Understanding audit logs

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 (/logging/docs/audit).

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` (/logging/docs/reference/v2/rest/v2/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` (/logging/docs/audit/api/ref/rest/Shared.Types/AuditLog) object that stores the audit logging data.

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 (/logging/docs/api/v2/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 (/logging/docs/api/v2/resource-list#service-names).

- A payload, which is the **protoPayload** type. The payload of each audit log entry is an object of type **AuditLog** (/logging/docs/audit/api/ref/rest/Shared.Types/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 (#servicedata-services).
- A log name: Audit log entries belong to logs within billing accounts, projects, folders, and organizations. The following table lists log names:

```
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_event
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.com%2Factivit
billingAccounts/BILLING_ACCOUNT_ID/logs/cloudaudit.googleapis.com%2Fdata_ac
billingAccounts/BILLING_ACCOUNT_ID/logs/cloudaudit.googleapis.com%2Fsystem_
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 billing account, project, folder, or organization, these log names are typically abbreviated as **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.

The following sample is an Admin Activity audit log entry written by App Engine (/appengine/docs) to record a change to an Identity and Access Management (IAM) policy with *PROJECT_ID* `my-gcp-project-id`. For brevity, some parts of the log entry are omitted, and some fields are highlighted:

```
{
  protoPayload: {
    @type: "type.googleapis.com/google.cloud.audit.AuditLog",
    status: {},
    authenticationInfo: {
      principalEmail: "user@example.com"
    },
    serviceName: "appengine.googleapis.com",
    methodName: "SetIamPolicy",
    authorizationInfo: [...],
    serviceData: {
      @type: "type.googleapis.com/google.appengine.legacy.AuditData",
      policyDelta: { bindingDeltas: [
          action: "ADD",
          role: "roles/logging.privateLogViewer",
          member: "user:user@example.com"
      ], }
    },
    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.com%2Facti
  }
```

Here is the query that was used to select the previous audit log entry sample. The query can be used in the Logs Explorer, Logging API, or Google Cloud CLI. The project identifier is in the log's name:

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

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%2Factivity"
```

Interpreting the sample audit log entry

In the previous audit log entry sample (#sample), the **protoPayload**, **insertId**, **resource**, **timestamp**, **severity** and **logName** fields shown are part of the **LogEntry** (/logging/docs/reference/v2/rest/v2/LogEntry) object. The value of the **protoPayload** field is an **AuditLog** (/logging/docs/audit/api/ref/rest/Shared.Types/AuditLog) object. It encapsulates the audit logging data.

Looking at the audit log entry sample, 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 information is listed in the `protoPayload.serviceName` field of the audit log entry.
- **What operation is being audited?** `SetIamPolicy`, as specified in the `protoPayload.methodName` field, is being audited. More information about the audited operation is in the `AuditData` object 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 (/logging/docs/api/v2/resource-list).

For more information, see the `LogEntry` type (/logging/docs/reference/v2/rest/v2/LogEntry), the `AuditLog` type (/logging/docs/audit/api/ref/rest/Shared.Types/AuditLog), and the IAM `AuditData` type (/logging/docs/audit/api/ref/rest/Shared.Types/AuditData).

Audit logs for long-running operations

APIs that are long-running operations (https://google.aip.dev/151) 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` (/logging/docs/reference/v2/rest/v2/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 entry that was written has `LogEntry.operation.first=true`, and the completion log entry has `LogEntry.operation.last=true`.

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

Some services don't populate the `LogEntry.operation` field when the operation fails. However, you can determine which operations are long-running operations by referring to the service's audit logging documentation (/logging/docs/audit/services).

These APIs implement the Operations (https://github.com/googleapis/googleapis/blob/master/google/longrunning/operations.proto) service. This service generally emit audit log entries 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 operation itself.

See Google Cloud services with audit logs (/logging/docs/audit/services) for details about which APIs are audited, as it can vary per service.

Audit logs for streaming APIs

Similar to long-running operations, streaming APIs emit two audit log entries; one when the API is first called and one when the streaming connection has ended.

In this case, the `LogEntry` (/logging/docs/reference/v2/rest/v2/LogEntry) object contains an `operation` field and 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 will have `LogEntry.operation.last=true`.

This API may also emit continuation log entries with neither `LogEntry.operation.first` nor `LogEntry.operation.last` set to indicate that the stream remains open.

Service-specific audit data

Some services extend the information stored in their `AuditLog` (/logging/docs/audit/api/ref/rest/Shared.Types/AuditLog) by placing a supplementary data structure in the audit log entry'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 (/appengine/docs)	`type.googleapis.com/google.appengine.v1.AuditData` (/logging/docs/audit/api/ref_gae4/rest/Shared.Types/AuditData)
App Engine (Legacy) (/appengine/docs)	`type.googleapis.com/google.appengine.legacy.AuditData` (/logging/docs/audit/api/ref_gaeL/rest/Shared.Types/AuditData)
BigQuery (/bigquery/docs)	`type.googleapis.com/google.cloud.bigquery.logging.v1.AuditData` (/logging/docs/audit/api/ref_bq/rest/Shared.Types/AuditData)
IAM (/iam/docs)	`type.googleapis.com/google.iam.v1.logging.AuditData` (/logging/docs/audit/api/ref/rest/Shared.Types/AuditLog)

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 (/resource-manager/docs/creating-managing-projects#identifying_projects) 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` (/logging/docs/reference/v2/rest/v2/LogEntry) fields. For more information about querying your logs, see Build queries in the Logs Explorer (/logging/docs/view/building-queries)

The Logs Explorer lets you view filter individual log entries. If you want to use SQL to analyze groups of log entries, then use the **Log Analytics** page. For more information, see:

- Query and view logs in Log Analytics (/logging/docs/analyze/query-and-view).
- Sample queries for security insights (/logging/docs/analyze/analyze-audit-logs).
- Chart query results (/logging/docs/analyze/charts).

Most audit logs can be viewed in Cloud Logging by using the Google Cloud console, the Google Cloud CLI, or the Logging API. However, for audit logs related to billing, you can only use the Google Cloud CLI or the Logging API.

Consolegcloud (#gcloud)REST (#rest)
(#console)

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 (https://console.cloud.google.com/logs/query)

   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**:

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

```
protoPayload."@type"="type.googleapis.com/google.cloud.audit.AuditLog'
```

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 (/logging/docs/view/logs-explorer-interface#troubleshooting) information.

For more information about querying by using the Logs Explorer, see Build queries in the Logs Explorer (/logging/docs/view/building-queries).

Last updated 2025-04-30 UTC.