This page provides supplemental information for using cloud audit logging (/logging/docs/audit/) with Cloud TPU.

Audit logs help you determine who did what, where, and when. Specifically, audit logs track how your Cloud TPU resources are modified and accessed within your Google Cloud projects.

Cloud Audit Logging returns two types of logs:

- Admin Activity log (/logging/docs/audit/#admin_activity_logs): Contains log entries for Cloud TPU API (/tpu/docs/reference/rest/) calls that modify the state or metadata of Cloud TPU resources in the system, such as creation and deletion of TPU Nodes or cancellation and deletion of TPU operations.
- Data Access log (/logging/docs/audit/#data_access_logs): Contains log entries for operations that perform read-only actions in the Cloud TPU API (/tpu/docs/reference/rest/), specifically get and list APIs.

Admin Activity logs are recorded by default. These logs do not count towards your log ingestion quota (/logging/quotas).

Data Access logs are not recorded by default. These logs count towards your log ingestion quota. You can enable and configure aspects for data access-types (/logging/docs/audit/configure-data-access) through the Google Cloud Console or programmatically using the API or Cloud SDK.

The following users can view Admin Activity logs:

- Project owners, editors, and viewers (/iam/docs/understanding-roles#primitive_roles).
- Users with the Logs Viewer (/iam/docs/understanding-roles#primitive_roles) IAM Role.
- Users with the **logging.logEntries.list** IAM permission.

The following users can view Data Access logs:

- Project owners.
- Users with the Private Logs Viewer (/logging/docs/access-control#permissions_and_roles) IAM role.
- Users with the **logging.privateLogEntries.list** IAM permission.

Project owners can grant, change, and revoke access (/iam/docs/granting-changing-revoking-access) to project members.

You can view a summary of the audit logs for your project from the Google Cloud Console (https://console.cloud.google.com/) ACTIVITY menu. A more detailed version of the logs can be found in the Logs Viewer (/logs/viewer?_ga=2.97606429.-349721430.1526422076).

You can also filter logs (/logging/docs/view/logs_viewer) in the Logs Viewer.

Cloud TPU audit-logs are logged to the generic **Audited Resource**.