This page describes the audit logs created by Cloud Source Repositories as part of Cloud Audit Logs (/logging/docs/audit/).

Google Cloud services write audit logs to help you answer the questions, "Who did what, where, and when?" Your Cloud projects each contain only the audit logs for resources that are directly within the project. Other entities, such as folders, organizations, and billing accounts, each contain the audit logs for the entity itself.

Cloud Source Repositories audit logging does not capture events from users searching and browsing within reposito er interface.

Cloud Source Repositories writes, and **provides by default**, audit logs for **Admin Activity**, which includes operations that modify the configuration or metadata of a resource.

Cloud Source Repositories writes, and **does not provide by default**, audit logs for **Data Access**, which record API calls that create, modify, or read user-provided data.

Data Access audit logs are divided into different categories:

- **Data Access (ADMIN_READ)**: Operations that read the configuration or metadata of a resource.

  Cloud Source Repositories does not provide Admin Read information by default.

- **Data Access (DATA_READ)**: Operations that read user-provided data from a resource.

  Cloud Source Repositories does not provide Data Read information by default.

- **Data Access (DATA_WRITE)**: Operations that write user-provided data to a resource.

  Cloud Source Repositories does not provide Data Write information by default.

Audit information that is not provided by default can be configured. For details, see Configuring Data Access Logs (/logging/docs/audit/configure-data-access).

Cloud Source Repositories audit logging does not capture events from users searching and browsing within reposito
er interface.

The following table summarizes which API operations correspond to each audit log type in Cloud Source Repositories:

Audit logs category	Cloud Source Repositories operations
Admin activity logs	SourceRepo.UpdateProjectConfig SourceRepo.UpdateRepo SourceRepo.CreateRepo SourceRepo.DeleteRepo SourceRepo.SetIamPolicy
Data Access logs (ADMIN_READ)	SourceRepo.GetProjectConfig SourceRepo.ListRepos SourceRepo.GetRepo SourceRepo.GetIamPolicy
Data Access logs (DATA_READ)	GitProtocol.LsRemote GitProtocol.UploadPack Browser.Access
Data Access logs (DATA_WRITE)	GitProtocol.ReceivePack

Audit log entries—which can be viewed in Stackdriver Logging using the Logs Viewer, the API, or the SDK `gcloud logging` command—include the following objects:

- The log entry itself, which is an object of type `LogEntry` (/logging/docs/reference/v2/rest/v2/LogEntry). Useful fields include the following:
  - `logName` contains the project identification and audit log type
  - `resource` contains the target of the audited operation
  - `timeStamp` contains the time of the audited operation
  - `protoPayload` contains the audited information

- The audit information, which is an `AuditLog` (/logging/docs/reference/audit/auditlog/rest/Shared.Types/AuditLog) object held in the `protoPayload` field of the log entry.
- Optional service-specific audit information, which is a service-specific object held in the `serviceData` field of the `AuditLog` object. For details, see Service-specific audit data (/logging/docs/audit/api/#servicedata-services).

For other fields in these objects, sample contents of them, and sample queries on information in the objects, see Audit Log Datatypes (/logging/docs/audit/api/).

Cloud Audit Logs log names indicate the project or other entity that owns the audit logs, and whether the log contains Admin Activity or Data Access information. For example, the following shows log names for a project's Admin Activity logs and an organization's Data Access logs.

The part of the log name following **`/logs/`** must be URL-encoded. This means that the forward-slash character, **`/`**, m
n as **`%2F`**.

Cloud Source Repositories audit logs use the service name `sourcerepo.googleapis.com`.

For more details on logging services, see Mapping services to resources (/logging/docs/api/v2/resource-list#service-names).

Cloud Source Repositories audit logs use the resource type `csr_repository` for all audit logs.

For a full list, see Monitored Resource Types (/monitoring/api/resources).

Admin Activity audit logs are enabled by default and cannot be disabled.

Most Data Access audit logs are disabled by default. The exception is Data Access audit logs for BigQuery, which are enabled by default and cannot be disabled; BigQuery Data Access logs do not count against your project's logging quota (/logging/quotas).

To enable some or all of your Data Access logs, see Configuring Data Access Logs (/logging/docs/audit/configure-data-access).

The Data Access logs that you configure can affect your logs pricing in Stackdriver. See the Pricing (#pricing) section on this page.

Cloud Identity and Access Management permissions and roles determine which audit logs you can view or export. Logs reside in projects and in some other entities including organizations, folders, and billing accounts. For more information, see Understanding Roles (/iam/docs/understanding-roles).

To view Admin Activity logs, you must have one of the following Cloud IAM roles in the project that contains your audit logs:

- **Project Owner**, **Project Editor**, or **Project Viewer**. See IAM Roles (/iam/docs/understanding-roles#primitive_roles).
- Logging's **Logs Viewer** (/logging/docs/access-control#permissions_and_roles) role.
- A custom Cloud IAM role (/iam/docs/creating-custom-roles) with the `logging.logEntries.list` Cloud IAM permission.

To view Data Access logs, you must have one of the following roles in the project that contains your audit logs:

- **Project Owner** (/iam/docs/understanding-roles#primitive_roles).
- Logging's **Private Logs Viewer** (/logging/docs/access-control#permissions_and_roles) role.
- A custom Cloud IAM role (/iam/docs/creating-custom-roles) with the `logging.privateLogEntries.list` Cloud IAM permission.

If you are using audit logs from a non-project entity, such as an organization, then change the **Project** roles to suitable organization roles.

To view audit logs for one of your projects, do one of the following:

- View a summary of your Admin Activity logs in the **Activity** dashboard:

  Go to Activity (https://console.cloud.google.com/home/activity)

- View all your audit logs using the Logs Viewer (/logging/docs/view/overview).

  Go to the Logs Viewer page (https://console.cloud.google.com/logs/viewer)

For more details, see the following options:

You can export audit logs in the same way you export other kinds of logs. For details about how to export your logs, see Exporting Logs (/logging/docs/export). Here are some applications of exporting audit logs:

- To keep audit logs for a longer period of time or to use more powerful search capabilities, you can export copies of your audit logs to Cloud Storage, BigQuery, or Pub/Sub. Using Pub/Sub, you can export to other applications, other repositories, and to third parties.
- To manage your audit logs across an entire organization, you can create aggregated export sinks (/logging/docs/export/aggregated_exports) that can export logs from any or all projects in the organization.
- If your enabled Data Access logs are pushing your projects over their logs allotments, you can export and exclude the Data Access logs from Logging. For details, see Excluding Logs (/logging/docs/exclusions).

Stackdriver Logging does not charge you for audit logs that are enabled by default, including all Admin Activity logs.

Stackdriver Logging charges you for Data Access logs that you explicitly request.

For more information on logs pricing, including audit logs pricing, see Stackdriver Pricing (/stackdriver/pricing_v2).