Cloud IAM proporciona las herramientas adecuadas para gestionar los permisos de recursos con la mínima complejidad y un alto nivel de automatización. No se otorgan permisos directamente a los usuarios, sino que se les asignan roles, que agrupan uno o más permisos. Esto permite asignar funciones laborales dentro de la empresa a grupos y roles. Los usuarios solo acceden a lo que necesitan para realizar su trabajo, y los administradores pueden otorgar fácilmente permisos predeterminados a grupos completos de usuarios.

Hay dos tipos de roles en Cloud IAM:

- Roles predefinidos
- Roles personalizados

Google crea y mantiene **los roles predefinidos . Sus permisos se actualizan automáticamente según sea necesario, por ejemplo, cuando se añaden nuevas funciones o servicios a Google Cloud.**

Los roles personalizados son definidos por el usuario y permiten agrupar uno o más permisos compatibles para satisfacer sus necesidades específicas. Google no mantiene los roles personalizados; cuando se añaden nuevos permisos, funciones o servicios a Google Cloud, los roles personalizados no se actualizan automáticamente. Para crear un rol personalizado, se combinan uno o más de los permisos de Cloud IAM disponibles. Los permisos permiten a los usuarios realizar acciones específicas en los recursos de Google Cloud.

Introducción a los roles personalizados de IAM

Cloud IAM también permite crear roles personalizados. Puede crear un rol personalizado con uno o más permisos y luego otorgarlo a los usuarios. Cloud IAM proporciona una interfaz de usuario y una API para crear y administrar roles personalizados.

Punto clave: Los roles personalizados le permiten aplicar el principio del mínimo privilegio, garantizando que las cuentas de usuario y de servicio de su organización solo tengan los permisos esenciales para realizar las funciones previstas.

Nota: Puede crear un rol personalizado a nivel de organización y de proyecto. Sin embargo, no puede crear roles personalizados a nivel de carpeta.

Puedes crear un rol personalizado combinando uno o más de los permisos de Cloud IAM disponibles. Los permisos permiten a los usuarios realizar acciones específicas en los recursos de Google Cloud.

En el mundo de Cloud IAM, los permisos se representan en el formato:

<servicio>.<recurso>.<verbo>

Por ejemplo, el compute.instances.listpermiso permite a un usuario enumerar las instancias de Compute Engine que posee, mientras que compute.instances.stoppermite a un usuario detener una VM.

Los permisos suelen corresponderse exactamente con los métodos REST, aunque no siempre. Es decir, cada servicio de Google Cloud tiene un permiso asociado para cada

método REST. Para llamar a un método, quien lo llama necesita ese permiso. Por ejemplo, quien llama topic.publish()necesita el pubsub.topics.publishpermiso.

Los roles personalizados solo se pueden usar para otorgar permisos en políticas del mismo proyecto u organización que posee los roles o recursos. No se pueden otorgar roles personalizados de un proyecto u organización a un recurso que pertenece a otro proyecto u organización.

Permisos y roles necesarios

Para crear un rol personalizado, el llamador debe tener iam.roles.createpermiso.

A los usuarios que no sean propietarios, incluidos los administradores de la organización, se les debe asignar el rol de Administrador de roles de organización (roles/iam.organizationRoleAdmin) o el rol de Administrador de roles de IAM (roles/iam.roleAdmin). El rol de Revisor de seguridad de IAM (roles/iam.securityReviewer) permite ver roles personalizados, pero no administrarlos.

La interfaz de usuario de roles personalizados se encuentra en la consola de Cloud, en Roles de IAM. Solo está disponible para los usuarios con permisos para crear o administrar roles personalizados. De forma predeterminada, solo los propietarios de proyectos pueden crear nuevos roles. Los propietarios de proyectos pueden controlar el acceso a esta función otorgando el rol de Administrador de roles de IAM a otros usuarios del mismo proyecto. En el caso de las organizaciones, solo los administradores de la organización pueden otorgar el rol de Administrador de roles de la organización.

Prepárese para crear un rol personalizado

Antes de crear un rol personalizado, es posible que quieras saber lo siguiente:

- ¿Qué permisos se pueden aplicar a un recurso?
- ¿Qué roles se pueden otorgar en un recurso?
- ¿Qué son los metadatos de un rol?

Tarea 1. Ver los permisos disponibles para un recurso

Antes de crear un rol personalizado, conviene saber qué permisos se pueden aplicar a un recurso. Puede obtener todos los permisos aplicables a un recurso y a los recursos inferiores en la jerarquía mediante la herramienta de línea de comandos de gcloud, Cloud Console o la API de IAM. Por ejemplo, puede obtener todos los permisos aplicables a una organización y a sus proyectos.

- Ejecute lo siguiente para obtener la lista de permisos disponibles para su proyecto:

```
gcloud iam list-testable-permissions
//cloudresourcemanager.googleapis.com/projects/$DEVSHELL_PROJECT_ID
```

Tarea 2. Obtener los metadatos del rol

Antes de crear un rol personalizado, conviene obtener los metadatos de los roles predefinidos y personalizados. Estos metadatos incluyen el ID y los permisos del rol. Puede consultarlos mediante Cloud Console o la API de IAM.

- Para ver los metadatos del rol, use el comando a continuación, reemplazando [ROLE_NAME]por el rol. Por ejemplo: roles/viewero roles/editor:

gcloud iam roles describe [ROLE_NAME]

Tarea 3. Ver los roles otorgables en los recursos

Utilice el gcloud iam list-grantable-rolescomando para devolver una lista de todos los roles que se pueden aplicar a un recurso determinado.

- Ejecute el siguiente gcloudcomando para enumerar los roles que se pueden otorgar desde su proyecto:

gcloud iam list-grantable-roles
//cloudresourcemanager.googleapis.com/projects/$DEVSHELL_PROJECT_ID

Tarea 4. Crear un rol personalizado

Para crear un rol personalizado, el usuario debe tener iam.roles.createpermiso. De forma predeterminada, el propietario de un proyecto u organización tiene este permiso y puede crear y administrar roles personalizados.

A los usuarios que no sean propietarios, incluidos los administradores de la organización, se les debe asignar el rol de Administrador de rol de organización o el rol de Administrador de rol de IAM.

Utilice el gcloud iam roles createcomando para crear nuevos roles personalizados de dos maneras:

- Proporcione un archivo YAML que contenga la definición del rol
- Especifique la definición del rol mediante indicadores

Al crear un rol personalizado, debe especificar si se aplica a nivel de organización o de proyecto mediante los indicadores --organization [ORGANIZATION_ID]o --project [PROJECT_ID]. Cada ejemplo a continuación crea un rol personalizado a nivel de proyecto.

En las siguientes secciones crearás roles personalizados a nivel de proyecto.

Crear un rol personalizado usando un archivo YAML

Cree un archivo YAML que contenga la definición de su rol personalizado. El archivo debe estar estructurado de la siguiente manera:

título: [TÍTULO DEL ROL]

Descripción: [DESCRIPCIÓN DEL ROL]

escenario: [ETAPA DE LANZAMIENTO]

Permisos incluidos:

- [PERMISO_1]

- [PERMISO_2]

Cada uno de los valores de marcador de posición se describe a continuación:

- [ROLE_TITLE]es un título amigable para el rol, como **Visor de roles** .
- [ROLE_DESCRIPTION]es una breve descripción sobre el rol, como **Mi descripción de rol personalizada** .
- [LAUNCH_STAGE]Indica la etapa de un rol en el ciclo de vida del lanzamiento, como ALPHA, BETA o GA.
- includedPermissionsespecifica la lista de uno o más permisos para incluir en el rol personalizado, como **iam.roles.get** .

1. ¡A empezar! Crea tu archivo YAML de definición de rol ejecutando:

nano role-definition.yaml

2. Agregue esta definición de rol personalizada al archivo YAML:

title: "Role Editor"

description: "Edit access for App Versions"

stage: "ALPHA"

includedPermissions:

- appengine.versions.create

- appengine.versions.delete

3. Luego guarde y cierre el archivo presionando **CTRL+X** , **Y** y luego **ENTER** .
4. Ejecute el siguiente gcloudcomando:

gcloud iam roles create editor --project $DEVSHELL_PROJECT_ID --file role-definition.yaml

Ahora usarás el método de bandera para crear un nuevo rol personalizado. Las banderas tienen un formato similar al del archivo YAML, por lo que reconocerás cómo se crea el comando.

- Ejecute el siguiente gcloudcomando para crear un nuevo rol usando banderas:

**gcloud iam roles create viewer --project $DEVSHELL_PROJECT_ID **

**--title "Role Viewer" --description "Custom role description." **

--permissions compute.instances.get,compute.instances.list --stage ALPHA

Tarea 5. Enumere los roles personalizados

1. Ejecute el siguiente gcloudcomando para enumerar roles personalizados, especificando roles personalizados a nivel de proyecto o de organización:

gcloud iam roles list --project $DEVSHELL_PROJECT_ID

Para enumerar los roles eliminados, también puedes especificar la --show-deletedbandera.

2. Ejecute el siguiente gcloudcomando para enumerar los roles predefinidos:

gcloud iam roles list

Tarea 6. Actualizar un rol personalizado existente

Un patrón común para actualizar los metadatos de un recurso, como un rol personalizado, consiste en leer su estado actual, actualizar los datos localmente y, a continuación, enviar los datos modificados para su escritura. Este patrón podría causar un conflicto si dos o más procesos independientes intentan la secuencia simultáneamente.

Por ejemplo, si dos propietarios de un proyecto intentan realizar cambios conflictivos en un rol al mismo tiempo, algunos cambios podrían fallar.

Cloud IAM soluciona este problema mediante una etagpropiedad en los roles personalizados. Esta propiedad se usa para verificar si el rol personalizado ha cambiado desde la última solicitud. Al realizar una solicitud a Cloud IAM con un valor de etag, Cloud IAM compara dicho valor con el existente asociado al rol personalizado. Solo registra el cambio si los valores de etag coinciden.

Utilice el gcloud iam roles updatecomando para actualizar roles personalizados de una de dos maneras:

- Un archivo YAML que contiene la definición de rol actualizada
- Banderas que especifican la definición de rol actualizada

Al actualizar un rol personalizado, debe especificar si se aplica a nivel de organización o de proyecto mediante los indicadores --organization [ORGANIZATION_ID]o --project [PROJECT_ID]. Cada ejemplo a continuación crea un rol personalizado a nivel de proyecto.

El describecomando devuelve la definición del rol e incluye un valor etag que identifica de forma única la versión actual del rol. El valor etag debe proporcionarse en la definición del rol actualizada para garantizar que no se sobrescriban los cambios simultáneos en el rol.

Actualizar un rol personalizado mediante un archivo YAML

1. Obtenga la definición actual del rol ejecutando el siguiente gcloudcomando, reemplazándolo [ROLE_ID]con **editor** .

gcloud iam roles describe [ROLE_ID] --project $DEVSHELL_PROJECT_ID

2. Copie la salida para usarla para crear un nuevo archivo YAML en los próximos pasos.
3. Crea un new-role-definition.yamlarchivo con tu editor:

nano new-role-definition.yaml

4. Pegue la salida del último comando y agregue estos dos permisos en includedPermissions:

- storage.buckets.get

- storage.buckets.list

5. Guarde y cierre el archivo **CTRL+X** , **Y** y luego **ENTER** .
6. Ahora usará el updatecomando para actualizar el rol. Ejecute el siguiente gcloudcomando, reemplazando [ROLE_ID]por **"editor"** :

gcloud iam roles update [ROLE_ID] --project $DEVSHELL_PROJECT_ID \

--file new-role-definition.yaml

Actualizar un rol personalizado usando indicadores

Cada parte de una definición de rol se puede actualizar mediante su indicador correspondiente. Para obtener una lista de todos los indicadores posibles en la documentación de referencia del SDK, consulte el tema "gcloud iam roles update" .

Utilice las siguientes banderas para agregar o eliminar permisos:

- --add-permissions:Agrega uno o más permisos separados por comas al rol.
- --remove-permissions:Elimina uno o más permisos separados por comas del rol.

Como alternativa, puede simplemente especificar los nuevos permisos utilizando la --permissions [PERMISSIONS]bandera y proporcionando una lista de permisos separados por comas para reemplazar la lista de permisos existente.

- Ejecute el siguiente gcloudcomando para agregar permisos al rol de **espectador** usando indicadores:

gcloud iam roles update viewer --project $DEVSHELL_PROJECT_ID \

--add-permissions storage.buckets.get,storage.buckets.list

Tarea 7. Deshabilitar un rol personalizado

Cuando se deshabilita un rol, se desactivan todos los enlaces de políticas relacionados con el rol, lo que significa que no se otorgarán los permisos en el rol, incluso si se otorga el rol a un usuario.

La forma más fácil de deshabilitar un rol personalizado existente es usar la --stagebandera y establecerlo como DESHABILITADO.

- Ejecute el siguiente gcloudcomando para deshabilitar la función de **espectador** :

gcloud iam roles update viewer --project $DEVSHELL_PROJECT_ID \

--stage DISABLED

Tarea 8. Eliminar un rol personalizado

- Utilice el gcloud iam roles deletecomando para eliminar un rol personalizado. Una vez eliminado, el rol queda inactivo y no se puede usar para crear nuevos enlaces de políticas de IAM:

gcloud iam roles delete viewer --project $DEVSHELL_PROJECT_ID

Tras eliminar el rol, las vinculaciones existentes se conservan, pero están inactivas. El rol se puede recuperar en un plazo de 7 días. Después de 7 días, el rol entra en un proceso de eliminación permanente que dura 30 días. Después de 37 días, el ID del rol puede volver a utilizarse.

Tarea 9. Restaurar un rol personalizado

- Dentro del plazo de 7 días, puede restaurar un rol. Los roles eliminados se encuentran en estado **DESACTIVADO** . Para que vuelvan a estar disponibles, actualice la --stagemarca:

gcloud iam roles undelete viewer --project $DEVSHELL_PROJECT_ID