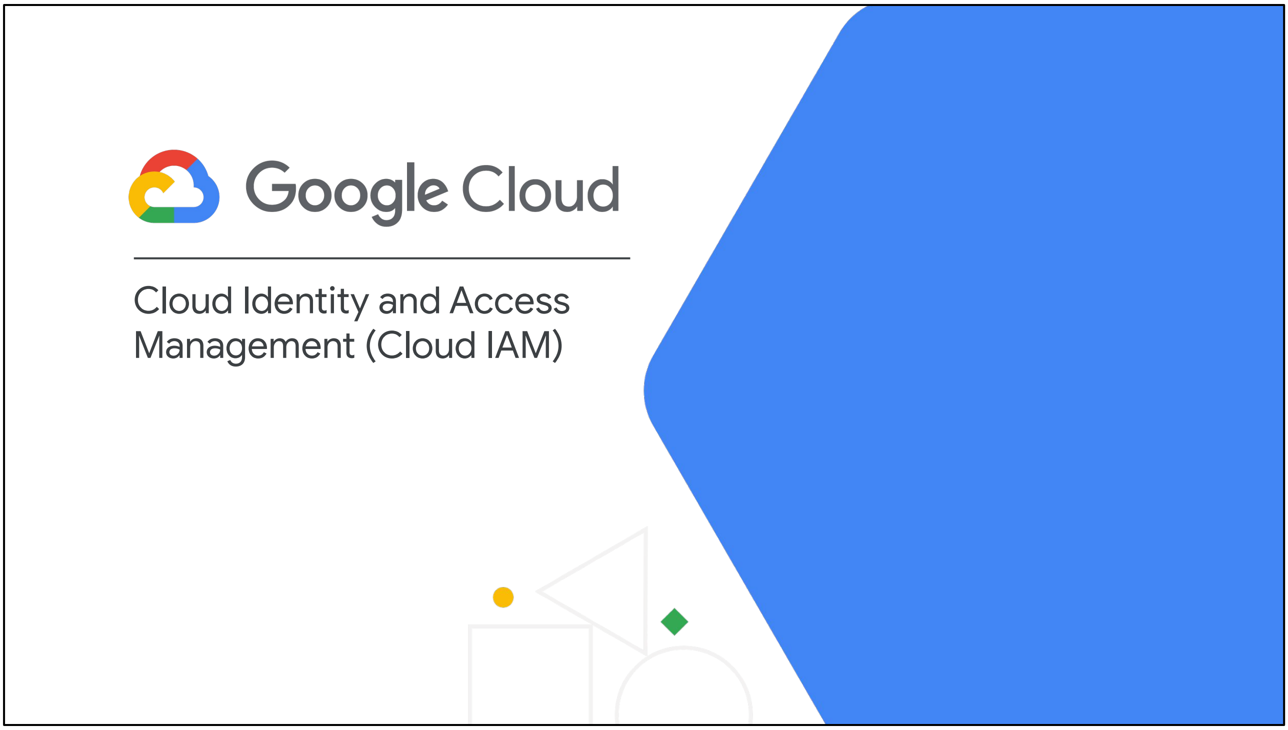
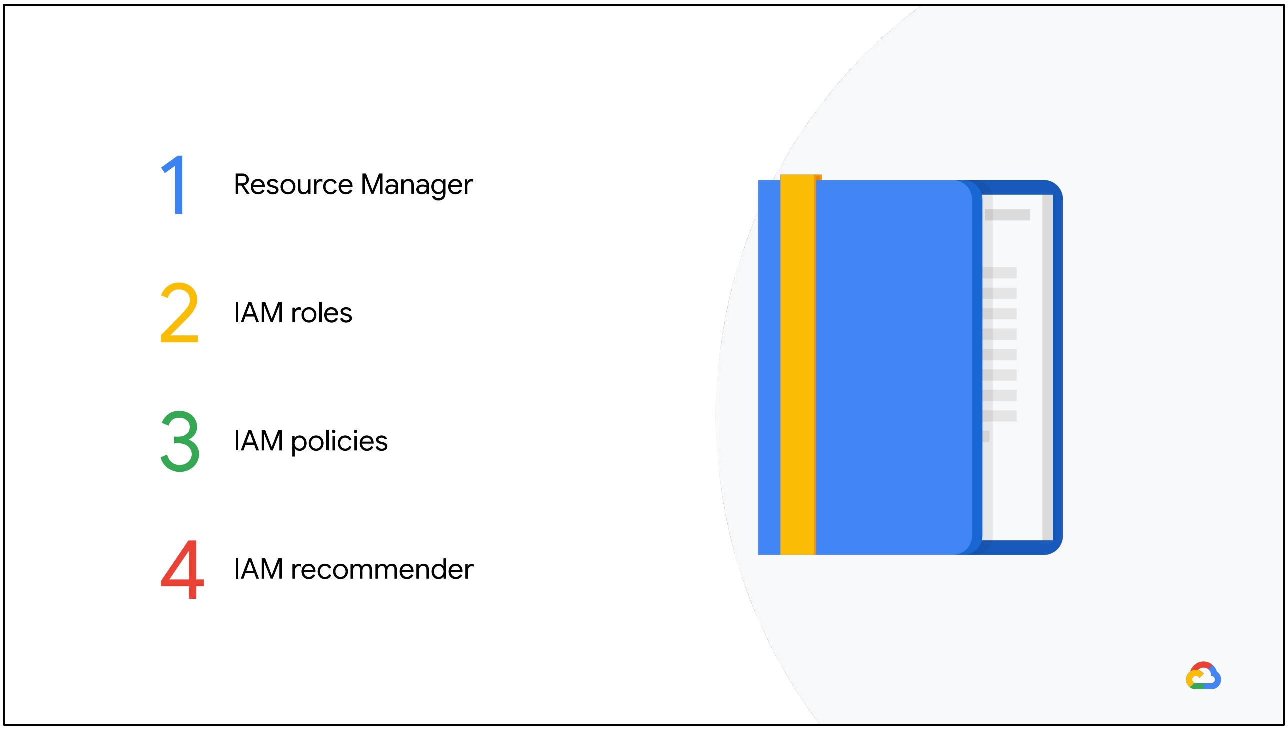


Google Cloud

Cloud Identity and Access Management (Cloud IAM)

Welcome to the Cloud Identity and Access Management module, part of the Security in Google Cloud course.

Cloud Identity and Access Management (or Cloud IAM as it is known) lets administrators authorize who can take action on specific resources, giving you full control and visibility to manage your cloud resources centrally.



1 Resource Manager

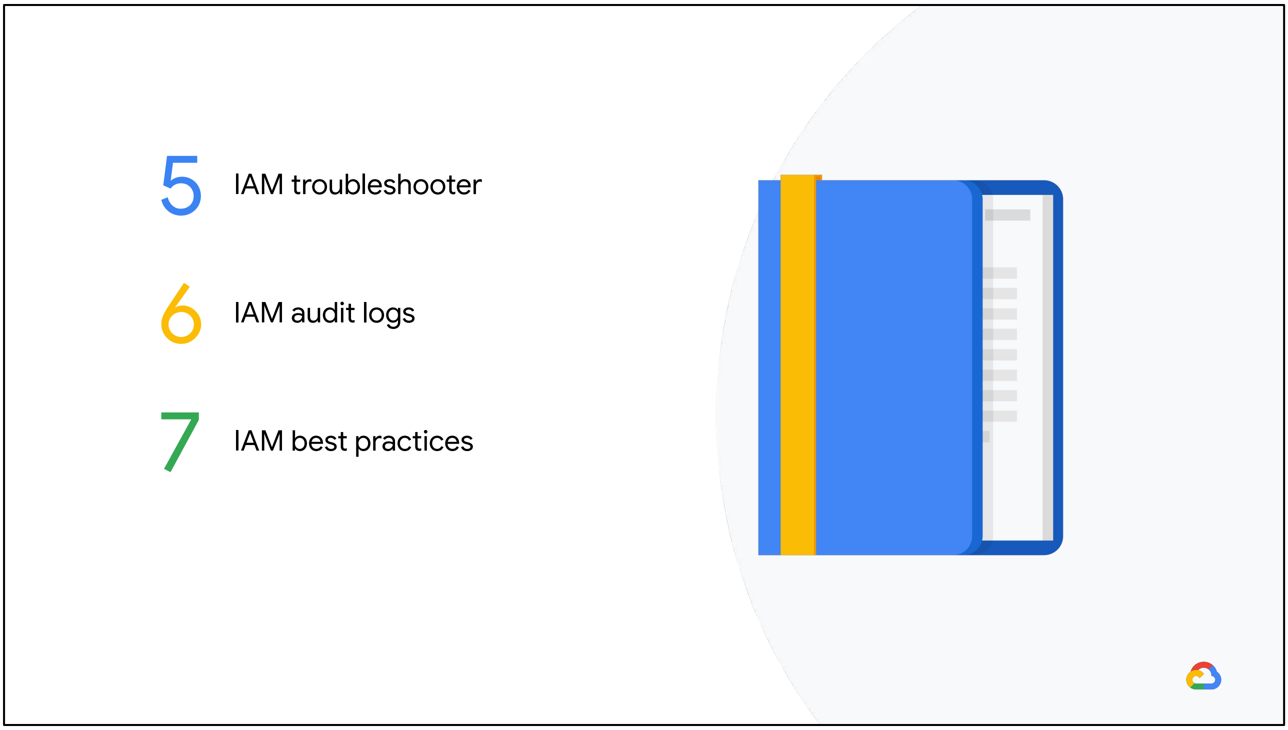
2 IAM roles

3 IAM policies

4 IAM recommender

More specifically, we will cover the **Resource Manager** which enables you to centrally manage projects, folders, and organizations, **IAM roles** and **policies**, including custom roles, and IAM labels.

After this, we will cover **IAM Recommender**, which helps you make sure users have ***only the permissions they need*** to do their work, but no more than what is required.



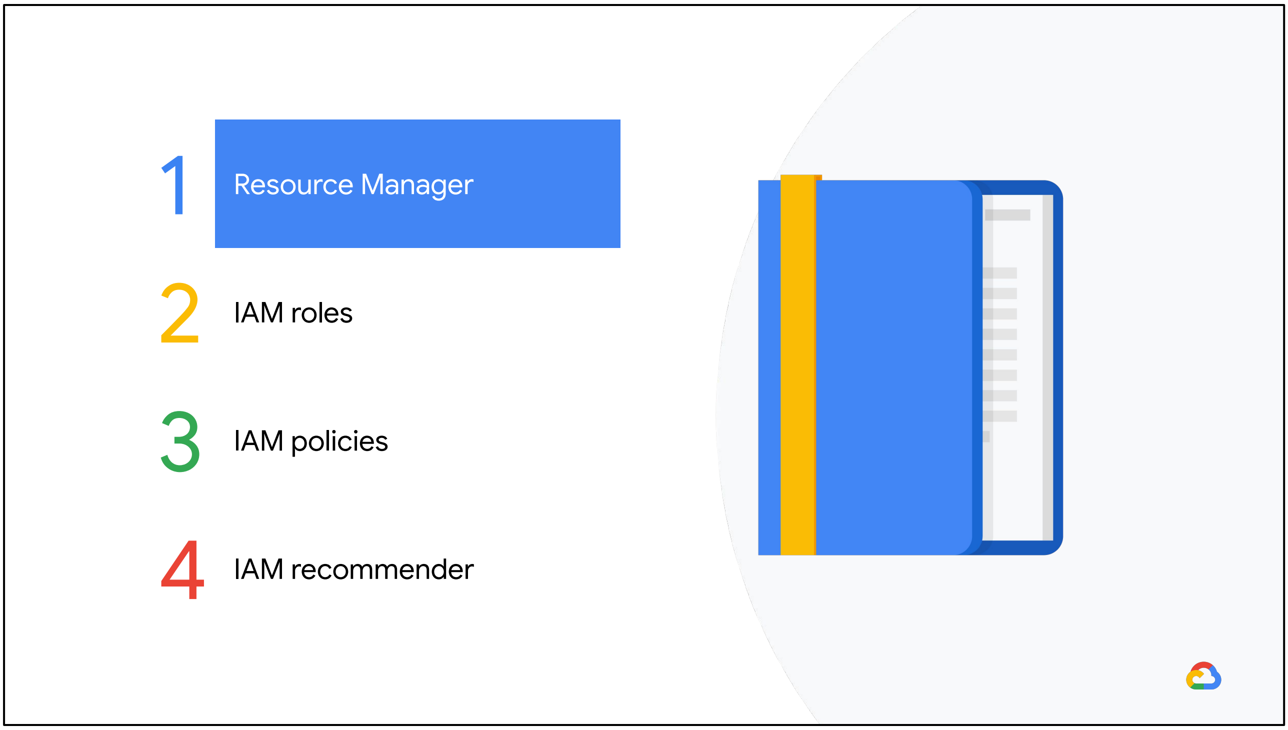
5 IAM troubleshooter

6 IAM audit logs

7 IAM best practices

And then, we will cover **IAM Troubleshooter**, and **Audit logs**, finishing with a look at **best practices**, including separation of duties and the principle of least privilege.

Let’s get started!



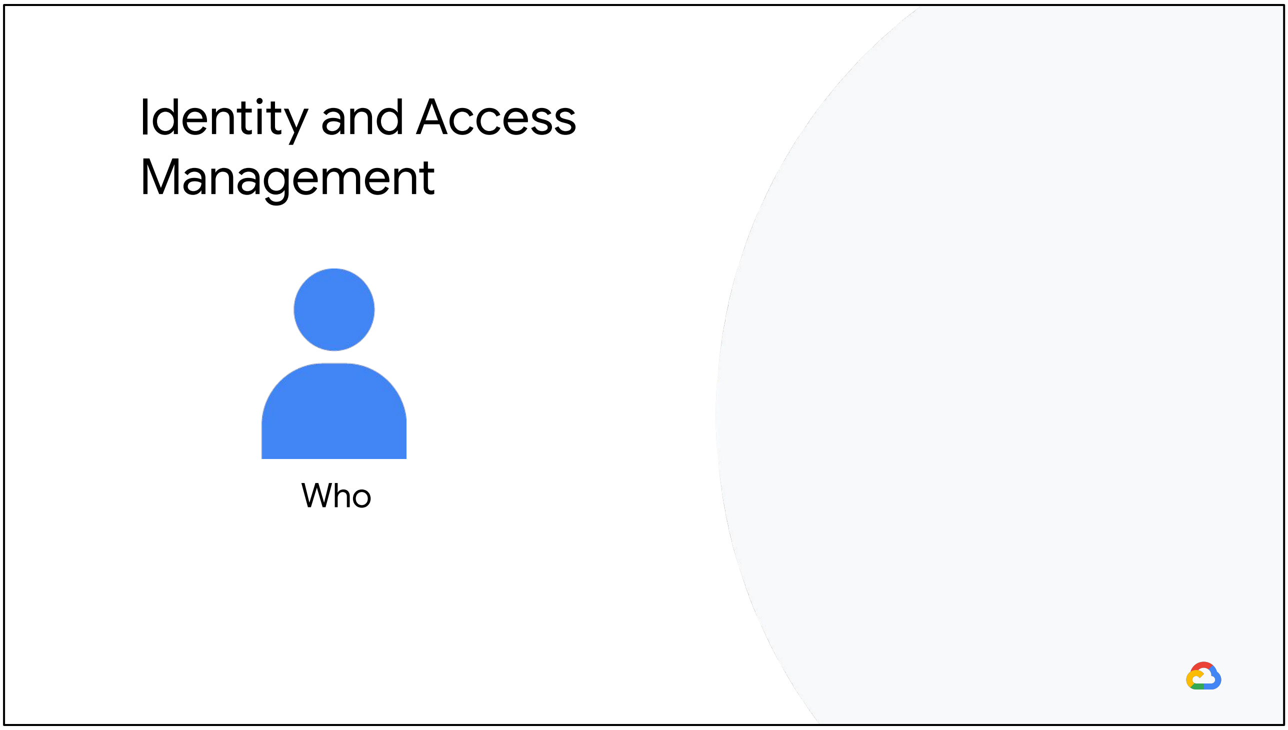
1 Resource Manager

2 IAM roles

3 IAM policies

4 IAM recommender

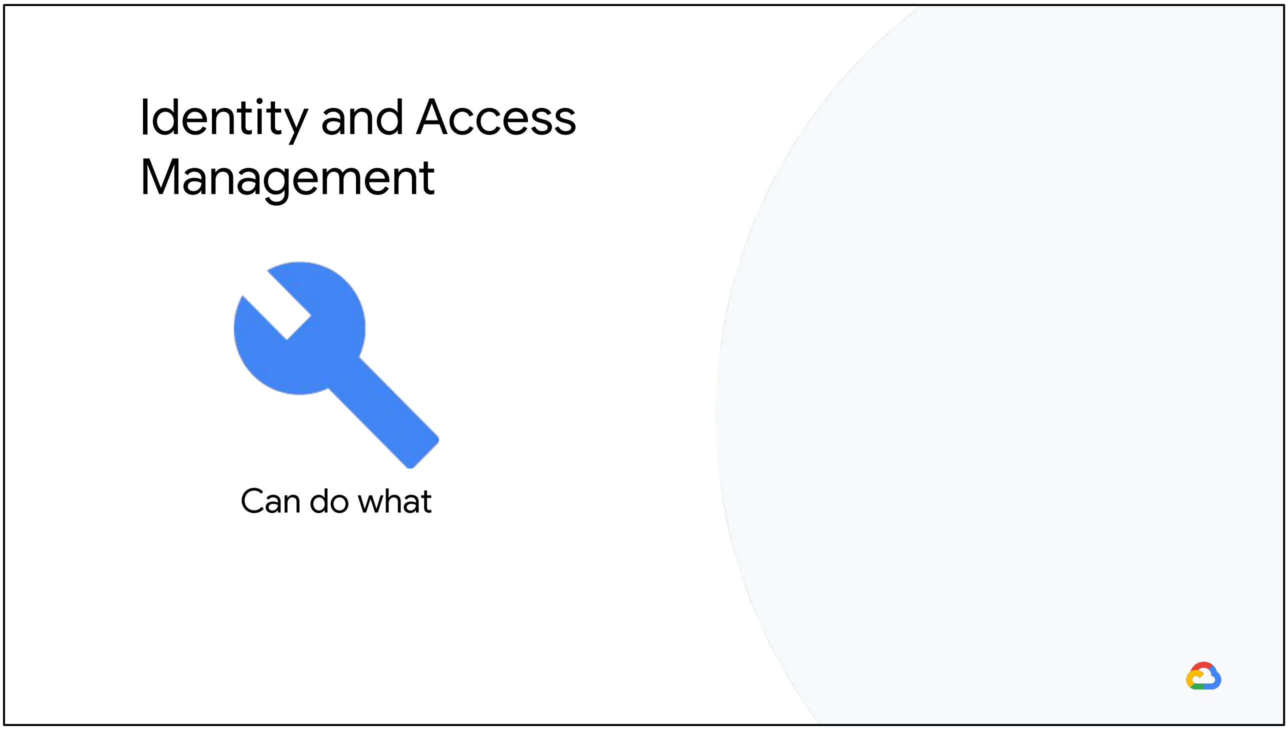
OK, let's dive into Cloud IAM and how to centrally manage your resources with the Resource Manager.



Identity and Access Management

Who

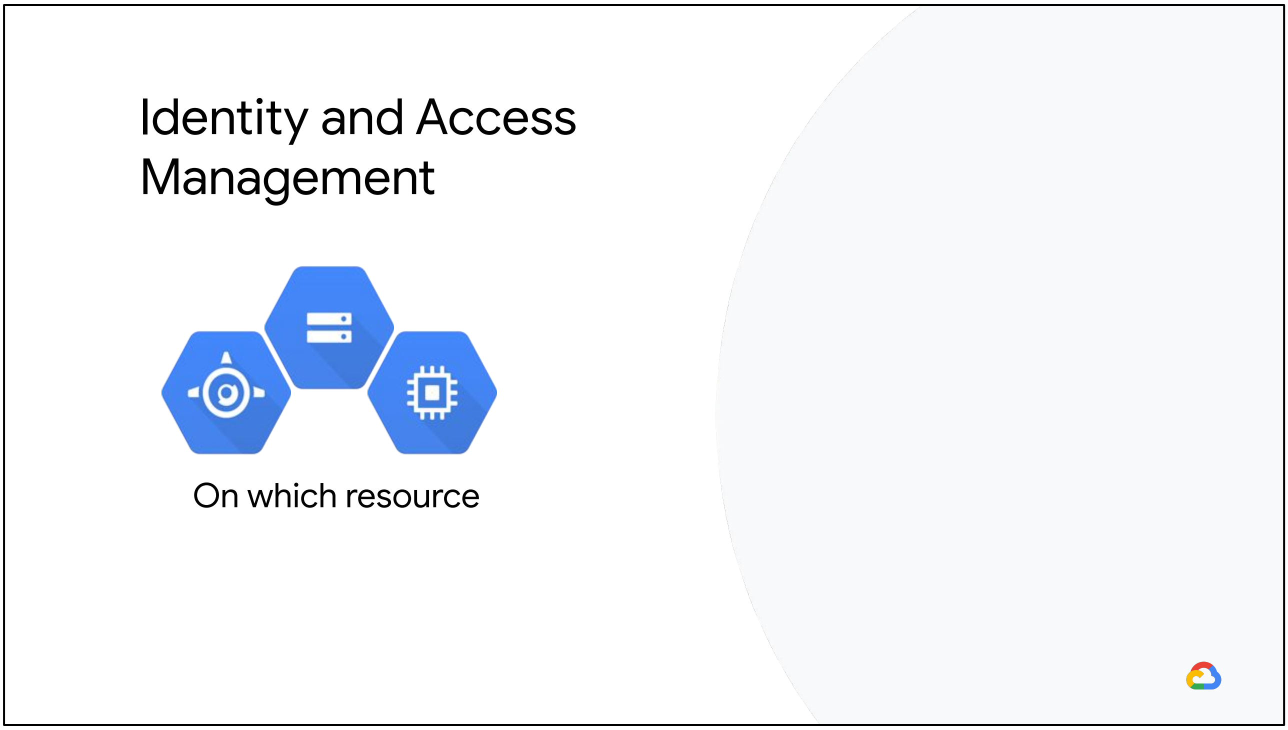
Cloud Identity and Access Management, or Cloud IAM, lets administrators authorize who



Identity and Access Management

Can do what

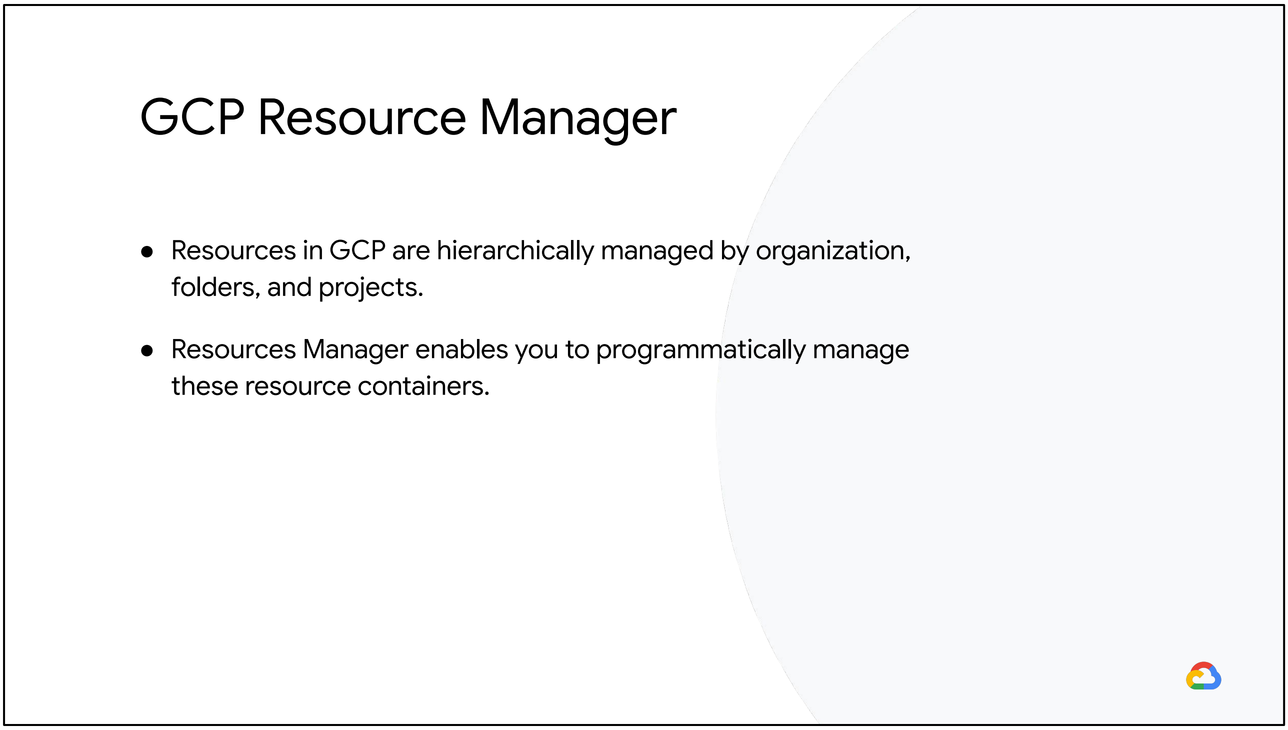
Can do what



Identity and Access Management

On which resource

On which resources in GCP.
It provides full control and visibility to manage cloud resources centrally.

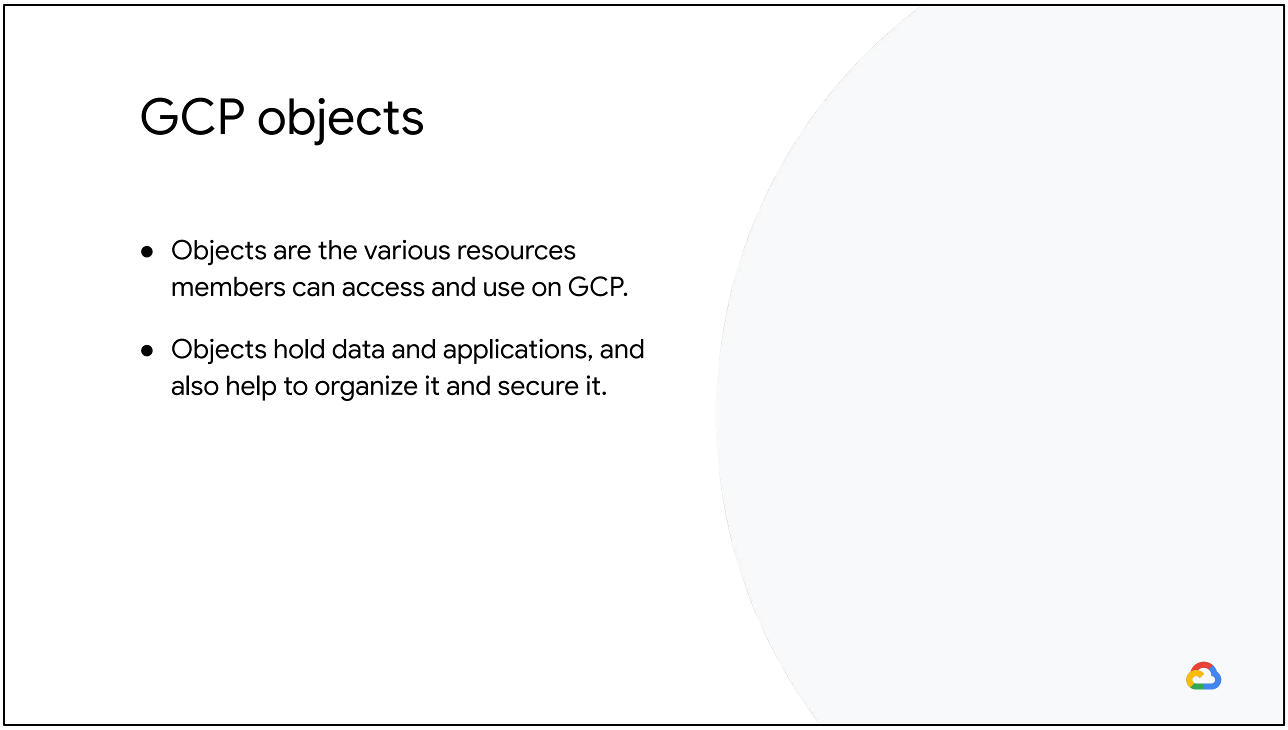


GCP Resource Manager

- Resources in GCP are hierarchically managed by organization, folders, and projects.
- Resources Manager enables you to programmatically manage these resource containers.

Google Cloud Platform provides resource containers such as Organizations, Folders, and Projects, which allow you to group and hierarchically organize cloud resources. This hierarchical organization lets you easily manage common aspects of your resources, like access control and configuration settings.

The Resource Manager enables you to programmatically manage these resource containers.

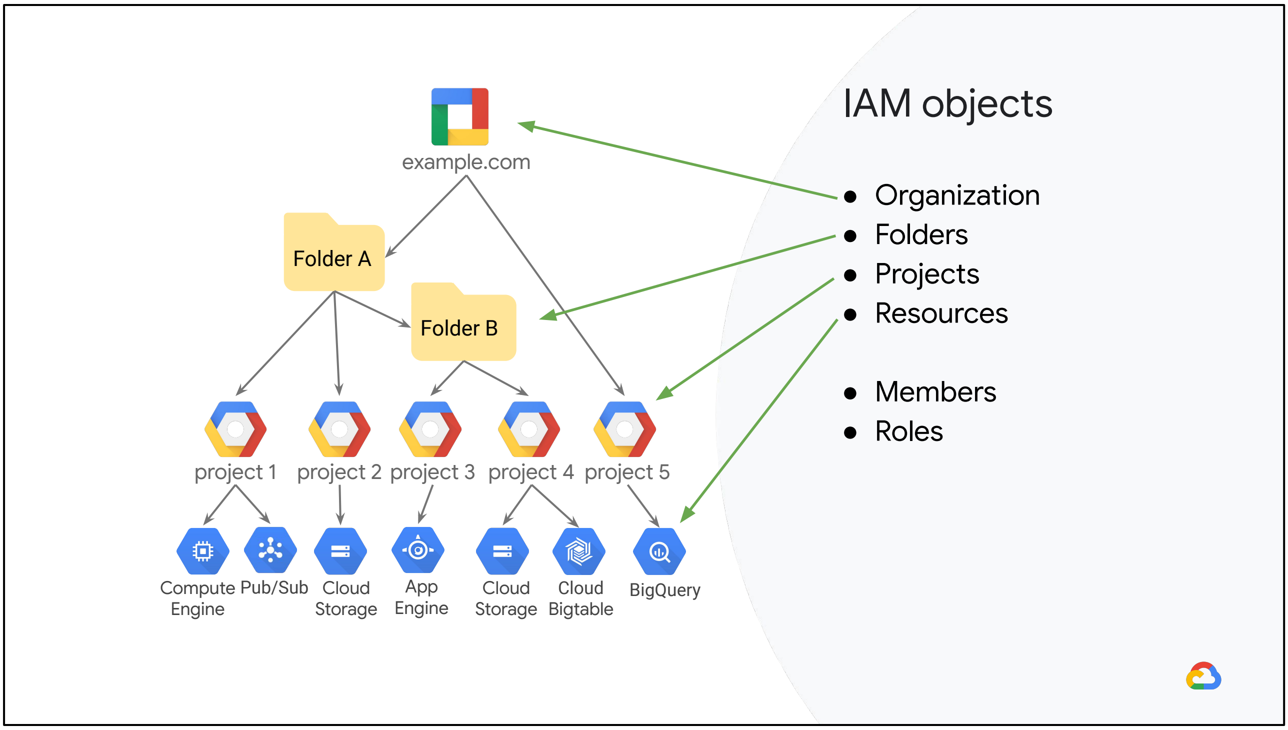


GCP objects

- Objects are the various resources members can access and use on GCP.
- Objects hold data and applications, and also help to organize it and secure it.

There are several objects that are important when discussing Cloud IAM in GCP.
These objects are:

- Organization
- Folders
- Projects
- Resources
- Members and
- Roles

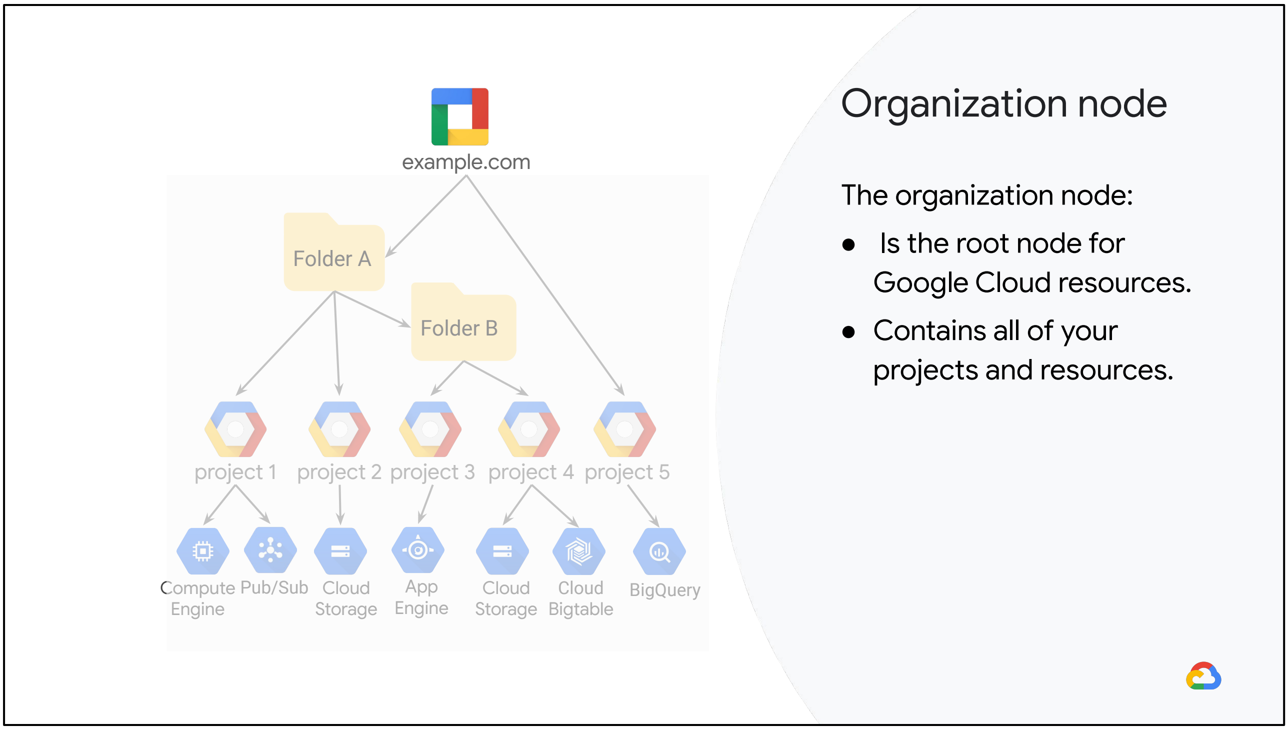


IAM objects

- Organization
- Folders
- Projects
- Resources

- Members
- Roles

These objects together form a resource hierarchy that can be managed using the Resource Manager.
This GCP resource hierarchy allows you to map your organization onto appropriate GCP objects and presents logical attach points for access management policies.



example.com

Folder A

Folder B

project 1 project 2 project 3 project 4 project 5

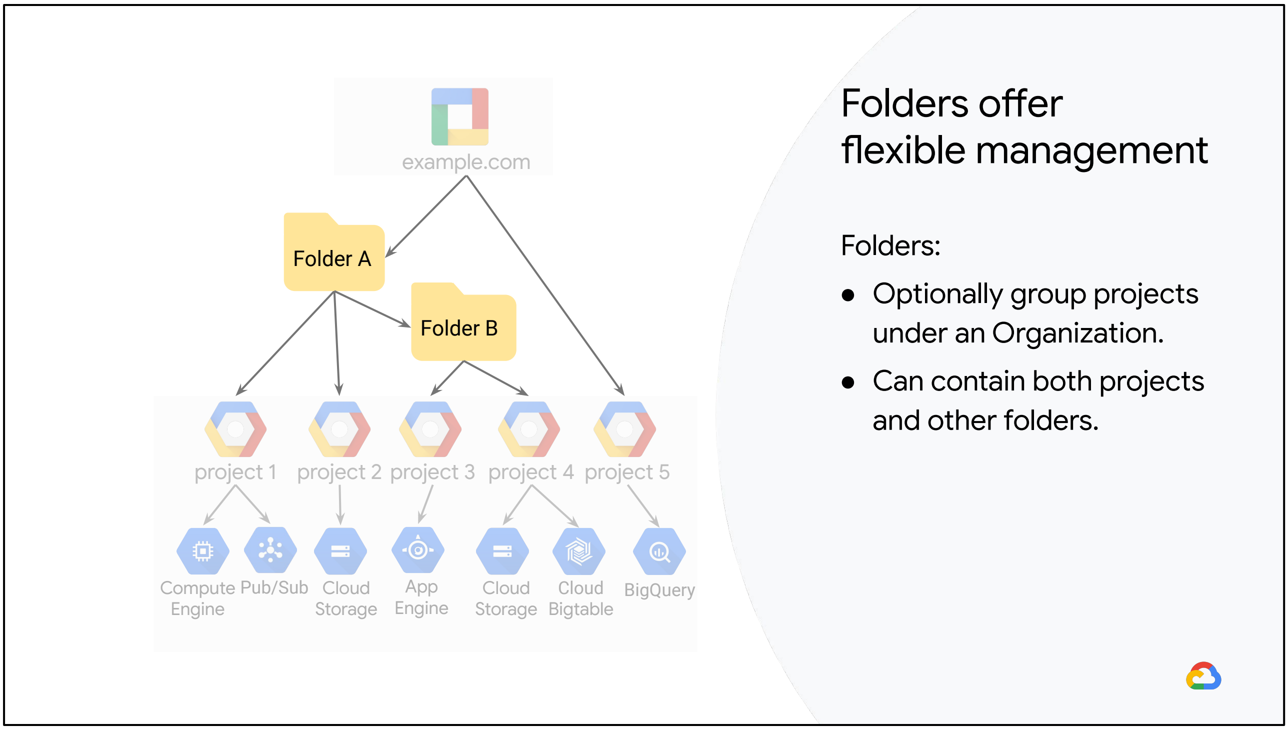
Compute Engine Pub/Sub Cloud Storage App Engine Cloud Storage Cloud Bigtable BigQuery

Organization node

The organization node:

- Is the root node for Google Cloud resources.
- Contains all of your projects and resources.

The organization node is the root node for Google Cloud resource hierarchy. It is the “super node” for all of your projects and resources and represents your organization.

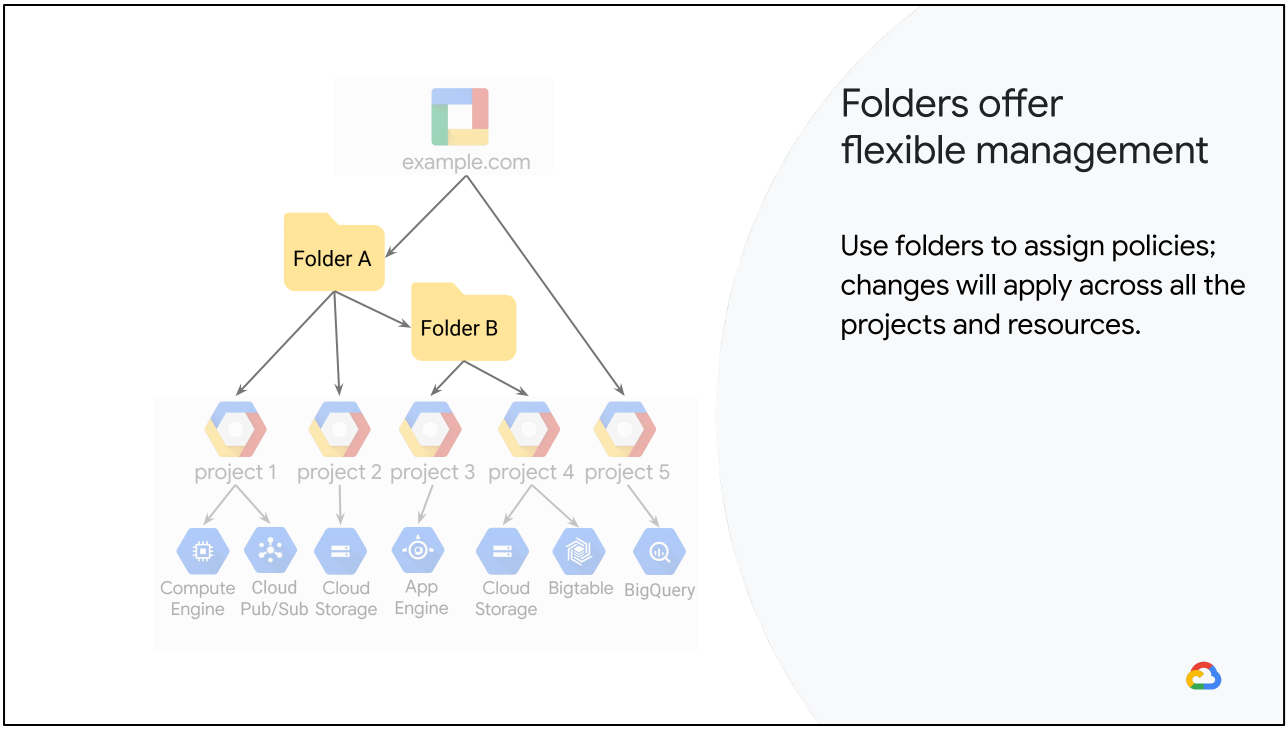


Folders offer flexible management

Folders:

- Optionally group projects under an Organization.
- Can contain both projects and other folders.

Folders can be used to implement organizational structure and/or group projects by department, team, application or environment.
A folder can contain projects, other folders, or a combination of both.
Organizations can use folders to group projects under the organization node in a hierarchy.
For example, your organization might contain multiple departments, each with its own set of GCP resources.
Folders allow you to group these resources on a per-department basis.
While a folder can contain multiple child folders or other resources, each folder or resource can only have exactly **one** parent.



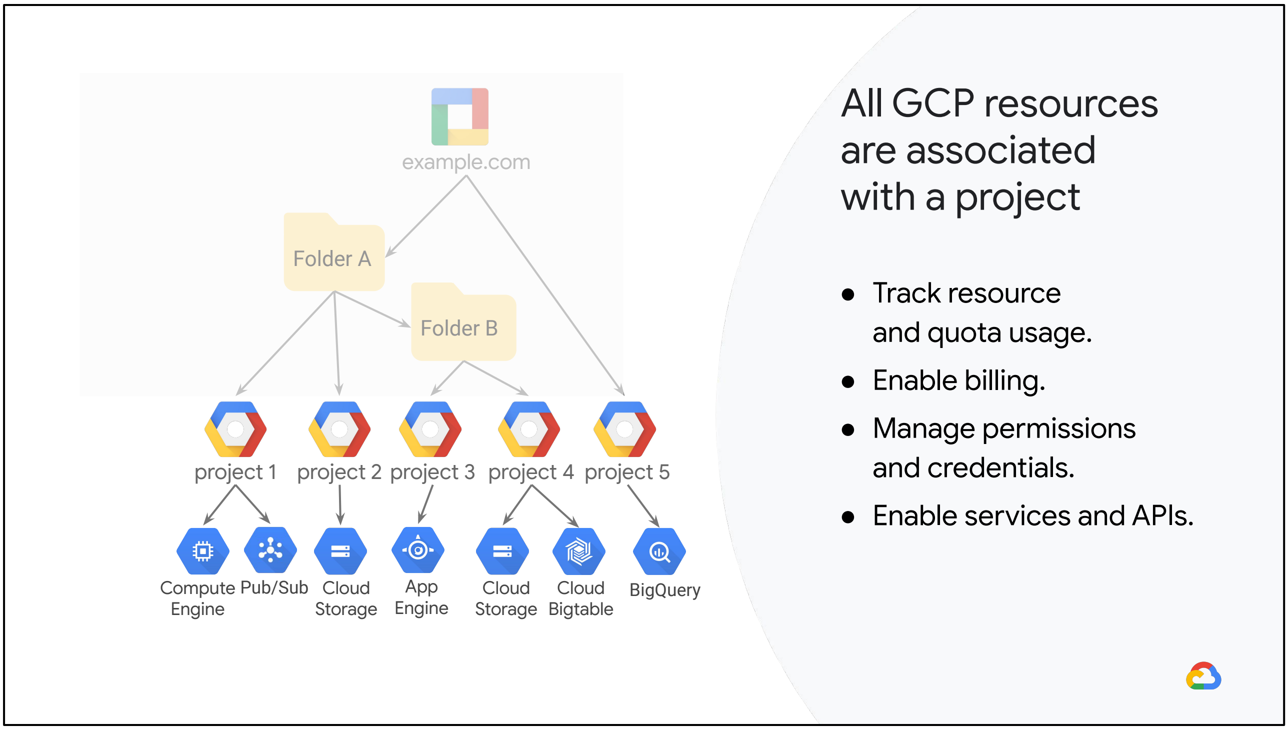
Folders offer flexible management

Use folders to assign policies; changes will apply across all the projects and resources.

Folders are used to group resources that share common IAM policies. You can use folder-level IAM policies to control access to the resources the folder contains.

For example, if a user is granted the Compute Instance Admin role on a folder, that user has the Compute Instance Admin role for all of the projects in the folder.

It is important to note that the use of folders to organize resources is optional.



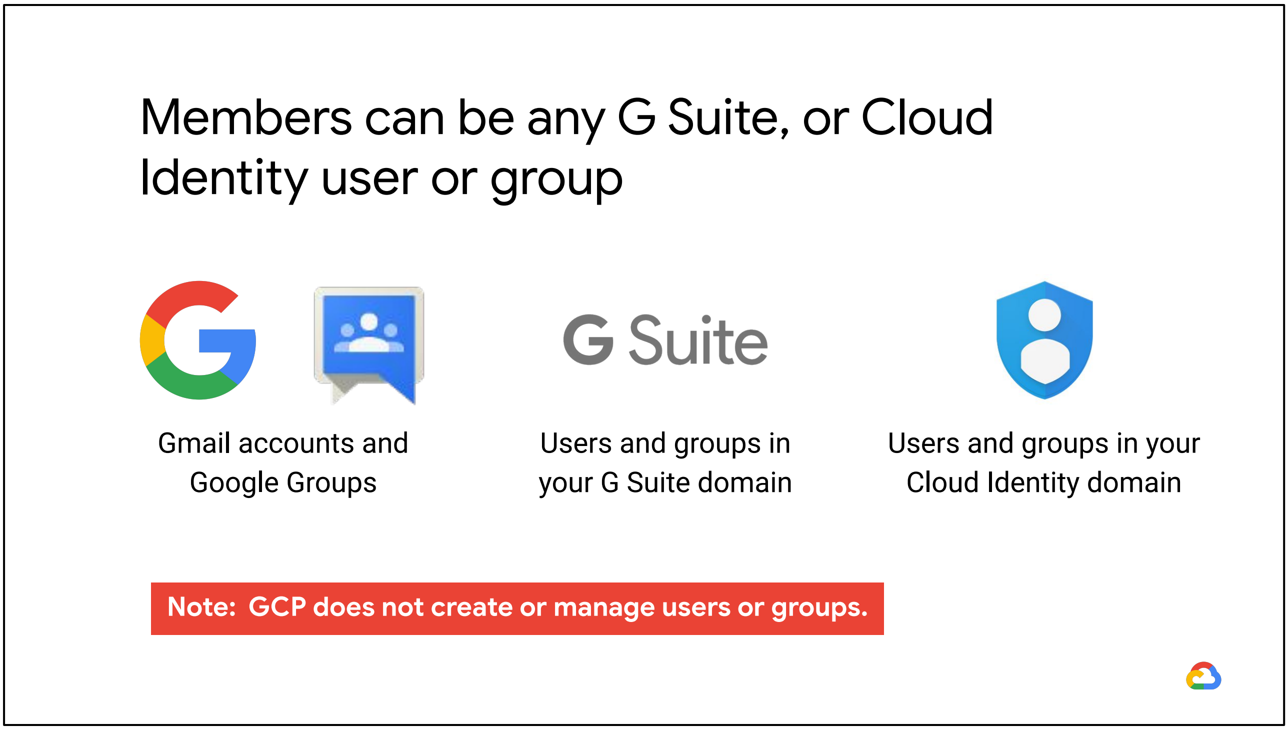
All GCP resources are associated with a project

- Track resource and quota usage.
- Enable billing.
- Manage permissions and credentials.
- Enable services and APIs.

Projects, however, are required in GCP and any resource that is deployed must be associated with a project.

Projects provide many management-related features, such as the ability to:

- Track resource and quota usage.
- Assign projects to different billing accounts.
- Assign manager permissions and credentials and selectively enable specific services and APIs at the project level.



Members can be any G Suite, or Cloud Identity user or group

Gmail accounts and Google Groups

Users and groups in your G Suite domain

Users and groups in your Cloud Identity domain

Note: GCP does not create or manage users or groups.

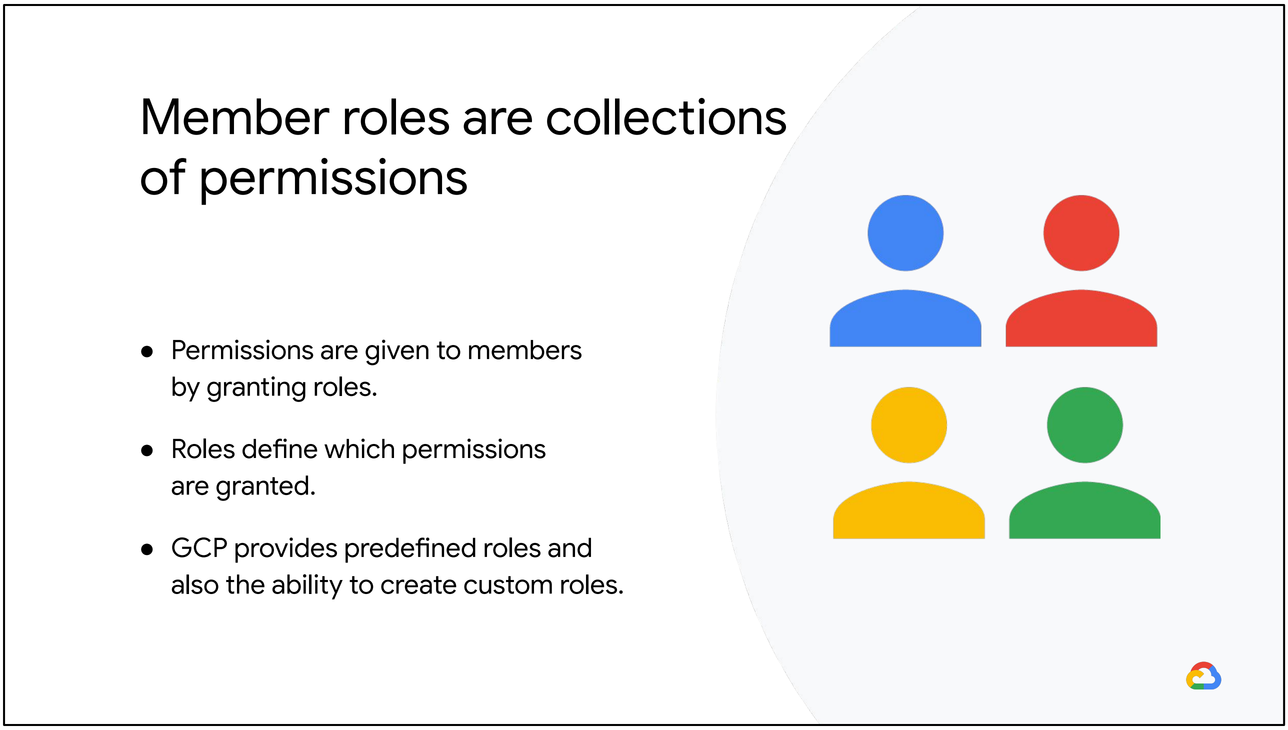
Many new GCP customers get started by logging into the GCP console with a Gmail account.

Gmail accounts and Google groups are often the easiest to get started, but they offer no centralized way manage these users.

GCP customers who are also G Suite customers can define GCP policies in terms of G Suite users and groups. This way, when someone leaves your organization, an administrator can immediately disable their account and remove them from groups using the Google Admin Console.

GCP customers who are not G Suite customers can get these same capabilities through Cloud Identity. Cloud Identity lets you manage users and groups using the Google Admin Console, but you do not pay for or receive G Suite’s collaboration products such as Gmail, Docs, Drive, and Calendar. Cloud Identity is available in both a free and a premium edition.

The premium edition adds capabilities for mobile device management.

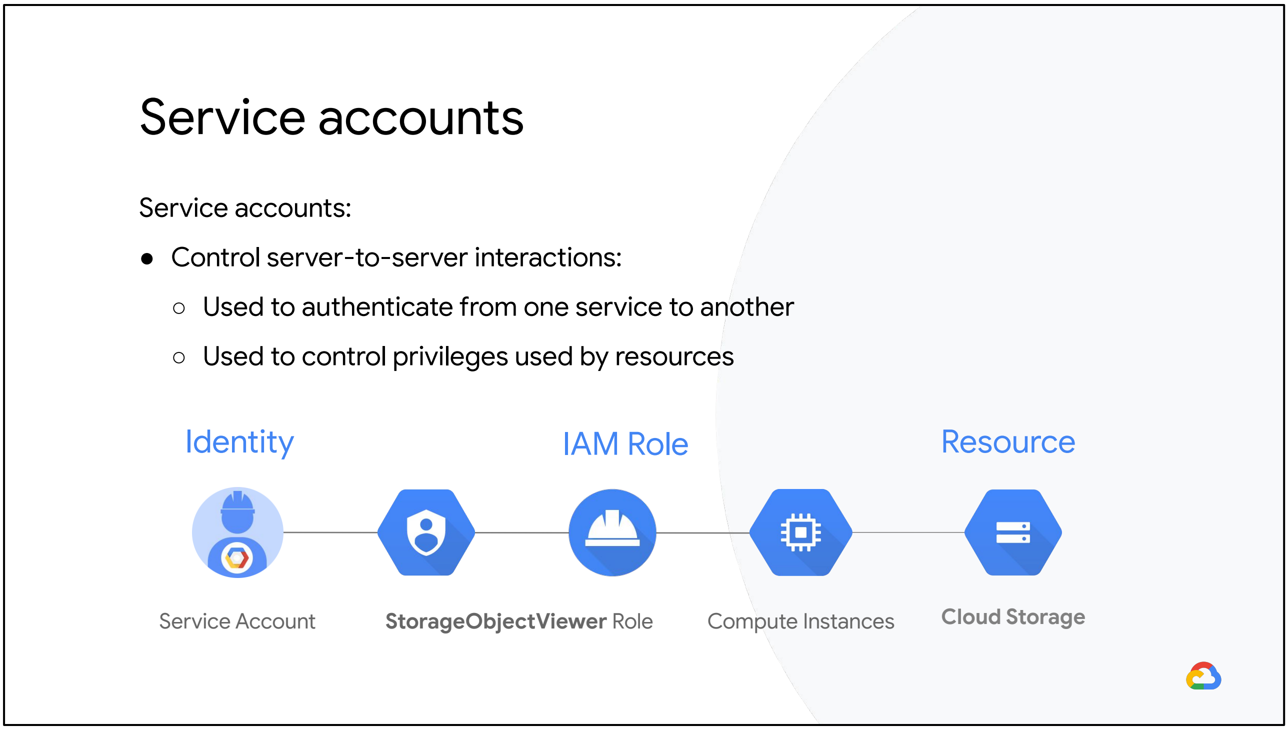


Member roles are collections of permissions

- Permissions are given to members by granting roles.
- Roles define which permissions are granted.
- GCP provides predefined roles and also the ability to create custom roles.

As you already know, a role is a collection of permissions. You cannot assign a permission to the user directly; instead you grant them a role.

Members can be individual users, groups, domains, or even the public as a whole. When you add a new project member to your project, you can assign Cloud IAM roles to the new member using Cloud IAM policies.



Service accounts

Service accounts:

- Control server-to-server interactions:
  - Used to authenticate from one service to another
  - Used to control privileges used by resources

Identity

IAM Role

Resource

Service Account

StorageObjectViewer Role

Compute Instances

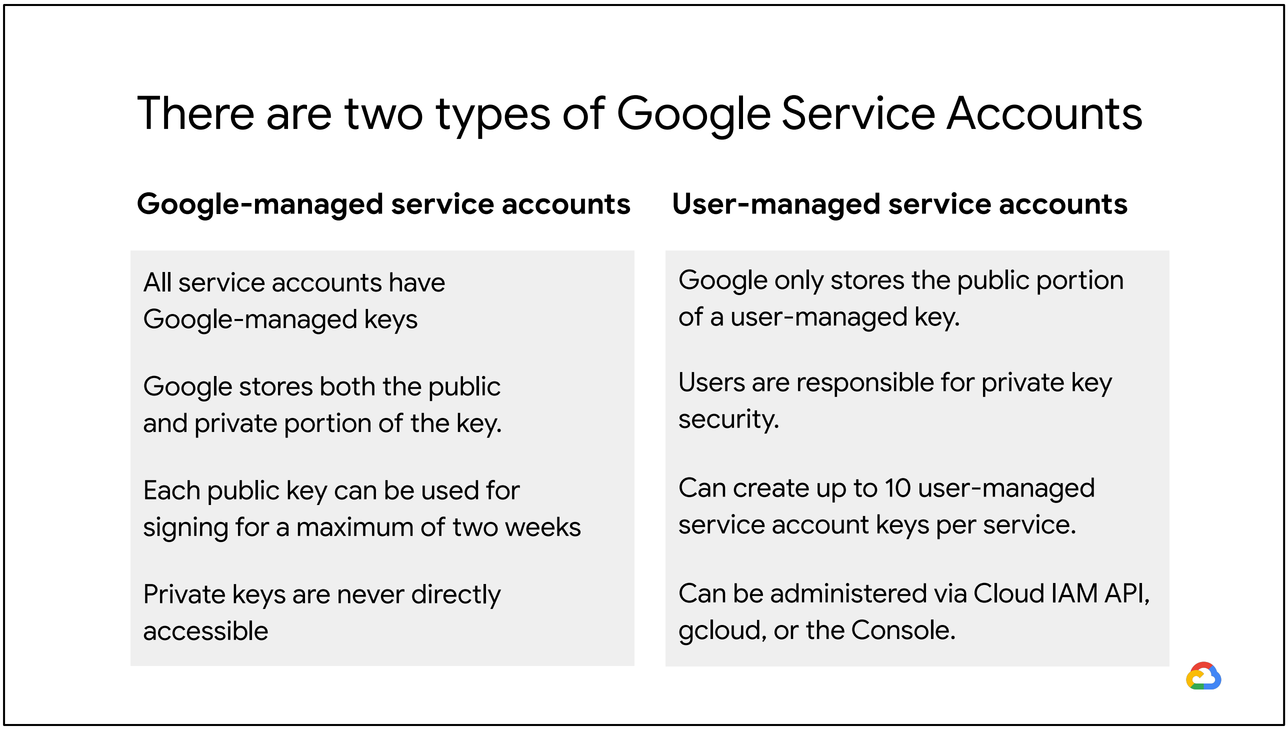
Cloud Storage

In addition to the members already mentioned, you can also grant roles to service accounts.

Service Accounts control server-to-server interactions and are used to authenticate from one service to another and control what actions applications running on a service can perform.
For example, if an application running on a compute engine instance needs to read a file from cloud storage, a service account with cloud storage object viewer role can be assigned to the compute engine instance.

An application running on that instance would then be permitted to read a file from cloud storage.

Service accounts are identified with a Google-managed email address in the gserviceaccount.com domain.



There are two types of Google Service Accounts

Google-managed service accounts

All service accounts have Google-managed keys

Google stores both the public and private portion of the key.

Each public key can be used for signing for a maximum of two weeks

Private keys are never directly accessible

User-managed service accounts

Google only stores the public portion of a user-managed key.

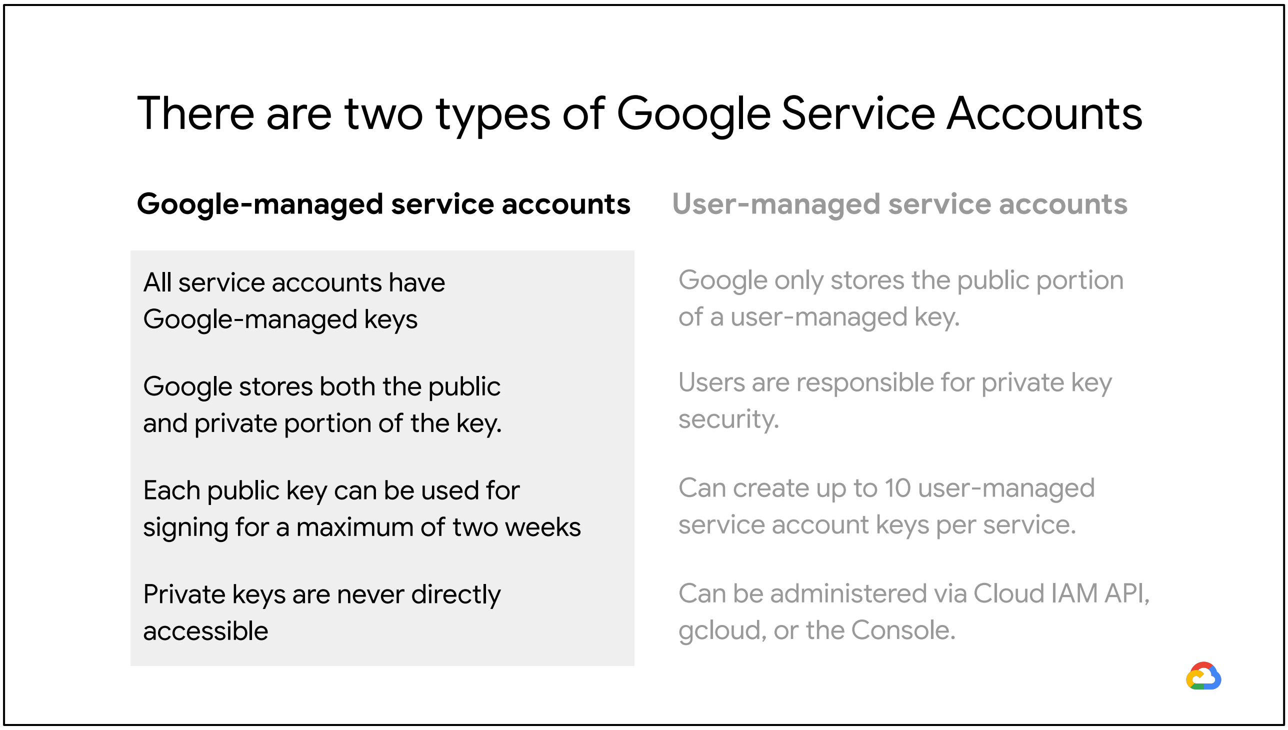
Users are responsible for private key security.

Can create up to 10 user-managed service account keys per service.

Can be administered via Cloud IAM API, gcloud, or the Console.

There are two types of Google Service Accounts.

By default, when using service accounts within Google Cloud (for example, from Compute Engine or App Engine) Google automatically manages the keys for service accounts. However, if you want to be able to use service accounts outside of Google Cloud, or want a different rotation period, it is possible to also manually create and manage your own service account keys.



There are two types of Google Service Accounts

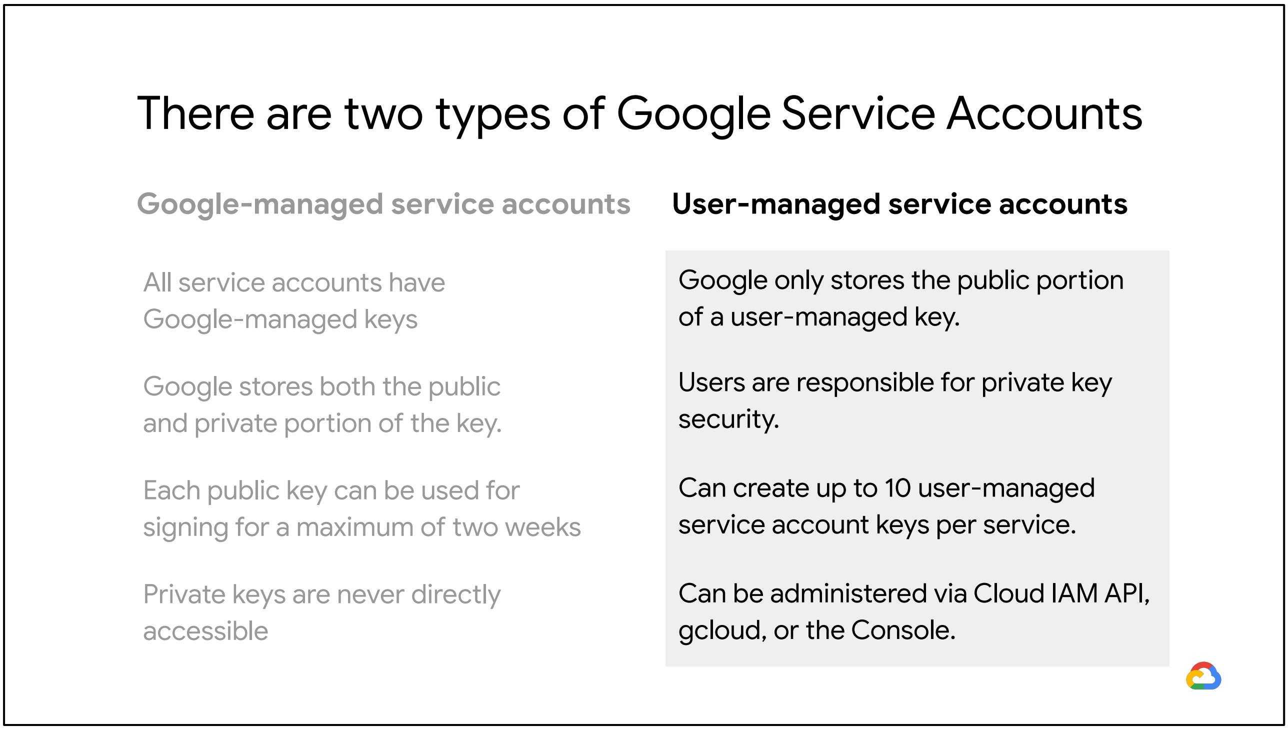
Google-managed service accounts	User-managed service accounts
All service accounts have Google-managed keys	Google only stores the public portion of a user-managed key.
Google stores both the public and private portion of the key.	Users are responsible for private key security.
Each public key can be used for signing for a maximum of two weeks	Can create up to 10 user-managed service account keys per service.
Private keys are never directly accessible	Can be administered via Cloud IAM API, gcloud, or the Console.

All service accounts have Google-managed key-pairs.

With Google-managed service account keys, Google stores both the public and private portion of the key, and rotates them regularly.

Each public key can be used for signing for a maximum of two weeks.

Your private key is always held securely in escrow and is never directly accessible.



There are two types of Google Service Accounts

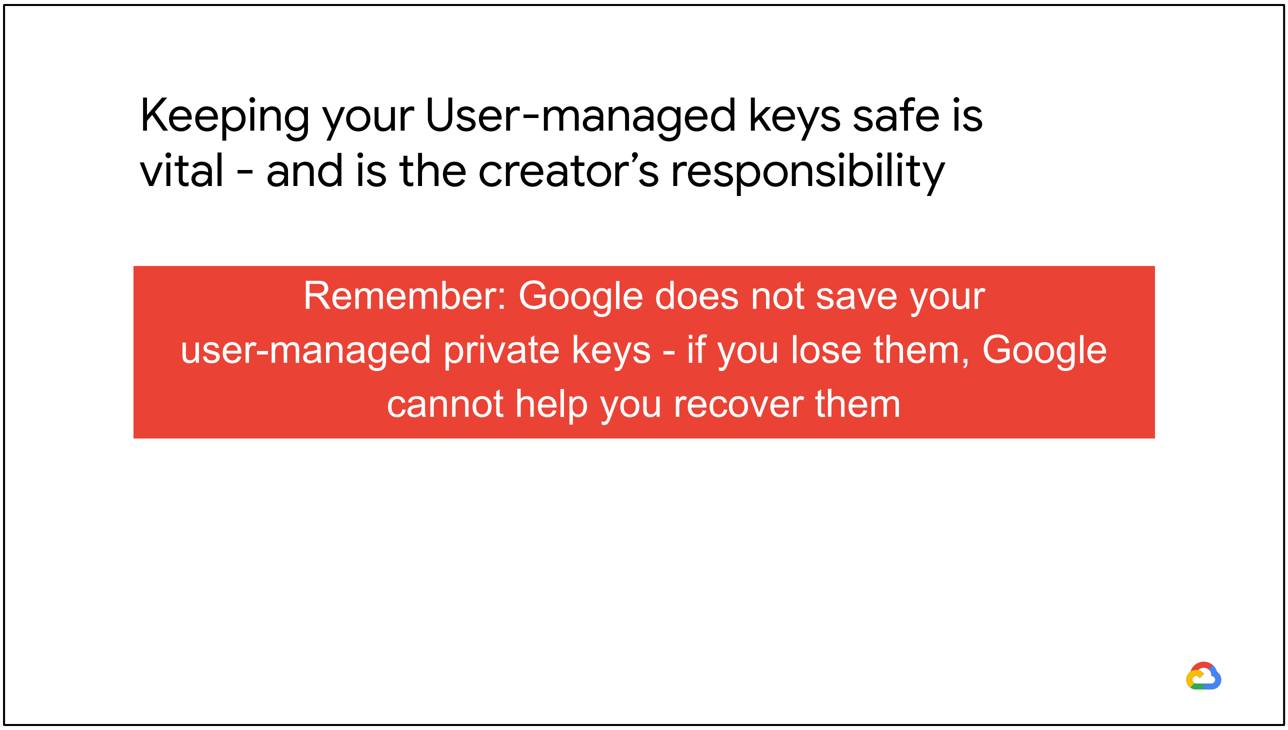
Google-managed service accounts	User-managed service accounts
All service accounts have Google-managed keys	Google only stores the public portion of a user-managed key.
Google stores both the public and private portion of the key.	Users are responsible for private key security.
Each public key can be used for signing for a maximum of two weeks	Can create up to 10 user-managed service account keys per service.
Private keys are never directly accessible	Can be administered via Cloud IAM API, gcloud, or the Console.

You may optionally create one or more user-managed key pairs (also known as "external" keys) that can be used from outside of Google Cloud. Google only stores the public portion of a user-managed key.

The User is responsible for security of the private key and performing other management operations such as key rotation, whether manually or programmatically.

Users can create up to 10 service account keys per service account to facilitate key rotation.

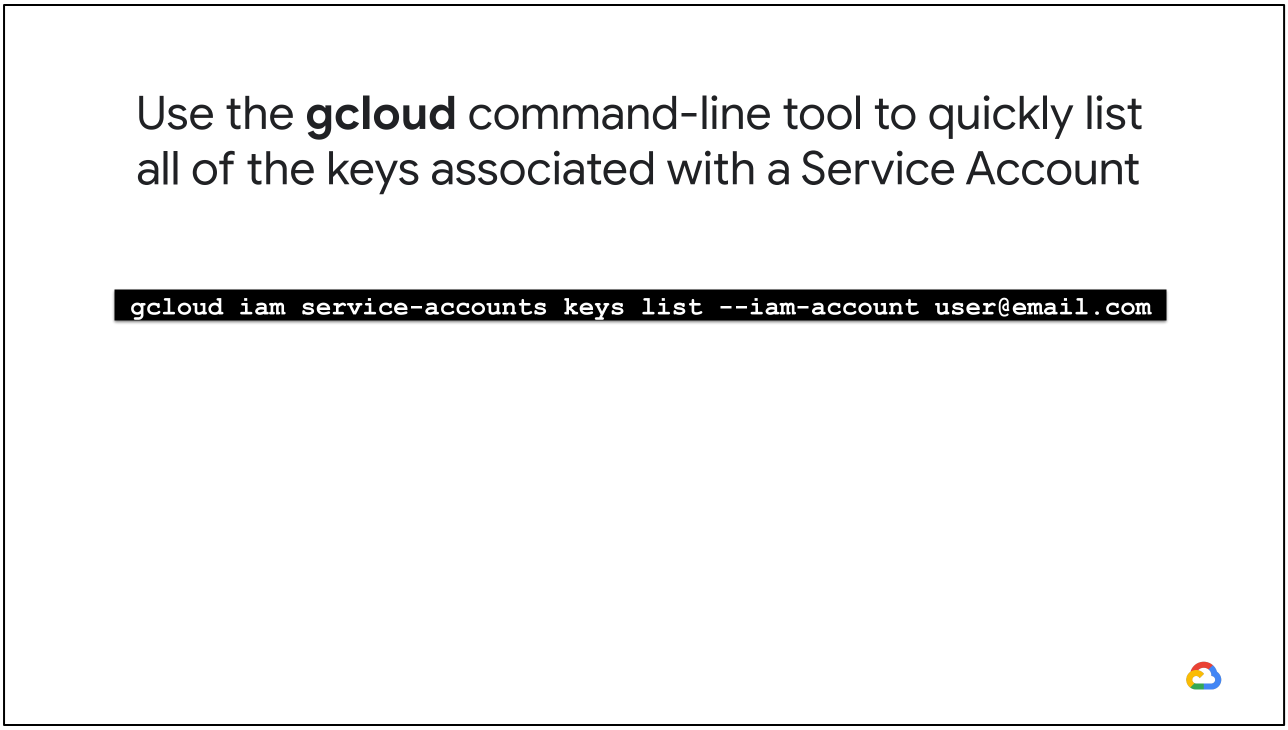
User-managed keys can be managed by using the Cloud IAM API, the `gcloud` command-line tool, or the Service Accounts page in the Cloud Console.



Keeping your User-managed keys safe is vital - and is the creator’s responsibility

Remember: Google does not save your user-managed private keys - if you lose them, Google cannot help you recover them

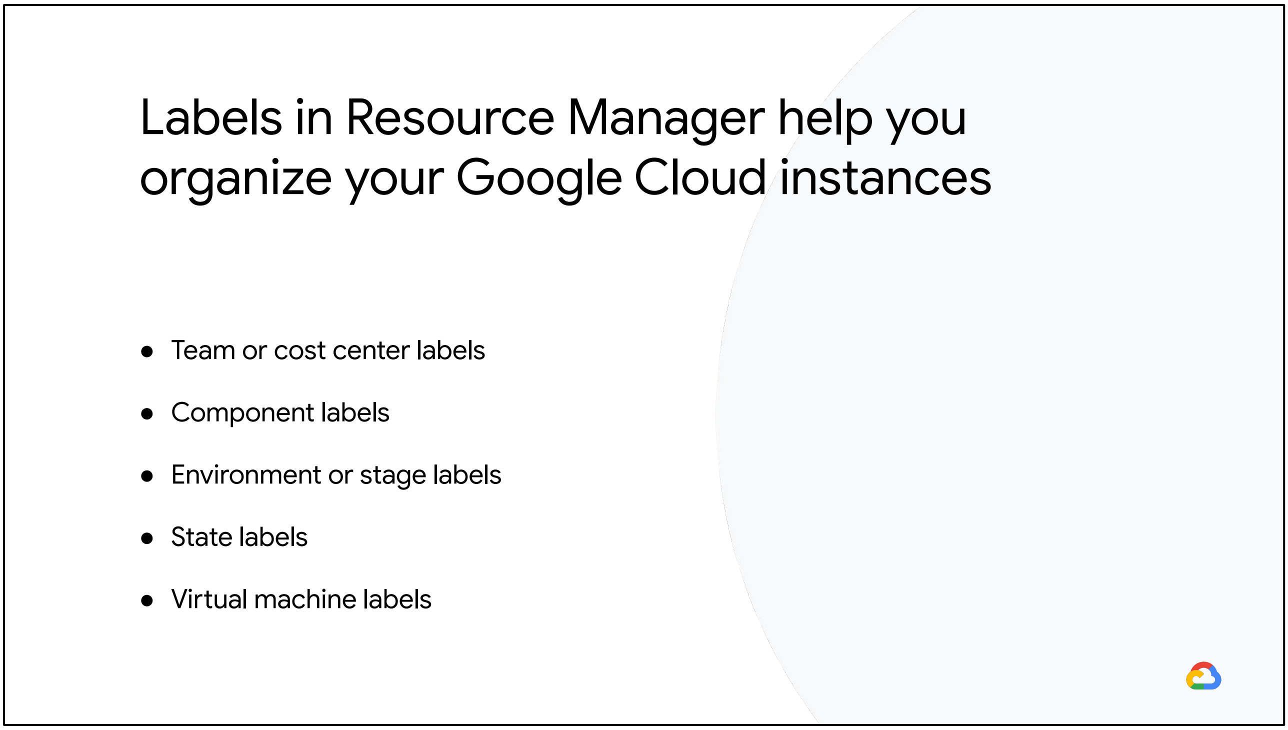
Google does not save your user-managed private keys, so if you lose them, Google cannot help you recover them.
You are responsible for keeping these keys safe and also responsible for performing key rotation.



Use the **gcloud** command-line tool to quickly list all of the keys associated with a Service Account

```
gcloud iam service-accounts keys list --iam-account user@email.com
```

The `gcloud` command line shown on this slide is a fast and easy way to list all of the keys associated with a particular service account.



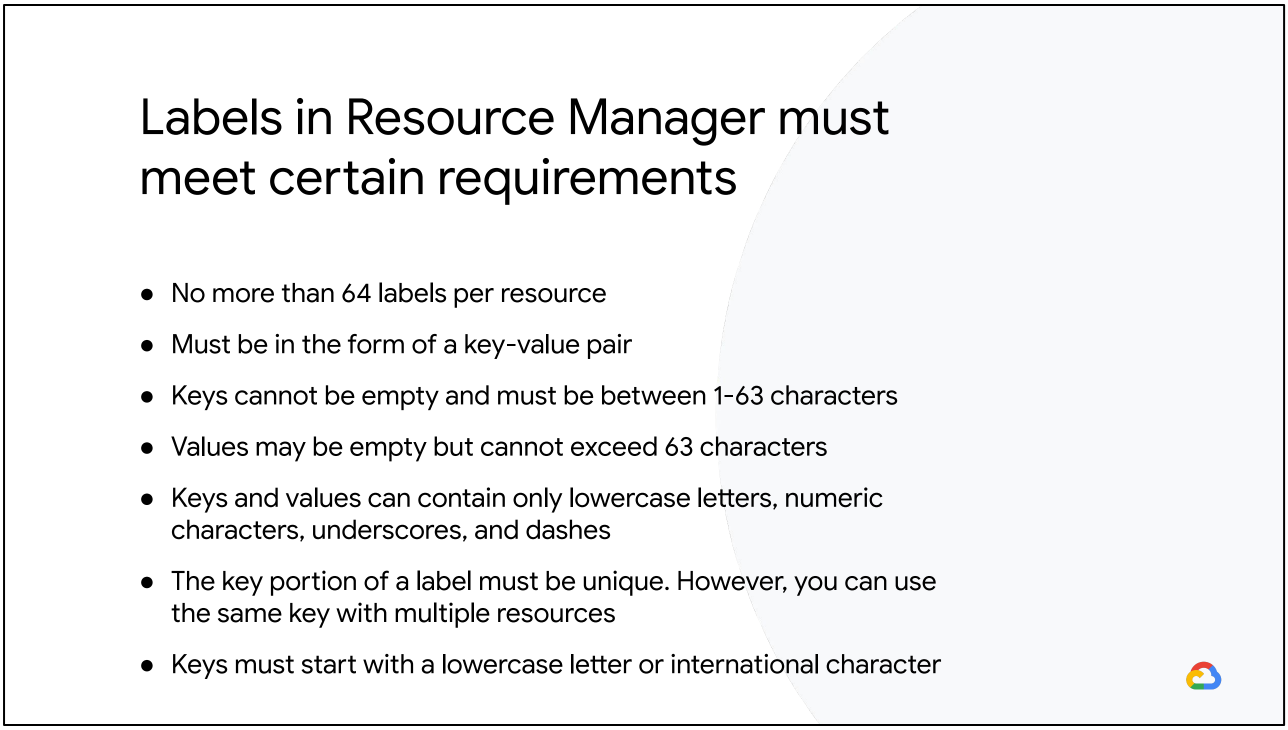
Labels in Resource Manager help you organize your Google Cloud instances

- Team or cost center labels
- Component labels
- Environment or stage labels
- State labels
- Virtual machine labels

Labels are created in the form of a “key-value” pair and are used to help you organize and manage your Cloud resources.

There are many reasons you might want to use labels:

- To distinguish between resources owned by different teams for budgeting or billing purposes (team or cost center labels)
- To label the different components of large, distributed applications, like “frontend” or “dashboard” (component labels)
- To show which systems in your network are for production use and which are for testing (environment labels)
- To indicate the “state” of an instance of a resource, for example, if it is the active instance or one that is ready to be archived (state labels)
- To distinguish between virtual machines, which may otherwise be virtually identical! (VM labels)



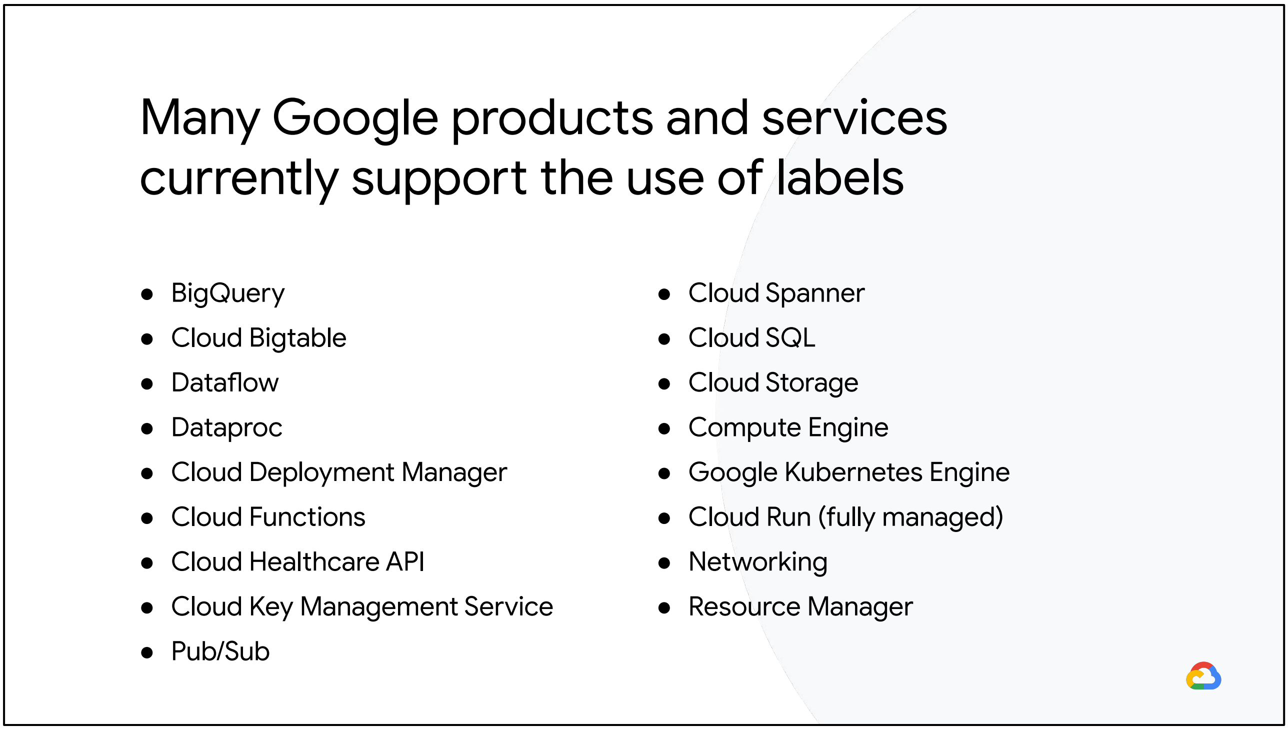
Labels in Resource Manager must meet certain requirements

- No more than 64 labels per resource
- Must be in the form of a key-value pair
- Keys cannot be empty and must be between 1-63 characters
- Values may be empty but cannot exceed 63 characters
- Keys and values can contain only lowercase letters, numeric characters, underscores, and dashes
- The key portion of a label must be unique. However, you can use the same key with multiple resources
- Keys must start with a lowercase letter or international character

As with any type of data being exchanged or used within a system, there are technical requirements for labels used for Google Cloud resources. This list covers the current requirements for label names and values.

Remember that when planning your labels is to be sure you do not include sensitive information in the label's name or values. This includes any information that may be personally identifiable, such as a person's name, their title, or employee number.

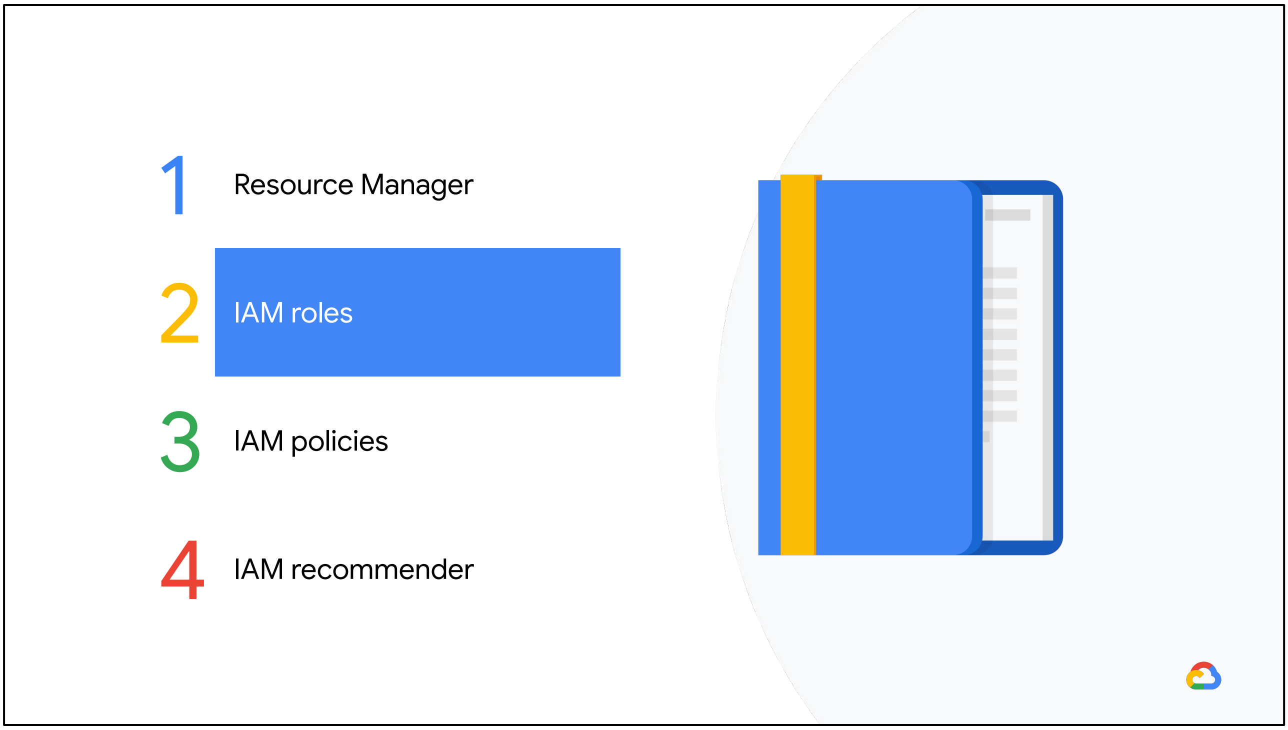
Labels are not designed to hold sensitive information, and doing so may pose a security risk to your data.



Many Google products and services currently support the use of labels

- BigQuery
- Cloud Bigtable
- Dataflow
- Dataproc
- Cloud Deployment Manager
- Cloud Functions
- Cloud Healthcare API
- Cloud Key Management Service
- Pub/Sub
- Cloud Spanner
- Cloud SQL
- Cloud Storage
- Compute Engine
- Google Kubernetes Engine
- Cloud Run (fully managed)
- Networking
- Resource Manager

The current list of products that support labels can be found in the documentation for Resource Manager.



1 Resource Manager

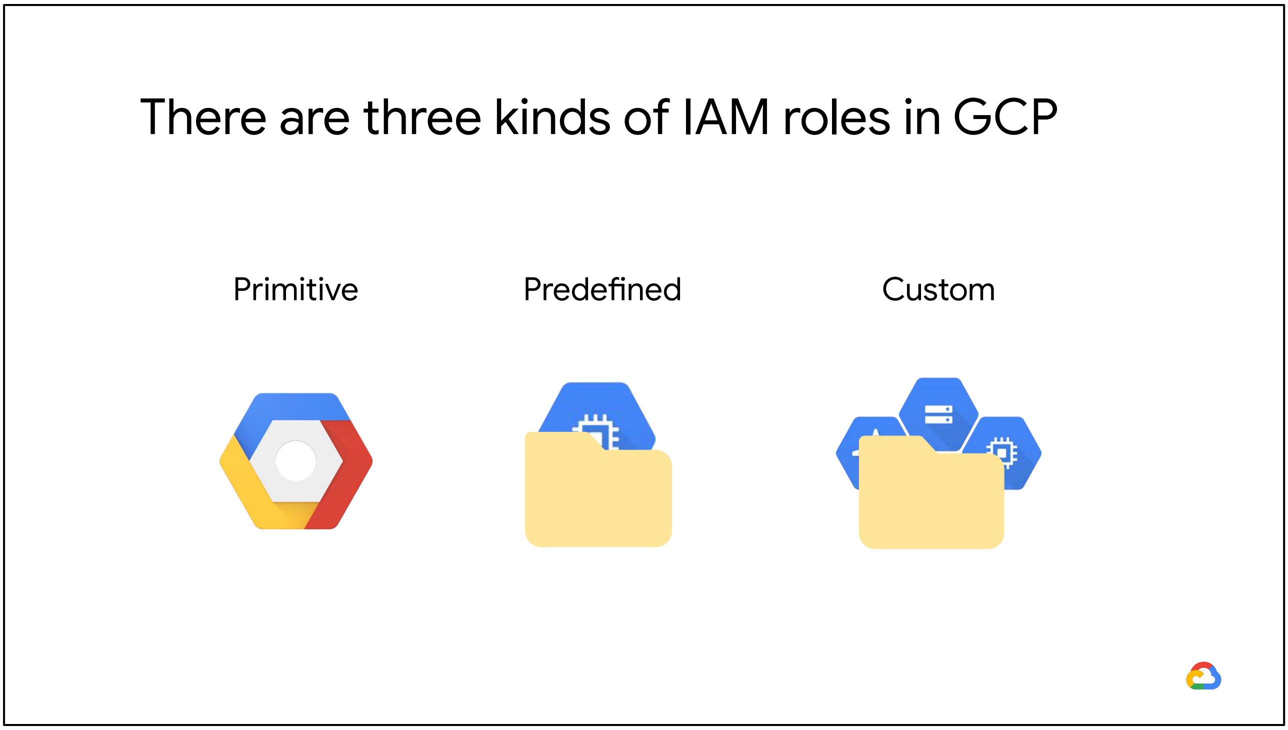
2 IAM roles

3 IAM policies

4 IAM recommender

In Google Cloud, you can grant permissions by granting **roles**.

In this section we will first review, and then take a more in-depth look at the different types of roles.



There are three kinds of IAM roles in GCP

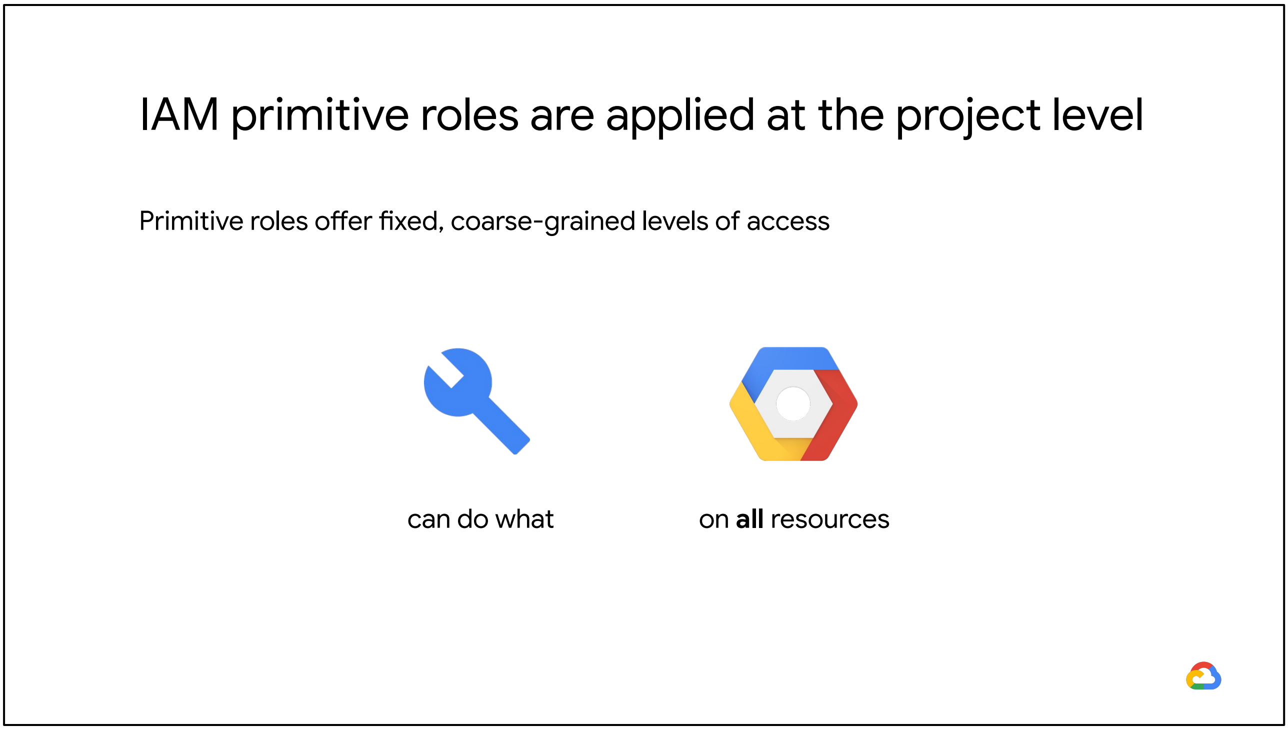
Primitive

Predefined

Custom

There are three kinds of roles in Cloud IAM:

- *Primitive roles*: The roles that have been historically available in the Cloud Console. These roles existed prior to the introduction of Cloud IAM.
- *Predefined roles*: Also sometimes called “curated roles,” are the IAM roles that give finer-grained access control than the primitive roles. Each GCP service offers a set of predefined roles.
- *Custom roles*: You can define roles consisting of permissions and resources of your choice.



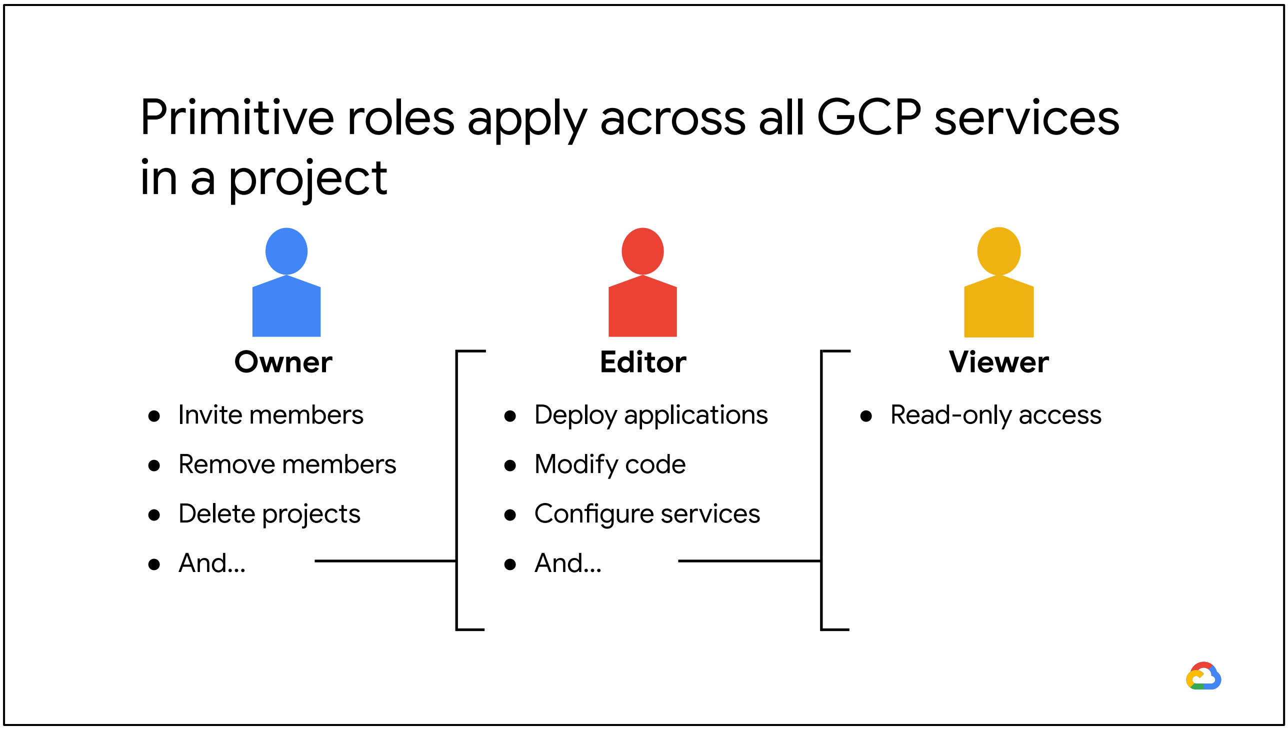
IAM primitive roles are applied at the project level

Primitive roles offer fixed, coarse-grained levels of access

can do what

on **all** resources

The IAM primitive roles are applied at the project or service resource levels and control access to **all** resources in that project or resource.
The level of access these provide is very coarse-grained and that is why they are called primitive roles.
They control what can be done on all resources in a project.



Primitive roles apply across all GCP services in a project

Owner

- Invite members
- Remove members
- Delete projects
- And...

Editor

- Deploy applications
- Modify code
- Configure services
- And...

Viewer

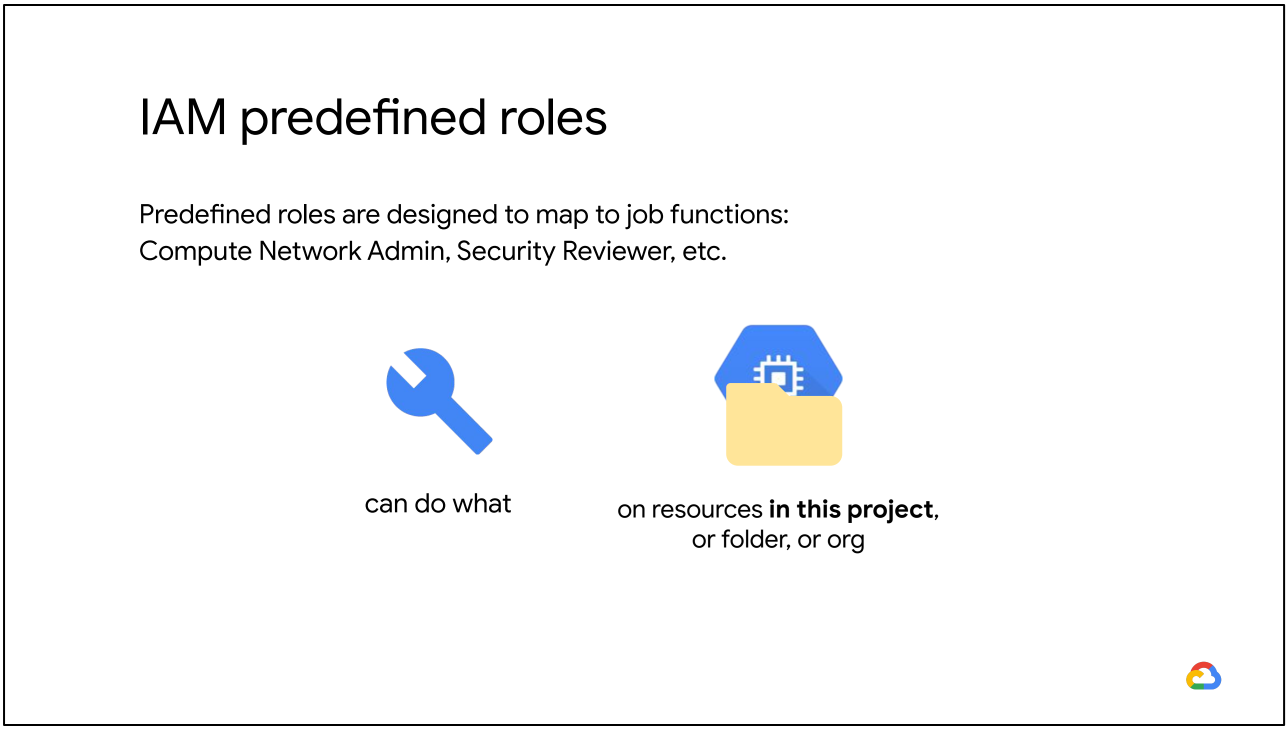
- Read-only access

There are three primitive roles: Owner, Editor, and Viewer. These roles are concentric; that is, the Owner role includes the permissions in the Editor role, and the Editor role includes the permissions in the Viewer role.

The viewer role, as its name implies, provides view or read-only access to a project and all its resources.

The editor role provides the ability to modify or edit all resources in the project, as well as all the read-only access from the viewer role.

The owner role provides the ability to manage the project itself, such as deleting the project, and adding or removing other members to the project, as well as all the editor role permissions plus the read-only access from the viewer role.



IAM predefined roles

Predefined roles are designed to map to job functions:
Compute Network Admin, Security Reviewer, etc.

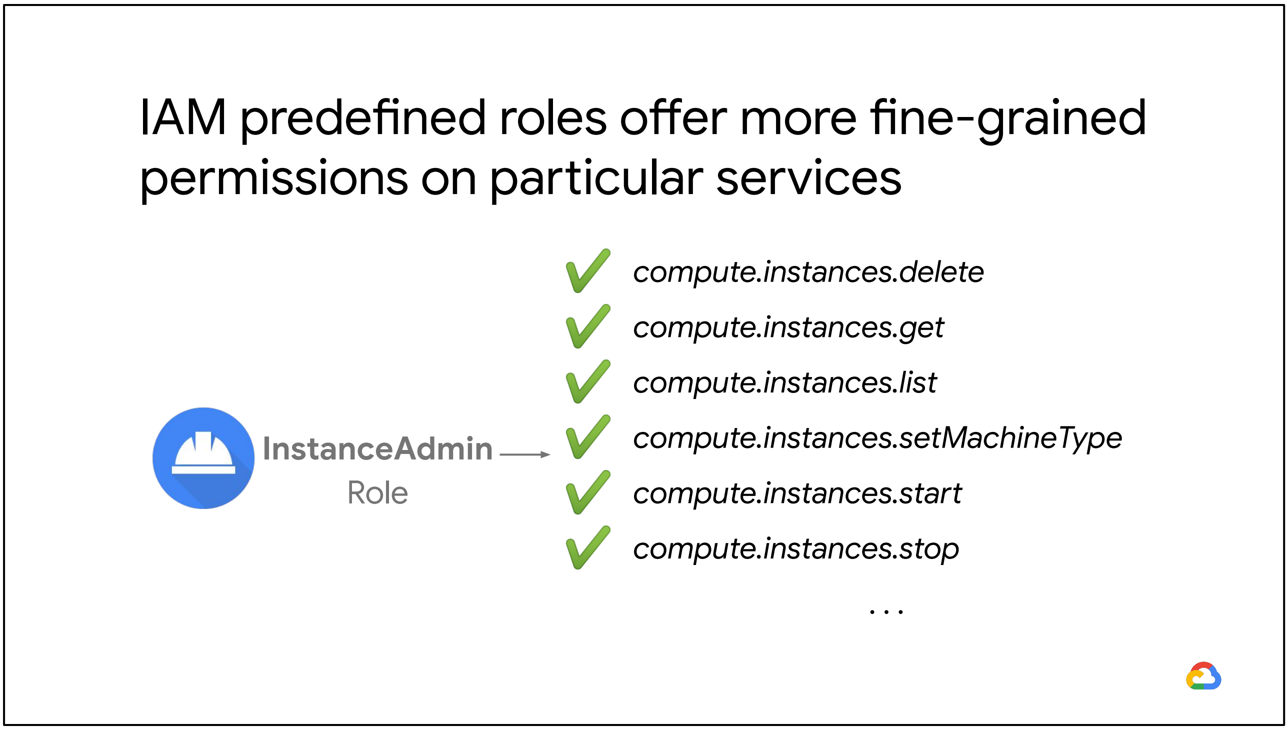
can do what

on resources **in this project**,
or folder, or org

As you have seen, primitive roles are very coarse-grained and are applied at the project level.

Predefined roles provide granular access for a specific service. They are designed to map to job functions, for example, Compute Network Admin, Security Reviewer, Storage Admin, etc.

Predefined roles are managed by Google Cloud. So if a new feature or service is added in the future, the appropriate permissions will be added to any predefined role that requires them.



IAM predefined roles offer more fine-grained permissions on particular services

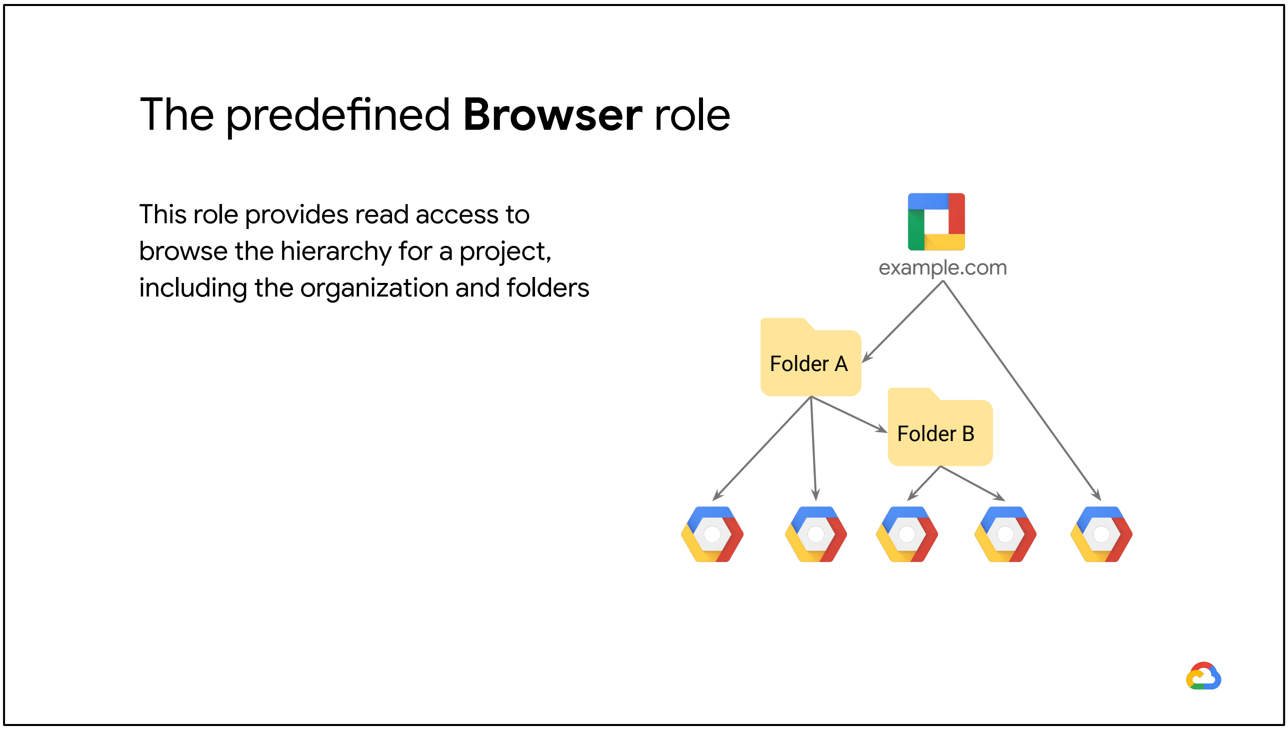
InstanceAdmin →
Role

- ✓ *compute.instances.delete*
- ✓ *compute.instances.get*
- ✓ *compute.instances.list*
- ✓ *compute.instances.setMachineType*
- ✓ *compute.instances.start*
- ✓ *compute.instances.stop*

. . .

A predefined role is simply a collection of permissions for a particular service. For example, the *InstanceAdmin* predefined role provides the permissions needed to manage Compute Engine instances.

An example of some of the permissions inherent in this role are shown here on the slide.

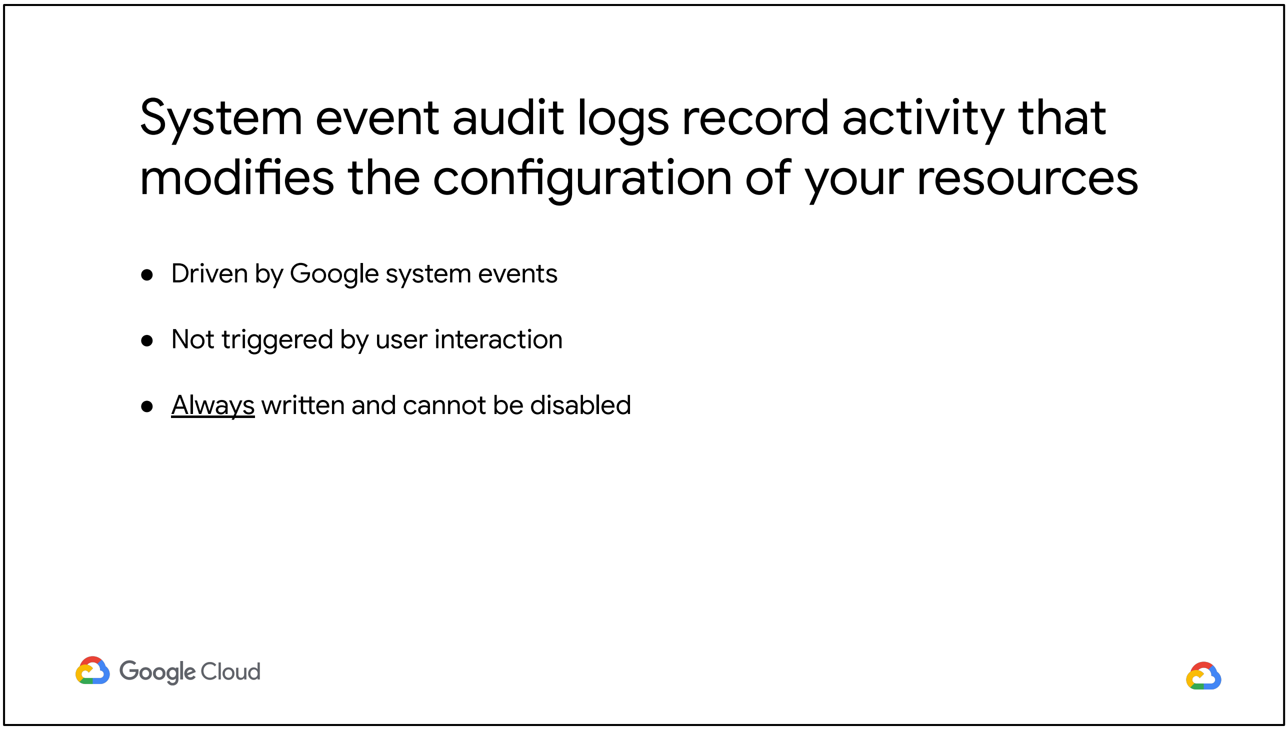


The predefined **Browser** role

This role provides read access to browse the hierarchy for a project, including the organization and folders

The predefined Browser role provides read-access to browse the **hierarchy** for a project, including the folder, organization, and Cloud IAM policy.

The Browser role does not include permission to view **resources** in the project
.



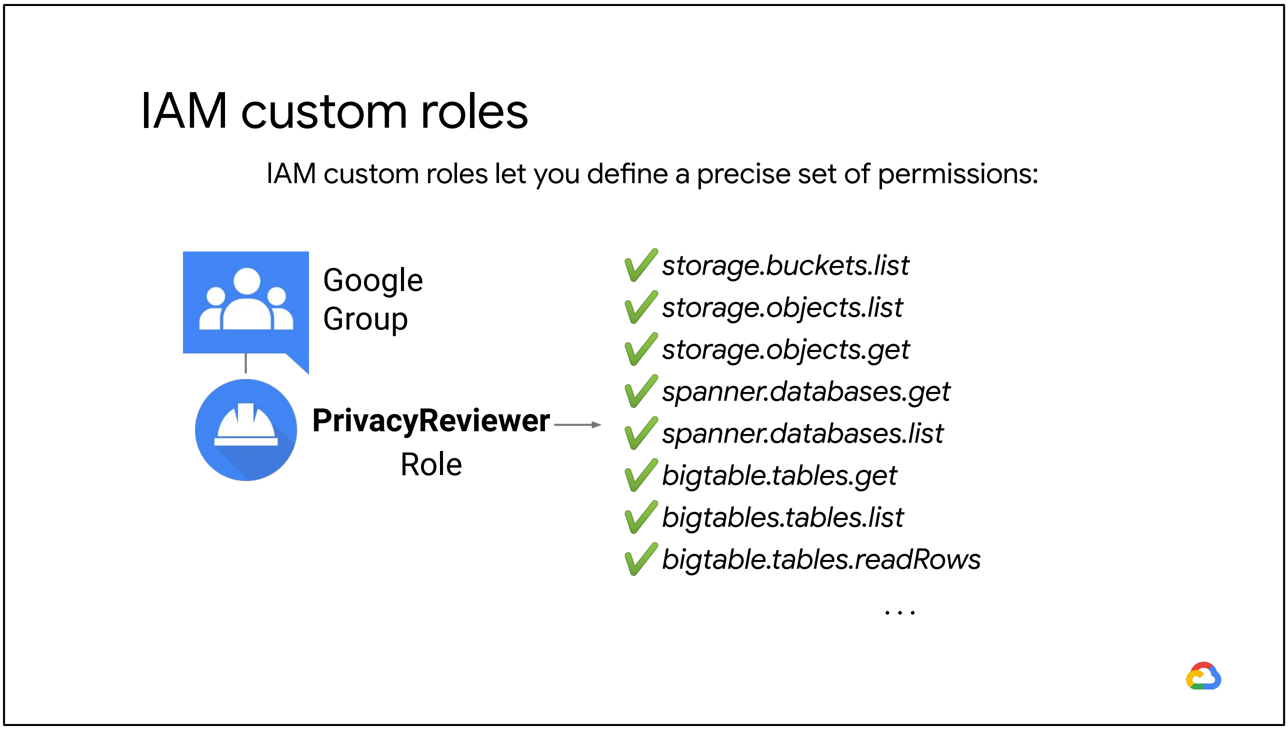
System event audit logs record activity that modifies the configuration of your resources

- Driven by Google system events
- Not triggered by user interaction
- Always written and cannot be disabled

System Event audit logs contain log entries for Google Cloud administrative actions that modify the configuration of resources.

System Event audit logs are generated by Google systems; they are not driven by direct user action.

System Event audit logs are always written; just like Admin Activity audit logs, you cannot configure or disable them. There is no charge for your System Event audit logs, however there are logging usage limits.



IAM custom roles

IAM custom roles let you define a precise set of permissions:

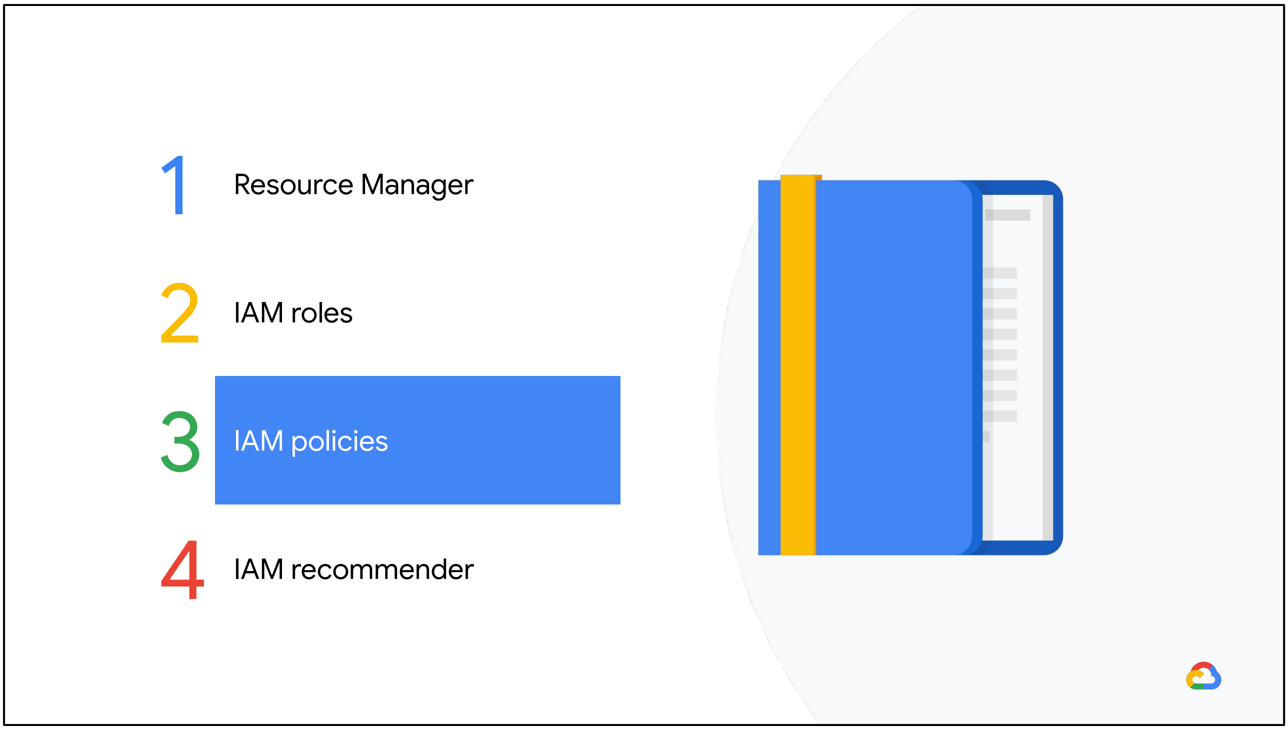
✓ *storage.buckets.list*
✓ *storage.objects.list*
✓ *storage.objects.get*
✓ *spanner.databases.get*
✓ *spanner.databases.list*
✓ *bigtable.tables.get*
✓ *bigtables.tables.list*
✓ *bigtable.tables.readRows*
. . .

What if you need something even finer-grained?

This is when you might use a Custom role, which will allow you to map specific permissions to specific job roles. For example, maybe you need to define a “Privacy Reviewer” role, to allow some users the ability to audit data that is stored in Google cloud storage, spanner, BigTable and other data repositories.

You can create a Custom role which contains **all** of the specific permissions needed to do that particular job - and **only** those permissions. Be aware that once Custom roles are created, you must manage the permissions granted for them.

If, for example, a new data storage service is created in the future that will need to be audited, permissions for that new service would need to be added to your Privacy Reviewer role.



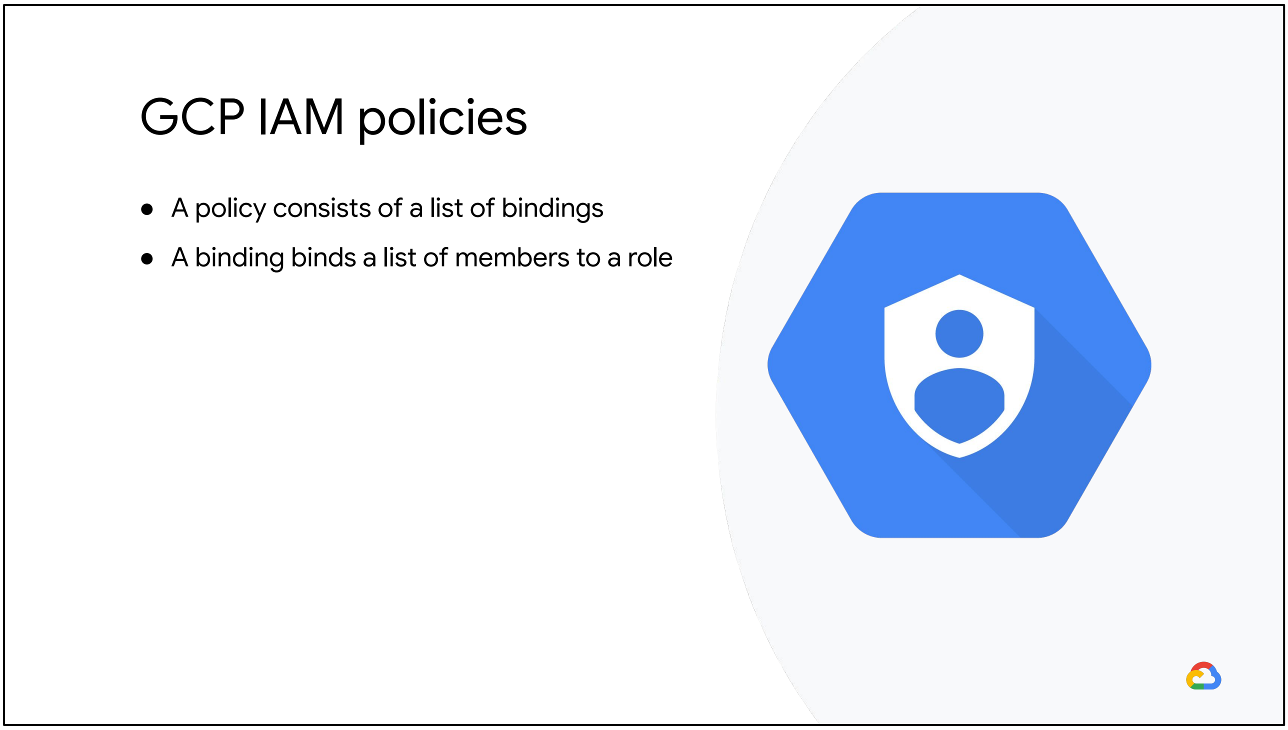
1 Resource Manager

2 IAM roles

3 IAM policies

4 IAM recommender

A Cloud IAM policy is used to specify access control policies for Google Cloud resources.



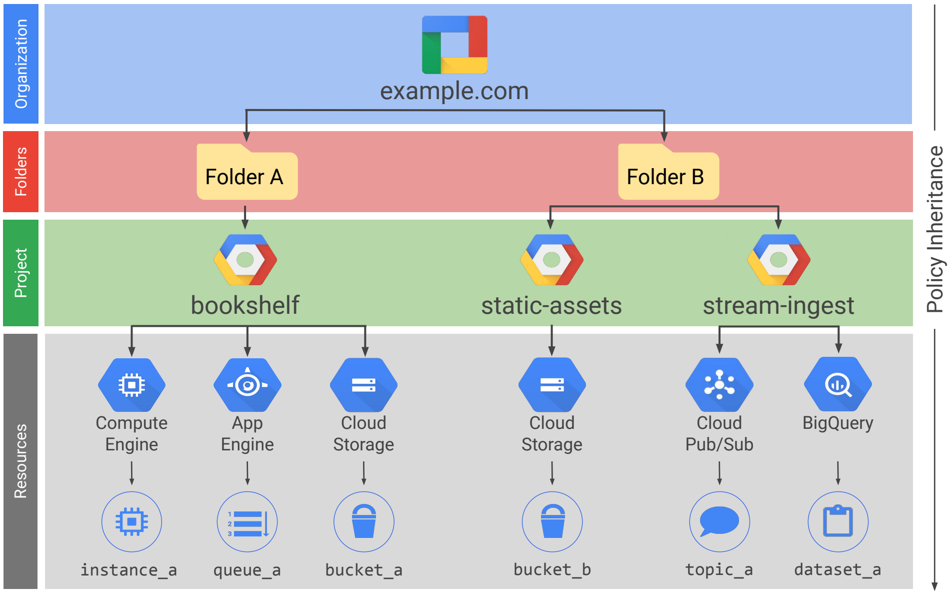
GCP IAM policies

- A policy consists of a list of bindings
- A binding binds a list of members to a role

A policy consists of a list of bindings.

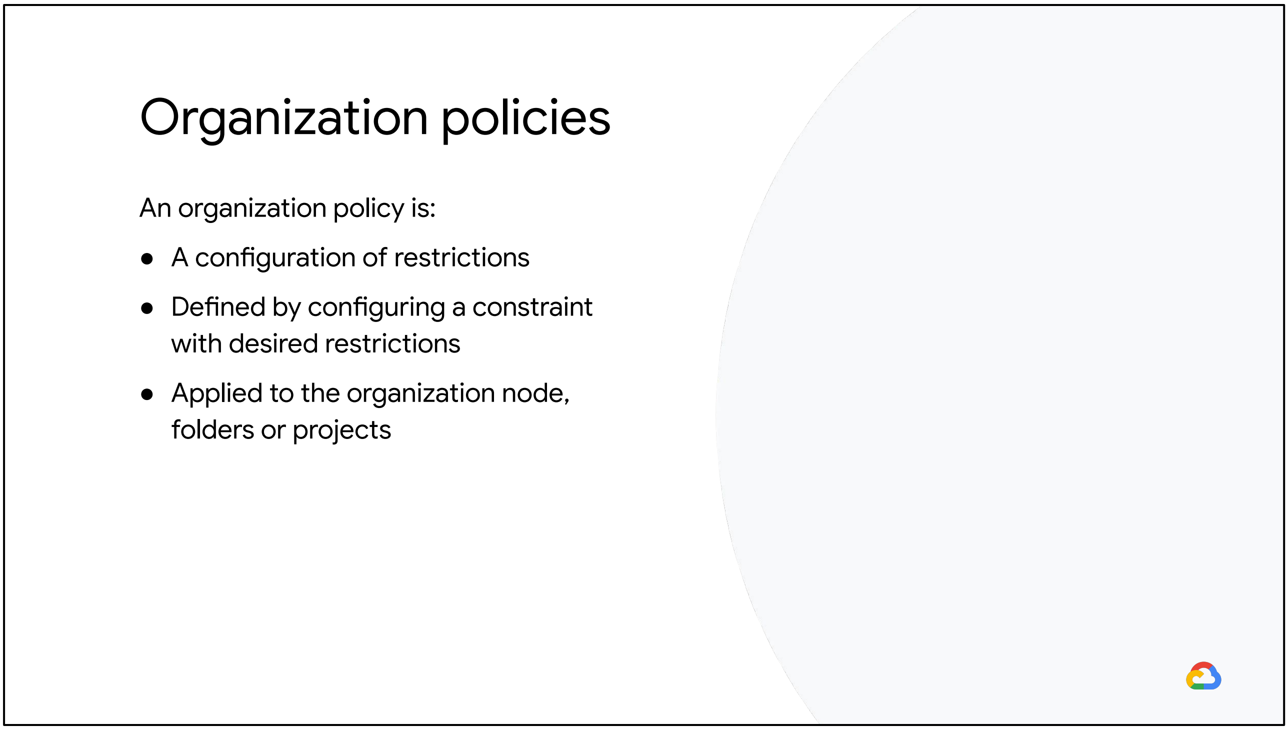
A binding binds a list of members to a role, where the members can be user accounts, Google groups, Google domains, and service accounts.A role is a named list of permissions defined by Cloud IAM.

IAM resource hierarchy



A policy is a collection of access statements attached to a resource.

Each policy contains a set of roles and role members, with resources inheriting policies from their parent. Think of it like this: resource policies are *a union of parent and resource*, where a *less* restrictive parent policy will always override a *more* restrictive resource policy.



Organization policies

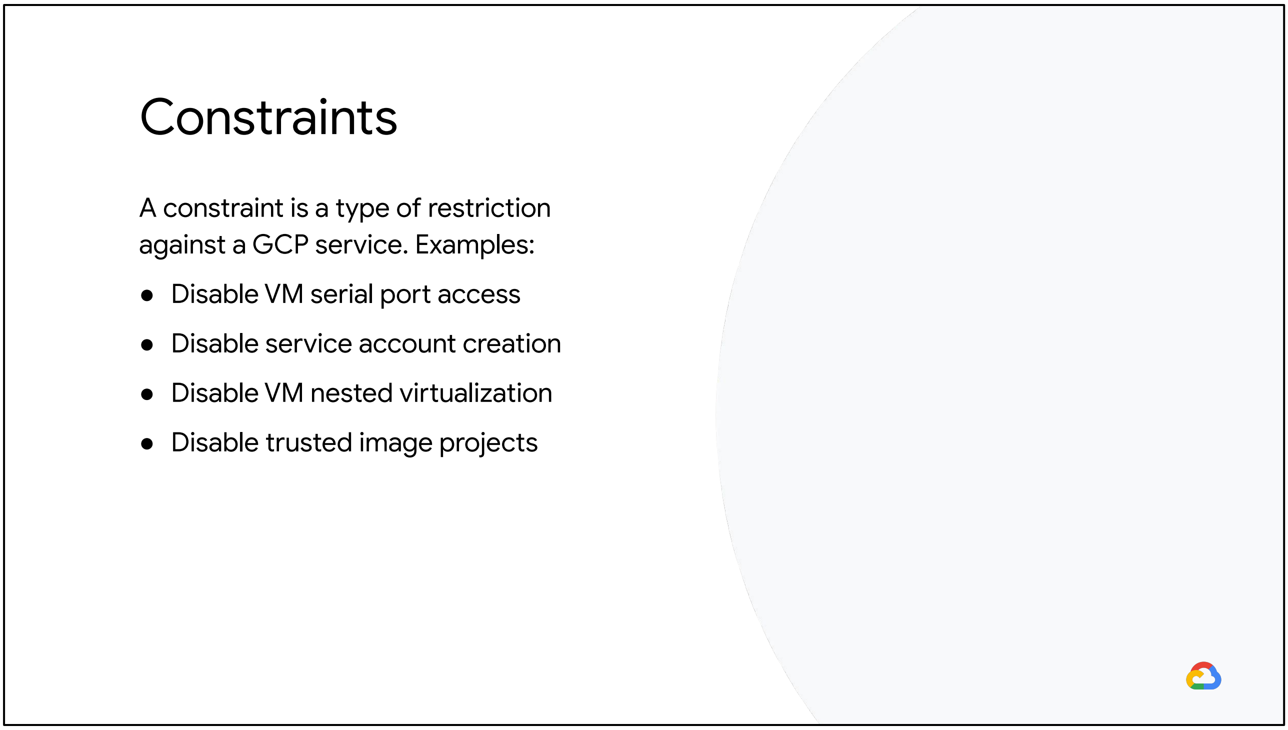
An organization policy is:

- A configuration of restrictions
- Defined by configuring a constraint with desired restrictions
- Applied to the organization node, folders or projects

An organization policy is a configuration of restrictions, defined by configuring a constraint with the desired restrictions for that organization.

An organization policy can be applied to the organization node, and all of its folders or projects within that node. Descendants of the targeted resource hierarchy node inherit the organization policy that has been applied to their parents.

Exceptions to these policies can be made, but only by a user who has the organization policy admin role.



Constraints

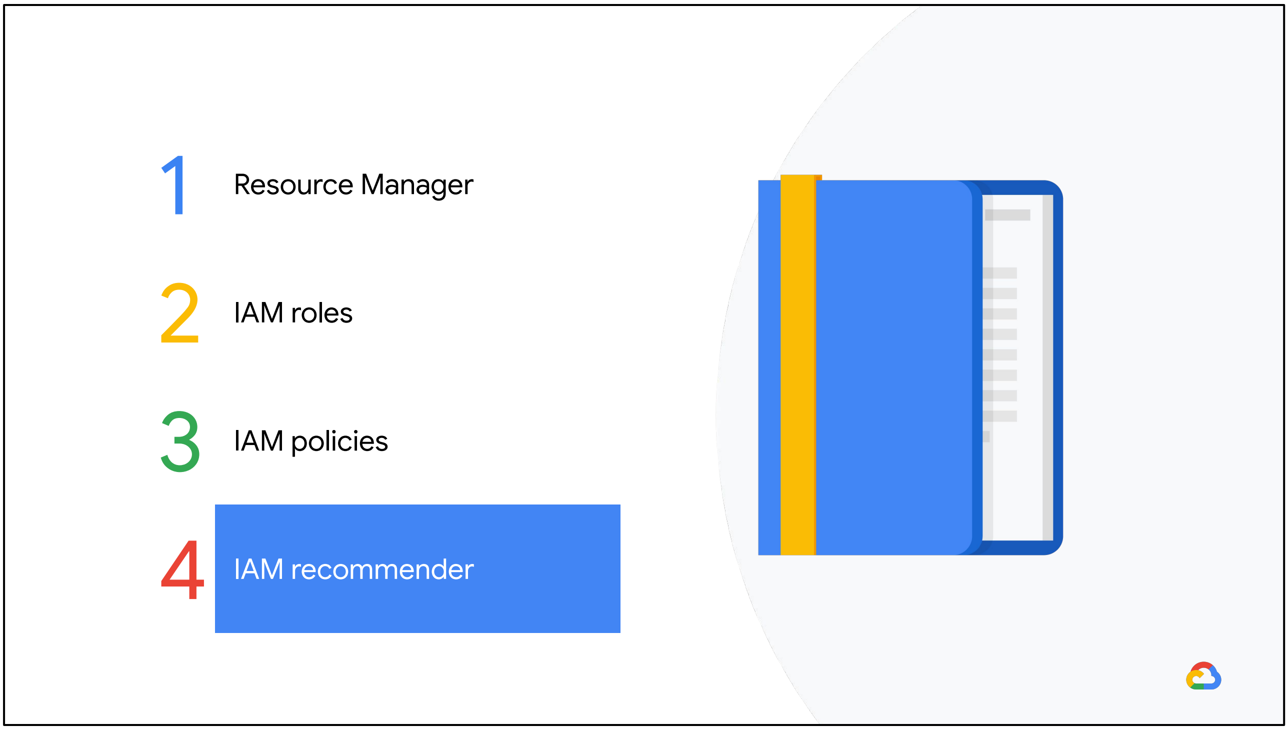
A constraint is a type of restriction against a GCP service. Examples:

- Disable VM serial port access
- Disable service account creation
- Disable VM nested virtualization
- Disable trusted image projects

A constraint is a type of restriction against a Google Cloud service or a list of Google Cloud services.

Think of the constraint as a blueprint that defines what behaviors are controlled - for example, disabling access to serial ports, and removing the ability to create service accounts. Once created, this blueprint is then applied to a resource hierarchy node as an organization policy, which implements the rules defined in the constraint.

The Google Cloud service mapped to that constraint and associated with that resource hierarchy node will then enforce the restrictions configured within the organization policy.



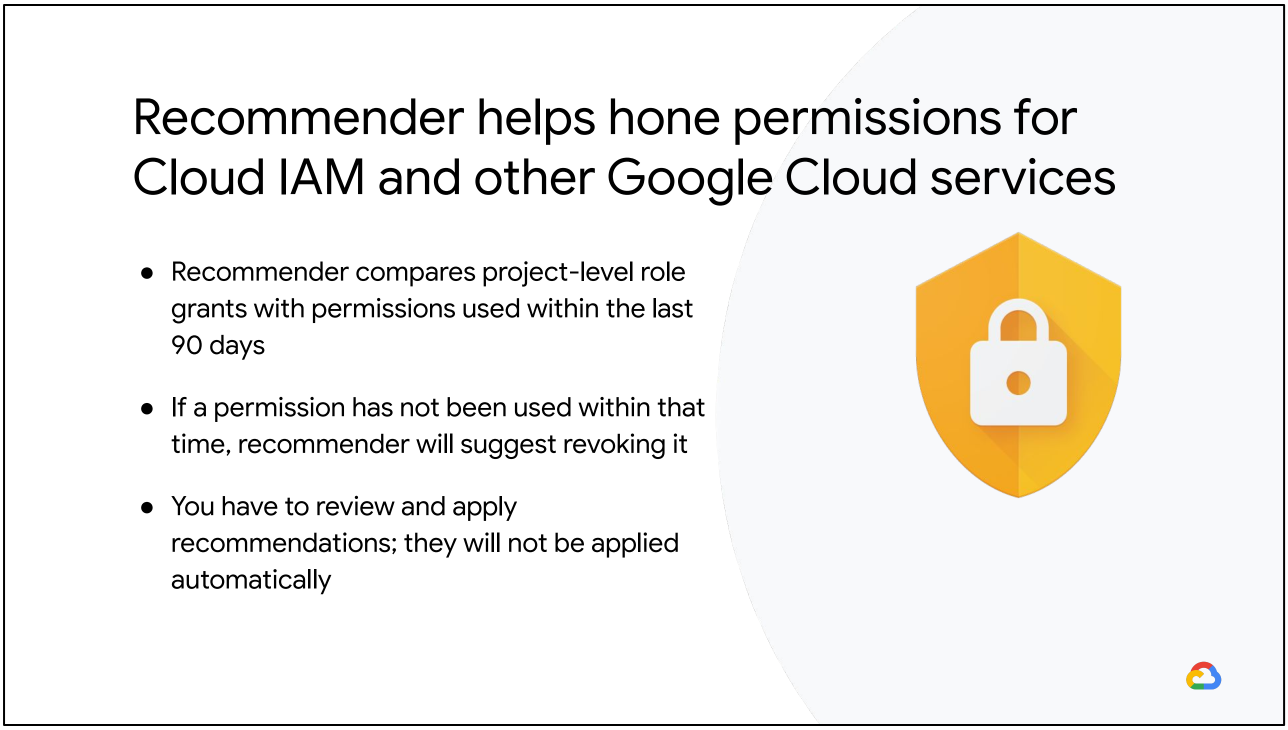
1 Resource Manager

2 IAM roles

3 IAM policies

4 IAM recommender

The Cloud IAM recommender helps you enforce the principle of least privilege by ensuring that members have only the permissions that they actually need

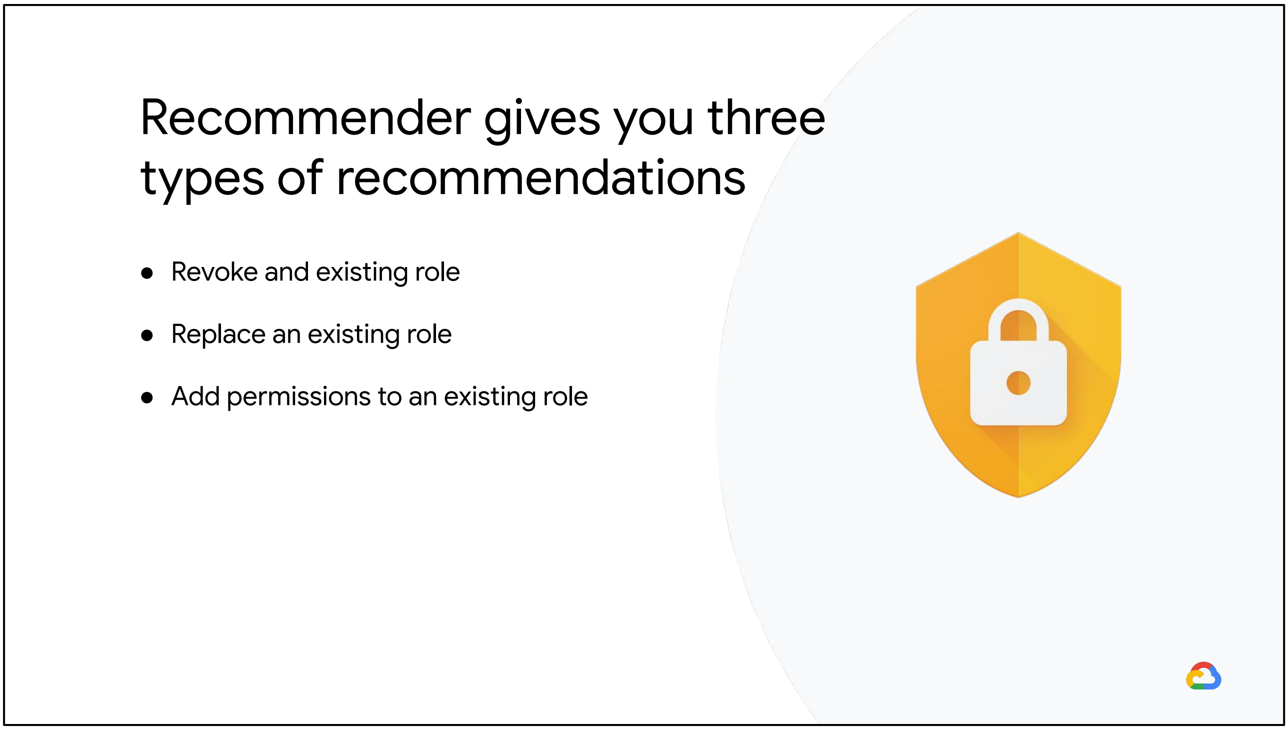


Recommender helps hone permissions for Cloud IAM and other Google Cloud services

- Recommender compares project-level role grants with permissions used within the last 90 days
- If a permission has not been used within that time, recommender will suggest revoking it
- You have to review and apply recommendations; they will not be applied automatically

The Cloud IAM recommender evaluates only role grants that were made at the project level and that have existed for at least 90 days. It does not evaluate any of the following items:

- Conditional role grants
- Role grants for Google-managed service accounts
- Access controls that are separate from Cloud IAM



Recommender gives you three types of recommendations

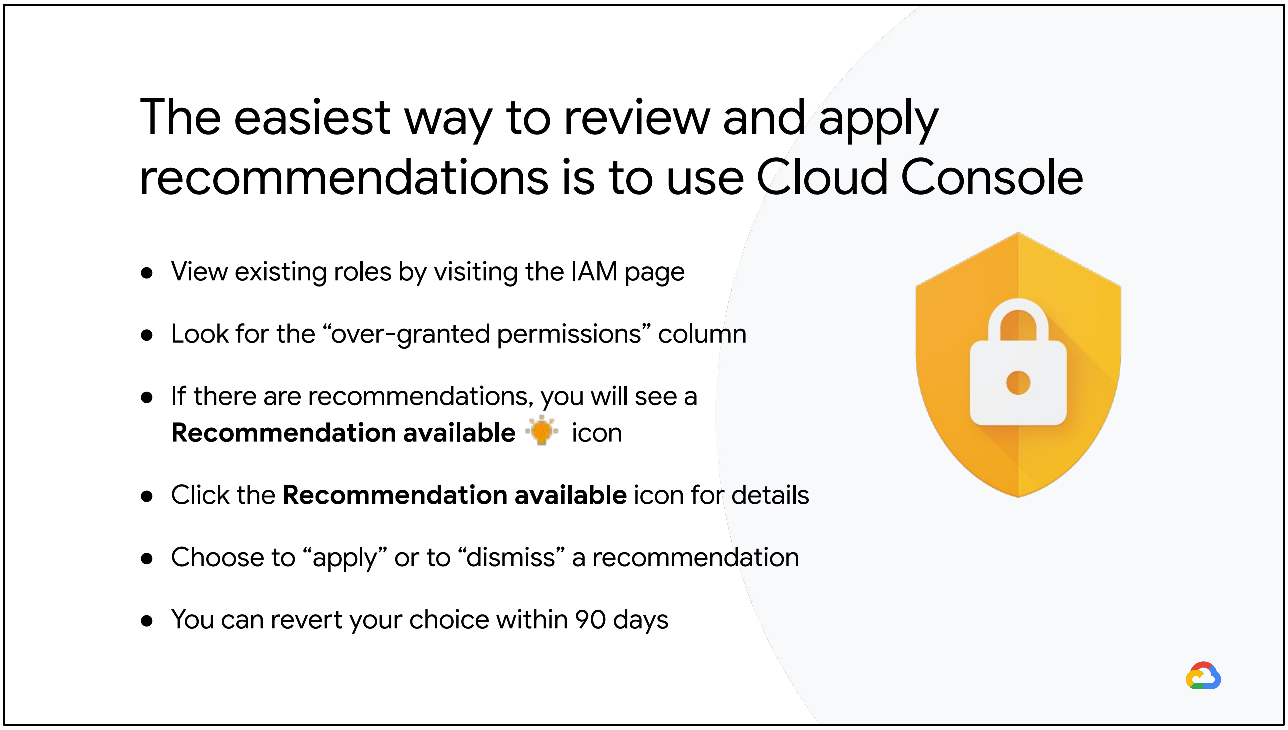
- Revoke and existing role
- Replace an existing role
- Add permissions to an existing role

Recommender will suggest that you revoke an existing role when it has been in effect for 90 days or more and when it has not been used within the past 90 days.

The theory with this type of recommendation is that if the policy has not been used within the past 90 days, it may have been unnecessary originally, or it may have outlived its usefulness.
Removing such permissions keeps your roles pruned down to only those permissions that are actually required, which is a foundational security concept. Recommender may also suggest that you replace a particular role with another role or set of roles.

For example, if a service account has an assigned role with permissions that are not used, it would be more secure if you revise it to use a combination of less-permissive roles that have only the necessary permissions.

And, finally, Recommender may suggest that you add permissions to a role, even if those permissions are not currently being used. Recommender uses machine learning to predict which permissions may be needed by a particular role in the future. If those permissions are not currently enabled, Recommender will suggest adding them.



The easiest way to review and apply recommendations is to use Cloud Console

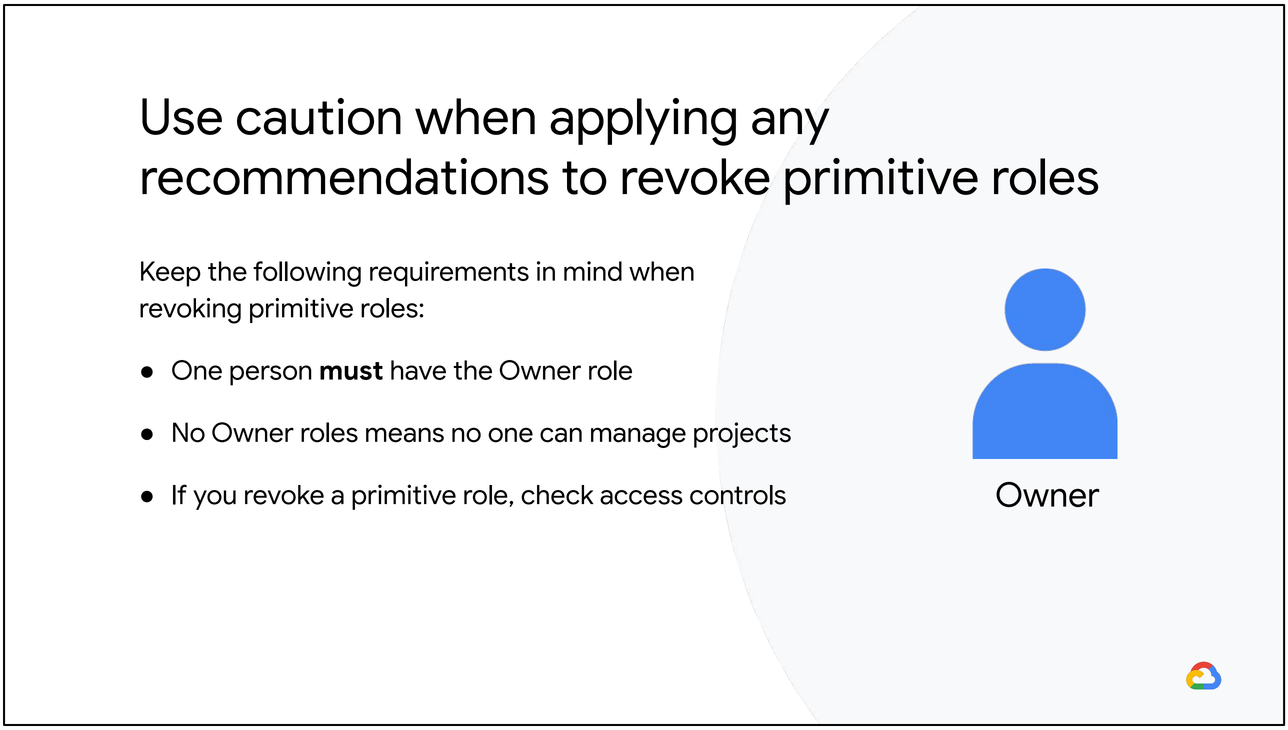
- View existing roles by visiting the IAM page
- Look for the “over-granted permissions” column
- If there are recommendations, you will see a **Recommendation available** 💡 icon
- Click the **Recommendation available** icon for details
- Choose to “apply” or to “dismiss” a recommendation
- You can revert your choice within 90 days

Your recommendations can be found on the IAM page in the list of current roles for your account. Next to each role, in the “over granted permissions” column, you will see one of two icons: a lightbulb that is either greyed out or one that is golden-orange and “lit,” indicating that there are recommendations available for that role.

If a role has recommendations, clicking on the Recommendation available icon will show you more details about the recommendation, and you can then choose to accept and apply a recommendation or dismiss it.

If you change your mind within 90 days about accepting or dismissing a recommendation, you can use the Cloud IAM Recommender logs to revert that decision.

While using the Cloud Console is the easiest way to manage your recommendations, you can also review and apply recommendations using the `gcloud` command-line tool and the Recommender API.



Use caution when applying any recommendations to revoke primitive roles

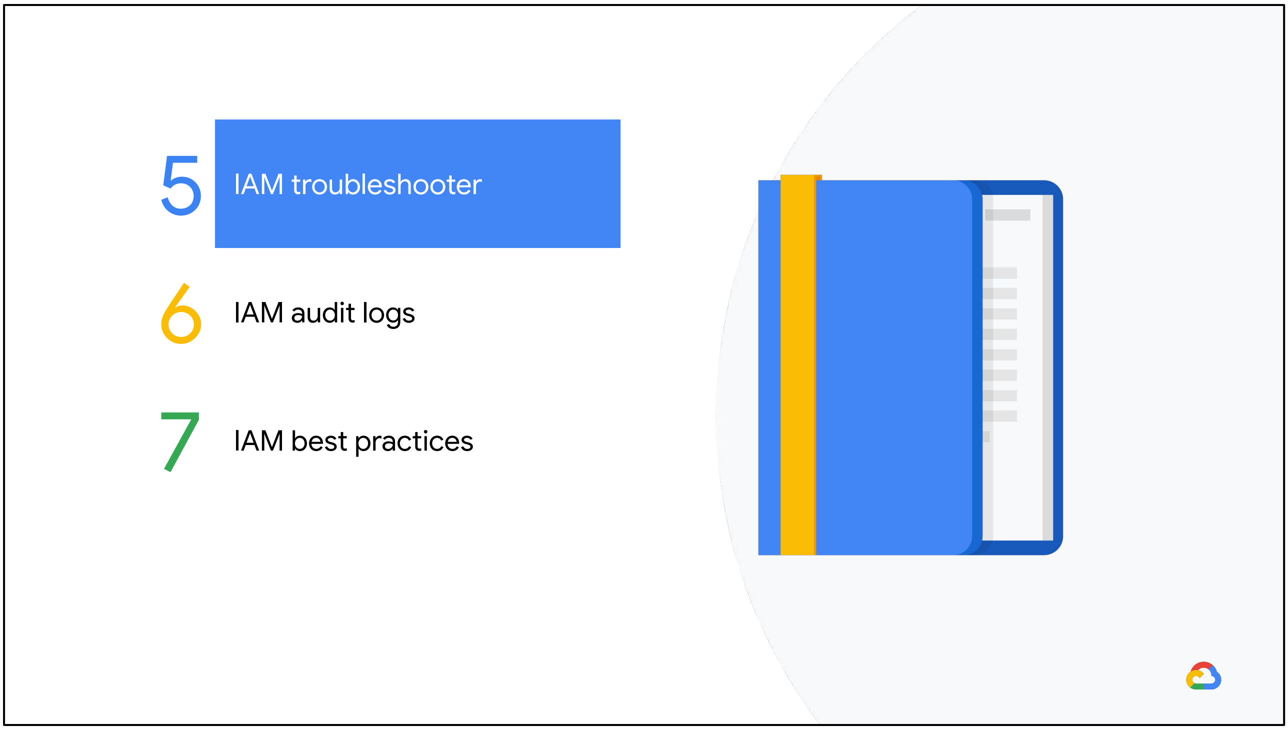
Keep the following requirements in mind when revoking primitive roles:

- One person **must** have the Owner role
- No Owner roles means no one can manage projects
- If you revoke a primitive role, check access controls

Owner

At least one person in your org **must** have the Owner role in order for the organization's resources to function. If you remove Owner roles from all organizational members, no one will be able to manage projects.

If you need to revoke a primitive role, but you are using other access control measures, make sure they still work after you revoke the primitive role.

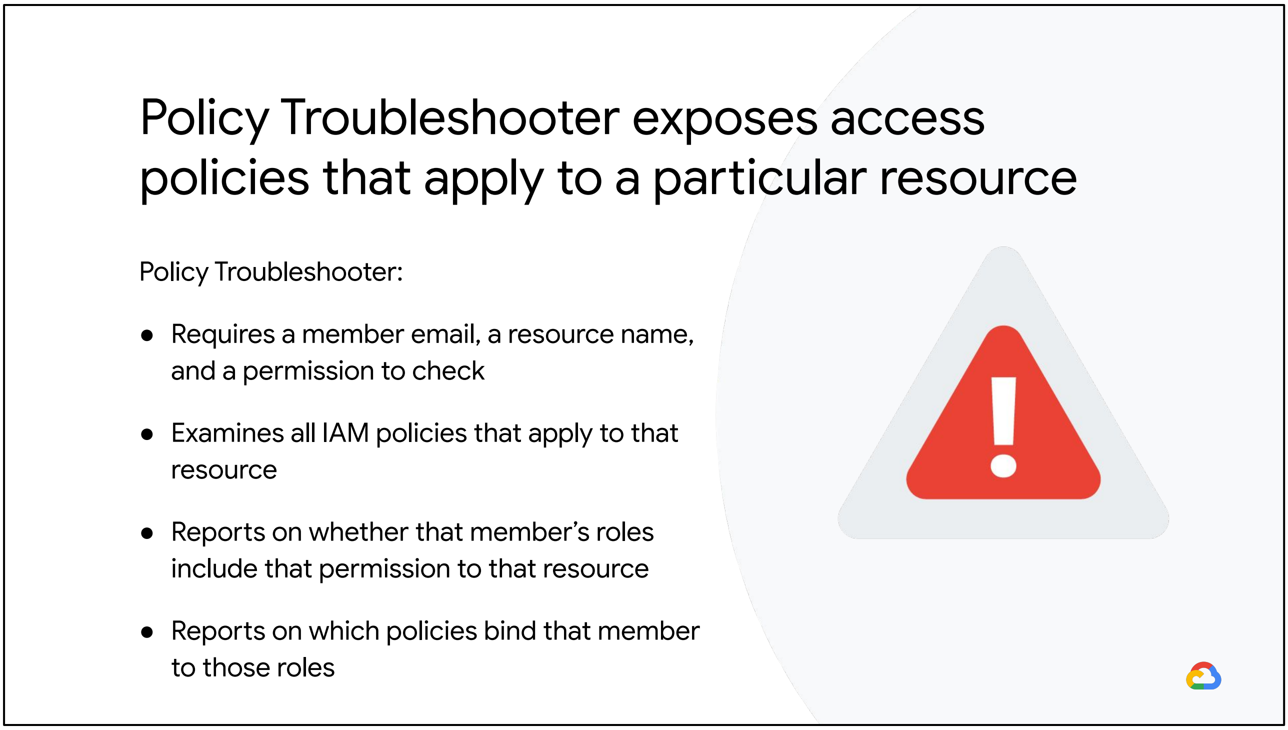


5 IAM troubleshooter

6 IAM audit logs

7 IAM best practices

IAM Policy Troubleshooter helps you more closely examine policies that govern user access to a particular resource.



Policy Troubleshooter exposes access policies that apply to a particular resource

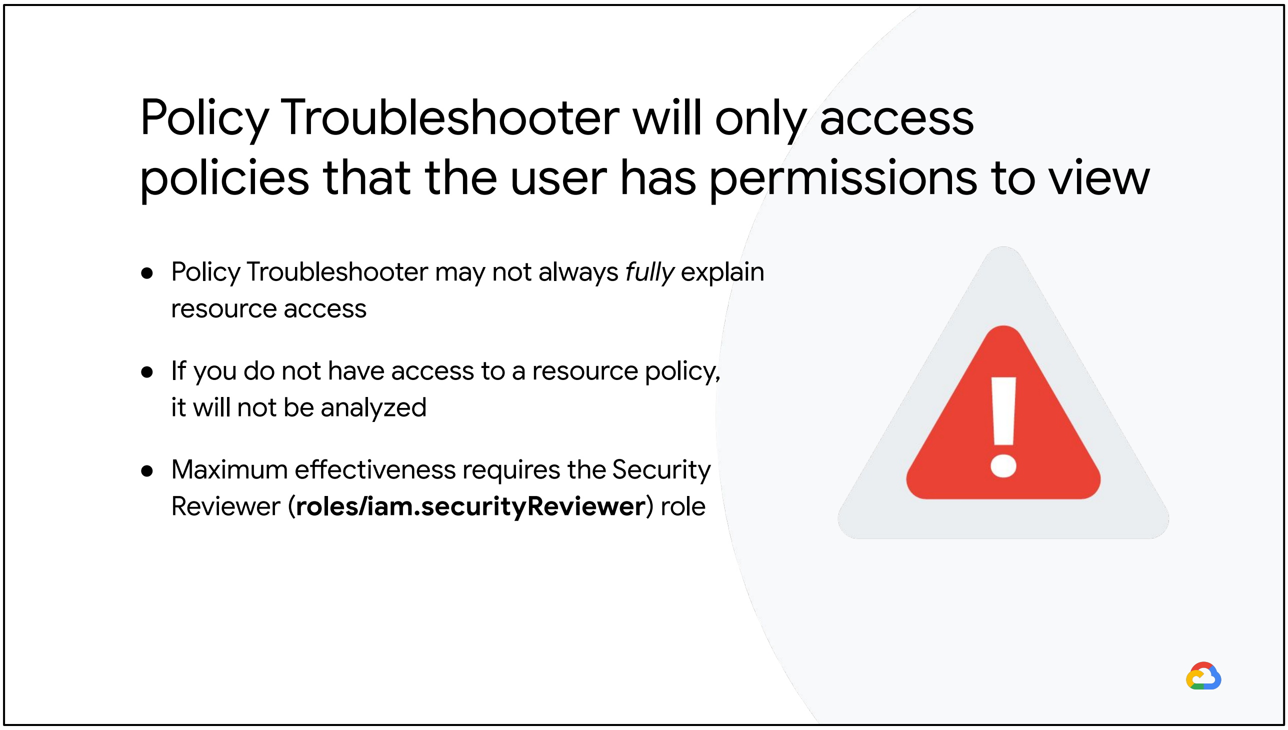
Policy Troubleshooter:

- Requires a member email, a resource name, and a permission to check
- Examines all IAM policies that apply to that resource
- Reports on whether that member's roles include that permission to that resource
- Reports on which policies bind that member to those roles

IAM Policy Troubleshooter makes it easier to understand why a user has access to a resource or doesn't have permission to call an API.

In order to generate a Policy Troubleshooter report, you will need the email of the user who needs access, the full name of the resource they need access to, and a permission that you want to check for.

Troubleshooter will take this information and examine all the IAM policies that apply to that particular resource and then report on whether it found that permission for that user in the resource's list of permissions. It will also report on the policies that bind that user to those roles.

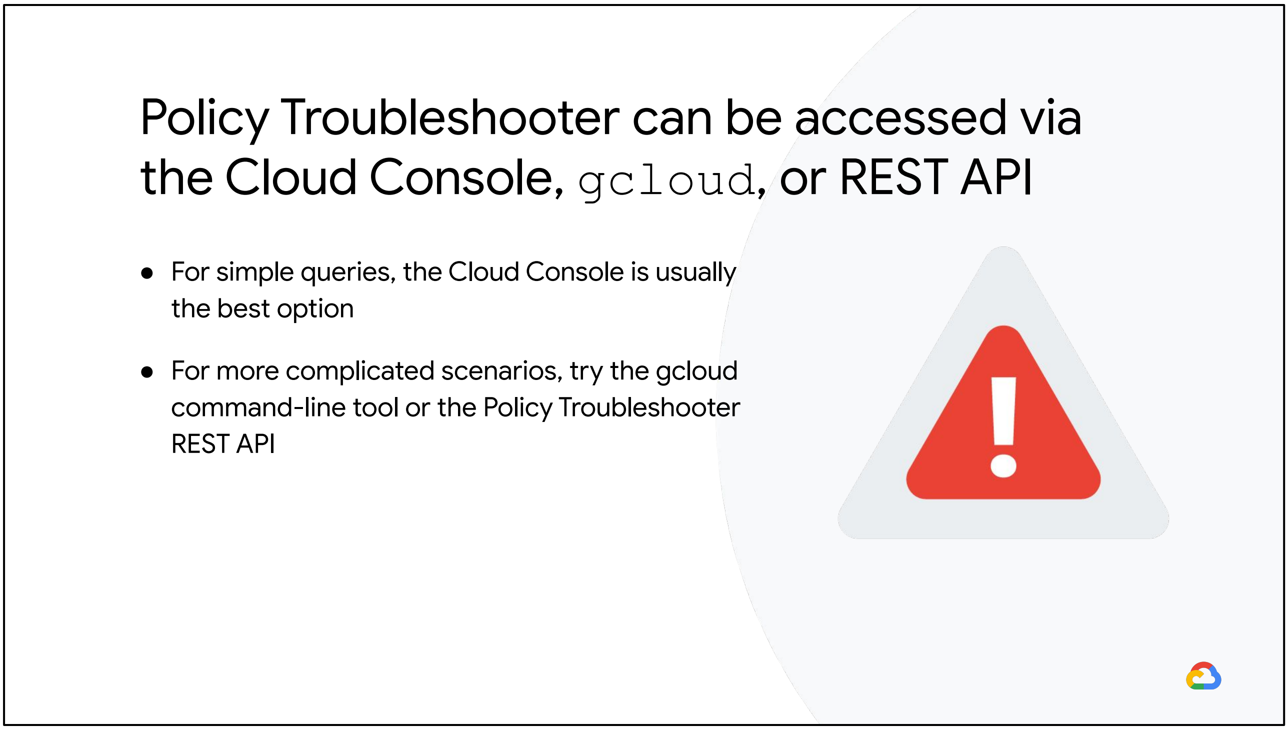


Policy Troubleshooter will only access policies that the user has permissions to view

- Policy Troubleshooter may not always *fully* explain resource access
- If you do not have access to a resource policy, it will not be analyzed
- Maximum effectiveness requires the Security Reviewer (**roles/iam.securityReviewer**) role

For security reasons, Policy Troubleshooter can only examine policies that the person using it has permissions to access. Because Troubleshooter cannot analyze permissions it does not have access to, it may not always be able to fully explain a resource's access policies.

If maximum effectiveness is the overriding concern, the member using the Policy Troubleshooter must be granted the Security Reviewer (roles/iam.securityReviewer) role.

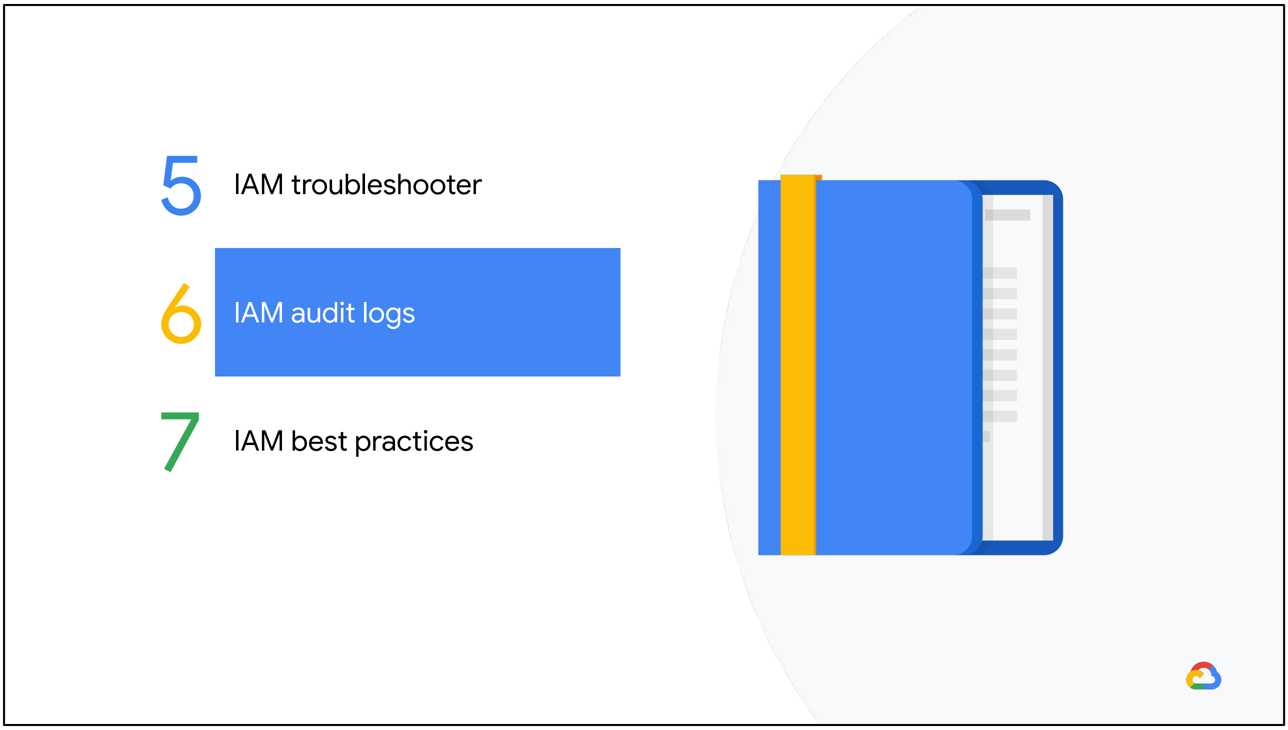


Policy Troubleshooter can be accessed via the Cloud Console, `gcloud`, or REST API

- For simple queries, the Cloud Console is usually the best option
- For more complicated scenarios, try the gcloud command-line tool or the Policy Troubleshooter REST API

There are three ways you can access Policy Troubleshooter, either by using the Cloud Console, the `gcloud` command-line tool, or the Policy Troubleshooter API.

Choose how to access the Policy Troubleshooter based on how complicated a query you need to perform. For example, simple queries are more easily executed using the Cloud Console. A more complicated or programmatic approach would require the `gcloud` command-line tool or the Policy Troubleshooter REST API.

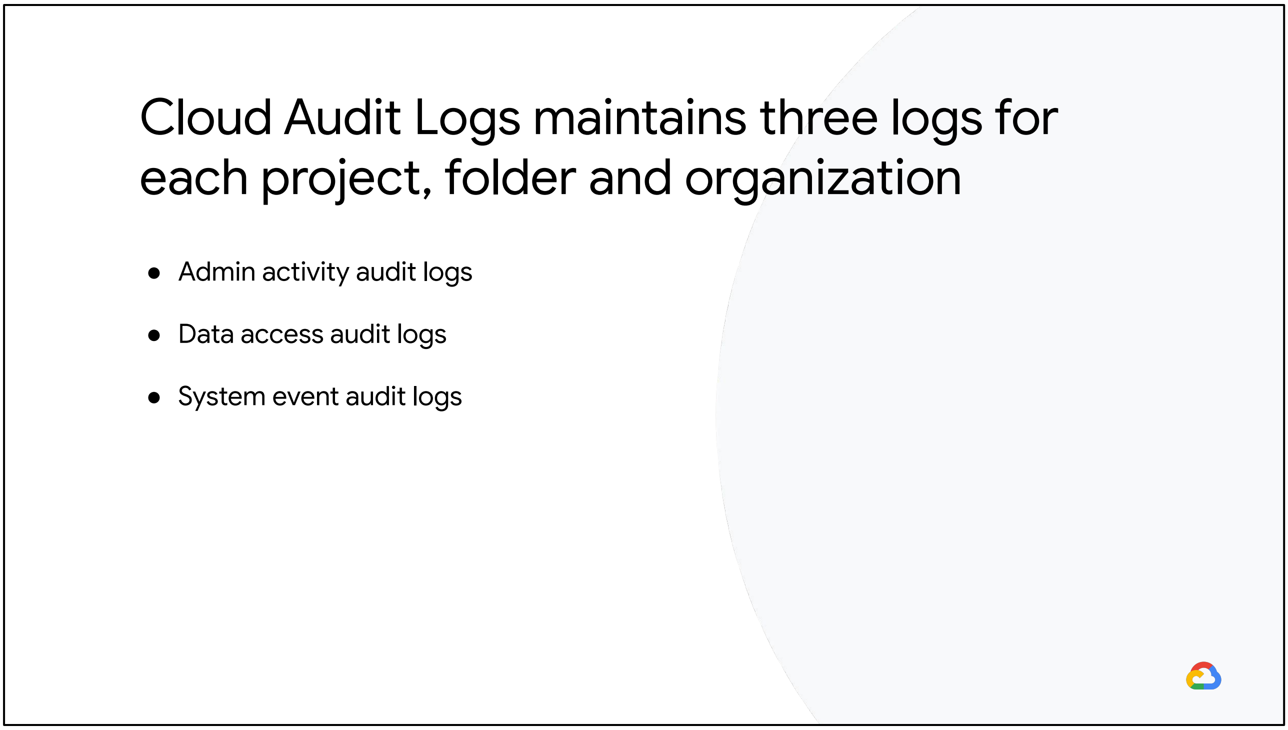


5 IAM troubleshooter

6 IAM audit logs

7 IAM best practices

Google Cloud services write audit log entries to help you answer the questions of "who did what, where, and when?" within your Google Cloud resources.

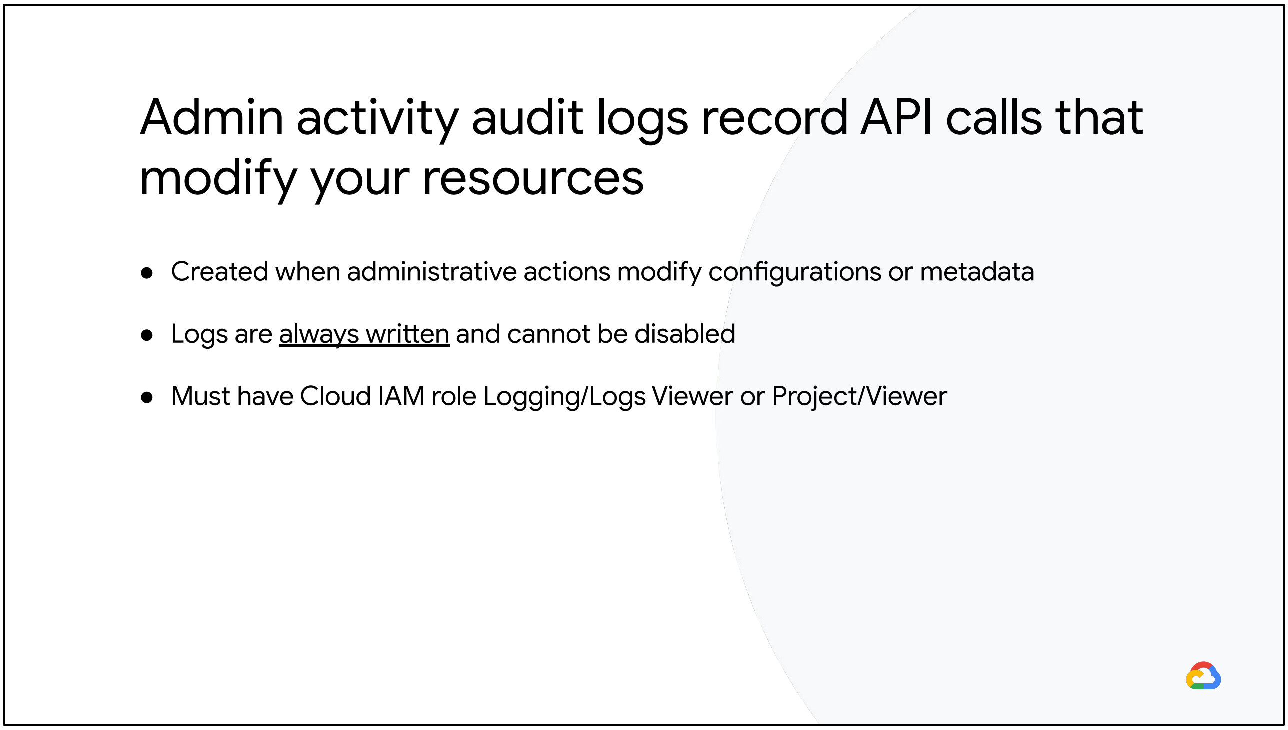


Cloud Audit Logs maintains three logs for each project, folder and organization

- Admin activity audit logs
- Data access audit logs
- System event audit logs

Google Cloud services write near-real-time audit log entries to these three types of logs to help you answer the questions of "who did what, where, and when?" within your Google Cloud resources, allowing you to quickly assess and act on any unusual behavior.

Cloud Audit Logs are encrypted at rest using either AES256 or AES128, which are the encryption standards that are also used to help protect the rest of Google’s infrastructure.



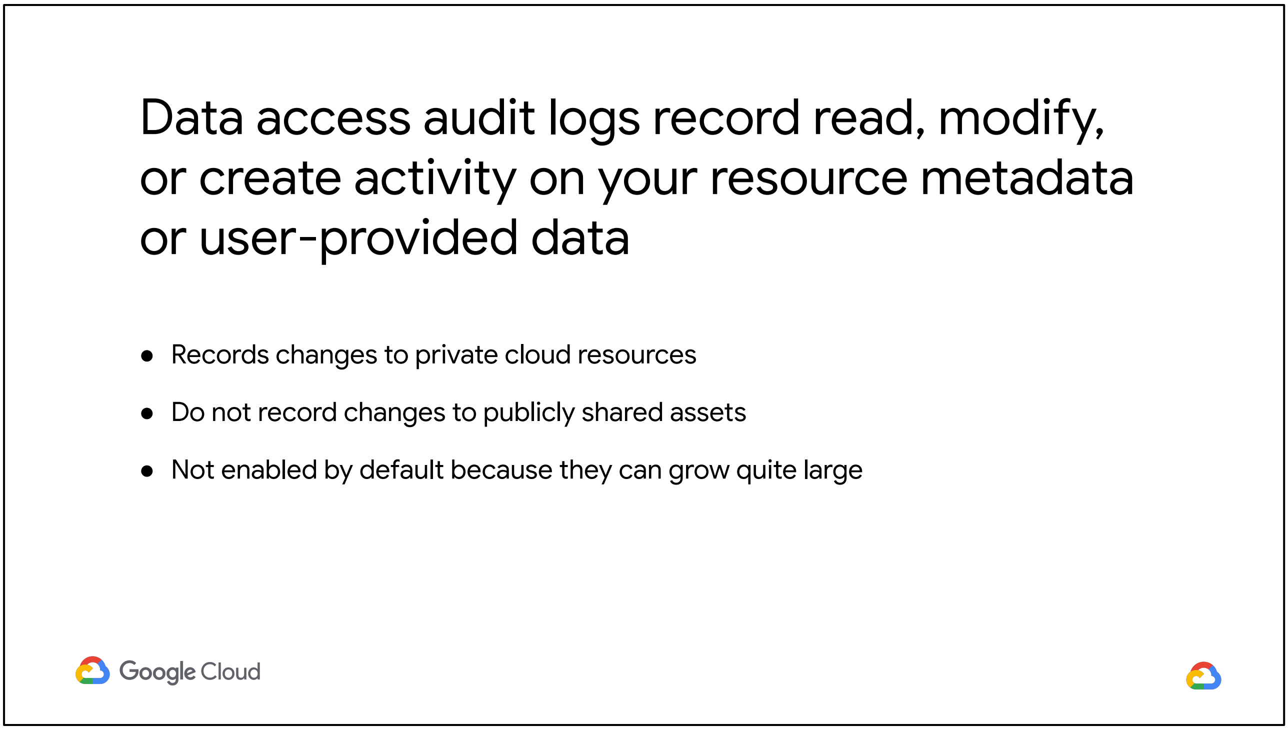
Admin activity audit logs record API calls that modify your resources

- Created when administrative actions modify configurations or metadata
- Logs are always written and cannot be disabled
- Must have Cloud IAM role Logging/Logs Viewer or Project/Viewer

Admin Activity audit logs contain log entries for administrative actions that modify the configuration or metadata of your resources, for example, when users have created a VM instance or changed Cloud Identity and Access Management permissions on a resource.
There is no charge for using Admin Activity logs.

Admin Activity audit logs are **always written and cannot be disabled** - which improves your resource security because you can be assured that every activity of this kind will be recorded and available for review later if a problem arises.

In order to view Admin activity audit logs, you must have the Cloud IAM Logging/Logs Viewer or Project/Viewer role.



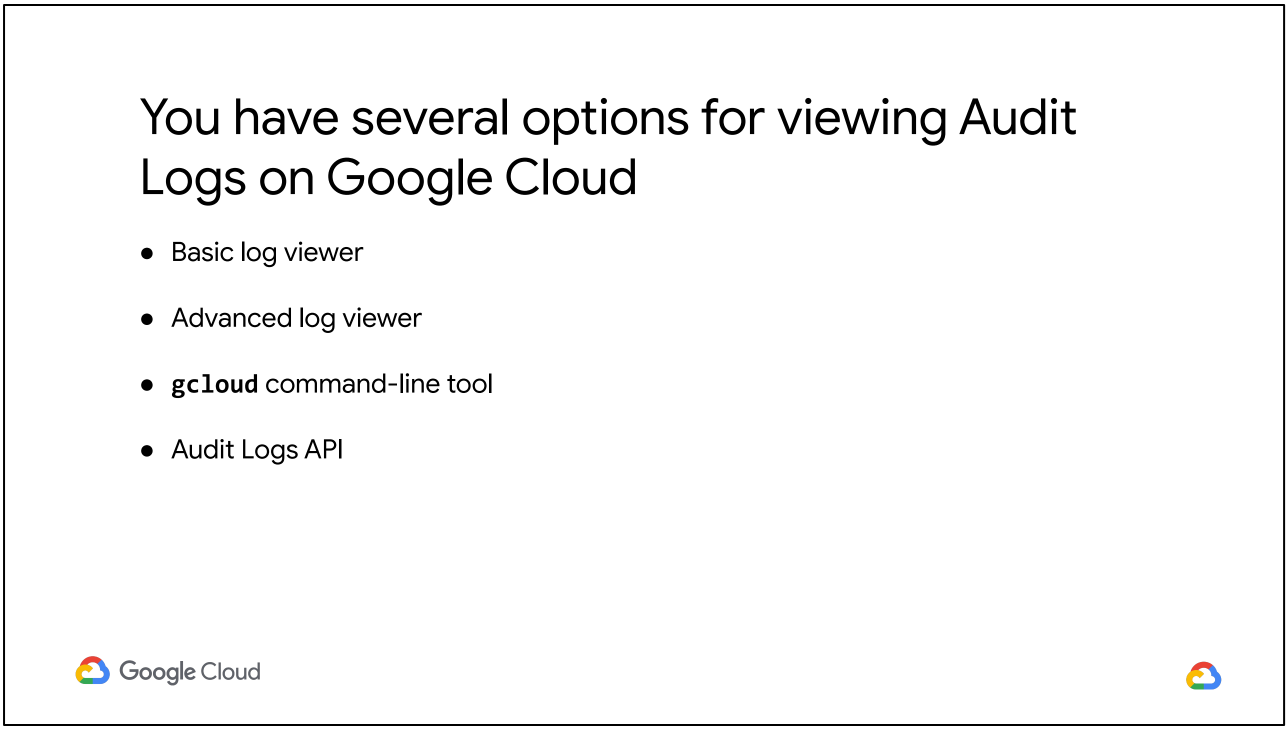
Data access audit logs record read, modify, or create activity on your resource metadata or user-provided data

- Records changes to private cloud resources
- Do not record changes to publicly shared assets
- Not enabled by default because they can grow quite large

Data Access audit logs record when an API call reads the configuration or metadata of a resource. These logs also record when a user-driven API makes calls that create, modify, or read user-provided resource data. Data Access audit logs can be enabled, or disabled using the Cloud Console. You can also use the API or Cloud SDK to perform these tasks programmatically.

Data Access audit logs do not record data-access operations on resources that are publicly shared, or that can be accessed without logging into Google Cloud. An example of this kind of resource might be a .PDF file in a publicly shared storage bucket, that is generally accessed via a URL.

You can enable Data Access audit logs on your entire Organization, or only on a particular resource within that organization, such as a folder, a project, a particular configuration or service. On a busy system, data is accessed quite frequently, therefore, a Data Access audit log can quickly grow to an enormous size. For this reason, data access logs are not enabled by default - you will need to enable it manually on the systems you wish to monitor.
Something else to keep in mind is enabling Data Access audit logs may result in additional log usage charges on your project.

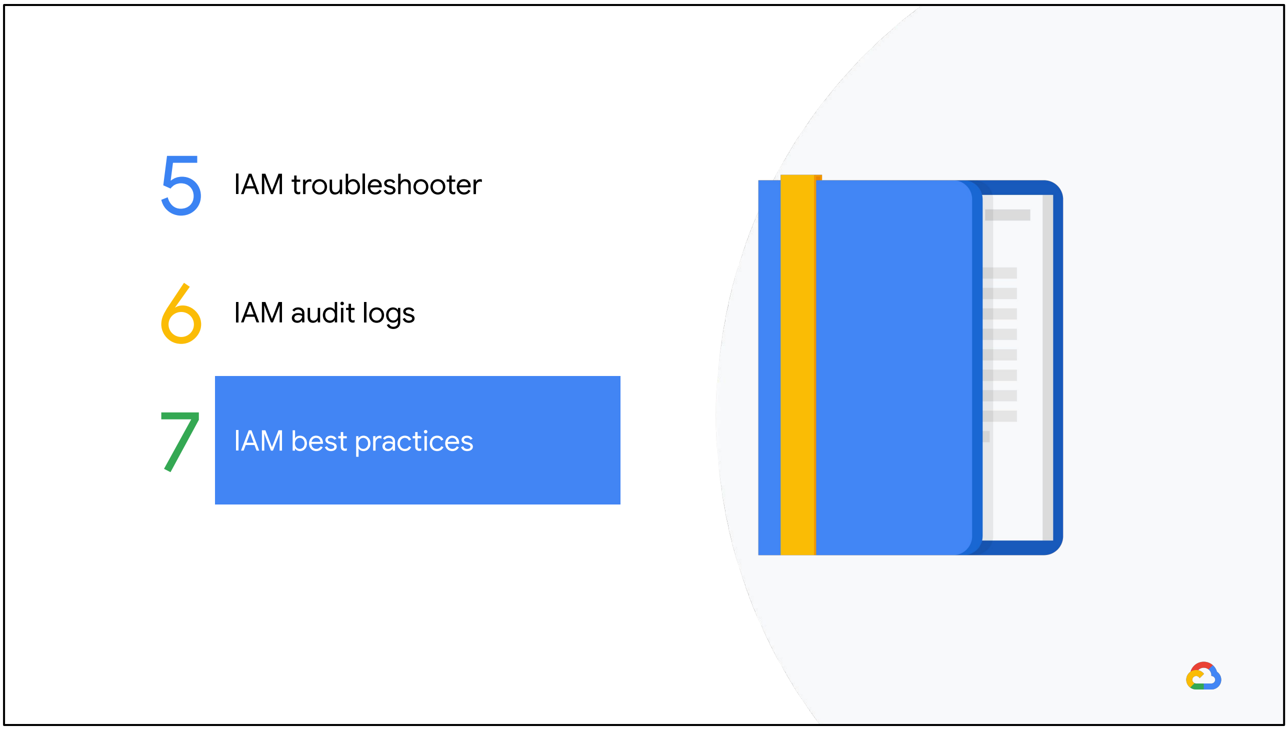


You have several options for viewing Audit Logs on Google Cloud

- Basic log viewer
- Advanced log viewer
- **`gcloud`** command-line tool
- Audit Logs API

There are four ways you can view your Audit Logs on Google Cloud: the basic or advanced log viewers, the gcloud command-line tool, or programmatically using the Audit Logs API.

The Cloud Console Logs Viewer currently supports viewing logs for projects only. To read log entries for a specified folder or organization, use the Logging API or `gcloud` command-line tool.

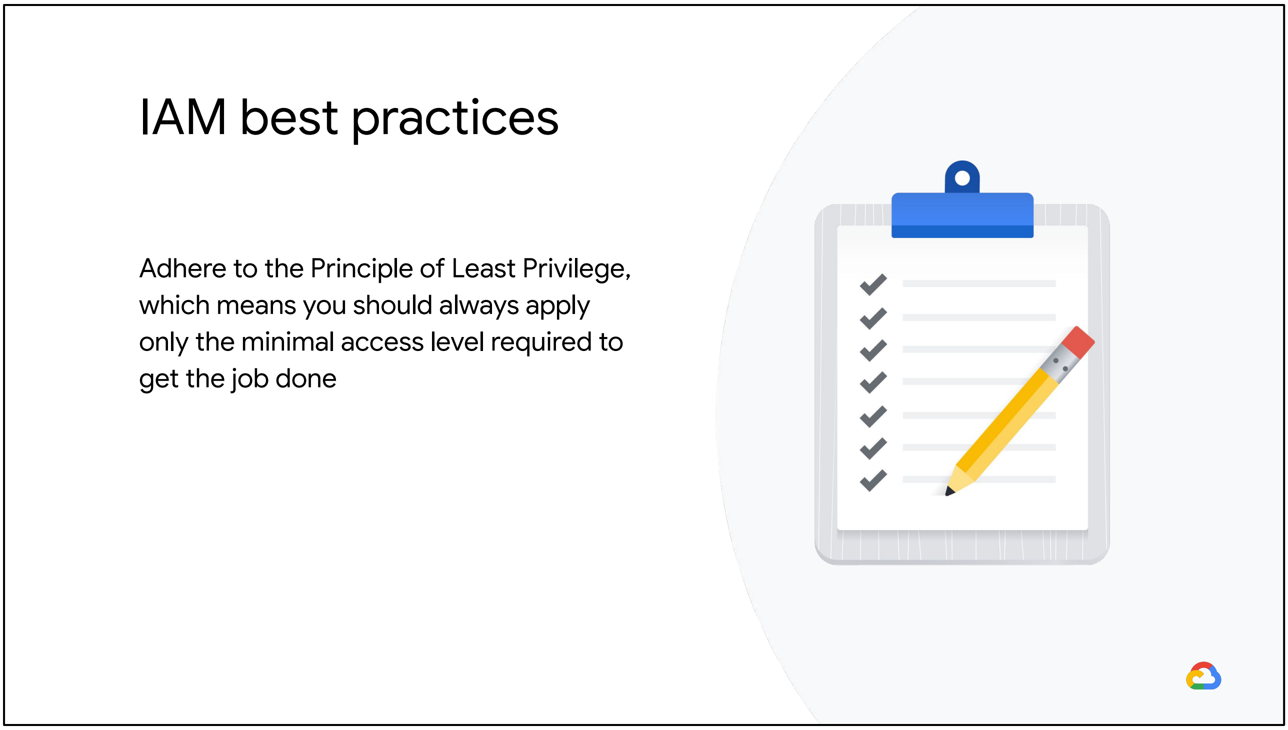


5 IAM troubleshooter

6 IAM audit logs

7 IAM best practices

Now, let’s discuss best practices...

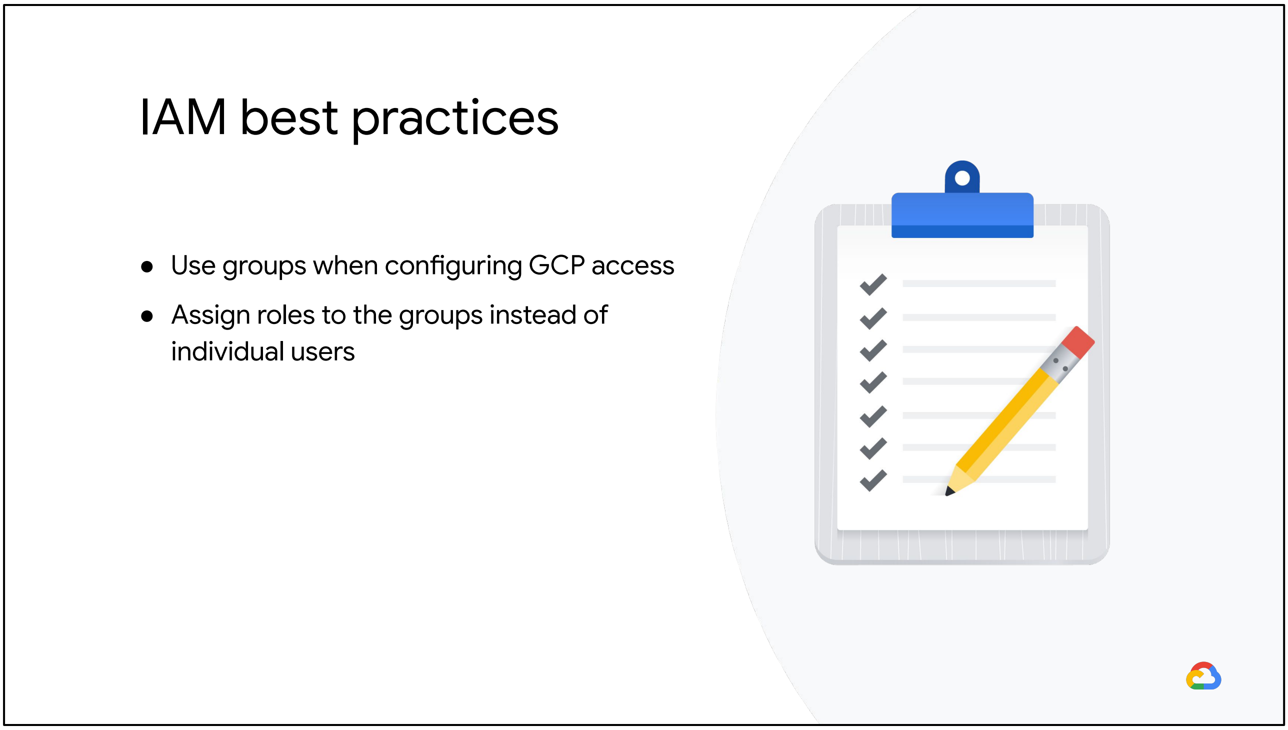


IAM best practices

Adhere to the Principle of Least Privilege, which means you should always apply only the minimal access level required to get the job done

The first is to always use the principle of least privilege - which just means always apply the minimal access level required to get the job done. If a particular role has too many permissions for that job, create a Custom role so you can whittle permissions down to only what is needed.   Not only is this practice more secure, it can also help prevent incidents from occurring - such as the accidental editing or removal of a required resource.

When creating policies, remember that a less restrictive parent policy will always override a more restrictive resource policy, so check when implementing parent policies to make sure you do not inadvertently grant more access to a child resource than you intended. For example, if someone in your organization is a project editor, you cannot restrict their access to a specific resource within that project.

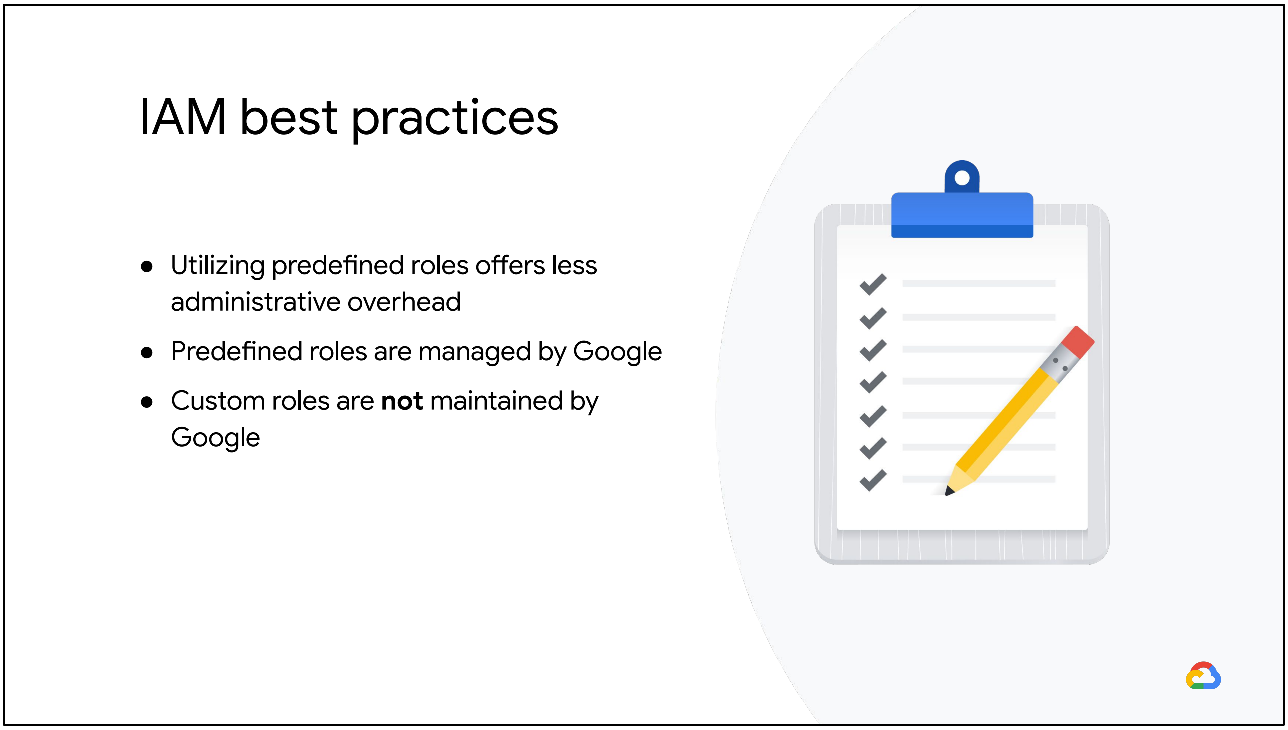


IAM best practices

- Use groups when configuring GCP access
- Assign roles to the groups instead of individual users

It is best to use groups when configuring Google Cloud access - assign roles to the groups instead of individual users.

Groups are defined and maintained in the Cloud Console for G Suite or Cloud Identity domains, they are not configured in Google Cloud, so using groups will drastically reduce the administration needed by Google Cloud admins. Only minimal changes will be needed within Google Cloud once groups and roles are defined. Then users can simply be added or removed from groups by your G Suite or Cloud Identity admin.



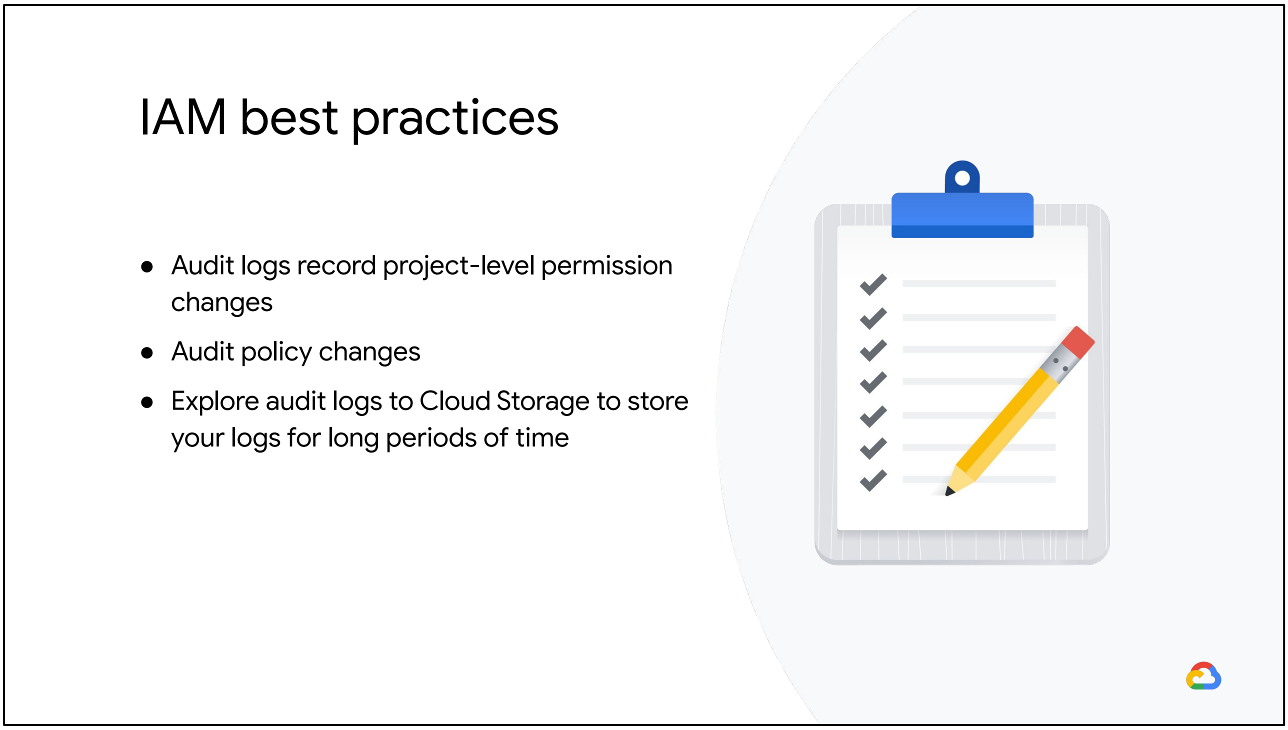
IAM best practices

- Utilizing predefined roles offers less administrative overhead
- Predefined roles are managed by Google
- Custom roles are **not** maintained by Google

Try to utilize predefined roles if they meet your requirements as predefined roles offer less administration. Predefined roles are managed by Google and their permissions are automatically updated as necessary.

For example: when new features or services are added to Google Cloud, all related predefined roles will be updated as needed.

Custom roles on the other hand are not maintained by Google. When new permissions, features, or services are added to Google Cloud, your custom roles will not be updated automatically.

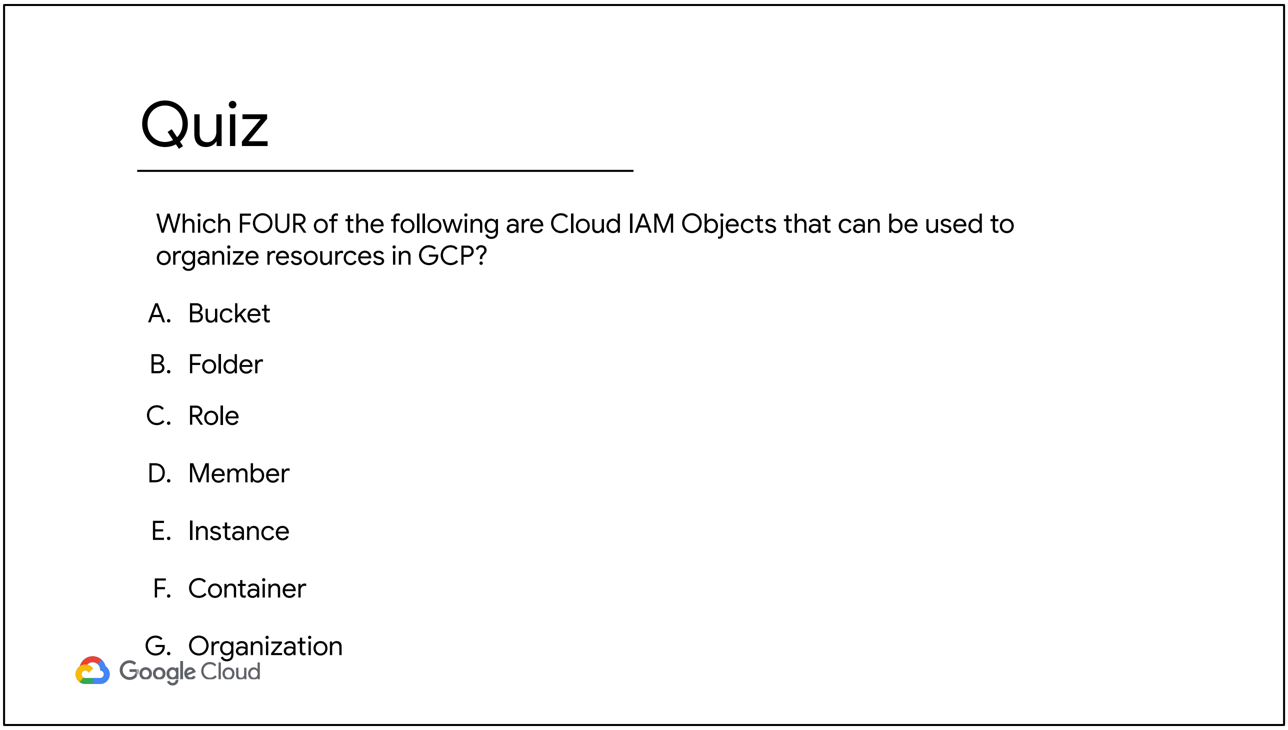


IAM best practices

- Audit logs record project-level permission changes
- Audit policy changes
- Explore audit logs to Cloud Storage to store your logs for long periods of time

Audit logs record project-level permission changes, and these should be used to audit any policy changes made. To perform the audit, export the audit logs to Cloud Storage or BigQuery. This will be covered in more detail in a later module.

Exporting the logs to cloud storage can also allow audit logs to be stored indefinitely.



Quiz

Which FOUR of the following are Cloud IAM Objects that can be used to organize resources in GCP?

A. Bucket

B. Folder

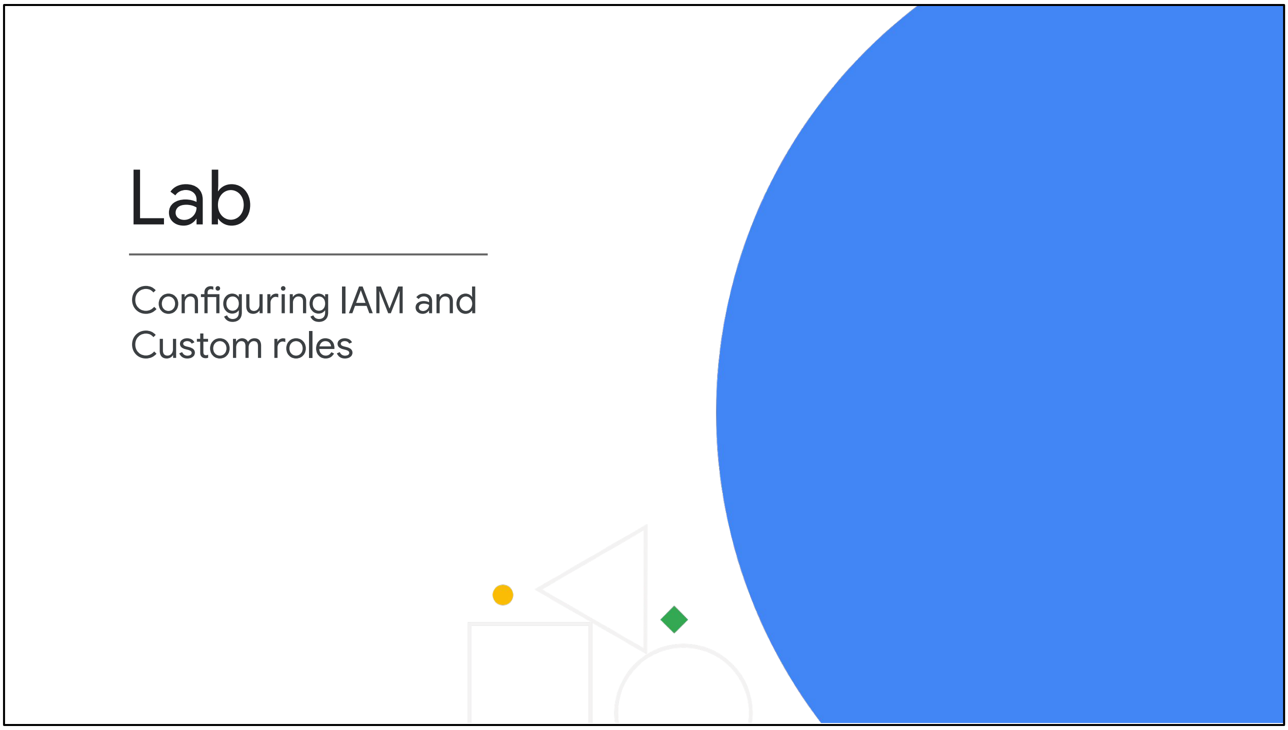
C. Role

D. Member

E. Instance

F. Container

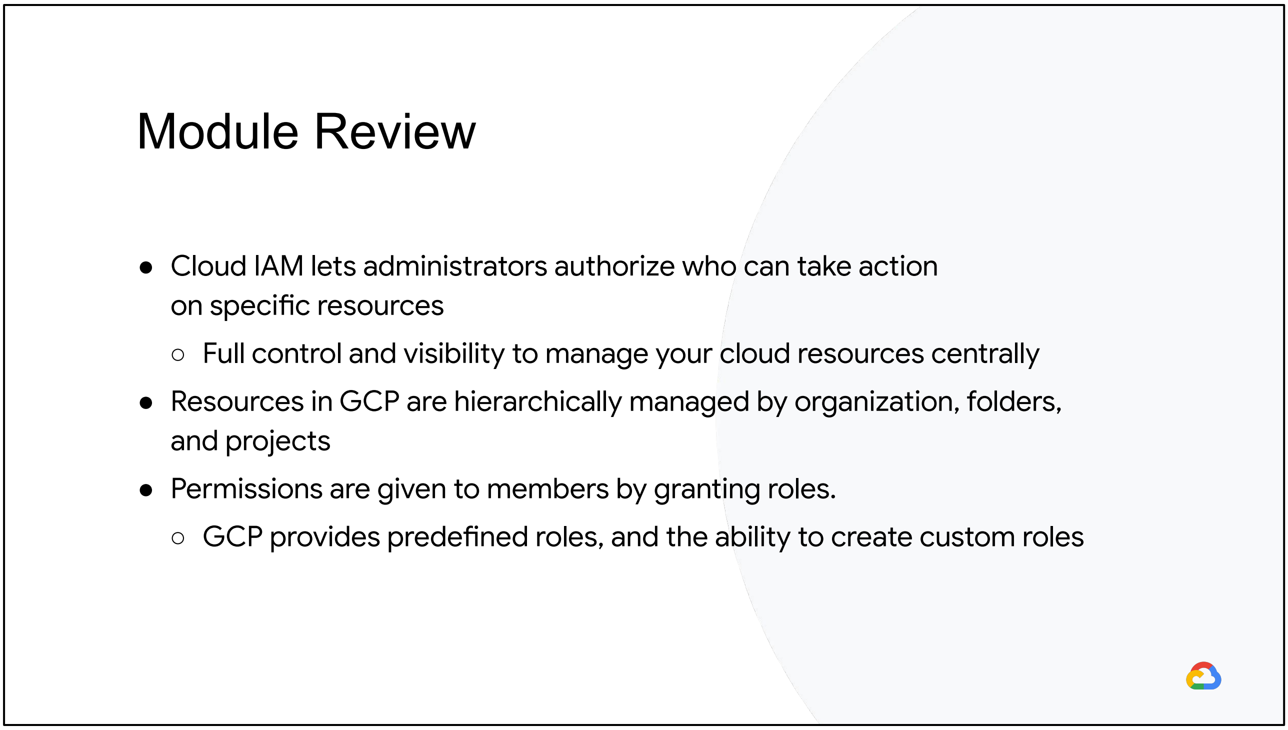
G. Organization



Lab

Configuring IAM and Custom roles

In this lab, you learn how to perform the following tasks:
Use Cloud IAM to implement access control, restrict access to specific features or resources, and use predefined roles to provide Google Cloud access
You also learn how to create and modify custom IAM roles to provide permissions based on your own job roles.



Module Review

- Cloud IAM lets administrators authorize who can take action on specific resources
    - Full control and visibility to manage your cloud resources centrally
- Resources in GCP are hierarchically managed by organization, folders, and projects
- Permissions are given to members by granting roles.
    - GCP provides predefined roles, and the ability to create custom roles