



Contact Us

Start free

Google Cloud Observability > Logging > Documentation > Guides

Was this helpful?  

# Understanding audit logs



Send feedback

## On this page

Format of audit log entries

Sample audit log entry

Interpreting the sample audit log entry

Audit logs for long-running operations

Audit logs for streaming APIs

Service-specific audit data

Viewing audit logs

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

Contact Us

Start free

In short, every audit log entry is characterized by the following information:

- The project, folder, or organization that owns the log entry.
- The resource to which the log entry applies. This information consists of a resource type from the [Monitored resource list](#) and additional values that denote a specific instance. For example, you can view audit log entries from a single Compute Engine VM instance or from all VM instances.
- A timestamp.
- A service: Services are individual Google Cloud products, such as Compute Engine, Cloud SQL, or Pub/Sub. Each service is identified by name: Compute Engine is `compute.googleapis.com`, Cloud SQL is `cloudsql.googleapis.com`, and so forth. This information is listed in the `protoPayload.serviceName` field of the audit log entry.

Resource types belongs to a single service, but a service can have several resource types. For a list of services and resources, go to [Mapping services to resources](#).

Contact Us

Start free

```
billingAccounts/BILLING_ACCOUNT_ID /logs/cloudaudit.googleapis.com%2Factivity  
billingAccounts/BILLING_ACCOUNT_ID /logs/cloudaudit.googleapis.com%2Fsystem_e  
billingAccounts/BILLING_ACCOUNT_ID /logs/cloudaudit.googleapis.com%2Fpolicy  
  
organizations/ORGANIZATION_ID /logs/cloudaudit.googleapis.com%2Factivity  
organizations/ORGANIZATION_ID /logs/cloudaudit.googleapis.com%2Fdata_access  
organizations/ORGANIZATION_ID /logs/cloudaudit.googleapis.com%2Fsystem_event  
organizations/ORGANIZATION_ID /logs/cloudaudit.googleapis.com%2Fpolicy
```

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.

Contact Us

Start free

```
,
  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"
```

Contact Us

Start free

## Interpreting the sample audit log entry

In the [audit log entry sample](#) above, the `protoPayload`, `insertId`, `resource`, `timestamp`, `severity` and `logName` fields shown are part of the `LogEntry` object. The value of the `protoPayload` field is an `AuditLog` object. It encapsulates the audit logging data.

Looking at the audit log entry sample above, you might have some questions:

- **Is this an audit log entry?** It is, which you can tell in two ways:
  - The `protoPayload.@type` field is `type.googleapis.com/google.cloud.audit.AuditLog`.
  - The `logName` field includes the domain `cloudaudit.googleapis.com`.
- **What service wrote the audit log?** The log was written by App Engine. This

Contact Us

Start free

`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`

Contact Us

Start free

## 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          | <a href="#">type.googleapis.com/google.appengine.v1.AuditData</a>              |
| App Engine (legacy) | <a href="#">type.googleapis.com/google.appengine.legacy.AuditData</a>          |
| BigQuery            | <a href="#">type.googleapis.com/google.cloud.bigquery.logging.v1.AuditData</a> |
| IAM                 | <a href="#">type.googleapis.com/google.iam.v1.logging.AuditData</a>            |

Contact Us

Start free

In the Google Cloud console, you can use the Logs Explorer to retrieve your audit log entries for your Google Cloud project, folder, or organization:

★ **Note:** You can't view audit logs for Cloud Billing accounts in the Google Cloud console. You must use the API or the gcloud CLI.

1. In the Google Cloud console, go to the **Logs Explorer** page:

Go to Logs Explorer

If you use the search bar to find this page, then select the result whose subheading is **Logging**.

2. Select an existing Google Cloud project, folder, or organization.
3. To display all audit logs, enter either of the following queries into the query-editor field, and then click **Run query**:



Contact Us

Start free

- 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](#).

Was this helpful?



[Send feedback](#)



[Sign in](#)

[Contact Us](#)

[Start free](#)

[Analyst reports](#)

[Whitepapers](#)

[Blog](#)

[Industry solutions](#)

[DevOps solutions](#)

[Small business solutions](#)

[See all solutions](#)

[Cloud Architecture Center](#)

[Training](#)

[Certifications](#)

[Google for Developers](#)

[Google Cloud for Startups](#)

[System status](#)

[Release Notes](#)

[Learn on YouTube](#)


[Follow on X](#)

[Join User Research](#)

[We're hiring. Join Google Cloud!](#)

[Google Cloud Community](#)

[About Google](#) | [Privacy](#) | [Site terms](#) | [Google Cloud terms](#)

 [Our third decade of climate action: join us](#)

Sign up for the Google Cloud newsletter

[Subscribe](#)



Language ▼

cloud.google.com uses cookies from Google to deliver and enhance the quality of its services and to analyze traffic. [Learn more.](#)