

Working with Cloud Audit Logs



In this module, we investigate the core Cloud Audit Logs that Google Cloud collects.

Objectives

- 01 Explain Cloud Audit Logs.
- 02 List and explain different audit logs.
- 03 Explain the features and functionalities of the different audit logs.
- 04 List the best practices to implement audit logs.



In this module, you learn to:

- Explain Cloud Audit Logs.
- List and explain different audit logs.
- Explain the features and functionalities of the different audit logs.
- List the best practices to implement audit logs.

In this section, you explore



✓ Cloud Audit Logs

✓ Data Access audit logs

✓ Audit logs entry format

✓ Best practices

We start with an overview of what audit logs do for us. Then we move to using the optional Data Access audit logs, explore the format of audit log entries, and end up with some logging best practices.

In terms of sheer volume of useful information, probably the most important group of logs in Google Cloud are the Cloud Audit Logs.

Cloud Audit Logs: “Who did what, where, and when?”

Admin Activity audit logs	System Event audit logs	Data Access audit logs	Policy Denied audit logs
<p>Records modifications to configuration or metadata.</p> <p>Helps answer questions such as “Who added that VM?”</p>	<p>Records Google Cloud non-human admin actions that modify configurations.</p> <p>Helps answer questions such as “Did a live-migration event occur?”</p>	<p>Records calls that read metadata, configurations, or that create, modify, or read user-provided data.</p> <p>Helps answer questions such as “Who modified that Cloud Storage file?”</p>	<p>Records a security policy violation.</p> <p>Helps answer question such as “Who tried to breach a security policy?”</p>

Google Cloud

[Cloud Audit Logs](#) help answer the question, “Who did what, where, and when?”

It maintains four audit logs for each Google Cloud project, folder, and organization:

- **Admin Activity audit logs**
- **Data Access audit logs**
- **System Event audit logs**
- **Policy Denied audit logs**

All Google Cloud services will eventually provide audit logs. For now, see the [Google services with audit logs](#) documentation for coverage details.

Admin Activity audit logs:

- Admin Activity audit logs contain log entries for API calls or other administrative actions that modify the configuration or metadata of resources.
- For example, these logs record when users create VM instances or change Identity and Access Management permissions.
- They are always on, are retained for 400 days, and are available at no charge.
- To view these logs, you must have the IAM role **Logging/Logs Viewer** or **Project/Viewer**.

System Event audit logs:

- System Event audit logs contain log entries for Google Cloud administrative actions that modify the configuration of resources.
- System Event audit logs are generated by Google systems; they are not driven

- by direct user action.
- They are always enabled, free, retained for 400 days.
- To view these logs, you must have the IAM role **Logging/Logs Viewer** or **Project/Viewer**.

Data Access audit logs:

- Data Access audit logs contain API calls that read the configuration or metadata of resources. Also, user-driven API calls that create, modify, or read user-provided resource data.
- Data Access audit logs don't record the data-access operations on resources that are publicly shared (available to **All Users** or **All Authenticated Users**). Data Access audit logs also don't record the data-access operations on resources that can be accessed without logging into Google Cloud.
- They are disabled by default (except for BigQuery), and when enabled, the default retention is 30 days.
- To view these logs, you must have the IAM roles **Logging/Private Logs Viewer** or **Project/Owner**.

Policy Denied audit logs:

- When a security policy is violated, this type of audit logs records when access to a user or service account is denied by Google Cloud service.
- Policy Denied audit logs are generated by default and your Google Cloud project is charged for the logs storage.
- You can't disable Policy Denied audit logs. However, you can use exclusion filters to prevent Policy Denied audit logs from being ingested and stored in Cloud Logging.

Filtering audit logs, log names

The screenshot shows the Google Cloud Logs Explorer interface. The top navigation bar includes 'Logs Explorer', 'REFINE SCOPE', 'Project', 'SHARE LINK', and 'LEARN'. Below this, there are tabs for 'Query', 'Recent (2)', 'Saved (0)', 'Suggested (2)', and 'Library'. The 'Query' tab is active, showing a search bar with 'Last 1 hour' and 'Search all fields'. The 'Log name' dropdown menu is open, displaying a list of log categories: OTHER, VERTEX AI API, BIGQUERY DATA, CLOUD AUDIT, activity, data_access, system_event, CLOUD SCHEDULER API, and executions. A blue callout box points to the 'Log name' dropdown with the text: 'If an audit logs category is missing, that simply means it doesn't currently have any entries.'

Google Cloud

To view and filter audit logs:

1. Navigate to Logs Explorer
2. Filter by using the **Log name** drop-down menu.

Note: typing *clouddaudit* into the filter box is frequently quicker than scrolling.

If one of the four audit logs is missing, that simply means it doesn't currently have any entries.




The example here filters the logs by a project and you can select the log entries you would like to audit.

You can even use the query builder to filter audit logs. This query is auto populated in the query section when using the UI. For details check out the [documentation](#) page.

Access Transparency logs



Show **how** and **why** customer data is accessed once it has been stored in Google Cloud.

	Logs actions of accesses
	Tracks actions by Google personnel
	Supports approval and surfaced through App APIs and UIs, Security Command Center

Google Cloud

Whether it's a hardware support engineer, or a rep working on a ticket, having dedicated experts manage parts of the infrastructure is a key benefit of operating in Google Cloud.

- Very similar to Cloud Audit logs, Access Transparency logs help by providing logs of accesses to your data by human Googlers (as opposed to automated systems).
- Enterprises with appropriate support packages can enable the logs, and receive the log events in near-real time. The log events are surfaced through the APIs, Cloud Logging, and Security Command Center.

Access Transparency logs give you different information than Cloud Audit Logs. Cloud Audit Logs record the actions that members of your Google Cloud organization have taken in your Google Cloud resources, whereas Access Transparency logs record the actions taken by Google personnel.

In this section, you explore

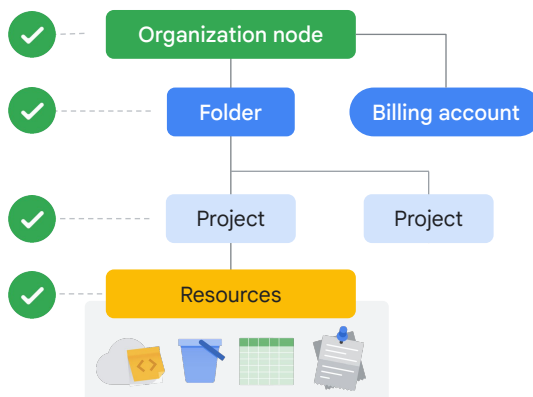


- ✓ Cloud Audit Logs
- ✓ **Data Access audit logs**
- ✓ Audit logs entry format
- ✓ Best practices

Let's continue by looking at Data Access audit logs.

Enabling Data Access audit logs in the organization

- Data Access audit logs can be enabled at:
 - Organization
 - Folder
 - Project
 - Resource
 - Billing accounts
- You can even exempt principals from recording data access logs
- Final scope is the union of the configurations



Google Cloud

Data Access audit logs can be enabled at various levels in the resource hierarchy. These levels include:

- Organization
- Folder
- Project,
- Resources, and
- Billing accounts

You can also exempt principals from recording data access logs.

The final configuration of Data Access audit logs is the union of the configurations. For example, at a project level, you can enable logs for a Google Cloud service. But you can't disable logs for a Google Cloud service that is enabled in a parent organization or folder.

The added logging does add to the cost, currently: \$0.50 per gigabyte for ingestion.

Enabling Data Access access logs per Google Cloud service

Default configuration

Admin Read: Disabled

Data Read: Disabled

Data Write: Disabled

0 exempted principals

Data Access audit logs configuration

The effective data access configuration below combines the configuration for the currently selected resource and the data access configurations set on all parent resources.

Filter: Enter property name or value

Service	Admin Read	Data Read	Data Write	Exempted principals	Inherited exempted principals
<input checked="" type="checkbox"/> Access Approval	—	—	—	0	0
<input type="checkbox"/> AI Platform Notebooks	—	—	—	0	0
<input type="checkbox"/> AlloyDB API	—	—	—	0	0
<input type="checkbox"/> Anthos Multi-	—	—	—	0	0

Access Approval

LOG TYPES

EXEMPTED PRINCIPALS

You can configure what types of operations are recorded in your Data Access audit logs for the selected services. There are several subtypes of Data Access audit logs:

- ☐ **Admin Read**
Records operations that read metadata or configuration information.
- ☐ **Data Read**
Records operations that read user-provided data.
- ☐ **Data Write**
Records operations that write user-provided data.

SAVE

Data Access logs can be enabled and configured at the service level.

Data Access helps control what type of information is recorded in the Data Access audit logs.

Google Cloud

Data Access audit logs are disabled by default, for everything but BigQuery. They may be enabled and configured at the organization, folder, project, or service level.

You can control what type of information is kept in the audit logs.

There are three types of Data Access audit logs information:

- **Admin-read:** Records operations that read metadata or configuration information. For example, you looked at the configurations for your bucket.
- **Data-read:** Records operations that read user-provided data. For example, you listed files and then downloaded one from Cloud Storage.
- **Data-write:** Records operations that write user-provided data. For example, you created a new Cloud Storage file.

Exempt specific users or groups

Audit Logs
[SET DEFAULT CONFIGURATION](#)

[HELP ASSISTANT](#)
[LEARN](#)
[HIDE INFO PANEL](#)

Default configuration

0 exempted principals

Admin Read:
☐ Disabled

Data Read:
☐ Disabled

Data Write:
☐ Disabled

Data Access audit logs configuration

The effective data access configuration below combines the configuration for the currently selected resource and the data access configurations set on all parent resources.

Filter

Enter property name or value

Service	Admin Read	Data Read	Data Write	Exempted principals	Inherited exempted principals
<input checked="" type="checkbox"/> Access Approval	—	—	—	0	0
<input type="checkbox"/> AI Platform Notebooks	—	—	—	0	0
<input type="checkbox"/> AlloyDB API	—	—	—	0	0
<input type="checkbox"/> Anthos Multi-cloud API	—	—	—	0	0
<input type="checkbox"/> Apigee	—	—	—	0	0

Access Approval

LOG TYPES
[EXEMPTED PRINCIPALS](#)

When you [exempt a principal](#), Data Access audit logs are not generated for that principal for the selected log types. Enter the principals that should be exempted.

Exempted principals

New exempted principal

Disabled Log Types
☐ Admin Read
☐ Data Read
☐ Data Write

You can exempt specific users or groups from having their data accesses recorded. This functionality comes in handy when you want reduce the cost and noise associated with the volume of logs that are not of your interest. Data Access audit logs can be of high volume, so cost associated is directly proportional to the volume of data logs.

Programmatically enabling Data Access audit logs

Step 1

```
gcloud projects get-iam-policy [project-id] > policy.yaml
```

Step 2

```
auditConfigs:
- auditLogConfigs:
- logType: ADMIN_READ
- logType: DATA_READ
- logType: DATA_WRITE
  service: run.googleapis.com #Could also be all Services
bindings:
- members:
  ...
```

Step 3

```
gcloud projects set-iam-policy [project-id] policy.yaml
```

You can also use the Google Cloud CLI or the API to enable Data Access audit logs.

1. If you're using the gcloud CLI frequently, the easiest way is to get the current IAM policies, as seen in step 1, and write them to a file.
2. Then you can edit the /tmp/policy.yaml file to add or edit the auditLogConfigs. You can also add the log details per service, like this example is enabling logging for Cloud Run. You can even enable logging on all services.
3. Then, as seen in step 3, you would set that as the new IAM policy.

In this section, you explore



✓ Cloud Audit Logs

✓ Data Access audit logs

✓ **Audit logs entry format**

✓ Best practices

Now that we can enable the logs we need, let's examine the logging entries themselves.

Cloud Audit Log entries

```
{
  insertId: "-77e5fge38tyo"
  logName: "projects/<projectID>/logs/cloudaudit.googleapis.com%2Fdata_access"
  operation: {
    first: true
    id: "1581200795118:bquxjob_56996f5_17026e67aa2"
    producer: "bigquery.googleapis.com"
  }

  protoPayload: {
    @type: "type.googleapis.com/google.cloud.audit.AuditLog"
    authenticationInfo: {
      principalEmail: "cloudysanfrancisco@gmail.com"
    }
  }
}
```

Identify an
audit log type

Identify the resource
generating log by looking at
producer

Identify an audit log entry by
looking at the **protoPayload**

Identify the principal
generating log by looking at the
principalEmail

Google Cloud

Every audit log entry in Cloud Logging is an object of type [LogEntry](#).

What distinguishes an audit log entry from other log entries is the `protoPayload` field, which contains an [AuditLog](#) object that stores the audit logging data.

Note the log name, which tells us that we're looking at an example from Data Access audit logs.

Identify the principal generating log by looking at the `principalEmail`.

The `operation` field only exists for a large or long-running audit log entries.

Google has a standard [List of official service names](#). You can use this list as a handy reference.

Cloud Audit Log entries

```
authorizationInfo: [2]
methodName: "jobservice.getqueryresults"
requestMetadata: {...}
resourceName: "projects/<project_ID>/queries/bquxjob_1eb1f384_17026e9d185"
serviceData: {...}
serviceName: "bigquery.googleapis.com"
status: {...} }
receiveTimestamp: "2020-02-08T22:27:06.410866127Z"
resource: {
  labels: { project_id: "<project_ID>", op_unit: "USA"
  }
  type: "bigquery_resource"
}
severity: "INFO"
timestamp: "2020-02-08T22:27:05.908Z"
}
```

On this slide, you can tell we're looking at a query that was run in BigQuery.

If you expanded the serviceData field, you could actually see the query itself.

So, when someone at your organization runs that unexpected, \$40,000 query, you can figure out who ran it and what the query was.

Then you can go learn more about price controls and BigQuery.

In this section, you explore



✓ Cloud Audit Logs

✓ Data Access audit logs

✓ Audit logs entry format

✓ **Best practices**

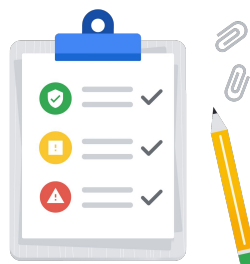
Let's go over a few best practices before we wrap up this module.

Plan and create test project

Create a [plan](#) for Data Access audit logs.

Create a [test project](#) and test plan.

Roll out the plan.



Like anything in the cloud, start by planning first.

Spend time and create a solid plan for Data Access audit logs. Think organization, folder, then project. Like most organizations, some of your projects will be very specialized, but usually, they do break down into common organizational types.

Then, create a test project and experiment to see if the logging works the way you expect.

Then roll out the plan, and don't forget automation (Infrastructure as Code, coming soon).

Decide and set org level data access

Advantages:

- Detailed information on who, accessed/edited/deleted what, and when
- Free tier
- Some logs are free

Disadvantage:

- Logs can be large and the Queries Per Second (QPS) can be high based on the number data access requests

Access Approval

LOG TYPESEXEMPTED PRINCIPALS

You can configure what types of operations are recorded in your Data Access audit logs for the selected services. There are several subtypes of Data Access audit logs:

☐ **Admin Read**
Records operations that read metadata or configuration information.

☐ **Data Read**
Records operations that read user-provided data.

☐ **Data Write**
Records operations that write user-provided data.

SAVE

Remember that Data Access audit logs can be enabled as high as the organization.

The pro would be detailed information on exactly who accessed, edited, and deleted what, and when.

The con is that Data Access logs can grow to be large, and are billed per gigabyte. This also results in higher Queries Per Second based on the number of data access requests.

Infrastructure as Code (IaC)

Terraform: OSS or Enterprise

- ✓ Run OSS or pay for enterprise version.
- ✓ State can be stored locally or remote in Cloud Storage or Terraform Cloud.
- ✓ You can use Terraform to enable audit logs.
- ✓ Audit logs keep you informed of the resources provisioned using an IaC tool.

Google Cloud

Infrastructure as Code (IaC) is essentially the process of automating the creation and modifications to your infrastructure using a platform. The platform supports configuration files, which can be put through a CI/CD pipeline, like with code.

Terraform is an open source package from HashiCorp or paid for enterprise version.

It isn't hosted directly in Google Cloud, though it's installed by default in Cloud Shell.

State management is a decision point for your organization. It can be remote or local.

Remote options include using Cloud Storage or Terraform Cloud. Local storage involves setting up something local to your organization, or using the pay-to-use HashiCorp Enterprise service.

Audit logs also keep you informed of the resources provisioned using an IaC tool. It is really useful if you want to control log sink filters at the project level. With terraform you can set default include/exclude filters and have them applied to every project.

Aggregate and store your organization's logs

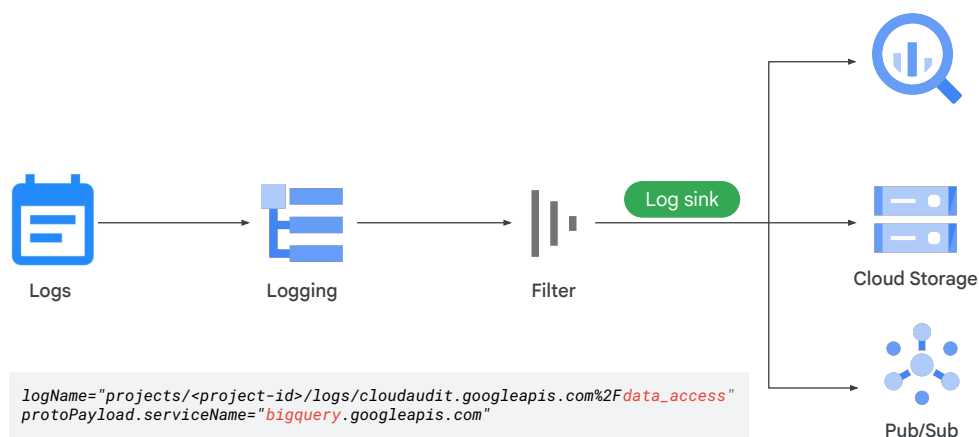
- ✓ Centralize or subdivide log storage by creating user-defined buckets
- ✓ This helps meet latency, compliance and availability requirements
- ✓ Configure a default storage location at the organization level to automatically apply a region
- ✓ Protect your audit logs storage by configuring CMEK.

To manage your Google Cloud organization's logs, you can aggregate them from across your organization into a single Cloud Logging bucket.

It is recommended to create user-defined buckets to centralize or subdivide your log storage. Based on compliance and usage requirements, customize your logs storage by choosing where your logs are stored and defining the data retention period. Some organization might have latency, compliance, and availability requirement in specific regions. Configure a default storage location to automatically apply a region in which buckets are create for log data.

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.

Plan and configure exports



We've discussed the options and benefits of exporting logs. Again, make this part of your plan.

Start by deciding what, if anything, you will export from Aggregated Exports at the organization level.

Next, decide what options you will use, project by project, folder by folder, and so on.

Then, carefully consider your filters—both what they leave in, and what they leave out.

Filters apply to all logging, not just to exports.

Lastly, carefully consider what, if anything, you will fully exclude from logging.

Remember that **excluded entries will be gone forever**.

Principle of least privilege

- Side-channel leakage of data through logs is a common issue.
- Plan the project to monitoring project relationships.
- Use appropriate IAM controls on both Google Cloud-based and exported logs.
- Data Access audit logs contain Personally Identifiable Information (PII).

Side-channel leakage of data through logs is a common issue.

You need to be careful who gets what kind of access, to which logs.

Remember some of the discussions earlier in this course on monitoring metrics scope? And how to monitor a current project?
That's where your security starts.

Are you monitoring project by project, or are you selectively grouping work projects into higher-level monitored projects?

Use appropriate IAM controls on both Google Cloud-based and exported logs, only allowing the minimal access required to get the job done.

Especially scrutinize the Data Access audit log permissions, as they will often contain Personally Identifiable Information (PII).

Configure log views

- Log views help control access to logs in a log bucket
- It helps control access specific to a project or a set of users
- It also help protect sensitive log data
- It ensures only authorized users have access to.

Log buckets store logs, including audit logs. Log views control access to logs in a log bucket. Custom log views can be created to control access to logs from specific projects or users. This helps protect sensitive data and ensures only authorized users have access.

Scenario: Operational monitoring

- CTO: **resourcemanager.organizationAdmin**
 - Assigns permissions to security team and service account.
- Security team: **logging.viewer**
 - Ability to view Admin Activity audit logs.
- Security team: **logging.privateLogViewer**
 - Ability to view Data Access audit logs.
- All permissions assigned at Org level.
- Control exported data access through Cloud Storage and BigQuery IAM roles.
- Explore using Sensitive Data Protection to **redact PII**.

Lastly, [a few access scenarios](#), starting with operational monitoring.

Let's explore your high-level teams and assignments.

By job:

CTO: **resourcemanager.organizationAdmin**, so they can assign permissions to the security team and service accounts.

The CTO can then give the security team **logging.viewer** so they can view the Admin Activity audit logs. Also, **logging.privateLogViewer**, so they can view the Data Access audit logs.

The view permissions are assigned at the organization level, so they are global.

Access control to data exported to Cloud Storage or BigQuery will be secured selectively with IAM.

You might also want to explore Sensitive Data Protection to redact the PII. Data in the Data Access audit logs is deemed as personally identifiable information (PII) for this organization. Integrating the application with Sensitive Data Protection gives the ability to redact sensitive PII data when viewing Data Access logs whether they are in the Data Access audit logs or from the historical archive in Cloud Storage.

Scenario: Dev teams monitoring Audit Logs

- Security team, same:
 - **logging.viewer**, **logging.privateLogViewer**
- Dev team: **logging.viewer** at folder level
 - See Admin Activity audit logs by dev projects in folder.
- Dev team: **logging.privateLogViewer** at folder
 - See Data Access audit logs.
- Use Cloud Storage or BigQuery IAM to control access to exported logs
 - Providing a Dashboard might be helpful.

Moving on to development teams.

The security team is unchanged from the last slide. They already have **logging.viewer**, and **logging.privateLogViewer** from the global assignment.

The dev team might get **logging.viewer** at the folder level so they can see the Admin Activity audit logs for the projects within their development control.

They probably also need **logging.privateLogViewer** at the dev folder so they can see the Data Access audit logs. Limit data they test with though, so they aren't viewing actual customer information.

Again, use Cloud Storage or BigQuery IAM to control access to exported logs. Prebuilding dashboards might also be a good option.

Scenario: External auditors

- Provide Dashboards for auditor usage.
- **logging.viewer** at Org level
 - See Admin Activity audit logs by dev projects in folder.
- **bigquery.dataViewer** at exported dataset
 - Backend for Dashboards.
- For Cloud Storage, use IAM and/or, signed, temporary, URLs.

For external auditors, provide pre-created dashboards where possible.

If they need broad access, you might make them **logging.viewer** at the org level.

For BigQuery, they could be **bigquery.dataViewer** on the exported dataset.

For Cloud Storage, again, you could use IAM, but also remember the temporary access URLs that Cloud Storage supports.



Knowledge Check



Quiz | Question 1

Question




Why are the Data Access audit logs off by default? Select THREE answers.

- A. They can be large
- B. They can be small
- C. They may contain sensitive information
- D. They can be expensive to store
- E. They are formatted incorrectly
- D. They cannot be filtered

Quiz | Question 1

Answer

Why are the Data Access audit logs off by default? Select THREE answers.

- A. They can be large 
- B. They can be small
- C. They may contain sensitive information 
- D. They can be expensive to store 
- E. They are formatted incorrectly
- D. They cannot be filtered

Quiz | Question 2

Question

If you want to provide an external auditor access to your logs, what IAM role would be best?

- A. Project Viewer
- B. Project Editor
- C. Logging Viewer
- D. Logging Admin

Quiz | Question 2

Answer

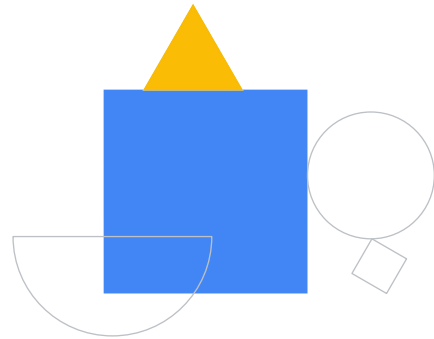
If you want to provide an external auditor access to your logs, what IAM role would be best?

- A. Project Viewer
- B. Project Editor
- C. Logging Viewer
- D. Logging Admin



Lab Intro

Cloud Audit Logs



Google Cloud

In this lab, you investigate Cloud Audit Logs. Cloud Audit Logging maintains multiple audit logs for each project, folder, and organization, all of which help answer the question, "Who did what, when, and where?"

Recap

- 01 Explain Cloud Audit Logs.
- 02 List and explain different audit logs.
- 03 Explain the features and functionalities of the different audit logs.
- 04 List the best practices to implement audit logs.



In this module, you learn to:

- Explain Cloud Audit Logs.
- List and explain different audit logs.
- Explain the features and functionalities of the different audit logs.
- List the Best Practices to implement audit logs.

