GKE audit logging information

AUTOPILOT STANDARD

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

  - 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

★ **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

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:

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:

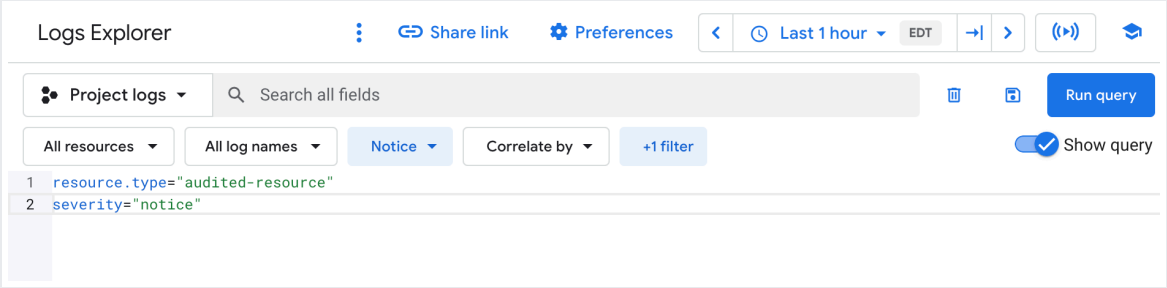
```
protoPayload."@type"="type.googleapis.com/google.cloud.audit.Aud
```

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**.

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:



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:

Changes to Role-Based Access Control role bindings, excluding automated system changes	logName="projects/*PROJECT_ID*/logs/cloudaudit.googl 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.googl resource.type="k8s_cluster" protoPayload.resourceName:"certificates.k8s.io/v1beta
Unauthenticated web requests	logName="projects/*PROJECT_ID*/logs/cloudaudit.googl resource.type="k8s_cluster" protoPayload.authenticationInfo.principalEmail:"syste
kubelet bootstrap identity calls	logName="projects/*PROJECT_ID*/logs/cloudaudit.googl resource.type="k8s_cluster" protoPayload.authenticationInfo.principalEmail:"kubel
Node authenticated requests	logName="projects/*PROJECT_ID*/logs/cloudaudit.googl resource.type="k8s_cluster" protoPayload.authenticationInfo.principalEmail:"syste

type and have a `severity` value of `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.googl`
	`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.googl`
	`resource.type="k8s_cluster"`
	`protoPayload.methodName:"io.k8s.core.v1.pods"`
	`protoPayload.authenticationInfo.principalEmail="dev@e`

Route audit logs

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.