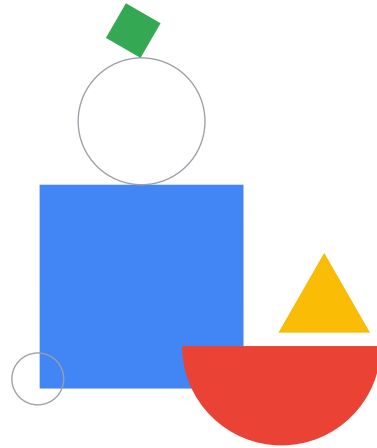


Preparing for Your Associate Cloud Engineer Journey

Módulo 5: Configura el acceso y la seguridad



Te damos la bienvenida al Módulo 5: Configura el acceso y la seguridad.



Temario del módulo



- 01 Administración del acceso para las soluciones en la nube de Cymbal Superstore
- 02 Preguntas de diagnóstico
- 03 Revisión y plan de estudios

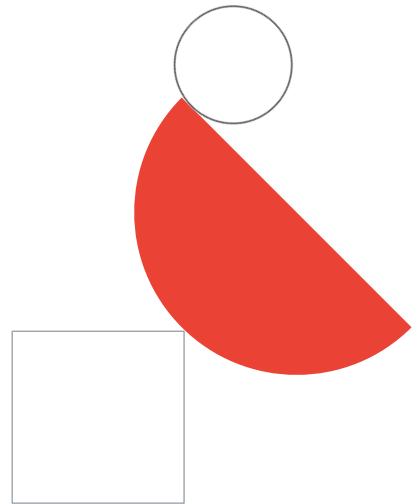
Google Cloud

En este módulo, explorarás el alcance de las tareas de configuración del acceso y la seguridad. Esto incluye la administración de IAM, así como las cuentas de servicio para soluciones en la nube. Estas áreas corresponden a la quinta (y última) sección de la guía para el examen de Associate Cloud Engineer.

Comenzaremos analizando tu rol como Associate Cloud Engineer en la administración del acceso a las soluciones en la nube de Cymbal Superstore. A continuación, evaluarás tus habilidades en esta sección de la guía del examen con 7 preguntas de diagnóstico. Este módulo cuenta con menos preguntas. Si bien es importante que comprendas esta área como Associate Cloud Engineer, su alcance es menos amplio.

Cuando revisemos las preguntas, debes identificar los recursos que querrás incluir en tu plan de estudio.

Administración del acceso para las soluciones en la nube de Cymbal Superstore

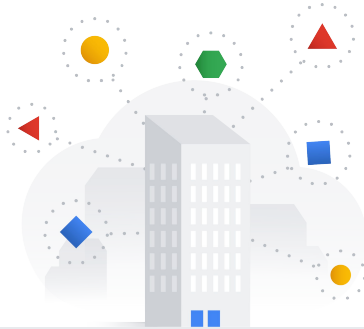


Google Cloud

Dado que Cymbal Superstore usa sus aplicaciones en Google Cloud, un Associate Cloud Engineer trabaja de forma continua en la configuración y administración del acceso de IAM y las cuentas de servicio. Veamos algunos ejemplos de cómo puedes llevar a cabo estas tareas en Cymbal Superstore.

El paso siguiente:

Acceso y seguridad continuos
para las soluciones en la nube de
Cymbal Superstore



- Administra Identity and Access Management (IAM)
- Administra cuentas de servicio
- Consultar registros de auditoría



Para desempeñar con éxito el rol de Associate Cloud Engineer en Cymbal Superstore, debes poder administrar Identity and Access Management (IAM) en Google Cloud. Ya analizamos los conceptos básicos de IAM en el primer módulo desde la perspectiva de la configuración de las cuentas y los proyectos en la nube. Aquí, evaluaremos las habilidades necesarias para administrar el acceso. También debes tener experiencia con las cuentas de servicio y las prácticas recomendadas para administrarlas en Google Cloud. Además, debes saber cómo visualizar los registros de auditoría cuando sea necesario.

Configuración de una cuenta de servicio para la aplicación de la cadena de suministro de Cymbal Superstore



- 1 Crear una cuenta de servicio
- 2 Asignar permisos
- 3 Conectar a una VM

Google Cloud

Para que conozcas cómo es la configuración del acceso y la seguridad en la práctica, examinaremos un ejemplo de los casos en los que podrías usar una cuenta de servicio en Cymbal Superstore.

La aplicación de cadena de suministro de Cymbal Superstore está compilada en una pila de LAMP que usa instancias de VM de Compute Engine. Utiliza Cloud SQL como almacén de datos de respaldo. La aplicación debe comunicarse con Cloud SQL a fin de actualizar los niveles de inventario. Para ello, usa una cuenta de servicio adjunta a la VM en la que se ejecuta.

Las cuentas de servicio están diseñadas para permitir la comunicación entre máquinas con este propósito precisamente.

El primer paso en la configuración de una cuenta de servicio para la aplicación de cadena de suministro de Cymbal Superstore es crearla.

Luego, debes asignarle permisos a la cuenta de servicio que creaste.

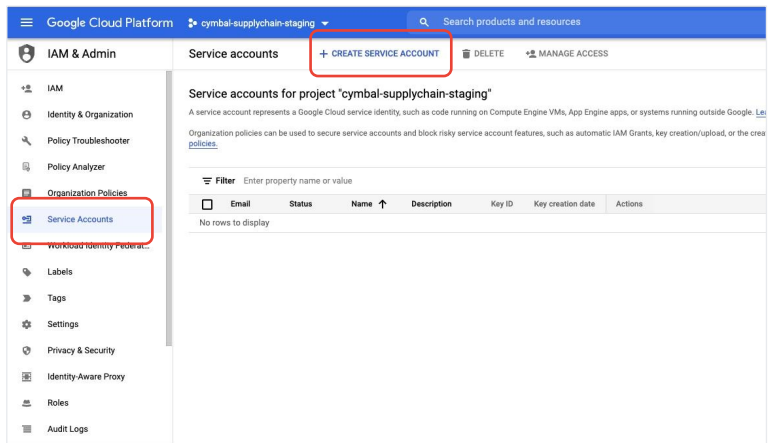
Por último, debes adjuntar esa cuenta de servicio a una VM de Compute Engine. Cuando se adjunta una cuenta de servicio, la VM y todas las aplicaciones que se ejecutan en ella usan los permisos asignados a esa cuenta.

Analicemos estos pasos con más detalle.

01

Crear una cuenta de servicio:

Dónde buscar



Google Cloud

Ve al proyecto en el que quieres agregar la cuenta de servicio. Las cuentas de servicio son identidades y recursos administrados de Google Cloud. Selecciona el vínculo de la **cuenta de servicio** en el menú IAM de tu proyecto.

Luego, selecciona **Crear cuenta de servicio**.

01

Crear una cuenta de servicio: Ingresa los detalles de la cuenta de servicio

Google Cloud Platform cymbal-supplychain-staging Search products and resources

IAM & Admin

1 Service account details

Service account name
vm-service-account

Display name for this service account

Service account ID
vm-service-account @helpful-chiller-326713.iam.gserviceaccount.com

Service account description
service account to be attached to vm's for supply chain app

Describe what this service account will do

CREATE AND CONTINUE

2 Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

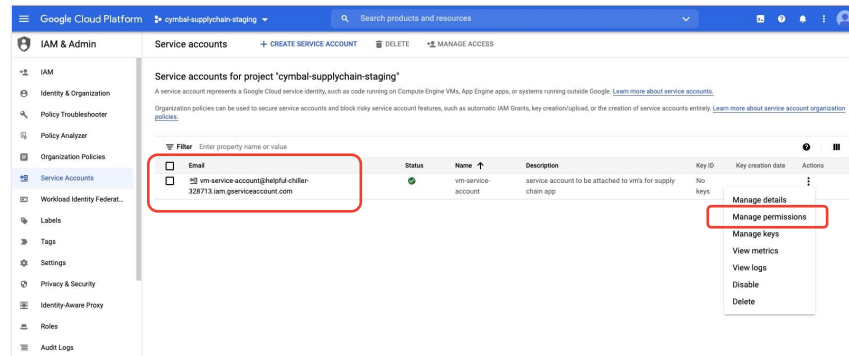
DONE CANCEL

Google Cloud

En el diálogo que aparece, asigna un nombre a la cuenta de servicio y toma nota de la dirección de correo electrónico asociada. También puedes ingresar una descripción sobre la función de esta cuenta de servicio.

02

Asignar permisos: Dónde buscar



Google Cloud

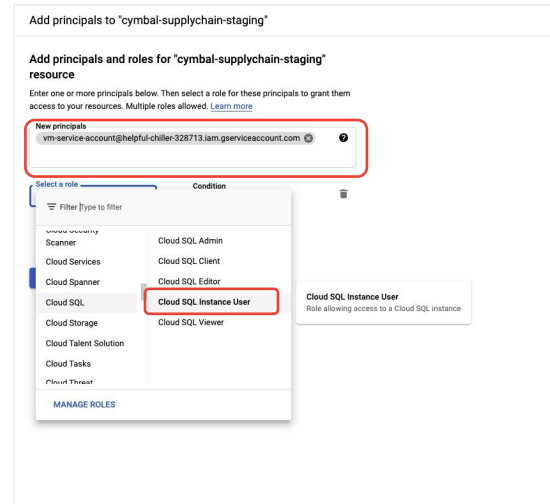
Una vez que selecciones **Crear y continuar** (Create and continue), la nueva cuenta de servicio se agregará a la lista de todas tus cuentas de servicio.

Selecciona los tres puntos que se encuentran debajo de "Acciones" para ver una lista de todas las acciones que puedes realizar en tu cuenta de servicio nueva.

Más adelante, usaremos una de estas opciones para administrar los permisos de la cuenta de servicio.

02

Asignar permisos: Agrega los permisos necesarios



Google Cloud

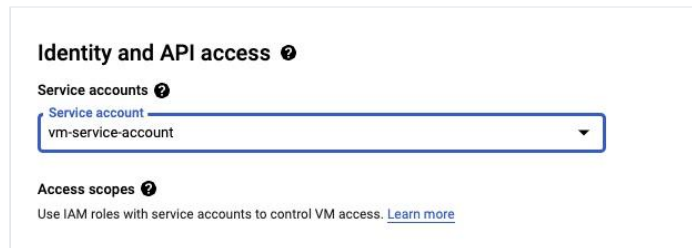
Selecciona **Administrar permisos** (Manage permissions) debajo del encabezado Acciones (Actions) que aparece en la lista de cuentas de servicio. Se abrirá un nuevo menú que te permitirá elegir tu cuenta de servicio y agregarle permisos.

Copia el identificador de la dirección de correo electrónico de tu cuenta de servicio. Busca o explora los permisos a fin de encontrar los que debes agregar. En este ejemplo, le otorgaremos los permisos de un Usuario de instancia de Cloud SQL a nuestra cuenta de servicio.

03

Agregar a una instancia de VM

Dónde buscar



Identity and API access ⓘ

Service accounts ⓘ

Service account
vm-service-account ▼

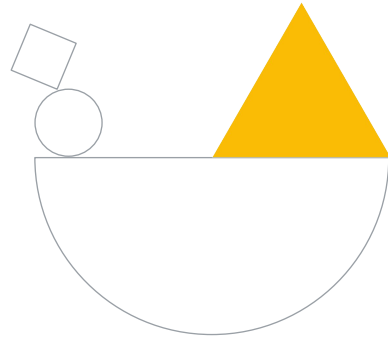
Access scopes ⓘ

Use IAM roles with service accounts to control VM access. [Learn more](#)

Google Cloud

Por último, puedes agregar la cuenta de servicio a tu instancia de VM en la sección Identidad y acceso a la API. Esto incluye la autorización. La autenticación de las cuentas de usuario y las de servicio es otro aspecto importante que debes conocer como Associate Cloud Engineer.

Preguntas de diagnóstico



Google Cloud

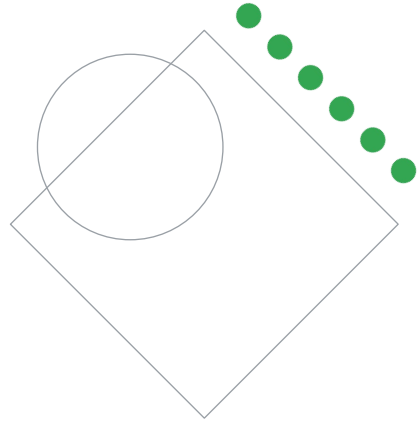
Ahora que tienes algo de contexto sobre los objetivos en esta sección del examen, es momento de realizar un autodiagnóstico centrado en la configuración del acceso y la seguridad de las soluciones de Google Cloud.

Responde las preguntas de diagnóstico ahora

- En la misma sección que esta lección, encontrarás el vínculo a la versión en PDF (Lectura) de las preguntas de diagnóstico del módulo.
- Las preguntas de diagnóstico también están disponibles en el cuaderno de ejercicios.



Revisión y plan de estudios

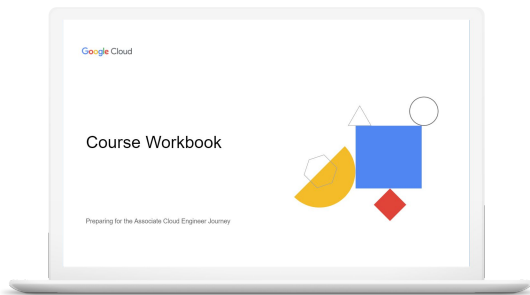


Google Cloud

¿En qué áreas debes desarrollar tus habilidades para administrar correctamente el acceso de las soluciones de Google Cloud? Recuerda que esta sección del examen tiene un alcance menos amplio, pero es igualmente importante para el rol de Associate Cloud Engineer. Revisemos las preguntas de diagnóstico para que puedas orientar el tiempo de estudio y centrarte en las áreas en las que debes desarrollar sus habilidades.

Tu plan de estudios:

Asegura la operación exitosa de una solución en la nube



5.1

Administra Identity and Access Management (IAM)

5.2

Administra cuentas de servicio

5.3

Consultar registros de auditoría

Google Cloud

En la revisión, veremos los objetivos de esta sección del examen y las preguntas que acabas de responder sobre cada uno de ellos. Presentaremos un objetivo, revisaremos brevemente las respuestas a las preguntas relacionadas y hablaremos sobre dónde puedes encontrar más información en los recursos de aprendizaje o en la documentación de Google Cloud. A medida que revisemos el objetivo de cada sección, usa la página del cuaderno de ejercicios para marcar la documentación, los cursos (y módulos) y las insignias de habilidad específicas que quieras enfatizar en tu plan de estudios.

Si bien esta sección cuenta con menos objetivos y tareas, recuerda tenerlos en cuenta al momento de estudiar.

5.1 | Administra Identity and Access Management (IAM)

Se incluyen las siguientes tareas:

- Visualizar las políticas de IAM
- Crear políticas de IAM
- Administrar los distintos tipos de roles y definir roles de IAM personalizados (p. ej., básicos, predefinidos y personalizados)

Google Cloud

En una sección previa del curso, trabajamos en la planificación de una jerarquía de recursos de Cymbal Superstore. La organización está dividida en carpetas, y las carpetas en proyectos. Identity and Access Management permite que tus usuarios y grupos accedan a los recursos de Google Cloud. Como Associate Cloud Engineer, es importante que sepas qué usuarios y grupos implementar según las necesidades de Cymbal Superstore y cómo implementarlos.

Las tareas comprendidas en esta parte de tu trabajo como Associate Cloud Engineer incluyen ver y crear políticas de IAM, y saber cuándo implementar los distintos tipos de políticas, como los roles básicos, predefinidos y personalizados.

Estas son las preguntas de diagnóstico que respondiste en relación con esta área:

Pregunta 1: Identifica los tipos de miembros a los que puedes asignarles acceso en IAM.

Pregunta 2: Describe cómo asignar roles en la interfaz de IAM.

Pregunta 3: Enumera los pasos necesarios para crear un rol personalizado en IAM.

5.1 | Análisis de la pregunta de diagnóstico 1



Debes configurar el acceso a Cloud Spanner desde el clúster de GKE que está respaldando la aplicación de microservicios de comercio electrónico de Cymbal Superstore. Debes especificar un tipo de cuenta para configurar los permisos apropiados.

¿Qué deberías hacer?

- A. Asignar permisos a una Cuenta de Google a la que haga referencia la aplicación
- B. Asignar permisos mediante una cuenta de Google Workspace a la que haga referencia la aplicación
- C. Asignar permisos mediante una cuenta de servicio a la que haga referencia la aplicación
- D. Asignar permisos mediante una cuenta de Cloud Identity a la que haga referencia la aplicación

Google Cloud

Pregunta:


Debes configurar el acceso a Cloud Spanner desde el clúster de GKE que está respaldando la aplicación de microservicios de comercio electrónico de Cymbal Superstore. Debes especificar un tipo de cuenta para configurar los permisos apropiados. ¿Qué deberías hacer?

5.1 | Análisis de la pregunta de diagnóstico 1



Debes configurar el acceso a Cloud Spanner desde el clúster de GKE que está respaldando la aplicación de microservicios de comercio electrónico de Cymbal Superstore. Debes especificar un tipo de cuenta para configurar los permisos apropiados.

¿Qué deberías hacer?

- A. Asignar permisos a una Cuenta de Google a la que haga referencia la aplicación
- B. Asignar permisos mediante una cuenta de Google Workspace a la que haga referencia la aplicación
- C. Asignar permisos mediante una cuenta de servicio a la que haga referencia la aplicación 
- D. Asignar permisos mediante una cuenta de Cloud Identity a la que haga referencia la aplicación

Google Cloud

Comentarios:

A. Asignar permisos a una Cuenta de Google a la que haga referencia la aplicación.

Comentarios: Incorrecto. Una Cuenta de Google usa un nombre de usuario y contraseña para autenticar a un usuario. Una aplicación no realiza la autenticación de forma interactiva con este tipo de cuenta.

B. Asignar permisos mediante una cuenta de Google Workspace a la que haga referencia la aplicación.

Comentarios: Incorrecto. Una cuenta de Google Workspace es una cuenta que creas como parte de una organización que usa productos de Google Workspace para trabajar de forma colaborativa. No es adecuada para administrar los permisos que una aplicación necesita a fin de comunicarse con un backend.

*C. Asignar permisos mediante una cuenta de servicio a la que haga referencia la aplicación

Comentarios: Correcto. Una cuenta de servicio usa una identidad de cuenta y una clave de acceso. Las aplicaciones las usan para conectarse con los servicios.

D. Asignar permisos mediante una cuenta de Cloud Identity a la que haga referencia la aplicación.

Comentarios: Incorrecto. Cloud Identity es una herramienta de administración de usuarios que se usa para proporcionar credenciales de acceso a los usuarios de una organización que no cuentan con las herramientas de colaboración de Google Workspace. Cloud Identity no se usa para administrar la autenticación de la

aplicación.

Dónde buscar:

<https://cloud.google.com/iam/docs/overview>

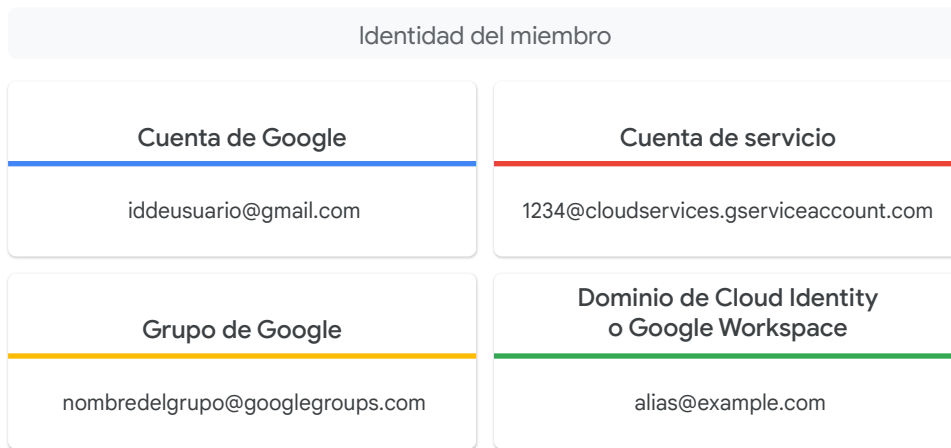
Mapa de contenidos:

- Google Cloud Fundamentals: Core Infrastructure (ILT y a pedido)
 - M2 Recursos y acceso en la nube
- Architecting with Google Compute Engine (ILT)
 - M4 Identity and Access Management
- Essential Google Cloud Infrastructure: Core Services (a pedido)
 - M1 Identity and Access Management
- Insignia de habilidad: Set Up and Configure a Cloud Environment in Google Cloud (https://www.cloudskillsboost.google/course_templates/625)

Resumen:

Explicación/resumen en la siguiente diapositiva.

Asigna acceso a los miembros con IAM



Google Cloud

Una Cuenta de Google representa a cualquier persona que interactúe con Google Cloud. Cuando te registras para obtener una Cuenta de Google, se te pedirá que proporciones una dirección de correo electrónico asociada con la cuenta. No es necesario que el correo electrónico provenga del dominio de Gmail.

Una cuenta de servicio es el medio por el que las aplicaciones y recursos autentican y acceden a los servicios en Google Cloud. Dado que las aplicaciones no pueden acceder de forma interactiva con un nombre de usuario y contraseña, las cuentas de servicio usan claves para realizar la autenticación.

Los Grupos de Google son conjuntos de principales de identidad a los que puede hacer referencia la dirección de correo electrónico asignada al grupo. Puedes aplicar políticas de acceso a un grupo. Cada miembro del grupo recibirá los permisos que especifiques en la política del grupo cuando se autentifiquen.

Los dominios de Google Workspace y Cloud Identity permiten administrar a los usuarios según el modo en que tu organización interactúa con Google. Cada método te brinda un grupo virtual que representa a todos los usuarios registrados en tu organización y te permite agregar, modificar y borrar usuarios y grupos.

5.1 | Análisis de la pregunta de diagnóstico 2



Estás intentando asignar roles a los proyectos de desarrollo y producción de la aplicación de comercio electrónico de Cymbal Superstore, pero recibes un error cuando quieres ejecutar la política **set-iam policy**. Los proyectos están organizados en una carpeta de comercio electrónico en la jerarquía de la organización de Cymbal Superstore. Quieres seguir las prácticas recomendadas para los permisos que necesitas y, al mismo tiempo, respetar el principio de privilegio mínimo.

¿Qué deberías hacer?

- A. Pedirle a tu administrador los roles de `resource manager.projects.setIamPolicy` para cada proyecto
- B. Pedirle a tu administrador los roles de `roles/resource manager.folderIamAdmin` para cada carpeta de comercio electrónico
- C. Pedirle a tu administrador el rol de `roles/resource manager.organizationAdmin` para Cymbal Superstore
- D. Pedirle a tu administrador los roles de `roles/iam.securityAdmin` en IAM

Google Cloud

Pregunta:

Estás intentando asignar roles a los proyectos de desarrollo y producción de la aplicación de comercio electrónico de Cymbal Superstore, pero recibes un error cuando quieres ejecutar la política **set-iam policy**. Los proyectos están organizados en una carpeta de comercio electrónico en la jerarquía de la organización de Cymbal Superstore. Quieres seguir las prácticas recomendadas para los permisos que necesitas y, al mismo tiempo, respetar el principio de privilegio mínimo. ¿Qué deberías hacer?

5.1 | Análisis de la pregunta de diagnóstico 2



Estás intentando asignar roles a los proyectos de desarrollo y producción de la aplicación de comercio electrónico de Cymbal Superstore, pero recibes un error cuando quieres ejecutar la política **set-iam policy**. Los proyectos están organizados en una carpeta de comercio electrónico en la jerarquía de la organización de Cymbal Superstore. Quieres seguir las prácticas recomendadas para los permisos que necesitas y, al mismo tiempo, respetar el principio de privilegio mínimo.

¿Qué deberías hacer?

- A. Pedirle a tu administrador los roles de `resourcemanager.projects.setIamPolicy` para cada proyecto
- B. Pedirle a tu administrador los roles de `roles/resourcemanager.folderIamAdmin` para cada carpeta de comercio electrónico
- C. Pedirle a tu administrador el rol de `roles/resourcemanager.organizationAdmin` para Cymbal Superstore
- D. Pedirle a tu administrador los roles de `roles/iam.securityAdmin` en IAM



Google Cloud

Comentarios:

A. Pedirle a tu administrador los roles de

`resourcemanager.projects.setIamPolicy` para cada proyecto

Comentarios: Incorrecto. La práctica recomendada es minimizar la cantidad de políticas de acceso necesarias.

*B. Pedirle a tu administrador los roles de

`roles/resourcemanager.folderIamAdmin` para la carpeta de comercio electrónico

Comentarios: Correcto. Con esta opción, obtienes los permisos necesarios y, al mismo tiempo, se minimiza la cantidad de recursos individuales para los que debes configurar permisos.

C. Pedirle a tu administrador el rol de

`roles/resourcemanager.organizationAdmin` para Cymbal Superstore

Comentarios: Incorrecto. Esta opción no cumple con los requisitos del principio de privilegio mínimo.

D. Pedirle a tu administrador los roles de `roles/iam.securityAdmin` en IAM

Comentarios: Incorrecto. El rol de Administrador de seguridad te permite acceder a la mayoría de los recursos de Google Cloud. La asignación de este rol no cumple con los requisitos de privilegio mínimo.

Dónde buscar:

https://cloud.google.com/architecture/prepare-kubernetes-engine-for-prod#managing_identity_and_access

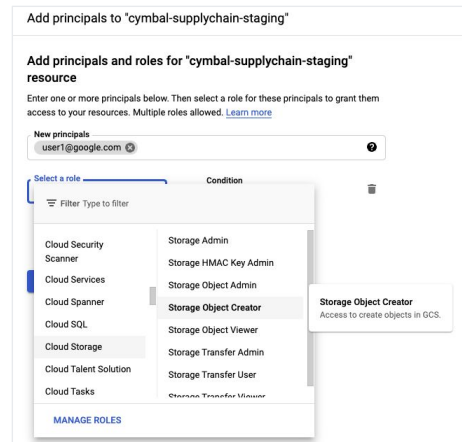
Mapa de contenidos:

- Google Cloud Fundamentals: Core Infrastructure (ILT y a pedido)
 - M2 Recursos y acceso en la nube
- Architecting with Google Compute Engine (ILT)
 - M4 Identity and Access Management
- Essential Google Cloud Infrastructure: Core Services (a pedido)
 - M1 Identity and Access Management
- Insignia de habilidad: Set Up and Configure a Cloud Environment in Google Cloud (https://www.cloudskillsboost.google/course_templates/625)

Resumen:

Explicación/resumen en la siguiente diapositiva.

Asigna roles en la interfaz de IAM



Google Cloud

Estos son los pasos necesarios para asignar roles en la interfaz de IAM.

1. Ir a la página de IAM
2. Selecciona un proyecto, una carpeta o una organización.
3. Abre el panel de información si no está disponible.
4. Haz clic en Permisos.
5. Selecciona o agrega la principal a la cual le agregarás un rol.
 - a. Si la principal ya existe, haz clic en Agregar otro rol.
 - b. Para usar una principal nueva, haz clic en Agregar y, luego, ingresa la dirección de correo electrónico de la principal.
6. Selecciona el rol que deseas asignar.
7. Agrega una condición.
8. Haz clic en Guardar

5.1 | Análisis de la pregunta de diagnóstico 3



Tienes un rol personalizado implementado para la administración del entorno de desarrollo y pruebas de la aplicación de administración del transporte de Cymbal Superstore. Estás desarrollando una prueba piloto para usar Cloud Run en lugar de Cloud Functions. Quieres asegurarte de que tus administradores tengan el acceso correcto a los nuevos recursos.

¿Qué deberías hacer?

- A. Aplicar el cambio en el rol personalizado de forma local y ejecutar una actualización en él
- B. Borrar el rol personalizado y volver a crear uno nuevo con los permisos necesarios
- C. Copiar el rol existente, agregar los permisos nuevos a la copia y borrar el rol anterior
- D. Crear un rol nuevo con los permisos necesarios y migrar a los usuarios a él

Google Cloud

Pregunta:

Tienes un rol personalizado implementado para la administración del entorno de desarrollo y pruebas de la aplicación de administración del transporte de Cymbal Superstore. Estás desarrollando una prueba piloto para usar Cloud Run en lugar de Cloud Functions. Quieres asegurarte de que tus administradores tengan el acceso correcto a los nuevos recursos. ¿Qué deberías hacer?

5.1 | Análisis de la pregunta de diagnóstico 3



Tienes un rol personalizado implementado para la administración del entorno de desarrollo y pruebas de la aplicación de administración del transporte de Cymbal Superstore. Estás desarrollando una prueba piloto para usar Cloud Run en lugar de Cloud Functions. Quieres asegurarte de que tus administradores tengan el acceso correcto a los nuevos recursos.

¿Qué deberías hacer?

- A. Aplicar el cambio en el rol personalizado de forma local y ejecutar una actualización en él
- B. Borrar el rol personalizado y volver a crear uno nuevo con los permisos necesarios
- C. Copiar el rol existente, agregar los permisos nuevos a la copia y borrar el rol anterior
- D. Crear un rol nuevo con los permisos necesarios y migrar a los usuarios a él



Google Cloud

Comentarios:

*A. Aplicar el cambio en el rol personalizado de forma local y ejecutar una actualización en él

Comentarios: Correcto. Este es un proceso recomendado para actualizar un rol personalizado existente. Actualiza la política existente de forma local y escribe la política actualizada en Google Cloud. Los comandos de gcloud que se usan en este proceso incluyen los subcomandos get y updatePolicy.

B. Borrar el rol personalizado y volver a crear uno nuevo con los permisos necesarios

Comentarios: Incorrecto. No es necesario volver a crear un rol personalizado en este caso. Puedes actualizar el existente.

C. Copiar el rol existente, agregar los permisos nuevos a la copia y borrar el rol anterior

Comentarios: Incorrecto. Si copias un rol existente, se creará un rol personalizado nuevo. No es necesario crear un rol personalizado nuevo en este caso.

D. Crear un rol nuevo con los permisos necesarios y migrar a los usuarios a él

Comentarios: Incorrecto. Encontrar a todos los usuarios con este rol y volver a asignarlos puede requerir mucho tiempo. En su lugar, debes actualizar el rol personalizado existente.

Dónde buscar:

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

Mapa de contenidos:

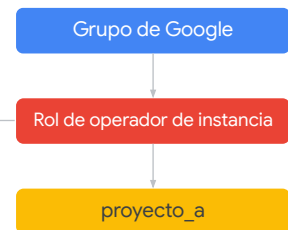
- Architecting with Google Compute Engine (ILT)
 - M4 Identity and Access Management
- Essential Google Cloud Infrastructure: Core Services (a pedido)
 - M1 Identity and Access Management
- Insignia de habilidad: Set Up and Configure a Cloud Environment in Google Cloud (https://www.cloudskillsboost.google/course_templates/625)

Resumen:

Explicación/resumen en la siguiente diapositiva.

Crea roles personalizados

- ✓ `compute.instances.get`
- ✓ `compute.instances.list`
- ✓ `compute.instances.start`
- ✓ `compute.instances.stop`



Google Cloud

Lo primero que debes hacer cuando creas permisos personalizados es familiarizarte con los permisos y roles que están disponibles en tu proyecto o en tu organización.

El comando de gcloud que debe ejecutar es:

```
gcloud iam list-testable-permissions <full-resource-name>
```

Para asegurarte de que no haya otro rol existente que pueda satisfacer tus necesidades, puedes consultar los metadatos de un rol a fin de ver los permisos que tiene asignados. Los metadatos de un rol incluyen el ID del rol y los permisos asociados con ese rol.

Los roles personalizados se pueden crear al nivel del proyecto o de la organización.

Debes contar con el permiso `iam.roles.create`. Debes ser el propietario del grupo o proyecto, o tener un rol de administrador de la organización o de administrador de roles de IAM.

Puedes crear roles a partir de permisos individuales, o bien seleccionar permisos desde roles predefinidos.

Para actualizar un rol existente, ejecuta `roles.get()`, actualiza el rol de forma local y, luego, ejecuta `roles.patch()`.

5.1 | Administra Identity and Access Management (IAM)

Cursos

[Google Cloud Fundamentals: Core Infrastructure](#)

- M2 Recursos y acceso en la nube

[Architecting with Google Compute Engine](#)

- M4 Identity and Access Management (IAM)



=

[Essential Google Cloud Infrastructure: Core Services](#)

- M1 Identity and Access Management (IAM)



Insignia de habilidad



[Set Up and Configure a Cloud Environment in Google Cloud](#)

Documentación

[Descripción general | Documentación de IAM](#)

[Descripción general de la seguridad de Google Kubernetes Engine](#)

Dedicemos un momento a analizar los recursos que pueden ayudarte a desarrollar tu conocimiento y tus habilidades en esta área.

Los conceptos de las preguntas de diagnóstico que acabamos de revisar se abordan en estos módulos y documentos. Encontrarás esta lista en tu cuaderno de ejercicios, de modo que puedes anotar lo que deseas incluir más adelante cuando elabores tu plan de estudios. A partir de tu experiencia con las preguntas de diagnóstico, puede ser recomendable que incluyas algunos de estos recursos o todos.

[Google Cloud Fundamentals: Core Infrastructure \(a pedido\)](#)

[Architecting with Google Compute Engine \(ILT\)](#)

[Essential Google Cloud Infrastructure: Core Services \(a pedido\)](#)

[Set Up and Configure a Cloud Environment in Google Cloud \(insignia de habilidad\)](#)

<https://cloud.google.com/iam/docs/overview>

<https://cloud.google.com/kubernetes-engine/docs/concepts/security-overview>

5.2 | Administra cuentas de servicio

Se incluyen las siguientes tareas:

- Crear cuentas de servicio
- Usar cuentas de servicio en políticas de IAM con permisos mínimos
- Asignar cuentas de servicio a los recursos
- Administrar la IAM de una cuenta de servicio
- Administrar la identidad temporal como cuenta de servicio
- Crear y administrar credenciales de cuenta de servicio de corta duración

Google Cloud

Las tres aplicaciones de Cymbal Superstore que se migrarán cuentan con recursos de frontend y backend necesarios para implementar las soluciones finales. Ya analizamos los recursos que se necesitan para el almacenamiento del backend, como Cloud Spanner, Bigtable y Cloud SQL.

Hay otra cuestión relacionada con la seguridad que aún no hemos examinado en detalle. ¿Cómo habilitamos los requisitos de acceso entre máquinas o entre servidores para que la aplicación se comuniquen con esos backends?

Tomemos la aplicación de administración de la cadena de suministro como ejemplo. Los datos están almacenados en Cloud SQL. La aplicación necesita contar con permisos para escribir datos en el servicio de Cloud SQL.

¿Cómo haces para otorgarles a las VMs implementadas como parte de la aplicación de administración de la cadena de suministro los permisos necesarios para conectarse con la base de datos de Cloud SQL de un modo seguro?

La solución para el acceso entre máquinas es una cuenta de servicio. Como Associate Cloud Engineer, debes saber cómo crear una cuenta de servicio y asignarle roles. También debes saber cómo visualizar los permisos de una cuenta de servicio y permitir que otros usuarios hereden esos permisos, es decir, que actúen como una cuenta de servicio. Por último, dado que no acceden de forma interactiva como lo hacen los usuarios, las cuentas de servicio usan claves para la autenticación. Administrar esas claves y proporcionar credenciales temporales por medio de código son aspectos importantes que debes conocer para poder proteger tus soluciones en la nube.

Estas preguntas de diagnóstico se centran en la administración de las cuentas de servicio:

Pregunta 4: Diferencia las Cuentas de Google de las cuentas de servicio en IAM.

Pregunta 5: Identifica la sección de la API de Google que especifica un permiso de IAM.

5.2 | Análisis de la pregunta de diagnóstico 4



¿Cuál de estos ejemplos es una situación en la que deberías usar una cuenta de servicio?

- A. Para acceder directamente a los datos del usuario
- B. Para entornos de desarrollo
- C. Para análisis interactivos
- D. Para Pods de GKE individuales

Pregunta:

¿Cuál de estos ejemplos es una situación en la que deberías usar una cuenta de servicio?

5.2 | Análisis de la pregunta de diagnóstico 4



¿Cuál de estos ejemplos es una situación en la que deberías usar una cuenta de servicio?

- A. Para acceder directamente a los datos del usuario
- B. Para entornos de desarrollo
- C. Para análisis interactivos
- D. Para Pods de GKE individuales



Google Cloud

Comentarios:

A. Para acceder directamente a los datos del usuario

Comentarios: Incorrecto. Las cuentas de servicio no deberían usarse para acceder a los datos del usuario sin su consentimiento.

B. Para entornos de desarrollo

Comentarios: Incorrecto. Las cuentas de servicio no deberían usarse para los entornos de desarrollo. Usa las credenciales predeterminadas de la aplicación.

C. Para análisis interactivos

Comentarios: Incorrecto. Las cuentas de servicio deberían usarse para actividades sin supervisión que no requieren de la interacción de los usuarios.

*D. Para Pods de GKE individuales

Comentarios: Correcto. Durante la configuración del acceso de GKE, debes configurar cuentas de servicio específicas para cada Pod. Luego, debe usar Workload Identity para asignarlas a las cuentas de servicio específicas de Kubernetes.

Dónde buscar:

<https://cloud.google.com/docs/authentication/production#automatically>

Mapa de contenidos:

- Google Cloud Fundamentals: Core Infrastructure (ILT y a pedido)
 - M2 Recursos y acceso en la nube
- Architecting with Google Compute Engine (ILT)
 - M4 Identity and Access Management
- Essential Google Cloud Infrastructure: Core Services (a pedido)
 - M1 Identity and Access Management

Resumen:

Explicación/resumen en la siguiente diapositiva.

Crea, usa y asigna cuentas de servicios

01

Para crear una cuenta de servicio:

```
gcloud iam  
service-accounts create
```

02

Para asignar políticas:

```
gcloud projects  
add-iam-policy
```

03

Conecta una cuenta de servicio a un recurso cuando lo creas

```
gcloud compute instances create  
cymbal-vm --service-account \  
<name-of-service-account@gservic  
eaccount.com> \  
--scopes  
https://www.googleapis.com/auth/  
cloud-platform
```

Google Cloud

Crear una cuenta de servicio

https://cloud.google.com/iam/docs/creating-managing-service-accounts#creating_a_service_account

Para crear una cuenta de servicio, debes usar el comando “gcloud iam service-accounts create”.

Uso de las cuentas de servicio con las políticas de IAM

Para agregar una política a una cuenta de servicio, debes ejecutar el comando “gcloud projects add-iam-policy-binding”.

El argumento “--member” debe ser una cadena que comience con “serviceAccount:” y que tenga el ID de tu cuenta de servicio y un sufijo con la dirección de correo electrónico “@project_id.iam.gserviceaccount.com”. El argumento “--role” contiene el rol que deseas asignar a la cuenta de servicio.

Asignar cuentas de servicio a los recursos

Los recursos en Google Cloud se pueden asignar a una cuenta de servicio que actúe como la identidad predeterminada del recurso. Este proceso se conoce como adjuntar una cuenta de servicio a un recurso. El recurso, o las aplicaciones que se ejecutan en el recurso, actúan como la cuenta de servicio conectada para acceder a las APIs de Google Cloud.

<https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances#using>

Varias instancias de máquina virtual pueden usar la misma cuenta de servicio, pero una máquina virtual solo puede tener una identidad de cuenta de servicio. Los cambios que se apliquen a la cuenta de servicio afectarán a todas las instancias de máquina virtual que usen la cuenta de servicio. Puedes usar un permiso "cloud-platform" para permitir el acceso a la mayoría de las API de Cloud y, luego, otorgarle a la cuenta de servicio los roles de IAM correspondientes.

En gcloud, puedes identificar la cuenta de servicio que deseas usar con el argumento "--service-account".

<https://developers.google.com/identity/protocols/oauth2/service-account#python>

Hay dos tipos de clave disponibles para la autenticación de una cuenta de servicio: las claves administradas por el usuario y las claves administradas por Google. Puedes crear y gestionar las claves administradas por el usuario tú mismo. Google solo almacena la clave pública.

Con las claves administradas por Google, Google almacena tanto la parte pública como la privada de las claves. Google cuenta con API que puedes usar para firmar las solicitudes con la clave privada.

5.2 | Análisis de la pregunta de diagnóstico 5



Cymbal Superstore está implementando una aplicación para dispositivos móviles con el fin de que los usuarios finales puedan hacer un seguimiento del envío de sus entregas. La aplicación necesita acceder a los datos sobre la ubicación de los vehículos desde Pub/Sub con las prácticas recomendadas de Google.

- A. Clave de API
- B. Cliente de OAuth 2.0
- C. Cuenta de servicio proporcionada por el entorno
- D. Clave de cuenta de servicio

¿Qué tipo de credenciales deberías usar?

Google Cloud

Pregunta:

Cymbal Superstore está implementando una aplicación para dispositivos móviles con el fin de que los usuarios finales puedan hacer un seguimiento del envío de sus entregas. La aplicación necesita acceder a los datos sobre la ubicación de los vehículos desde Pub/Sub con las prácticas recomendadas de Google. ¿Qué tipo de credenciales deberías usar?

5.2 | Análisis de la pregunta de diagnóstico 5



Cymbal Superstore está implementando una aplicación para dispositivos móviles con el fin de que los usuarios finales puedan hacer un seguimiento del envío de sus entregas. La aplicación necesita acceder a los datos sobre la ubicación de los vehículos desde Pub/Sub con las prácticas recomendadas de Google.

- A. Clave de API
- B. Cliente de OAuth 2.0
- C. Cuenta de servicio proporcionada por el entorno
- D. Clave de cuenta de servicio



¿Qué tipo de credenciales deberías usar?

Google Cloud

Comentarios:

A. Clave de API

Comentarios: Incorrecto. Las claves de API se usan para acceder a datos disponibles públicamente.

B. Cliente de OAuth 2.0

Comentarios: Incorrecto. Los clientes de OAuth 2.0 ofrecen acceso a los datos privados de una aplicación en nombre de los usuarios finales.

C. Cuenta de servicio proporcionada por el entorno

Comentarios: Incorrecto. Las cuentas de servicio proporcionadas por el entorno son para las aplicaciones que se ejecutan en los recursos dentro de Google Cloud.

*D. Clave de cuenta de servicio

Comentarios: Correcto. Las claves de cuenta de servicio se usan para acceder a los datos privados, como la información de los vehículos de Pub/Sub, desde un entorno externo, como una aplicación para dispositivos móviles que se ejecuta en un teléfono.

Dónde buscar:

<https://cloud.google.com/docs/authentication/>

Mapa de contenidos:

- Architecting with Google Compute Engine (ILT)
 - M4 Identity and Access Management
- Essential Google Cloud Infrastructure: Core Services (a pedido)
 - M1 Identity and Access Management

Resumen:

Explicación/resumen en la siguiente diapositiva.

Tipos de clave de autenticación



Google Cloud

Las credenciales de la aplicación se basan en los recursos a los que necesita acceder la aplicación y desde dónde necesita ejecutarlos.

- Si quieres acceder a datos públicos, la recomendación es usar una clave de API.
- Si quieres acceder a datos privados en nombre de un usuario final, deberías usar el cliente de OAuth2.0 de la API.
- Si quieres acceder a datos privados en nombre de una cuenta de servicio adjunta a recursos que están dentro del entorno de Google Cloud, deberías usar una cuenta de servicio proporcionada por el entorno.
- Si quieres acceder a datos privados en nombre de una cuenta de servicio que se está ejecutando fuera de Google Cloud, deberías crear y usar una clave de cuenta de servicio.

5.2 | Administra cuentas de servicio

Cursos

[Google Cloud Fundamentals: Core Infrastructure](#)

- M2 Recursos y acceso en la nube

[Architecting with Google Compute Engine](#)

- M4 Identity and Access Management (IAM)



=

[Essential Google Cloud Infrastructure: Core Services](#)

- M1 Identity and Access Management (IAM)



Documentación

[Autenticación como una cuenta de servicio | Autenticación](#)

[Descripción general de la autenticación](#)

Dediquemos un momento a analizar los recursos que pueden ayudarte a desarrollar tu conocimiento y tus habilidades en esta área.

Los conceptos de las preguntas de diagnóstico que acabamos de revisar se abordan en estos módulos y documentos. Encontrarás esta lista en tu cuaderno de ejercicios, de modo que puedes anotar lo que deseas incluir más adelante cuando elabores tu plan de estudios. A partir de tu experiencia con las preguntas de diagnóstico, puede ser recomendable que incluyas algunos de estos recursos o todos.

[Google Cloud Fundamentals: Core Infrastructure \(a pedido\)](#)

[Architecting with Google Compute Engine \(ILT\)](#)

[Essential Google Cloud Infrastructure: Core Services \(a pedido\)](#)

<https://cloud.google.com/docs/authentication/production#automatically>

<https://cloud.google.com/docs/authentication/>

5.3 | Consultar registros de auditoría

Google Cloud

Google Cloud's operations suite ofrece registros de auditoría para que estés al tanto de quién hizo qué, a quién y cuándo. Esta es otra parte del escudo de seguridad que proporcionas cuando implementas una solución de Google Cloud. ¿Quién accedió a su aplicación de comercio electrónico y cuándo lo hizo? Supongamos que agregaste una instancia a su clúster de Cloud Spanner para brindar asistencia a los usuarios en una nueva área geográfica. Tu Registro de actividad de administrador registrará cuándo se creó la instancia nueva. Si necesitas ver una lista de tus instancias, se creará una entrada de `admin_read` de acceso a los datos. Cuando un usuario crea un carrito de compras y vuelve a acceder a él desde su dispositivo móvil en otro momento, se publica una entrada de registro de `data_read` por la transacción de lectura en el registro de acceso a los datos. Hacer un seguimiento de estas acciones importantes es un paso significativo en una estrategia de seguridad general.

La visualización de los registros de auditoría se incluyó en las siguientes preguntas:

Pregunta 6: Compare los distintos tipos de registros de auditoría.

Pregunta 7: Describa dónde se puede acceder a los Registros de auditoría de Cloud

5.3 | Análisis de la pregunta de diagnóstico 6



¿Qué Registro de auditoría de Cloud está inhabilitado en la configuración predeterminada con algunas excepciones?

- A. Registros de auditoría de actividad del administrador
- B. Registros de auditoría de acceso a los datos
- C. Registros de auditoría de eventos del sistema
- D. Registros de auditoría de política denegada

Pregunta:

¿Qué Registro de auditoría de Cloud está inhabilitado en la configuración predeterminada con algunas excepciones?

5.3 | Análisis de la pregunta de diagnóstico 6



¿Qué Registro de auditoría de Cloud está inhabilitado en la configuración predeterminada con algunas excepciones?

A. Registros de auditoría de actividad del administrador

B. Registros de auditoría de acceso a los datos



C. Registros de auditoría de eventos del sistema

D. Registros de auditoría de política denegada

Google Cloud

Comentarios:

A. Registros de auditoría de actividad del administrador

Comentarios: Incorrecto. Los Registros de auditoría de actividad de administrador siempre están habilitados y no se pueden inhabilitar.

*B. Registros de auditoría de acceso a los datos

Comentarios: Correcto. Los Registros de auditoría de acceso a los datos están inhabilitados de forma predeterminada, excepto en BigQuery.

C. Registros de auditoría de eventos del sistema

Comentarios: Incorrecto. Los Registros de auditoría de eventos del sistema están siempre habilitados.

D. Registros de auditoría de política denegada

Comentarios: Incorrecto. Los Registros de auditoría de política denegada están siempre habilitados y no se pueden inhabilitar.

Dónde buscar:

<https://cloud.google.com/logging/docs/audit>

Mapa de contenidos:

- Google Cloud Fundamentals: Core Infrastructure (ILT y a pedido)
 - M7 Desarrollo e implementación en la nube

- Architecting with Google Compute Engine (ILT)
 - M7 Supervisión de recursos
- Essential Google Cloud Infrastructure: Core Services (a pedido)
 - M4 Supervisión de recursos

Hay cuatro tipos de registros de auditoría disponibles para cada proyecto, carpeta y organización de Cloud.

- Los Registros de auditoría de la actividad del administrador tienen información sobre las llamadas a la API que crean o modifican los metadatos de los recursos. Por ejemplo, los Registros de auditoría de la actividad del administrador registran si se modifican los permisos de acceso o se crean instancias de VM. Los Registros de auditoría de la actividad del administrador están siempre habilitados. Estos no se pueden inhabilitar.
- Las entradas del Registro de auditoría de acceso a los datos se escriben cuando se lee la configuración o los metadatos de los recursos. Las llamadas para crear, modificar o leer los datos de los recursos también se escriben en los Registros de auditoría de acceso a los datos. Están inhabilitados de forma predeterminada.
- Los Registros de auditoría de eventos del sistema escriben las acciones que modifican la configuración de los recursos. Están siempre habilitados.
- Las entradas del Registro de auditoría de política denegada se crean cuando un servicio de Google Cloud deniega el acceso a un usuario o cuenta de servicio que no tiene el acceso correcto en la política de seguridad. Se generan de forma predeterminada y no se pueden inhabilitar.

5.3 | Análisis de la pregunta de diagnóstico 7



Estás configurando el registro de auditoría de Cloud Storage. Quieres saber cuándo se agregan objetos a un bucket.

¿Qué tipo de entrada de registro de auditoría deberías supervisar?

- A. Las entradas del Registro de actividad del administrador
- B. Las entradas de registro de ADMIN_READ
- C. Las entradas de registro de DATA_READ
- D. Las entradas de registro de DATA_WRITE

Google Cloud

Pregunta:

Estás configurando el registro de auditoría de Cloud Storage. Quieres saber cuándo se agregan objetos a un bucket. ¿Qué tipo de entrada de registro de auditoría deberías supervisar?

5.3 | Análisis de la pregunta de diagnóstico 7



Estás configurando el registro de auditoría de Cloud Storage. Quieres saber cuándo se agregan objetos a un bucket.

¿Qué tipo de entrada de registro de auditoría deberías supervisar?

- A. Las entradas del Registro de actividad del administrador
- B. Las entradas de registro de ADMIN_READ
- C. Las entradas de registro de DATA_READ
- D. Las entradas de registro de DATA_WRITE



Google Cloud

Comentarios:

A. Las entradas del Registro de actividad del administrador

Comentarios: Incorrecto. Los Registros de actividad del administrador escriben entradas cuando se crean y borran los buckets.

B. Las entradas de registro de ADMIN_READ

Comentarios: Incorrecto. Las entradas de registro de ADMIN_READ se crean cuando se muestran listas de los buckets y cuando se accede a los metadatos de los buckets.

C. Las entradas de registro de DATA_READ

Comentarios: Incorrecto. Las entradas de registro de DATA_READ registran operaciones como cuando se muestran listas o se obtienen datos de objetos.

*D. Las entradas de registro de DATA_WRITE

Comentarios: Correcto. Las entradas de registro de DATA_WRITE incluyen información sobre el momento en que se crean o borran objetos.

Dónde buscar:

<https://cloud.google.com/storage/docs/audit-logging>

Mapa de contenidos:

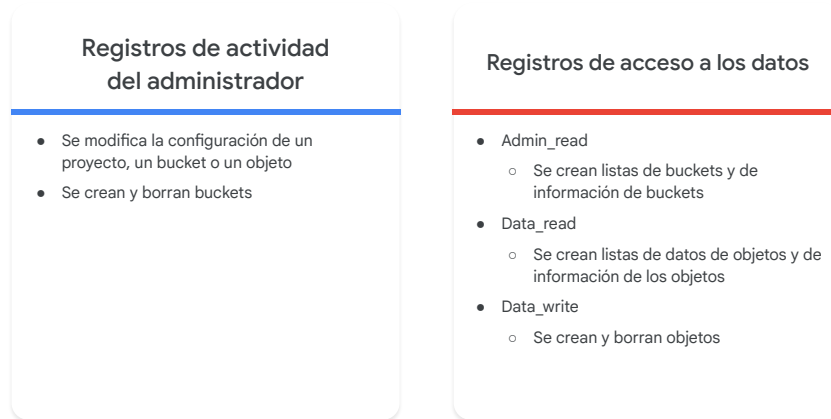
- Google Cloud Fundamentals: Core Infrastructure (ILT y a pedido)

- M7 Desarrollo e implementación en la nube
- Architecting with Google Compute Engine (ILT)
 - M7 Supervisión de recursos
- Essential Google Cloud Infrastructure: Core Services (a pedido)
 - M4 Supervisión de recursos

Resumen:

Explicación/resumen en la siguiente diapositiva.

Tipos de entradas en los registros de auditoría de Cloud Storage



Google Cloud

Los registros de auditoría de Cloud Storage incluyen los Registros de actividad del administrador y los Registros de acceso a los datos.

Los Registros de actividad del administrador incluyen entradas de cuando se modifica la configuración de un proyecto, de un bucket o de un objeto. También incluyen operaciones como la creación y eliminación de buckets.

Los Registros de acceso a los datos incluyen tres tipos de entradas diferentes: ADMIN_READ, DATA_READ y DATA_WRITE.

- Las entradas de ADMIN_READ incluyen las operaciones de crear listas de buckets y obtener metadatos de los buckets.
- Las entradas de DATA_READ incluyen las operaciones de crear listas y obtener datos de objetos.
- Las entradas de DATA_WRITE incluyen las operaciones de crear y borrar objetos.

5.3 | Consultar registros de auditoría

Cursos

[Google Cloud Fundamentals: Core Infrastructure](#)

- M7 Desarrollo e implementación en la nube

[Architecting with Google Compute Engine](#)

- M7 Supervisión de recursos



=

[Essential Google Cloud Infrastructure: Core Services](#)

- M4 Supervisión de recursos



Documentación

[Descripción general de los registros de auditoría de Cloud | Cloud Logging](#)

[Registros de auditoría de Cloud con Cloud Storage](#)

Dediquemos un momento a analizar los recursos que pueden ayudarte a desarrollar tu conocimiento y tus habilidades en esta área.

Los conceptos de las preguntas de diagnóstico que acabamos de revisar se abordan en estos módulos y documentos. Encontrarás esta lista en tu cuaderno de ejercicios, de modo que puedes anotar lo que deseas incluir más adelante cuando elabores tu plan de estudios. A partir de tu experiencia con las preguntas de diagnóstico, puede ser recomendable que incluyas algunos de estos recursos o todos.

[Google Cloud Fundamentals: Core Infrastructure \(a pedido\)](#)

[Architecting with Google Compute Engine \(ILT\)](#)

[Essential Google Cloud Infrastructure: Core Services \(a pedido\)](#)

<https://cloud.google.com/logging/docs/audit>

<https://cloud.google.com/storage/docs/audit-logging>