Log types: A breakdown

In this reading, you'll explore common log types used in the cloud and log management. As a reminder, a **log** is a record of events that occur within an organization’s systems. Logs provide context and transparency around events that happen in a cloud environment. Examples include the details of a compute instance starting up, or a new file uploaded to a bucket. **Logging** is the recording of events happening on computer systems and networks. Security professionals use **log analysis,** which is the process of examining logs, to identify events of interest. Log analysis is essential during the investigation of a security incident because the analysis can help you uncover details of how and when an incident occurred.

Cloud service providers offer different types of logs depending on the activity they record and collect from cloud resources. In this reading, you'll also examine the different log types found in Google Cloud Platform, including security logs, identity logs, and application logs.

Security logs

Google Cloud generates security logs known as audit logs. **Audit logs** record administrative activities and accesses within Google Cloud resources. Audit logs are used to track down who did what, where they did it, and when they did it. Audit logs support the goals of both security operations and compliance to monitor cloud resources for unusual activity, potential threats, data misuse, and access violations. These types of audit logs are generated in Google Cloud:

- **Admin Activity**: Records modifications made to the configuration settings of resources, like Identity and Access Management (IAM) permissions modifications
- **Data Access**: Records who accesses which data, when they accessed the data, and what actions they performed with the data
- **System Event**: Records Google Cloud system actions that modify the configuration of resources
- **Policy Denied**: Records when a user or service account is denied access to a resource because of a security policy violation

Table 1 provides an overview of each type of Google Cloud Audit Log:

Log Type	Description	Default Configuration	Default Retention	Example
Admin Activity Audit Log	API calls or other actions that modify the configuration or metadata of resources	• On by default • Cannot be turned off	400 days	• User creates a VM instance
Data Access Audit Logs	API calls that read the configuration or metadata of resources, as well as user-driven API calls that create, modify, or read user-provided resource data	• Disabled by default • Can be enabled per service; see section, Priority Data Access logs	30 days	• ADMIN_READ: Reads metadata or configuration information, like listing buckets or nodes in a GKE cluster • DATA_READ: Records operations that read user-provided data, like listing data in a bucket • DATA_WRITE: Records operations that write user-provided data, like writing data in a bucket
System Event Audit Logs	Logs generated by Google systems that modify the configuration of resources; they aren't driven by direct user action	• On by default • Cannot be turned off	400 days	• GCE migrates a VM to another host for maintenance purposes

Policy Denied Audit Logs	Recorded when a Google Cloud service denies access to a user or service account because of a security policy violation	• On by default • Can be disabled via exclusion filters	30 days	• Security policy violation event

Table 1: Google Cloud Audit Logs

These resources include examples of audit logs:

- Understand audit logs: provides a sample audit log entry and identifies how to find the most important information in audit log entries
- Login audit samples: provides samples of audit logs for Login Audit according to event type and event name

Identity logs

Identity logs record activities surrounding user accounts. They provide valuable insights into the activity of users that security operations teams can use to identify unusual patterns of activity, unauthorized access, and abuse of privilege. Google's Cloud Identity provides two types of identity logs:

1. **Admin logs**: Records actions performed by administrator accounts, like when an administrator adds a user
2. **User logs**: Records actions that users take on their accounts, like changing their passwords and updating their account recovery information

Application logs

Application logs are versatile and can be used for monitoring, troubleshooting, and debugging applications running in the cloud. They contain information about the performance, behavior, and errors that your applications may encounter. From a security perspective, application logs can be helpful in determining if an application was compromised and if data was stolen.

In Google Cloud, application logs are known as *user-written logs*. They're written by logging agents, logging application programming interfaces (APIs), or client libraries.

Log management

In order for security operations teams to make the most out of logs, they must appropriately manage their logs. This process of collecting, storing, analyzing, and disposing of log data is called **log management**. Some log management best practices include building an effective log management policy, storing logs with sinks, and filtering and routing logs with routers.

Build an effective log management policy

Organizations must build an effective log management policy not only to help maintain their security posture, but also to meet regulatory and compliance requirements if necessary. For example, organizations operating in the U.S. healthcare industry may need to comply with U.S.-specific healthcare regulations, like keeping logs for a specific period of time. So, a cloud security team might need to configure custom cloud retention periods depending on regulatory requirements.

Pro tip: It's common for cloud providers to charge fees for log storage depending on usage, retention period, and size. A well-defined log management policy should consider needs, budget, and leverage cost management strategies to choose a solution that best meets the needs of an organization.

Store logs with sinks

Cloud audit log sinks are destinations where Cloud Audit Logs are routed for storage or analysis. Sinks can be used to store logs in Cloud Storage buckets, BigQuery datasets, or Pub/Sub topics. They can also be used to stream logs to external systems.

Importance: Cloud audit log sinks are important because they provide a way to retain and analyze audit logs for compliance, security, and operational purposes. By routing audit logs to sinks, organizations can ensure that they have a complete record of all activity that takes place in their Google Cloud environment.

Table 2 provides an overview of use cases for storing logs with sinks:

Use Case	Description	Example
Compliance	Demonstrate compliance with industry regulations or internal policies	Organizations in the healthcare industry may be required to retain audit logs for a certain period of time

Security	Investigate security incidents	An organization experiences a data breach, they can use audit logs to determine who accessed the affected data and when
Operations	Troubleshoot operational issues	An organization is experiencing performance problems, they can use audit logs to identify the root cause of the problem

Table 2: Use cases for storing logs with sinks

Filter and route logs with routers

Cloud audit log routers are used to control how audit logs are routed to sinks. Routers can be used to filter logs based on their contents, or to route logs to different destinations based on their source.

Cloud audit log routers are important because they allow organizations to tailor their logging configuration to meet their specific needs. For example, an organization may want to route all audit logs from a particular project to a dedicated Cloud Storage bucket.

Table 3 provides an overview of use cases for filtering and routing logs:

Use Case	Description	Example
Data Segregation	Segregate audit logs from different projects or services	An organization may want to store audit logs from their production environment in a different location than audit logs from their development environment
Log Filtering	Filter audit logs based on their contents	An organization may want to only route audit logs that contain certain keywords.
Log Enrichment	Enrich audit logs with additional information	An organization may want to add the IP address of the user who generated the log entry

Table 3: Use cases for filtering and routing logs

Key takeaways

Security, identity, and application are examples of the different types of logs that you can use to gain insight into your cloud environment. Logs are essential in providing transparency around the activity happening in your environment, which is why organizations must have a clearly defined log management policy. As part of that policy, you can use audit sinks and routers to help to control the flow of audit logs in Google Cloud.