Access Control

This page describes the access control options available to you for the Cloud Asset API.

Overview

Cloud Asset Inventory uses Identity and Access Management (/iam) (IAM) for access control.

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

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

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

Permissions and roles

This section summarizes Cloud Asset API permissions and roles that IAM supports.

Required permissions

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

Permission	API Methods
`cloudasset.assets.searchAllResources`	`*.searchAllResources`
`cloudasset.assets.searchAllIamPolicies`	`*.searchAllIamPolicies`
`cloudasset.assets.analyzeIamPolicy`	`*.analyzeIamPolicy`
	`*.exportIamPolicyAnalysis`

`cloudasset.feeds.get`	`*.getFeed`
`cloudasset.feeds.list`	`*.listFeeds`
`cloudasset.feeds.delete`	`*.deleteFeed`
`cloudasset.feeds.create`, `cloudasset.assets.exportResource` or `cloudasset.assets.exportIamPolicy` based on the `content_type`	`*.createFeed`
`cloudasset.feeds.update`, `cloudasset.assets.exportResource` or `cloudasset.assets.exportIamPolicy` based on the `content_type`	`*.updateFeed`
`cloudasset.assets.exportResource`, `cloudasset.assets.exportIamPolicy`, `cloudasset.assets.exportOrgPolicy` or `cloudasset.assets.exportAccessPolicy` based on the `content_type`	`*.batchGetAssetsHistory`
	`*.exportAssets`
	`*.operations.get`

Note that when using the `*.exportAssets` API to export resource metadata of specified asset types with `RESOURCE` or an unspecified content type, if the caller has not been granted the `cloudasset.assets.exportResource` permission, an alternative requirement is that caller has the appropriate per-resource-type permissions (/asset-inventory/docs/per-resource-type-permission) for every asset type that's specified in the request.

Roles

Cloud Asset Inventory has two IAM roles:

- Cloud Asset Owner (`roles/cloudasset.owner`), which grants full access to cloud asset metadata. It grants all `cloudasset.*` permissions.
- Cloud Asset Viewer (`roles/cloudasset.viewer`), which grants read-only access to cloud asset metadata. It grants all `cloudasset.assets.*` permissions (it does not grant `cloudasset.feeds.*` permissions).

Choose the appropriate role that contains the permissions necessary for your needs. In general, only the Cloud Asset Owner role grants all the required permissions (#required_permissions) to call the Cloud Asset API and allows full use of all methods.

Primitive roles (/iam/docs/understanding-roles#primitive_roles) include the following permissions:

- Owner role (`roles/owner`) grants all `cloudasset.*` permissions.
- Editor role (`roles/editor`) grants `cloudasset.assets.search*` and `cloudasset.assets.analyzeIamPolicy` permissions.
- Viewer role (`roles/viewer`) grants `cloudasset.assets.search*` and `cloudasset.assets.analyzeIamPolicy` permissions.

We recommend granting one of the Cloud Asset roles instead of a primitive role, because primitive roles contain many permissions for other Google Cloud services and may result in granting a larger access scope than intended.

Manage Access

You can grant roles to users at the organization, folder, or project level. See Granting, Changing, and Revoking Access to Project Members (/iam/docs/granting-changing-revoking-access#granting-console) for more information.

VPC Service Controls

VPC Service Controls can be used with Cloud Asset Inventory to provide additional security for your assets. To learn more about VPC Service Controls, see the VPC Service Controls overview (/vpc-service-controls/docs/overview).

To learn about the limitations in using Cloud Asset Inventory with VPC Service Controls, see the supported products and limitations (/vpc-service-controls/docs/supported-products).

Last updated 2020-08-05 UTC.