Google Cloud Concepts

Discussed topics

- Google Cloud projects & resources
- Identity & Access Managament

Google Cloud projects & resources

> Cloud **resources** are the **instanciations** of Google Cloud **products** such as Google Kubernetes Engine (GKE), Google Cloud Storage (GCS), etc.

> Google Cloud resources **must** be **in** a Google Cloud project.

Google cloud projects

On google cloud, **projects** are logical containers for **organizing** Google Cloud **resources**.

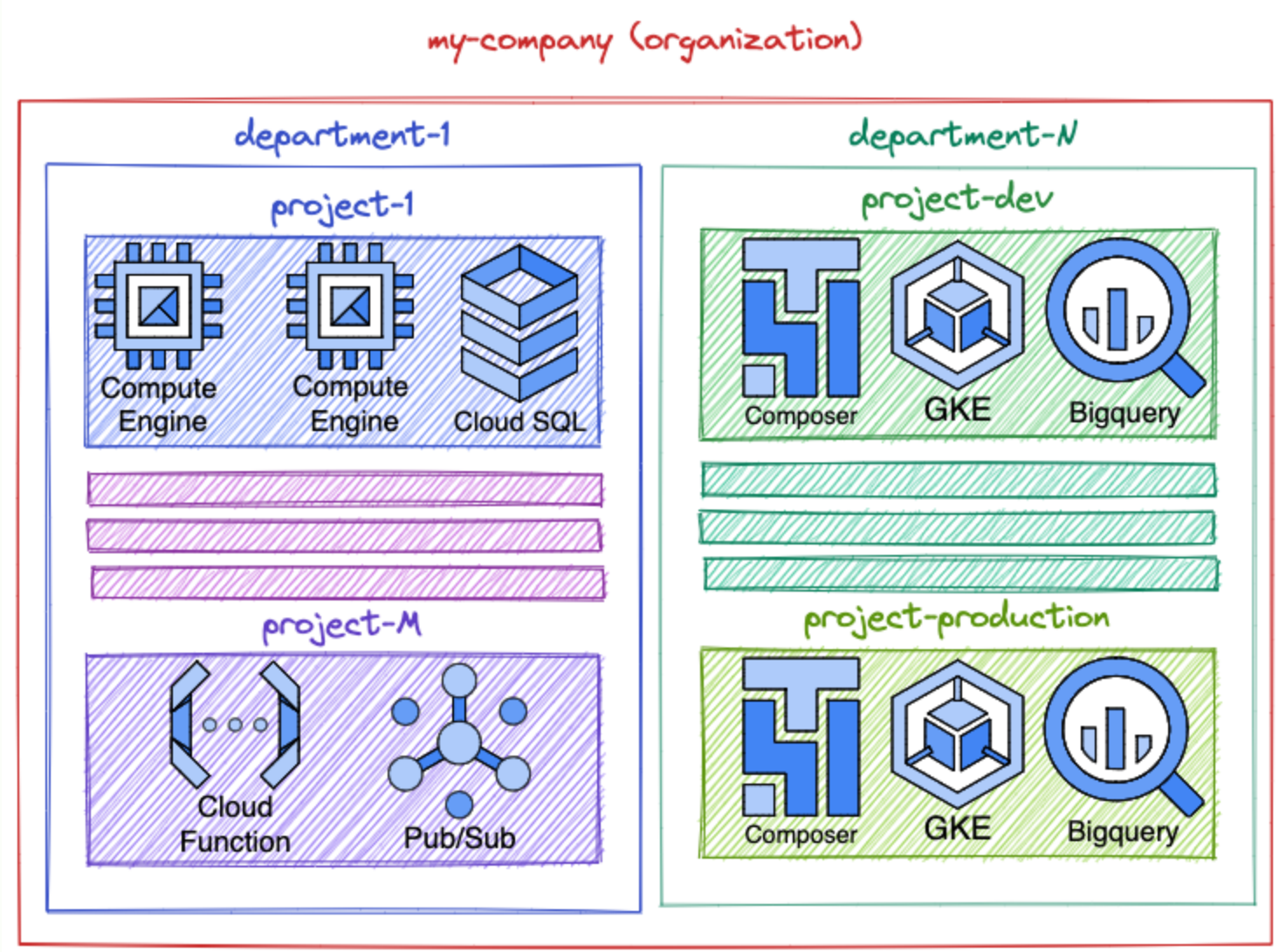
Projects provide a **central** point for **managing** aspects such as:

- Billing
- Quotas
- Permissions

Every Google Cloud **project** has:

- **Project name:** name chosen by the user during project creation.
- **Project ID:** unique name in all of Google Cloud. Either project name or project name suffixed with a unique id.
- **Project number:** not relevant to this presentation.

Organizing resources (1/2)



Organizing resources (2/2)

- Resources **must** be created in a project.
- Projects **can** be placed into a folder.
  - If **no** organization is available, folders **cannot** be used.
  - An **organization** represents an actual **company** (name, address, contact number, etc).
  - **organizations** are related to a google workspace subscription (which is not covered by this presentation).
  - For instance, **personal** gmail accounts do **not** grant access to folder or organization creation
- Folders **can** contain folders, projects or both.

Identity & Access Managament

> Who ?

> Do What ?

> Which resource ?

Overview

Identity & Access Managament (IAM) is about answering the following questions:

- **Who** are you?
- **What** are you allowed to do ?
- **On which** resources can you do these actions ?

Identity - Who ?

In Google Cloud, identity has many forms:

- **Personal account:** refers to single person `john-doe@his-company.com`
- **Service account:** refers to a **non human** user such as an account for a machine or service `my-machine-user@project-id.iam.gserviceaccount.com`
- **Google group member:** refers to a **group** of individuals. For example `developers@their-company.com` or `data-engineers@their-company.com`.

Access - What on which ?

In Google Cloud, access is about "What can a member do?"

- **Permissions** are defined. For example:
  - a member can **view** data from a dataset
  - a member can **create** a new machine
- **Prohibited actions** are **not explicitly** defined, instead, whatever is not permitted is **implicitly** prohibited.
- **Permissions** can be granted on **organization**, **folder**, **project** and **resource** levels.

Permissions & resources organization

Permissions are prioritized from **top to bottom** levels, which means:

- If a permission is **granted** to a member on the **organization** level, it will be **effective** on **all folders, projects and resources**.
- If a permission is **granted** to a member on the **folder** level, it will be **effective** on **all projects and resources in the folder**.
- If a permission is **granted** to a member on the **project** level, it will be **effective** on **all resources in the project**.
- If a permission is **granted** to a member on the **resource** level, it will be effective **only on the resource**.

Roles

Roles are permissions grouped together.

For example BigQuery Job User has the following permissions: `bigquery.config.get`, `bigquery.jobs.create`, `resourcemanager.projects.get`, `resourcemanager.projects.list`

Roles can be of **3 types**:

- Basic
- Predefined
- Custom

Basic roles

3 basic roles exist:

- Viewer
- Editor
- Owner

Basic roles are **not product scoped** which makes them **too broad**.

For example, granting `Editor` role on a project, folder or organisation will give access to many actions on multiple unrelated products such as `compute instances`, `big query datasets`, `cloud storage`, `pub/sub`, etc.

Basic roles should be **avoided**.

Predefined roles

Predefined roles are **product scoped**.

Examples for **predefined roles** are:

- BigQuery Data Editor
- Kubernetes Engine Cluster Admin
- Storage Object Viewer

Predefined roles should be used **whenever possible** and follow the **principle of least privilege (PoLP)**.

> Grant just enough permission to the operator for it to be able to do the required task.

The LPP **reduces error** impact and helps to **better** manage **responsibility & accountability**.

Custom roles

When in need of a specific set of permissions & **no predefined role** is suitable, a **custom role** can be **defined**.

Custom roles can be created **from scratch** and contain up to **3k** permisssions.

Custom roles can be created **from predefined roles** to which permissions are added or removed.

IAM best practices

- Try not to use **basic roles**.
- Use **predefined roles** as much as possible.
- Grant roles to **groups** instead of individuals.
- Apply the **Princple of Least Privilege**.
- If the permission is to be granted for a **limted duration**, set the **expiration time** to the appropriate date.