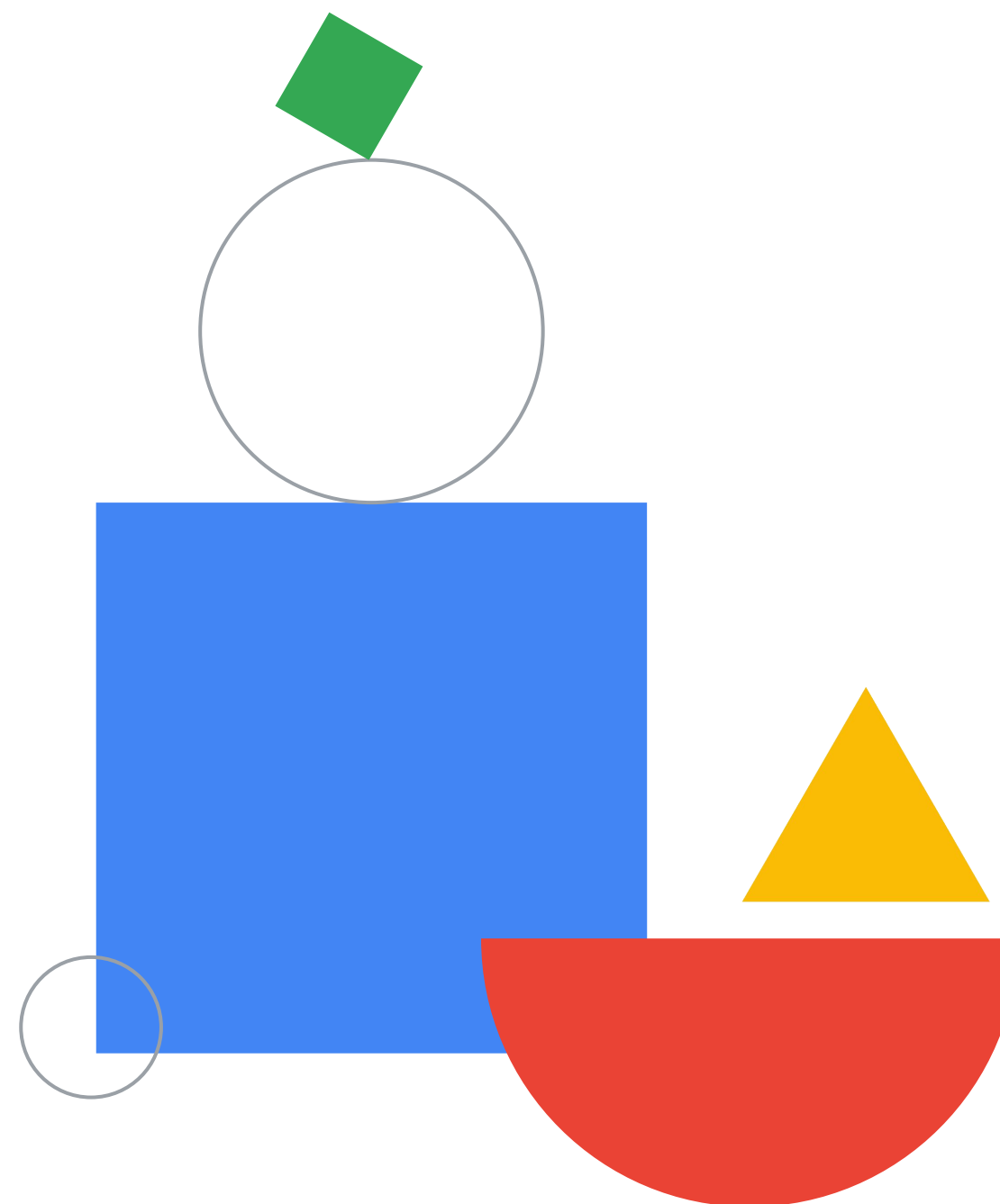


Preparing for Your Associate Cloud Engineer Journey

Module 5: Configuring Access and Security



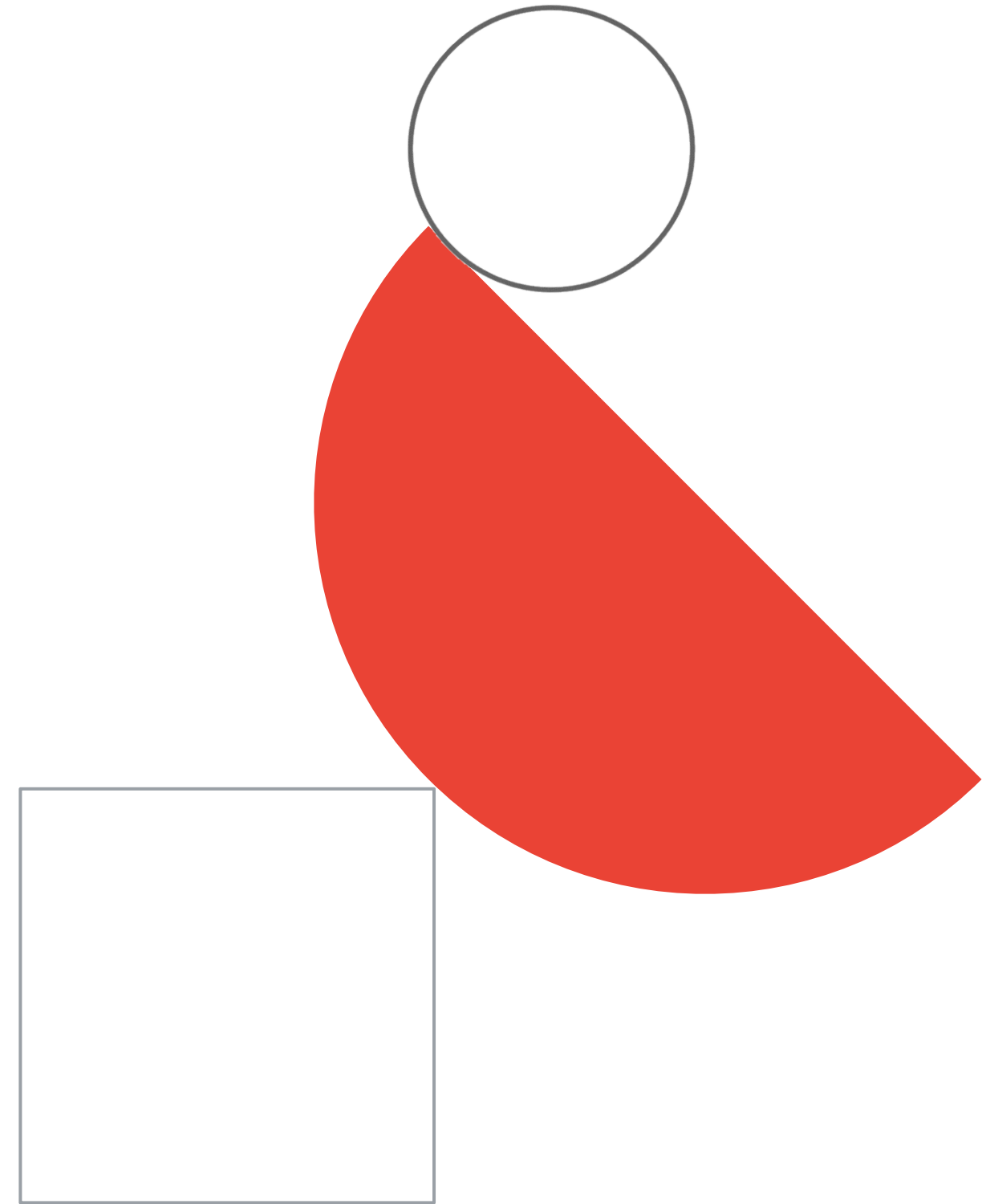


Module agenda

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

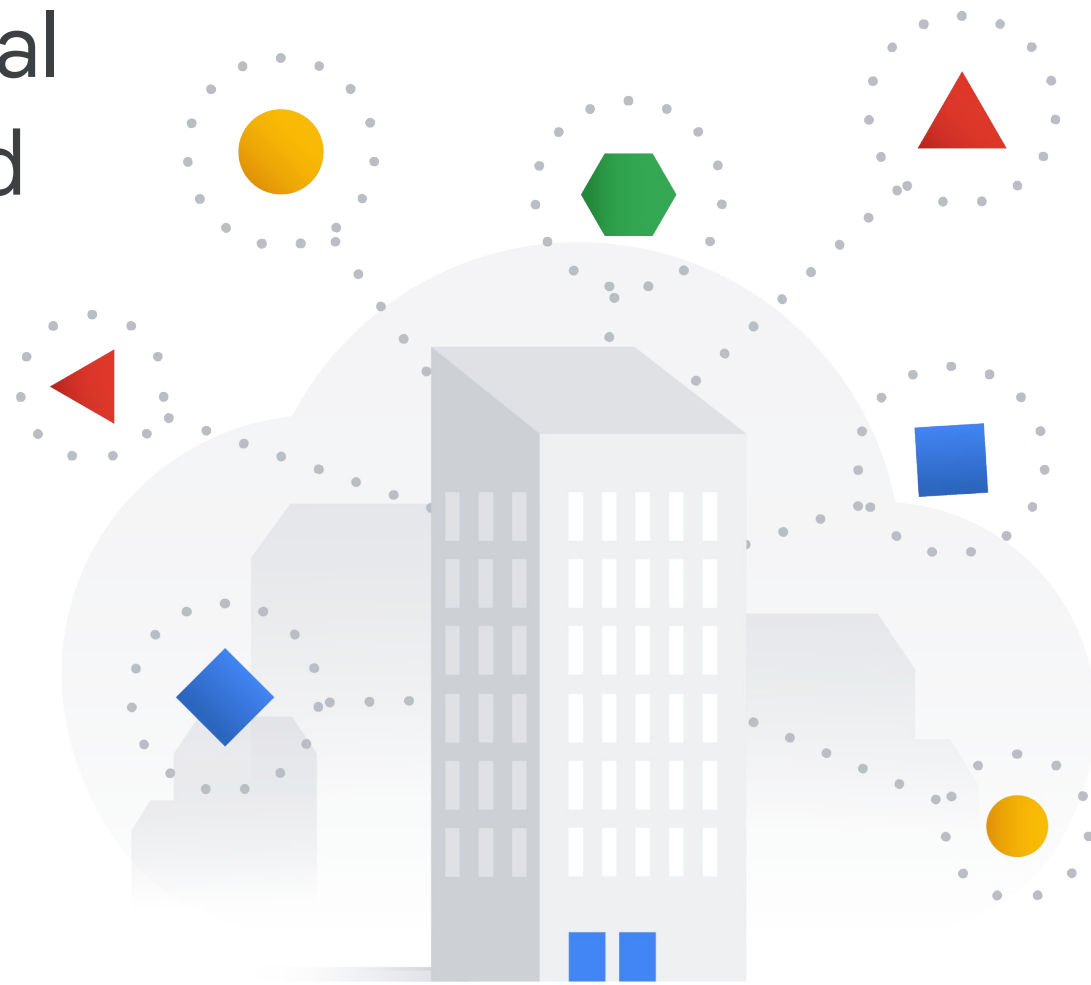


Managing access for Cymbal Superstore's cloud solutions



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

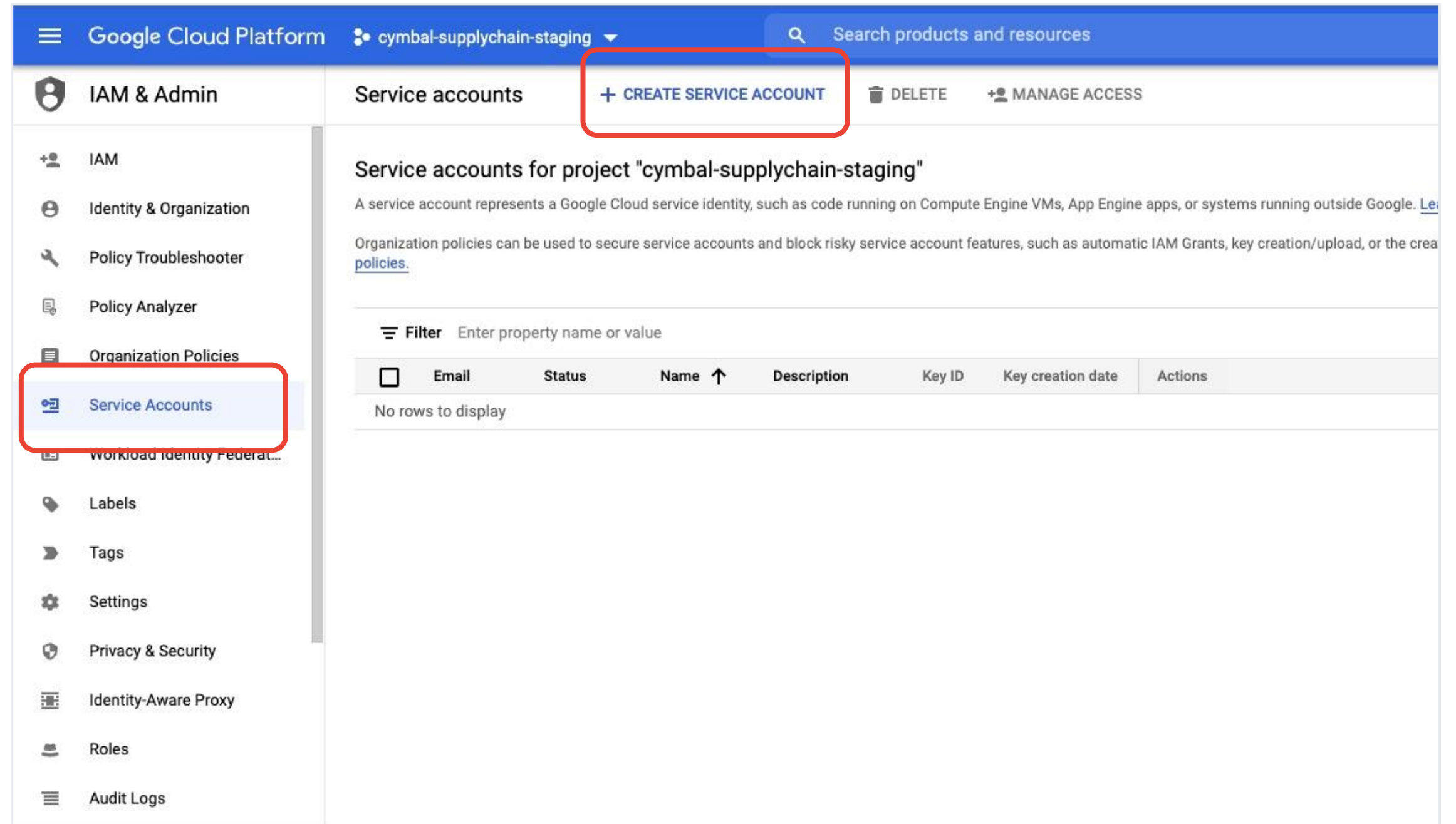


- 1 Create a service account
- 2 Assign Permissions
- 3 Attach to a VM

01

Create a service account:

Where to look



01

Create a service account:

Enter service account details

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

IAM & Admin

- 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

Create service account

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 ↺

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

IAM & Admin

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

Google Cloud Platform

cymbal-supplychain-staging

Search products and resources

Service accounts

+ CREATE SERVICE ACCOUNT

DELETE

+ MANAGE ACCESS



Service accounts for project "cymbal-supplychain-staging"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. [Learn more about service accounts.](#)

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. [Learn more about service account organization policies.](#)

Filter

Enter property name or value

| | Email | Status | Name ↑ | Description | Key ID | Key creation date | Actions |
|--------------------------|---|---|--------------------|---|---------|-------------------|---|
| <input type="checkbox"/> | | | | | | | |
| <input type="checkbox"/> |  vm-service-account@helpful-chiller-328713.iam.gserviceaccount.com |  | vm-service-account | service account to be attached to vm's for supply chain app | No keys | | <div><div>Manage details</div><div>Manage permissions</div><div>Manage keys</div><div>View metrics</div><div>View logs</div><div>Disable</div><div>Delete</div></div> |

02 Assign permissions: Add necessary permissions

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

vm-service-account@helpful-chiller-328713.iam.gserviceaccount.com

Select a role

Filter | Type to filter

| | |
|------------------------|--------------------------------|
| Cloud Security Scanner | Cloud SQL Admin |
| Cloud Services | Cloud SQL Client |
| Cloud Spanner | Cloud SQL Editor |
| Cloud SQL | Cloud SQL Instance User |
| Cloud Storage | Cloud SQL Viewer |
| Cloud Talent Solution | |
| Cloud Tasks | |
| Cloud Threat | |

[MANAGE ROLES](#)

Cloud SQL Instance User
Role allowing access to a Cloud SQL instance

03

Add to a VM instance

Where to look

Identity and API access ?

Service accounts ?

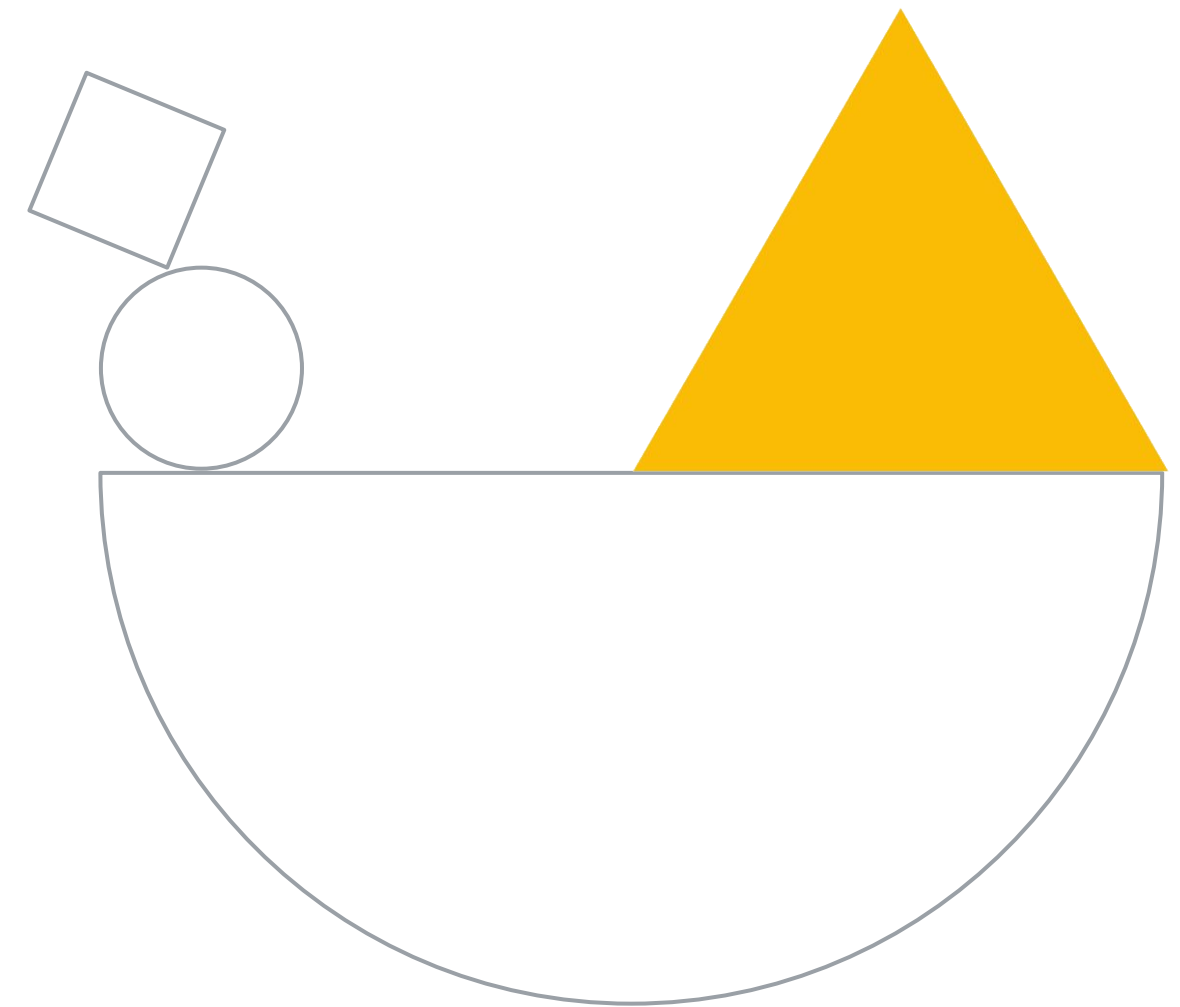
Service account

vm-service-account

Access scopes ?

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

Diagnostic questions

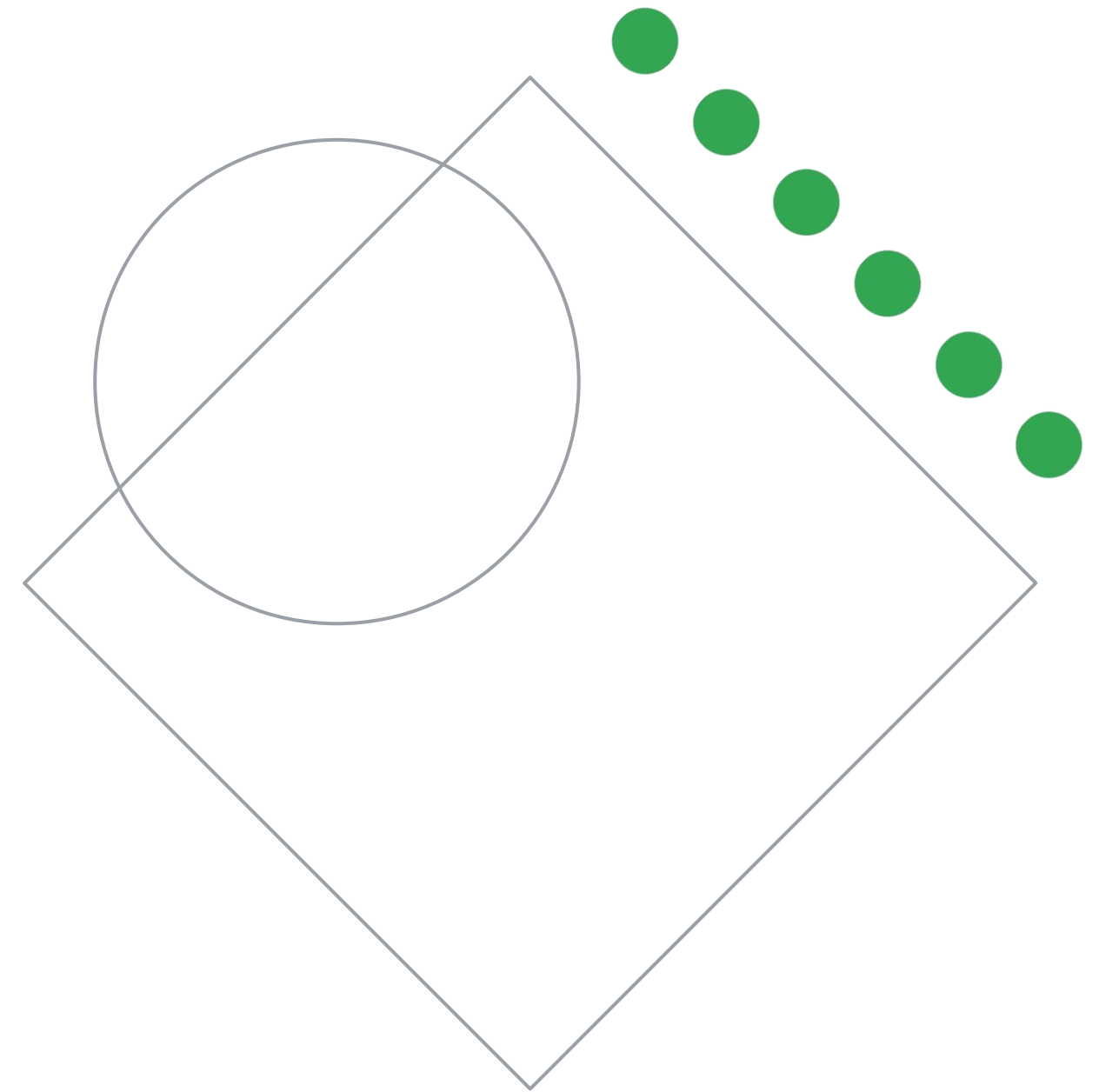


Please complete the diagnostic questions now

The diagnostic questions are also available in the workbook.

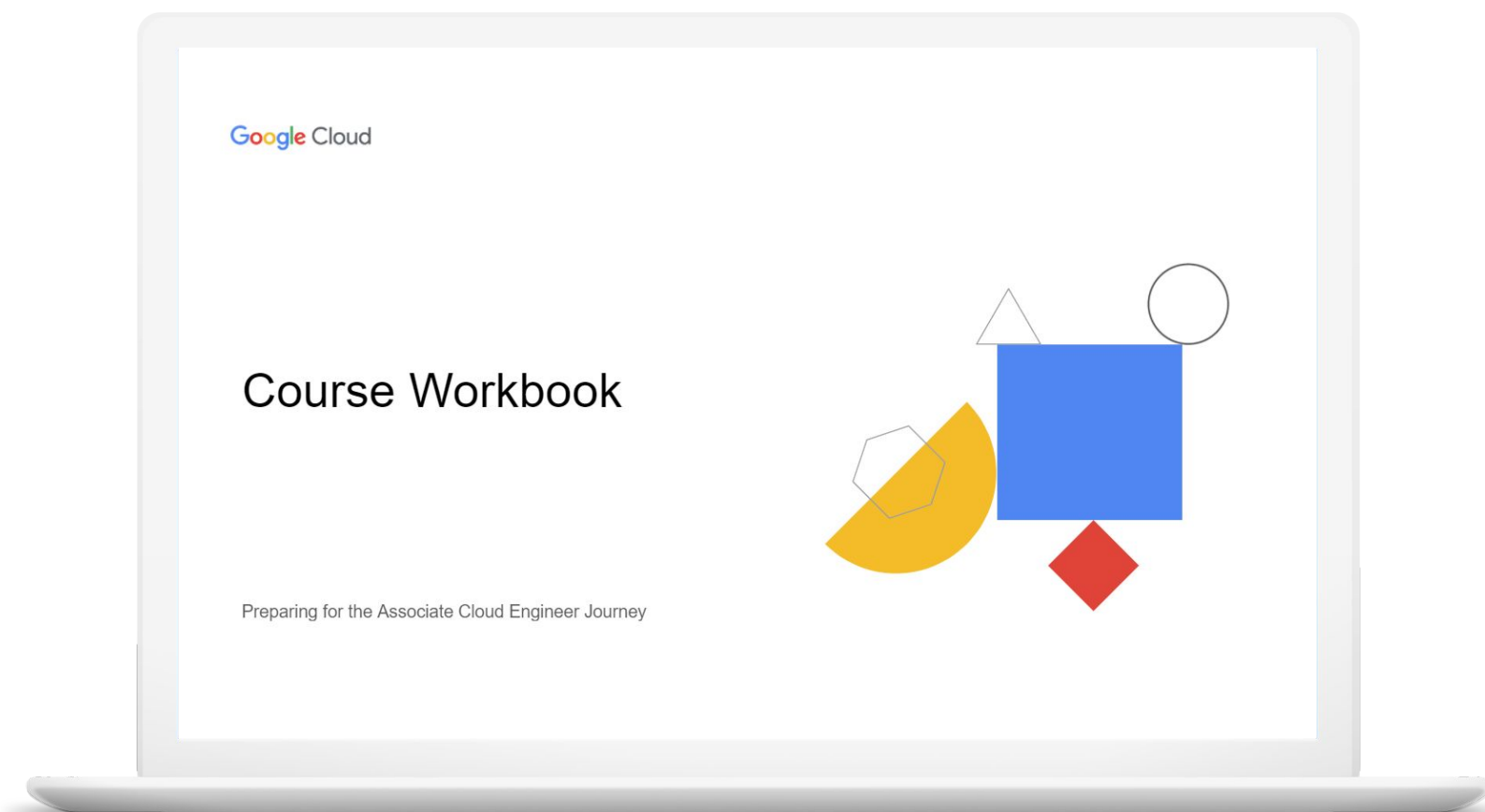


Review and study planning



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 | |
|---|---|
| <div>Google Account</div> <div>userid@gmail.com</div> | <div>Service Account</div> <div>1234@cloudservices.gserviceaccount.com</div> |
| <div>Google Group</div> <div>groupname@googlegroups.com</div> | <div>Cloud Identity or Google Workspace Domain</div> <div>alias@example.com</div> |

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.

- 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.

What should you do?

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.

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.

What should you do?

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

Select a role

Condition

Filter Type to filter

Cloud Security Scanner

Cloud Services

Cloud Spanner

Cloud SQL

Cloud Storage

Cloud Talent Solution

Cloud Tasks

Storage Admin

Storage HMAC Key Admin

Storage Object Admin

Storage Object Creator

Storage Object Viewer

Storage Transfer Admin

Storage Transfer User

Storage Transfer Viewer

MANAGE ROLES

Storage Object Creator

Access to create objects in GCS.

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.

- 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.

What should you do?

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`

Google Group

Instance Operator Role

project_a

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)



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

- M1 Identity and Access Management (IAM)



Skill Badge



Google Cloud

[Develop your Google Cloud Network](#)



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@gservic  
eaccount.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

