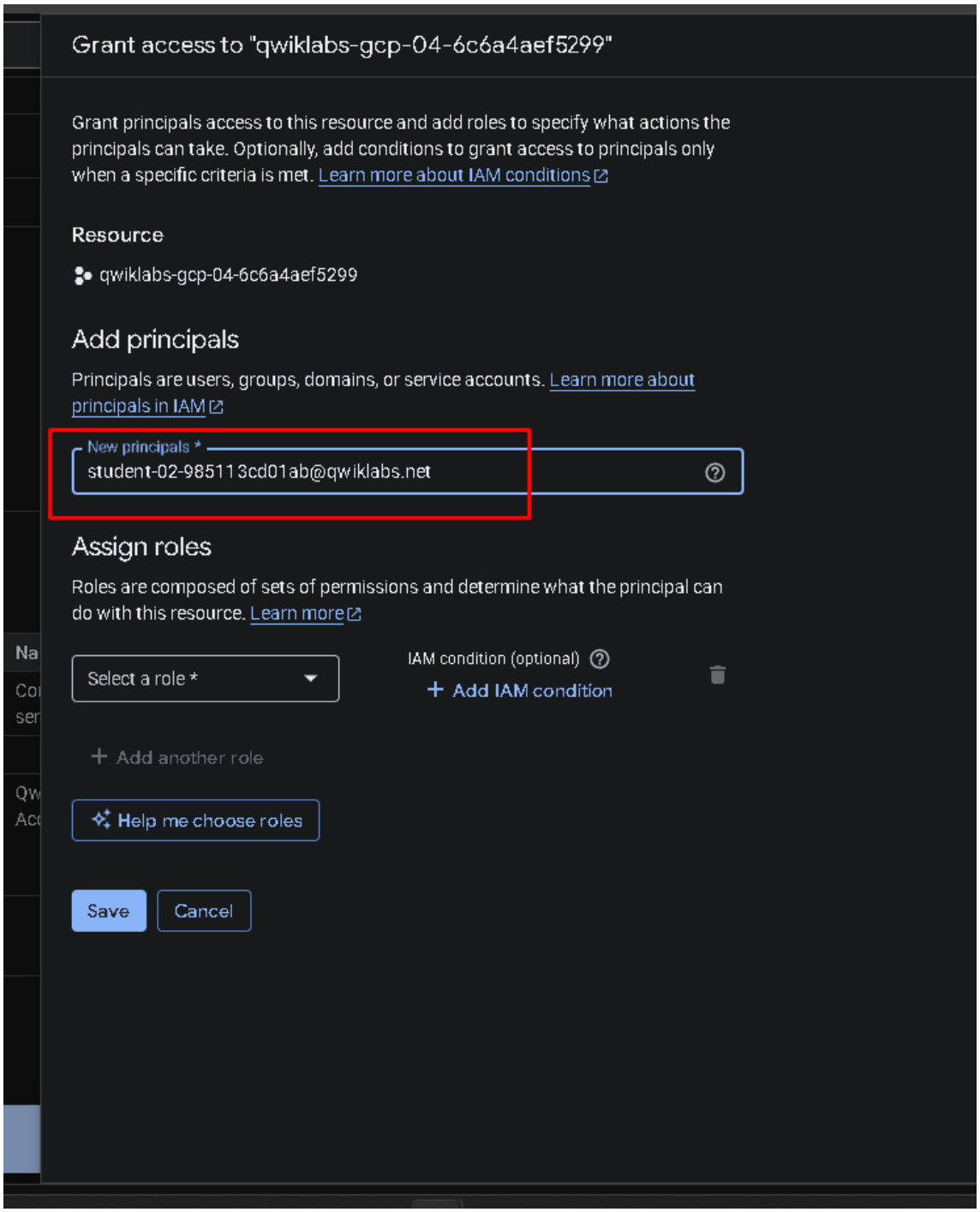

IAM
PAM
Principal Access Boundary
Security Insights
Preview
Identity & Organization
Policy Troubleshooter
Policy Analyzer
Organization Policies
Service Accounts
Workload Identity Federation
Workforce Identity Federati...
Labels
Tags
Settings
Privacy & Security
Identity-Aware Proxy
Roles
Audit logs
Asset Inventory
Manage Resources
Release Notes
Roles
+ Create role
Delete
Show info panel
Roles for "qwiklabs-gcp-04-6c6a4aef5299" project
A role is a group of permissions that you can assign to principals. You can create a role and add permissions to it, or copy an existing role and adjust its permissions.
Learn more
Filter
Enter property name or value
Type
Title
Used in
Status
Audit Team Reviewer
Custom
Enabled
[Deprecated] Kubernetes Engine Node Service Agent
Service Agents
Enabled
Access Approval Approver
Access Approval
Enabled
Access Approval Config Editor
Access Approval
Enabled
Access Approval Invalidator
Access Approval
Enabled
Access Approval Viewer
Access Approval
Enabled
Access Context Manager Admin
Access Context Manager
Enabled
Access Context Manager Editor
Access Context Manager
Enabled
Access Context Manager Reader
Access Context Manager
Enabled
Access Policy Admin (Beta)
IAM
Enabled
Access Policy User (Beta)
IAM
Enabled
Access Policy Viewer (Beta)
IAM
Enabled
Access Transparency Admin
Organization Policy
Enabled
Account Hierarchy Manager
Billing
Enabled
Actions Admin
Actions
Enabled
Actions Viewer
Actions
Enabled
Activity Analysis Viewer (Beta)
Other
Enabled
Admin of Tenancy Units (Beta)
Advisory Notifications Admin
Role created

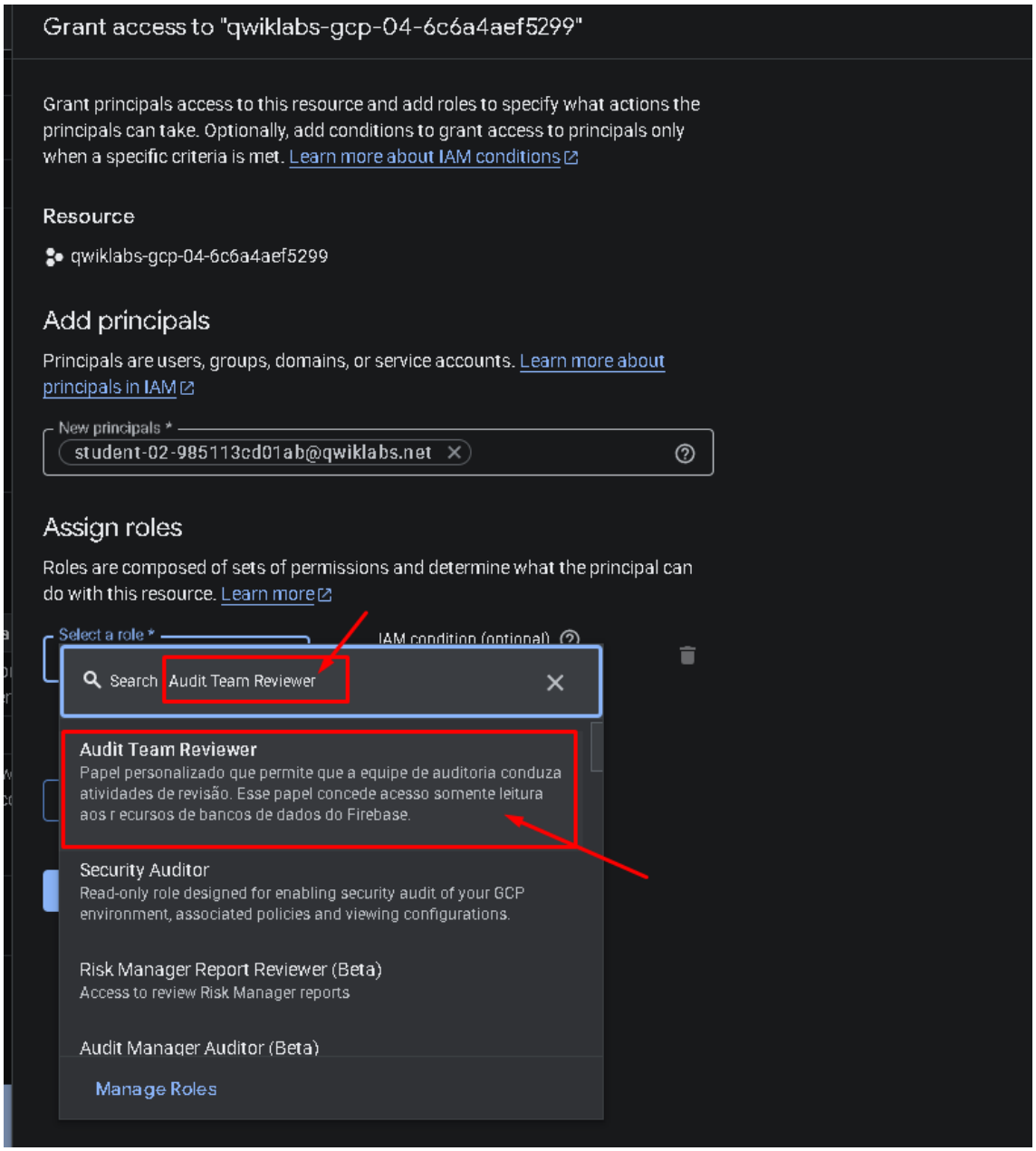

atividades de revisão. Esse papel concede acesso somente leitura aos r
ecursos de bancos de dados do Firebase.
176 / 256 characters
ID *
CustomRole
Role launch stage
General Availability
+ Add permissions
2 assigned permissions
Filter
Enter property name or value
Permission
Status
firebase.clients.list
Supported
firebasedatabase.instances.list
Supported
Some permissions might be associated with and checked by third parties. These permissions contain the third party's service and domain name in the permission prefix.
Show added and removed permissions
2 permissions added

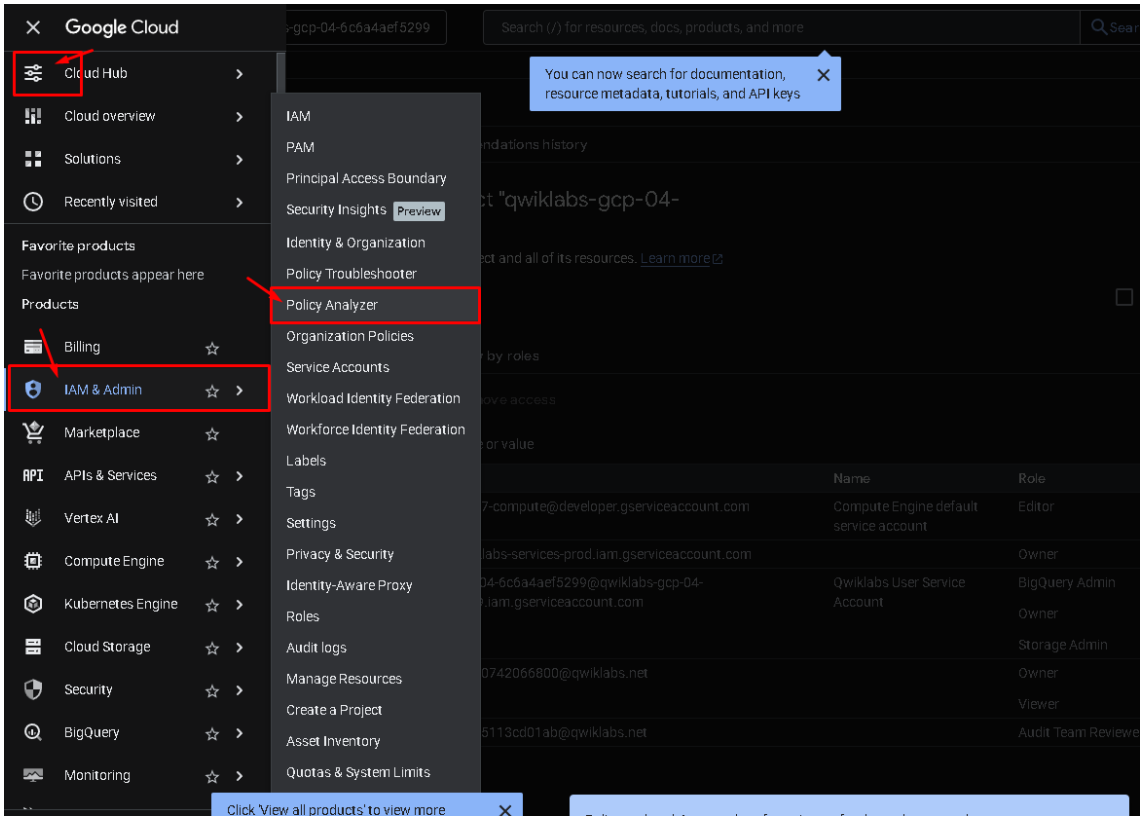

Google Cloud
qwiklabs-gcp-04-6c6a4aef5299
Search (/) for resources, docs, products, and more
Search
IAM & Admin / IAM
You can now search for documentation, resource metadata, tutorials, and API keys
IAM
PAM
Principal Access Boundary
Security Insights
Preview
Identity & Organization
Policy Troubleshooter
Policy Analyzer
Organization Policies
Service Accounts
Workload Identity Federation
Workforce Identity Federati...
Labels
Tags
Settings
Privacy & Security
Identity-Aware Proxy
Roles
Audit logs
Asset Inventory
Manage Resources
Release Notes
IAM
Allow
Deny
Recommendations history
Permissions for project "qwiklabs-gcp-04-6c6a4aef5299"
These permissions affect this project and all of its resources. Learn more
Include Google-provided role grants
View by principals
View by roles
Grant access
Remove Access
Filter
Enter property name or value
Role / Principal
Name
Inheritance
BigQuery Admin (1)
Editor (1)
Owner (3)
Storage Admin (1)
Viewer (1)
student-02-910742066800@qwiklabs.net
Role created

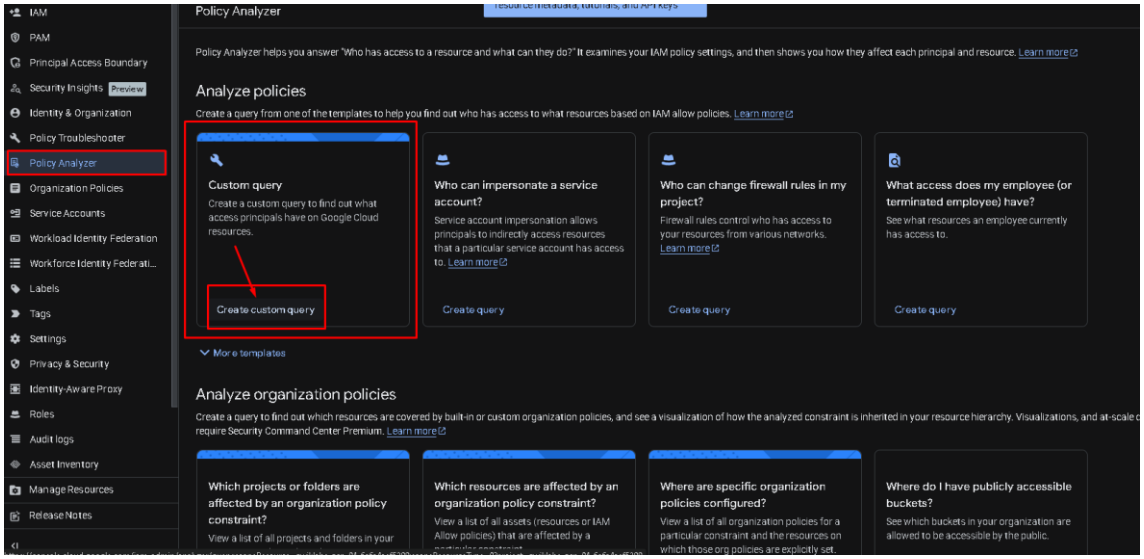

IAM & Admin / IAM
You can now search for documentation, resource metadata, tutorials, and API keys
IAM
PAM
Principal Access Boundary
Security Insights
Preview
Identity & Organization
Policy Troubleshooter
Policy Analyzer
Organization Policies
Service Accounts
Workload Identity Federation
Workforce Identity Federati...
Labels
Tags
Settings
Privacy & Security
Identity-Aware Proxy
Roles
Audit logs
Asset Inventory
Manage Resources
Release Notes
IAM
Learn
Allow
Deny
Recommendations history
Permissions for project "qwiklabs-gcp-04-6c6a4aef5299"
These permissions affect this project and all of its resources. Learn more
Include Google-provided role grants
View by principals
View by roles
Grant access
Remove access
Filter
Enter property name or value
Type
Principal
Name
Role
Security insights
743557608637-compute@developer.gserviceaccount.com
Compute Engine default service account
Editor
admiral@qwiklabs-services-prod.iam.gserviceaccount.com
Owner
qwiklabs-gcp-04-6c6a4aef5299@qwiklabs-gcp-04-6c6a4aef5299.iam.gserviceaccount.com
Qwiklabs User Service Account
BigQuery Admin
Owner
Storage Admin
student-02-910742066800@qwiklabs.net
Owner
Viewer
Role created

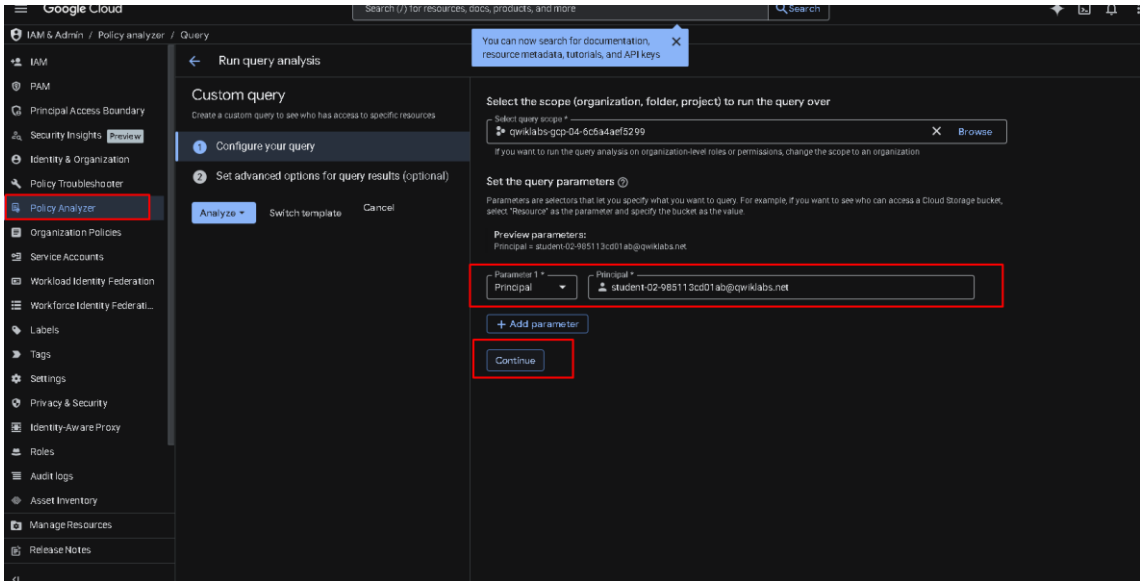

Google Cloud
qwiklabs-gcp-04-6c6a4aef5299
Search (/) for resources, docs, products, and more
IAM & Admin / IAM
You can now search for documentation, resource metadata, tutorials, and API keys
IAM
PAM
Principal Access Boundary
Security Insights
Preview
Identity & Organization
Policy Troubleshooter
Policy Analyzer
Organization Policies
Service Accounts
Workload Identity Federation
Workforce Identity Federati...
Labels
Tags
Settings
Privacy & Security
Identity-Aware Proxy
Roles
Audit logs
Asset Inventory
Manage Resources
Release Notes
IAM
Allow
Deny
Recommendations history
Permissions for project "qwiklabs-gcp-04-6c6a4aef5299"
These permissions affect this project and all of its resources. Learn more
View by principals
View by roles
Grant access
Remove access
Filter
Enter property name or value
Type
Principal
743557608637-compute@developer.gserviceaccount.com
admiral@qwiklabs-services-prod.iam.gserviceaccount.com
qwiklabs-gcp-04-6c6a4aef5299@qwiklabs-gcp-04-6c6a4aef5299.iam.gserviceaccount.com
student-02-910742056800@qwiklabs.net
Role created
Grant access to "qwiklabs-gcp-04-6c6a4aef5299"
Grant principals access to this resource and add roles to specify what actions the principals can take. Optionally, add conditions to grant access to principals only when a specific criteria is met. Learn more about IAM conditions
Resource
qwiklabs-gcp-04-6c6a4aef5299
Add principals
Principals are users, groups, domains, or service accounts. Learn more about principals in IAM
New principals *
Assign roles
Roles are composed of sets of permissions and determine what the principal can do with this resource. Learn more
Select a role *
IAM condition (optional)
Add IAM condition
Add another role
Help me choose roles
Save
Cancel

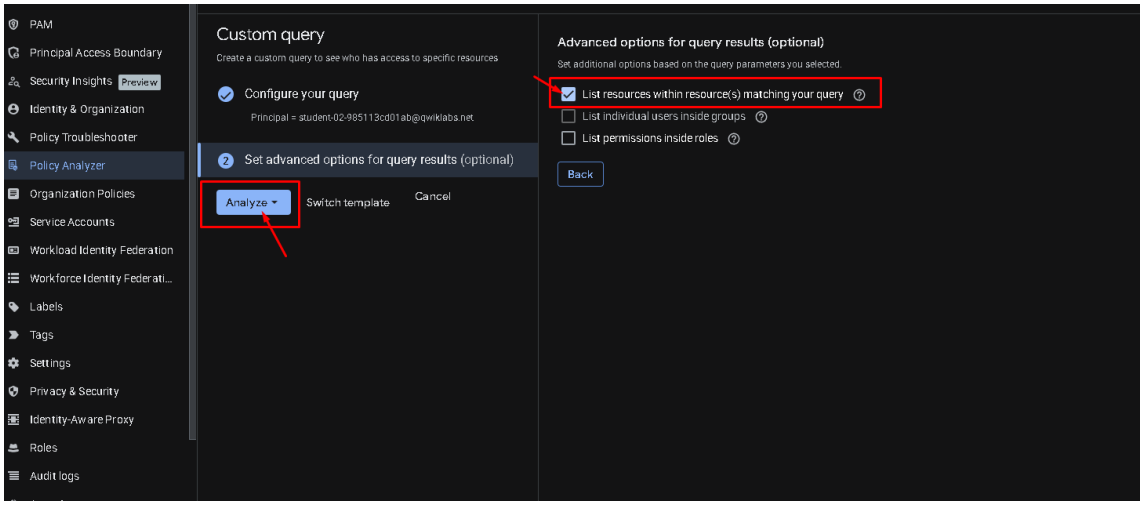

Grant access to "qwiklabs-gcp-04-6c6a4aef5299"
Grant principals access to this resource and add roles to specify what actions the principals can take. Optionally, add conditions to grant access to principals only when a specific criteria is met. Learn more about IAM conditions
Resource
qwiklabs-gcp-04-6c6a4aef5299
Add principals
Principals are users, groups, domains, or service accounts. Learn more about principals in IAM
New principals *
student-02-98513cd01ab@qwiklabs.net
Assign roles
Roles are composed of sets of permissions and determine what the principal can do with this resource. Learn more
Select a role *
IAM condition (optional)
Add IAM condition
Add another role
Help me choose roles
Save
Cancel

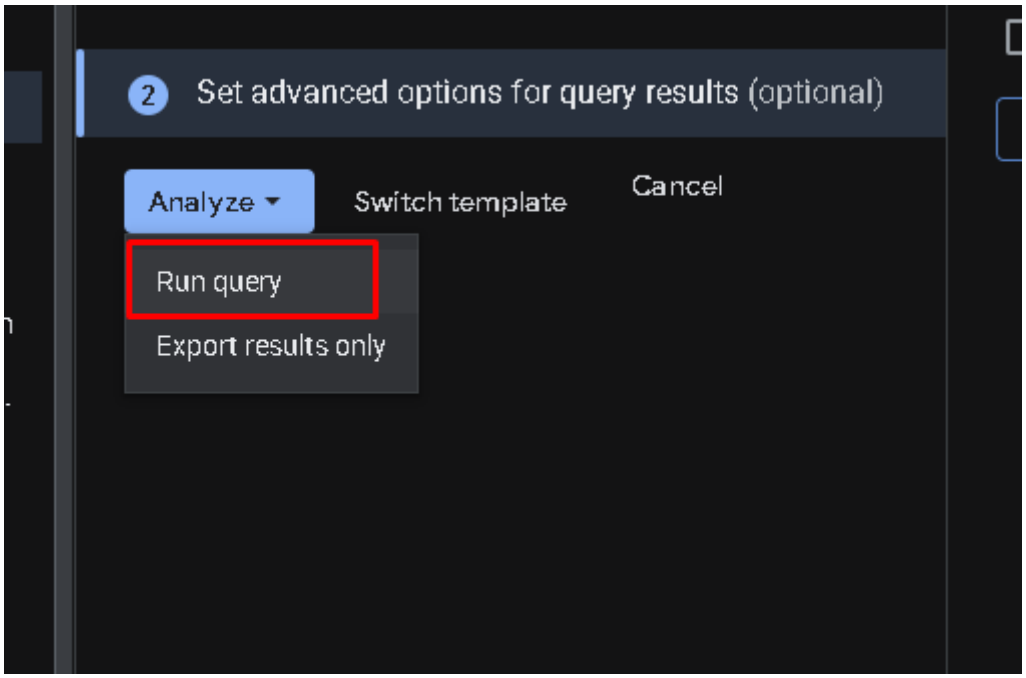

Grant access to "qwiklabs-gcp-04-6c6a4aef5299"
Grant principals access to this resource and add roles to specify what actions the principals can take. Optionally, add conditions to grant access to principals only when a specific criteria is met. Learn more about IAM conditions
Resource
qwiklabs-gcp-04-6c6a4aef5299
Add principals
Principals are users, groups, domains, or service accounts. Learn more about principals in IAM
New principals *
student-02-985113cd01ab@qwiklabs.net
Assign roles
Roles are composed of sets of permissions and determine what the principal can do with this resource. Learn more
Select a role *
IAM condition (optional)
Search
Audit Team Reviewer
Audit Team Reviewer
Papel personalizado que permite que a equipe de auditoria conduza atividades de revisão. Esse papel concede acesso somente leitura aos r ecursos de bancos de dados do Firebase.
Security Auditor
Read-only role designed for enabling security audit of your GCP environment, associated policies and viewing configurations.
Risk Manager Report Reviewer (Beta)
Access to review Risk Manager reports
Audit Manager Auditor (Beta)
Manage Roles

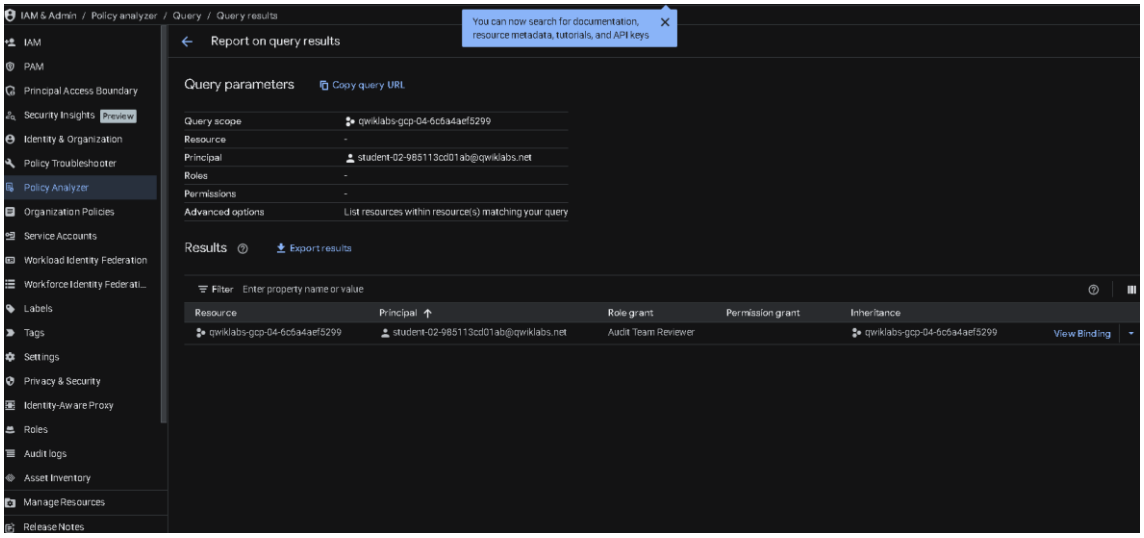

Google Cloud
Cloud Hub
Cloud overview
Solutions
Recently visited
Favorite products
Favorite products appear here
Products
Billing
IAM & Admin
Marketplace
APIs & Services
Vertex AI
Compute Engine
Kubernetes Engine
Cloud Storage
Security
BigQuery
Monitoring
IAM
PAM
Principal Access Boundary
Security Insights
Preview
Identity & Organization
Policy Troubleshooter
Policy Analyzer
Organization Policies
Service Accounts
Workload Identity Federation
Workforce Identity Federation
Labels
Tags
Settings
Privacy & Security
Identity-Aware Proxy
Roles
Audit logs
Manage Resources
Create a Project
Asset Inventory
Quotas & System Limits
You can now search for documentation, resource metadata, tutorials, and API keys
Click 'View all products' to view more


Policy Analyzer
Policy Analyzer helps you answer "Who has access to a resource and what can they do?" It examines your IAM policy settings, and then shows you how they affect each principal and resource.
Analyze policies
Create a query from one of the templates to help you find out who has access to what resources based on IAM allow policies.
Custom query
Create a custom query to find out what access principals have on Google Cloud resources.
Create custom query
Who can impersonate a service account?
Service account impersonation allows principals to indirectly access resources that a particular service account has access to.
Who can change firewall rules in my project?
Firewall rules control who has access to your resources from various networks.
What access does my employee (or terminated employee) have?
See what resources an employee currently has access to.
Create query
More templates
Analyze organization policies
Which projects or folders are affected by an organization policy constraint?
Which resources are affected by an organization policy constraint?
Where are specific organization policies configured?
Where do I have publicly accessible buckets?
See which buckets in your organization are allowed to be accessible by the public.


Google Cloud
IAM & Admin / Policy analyzer / Query
You can now search for documentation, resource metadata, tutorials, and API keys
IAM
PAM
Principal Access Boundary
Security Insights Preview
Identity & Organization
Policy Troubleshooter
Policy Analyzer
Organization Policies
Service Accounts
Workload Identity Federation
Workforce Identity Federati...
Labels
Tags
Settings
Privacy & Security
Identity-Aware Proxy
Roles
Audit logs
Asset Inventory
Manage Resources
Release Notes
Run query analysis
Custom query
Create a custom query to see who has access to specific resources
Configure your query
Set advanced options for query results (optional)
Analyze
Switch template
Cancel
Select the scope (organization, folder, project) to run the query over
Select query scope *
qwiklabs-gcp-04-6c6a4aef5299
Browse
If you want to run the query analysis on organization-level roles or permissions, change the scope to an organization
Set the query parameters
Parameters are selectors that let you specify what you want to query. For example, if you want to see who can access a Cloud Storage bucket, select "Resource" as the parameter and specify the bucket as the value.
Preview parameters:
Principal = student-02-985113cd01ab@qwiklabs.net
Parameter 1 *
Principal
Principal *
student-02-985113cd01ab@qwiklabs.net
+ Add parameter
Continue


PAM
Principal Access Boundary
Security Insights Preview
Identity & Organization
Policy Troubleshooter
Policy Analyzer
Organization Policies
Service Accounts
Workload Identity Federation
Workforce Identity Federati...
Labels
Tags
Settings
Privacy & Security
Identity-Aware Proxy
Roles
Audit logs
Custom query
Create a custom query to see who has access to specific resources
Configure your query
Principal = student-02-985113cd01ab@qwiklabs.net
Set advanced options for query results (optional)
Analyze
Switch template
Cancel
Advanced options for query results (optional)
Set additional options based on the query parameters you selected.
List resources within resource(s) matching your query
List individual users inside groups
List permissions inside roles
Back


2 Set advanced options for query results (optional)
Analyze
Switch template
Cancel
Run query
Export results only


IAM & Admin / Policy analyzer / Query / Query results
You can now search for documentation, resource metadata, tutorials, and API keys
IAM
PAM
Principal Access Boundary
Security Insights Preview
Identity & Organization
Policy Troubleshooter
Policy Analyzer
Organization Policies
Service Accounts
Workload Identity Federation
Workforce Identity Federati...
Labels
Tags
Settings
Privacy & Security
Identity-Aware Proxy
Roles
Audit logs
Asset Inventory
Manage Resources
Release Notes
Report on query results
Query parameters
Copy query URL
Query scope qwiklabs-gcp-04-6c6a4aef5299
Resource -
Principal student-02-985113cd01ab@qwiklabs.net
Roles -
Permissions -
Advanced options List resources within resource(s) matching your query
Results
Export results
Filter Enter property name or value
Resource
Principal
Role grant
Permission grant
Inheritance
qwiklabs-gcp-04-6c6a4aef5299
student-02-985113cd01ab@qwiklabs.net
Audit Team Reviewer
qwiklabs-gcp-04-6c6a4aef5299
View Binding