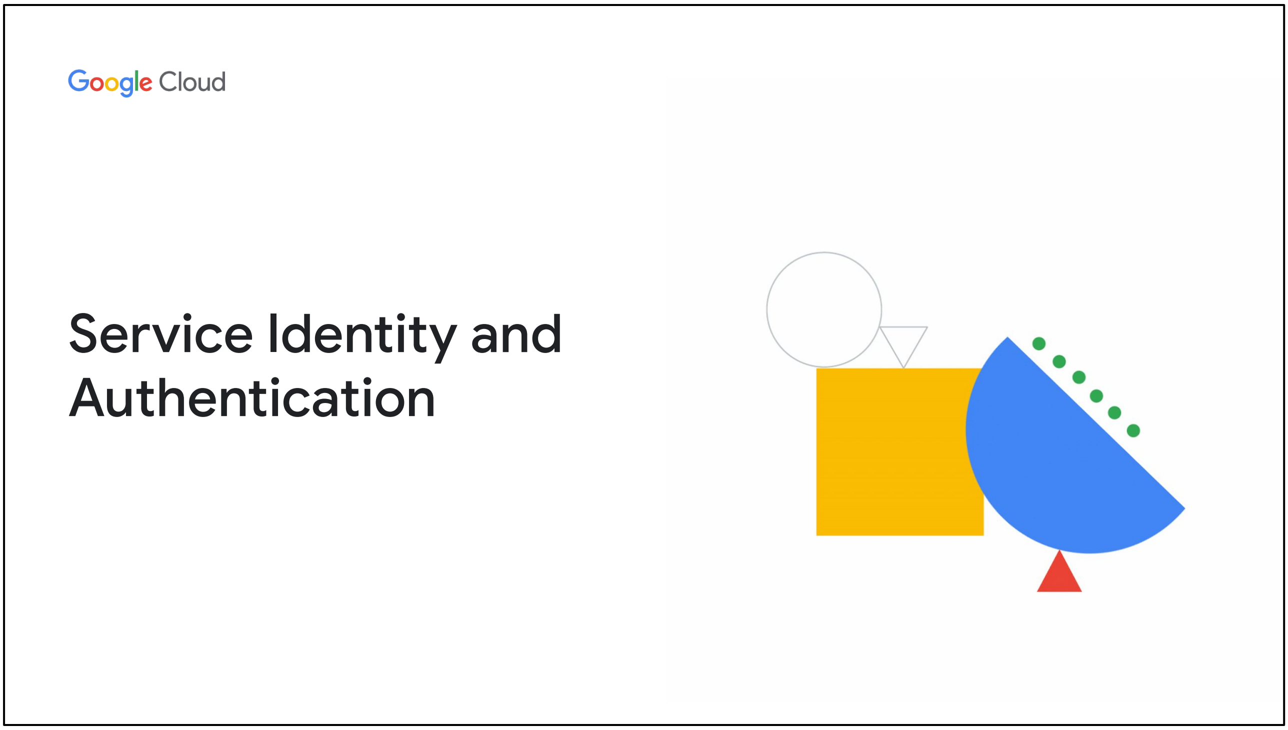
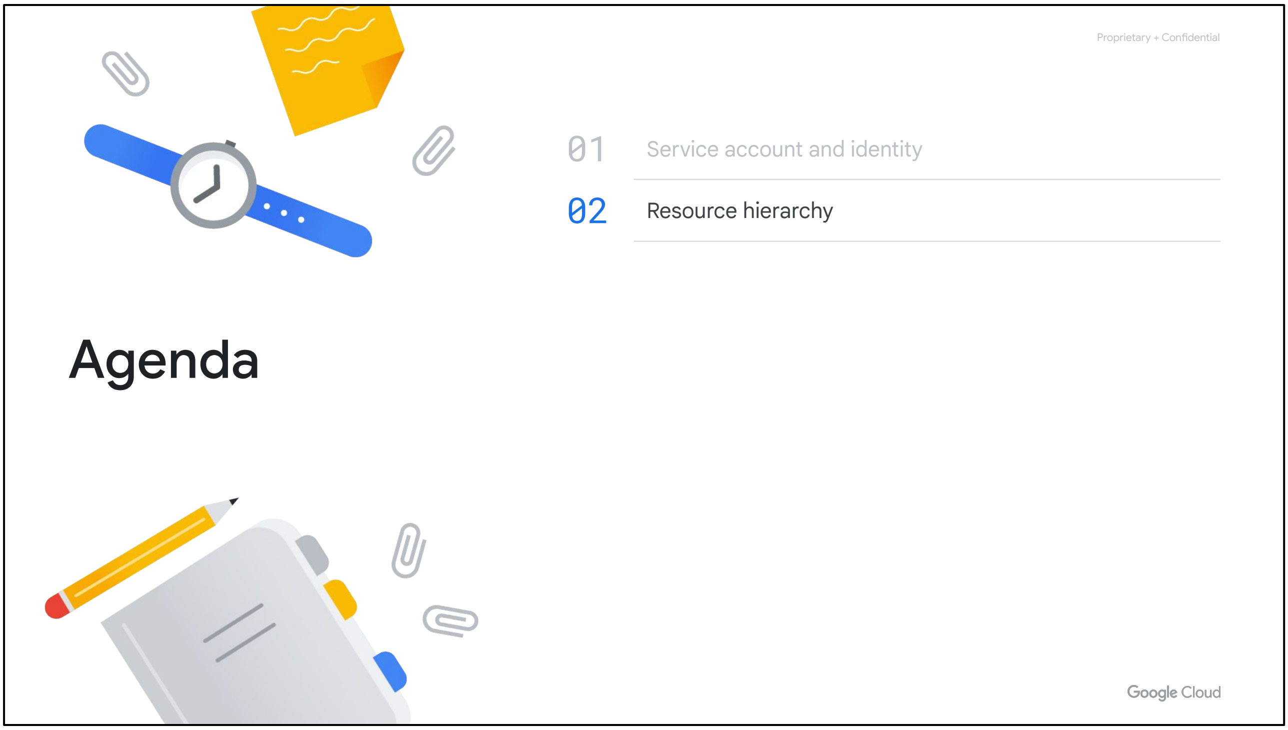


Google Cloud

Service Identity and Authentication

In this module, we discuss the fundamentals of service identity, and how you can invoke other Google Cloud services from your Cloud Run service.

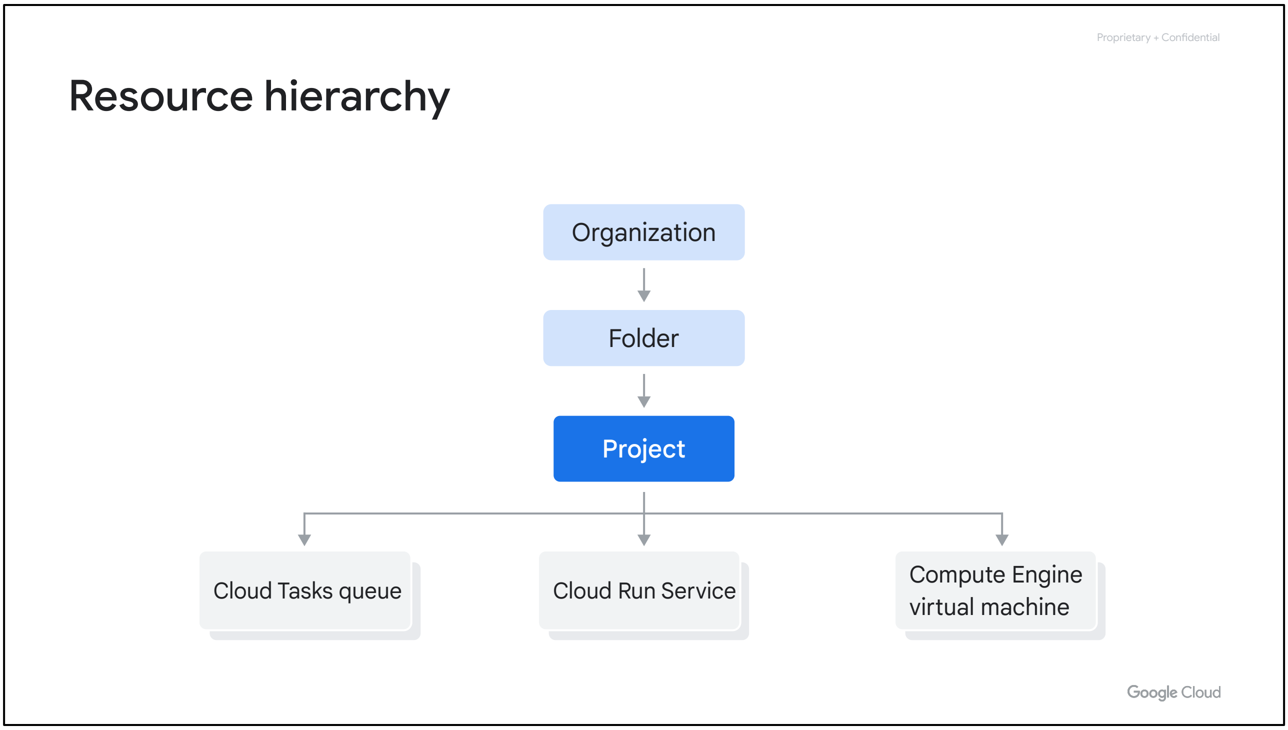


Agenda

01 Service account and identity

02 Resource hierarchy

Next, let’s look at how you can use Google Cloud resource hierarchy to simplify permissions.



Resource hierarchy

Organization

Folder

Project

Cloud Tasks queue

Cloud Run Service

Compute Engine virtual machine

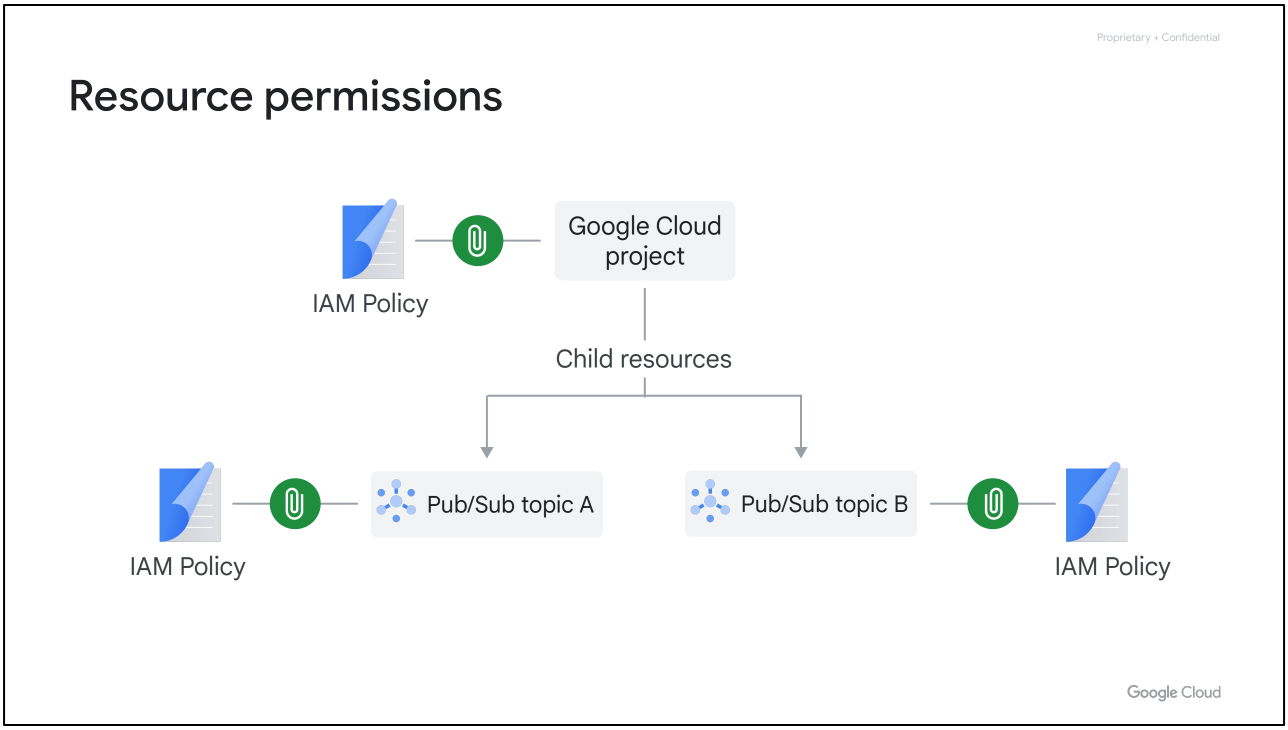
Google Cloud resources are organized hierarchically. A Google Cloud project is your primary means to organize resources, where every resource needs to be in a project.

A cloud resource can be, for example, a Cloud Tasks Queue, a Cloud Run service, or a Compute Engine virtual machine.

The organization resource is the root node of the resource hierarchy. It provides central visibility and control over every other resource that belongs to the organization.
An additional and optional grouping mechanism under the organization node is the folder. Folders can be mapped to departments, teams, or business units within an organization.

The project is the base-level entity for organizing resources. It's required to create resources, use Cloud APIs and services, manage permissions, and enable billing among other things. You can organize projects into folders.

Each resource has exactly one parent (except for the top organization node which has none).



Resource permissions

IAM Policy

Google Cloud project

Child resources

IAM Policy

Pub/Sub topic A

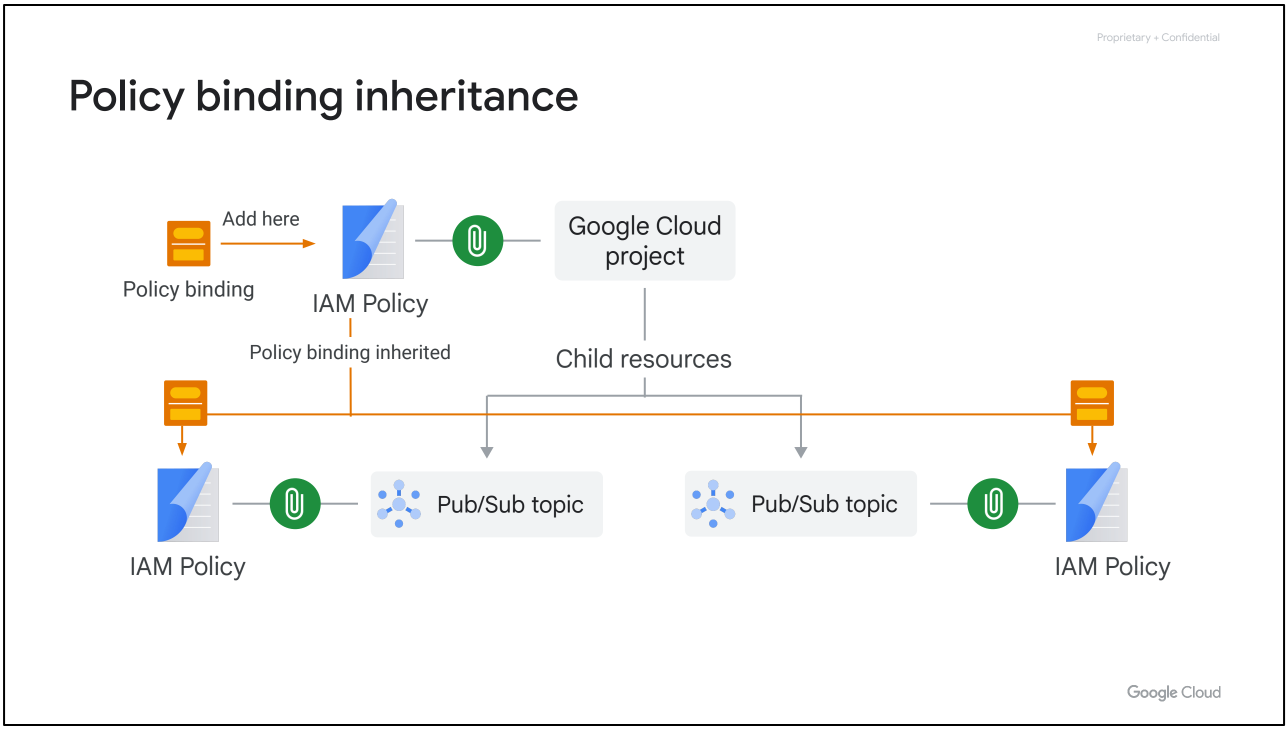
Pub/Sub topic B

IAM Policy

Every resource in the hierarchy has an IAM Policy, and you can grant permissions on it using policy bindings.

A policy binding binds an identity to a role and grants permissions to that identity on that resource.

If you think back to the example of publishing a message to a Pub/Sub topic - what was the role you needed? “Pub/Sub Publisher”.



Proprietary + Confidential

Policy binding inheritance

Policy binding

Add here

IAM Policy

Google Cloud project

Policy binding inherited

Child resources

IAM Policy

Pub/Sub topic

Pub/Sub topic

IAM Policy

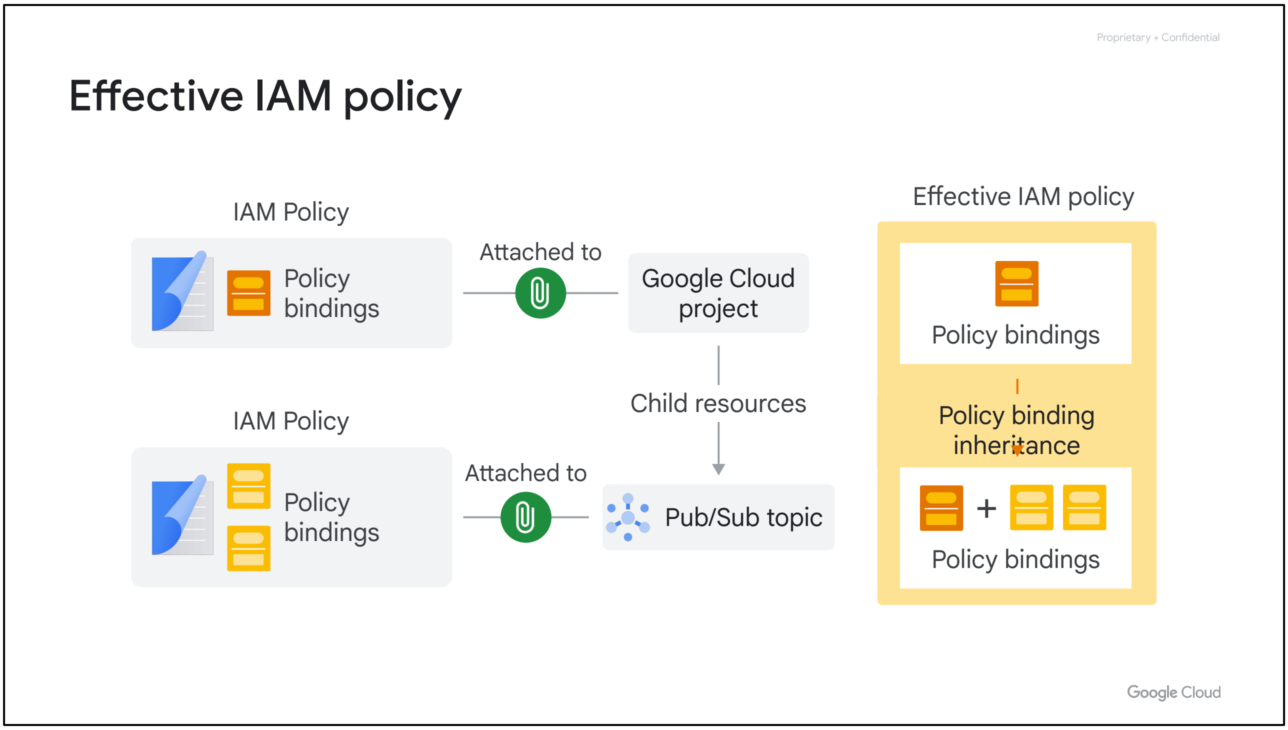
Google Cloud

How useful would it be to add that policy binding to a project, instead of to an individual Pub/Sub topic?

It turns out that that is very useful, because if you add a policy binding to a higher level resource, it’s inherited by lower level resources.

In this example, the lower level resources such as the Pub/Sub topics inherit policy bindings from their parent resource, the Google Cloud project.

This is useful when you need to grant permission to publish messages on *all topics in a project*, as opposed to just to a single topic.



Effective IAM policy

IAM Policy

Policy bindings

Attached to

Google Cloud project

Child resources

IAM Policy

Policy bindings

Attached to

Pub/Sub topic

Effective IAM policy

Policy bindings

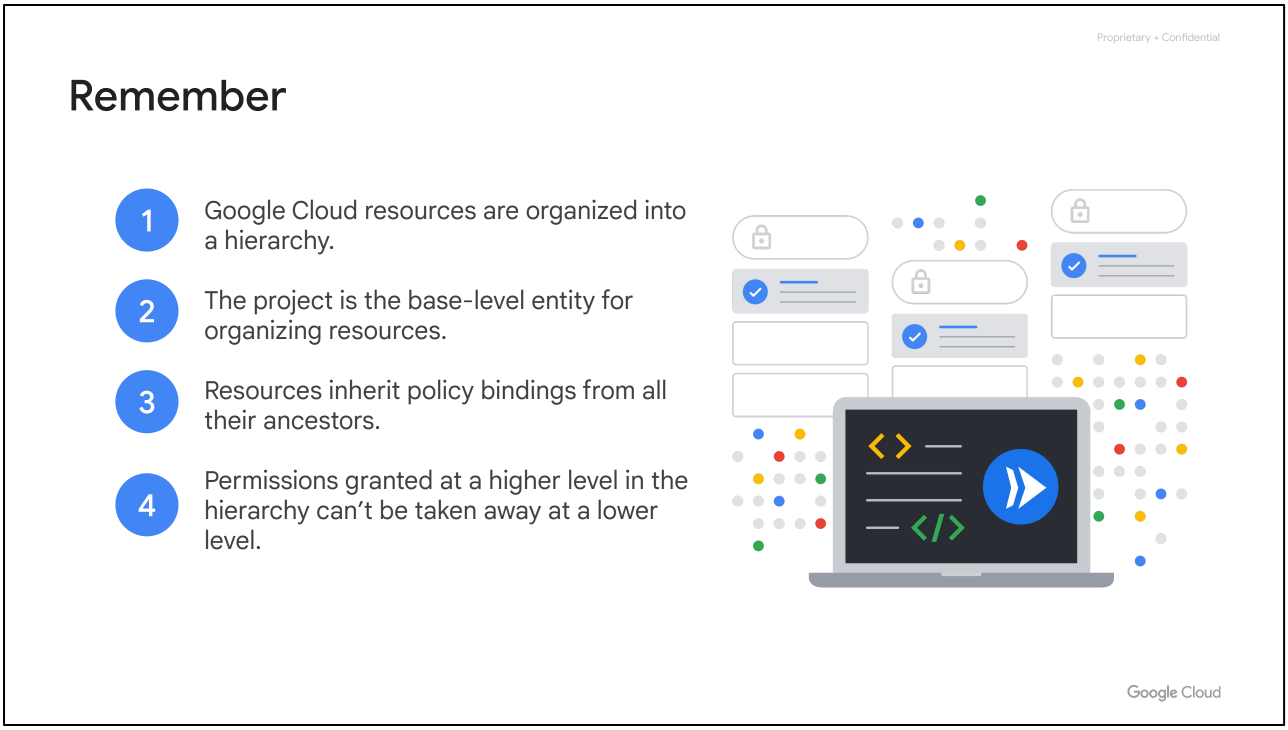
Policy binding inheritance

+

Policy bindings

Here’s another way to look at policy binding inheritance.

When IAM evaluates access to a resource, it evaluates policy bindings from the parent resource (and their parent) as well. The effective IAM policy on the resource includes those bindings that are granted to a parent which you cannot take away.



Proprietary + Confidential

Remember

1. Google Cloud resources are organized into a hierarchy.
2. The project is the base-level entity for organizing resources.
3. Resources inherit policy bindings from all their ancestors.
4. Permissions granted at a higher level in the hierarchy can’t be taken away at a lower level.

Google Cloud

In summary:

- Google Cloud resources are organized into a hierarchy, with the *project* as the base-level entity for organizing resources.
- Resources inherit policy bindings from their parent and all their ancestors.
- Permissions granted at a higher level in the hierarchy can’t be taken away at a lower level.