Security & Identity Products (https://cloud.google.com/products/security/)
Resource Manager (https://cloud.google.com/resource-manager/)
Documentation (https://cloud.google.com/resource-manager/docs/) Guides

Resource Hierarchy

This page describes the Google Cloud resource hierarchy and the resources that can be managed using Resource Manager.

The purpose of the Google Cloud resource hierarchy is two-fold:

- Provide a hierarchy of ownership, which binds the lifecycle of a resource to its immediate parent in the hierarchy.
- Provide attach points and inheritance for access control and organization policies.

Metaphorically speaking, the Google Cloud resource hierarchy resembles the file system found in traditional operating systems as a way of organizing and managing entities hierarchically. Each resource has exactly one parent. This hierarchical organization of resources enables you to set access control policies and configuration settings on a parent resource, and the policies and Cloud Identity and Access Management (Cloud IAM) settings are inherited by the child resources.

Google Cloud resource hierarchy in detail

At the lowest level, resources are the fundamental components that make up all Google Cloud services. Examples of resources include Compute Engine Virtual Machines (VMs), Pub/Sub topics, Cloud Storage buckets, App Engine instances. All these lower level resources can only be parented by projects, which represent the first grouping mechanism of the Google Cloud resource hierarchy.

G Suite and Cloud Identity customers have access to additional features of the Google Cloud resource hierarchy that provide benefits such as centralized visibility and control, and further grouping mechanisms, such as folders. We have launched the Cloud Identity management tool. For details on how to use Cloud Identity, see Migrating to Cloud Identity (https://cloud.google.com/iam/docs/migrating-to-cloud-identity).

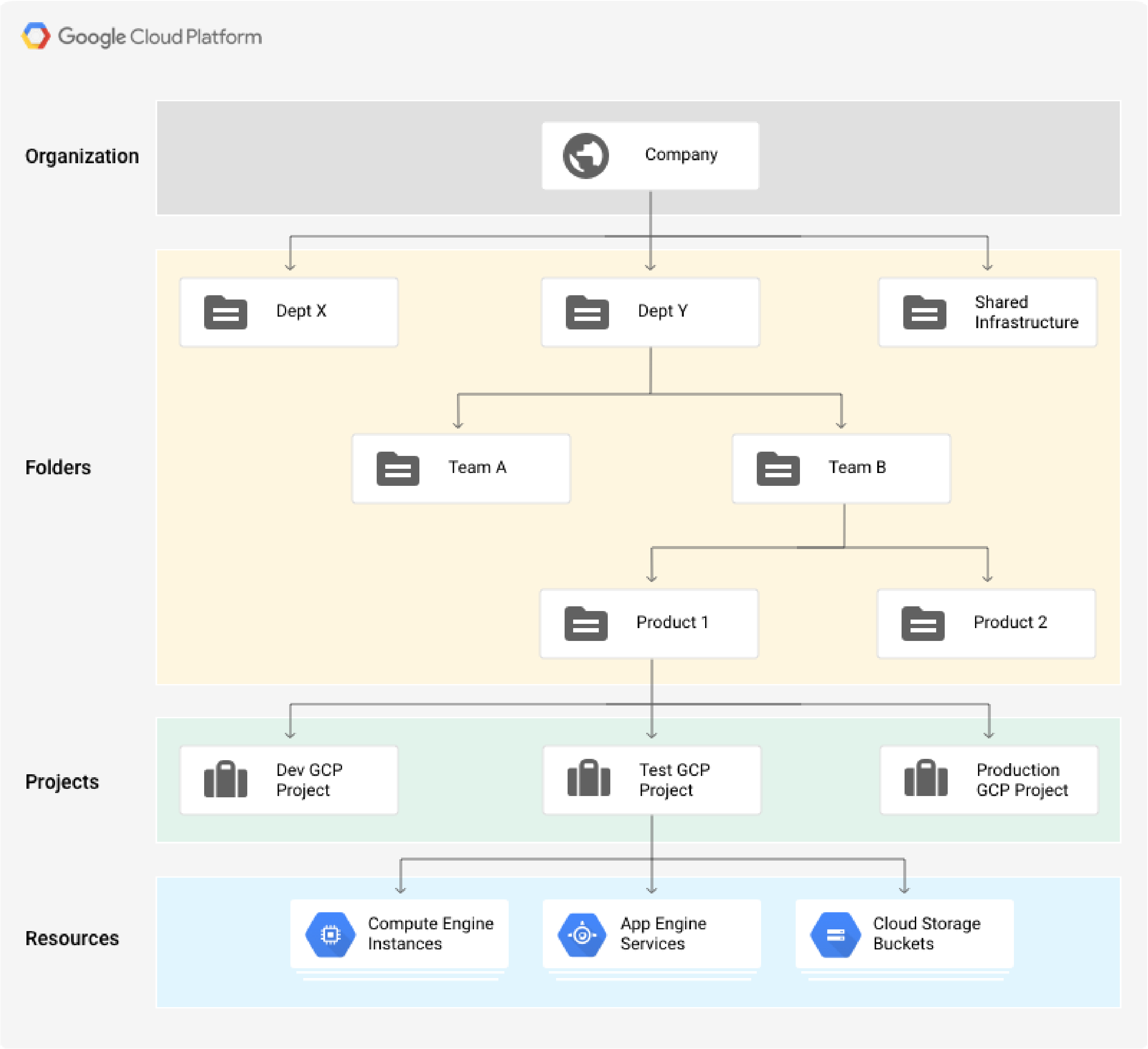
Google Cloud resources are organized hierarchically. Starting from the bottom of the hierarchy, projects are the first level, and they contain other resources. All resources except for organizations have exactly one parent. The Organization is the top of the hierarchy and does not have a parent.

The Organization resource is the root node of the Google Cloud resource hierarchy and all resources that belong to an organization are grouped under the organization node. This provides central visibility and control over every resource that belongs to an organization.

Folders are an additional grouping mechanism on top of projects. You are required to have an Organization resource as a prerequisite to use folders. Folders and projects are all mapped under the Organization resource.

The Google Cloud resource hierarchy, especially in its most complete form which includes an Organization resource and folders, allows companies to map their organization onto Google Cloud and provides logical attach points for access management policies (Cloud IAM) and Organization policies (https://cloud.google.com/resource-manager/docs/organization-policy/overview). Both Cloud IAM and Organization policies are inherited through the hierarchy, and the effective policy at each node of the hierarchy is the result of policies directly applied at the node and policies inherited from its ancestors.

The diagram below represents an example Google Cloud resource hierarchy in complete form:



The Organization resource

The Organization (https://cloud.google.com/resource-manager/reference/rest/v1/organizations) resource represents an organization (for example, a company) and is the root node in the Google Cloud resource hierarchy. The Organization resource is the hierarchical ancestor of project resources and Folders. The Cloud IAM access control policies applied on the Organization resource apply throughout the hierarchy on all resources in the organization.

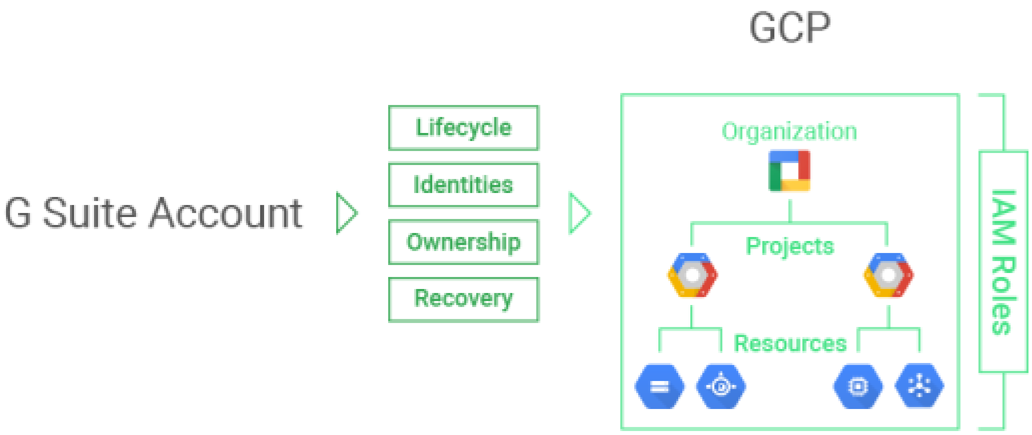
Google Cloud users are not required to have an Organization resource, but some features of Resource Manager will not be usable without one. The Organization resource is closely associated with a G Suite (https://gsuite.google.com) or Cloud Identity (https://cloud.google.com/identity) account. When a user with a G Suite or Cloud Identity account creates a Google Cloud Project, an Organization resource is automatically provisioned for them.

A G Suite or Cloud Identity account may have exactly one Organization provisioned with it. Once an Organization resource is created for a domain, all Google Cloud projects created by members of the account domain will by default belong to the Organization resource.

Link with G Suite or Cloud Identity accounts

For simplicity we will refer to G Suite meaning both G Suite and Cloud Identity users.

The G Suite or Cloud Identity account represents a company and is a prerequisite to have access to the Organization resource. In the Google Cloud context, it provides identity management, recovery mechanism, ownership and lifecycle management. The picture below shows the link between the G Suite account, Cloud Identity, and the Google Cloud resource hierarchy.



The G Suite super admin is the individual responsible for domain ownership verification and the contact in cases of recovery. For this reason, the G Suite super admin is granted the ability to assign Cloud IAM roles by default. The G Suite super admin's main duty with respect to Google Cloud is to assign the Organization Administrator Cloud IAM role to appropriate users in their domain. This will create the separation between G Suite and Google Cloud administration responsibilities that users typically seek.

Benefits of the Organization resource

With an Organization resource, projects belong to your organization instead of the employee who created the project. This means that the projects are no longer deleted when an employee leaves the company; instead they will follow the organization's lifecycle on Google Cloud.

Furthermore, organization administrators have central control of all resources. They can view and manage all of your company's projects. This enforcement means that there can no longer be shadow projects or rogue admins.

Also, you can grant roles at the organization level, which are inherited by all projects and folders under the Organization resource. For example, you can grant the Network Admin role to your networking team at the organization level, allowing them to manage all the networks in all projects in your company, instead of granting them the role for all individual projects.

An Organization resource created using the Resource Manager API consists of the following:

- An organization ID, which is a unique identifier for an organization.
- A display name, which is generated from the primary domain name in G Suite or Cloud Identity.
- The creation time of the organization.
- The last modified time of the organization.
- The owner of the organization. The owner is specified when creating the Organization resource. It cannot be changed once it is set. It is the G Suite customer ID that is specified in the Directory API (https://developers.google.com/admin-sdk/directory/).

The following code snippet shows the structure of an Organization resource:

```
{
  "displayName": "myorganization",
  "organizationId":"34739118321",
  "createTime": "2016-01-07T21:59:43.314Z"
  "owner": {
    "directoryCustomerId": "C012BA234"
   }
}
```

The initial Cloud IAM policy for a newly created Organization resource grants the Project Creator and Billing Account Creator roles to the entire G Suite domain. This means users will be able to continue creating projects and billing accounts as they did before the organization existed. No other resources are created when an Organization resource is created.

The Folder resource

Folder resources provide an additional grouping mechanism and isolation boundaries between projects. They can be seen as sub-organizations within the Organization. Folders can be used to model different legal entities, departments, and teams within a company. For example, a first level of folders could be used to represent the main departments in your organization. Since folders can contain projects and other folders, each folder could then include other sub-folders, to represent different teams. Each team folder could contain additional sub-folders to represent different applications. For more details about using folders, see Creating and Managing Folders (https://cloud.google.com/resource-manager/docs/creating-managing-folders).

If Folder resources exist in your organization and you have appropriate viewing permissions, you can view them from the Google Cloud Console. For more detailed instructions, see Viewing or Listing Folders and Projects (https://cloud.google.com/resource-manager/docs/creating-managing-folders#viewing_or_listing_folders_and_projects)
.

Folders allow delegation of administration rights, so for example, each head of a department can be granted full ownership of all Google Cloud resources that belong to their departments. Similarly, access to resources can be limited by folder, so users in one department can only access and create Cloud resources within that folder.

The following code snippet shows the structure of a folder:

```
{
 "name" : "folders/my-folder",
 "parent" : "organizations/my-organization",
 "displayName" : "Engineering",
 "lifecycleState" : "ACTIVE",
 "createTime": "2016-01-07T21:59:43.314Z"
}
```

Like organizations and projects, folders act as a policy inheritance point for Cloud IAM and Organization policies. Cloud IAM roles granted on a folder are automatically inherited by all projects and folders included in that folder.

The Project resource

The project resource is the base-level organizing entity. Organizations and folders may contain multiple projects. A project is required to use Google Cloud, and forms the basis for creating, enabling, and using all Google Cloud services, managing APIs, enabling billing, adding and removing collaborators, and managing permissions.

All projects consist of the following:

- Two identifiers:
    1. Project ID, which is a unique identifier for the project.
    2. Project number, which is automatically assigned when you create the project. It is read-only.
- One mutable display name.
- The lifecycle state of the project; for example, ACTIVE or DELETE_REQUESTED.
- A collection of labels that can be used for filtering projects.
- The time when the project was created.

The following code snippet shows the structure of a project:

```
{
  "name": "myproject",
  "projectId": "my-project-123",
  "labels":
   {
     "my-label": "prod"
   },
   "projectNumber": "464036093014",
   "lifecycleState": "ACTIVE",
   "createTime": "2016-01-07T21:59:43.314Z"
}
```

In order to interact with most Google Cloud resources, you must provide the identifying project information for every request. You can identify a project in either of two ways: a project ID, or a project number (`projectId` and `projectNumber` in the code snippet).

A project ID is the customized name you chose when you created the project. If you activate an API that requires a project, you will be directed to create a project or select a project using its project ID. (Note that the `name` string, which is displayed in the UI, is not the same as the project ID.)

A project number is automatically generated by Google Cloud. Both the project ID and project number can be found on the dashboard of the project in the Google Cloud Console. For information on getting project identifiers and other management tasks for projects see Creating and Managing Projects (https://cloud.google.com/resource-manager/docs/creating-managing-projects).

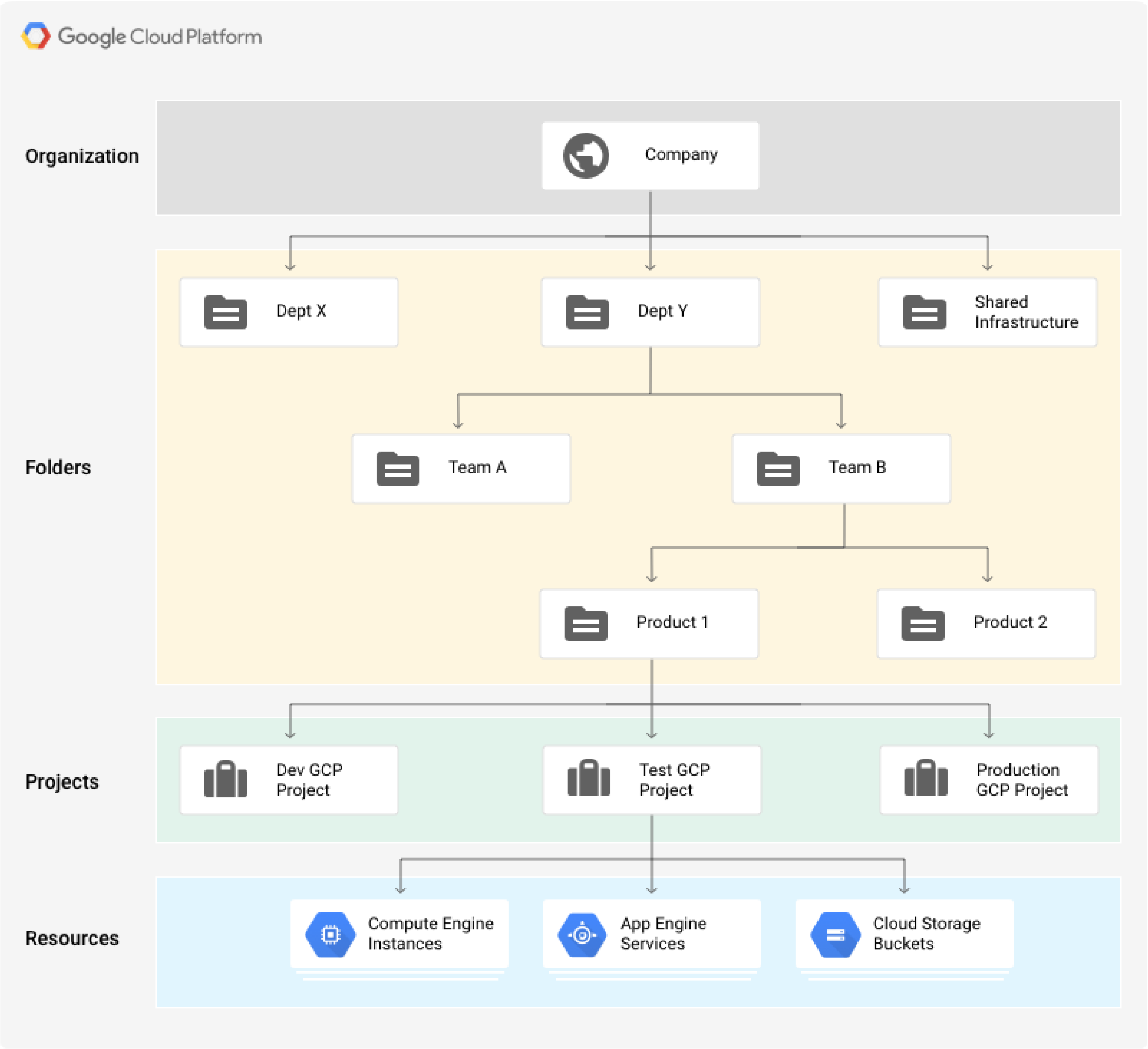
The initial Cloud IAM policy for the newly created project resource grants the owner role to the creator of the project.

Cloud IAM policy inheritance

Google Cloud offers Cloud IAM (https://cloud.google.com/iam/docs/overview), which lets you assign granular access to specific Google Cloud resources and prevents unwanted access to other resources. Cloud IAM lets you control who (**users**) has what access (**roles**) to which **resources** by setting Cloud IAM policies on the resources.

You can set an Cloud IAM policy at the organization level (https://cloud.google.com/resource-manager/docs/access-control-org), the folder level (https://cloud.google.com/resource-manager/docs/access-control-folders), the project level (https://cloud.google.com/resource-manager/docs/access-control-proj), or (in some cases) the resource level. Resources inherit the policies of the parent node. If you set a policy at the Organization level, it is inherited by all its child folders and projects, and if you set a policy at the project level, it is inherited by all its child resources.

The effective policy for a resource is the union of the policy set on the resource and the policy inherited from its ancestors. This inheritance is transitive. In other words, resources inherit policies from the project, which inherit policies from the organization. Therefore, the organization-level policies also apply at the resource level.



For example, in the resource hierarchy diagram above, if you set a policy on folder "Dept Y" that grants Project Editor role to bob@example.com, then Bob will have editor role on projects "Dev GCP Project," "Test GCP Project," and "Production GCP Project." Conversely, if you assign alice@example.com the Instance Admin role on project "Test GCP Project", she will only be able to manage Compute Engine instances in that project.

The Cloud IAM policy hierarchy follows the same path as the Google Cloud resource hierarchy. If you change the resource hierarchy, the policy hierarchy changes as well. For example, moving a project into an organization will update the project's Cloud IAM policy to inherit from the organization's Cloud IAM policy. Similarly, moving a project from one folder to another will change the inherited permissions. Permissions that were inherited by the project from the original parent will be lost when the project is moved to a new folder. Permissions set at the destination folder will be inherited by the project as it is moved.

Last updated November 19, 2019.