Best practices for Cloud Audit Logs

This document recommends a sequence of audit logging tasks to help your organization maintain security and minimize risk.

This document isn't an exhaustive list of recommendations. Instead, its goal is to help you understand the scope of audit logging activities and plan accordingly.

Each section provides key actions and includes links for further reading.

Understand Cloud Audit Logs

Audit logs are available for most Google Cloud services. Cloud Audit Logs provides the following types of audit logs for each Google Cloud project, billing account, folder, and organization:

Audit log type	Configurable	Chargeable
Admin Activity audit logs (/logging/docs/audit#admin-activity)	No; always written	No
Data Access audit logs (/logging/docs/audit#data-access)	Yes	Yes
Policy Denied audit logs (/logging/docs/audit#policy_denied)	Yes; you can exclude these logs from being written to log buckets	Yes
System Event audit logs (/logging/docs/audit#system-event)	No; always written	No

Data Access audit logs—except for BigQuery—are disabled by default. If you want Data Access audit logs to be written for Google Cloud services, then you must explicitly enable them; for details, see Configure Data Access audit logs (#config-data-access) on this page.

For information about the overall landscape for audit logging with Google Cloud, see Cloud Audit Logs overview (/logging/docs/audit).

Control access to logs

Due to the sensitivity of audit logging data, it is especially important to configure the appropriate access controls for your organization's users.

Depending on your compliance and usage requirements, set these access controls as follows:

- Set IAM permissions (#privilege-best-practices)
- Configure log views (#log-views)
- Set log entry field-level access controls (#field-level-access)

Set IAM permissions

IAM permissions (/iam/docs/overview#permissions) and roles (/iam/docs/overview#roles) determine users' ability to access audit logs data in the Logging API (/logging/docs/reference/v2/rest), the Logs Explorer (/logging/docs/view/logs-explorer-interface), and the Google Cloud CLI (/logging/docs/reference/tools/gcloud-logging). Use IAM to grant granular access to specific Google Cloud buckets and prevent unwanted access to other resources.

The permission-based roles that you grant to your users depend on their auditing-related functions within your organization. For example, you might grant your CTO broad administrative permissions whereas your developer team members might require logs-viewing permissions. For guidance on which roles to grant to your organization's users, see configuring roles for audit logging (/iam/docs/roles-audit-logging).

When setting IAM permissions, apply the security principle of least privilege, so you grant users only the necessary access to your resources:

- Remove all nonessential users.
- Grant essential users the correct and minimal permissions.

For instructions on setting IAM permissions, see Manage access to projects, folders, and organizations (/iam/docs/granting-changing-revoking-access).

Configure log views

All logs, including audit logs, received by Logging are written into storage containers called log buckets (/logging/docs/routing/overview#buckets). Log views (/logging/docs/routing/overview#log-views) let you control who has access to the logs within your log buckets.

Because log buckets can contain logs from multiple Google Cloud projects, you might need to control which Google Cloud projects different users can view logs from. Create custom log views, which give you more granular access control for those buckets.

You can query log views with the Logs Explorer or with Log Analytics. For more information, see Query and view logs overview (/logging/docs/log-analytics).

For instructions on creating and managing log views, see Configure log views on a log bucket (/logging/docs/logs-views).

Set log field-level access controls

Field-level access controls let you hide individual `LogEntry` fields from users of a Google Cloud project, providing you a more granular way to control the logs data a user can access. Compared to logs views (#log-views), which hide the entire `LogEntry`, field-level access controls hide individual fields of the `LogEntry`. For example, you might want to redact external user PII, such as an email address contained in the log entry payload, from the majority of your organization's users.

If you plan to use Log Analytics (/logging/docs/log-analytics#analytics) to analyze your audit logs, then don't configure field-level access controls on the log bucket that stores those logs. You can't use Log Analytics on log buckets that have field-level access controls configured.

For instructions on configuring field-level access controls, see Configure field-level access (/logging/docs/field-level-acl).

Configure Data Access audit logs

When enabling new Google Cloud services, evaluate whether or not to enable Data Access audit logs (/logging/docs/audit#data-access).

Data Access audit logs help Google Support troubleshoot issues with your account. Therefore, we recommend enabling Data Access audit logs when possible.

Note: Data Access audit logs can be large and that you might incur additional costs for storage. For pricing information, see Google Cloud Observability pricing: Cloud Logging (/stackdriver/pricing#logging-costs).

To enable all audit logs for all services, follow the instructions to update the Identity and Access Management (IAM) policy (/logging/docs/audit/configure-data-access#example) with the configuration listed in the audit policy (/logging/docs/audit/configure-data-access#enable_all_access_logs).

After you define your organization-level data access policy and enable Data Access audit logs, use a test Google Cloud project to validate the configuration of your audit logs collection before creating developer and production Google Cloud projects in the organization.

For instructions on enabling Data Access audit logs, see Enable Data Access audit logs (/logging/docs/audit/configure-data-access).

Control how your logs are stored

You can configure aspects of your organization's buckets and also create user-defined buckets to centralize or subdivide your log storage. Depending on your compliance and usage requirements, you might want to customize your logs storage as follows:

- Choose where your logs are stored.
- Define the data retention period.
- Protect your logs with customer-managed encryption keys (CMEK).

Choose where your logs are stored

In Logging buckets are regional resources: the infrastructure that stores, indexes, and searches your logs is located in a specific geographical location.

Your organization might be required to store its logs data in specific regions. The primary factors in selecting the region where your logs are stored include meeting your organization's latency, availability, or compliance requirements.

To automatically apply a particular storage region to the new `_Default` and `_Required` buckets created in your organization, you can configure a default resource location.

For instructions on configuring default resource locations, see Configure default settings for organizations (/logging/docs/default-settings#specify-region).

Define data retention periods

Cloud Logging retains logs according to retention rules applying to the log bucket type where the logs are held.

To meet your compliance needs, configure Cloud Logging to retain logs between 1 day and 3650 days. Custom retention rules apply to all the logs in a bucket, regardless of the log type or whether that log has been copied from another location.

For instructions on setting retention rules for a log bucket, see Configure custom retention (/logging/docs/buckets#custom-retention).

Protect your audit logs with customer-managed encryption keys

By default, Cloud Logging encrypts customer content stored at rest. Your organization might have advanced encryption requirements that the default encryption at rest doesn't provide. To meet your organization's requirements, instead of Google managing the key encryption keys that protect your data, configure customer-managed encryption keys (CMEK) to control and manage your own encryption.

For instructions on configuring CMEK, see Configure CMEK for logs storage (/logging/docs/routing/managed-encryption-storage).

Pricing

Cloud Logging doesn't charge to route logs to a supported destination; however, the destination might apply charges. With the exception of the `_Required` log bucket, Cloud Logging charges to stream logs into log buckets and for storage longer than the default retention period of the log bucket.

Cloud Logging doesn't charge for copying logs, for creating log scopes (/logging/docs/log-scope/create-and-manage) or analytics views (/logging/docs/analyze/about-analytics-views), or for queries issued through the **Logs Explorer** or **Log Analytics** pages.

For more information, see the following documents:

- Cloud Logging pricing summary (/stackdriver/pricing#logs-pricing-summary)
- Destination costs:
  - Cloud Storage pricing (/storage/pricing)
  - BigQuery pricing (/bigquery/pricing#data_ingestion_pricing)
  - Pub/Sub pricing (/pubsub/pricing)
  - Cloud Logging pricing (/stackdriver/pricing#logging-cost)
- VPC flow log generation charges (/vpc/network-pricing#network-telemetry) apply when you send and then exclude your Virtual Private Cloud flow logs from Cloud Logging.

As you configure and use your audit logs, we recommend the following pricing-related best practices:

- Estimate your bills (/stackdriver/estimating-bills) by viewing your usage data and configuring alerting policies.
- Be aware that Data Access audit logs can be large and that you might incur additional costs for storage.
- Manage your costs by excluding audit logs (/logging/docs/routing/overview#exclusions) that aren't useful. For example, you can probably exclude Data Access audit logs in development projects.

Query and view audit logs

If you need to troubleshoot, being able to quickly look at logs is a requirement. In the Google Cloud console, use the Logs Explorer to retrieve your audit log entries for your organization:

1. In the Google Cloud console, go to the **Logs Explorer** page:

   Go to Logs Explorer (https://console.cloud.google.com/logs/query)

   If you use the search bar to find this page, then select the result whose subheading is **Logging**.

2. Select your organization.

3. In the **Query** 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**.

      If you don't see these options, then there aren't any audit logs of that type available in the organization.
    - In the query editor, further specify the audit log entries that you want to see. For examples of common queries, see Sample queries using the Logs Explorer (/logging/docs/view/query-library).
4. Click **Run query**.

For more information about querying by using the Logs Explorer, see Build queries in the Logs Explorer (/logging/docs/view/building-queries).

Monitor your audit logs

You can use Cloud Monitoring to notify you when conditions you describe occur. To provide Cloud Monitoring with data from your logs, Logging lets you create log-based alerting policies, which notify you anytime that a specific event appears in a log.

Configure alerting policies to distinguish between events that require immediate investigation versus low-priority events. For example, if you want to know when an audit log records a particular data-access message, you can create a log-based alerting policy that matches the message and notifies you when the message appears.

For instructions about configuring log-based alerting policies, see Managing log-based alerting policies (/logging/docs/alerting/log-based-alerts).

Route logs to supported destinations

Your organization may face requirements for creating and preserving audit logs. Using sinks (/logging/docs/routing/overview#sinks), you can route some or all of your logs to these supported destinations:

- Cloud Storage (/storage/docs/creating-buckets)
- Pub/Sub (/pubsub/docs/create-topic-console#create_a_topic), including third parties such as Splunk (/architecture/exporting-stackdriver-logging-for-splunk)
- BigQuery (/bigquery/quickstart-command-line#createtable)
- Another Cloud Logging bucket

Tip: For longer term retention, configure sinks prior to your organization receiving logs data.

Determine whether you need folder-level or organization-level sinks, and route logs from all the Google Cloud projects inside the organization or folder using aggregated sinks (/logging/docs/export/aggregated_sinks). For example, you might consider these routing use cases:

- Organization-level sink: If your organization uses a SIEM to manage multiple audit logs, you might want to route all of your organization's audit logs. Thus, an organization-level sink makes sense.
- Folder-level sink: Sometimes, you might want to only route departmental audit logs. For example, if you have a "Finance" folder and an "IT" folder, you might find value in only routing the audit logs belonging to the "Finance" folder, or the other way around.

  For more information on folders and organizations, see Resource hierarchy (/resource-manager/docs/cloud-platform-resource-hierarchy).

Apply the same access policies to the Google Cloud destination that you use to route logs as you applied to the Logs Explorer.

For instructions on creating and managing aggregated sinks, see Collate and route organization-level logs to supported destinations (/logging/docs/export/aggregated_sinks).

Understand data format in sink destinations

When routing audit logs to destinations outside of Cloud Logging, understand the format of the data that has been sent.

For example, if routing logs to BigQuery, Cloud Logging applies rules to shorten BigQuery schema field names for audit logs (/logging/docs/export/bigquery#audit-logs) and for certain structured payload fields.

To understand and find log entries that you routed from Cloud Logging to supported destinations, see View logs in sink destinations (/logging/docs/export/using_exported_logs).

Copy log entries

Depending on your organization's compliance needs, you might need to share audit log entries with auditors outside of Logging. If you need to share log entries that are already stored in Cloud Logging buckets, you can manually copy them to Cloud Storage buckets.

When you copy log entries to Cloud Storage, the log entries also remain in the log bucket they were copied from.

Note that copy operations don't replace sinks, which automatically send all incoming log entries to a pre-selected supported storage destination, including Cloud Storage.

For instructions on routing logs to Cloud Storage retroactively, see Copy log entries (/logging/docs/routing/copy-logs).

Last updated 2025-05-09 UTC.