Understanding audit logs

Send feedback

This page describes Cloud Audit Logs log entries in detail: their structure, how to read them, and how to interpret them.

Cloud Audit Logs provides the following audit logs for each Google Cloud project, folder, and organization:

- Admin Activity audit logs
- Data Access audit logs
- System Event audit logs
- Policy Denied audit logs

For a general overview of Cloud Audit Logs, see Cloud Audit Logs.

Format of audit log entries

An audit log entry is a type of Cloud Logging log entry. Like all Logging log entries, an audit log entry is stored in a `LogEntry` object. What distinguishes an audit log entry from other log entries is the `protoPayload` field. In audit log entries, the log entry's `protoPayload` field contains an `AuditLog` object that stores the audit logging data.

Mapping services to resources.

- A payload, which is the `protoPayload` type. The payload of each audit log entry is an object of type `AuditLog`, which defines a set of fields specific to Cloud Audit Logs, such as `serviceName` and `authenticationInfo`. It also has an optional field, `metadata`, that Google Cloud services use to list service-specific information in the audit log entry. Some Google Cloud services still use the older `serviceData` field to list service-specific information. For a list of services that use the `serviceData` field, see Service-specific audit data.
- A log name: Audit log entries belong to logs within projects, folders, and organizations. The log names are listed below:

```
projects/PROJECT_ID/logs/cloudaudit.googleapis.com%2Factivity
projects/PROJECT_ID/logs/cloudaudit.googleapis.com%2Fdata_access
projects/PROJECT_ID/logs/cloudaudit.googleapis.com%2Fsystem_even
projects/PROJECT_ID/logs/cloudaudit.googleapis.com%2Fpolicy

folders/FOLDER_ID/logs/cloudaudit.googleapis.com%2Factivity
folders/FOLDER_ID/logs/cloudaudit.googleapis.com%2Fdata_access
folders/FOLDER_ID/logs/cloudaudit.googleapis.com%2Fsystem_event
folders/FOLDER_ID/logs/cloudaudit.googleapis.com%2Fpolicy

billingAccounts/BILLING_ACCOUNT_ID/logs/cloudaudit.googleapis.co
billingAccounts/BILLING_ACCOUNT_ID/logs/cloudaudit.googleapis.co
billingAccounts/BILLING_ACCOUNT_ID/logs/cloudaudit.googleapis.co
billingAccounts/BILLING_ACCOUNT_ID/logs/cloudaudit.googleapis.co

organizations/ORGANIZATION_ID/logs/cloudaudit.googleapis.com%2Fa
organizations/ORGANIZATION_ID/logs/cloudaudit.googleapis.com%2Fd
organizations/ORGANIZATION_ID/logs/cloudaudit.googleapis.com%2Fs
organizations/ORGANIZATION_ID/logs/cloudaudit.googleapis.com%2Fp
```

Within a project, folder, or organization, these log names are typically abbreviated **activity**, **data_access**, **system_event**, and **policy**.

Sample audit log entry

This section uses a sample audit log entry to explain how to find the most important information in audit log entries.

```
    request: {
      resource: "my-gcp-project-id",
      policy: { bindings: [...], }
    },
    response: {
      bindings: [
        {
          role: "roles/logging.privateLogViewer",
          members: [ "user:user@example.com" ]
        }
      ],
    }
  },
  insertId: "53179D9A9B559.AD6ACC7.B40604EF",
  resource: {
    type: "gae_app",
    labels: { project_id: "my-gcp-project-id" }
  },
    timestamp: "2019-05-27T16:24:56.135Z",
    severity: "NOTICE",
    logName: "projects/my-gcp-project-id/logs/cloudaudit.googleapis
}
```

Here is the query that was used to select the audit log entry sample above. It can be used in the Logs Explorer, Logging API, or Google Cloud CLI. The project identifier is in the log's name, and the query is fast because the `logName` field is indexed:

```
resource.type = "gae_app"
logName = "projects/PROJECT_ID/logs/cloudaudit.googleapis.com%2
```

If you are looking for audit logs from a single instance of a resource type, such as `gce_instance`, add an instance qualifier:

```
resource.type = "gce_instance"
resource.instance_id = "INSTANCE_ID"
logName = "projects/PROJECT_ID/logs/cloudaudit.googleapis.com%2
```

Interpreting the sample audit log entry

in `protoPayload.serviceData`.

- **What resource is being audited?** An application running in App Engine, associated with a Google Cloud project `my-gcp-project-id`, is being audited. You can determine this from the `resource` field, which specifies the resource type `gae_app` and the project identifier `my-gcp-project-id`. In this example, you would find details on the resource type in the monitored resource type list.

For more information, see the `LogEntry` type, the `AuditLog` type, and the IAM `AuditData` type.

Audit logs for long-running operations

APIs that are long-running operations emit two audit logs; one when the API is called and the operation starts, and one when the operation completes.

In this case, the `LogEntry` object contains an `operation` field. Log entries for the same operation have the same value for both `LogEntry.operation.id` and `LogEntry.operation.producer`. The first log written has `LogEntry.operation.first=true`, and the completion log has `LogEntry.operation.last=true`.

In cases where the operation completes immediately, there is only one log containing both `LogEntry.operation.first=true` and `LogEntry.operation.last=true`.

These APIs implement the Operations service. This service generally emit audit logs when called. Depending on which APIs are called, `protoPayload.methodName` is one of the following:

- `google.longrunning.Operations.ListOperations`
- `google.longrunning.Operations.GetOperation`
- `google.longrunning.Operations.CancelOperation`
- `google.longrunning.Operations.WaitOperation`
- `google.longrunning.Operations.DeleteOperation`

`LogEntry.operation` isn't specified in this case, as this API returns metadata about long-running operations, but is not a long-running

Service-specific audit data

Some services extend the information stored in their `AuditLog` by placing a supplementary data structure in the audit log's `serviceData` field. The following table lists the services that use `serviceData` field and provides a link to their `AuditData` type.

Service	Service data type
App Engine	`type.googleapis.com/google.appengine.v1.AuditData`
App Engine (legacy)	`type.googleapis.com/google.appengine.legacy.AuditData`
BigQuery	`type.googleapis.com/google.cloud.bigquery.logging.v1.A`
IAM	`type.googleapis.com/google.iam.v1.logging.AuditData`

Viewing audit logs

You can query for all audit logs or you can query for logs by their audit log name. The audit log name includes the resource identifier of the Google Cloud project, folder, billing account, or organization for which you want to view audit logging information. Your queries can specify indexed `LogEntry` fields, and if you use the **Log Analytics** page, which supports SQL queries, then you can view your query results as a chart.

For more information about querying your logs, see the following pages:

- Build queries in the Logs Explorer.
- Query and view logs in Log Analytics.
- Sample queries for security insights.

You can view audit logs in Cloud Logging by using the Google Cloud console, the Google Cloud CLI, or the Logging API.

Console gcloud API

```
logName:"cloudaudit.googleapis.com"
```

```
protoPayload."@type"="type.googleapis.com/google.c
```

4. To display the audit logs for a specific resource and audit log type, in the **Query builder** pane, do the following:
   - In **Resource type**, select the Google Cloud resource whose audit logs you want to see.
   - In **Log name**, select the audit log type that you want to see:
     - For Admin Activity audit logs, select **activity**.
     - For Data Access audit logs, select **data_access**.
     - For System Event audit logs, select **system_event**.
     - For Policy Denied audit logs, select **policy**.
   - Click **Run query**.

   If you don't see these options, then there aren't any audit logs of that type available in the Google Cloud project, folder, or organization.

   If you're experiencing issues when trying to view logs in the Logs Explorer, see the troubleshooting information.

   For more information about querying by using the Logs Explorer, see Build queries in the Logs Explorer. For information about summarizing log entries in the Logs Explorer by using Gemini, see Summarize log entries with Gemini assistance.