This page describes the relationship between Google Cloud Console projects and Cloud Storage resources. To learn more about Google Cloud Console projects in general, read Projects (/docs/overview/#projects) in the Overview of Google Cloud.

A project organizes all your Google Cloud resources. A project consists of a set of users; a set of APIs; and billing, authentication, and monitoring settings for those APIs. So, for example, all of your Cloud Storage buckets and objects, along with user permissions for accessing them, reside in a project. You can have one project, or you can create multiple projects and use them to organize your Google Cloud resources, including your Cloud Storage data, into logical groups.

Most of the time, you do not need to specify a project when performing actions in Cloud Storage; however you should include either the project ID or the project number in the following cases:

For each project, you can use Identity and Access Management (IAM) (/storage/docs/access-control/iam) to add team members who can manage and work on your project. IAM allows you to specify each team member's *role* or *roles*: different roles have permissions that allow a member to do different things within your project.

While many IAM roles can be set at both the project-level (thus applying to all buckets in the project) or the bucket-level (thus applying only to an individual bucket), there are several roles that you can **only** apply to a project. These roles are *primitive roles* (/iam/docs/understanding-roles#primitive_roles). Primitive roles have the following properties for Cloud Storage:

Role	Intrinsic Behavior	Modifiable Behavior

Role	Intrinsic Behavior	Modifiable Behavior
`roles/viewer`	Members with this role can list buckets in the project, as well as list and get HMAC keys in the project.	• Members with this role are granted, as a group, the `roles/storage.legacyBucketReader` role for each bucket in the project. • Members with this role are a `READER` in the default object Access Control List (/storage/docs/access-control/lists#defaultobjects) for each bucket in the project. • Members with this role are granted, as a group, the `roles/storage.legacyObjectReader` role for any bucket in the project created with uniform bucket-level access (/storage/docs/uniform-bucket-level-access) enabled.
`roles/editor`	Members with this role can list, create and delete buckets in the project, as well as have full control over HMAC keys in the project.	• Members with this role are granted, as a group, the `roles/storage.legacyBucketOwner` role for each bucket in the project. • Members with this role are a `OWNER` in the default object Access Control List (/storage/docs/access-control/lists#defaultobjects) for each bucket in the project. • Members with this role are granted, as a group, the `roles/storage.legacyObjectOwner` role for any bucket in the project created with uniform bucket-level access (/storage/docs/uniform-bucket-level-access) enabled.

Role	Intrinsic Behavior	Modifiable Behavior
`roles/owner`	Members with this role can list, create and delete buckets in the project, as well as have full control over HMAC keys in the project. Within Google Cloud more generally, members with `roles/owner` can perform administrative tasks such as changing members' roles for the project or changing billing.	• Members with this role are granted, as a group, the `roles/storage.legacyBucketOwner` role for each bucket in the project. • Members with this role are a **OWNER** in the default object Access Control List (/storage/docs/access-control/lists#defaultobjects) for each bucket in the project. • Members with this role are granted, as a group, the `roles/storage.legacyObjectOwner` role for any bucket in the project created with uniform bucket-level access (/storage/docs/uniform-bucket-level-access) enabled.

For a list of available roles that apply to Cloud Storage, see Cloud Storage IAM roles (/storage/docs/access-control/iam-roles).

For instructions for adding, viewing, and removing members from roles at the project level, see Using IAM with projects (/storage/docs/access-control/using-iam-permissions#project-iam).

As illustrated in the **Modifiable Behavior** column above, project team members may have additional access beyond that granted intrinsically by the primitive IAM roles. This additional access comes from two sources:

- **IAM roles applied to buckets**: When a user creates a bucket, IAM roles are applied to it by default. You can edit this access once the bucket is created.
- **Access Control Lists (ACLs)** (/storage/docs/access-control/lists) **applied to objects**: When a user creates an object, an ACL is applied to it. The ACL can either be specified explicitly (/storage/docs/access-control/create-manage-lists#set-an-acl) or applied by default (/storage/docs/access-control/lists#defaultobjects). In either case, the ACL grants access specifically to the created object.

Note that in both cases, you can grant access to both individual users and all holders of a primitive role. Moreover, the access granted may be greater than the access that a user has in general for project, but not more restricted.

Service accounts (/iam/docs/service-accounts) allow applications to authenticate and access Google Cloud resources and services. For example, you can create a service account that your Compute Engine instances use to access objects stored in Cloud Storage buckets.

Service accounts are created within a project and have a unique email address that identifies them. While most service accounts are created and managed by a user, some service accounts are automatically created and managed by Google Cloud services. Cloud Storage creates one such service account with an email address that has the following format:

Where `[PROJECT_NUMBER]` is the project number (/resource-manager/docs/creating-managing-projects#identifying_projects) of the project that owns the service account.

ant: The Cloud Storage service account, including its email address, is not initially available when you make a project d, it is automatically activated the first time it's called, such as when you request the service account's name age/docs/getting-service-account). The service account must be activated prior to assigning permissions age/docs/access-control/using-iam-permissions#project-iam) to it.

The following features use Cloud Storage service accounts:

- Pub/Sub Notifications for Cloud Storage (/storage/docs/pubsub-notifications).
- Customer-Managed Encryption Keys (/storage/docs/encryption/customer-managed-keys).

Examples of actions that non-Cloud Storage service accounts can take which use Cloud Storage resources:

- Performing Storage Transfer Service (/storage-transfer/docs/overview) transfers.
- Moving data to/from Cloud SQL instances (/sql/docs/mysql/import-export/).
- Creating signed URLs (/storage/docs/access-control/signed-urls).

- Complete the Cloud Console quickstart (/storage/docs/quickstart-console) and gsutil quickstart (/storage/docs/quickstart-gsutil).
- Learn about key terms for working with Cloud Storage (/storage/docs/key-terms).
- Find out how to use the Cloud Console to manage your data (/storage/docs/cloud-console).
- Manage your project's service accounts (https://console.cloud.google.com/iam-admin/serviceaccounts).