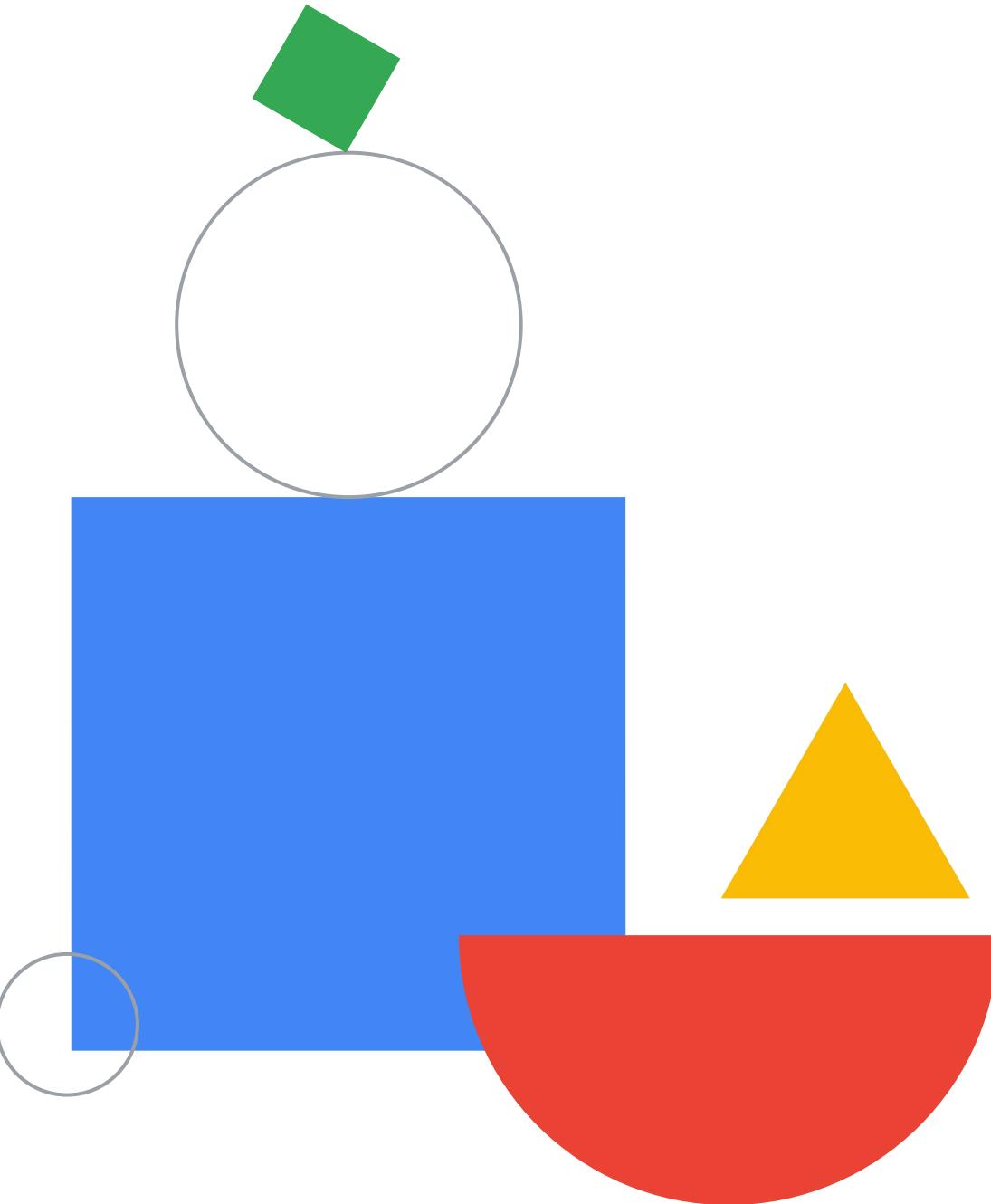


Preparing for Your Associate Cloud Engineer Journey

Module 5: Configuring Access and Security



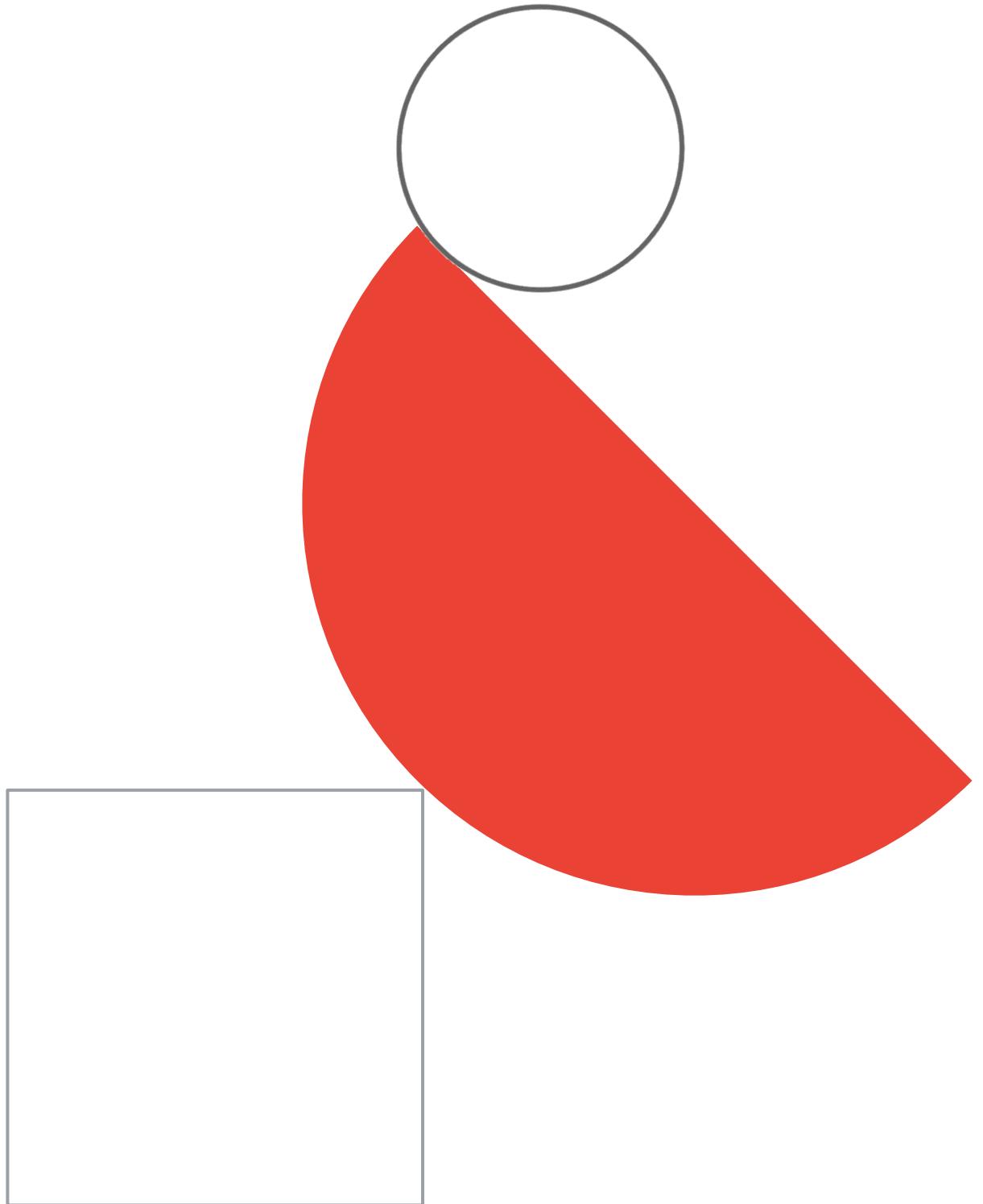


Module agenda

- 01** Managing access for Cymbal Superstore's cloud solutions
- 02** Diagnostic questions
- 03** Review and study planning

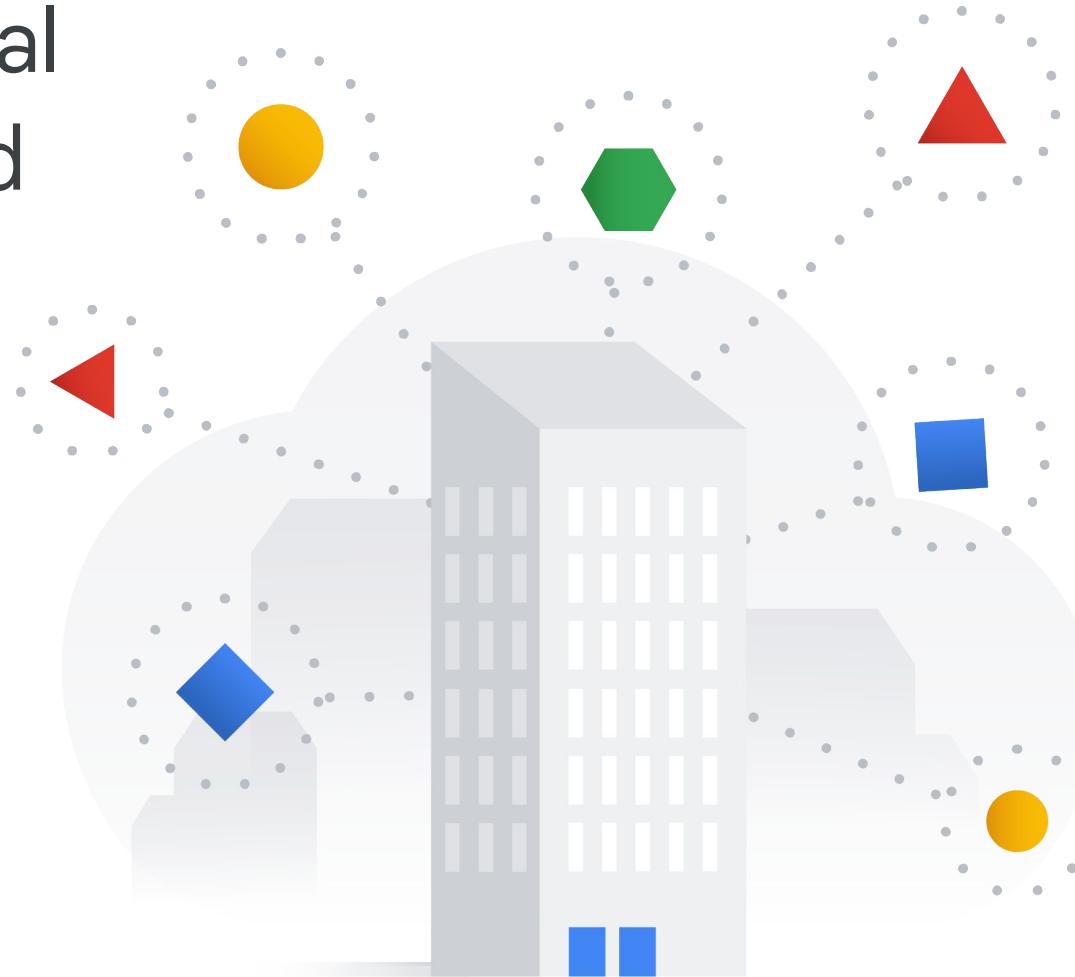


Managing access for Cymbal Superstore's cloud solutions



The next step:

ongoing access and security for Cymbal Superstore's cloud solutions



- Managing Identity and Access Management (IAM)
- Managing service accounts



Setting up a service account for Cymbal Superstore's supply chain app



- 1 Create a service account
- 2 Assign Permissions
- 3 Attach to a VM

01

Create a service account:

Where to look

The screenshot shows the Google Cloud Platform interface for the project "cymbal-supplychain-staging". The left sidebar under "IAM & Admin" has a red box around the "Service Accounts" link. The main content area shows the "Service accounts" page with a red box around the "+ CREATE SERVICE ACCOUNT" button. The page title is "Service accounts for project 'cymbal-supplychain-staging'". It includes a brief description of what service accounts are and how organization policies can be used to secure them. A table at the bottom shows no rows displayed.

Email	Status	Name ↑	Description	Key ID	Key creation date	Actions
No rows to display						

01

Create a service account:

Enter service account details

Google Cloud Platform cymbal-supplychain-staging Search products and resources

IAM & Admin Create service account

IAM Identity & Organization Policy Troubleshooter Policy Analyzer Organization Policies Service Accounts Workload Identity Federat... Labels Tags Settings Privacy & Security Identity-Aware Proxy Roles Audit Logs Manage Resources

1 Service account details

Service account name: vm-service-account
Display name for this service account

Service account ID: vm-service-account @helpful-chiller-328713.iam.gserviceaccount X C

Service account description: service account to be attached to vm's for supply chain app

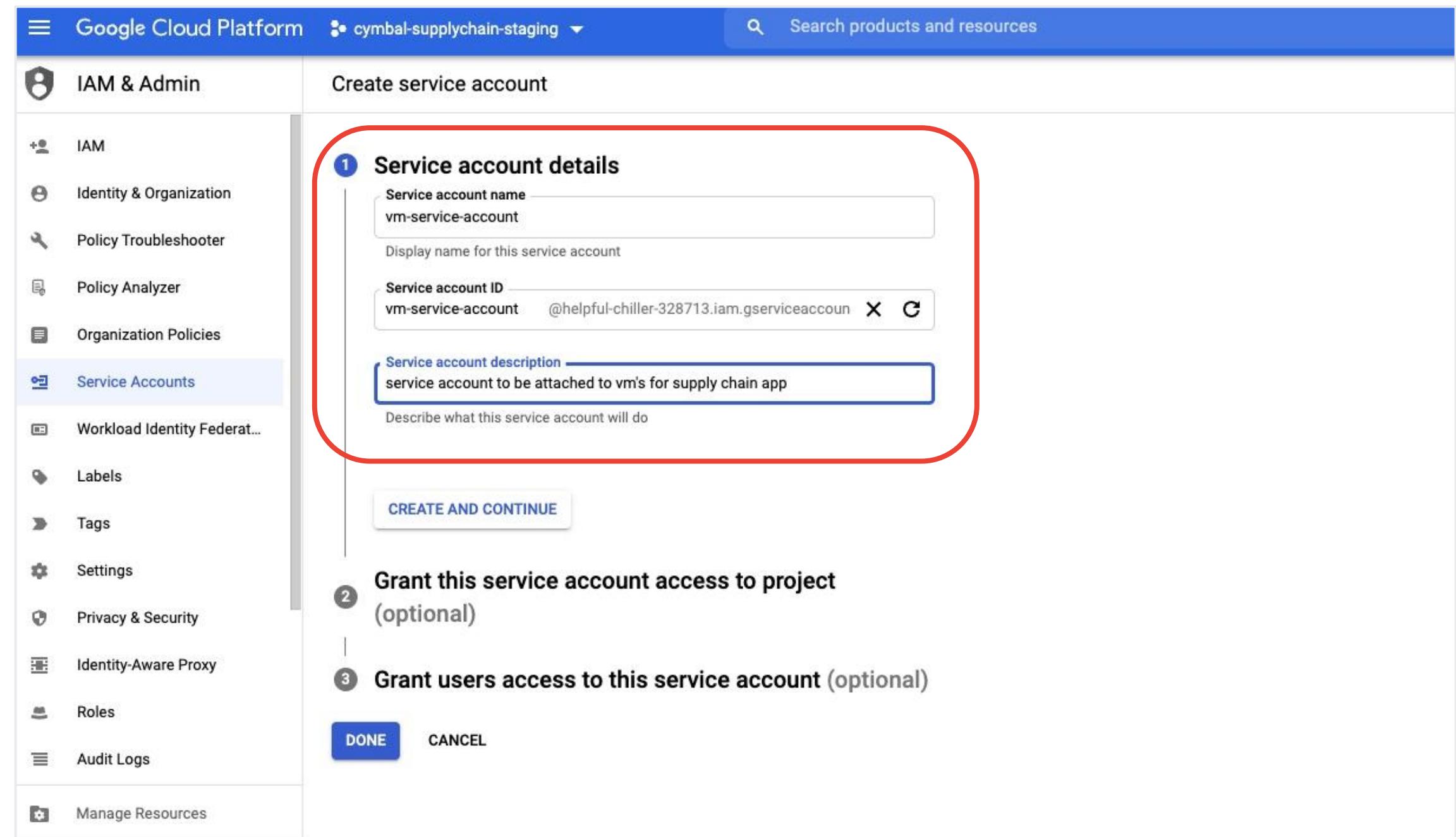
Describe what this service account will do

CREATE AND CONTINUE

2 Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

DONE CANCEL



02

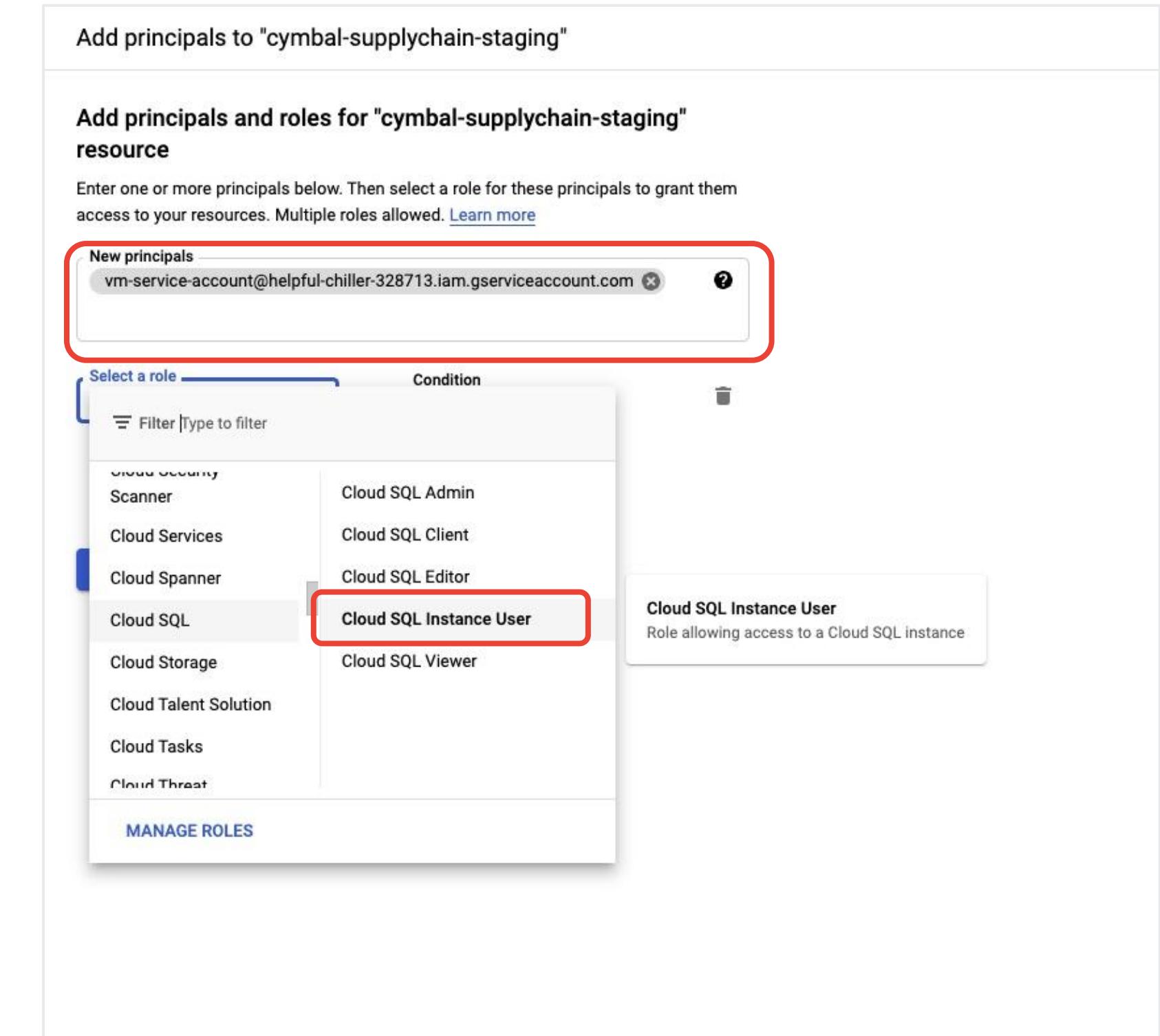
Assign permissions: Where to look

The screenshot shows the Google Cloud Platform IAM & Admin Service Accounts page. The left sidebar lists various IAM-related options. The main area displays a table of service accounts for the project "cymbal-supplychain-staging". One specific service account, "vm-service-account@helpful-chiller-328713.iam.gserviceaccount.com", is selected and highlighted with a red box. A context menu is open for this account, with the "Manage permissions" option also highlighted by a red box.

Status	Name ↑	Description	Key ID	Key creation date	Actions
✓	vm-service-account	service account to be attached to vm's for supply chain app	No keys		<ul style="list-style-type: none">⋮Manage detailsManage permissionsManage keysView metricsView logsDisableDelete

02

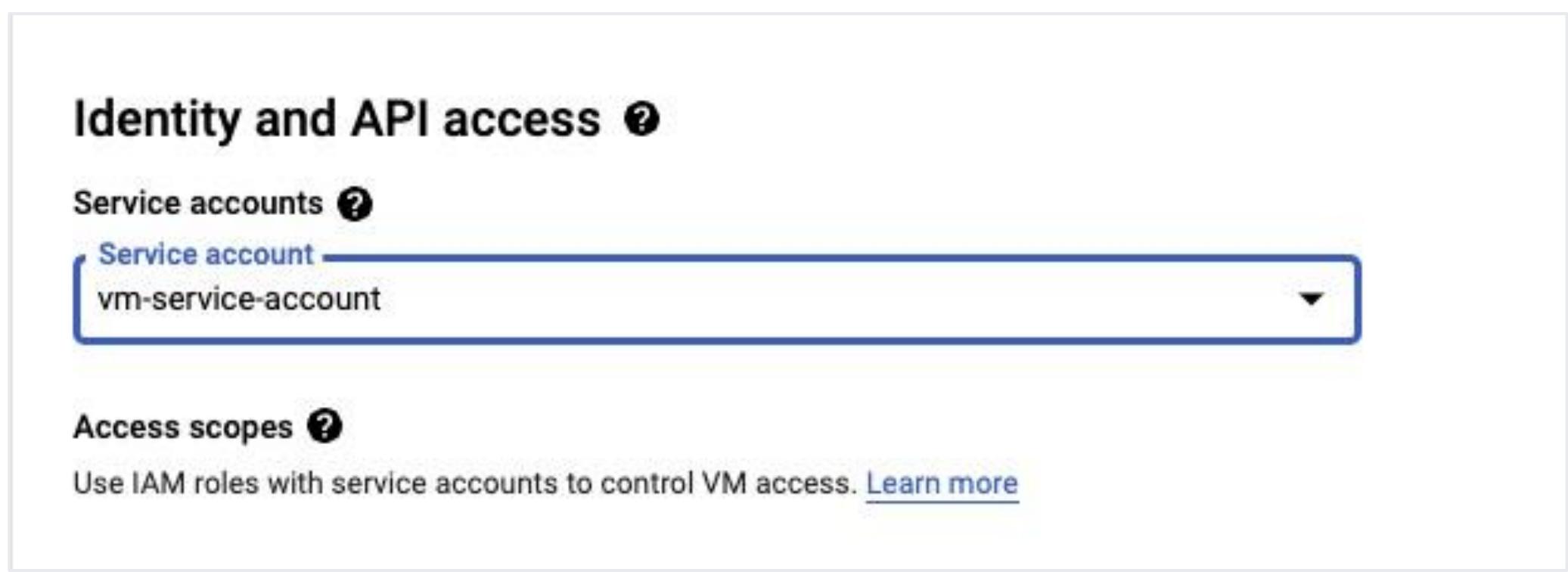
Assign permissions: Add necessary permissions



03

Add to a VM instance

Where to look



The screenshot shows the 'Identity and API access' section of the Google Cloud console. It displays a dropdown menu for 'Service accounts' with one item selected: 'vm-service-account'. Below this, there is a section for 'Access scopes' with a note: 'Use IAM roles with service accounts to control VM access.' and a link to 'Learn more'.

Identity and API access ?

Service accounts ?

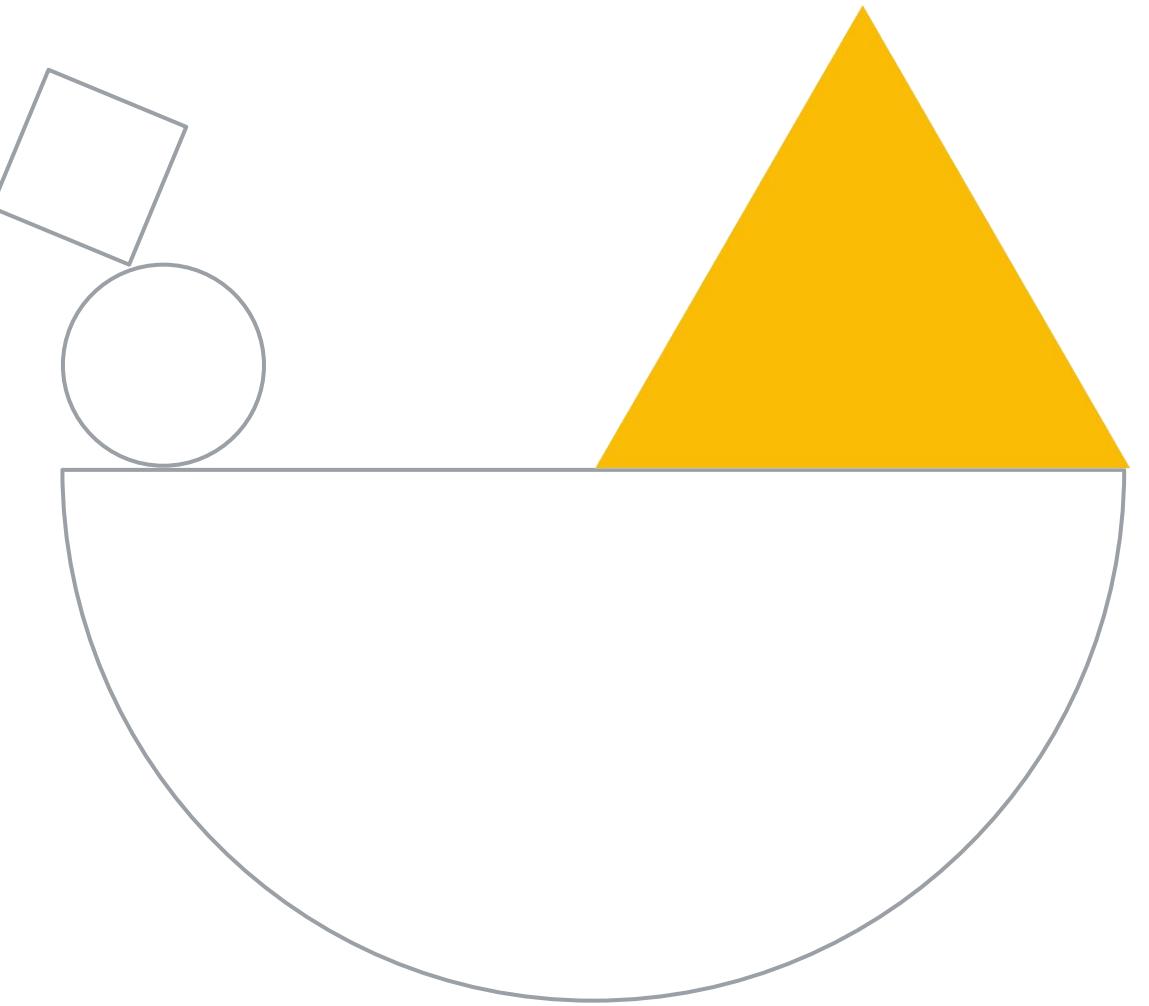
Service account ▼

vm-service-account

Access scopes ?

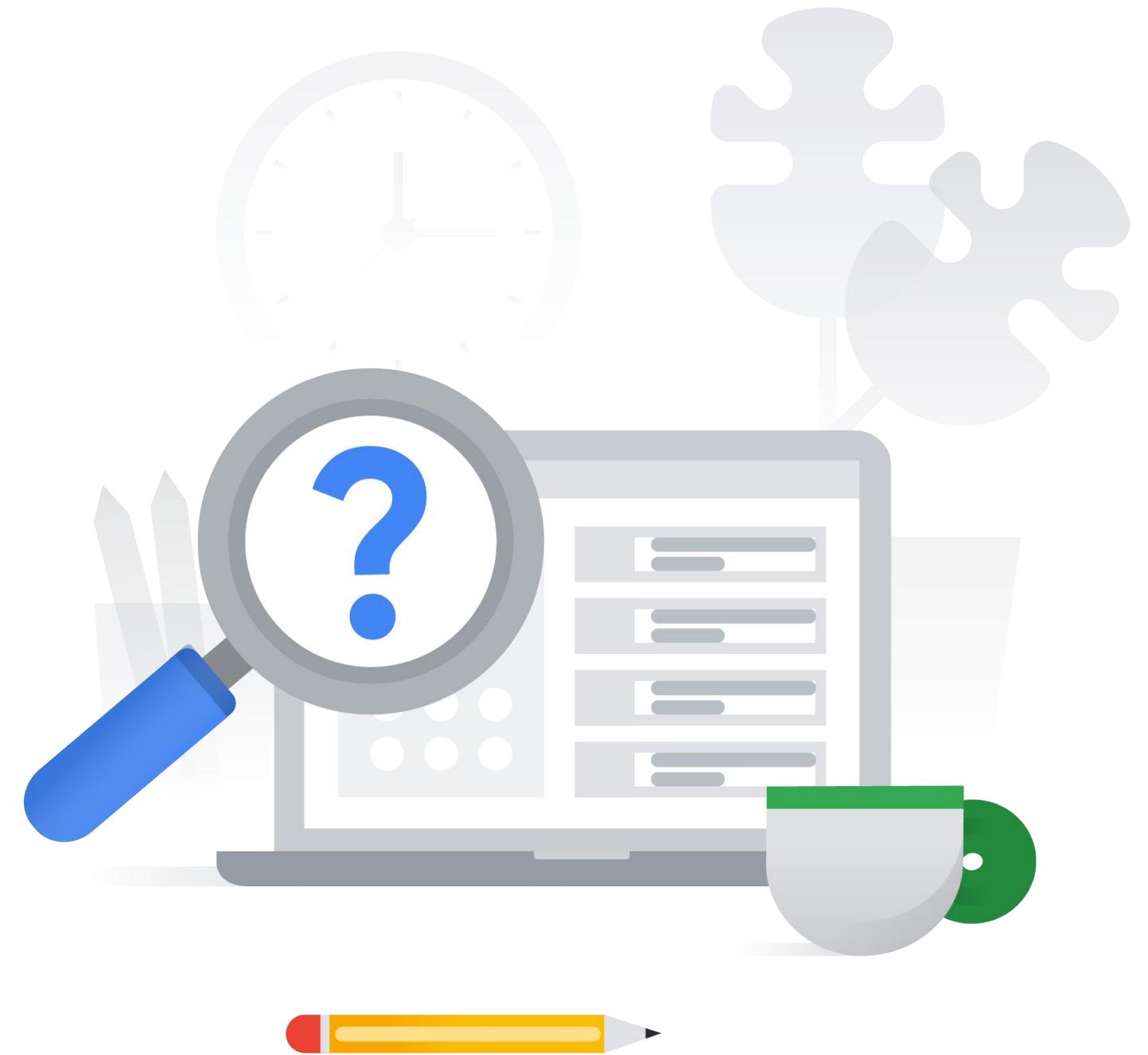
Use IAM roles with service accounts to control VM access. [Learn more](#)

Diagnostic questions

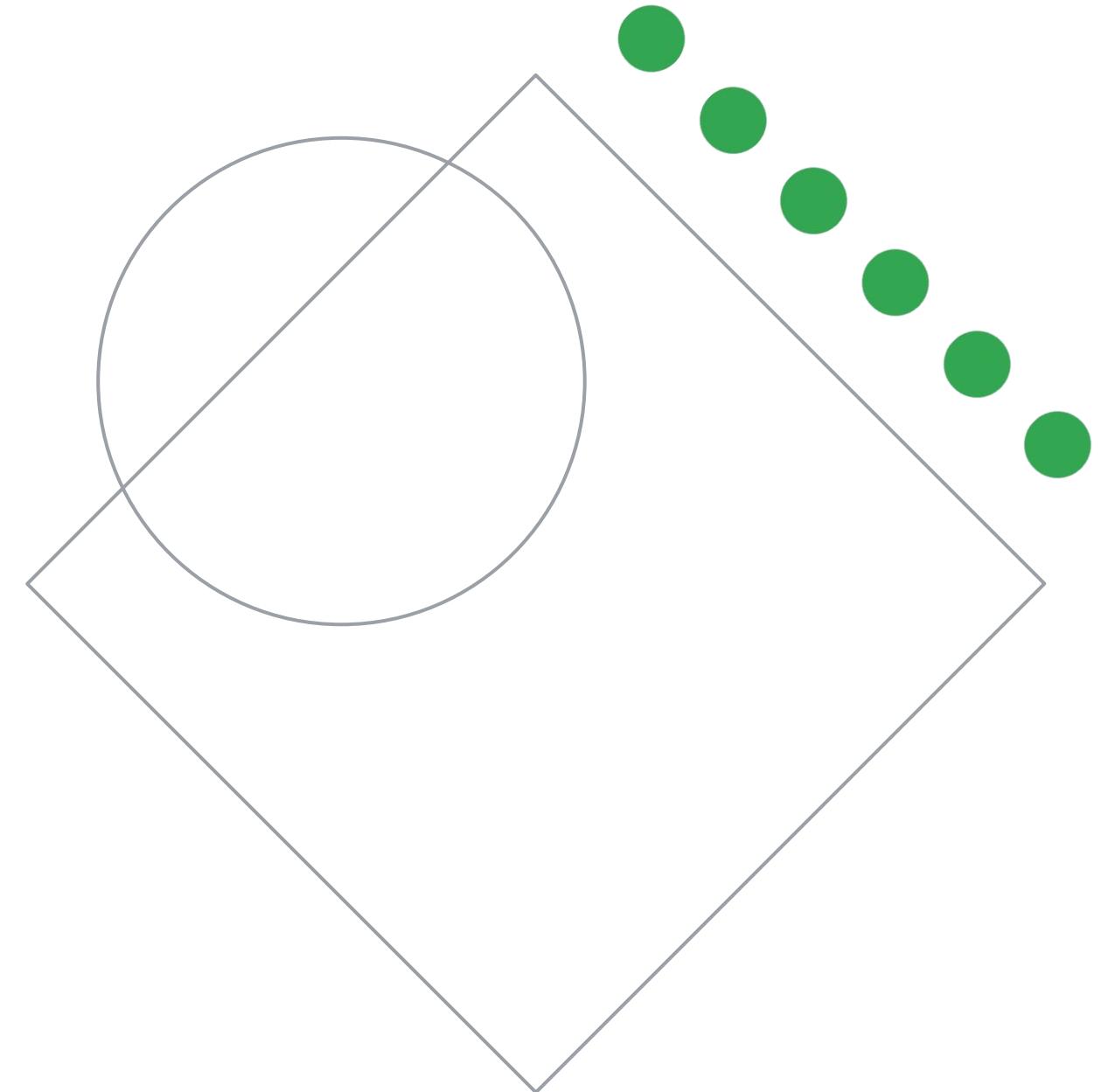


Please complete the diagnostic questions now

The diagnostic questions are also available in the workbook.

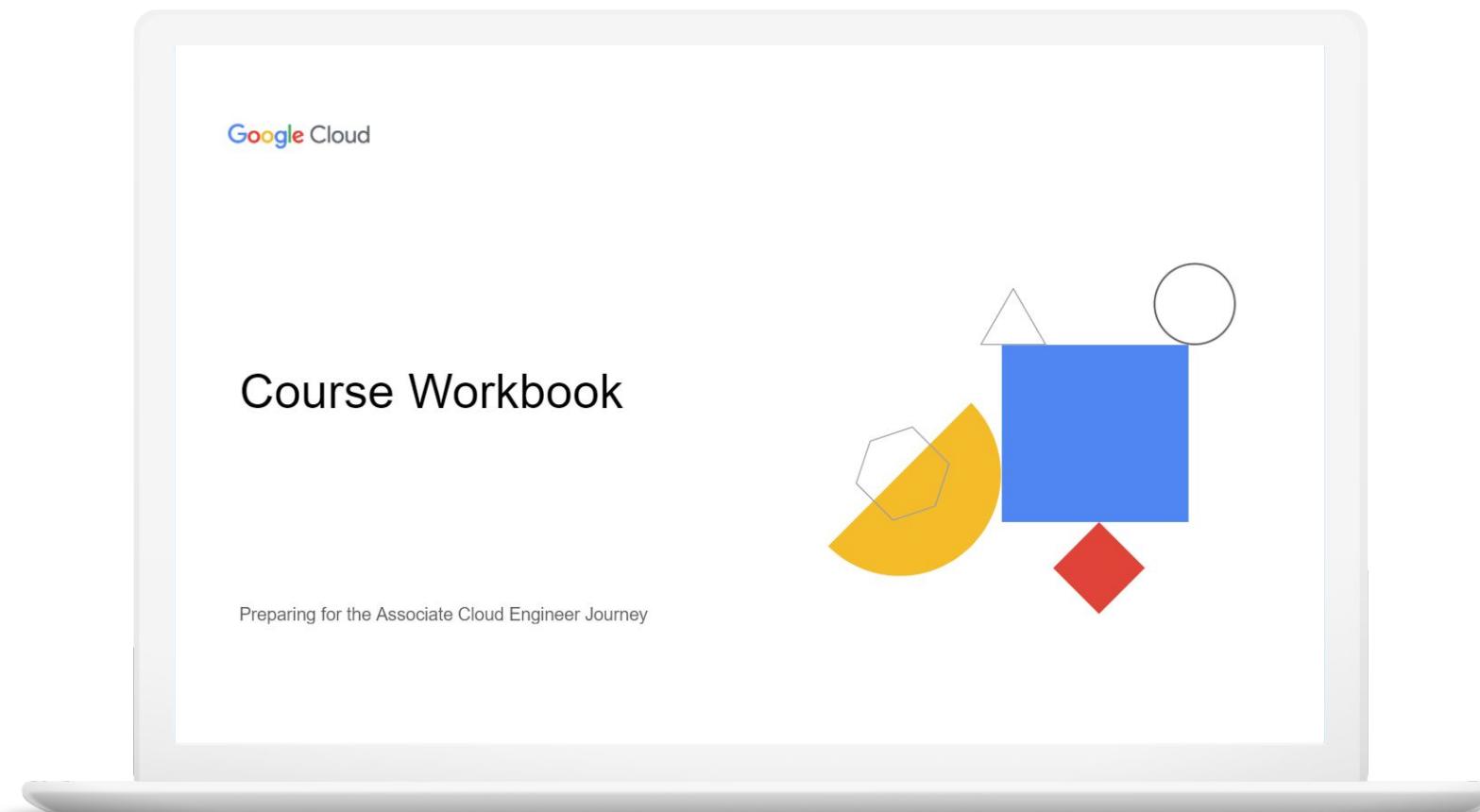


Review and study planning



Your study plan:

Configuring access and security



5.1

Managing Identity and Access Management (IAM)

5.2

Managing service accounts

5.1

Managing Identity and Access Management (IAM)

Considerations include:

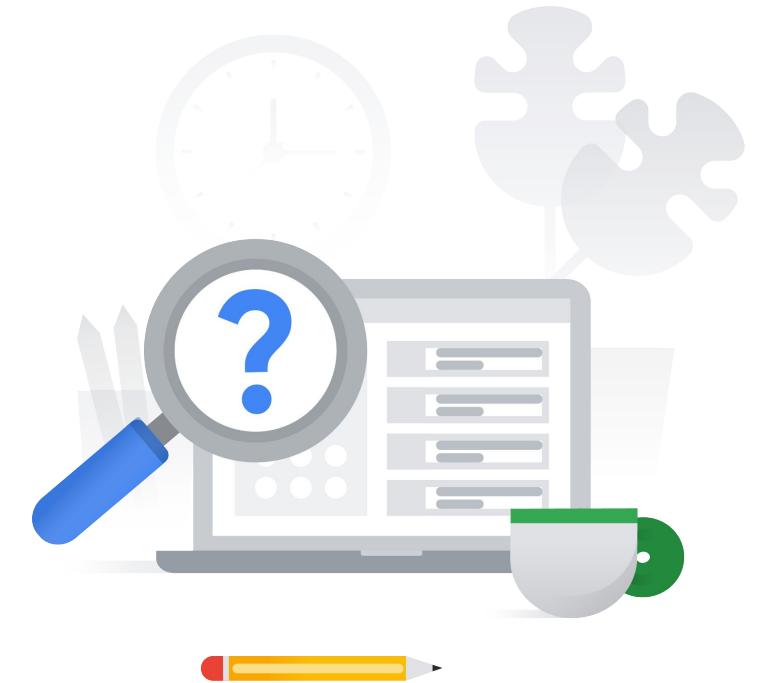
- Viewing and creating IAM policies
- Managing the various role types and defining custom IAM roles
(e.g., basic, predefined and custom)

5.1 | Diagnostic Question 01 Discussion

You need to configure access to Spanner from the GKE cluster that is supporting Cymbal Superstore's ecommerce microservices application. You want to specify an account type to set the proper permissions.

What should you do?

- A. Assign permissions to a Google account referenced by the application.
- B. Assign permissions through a Google Workspace account referenced by the application.
- C. Assign permissions through service account referenced by the application.
- D. Assign permissions through a Cloud Identity account referenced by the application.



5.1 | Diagnostic Question 01 Discussion

You need to configure access to Spanner from the GKE cluster that is supporting Cymbal Superstore's ecommerce microservices application. You want to specify an account type to set the proper permissions.

What should you do?

- A. Assign permissions to a Google account referenced by the application.
- B. Assign permissions through a Google Workspace account referenced by the application.
- C. Assign permissions through service account referenced by the application.** 
- D. Assign permissions through a Cloud Identity account referenced by the application.



Assign access to members using IAM

Member Identity

Google Account

userid@gmail.com

Service Account

1234@cloudservices.gserviceaccount.com

Google Group

groupname@googlegroups.com

Cloud Identity or Google Workspace Domain

alias@example.com

5.1 | Diagnostic Question 02 Discussion

You are trying to assign roles to the dev and prod projects of Cymbal Superstore's e-commerce app but are receiving an error when you try to run **set-iam policy**. The projects are organized into an ecommerce folder in the Cymbal Superstore organizational hierarchy. You want to follow best practices for the permissions you need while respecting the practice of least privilege.

What should you do?

- A. Ask your administrator for resourcemanager.projects.setIamPolicy roles for each project.
- B. Ask your administrator for the roles/resourcemanager.folderIamAdmin for the ecommerce folder.
- C. Ask your administrator for the roles/resourcemanager.organizationAdmin for Cymbal Superstore.
- D. Ask your administrator for the roles/iam.securityAdmin role in IAM.



5.1 | Diagnostic Question 02 Discussion

You are trying to assign roles to the dev and prod projects of Cymbal Superstore's e-commerce app but are receiving an error when you try to run **set-iam policy**. The projects are organized into an ecommerce folder in the Cymbal Superstore organizational hierarchy. You want to follow best practices for the permissions you need while respecting the practice of least privilege.

What should you do?

- A. Ask your administrator for resourcemanager.projects.setIamPolicy roles for each project.
- B. Ask your administrator for the roles/resourcemanager.folderIamAdmin for the ecommerce folder. ✓
- C. Ask your administrator for the roles/resourcemanager.organizationAdmin for Cymbal Superstore.
- D. Ask your administrator for the roles/iam.securityAdmin role in IAM.



Assign roles in the IAM interface

Add principals to "cymbal-supplychain-staging"

Add principals and roles for "cymbal-supplychain-staging" resource

Enter one or more principals below. Then select a role for these principals to grant them access to your resources. Multiple roles allowed. [Learn more](#)

New principals
user1@google.com [X](#) [?](#)

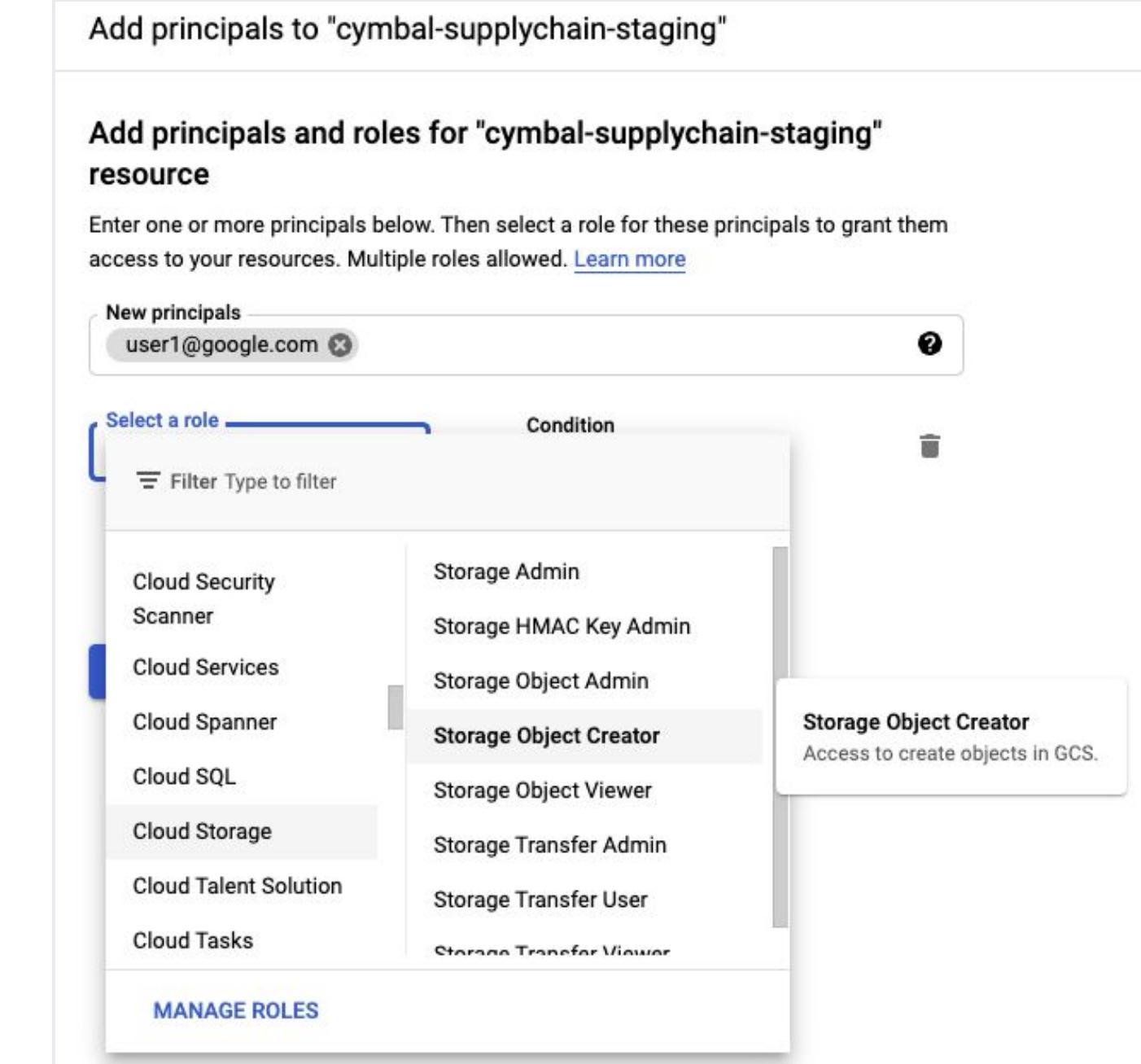
Select a role [Condition](#)

Filter Type to filter

Cloud Security	Storage Admin
Scanner	Storage HMAC Key Admin
Cloud Services	Storage Object Admin
Cloud Spanner	Storage Object Creator
Cloud SQL	Storage Object Viewer
Cloud Storage	Storage Transfer Admin
Cloud Talent Solution	Storage Transfer User
Cloud Tasks	Storage Transfer Viewer

Storage Object Creator
Access to create objects in GCS.

[MANAGE ROLES](#)



5.1 | Diagnostic Question 03 Discussion

You have a custom role implemented for administration of the dev/test environment for Cymbal Superstore's transportation management application. You are developing a pilot to use Cloud Run instead of Cloud Run functions. You want to ensure your administrators have the correct access to the new resources.

What should you do?

- A. Make the change to the custom role locally and run an update on the custom role.
- B. Delete the custom role and recreate a new custom role with required permissions.
- C. Copy the existing role, add the new permissions to the copy, and delete the old role.
- D. Create a new role with needed permissions and migrate users to it.



5.1 | Diagnostic Question 03 Discussion

You have a custom role implemented for administration of the dev/test environment for Cymbal Superstore's transportation management application. You are developing a pilot to use Cloud Run instead of Cloud Run functions. You want to ensure your administrators have the correct access to the new resources.

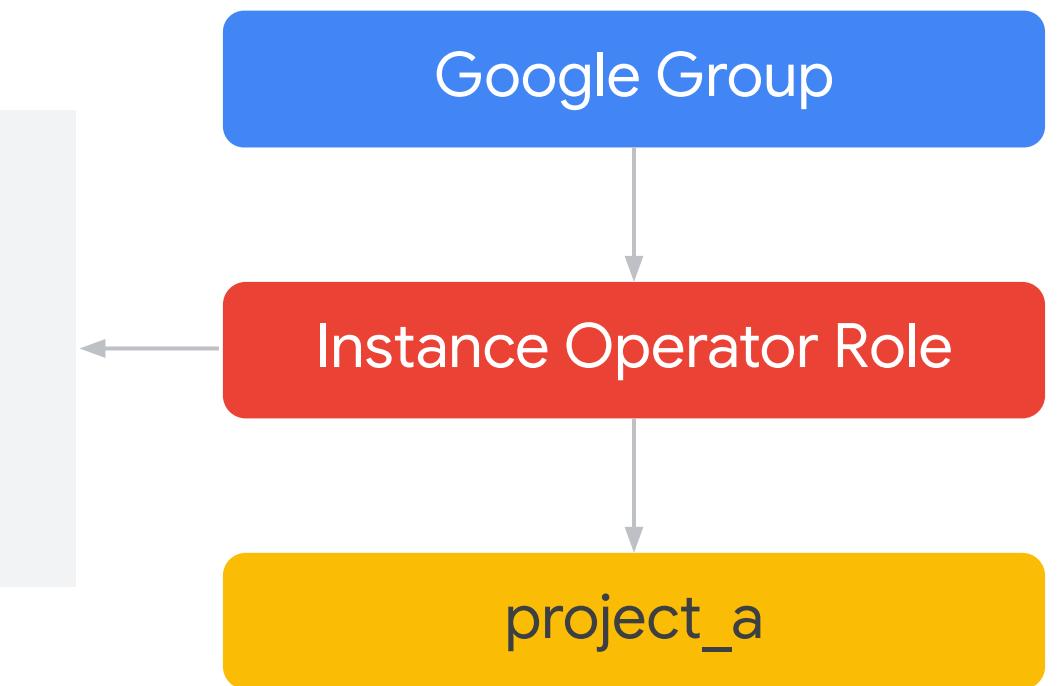
What should you do?

- A. Make the change to the custom role locally and run an update on the custom role.
- B. Delete the custom role and recreate a new custom role with required permissions.
- C. Copy the existing role, add the new permissions to the copy, and delete the old role.
- D. Create a new role with needed permissions and migrate users to it.



Create custom roles

- ✓ compute.instances.get
- ✓ compute.instances.list
- ✓ compute.instances.start
- ✓ compute.instances.stop



5.1

Managing Identity and Access Management (IAM)

Courses

[Google Cloud Fundamentals: Core Infrastructure](#)

- M2 Resources and Access in the Cloud

[Architecting with Google Compute Engine](#)

- M4 Identity and Access Management (IAM)



Skill Badge



[Develop your Google Cloud Network](#)



[Essential Google Cloud Infrastructure: Core Services](#)

- M1 Identity and Access Management (IAM)

Documentation

[Overview | IAM Documentation](#)

[Google Kubernetes Engine security overview](#)

5.2 | Managing service accounts

Considerations include:

- Creating service accounts
- Using service accounts in IAM policies with minimum permissions
- Assigning service accounts to resources
- Managing IAM of a service account
- Managing service account impersonation
- Creating and managing short-lived service account credentials

5.2 | Diagnostic Question 04 Discussion

Which of the scenarios below is an example of a situation where you should use a service account?

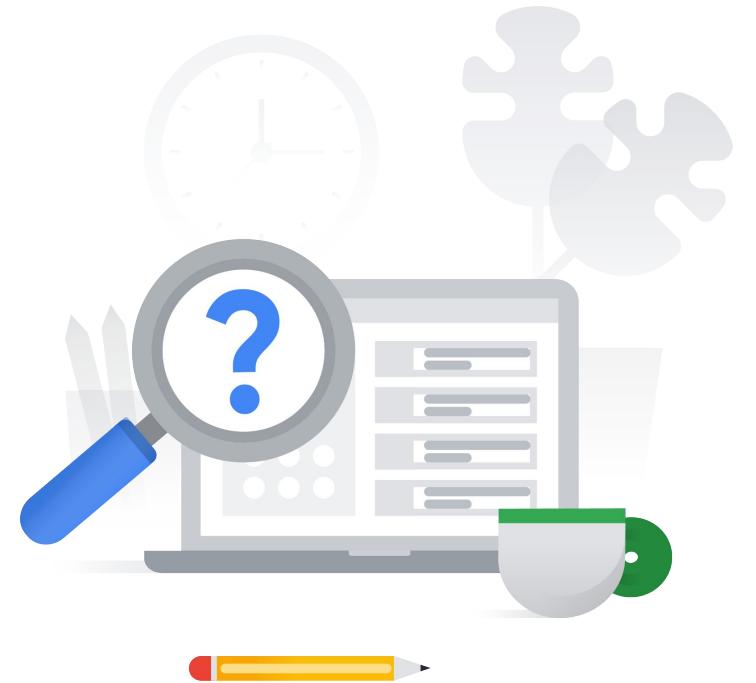
- A. To directly access user data
- B. For development environments
- C. For interactive analysis
- D. For individual GKE pods



5.2 | Diagnostic Question 04 Discussion

Which of the scenarios below is an example of a situation where you should use a service account?

- A. To directly access user data
- B. For development environments
- C. For interactive analysis
- D. For individual GKE pods



Create, use, and assign service accounts

01

To create a service account:

```
gcloud iam  
service-accounts create
```

02

To assign policies:

```
gcloud projects  
add-iam-policy
```

03

Attach a service account to a resource as you create it

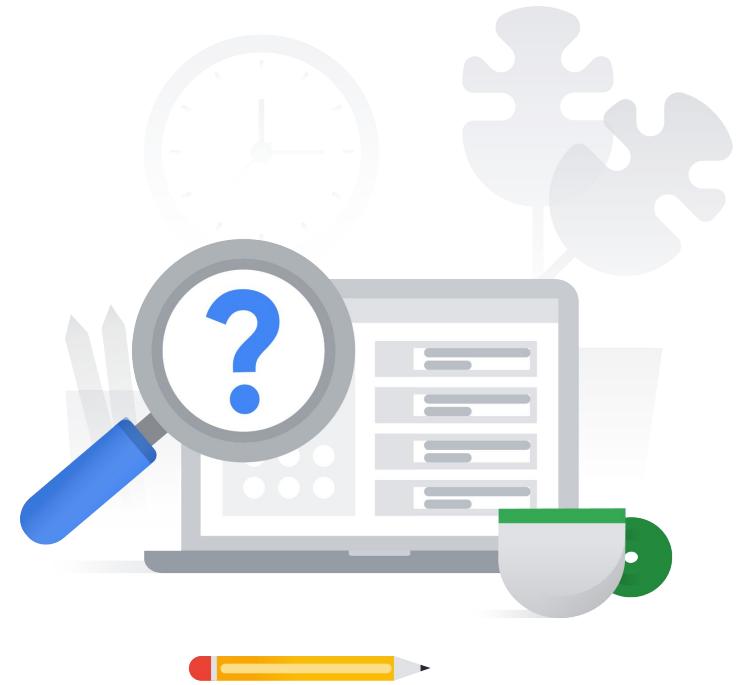
```
gcloud compute instances create  
cymbal-vm --service-account \  
<name-of-service-account@gservice  
account.com> \  
--scopes  
https://www.googleapis.com/auth/  
cloud-platform
```

5.2 | Diagnostic Question 05 Discussion

Cymbal Superstore is implementing a mobile app for end users to track deliveries that are en route to them. The app needs to access data about truck location from Pub/Sub using Google recommended practices.

- A. API key
- B. OAuth 2.0 client
- C. Environment provided service account
- D. Service account key

What kind of credentials should you use?

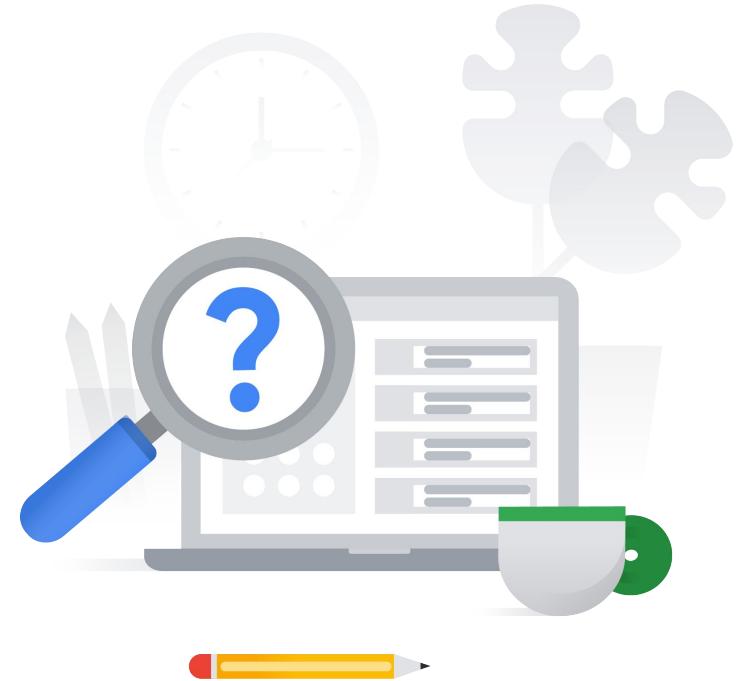


5.2 | Diagnostic Question 05 Discussion

Cymbal Superstore is implementing a mobile app for end users to track deliveries that are en route to them. The app needs to access data about truck location from Pub/Sub using Google recommended practices.

What kind of credentials should you use?

- A. API key
- B. OAuth 2.0 client
- C. Environment provided service account
- D. Service account key



Types of authentication keys

01

API Key

To access public data

02

OAuth2.0 Client

To access private end-user data

03

Environment provided service account

To access resources with a service account internal to Google Cloud

04

Service account key

To access resources with a service account outside of Google Cloud

5.2 | Managing service accounts

Courses

[Google Cloud Fundamentals: Core Infrastructure](#)

- M2 Resources and Access in the Cloud

[Architecting with Google Compute Engine](#)

- M4 Identity and Access Management (IAM)



=

[Essential Google Cloud Infrastructure: Core Services](#)

- M1 Identity and Access Management (IAM)



Documentation

[Authenticating as a service account | Authentication](#)
[Authentication overview](#)

Knowledge Check 1

What kind of account is meant for machine-to-machine communication in Google Cloud?

- A. User Account
- B. Google Workspace account
- C. Service Account
- D. Cloud Identity account



Knowledge Check 1

What kind of account is meant for machine-to-machine communication in Google Cloud?

- A. User Account
- B. Google Workspace account
- C. Service Account
- D. Cloud Identity account



Knowledge Check 2

You are authenticating an application to service APIs. Both resources are internal to the Google Cloud environment. What type of credentials should you use?

- A. User account credentials
- B. Locally stored keys
- C. API keys
- D. Temporary credentials



Knowledge Check 2

You are authenticating an application to service APIs. Both resources are internal to the Google Cloud environment. What type of credentials should you use?

- A. User account credentials
- B. Locally stored keys
- C. API keys
- D. Temporary credentials

