Access control

This page describes the access control options available to you in Cloud Composer API.

Overview

Cloud Composer API uses Identity and Access Management (IAM) (/iam) for access control.

In the Cloud Composer API, access control can be configured at the *project level*. For example, you can grant access to all Cloud Composer API resources within a project to a group of developers.

For a detailed description of IAM and its features, see the IAM documentation (/iam/docs). In particular, see Managing IAM Policies (/iam/docs/managing-policies).

Every Cloud Composer API method requires the caller to have the necessary permissions. See Permissions and roles (#permissions) for more information.

Cloud Composer creates Google-managed service accounts (/iam/docs/service-accounts) for the services ated with your environment. The service accounts have the appropriate permissions to manage your environr ecute workflows. To avoid access control issues, do not remove or change the service account's role or ssions.

Required permissions

The following table lists the permissions that the caller must have to call each API method in the Cloud Composer API or to perform tasks using Google Cloud tools that use the API, such as Google Cloud Console or Cloud SDK.

By default, Cloud Composer environments run using the Compute Engine default service account. During nment creation, you can specify a custom service account. At minimum, this service account requires the ssions that the **`composer.worker`** role provides to access resources in the Cloud Composer environment. You e authorized to "act as" the service account by having the **`iam.serviceAccounts.actAs`** permission enabled rvice account or project that contains the environment. Please note that the Composer Administrator role by it

ot provide this permission. For more information, see Creating environments
poser/docs/how-to/managing/creating#access-control).

Method	Permission
`environments.create`	composer.environments.create iam.serviceAccounts.actAs (on the service account under which the environment will run)
`environments.delete`	composer.environments.delete
`environments.get`	composer.environments.get
`environments.list`	composer.environments.list
`environments.update`	composer.environments.update
`operations.delete`	composer.operations.delete
`operations.get`	composer.operations.get
`operations.list`	composer.operations.list

Roles

Role	Title	Description	Permissions
`roles/composer.admin`	Composer Administrator	Provides full control of Cloud Composer resources.	composer.* serviceusage.quotas.get serviceusage.services.get serviceusage.services.list

Role	Title	Description	Permissions
roles/composer.environmentAndStorageObjectAdmin	Environment and Storage Object Administrator	Provides full control of Cloud Composer resources and of the objects in all project buckets.	composer.* resourcemanager.projects. resourcemanager.projects. serviceusage.quotas.get serviceusage.services.get serviceusage.services.list storage.objects.*
roles/composer.environmentAndStorageObjectViewer	Environment User and Storage Object Viewer	Provides the permissions necessary to list and get Cloud Composer environments and operations. Provides read-only access to objects in all project buckets.	composer.environments.ge composer.environments.lis composer.imageversions.* composer.operations.get composer.operations.list resourcemanager.projects. resourcemanager.projects. serviceusage.quotas.get serviceusage.services.get serviceusage.services.list storage.objects.get storage.objects.list
roles/composer.user	Composer User	Provides the permissions necessary to list and get Cloud Composer environments and operations.	composer.environments.ge composer.environments.lis composer.imageversions.* composer.operations.get composer.operations.list serviceusage.quotas.get serviceusage.services.get serviceusage.services.list
roles/composer.worker	Composer Worker	Provides the permissions necessary to run a Cloud Composer environment	artifactregistry.* cloudbuild.* container.* containeranalysis.occurrer containeranalysis.occurrer containeranalysis.occurrer

Role	Title	Description	Permissions
		VM. Intended for service accounts.	containeranalysis.occurrer containeranalysis.occurrer logging.logEntries.create monitoring.metricDescriptc monitoring.metricDescriptc monitoring.metricDescriptc monitoring. monitoredResourceDesc monitoring.timeSeries.* pubsub.snapshots.create pubsub.snapshots.delete pubsub.snapshots.get pubsub.snapshots.list pubsub.snapshots.seek pubsub.snapshots.update pubsub.subscriptions.cons pubsub.subscriptions.crea pubsub.subscriptions.dele pubsub.subscriptions.get pubsub.subscriptions.list pubsub.subscriptions.upd pubsub.topics.attachSubs pubsub.topics.create pubsub.topics.delete pubsub.topics.detachSubs pubsub.topics.get pubsub.topics.list pubsub.topics.publish pubsub.topics.update pubsub.topics.updateTag remotebuildexecution.blob resourcemanager.projects. resourcemanager.projects. serviceusage.quotas.get serviceusage.services.get serviceusage.services.list source.repos.get source.repos.list storage.buckets.create storage.buckets.get storage.buckets.list storage.objects.*

Primitive roles

Role	Title	Description	Permissions	Lowest Resource
`roles/owner`	Owner	Primitive role that allows full control of Cloud Composer resources.	composer.operations.list composer.operations.get composer.operations.delete composer.environments.list composer.environments.get composer.environments.delete composer.environments.update composer.environments.create iam.serviceAccounts.actAs	Project
`roles/editor`	Editor	Primitive role that allows full control of Cloud Composer resources.	composer.operations.list composer.operations.get composer.operations.delete composer.environments.list composer.environments.get composer.environments.delete composer.environments.update composer.environments.create iam.serviceAccounts.actAs	Project
`roles/reader`	Viewer	Primitive role that allows a user to list and get Cloud Composer resources.	composer.operations.list composer.operations.get composer.environments.list composer.environments.get	Project

The primitive roles **`Owner`**, **`Editor`**, and **`Viewer`** include permissions for other Google Cloud services, as well.

Permissions for common tasks

Roles are a collection of permissions. This section lists the roles or permissions required for common tasks.

Task	Permissions and/or roles
Access the IAP-protected Airflow web interface	composer.environments.get

Run Airflow CLI using the `gcloud` command-line tool	composer.environments.get container.clusters.getCredentials roles/container.developer
View the Environments page in the Cloud Console	composer.environments.list servicemanagement.projectSettings.get (/service-management/access-control#iam_permissions)
View Google Cloud's operations suite logs and metrics	roles/logging.viewer (/logging/docs/access-control#permissions_and_roles) roles/monitoring.viewer (/monitoring/access-control#predefined_roles)
Create an environment	composer.environments.create iam.serviceAccounts.actAs (on the service account under which the environment will run)
Update and delete an environment, including setting environment variables and installing/updating Python packages	environments.delete environments.update
Upload files to the DAGs and Plugins folders and access Airflow logs in the Logs folder	storage.objectAdmin (/storage/docs/access-control/iam-roles) assigned at the bucket or the project level composer.environments.get to look up the DAG destination bucket

Access control via `gcloud`

To assign predefined roles, execute the `gcloud projects get-iam-policy` (/sdk/gcloud/reference/projects/get-iam-policy) command to get the current policy, update the policy binding with either the `roles/composer.admin` (Composer Administrator) role or the `roles/composer.user` (Composer User) role, and then execute the `gcloud projects set-iam-policy` (/sdk/gcloud/reference/projects/set-iam-policy) command. See the Granting, Changing, and Revoking Access to Resources (/iam/docs/granting-changing-revoking-access) page of the IAM documentation for more information about assigning roles using `gcloud`.

To configure a custom role with Cloud Composer permissions, execute the `gcloud iam roles create` (/sdk/gcloud/reference/iam/roles/create) command, including the desired list of permissions from the roles table (#roles). Then, update the IAM policy with the newly configured custom role. See the Creating a custom role (/iam/docs/creating-custom-roles#creating_a_custom_role) page in the IAM documentation for more information.

Access control via the Cloud Console

You can use the Cloud Console to manage access control for your environments and projects.

To set access controls at the project level:

1. Open the IAM page (https://console.cloud.google.com/project/_/iam-admin/iam) in the Google Cloud Console.
2. Select your project, and click **Continue**.
3. Click **Add Member**.
4. Enter the email address of a new member to whom you have not granted any IAM role previously.
5. Select the desired role from the drop-down menu.
6. Click **Add**.
7. Verify that the member is listed under the role that you granted.

Last updated 2020-08-11 UTC.