Viewing OS Config audit logs

ature is covered by the Pre-GA Offerings Terms (/terms/service-terms#1) of the Google Cloud Platform Terms
. Pre-GA features may have limited support, and changes to pre-GA features may not be compatible with othe
sions. For more information, see the launch stage descriptions (/products#product-launch-stages).

This page describes the audit logs created by OS Config as part of Cloud Audit Logs (/logging/docs/audit).

Overview

Google Cloud services write audit logs to help you answer the questions, "Who did what, where, and when?" Your Cloud project 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 (/logging/docs/audit). For a deeper understanding of Cloud Audit Logs, review Understanding audit logs (/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

Only if explicitly enabled, OS Config 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.

OS Config doesn't write **Admin Activity** audit logs.

OS Config doesn't write **System Event** audit logs.

Audited operations

The following summarizes which API operations correspond to each audit log type in OS Config:

Audit logs category	OS Config operations
Admin Activity audit logs	N/A
Data Access audit logs	• ExecutePatchJob • GetPatchJob • CancelPatchJob • ListPatchJobs • ListPatchJobInstanceDetails • CreatePatchDeployment • GetPatchDeployment • ListPatchDeployments • DeletePatchDeployment • CreateGuestPolicy • GetGuestPolicy • ListGuestPolicies • UpdateGuestPolicy • DeleteGuestPolicy • LookupEffectiveGuestPolicy
System Event audit logs	N/A

Audit log format

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

- The log entry itself, which is an object of type `LogEntry` (/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` (/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 (/logging/docs/audit/api#servicedata-services).

For other fields in these objects, plus how to interpret them, review Understanding audit logs (/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:

```
cts/[PROJECT_ID]/logs/cloudaudit.googleapis.com%2Factivity
izations/[ORGANIZATION_ID]/logs/cloudaudit.googleapis.com%2Fdata_access
```

The part of the log name following **`/logs/`** must be URL-encoded. This means that the forward-slash charact
e written as **`%2F`**.

Service name

OS Config audit logs use the service name `osconfig.googleapis.com`.

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

Resource types

OS Config audit logs use the resource type `audited_resource` for all audit logs.

For a full list, go to Monitored resource types (/monitoring/api/resources).

Enabling audit logging

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 (/logging/docs/audit/configure-data-access).

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

OS Config doesn't write Admin Activity audit logs.

Audit log permissions

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 (/iam/docs/understanding-roles).

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

- **Project Owner**, **Project Editor**, or **Project Viewer**.
- Logging's **Logs Viewer** (/logging/docs/access-control#permissions_and_roles) role.
- A custom IAM role (/iam/docs/creating-custom-roles) with the `logging.logEntries.list` 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** (/iam/docs/understanding-roles#primitive_roles).
- Logging's **Private Logs Viewer** (/logging/docs/access-control#permissions_and_roles) role.
- A custom IAM role (/iam/docs/creating-custom-roles) with the `logging.privateLogEntries.list` 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

To find and view audit logs, you need to know the identifier of the Cloud project, folder, or organization for which you want to view audit logging information. You can further specify other indexed `LogEntry` (/logging/docs/reference/v2/rest/v2/LogEntry) fields, like `resource.type`; for details, review Finding log entries quickly (/logging/docs/view/advanced-queries#finding-quickly).

The following are the audit log names; they include variables for the identifiers of the Cloud project, folder, or organization:

```
ojects/project-id/logs/cloudaudit.googleapis.com%2Factivity
ojects/project-id/logs/cloudaudit.googleapis.com%2Fdata_access
ojects/project-id/logs/cloudaudit.googleapis.com%2Fsystem_event

lders/folder-id/logs/cloudaudit.googleapis.com%2Factivity
lders/folder-id/logs/cloudaudit.googleapis.com%2Fdata_access
lders/folder-id/logs/cloudaudit.googleapis.com%2Fsystem_event

ganizations/organization-id/logs/cloudaudit.googleapis.com%2Factivity
ganizations/organization-id/logs/cloudaudit.googleapis.com%2Fdata_access
ganizations/organization-id/logs/cloudaudit.googleapis.com%2Fsystem_event
```

You have several options for viewing your audit log entries.

The Cloud Console Logs Viewer currently supports viewing logs for Google Cloud projects only. To read log ent pecified folder or organization, use the Cloud Logging API or the **`gcloud`** command-line tool.

ConsoleAPI (#api)gcloud (#gcloud)

You can use the Logs Viewer in the Cloud Console to retrieve your audit log entries for your Cloud project:

1. In the Cloud Console, go to the **Cloud Logging > Logs** (Logs Viewer) page:

   Go to the Logs Viewer page (https://console.cloud.google.com/logs/viewer)

2. From **Classic**, select **Preview the new Logs Viewer**.
3. Select an existing Cloud project.
4. In the **Query builder** pane, do the following:
   - From **Resource**, select the Google Cloud resource type whose audit logs you want to see.
   - From **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_events`.

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

   For more details about querying using the new Logs Viewer, see Building log queries (Preview) (/logging/docs/view/building-queries).

For a sample audit log entry and how to find the most important information in it, see Understanding audit logs (/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 (/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 sinks (/logging/docs/export/aggregated_sinks) 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 (/logging/docs/exclusions).

Pricing

Cloud Logging charges you for Data Access audit logs that you explicitly request. OS Config doesn't write Admin Activity audit logs or System Event audit logs.

For more information on audit logs pricing, review Google Cloud's operations suite pricing (/stackdriver/pricing).

Last updated 2020-07-30 UTC.