

Preparing for your Professional Cloud Security Engineer Journey

Module 1: Configuring Access Within a Cloud
Solution Environment

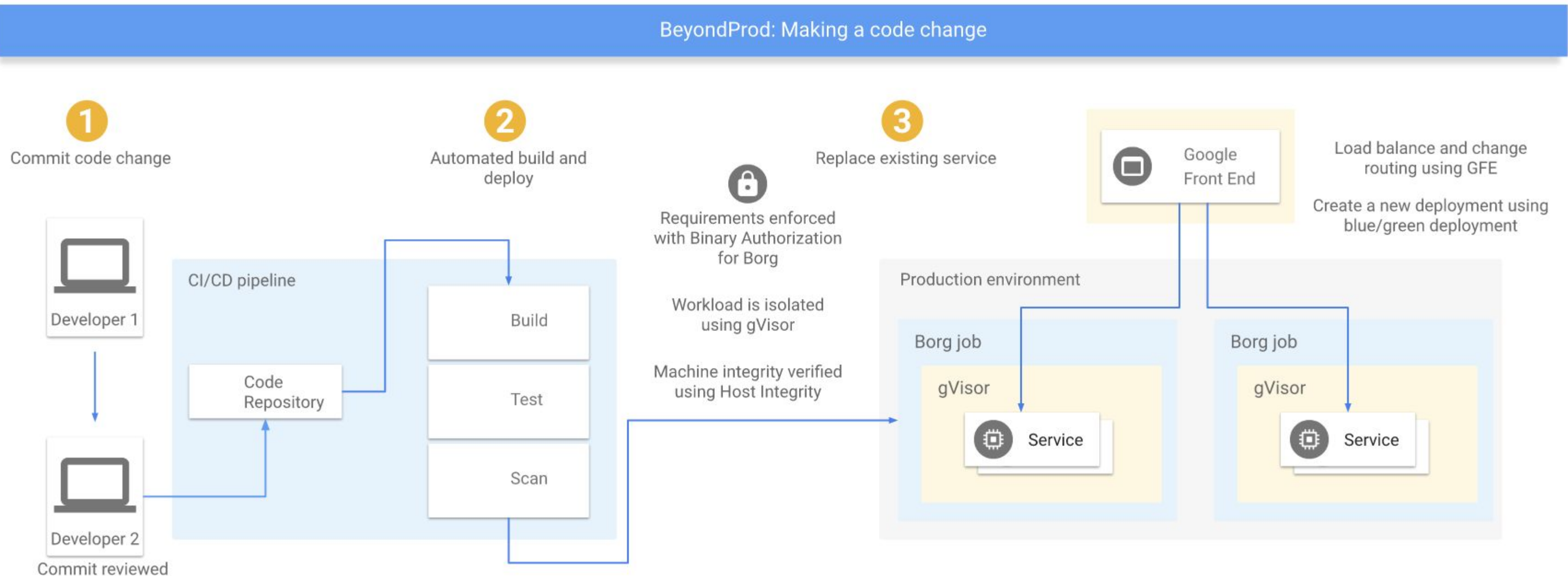


Module agenda

- 01 Planning Cymbal Bank's cloud identity and access management
- 02 Diagnostic questions
- 03 Review and study planning

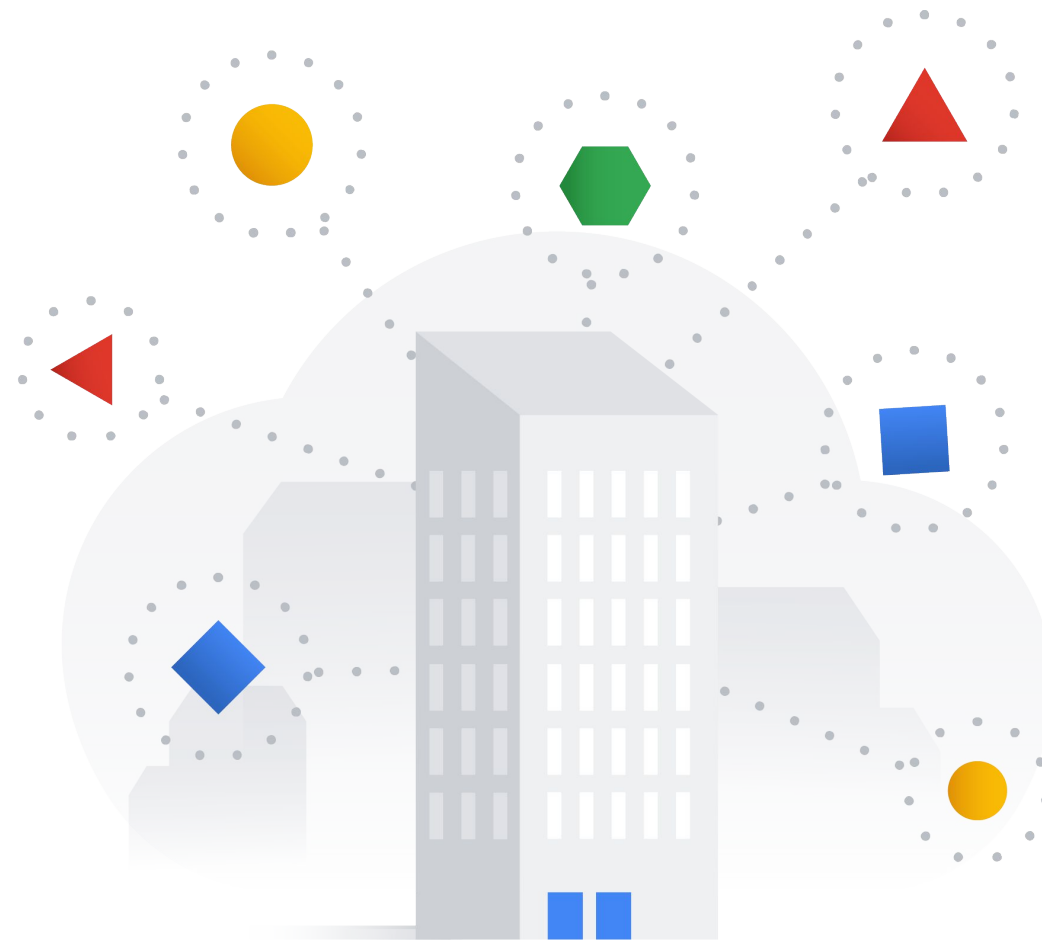


BeyondProd -> Google's approach to Zero Trust model



[BeyondProd whitepaper](#)

Setting a secure identity and access foundation



- Configuring Cloud Identity
- Managing service accounts
- Managing authentication
- Managing and implementing authorization controls
- Defining Resource Hierarchy



**Cymbal
Bank**

High level overview - service comparison

Service	What it is	Use cases
Cloud Identity	An identity provider (IdP) service that lets you create, manage, and delete identities for authentication purpose. It supports single sign-on, multi factor authentication and mobile device management.	<ul style="list-style-type: none">• Cloud-based directory• Authentication (e.g. SSO) & Authorization• User Lifecycle Management• MFA & Endpoint management
Google Cloud Directory Sync	Synchronize the data in your Google Account with your Microsoft Active Directory or LDAP server.	<ul style="list-style-type: none">• Syncs users, aliases, groups, and other data with your Google Account from LDAP of Microsoft AD
Managed Microsoft Active Directory	Extend Microsoft Active Directory on-premises service and configuration to your Google Cloud deployments	<ul style="list-style-type: none">• Manage authentication and authorization for AD-dependent apps and servers• Automate AD server maintenance and security configuration
Identity Platform	Add identity and access management functionality to your applications	Customer identity and access management (CIAM) system used for: <ul style="list-style-type: none">• Multi-tenant SaaS applications• Mobile and web apps• Games, APIs and more

Cloud Identity vs IAM

Cloud Identity	IAM
Identity as a Service (IDaaS) solution that centrally manages users and groups. Often configured to federate identities between Google and other identity providers (AD etc).	Service that lets authorize who can take action on specific GCP resources
In Cloud Identity, you manage BOTH identities AND privileges (via roles). However, it's NOT GCP-specific...	With IAM, you manage privileges (via roles) only. Identities need to be created in advance, in most cases: in Cloud Identity (with the exception of Service Accounts).
Most important role: Super Admin (full access and manage other Admins). Needed to configure GCP organization (= grant Organization Administrator role to others). NOT for daily use. Should use MFA	Most important role: Organization Administrator. Designed to manage day to day organization operations in GCP (= mostly grant IAM roles to identities).
Has a Free and Premium editions, each with different features.	

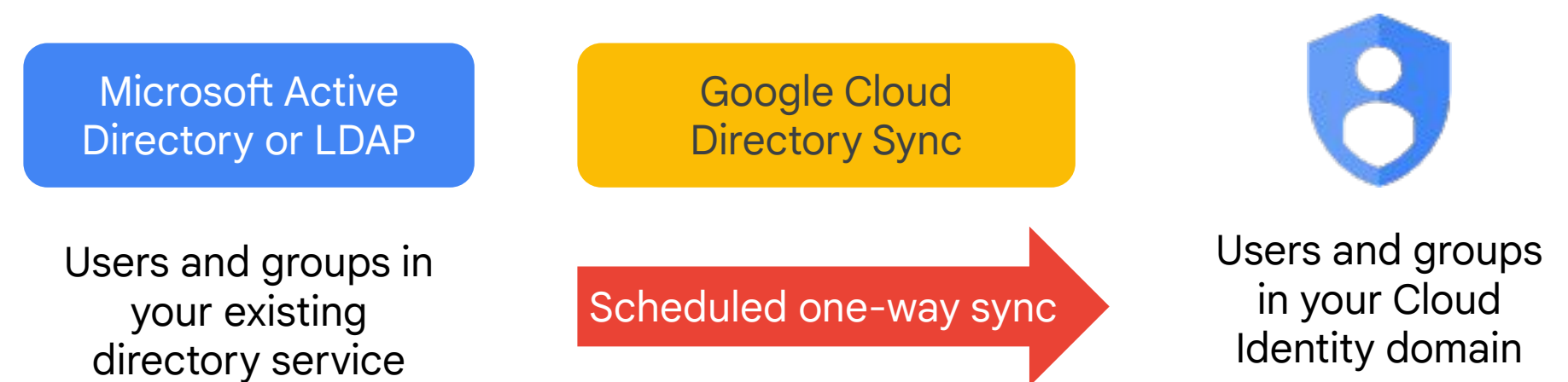
Exam Tips:

- Make sure to differentiate and know best practices of Super Admin (Cloud Identity role) vs Organization Administrator (IAM Role)
- *If you'd like to know how to create new GCP organization, see [this guide](#).*

Synchronizing Cymbal Bank's identities to Google Cloud

One-way synchronization of LDAP or Active Directory (AD) identities using Google Cloud Directory service (GCDS)

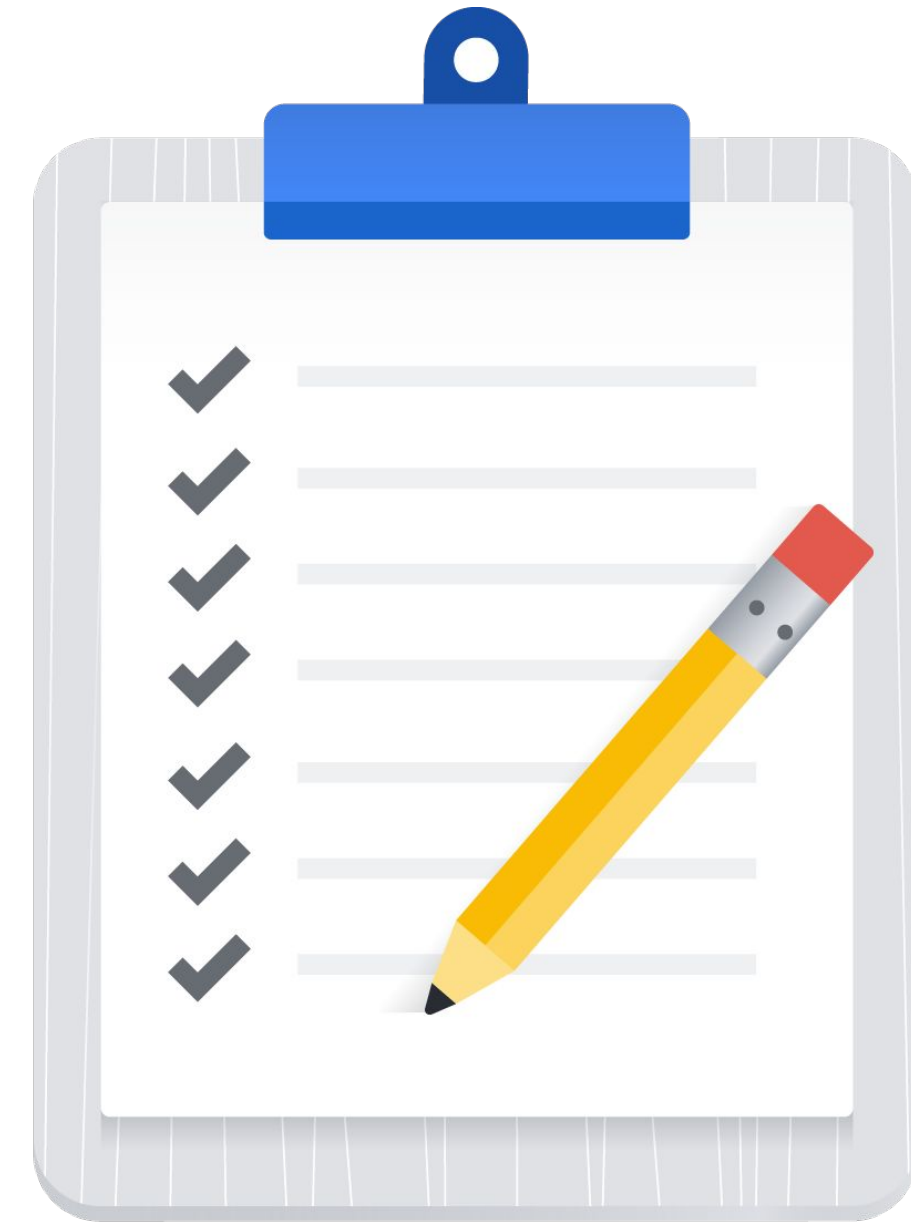
- AD users and groups synchronized to Cloud Identity by GCDS on daily schedule after daily updates to AD system



[GCDS Best Practices](#)

How Google Cloud Directory Sync works

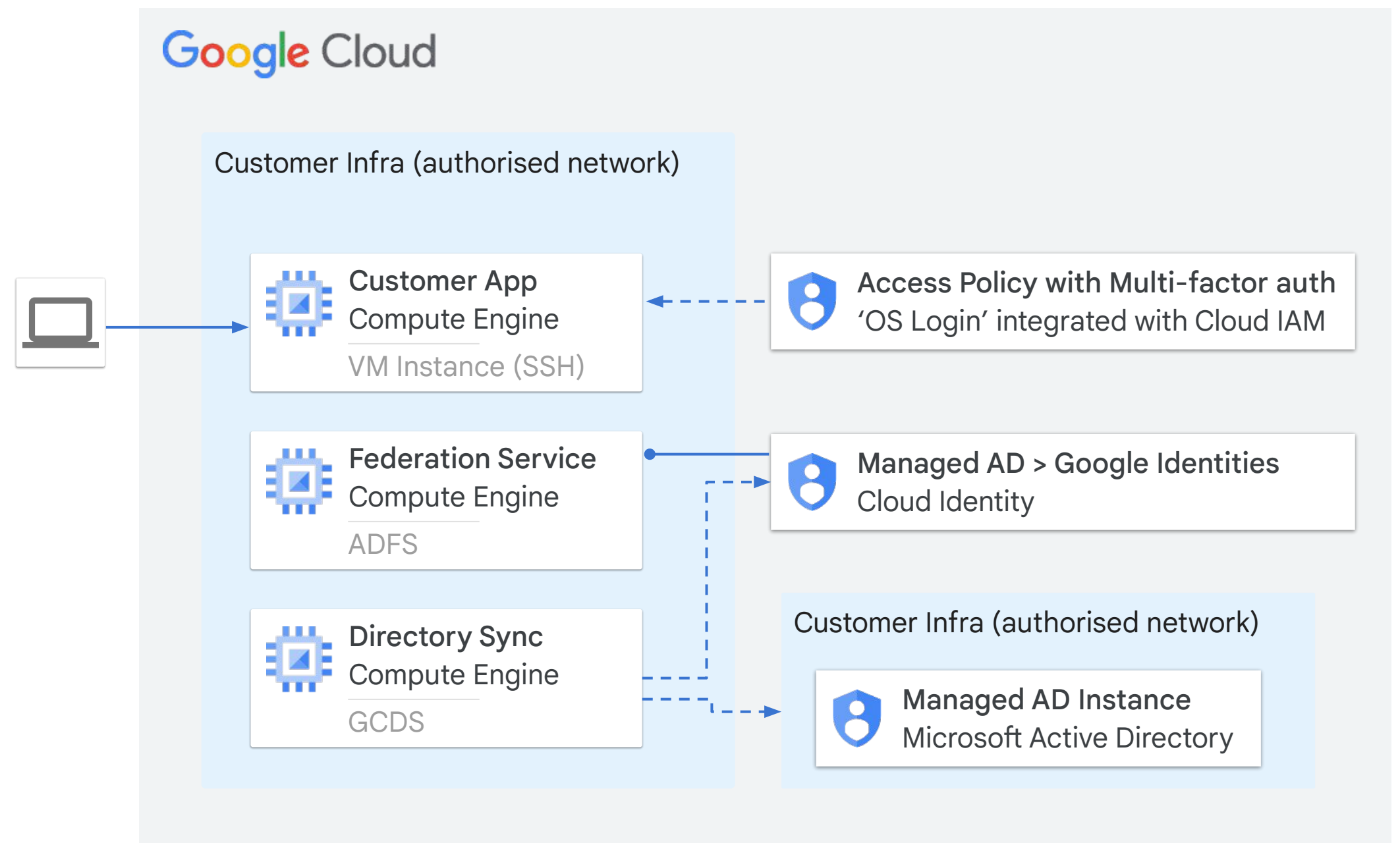
- 1 Data is exported from your LDAP server or Active Directory.
- 2 GCDS connects to the Google domain and generates a list of Google users, groups, and shared contacts that you specify.
- 3 GCDS compares these lists and updates your Google domain to match the data.
- 4 When the synchronization is complete, a report is emailed.



Managed Microsoft AD allows you to manage your cloud-based, AD-dependent workloads

Managed Service for Microsoft Active Directory (Managed Microsoft AD):

- Runs actual Microsoft AD controllers
- Is virtually maintenance-free
- Supports both hybrid cloud and standalone cloud domains



Configuring Cymbal Bank's single sign-on to Google Cloud

SAML2 single sign-on configuration

- Federate using SAML2 for Single sign-on (SSO)
- Active Directory is the Identity provider (IdP) and Google Cloud is the service provider (SP)

☒ Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below. ?

Sign-in page URL

https://sso.your-domain.com/auth

URL for signing in to your system and G Suite

Sign-out page URL

https://sso.your-domain.com/logout

URL for redirecting users to when they sign out

Change password URL

https://sso.your-domain.com/info

URL to let users change their password in your system; when defined here, this is Shown even when Single Sign-on is not enabled.

Verification certificate

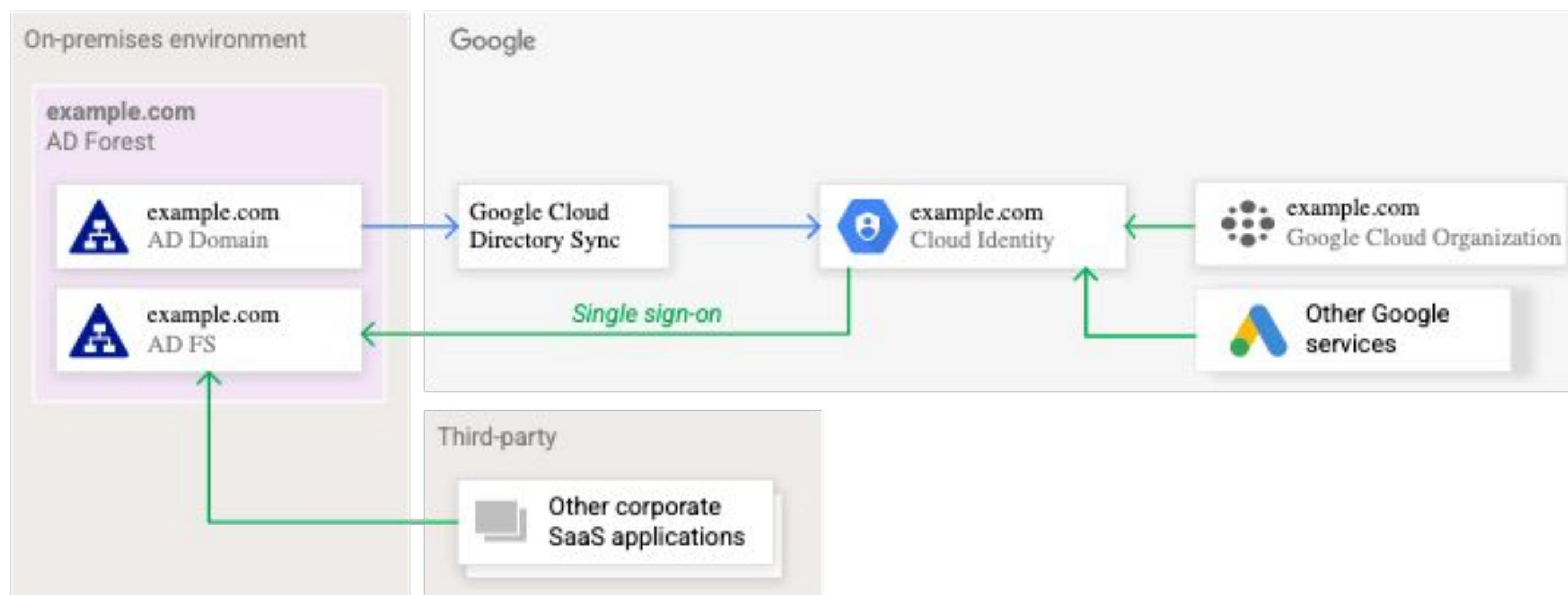
Choose File

Certificate.pem

UPLOAD

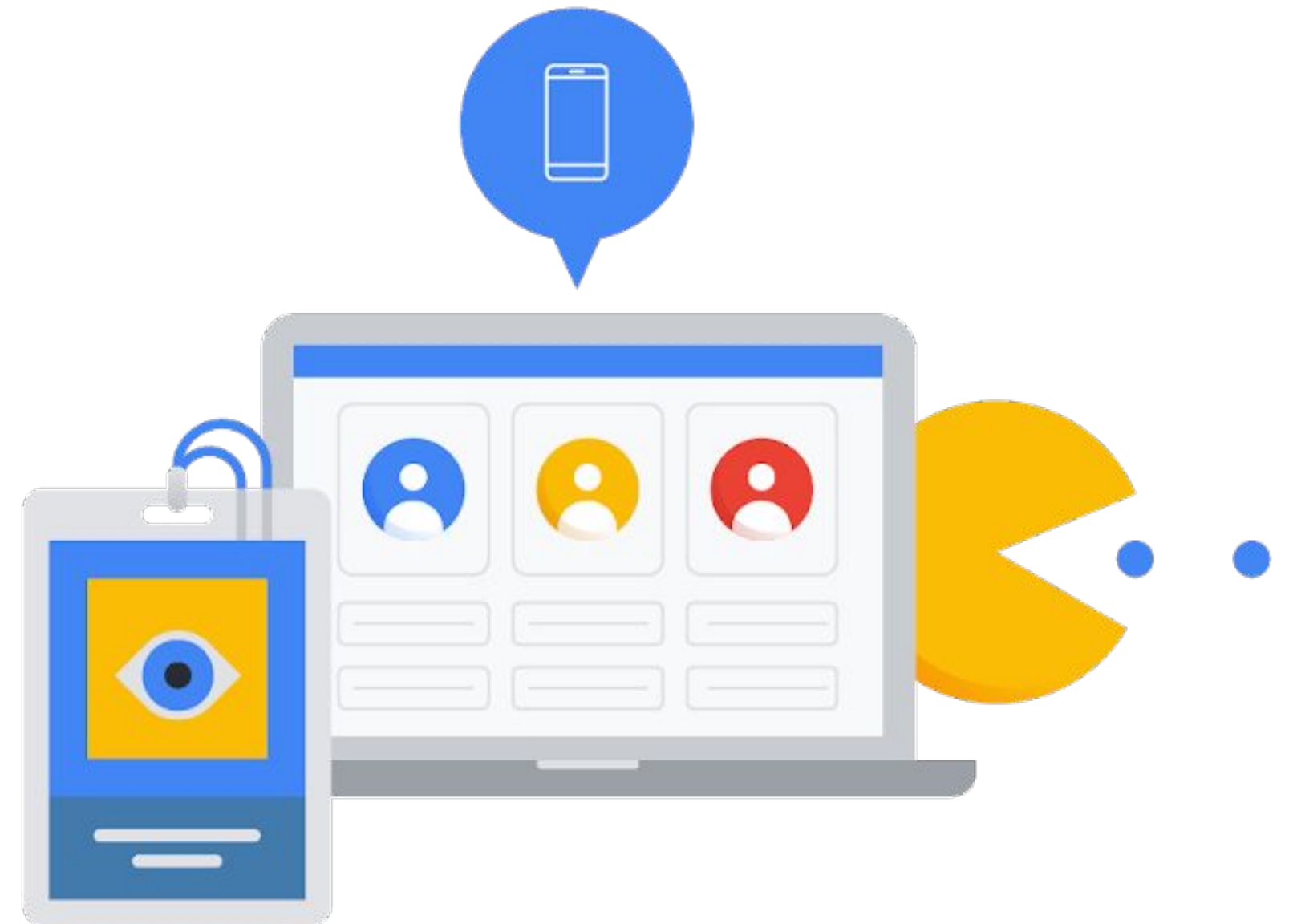
The certificate file must contain the public key for Google to verify sign-in requests.

SSO: ADFS + GCDS



Identity Platform overview

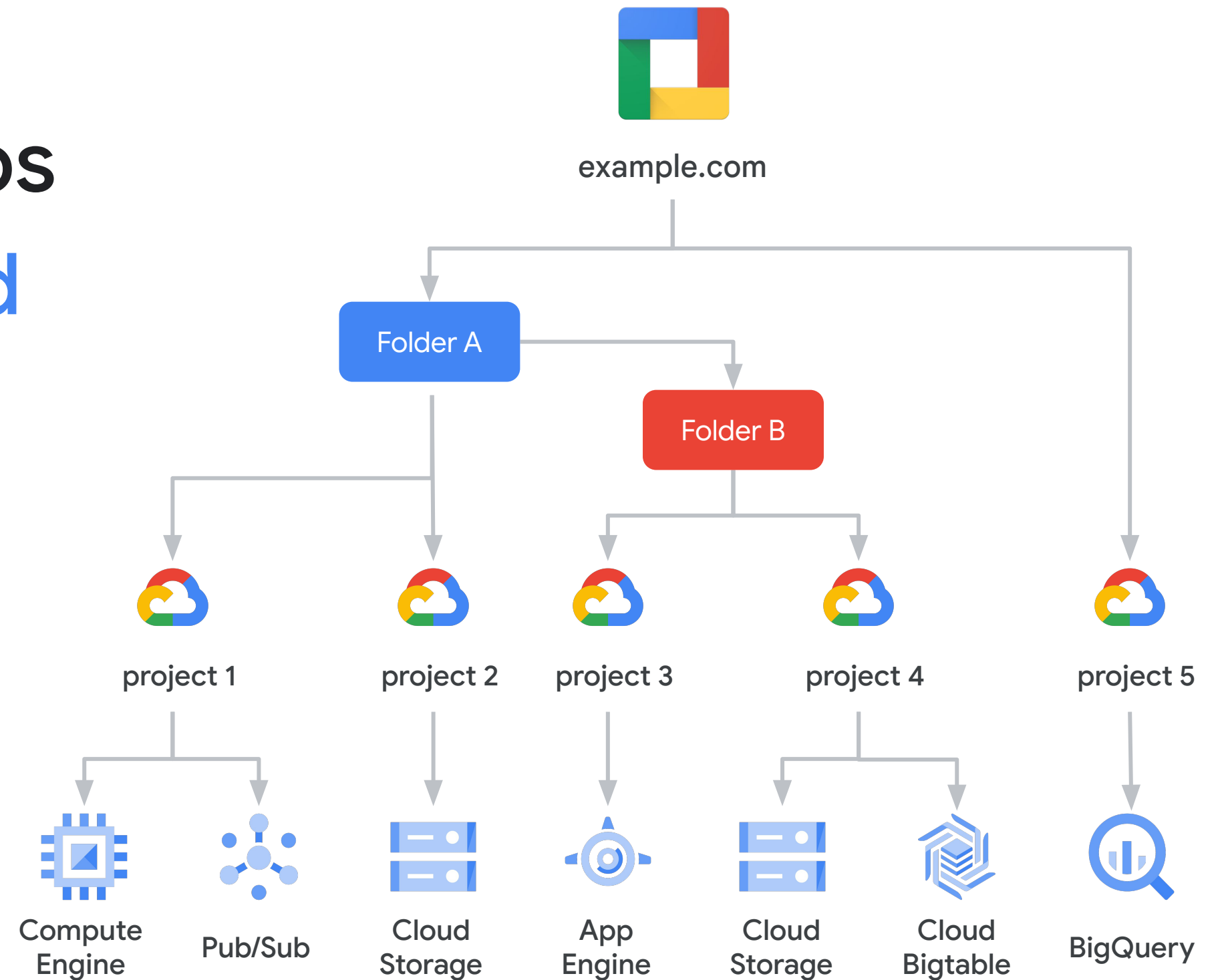
- Customer identity and access management (CIAM) system
- Used for:
 - Multi-tenant SaaS applications
 - Mobile and web apps
 - Games
 - APIs and more



Organization hierarchy helps organize access **control and** **policy for resources**

Folders provide for flexible
hierarchy of Projects

- Organization policy and access control can be bound at any level and flow downwards



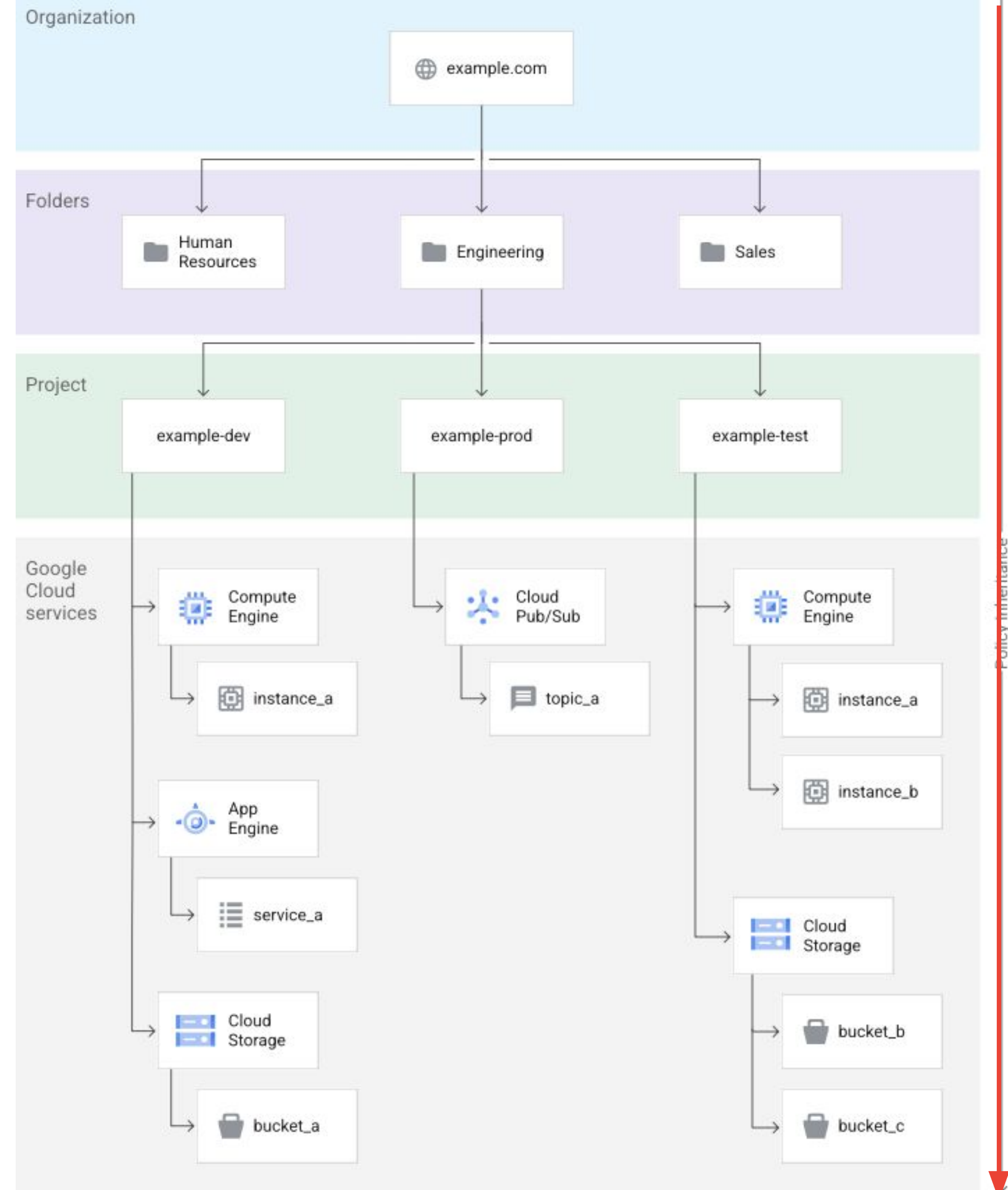
[Know how to migrate projects across folders / orgs](#)

IAM Policies inheritance

IAM lets you set allow policies at the following levels of the resource hierarchy:

- **Organization level.** The organization resource represents your company. IAM roles granted at this level are inherited by all resources under the organization.
- **Folder level.** Folders can contain projects, other folders, or a combination of both. Roles granted at the highest folder level will be inherited by projects or other folders that are contained in that parent folder.
- **Project level.** Projects represent a trust boundary within your company. IAM roles granted at the project level are inherited by resources within that project.
- **Resource level.** Some resources support lower-level roles so that you can grant certain users permission to a single resource within a project.

Deny policies? Yes... and no...



Bind roles to identities to provide access to resources

Roles are collections of permissions which align with the required access for an abstract job function

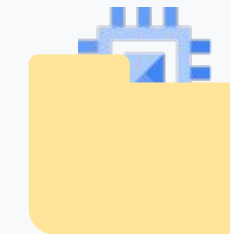
- Facilitate least privilege access control and separation of duties
- Can be bound at organization, folder, project, or resource level and flows downwards

Additional IAM-related services:

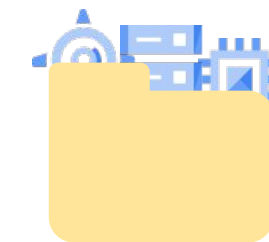
- [Policy Simulator](#)
- [Policy Analyzer](#)
- [Policy Troubleshooter](#)



Basic



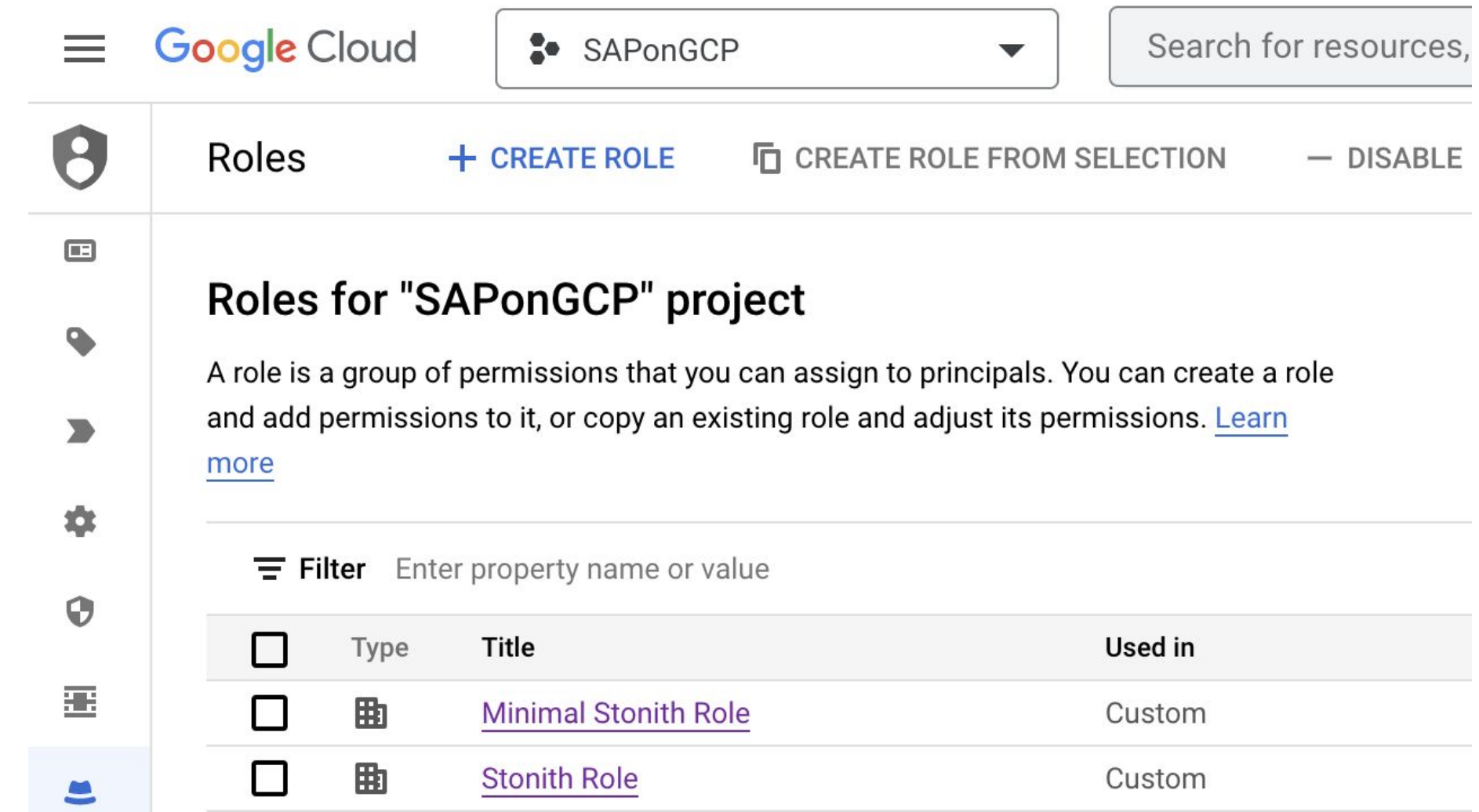
Predefined



Custom

Know how to...

- [Update existing IAM Policy](#)
- [Create a custom IAM role](#)



The screenshot shows the Google Cloud IAM Roles interface for the 'SAPonGCP' project. The page title is 'Roles for "SAPonGCP" project'. Below the title, there is a description: 'A role is a group of permissions that you can assign to principals. You can create a role and add permissions to it, or copy an existing role and adjust its permissions. [Learn more](#)'. A table lists the roles for this project. The table has columns: 'Type', 'Title', and 'Used in'. There are three roles listed: 'Minimal Stonith Role' and 'Stonith Role', both of which are 'Custom' roles. The 'Stonith Role' is highlighted with a blue background.

Type	Title	Used in
	Minimal Stonith Role	Custom
	Stonith Role	Custom

```
gcloud RESOURCE_TYPE get-iam-policy RESOURCE_ID --format=FORMAT > PATH
```

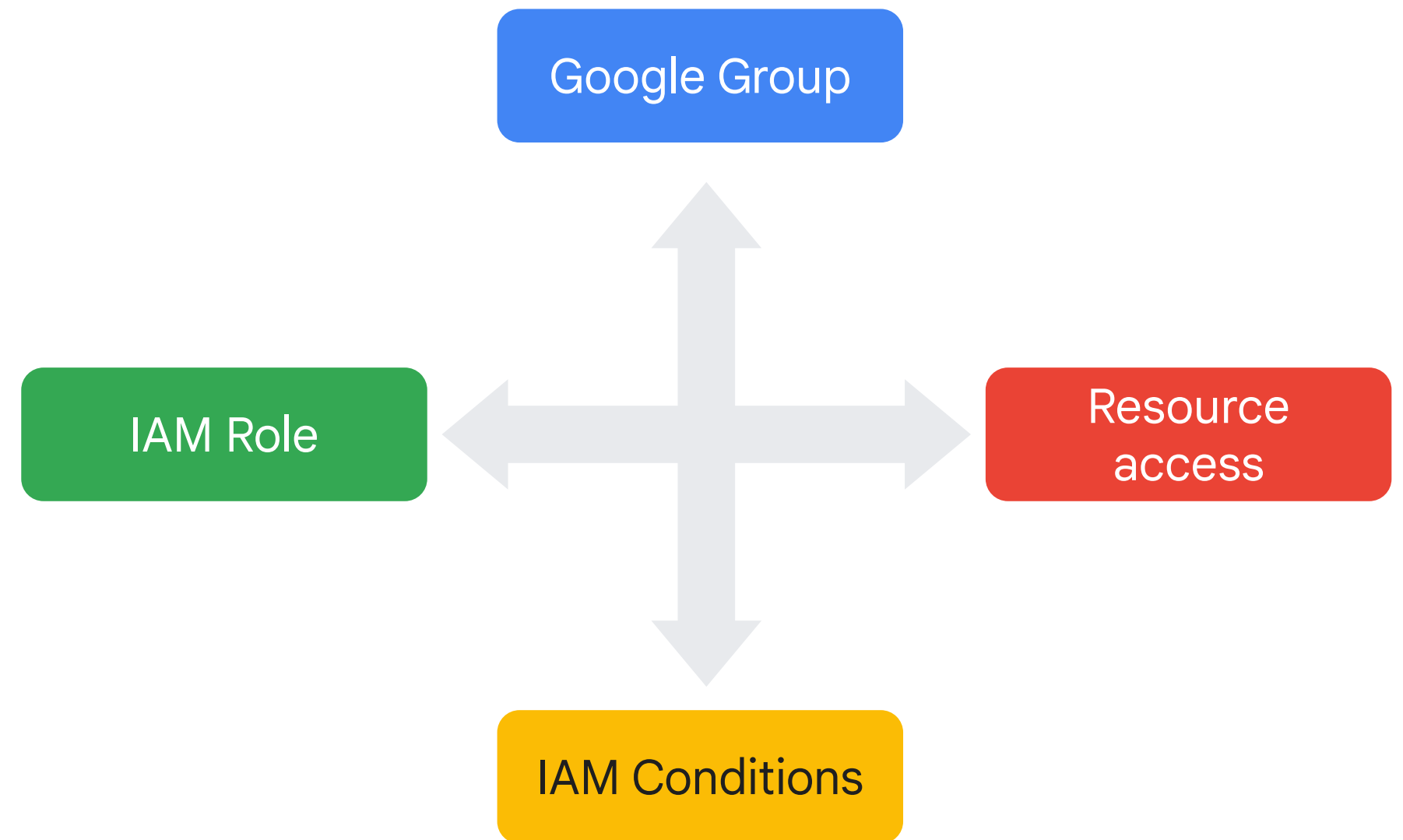
```
gcloud RESOURCE_TYPE set-iam-policy RESOURCE_ID PATH
```

```
gcloud RESOURCE_TYPE add-iam-policy-binding RESOURCE_ID \
  --member=PRINCIPAL --role=ROLE_ID \
  --condition=CONDITION
```

IAM conditions to control the where, when, how of access to resources

IAM conditions can be added to role bindings to control from where, when, and how the access can be used

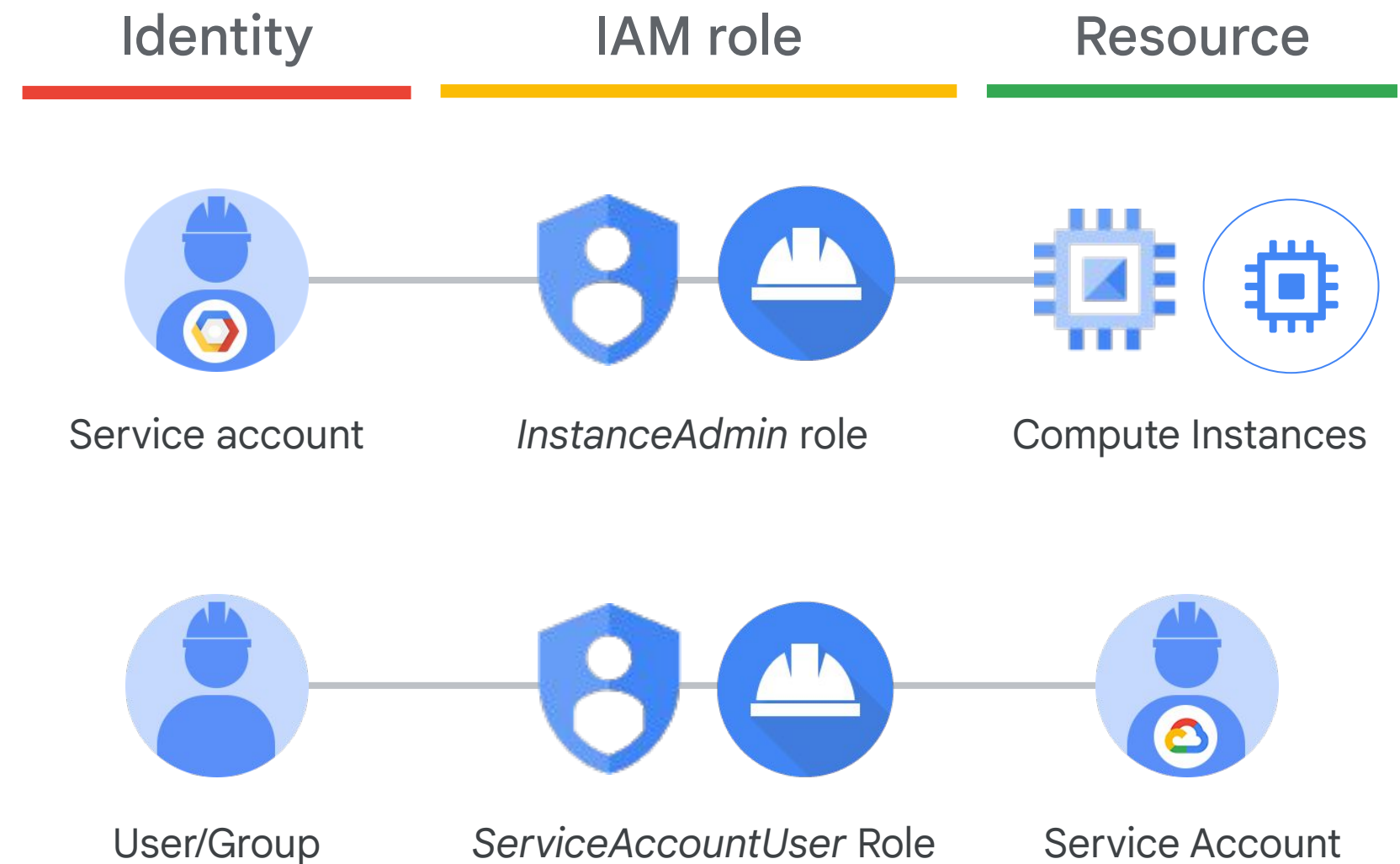
- Allows for even better least privilege access control



Service accounts provide service access to Google Cloud

Service accounts used as service identities for workloads running in or outside Google Cloud

- Given access to resources like user and group identities
- Authenticate with private keys
- Leverage Google key management for most secure usage



[All Service Account recommendations](#)

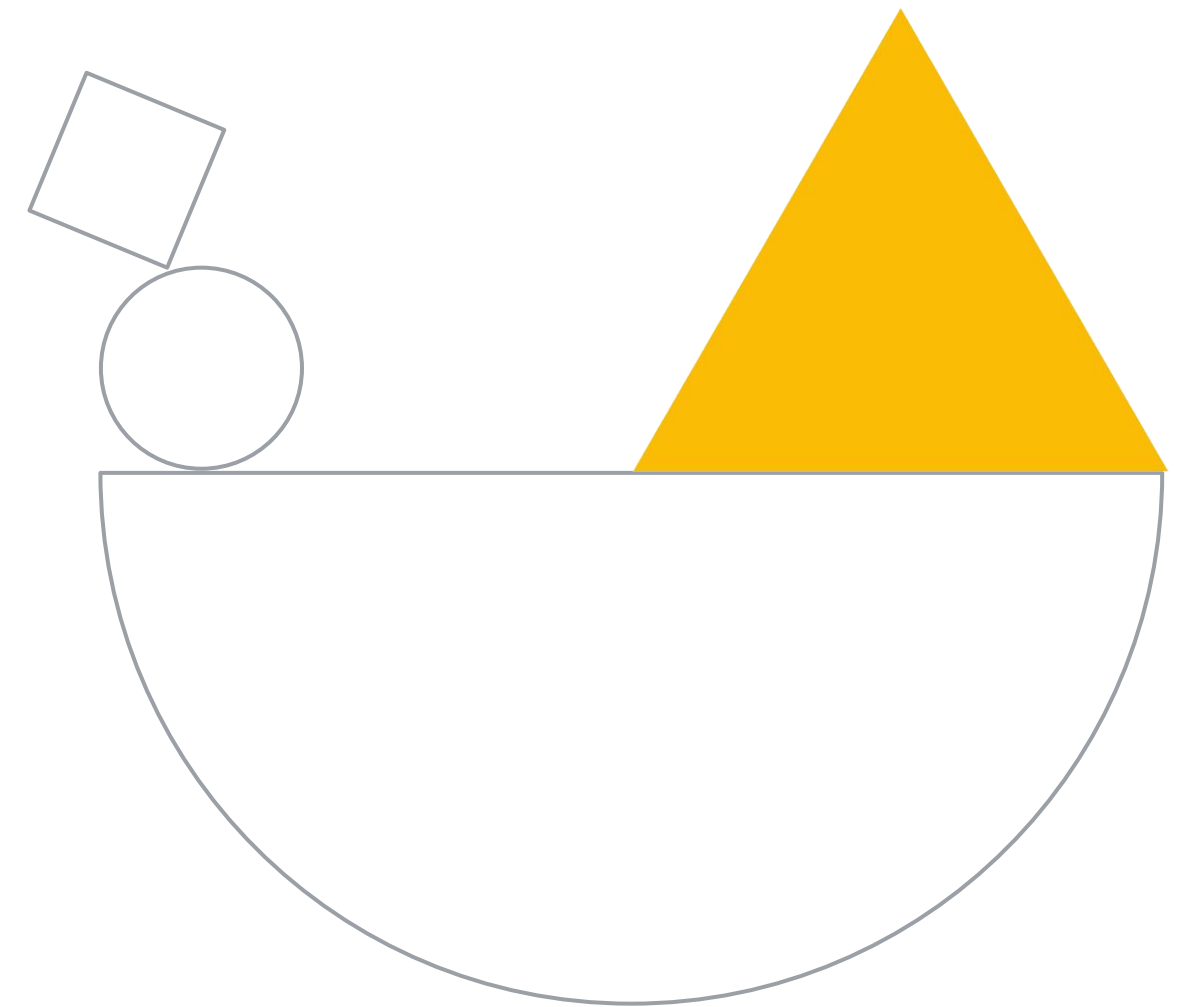
Service account keys **recommendations**

- Not recommended to generate SA keys at all if not absolutely needed. What are the alternatives?
 - [Workload Identity](#)
 - [Workload Identity Federation](#)
 - [Short-lived credentials](#)
- [Limit projects where you can create Service Accounts / Service Account keys.](#)
- Don't keep keys in source code repos / program binaries
- Don't store keys in Secret Manager! It's for secrets, not encryption keys
- If you generated the public/private key pair yourself, stored the private key in a hardware security module (HSM), and uploaded the public key to Google.
- etc...



[All Service Account keys recommendations](#)

Diagnostic questions

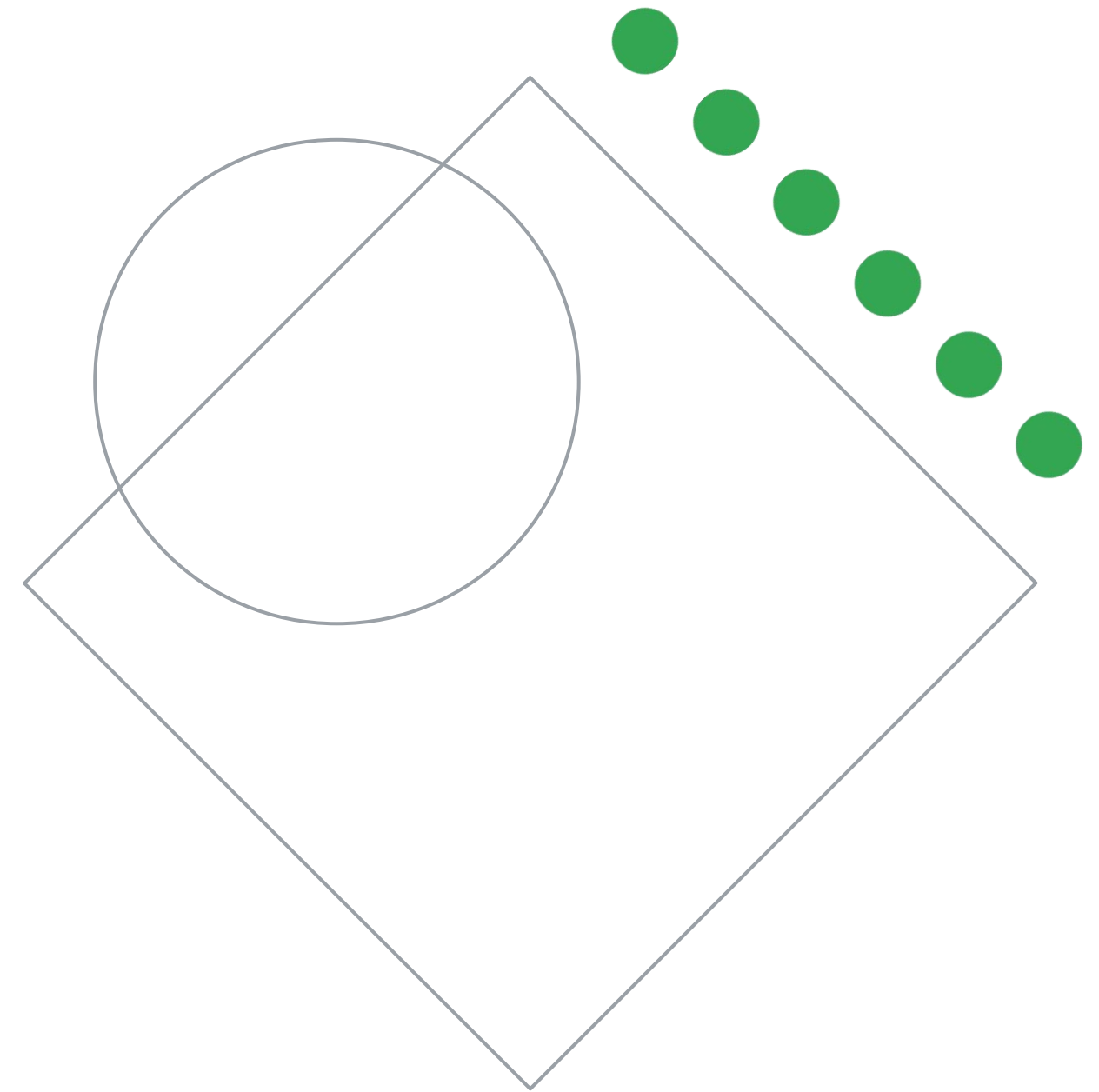


Please complete the diagnostic questions now

- Forms are provided for you to answer the diagnostic questions
- The instructor will provide you a link to the forms
- The diagnostic questions are also available in the workbook

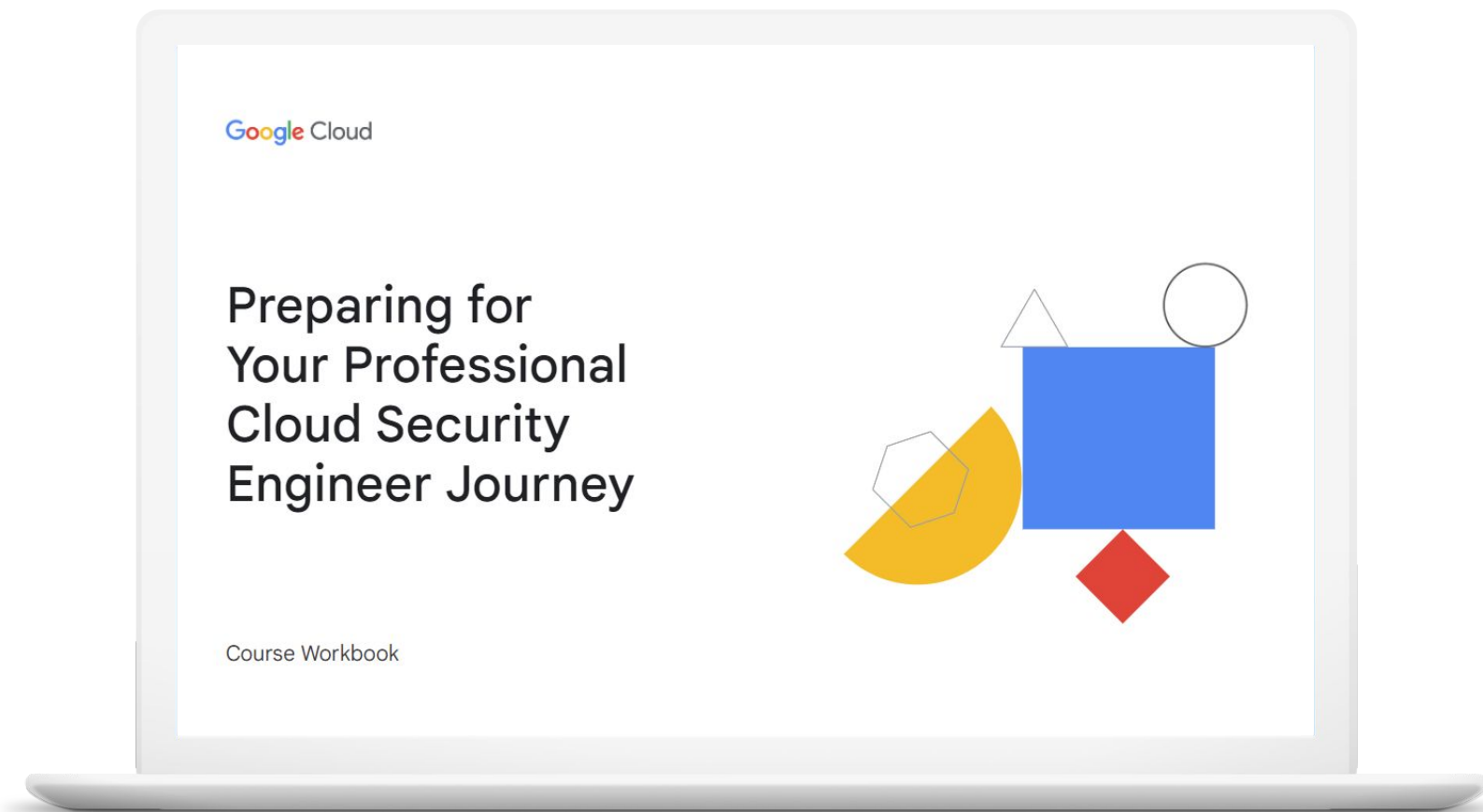


Review and study planning



Your study plan:

Configuring access within a cloud solution environment



1.1

Configuring Cloud Identity

1.2

Managing service accounts

1.3

Managing authentication

1.4

Managing and implementing authorization controls

1.5

Defining Resource Hierarchy

1.1 | Configuring Cloud Identity

Considerations include:

- Managing Cloud Identity
- Configuring Google Cloud Directory Sync
- Managing super administrator account
- Automating user lifecycle management process
- Administering user accounts and groups programmatically

1.1 | 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.



1.1 | 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.



1.1 | 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.



1.1 | 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.



1.1 | Configuring Cloud Identity

Courses



[Security in Google Cloud](#)

- M2 Cloud Identity



[Managing Security in Google Cloud](#)

- M2 Cloud Identity

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](#)

1.2 | 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, authorizing, and securing service accounts
- Securely managing API access management
- Managing and creating short-lived credentials

1.2 | 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.



1.2 | 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.



1.2 | 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 **Enforcement** 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.



1.2 | 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 **Enforcement** 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.



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 Kubernetes: Techniques and Best Practices

Skill Badges



Google Cloud

[Ensure Access and Identity in Google Cloud Quest](#)

Documentation

[Creating short-lived service account credentials | Cloud IAM Documentation](#)

[Restricting service account usage | Resource Manager Documentation | Google Cloud](#)

1.3 | Managing authentication

Considerations include:

- Creating a password policy for user accounts
- Establishing Security Assertion Markup Language (SAML)
- Configuring and enforcing two-factor authentication

1.3 | 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.



1.3 | 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.



1.3 | Diagnostic Question 06 Discussion



Cymbal Bank's Mobile Development Team has an AI Platform instance in a Google Cloud Project. An auditor needs to record the AI Platform jobs and models, along with their usage. You need to assign permissions to the external auditors so that they can view the models and jobs but not retrieve specific details on any of them.

What should you do?

- A. Create a custom role for auditors at the Organization level. Create a JSON file with required permissions `ml.models.list` and `ml.jobs.list`. Use `gIAM roles create role-id -- organization organization-id --file=json-file-path`.
- B. Create a custom role for auditors at the Project level. Create a YAML file with required permissions `ml.models.list` and `ml.jobs.list`. Use `gIAM roles create role-id --project project-id --file=yaml-file-path`.
- C. Create a custom role for auditors at the Project level. Use `gIAM roles create role-name --project project-id --permissions= ml.models.get, ml.jobs.get`.
- D. Create a custom role for auditors at the Organization level. Create a JSON file with required permissions `ml.models.list` and `ml.jobs.list`. Use `gIAM role create role-id --organization organization-id --file=json-file-path`.

1.3 | Diagnostic Question 06 Discussion



Cymbal Bank's Mobile Development Team has an AI Platform instance in a Google Cloud Project. An auditor needs to record the AI Platform jobs and models, along with their usage. You need to assign permissions to the external auditors so that they can view the models and jobs but not retrieve specific details on any of them.

What should you do?

- A. Create a custom role for auditors at the Organization level. Create a JSON file with required permissions `ml.models.list` and `ml.jobs.list`. Use `gIAM roles create role-id -- organization organization-id --file=json-file-path`.
- B. Create a custom role for auditors at the Project level. Create a YAML file with required permissions `ml.models.list` and `ml.jobs.list`. Use `gIAM roles create role-id --project project-id --file=yaml-file-path`.
- C. Create a custom role for auditors at the Project level. Use `gIAM roles create role-name --project project-id --permissions= ml.models.get, ml.jobs.get`.
- D. Create a custom role for auditors at the Organization level. Create a JSON file with required permissions `ml.models.list` and `ml.jobs.list`. Use `gIAM role create role-id --organization organization-id --file=json-file-path`.

1.3 | Managing authentication

Courses



Security in Google Cloud

- M2 Cloud Identity
- M3 Identity and Access Management (IAM)



Managing Security in Google Cloud

- M2 Cloud Identity
- 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 | Cloud IAM Documentation](#)

[Understanding IAM custom roles | Cloud IAM Documentation | Google Cloud](#)

[Understanding roles | Cloud IAM Documentation](#)

1.4 | Managing and implementing authorization controls

Considerations include:

- Managing privileged roles and separation of duties
- Managing IAM permissions with basic, predefined, and custom roles
- Granting permissions to different types of identities
- Understanding difference between Cloud Storage IAM and ACLs
- Designing identity roles at the organization, folder, project, and resource level
- Configuring Access Context Manager

1.4 | 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.



1.4 | 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.

1.4 | Diagnostic Question 08 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. 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.



1.4 | Diagnostic Question 08 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. 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.

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 | Cloud IAM Documentation](#)

[Understanding roles | Cloud IAM Documentation](#)

1.5 | Defining resource hierarchy

Considerations include:

- Creating and managing organizations
- Designing resource policies for organizations, folders, projects, and resources
- Managing Organization constraints
- Using Resource Hierarchy for Access Control and permissions inheritance
- Designing and managing trust and security boundaries within Google Cloud projects

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.



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.



1.5 | 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. Add developers to the 'dev' folder, and add administrators 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. Add developers to the 'dev' folder, and add administrators 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. Add developers to the 'dev' folder, and add administrators 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. Add developers to the 'dev' folder, and add administrators to the 'admin' folder.



1.5 | 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. Add developers to the 'dev' folder, and add administrators 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. Add developers to the 'dev' folder, and add administrators 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. Add developers to the 'dev' folder, and add administrators 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. Add developers to the 'dev' folder, and add administrators to the 'admin' folder.

1.5 | Defining resource hierarchy

Courses



[Security in Google Cloud](#)

- M2 Cloud Identity
- M3 Identity and Access Management (IAM)



[Managing Security in Google Cloud](#)

- M2 Cloud Identity
- 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](#)

Knowledge Check 1

Which tool will Cymbal Bank use to synchronize their identities from their on-premise identity management system to Google Cloud?

- A. Active Directory
- B. Service Accounts
- C. Google Cloud Directory Sync
- D. Cloud Identity



Knowledge Check 1

Which tool will Cymbal Bank use to synchronize their identities from their on-premise identity management system to Google Cloud?

- A. Active Directory
- B. Service Accounts
- C. Google Cloud Directory Sync
- D. Cloud Identity



Knowledge Check 2

Which feature of Google Cloud will Cymbal Bank use to control the source locations and times that authorized identities will be able to access resources?

- A. IAM Conditions
- B. IAM Roles
- C. Service Accounts
- D. Identity-aware Proxy



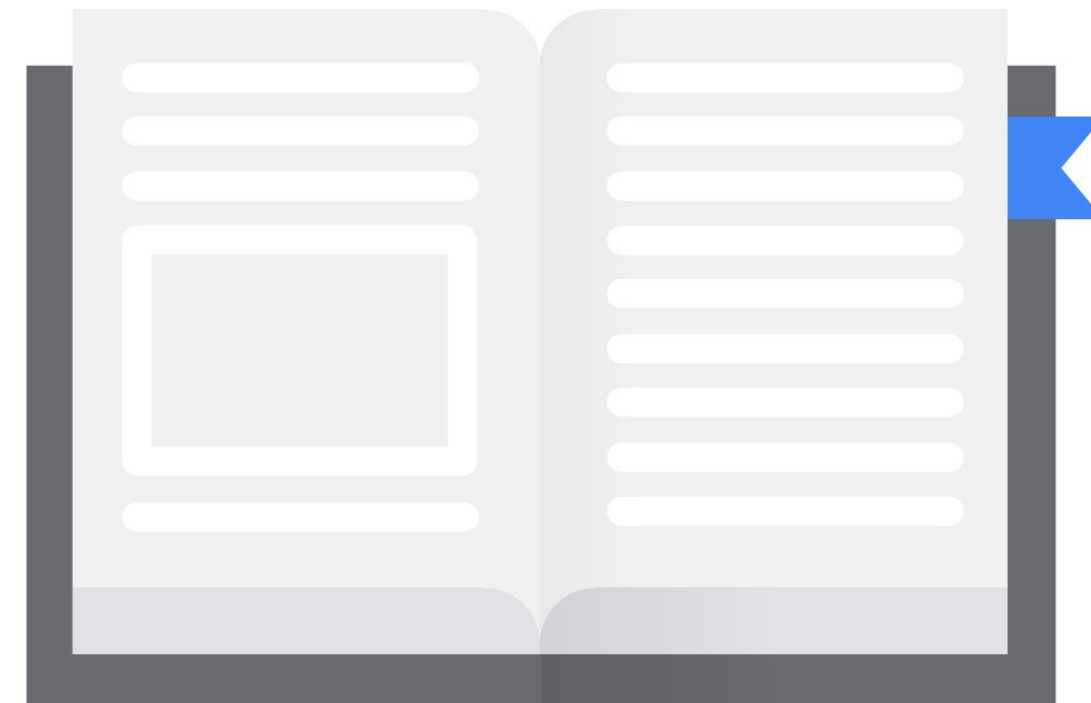
Knowledge Check 2

Which feature of Google Cloud will Cymbal Bank use to control the source locations and times that authorized identities will be able to access resources?

- A. IAM Conditions
- B. IAM Roles
- C. Service Accounts
- D. Identity-aware Proxy



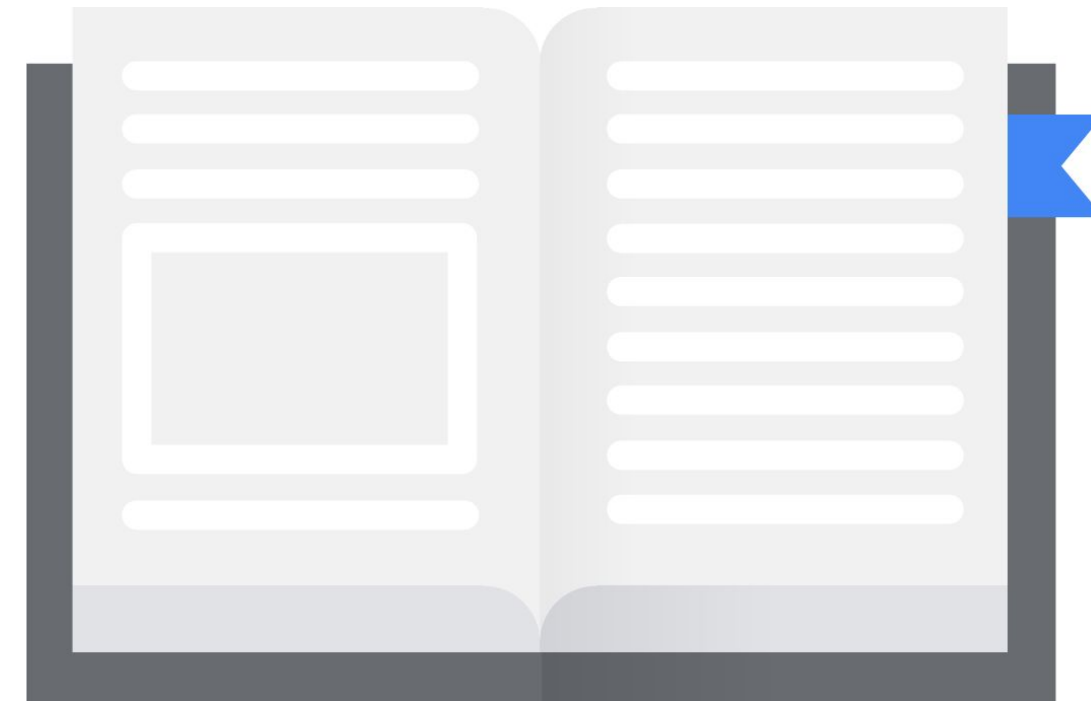
This week's learning plan



Tasks for this week:

- [Course] GCP Fundamentals - Core Infrastructure
 - [Coursera](#)
 - [Pluralsight](#)
 - [CloudSkillsBoost](#)

Additional content



Additional content 1

[READING]

- [Configuration of GCDS using Configuration Manager](#) - it's good to have an overview of this process
- [Google Workspace - Secure LDAP](#) - what is a Secure LDAP Service?
- [Patterns for authenticating corporate users in a hybrid environment](#)
- [Best practices for federating identities](#)
- [Super administrator account best practices](#)
- [Security best practices for administrator accounts](#)
- [Understanding roles](#)
- [Understanding IAM custom roles](#)
- [Creating and managing custom roles](#)
- [Overview of Google identity management](#)
- [Audit logs for service accounts](#) - Just to get a feeling what kind of information is ingested into Cloud Logging
- [Best practices for managing service account keys](#) - lengthy, but super important!
- [Creating and managing service accounts](#)
- [Manage service account insights](#)
- [Delegating domain-wide authority to the service account](#)
- [Enforce and monitor password requirements for users](#)
- [Managing SAML and OIDC providers](#)

Additional content 2

- [Deploy 2-Step Verification](#)
- [Adding multi-factor authentication to your web app](#)
- [Setting up OS Login with 2-step verification](#) - important for secure logging to VMs via ssh
- [Overview of IAM Conditions](#)
- [What is an IAM Policy?](#)
- [Understanding IAM Policies](#)
- [IAM Policy Troubleshooter](#) - how to check why a user has access to a resource or doesn't have permission to call an API
- [Using IAM securely](#) - best practices for using IAM
- [IAM details for GCS Buckets](#)
- [Creating and managing organizations](#)
- [IAM roles on Organization level](#)
- [Resource Hierarchy](#)
- [How to migrate projects](#) - also between organizations
- [Introduction to the Organization Policy Service](#) (Org Policies are NOT the same as IAM Policies!)
- [Understanding Constraints in Organization Policies](#)
- [Service Account Key rotation](#) and [best practices](#)

Additional content 3

[VIDEOS]

- [Security in the Cloud](#) (vs on premises)
- [6 layers of Google Cloud data center security](#)
 - a. It also contains introduction to SCC (Security Command Center)
- great Cloud Identity (& more) demo from ~12:30 to ~28:00: [Cloud OnAir: Unify identity, device, and app management with Cloud Identity](#)
- How to start with GCP as an organization - a unique opportunity to see how to validate & attach a domain to GCP, create an organization and set up Cloud Identity in a recommended, secure way: [Level Up From Zero Episode 1: Domains, Identity, and Admin Accounts](#)
- How to design resource hierarchy in GCP: [Level Up From Zero Episode 2: Organizations & the Resource Hierarchy](#)
- Creating IAM Policies (= granting permissions) at different levels of a resource hierarchy in a recommended, secure-oriented manner: [Level Up From Zero Episode 3: Identity & Access Management](#)
- [Advanced IAM: Hacks, tips, and tricks for policy management](#)
- [How to secure your Service Accounts](#)
- [Service Account keys and impersonation](#)
- Super-important to know how to use and impersonate Service Accounts: [Service Accounts in action](#)
- Organization Policy Service example: [How to limit public IPs on Google Cloud](#)

Additional content 4

[PODCASTS]

- [Zero Trust: Fast Forward from 2010 to 2021](#)
- (**RECOMMENDED**; super helpful in understand identities and privilege concepts in GCP vs on-premises):
[Impersonating Service Accounts in GCP and Beyond](#)
- [Cloud Migrations: Security Perspectives from The Field](#)
- [Preparing for Cloud Migrations from a CISO Perspective, Part 1](#)

[DEEP DIVES]

- [Customer-Supplied Encryption Keys overview.](#)
- [Google infrastructure security design overview.](#)
- [High-level GCP security overview.](#)

Security-related glossary

- SOC: Security Operations Center
- NOC: Network Operations Center
- CISO: Chief Information Security Officer
- **Toil:** *“the kind of work tied to running a production service that tends to be manual, repetitive, automatable, tactical, devoid of enduring value, and that scales linearly as a service grows.”*. **Alternative definition:** *“If your service remains in the same state after you have finished a task, the task was probably toil.”*
- DevSecOps - Security part of DevOps team
- IDS: Intrusion Detection System
- IPS: Intrusion Prevention System
- SIEM: security information & event management
- NTA: network traffic analytics
- Shifting left: The process of checking for vulnerabilities earlier in development
- Forensics is the application of science to criminal and civil laws. It is a proven approach for gathering and processing evidence at a crime scene.
- IP: Intellectual Property
- TTP: Tactics, Techniques and Procedures
- IOC - Indicator Of Compromise