ĐIỆN TOÁN ĐÁM MÂY
(Cloud Computing)

PRACTICES
Practice 3 – Cloud Resources and Management

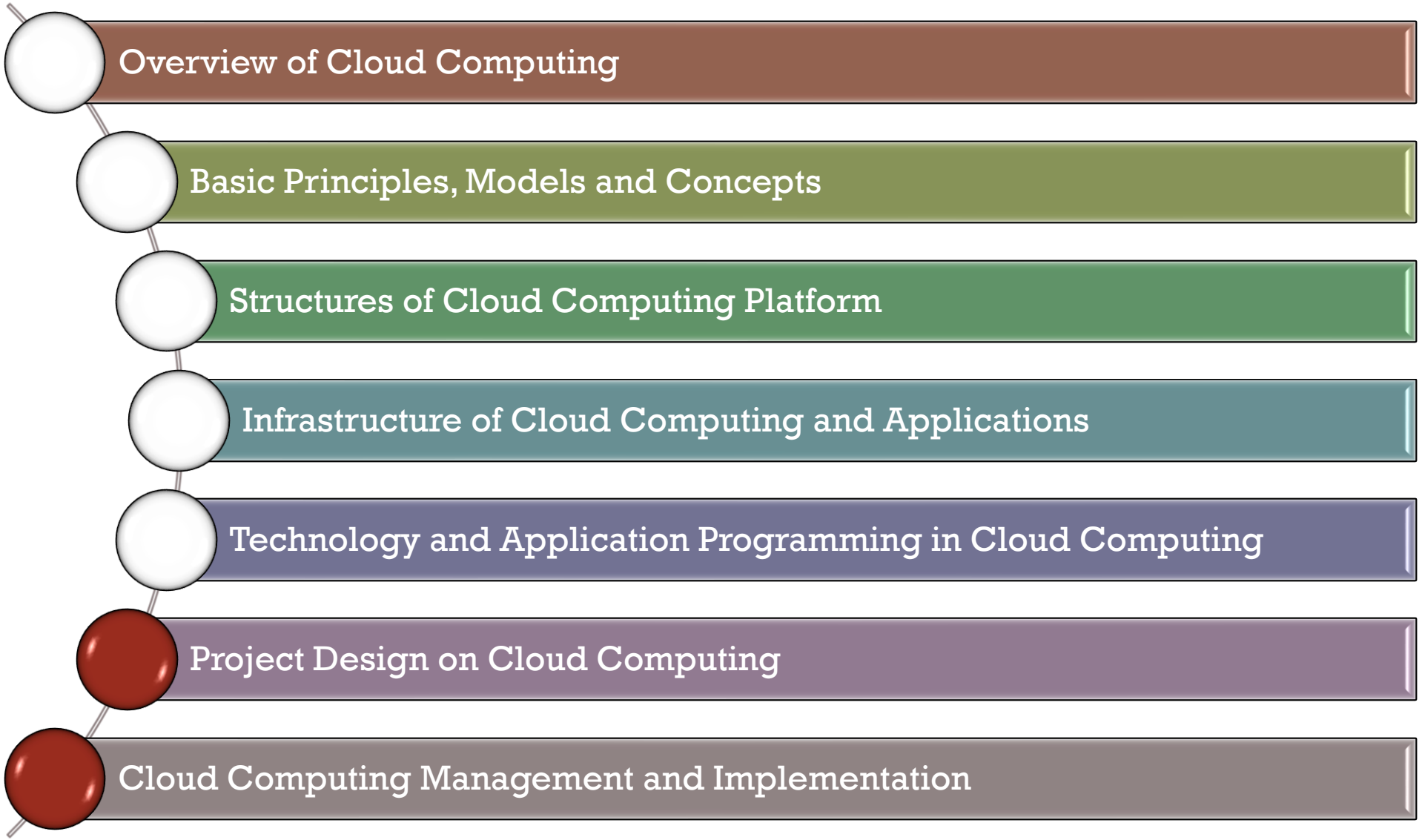
Presenter: **Dr. Nguyen Dinh Long**

Email: dinhlonghcmut@gmail.com

Google-site: https://sites.google.com/view/long-dinh-nguyen

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 Application 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

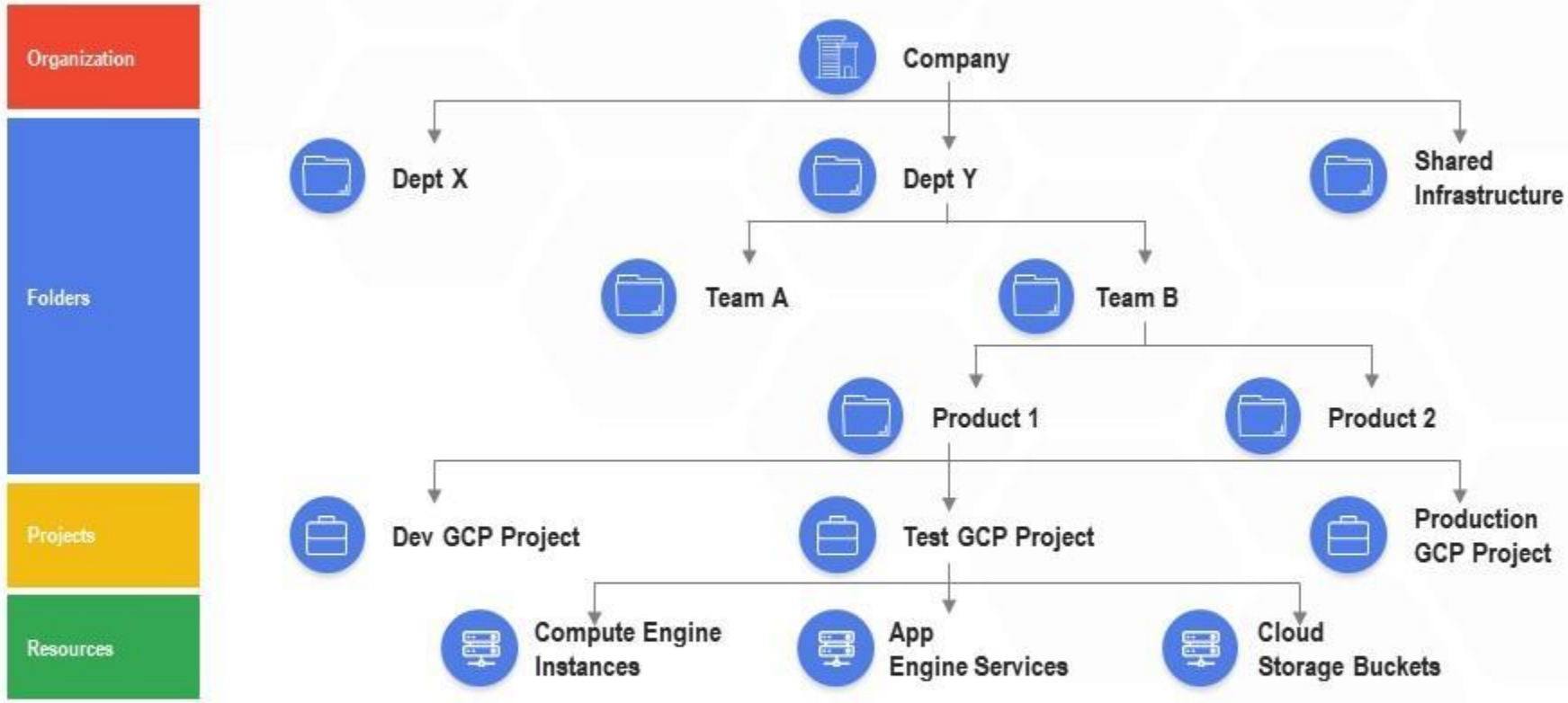
Content of Practice 3

1. Resource settings
2. Resource API
3. Resource logging
4. Resource billing

Cloud Resource

Hierarchy of Google Cloud Resources

This slide represents the hierarchy of the Google Cloud resources, which tells that organization is the parent node, folders, projects are the children of the organization, and the projects are the parent of resources.



Key Takeaways:

- At the lowest level, resources are the principal segments that make up all Google Cloud administrations, e.g., VMs, Pub/Sub topics, storage buckets, and app engine instances
- Every one of these lower-level resources is parented by projects, which address the primary group mechanism of the Google Cloud resource hierarchy
- Add text here

Cloud Resources

- **Manage your Google Cloud resources:**

- This page explains how to view and manage your Google Cloud resources, grant Identity and Access Management (IAM) roles at the organization level, and manage organization resource billing accounts using the Google Cloud console.

View your resources

To view your Google Cloud resources, follow the steps below:

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

   Go to Manage Resources

2. On the dropdown at the top of the page, select the organization resource for which you want to manage resources.

3. All Projects and Folders in the organization resource are listed on the page.

Cloud Resources

- **Manage your Google Cloud resources:**

.

Before you begin

1. You'll need an organization resource to complete these exercises.

   An organization resource is available for Google Workspace and Cloud Identity customers:

   - **Google Workspace:** Sign up for Google Workspace.
   - **Cloud Identity:** Sign up for Cloud Identity.

   Once you have created your Google Workspace or Cloud Identity account and associated it with a domain, your organization resource will be automatically created for you. The resource will be provisioned at different times depending on your account status:

   - If you are new to Google Cloud and have not created a project yet, the organization resource will be created for you when you log in to the Google Cloud console and accept the terms and conditions.
   - If you are an existing Google Cloud user, the organization resource will be created for you when you create a new project or billing account. Any projects you created previously will be listed under "No organization", and this is normal. The organization resource will appear and the new project you created will be linked to it automatically.

     You will need to move any projects you created under "No organization" into your new organization resource. For instructions on how to move your projects, see Migrating projects into an organization resource.

Cloud Resources

- **Manage your Google Cloud resources:**
  - This page explains how to view and manage your Google Cloud resources, grant IAM roles.

Create a Folder resource

Once you have an organization resource, you can create Folder resources and begin to organize your resource hierarchy.
To create a Folder in your organization resource, follow the steps below:

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

   Go to Manage Resources

2. On the dropdown at the top of the page, select the organization resource for which you want to create a Folder resource.
3. Click **Create Folder**.
4. In the **Create Folder** window that appears, enter a Folder name.
5. If you want to create the Folder resource inside a Folder that already exists, enter the parent Folder name in the **Destination** box.
6. When you're finished entering new Folder details, click **Create**.

Cloud Resources

- **Manage your Google Cloud resources:**
  - This page explains how to view and manage your Google Cloud resources, grant IAM roles.

Create a Project resource

To create a Project resource, follow the steps below:

To create a new project, do the following:

1. Go to the **Manage resources** page 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**.

Once you have created your first Project, your organization resource will be provisioned automatically.

Cloud Resources

- **Google Cloud resources:**

Grant IAM roles at the organization level

To grant organization-level roles, follow the steps below:

1. Go to the Google Cloud console IAM & admin page:

   Go to IAM & Admin

2. Click **Select**, then use the drop-down to select the organization resource for which you want to manage IAM permissions.

   a. In the list of resources that appears, click the name of the organization resource.

   b. The **IAM** page that appears shows the following details:

   - The **Principals** column shows the accounts that have roles in the organization resource, including your account and domain.
   - The **Role(s)** column shows the roles that each principal has.
     - Next to your account, you should see **Organization Administrator** under **Role(s)**.
     - Next to the domain account, you should see **Project Creator** under **Roles(s)**.
     - If you see **Multiple** under **Role(s)**, the account has more than one role. Click the drop-down to see what roles a principal has.

c. To grant roles to an existing principal, click the drop-down under **Role(s)** and then select each role you want the principal to have.

   i. When you're finished selecting roles, click **Save**.

d. To add a new principal, click **Add** at the top of the page. In the **Add principals** dialog that appears:

   i. Enter an email address in the **Principals** box.

   ii. Under **Roles**, select each role you want the principal to have.

   iii. When you're finished selecting roles, click **Add**.

The principals you added now have the organization-level permissions you selected.

Cloud Resources

- **Manage your Google Cloud resources:**
  - This page explains how to view and manage your Google Cloud resources, grant IAM roles.

Create a billing account

1. Go to the Google Cloud console Billing page:

   GO TO THE BILLING PAGE

2. In the drop-down at the top of the page, select the organization resource for which you want to add a billing account.
3. Click **Create account**.
4. On the **Create a new billing account** window that appears, enter the appropriate details, including a billing account name and your billing information.
   - The options you see depend on the country of your billing address.
   - For United States accounts, you can't change tax status after you create the billing account.
5. When you're finished entering details, click **Submit and enable billing**.

You've now created a new billing account for your organization resource.

Cloud Resources

Manage your Google Cloud resources:

- This page explains how to view and manage your Google Cloud resources, grant IAM roles.

To migrate your existing billing accounts into an organization resource, follow the steps below:

1. Go to the Google Cloud console Billing page:

   Go to the Billing page

2. From the **Select an organization** menu, select an organization resource to see the Cloud Billing accounts associated with it, or select **No organization** to see billing accounts that aren't associated with an organization resource.

3. Under **Billing account name**, click the name of the Cloud Billing account that you want to migrate. The billing account overview page opens.

4. In the Billing navigation menu, click **Account management**.

5. At the top of the Account management page, click **Change Organization**, then select the organization resource to which you want to migrate the Cloud Billing account.

Cloud Resources

Cloud resources billing:

- Cloud Billing pricing:

All use of the Cloud Billing APIs is free of charge. The Cloud Billing APIs include:

- Cloud Billing Account API
- Cloud Billing Catalog API
- Cloud Billing Budget API

For the Cloud Billing Account API:

- Get a list of all your Cloud Billing Accounts.
- Get information about a particular Cloud Billing Account.
- List any Google Cloud project associated with a Cloud Billing Account.
- Get billing information for a Cloud project.
- Enable billing on a Cloud project (by associating it with a Cloud Billing Account).
- Disable billing on a Cloud project (by removing its Cloud Billing Account).
- Change which Cloud Billing Account is associated with a Cloud project.

Cloud Resources

Cloud Resource and Resource Hierarchy for access control:

Google Cloud resources are organized hierarchically, where the organization node is the root node in the hierarchy, the projects are the children of the organization, and the other resources are descendants of projects.

Các tài nguyên của Google Cloud được tổ chức theo thứ bậc, trong đó nút tổ chức là nút gốc trong hệ thống phân cấp, các dự án là con của tổ chức và các tài nguyên khác là con của các dự án.

You can set allow policies at different levels of the resource hierarchy.

Bạn có thể đặt các chính sách cho phép ở các cấp độ khác nhau của hệ thống phân cấp tài nguyên.

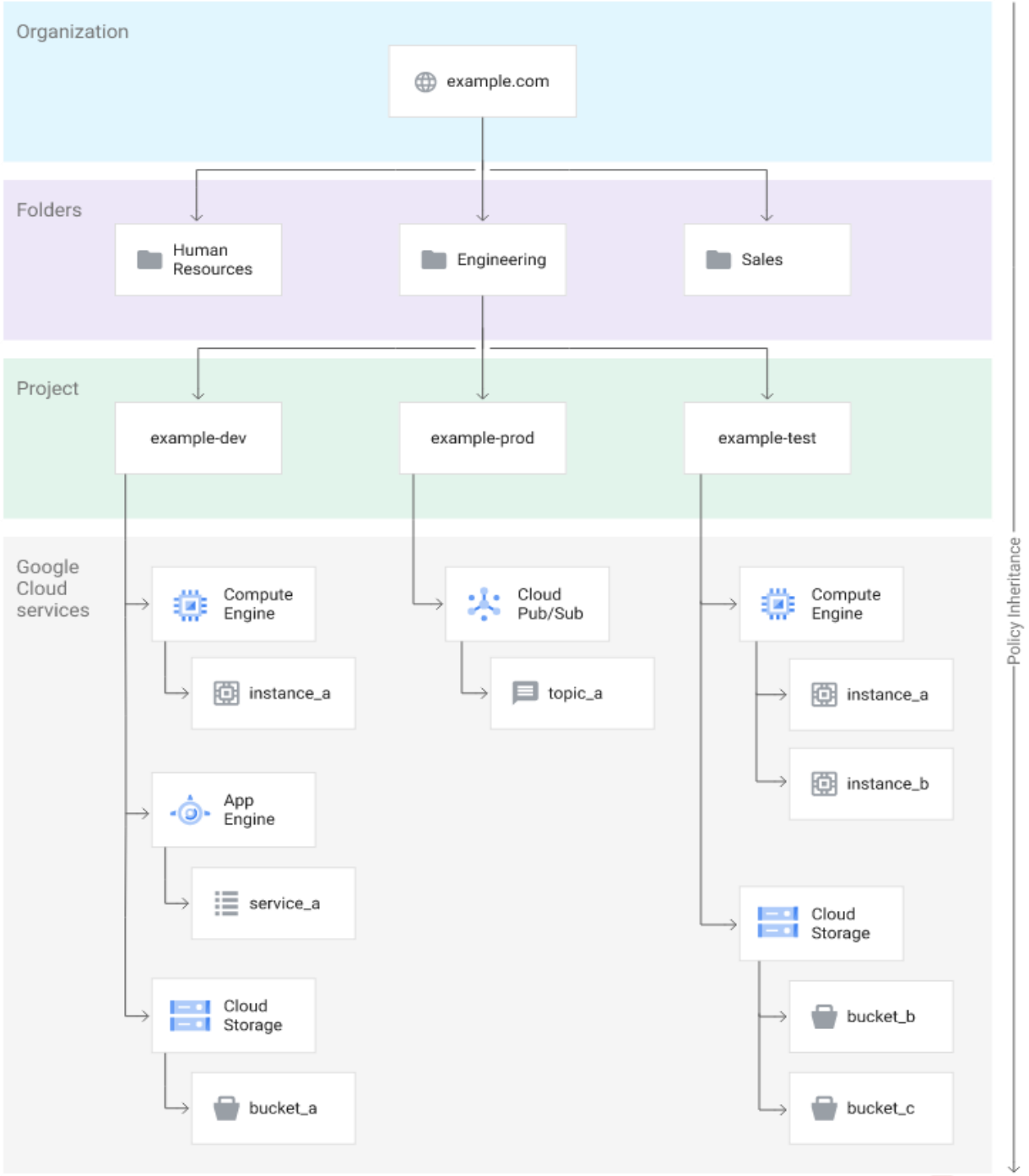
Resources inherit the allow policies of the parent resource. The effective allow policy for a resource is the union of the allow policy set at that resource and the allow policy inherited from its parent.

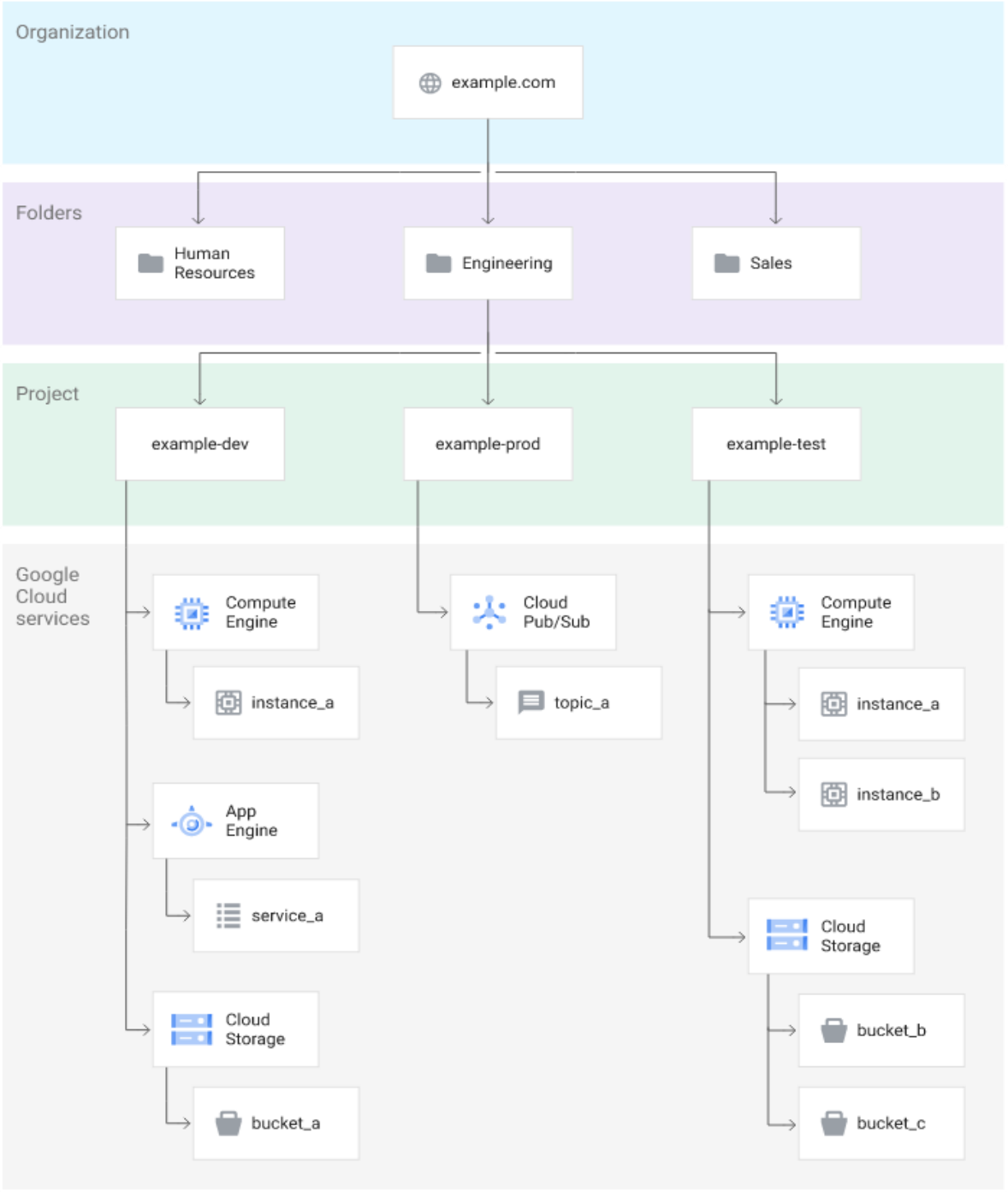
Tài nguyên kế thừa các chính sách của tài nguyên mẹ. Chính sách cấp phép hiệu quả đối với một tài nguyên là sự kết hợp của chính sách cấp phép được đặt tại tài nguyên đó và chính sách cấp phép được kế thừa từ nguồn gốc của nó.

Cloud Resources

- **Cloud Resource and Resource Hierarchy …:**

Some examples of how allow policy inheritance works and explains the best practices that you must take into consideration when you create resources during Identity and Access Management (IAM) deployment.





Organization level. The organization resource represents your company. IAM roles granted at this level are inherited by all resources under the organization.

Folder level. Folders can contain projects, other folders, or a combination of both. Roles granted at the highest folder level will be inherited by projects or other folders that are contained in that parent folder. For more information

Project level. Projects represent a trust boundary within your company. Services within the same project have a default level of trust. For example, App Engine instances can access Cloud Storage buckets within the same project. IAM roles granted at the project level are inherited by resources within that project

Resource level. In addition to the existing Cloud Storage and BigQuery ACL systems, additional resources such as Genomics Datasets, Pub/Sub topics, and Compute Engine instances support lower-level roles so that you can grant certain users permission to a single resource within a project.

Cloud Resources

IAM overview:

IAM lets you grant granular access to specific Google Cloud resources and helps prevent access to other resources. IAM lets you adopt the security principle of least privilege, which states that nobody should have more permissions than they actually need.

- With IAM, you manage access control by defining who (identity) has what access (role) for which resource. For example, Compute Engine virtual machine instances, Google Kubernetes Engine (GKE) clusters, and Cloud Storage buckets are all Google Cloud resources. The organizations, folders, and projects that you use to organize your resources are also resources.

- In IAM, permission to access a resource isn't granted directly to the end user. Instead, permissions are grouped into roles, and roles are granted to authenticated principals. (In the past, IAM often referred to principals as members. Some APIs still use this term.)

- An allow policy, also known as an IAM policy, defines and enforces what roles are granted to which principals. Each allow policy is attached to a resource. When an authenticated principal attempts to access a resource, IAM checks the resource's allow policy to determine whether the action is permitted.

Cloud Resources

Cloud Resource Manager API:

- Creates, reads, and updates metadata for Google Cloud Platform resource containers.

- Service: cloudresourcemanager.googleapis.com

To call this service, we recommend that you use the Google-provided client libraries. If your application needs to use your own libraries to call this service, use the following information when you make the API requests.

https://cloud.google.com/resource-manager/reference/rest

REST Resource: v3.effectiveTags
REST Resource: v3.folders
REST Resource: v3.liens
REST Resource: v3.operations
REST Resource: v3.organizations
REST Resource: v3.projects
REST Resource: v3.tagBindings
REST Resource: v3.tagKeys
REST Resource: v3.tagValues
REST Resource: v3.tagValues.tagHolds

Resource Settings API:
The Resource Settings API allows users to control and modify the behavior of their GCP resources (e.g., VM, firewall, Project, etc.) across the Cloud Resource Hierarchy.

Cloud Resources

Resource Settings:

- Resource Settings represent a dimension of a Google Cloud resource or service that you can configure. For example, a Cloud Storage bucket creation location setting could determine the default location at which new bucket resources is created.

- Each resource setting has the following key properties:

Name

Metadata:

  Data type

  Default value

  Read only

Local value

Effective value

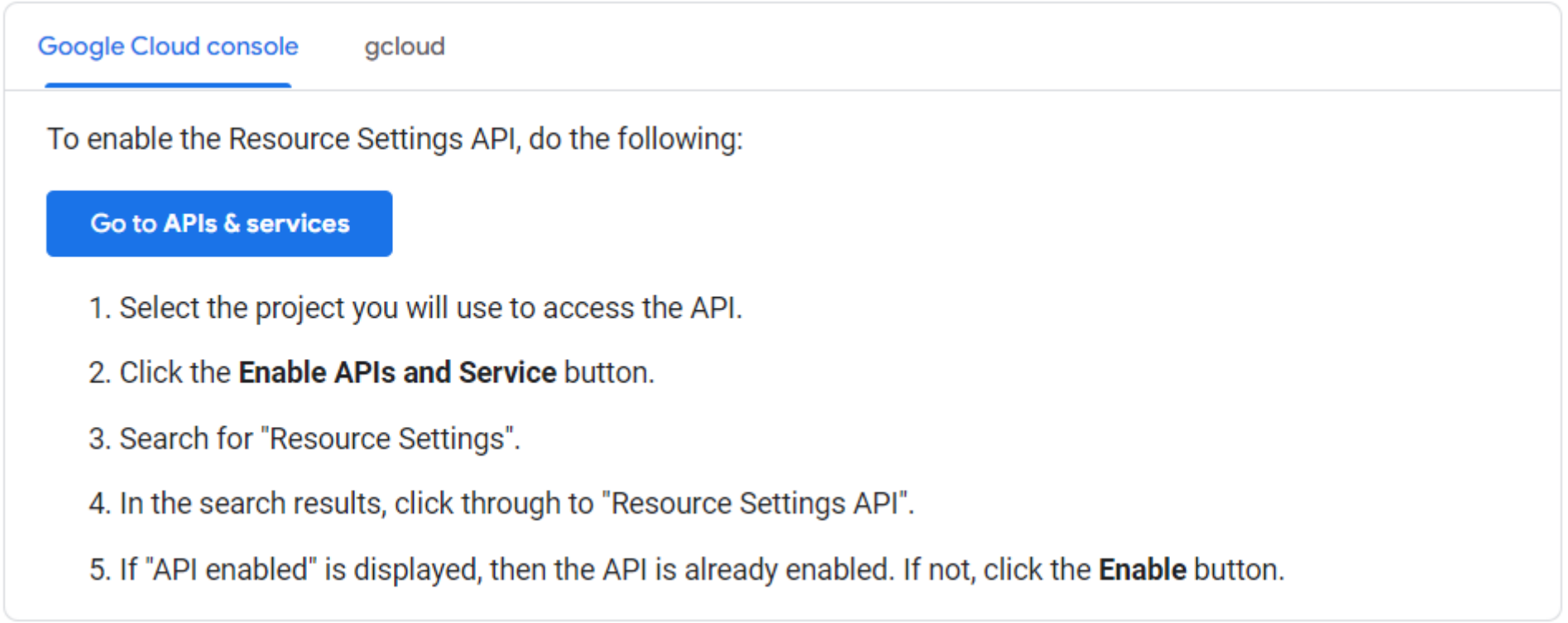
Cloud Resources

Manage resource settings:

- This guide describes how to manage resource settings. You can use the Resource Settings to centrally configure settings for your Google Cloud projects, folders, and organization. Each resource setting allows you to control an aspect of a supported service.

- Enable the API

The Resource Settings API can be enabled for individual projects.



Cloud Resources

- **Manage resource settings:**
  - Required permissions

The permissions you need depend on the action you need to perform.

To gain these permissions, ask your administrator to grant the suggested role at the appropriate level of the resource hierarchy.

View resource settings

To view the resource settings available for use on a resource, as well as the local an effective setting values on a resource, you need the **Resource Settings Viewer** role (`roles/resourcesettings.viewer`), or another role that includes the following permissions:

- `resourcesettings.settings.get`
- `resourcesettings.settings.list`

Administer resource settings

To create, update, and delete resource setting values on a resource, you need the **Resource Settings Administrator** role (`roles/resourcesettings.admin`), or another role that includes the following permissions:

- `resourcesettings.settings.get`
- `resourcesettings.settings.list`
- `resourcesettings.settings.update`

Cloud Resources

- **Manage resource settings:**
  - List available settings

You can get a list of all available resource settings for a given resource. This list displays all resource settings that can be applied to the resource. Resource settings in preview status are only available to those that have been given explicit permission to use them.

gcloud API

To get a list of all settings available for use on a resource, use the following `gcloud resource-settings list` command:

```
gcloud resource-settings list --RESOURCE_ID
```

Where *RESOURCE_ID* is the ID of the folder, project, or organization for which you want to find available resource settings. For example: `--project=7890123456`

Cloud Resources

- **Resource Settings audit logging information:**

- The Resource Settings API allows users to control and modify the behavior of their GCP resources (e.g., VM, firewall, Project, etc.) across the Cloud Resource Hierarchy.

- Overview:

Google Cloud services write audit logs to help you answer the questions, "Who did what, where, and when?" within your Google Cloud resources.

Your Google Cloud projects contain only the audit logs for resources that are directly within the Cloud project. Other Google Cloud resources, such as folders, organizations, and billing accounts, contain the audit logs for the entity itself.

For a general overview of Cloud Audit Logs, see Cloud Audit Logs overview. For a deeper understanding of the audit log format, see Understand audit logs.

Cloud Resources

- **Resource Settings audit logging information:**
  - The Resource Settings API allows users to control and modify the behavior of their GCP resources (e.g., VM, firewall, Project, etc.) across the Cloud Resource Hierarchy.

Available audit logs:

The following types of audit logs are available for Resource Manager:

- Admin Activity audit logs

Includes "admin write" operations that write metadata or configuration information.

You can't disable Admin Activity audit logs.

- Data Access audit logs

Includes "admin read" operations that read metadata or configuration information. Also includes "data read" and "data write" operations that read or write user-provided data.

To receive Data Access audit logs, you must explicitly enable them.

For fuller descriptions of the audit log types, see Types of audit logs.

https://cloud.google.com/logging/docs/audit#types

Cloud Resources

- **Resource Settings audit logging information:**
  - The Resource Settings API allows users to control and modify the behavior of their GCP resources (e.g., VM, firewall, Project, etc.) across the Cloud Resource Hierarchy.

Permissions and roles

IAM permissions and roles determine your ability to access audit logs data in Google Cloud resources.

When deciding which Logging-specific permissions and roles apply to your use case, consider the following:

- The Logs Viewer role (`roles/logging.viewer`) gives you read-only access to Admin Activity, Policy Denied, and System Event audit logs. If you have just this role, you cannot view Data Access audit logs that are in the `_Required` and `_Default` buckets.
- The Private Logs Viewer role (`roles/logging.privateLogViewer`) includes the permissions contained in `roles/logging.viewer` , plus the ability to read Data Access audit logs in the `_Required` and `_Default` buckets.

  Note that if these private logs are stored in user-defined buckets, then any user who has permissions to read logs in those buckets can read the private logs. For more information about log buckets, see Routing and storage overview.

For more information about the IAM permissions and roles that apply to audit logs data, see Access control with IAM.

Cloud Resources

- **Resource Settings audit logging informatio**

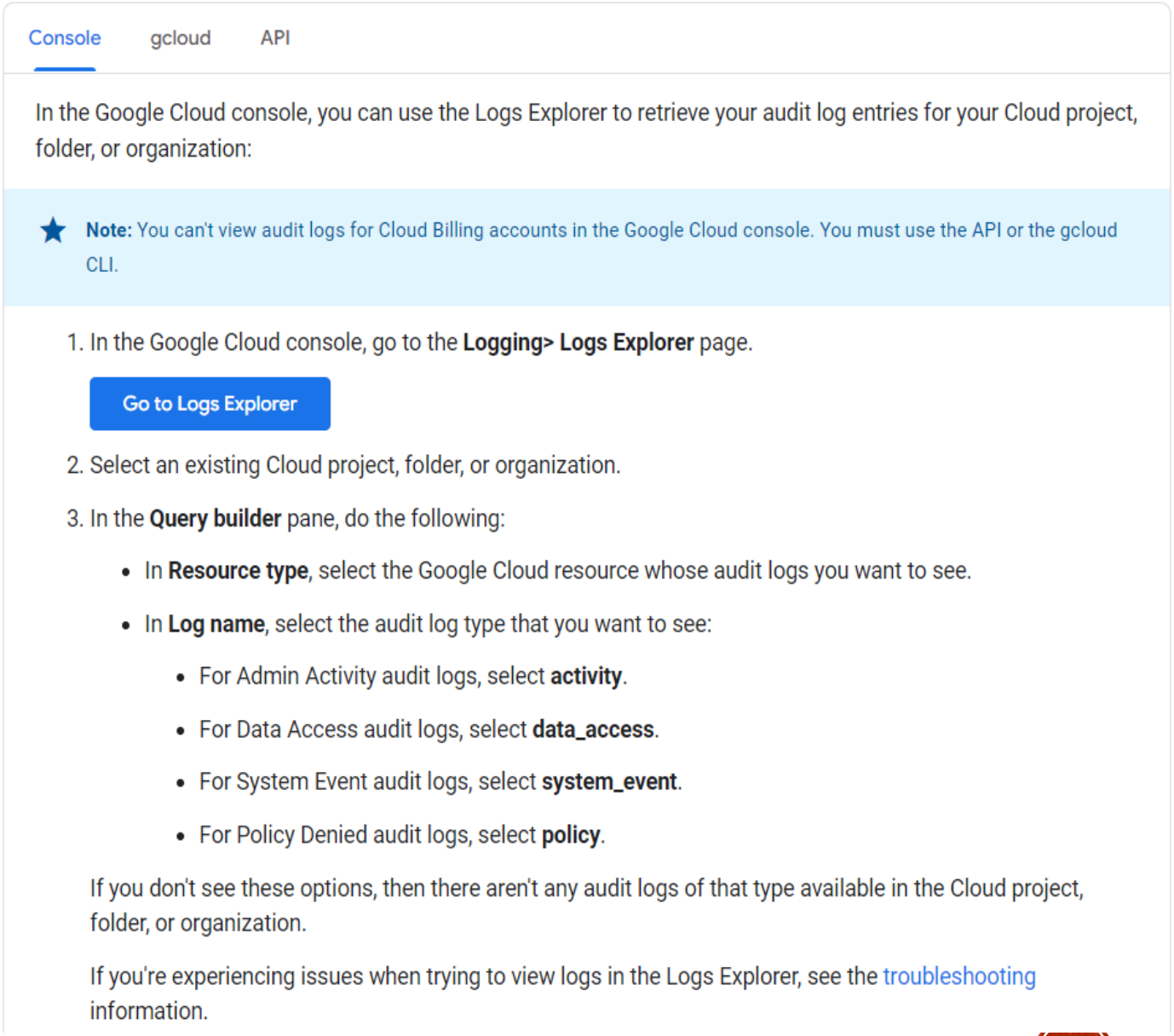
.

- View logs:

To query for audit logs, you need to know the audit log name, which includes the resource identifier of the Cloud project, folder, billing account, or organization for which you want to view audit logging information.

In your query, you can further specify other indexed LogEntry fields, such as resource.type.

For more information on querying, see Build queries in the Logs Explorer.



Console gcloud API

In the Google Cloud console, you can use the Logs Explorer to retrieve your audit log entries for your Cloud project, folder, or organization:

Note: You can't view audit logs for Cloud Billing accounts in the Google Cloud console. You must use the API or the gcloud CLI.

1. In the Google Cloud console, go to the **Logging> Logs Explorer** page.

   Go to Logs Explorer

2. Select an existing Cloud project, folder, or organization.
3. In the **Query builder** pane, do the following:
   - In **Resource type**, select the Google Cloud resource whose audit logs you want to see.
   - In **Log name**, select the audit log type that you want to see:
     - For Admin Activity audit logs, select **activity**.
     - For Data Access audit logs, select **data_access**.
     - For System Event audit logs, select **system_event**.
     - For Policy Denied audit logs, select **policy**.

   If you don't see these options, then there aren't any audit logs of that type available in the Cloud project, folder, or organization.

   If you're experiencing issues when trying to view logs in the Logs Explorer, see the troubleshooting information.

Cloud Resources

Google Cloud CLI:

- The Google Cloud CLI is a set of tools to create and manage Google Cloud resources. You can use these tools to perform many common platform tasks from the command line or through scripts and other automation.

For example, you can use the gcloud CLI to create and manage the following:

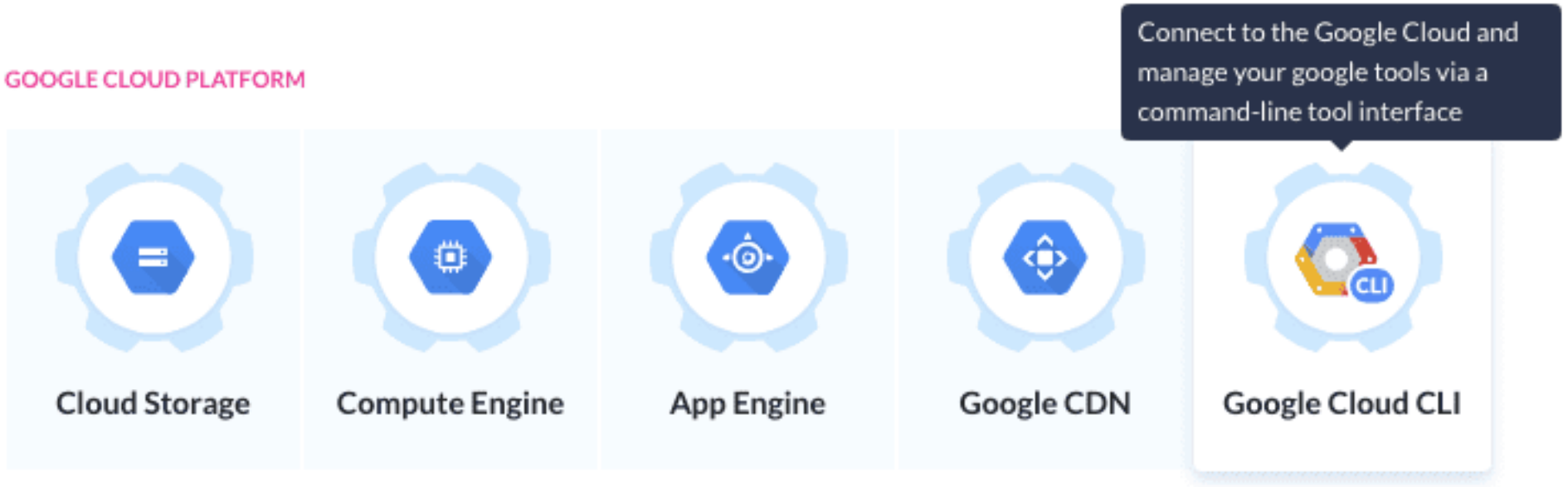
- Compute Engine virtual machine instances and other resources
- Cloud SQL instances
- Google Kubernetes Engine clusters
- Dataproc clusters and jobs
- Cloud DNS managed zones and record sets
- Cloud Deployment Manager deployments

You can also use the gcloud CLI to deploy App Engine applications, manage authentication, customize local configuration, and perform other tasks.

Cloud Resources

Google Cloud CLI:

- This quickstart guides you through installing and initializing the Google Cloud CLI and running a few core gcloud CLI commands.



Cloud Resources

❑ Google Cloud CLI:

- Initializing the gcloud CLI: Use the gcloud init command to perform several common gcloud CLI setup tasks.

1. Initialize the gcloud CLI:

```
gcloud init
```

> **Note:** To prevent the command from launching a web browser, use **`gcloud init --console-only`**. To authorize without a web browser and non-interactively, create a service account with the appropriate scopes using the Google Cloud console and use **`gcloud auth activate-service-account`** with the corresponding JSON key file.

2. Accept the option to log in using your Google user account:

```
To continue, you must log in. Would you like to log in (Y/n)? Y
```

3. In your browser, log in to your Google user account when prompted and click **Allow** to grant permission to access Google Cloud resources.

4. At the command prompt, select a Google Cloud project from the list of projects where you have **Owner**, **Editor** or **Viewer** permissions:

```
Pick cloud project to use:
 [1] [my-project-1]
 [2] [my-project-2]
 ...
 Please enter your numeric choice:
```

If you only have one project, `gcloud init` selects it for you.

If you have access to more than 200 projects, you will be prompted to enter a project id, create a new project, or list projects.

```
This account has a lot of projects! Listing them all can take a while.
 [1] Enter a project ID
 [2] Create a new project
 [3] List projects
Please enter your numeric choice:
```

> **Note:** If you choose to create a project, you'll also need to enable billing on your project to use Google Cloud services.

5. If you have the Compute Engine API enabled, `gcloud init` allows you to choose a default Compute Engine zone:

```
Which compute zone would you like to use as project default?
 [1] [asia-east1-a]
 [2] [asia-east1-b]
 ...
 [14] Do not use default zone
 Please enter your numeric choice:
```

`gcloud init` confirms that you have complete the setup steps successfully:

```
gcloud has now been configured!
You can use [gcloud config] to change more gcloud settings.

Your active configuration is: [default]
```

Cloud Monitoring - Report

TASK I-a: Cloud billing

Show giao diện "report" của mục cloud billing:

- Hiển thị giao diện/bảng tính tiền của Cloud với tính năng
  - Invoice tính theo tháng (invoice by month)
  - Invoice tính theo tài nguyên sử dụng (invoice by usage)

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

(*lưu ý: thử với tài khoản là vai trò owner chính (first owner role)*)

Cloud Monitoring - Report

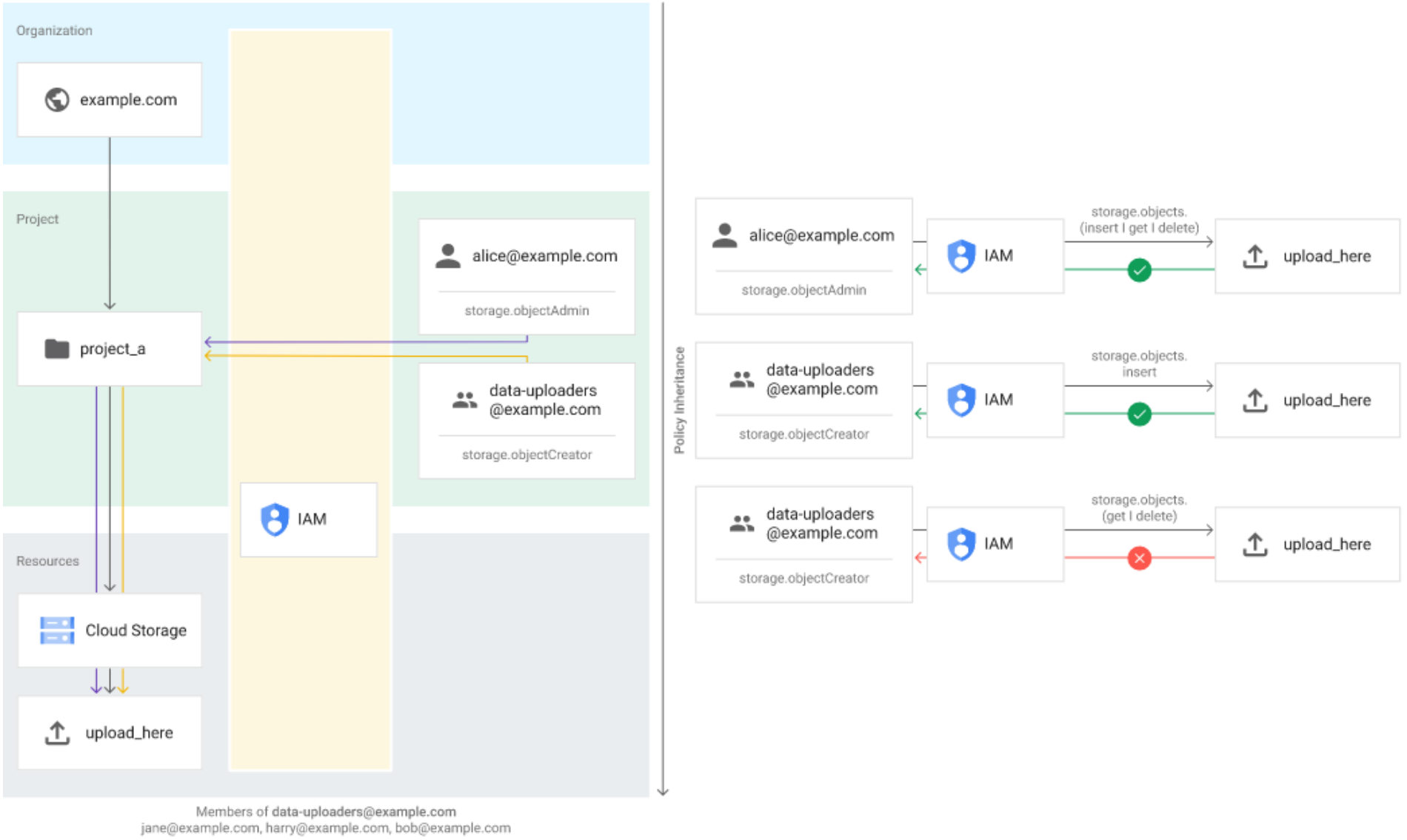
TASK I-b: Resource Hierarchy for access control

Explain:

Lưu đồ hoạt động

Lý do tại sao xảy ra lỗi “đỏ”?

Giải quyết bằng cách nào để hết xảy ra lỗi?



Cloud Resources - Report

TASK II: Resource setting

https://cloud.google.com/resource-manager/docs/resource-settings/overview

- ☺ Phân tích ý nghĩa của các Key properties of resource setting

Cloud Resources - Report

TASK III: Cloud Resource Manager API

Using https://cloud.google.com/resource-manager/reference/rest

- *Đưa ra "command" để thực hiện các tác vụ sau*:

☺ Yêu cầu tạo ra 1 project mới

☺ Liệt kê các project là con của tài nguyên tổ chức được chỉ định

☺ Khôi phục 1 project (đã bị xóa) với tên được chỉ định: name=projects/<12345678>

☺ Muốn có quyền truy cập với kiểm soát chính sách của một tài nguyên tổ chức

☺ Tạo một thư mục (folder) trong hệ thống phân cấp tài nguyên

Cloud Resources - Report

TASK VI: Resource Settings audit logging

Access role and view log

- Cấp phép quyền cho 1 User có thể: view logging

Trình tự các bước thực hiện, ảnh chụp minh chứng

- User này sẽ view logging for:

activity, data_access, system_event, policy

Trình tự các bước thực hiện, ảnh chụp minh chứng

Cloud Resources - Report

TASK V: Google Cloud CLI

Using gcloud CLI cheat sheet

- ☺ What is full name of CLI?
- ☺ Activate/Open “Cloud Shell” để code trên Google Cloud Platform
- ☺ Sử dụng “*gcloud init*” và thực hiện các bước để cấp quyền, điều chỉnh cấu hình tài khoản đúng theo <your project>
- ☺ Display version and installed components: *gcloud version*
- ☺ Display metadata for a project (including its ID): *gcloud projects describe*

→ Các ảnh chụp minh chứng