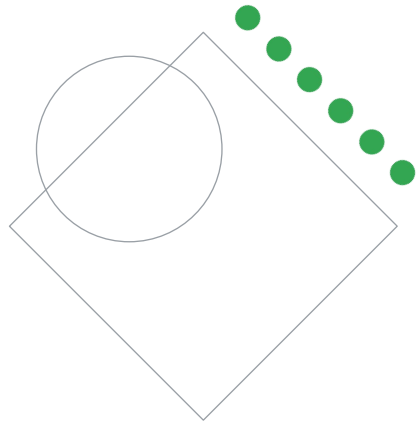# Preparing for your Professional Cloud Security Engineer Journey

Module 1: Configuring Access Within a Cloud Solution Environment

Welcome to Module 1: Configuring Access Within a Cloud Solution Environment.
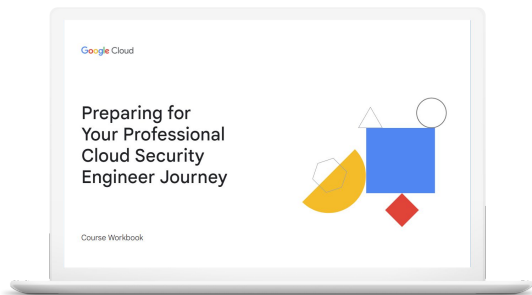
Review and study planning

Now let's review how to use these diagnostic questions to help you identify what to include in your study plan.

Your study plan:

Configuring access within a cloud solution environment

Preparing for Your Professional Cloud Security Engineer Journey

Course Workbook

Google Cloud

1.1	Managing Cloud Identity
1.2	Managing service accounts
1.3	Managing authentication
1.4	Managing and implementing authorization controls
1.5	Defining resource hierarchy

Google Cloud

We'll approach this review by looking at the key areas of this exam section and the questions you just answered about each one. We'll talk about where you can find out more about each area in the learning path for this certification and/or where to find the information in Google Cloud documentation.

As we go through each one, take notes on the specific courses (and modules!), quests, and documentation pages you'll want to emphasize in your study plan.

1.1 | Managing Cloud Identity

Considerations include:
- Configuring Google Cloud Directory Sync and third-party connectors
- Managing a super administrator account
- Automating the user lifecycle management process
- Administering user accounts and groups programmatically

As Professional Cloud Security Engineer, you should be able to design and implement and identity and access management scheme for the Google Cloud resources of an organization. This includes managing users, groups, and group membership, optionally synchronizing and federating to external identity management systems and designing and leveraging an organizational hierarchy for policy and access control.

Question 1 tested your knowledge of the process used to sync external identities to Cloud Identity. Question 2 asked you to create dynamic groups in Cloud Identity.

| Diagnostic Question 01 Discussion

Cymbal Bank has acquired a non-banking financial company (NBFC). This NBFC uses Active Directory as their central directory on an on-premises Windows Server. You have been tasked with migrating all the NBFC users and employee information to Cloud Identity.

What should you do?

A. Run Microsoft System Center Configuration Manager (SCCM) on a Compute Engine instance. Leave the channel unencrypted because you are in a secure Google Cloud environment. Deploy Google Cloud Directory Sync on the Compute Engine instance. Connect to the on-premises Windows Server environment from the instance, and migrate users to Cloud Identity.

B. Run Configuration Manager on a Compute Engine instance. Copy the resulting configuration file from this machine onto a new Compute Engine instance to keep the production environment separate from the staging environment. Leave the channel unencrypted because you are in a secure Google Cloud environment. Deploy Google Cloud Directory Sync on this new instance. Connect to the on-premises Windows Server environment from the new instance, and migrate users to Cloud Identity.

C. Use Cloud VPN to connect the on-premises network to your Google Cloud environment. Select an on-premises domain-joined Windows Server. On the domain-joined Windows Server, run Configuration Manager and Google Cloud Directory Sync. Use Cloud VPN's encrypted channel to transfer users from the on-premises Active Directory to Cloud Identity.

D. Select an on-premises domain-joined Windows Server. Run Configuration Manager on the domain-joined Windows Server, and copy the resulting configuration file to a Compute Engine instance. Run Google Cloud Directory Sync on the Compute Engine instance over the internet, and use Cloud VPN to sync users from the on-premises Active Directory to Cloud Identity.

Google Cloud

Feedback:
A. Incorrect. Active Directory uses unencrypted LDAP. When you use a Compute Engine instance, the communication channel must be encrypted even if it is a trusted Google Cloud environment. Use either LDAPs or Cloud VPN.

B. Incorrect. Active Directory uses unencrypted LDAP. When you use a Compute Engine instance, the communication channel must be encrypted. Use either LDAPs or Cloud VPN.

C. Correct! If you are in an on-premises environment, you can access Active Directory using LDAP. Google Cloud Directory Sync to Cloud Identity communication will be over an HTTPs channel using Cloud VPN.

D. Incorrect. Copying configuration files will not give desired results. Google Cloud Directory Sync on a Compute Engine instance would also need this instance to be a part of an on-premises Windows Active Directory server farm.

Where to look:
- https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-synchronizing-user-accounts
- https://support.google.com/a/answer/6126578?hl=en#:~:text=Configuration%20Manager%20is%20a%20step,test%2C%20and%20run%20a%20synchronization

Content mapping:
- ● ILT course: **Security in Google Cloud**
  - ○ M2 Securing Access to Google Cloud

- ● On-demand course: **Managing Security in Google Cloud**
  - ○ M2 Securing Access to Google Cloud

Summary:
Google Cloud Directory Sync deployment requires a secure, isolated environment. Because Active Directory uses LDAP, which is unencrypted, the safest choice is to deploy on-premises. When running Google Cloud Directory Sync remotely or on Google Cloud, ensure that the communication channel is encrypted. You can do this by using Secure LDAP or Cloud VPN. Although this might add a layer of complexity to the process, it ensures that your data transfers are secure. If the source servers support GUI, you can run Configuration Manager to ease the process.

Diagnostic Question 02 Discussion

Cymbal Bank has certain default permissions and access for their analyst, finance, and teller teams. These teams are organized into groups that have a set of role-based IAM permissions assigned to them. After a recent acquisition of a small bank, you find that the small bank directly assigns permissions to their employees in IAM. You have been tasked with applying Cymbal Bank's organizational structure to the small bank. Employees will need access to Google Cloud services.

What should you do?

A. Leave all user permissions as-is in the small bank's IAM. Use the Directory API in the Google Workspace Admin SDK to create Google Groups. Use a Python script to allocate users to the Google Groups.

B. Reset all user permissions in the small bank's IAM. Use Cloud Identity to create dynamic groups for each of the bank's teams. Use the dynamic groups' metadata field for team type to allocate users to their appropriate group with a Python script.

C. Reset all user permissions in the small bank's IAM. Use Cloud Identity to create the required Google Groups. Upgrade the Google Groups to Security Groups. Use a Python script to allocate users to the groups.

D. Reset all user permissions in the small bank's IAM. Use the Directory API in the Google Workspace Admin SDK to create Google Groups. Use a Python script to allocate users to the groups.

Google Cloud

Feedback:
A. Incorrect. You need to reset permissions in IAM and create Dynamic Groups. Using Google Groups from the Workspace Admin SDK Directory APIs allows access to Google Drive and Docs, but not to Google Cloud resources. Dynamic groups allow you to create and automatically manage users based on identity attributes.

B. Correct! Use Dynamic Groups to create groups based on Identity attributes, such as department, and place the users in a flat hierarchy. Dynamic group metadata helps build the structure to identify the users.

C. Incorrect. Upgrading to Security Groups helps create a protective access layer, but does not fulfill your criterion to apply Cymbal Bank's structure.

D. Incorrect. Using Google Groups from the Workspace Admin SDK Directory APIs allows access to Google Drive and Docs, but not to Google Cloud resources.

Where to look:
- https://support.google.com/a/answer/10286834
- https://cloud.google.com/identity/docs/how-to/create-dynamic-groups
- https://support.google.com/a/answer/10427204

Content mapping:
- ILT course: **Security in Google Cloud**
  - M2 Securing Access to Google Cloud

- On-demand course: **Managing Security in Google Cloud**
  - M2 Securing Access to Google Cloud

Summary:
Cloud Identity supports creating groups and then placing users inside those groups. Groups help with managing permissions, access controls, and organizational policies. In Dynamic Groups, users are automatically managed and added based on Identity attributes, such as department.

1.1 Managing Cloud Identity

Courses

Security in Google Cloud
M2 Securing Access to Google Cloud

Managing Security in Google Cloud
M2 Securing Access to Google Cloud

Documentation

Active Directory user account provisioning | Identity and access management | Google Cloud

What is Configuration Manager? - Google Workspace Admin Help

Manage membership automatically with dynamic groups - Google Workspace Admin Help

Creating and updating a dynamic group | Cloud Identity

Create and manage groups using APIs - Google Workspace Admin Help

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. Reviewing the documentation is highly recommended. 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/architecture/identity/federating-gcp-with-active-directory-synchronizing-user-accounts
- https://support.google.com/a/answer/6126578?hl=en#:~:text=Configuration%20Manager%20is%20a%20step,test%2C%20and%20run%20a%20synchronization
- https://support.google.com/a/answer/10286834
- https://cloud.google.com/identity/docs/how-to/create-dynamic-groups
- https://support.google.com/a/answer/10427204

Managing service accounts

Considerations include:
● Protecting and auditing service accounts and keys
● Automating the rotation of user-managed service account keys
● Identifying scenarios requiring service accounts
● Creating, disabling, authorizing, and securing service accounts
● Managing and creating short-lived credentials
● Configuring workload identity federation
● Securing default service accounts
● Managing service account impersonation

Google Cloud

A Professional Cloud Security Engineer should be familiar with Google Cloud service accounts, the key details of their usage and maintenance, and best practices for using them securely.

Question 3 tested your knowledge of applying Google-recommended practices to create and manage service accounts. Question 4 asked you to define service account usage policy based on organizational requirements.

Diagnostic Question 03 Discussion

Cymbal Bank leverages Google Cloud storage services, an on-premises Apache Spark Cluster, and a web application hosted on a third-party cloud. The Spark cluster and web application require limited access to Cloud Storage buckets and a Cloud SQL instance for only a few hours per day. You have been tasked with sharing credentials while minimizing the risk that the credentials will be compromised.

What should you do?

A. Create a service account with appropriate permissions. Authenticate the Spark Cluster and the web application as direct requests and share the service account key.

B. Create a service account with appropriate permissions. Have the Spark Cluster and the web application authenticate as delegated requests, and share the short-lived service account credential as a JWT.

C. Create a service account with appropriate permissions. Authenticate the Spark Cluster and the web application as a delegated request, and share the service account key.

D. Create a service account with appropriate permissions. Have the Spark Cluster and the web application authenticate as a direct request, and share the short-lived service account credentials as XML tokens.

Google Cloud

Feedback:
A. Incorrect. Sharing a service account key creates unnecessary exposure, which increases the possibility of spoofing and unauthorized impersonation. This also violates the principle of least privilege.

B. Correct! Delegated requests allow a service account to authenticate into a chain of services. Using short-lived service account credentials provides limited access to trusted services.

C. Incorrect. Although a delegate request is the correct method, sharing a service account key for long durations increases the risk exposure to unauthorized parties.

D. Incorrect. Although short-lived service account credentials are the most secure option, delegated requests instead of direct requests should be used by applications.

Where to look:
https://cloud.google.com/iam/docs/create-short-lived-credentials-direct

Content mapping:
- ILT course: **Security in Google Cloud**
  - M3 Identity and Access Management (IAM)
  - M5 Securing Compute Engine: Techniques and Best Practices
  - M8 Securing Google Kubernetes Engine: Techniques and Best Practices

- On-demand course: **Managing Security in Google Cloud**
  - M3 Identity and Access Management (IAM)

- On-demand course: **Security Best Practices in Google Cloud**
  - M1 Securing Compute Engine: Techniques and Best Practices
  - M4 Securing Google Kubernetes Engine: Techniques and Best Practices

- Quest: Ensure Access & Identity in Google Cloud

Summary:
Short-lived credentials help a service account share credentials to trusted requests without compromising the access key and similar credentials. Credential types could be self-signed JWT or blobs, OAuth 2.0 access tokens, or OpenID Connect ID Tokens. Delegated requests help a service account authenticate to a chain of services, with limited and separate permissions for each service.

Diagnostic Question 04 Discussion

Cymbal Bank recently discovered service account key misuse in one of the teams during a security audit. As a precaution, going forward you do not want any team in your organization to generate new external service account keys. You also want to restrict every new service account's usage to its associated Project.

What should you do?

A. Navigate to Organizational policies in the Google Cloud Console. Select your organization. Select `iam.disableServiceAccountKeyCreation`. Customize the **applied to** property, and set **Enforcemen**t to 'On'. Click Save. Repeat the process for `iam.disableCrossProjectServiceAccountUsage`.

B. Run the `gcloud resource-manager org-policies enable-enforce` command with the constraints iam.disableServiceAccountKeyCreation, and `iam.disableCrossProjectServiceAccountUsage` and the Project IDs you want the constraints to apply to.

C. Navigate to Organizational policies in the Google Cloud Console. Select your organization. Select `iam.disableServiceAccountKeyCreation`. Under Policy Enforcement, select **Merge with parent**. Click **Save**. Repeat the process for `iam.disableCrossProjectServiceAccountLienRemoval`.

D. Run the `gcloud resource-manager org-policies` allow command with the boolean constraints iam.disableServiceAccountKeyCreation and `iam.disableCrossProjectServiceAccountUsage` with Organization ID.

Google Cloud

Feedback:

A. Correct! Boolean constraints help you limit service account usage. `iam.disableServiceAccountKeyCreation` will restrict the creation of new external service account keys. `iam.disableCrossProjectServiceAccountUsage` will prevent service accounts from being attached to resources in other projects.

B. Incorrect. You use the enable-enforce command with individual boolean constraints. You would also pass the organization ID, not the Project ID, to enforce the constraint.

C. Incorrect. Policy Enforcement and Merge with parent are used to merge list constraints to parent policies. For boolean constraints, first select the constraint, and then under **Applies to**, click **Customize**. Set **Enforcement** to **On**.

D. Incorrect. The command `org-policies allow` is used to consume list constraints, not boolean constraints. Run the command to select boolean constraints individually with the Organization ID.

Where to look:
https://cloud.google.com/resource-manager/docs/organization-policy/restricting-service-accounts

Content mapping:

- ILT course: **Security in Google Cloud**
  - M3 Identity and Access Management (IAM)
  - M5 Securing Compute Engine: Techniques and Best Practices
  - M8 Securing Google Kubernetes Engine: Techniques and Best Practices

- On-demand course: **Managing Security in Google Cloud**
  - M3 Identity and Access Management (IAM)

- On-demand course: **Security Best Practices in Google Cloud**
  - M1 Securing Compute Engine: Techniques and Best Practices
  - M4 Securing Google Kubernetes Engine: Techniques and Best Practices

- Quest: Ensure Access & Identity in Google Cloud

Summary:
Service account usage policies can expose or limit the actions that service accounts can take. At an organization level, it is important to limit the service account activities because service accounts are prone to impersonation. Sharing between projects and exposing their keys for a long time can compromise the key.

1.2 | Managing service accounts

Courses

Security in Google Cloud
- M3 Identity and Access Management (IAM)
- M5 Securing Compute Engine: Techniques and Best Practices
- M8 Securing Kubernetes: Techniques and Best Practices

Managing Security in Google Cloud
- M3 Identity and Access Management (IAM)

Security Best Practices in Google Cloud
- M1 Securing Compute Engine: Techniques and Best Practices
- M4 Securing Google Kubernetes Engine: Techniques and Best Practices

Skill Badges

Google Cloud

Ensure Access and Identity in Google Cloud Quest
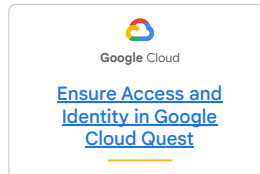
Documentation

Creating short-lived service account credentials | IAM Documentation

Restricting service account usage | Resource Manager Documentation | Google Cloud

---

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. Reviewing the documentation is highly recommended. 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/creating-short-lived-service-account-credentials#before_you_begin
- https://cloud.google.com/resource-manager/docs/organization-policy/restricting-service-accounts

1.3 | Managing authentication

Considerations include:

- Creating a password and session management policy for user accounts
- Setting up Security Assertion Markup Language (SAML) and OAuth
- Configuring and enforcing two-factor authentication

As a Professional Cloud Security Engineer, you should be able to define the authentication process for an organization based on requirements. You should be familiar with federated identity authentication and single-sign on with SAML and the benefits and details of configuration for enforcing two-factor authentication.

Question 5 tested your ability to enable SSO for Google Cloud using SAML configuration. Question 6 tested your knowledge of the steps to create custom IAM roles.

Diagnostic Question 05 Discussion

Cymbal Bank publishes its APIs through Apigee. Cymbal Bank has recently acquired ABC Corp, which uses a third-party identity provider. You have been tasked with connecting ABC Corp's identity provider to Apigee for single sign-on (SSO). You need to set up SSO so that Google is the service provider. You also want to monitor and log high-risk activities. Which two choices would you select to enable SSO?

Which two choices would you select to enable SSO?

A. Use openssl to generate public and private keys. Store the public key in an X.509 certificate, and encrypt using RSA or DSA for SAML. Sign in to the Google Admin console, and under **Security**, upload the certificate.

B. Use openssl to generate a private key. Store the private key in an X.509 certificate, and encrypt using AES or DES for SAML. Sign in to the Google Workspace Admin Console and upload the certificate.

C. Use openssl to generate public and private keys. Store the private key in an X.509 certificate, and encrypt using AES or DES for SAML. Sign in to the Google Admin console, and under Security, upload the certificate.

D. Review Network mapping results, and assign SSO profiles to required users.

E. Review Network mapping results, and assign SAML profiles to required users.

Google Cloud

Feedback:

A. Correct! The first step is to generate a set of public and private keys. The public key is then stored in an X.509 certificate encrypted with RSA or DSA. Navigate to the Google Admin console to upload the certificate. The generated private key will be used to sign the SAML messages and responses.

B. Incorrect. AES and DES are symmetric encryptions and generate only private keys. You need an asymmetric encryption to generate two keys: public and private. To upload the certificate, you need to use the Google Admin console, not the Google Workspace Admin Console.

C. Incorrect. AES and DES are symmetric encryptions and generate only private keys. You need an asymmetric encryption to generate two keys: public and private. The public key will be stored in an X.509 certificate. The private key will be used to sign the SAML messages and responses. However, using the Google Admin console to upload the certificate is the right choice.

D. Correct! Network maps and masks control the allocated IP address ranges and redirections.

E. Incorrect. An SSO profile must be assigned to the selected users. SAML profiles are assertions and policies to enable SSO profiles.

Where to look:

- https://cloud.google.com/apigee/docs/api-platform/system-administration/saml-overview
- https://support.google.com/a/answer/60224
- https://support.google.com/a/answer/10723804
- https://support.google.com/a/answer/6369487

Content mapping:
- ILT course: **Security in Google Cloud**
  - M2 Securing Access to Google Cloud

- On-demand course: **Managing Security in Google Cloud**
  - M2 Securing Access to Google Cloud

Summary:
SAML allows third-party identity services to enable single sign-on to Google platforms (Google being the service provider). Apigee uses SAML to enable single sign-on capabilities that are managed through the Google Admin console and require you to generate encrypted X.509 certificates storing public keys.

| Diagnostic Question 06 Discussion

You are an administrator for Cymbal Bank's Mobile Development Team. You want to control how long different users can access the Google Cloud console, the Cloud SDK, and any applications that require user authorization for Google Cloud scopes without having to reauthenticate. More specifically, you want users with elevated privileges (project owners and billing administrators) to reauthenticate more frequently than regular users at the organization level.

What should you do?

A. Open all Google Cloud projects that belong to Cymbal Bank's Mobile Development team. Find each project's Google Cloud session control setting, and configure a reauthentication policy that requires reauthentication. Choose the reauthentication frequency from the drop-down list.

B. In the Admin console, select Google Cloud session control and set a reauthentication policy that requires reauthentication. Choose the reauthentication frequency from the drop-down list.

C. Create a custom role for project owners and billing administrators at the organization level in the Google Cloud console. Add the `reauthenticationRequired` permission to this role. Assign this role to each project owner and billing administrator.

D. Create a custom role for project owners and billing administrators at the organization level in the Google Cloud console. Add the `reauthenticationRequired` permission to this role. Create a Google Group that contains all billing administrators and project owners. Apply the custom role to the group.

Google Cloud

Feedback:
A. Incorrect. Reauthentication policies are configured in the Admin console. The question also asks to configure this at the organization, not project level.

B. Correct! Session control settings are configured in the Admin console. These settings will be set at the organization level and will include all project owners and billing administrators in the organization.

C. Incorrect. The reauthenticationRequired permissions do not exist. Your set reauthentication policies are configured in the Admin console.

D. Incorrect. While applying roles to Google Groups is a best practice, the reauthenticationRequired permission does not exist. Your set reauthentication policies are configured in the Admin console.

Where to look:
- https://support.google.com/a/answer/9368756?hl=en

Summary:
As an administrator, you can control how long different users can access the Google Cloud console and Cloud SDK without having to reauthenticate. For example, you might want users with elevated privileges, like project owners, billing administrators, or others with administrator roles, to reauthenticate more frequently than regular users. If you set a session length, they're prompted to sign in again to start a new

session.

The session length setting applies to:
- The Google Cloud console
- The gcloud command-line tool (Cloud SDK)
- Any applications (including third-party applications, or your own applications) that require user authorization for Google Cloud scopes. To review the apps requiring Google Cloud scopes in the Apps access control UI, see Control which third-party & internal apps access Google Workspace data.

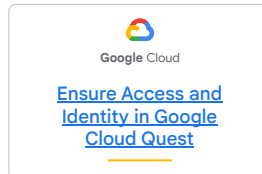# Managing authentication

Courses

Security in Google Cloud
- M2 Securing Access to Google Cloud
- M3 Identity and Access Management (IAM)

Managing Security in Google Cloud
- M2 Securing Access to Google Cloud
- M3 Identity and Access Management (IAM)

Skill Badges

Google Cloud

Ensure Access and Identity in Google Cloud Quest

Documentation

SAML overview | Apigee X | Google Cloud

Set up single sign-on for managed Google Accounts using third-party Identity providers - Google Workspace Admin Help

Assign SSO profile to organizational units or groups - Google Workspace Admin Help

Network Mapping results - Google Workspace Admin Help

Creating and managing custom roles | IAM Documentation

Understanding IAM custom roles | IAM Documentation | Google Cloud

Understanding roles | IAM Documentation

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. Reviewing the documentation is highly recommended. 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/apigee/docs/api-platform/system-administration/saml-overview
- https://support.google.com/a/answer/60224
- https://support.google.com/a/answer/10723804
- https://support.google.com/a/answer/6369487
- https://cloud.google.com/iam/docs/creating-custom-roles
- https://cloud.google.com/iam/docs/understanding-custom-roles
- https://cloud.google.com/iam/docs/understanding-roles#billing-roles

1.4 | Managing and implementing authorization controls

Considerations include:
● Managing privileged roles and separation of duties with Identity and Access Management (IAM) roles and permissions
● Granting permissions to different types of identities
● Managing IAM and access control list (ACL) permissions
● Managing Cloud Storage IAM and ACL permissions
● Designing identity roles at the organization, folder, project, and resource level
● Configuring Access Context Manager
● Applying Policy Intelligence for better permission management
● Managing permissions through groups

A Professional Cloud Security Engineer should be familiar with the authorization model of Google Cloud. You should be familiar with the Google Cloud concept of members (or identities or principals), roles, and permissions. You should be able to leverage basic, predefined, and custom roles bound to identities at various levels of the organization hierarchy to enforce least privilege access and separation of duties. Additionally, you should understand supplementary access control capabilities such as access levels in the Access Context Manager.

Question 7 tested your understanding of using roles at different levels of an organizational hierarchy. Question 8 asked you to select basic, predefined, or custom IAM roles for a specific scenario.

| **Diagnostic Question 07 Discussion**

Cymbal Bank's organizational hierarchy divides the Organization into departments. The Engineering Department has a 'product team' folder. This folder contains folders for each of the bank's products. Each product folder contains one Google Cloud Project, but more may be added. Each project contains an App Engine deployment.

Cymbal Bank has hired a new technical product manager and a new web developer. The technical product manager must be able to interact with and manage all services in projects that roll up to the Engineering Department folder. The web developer needs read-only access to App Engine configurations and settings for a specific product.

How should you provision the new employees' roles into your hierarchy following principles of least privilege?

A. Assign the Project Editor role in each individual project to the technical product manager. Assign the Project Editor role in each individual project to the web developer.

B. Assign the Project Owner role in each individual project to the technical product manager. Assign the App Engine Deployer role in each individual project to the web developer.

C. Assign the Project Editor role at the Engineering Department folder level to the technical product manager. Assign the App Engine Deployer role at the specific product's folder level to the web developer.

D. Assign the Project Editor role at the Engineering Department folder level to the technical product manager. Create a Custom Role in the product folder that the web developer needs access to. Add the appengine.versions.create and appengine.versions.delete permissions to that role, and assign it to the web developer.

Google Cloud

Feedback:
A. Incorrect. Binding the technical product manager on each project separately will provide the required access, but is not the most efficient approach. This also doesn't address the possibility of new folders (and new projects) that can be added in the future. Providing the web developer with Editor access on the required Project will allow them unnecessary access to other Google Cloud services.

B. Incorrect. Assigning Owner roles in all projects to the technical product manager will provide them with more access than necessary. The web developer should be assigned the predefined 'App Engine Deployer' role, but only for the appropriate folder.

C. Correct! Because the technical product manager must be able to work with services across all projects, you should provide permissions at the Department folder level. The web developer should only be able to administer App Engine deployments in their product folder.

D. Incorrect. Although the correct permissions are assigned to the technical product manager, the web developer is provided permissions that are overly permissive. Custom roles are also not required because the App Engine Deployer role gives the web developer all the required permissions.

Where to look:
- https://cloud.google.com/resource-manager/docs/access-control-proj

- https://cloud.google.com/resource-manager/docs/access-control-org
- https://cloud.google.com/resource-manager/docs/access-control-folders

Content mapping:
- ILT course: **Security in Google Cloud**
  - M3 Identity and Access Management (IAM)

- On-demand course: **Managing Security in Google Cloud**
  - M3 Identity and Access Management (IAM)

Summary:
Folders help create layers of hierarchy and access control between Organization and Projects. Use Folders to create an inheritance of roles and permissions. Provide access at the Project level when the target role needs to work with limited resources. Provide access at the Folder level when the target role needs to work with multiple roles, permissions, and projects.

Cymbal Bank's organizational hierarchy divides the Organization into departments. The Engineering Department has a 'product team' folder. This folder contains folders for each of the bank's products. One folder titled "analytics" contains a Google Cloud Project that contains an App Engine deployment and a Cloud SQL instance.

A team needs specific access to this project. The team lead needs full administrative access to App Engine and Cloud SQL. A developer must be able to configure and manage all aspects of App Engine deployments. There is also a code reviewer who may periodically review the deployed App Engine source code without making any changes.

What types of permissions would you provide to each of these users?

A. Create custom roles for all three user types at the "analytics" folder level. For the team lead, provide all appengine.* and cloudsql.* permissions. For the developer, provide appengine.applications.* and appengine.instances.* permissions. For the code reviewer, provide the appengine.instances.* permissions.

B. Assign the basic 'App Engine Admin' and 'Cloud SQL Admin" roles to the team lead. Assign the 'App Engine Admin' role to the developer. Assign the 'App Engine Code Viewer' role to the code reviewer. Assign all these permissions at the analytics project level.

C. Create custom roles for all three user types at the project level. For the team lead, provide all appengine.* and cloudsql.* permissions. For the developer, provide appengine.applications.* and appengine.instances.* permissions. For the code reviewer, provide the appengine.instances.* permissions.

D. Assign the basic 'Editor' role to the team lead. Create a custom role for the developer. Provide all appengine.* permissions to the developer. Provide the predefined 'App Engine Code Viewer' role to the code reviewer. Assign all these permissions at the "analytics" folder level.

Google Cloud

Feedback:
A. Incorrect. Custom roles are not required in this scenario. The team lead, developer, and code reviewer can all be assigned predefined roles to match their job functions. Permissions also need to be set at the project, not folder, level.

B. Correct! The team lead needs full access to the App Engine and Cloud SQL services. The developer needs to administer App Engine deployments. The 'App Engine Code Viewer' role allows the code reviewer to access deployed source code.

C. Incorrect. Although the permissions are set at the project level, there is no requirement for custom roles. Also, the developer would need more than appengine.applications.* and appengine.instances.* for full administrative access to the tool.

D. Incorrect. The basic 'Editor' role is too coarse-grained for the team lead. The Developer needs the predefined role of 'App Engine Admin'. You can assign the 'App Engine Code Viewer' for the code reviewer; a custom role is not required. Permissions also need to be set at the project, not folder, level.

Where to look:
- https://cloud.google.com/iam/docs/understanding-roles
- https://cloud.google.com/iam/docs/understanding-roles#app-engine-roles

Content mapping:

- ILT course: **Security in Google Cloud**
  - M3 Identity and Access Management (IAM)

- On-demand course: **Managing Security in Google Cloud**
  - M3 Identity and Access Management (IAM)

- Quest: Ensure Access & Identity in Google Cloud

Summary:
IAM roles are of 3 types: basic, predefined, and custom. Basic roles of 'Owner,' 'Editor,' and 'Viewer' provide a large set of broad permissions that existed before IAM. Most often, basic roles are not recommended because of the large number of permissions they contain. Predefined roles limit the permissions and access that a role has and are defined separately for each Google Cloud resource. Create custom roles when the predefined roles provide more permission than required.

1.4 | Managing and implementing authorization controls
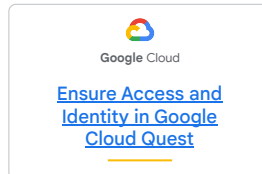
Courses

Security in Google Cloud
M3 Identity and Access Management (IAM)

Managing Security in Google Cloud
M3 Identity and Access Management (IAM)

Skill Badges

Google Cloud

Ensure Access and Identity in Google Cloud Quest

Documentation

Access control for projects with IAM | Resource Manager Documentation | Google Cloud

Access control for organizations with IAM | Resource Manager Documentation | Google Cloud

Access control for folders with IAM | Resource Manager Documentation | Google Cloud

Understanding roles | IAM Documentation

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. Reviewing the documentation is highly recommended. 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/resource-manager/docs/access-control-proj
- https://cloud.google.com/resource-manager/docs/access-control-org
- https://cloud.google.com/resource-manager/docs/access-control-folders
- https://cloud.google.com/iam/docs/understanding-roles
- https://cloud.google.com/iam/docs/understanding-roles#app-engine-roles

1.5 | Defining resource hierarchy

Considerations include:

- Creating and managing organizations
- Managing organization policies for organization folders, projects, and resources
- Using resource hierarchy for access control and permissions inheritance

Google Cloud

As a Professional Cloud Security Engineer, you are expected to help design and implement the organizational hierarchy. You will leverage this hierarchy to set trust and security boundaries via access control and organizational policy constraints bound at various levels of the hierarchy.

Question 9 asked you to create a resource hierarchy that aligns with a given organizational structure and access control requirements. Question 10 tested your knowledge of designing a hierarchy and policies to control access to Google Cloud resources.

1.5 | Diagnostic Question 09 Discussion

Cymbal Bank is divided into separate departments. Each department is divided into teams. Each team works on a distinct product that requires Google Cloud resources for development.

How would you design a Google Cloud organization hierarchy to best match Cymbal Bank's organization structure and needs?

A. Create an Organization node. Under the Organization node, create Department folders. Under each Department, create Product folders. Under each Product, create Teams folders. In the Teams folder, add Projects.

B. Create an Organization node. Under the Organization node, create Department folders. Under each Department, create Product folders. Add Projects to the Product folders.

C. Create an Organization node. Under the Organization node, create Department folders. Under each Department, create Teams folders. Add Projects to the Teams folders.

D. Create an Organization node. Under the Organization node, create Department folders. Under each Department, create a Teams folder. Under each Team, create Product folders. Add Projects to the Product folders.

Google Cloud

Feedback:
A. Incorrect. This hierarchy would place Teams under Product. Teams should be above products.

B. Incorrect. This hierarchy is missing the Teams layer.

C. Incorrect. Creating Projects directly inside Teams would make it difficult to distinguish teams and their roles in different Projects. Teams should have Product folders with Projects inside them.

D. Correct! Departments have teams, which work on products. This hierarchy best fits Cymbal Bank's organization structure.

Where to look:
https://cloud.google.com/resource-manager/docs/organization-policy/understanding-hierarchy

Content mapping:
- ● ILT course: **Security in Google Cloud**
  - ○ M3 Identity and Access Management (IAM)

- ● On-demand course: **Managing Security in Google Cloud**
  - ○ M3 Identity and Access Management (IAM)

Summary:
Organization hierarchy helps build an inheritance of policies and permissions. Although Projects can be placed directly in an Organization, creating layers of folders in between helps with managing different permissions for different access. You can also use folders to derive an inheritance of policies and permissions.

Diagnostic Question 10 Discussion

Cymbal Bank has a team of developers and administrators working on different sets of Google Cloud resources. The Bank's administrators should be able to access the serial ports on Compute Engine Instances and create service accounts. Developers should only be able to access serial ports.

How would you design the organization hierarchy to provide the required access?

A. Deny Serial Port Access and Service Account Creation at the Organization level. Create an 'admin' folder and set enforced: false for constraints/compute.disableSerialPortAccess. Create a new 'dev' folder inside the 'admin' folder, and set enforced: false for constraints/iam.disableServiceAccountCreation. Give developers access to the 'dev' folder, and administrators access to the 'admin' folder.

B. Deny Serial Port Access and Service Account Creation at the organization level. Create a 'dev' folder and set enforced: false for constraints/compute.disableSerialPortAccess. Create a new 'admin' folder inside the 'dev' folder, and set enforced: false for constraints/iam.disableServiceAccountCreation. Give developers access to the 'dev' folder, and administrators access to the 'admin' folder.

C. Deny Serial Port Access and Service Account Creation at the organization level. Create a 'dev' folder and set enforced: true for constraints/compute.disableSerialPortAccess and enforced: true for constraints/iam.disableServiceAccountCreation. Create a new 'admin' folder inside the 'dev' folder, and set enforced: false for constraints/iam.disableServiceAccountCreation. Give developers access to the 'dev' folder, and administrators access to the 'admin' folder.

D. Allow Serial Port Access and Service Account Creation at the organization level. Create a 'dev' folder and set enforced: true for constraints/iam.disableServiceAccountCreation. Create another 'admin' folder that inherits from the parent inside the organization node. Give developers access to the 'dev' folder, and administrators access to the 'admin' folder.

Google Cloud

Feedback:
A. Incorrect. Although this hierarchy allows serial port access in the 'admin' folder, it will not allow Admins to create service accounts. This hierarchy incorrectly lets Developers create service accounts.

B. Correct! These organizational constraints will prevent all users from accessing serial ports on Compute Engine instances and creating service accounts. You can override these constraints in a new folder by setting the common constraint for serial port access. Creating another folder inside a parent folder will allow you to inherit the constraint and will allow you to add additional constraints to create a service account. Admins and developers are added appropriately.

C. Incorrect. This hierarchy disables serial port access for developers and service account creation for admins. Hierarchies should be defined cleanly and with the fewest contradictions to avoid confusion.

D. Incorrect. Allowing Serial Port Access and Service Account Creation at the organization level defeats the problem statement, which specifies that only the bank's Administrators should be able to access the serial ports on Compute Engine Instances and create service accounts. You should 'DENY' the permissions at the organization level and enable them at the folder or Project level.

Where to look:
● https://cloud.google.com/resource-manager/docs/creating-managing-organizat

- [ion](#)
- https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations

Content mapping:
- ILT course: **Security in Google Cloud**
  - M3 Identity and Access Management (IAM)

- On-demand course: **Managing Security in Google Cloud**
  - M3 Identity and Access Management (IAM)

Summary:
Organization hierarchies allow you to place lists and boolean constraints. These constraints can be inherited into folders and subsequently into sub-folders and Projects.

1.5 | Defining resource hierarchy

Courses

Security in Google Cloud

M3 Identity and Access Management (IAM)

Managing Security in Google Cloud

M3 Identity and Access Management (IAM)

Documentation

Understanding hierarchy evaluation | Resource Manager Documentation | Google Cloud

Creating and managing organizations | Resource Manager Documentation | Google Cloud

Best practices for enterprise organizations | Documentation | Google Cloud

---

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. Reviewing the documentation is highly recommended. 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/resource-manager/docs/organization-policy/understanding-hierarchy
- https://cloud.google.com/resource-manager/docs/creating-managing-organization
- https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations