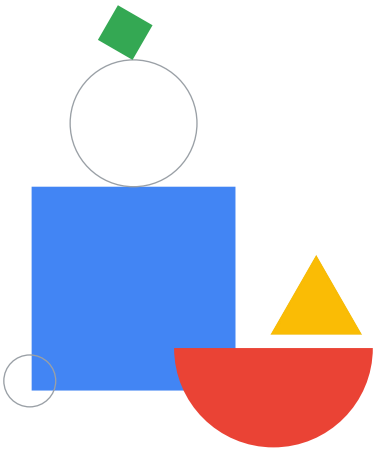
Google Cloud

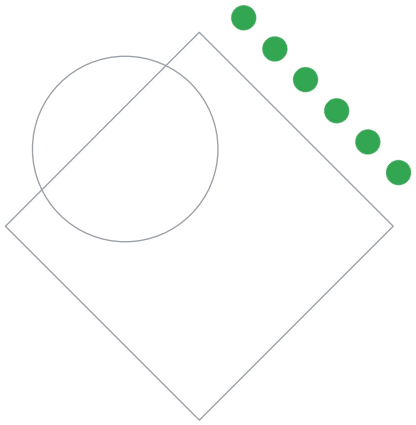
Preparing for Your Associate Cloud Engineer Journey



Module 5: Configuring Access and Security

Welcome to Module 5: Configuring Access and Security.

Review and study planning

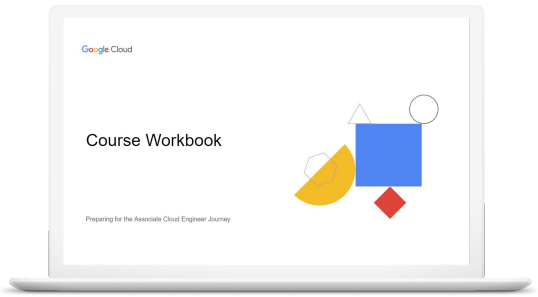


Google Cloud

What areas do you need to develop your skills in order to successfully manage access for Google Cloud solutions? Recall that this exam section is narrower in scope but nevertheless important for the role of an Associate Cloud Engineer. Let’s review the diagnostic questions to help you target your study time to focus on the areas where you need to develop your skills.

Your study plan:

Ensuring successful operation of a cloud solution



5.1 Managing Identity and Access Management (IAM)

5.2 Managing service accounts

5.3 Viewing audit logs

Google Cloud

We'll approach this review by looking at the objectives of this exam section and the questions you just answered about each one. We'll introduce an objective, briefly review the answers to the related questions, then talk about where you can find out more in the learning resources and/or in Google Cloud documentation. As we go through each section objective, use the page in your workbook to mark the specific documentation, courses (and modules!), and quests you'll want to emphasize in your study plan.

There are fewer objectives and tasks involved with this section - but don't forget to plan for them in your study time.

5.1 Managing Identity and Access Management (IAM)

Tasks include:

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

Google Cloud

We worked on planning Cymbal Superstore's resource hierarchy earlier in the course. The organization is divided into folders, and the folders into projects. Identity and Access Management lets your users and groups access Google Cloud resources. As an Associate Cloud Engineer, it is important that you know both what users and groups to implement for Cymbal Superstore's needs and how to implement them.

The tasks included in this part of your job as an Associate Cloud Engineer include viewing IAM policies, creating IAM policies, and knowing when to implement the different types of policies, including basic, predefined and custom roles.

These are the diagnostic questions you answered that relate to this area:
Question 1: Identify types of members you can assign access to in IAM.
Question 2: Describe how to assign roles in the IAM interface.
Question 3: List the steps to create a custom role in IAM.

5.1 Diagnostic Question 01 Discussion

You need to configure access to Cloud 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.

Google Cloud

Question:
You need to configure access to Cloud 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
Feedback: Incorrect. A Google account uses a username and password to authenticate a user. An application does not authenticate interactively with this type of account.

B. Assign permissions through a Google Workspace account referenced by the application
Feedback: Incorrect. A Google Workspace account is an account created for you as part of an organization that is using Google Workspace products to collaborate with one another. It is not appropriate for managing the permissions an application needs to communicate with a backend.

*C. Assign permissions through service account referenced by the application
Feedback: Correct! A service account uses an account identity and an access key. It is used by applications to connect to services.

D. Assign permissions through a Cloud Identity account referenced by the application
Feedback: Incorrect. Cloud Identity is a user management tool for providing login

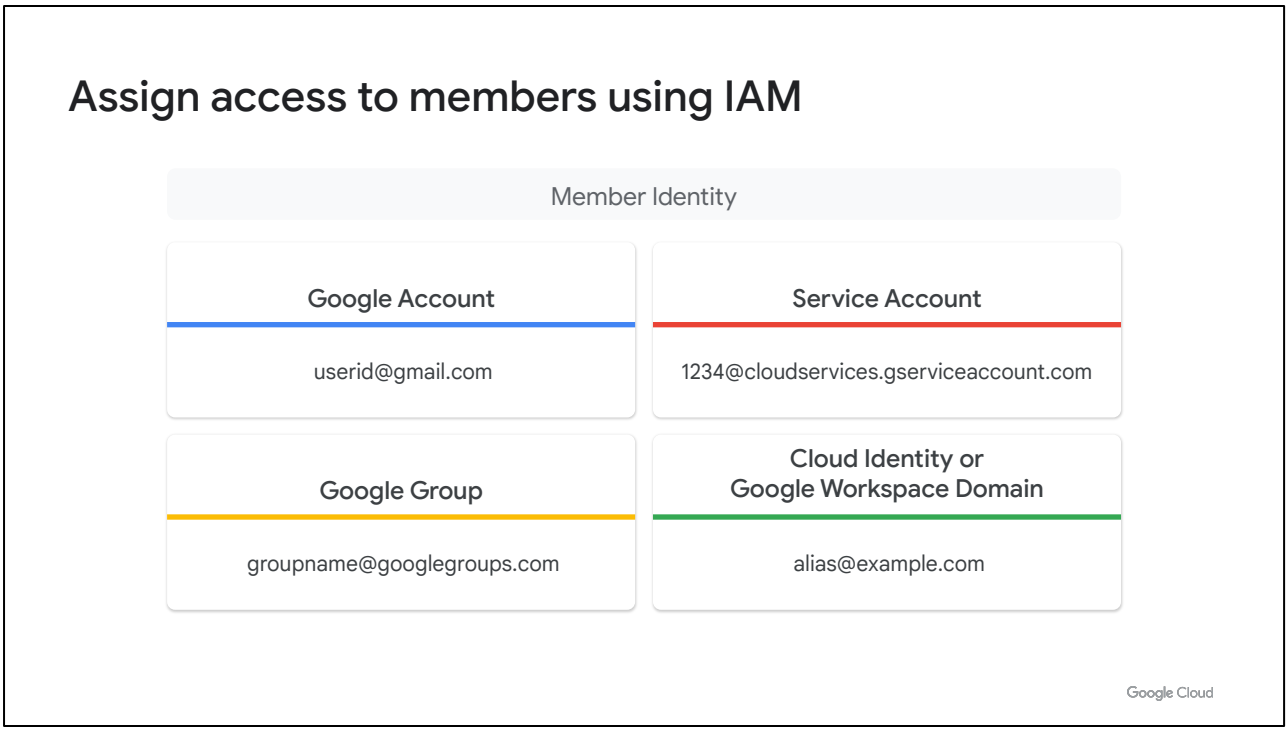
credentials to users of an organization that does not use Google Workspace collaboration tools. Cloud Identity is not used to manage application authentication.

Where to look:
https://cloud.google.com/iam/docs/overview

Content mapping:

- Instructor-led Training/OnDemand
  - Google Cloud Fundamentals: Core Infrastructure
    - M2 Getting Started with Google Cloud
  - Architecting with Google Compute Engine
    - M4 Cloud IAM
- Quests
  - Set Up and Configure a Cloud Environment in Google Cloud (https://www.qwiklabs.com/quests/119)

Summary:
Explanation/summary on the following slide.



A Google account represents anyone who interacts with Google Cloud. When signing up for a Google account you will be asked to provide an email address that is associated with the account. The email does not have to come from the gmail domain.

A service account is how applications and resources authenticate and access services in Google Cloud. Since apps cannot sign in interactively with a username and password, service accounts use keys to authenticate.

Google groups are collections of identity principals that can be referenced by the email address assigned to the group. You can apply access policies to a group. Each member of the group will receive the permissions you specify in the group policy as they authenticate.

Google Workspace and Cloud Identity domains give you the ability to manage users based on the way your organization interacts with Google. Each method gives you a virtual group representing all the registered users in your organization and the ability to add, modify, and delete users and groups.

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.

Google Cloud

Question:
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
Feedback: Incorrect. Best practice is to minimize the number of access policies you require.

*B. Ask your administrator for the `roles/resourcemanager.folderIamAdmin` for the ecommerce folder
Feedback: Correct! This choice gives you the required permissions while minimizing the number of individual resources you have to set permissions for.

C. Ask your administrator for the `roles/resourcemanager.organizationAdmin` for Cymbal Superstore
Feedback: Incorrect. This does not meet the requirements for least privilege.

D. Ask your administrator for the `roles/iam.securityAdmin` role in IAM.
Feedback: Incorrect. Security Admin allows you to access most Google Cloud

resources. Assigning the security Admin role does not meet least privilege requirements.

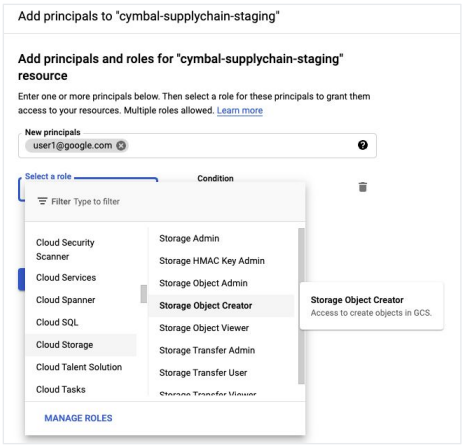
Where to look:
https://cloud.google.com/architecture/prep-kubernetes-engine-for-prod#managing_identity_and_access

Content mapping:

- Instructor-led Training/OnDemand
  - Google Cloud Fundamentals: Core Infrastructure
    - M2 Getting Started with Google Cloud
  - Architecting with Google Compute Engine
    - M4 Cloud IAM
- Quests
  - Set Up and Configure a Cloud Environment in Google Cloud (https://www.qwiklabs.com/quests/119)

Summary:
Explanation/summary on the following slide.

Assign roles in the IAM interface



Google Cloud

These are the steps to assign roles in the IAM interface.

1. Go to the IAM page
2. Select project, folder, or organization
3. Show info panel if it is not available
4. Click permissions
5. Select or add a principal to add a role to
    a. If the principal already exists click on Add another role
    b. For a new principal click add and enter the principals email address
6. Select a role to grant
7. Add a condition
8. Click Save

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 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.

Google Cloud

Question:
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 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
Feedback: Correct! There is a recommended process to update an existing custom role. You get the current policy, update it locally, and write the updated policy back into Google Cloud. The gcloud commands used in this process include the get and update policy subcommands.

B. Delete the custom role and recreate a new custom role with required permissions
Feedback: Incorrect. Recreating a custom role is not necessary in this scenario. You can update the existing one.

C. Copy the existing role, add the new permissions to the copy, and delete the old role
Feedback: Incorrect. Copying an existing role creates a new custom role. Creating a new custom role is not required for this scenario.

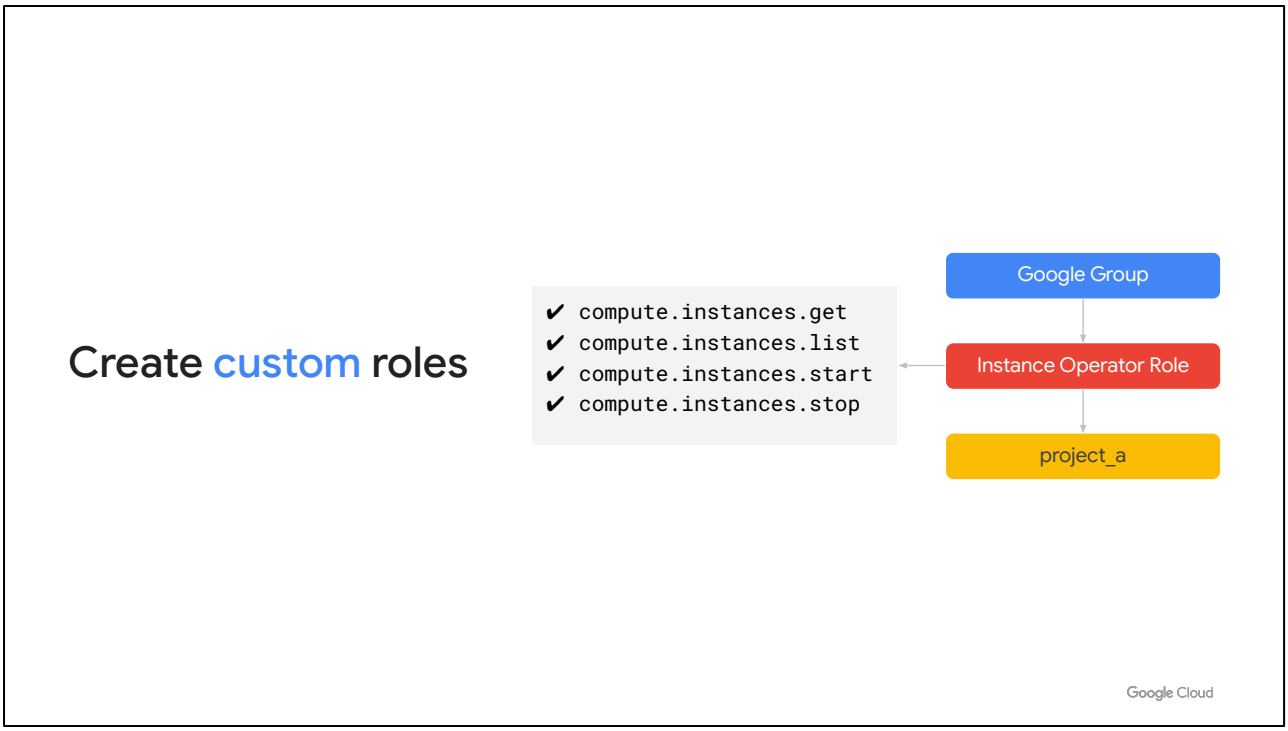
D. Create a new role with needed permissions and migrate users to it.
Feedback: Incorrect. Finding all users with this role and reassigning them could be very time consuming. You should update the existing custom role instead.

Where to look:
https://cloud.google.com/iam/docs/creating-custom-roles

Content mapping:

- Instructor-led Training/OnDemand
  - Architecting with Google Compute Engine
    - M4 IAM
- Quests
  - Set Up and Configure a Cloud Environment in Google Cloud (https://www.qwiklabs.com/quests/119)

Summary:
Explanation/summary on the following slide.



The first thing you need to do when creating custom permissions is be familiar with the permissions and roles that are available in your project or organization.

The gcloud command you need to run is:

gcloud iam list-testable-permissions <full-resource-name>

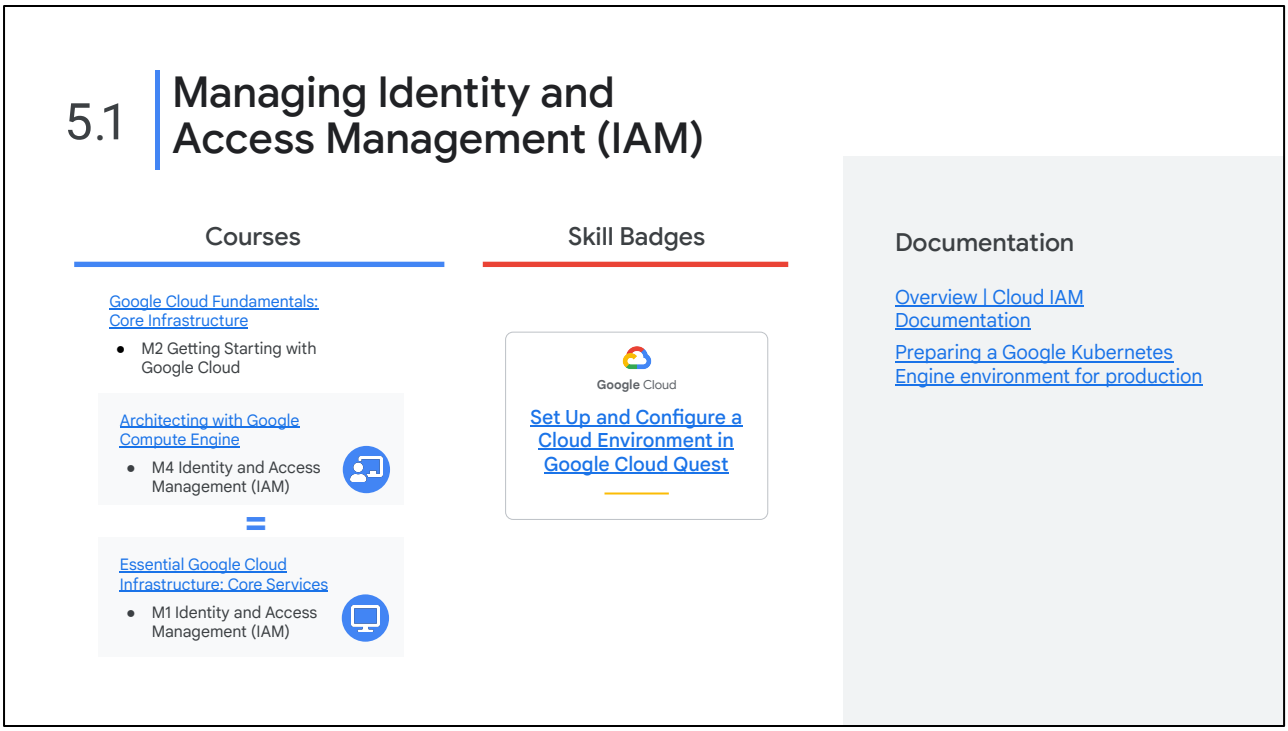
To make sure there isn't already another role that will fill your needs, you can also look at the permissions assigned to a specific role by looking at the role metadata. The role metadata includes the role ID and the permissions associated with that role.

Custom roles can be created at the project or organizational level.

You need to have the Iam.roles.create permission. You have to be the owner of the group or project, or have an organization administrator role or the IAM Role Administrator role.

You can create roles from individual permissions, or you can select and pick permissions from predefined roles.

To update an existing role, you run roles.get(), update the role locally, and then run roles.patch().



Let's take a moment to consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic questions we just reviewed are covered in these modules and in this documentation. You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these.

https://cloud.google.com/iam/docs/overview
https://cloud.google.com/architecture/prep-kubernetes-engine-for-prod#managing_identity_and_access

5.2 Managing service accounts

Tasks 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

Google Cloud

Cymbal Superstore's three applications targeted for migration all have frontend and backend resources required to implement their final solutions. We've discussed what resources are required to support the backend stores, to include Cloud Spanner, Bigtable, and Cloud SQL.

There is another security concern we haven't talked about in detail. How do we enable the machine-to-machine or server-to-server access requirements for the application to talk to those backends?
Let's look at the supply chain management application for an example. The data for it is stored in Cloud SQL. The application needs permissions to write data to the Cloud SQL service.
How do you get the VMs implemented as part of the supply chain management app the permissions required to connect to the Cloud SQL database in a secure manner?

The solution to machine-to-machine access is a service account. As an Associate Cloud Engineer, you need to know how to create a service account and assign roles to it. You also need to know how to list a service account's permissions, and allow other users to inherit its permissions - also called impersonation. Finally, because they don't sign in interactively like a user does, service accounts authenticate via keys. Managing those keys and providing temporary credentials through code are important things for you to know as you help secure your cloud solutions.

These diagnostic questions addressed managing service accounts:
Question 4: Differentiate between Google accounts and service accounts in IAM.

Question 5: Identify the section of the Google API that specifies an IAM scope.

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

Google Cloud

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

A. To directly access user data
Feedback: Incorrect. Service accounts should not be used to access user data without consent.

B. For development environments
Feedback: Incorrect. Service accounts should not be used for development environments. Use the application default credentials.

C. For interactive analysis
Feedback: Incorrect. Service accounts should be used for unattended work that does not require user interaction.

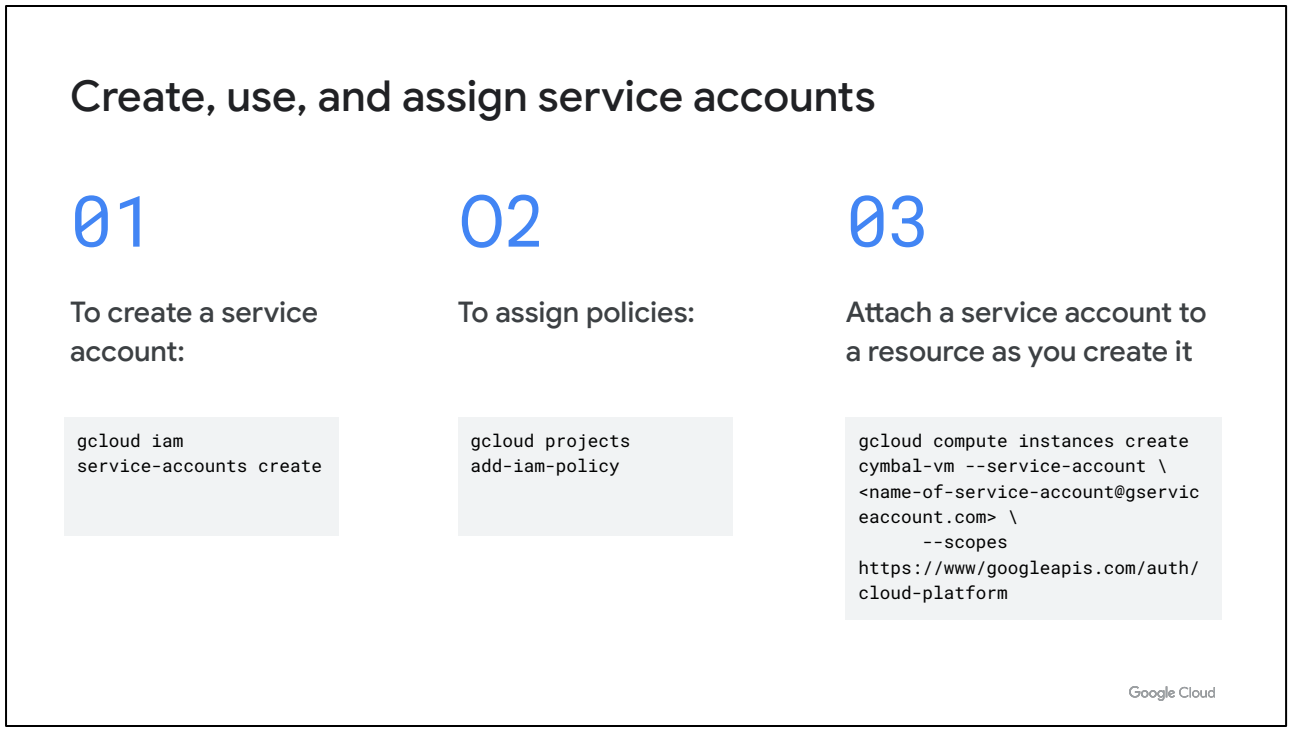
*D. For individual GKE pods
Feedback: Correct! When configuring access for GKE, you set up dedicated service accounts for each pod. You then use workload identity to map them to dedicated Kubernetes service accounts.

Where to look:
https://cloud.google.com/docs/authentication/production#automatically

Content mapping:

- Instructor-led Training/OnDemand
  - Google Cloud Fundamentals: Core Infrastructure
    - M2 Getting Started with Google Cloud
  - Architecting with Google Compute Engine
    - M4 IAM

Summary:
Explanation/summary on the following slide.



Creating a service account

https://cloud.google.com/iam/docs/creating-managing-service-accounts#creating_a_service_account

To create a service account you use the “gcloud iam service-accounts create” command.

Using service accounts with IAM policies

To add a policy to a service account run the “gcloud projects add-iam-policy-binding” command.
The “--member” argument should be a string starting with “serviceAccount:” and containing your service account id with an email address suffix of “@project_id.iam.gserviceaccount.com.” A “--role” argument contains the role you want to assign to the service account.

Assigning service accounts to resources

Resources in Google Cloud can be assigned a service account that acts as the resource’s default identity. This process is known as attaching a service account to a resource. The resource, or apps running on the resource, impersonate the attached service account to access Google Cloud APIs.

https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances#using

Multiple virtual machine instances can use the same service account, but a virtual machine can only have one service account identity. Service account changes will affect all virtual machine instances using the service account. You can allow access via a cloud-platform scope that allows access to most cloud api's and then grant the service account the relevant IAM roles.

In gcloud you identify the service account you want to use by using the "--service-account" argument.

https://developers.google.com/identity/protocols/oauth2/service-account#python

Two types of keys are available for authentication of a service account: user managed keys and Google managed keys. You create and manage user managed keys yourself. Google only stores the public key.
With Google managed keys Google stores both the public and private portion of the keys. Google has APIs you can use to sign requests with the private key.

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

Google Cloud

Question:
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
Feedback: Incorrect. API keys are used to access publicly available data.

B. OAuth 2.0 client
Feedback: Incorrect. OAuth 2.0 clients provide access to an application for private data on behalf of end users.

C. Environment provided service account
Feedback: Incorrect. Environment-provided service accounts are for applications running on resources inside Google Cloud.

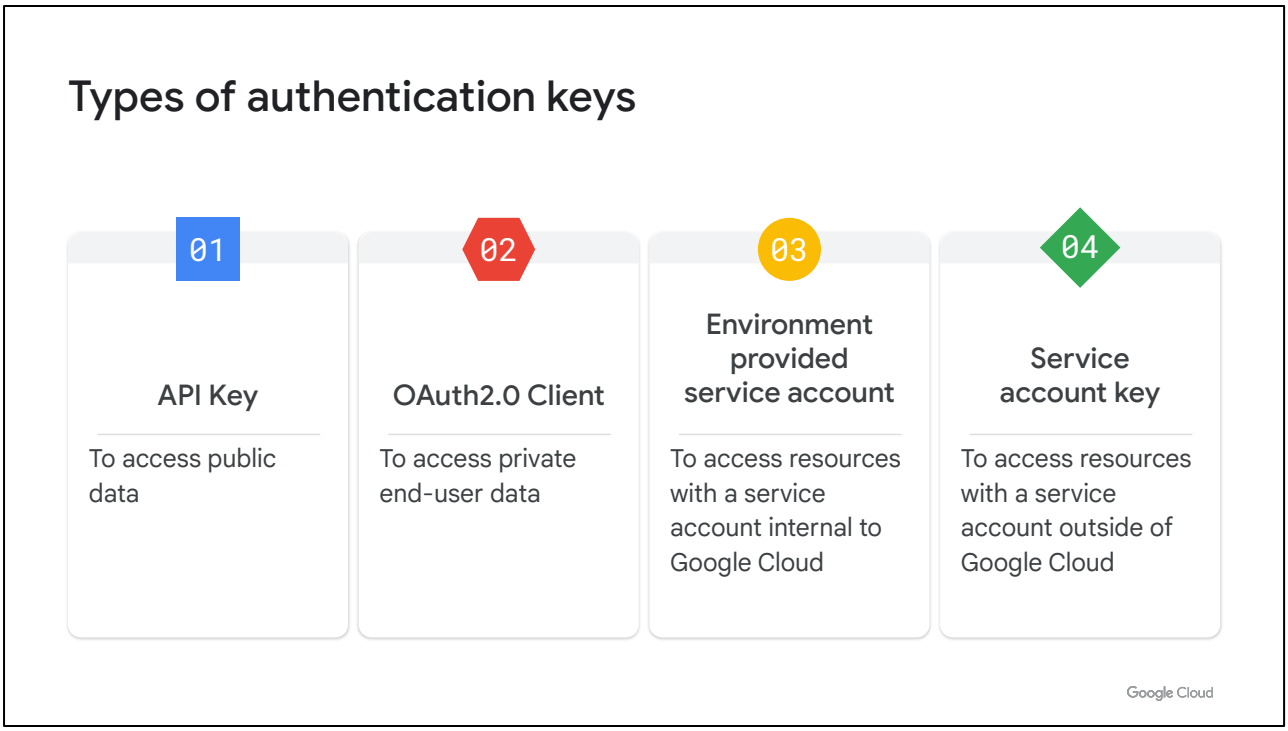
*D. Service account key
Feedback: Correct! Service account keys are used for accessing private data such as your Pub/Sub truck information from an external environment such as a mobile app running on a phone.

Where to look:
https://cloud.google.com/docs/authentication/

Content mapping:

- Instructor-led Training/OnDemand
  - Architecting with Google Compute Engine
    - M4 IAM

Summary:
Explanation/summary on the following slide.



Application credentials are based on what the application needs to access and where it needs to run from.

- If you are accessing public data, the recommendation is to use an API key.
- If you are accessing private data on behalf of an end user, you should you use the API's OAuth2.0 client.
- If you are accessing private data on behalf of a service account attached to resources inside a Google Cloud environment, you should use an environment provided service account.
- If you are accessing private data on behalf of a service account running outside of Google Cloud, you should create and use a service account key.

5.2 Managing service accounts

Courses

Google Cloud Fundamentals: Core Infrastructure
- M2 Getting Starting with Google 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

Let's take a moment to consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic questions we just reviewed are covered in these modules and in this documentation. You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these.

https://cloud.google.com/docs/authentication/production#automatically
https://cloud.google.com/docs/authentication/

5.3 Viewing audit logs

Google Cloud

Google Cloud's operations suite provides audit logs so you know who did what to whom and when. This is another link in the security armor you provide when implementing a Google Cloud solution. Who accessed your ecommerce app, and when? Say you add an instance to your Cloud Spanner cluster to support users in a new geographic area. Your Admin Activity log will record when that new instance was created. If you need to list your instances, a data access admin_read entry will be created. When a user creates a shopping cart and accesses it on their mobile device at a later time, a data_read log entry will be posted for a read transaction in the data access log. Keeping track of these important actions is an important step in an overarching security strategy.

Viewing audit logs were covered in the following questions:
Question 6: Contrast the types of audit logging.
Question 7: Outline where cloud audit logs can be accessed

5.3 Diagnostic Question 06 Discussion

Which Cloud Audit log is disabled by default with a few exceptions?

A. Admin Activity audit logs
B. Data Access audit logs
C. System Event audit logs
D. Policy Denied audit logs

Google Cloud

Question:
Which Cloud Audit log is disabled by default with a few exceptions?

A. Admin Activity audit logs
Feedback: Incorrect. Admin Activity audit logs are always written and you cannot disable them.

*B. Data Access audit logs
Feedback: Correct! Data Access audit logs are disabled by default except for BigQuery.

C. System Event audit logs
Feedback: Incorrect. System Event audit logs are always written.

D. Policy Denied audit logs
Feedback: Incorrect. Policy Denied audit logs are always written and cannot be disabled.

Where to look:
https://cloud.google.com/logging/docs/audit

Content mapping:

- Instructor-led Training/OnDemand
  - Google Cloud Fundamentals: Core Infrastructure
    - M7 Deployment and Monitoring
  - Architecting with Google Compute Engine
    - M7 Resource Monitoring

There are four types of audit logs available for each Cloud project, folder, and organization:

- Admin Activity audit logs contain information about API calls that create or change resource metadata. For example, changing access permissions or creating VM instances are both recorded by Admin Activity audit logs. Admin Activity audit logs are always written. You cannot disable them.
- Data Access audit log entries are written when the configuration or metadata of resources are read. Calls to create, modify or read resource data are also written to Data Access audit logs. They are disabled by default.
- System Event audit logs record actions that modify the configuration of resources. They are always written.
- Policy Denied audit log entries are created when a Google Cloud service denies access to a user or service account without the correct access in their security policy. They are generated by default and you can’t disable them.

5.3 Diagnostic Question 07 Discussion

You are configuring audit logging for Cloud Storage. You want to know when objects are added to a bucket.

Which type of audit log entry should you monitor?

A. Admin Activity log entries
B. ADMIN_READ log entries
C. DATA_READ log entries
D. DATA_WRITE log entries

Google Cloud

Question:
You are configuring audit logging for Cloud Storage. You want to know when objects are added to a bucket. Which type of audit log entry should you monitor?

A. Admin Activity log entries
Feedback: Incorrect. Admin Activity logs record when buckets are created and deleted.

B. ADMIN_READ log entries
Feedback: Incorrect. ADMIN_READ log entries are created when buckets are listed and bucket metadata is accessed.

C. DATA_READ log entries
Feedback: Incorrect. DATA_READ log entries contain operations such as listing and getting object data.

*D. DATA_WRITE log entries
Feedback: Correct! DATA_WRITE log entries include information about when objects are created or deleted.

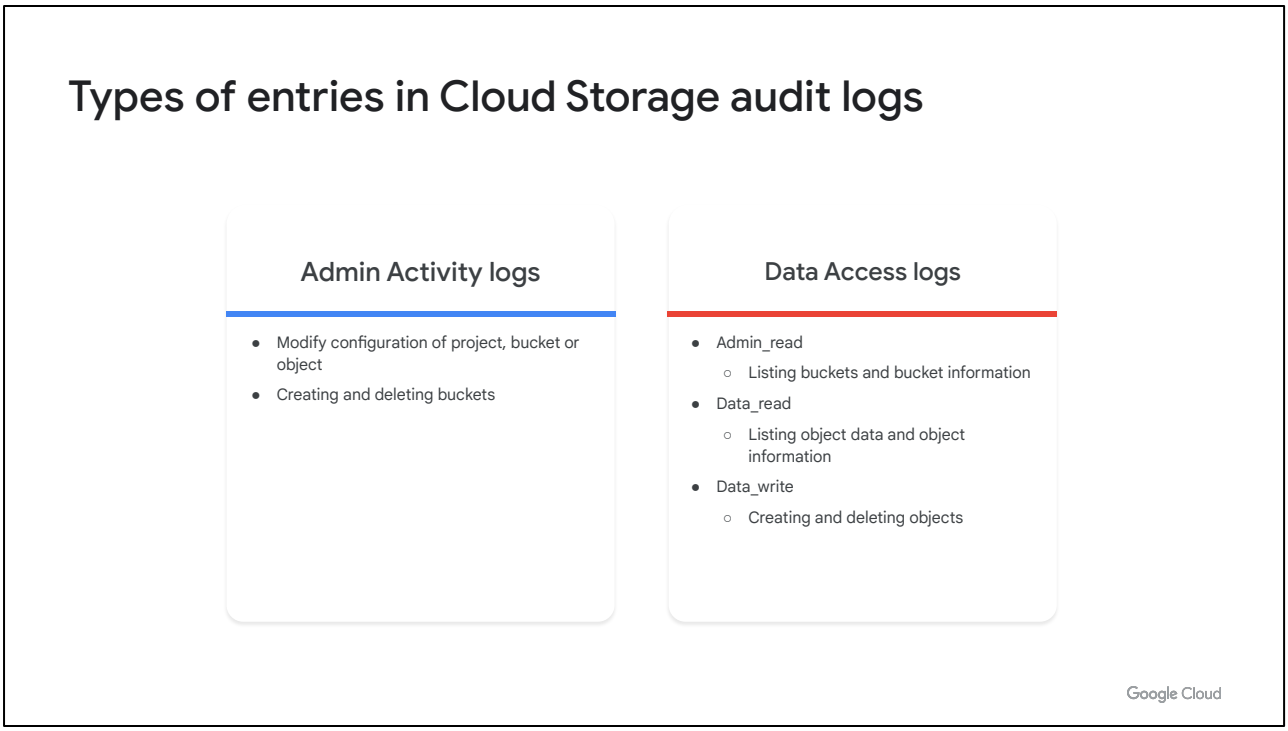
Where to look:

https://cloud.google.com/storage/docs/audit-logging

Content mapping:

- Instructor-led Training/OnDemand
  - Google Cloud Fundamentals: Core Infrastructure
    - M7 Deployment and Monitoring
  - Architecting with Google Compute Engine
    - M7 Resource Monitoring

Summary:
Explanation/summary on the following slide.



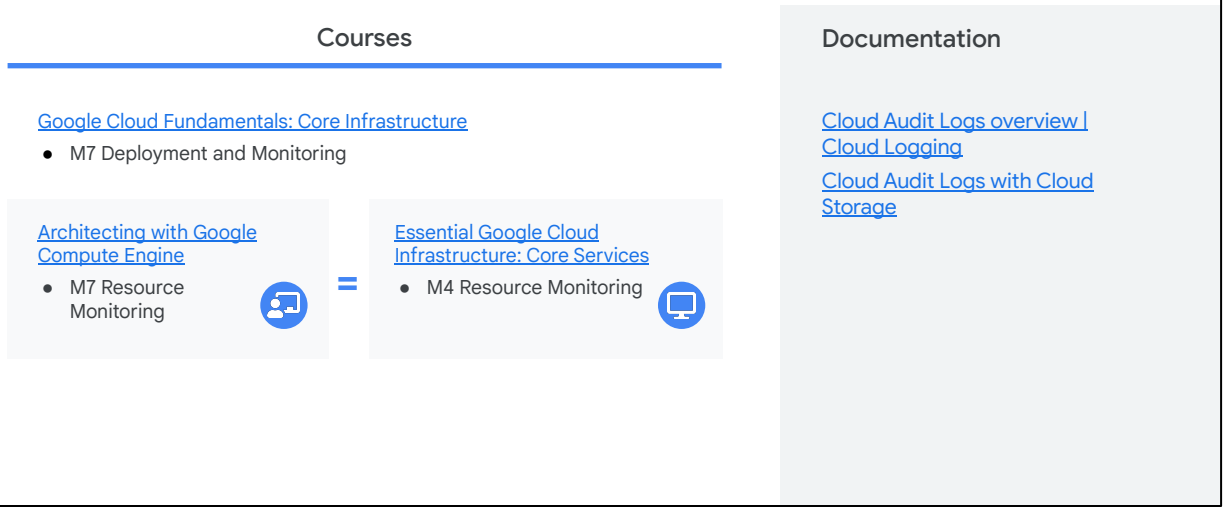
Cloud Storage audit logs include Admin Activity logs and Data Access logs.

Admin Activity logs include entries that modify the configuration of a project, bucket or object. They also include operations such as creating and deleting buckets.

Data Access logs include three different types of entries: ADMIN_READ, DATA_READ, AND DATA_WRITE.

- ADMIN_READ entries include operations such as listing buckets and getting bucket metadata.
- DATA_READ entries include operations such as listing and getting object data.
- DATA_WRITE entries include operations such as creating and deleting objects.

5.3 Viewing audit logs



Let's take a moment to consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic questions we just reviewed are covered in these modules and in this documentation. You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these.

https://cloud.google.com/logging/docs/audit
https://cloud.google.com/storage/docs/audit-logging