Security & Identity Products (https://cloud.google.com/products/security/)
Resource Manager (https://cloud.google.com/resource-manager/)
Documentation (https://cloud.google.com/resource-manager/docs/) Guides

Resource Manager audit logging information

This page describes the audit logs created by Resource Manager as part of Cloud Audit Logs (https://cloud.google.com/logging/docs/audit/).

Overview

Google Cloud services write audit logs to help you answer the questions, "Who did what, where, and when?" Your Google Cloud projects each contain only the audit logs for resources that are directly within the project. Other entities, such as folders, organizations, and billing accounts, each contain the audit logs for the entity itself.

For a general overview of Cloud Audit Logs, go to Cloud Audit Logs (https://cloud.google.com/logging/docs/audit/). For a deeper understanding of Cloud Audit Logs, review Understanding audit logs (https://cloud.google.com/logging/docs/audit/understanding-audit-logs).

Cloud Audit Logs maintains three audit logs for each Google Cloud project, folder, and organization:

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

Resource Manager writes **Admin Activity** audit logs, which record operations that modify the configuration or metadata of a resource. You can't disable Admin Activity audit logs.

Only if explicitly enabled, Resource Manager writes **Data Access** audit logs. Data Access audit logs contain API calls that read the configuration or metadata of resources, as well as user-driven API calls that create, modify, or read user-provided resource data. Data Access audit logs do not record the data-access operations on resources that are publicly shared (available to **All Users** or **All Authenticated Users**) or that can be accessed without logging into Google Cloud.

Resource Manager doesn't write **System Event** audit logs.

Audited operations

The following summarizes which API operations correspond to each audit log type in Resource Manager:

Audit logs category	Resource Manager operations
Admin Activity logs (ADMIN_WRITE)	• `UpdateContactInfo` v2beta1: • `cloudresourcemanager.v2beta1.folders.create` • `cloudresourcemanager.v2beta1.folders.delete` • `cloudresourcemanager.v2beta1.folders.move` • `cloudresourcemanager.v2beta1.folders.patch` • `cloudresourcemanager.v2beta1.folders.setIamPolicy` • `cloudresourcemanager.v2beta1.folders.undelete` v2: • `cloudresourcemanager.v2.folders.create` • `cloudresourcemanager.v2.folders.delete` • `cloudresourcemanager.v2.folders.move` • `cloudresourcemanager.v2.folders.patch` • `cloudresourcemanager.v2.folders.setIamPolicy` • `cloudresourcemanager.v2.folders.undelete` v1beta1: • `cloudresourcemanager.v1beta1.organizations.setIamPolicy` • `cloudresourcemanager.v1beta1.organizations.update` • `cloudresourcemanager.v1beta1.projects.create` • `cloudresourcemanager.v1beta1.projects.delete` • `cloudresourcemanager.v1beta1.projects.setIamPolicy` • `cloudresourcemanager.v1beta1.projects.undelete` • `cloudresourcemanager.v1beta1.projects.update` v1:

Audit logs category	Resource Manager operations
	• `cloudresourcemanager.v1.folders.clearOrgPolicy` • `cloudresourcemanager.v1.folders.setOrgPolicy` • `cloudresourcemanager.v1.organizations.clearOrgPolicy` • `cloudresourcemanager.v1.organizations.setIamPolicy` • `cloudresourcemanager.v1.organizations.setOrgPolicy` • `cloudresourcemanager.v1.projects.clearOrgPolicy` • `cloudresourcemanager.v1.projects.create` • `cloudresourcemanager.v1.projects.delete` • `cloudresourcemanager.v1.projects.setIamPolicy` • `cloudresourcemanager.v1.projects.setOrgPolicy` • `cloudresourcemanager.v1.projects.undelete` • `cloudresourcemanager.v1.projects.update`
Data Access logs (ADMIN_READ)	• `GetContactInfo` v2beta1: • `cloudresourcemanager.v2beta1.folders.get` • `cloudresourcemanager.v2beta1.folders.getIamPolicy` • `cloudresourcemanager.v2beta1.folders.list` v2: • `cloudresourcemanager.v2.folders.get` • `cloudresourcemanager.v2.folders.getIamPolicy` • `cloudresourcemanager.v2.folders.list` v1beta1: • `cloudresourcemanager.v1beta1.organizations.get` • `cloudresourcemanager.v1beta1.organizations.getIamPolicy` • `cloudresourcemanager.v1beta1.projects.get` • `cloudresourcemanager.v1beta1.projects.getIamPolicy` v1:

Audit logs category	Resource Manager operations
	• `cloudresourcemanager.v1.folders.getEffectiveOrgPolicy` • `cloudresourcemanager.v1.folders.getOrgPolicy` • `cloudresourcemanager.v1.folders.listAvailableOrgPolicyConstraints` • `cloudresourcemanager.v1.folders.listOrgPolicies` • `cloudresourcemanager.v1.organizations.get` • `cloudresourcemanager.v1.organizations.getEffectiveOrgPolicy` • `cloudresourcemanager.v1.organizations.getIamPolicy` • `cloudresourcemanager.v1.organizations.getOrgPolicy` • `cloudresourcemanager.v1.organizations.listAvailableOrgPolicyConstrain` • `cloudresourcemanager.v1.organizations.listOrgPolicies` • `cloudresourcemanager.v1.projects.get` • `cloudresourcemanager.v1.projects.getEffectiveOrgPolicy` • `cloudresourcemanager.v1.projects.getIamPolicy` • `cloudresourcemanager.v1.projects.listAvailableOrgPolicyConstraints` • `cloudresourcemanager.v1.projects.listOrgPolicies`

The `GetContactInfo` and `UpdateContactInfo` operations support the `ContactInfo` service for the EU General Data Protection Regulation (GDPR). These operations update and retrieve contact information for an EU Representative and a Data Protections Officer, which can be modified in the Google Cloud Console on the Google Cloud Privacy & Security (https://console.cloud.google.com/iam-admin/privacy) page.

Audit log format

Audit log entries—which can be viewed in Stackdriver Logging using the Logs Viewer, the Stackdriver Logging API, or the `gcloud` command-line tool—include the following objects:

- The log entry itself, which is an object of type `LogEntry` (https://cloud.google.com/logging/docs/reference/v2/rest/v2/LogEntry). Useful fields include the following:
    - `logName` contains the project identification and audit log type

    - `resource` contains the target of the audited operation
    - `timeStamp` contains the time of the audited operation
    - `protoPayload` contains the audited information
- The audit logging data, which is an [`AuditLog`](https://cloud.google.com/logging/docs/reference/audit/auditlog/rest/Shared.Types/AuditLog) (https://cloud.google.com/logging/docs/reference/audit/auditlog/rest/Shared.Types/AuditLog) object held in the `protoPayload` field of the log entry.
- Optional service-specific audit information, which is a service-specific object held in the `serviceData` field of the `AuditLog` object. For details, go to Service-specific audit data (https://cloud.google.com/logging/docs/audit/api/#servicedata-services).

For other fields in these objects, plus how to interpret them, review Understanding audit logs (https://cloud.google.com/logging/docs/audit/understanding-audit-logs).

Log name

Cloud Audit Logs resource names indicate the project or other entity that owns the audit logs, and whether the log contains Admin Activity, Data Access, or System Event audit logging data. For example, the following shows log names for a project's Admin Activity audit logs and an organization's Data Access audit logs:

```
projects/[PROJECT_ID]/logs/cloudaudit.googleapis.com%2Factivity
organizations/[ORGANIZATION_ID]/logs/cloudaudit.googleapis.com%2Fdata_access
```

Note: The part of the log name following `/logs/` must be URL-encoded. This means that the forward-slash character, `/`, must be written as `%2F`.

Service name

Resource Manager audit logs use the service name `cloudresourcemanager.googleapis.com`.

For more details on logging services, go to Mapping services to resources (https://cloud.google.com/logging/docs/api/v2/resource-list#service-names).

Resource types

Resource Manager audit logs use the resource type `project` for all audit logs.

For a full list, go to Monitored resource types (https://cloud.google.com/monitoring/api/resources).

Enabling audit logging

Admin Activity audit logs are always enabled; you can't disable them.

Data Access audit logs are disabled by default and aren't written unless explicitly enabled (the exception is Data Access audit logs for BigQuery, which cannot be disabled).

For instructions on enabling some or all of your Data Access audit logs, go to Configuring Data Access logs (https://cloud.google.com/logging/docs/audit/configure-data-access).

The Data Access audit logs that you configure can affect your logs pricing in Stackdriver. Review the Pricing (#pricing) section on this page.

Audit log permissions

Cloud Identity and Access Management permissions and roles determine which audit logs you can view or export. Logs reside in projects and in some other entities including organizations, folders, and billing accounts. For more information, go to Understanding roles (https://cloud.google.com/iam/docs/understanding-roles).

To view Admin Activity audit logs, you must have one of the following Cloud IAM roles in the project that contains your audit logs:

- **Project Owner**, **Project Editor**, or **Project Viewer**.
- Logging's **Logs Viewer** (https://cloud.google.com/logging/docs/access-control#permissions_and_roles) role.
- A custom Cloud IAM role (https://cloud.google.com/iam/docs/creating-custom-roles) with the `logging.logEntries.list` Cloud IAM permission.

To view Data Access audit logs, you must have one of the following roles in the project that contains your audit logs:

- **Project Owner** (https://cloud.google.com/iam/docs/understanding-roles#primitive_roles).

- Logging's **Private Logs Viewer** (https://cloud.google.com/logging/docs/access-control#permissions_and_roles) role.
- A custom Cloud IAM role (https://cloud.google.com/iam/docs/creating-custom-roles) with the `logging.privateLogEntries.list` Cloud IAM permission.

If you are using audit logs from a non-project entity, such as an organization, then change the **Project** roles to suitable organization roles.

Viewing logs

You have several options for viewing your audit log entries:

BASIC VIEWER ADVANCED VIEWER MORE

You can use the Logs Viewer basic interface in the Cloud Console to retrieve your audit log entries. Do the following:

1. Go to the **Stackdriver Logging > Logs** (Logs Viewer) page in the Cloud Console:

   GO TO THE LOGS VIEWER PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/LOGS/VIEWER)

2. Select an existing Google Cloud project at the top of the page, or create a new project.
3. In the first drop-down menu, select the resource type whose audit logs you wish to view. You can select a specific resource or `Global` for all resources.
4. In the second drop-down menu, select the log type you want to view: `activity` for Admin Activity audit logs,`data_access` for Data Access audit logs, and `system_events` for System Event audit logs.

   If none of these options are displayed, then there are no audit logs of that type available in the project.

Note: You can't view folder and organization logs using the Logs Viewer. To read log entries associated with the specified folder or organization, rather than the default project, use the Stackdriver Logging API method entries.list (https://cloud.google.com/logging/docs/reference/v2/rest/v2/entries/list) or go to Reading log entries (https://cloud.google.com/logging/docs/reference/tools/gcloud-logging#reading_log_entries) using the `gcloud` command-line tool.

For a sample audit log entry and how to find the most important information in it, go to Understanding audit logs (https://cloud.google.com/logging/docs/audit/understanding-audit-logs).

Exporting audit logs

You can export audit logs in the same way you export other kinds of logs. For details about how to export your logs, go to Exporting logs (https://cloud.google.com/logging/docs/export). Here are some applications of exporting audit logs:

- To keep audit logs for a longer period of time or to use more powerful search capabilities, you can export copies of your audit logs to Cloud Storage, BigQuery, or Pub/Sub. Using Pub/Sub, you can export to other applications, other repositories, and to third parties.
- To manage your audit logs across an entire organization, you can create aggregated export sinks (https://cloud.google.com/logging/docs/export/aggregated_exports) that can export logs from any or all projects in the organization.
- If your enabled Data Access audit logs are pushing your projects over their logs allotments, you can export and exclude the Data Access audit logs from Logging. For details, go to Excluding logs (https://cloud.google.com/logging/docs/exclusions).

Pricing

Stackdriver Logging does not charge you for audit logs that cannot be disabled, including all Admin Activity audit logs. Stackdriver Logging charges you for Data Access audit logs that you explicitly request.

For more information on audit logs pricing, review Stackdriver pricing (https://cloud.google.com/stackdriver/pricing).

Last updated December 4, 2019.