CLOUD COMPUTING
(Undergraduate Course)

PRACTICES
Practice 1 – Cloud Account, Project and Monitoring

Presenter: **Dr. Nguyen Dinh Long**

Email: dinhlonghcmut@gmail.com

Oct. 2022

Outline

- Overview of Cloud Computing
- Basic Principles, Models and Concepts
- Structures of Cloud Computing Platform
- Infrastructure of Cloud Computing and Applications
- Technology and Programming in Cloud Computing
- Project Design on Cloud Computing
- Cloud Computing Management and Implementation

References

Main:

- Thomas Erl, Zaigham Mahmood, and Ricardo Puttini. 2013. *Cloud Computing Concepts, Technology & Architecture*. Prentice Hall.
- Michael J. Kavis. 2014. *Architecting the Cloud: Design Decisions for Cloud Computing Service Models*. Wiley
- Arshdeep Bahga, and Vijay Madisetti. 2013. *Cloud Computing: A Hands-On Approach*. CreateSpace Independent Publishing Platform

More:

- Rajkuma Buyya, Jame Broberg and Andrzej Goscinski. 2011. *Cloud Computing –Principles and paradigms*, Wiley
- Nick Antonopoulos, and Lee Gillam. 2010. *Cloud Computing - Principles, Systems and Applications*, Springer-Verlag London Limited.

- Slides here are modified from several sources in Universities and Internet.

Cloud Computing: Practices

NLU – DH20HM
Course: Cloud Computing

PRACTICES – Google Cloud Platform (GCP)

Levels: Beginning (3 weeks) – Intermediate (3 weeks) – Advanced (3 weeks)

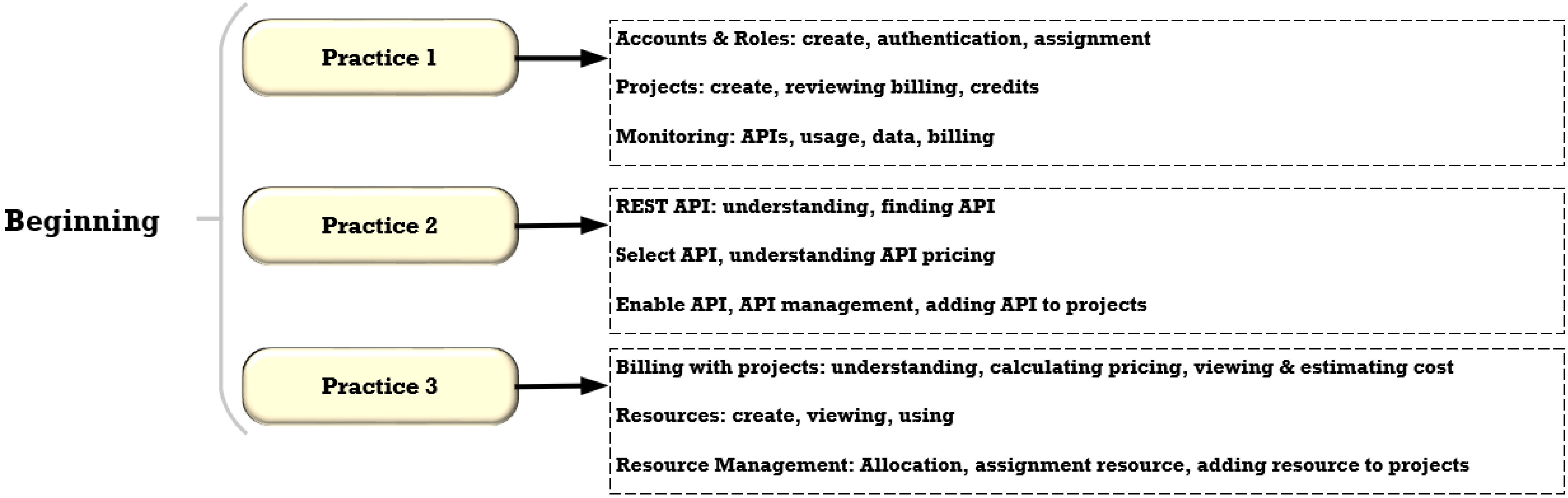
Groups: 9 with 5 person/group

Practice: submit a report for each group, submit to our Google Classroom

Cloud Computing: Practices

NLU – DH20HM
Course: Cloud Computing

PRACTICES – Google Cloud Platform (GCP)



Beginning

Practice 1

- Accounts & Roles: create, authentication, assignment
- Projects: create, reviewing billing, credits
- Monitoring: APIs, usage, data, billing

Practice 2

- REST API: understanding, finding API
- Select API, understanding API pricing
- Enable API, API management, adding API to projects

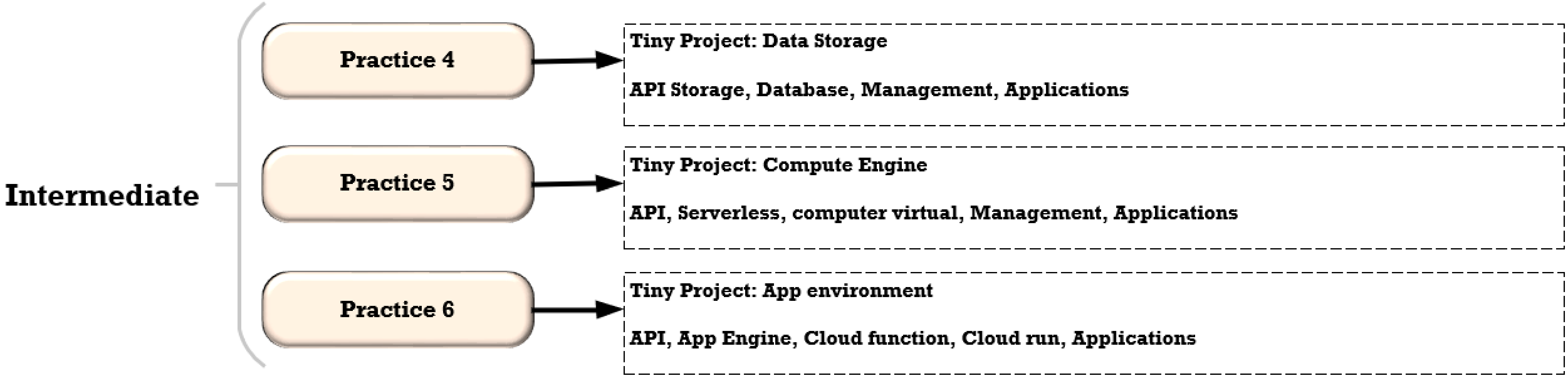
Practice 3

- Billing with projects: understanding, calculating pricing, viewing & estimating cost
- Resources: create, viewing, using
- Resource Management: Allocation, assignment resource, adding resource to projects

Cloud Computing: Practices

NLU – DH20HM
Course: Cloud Computing

PRACTICES – Google Cloud Platform (GCP)



Intermediate

Practice 4

Tiny Project: Data Storage

API Storage, Database, Management, Applications

Practice 5

Tiny Project: Compute Engine

API, Serverless, computer virtual, Management, Applications

Practice 6

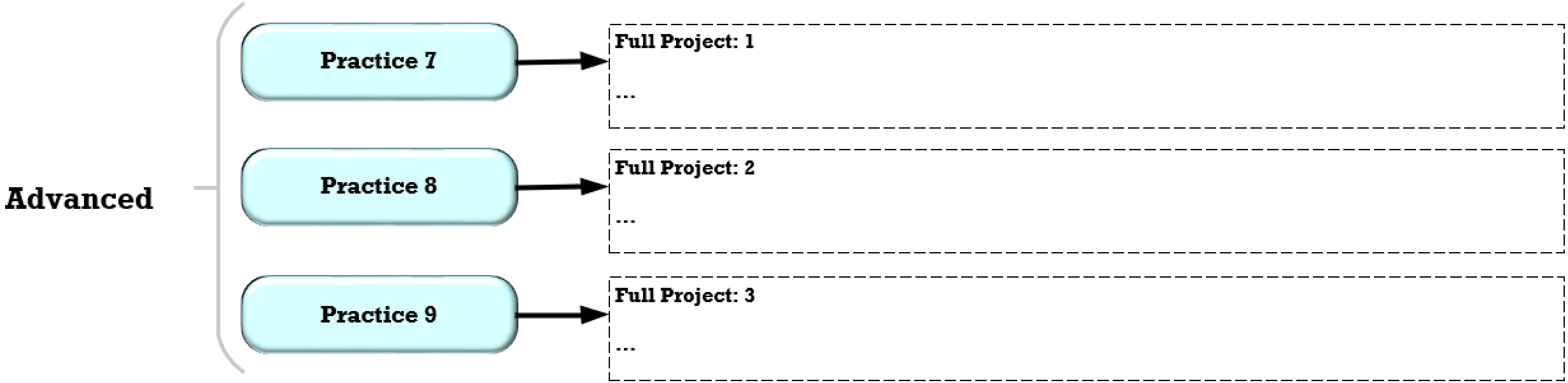
Tiny Project: App environment

API, App Engine, Cloud function, Cloud run, Applications

Cloud Computing: Practices

NLU – DH20HM
Course: Cloud Computing

PRACTICES – Google Cloud Platform (GCP)



Advanced

Practice 7

Full Project: 1

…

Practice 8

Full Project: 2

…

Practice 9

Full Project: 3

…

Content of Practice 1

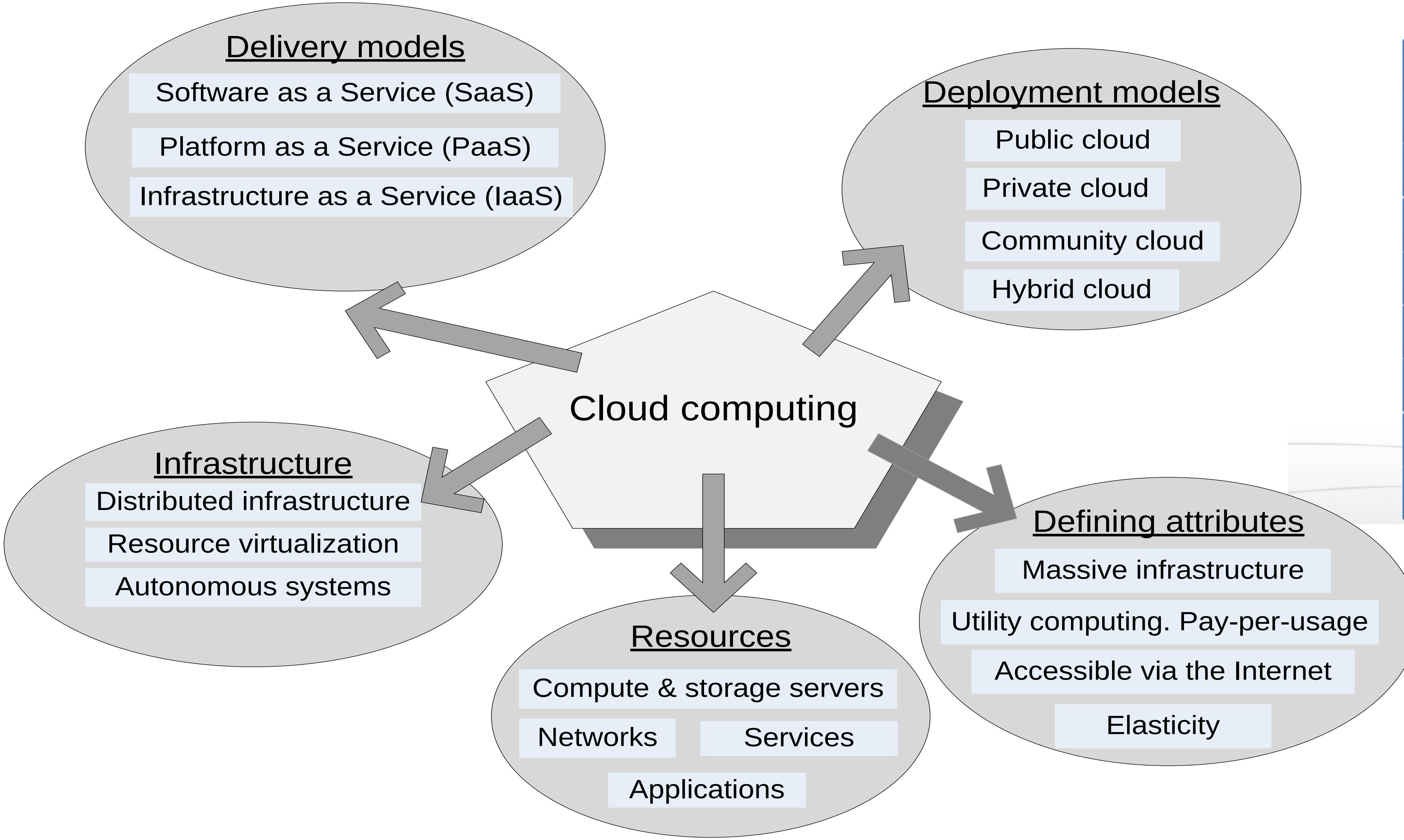
1. Cloud Account

2. Cloud Projects

3. Cloud Resource Roles (Grant accessing)

4. Cloud Monitoring

CLOUD CONCEPTS AND PRINCIPLES



Cloud computing

Delivery models
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

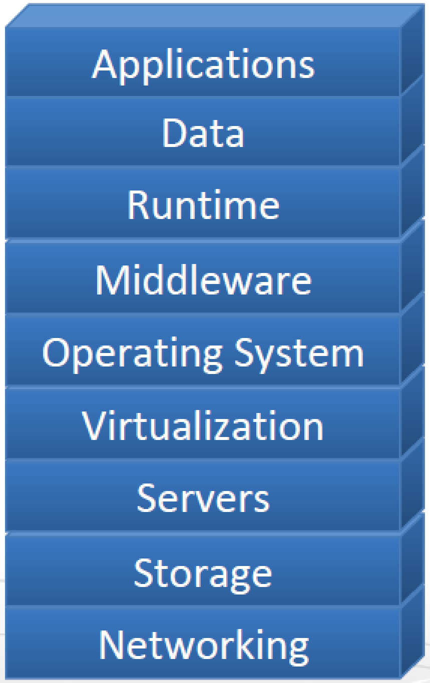
Deployment models
- Public cloud
- Private cloud
- Community cloud
- Hybrid cloud

Infrastructure
- Distributed infrastructure
- Resource virtualization
- Autonomous systems

Resources
- Compute & storage servers
- Networks
- Services
- Applications

Defining attributes
- Massive infrastructure
- Utility computing. Pay-per-usage
- Accessible via the Internet
- Elasticity

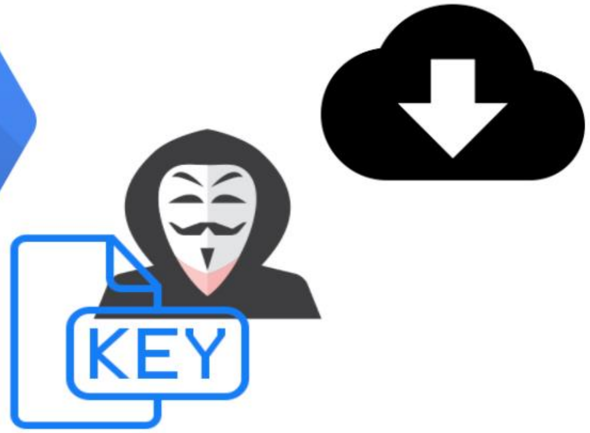
The Cloud Stack

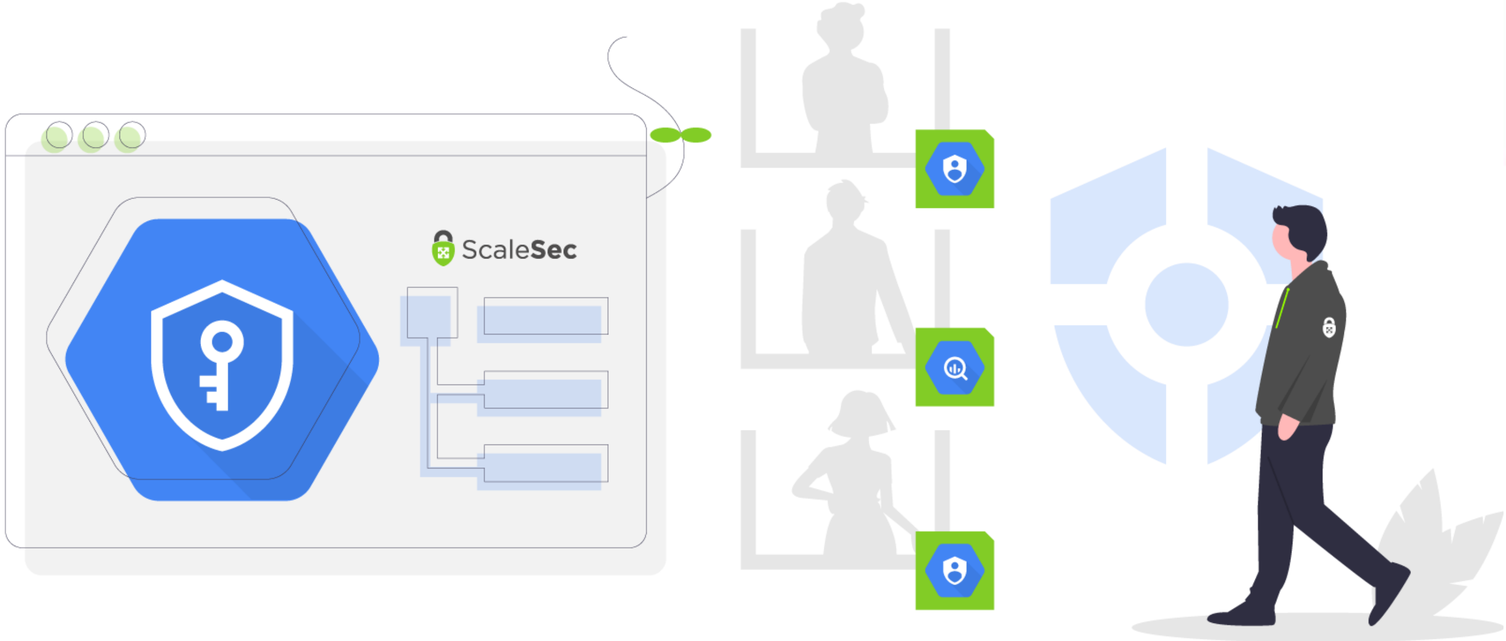


- Applications
- Data
- Runtime
- Middleware
- Operating System
- Virtualization
- Servers
- Storage
- Networking

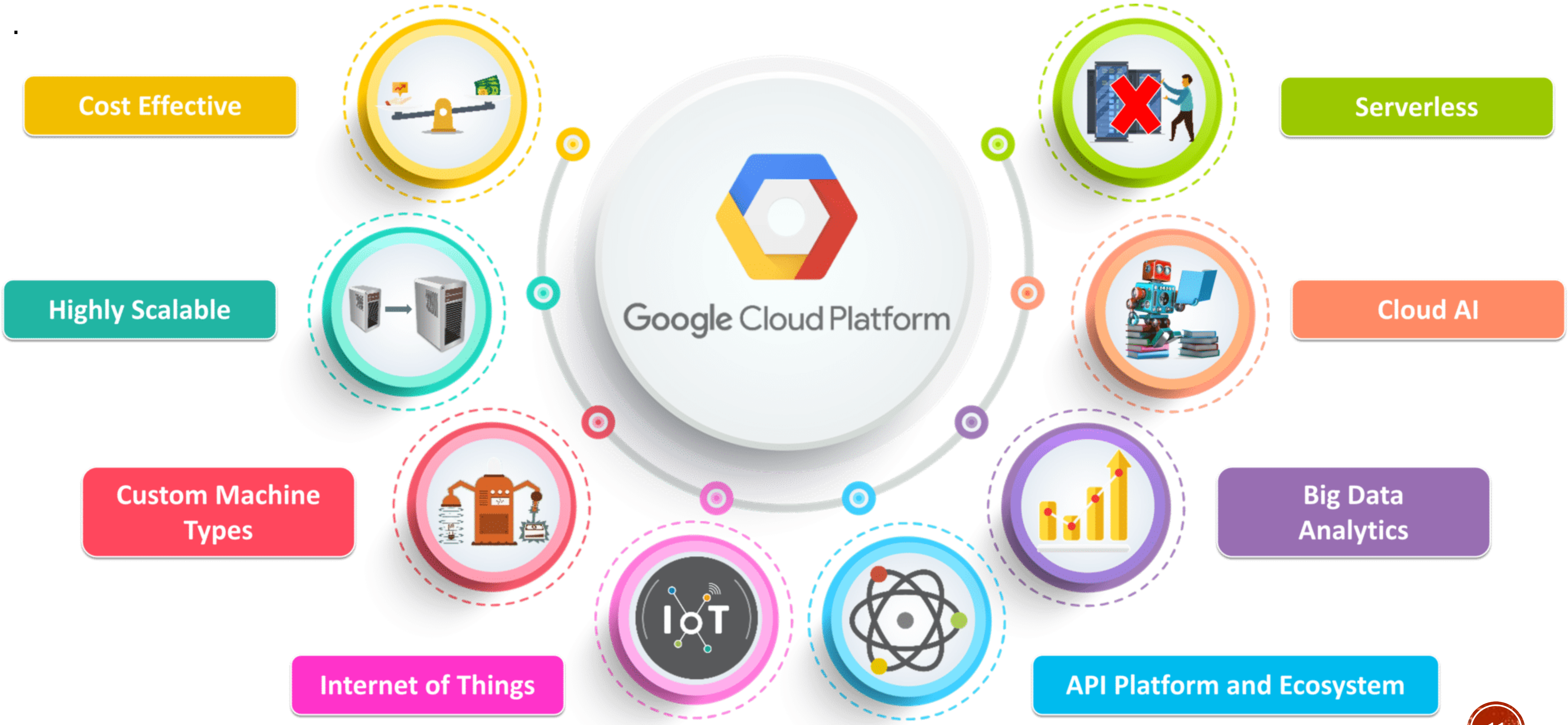
Practice 1 - Accounts

.





Practice 1 - Projects



Google Cloud Platform

Cost Effective

Serverless

Highly Scalable

Cloud AI

Custom Machine Types

Big Data Analytics

Internet of Things

API Platform and Ecosystem

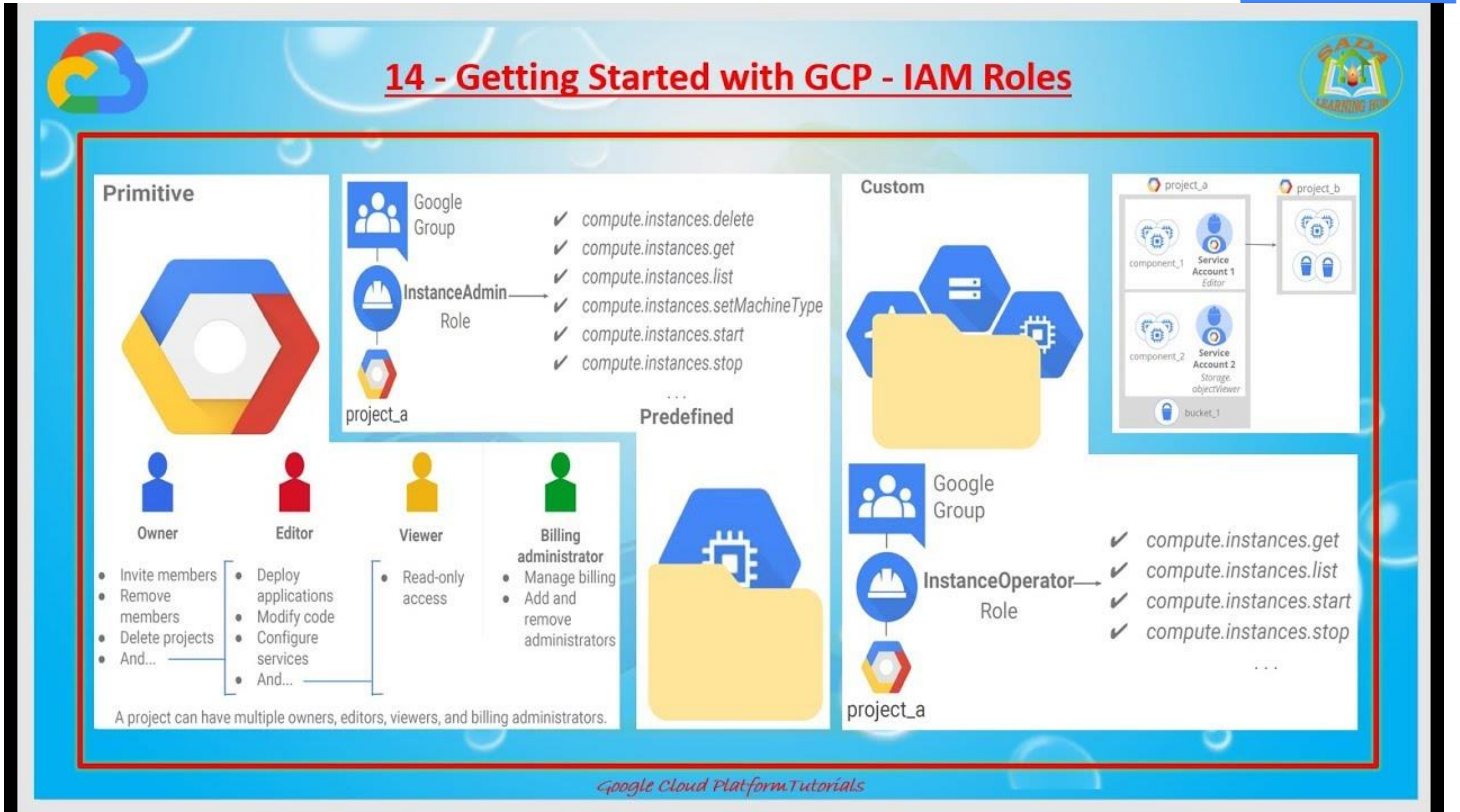
Practice 1 – Resource Roles

.

Who

can do what

on which resource



14 - Getting Started with GCP - IAM Roles

Primitive

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.

Predefined

Google Group

InstanceAdmin Role →

project_a

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

. . .

Custom

Google Group

InstanceOperator Role →

project_a

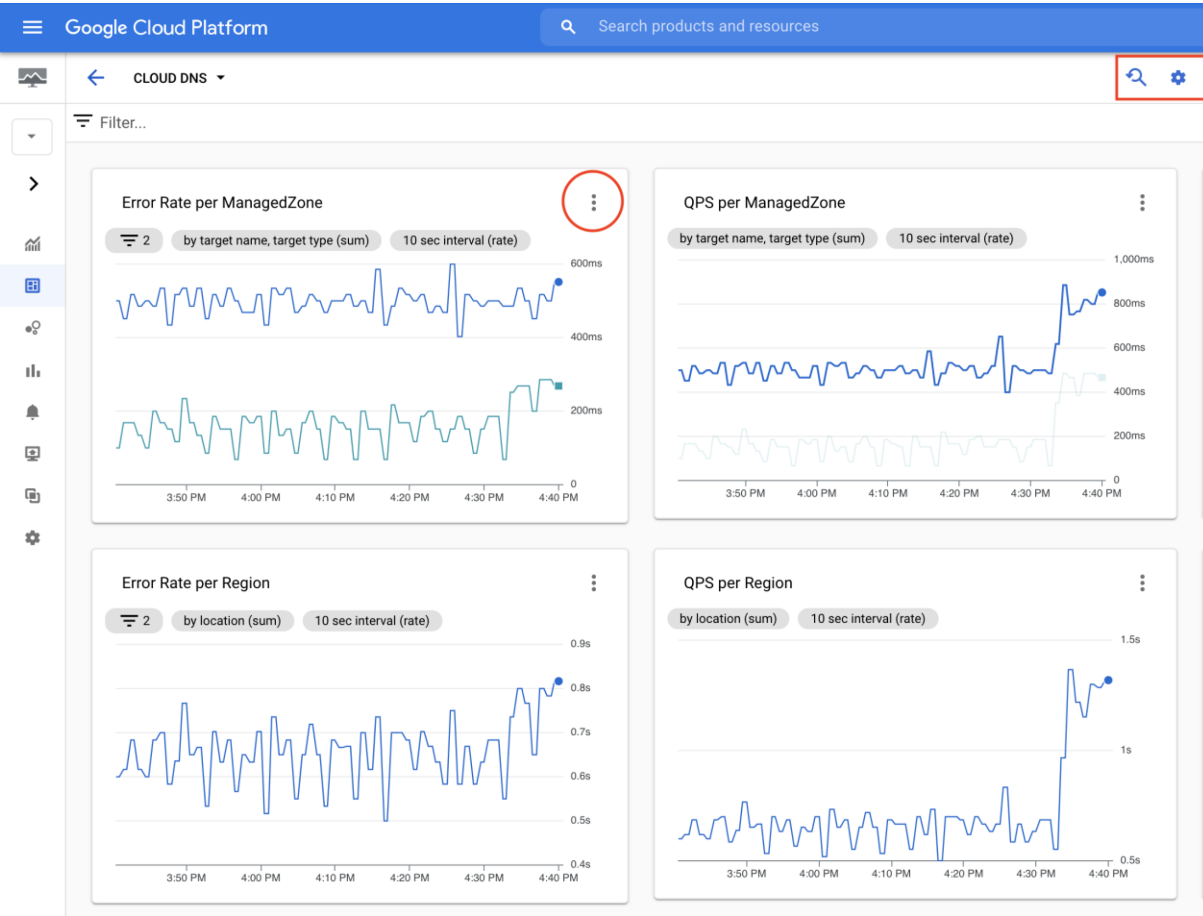
- ✓ compute.instances.get
- ✓ compute.instances.list
- ✓ compute.instances.start
- ✓ compute.instances.stop

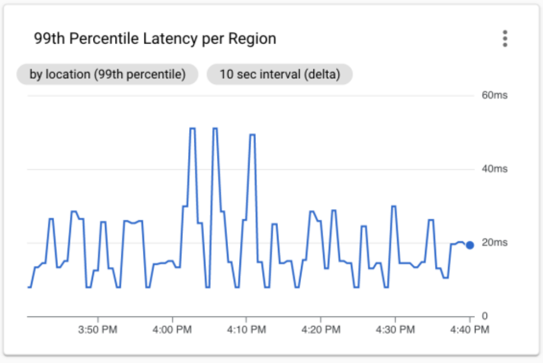
. . .

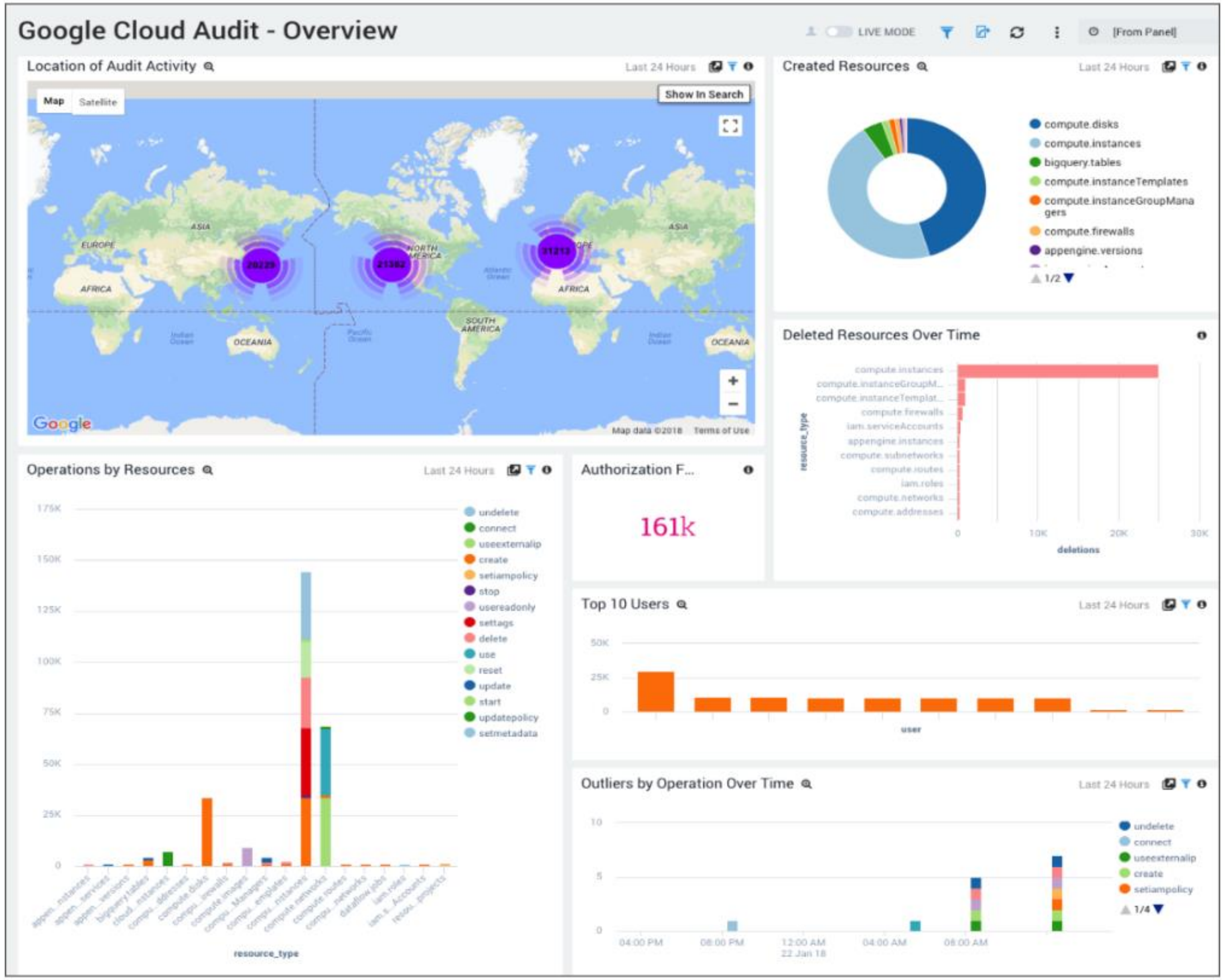
Google Cloud Platform Tutorials

Practice 1 - Monitoring

-







Cloud Accounts

- **Create a Google Account:**

- A Google Account gives you access to many Google products. With a Google Account, you can do things like:

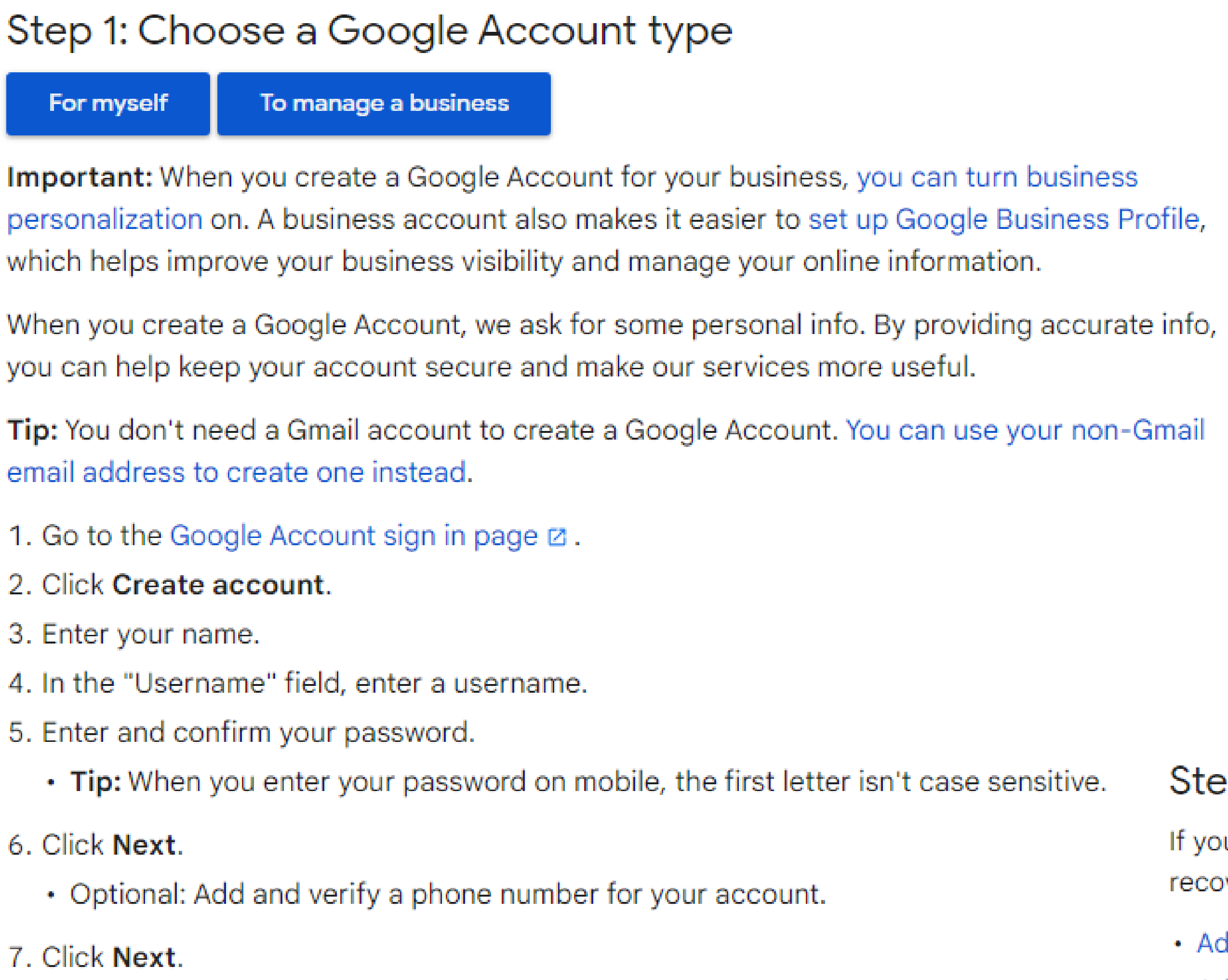
- Send and receive email using Gmail

- Find your new favorite video on YouTube

- Download apps from Google Play

Cloud Accounts

- **Create a Google Account:**



Step 1: Choose a Google Account type

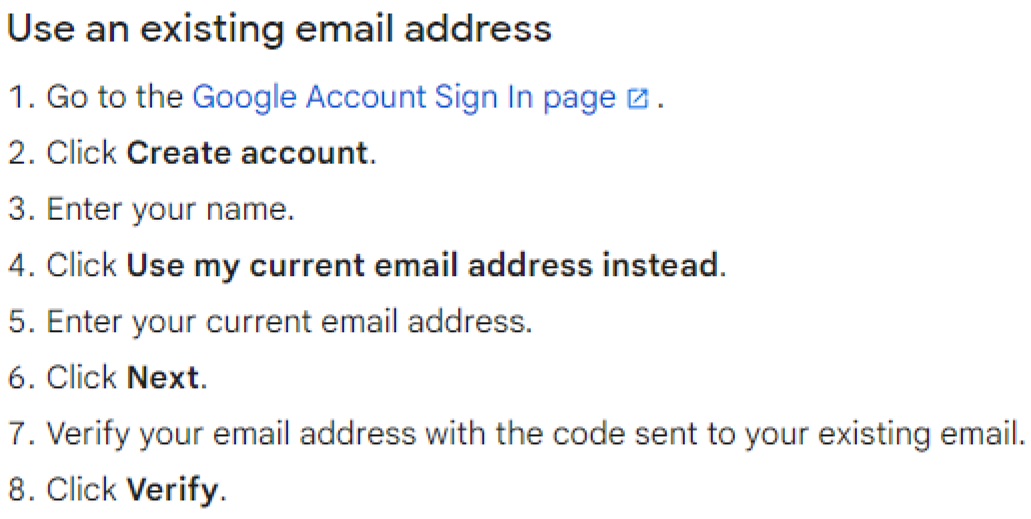
For myself | To manage a business

Important: When you create a Google Account for your business, you can turn business personalization on. A business account also makes it easier to set up Google Business Profile, which helps improve your business visibility and manage your online information.

When you create a Google Account, we ask for some personal info. By providing accurate info, you can help keep your account secure and make our services more useful.

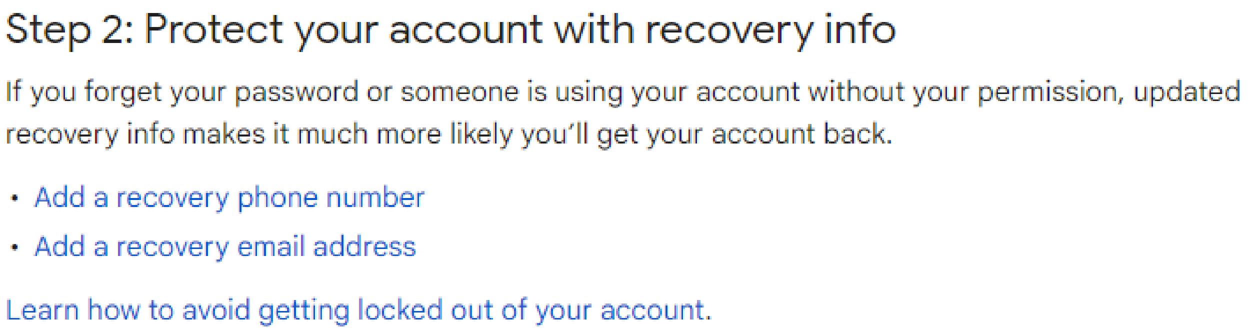
Tip: You don't need a Gmail account to create a Google Account. You can use your non-Gmail email address to create one instead.

1. Go to the Google Account sign in page ⧉ .
2. Click **Create account**.
3. Enter your name.
4. In the "Username" field, enter a username.
5. Enter and confirm your password.
   - **Tip:** When you enter your password on mobile, the first letter isn't case sensitive.
6. Click **Next**.
   - Optional: Add and verify a phone number for your account.
7. Click **Next**.



Use an existing email address

1. Go to the Google Account Sign In page ⧉ .
2. Click **Create account**.
3. Enter your name.
4. Click **Use my current email address instead**.
5. Enter your current email address.
6. Click **Next**.
7. Verify your email address with the code sent to your existing email.
8. Click **Verify**.



Step 2: Protect your account with recovery info

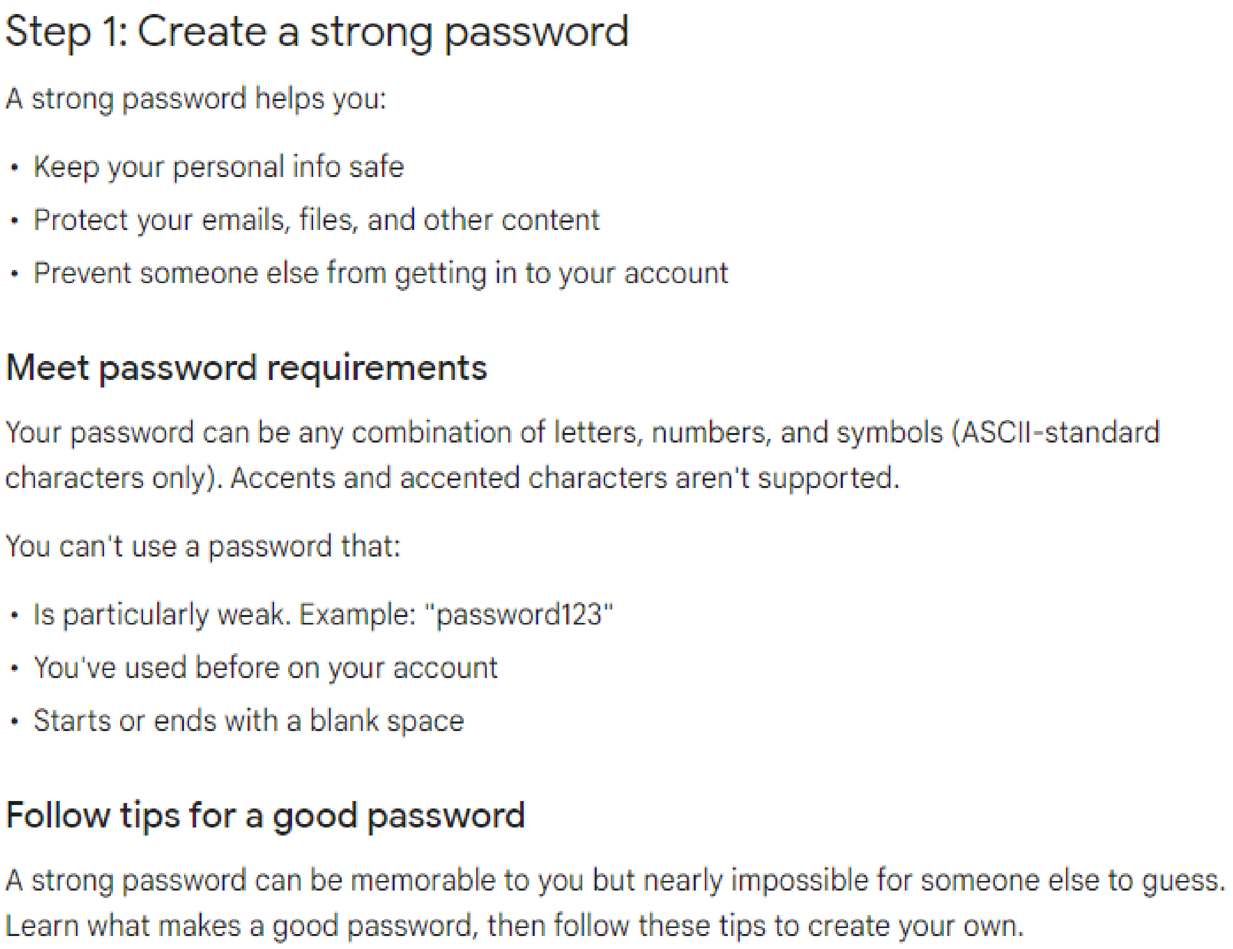
If you forget your password or someone is using your account without your permission, updated recovery info makes it much more likely you'll get your account back.

- Add a recovery phone number
- Add a recovery email address

Learn how to avoid getting locked out of your account.

Cloud Accounts

- **Create a strong password & a more secure account:**



Step 1: Create a strong password

A strong password helps you:

- Keep your personal info safe
- Protect your emails, files, and other content
- Prevent someone else from getting in to your account

Meet password requirements

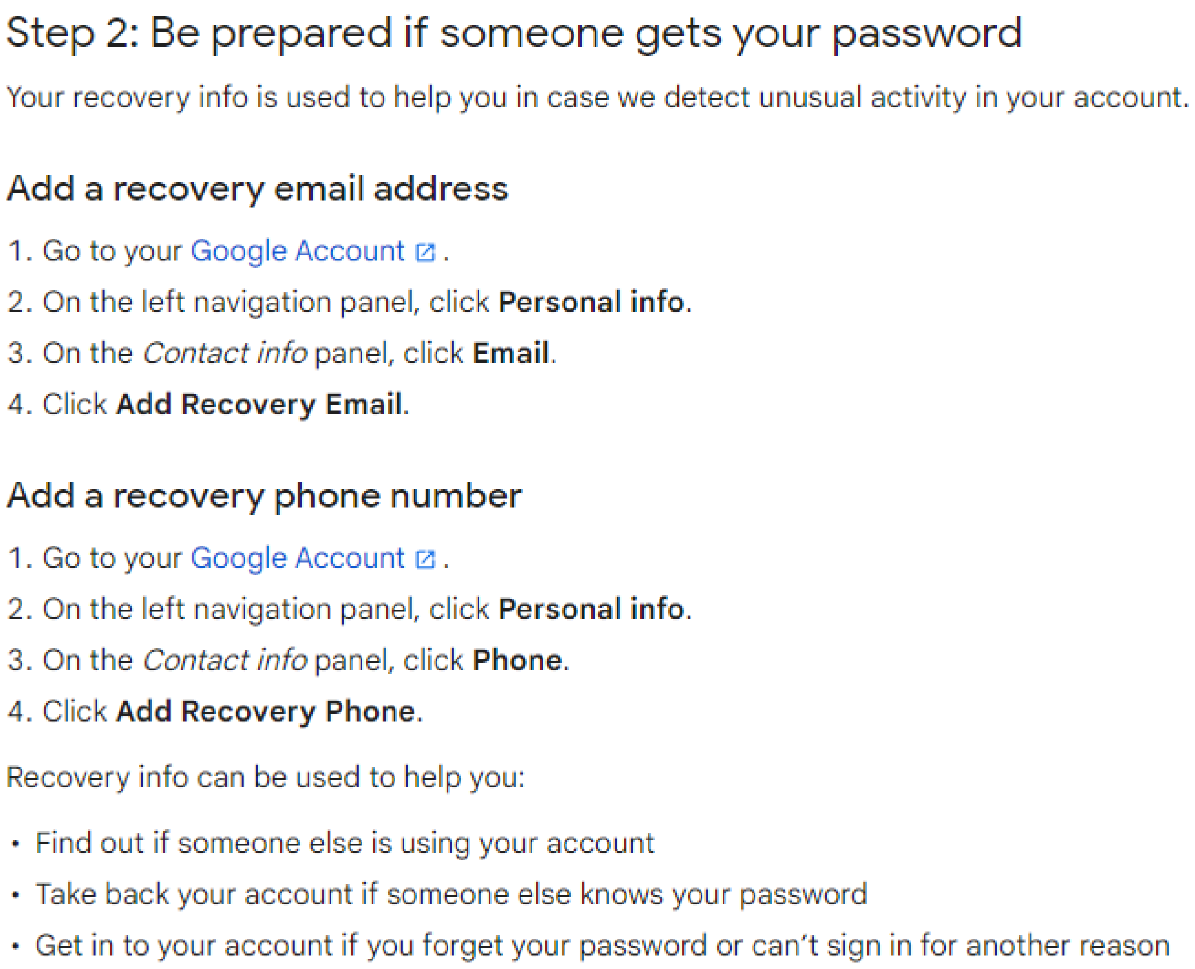
Your password can be any combination of letters, numbers, and symbols (ASCII-standard characters only). Accents and accented characters aren't supported.

You can't use a password that:

- Is particularly weak. Example: "password123"
- You've used before on your account
- Starts or ends with a blank space

Follow tips for a good password

A strong password can be memorable to you but nearly impossible for someone else to guess. Learn what makes a good password, then follow these tips to create your own.



Step 2: Be prepared if someone gets your password

Your recovery info is used to help you in case we detect unusual activity in your account.

Add a recovery email address

1. Go to your Google Account ↗ .
2. On the left navigation panel, click **Personal info**.
3. On the *Contact info* panel, click **Email**.
4. Click **Add Recovery Email**.

Add a recovery phone number

1. Go to your Google Account ↗ .
2. On the left navigation panel, click **Personal info**.
3. On the *Contact info* panel, click **Phone**.
4. Click **Add Recovery Phone**.

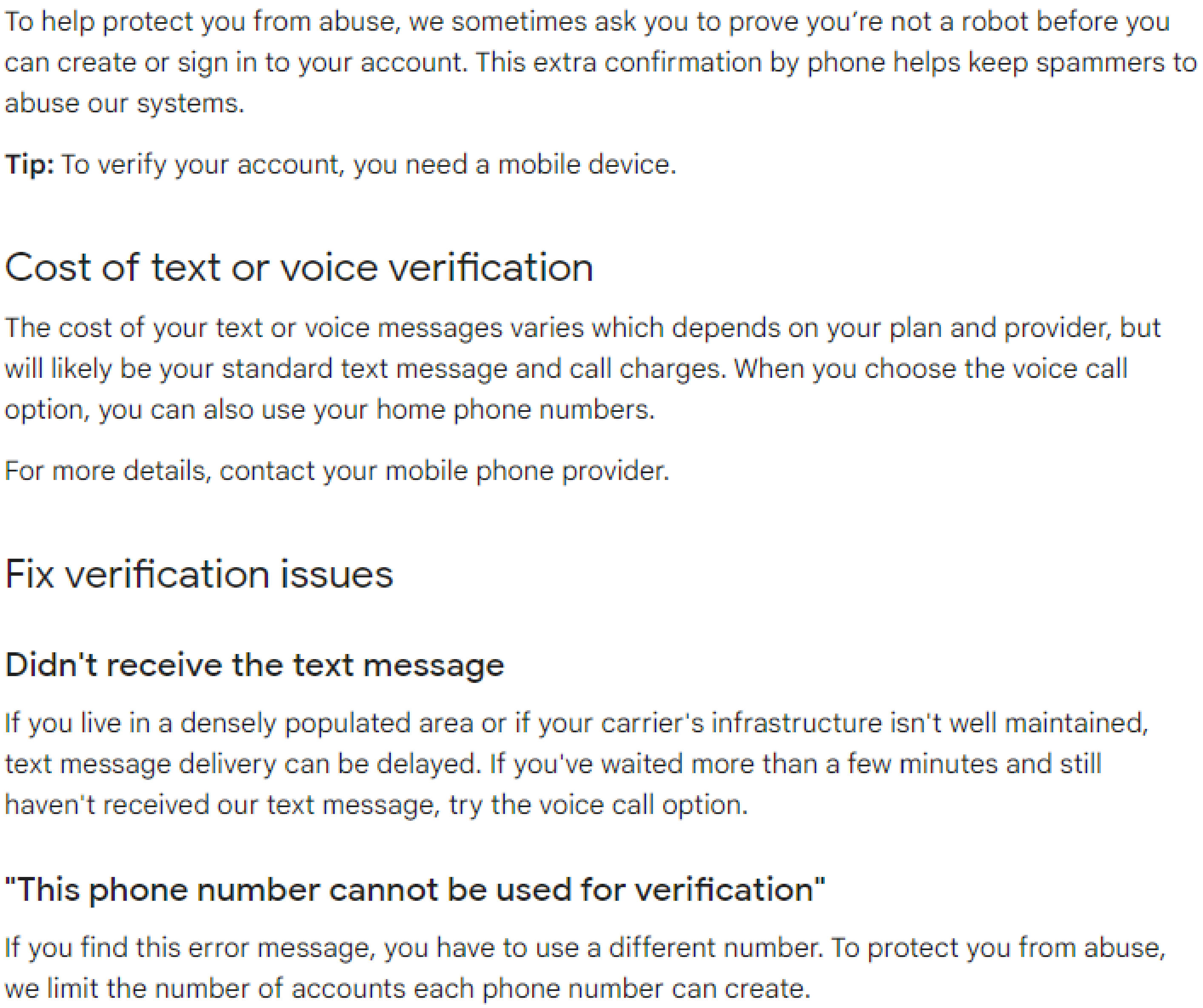
Recovery info can be used to help you:

- Find out if someone else is using your account
- Take back your account if someone else knows your password
- Get in to your account if you forget your password or can't sign in for another reason

Cloud Accounts

- ❑ **Verify your account:**

.



To help protect you from abuse, we sometimes ask you to prove you're not a robot before you can create or sign in to your account. This extra confirmation by phone helps keep spammers to abuse our systems.

Tip: To verify your account, you need a mobile device.

Cost of text or voice verification

The cost of your text or voice messages varies which depends on your plan and provider, but will likely be your standard text message and call charges. When you choose the voice call option, you can also use your home phone numbers.

For more details, contact your mobile phone provider.

Fix verification issues

Didn't receive the text message

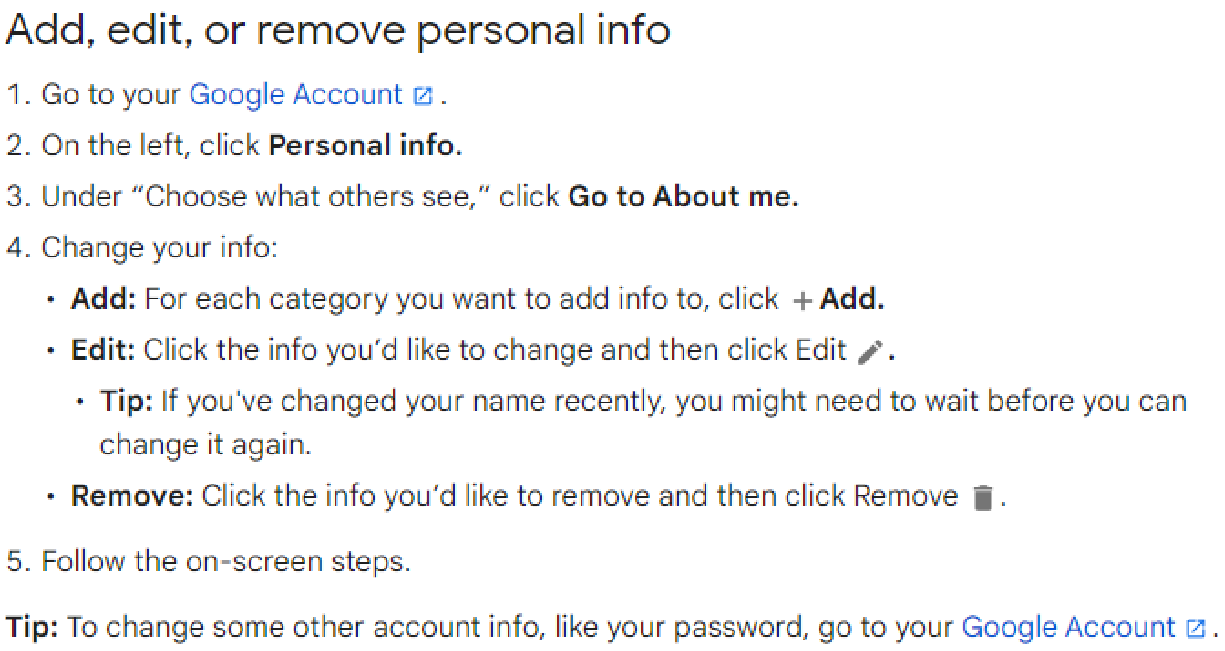
If you live in a densely populated area or if your carrier's infrastructure isn't well maintained, text message delivery can be delayed. If you've waited more than a few minutes and still haven't received our text message, try the voice call option.

"This phone number cannot be used for verification"

If you find this error message, you have to use a different number. To protect you from abuse, we limit the number of accounts each phone number can create.

Cloud Accounts

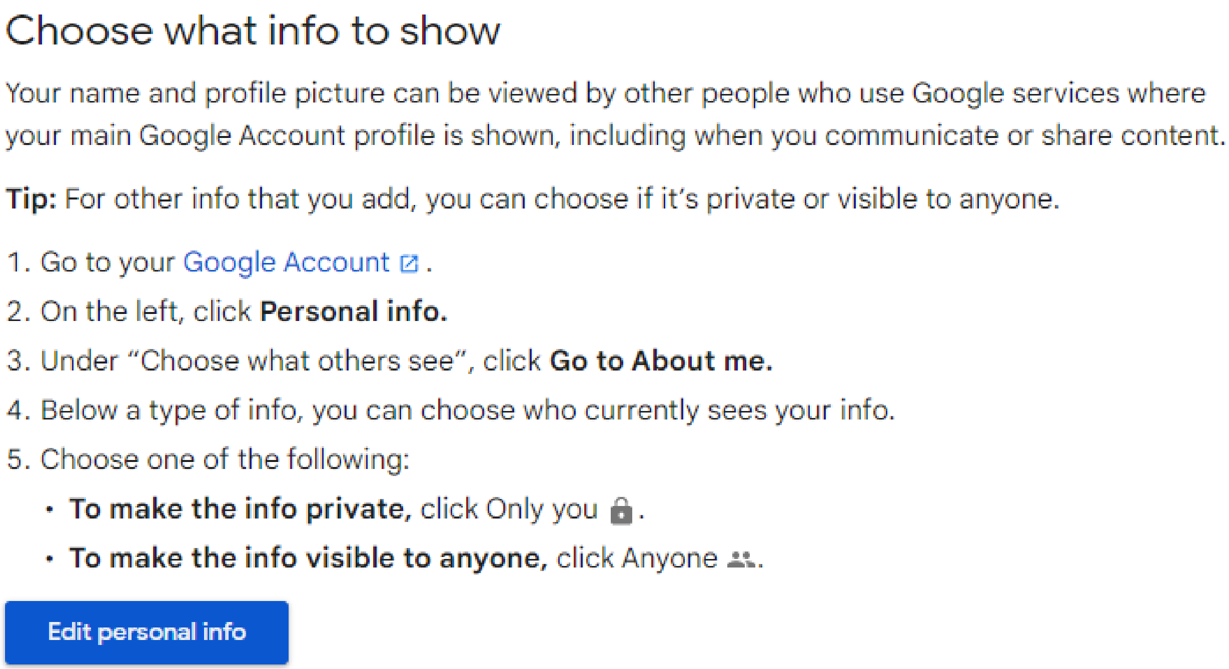
- **Control what others see about you across Google services:**



Add, edit, or remove personal info

1. Go to your Google Account .
2. On the left, click **Personal info.**
3. Under "Choose what others see," click **Go to About me.**
4. Change your info:
   - **Add:** For each category you want to add info to, click + **Add.**
   - **Edit:** Click the info you'd like to change and then click Edit ✎**.**
     - **Tip:** If you've changed your name recently, you might need to wait before you can change it again.
   - **Remove:** Click the info you'd like to remove and then click Remove 🗑 .
5. Follow the on-screen steps.

Tip: To change some other account info, like your password, go to your Google Account .

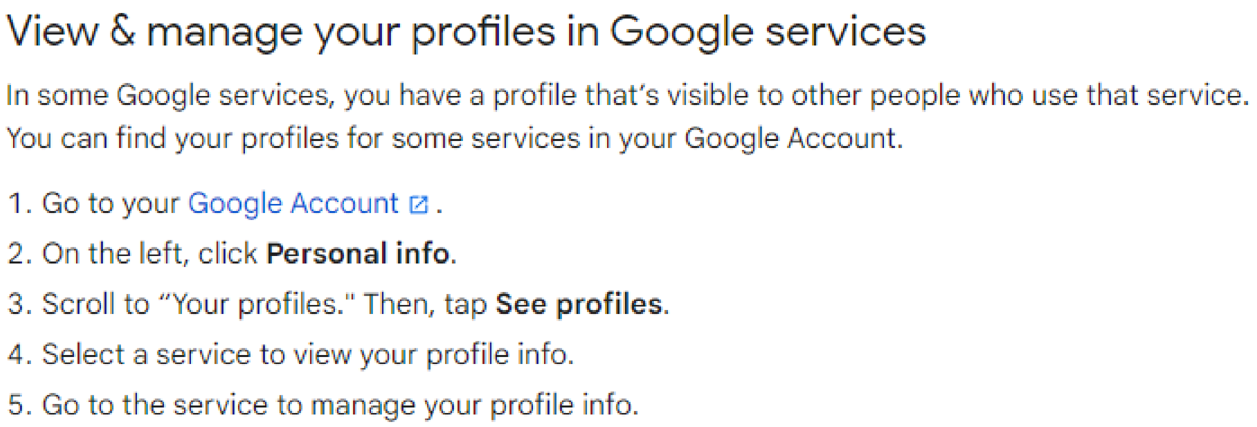


Choose what info to show

Your name and profile picture can be viewed by other people who use Google services where your main Google Account profile is shown, including when you communicate or share content.

Tip: For other info that you add, you can choose if it's private or visible to anyone.

1. Go to your Google Account .
2. On the left, click **Personal info.**
3. Under "Choose what others see", click **Go to About me.**
4. Below a type of info, you can choose who currently sees your info.
5. Choose one of the following:
   - **To make the info private,** click Only you 🔒.
   - **To make the info visible to anyone,** click Anyone 👥.



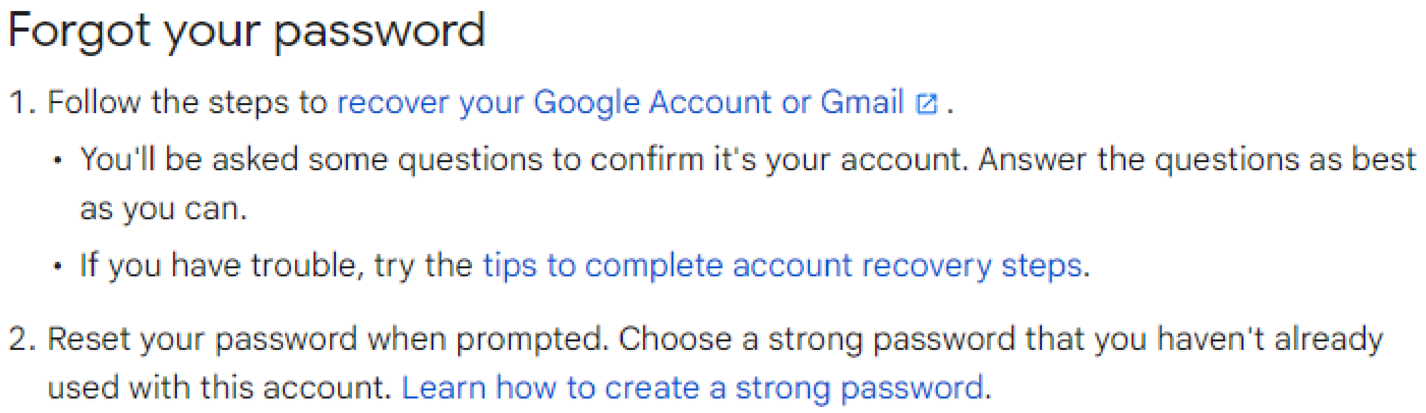
View & manage your profiles in Google services

In some Google services, you have a profile that's visible to other people who use that service. You can find your profiles for some services in your Google Account.

1. Go to your Google Account .
2. On the left, click **Personal info**.
3. Scroll to "Your profiles." Then, tap **See profiles**.
4. Select a service to view your profile info.
5. Go to the service to manage your profile info.

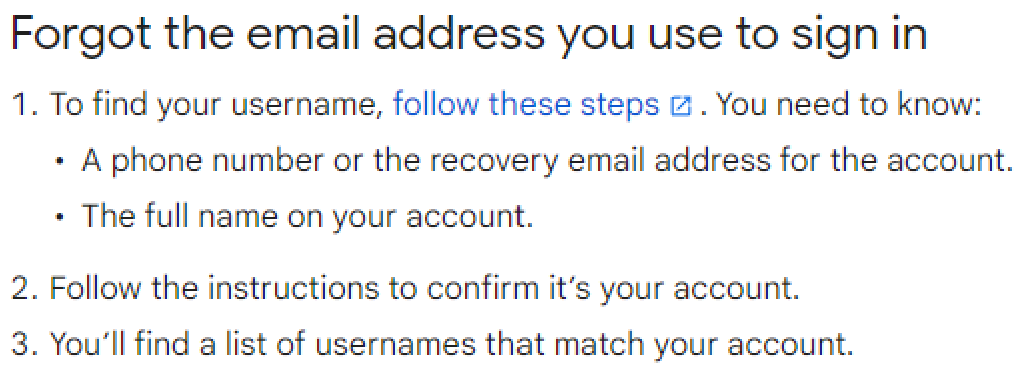
Cloud Accounts

- **How to recover your Google Account or Gmail:**



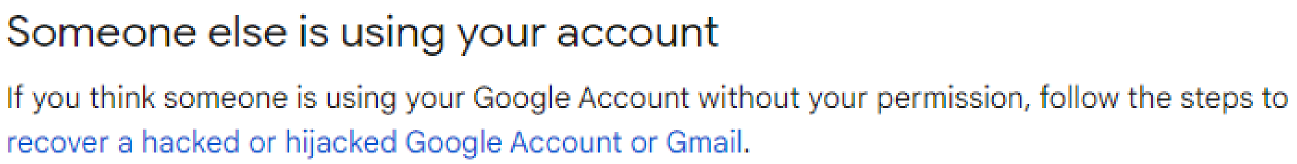
Forgot your password

1. Follow the steps to recover your Google Account or Gmail ⧉ .
   - You'll be asked some questions to confirm it's your account. Answer the questions as best as you can.
   - If you have trouble, try the tips to complete account recovery steps.
2. Reset your password when prompted. Choose a strong password that you haven't already used with this account. Learn how to create a strong password.



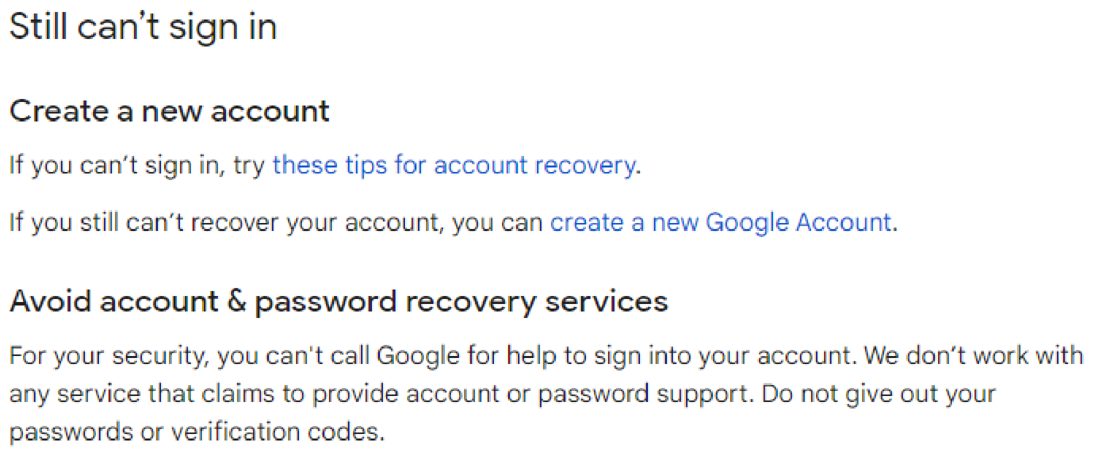
Forgot the email address you use to sign in

1. To find your username, follow these steps ⧉ . You need to know:
   - A phone number or the recovery email address for the account.
   - The full name on your account.
2. Follow the instructions to confirm it's your account.
3. You'll find a list of usernames that match your account.



Someone else is using your account

If you think someone is using your Google Account without your permission, follow the steps to recover a hacked or hijacked Google Account or Gmail.



Still can't sign in

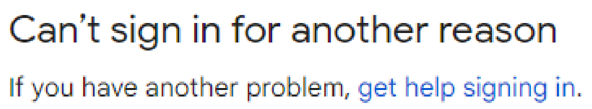
Create a new account

If you can't sign in, try these tips for account recovery.

If you still can't recover your account, you can create a new Google Account.

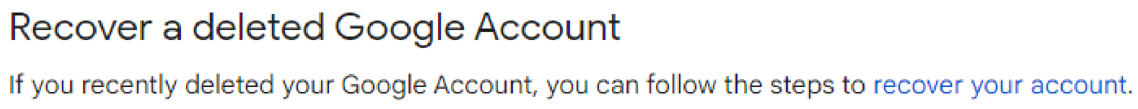
Avoid account & password recovery services

For your security, you can't call Google for help to sign into your account. We don't work with any service that claims to provide account or password support. Do not give out your passwords or verification codes.



Can't sign in for another reason

If you have another problem, get help signing in.

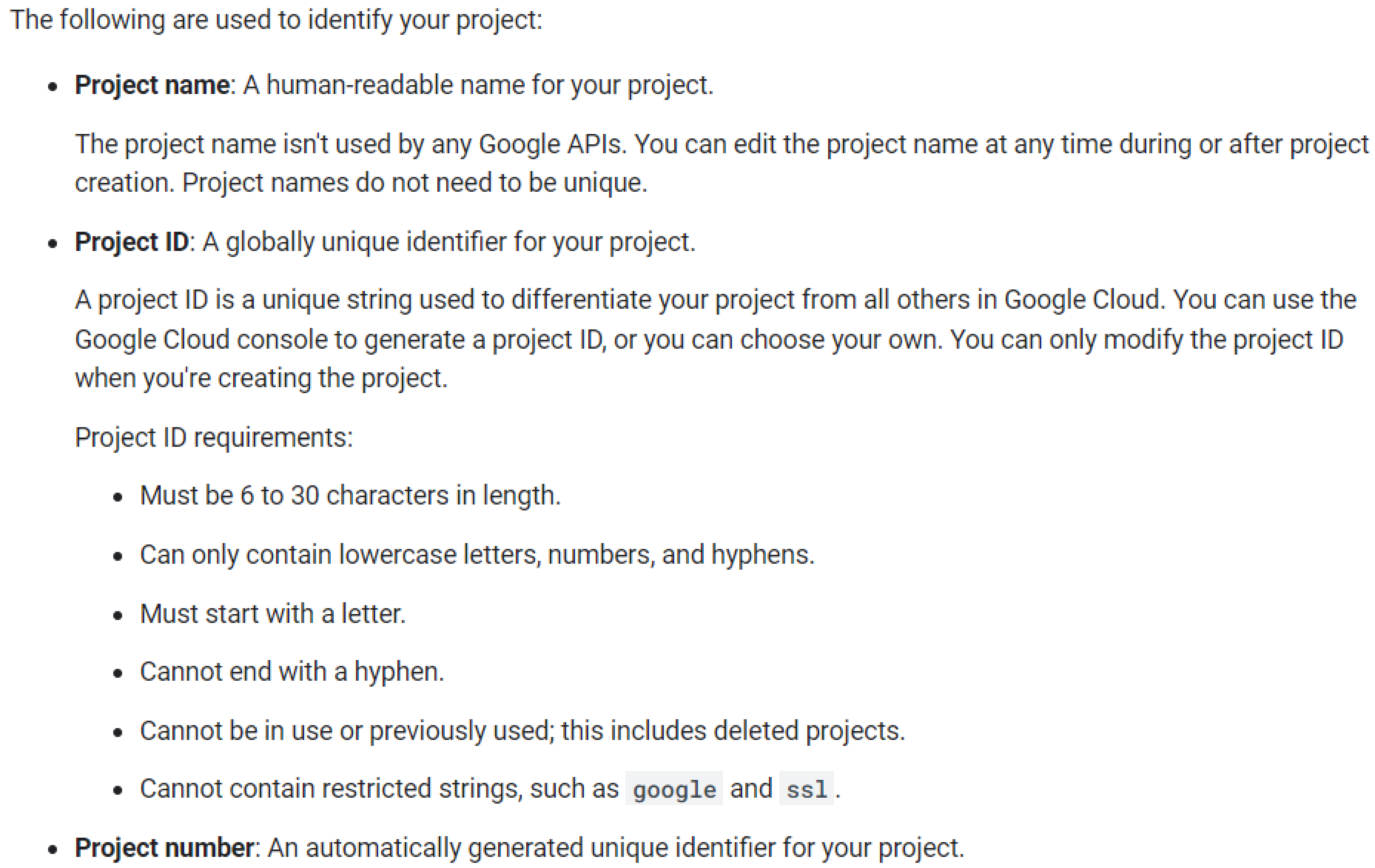


Recover a deleted Google Account

If you recently deleted your Google Account, you can follow the steps to recover your account.

Cloud Projects

- **Before you begin**:



The following are used to identify your project:

- **Project name**: A human-readable name for your project.

  The project name isn't used by any Google APIs. You can edit the project name at any time during or after project creation. Project names do not need to be unique.

- **Project ID**: A globally unique identifier for your project.

  A project ID is a unique string used to differentiate your project from all others in Google Cloud. You can use the Google Cloud console to generate a project ID, or you can choose your own. You can only modify the project ID when you're creating the project.

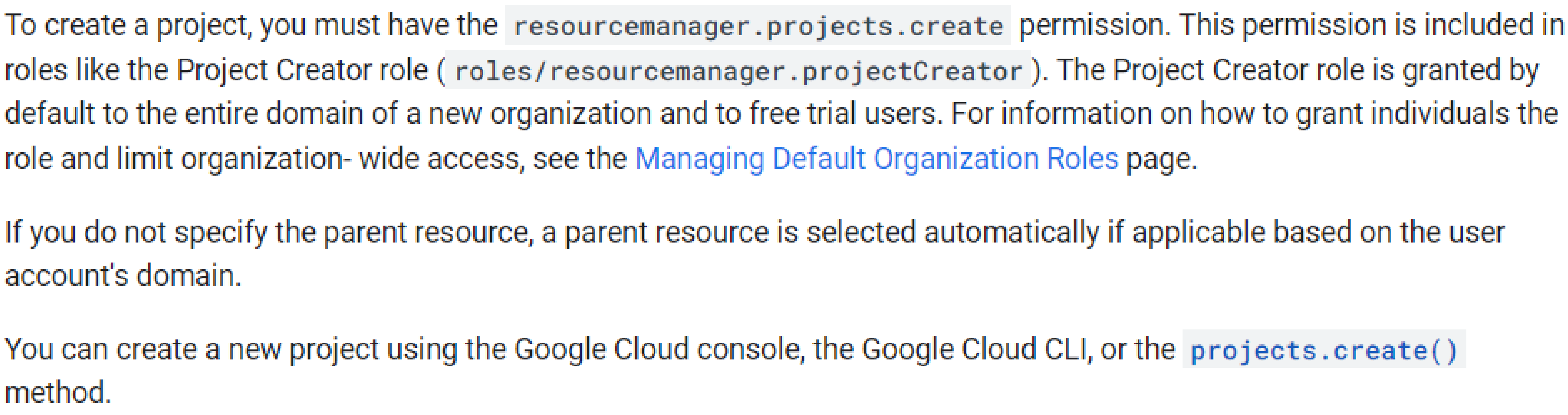
  Project ID requirements:

  - Must be 6 to 30 characters in length.
  - Can only contain lowercase letters, numbers, and hyphens.
  - Must start with a letter.
  - Cannot end with a hyphen.
  - Cannot be in use or previously used; this includes deleted projects.
  - Cannot contain restricted strings, such as `google` and `ssl`.

- **Project number**: An automatically generated unique identifier for your project.

Cloud Projects

- **Creating a project**:



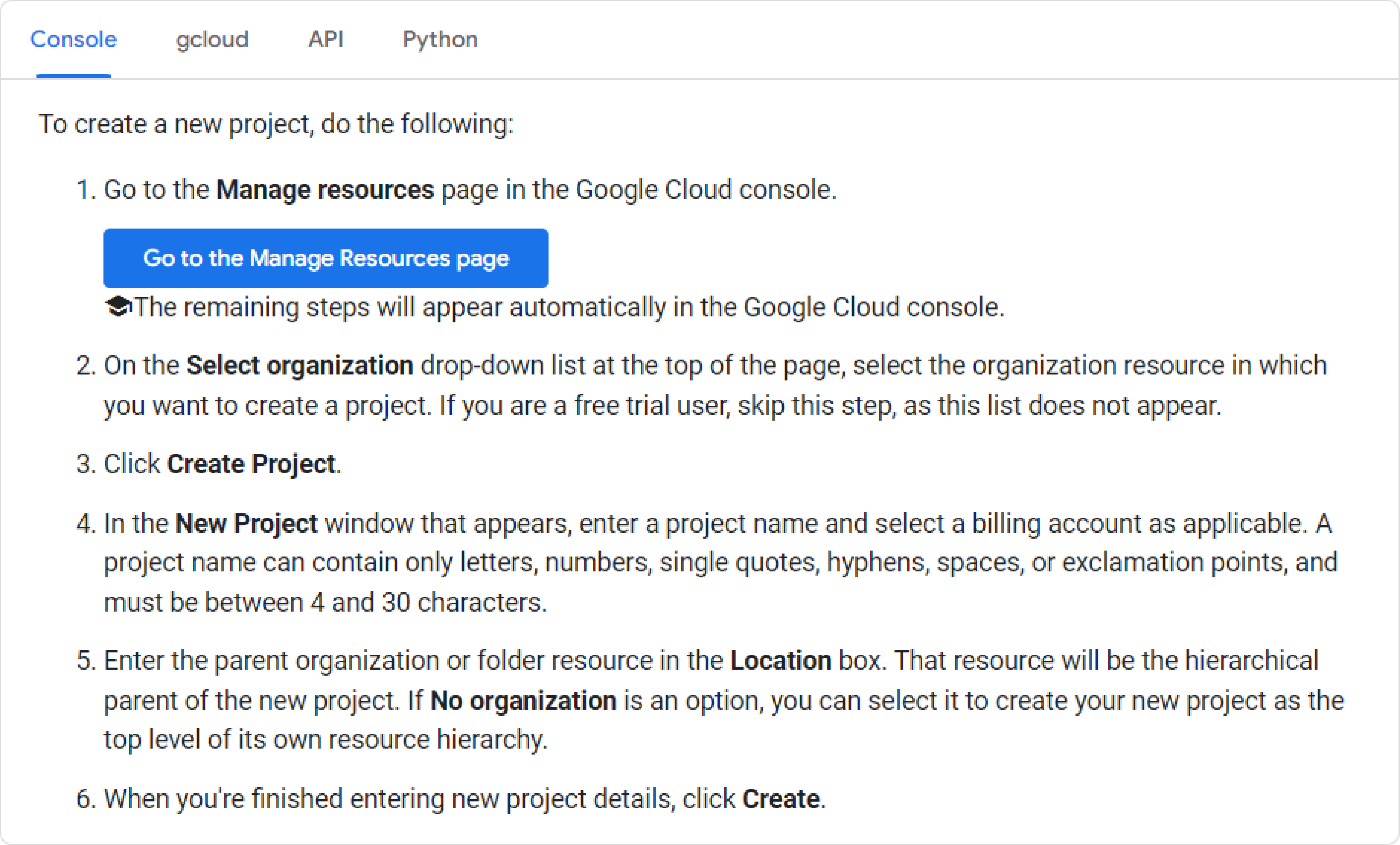
To create a project, you must have the `resourcemanager.projects.create` permission. This permission is included in roles like the Project Creator role (`roles/resourcemanager.projectCreator`). The Project Creator role is granted by default to the entire domain of a new organization and to free trial users. For information on how to grant individuals the role and limit organization- wide access, see the Managing Default Organization Roles page.

If you do not specify the parent resource, a parent resource is selected automatically if applicable based on the user account's domain.

You can create a new project using the Google Cloud console, the Google Cloud CLI, or the `projects.create()` method.

Cloud Projects

- **Creating a project**:



To create a new project, do the following:

1. Go to the **Manage resources** page in the Google Cloud console.

   🎓The remaining steps will appear automatically in the Google Cloud console.

2. On the **Select organization** drop-down list at the top of the page, select the organization resource in which you want to create a project. If you are a free trial user, skip this step, as this list does not appear.

3. Click **Create Project**.

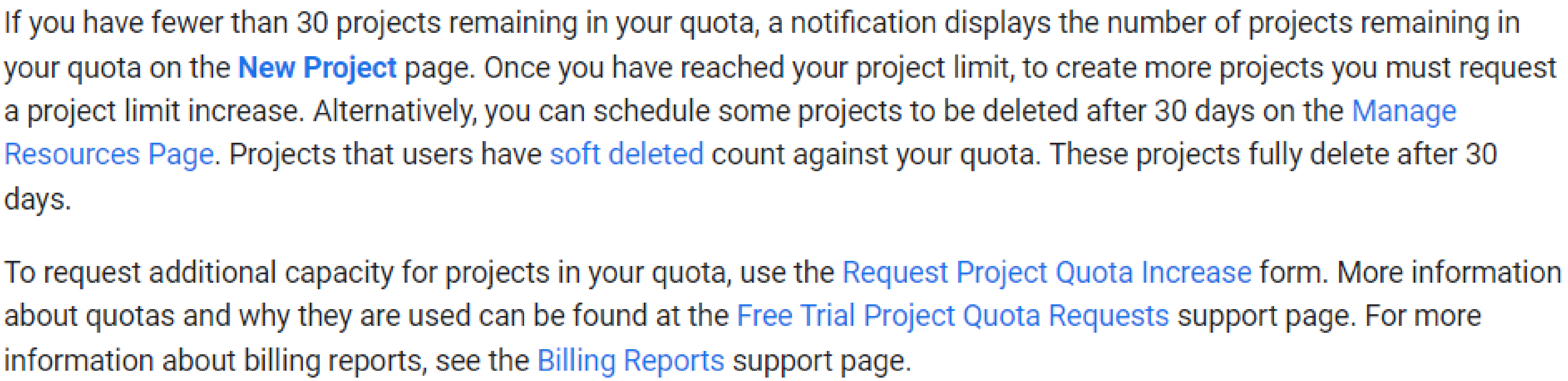
4. In the **New Project** window that appears, enter a project name and select a billing account as applicable. A project name can contain only letters, numbers, single quotes, hyphens, spaces, or exclamation points, and must be between 4 and 30 characters.

5. Enter the parent organization or folder resource in the **Location** box. That resource will be the hierarchical parent of the new project. If **No organization** is an option, you can select it to create your new project as the top level of its own resource hierarchy.

6. When you're finished entering new project details, click **Create**.

Cloud Projects

- **Managing project quotas**:



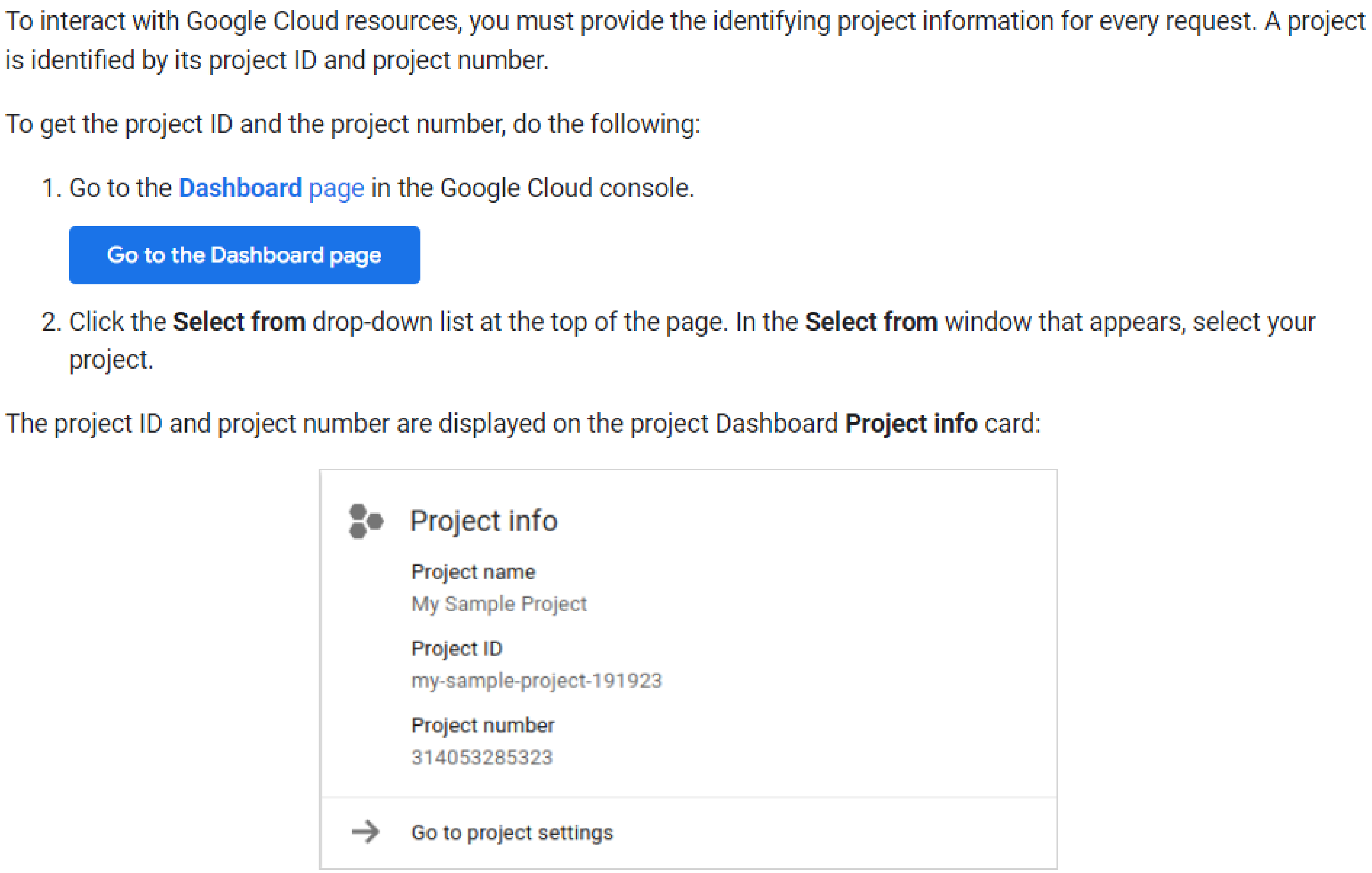
If you have fewer than 30 projects remaining in your quota, a notification displays the number of projects remaining in your quota on the **New Project** page. Once you have reached your project limit, to create more projects you must request a project limit increase. Alternatively, you can schedule some projects to be deleted after 30 days on the Manage Resources Page. Projects that users have soft deleted count against your quota. These projects fully delete after 30 days.

To request additional capacity for projects in your quota, use the Request Project Quota Increase form. More information about quotas and why they are used can be found at the Free Trial Project Quota Requests support page. For more information about billing reports, see the Billing Reports support page.

Cloud Projects

https://cloud.google.com/apigee/docs/hybrid/v1.5/precog-gcpproject

- **Identifying projects**:



To interact with Google Cloud resources, you must provide the identifying project information for every request. A project is identified by its project ID and project number.

To get the project ID and the project number, do the following:

1. Go to the **Dashboard** page in the Google Cloud console.

   Go to the Dashboard page

2. Click the **Select from** drop-down list at the top of the page. In the **Select from** window that appears, select your project.

The project ID and project number are displayed on the project Dashboard **Project info** card:

Project info

Project name
My Sample Project

Project ID
my-sample-project-191923

Project number
314053285323

→ Go to project settings

Cloud Resource Roles

❑ **Access control for projects with IAM:**

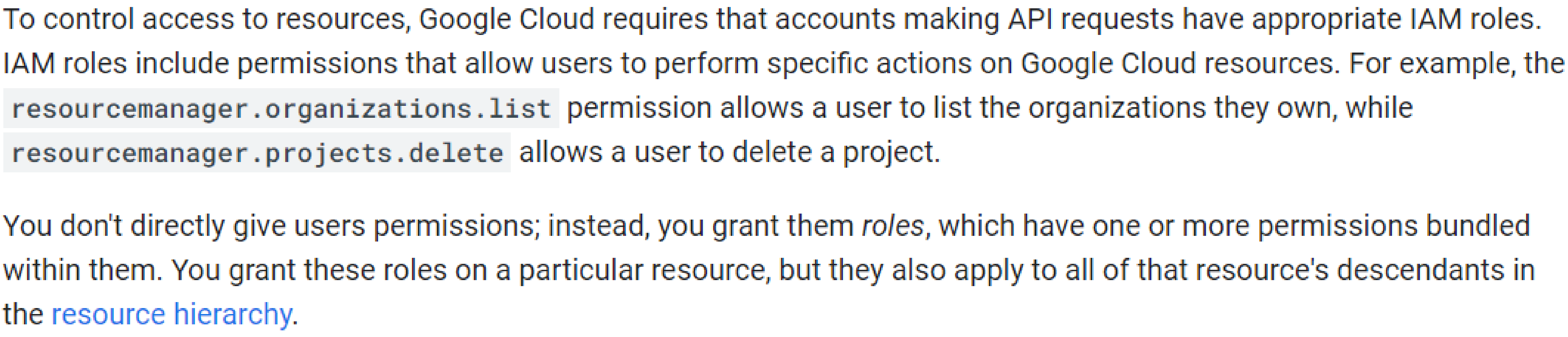
- Google Cloud offers Identity and Access Management (IAM), which lets you give more granular access to specific Google Cloud resources and prevents unwanted access to other resources. IAM lets you adopt the security principle of least privilege, so you grant only the necessary access to your resources.

- IAM lets you control **who (users)** has **what access (roles)** to **which resources** by setting IAM policies, which grant specific roles that contain certain permissions.

- This page explains the IAM permissions and roles that you can use to manage access to projects. For a detailed description of IAM, read the IAM documentation. In particular, see Granting, changing, and revoking access.

Cloud Resource Roles

❑ Permissions and roles:



- To control access to resources, Google Cloud requires that accounts making API requests have appropriate IAM roles. IAM roles include permissions that allow users to perform specific actions on Google Cloud resources. For example, the `resourcemanager.organizations.list` permission allows a user to list the organizations they own, while `resourcemanager.projects.delete` allows a user to delete a project.

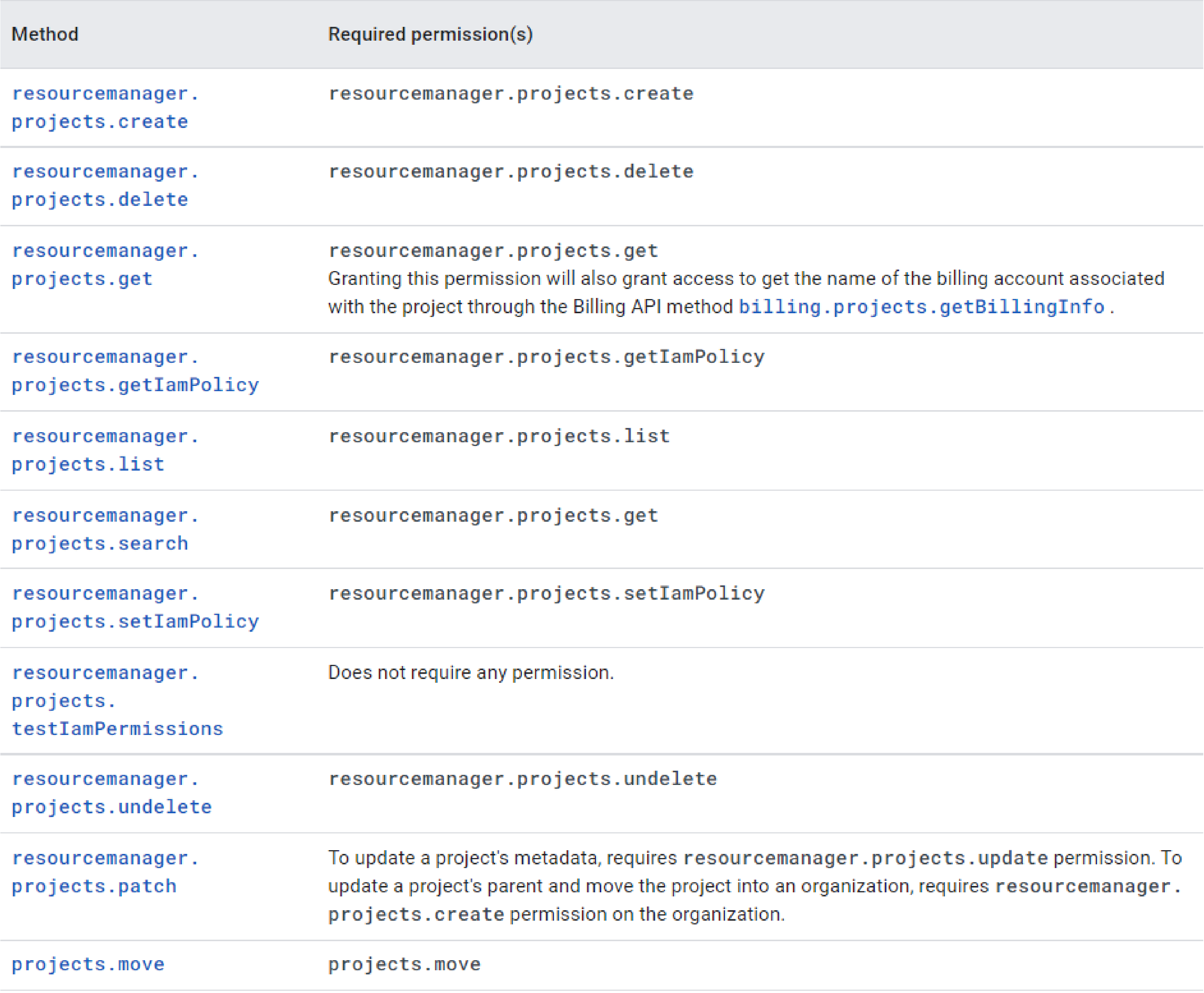
  You don't directly give users permissions; instead, you grant them *roles*, which have one or more permissions bundled within them. You grant these roles on a particular resource, but they also apply to all of that resource's descendants in the resource hierarchy.

Cloud Resource Roles

- **Permissions:**

- To manage projects, the caller must have a role that includes the following permissions.

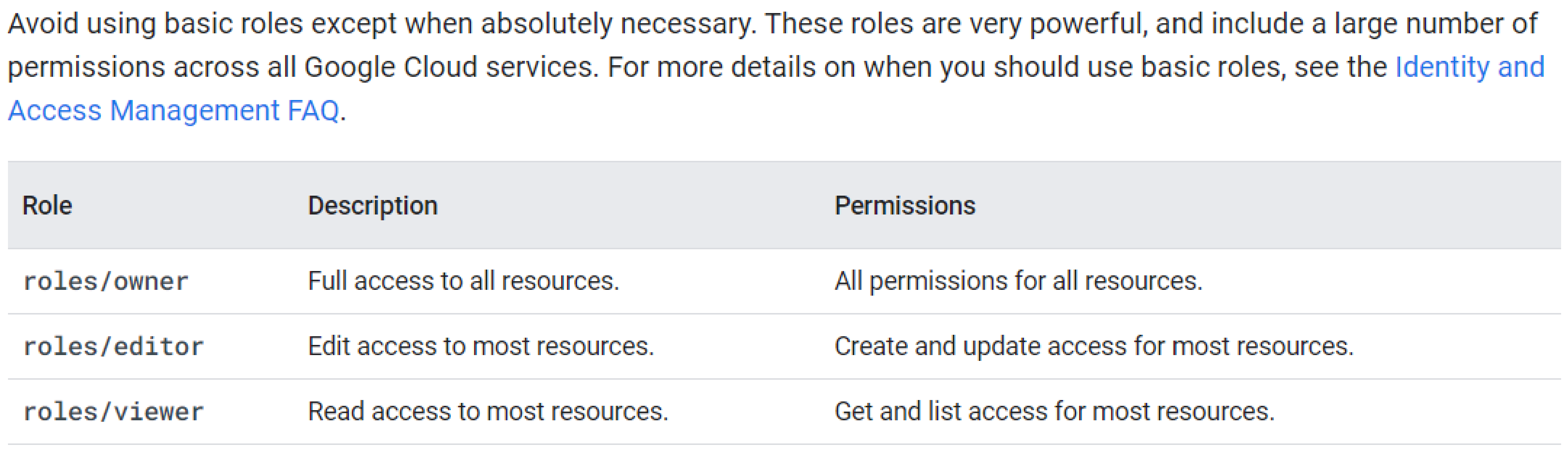
- The role is granted on the organization or folder that contains the projects:



Method	Required permission(s)
`resourcemanager.projects.create`	`resourcemanager.projects.create`
`resourcemanager.projects.delete`	`resourcemanager.projects.delete`
`resourcemanager.projects.get`	`resourcemanager.projects.get` Granting this permission will also grant access to get the name of the billing account associated with the project through the Billing API method `billing.projects.getBillingInfo` .
`resourcemanager.projects.getIamPolicy`	`resourcemanager.projects.getIamPolicy`
`resourcemanager.projects.list`	`resourcemanager.projects.list`
`resourcemanager.projects.search`	`resourcemanager.projects.get`
`resourcemanager.projects.setIamPolicy`	`resourcemanager.projects.setIamPolicy`
`resourcemanager.projects.testIamPermissions`	Does not require any permission.
`resourcemanager.projects.undelete`	`resourcemanager.projects.undelete`
`resourcemanager.projects.patch`	To update a project's metadata, requires `resourcemanager.projects.update` permission. To update a project's parent and move the project into an organization, requires `resourcemanager.projects.create` permission on the organization.
`projects.move`	`projects.move`

Cloud Resource Roles

- **Basic roles and Creating custom roles:**

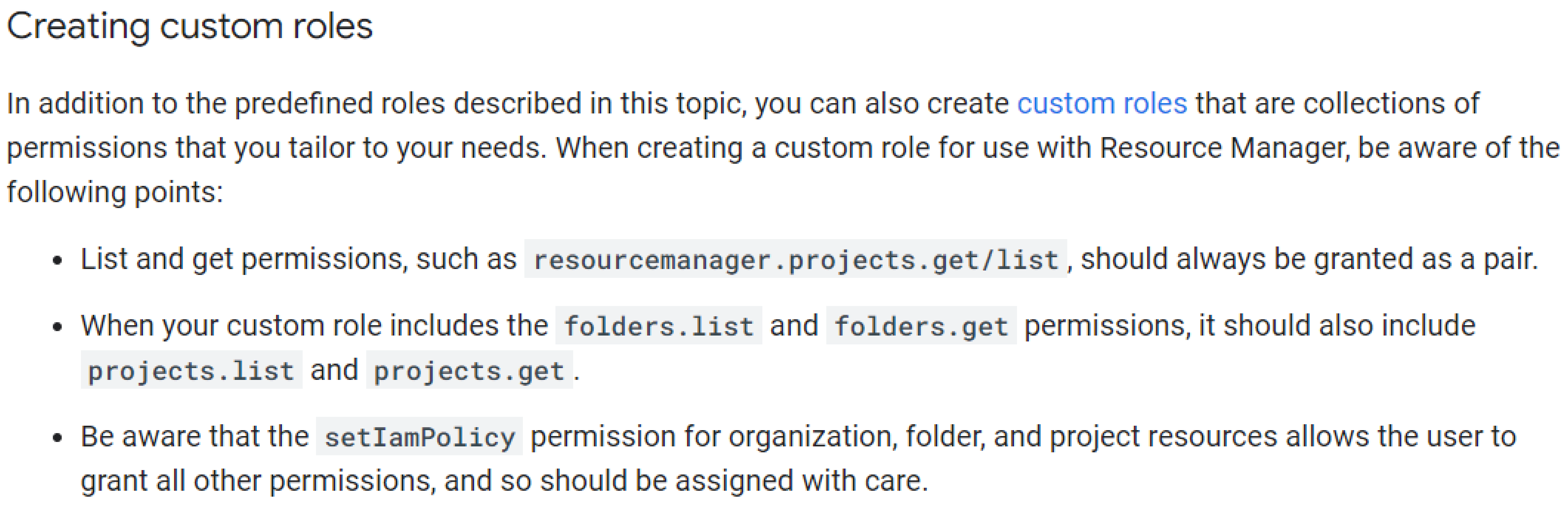


Avoid using basic roles except when absolutely necessary. These roles are very powerful, and include a large number of permissions across all Google Cloud services. For more details on when you should use basic roles, see the Identity and Access Management FAQ.

Role	Description	Permissions
`roles/owner`	Full access to all resources.	All permissions for all resources.
`roles/editor`	Edit access to most resources.	Create and update access for most resources.
`roles/viewer`	Read access to most resources.	Get and list access for most resources.

Cloud Resource Roles

- **Basic roles and Creating custom roles:**



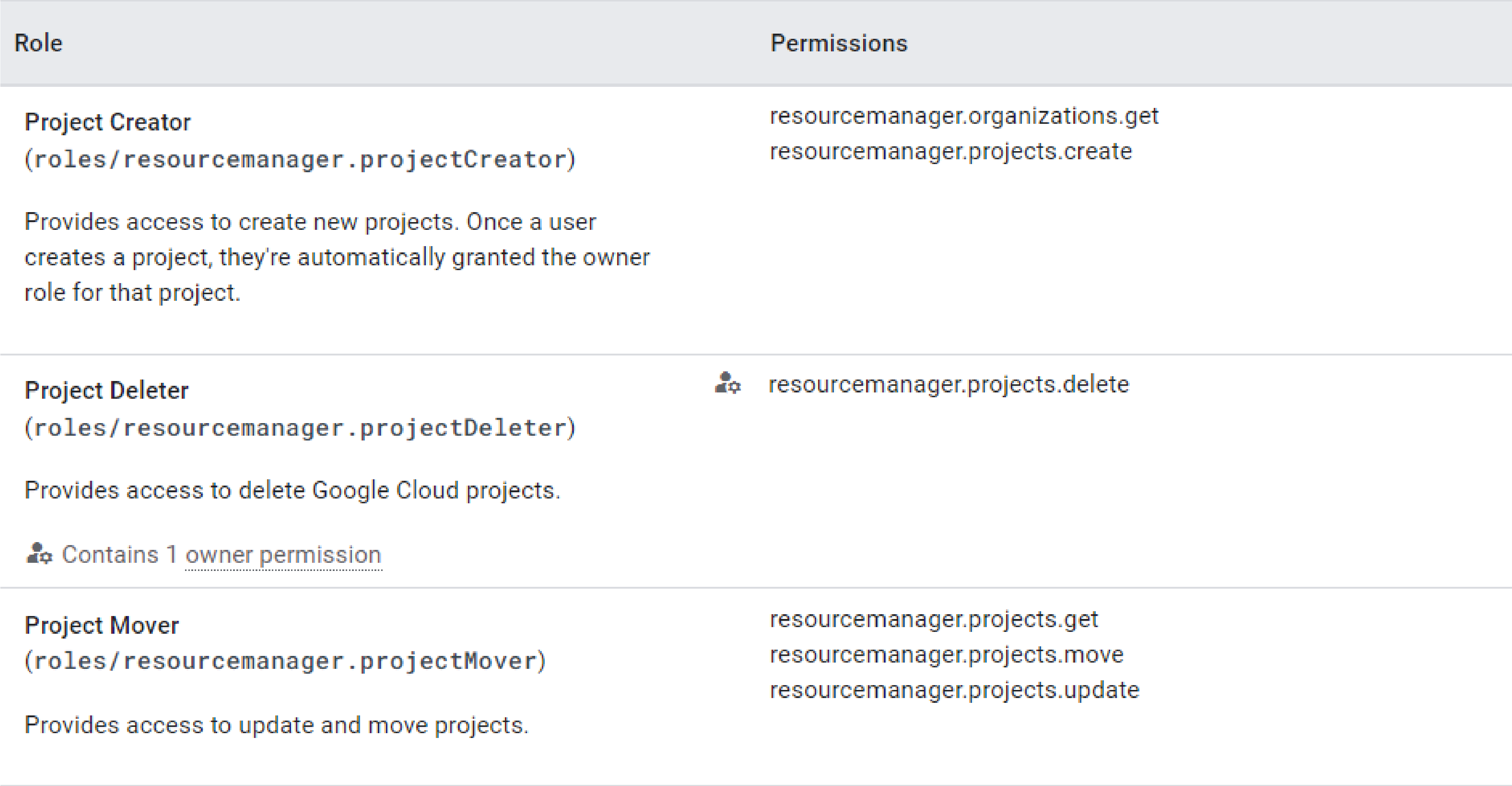
Creating custom roles

In addition to the predefined roles described in this topic, you can also create custom roles that are collections of permissions that you tailor to your needs. When creating a custom role for use with Resource Manager, be aware of the following points:

- List and get permissions, such as `resourcemanager.projects.get/list`, should always be granted as a pair.
- When your custom role includes the `folders.list` and `folders.get` permissions, it should also include `projects.list` and `projects.get`.
- Be aware that the `setIamPolicy` permission for organization, folder, and project resources allows the user to grant all other permissions, and so should be assigned with care.

Cloud Resource Roles

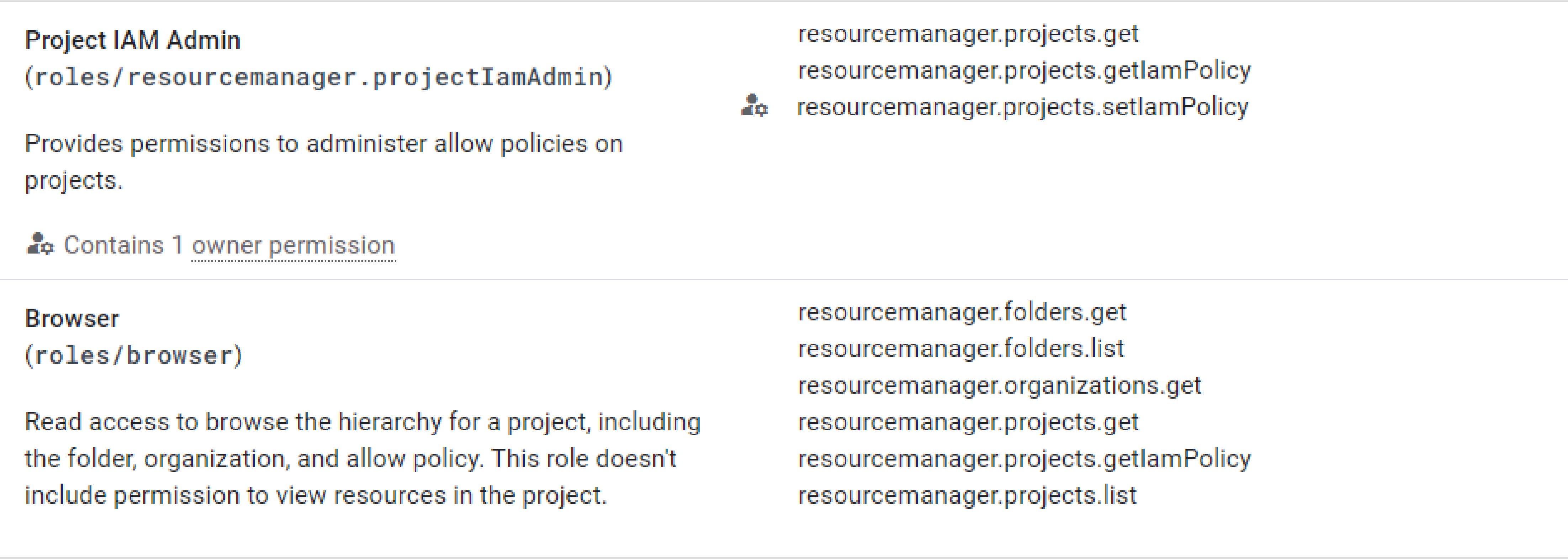
- **Using predefined roles:**



Role	Permissions
Project Creator (`roles/resourcemanager.projectCreator`) Provides access to create new projects. Once a user creates a project, they're automatically granted the owner role for that project.	resourcemanager.organizations.get resourcemanager.projects.create
Project Deleter (`roles/resourcemanager.projectDeleter`) Provides access to delete Google Cloud projects. Contains 1 owner permission	resourcemanager.projects.delete
Project Mover (`roles/resourcemanager.projectMover`) Provides access to update and move projects.	resourcemanager.projects.get resourcemanager.projects.move resourcemanager.projects.update

Cloud Resource Roles

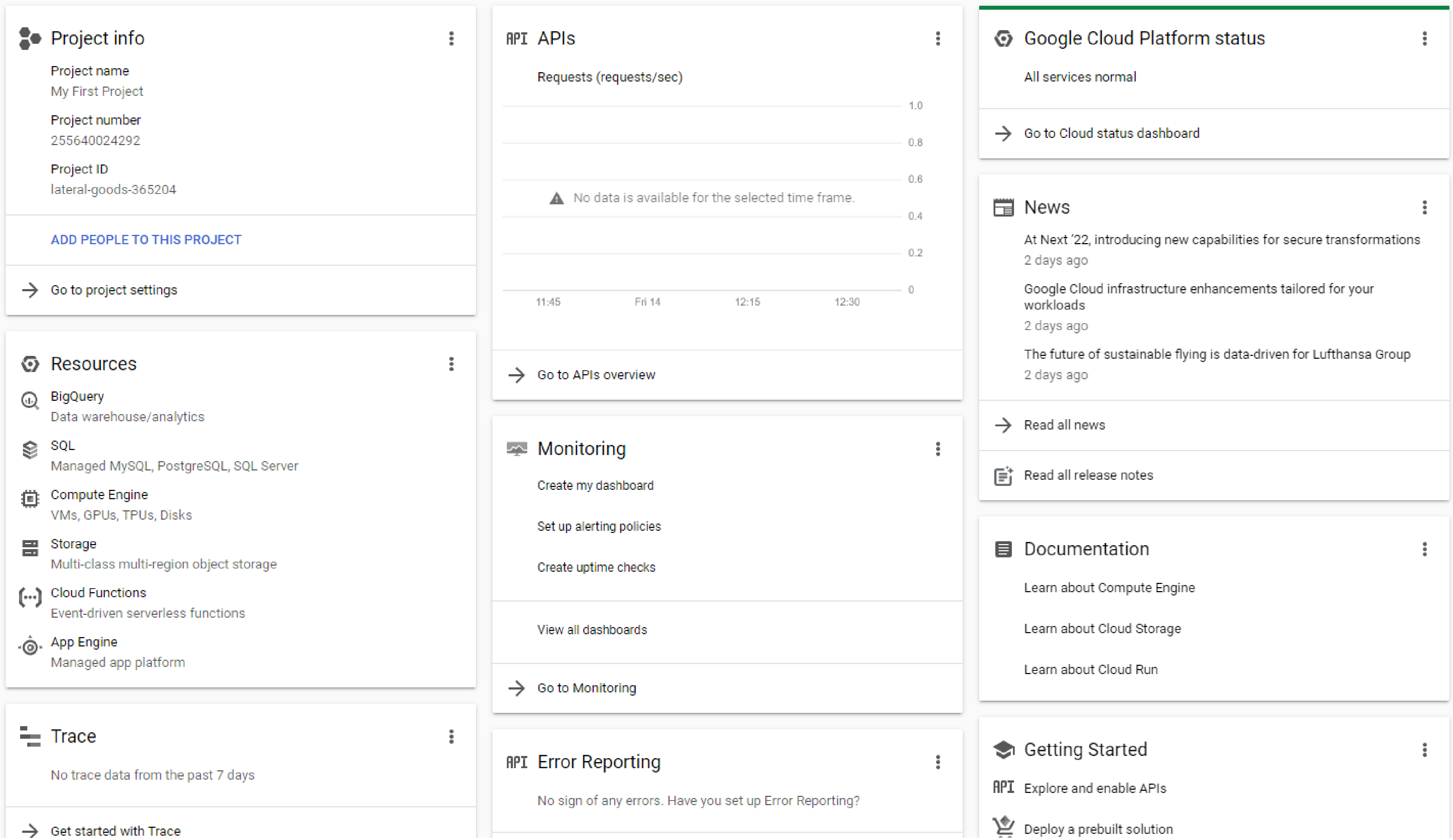
- **Using predefined roles:**



Project IAM Admin (`roles/resourcemanager.projectIamAdmin`) Provides permissions to administer allow policies on projects. Contains 1 owner permission	resourcemanager.projects.get resourcemanager.projects.getIamPolicy resourcemanager.projects.setIamPolicy
Browser (`roles/browser`) Read access to browse the hierarchy for a project, including the folder, organization, and allow policy. This role doesn't include permission to view resources in the project.	resourcemanager.folders.get resourcemanager.folders.list resourcemanager.organizations.get resourcemanager.projects.get resourcemanager.projects.getIamPolicy resourcemanager.projects.list

Cloud Monitoring

- **Cloud Monitoring**:



Project info

Project name
My First Project

Project number
255640024292

Project ID
lateral-goods-365204

ADD PEOPLE TO THIS PROJECT

→ Go to project settings

Resources

BigQuery
Data warehouse/analytics

SQL
Managed MySQL, PostgreSQL, SQL Server

Compute Engine
VMs, GPUs, TPUs, Disks

Storage
Multi-class multi-region object storage

Cloud Functions
Event-driven serverless functions

App Engine
Managed app platform

Trace

No trace data from the past 7 days

→ Get started with Trace

APIs

Requests (requests/sec)

No data is available for the selected time frame.

→ Go to APIs overview

Monitoring

Create my dashboard

Set up alerting policies

Create uptime checks

View all dashboards

→ Go to Monitoring

Error Reporting

No sign of any errors. Have you set up Error Reporting?

Google Cloud Platform status

All services normal

→ Go to Cloud status dashboard

News

At Next '22, introducing new capabilities for secure transformations
2 days ago

Google Cloud infrastructure enhancements tailored for your workloads
2 days ago

The future of sustainable flying is data-driven for Lufthansa Group
2 days ago

→ Read all news

Read all release notes

Documentation

Learn about Compute Engine

Learn about Cloud Storage

Learn about Cloud Run

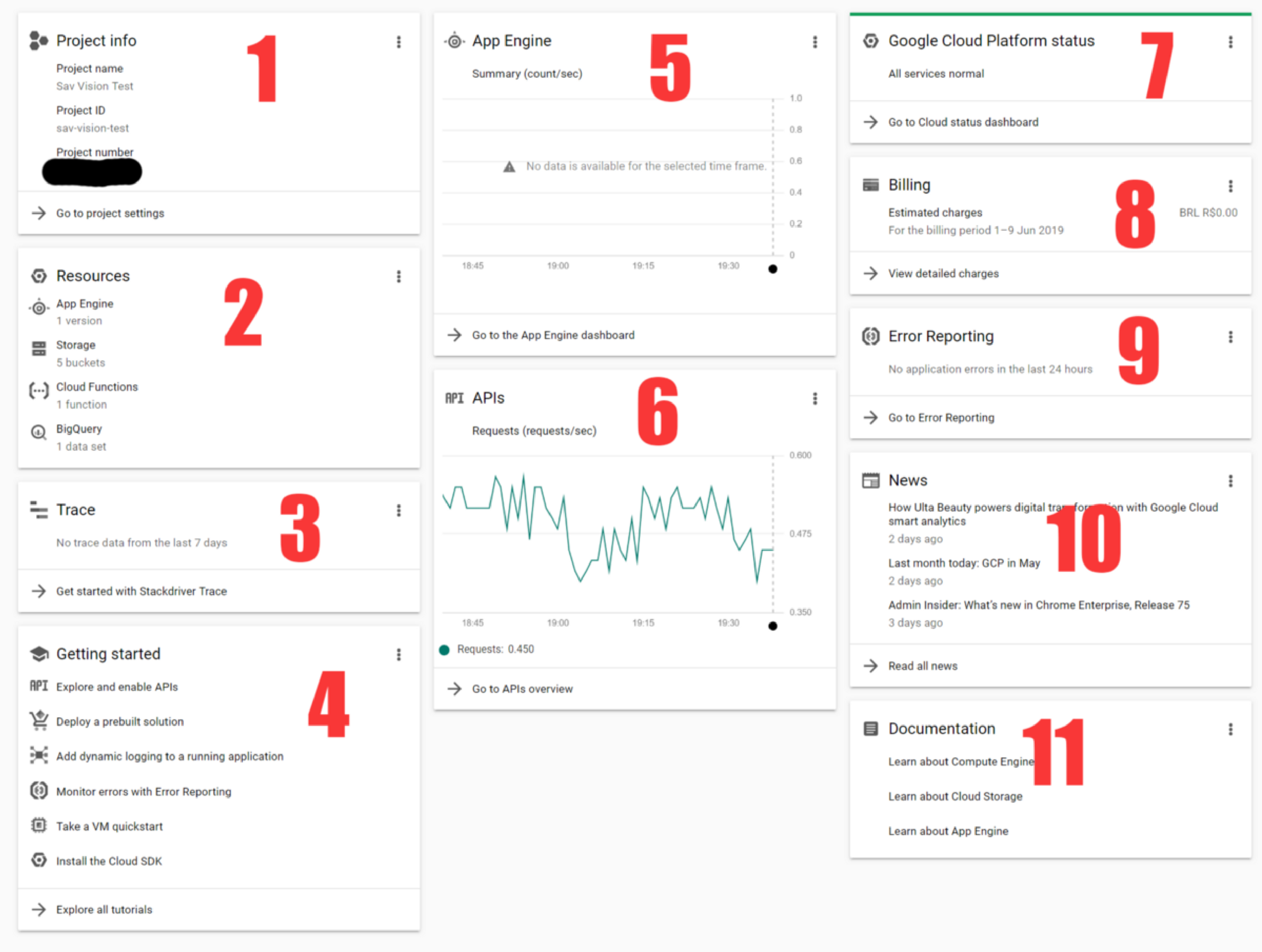
Getting Started

Explore and enable APIs

Deploy a prebuilt solution

Cloud Monitoring

- **Cloud Monitoring**:



Project info

Project name
Sav Vision Test

Project ID
sav-vision-test

Project number
[redacted]

→ Go to project settings

Resources

App Engine
1 version

Storage
5 buckets

Cloud Functions
1 function

BigQuery
1 data set

Trace

No trace data from the last 7 days

→ Get started with Stackdriver Trace

Getting started

Explore and enable APIs

Deploy a prebuilt solution

Add dynamic logging to a running application

Monitor errors with Error Reporting

Take a VM quickstart

Install the Cloud SDK

→ Explore all tutorials

App Engine

Summary (count/sec)

No data is available for the selected time frame.

→ Go to the App Engine dashboard

APIs

Requests (requests/sec)

● Requests: 0.450

→ Go to APIs overview

Google Cloud Platform status

All services normal

→ Go to Cloud status dashboard

Billing

Estimated charges BRL R$0.00
For the billing period 1–9 Jun 2019

→ View detailed charges

Error Reporting

No application errors in the last 24 hours

→ Go to Error Reporting

News

How Ulta Beauty powers digital tra for n with Google Cloud smart analytics
2 days ago

Last month today: GCP in May
2 days ago

Admin Insider: What's new in Chrome Enterprise, Release 75
3 days ago

→ Read all news

Documentation

Learn about Compute Engine

Learn about Cloud Storage

Learn about App Engine

Cloud Monitoring

- **Cloud Monitoring**:

- Cloud Monitoring lets you monitor the performance of your applications and infrastructure, visualize it in dashboards, create uptime checks to detect resources that are down and alert you based on these checks so that you can fix problems in your environment. You can monitor resources in GCP, AWS, and even on-premise.

- It is recommended to create a separate project for Cloud Monitoring since it can keep track of resources across multiple projects.

- Also, it is recommended to install a monitoring agent in your virtual machines to send application metrics (including many third-party applications) to Cloud Monitoring. Otherwise, Cloud Monitoring will only display CPU, disk traffic, network traffic, and uptime metrics.

Cloud Monitoring

❑ **Alerts**:

- To receive alerts, you must declare an **alerting policy**. An alerting policy defines the **conditions** under which a service is considered unhealthy. When the conditions are met, a new incident will be created and notifications will be sent (via email, Slack, SMS, PagerDuty, etc).
- A policy belongs to an individual workspace, which can contain a maximum of 500 policies.

❑ **Trace**

- Trace helps **find bottlenecks in your services**. You can use this service to figure out how long it takes to handle a request, which microservice takes the longest to respond, where to focus to reduce the overall latency, and so on.
- It is enabled by default for applications running on Google App Engine (GAE) - Standard environment - but can be used for applications running on GCE, GKE, and Google App Engine Flexible.

❑ **Error Reporting**

- Error Reporting will aggregate and display errors produced in services written in Go, Java, Node.js, PHP, Python, Ruby, or .NET. running on GCE, GKE, GAP, Cloud Functions, or Cloud Run.

Cloud Monitoring

- **Debug**:

- Debug lets you inspect the application's state without stopping your service. Currently supported for Java, Go, Node.js and Python. It is automatically integrated with GAE but can be used on GCE, GKE, and Cloud Run.

- **Profile**

- Profiler that continuously gathers CPU usage and memory-allocation information from your applications. To use it, you need to install a profiling agent.

Cloud Monitoring - Report

TASK I:

Phân quyền cho ít nhất 2 user (grant access):

- 1st email: quyền viewer
- 2nd email: quyền editor

- Trình tự các bước thực hiện (tính từ giao diện Dashboard …)

- Ảnh chụp minh chứng

Cloud Monitoring - Report

TASK II:

Show bảng “quotas” của [project]:

- Trình tự các bước thực hiện (tính từ giao diện Dashboard …)
- Ảnh chụp minh chứng

Cloud Monitoring - Report

TASK III:

Liệt kê tất cả các roles (grant access) liên quan Data storage:

- Trình tự các bước thực hiện (tính từ giao diện Dashboard …)
- Bảng liệt kê

Cloud Monitoring - Report

TASK IV:

Nêu ý nghĩa thực tiễn của các phần trong Practice 01:

- Cloud Accounts

- Cloud Projects

- Cloud Roles

- Cloud Monitoring