Access control examples

Example scenarios

The following examples involve a group of data scientists who all belong to a Google group (/iam/docs/overview#google_group) named AnalystGroup.

Read and write access to data in a dataset

CompanyProject is a project that includes dataset1 and dataset2. AnalystGroup1 is a group of data scientists who work only on dataset1 and AnalystGroup2 is a group that works only on dataset2. The data scientists should have full access only to the dataset that they work on, including access to run queries against the data.

Read and write access to a dataset

On dataset CompanyProject:dataset1	Grant AnalystGroup1 WRITER (/bigquery/docs/access-control-primitive-roles) access on dataset1. This role maps to the predefined IAM role: bigquery.dataEditor (/bigquery/docs/access-control#bigquery.dataEditor).
On dataset CompanyProject:dataset2	Grant AnalystGroup2 WRITER (/bigquery/docs/access-control-primitive-roles) access on dataset2. This role maps to the predefined IAM role: bigquery.dataEditor (/bigquery/docs/access-control#bigquery.dataEditor).
On project CompanyProject	Grant AnalystGroup1 and AnalystGroup2 bigquery.user (/bigquery/docs/access-control#bigquery.user) access on CompanyProject.

Giving the data scientists `WRITER` access at the dataset level gives them the ability to query data in the dataset's tables, but it does not give them permissions to run query jobs in the project. To be able to run query jobs against a dataset they've been given access to, the data scientist groups must be granted the project-level, predefined role: bigquery.user (/bigquery/docs/access-control#bigquery.user). The `bigquery.user` role grants `bigquery.jobs.create` permissions.

Alternatively, you can add the data scientist groups to a project-level, IAM <u>custom role</u>
(/bigquery/docs/access-control#custom_roles) that grants `bigquery.jobs.create` permissions.

Full access to data in a project

AnalystGroup is a group of data scientists working on BigQuery, responsible for all facets of its
use within a project named CompanyProject. The group prefers for all members to have read
and write access to all data. Other groups at the organization work with other Google Cloud
products, but no one else interacts with BigQuery. AnalystGroup does not use any other Google
Cloud services.

Full access to data in a project	
On project CompanyProject	Add AnalystGroup to the predefined role `bigquery.admin` (/bigquery/docs/access-control#bigquery.admin).

Full access across an organization

CompanyA is an organization that wants a specific person, named Admin1, to be the
administrator for all BigQuery data across all of their projects. MonitoringServiceAccount is a
<u>service account</u> (/iam/docs/overview#service_account) that's responsible for monitoring the size of
all the tables across all projects in the organization.

Full access across an organization	
On organization CompanyA	- Add Admin1 to the predefined role `bigquery.admin` (/bigquery/docs/access-control#bigquery.admin). - Add MonitoringServiceAccount to the predefined role `bigquery.dataViewer` (/bigquery/docs/access-control#bigquery.dataViewer).

If the company decides that MonitoringServiceAccount should also trim the size of tables that
exceed a certain size and remove data that is older than a specific time period,
MonitoringServiceAccount would need to be added to the predefined role `bigquery.user`
(/bigquery/docs/access-control#bigquery.user).

Read access to data in the same project

AnalystGroup is a set of data scientists responsible for analytics services within a project named CompanyProject. OperationsServiceAccount is a <u>service account</u> (/iam/docs/overview#service_account) that's responsible for loading application logs into BigQuery by using bulk load jobs to a specific CompanyProject:AppLogs dataset. The analysts are not allowed to modify the logs.

Read access to data in the same project

On project CompanyProject	• Add OperationsServiceAccount to the predefined role `bigquery.user` (/bigquery/docs/access-control#bigquery.user). • Add AnalystGroup to the predefined role `bigquery.user` (/bigquery/docs/access-control#bigquery.user).
On dataset CompanyProject:AppLogs	• Add OperationsServiceAccount to the predefined role `bigquery.dataEditor` (/bigquery/docs/access-control#bigquery.dataEditor). • Add AnalystGroup to the predefined role `bigquery.dataViewer` (/bigquery/docs/access-control#bigquery.dataViewer).

Read access to data in a different project

AnalystGroup is a set of data scientists responsible for analytics services within a project named CompanyAnalytics. The data they analyze, however, resides in a separate project named CompanyLogs. OperationsServiceAccount is a <u>service account</u> (/iam/docs/overview#service_account) that's responsible for loading application logs into BigQuery by using bulk load jobs to a variety of datasets in the CompanyLogs project.

AnalystGroup can only read data in the CompanyLogs project and cannot create additional storage or run any query jobs in that project. Instead, the analysts use project CompanyAnalytics to perform their work, and maintain their output within the CompanyAnalytics project.

Read access to data in a different project

On project CompanyLogs	• Add OperationsServiceAccount to the predefined role `bigquery.admin` (/bigquery/docs/access-control#bigquery.admin). • Add AnalystGroup to the predefined role `bigquery.dataViewer` (/bigquery/docs/access-control#bigquery.dataViewer).

Read access to data in a different project	
On project CompanyAnalytics	• Add AnalystGroup to the predefined role `bigquery.user` (/bigquery/docs/access-control#bigquery.user).

Additional information

The following topics provide more information about BigQuery access control.

- [Controlling access to datasets](/bigquery/docs/dataset-access-controls) (/bigquery/docs/dataset-access-controls)

- [Controlling access to tables and views](/bigquery/docs/table-access-controls) (/bigquery/docs/table-access-controls)

- [Restricting access with BigQuery Column-level security](/bigquery/docs/column-level-security) (/bigquery/docs/column-level-security)