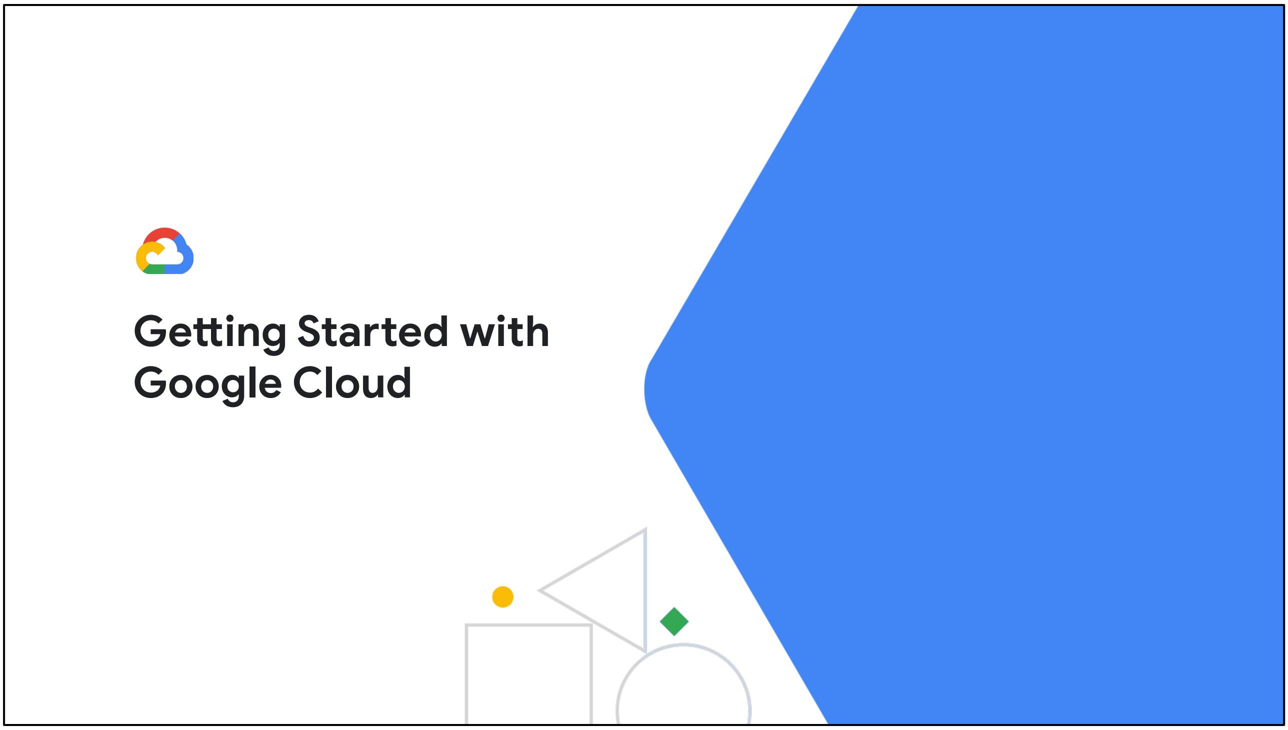


Getting Started with Google Cloud

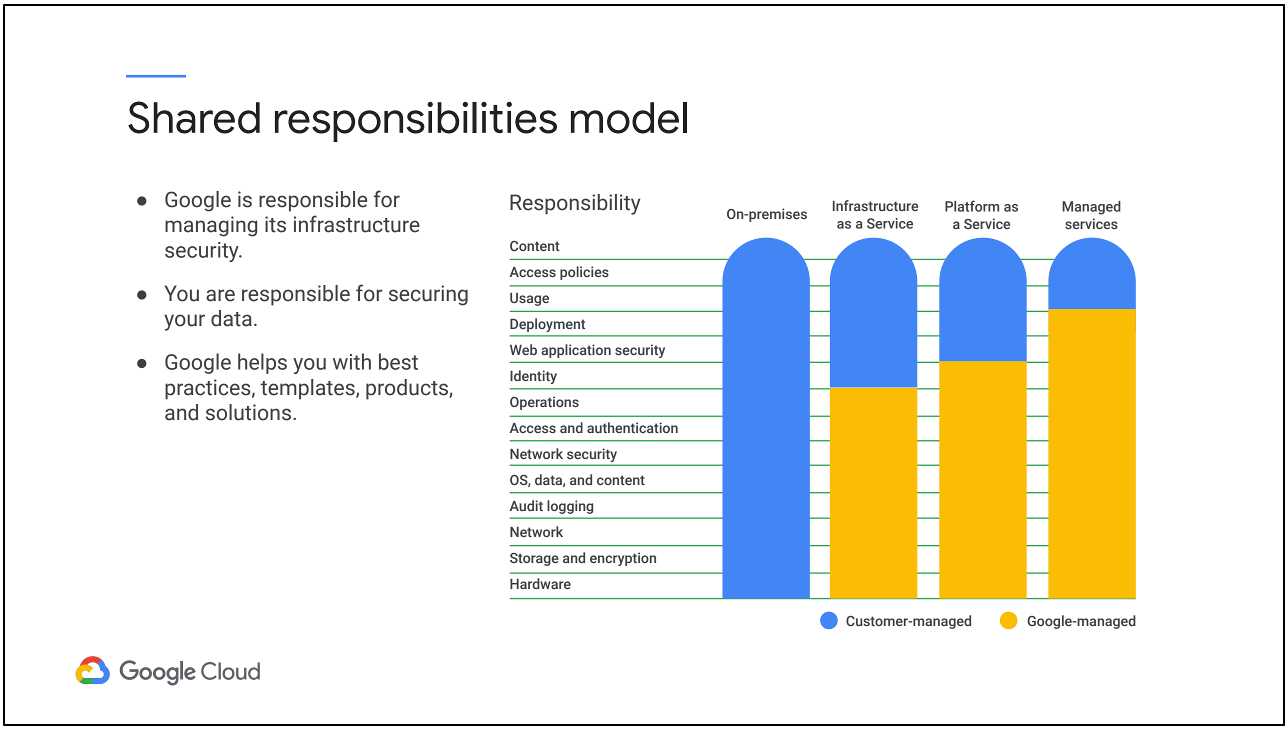
When you run your workloads in Google Cloud, you use projects to organize them. You use Cloud Identity and Access Management, also called “Cloud IAM,” to control who can do what. And you use your choice of several interfaces to connect. In this module, you’ll use these basics to get started.

Projects are the main way you organize the resources you use in Google Cloud. Use them to group together related resources, usually because they have a common business objective.

The principle of least privilege is very important in managing any kind of compute infrastructure, whether it’s in the cloud or on-premises. This principle says that each user should have only those system privileges needed to do their jobs. In a least-privilege environment, people are protected from an entire class of errors. A coworker of mine once accidentally deleted a running production database. Why? Because he was working as the root user on the system when he shouldn’t have been. His name is Brian, and he is still very very sorry! Google Cloud customers use IAM to implement least privilege, and it makes everybody happier.

There are four ways to interact with Google Cloud’s management layer: through the web-based Cloud Console, through the Cloud SDK and its command-line tools, through APIs, and through the mobile app. In this class, you’ll mostly use the Cloud

Console and the command-line tools.



Shared responsibilities model

- Google is responsible for managing its infrastructure security.
- You are responsible for securing your data.
- Google helps you with best practices, templates, products, and solutions.

Google Cloud

When you build an application on your on-premises infrastructure, you're responsible for the entire stack's security: from the physical security of the hardware and the premises in which they are housed, through the encryption of the data on disk, the integrity of your network, and all the way up to securing the content stored in those applications. When you move an application to Google Cloud, Google handles many of the lower layers of security. Because of its scale, Google can deliver a higher level of security at these layers than most of its customers could afford to do on their own.

The upper layers of the security stack remain the customer's responsibility. Google provides tools, such as Cloud Identity and Access Management, to help customers implement the policies they choose at these layers.

Agenda

Google Cloud Resource Hierarchy

Cloud Identity and Access Management (Cloud IAM)

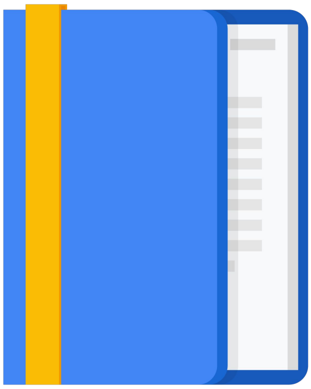
Cloud Identity

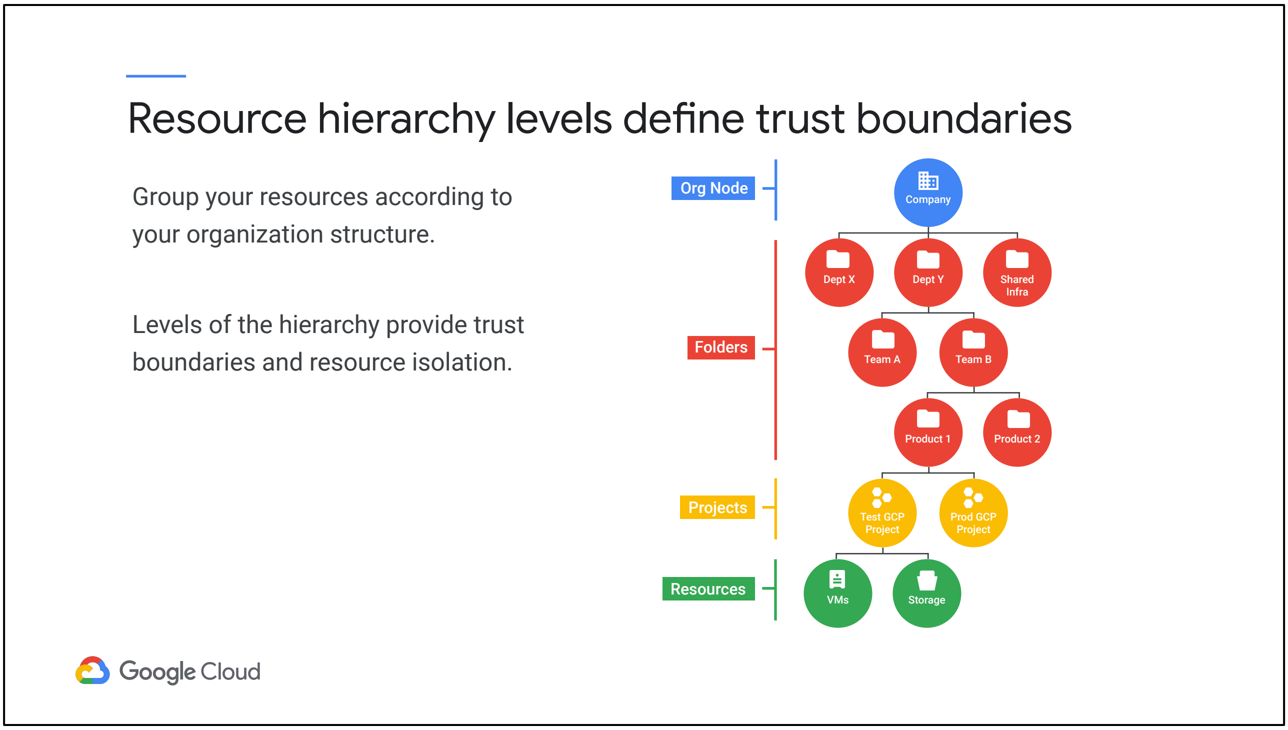
Interacting with Google Cloud

Google Cloud Marketplace

Quiz and Lab

Resources





Resource hierarchy levels define trust boundaries

Group your resources according to your organization structure.

Levels of the hierarchy provide trust boundaries and resource isolation.

Org Node
Company

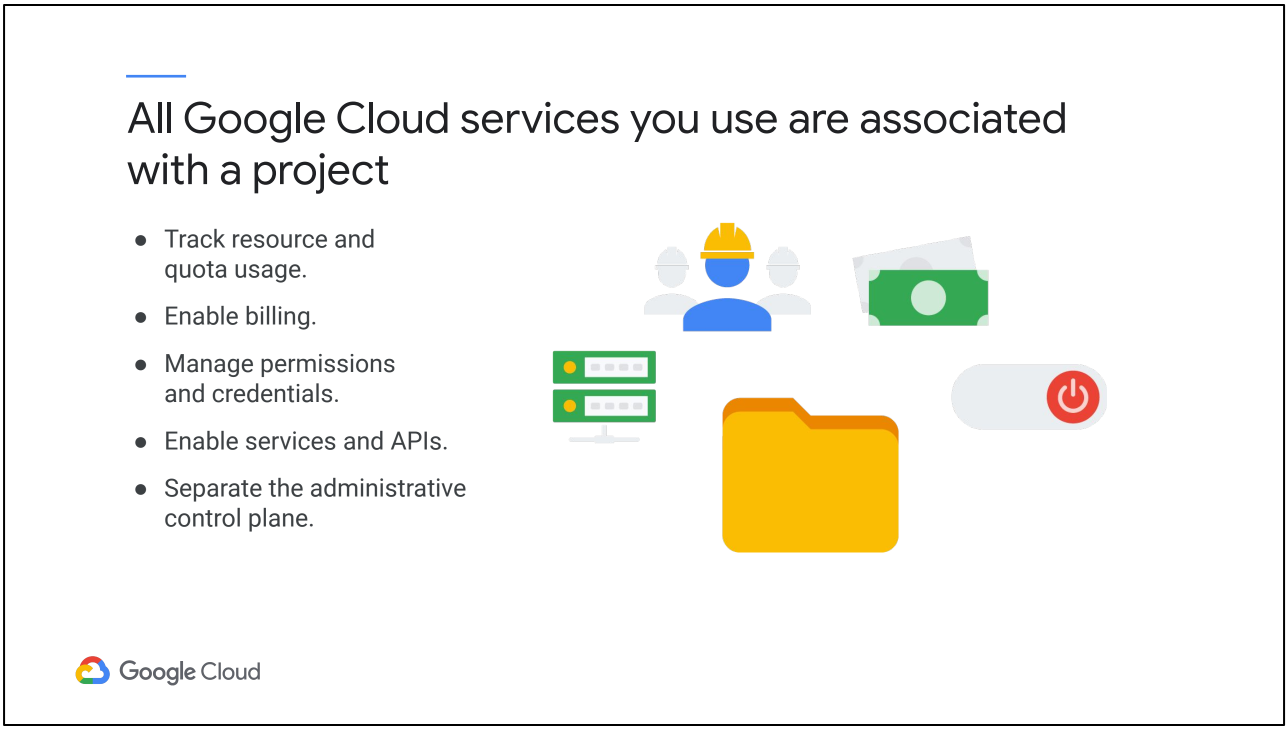
Folders
Dept X
Dept Y
Shared Infra
Team A
Team B
Product 1
Product 2

Projects
Test GCP Project
Prod GCP Project

Resources
VMs
Storage

You may find it easiest to understand the Google Cloud resource hierarchy from the bottom up. All the resources you use--whether they're virtual machines, Cloud Storage buckets, tables in BigQuery, or anything else in Google Cloud--are organized into projects. Optionally, these projects may be organized into folders; folders can contain other folders. All the folders and projects used by your organization can be brought together under an organization node. Projects, folders, and organization nodes are all places where policies can be defined. Some Google Cloud resources let you put policies on individual resources too, like Cloud Storage buckets. (This course discusses Cloud Storage buckets later in the course.)

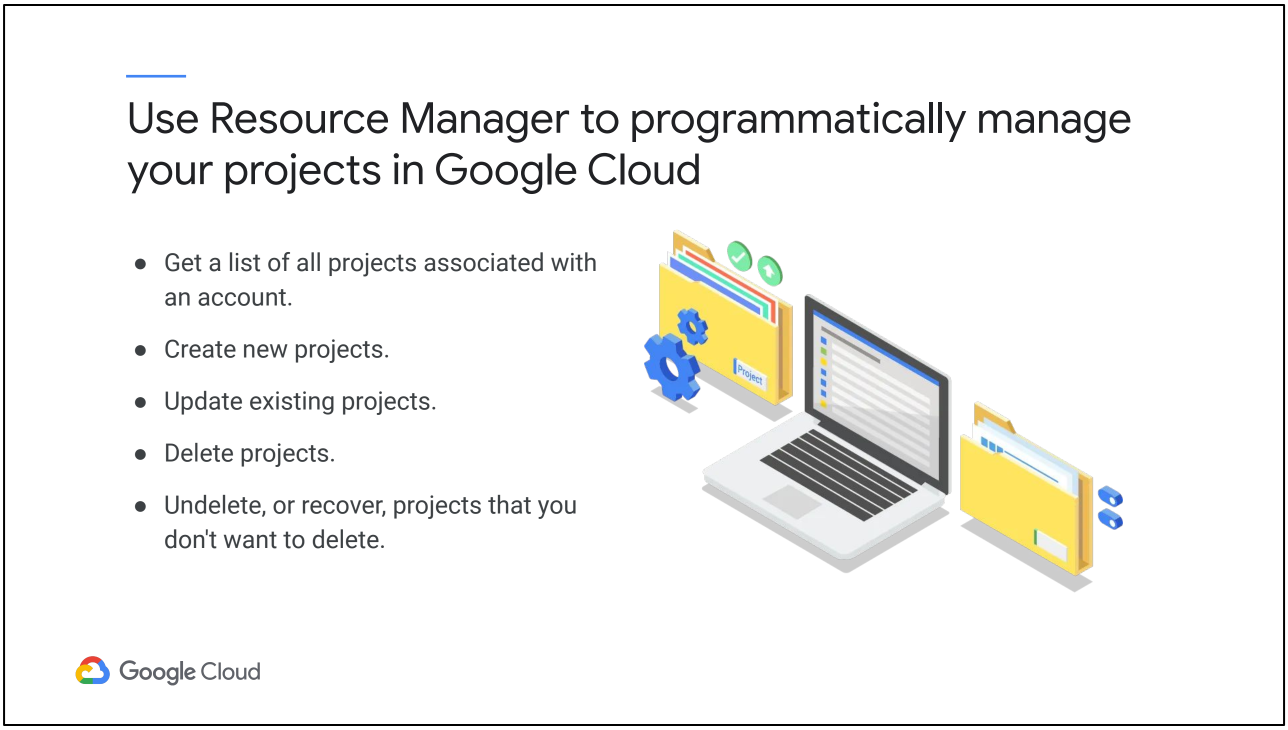
Policies are inherited downwards in the hierarchy.



All Google Cloud services you use are associated with a project

- Track resource and quota usage.
- Enable billing.
- Manage permissions and credentials.
- Enable services and APIs.
- Separate the administrative control plane.

All Google Cloud resources belong to a Google Cloud project. Projects are the basis for enabling and using Google Cloud services, like managing APIs, enabling billing, adding and removing collaborators, and enabling other Google services. Each project is a separate compartment, and each resource belongs to exactly one. Projects can have different owners and users. They're billed separately, and they're managed separately.



Use Resource Manager to programmatically manage your projects in Google Cloud

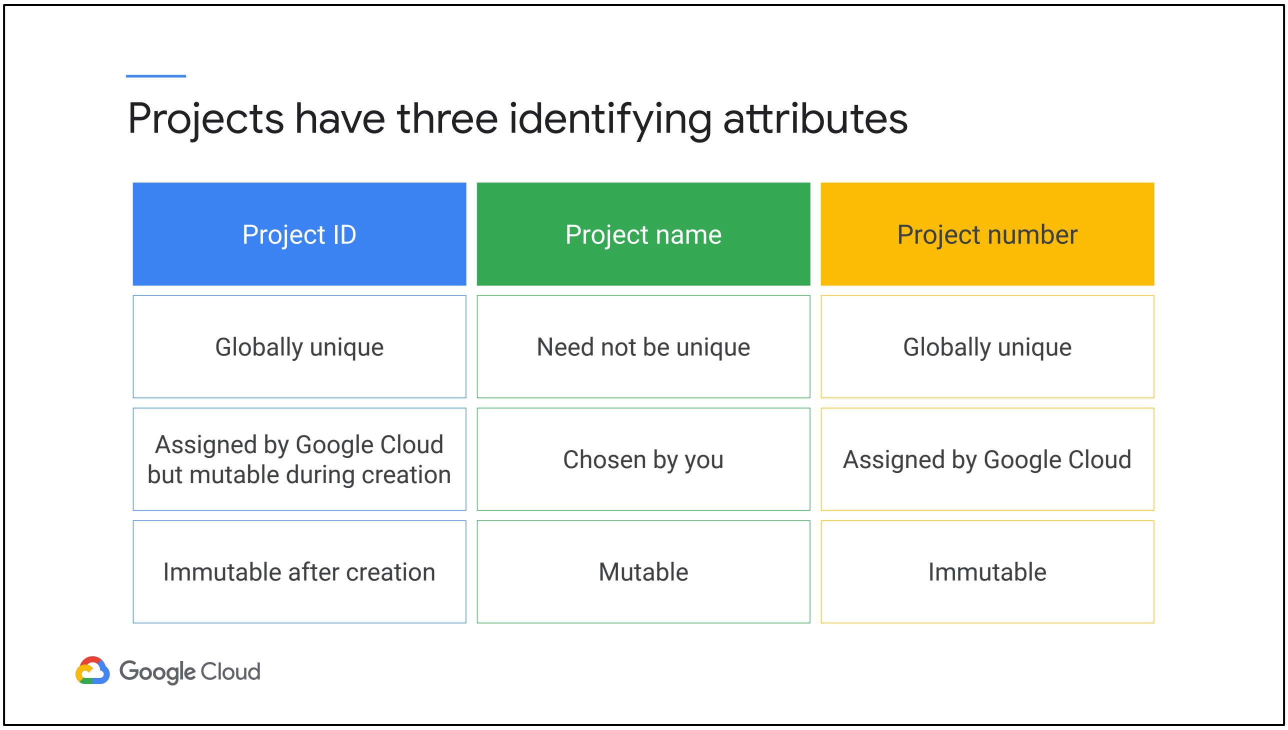
- Get a list of all projects associated with an account.
- Create new projects.
- Update existing projects.
- Delete projects.
- Undelete, or recover, projects that you don't want to delete.

Resource Manager provides methods that you can use to programmatically manage your projects in Google Cloud. With this API, you can do the following:

- Get a list of all projects associated with an account.
- Create new projects.
- Update existing projects.
- Delete projects.
- Undelete, or recover, projects that you don't want to delete.

You can access Resource Manager in either of the following ways:

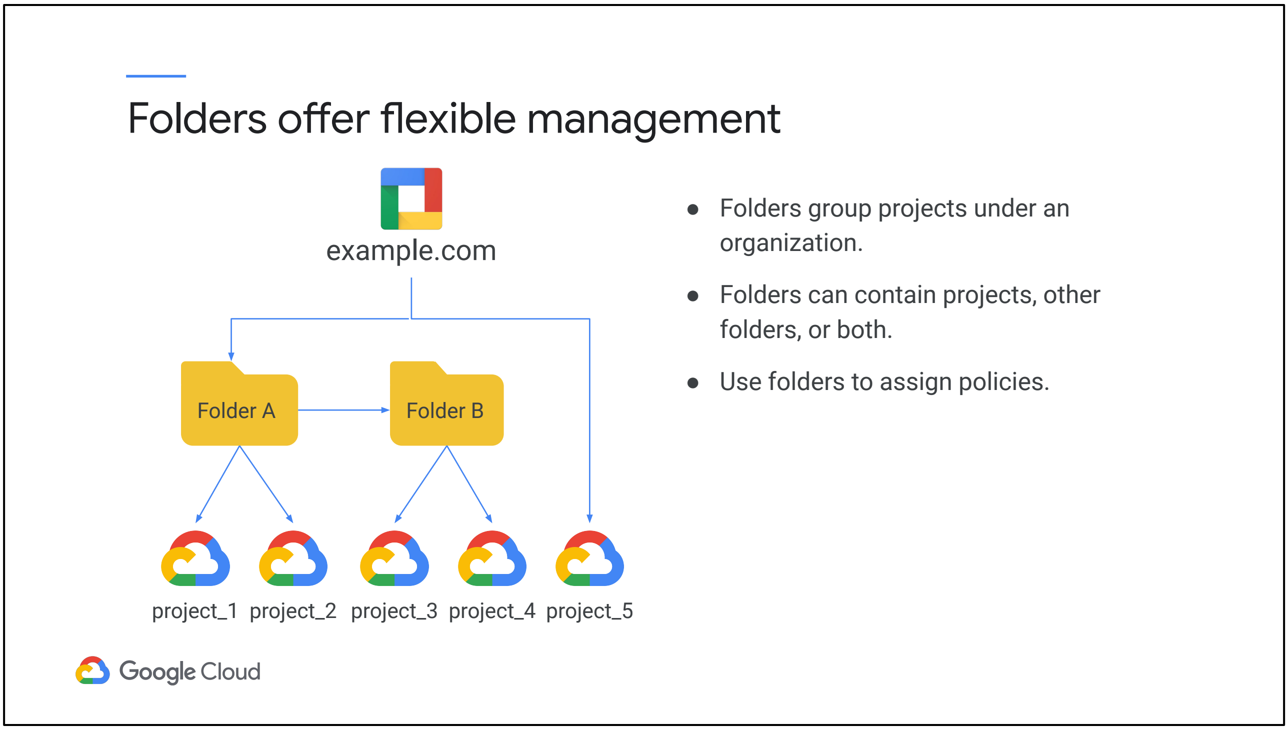
- Through the RPC API
- Through the REST API



Projects have three identifying attributes

Project ID	Project name	Project number
Globally unique	Need not be unique	Globally unique
Assigned by Google Cloud but mutable during creation	Chosen by you	Assigned by Google Cloud
Immutable after creation	Mutable	Immutable

Each Google Cloud project has a name and project ID you assign. The project ID is a permanent, unchangeable identifier, and it has to be unique across Google Cloud. You'll use project IDs in several contexts to tell Google Cloud which project you want to work with. On the other hand, project names are for your convenience, and you can change them. Google Cloud also assigns each of your projects a unique project number, and you'll see it displayed to you in various contexts, but using it is mostly outside the scope of this course. In general, project IDs are made to be human-readable strings, and you'll use them frequently to refer to projects.



Folders offer flexible management

example.com

Folder A

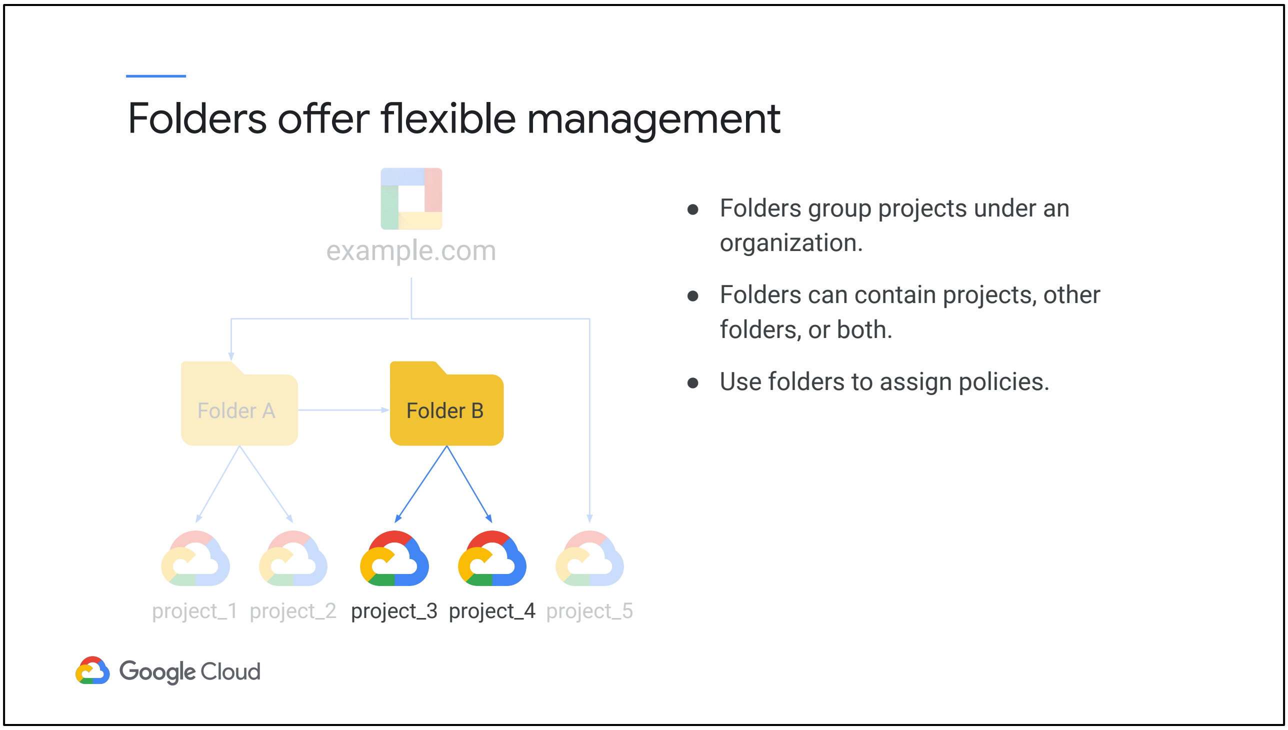
Folder B

project_1 project_2 project_3 project_4 project_5

- Folders group projects under an organization.
- Folders can contain projects, other folders, or both.
- Use folders to assign policies.

Google Cloud

You can organize projects into folders, although you don’t have to. They’re a tool at your disposal to make your life easier. For example, you can use folders to represent different departments, teams, applications or environments in your organization. Folders let teams have the ability to delegate administrative rights, so that they can work independently.



Folders offer flexible management

example.com

Folder A

Folder B

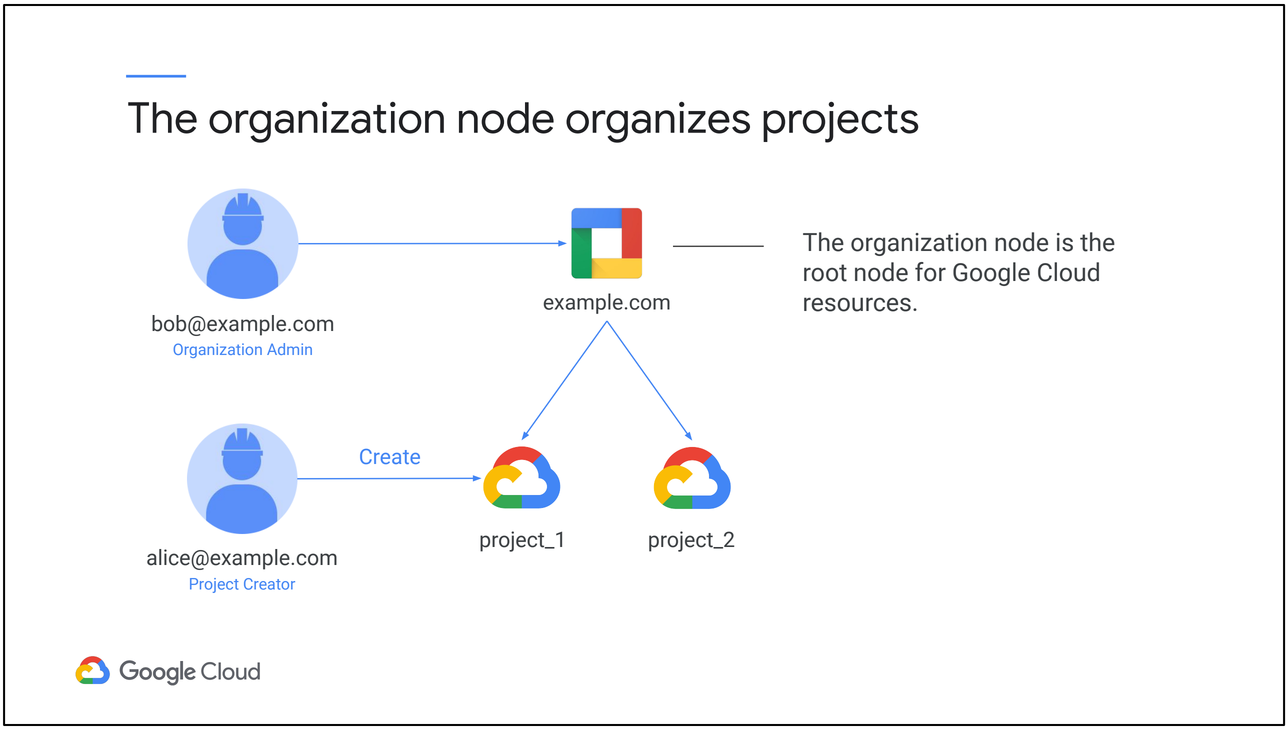
project_1 project_2 project_3 project_4 project_5

- Folders group projects under an organization.
- Folders can contain projects, other folders, or both.
- Use folders to assign policies.

Google Cloud

The resources in a folder inherit IAM policies from the folder. So, if project 3 and project 4 are administered by the same team by design, you can put IAM policies onto Folder B instead. Doing it the other way-- putting duplicate copies of those policies on project 3 and project 4-- would be tedious and error-prone.

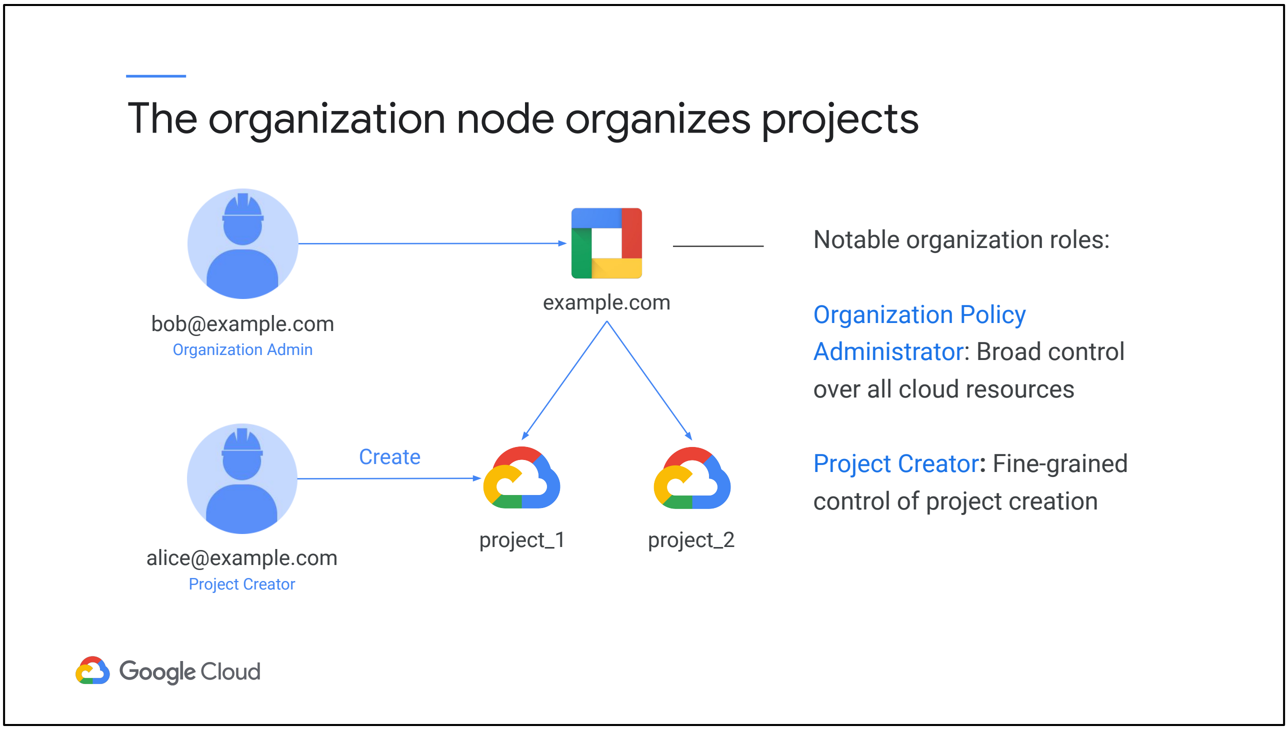
One word of caution: to use folders, you need an organization node at the top of the hierarchy.



The organization node organizes projects

The organization node is the root node for Google Cloud resources.

You probably want to organize all the projects in your company into a single structure. Most companies want the ability to apply to have centralized visibility of how resources are being used, and also to apply policies centrally. That’s what the organization node is for. It’s the top of the hierarchy.



The organization node organizes projects

Notable organization roles:

Organization Policy Administrator: Broad control over all cloud resources

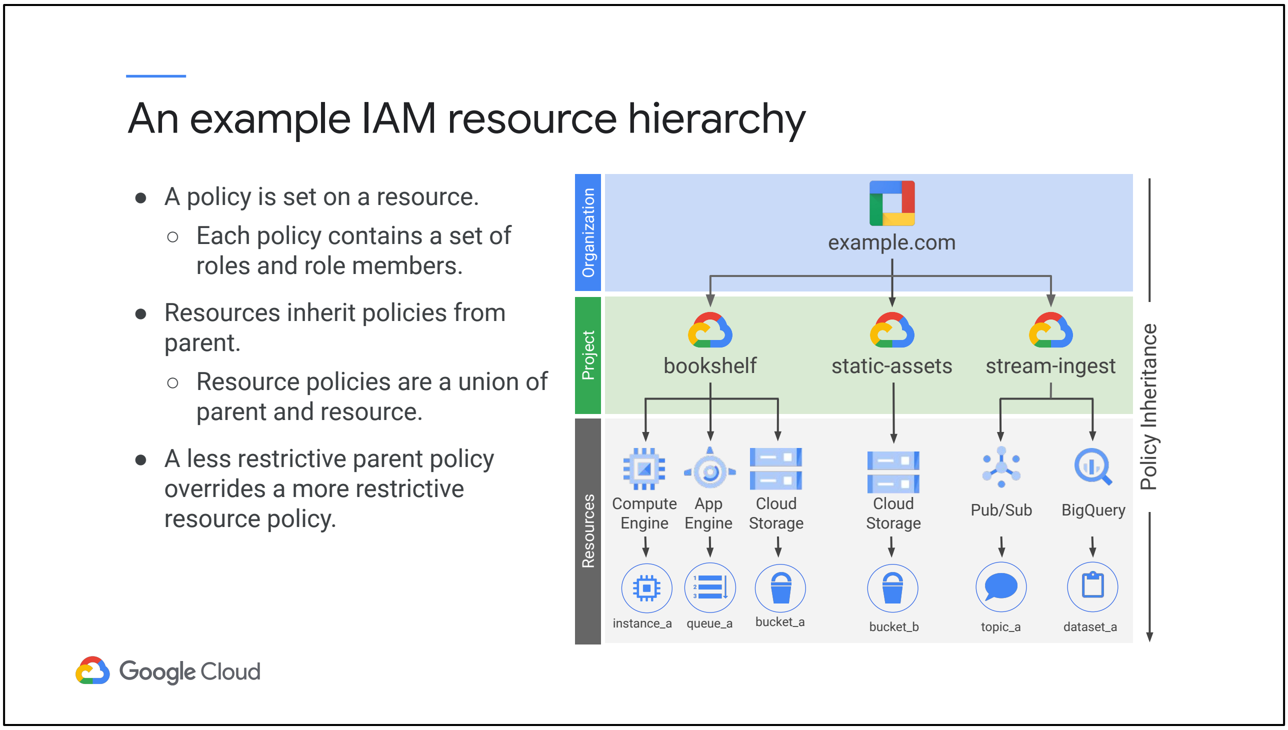
Project Creator: Fine-grained control of project creation

There are some special roles associated with it. For example, you can designate an organization policy administrator, so that only people with privilege can change policies. You can also assign a project creator role, which is a great way to control who can spend money.

So how do you get an organization node? In part the answer depends on whether your company is also a Google Workspace customer. If you have a Workspace domain, Google Cloud projects will automatically belong to your organization node. Otherwise, you can use Google Cloud Identity to create one.

Here’s a tip: when you get a new organization node, it lets anyone in the domain create projects and billing accounts, just as they could before. That’s to avoid surprises and disruption. But it’d be a great first step with a new organization node to decide who on your team really should be able to do those things.

Once you have an organization node, you can create folders underneath it and put projects in.



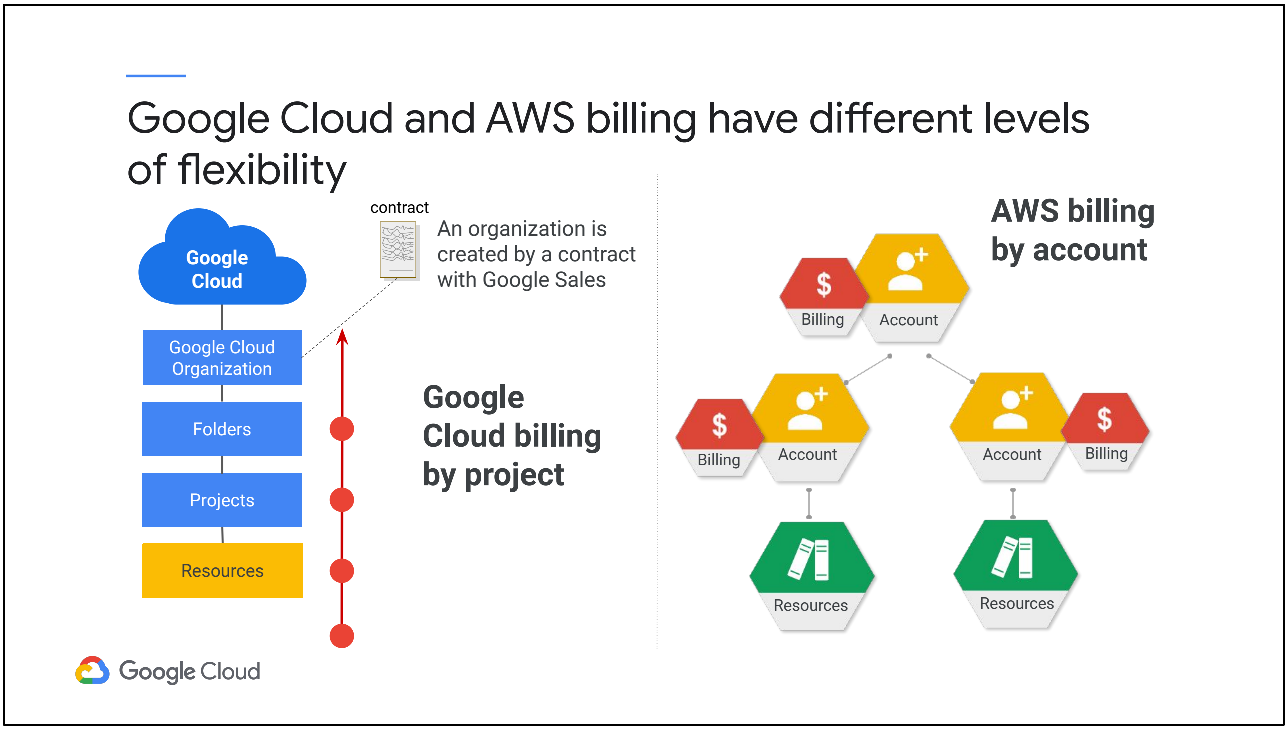
An example IAM resource hierarchy

- A policy is set on a resource.
  - Each policy contains a set of roles and role members.
- Resources inherit policies from parent.
  - Resource policies are a union of parent and resource.
- A less restrictive parent policy overrides a more restrictive resource policy.

Here's an example of how you might organize your resources. There are three projects, each of which uses resources from several Google Cloud services. In this example, we haven't used any folders, although we always could move projects into folders if that became helpful.

Resources inherit the policies of their parent resource. For instance, if you set a policy at the organization level, it is automatically inherited by all its children projects. And this inheritance is transitive, which means that all the resources in those projects inherit the policy too.

There's one important rule to keep in mind. The policies implemented at a higher level in this hierarchy can't take away access that's granted at lower level. For example, suppose that a policy applied on the "bookshelf" project gives user Pat the right to modify a Cloud Storage bucket. But a policy at the organization level says that Pat can only view Cloud Storage buckets, not change them. The more generous policy takes effect. Keep this in mind as you design your policies.



Google Cloud and AWS billing have different levels of flexibility

An organization is created by a contract with Google Sales

Google Cloud billing by project

AWS billing by account

The resources hierarchy is different between Google Cloud and AWS, which results in differences in billing.

For Google Cloud, all resources and services must be leveraged in a project and everything built in a project is billed to that project.

Google Cloud provides a flexible billing mode:
Each project can have its own billing account,
One billing account can be used for the entire organization, or
Any combination can be configured as needed.

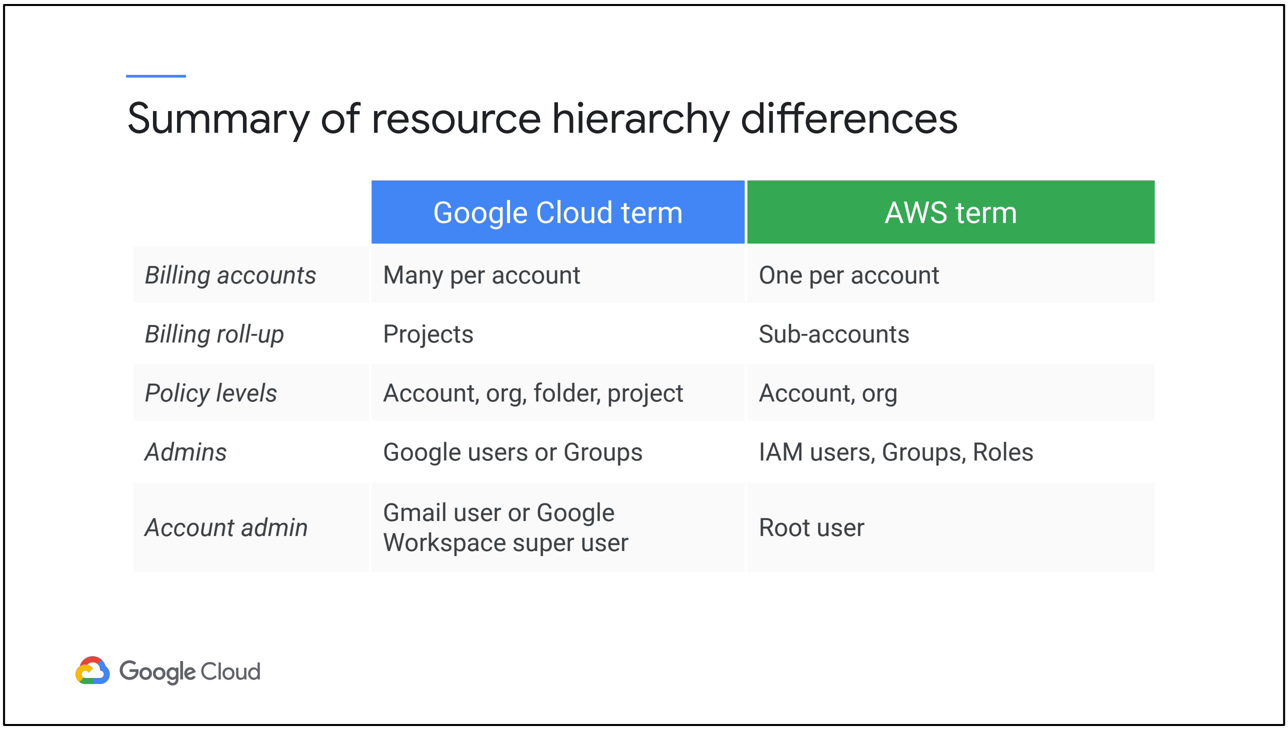
In this diagram, billing starts from the bottom up. Resources bill to projects, but billing can also be applied at the folder or organization levels.

By default, each AWS account has its own billing account. To combine multiple accounts to a single billing account, you have to set up consolidated billing, which creates a single account that will link to a group of subordinate accounts.

Each account will have its own root, or super user, to control the account. Root users have access to all resources in their account, but no other.

The linking structure can become complex with more accounts. You can also consolidate multiple accounts into a single organization that you create and centrally manage.

You can group your accounts for consolidated billing and attach policies that block access to services for users or roles in an account, and these policies override the account policies.



Summary of resource hierarchy differences

	Google Cloud term	AWS term
Billing accounts	Many per account	One per account
Billing roll-up	Projects	Sub-accounts
Policy levels	Account, org, folder, project	Account, org
Admins	Google users or Groups	IAM users, Groups, Roles
Account admin	Gmail user or Google Workspace super user	Root user

Google Cloud

The key Google Cloud resource differentiators are multiple billing accounts, billing grouped by projects, and simpler hierarchical administration.

- With Google Cloud, you have the flexibility to have many billing accounts per Google Cloud account, whereas you need one billing account per AWS account.
- Google Cloud can roll up billing by project, whereas AWS rolls up billing by Sub-account.
- You can apply policies in Google Cloud at the Account, Organization, Folder or Project level. In AWS, policies can only be applied at the Account and Organization level.
- Account admins can be Google Users or Groups in Google Cloud. In AWS, you use IAM Users with Groups and Roles for account admins.
- Google Cloud accounts can have a Gmail user or Google Workspace super user as an admin; AWS requires its own root user to administer the account.

Agenda

Google Cloud Resource Hierarchy

Cloud Identity and Access Management (Cloud IAM)

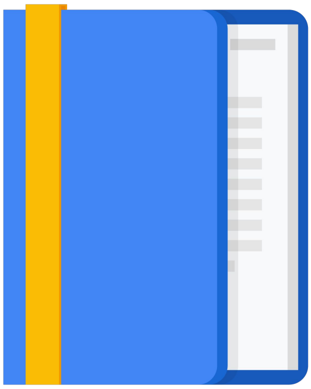
Cloud Identity

Interacting with Google Cloud

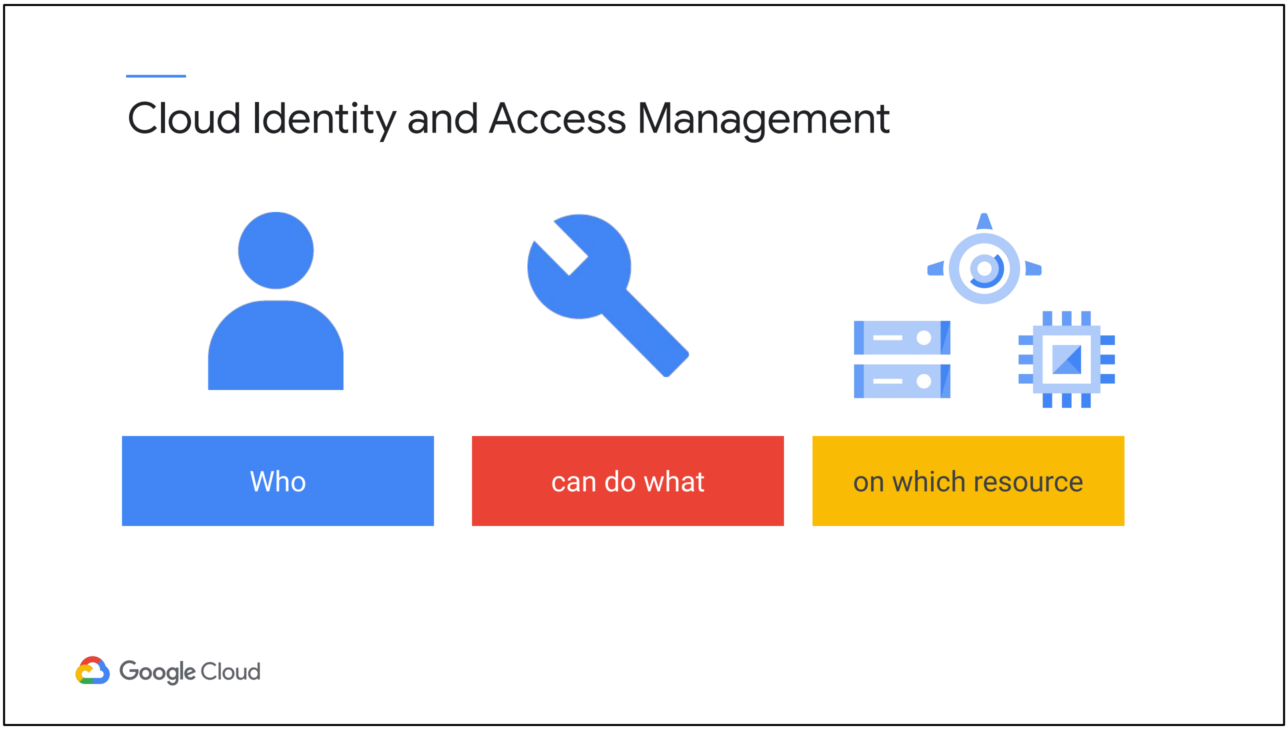
Google Cloud Marketplace

Quiz and Lab

Resources



Google Cloud



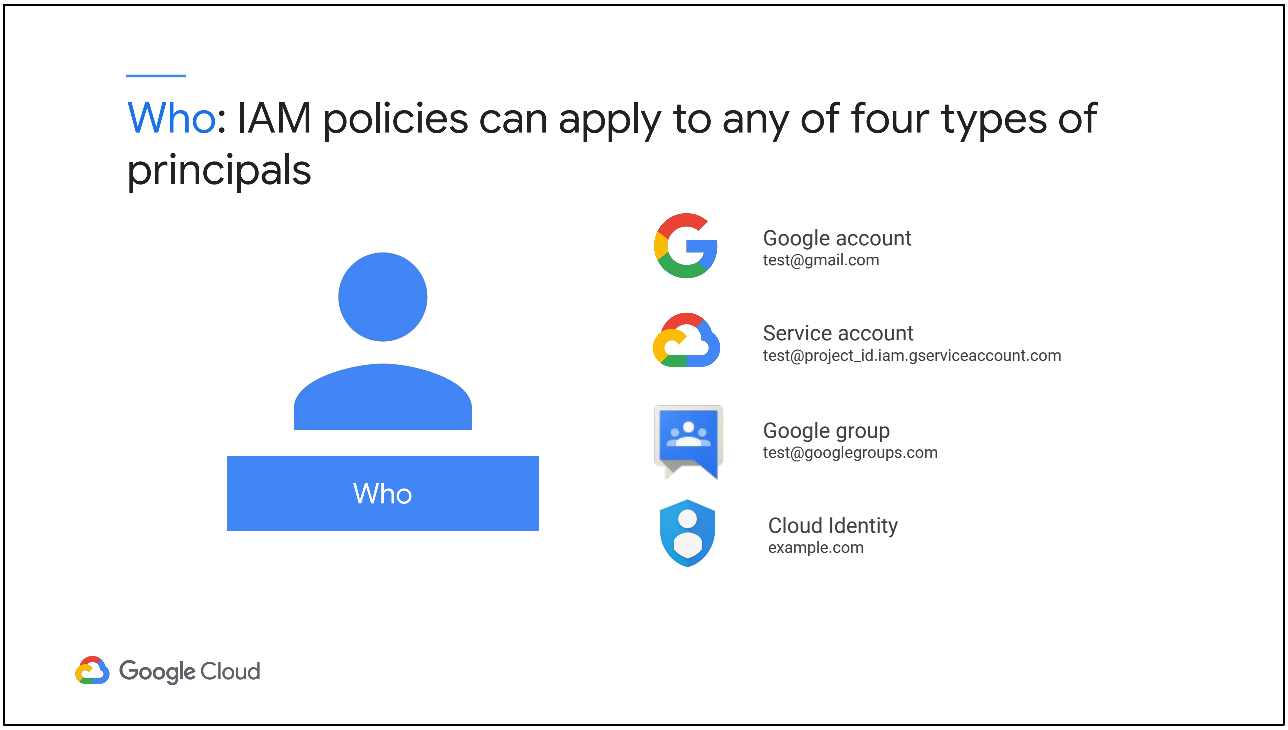
Cloud Identity and Access Management

Who

can do what

on which resource

IAM lets administrators authorize who can take action on specific resources. An IAM policy has a “who” part, a “can do what” part, and an “on which resource” part.



Who: IAM policies can apply to any of four types of principals

Who

Google account
test@gmail.com

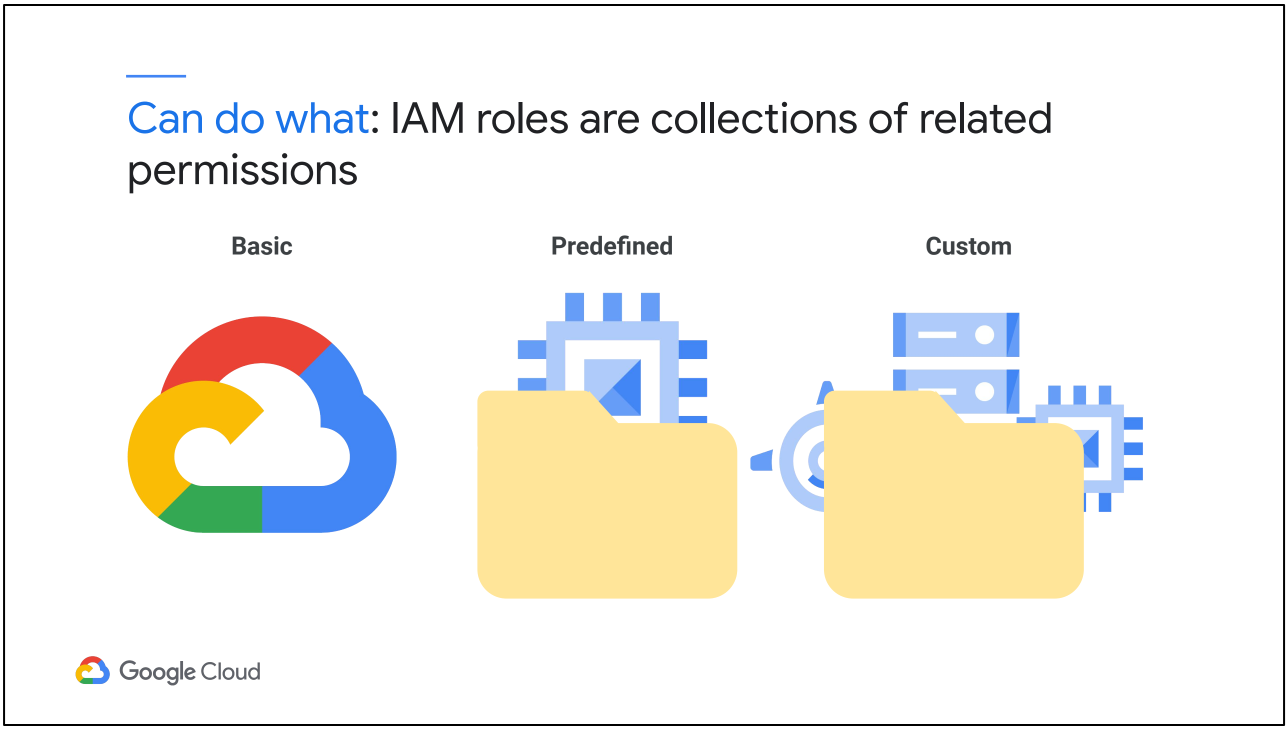
Service account
test@project_id.iam.gserviceaccount.com

Google group
test@googlegroups.com

Cloud Identity
example.com

Google Cloud

The “who” part of an IAM policy can be a Google account, a Google group, a service account, or an entire Workspace or Cloud Identity domain.



Can do what: IAM roles are collections of related permissions

Basic

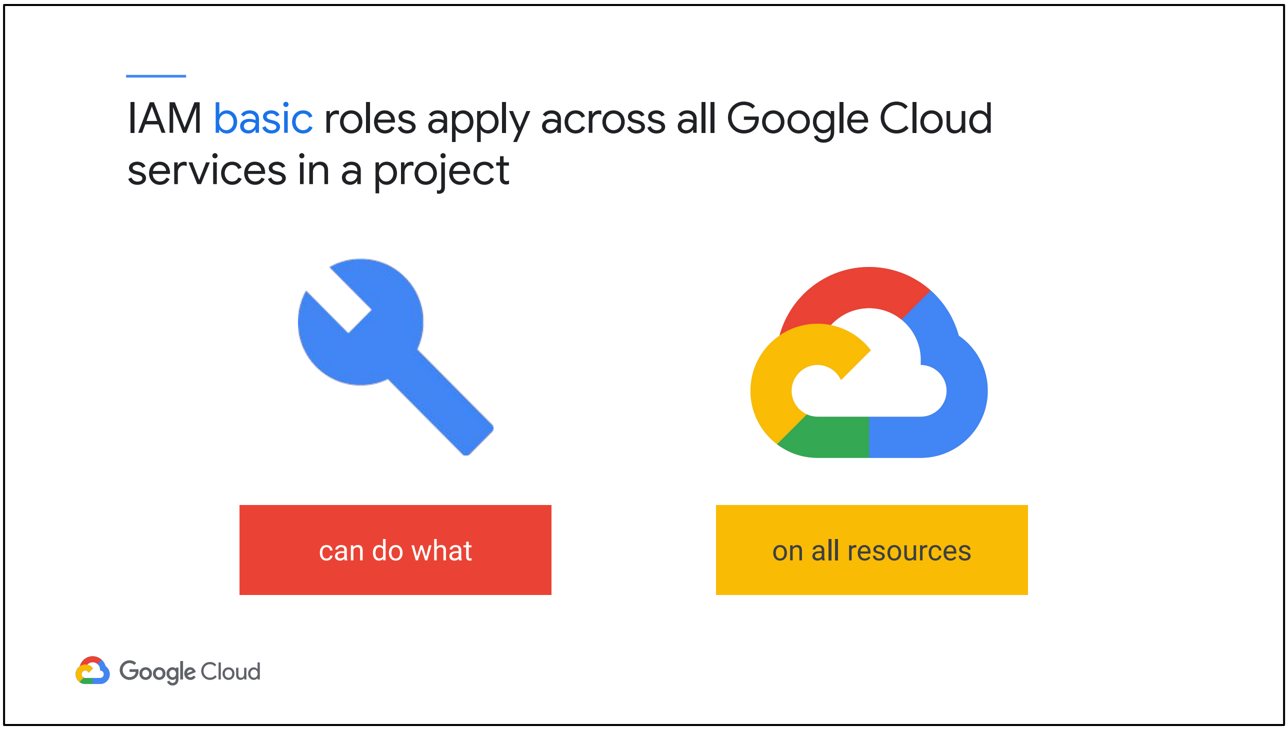
Predefined

Custom

Google Cloud

The “can do what” part of an IAM policy is defined by a role. An IAM role is a collection of permissions, because, most of the time you need more than 1 permission to do meaningful work. For example, to manage virtual machine instances in a project, you have to be able to create, delete, start, stop and change virtual machines. So these permissions are grouped together into a role to make them easier to understand and easier to manage.

There are three kinds of roles in Cloud IAM. Let’s talk about each in turn.



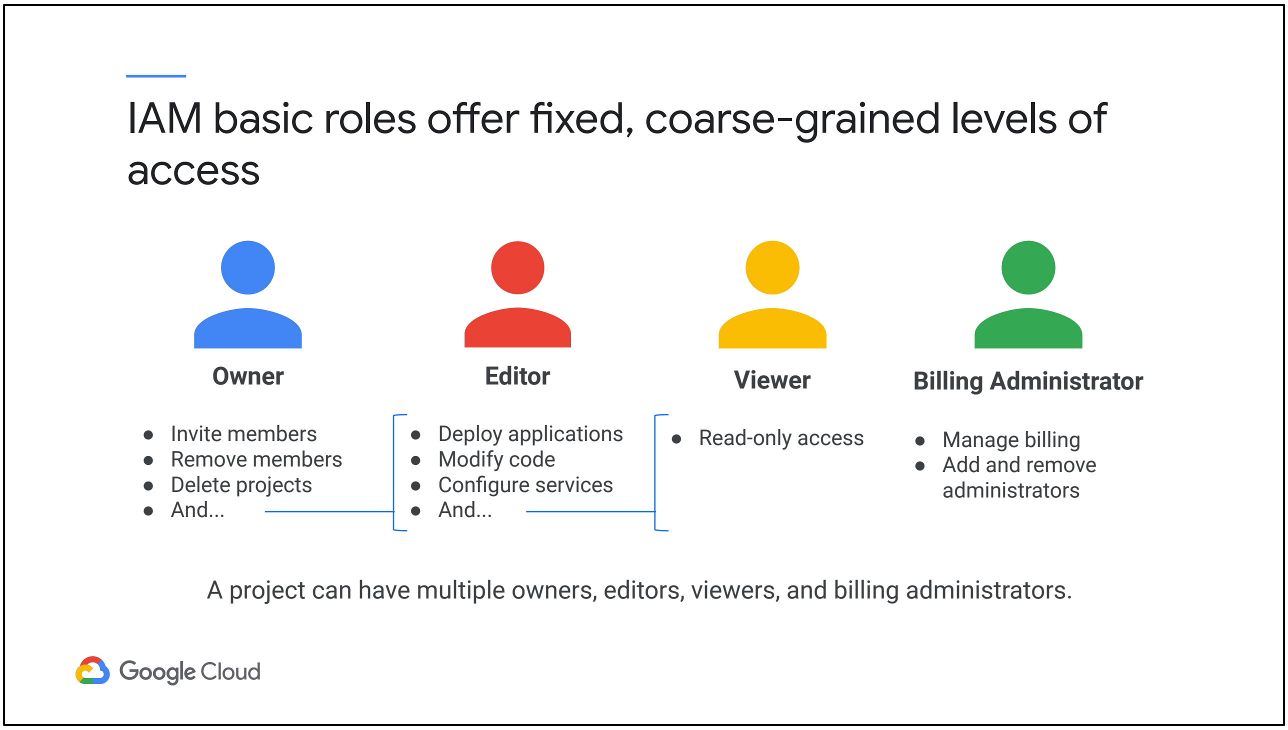
IAM basic roles apply across all Google Cloud services in a project

can do what

on all resources

Google Cloud

Basic roles are broad. You apply them to a Google Cloud project, and they affect all resources in that project.



IAM basic roles offer fixed, coarse-grained levels of access

Owner

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

Editor

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

Viewer

- Read-only access

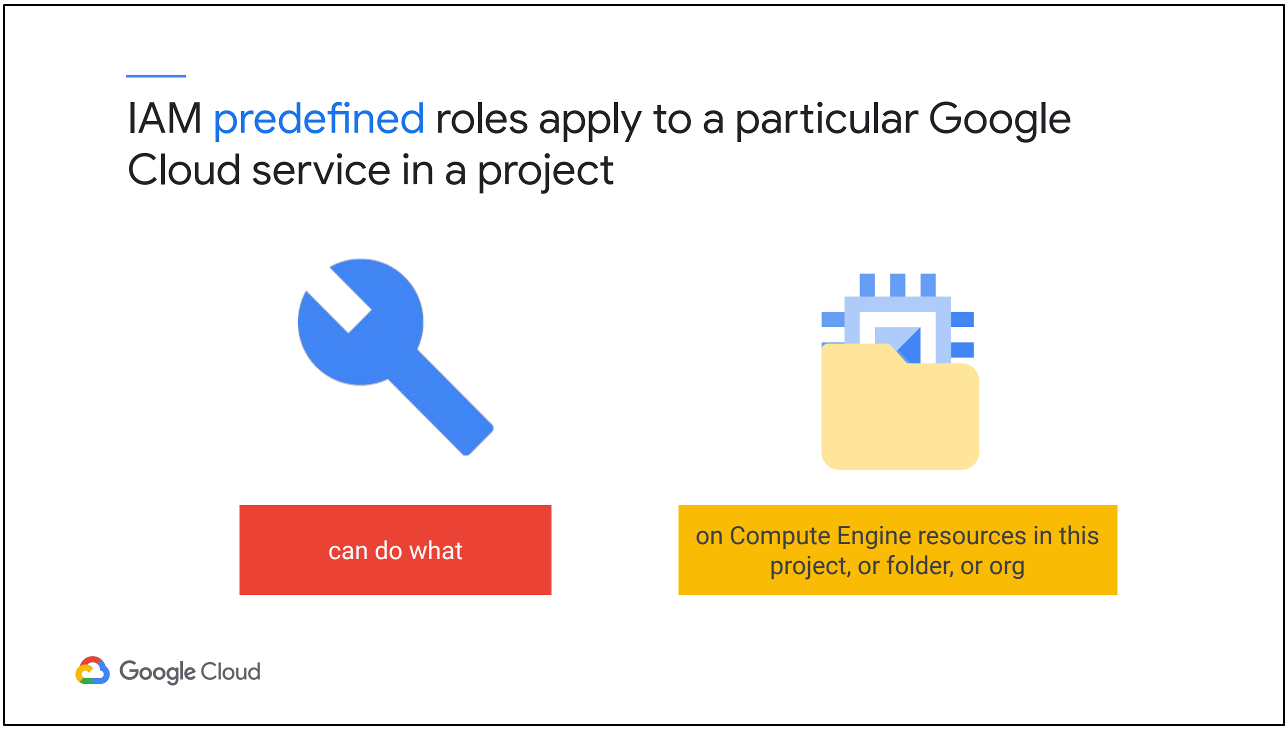
Billing Administrator

- Manage billing
- Add and remove administrators

A project can have multiple owners, editors, viewers, and billing administrators.

These are the Owner, Editor, and Viewer roles. If you're a viewer on a given resource, you can examine it but not change its state. If you're an editor, you can do everything a viewer can do plus change its state. And if you're an owner, you can do everything an editor can do plus manage roles and permissions on the resource. The owner role on a project lets you do one more thing too: you can set up billing. Often companies want someone to be able to control the billing for a project without the right to change the resources in the project, and that's why you can grant someone the billing administrator role.

Be careful! If you have several people working together on a project that contains sensitive data, basic roles are probably too coarse a tool. Fortunately, Google Cloud IAM provides finer-grained types of roles.



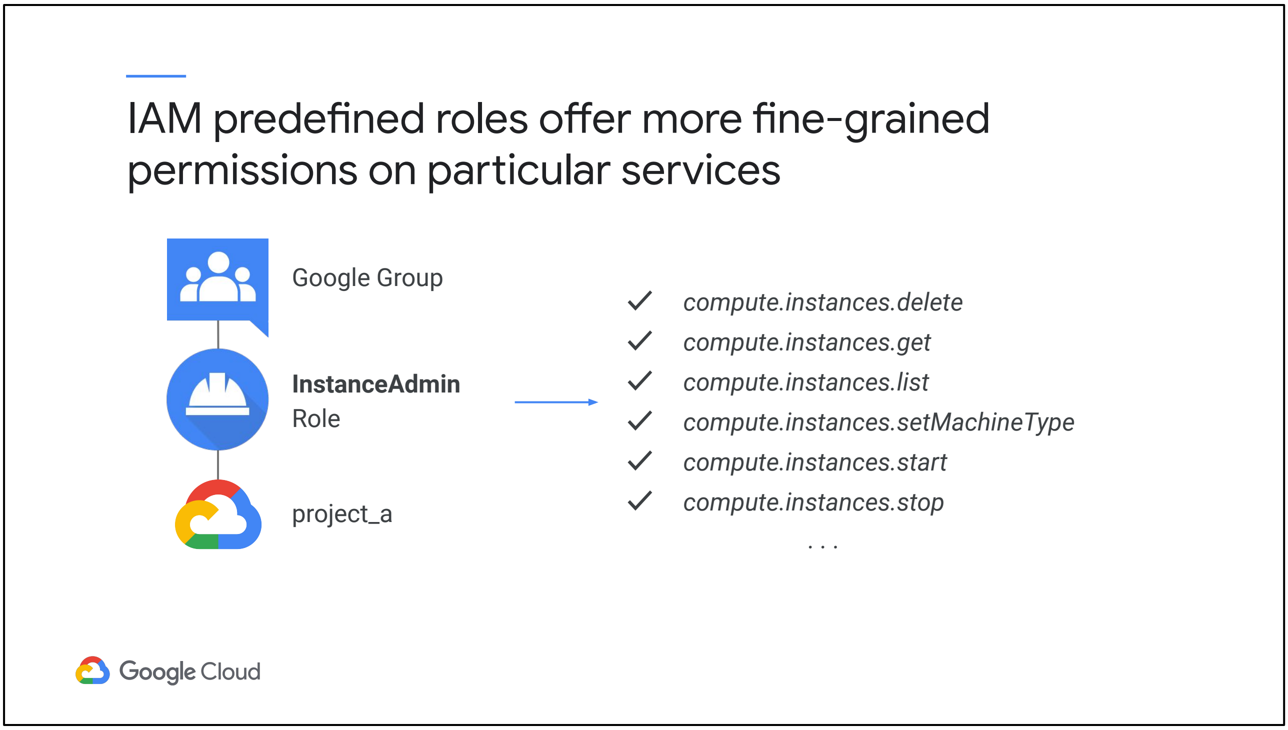
IAM predefined roles apply to a particular Google Cloud service in a project

can do what

on Compute Engine resources in this project, or folder, or org

Google Cloud services offers their own sets of predefined roles, and they define where those roles can be applied. For example, later in this course, we'll talk more about Compute Engine, which offers virtual machines as a service. Compute Engine offers a set of predefined roles, and you can apply them to Compute Engine resources in a given project, a given folder, or an entire organization.

Another example: consider Cloud Bigtable, which is a managed database service. Cloud Bigtable offers roles that can apply across an entire organization, to a particular project, or even to individual Bigtable database instances.



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

Google Group

InstanceAdmin
Role

project_a

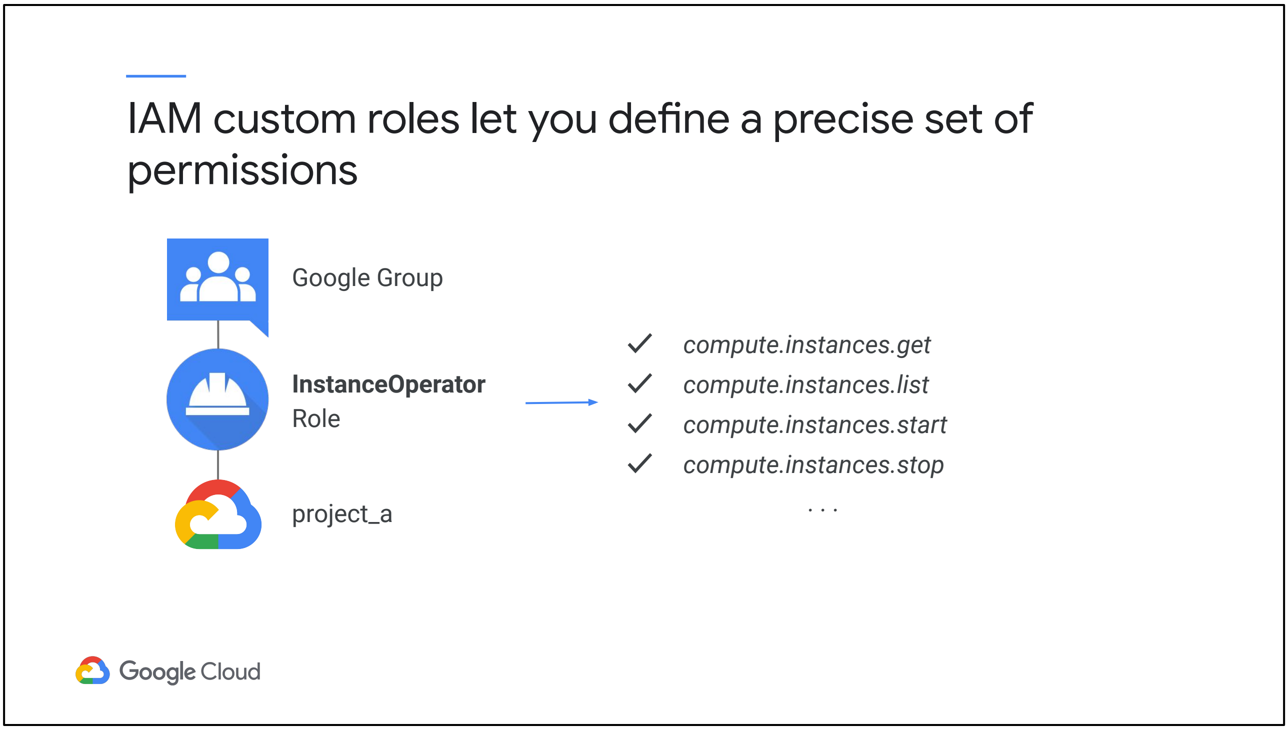
- ✓ *compute.instances.delete*
- ✓ *compute.instances.get*
- ✓ *compute.instances.list*
- ✓ *compute.instances.setMachineType*
- ✓ *compute.instances.start*
- ✓ *compute.instances.stop*

. . .

Google Cloud

Compute Engine’s instanceAdmin role let's whoever has it perform a certain set of actions on virtual machines. What set of actions? Those listed here: listing them, reading and changing their configurations, and starting and stopping them. And which virtual machines? Well, that depends on where the role is applied.

In this example, all the users of a certain Google group have the role, and they have it on all the virtual machines in project A.



IAM custom roles let you define a precise set of permissions

Google Group

InstanceOperator Role

project_a

✓ *compute.instances.get*

✓ *compute.instances.list*

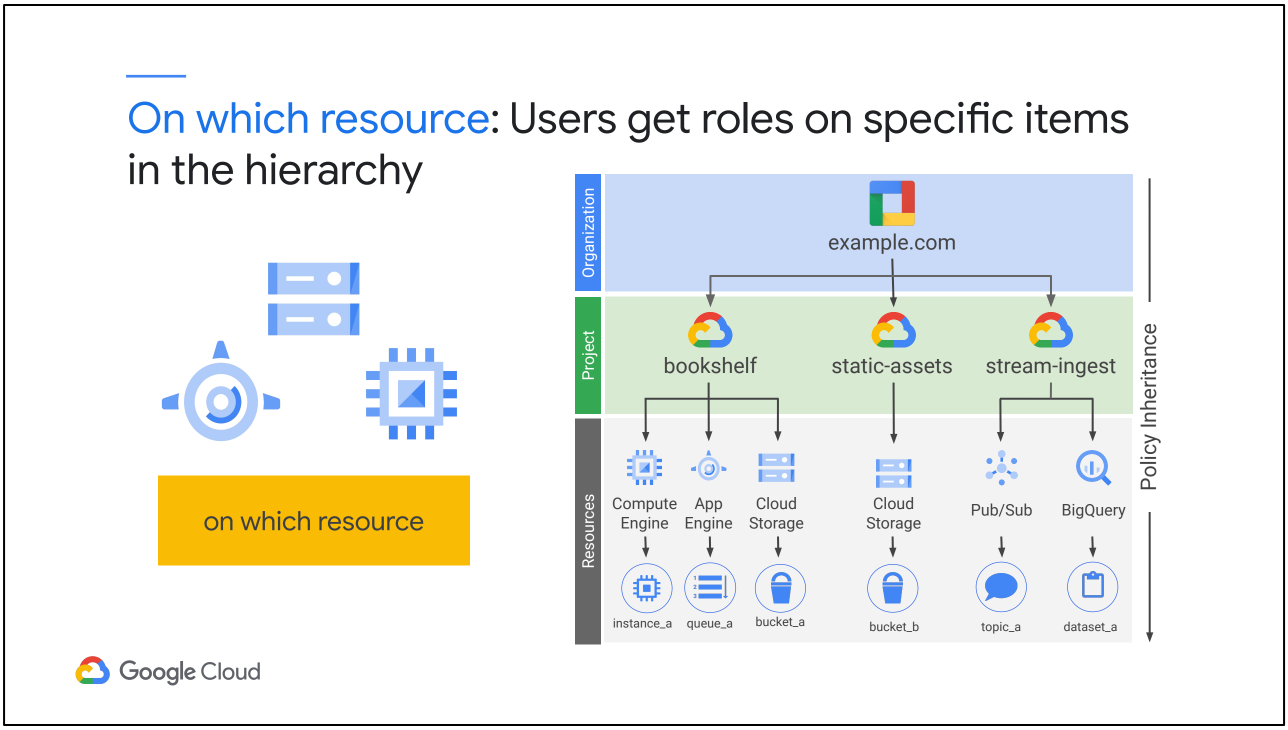
✓ *compute.instances.start*

✓ *compute.instances.stop*

. . .

What if you need something even finer-grained? That's what custom roles permit. A lot of companies use a "least-privilege" model, in which each person in your organization the minimal amount of privilege needed to do his or her job. So, for example, maybe I want to define an "instanceOperator" role, to allow some users to stop and start Compute Engine virtual machines but not reconfigure them. Custom roles allow me to do that.

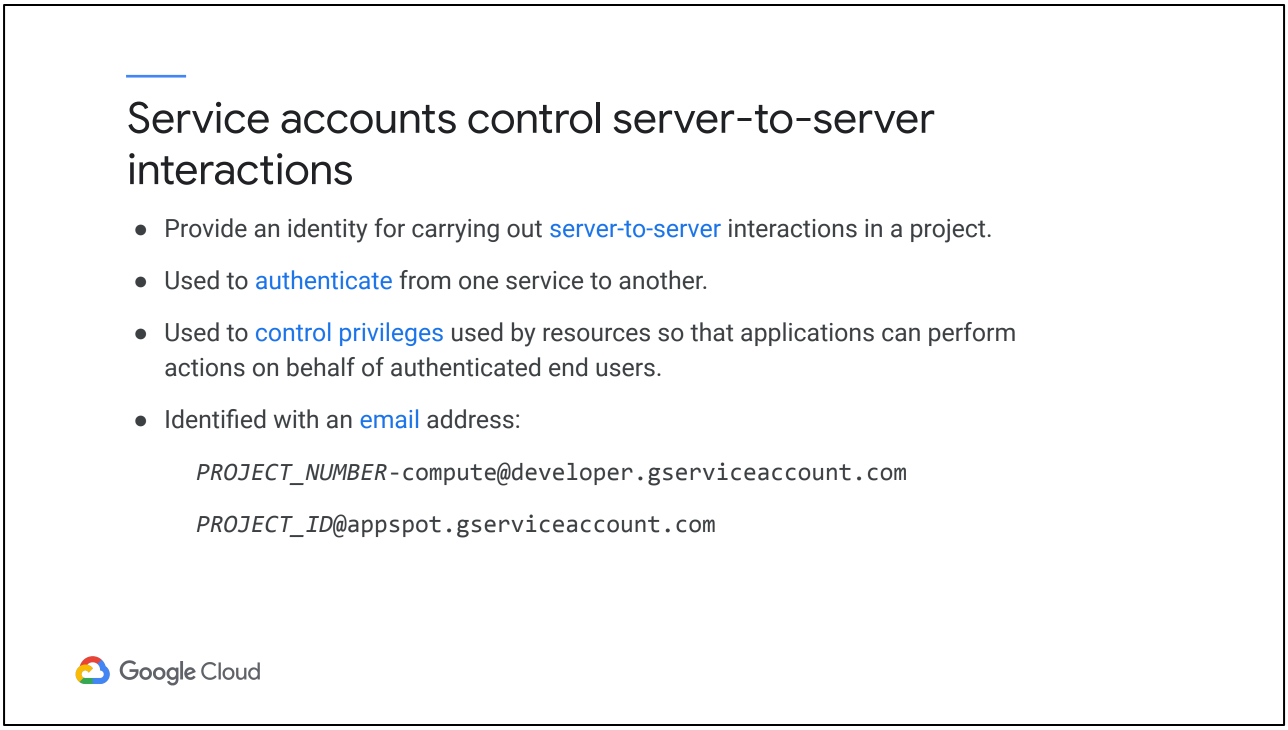
A couple of cautions about custom roles. First, if you decide to use custom roles, you'll need to manage the permissions that make them up. Some companies decide they'd rather stick with the predefined roles. Second, custom roles can only be used at the project or organization levels. They can't be used at the folder level.



On which resource: Users get roles on specific items in the hierarchy

on which resource

When you give a user, group, or service account a role on a specific element of the resource hierarchy, the resulting policy applies to the element you chose, as well as to elements below it in the hierarchy.



Service accounts control server-to-server interactions

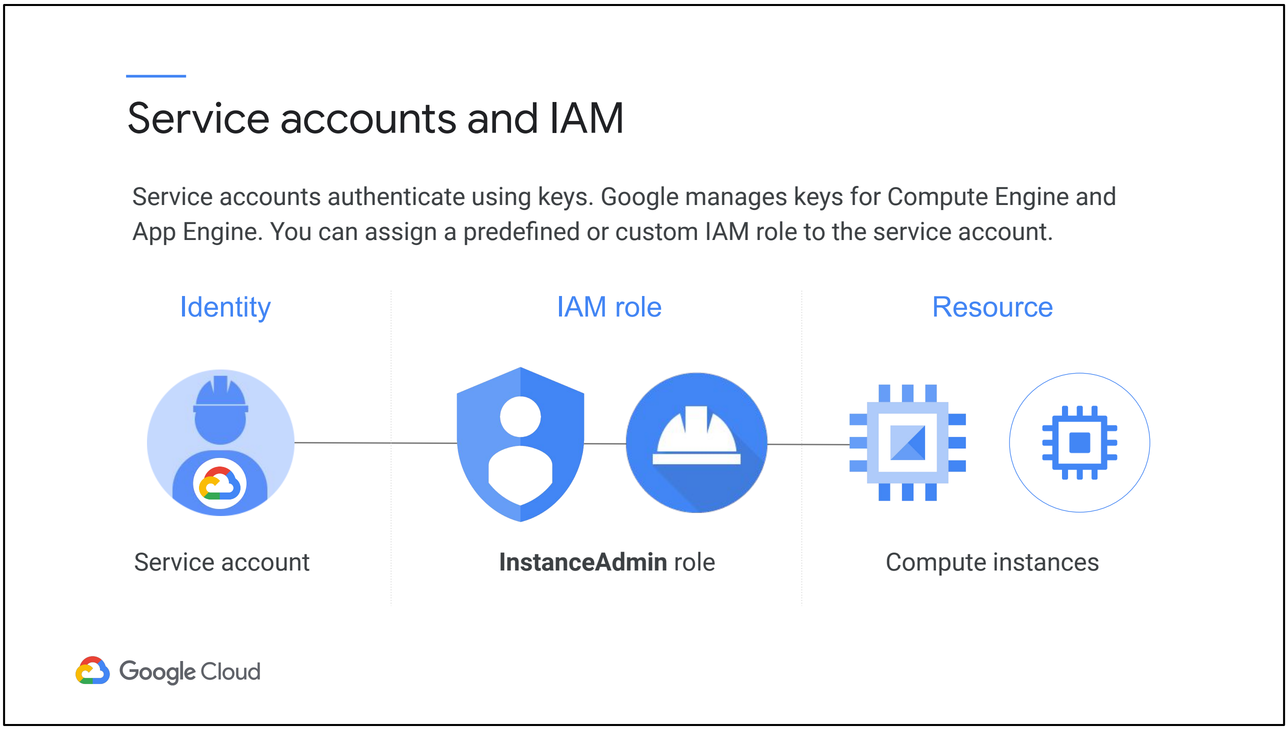
- Provide an identity for carrying out server-to-server interactions in a project.
- Used to authenticate from one service to another.
- Used to control privileges used by resources so that applications can perform actions on behalf of authenticated end users.
- Identified with an email address:

  PROJECT_NUMBER-compute@developer.gserviceaccount.com

  PROJECT_ID@appspot.gserviceaccount.com

Google Cloud

What if you want to give permissions to a Compute Engine virtual machine rather than to a person? That's what service accounts are for. For instance, maybe you have an application running in a virtual machine that needs to store data in Google Cloud Storage. But you don't want to let just anyone on the Internet have access to that data; only that virtual machine. So you'd create a service account to authenticate your VM to Cloud Storage. Service accounts are named with an email address, but instead of passwords they use cryptographic keys to access resources.



Service accounts and IAM

Service accounts authenticate using keys. Google manages keys for Compute Engine and App Engine. You can assign a predefined or custom IAM role to the service account.

Identity

Service account

IAM role

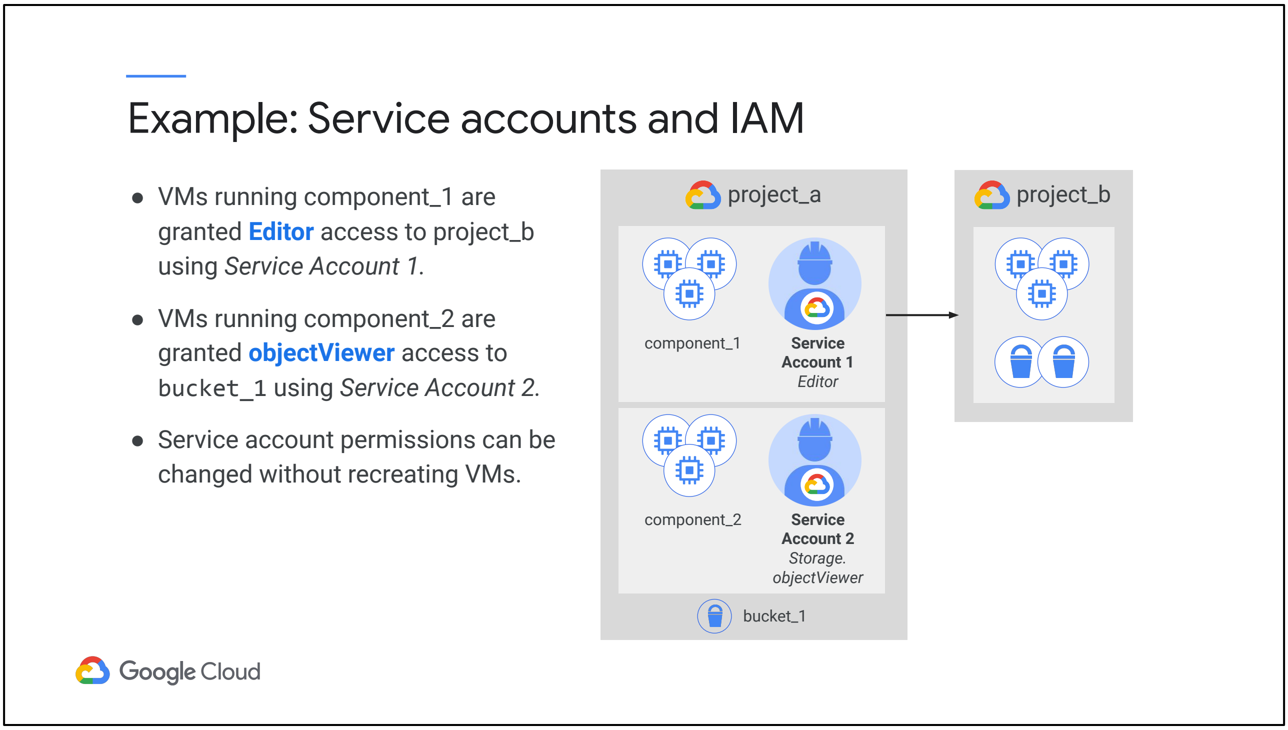
InstanceAdmin role

Resource

Compute instances

In this simple example, a service account has been granted Compute Engine’s Instance Admin role. This would allow an application running in a VM with that service account to create, modify, and delete other VMs.

Incidentally, service accounts need to be managed too! For example, maybe Alice needs to manage what can act as a given service account, while Bob just needs to be able to view what can. Fortunately, in addition to being an identity, a service account is also a resource! So it can have IAM policies of its own attached to it. For instance, Alice can have the editor role on a service account and Bob can have the viewer role. This is just like granting roles for any other Google Cloud resource.

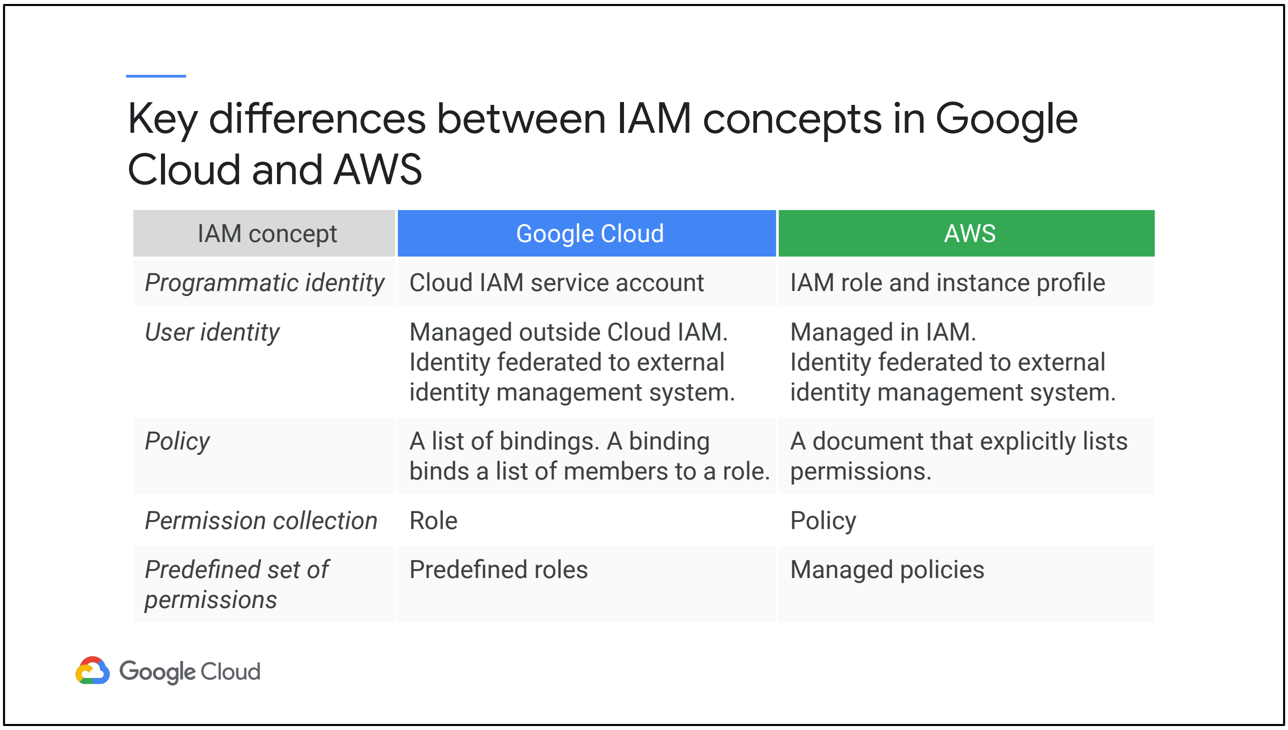


Example: Service accounts and IAM

- VMs running component_1 are granted **Editor** access to project_b using *Service Account 1*.
- VMs running component_2 are granted **objectViewer** access to `bucket_1` using *Service Account 2*.
- Service account permissions can be changed without recreating VMs.

You can grant different groups of VMs in your project different identities. This makes it easier to manage different permissions for each group. You also can change the permissions of the service accounts without having to recreate the VMs.

Here’s a more complex example. Say you have an application that’s implemented across a group of Compute Engine virtual machines. One component of your application needs to have an editor role on another project, but another component doesn’t. So you would create two different service accounts, one for each subgroup of virtual machines. Only the first service account has privilege on the other project. That reduces the potential impact of a miscoded application or a compromised virtual machine.



Key differences between IAM concepts in Google Cloud and AWS

IAM concept	Google Cloud	AWS
Programmatic identity	Cloud IAM service account	IAM role and instance profile
User identity	Managed outside Cloud IAM. Identity federated to external identity management system.	Managed in IAM. Identity federated to external identity management system.
Policy	A list of bindings. A binding binds a list of members to a role.	A document that explicitly lists permissions.
Permission collection	Role	Policy
Predefined set of permissions	Predefined roles	Managed policies

IAM for Google Cloud and AWS perform the same function: to provide a mechanism to secure user authentication and permissions for the cloud. IAM does not secure applications or operating systems; IAM is used to control who can do what in the cloud. Although IAM for Google and AWS perform the same function, they do it in very different ways.

- Google uses Service accounts to control service-to-service authentication; AWS uses IAM Roles and Profiles to accomplish this control.
- For Google Cloud, user identities are managed outside of Google Cloud. For example, Workspace or Gmail accounts can be used to manage identities. For AWS, user and group identities are created using AWS. For EC2, instance profiles can also be used.
- For Google Cloud, policies are a list of bindings that set a user's permissions by the role applied. Policy documents are used by AWS to apply permissions to users. The document is built using JSON and is applied on the resource.
- User/Role pairings on a resource determine a user's permissions in Google Cloud. In AWS, predefined permissions can be applied using managed policies, which are pre-built JSON documents used to apply default permissions.
- Google uses predefined roles, which are built to match job roles. AWS has something similar called managed policies. Managed policies are JSON documents that group permissions by job roles.

Agenda

Google Cloud Resource Hierarchy

Cloud Identity and Access Management (Cloud IAM)

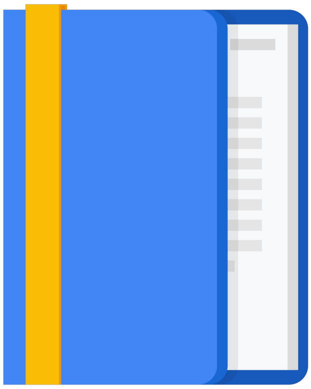
Cloud Identity

Interacting with Google Cloud

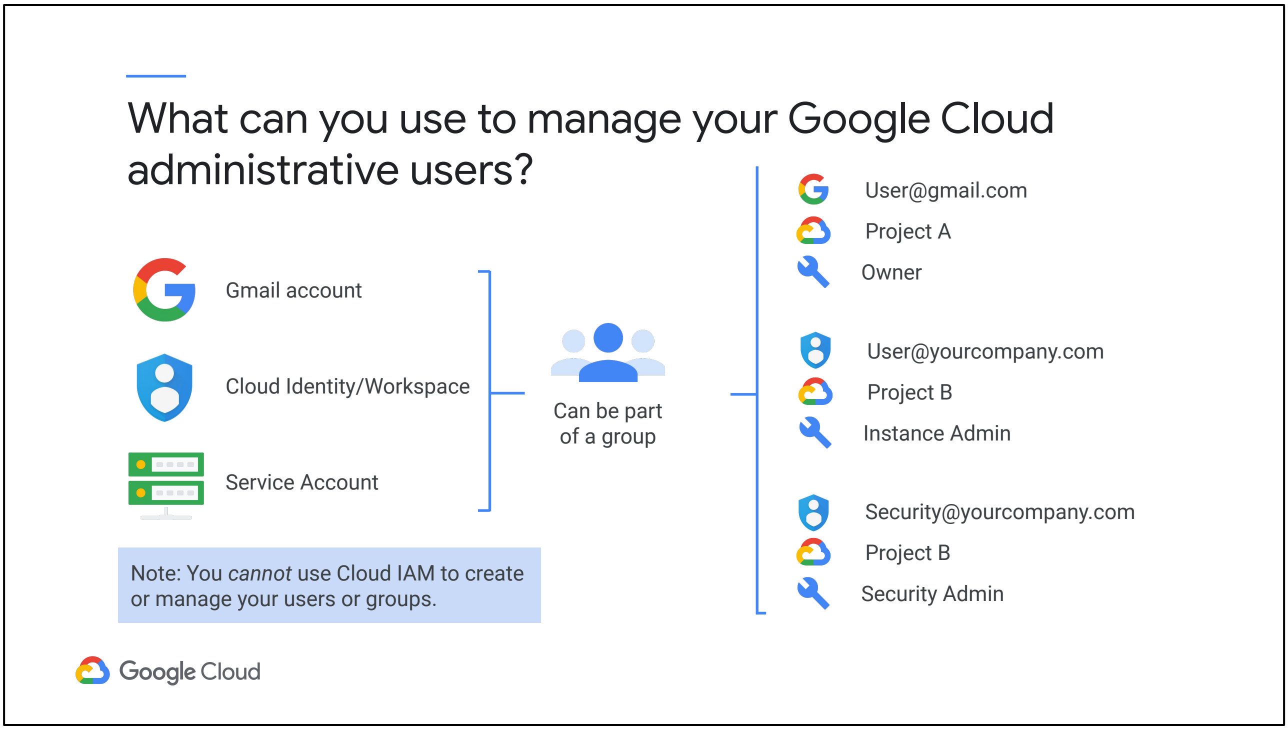
Google Cloud Marketplace

Quiz and Lab

Resources



Google Cloud



What can you use to manage your Google Cloud administrative users?

Gmail account

Cloud Identity/Workspace

Service Account

Can be part of a group

User@gmail.com
Project A
Owner

User@yourcompany.com
Project B
Instance Admin

Security@yourcompany.com
Project B
Security Admin

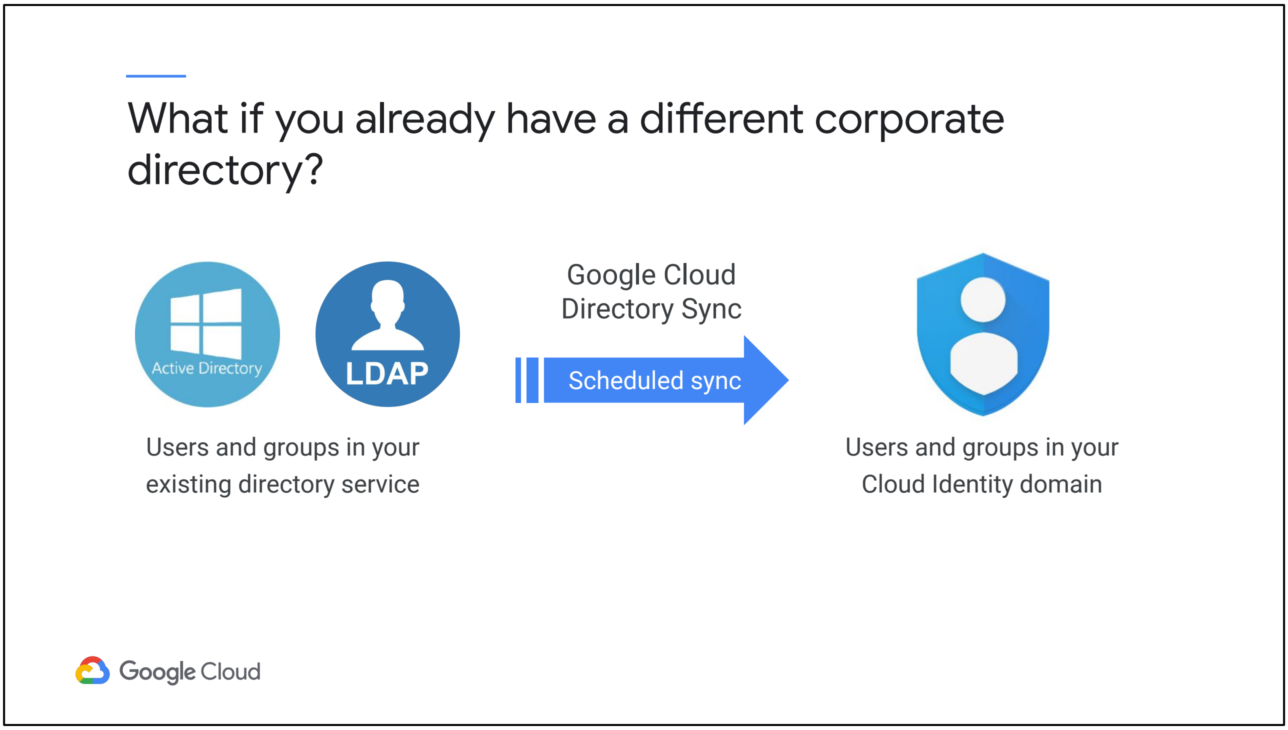
Note: You *cannot* use Cloud IAM to create or manage your users or groups.

Google Cloud

Many new Google Cloud customers get started by logging into the Cloud Console with a Gmail account. To collaborate with their teammates, they use Google Groups to gather together people who are in the same role. This approach is easy to get started with, but its disadvantage is that your team's identities are not centrally managed. For example, if someone leaves your organization, there is no centralized way to remove their access to your cloud resources immediately.

Google Cloud customers who are also Workspace customers can define Google Cloud policies in terms of Workspace 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.

Google Cloud customers who are not Workspace 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 Workspace's collaboration products such as Gmail, Docs, Drive, and Calendar. Cloud Identity is available in a free and a premium edition. The premium edition adds capabilities for mobile device management.



What if you already have a different corporate directory?

Active Directory

LDAP

Users and groups in your existing directory service

Google Cloud Directory Sync

Scheduled sync

Users and groups in your Cloud Identity domain

Google Cloud

Using Google Cloud Directory Sync, your administrators can log in and manage Google Cloud resources using the same usernames and passwords they already use. This tool synchronizes users and groups from your existing Active Directory or LDAP system with the users and groups in your Cloud Identity domain. The synchronization is one-way only; no information in your Active Directory or LDAP map is modified. Google Cloud Directory Sync is designed to run scheduled synchronizations without supervision, after its synchronization rules are set up.

Agenda

Google Cloud Resource Hierarchy

Cloud Identity and Access Management (Cloud IAM)

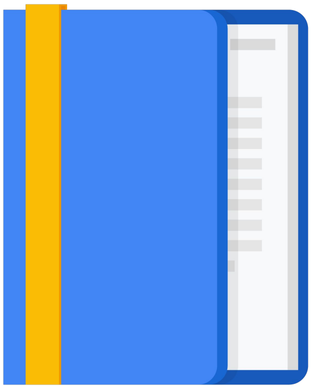
Cloud Identity

Interacting with Google Cloud

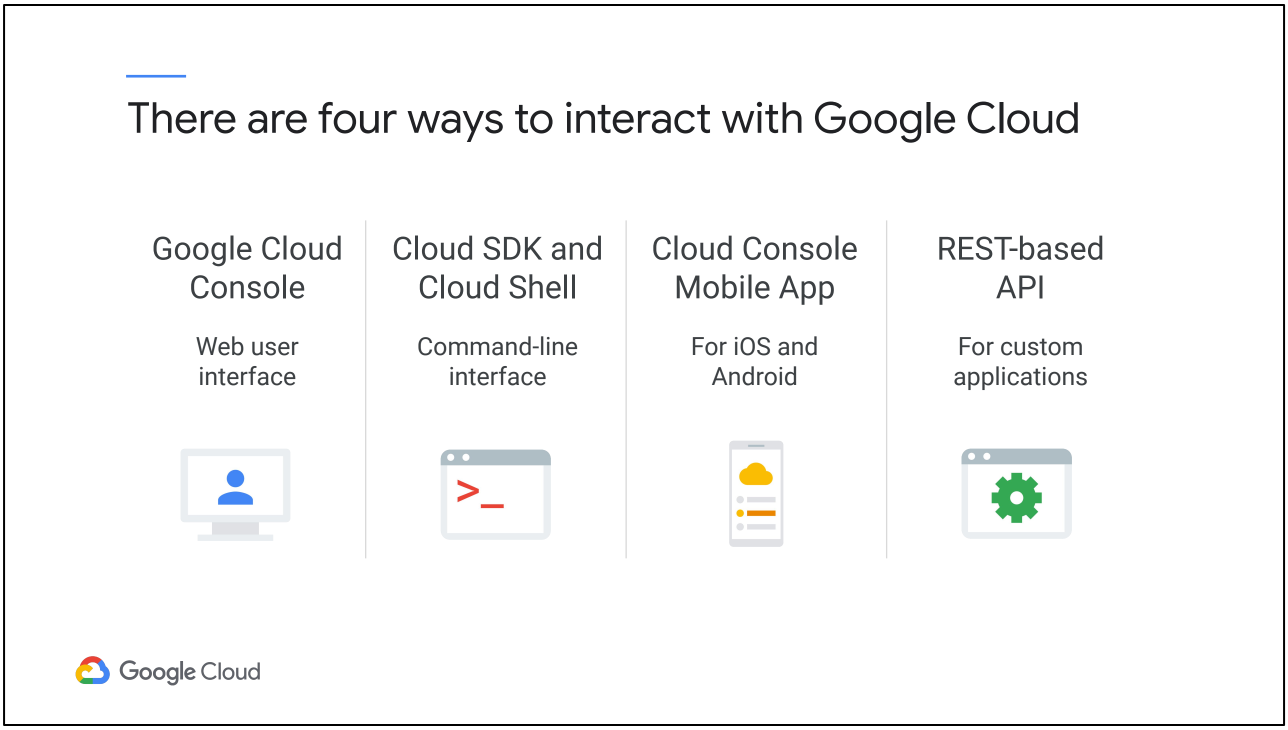
Google Cloud Marketplace

Quiz and Lab

Resources



Google Cloud



There are four ways to interact with Google Cloud

Google Cloud Console

Web user interface

Cloud SDK and Cloud Shell

Command-line interface

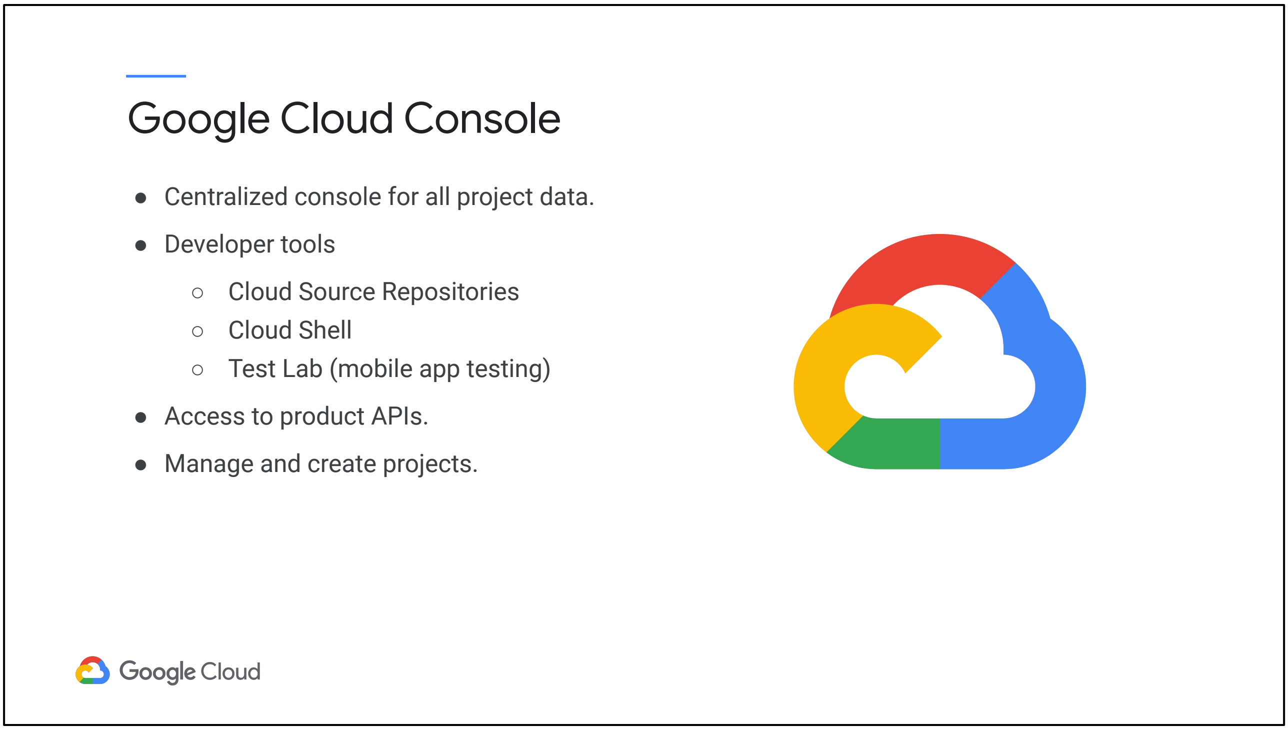
Cloud Console Mobile App

For iOS and Android

REST-based API

For custom applications

There are four ways you can interact with Google Cloud, and we'll talk about each in turn: the Cloud Console, the Cloud SDK and Cloud Shell, the mobile app, and the APIs.

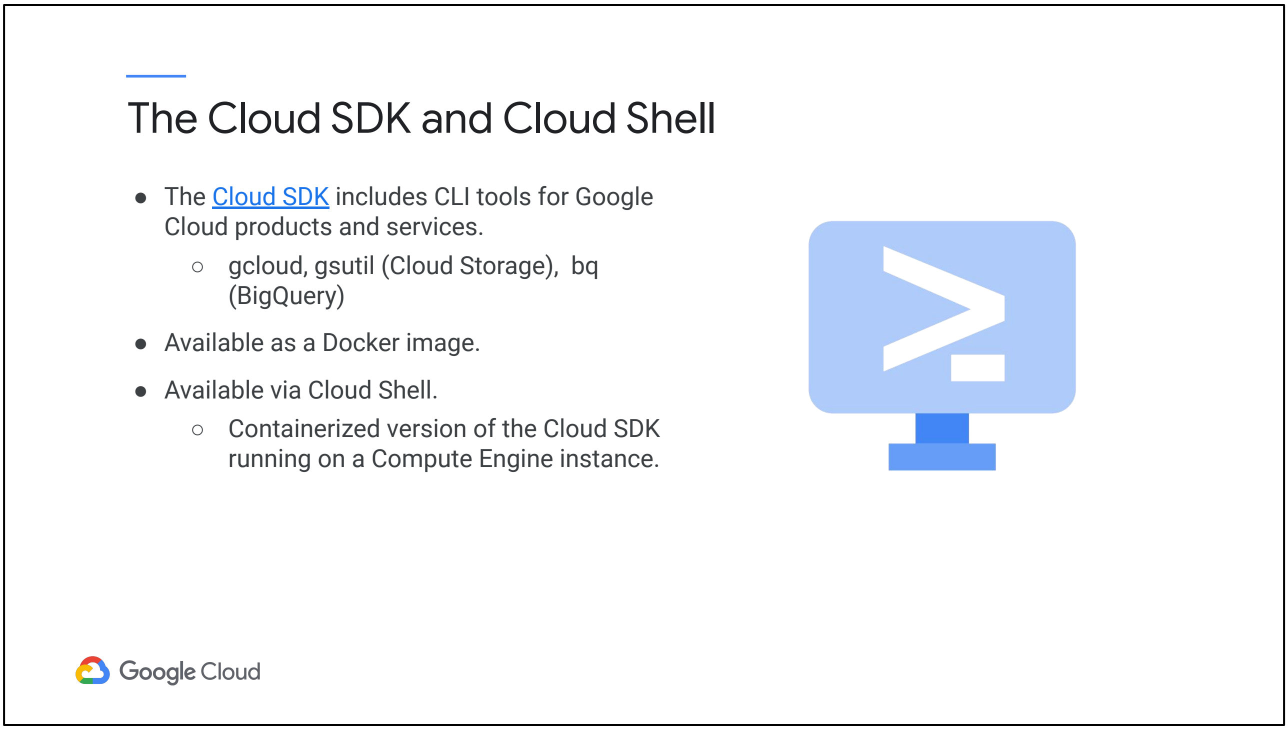


Google Cloud Console

- Centralized console for all project data.
- Developer tools
  - Cloud Source Repositories
  - Cloud Shell
  - Test Lab (mobile app testing)
- Access to product APIs.
- Manage and create projects.

Google Cloud

The Cloud Console is Google Cloud's Graphical User Interface (GUI) which helps you deploy, scale, and diagnose production issues in a simple web-based interface. With the Cloud Console, you can easily find your resources, check their health, have full management control over them, and set budgets to control how much you spend on them. Search to quickly find resources and connect to instances via SSH in the browser. Overcome the most complex tasks with Cloud Shell, your admin machine in the cloud, where you can use the built-in Cloud SDK.



The Cloud SDK and Cloud Shell

- The Cloud SDK includes CLI tools for Google Cloud products and services.
  - gcloud, gsutil (Cloud Storage), bq (BigQuery)
- Available as a Docker image.
- Available via Cloud Shell.
  - Containerized version of the Cloud SDK running on a Compute Engine instance.

Google Cloud

The Cloud SDK is a set of tools that you can use to manage resources and applications hosted on Google Cloud. These include the gcloud tool, which provides the main command-line interface for Google Cloud products and services, as well as gsutil and bq. When installed, all of the tools within the Cloud SDK are located under the bin directory.

Cloud Shell provides you with command-line access to your cloud resources directly from your browser. Cloud Shell is a Debian-based virtual machine with a persistent 5-GB home directory, which makes it easy for you to manage your Google Cloud projects and resources. With Cloud Shell, the Cloud SDK gcloud command and other utilities you need are always installed, available, up to date, and fully authenticated when you need them.

For more information on the SDK command-line tools, see:
https://cloud.google.com/sdk/cloudplatform

Note: Currently, the App Engine SDKs are separate downloads. For more information, see: https://cloud.google.com/appengine/downloads

Cloud Shell provides the following:

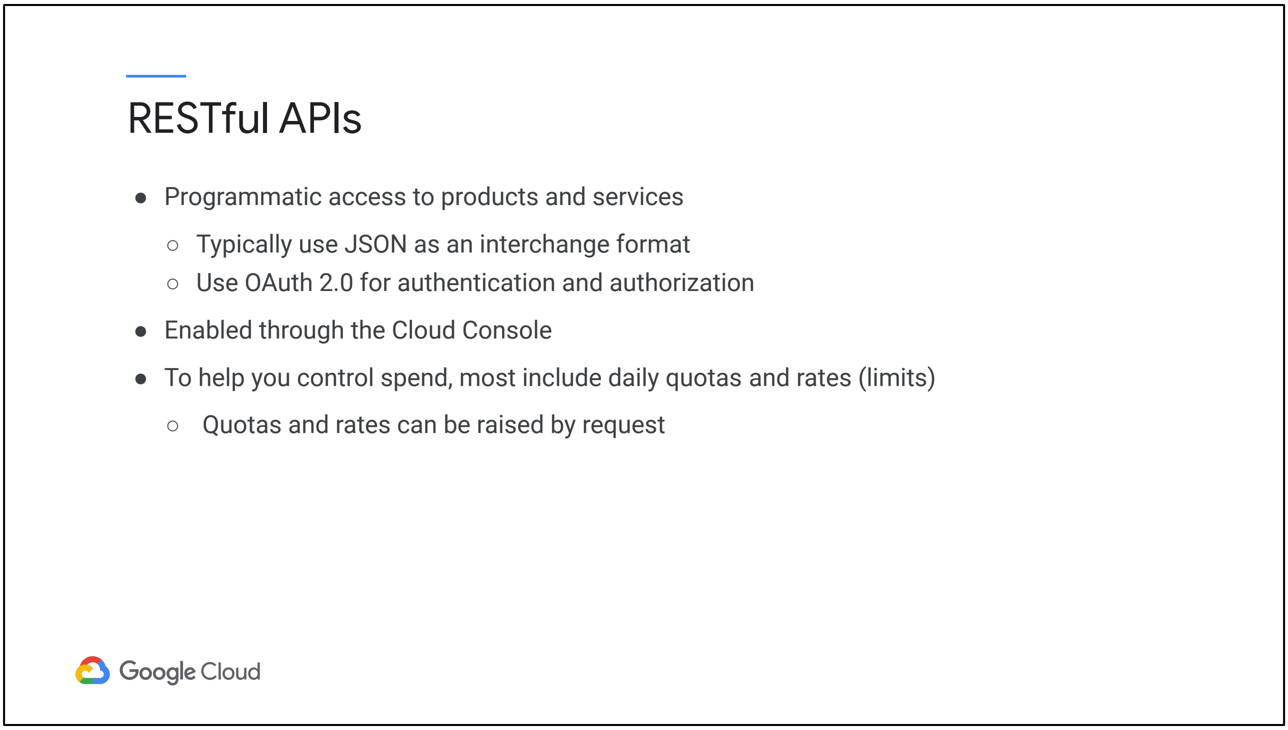
- A temporary Compute Engine virtual machine instance running a Debian-based Linux operating system
- Command-line access to the instance from a web browser using terminal windows in the Cloud Console

- 5 GB of persistent disk storage per user, mounted as your $HOME directory in Cloud Shell sessions across projects and instances
- The Cloud SDK and other tools pre-installed on the Compute Engine instance
- Language support, including SDKs, libraries, runtime environments and compilers for Java, Go, Python, Node.js, PHP and Ruby
- Web preview functionality, which allows you to preview web applications running on the Cloud Shell instance through a secure proxy
- Built-in authorization for access to projects and resources

You can use Cloud Shell to:

- Create and manage Compute Engine instances.
- Create and access Cloud SQL databases.
- Manage Cloud Storage data.
- Interact with hosted or remote Git repositories, including Cloud Source Repositories.
- Build and deploy App Engine applications.

You can also use Cloud Shell to perform other management tasks related to your projects and resources, using either the gcloud command or other available tools.



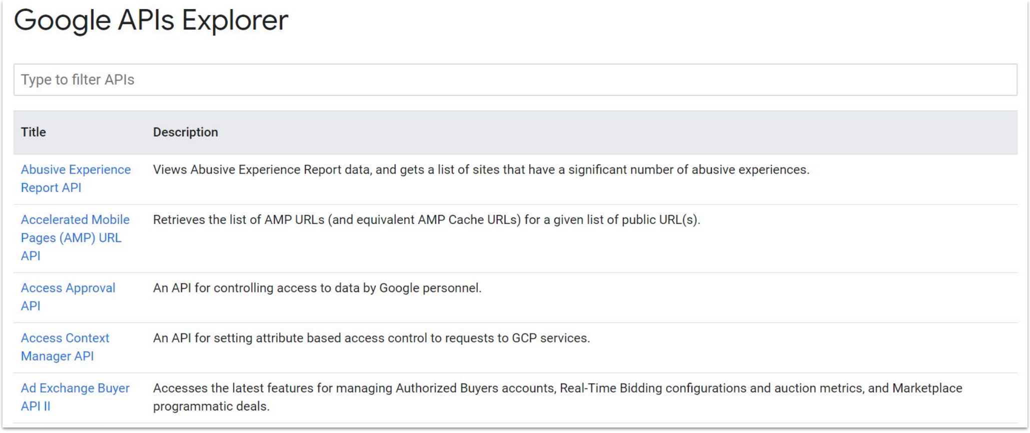
RESTful APIs

- Programmatic access to products and services
  - Typically use JSON as an interchange format
  - Use OAuth 2.0 for authentication and authorization
- Enabled through the Cloud Console
- To help you control spend, most include daily quotas and rates (limits)
  - Quotas and rates can be raised by request

The services that make up Google Cloud offer Application Programming Interfaces, so that code you write can control them. These APIs are what's called "RESTful"; in other words, they follow the "Representational state transfer" paradigm. We don't need to go into much detail of what that means here. Basically, it means that your code can use Google services in much the same way that web browsers talk to web servers. The APIs name resources in Google Cloud with URLs. Your code can pass information to the APIs using JSON, which is a very popular way of passing textual information over the Web. And there's an open system for user login and access control.

The Cloud Console lets you turn on and off APIs. Many APIs are off by default, and many are associated with quotas and limits. Why? These restrictions help protect you from using resources inadvertently. You can enable only those APIs you need, and you can request increases in quotas when you need more resources.

Use the Google APIs Explorer to help you write code



Google APIs Explorer

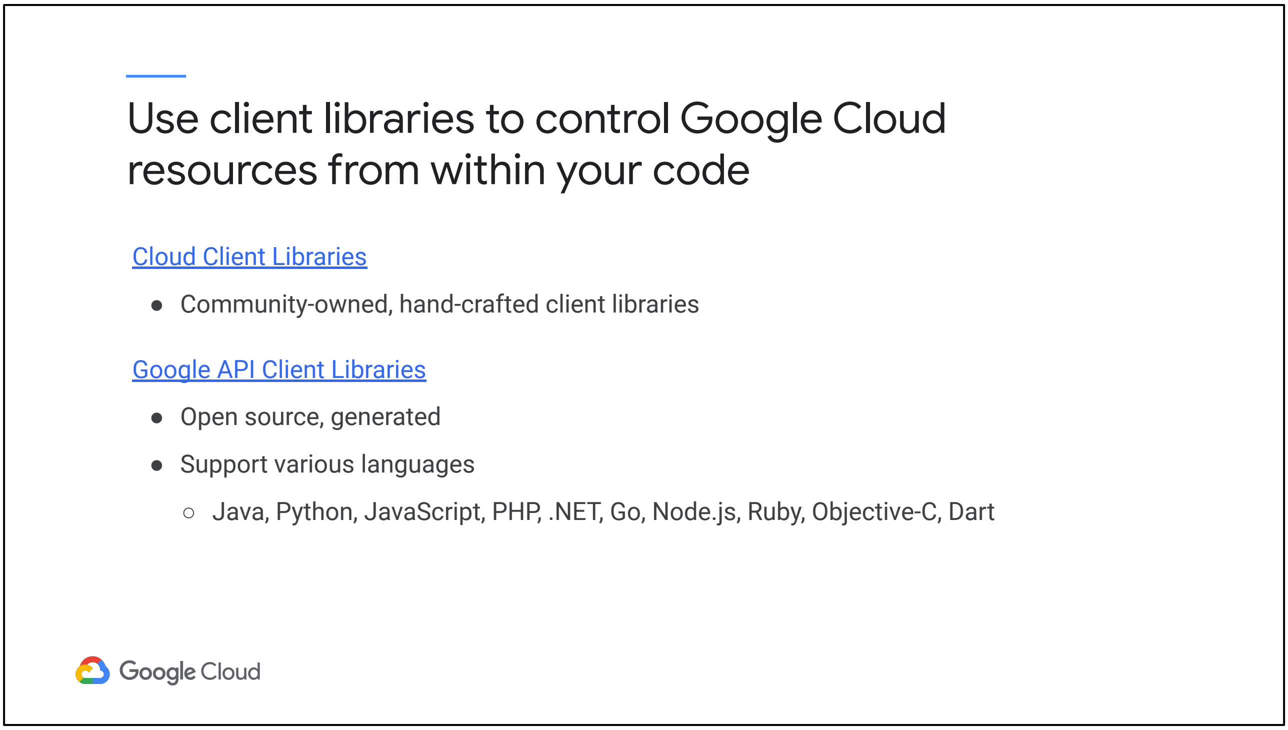
Type to filter APIs

Title	Description
Abusive Experience Report API	Views Abusive Experience Report data, and gets a list of sites that have a significant number of abusive experiences.
Accelerated Mobile Pages (AMP) URL API	Retrieves the list of AMP URLs (and equivalent AMP Cache URLs) for a given list of public URL(s).
Access Approval API	An API for controlling access to data by Google personnel.
Access Context Manager API	An API for setting attribute based access control to requests to GCP services.
Ad Exchange Buyer API II	Accesses the latest features for managing Authorized Buyers accounts, Real-Time Bidding configurations and auction metrics, and Marketplace programmatic deals.

Say you're writing an application that needs to control Google Cloud resources, so you'll need to get your use of the APIs just right. That's what Google APIs Explorer is for.

The Cloud Console includes a tool called the Google APIs Explorer that helps you learn about the APIs interactively. It lets you see what APIs are available, and in what versions. These APIs expect parameters, and documentation on them is built-in. You can try the APIs interactively, even with user authentication.

Suppose you've explored an API, and you're ready to build an application that uses it. Do you have to start coding from scratch? No. Google provides client libraries to take a lot of the drudgery out of the task of calling Google Cloud from your code.



Use client libraries to control Google Cloud resources from within your code

Cloud Client Libraries

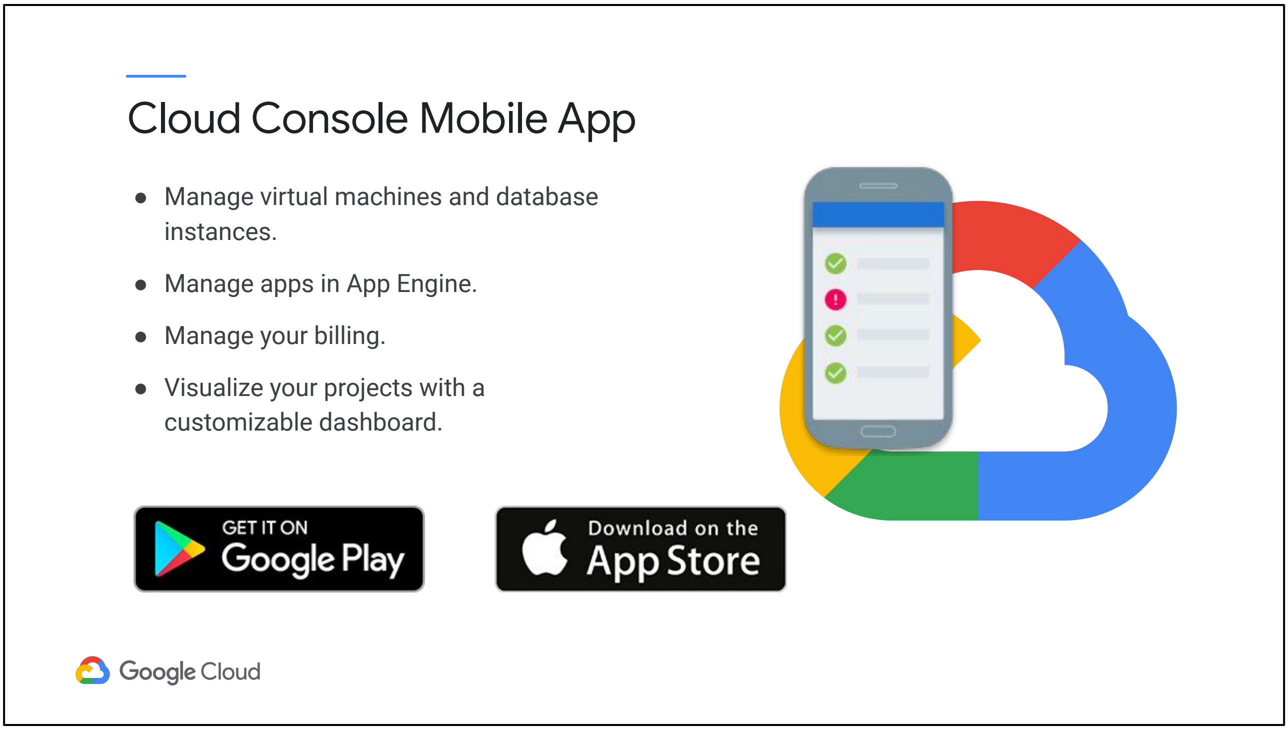
- Community-owned, hand-crafted client libraries

Google API Client Libraries

- Open source, generated
- Support various languages
  - Java, Python, JavaScript, PHP, .NET, Go, Node.js, Ruby, Objective-C, Dart

Google Cloud

There are two kinds of libraries. The Cloud Client libraries are Google Cloud’s latest and recommended libraries for its APIs. They adopt the native styles and idioms of each language. On the other hand, sometimes a Cloud Client library doesn’t support the newest services and features. In that case, you can use the Google API Client library for your desired languages. These libraries are designed for generality and completeness.



Cloud Console Mobile App

- Manage virtual machines and database instances.
- Manage apps in App Engine.
- Manage your billing.
- Visualize your projects with a customizable dashboard.

GET IT ON Google Play

Download on the App Store

Google Cloud

Finally, one more tool that's of interest to everyone, not just developers. There's a mobile app for Android and iOS that lets you examine and manage the resources you're using in Google Cloud. It lets you build dashboards, so that you can get the information you need at a glance.

Agenda

Google Cloud Resource Hierarchy

Cloud Identity and Access Management (Cloud IAM)

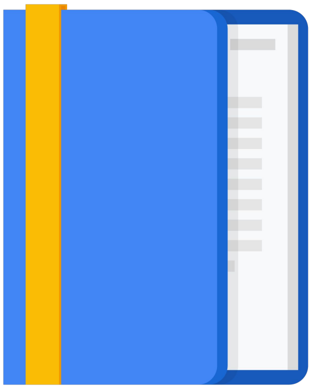
Cloud Identity

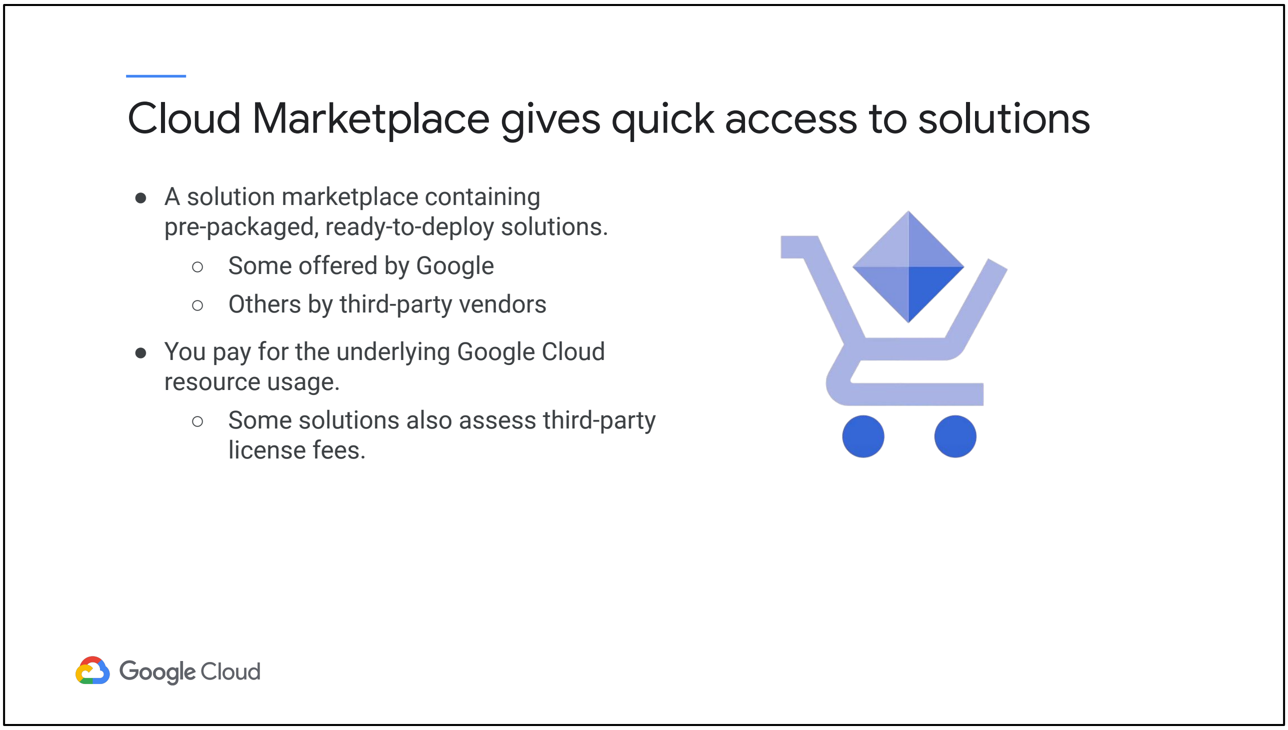
Interacting with Google Cloud

Google Cloud Marketplace

Quiz and Lab

Resources





Cloud Marketplace gives quick access to solutions

- A solution marketplace containing pre-packaged, ready-to-deploy solutions.
  - Some offered by Google
  - Others by third-party vendors
- You pay for the underlying Google Cloud resource usage.
  - Some solutions also assess third-party license fees.

Google Cloud

If you want a quick way to get started with Google Cloud, with minimal effort this is what Cloud Marketplace provides. It's a tool for quickly deploying functional software packages on Google Cloud. There's no need to manually configure the software, virtual machine instances, storage, or network settings, although you can modify many of them before you launch if you like.

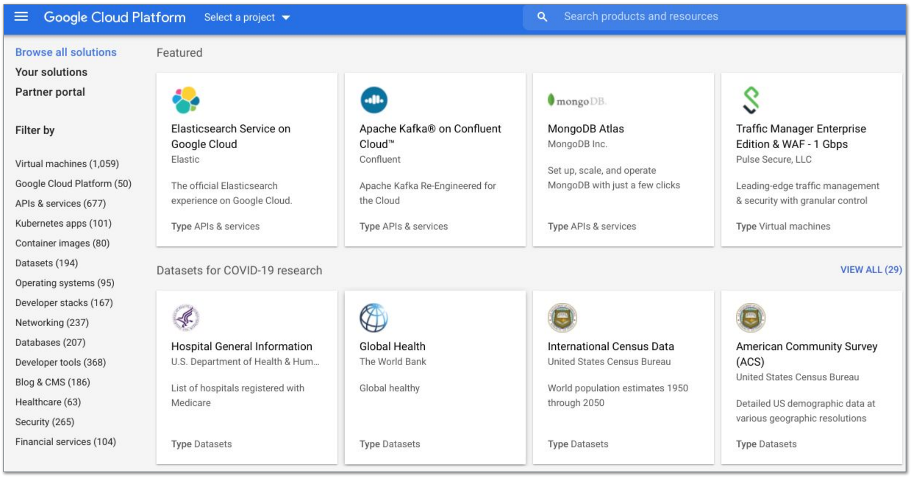
You will find solutions offered by Google in Cloud Marketplace as well as solutions offered by third-party vendors.

Most software packages in Cloud Marketplace are at no additional charge beyond the normal usage fees for Google Cloud resources. Some Cloud Marketplace images charge usage fees, particularly those published by third parties, with commercially licensed software. But they all show you estimates of their monthly charges before you launch them. Do be aware that these estimates are just that--estimates--and in particular they don't attempt to estimate networking costs, since those will vary based on how you use the applications.

A second note of caution: Google Cloud updates the base images for these software packages to fix critical issues and vulnerabilities, but it doesn't update software after it's been deployed. Fortunately, you'll have access to the deployed systems so you can maintain them.

See the Cloud Marketplace documentation for details.

Cloud Marketplace catalog



Google Cloud Platform   Select a project

Search products and resources

Browse all solutions
Your solutions
Partner portal

Filter by

Virtual machines (1,059)
Google Cloud Platform (50)
APIs & services (677)
Kubernetes apps (101)
Container images (80)
Datasets (194)
Operating systems (95)
Developer stacks (167)
Networking (237)
Databases (207)
Developer tools (368)
Blog & CMS (186)
Healthcare (63)
Security (265)
Financial services (104)

Featured

Elasticsearch Service on Google Cloud Elastic The official Elasticsearch experience on Google Cloud. Type APIs & services	Apache Kafka® on Confluent Cloud™ Confluent Apache Kafka Re-Engineered for the Cloud Type APIs & services	MongoDB Atlas MongoDB Inc. Set up, scale, and operate MongoDB with just a few clicks Type APIs & services	Traffic Manager Enterprise Edition & WAF - 1 Gbps Pulse Secure, LLC Leading-edge traffic management & security with granular control Type Virtual machines

Datasets for COVID-19 research   VIEW ALL (29)

Hospital General Information U.S. Department of Health & Hum... List of hospitals registered with Medicare Type Datasets	Global Health The World Bank Global healthy Type Datasets	International Census Data United States Census Bureau World population estimates 1950 through 2050 Type Datasets	American Community Survey (ACS) United States Census Bureau Detailed US demographic data at various geographic resolutions Type Datasets

Cloud Marketplace offers ready-to-go development stacks, solutions, and services to accelerate development. So you spend less time installing and more time developing. Benefits include:

- Deploying production-grade solutions in a few clicks,
- Single billing for all your Google Cloud and third-party services,
- Managing solutions using Deployment Manager,
- Notifications when a security update is available, and
- Direct access to partner support.

Agenda

Google Cloud Resource Hierarchy

Cloud Identity and Access Management (Cloud IAM)

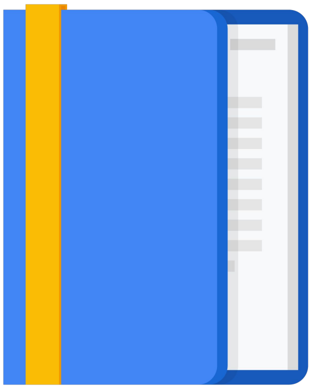
Cloud Identity

Interacting with Google Cloud

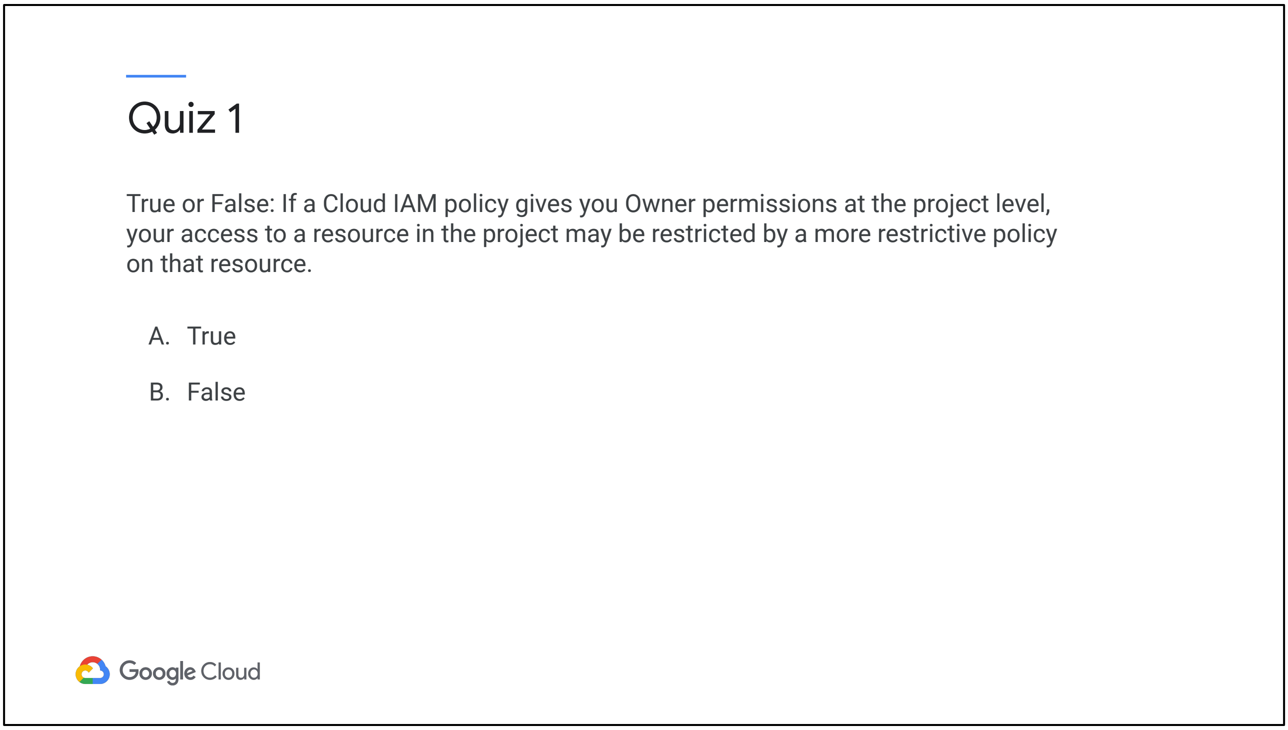
Google Cloud Marketplace

Quiz and Lab

Resources



Google Cloud

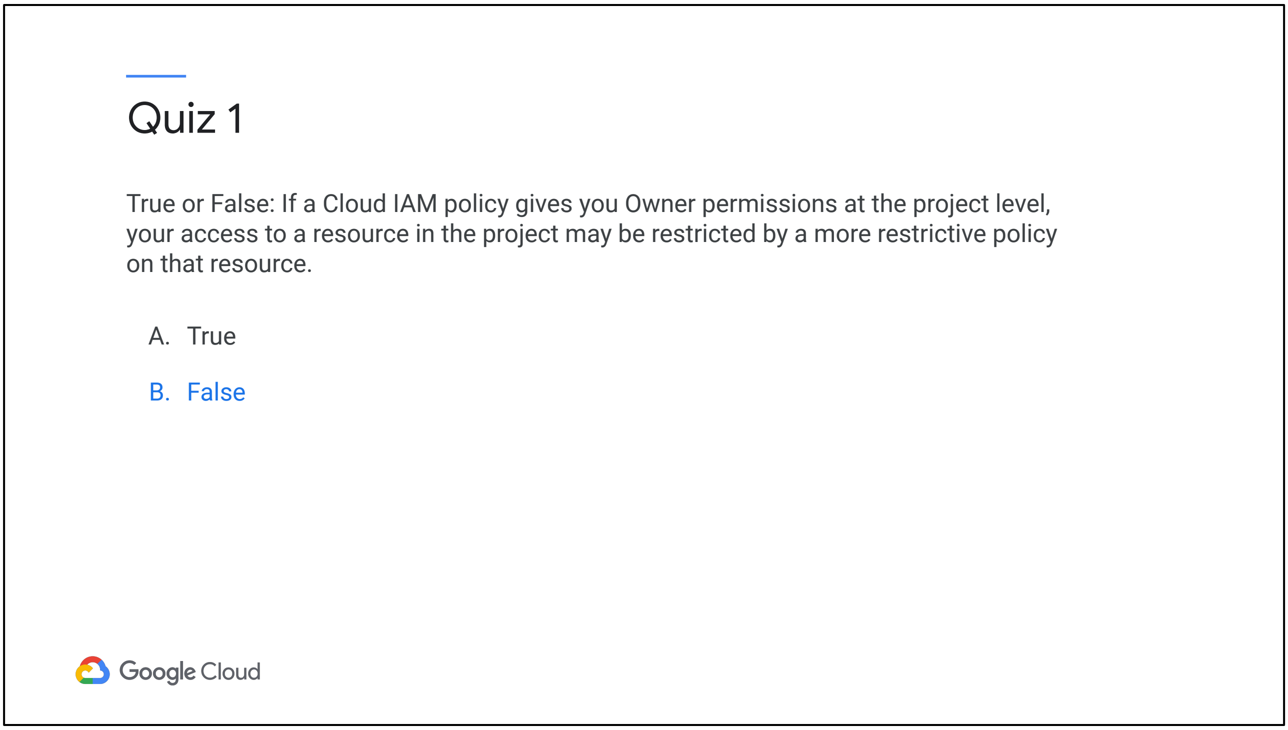


Quiz 1

True or False: If a Cloud IAM policy gives you Owner permissions at the project level, your access to a resource in the project may be restricted by a more restrictive policy on that resource.

A. True

B. False



Quiz 1

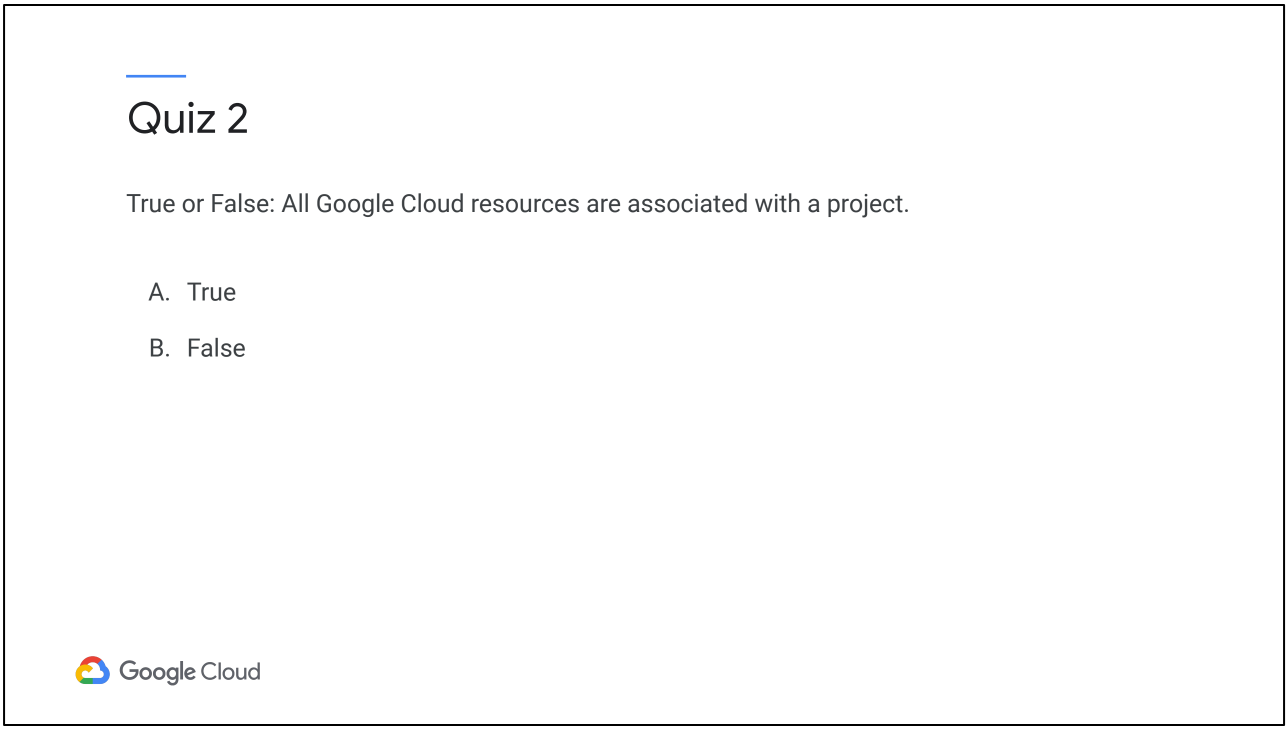
True or False: If a Cloud IAM policy gives you Owner permissions at the project level, your access to a resource in the project may be restricted by a more restrictive policy on that resource.

A. True

B. False

Google Cloud

False. Policies are a union of the parent and the resource. If a parent policy is less restrictive, it overrides a more restrictive resource policy.

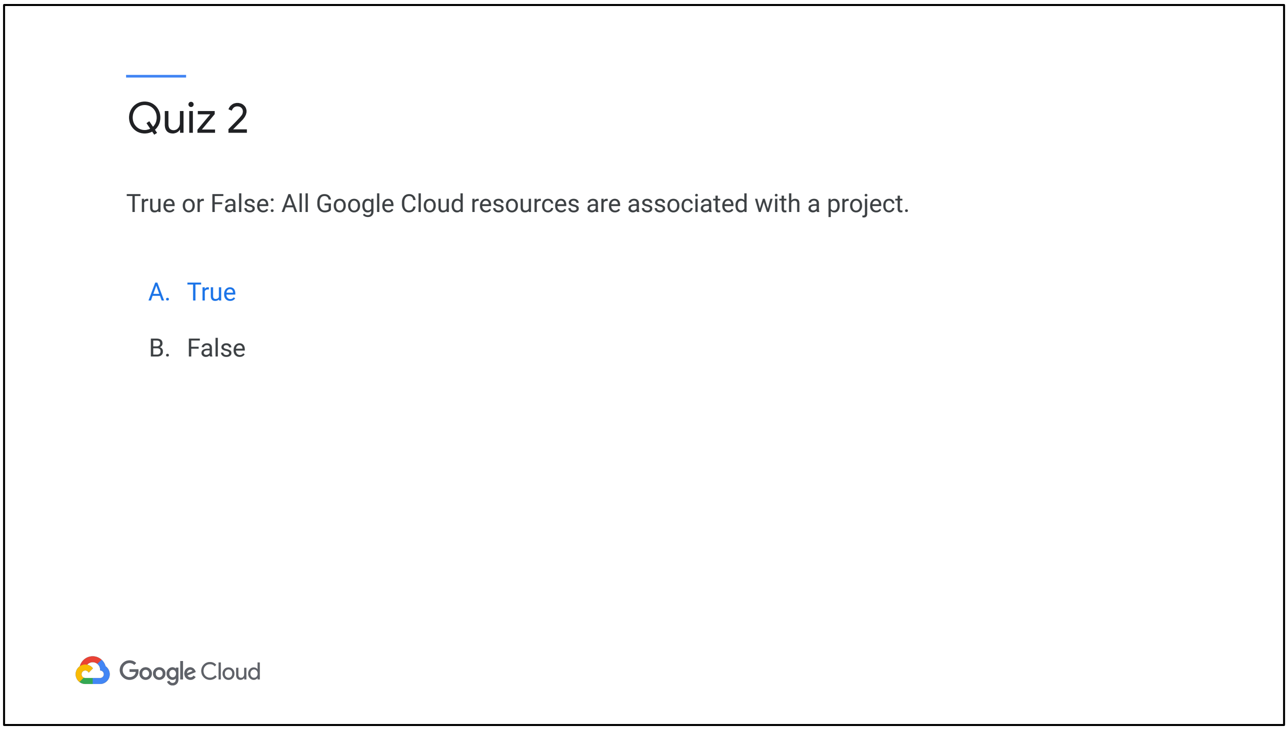


Quiz 2

True or False: All Google Cloud resources are associated with a project.

A. True

B. False



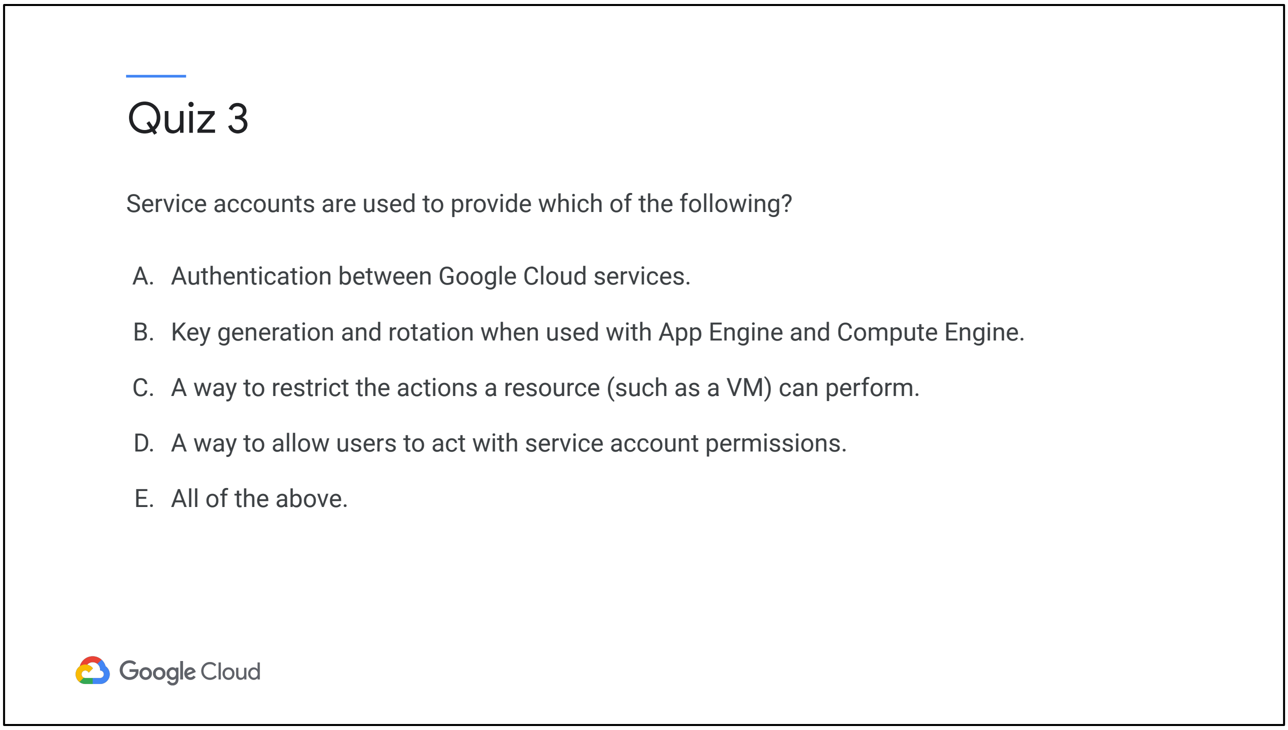
Quiz 2

True or False: All Google Cloud resources are associated with a project.

[✓ A. True]

B. False

Google Cloud



Quiz 3

Service accounts are used to provide which of the following?

A. Authentication between Google Cloud services.

B. Key generation and rotation when used with App Engine and Compute Engine.

C. A way to restrict the actions a resource (such as a VM) can perform.

D. A way to allow users to act with service account permissions.

E. All of the above.

Google Cloud

Quiz 3

Service accounts are used to provide which of the following?

A. Authentication between Google Cloud services.

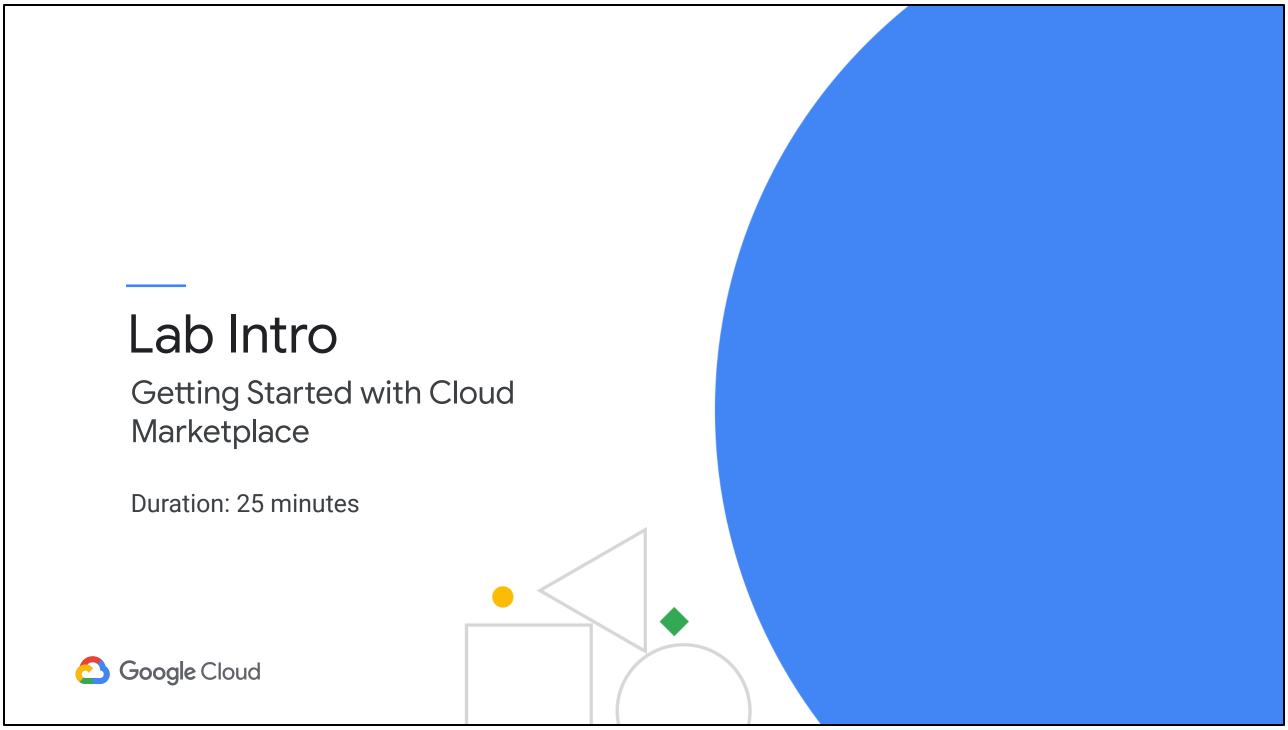
B. Key generation and rotation when used with App Engine and Compute Engine.

C. A way to restrict the actions a resource (such as a VM) can perform.

D. A way to allow users to act with service account permissions.

E. All of the above.

Google Cloud



Lab Intro

Getting Started with Cloud Marketplace

Duration: 25 minutes

In this lab, you deploy a virtual development environment using Cloud Marketplace. The objectives of the lab are to:

- Deploy a Bitnami LAMP stack to Compute Engine using Cloud Marketplace.
- Verify the deployment.

Agenda

Google Cloud Resource Hierarchy

Cloud Identity and Access Management (Cloud IAM)

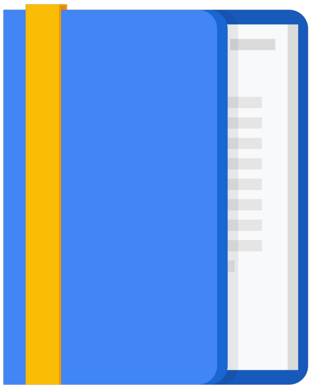
Cloud Identity

Interacting with Google Cloud

Google Cloud Marketplace

Quiz and Lab

Resources



Google Cloud

Resources

Google Cloud security https://cloud.google.com/security/

Configuring permissions https://cloud.google.com/docs/permissions-overview

Cloud Identity and Access Management (Cloud IAM) https://cloud.google.com/iam/

Cloud SDK installation and quick start https://cloud.google.com/sdk/#Quick_Start

gcloud tool guide https://cloud.google.com/sdk/gcloud/

Google Cloud