Stackdriver Logging is part of the Stackdriver suite of products in Google Cloud. It includes storage for logs, a user interface called the Logs Viewer, and an API to manage logs programmatically. Logging lets you read and write log entries, search and query your logs, export your logs, and create logs-based metrics.

Logs are associated primarily with Google Cloud projects, although other resources, such as organizations, folders, and billing accounts, can also have logs. The Logs Viewer shows only the logs from one project, but using the Logging API, you can read log entries across multiple resources.

A log entry records status or an event. The entry might be created by Google Cloud services, AWS services, third-party applications, or your own applications. The "message" the log entry carries is called the "payload"; it can be a simple string or structured data.

Your project receives log entries when you begin to use the services that routinely produce log entries, like Compute Engine or BigQuery. You also get log entries when you connect Stackdriver to AWS, when you install the Logging agent on your VM instances, and when you call the entries.write (/logging/docs/api/reference/rest/v2/entries/write) method in the Logging API.

A log is a named collection of log entries within a Google Cloud resource. Each log entry includes the name of its log. A log name can be a simple identifier, like `syslog`, or a structured name including the log's writer, like `compute.googleapis.com/activity`. Logs exist only if they have log entries.

Log entries are held in Stackdriver Logging for a limited time known as the retention period. After that, the entries are deleted. If you want to keep your log entries longer, export them (#sinks) outside of Stackdriver Logging.

The retention periods for different types of logs are listed in Logging Quotas and limits (/logging/quotas).

Each log entry indicates where it came from by including the name of a monitored resource. Examples are individual Compute Engine VM instances, individual Amazon EC2 VM instances, database instances, and so on. For a complete listing of monitored resource types, see Monitored resources and services (/logging/docs/api/v2/resource-list).

An advanced query (/logging/docs/view/advanced-queries) is a filter expression in the Logging query language. It is used in the Logs Viewer and the Logging API to select log entries, such as those from a particular VM instance or those arriving in a particular time period with a particular severity level.

All logs, including audit logs, platform logs, and user logs, are sent to the Stackdriver Logging API where they pass through the Logs Router. The Logs Router checks each log entry against existing rules to determine which log entries to ingest (store), which log entries to include in exports, and which log entries to discard. For more details, see Logs Router overview (/logging/docs/routing/overview).

Log entries received by Logging can be exported to Cloud Storage buckets, BigQuery datasets, and Pub/Sub topics. You export logs by configuring log sinks, which then continue to export log entries as they arrive in Logging. A sink includes a destination and a query that selects the log entries to export.

Metrics (/monitoring/api/v3/metrics) are a feature of Stackdriver Monitoring. A logs-based metric is a metric whose value is the number of log entries that match a query (/logging/docs/view/advanced-queries) that you specify.

Google Cloud services write audit logs to record certain administrative or user actions on Google Cloud resources. Audit logs appear in the Logs Viewer alongside other logs. For more information, read Cloud Audit Logs (/logging/docs/audit/).

The ability to access Logging logs is controlled by granting Cloud Identity and Access Management permissions to members.

Most logs can be read by any member with the Cloud IAM **Viewer** role. To read Data Access audit logs (/logging/docs/audit#data-access) or Access Transparency logs (/logging/docs/audit/access-transparency-overview), the member requires either the Cloud IAM **Owner** role or a custom role with special permissions.

For more information, see Access control (/logging/docs/access-control).