This page provides supplemental information for using Cloud Audit Logs (/logging/docs/audit) with Cloud Storage. Use Cloud Audit Logs to generate logs for API operations performed in Cloud Storage. To set up Cloud Audit Logs, see Configuring Data Access Logs (/logging/docs/audit/configure-data-access).

Cloud Audit Logs is separate from Cloud Storage Access Logs (/storage/docs/access-logs). Both features provide ation about who accesses your Cloud Storage resources, but Cloud Audit Logs is the recommended method for doin age/docs/access-logs#should-you-use).

Within Cloud Audit Logs, there are two types of logs:

- **Admin Activity logs** (/logging/docs/audit#admin-activity): Entries for operations that modify the configuration or metadata of a project, bucket, or object.
- **Data Access logs** (/logging/docs/audit#data-access): Entries for operations that modify objects or read a project, bucket, or object. There are several sub-types of data access logs:
    - `ADMIN_READ`: Entries for operations that read the configuration or metadata of a project, bucket, or object.
    - `DATA_READ`: Entries for operations that read an object.
    - `DATA_WRITE`: Entries for operations that create or modify an object.

The following table summarizes which Cloud Storage operations fall into each log type:

Log entry type	Sub-type	Operations
Admin Activity		• Creating buckets • Deleting buckets • Setting/changing IAM policies • Setting/changing object ACLs[3] • Updating bucket metadata

Log entry type	Sub-type	Operations
Data Access	`ADMIN_READ`	• Getting bucket metadata • Getting IAM policies • Getting object ACLs • Listing buckets
	`DATA_READ`	• Getting object data • Getting object metadata • Listing objects • Copying/composing objects[1]
	`DATA_WRITE`	• Creating objects • Deleting objects[2] • Updating non-ACL object metadata[2] • Copying/composing objects[1]

[1] Copying and composing are non-atomic: they each read and write data. As a result, they generate two log entries.

[2] Cloud Audit Logs does not log actions taken by the Object Lifecycle Management (/storage/docs/lifecycle) feature. For alternatives that track these actions, see Options for tracking Lifecycle actions (/storage/docs/lifecycle#tracking).

[3] If an object ACL is set to public, Admin Activity audit logs are not written for any updates to that object ACL.

Cloud Storage logs use an `AuditLog` (/logging/docs/reference/audit/auditlog/rest/Shared.Types/AuditLog) object and follow the same format as other Cloud Audit Logs logs. Logs contain information such as:

- The user who made the request, including the email address of that user.
- The resource name on which the request was made.
- The outcome of the request.

Logs pertaining to Cloud Storage operations are generated by the service `storage.googleapis.com`.

Admin Activity logs are recorded by default. These logs do not count towards your log ingestion quota (/logging/quotas).

Data Access logs pertaining to Cloud Storage operations are not recorded by default. To learn how to enable logs for data access-type operations, see Configuring Data Access Logs (/logging/docs/audit/configure-data-access). Note that unlike Admin Activity logs, Data Access logs count towards your log ingestion quota and can affect your logging charges in Stackdriver (/stackdriver/pricing_v2).

Data Access log generation is primarily driven as a part of the IAM validation process. To ensure that audit logs are
ated for all data access operations, grant users access to objects using IAM permissions, such as **`storage.objects`**
Access Control Lists (ACLs) (/storage/docs/access-control/lists), or the **`OWNER`/`EDITOR`/`VIEWER`** IAM roles
age/docs/projects#permissions), which can use ACLs, may result in some data access operations not being recorde

The following users can view Admin Activity logs:

- Project owners, editors, and viewers (/iam/docs/understanding-roles#primitive_roles).
- Users with the Logs Viewer (/logging/docs/access-control) IAM role.
- Users with the `logging.logEntries.list` IAM permission (/iam/docs/overview).

The following users can view Data Access logs:

- Project owners.
- Users with the Private Logs Viewer (/logging/docs/access-control) IAM role.
- Users with the `logging.privateLogEntries.list` IAM permission.

See Adding IAM members to a project (/storage/docs/access-control/using-iam-permissions#project-add) for instructions on granting access.

Access Control Lists (ACLs) (/storage/docs/access-control/lists) cannot be used to grant users access to Admin Ac
a Access logs.

Logs pertaining to Cloud Storage are categorized under the resource type `GCS bucket`.

You can view a summary of the audit logs for your project in the Activity Stream (https://console.cloud.google.com/home/activity) in the Google Cloud Console. A more detailed version of the logs can found in the Logs Viewer (https://console.cloud.google.com/logs/viewer).

For instructions on filtering logs in the Logs Viewer, see the Cloud Audit Logs guide (/logging/docs/view/logs_viewer).

Cloud Audit Logs uses standard log names for all audit logs. For information on the structure of log names, as well as examples of using log names as log result filters, see Viewing audit logs (/logging/docs/audit#viewing_audit_logs).

The following restrictions apply to Cloud Audit Logs with Cloud Storage:

- Cloud Audit Logs does not track access to public objects.
- Cloud Audit Logs does not track changes made by the Object Lifecycle Management (/storage/docs/lifecycle) feature.
- You cannot use authenticated browser downloads (/storage/docs/request-endpoints#cookieauth) to access objects when Cloud Audit Logs Data Access logs are enabled (/logging/docs/audit/configure-data-access) on the bucket containing the objects.

- Try the Exporting Stackdriver Logging (/solutions/exporting-stackdriver-logging-for-compliance-requirements) tutorial.