GKE audit logging information

Send feedback

AUTOPILOT STANDARD

This document describes the audit logs created by Google Kubernetes Engine as part of Cloud Audit Logs.

Overview

Google Cloud services write audit logs to help you answer the questions, "Who did what, where, and when?" within your Google Cloud resources.

Your Google Cloud projects contain only the audit logs for resources that are directly within the Google Cloud project. Other Google Cloud resources, such as folders, organizations, and billing accounts, contain the audit logs for the entity itself.

For a general overview of Cloud Audit Logs, see Cloud Audit Logs overview. For a deeper understanding of the audit log format, see Understand audit logs.

Available audit logs

The following types of audit logs are available for GKE:

- Admin Activity audit logs

  Includes "admin write" operations that write metadata or configuration information.

  You can't disable Admin Activity audit logs.

- Data Access audit logs

  Includes "admin read" operations that read metadata or configuration information. Also includes "data read" and "data write" operations that read or write user-provided data.

  To receive Data Access audit logs, you must explicitly enable them.

For fuller descriptions of the audit log types, see Types of audit logs.

Audited operations

The following table summarizes which API operations correspond to each audit log type in GKE:

Audit logs category	GKE operations
Admin Activity audit logs	`io.k8s.authorization.rbac.v1`
	`io.k8s.authorization.rbac.v1.roles`

★ **Note:** This table provides the most commonly audited operations; it isn't a complete list.

Audit log format

Audit log entries include the following objects:

- The log entry itself, which is an object of type `LogEntry`. Useful fields include the following:
  - The `logName` contains the resource ID and audit log type.
  - The `resource` contains the target of the audited operation.
  - The `timeStamp` contains the time of the audited operation.
  - The `protoPayload` contains the audited information.

- The audit logging data, which is an `AuditLog` object held in the `protoPayload` field of the log entry.
- Optional service-specific audit information, which is a service-specific object. For earlier integrations, this object is held in the `serviceData` field of the `AuditLog` object; later integrations use the `metadata` field.

For other fields in these objects, and how to interpret them, review Understand audit logs.

Log name

Cloud Audit Logs log names include resource identifiers indicating the Google Cloud project or other Google Cloud entity that owns the audit logs, and whether the log contains Admin Activity, Data Access, Policy Denied, or System Event audit logging data.

The following are the audit log names, including variables for the resource identifiers:

```
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%2Factivity
billingAccounts/BILLING_ACCOUNT_ID/logs/cloudaudit.googleapis.com%2Fdata_acces
billingAccounts/BILLING_ACCOUNT_ID/logs/cloudaudit.googleapis.com%2Fsystem_eve
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
```

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

Service name

Kubernetes audit logs use the service name `k8s.io`.

The `k8s.io` service is used for Kubernetes audit logs. These logs are generated by the Kubernetes API Server component and they contain information about actions performed using the Kubernetes API. For example, any changes you make on a Kubernetes resource by using the `kubectl` command are recorded by the `k8s.io` service. Kubernetes audit log entries are useful for investigating suspicious API requests, for collecting statistics, or for creating monitoring alerts for unwanted API calls.

For a list of all the Cloud Logging API service names and their corresponding monitored resource type, see Map services to resources.

Resource types

Kubernetes audit logs use the `k8s_cluster` resource type. Log entries written by the Kubernetes API server apply to the `k8s_cluster` resource type. These log entries describe operations on Kubernetes resources in your cluster, for example, Pods, Deployments, and Secrets.

For a list of all the Cloud Logging monitored resource types and descriptive information, see Monitored resource types.

Caller identities

The IP address of the caller is held in the `RequestMetadata.caller_ip` field of the `AuditLog` object. Logging might redact certain caller identities and IP addresses.

For information about what information is redacted in audit logs, see Caller identities in audit logs.

Enable 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 can't be disabled).

For information about enabling some or all of your Data Access audit logs, see Enable Data Access audit logs.

Permissions and roles

IAM permissions and roles determine your ability to access audit logs data in Google Cloud resources.

When deciding which Logging-specific permissions and roles apply to your use case, consider the following:

- The Logs Viewer role (`roles/logging.viewer`) gives you read-only access to Admin Activity, Policy Denied, and System Event audit logs. If you have just this role, you cannot view Data Access audit logs that are in the `_Default` bucket.
- The Private Logs Viewer role `(roles/logging.privateLogViewer`) includes the permissions contained in `roles/logging.viewer`, plus the ability to read Data Access audit logs in the `_Default` bucket.

  Note that if these private logs are stored in user-defined buckets, then any user who has permissions to read logs in those buckets can read the private logs. For more information about log buckets, see Routing and storage overview.

For more information about the IAM permissions and roles that apply to audit logs data, see Access control with IAM.

View 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.

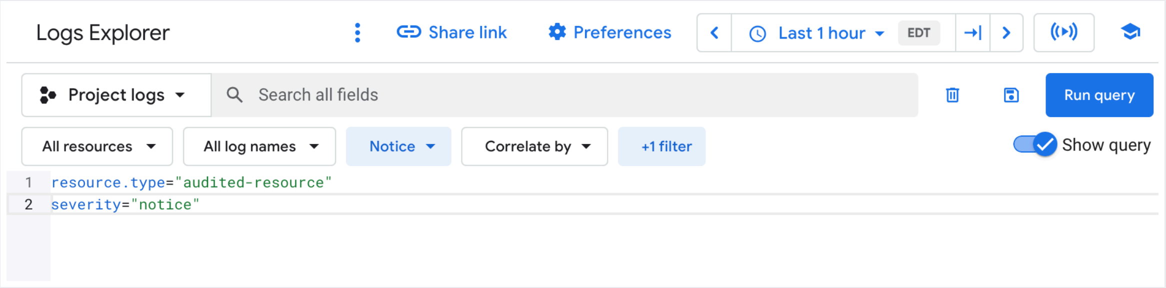
Sample queries

To use the sample queries in the following table, complete these steps:

1. Replace the variables in the query expression with your own project information, then copy the expression using the clipboard icon ⧉.
2. 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**.
3. Enable **Show query** to open the query-editor field, then paste the expression into the query-editor field:



```
resource.type="audited-resource"
severity="notice"
```

4. Click **Run query**. Logs that match your query are listed in the **Query results** pane.

To find audit logs for GKE, use the following queries in the Logs Explorer:

Query/filter name	Expression

Workload audit logs	`log_id("cloudaudit.googleapis.com/activity")`
	`resource.type="k8s_cluster"`
	`resource.labels.cluster_name="CLUSTER_NAME"`
	`protoPayload.request.metadata.name="WORKLOAD_NAME"`

Node metadata update for node object	`resource.type="k8s_cluster"`
	`log_id("cloudaudit.googleapis.com/activity")`
	`protoPayload.methodName="io.k8s.core.v1.nodes.update'`
	`resource.labels.cluster_name="CLUSTER_NAME"`
	`resource.labels.location="LOCATION_NAME"`

Changes to Role-Based Access Control, excluding automated system changes	`logName="projects/PROJECT_ID/logs/cloudaudit.googleap`
	`resource.type="k8s_cluster"`
	`protoPayload.methodName:"io.k8s.authorization.rbac.v1`
	`NOT protoPayload.authenticationInfo.principalEmail:"s`

Changes to Role-Based Access Control roles, excluding automated system changes	`logName="projects/PROJECT_ID/logs/cloudaudit.googleap`
	`resource.type="k8s_cluster"`
	`protoPayload.methodName:"io.k8s.authorization.rbac.v1`
	`NOT protoPayload.authenticationInfo.principalEmail:"s`

Changes to Role-Based Access Control role bindings, excluding automated system changes	`logName="projects/PROJECT_ID/logs/cloudaudit.googleap`
	`resource.type="k8s_cluster"`
	`protoPayload.methodName:"io.k8s.authorization.rbac.v1`
	`NOT protoPayload.authenticationInfo.principalEmail:"s`

Certificate signing requests	`logName="projects/PROJECT_ID/logs/cloudaudit.googleap`
	`resource.type="k8s_cluster"`
	`protoPayload.resourceName:"certificates.k8s.io/v1beta`

Unauthenticated web requests	`logName="projects/PROJECT_ID/logs/cloudaudit.googleap`
	`resource.type="k8s_cluster"`
	`protoPayload.authenticationInfo.principalEmail:"syste`

kubelet bootstrap identity calls	`logName="projects/PROJECT_ID/logs/cloudaudit.googleap`
	`resource.type="k8s_cluster"`
	`protoPayload.authenticationInfo.principalEmail:"kubel`

Node authenticated requests	`logName="projects/PROJECT_ID/logs/cloudaudit.googleap`
	`resource.type="k8s_cluster"`
	`protoPayload.authenticationInfo.principalEmail:"syste`

Calls outside an IP address range	`logName="projects/PROJECT_ID/logs/cloudaudit.googleap`
	`resource.type="k8s_cluster"`
	`protoPayload.requestMetadata.callerIp!="127.0.0.1"`

	`protoPayload.requestMetadata.callerIp!="::1"`
	`NOT protoPayload.requestMetadata.callerIp:"IP_ADDRES`

Admin Activity audit log entries that apply to the `k8s_cluster` resource type and describe creating a Deployment	`logName="projects/PROJECT_ID/logs/cloudaudit.googleap`
	`resource.type="k8s_cluster"`
	`protoPayload.methodName:"deployments.create"`

Admin Activity audit log entries that apply to the `k8s_cluster` resource type and have a `principalEmail` value of `system:anonymous`. These entries probably represent failed attempts to authenticate.	`logName="projects/PROJECT_ID/logs/cloudaudit.googleap`
	`resource.type="k8s_cluster"`
	`protoPayload.authenticationInfo.principalEmail="syste`

Admin Activity audit log entries that apply to the `gke_cluster` resource type and have a `severity` value of `ERROR`.	`logName="projects/PROJECT_ID/logs/cloudaudit.googleap`
	`resource.type="gke_cluster"`
	`severity="ERROR"`

Admin Activity audit log entries that apply to the `k8s_cluster` resource type and describe a write request to a Secret.	`logName="projects/PROJECT_ID/logs/cloudaudit.googleap`
	`resource.type="k8s_cluster"`
	`protoPayload.methodName:"io.k8s.core.v1.secrets"`
	`NOT protoPayload.methodName:"get"`
	`NOT protoPayload.methodName:"list"`
	`NOT protoPayload.methodName:"watch"`

Admin Activity audit log entries that apply to the `k8s_cluster` resource type and describe a Pod request from a particular user.	`logName="projects/PROJECT_ID/logs/cloudaudit.googleap`
	`resource.type="k8s_cluster"`
	`protoPayload.methodName:"io.k8s.core.v1.pods"`
	`protoPayload.authenticationInfo.principalEmail="dev@e`

Route audit logs

You can route audit logs to supported destinations in the same way that you can route other kinds of logs. Here are some reasons you might want to route your audit logs:

- To keep audit logs for a longer period of time or to use more powerful search capabilities, you can route copies of your audit logs to Cloud Storage, BigQuery, or Pub/Sub. Using Pub/Sub, you can route to other applications, other repositories, and to third parties.
- To manage your audit logs across an entire organization, you can create aggregated sinks that can route logs from any or all Google Cloud projects in the organization.
- If your enabled Data Access audit logs are pushing your Google Cloud projects over your log allotments, you can create sinks that exclude the Data Access audit logs from Logging.

For instructions about routing logs, see Route logs to supported destinations.

Pricing

For more information about pricing, see Cloud Logging pricing summary.

Setting up metrics and alerts

To set up metrics based on your log entries, you can use Cloud Monitoring. To set up charts and alerts, you can use log-based metrics.

Audit policy

The Kubernetes audit policy determines which log entries are exported by the Kubernetes API server. The Kubernetes Engine audit policy determines which entries go to your Admin Activity audit log and which entries go to your Data Access audit log.

For more information about audit policies in Kubernetes Engine, see Kubernetes Engine Audit Policy.

Send feedback

Last updated 2024-10-23 UTC.

Why Google

Choosing Google Cloud

Trust and security

Modern Infrastructure Cloud

Multicloud

Global infrastructure

Customers and case studies

Analyst reports

Whitepapers

Blog

Products and pricing

Google Cloud pricing

Google Workspace pricing

See all products

Solutions

Infrastructure modernization

Databases

Application modernization

Smart analytics

Artificial Intelligence

Security

Productivity & work transformation

Industry solutions

DevOps solutions

Small business solutions

See all solutions

Resources

Google Cloud Affiliate Program

Google Cloud documentation

Google Cloud quickstarts

Google Cloud Marketplace

Learn about cloud computing

Support

Code samples

Cloud Architecture Center

Training

Certifications

Google for Developers

Google Cloud for Startups

System status

Release Notes

Engage

Contact sales

Find a Partner

Become a Partner

Events

Podcasts

Developer Center

Press Corner

Google Cloud on YouTube

Google Cloud Tech 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