Preparing for the Associate Cloud Engineer (ACE) Exam: Configuring access & security

1. Section 5.1 - **Managing Identity and Access Management (IAM)**
2. Section 5.2 - Managing Service Accounts
3. Section 5.3 - Viewing audit logs for Project & Managed Services

Exam Guide: Section 5.1

5.1 Managing Identity and Access Management (IAM). Tasks include:

- Viewing account IAM assignments.
- Assigning IAM roles to accounts or Google Groups.
- Defining custom IAM roles.

Cloud IAM Overview

In Cloud IAM, you grant access to **members**. Members can be of the following types:

- Google account
- Service account
- Google group
- G Suite domain
- Cloud Identity domain

A Google account represents a developer, an administrator, or any other person who interacts with GCP.
A service account is an account that belongs to your application instead of an individual end user.
A Google group is a named collection of Google accounts and service accounts and each has a unique email address that is associated with that group.
A G Suite domain represents a virtual group of all the Google accounts that have been created in an organization's G Suite account.

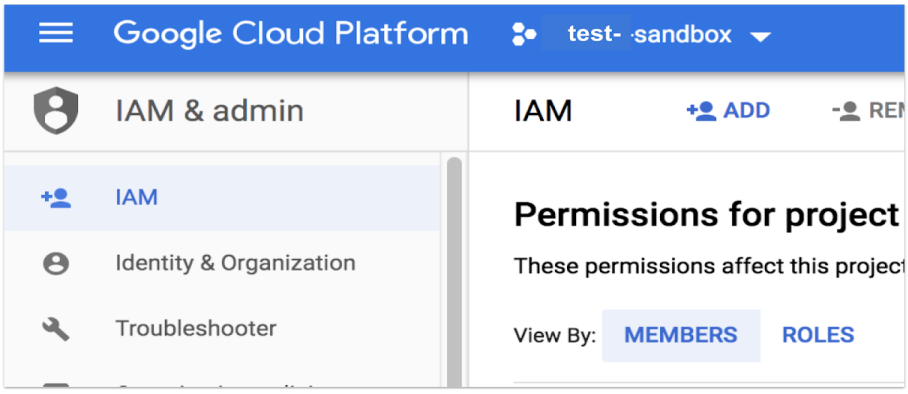
A Cloud Identity domain is like a G Suite domain because it represents a virtual group of all Google accounts in an organization - however, Cloud Identity domain users do not have access to G Suite applications and features.

Exam Guide: Section 5.1

5.1 Managing Identity and Access Management (IAM). Tasks include:

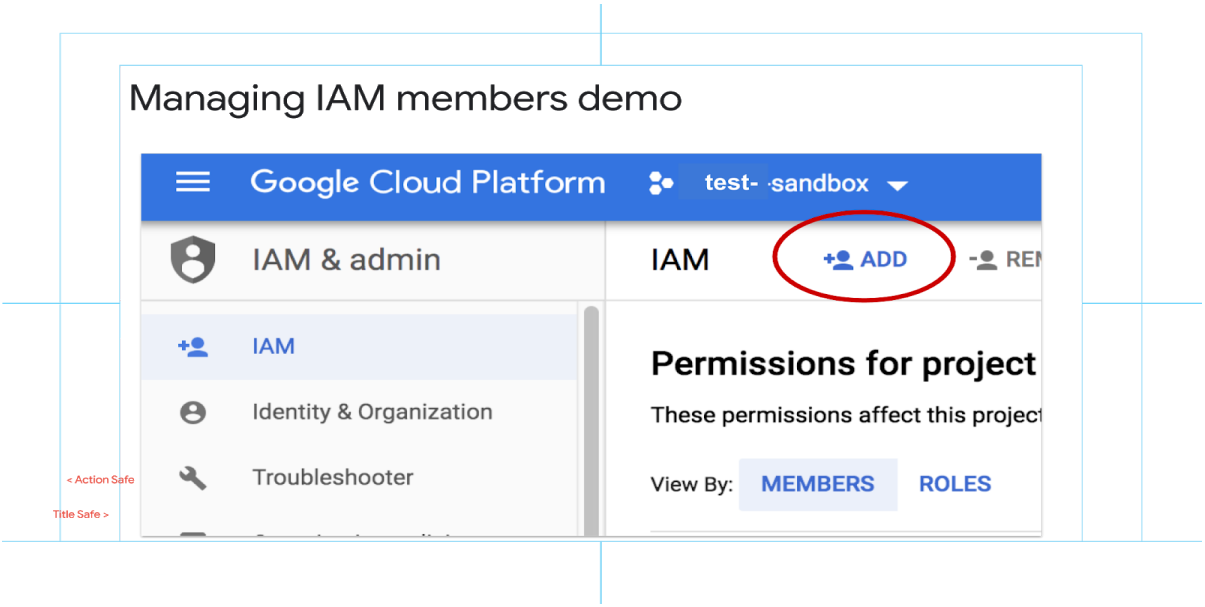
- **Viewing account IAM assignments.**
- **Assigning IAM roles to accounts or Google Groups.**
- Defining custom IAM roles.

Viewing IAM Assignments



Viewing IAM assignments is easy.

Open the IAM page in the GCP Console, click Select a Project, and then click Open.
The page will then display a list of members of that project and their roles.



https://cloud.google.com/iam/docs/granting-changing-revoking-access

To add a team member to a project and grant them a Cloud IAM role:
Open the IAM page in the GCP Console. OPEN THE IAM PAGE
Click Select a project, choose a project, and click Open.
Click Add.
Enter an email address. You can add individuals, service accounts, or Google Groups as members, but every project must have at least one individual as a member.
Select a role. Roles give members the appropriate level of permission. We recommend giving the member the least amount of privilege needed. Members with Owner-level permissions are also project owners and can manage all aspects of the project, including shutting it down.
Click Save.
To grant a role to a member for more than one project:
Open the IAM & Admin Projects page in the GCP Console. OPEN THE IAM & ADMIN PROJECTS PAGE
Select all the projects for which you want to grant permissions.
Click the Show Info Panel, followed by the Permissions tab.
Enter an email address in the Add members field, and select the desired role from the dropdown menu.
Click the Add button. The member will be granted the selected role in each of the selected projects.

Revoke access to a project
Open the IAM page in the Google Cloud Platform Console. OPEN THE IAM PAGE
Click Select a project.
Select a project and click Open.
Locate the member for whom you want to revoke access, and then click the Edit button on the right.
Click the Delete button for each role you want to revoke, and then click Save.
You can also use the gcloud command set to do this on the command line.

Exam Guide: Section 5.1

5.1 Managing Identity and Access Management (IAM). Tasks include:

- Viewing account IAM assignments.
- Assigning IAM roles to accounts or Google Groups.
- **Defining custom IAM roles.**

Creating custom Cloud IAM roles

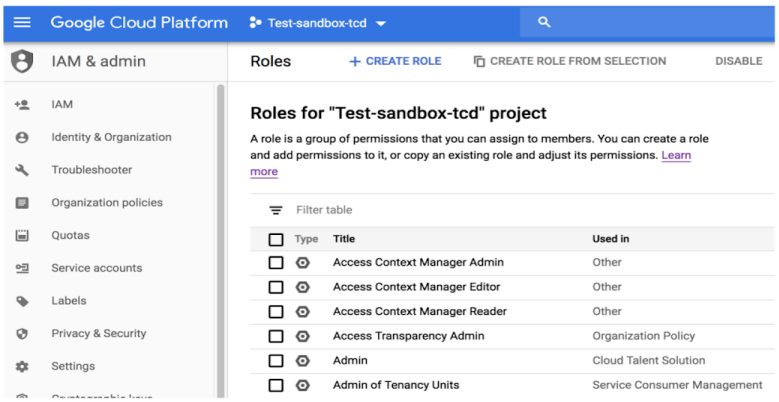
To create a custom role, you:

- Must know what permissions are available for that resource
- May want to get the role metadata, which includes the role ID and permissions contained in the role
- Must possess `iam.roles.create` permission on your account, which generally means you must be owner of the project or its organization

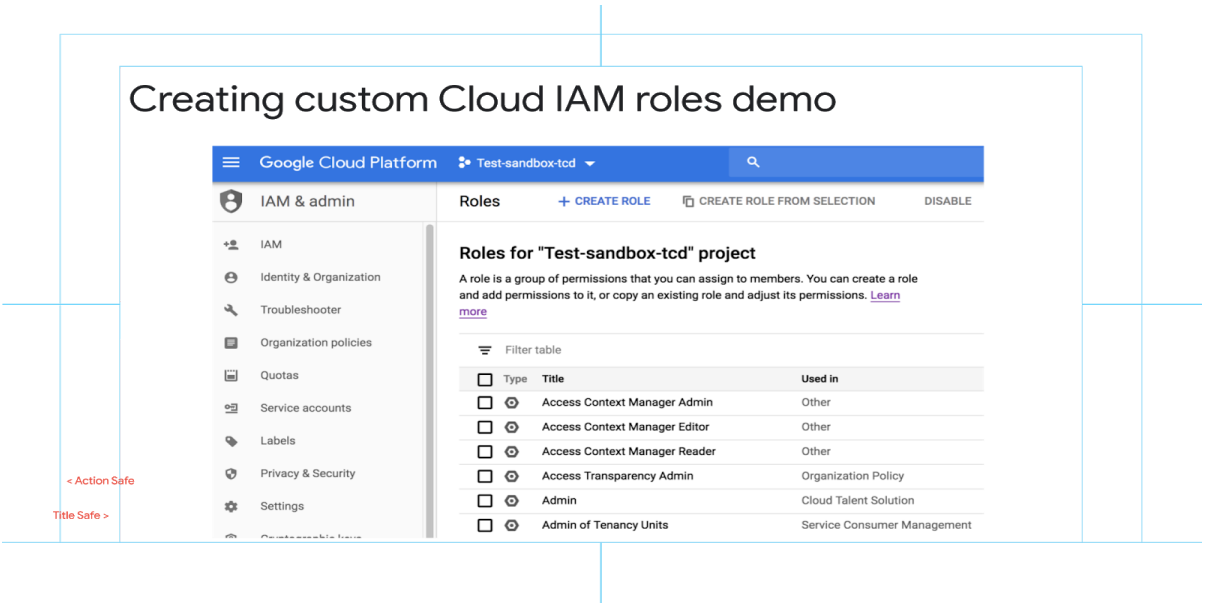
In addition to the predefined roles, Cloud IAM also provides the ability to create customized Cloud IAM roles.
You can create a custom Cloud IAM role with one or more permissions and then grant that custom role to users who are part of your organization.
Cloud IAM provides a UI and API for creating and managing custom roles.

Role metadata can be found by using the Google Cloud Platform Console or the IAM API.

Creating custom Cloud IAM roles



Once you have decided what to call your role, and what permissions to give it, creating the role and adding permissions is fairly simple.
You can also create a custom role using a “curated role” as its base.
This means you take a role that is similar to the one you need to create, and then add or remove permissions from a copy of that role until it meets your needs exactly.



https://cloud.google.com/iam/docs/creating-custom-roles

Go to the Roles page in the GCP Console. OPEN THE ROLES PAGE
Select your project from the drop-down at the top of the page.

Select the checkbox for a resource's admin role to view all the permissions that you can apply on that resource. For example, when you select the Compute Instance Admin role, the right side panel displays all the permissions that you can apply on a Compute Engine instance.
Before you create a custom role, you might want to get the metadata for both predefined and custom roles. Role metadata includes the role ID and permissions contained in the role. You can view the metadata using the Google Cloud Platform Console or the IAM API.

Go to the Roles page in the GCP Console. OPEN THE ROLES PAGE
Select your organization or project from the drop-down at the top of the page.
Select the checkbox for one or more roles to view the role permissions. The right side panel displays the permissions contained in the role(s), if any.
The icons beside the role indicate if it's a custom role ("factory" icon) or a predefined role (hexagon icon).
To create a custom role, a caller must possess iam.roles.create permission. By default, the owner of a project or an organization has this permission and can create and manage custom roles.
Users who are not owners, including organization admins, must be assigned either the Organization Role Administrator role, or the IAM Role Administrator role.

To create a new custom role from scratch:
Go to the Roles page in the GCP Console. OPEN THE ROLES PAGE
Select your organization from the Organization drop-down.
Click Create Role.
Enter a Name, a Title, and Description for the role.
Click Add Permissions.
Select the permissions you want to include in the role and click Add Permissions. Use the All Services and All Types drop-downs to filter and select permissions by services and types.
Creating a custom role based on an existing curated role:
Go to the Roles page in the GCP Console. OPEN THE ROLES PAGE
Select your organization from the Organization drop-down.
Select the roles on which you want to base the new custom role.
Click Create Role from Selection.
Enter a Name, a Title, and Description for the role.
Uncheck the permissions you want to exclude from the role.
Click Add Permissions to include any permissions.
Click Create.

1 Section 5.1 - Managing Identity and Access Management (IAM)

2 **Section 5.2 - Managing Service Accounts**

3 Section 5.3 - Viewing audit logs for Project & Managed Services

Exam Guide: Section 5.2

5.2 Managing service accounts. Tasks include:

- **Managing service accounts with limited scopes.**
- Assigning a service account to VM instances.
- Granting access to a service account in another project.

Service accounts...

- Are a special account that belongs to a Virtual Machine (VM) or an application
- Allow applications and VMs to call on the API of a service without a user being involved
- Are always associated with a key pair
- Come in two types: user-managed, and Google-managed
- Is also a type of resource, which has IAM policies attached to it
- Make use of both IAM roles, and *scopes*

First, let’s go over what a “service account” is.
A service account is a special Google account that belongs to your application or a virtual machine (VM), instead of to an individual end user. Your application uses the service account to call the Google API of a service, so that the users aren't directly involved.
For example, a Compute Engine VM may run as a service account, and that account can be given permissions to access the resources it needs. This way the service account is the identity of the service, and the service account's permissions control which resources the service can access.
A service account is identified by its email address, which is unique to the account.

Service account access scopes

- Access scopes are a legacy means of assigning permissions for your VMs
- They are no longer required for setting VM permissions - IAM roles now fill most of those functions
- They are still required for configuring instances to act as service accounts

Access scopes are the legacy method of specifying permissions for your VM. Before the existence of IAM roles, access scopes were the only mechanism for granting permissions to service accounts.
Although they are not the primary way of granting permissions now, you must still set access scopes when configuring an instance to run as a service account.
In addition, the permissions granted in the role and with a scope must agree - if they do not, the service account will not be able to perform the function you need it to.

Service account access scopes

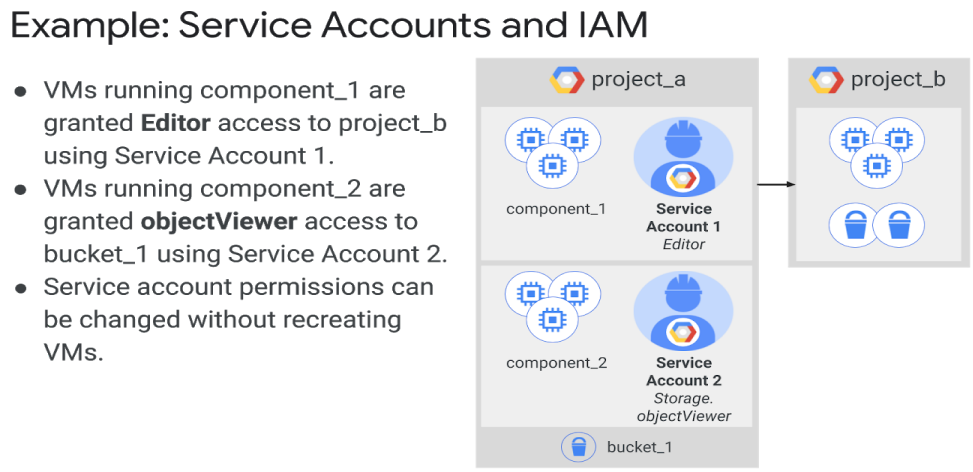
- Scopes take the form of a URL
- An example of a scope is:

  https://www.googleapis.com/auth/bigquery.insertdata

- The scope consists of the base URL up to the "auth" section, plus a specific permission being granted
- Scope can also be set on the command line using `set-scopes` with the `gcloud` command

An VM instance can only perform operations that are allowed by the roles assigned to the service account and the scopes that have been defined on the instance - and those permissions

cannot contradict.
For example, if a role only grants view only access to a resource, but a scope allows edit access, then the instance will not be able to edit that resource.
To enable edit access to the resource, the role would need to be modified so that it agreed with the permissions granted in the scope - in other words, it would need to be changed to allow editing.
If you need to change access scopes on an instance, you will need to stop that instance first, and then restart it for the changes to take effect.

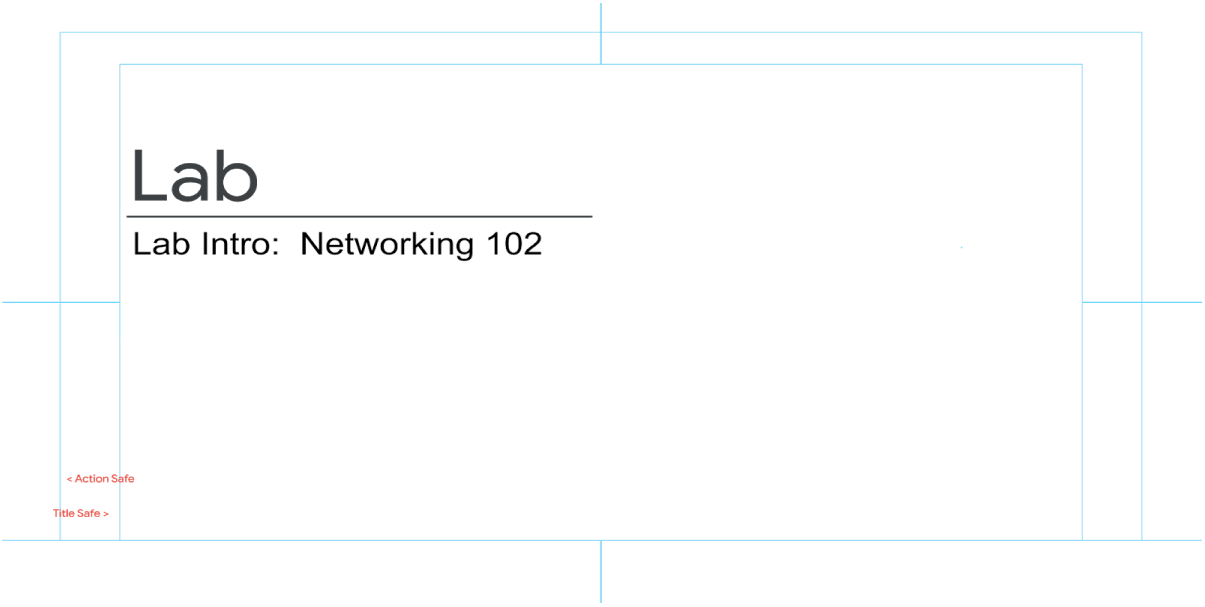


You can grant different groups of VMs in your project different identities. This makes it easier to manage different permissions for each group. You also can change the permissions of the service accounts without having to recreate the VMs. Here's a more complex example. Say you have an application that's implemented across a group of Compute Engine virtual machines. One component of your application needs to have an editor role on another project, but another component doesn't. So you would create two different service accounts, one for each subgroup of virtual machines. Only the first service account has privilege on the other project. That reduces the potential impact of a miscoded application or a compromised virtual machine.

Exam Guide: Section 5.2

5.2 Managing service accounts. Tasks include:

- Managing service accounts with limited scopes.
- **Assigning a service account to VM instances.**
- **Granting access to a service account in another project.**



In this lab you will allow and deny access to a network using firewall rules. You'll deploy the following lab environment of Projects, Networks, and Subnetworks to the Google Cloud Platform.

This lab is part of the Cloud Architecture quest

1 Section 5.1 - Managing Identity and Access Management (IAM)

2 Section 5.2 - Managing Service Accounts

3 **Section 5.3 - Viewing audit logs for Project & Managed Services**

Exam Guide: Section 5.3

5.3 Viewing audit logs for project and managed services.

Cloud Audit Logs

Three types of audit logs are kept for each of your projects:

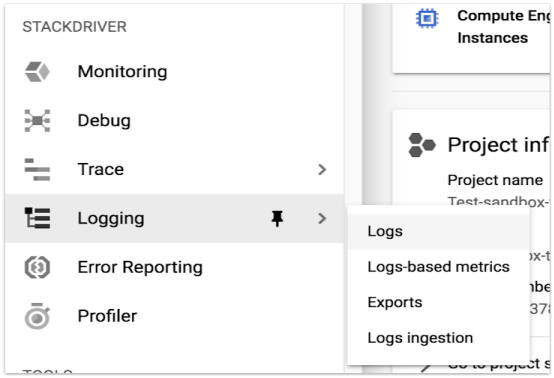
- Admin Activity
- System Events
- Data Access

```
projects/[PROJECT_ID]/logs/cloudaudit.googleapis.com%2Factivity
projects/[PROJECT_ID]/logs/cloudaudit.googleapis.com%2Fdata_access
projects/[PROJECT_ID]/logs/cloudaudit.googleapis.com%2Fsystem_event

folders/[FOLDER_ID]/logs/cloudaudit.googleapis.com%2Factivity
folders/[FOLDER_ID]/logs/cloudaudit.googleapis.com%2Fdata_access
folders/[FOLDER_ID]/logs/cloudaudit.googleapis.com%2Fsystem_event

organizations/[ORGANIZATION_ID]/logs/cloudaudit.googleapis.com%2Factivity
organizations/[ORGANIZATION_ID]/logs/cloudaudit.googleapis.com%2Fdata_access
organizations/[ORGANIZATION_ID]/logs/cloudaudit.googleapis.com%2Fsystem_event
```

Cloud Audit Logging maintains three audit logs for each project, folder, and organization: Admin Activity, System Event and Data Access.
Google Cloud Platform services write audit log entries to these logs to help you answer the questions of "who did what, where, and when?" within your GCP projects.
These logs contain the following information:
Resource: Each audit log entry includes a resource of some type. For example, you can view audit log entries from a single Compute Engine VM instance or from all VM instances.
Service: Services are individual GCP products, such as Compute Engine, Cloud SQL, or Cloud Pub/Sub. Each service is identified by name: Compute Engine is compute.googleapis.com, Cloud SQL is cloudsql.googleapis.com, and so forth.

Viewing Cloud Audit Logs in Stackdriver

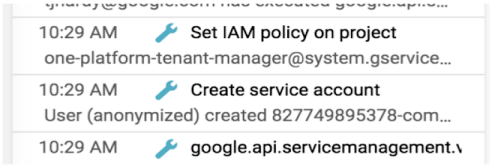
Cloud Audit logs can be viewed through the Stackdriver interface from the main console menu



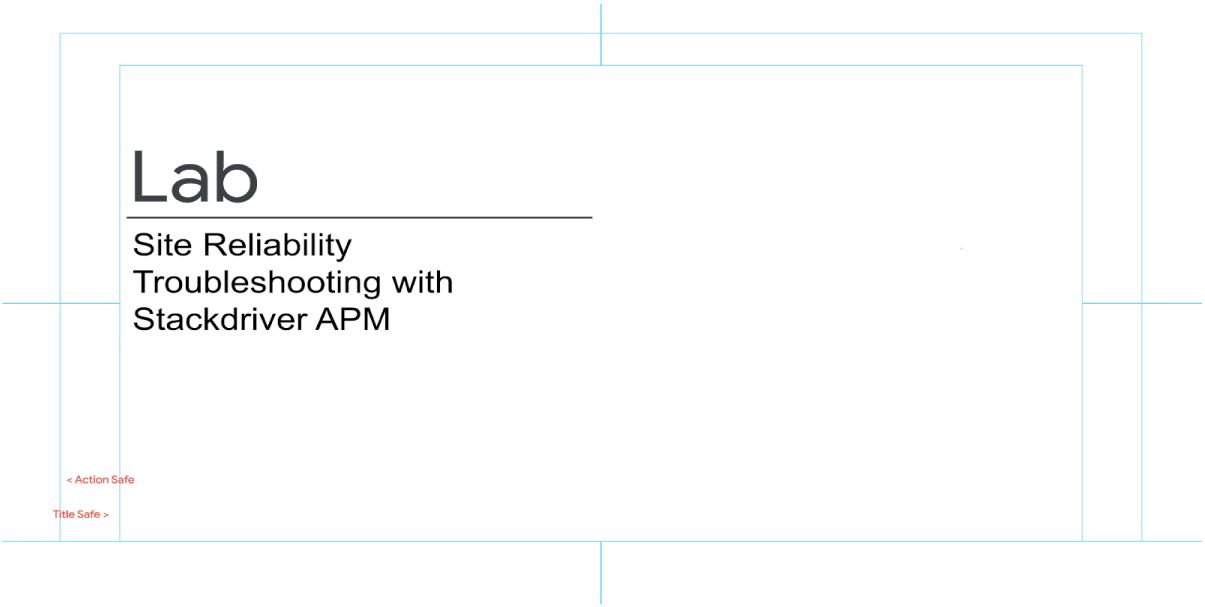
To view audit logs on a VM instance within a project, navigate to the Stackdriver section of the main console menu.
You will see options for Stackdriver components listed under the main heading.
Choose “Logging” and then “Logs” to view log entries for your instance.

Viewing Cloud Audit Logs in the Activity menu

You can also access abbreviated versions of your activity logs via the “Activity” link on the Home menu.



You can view abbreviated, project-level audit log entries in your project's Activity page in the GCP Console.
Navigate to the Home > Activity page, and then use Filter to select the entries you want to see.
As mentioned, these entries are abbreviated, so the actual audit log entries might contain more information than you see in the Activity page.



The objective of this lab is to familiarize yourself with the specific capabilities of Stackdriver to monitor GKE cluster infrastructure, Istio, and applications deployed on this infrastructure.

In this lab you:
Create a GKE cluster
Deploy a microservices application to it
Define latency and error SLIs and SLOs for it
Configure Stackdriver to monitor your SLIs
Deploy a breaking change to the application and use Stackdriver to troubleshoot and resolve the issues that result
Validate that your resolution addresses the SLO violation

This lab is part of the Qwiklabs Cloud Architecture Quest.

Suggested study resources for this section

Google Cloud IAM: https://cloud.google.com/iam/docs/

Security and Identity Fundamentals Quest: https://www.qwiklabs.com/quests/40

Cloud IAM Overview: https://cloud.google.com/iam/docs/overview

Understanding IAM roles: https://cloud.google.com/iam/docs/understanding-roles

Understanding Custom IAM roles: https://cloud.google.com/iam/docs/understanding-custom-roles

Granting or changing access in IAM:
https://cloud.google.com/iam/docs/granting-changing-revoking-access

Understanding Service Accounts: https://cloud.google.com/iam/docs/understanding-service-accounts

Service Accounts: https://cloud.google.com/iam/docs/service-accounts

Cloud Audit Logging overview: https://cloud.google.com/logging/docs/audit/

Services that product Audit Logs: https://cloud.google.com/logging/docs/audit/#services