
Setting up a Cloud
Solutions Environment

General tips for expanding on your study plan

1. **Assess your skill level**
   - Do you already have experience with all of the skills in a particular section?
   - Do you know how to apply these skills to typical business tasks and requirements?
2. **Update your study plan notes**
   - If you need a review or more practice with these skills, write that into your study plan notes for reference.
3. **Create a list of resources that will help you gain or hone these skills**
   - Depending on experience, you may decide to take the entire suggested program of courses and labs, or only concentrate on the areas you lack.
   - Suggested documentation pages and other resources for more in-depth study will be presented at the end of every module from here on.

Google Cloud

While many people will choose to just go through the full list of resources, taking all of the courses and working on all of the labs, it is helpful to know more about the areas you may need to spend the most time on.

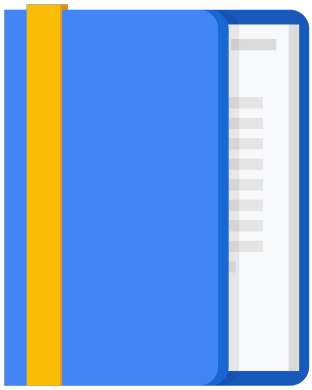
We will now go over each section in a bit more detail during the rest of this course, giving an overview of each topic and explaining some fundamental concepts to help get you started.

Agenda

Section 1.1 - Cloud Projects and Accounts

Section 1.2 - Billing Management

Section 1.3 - Command Line Interface (CLI)



Google Cloud

Exam Guide: Section 1.1

1.1 Setting up cloud projects and accounts.

Activities include:

- Creating projects.
- Assigning users to pre-defined IAM roles within a project.
- Linking users to Google Workspace identities.
- Enabling APIs within projects.
- Provisioning one or more Cloud Operations accounts.

Exam Guide: Section 1.1

1.1 Setting up cloud projects and accounts.

Activities include:

- **Creating projects.**
- **Assigning users to pre-defined IAM roles within a project.**
- Linking users to Google Workspace identities.
- Enabling APIs within projects.
- Provisioning one or more Cloud Operations accounts.

Google Cloud

The tasks listed under this section involve different areas of the Google Cloud Console - including the projects, user, API and Operations consoles.

Creating projects and assigning users to the predefined roles in those projects are very basic first tasks, so we will look at these first two items together.

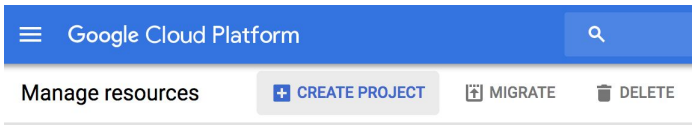
Google Cloud services are associated with a project

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

Google Cloud

You consume Google Cloud services by attaching them to, or enabling them within, a project - this is how they are billed and tracked and given permissions to operate.

Creating a Project



Project ID	Globally unique	Chosen by you	Immutable
Project name	Need not be unique	Chosen by you	Mutable
Project number	Globally unique	Assigned by Google Cloud	Immutable

Google Cloud

Creating a basic project is quick and easy - but it requires some attention to labeling and naming.

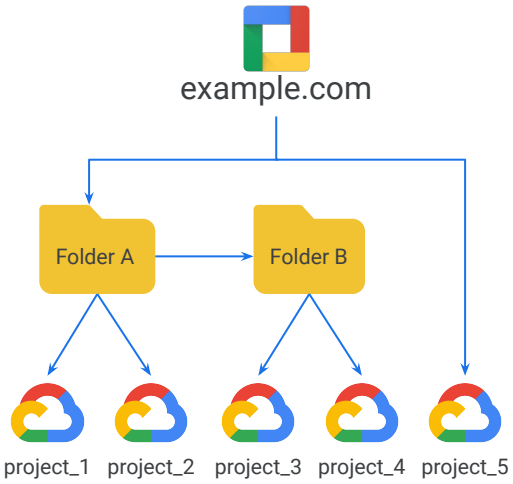
The two items highlighted are provided by the person setting up the project.

Project ID, once set, cannot be changed, so think this one through carefully.

The third - Project number - is automatically generated by the Google Cloud system and also cannot be changed.

Folders group projects and policies

- You do not have to use folders to organize your projects, but they often help.
- Folders group projects under an organization.
- Folders can contain projects, other folders, or both.
- You can use folders to assign access policies.



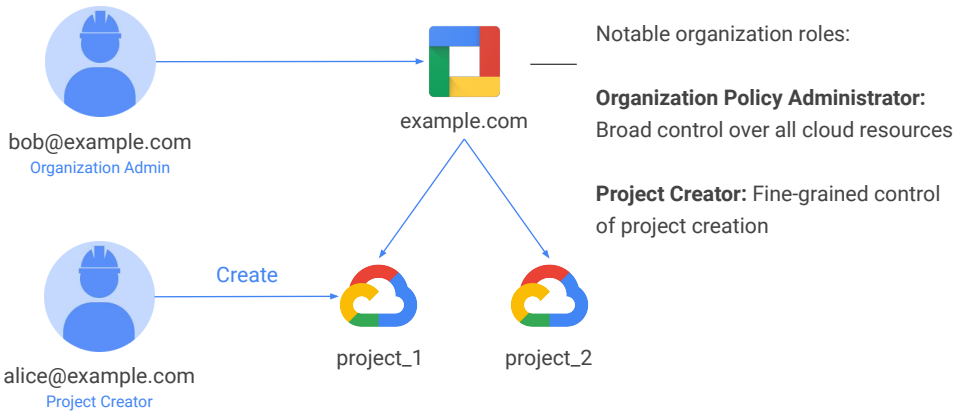
Google Cloud

The main thing to remember when it comes to organizing your projects is everything is arranged in a hierarchy.

The top of this hierarchy is the organization node.

Everything else rests under this main node.

Typical roles in an organization



Google Cloud

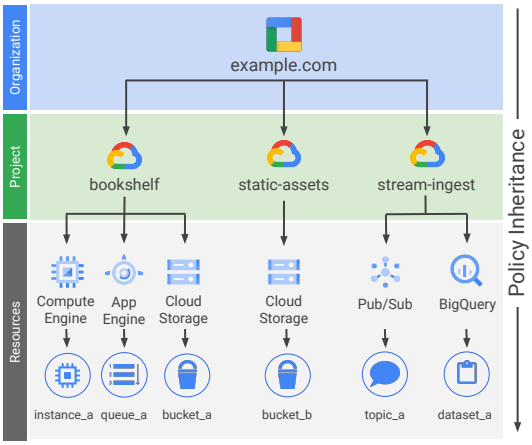
When you have a new organization node, by default it lets any user in the domain create projects and billing accounts.

But best practice with a new organization node is to first decide who on your team really **should** be able to do those things.

Then you can assign each user to a role (or roles) for easier and more secure administration.

Understanding permission 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.



Google Cloud

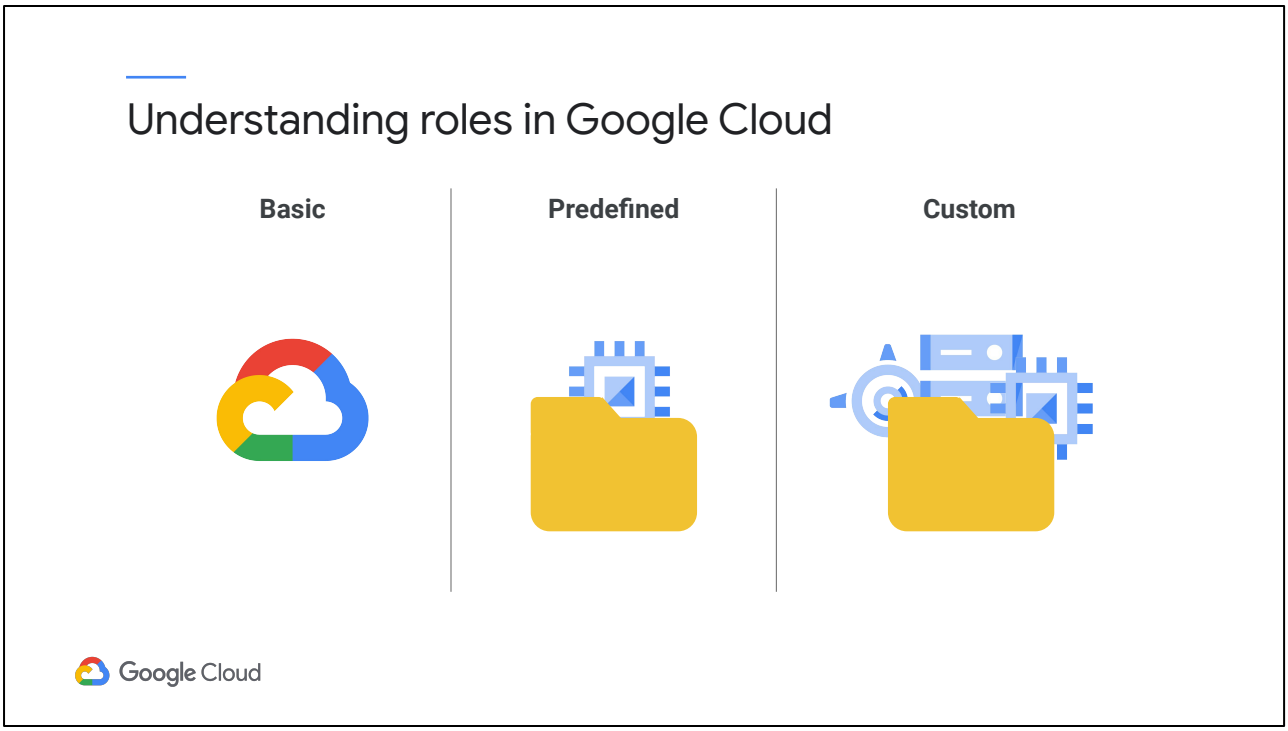
Permissions in Google Cloud are **inheritable** - this means that each resource that sits below another one in the hierarchy includes all of the permissions given to its parent.

Parent permissions given to a child resource **cannot be removed** by that child or by another resource at the same level or by anything further down in the hierarchy.

For example, if the parent gives a user or role permission to edit a resource, a child of that parent cannot take that edit permission away.

A child resource, however, **can add permissions** to the ones inherited from its parent.

This is how you get “finer-grained” control over who can use or modify resources.

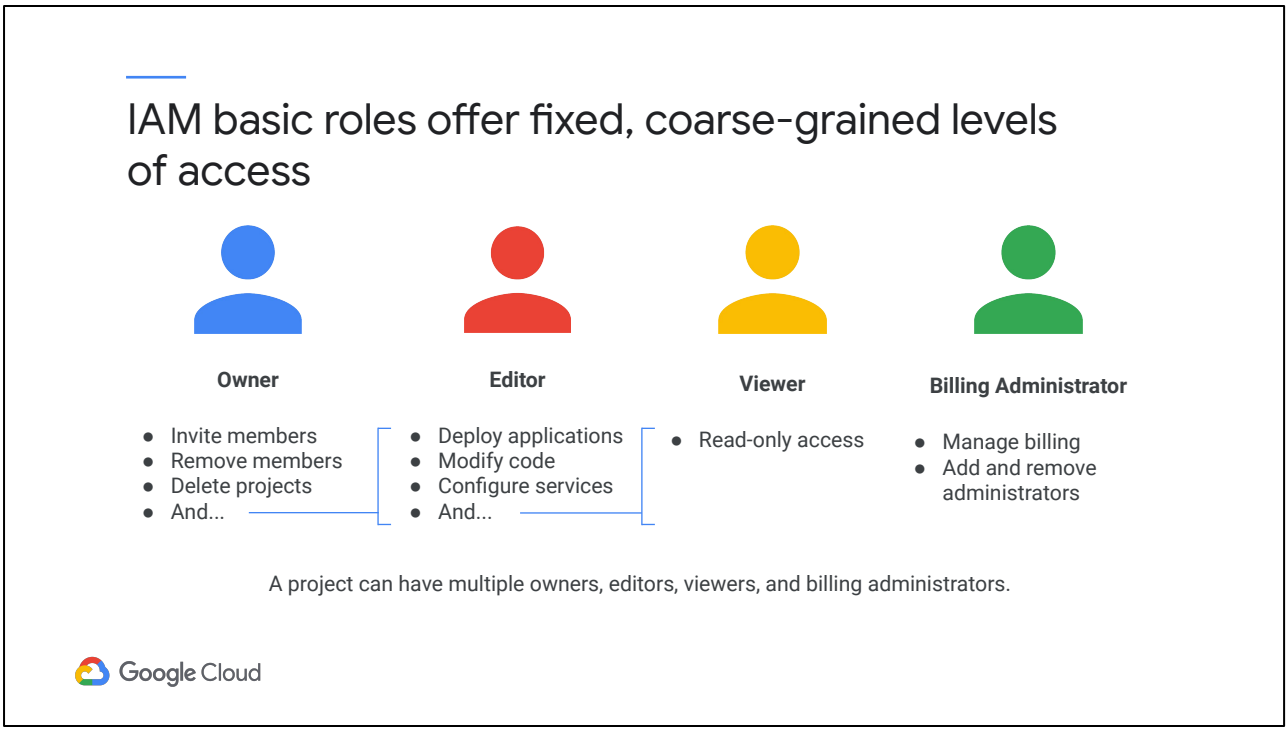


What is a “role” in the context of Google Cloud resources?

A role is simply a collection of permissions. Generally, roles exist to define what tasks can be performed on certain resources, and when assigned to users, who can perform them.

Roles help to simplify assigning and maintaining permissions on project resources. They assist administrators in providing everyone in the project just the right amount of access - and no more - to get their jobs done.

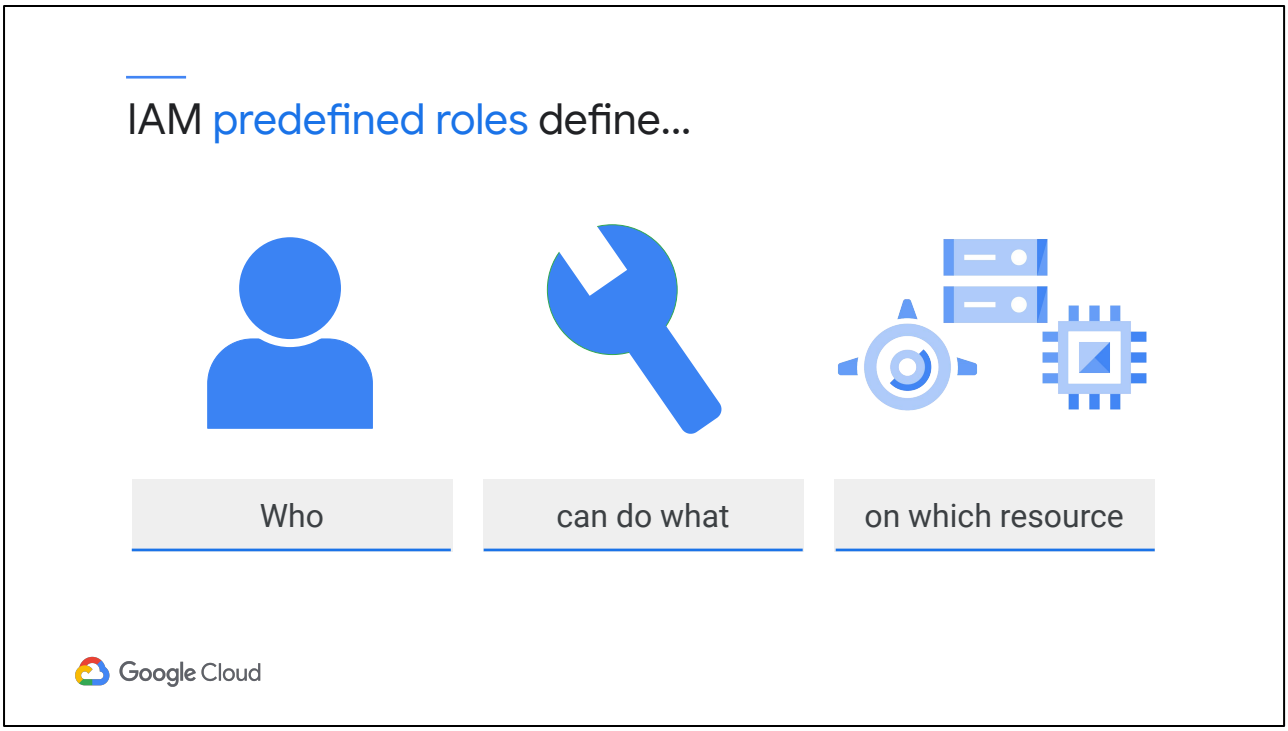
There are three main types of roles that can be applied to your Google Cloud users and resources: Basic, Predefined and Custom. We will not go into Custom roles in this module.



Let's look at the three basic roles first. These basic roles are the Owner, Editor, and Viewer.

- 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.

If you have several people working together on a project that contains sensitive data, basic roles are probably not fine enough. Fortunately, Cloud IAM provides other, finer-grained types of roles.



Permissions are said to define “who, can do what, on which resource.”

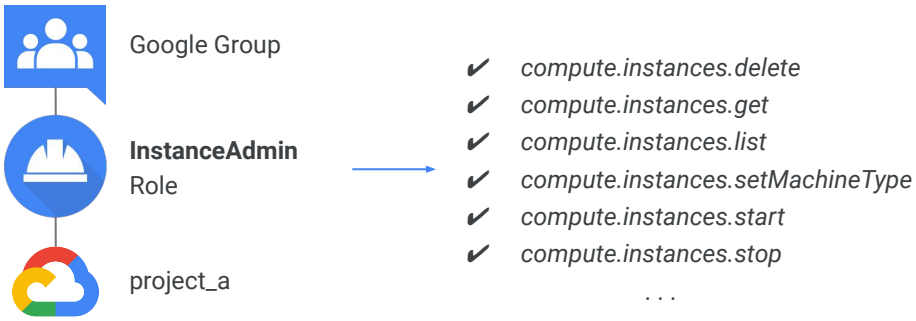
This is generally a very coarse way of assigning permissions in a project, as it generally means assigning view, edit or administrate levels of access. However, Google Cloud also offers predefined roles, which help narrow the scope down to...

Who can do what (from a long list of unique possibilities) **on that particular type of resource**.

- Each service has a defined list of possible permissions that can be granted to users working upon that resource.
- Pre-defined roles bundle selected permissions up into collections that correlate with common job-related business needs.
- So, instead of being granted all permissions, or an ad hoc list of separate permissions that might be missing something important, a user can simply be assigned a predefined role instead.

Compute Engine, for example, offers a set of predefined roles which can be applied to Compute Engine resources in a given project, a given folder, or over an entire organization. Let’s look at this in more detail.

IAM predefined roles are fine-grained permissions on particular services



Google Cloud

In this example, we see a partial list (the "..." indicates there are more options not shown) of the Compute Engine permissions that have been bundled into the predefined "**InstanceAdmin**" role. These permissions determine what that role is allowed to do with virtual machines. (Other pre-defined roles in Compute Engine will have their own customized list of permissions, depending on what tasks that role is generally expected to perform.)

Having these predefined roles in place for common job functions saves time and administrative overhead, since Google keeps these up to date with any new permissions that are deemed required for that role.

Why use pre-defined roles?

- Lowers business risk of accidental or deliberate damage to, or misuse of, vital data and systems.
- Increases overall system and data security.
- Finer granularity on permissions is considered a best practice.
- Using coarse permissions may allow or cause users to violate regulations.

Google Cloud

Wouldn't just giving everyone every permission on a service be much simpler to maintain?

Simpler, maybe, but much more risky as this violates the security "principle of least privilege" and increases the chance of accidental or deliberate damage to a company's vital services and data.

For example, an accountant as a user might need access to reporting data generated on a Compute Engine instance, but does NOT need to be able delete that Compute Engine instance.

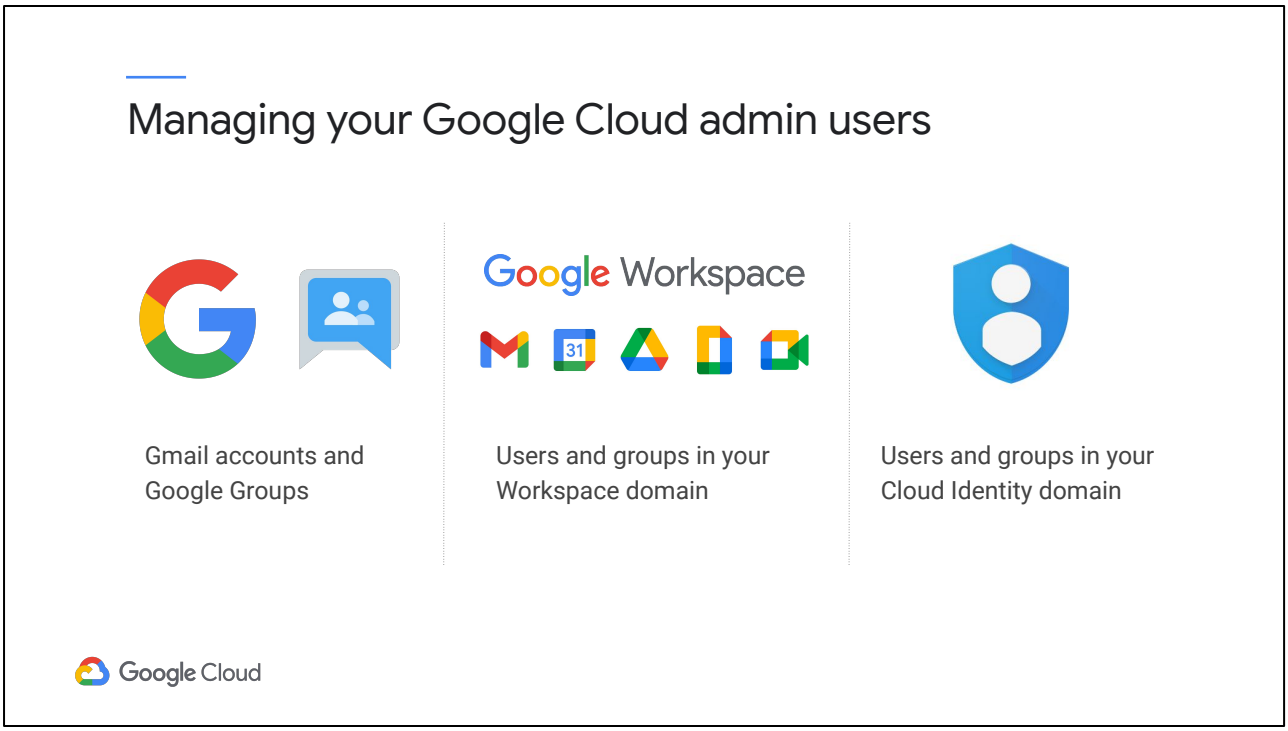
Giving them permissions to do so would not be good security practice, would increase risk of accidental deletions, and might in fact cause a company to violate certain regulations.

Exam Guide: Section 1.1

1.1 Setting up cloud projects and accounts.

Activities include:

- Creating projects.
- Assigning users to pre-defined IAM roles within a project.
- **Linking users to Google Workspace identities.**
- Enabling APIs within projects.
- Provisioning one or more Cloud Operations accounts.



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 Google 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.

Exam Guide: Section 1.1

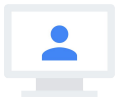
1.1 Setting up cloud projects and accounts.

Activities include:

- Creating projects.
- Assigning users to pre-defined IAM roles within a project.
- Linking users to Google Workspace identities.
- **Enabling APIs within projects.**
- Provisioning one or more Cloud Operations accounts.

There are four ways to interact with Google Cloud resources and services

Cloud Platform Console	Cloud SDK and Cloud Shell	Cloud Console Mobile App	REST-based API
Web user interface	Command-line interface	For iOS and Android	For custom applications




Google Cloud

There are four ways you can interact with Google Cloud, but here we'll talk about APIs.

(We will discuss the command-line interface in the last section.)

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 Google 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 directly.

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, but basically, it means that your code can use Google services in much the same way that web browsers talk to web servers.

Use APIs Explorer to help you write your code

- The APIs Explorer is an interactive tool that lets you easily try Google APIs using a browser.
- With the APIs Explorer, you can:
  - Browse quickly through available APIs and versions.
  - See methods available for each API and what parameters they support along with inline documentation.
  - Execute requests for any method and see responses in real time.
  - Easily make authenticated and authorized API calls.

The Cloud Console includes a tool called the APIs Explorer that helps you learn about available APIs interactively. These APIs expect parameters, and documentation on parameters and on using 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. Does that mean you now have to start coding your application 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.

Exam Guide: Section 1.1

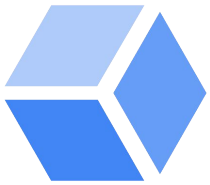
1.1 Setting up cloud projects and accounts.

Activities include:

- Creating projects.
- Assigning users to pre-defined IAM roles within a project.
- Linking users to Google Workspace identities.
- Enabling APIs within projects.
- **Provisioning one or more Cloud Operations accounts.**

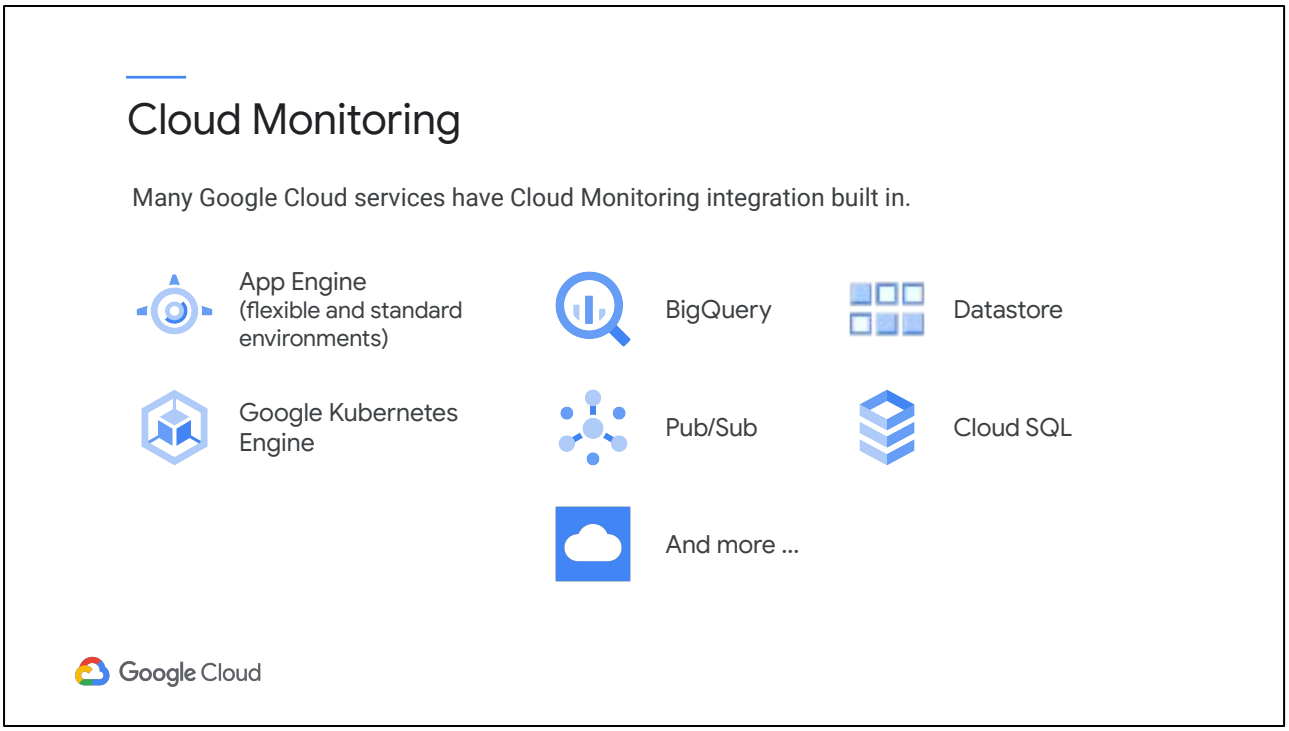
Google Cloud's operations suite

- Google Cloud's operations suite is a multi-cloud monitoring and management service that aggregates metrics, logs, and events.
  - Integrated monitoring, logging, diagnostics.
  - Manages across platforms (Google Cloud, AWS, and on-prem).
- It provides developers, operators, and security professionals a rich set of observable signals that speed root-cause analysis and reduce mean time to resolution (MTTR).

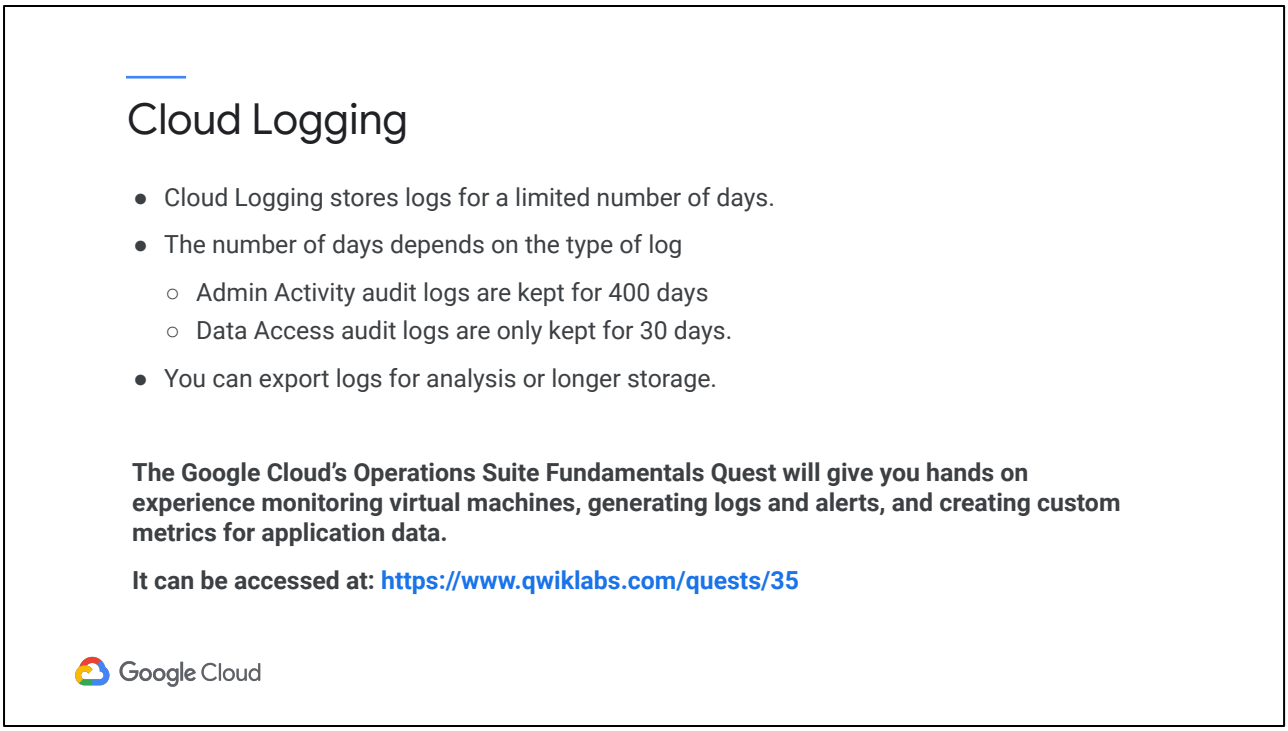


Google Cloud

One powerful option for logging and monitoring your servers and applications in Google Cloud is Google Cloud's operations suite.



Cloud Monitoring is already integrated into many Google Cloud services and products.



The best way to study for this section is to actually *use* Cloud Monitoring and Cloud Logging.

If you have never used these tools, the **Google Cloud's Operations Suite Fundamentals Quest** will give you hands on experience monitoring virtual machines, generating logs and alerts, and creating custom metrics for application data.

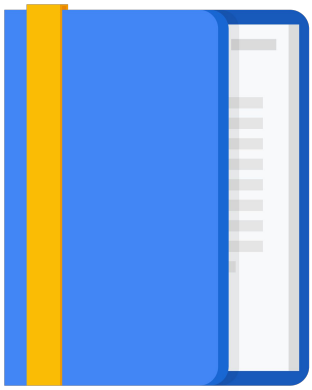
It can be accessed at: https://www.qwiklabs.com/quests/35

Agenda

Section 1.1 - Cloud Projects and Accounts

Section 1.2 - Billing Management

Section 1.3 - Command Line Interface (CLI)



Google Cloud

Exam Guide: Section 1.2

1.2 Managing billing configuration.

Activities include:

- Creating one or more billing accounts.
- Linking projects to a billing account.
- Establishing billing budgets and alerts.
- Setting up billing exports to estimate daily/monthly charges.

Understanding billing

- To manage billing accounts and to add projects to them, you must be a billing administrator.
- To change the billing account for an existing project, **you must be an owner on the project and a billing administrator on the destination billing account.**
- When you create a new project, you're prompted to choose which of your billing accounts you want to link to the project. If you have only one billing account, that account is automatically linked to your project.
- If you don't have a billing account, you must create one and enable billing for your project before you can use many Google Cloud features.

Understanding budgets and alerts

Avoid surprises on your bill by creating budgets to monitor all your Google Cloud charges in one place. After you've set a budget amount, you set budget alert rules that are used to trigger notifications, so you can stay informed of how your spend is tracking against your budget.

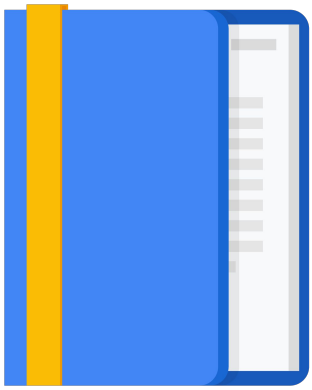
- To set a budget alert you must be a billing administrator.
- You can apply budget alerts to either a billing account or a project.
- You can set the budget to an amount you specify or match it to the previous month's spend.
- Setting a budget does ***not*** cap API usage. Your services will continue to operate and accrue costs, even if a budget alert has been triggered.

Agenda

Section 1.1 - Cloud Projects and Accounts

Section 1.2 - Billing Management

Section 1.3 - Command Line Interface (CLI)



Google Cloud

Exam Guide: Section 1.3

1.3 Installing and configuring the command line interface (CLI), specifically the Cloud SDK (e.g., setting the default project)

Google Cloud

Google Cloud Console

- Offers access to Cloud Shell.
  - A temporary virtual machine with the Cloud SDK preinstalled.

Google Cloud

The Google Cloud Console has a command-line interface to Google Cloud that's easily accessed from your browser - it's called Cloud Shell.

From Cloud Shell, you can use the tools provided by the Google Cloud Software Development Kit (SDK) without first having to install them somewhere.

What's the Software Development Kit? We'll talk about that next.

Cloud SDK

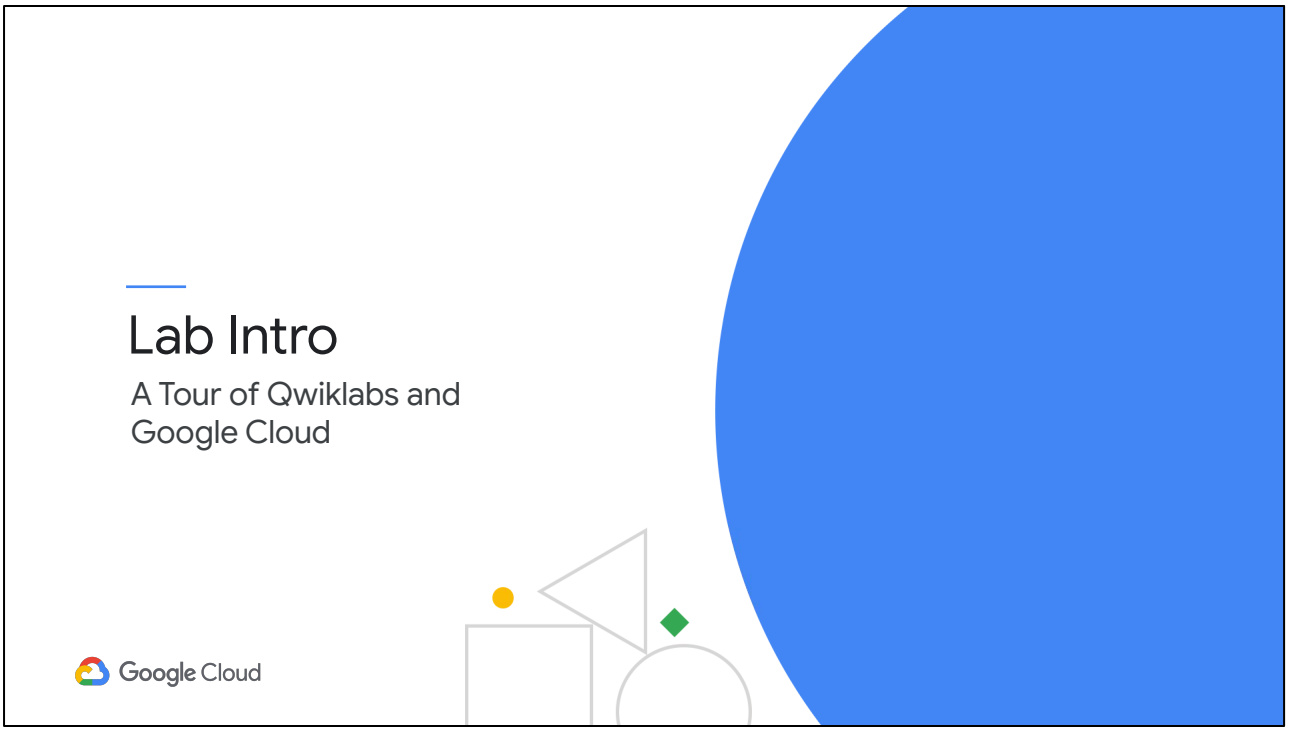
- Includes command-line tools for Google Cloud products and services.
  - gcloud, gsutil (Cloud Storage), bq (BigQuery)
- Access via the Cloud Shell button in the Cloud Console.
- Can also be installed on local machines.
- Is also available as a Docker image.

Google Cloud

The Cloud SDK is a set of tools that you can use to manage your resources and your applications on Google Cloud. These include the gcloud tool, which provides the main command-line interface for Google Cloud products and services. There's also gsutil, which is for Google Cloud Storage; and bq, which is for BigQuery.

The easiest way to get to the SDK commands is to click the Cloud Shell button in the Cloud Console. You will get a command line interface in your web browser on a virtual machine with all these commands already installed. You can also install the SDK on your own computers: your laptop, your on-premises servers, or virtual machines in other clouds.

The SDK is also available as a Docker image, which can be a really easy and clean way to work with it if your applications are containerized.



Google Cloud is a suite of cloud services hosted on Google's infrastructure. From computing and storage, to data analytics, machine learning, and networking, Google Cloud offers a wide variety of services and APIs that can be integrated with any cloud-computing application or project—be it personal or enterprise-grade.

In this introductory-level lab, you will take your first steps with Google Cloud by getting hands-on practice with the Google Cloud Console—an in-browser UI that lets you access and manage Google Cloud services. You will identify key features of Google Cloud and also learn the ins and outs of the Qwiklabs environment. If you are new to cloud computing or looking for an overview of Google Cloud and Qwiklabs, you are in the right place!

This lab is part of the Qwiklabs Google Cloud Essentials Quest.

Suggested study resources for this section

Google Cloud Overview: https://cloud.google.com/docs/overview/

Cloud Identity: https://cloud.google.com/identity/

Google Cloud Pricing Calculator: https://cloud.google.com/products/calculator/

Google Cloud Billing documentation: https://cloud.google.com/billing/docs/

Google Cloud's Operations Suite Fundamentals Quest: https://www.qwiklabs.com/quests/35

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

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


Google Cloud