Filter

Local SSD and ephemeral storage
File storage
Object storage

Configure cluster security
Plan cluster security
About security in GKE
Harden your clusters
Security patching
Security measures in GKE Autopilot
About control plane security
Audit logging for Kubernetes
Audit logging for Kubernetes Engine
Audit logging for Container Security API
About audit policy
Shared security responsibilities
About cluster trust
Mitigate security incidents
vTPM in Confidential GKE workloads

GKE audit logging information

Send feedback

On this page
Overview
Available audit logs
Audited operations
Audit log format
Log name
...

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

Local SSD and ephemeral storage
File storage
Object storage

Configure cluster security
Plan cluster security
About security in GKE
Harden your clusters
Security patching
Security measures in GKE Autopilot
About control plane security
Audit logging for Kubernetes
Audit logging for Kubernetes Engine
Audit logging for Container Security API
About audit policy
Shared security responsibilities
About cluster trust
Mitigate security incidents
vTPM in Confidential GKE workloads

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.

Local SSD and ephemeral storage
File storage
Object storage

Configure cluster security
Plan cluster security
About security in GKE
Harden your clusters
Security patching
Security measures in GKE Autopilot
About control plane security
Audit logging for Kubernetes
Audit logging for Kubernetes Engine
Audit logging for Container Security API
About audit policy
Shared security responsibilities
About cluster trust
Mitigate security incidents
vTPM in Confidential GKE workloads

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.

Local SSD and ephemeral storage
File storage
Object storage

Configure cluster security
Plan cluster security
About security in GKE
Harden your clusters
Security patching
Security measures in GKE Autopilot
About control plane security
Audit logging for Kubernetes
Audit logging for Kubernetes Engine
Audit logging for Container Security API
About audit policy
Shared security responsibilities
About cluster trust
Mitigate security incidents
vTPM in Confidential GKE workloads

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.

Console gcloud API

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

Local SSD and ephemeral storage
File storage
Object storage

Configure cluster security
Plan cluster security
About security in GKE
Harden your clusters
Security patching
Security measures in GKE Autopilot
About control plane security
Audit logging for Kubernetes
Audit logging for Kubernetes Engine
Audit logging for Container Security API
About audit policy
Shared security responsibilities
About cluster trust
Mitigate security incidents

```
protoPayload."@type"="type.googleapis.com/google.c
```

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 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.

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:

Local SSD and ephemeral storage
File storage
Object storage

Configure cluster security
Plan cluster security
About security in GKE
Harden your clusters
Security patching
Security measures in GKE Autopilot
About control plane security
Audit logging for Kubernetes
Audit logging for Kubernetes Engine
Audit logging for Container Security API
About audit policy
Shared security responsibilities
About cluster trust
Mitigate security incidents

	protoPayload.request.metadata.name="WORKLOA
Node metadata update for node object	resource.type="k8s_cluster" log_id("cloudaudit.googleapis.com/activity" protoPayload.methodName="io.k8s.core.v1.nod 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/cloudau resource.type="k8s_cluster" protoPayload.methodName:"io.k8s.authorizati NOT protoPayload.authenticationInfo.princip
Changes to Role-Based Access Control roles, excluding automated system changes	logName="projects/PROJECT_ID/logs/cloudau resource.type="k8s_cluster" protoPayload.methodName:"io.k8s.authorizati NOT protoPayload.authenticationInfo.princip
Changes to Role-Based Access Control role bindings, excluding automated system changes	logName="projects/PROJECT_ID/logs/cloudau resource.type="k8s_cluster" protoPayload.methodName:"io.k8s.authorizati NOT protoPayload.authenticationInfo.princip
Certificate signing requests	logName="projects/PROJECT_ID/logs/cloudau resource.type="k8s_cluster" protoPayload.resourceName:"certificates.k8s
Unauthenticated web requests	logName="projects/PROJECT_ID/logs/cloudau resource.type="k8s_cluster" protoPayload.authenticationInfo.principalEm
kubelet bootstrap identity calls	logName="projects/PROJECT_ID/logs/cloudau resource.type="k8s_cluster" protoPayload.authenticationInfo.principalEm
Node authenticated requests	logName="projects/PROJECT_ID/logs/cloudau resource.type="k8s_cluster" protoPayload.authenticationInfo.principalEm
Calls outside an IP address range	logName="projects/PROJECT_ID/logs/cloudau resource.type="k8s_cluster" protoPayload.requestMetadata.callerIp!="127 protoPayload.requestMetadata.callerIp!="::1 NOT protoPayload.requestMetadata.callerIp:"
Admin Activity audit log entries that apply to the `k8s_cluster` resource type and	logName="projects/PROJECT_ID/logs/cloudau resource.type="k8s_cluster" protoPayload.methodName:"deployments.create

Local SSD and ephemeral storage
File storage
Object storage

Configure cluster security
Plan cluster security
About security in GKE
Harden your clusters
Security patching
Security measures in GKE Autopilot
About control plane security
Audit logging for Kubernetes
Audit logging for Kubernetes Engine
Audit logging for Container Security API
About audit policy
Shared security responsibilities
About cluster trust
Mitigate security incidents
vTPM in Confidential GKE workloads

resource type and describe a write request to a Secret.	`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/cloudau`
	`resource.type="k8s_cluster"`
	`protoPayload.methodName:"io.k8s.core.v1.pod`
	`protoPayload.authenticationInfo.principalEm`

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

Local SSD and ephemeral storage
File storage
Object storage

Configure cluster security
Plan cluster security
About security in GKE
Harden your clusters
Security patching
Security measures in GKE Autopilot
About control plane security
Audit logging for Kubernetes
Audit logging for Kubernetes Engine
Audit logging for Container Security API
About audit policy
Shared security responsibilities
About cluster trust
Mitigate security incidents
vTPM in Confidential GKE workloads

Last updated 2024-10-30 UTC.