Administración de identidades y accesos (IAM) de Cloud

Architecting with GCP Fundamentals: Infrastructure

CLOUD IAM, CLOUD RESOURCE MANAGER

CLOUD IAM

Última modificación: 27-11-2017

Programa

- **Administración de identidades y accesos (IAM) de Cloud**
- Organización
- Funciones
- Miembros
- Cuentas de servicio
- Recomendaciones de Cloud IAM
- Cuestionario
- Lab

Google Cloud

Administración de identidades y accesos de Cloud

Quién

puede hacer qué

con qué recurso

Google Cloud

Los **propietarios del proyecto** invitan a los miembros a los proyectos y les otorgan funciones. Las funciones consisten en un conjunto de permisos para uno o más recursos.

Objetos de Cloud IAM

- Organización
- Carpetas
- Proyectos
- Miembros
- Funciones
- Recursos
- Productos
- Administradores avanzados de G Suite

Google Cloud

Jerarquía de recursos de Cloud IAM

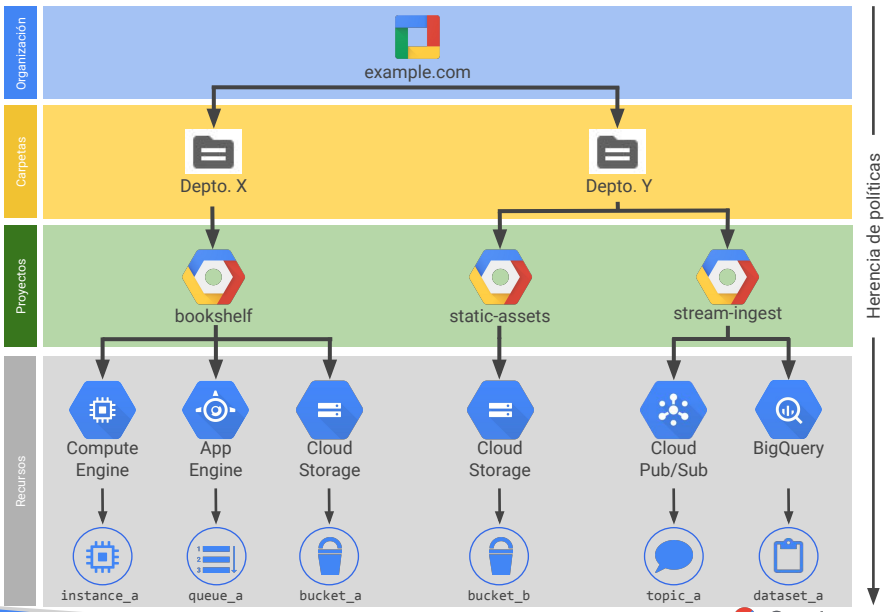
Se establece una política para un recurso y cada política contiene lo siguiente:

- Funciones
- Miembros de la función

Los recursos heredan políticas de un elemento superior:

- Las políticas de recursos son una unión del elemento superior y del recurso.

Si la política del elemento superior es menos restrictiva, anula la política del recurso más restrictiva.



Los recursos de Google Cloud Platform se organizan jerárquicamente, de modo que el nodo de la organización es el nodo raíz de la jerarquía, los proyectos son los elementos secundarios de la organización y los otros recursos son los elementos secundarios de los proyectos. Cada recurso tiene exactamente un elemento superior.

Cloud IAM le permite establecer políticas en los siguientes niveles de la jerarquía de recursos:

- Nivel de la organización: el recurso de la organización representa a su empresa. Todos los recursos de la organización heredan las funciones de Cloud IAM otorgadas en este nivel.
- Nivel del proyecto: los proyectos representa un límite de confianza dentro de su empresa. Los servicios dentro del mismo proyecto tienen un nivel de confianza predeterminado. Por ejemplo, las instancias de App Engine pueden acceder a los depósitos de Cloud Storage dentro del mismo proyecto. Los recursos dentro de ese proyecto heredan las funciones de Cloud IAM otorgadas a nivel del proyecto. Cuando establezca las políticas a nivel del proyecto, asegúrese de utilizar los registros de auditoría para hacer un seguimiento de los cambios de permisos a nivel de proyecto.
- Nivel del recurso: además de los sistemas existentes de LCA de BigQuery y Cloud Storage, los recursos adicionales, como los temas de Pub/Sub y los conjuntos de datos de Genomics, son compatibles con las funciones a nivel del recurso, a fin de que pueda otorgar a ciertos usuarios el permiso para utilizar un solo recurso.

Los recursos heredan las políticas del recurso superior. Si establece una política a nivel de la organización, todos sus proyectos secundarios la heredan automáticamente y, si establece una política a nivel de proyecto, todos sus recursos secundarios la heredan. La política eficaz para un recurso es la unión de la política establecida en ese recurso y la política heredada de su elemento superior. Esta herencia de política es transitiva, es decir que los recursos heredan políticas del proyecto, que hereda las políticas de la organización. Por lo tanto, las políticas a nivel de la organización también se aplican a nivel del recurso.

La jerarquía de la política de Cloud IAM sigue la misma ruta de la jerarquía de recursos de GCP. Si cambia la jerarquía de recursos, también cambia la jerarquía de políticas. Por ejemplo, trasladar un proyecto a la organización actualizará la política de Cloud IAM del proyecto para heredar la política de Cloud IAM de la organización.

Las políticas secundarias no pueden restringir el acceso otorgado en el nivel superior. Por ejemplo, si otorga la función de Editor a un usuario para un proyecto y otorga la función de Lector al mismo usuario para un recurso secundario, el usuario sigue teniendo la función de Editor para el recurso secundario.
Cuando utiliza Cloud IAM, una recomendación es seguir el principio de privilegios mínimos. El principio se aplica a identidades, funciones y recursos. Siempre seleccione el alcance mínimo que es necesario para reducir su exposición al riesgo. No quisiera otorgar a todos la función de Propietario para la organización completa: las modificaciones intencionales o los errores accidentales podrían desactivar sus aplicaciones. Es recomendable que sea específico y actúe a conciencia. Asigne a un grupo de administradores de seguridad específico la función de administrador de seguridad para controlar las reglas de firewall y SSL de proyectos específicos.

Para obtener más información, consulte: Resumen de administración de identidades y accesos

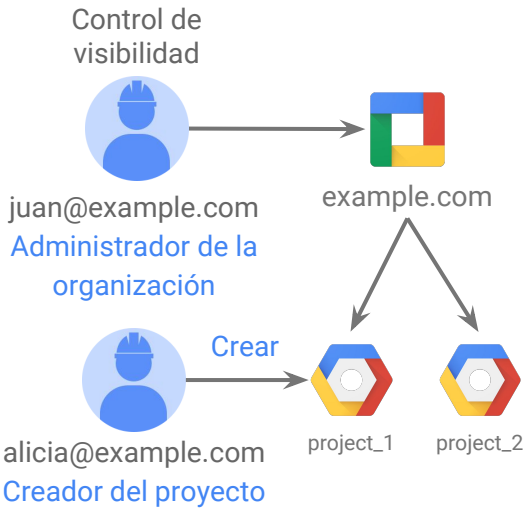
Programa

- Administración de identidades y accesos (IAM) de Cloud
- **Organización**
- Funciones
- Miembros
- Cuentas de servicio
- Recomendaciones de Cloud IAM
- Cuestionario
- Lab

Google Cloud

Nodo de organización

- Un nodo de organización es un nodo raíz para los recursos de Google Cloud.
- Funciones de la organización:
  - **Administrador de la organización:** controla todos los recursos de la nube; útil para auditorías
  - **Creador del proyecto:** controla la creación del proyecto; controla quién puede crear proyectos



Google Cloud

Para obtener más información, consulte:
https://cloud.google.com/resource-manager/docs/quickstart-organizations

Administrar una gran cantidad de proyectos puede volverse difícil a gran escala. Por eso, Cloud IAM incluye el concepto de *nodo de organización*. El nodo de organización se encuentra por encima de los proyectos y es el nodo raíz de su empresa para los recursos de Google Cloud. Si tiene una cuenta de Google for Work, cuando habilita el nodo de la organización, cualquier proyecto creado por los usuarios en su dominio pertenecerá automáticamente al nodo de su organización; ya no habrá proyectos paralelos ni administradores no autorizados.

La función de Administrador de la organización le brinda a su administrador visibilidad y control de todos los recursos de su empresa en Google Cloud Platform. Con la función de Creador del proyecto, puede aplicar restricciones sobre quién puede crear proyectos, independientemente de si tienen políticas para proyectos individuales. Las funciones del proyecto también se pueden aplicar a nivel de la organización y todos los proyectos de su empresa pueden heredarlas. Por ejemplo, puede asignar a su equipo de herramientas de redes la función de Administrador de red a nivel de la organización, de modo que tenga permisos para administrar todas las redes en todos los proyectos de su empresa.

Organización

- Google Sales crea la organización.
- Los Propietarios de la organización se establecen durante la creación.
  - Los administradores avanzados de **G Suite** son *los únicos* **Propietarios de la organización**
- **Propietario de la organización**
  - Asigna la función de Administrador de la organización desde la *Consola del administrador* de **G Suite** ***(la Consola*** *es un producto distinto)*
    - Los Administradores de la organización controlan GCP desde Cloud Console.
- Cuente siempre con más de un propietario de la organización por motivos de seguridad.

Google Cloud

Las cuentas personales o de prueba no tienen “organización” y las características de la organización están ocultas en la IU.
https://cloud.google.com/resource-manager/docs/creating-managing-organization
https://cloud.google.com/resource-manager/docs/quickstart

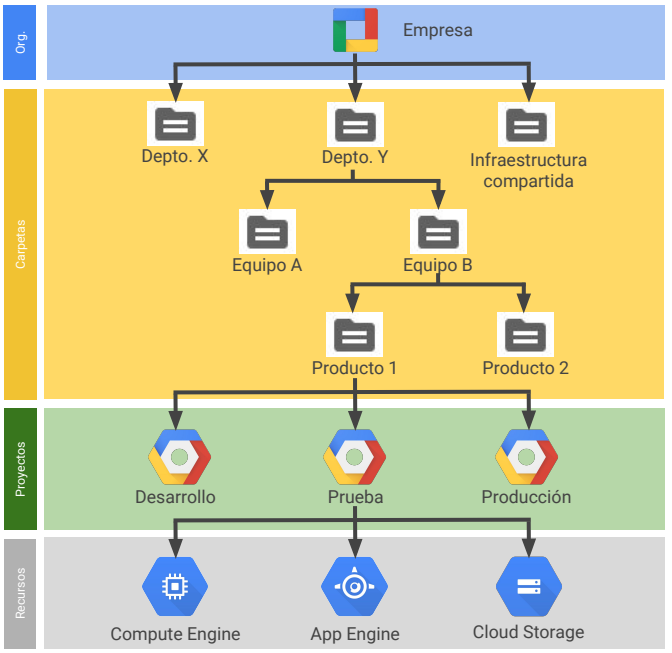
La cuenta con la función de Propietario de la organización tiene la capacidad de modificar todos los proyectos dentro de la organización.
Los cambios de la organización en sí se siguen realizando a través de Google Sales.
https://cloud.google.com/resource-manager/docs/overview#organization

Carpetas

Mecanismo de agrupamiento adicional y límites de aislamiento entre proyectos:

- Diferentes entidades legales
- Departamentos
- Equipos

Las carpetas permiten delegar derechos de administración.



Google Cloud

Los recursos de carpetas ofrecen un mecanismo de agrupamiento adicional y límites de aislamiento entre proyectos. Se pueden considerar como suborganizaciones dentro de la organización. Las carpetas se pueden utilizar para modelar diferentes entidades legales, departamentos y equipos dentro de la empresa. Por ejemplo, un primer nivel de carpetas se podría utilizar para representar los departamentos principales de su organización. Debido a que las carpetas pueden contener proyectos y otras carpetas, cada carpeta a su vez podría incluir otras subcarpetas para representar diferentes equipos. Cada carpeta del equipo podría contener subcarpetas adicionales para representar las diferentes aplicaciones.

Las carpetas permiten delegar derechos de administración, de modo que, por ejemplo, se puede otorgar a cada jefe de departamento la propiedad total de todos los recursos de GCP que pertenecen a su departamento. Asimismo, el acceso a recursos se puede limitar por carpeta, de manera que los usuarios en un departamento pueden acceder a recursos de Cloud y crearlos únicamente dentro de esa carpeta.

Funciones del Administrador de recursos

Organización
- **Administrador:** control total de todos los recursos
- **Lector**: acceso de lectura a todos los recursos

Carpeta
- **Administrador:** control total de las carpetas
- **Creador:** exploración de la jerarquía y creación de carpetas
- **Lector:** lectura de carpetas y proyectos dentro de un recurso

Proyecto
- **Creador:** creación de proyectos nuevos (propietario automático) y migración de proyectos nuevos a la organización
- **Eliminador:** eliminación de proyectos

Google Cloud

Los **Administradores a nivel de la organización** pueden otorgar una función a un miembro que abarca todos los proyectos. </1057
Ejemplo de uso: otorgar a un auditor de seguridad acceso de lectura a todos los registros (función de Lector de registros) para todos los proyectos.
Esto sería mucho más eficiente que otorgar al auditor de seguridad (o grupo de auditores de seguridad) acceso a cada proyecto individualmente.
Función de Administrador principal de la organización: asignada por Google; generalmente, no es el administrador avanzado de G Suite
Cambie los valores predeterminados de la política de Cloud IAM para la organización
La configuración a nivel del proyecto puede anular los valores predeterminados heredados
Administre las cuentas de facturación y las formas de pago

Consulte aquí la lista completa de funciones de administrador de recursos:
https://cloud.google.com/iam/docs/understanding-roles?hl=es-419&_ga=2.73506386.-1171753218.1503062023&_gac=1.254720634.1510004312.Cj0KCQiArYDQBRDoARIsAMR8s_TIY1w4BPcHZltQ3Mkv2jSj7fw17PcWR1DwvZZZMn9nvkfE8PO6YsEaAobUEALw_wcB#crm_name_short_roles

Modificador de retención del proyecto: una retención representa una restricción de las acciones que se pueden realizar con un recurso:
https://cloud.google.com/resource-manager/reference/rest/v1/liens

Tanto G Suite como GCP son parte de una sola línea de producto llamada "Google Cloud", pero son productos distintos.
Cuando se agrega una "Organización" a GCP, se firma un MSA (acuerdo de servicio estándar) que generalmente incluye un dominio alojado en Google con el producto Administrador de G Suite.
La recomendación es que la cuenta/persona que sea el Administrador avanzado de G Suite sea diferente de la cuenta/persona que es el *principal* Propietario de la organización de GCP.
El administrador de G Suite tiene DOS funciones respecto a GCP:

1. El administrador avanzado de G Suite puede asignar la función de Propietario de la organización de GCP a una cuenta dentro de la Consola del administrador de G Suite. Un Propietario de la organización de GCP también puede crear más propietarios de la organización asignando la función a una cuenta dentro de GCP Console. El administrador avanzado de G Suite no puede asignar otras funciones de GCP a cuentas desde la Consola del administrador.
2. El administrador avanzado de G Suite crea usuarios y grupos, controla la pertenencia de usuarios a grupos y controla los dominios alojados en Google (nombres de dominio: @miempresa1.com, @miempresa2.com).

Autorización de GPC

Utilice el sistema de credenciales de Google

- Administre cuentas con G Suite de Google**
- Sincronice credenciales existentes con Google Cloud Directory Sync
- De manera opcional, implemente el inicio de sesión único (SSO)

Características integradas

- Seguimiento de la actividad de la sesión
- Herramientas de administración de la sesión
- Alertas de seguridad
- Detección de actividades sospechosas

** O bien G Suite for Education de Google y G Suite for Government de Google

Google Cloud

Notas:
El mecanismo más sencillo para acceder a Google Cloud Platform es utilizar una cuenta de Google. Si bien es sencillo, el mecanismo no ofrece una administración de identidad centralizada. Las organizaciones deberían utilizar en su lugar la administración de usuarios de G Suite de Google para crear y administrar cuentas/credenciales. Nota: Esto es solo para la administración de usuarios. No requiere que utilice los productos de G Suite de Google, como Gmail, Documentos de Google y Presentaciones de Google.

La administración de usuarios de G Suite de Google es un lugar único para administrar y controlar cuentas, lo que incluye suspender cuentas problemáticas. Debido a que Google administra los inicios de sesión, usted obtiene los beneficios y la seguridad de la administración de autenticación de Google: restablecimientos de contraseña, administración de sesiones y dispositivos (cuándo/dónde acceden los usuarios) y detección y alertas de actividad sospechosa.

Para obtener más información sobre cómo administrar las cuentas de usuario de G Suite de Google, consulte: https://support.google.com/a/topic/14588?hl=es-419&ref_topic=2425090.

Google Cloud Directory Sync (GCDS)

- Sincroniza las cuentas de G Suite para hacer coincidir los datos de usuario con MS Active Directory o LDAP existentes
  - Sincroniza grupos y pertenencias, no contenido ni configuración
  - Compatible con reglas sofisticadas para la asignación personalizada de usuarios, grupos, contactos que no son empleados, perfiles de usuarios, alias y excepciones
- Sincronización unidireccional desde LDAP hacia el directorio
  - Administre en LDAP; luego, realice actualizaciones periódicamente en G Suite
- Se ejecuta como utilidad en el entorno de su servidor

Google Cloud

Con Google Cloud Directory Sync (GCDS), el administrador de G Suite puede agregar, modificar y borrar automáticamente usuarios, grupos y contactos que no sean empleados para sincronizar los datos en un dominio de G Suite con un servidor de directorio de LDAP o MS Active Directory. Los datos en el servidor de directorio de LDAP nunca se modifican ni se ven comprometidos. GCDS es una herramienta segura que ayuda a hacer un seguimiento de los usuarios y los grupos.

El administrador de G Suite utiliza Configuration Manager de GCDS para personalizar sincronizaciones y puede realizar sincronizaciones de prueba a fin de encontrar qué funciona mejor para la organización y, luego, programar sincronizaciones con el objeto de que se hagan cuando sea necesario.

https://support.google.com/a/answer/106368?hl=es-419

Inicio de sesión único (SSO)

- Utilice su propio mecanismo de autenticación y administre sus propias credenciales.
- Federe sus identidades en Google Cloud Platform (GCP).
- Los usuarios no tienen que ingresar por segunda vez para acceder a los recursos de GCP.
- Revoque el acceso a GCP con su administración de credenciales existente.
- Google Apps Directory Sync se integra con LDAP.

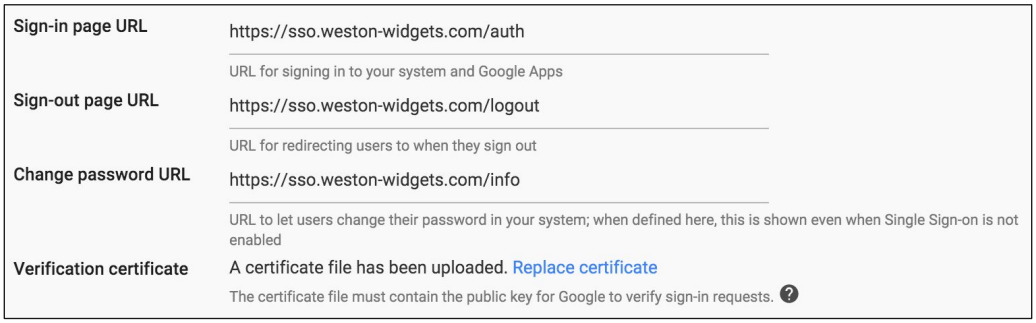
Google Cloud

Notas:
Si tiene su propio sistema de identidades, puede habilitar SSO. Puede continuar utilizando su propio sistema/procesos con el SSO configurado y, cuando se necesite autenticación de usuario, Google lo redireccionará a su sistema. Si el usuario es autenticado en su sistema, se da acceso a Google Cloud Platform. De lo contrario, se indica al usuario que ingrese.

Sus usuarios deben tener una cuenta correspondiente en el sistema de Google (un nombre de usuario coincidente), por lo general, aprovisionado con Google Apps Directory Sync.

Cómo configurar el SSO

- Si su autenticación existente es compatible con SAML2, la configuración de SSO son 3 vínculos y un certificado.
  - Si SAML2 no es compatible, utilice una solución de terceros.



Google Cloud

Notas:
La configuración de SSO es un proceso relativamente sencillo. SSO está integrado en SAML2, un protocolo estándar de la industria y seguro para intercambiar aserciones de usuario. Con el SSO de Google, la única aserción que se utiliza es el nombre de usuario.

Para evitar las alteraciones, SAML permite que la información se firme digitalmente. Para configurar esto, necesita un certificado digital utilizado para validar la firma. Esto garantiza que la información entrante la origine usted y no se haya alterado. Si su sistema no es compatible con SAML2, puede utilizar un complemento de administración de ID de terceros, como Okta o Ping.

Recomendaciones de Cloud IAM

Principio de privilegios mínimos

- Siempre aplique el nivel de acceso mínimo requerido.

Utilice grupos.

Controle quién puede cambiar las políticas y la pertenencia a grupos.

Audite los cambios de políticas.

- Audite los registros de cambios de permisos a nivel del proyecto.
- Se están agregando niveles adicionales.

Usuarios	Grupos	Funciones de Cloud IAM	
Ejemplo	Equipo de Op. de Seg.	Función de Administrador de seguridad Función de Lector de registros	Organización example.com

Google Cloud

Notas:

El principio de privilegios mínimos se aplica a identidades, funciones y recursos. Siempre seleccione el alcance mínimo necesario para reducir su exposición al riesgo. No quisiera otorgar a todos la función de Propietario para la organización completa: las modificaciones intencionales o los errores accidentales podrían desactivar sus aplicaciones. Es recomendable que sea específico y actúe a conciencia. Asigne a un grupo específico la función de Administrador de seguridad para controlar los certificados SSL y los firewalls de proyectos específicos.

Administrar los permisos de usuarios individuales puede ser complicado y susceptible a cometer errores. En su lugar, utilice grupos. En el ejemplo, hay un grupo de Op. de Seg. (para su equipo de operaciones de seguridad). Cuando se unan miembros nuevos al equipo, agréguelos al grupo. El equipo de Op. de Seg. probablemente necesita varias funciones, por ejemplo, Administrador de seguridad para administrar firewalls y Lector de registros para realizar auditorías. Asigne las funciones relevantes al grupo correspondiente.

Las políticas le permiten proteger sus recursos. Además, es recomendable que se asegure de controlar cómo los usuarios adicionales obtienen acceso a recursos a través de políticas y pertenencia a grupos. Sin un control estricto de los cambios de políticas y pertenencia a grupos, es posible que permita accidentalmente que los usuarios nuevos tengan más permisos de lo necesario (lo cual también infringe el principio de privilegios mínimos).

Recomendaciones: utilice grupos

Si el grupo de pertenencia es seguro, asigne funciones a los grupos y deje que el administrador de **G Suite** controle la pertenencia.

- Mantenga siempre una alternativa.
- Para áreas de alto riesgo, asigne funciones a personas directamente y prescinda de la conveniencia de la asignación grupal.

Google Cloud

Aléjese del estándar solo cuando lo necesite y cuando sepa por qué debe hacer el cambio y cómo se implementarán sus políticas.

Programa

- Administración de identidades y accesos (IAM) de Cloud
- Organización
- **Funciones**
- Miembros
- Cuentas de servicio
- Recomendaciones de Cloud IAM
- Cuestionario
- Lab

Google Cloud

Existen dos tipos de funciones en Cloud IAM:

- *Funciones básicas:* las funciones originales disponibles en Google Cloud Platform Console. Estas son las funciones de Propietario, Editor y Lector. Se continúan asignando a los proyectos de manera predeterminada. Las funciones básicas son bastante amplias.
- *Funciones seleccionadas*: las funciones seleccionadas son funciones nuevas de Cloud IAM que dan un control de acceso más específico que el de las funciones básicas (analizadas en la siguiente sección).

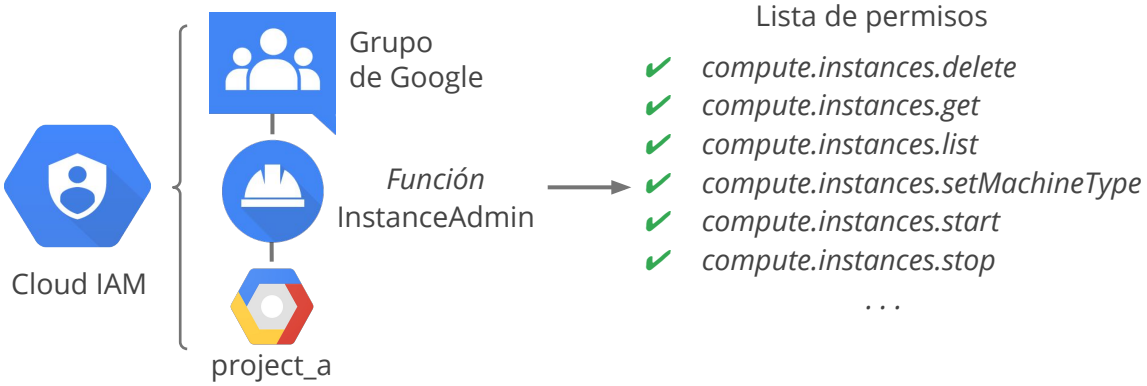
Los permisos otorgados por las funciones básicas son los siguientes:

- “es Propietario” permite tener acceso total de administrador. Esto incluye la capacidad de agregar miembros y establecer el nivel de autorización de los miembros del equipo.
- “puede editar” permite modificar y borrar el acceso. Esto permite al desarrollador implementar la aplicación y modificar o configurar sus recursos.
- “puede leer” permite el acceso de solo lectura.

Se recomienda asegurarse de que el proyecto tenga más de un propietario por motivos de continuidad. Muchas organizaciones crearán un Grupo de Google para tener la propiedad del proyecto y colocarán al menos dos cuentas de Google en ese grupo. Algunas organizaciones utilizarán una cuenta de propietario del proyecto dedicada. Si hay un único propietario y se borra su cuenta, también se eliminaría todo el proyecto.

La recomendación es utilizar las cuentas de Google para los miembros del equipo de su proyecto. Cuando alguien abandona la empresa, su administrador de G Suite debe utilizar la Consola del administrador de G Suite para marcar la cuenta como suspendida (en lugar de borrar la cuenta). Luego, el administrador del dominio puede realizar varias tareas, como reasignar la propiedad de las aplicaciones y los documentos, antes de borrar la cuenta del miembro del equipo.

Funciones seleccionadas



Las funciones seleccionadas de Cloud IAM ofrecen un mayor nivel de detalles para el otorgamiento de permisos.

Una función de Cloud IAM es un conjunto de permisos. La mayoría de las veces, para hacer una operación importante, necesita más de 1 permiso. Por ejemplo, para administrar las instancias de un proyecto, necesita crear, borrar, iniciar, detener y cambiar una instancia. De modo que los permisos se agrupan en una función para facilitar la administración.

Para dar a un usuario los permisos deseados, usted otorga una función al usuario destinada a un recurso. En esta diapositiva, se otorga a un grupo de usuarios la función InstanceAdmin de un proyecto, de manera que los usuarios puedan administrar las instancias del proyecto. Cuando sea posible, se recomienda utilizar grupos. Además, debe controlar estrictamente la capacidad para cambiar políticas y pertenencia a grupos que permitirá a los usuarios adicionales obtener acceso a los recursos.

Para obtener una lista completa de funciones por producto, consulte:
https://cloud.google.com/iam/docs/#supported_cloud_platform_services

Funciones

- Grupos de permisos
  - Representan *funciones abstractas*
  - Personalizan las funciones para ser compatibles con los *trabajos reales*
- Los permisos son clases y métodos en las API
  - `<service>.<resource>.<verb>`
  - Generalmente (pero no siempre), 1:1 con la API de REST
- Las funciones se pueden personalizar[BETA]

Google ofrece un conjunto de funciones seleccionadas para los productos.
Lea el documento de Cloud IAM específico del producto para comprender por qué las funciones se definieron de ese modo y por qué algunos permisos se incluyeron y no otros.
Realmente debe comprender la API del producto a fin de modificar los permisos, para que sepa de manera exacta qué comportamiento está habilitando o inhabilitando.
Los permisos son controles muy detallados.
https://cloud.google.com/iam/docs/understanding-roles
https://cloud.google.com/iam/docs/faq
La personalización de funciones está en fase Beta:
https://cloud.google.com/iam/docs/understanding-custom-roles

Funciones esenciales

- Funciones de la organización
- Funciones de la carpeta
- Funciones del proyecto
- Funciones específicas del producto
  - Diseñadas para cada recurso/producto (más de 20)
  - Documentación de Cloud IAM específica del producto
  - Algunas están en fase Beta

Google Cloud

Existen varios tipos de funciones Este curso analizará cada una de estas en contexto.

Las funciones son conjuntos de “permisos”. Los permisos se asignan directamente a clases y métodos en las API de Google Cloud Platform.
Cuando se otorga una función, los permisos que contiene autorizan al usuario a llamar a métodos específicos en las API.

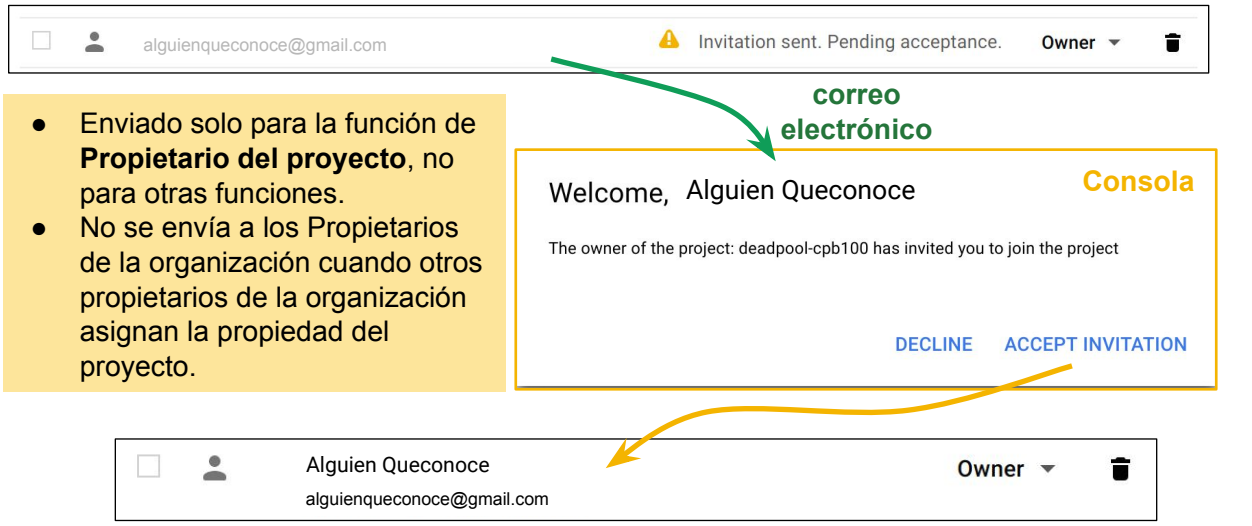
Funciones del proyecto

- Lector
  - Acciones de solo lectura que no modifican el estado
  - Función de navegador (en fase Beta): solo “información sobre” (metadatos)
- Editor
  - + acciones que modifican el estado
- Propietario
  - + administración del control de acceso para un proyecto y todos sus recursos
  - + configuración de la facturación del proyecto

Google Cloud

https://cloud.google.com/iam/docs/understanding-roles
Un usuario con la función de Propietario del proyecto para un proyecto particular puede invitar a otro usuario a fin de que también sea Propietario del proyecto.

Invitación del Propietario del proyecto y aceptación



- Enviado solo para la función de **Propietario del proyecto**, no para otras funciones.
- No se envía a los Propietarios de la organización cuando otros propietarios de la organización asignan la propiedad del proyecto.

Google Cloud

La invitación y la aceptación de miembros ofrecen verificación de identidad y un seguimiento de la responsabilidad.
Cualquiera con una identidad de Google válida es un posible invitado. Actualmente, no existe un método para establecer límites ni bloquear dominios, grupos o correos electrónicos específicos.
No se envían correos electrónicos cuando usted otorga una función que no sea la de Propietario.
No se envían correos electrónicos cuando un Propietario de la organización agrega a otro Propietario de la organización como propietario de un proyecto dentro de esa organización.
Los Propietarios de la organización no reciben correos electrónicos de invitación; simplemente se los agregan.

Funciones específicas del producto

- Funciones diseñadas para cada producto: *lea el documento de Cloud IAM*
- Ejemplo: funciones de Compute Engine
  - Administrador de instancia de Compute Engine: VM y discos
  - Usuario de la cuenta de servicio: cuentas de servicio
  - Usuario de imagen de Compute Engine: imágenes
  - Lector de red de Compute Engine: solo lectura para todas las redes
  - Administrador de red de Compute Engine: todas las redes, excepto las reglas de firewall y los certificados
  - Administrador de seguridad de Compute Engine: reglas de firewall, certificados SSL
  - Administrador de almacenamiento de Compute Engine: discos, imágenes, instantáneas

Google Cloud

https://cloud.google.com/iam/docs/understanding-roles
Existen más de 20 productos con funciones específicas del producto. Cada uno tiene un documento de Cloud IAM diferente que explica los detalles de los permisos y la estrategia detrás de la definición de funciones.
No hay invitaciones ni aceptaciones con las funciones específicas del producto.
Ejemplo de Compute Engine:
https://cloud.google.com/compute/docs/access/iam

Funciones específicas del producto: Ejemplos

Compute Engine

Administrador de red de Compute
Lector de red de Compute (en fase Beta)
Administrador de seguridad de Compute
Administrador de instancia de Compute
Administrador de almacenamiento de Compute (en fase Beta)

Cloud Storage

Administrador de almacenamiento
Administrador de objetos de almacenamiento
Creador de objetos de almacenamiento
Lector de objetos de almacenamiento

Logging

Lector de registros
Autor de registros
Lector de registros privados
Autor de config. de registros

BigQuery

Lector de BigQuery
Editor de BigQuery
Administrador de BigQuery
Usuario de BigQuery

App Engine

Administrador de App Engine
Implementador de App Engine
Administrador de servicios de App Engine
Lector de App Engine

Cloud Dataflow

Lector de Dataflow
Desarrollador de Dataflow
Trabajador de Dataflow

Cloud Pub/Sub

Lector de Pub/Sub
Editor de Pub/Sub
Administrador de Pub/Sub
Editor de Pub/Sub
Suscriptor de Pub/Sub

Otras funciones:

Administrador Deployment
Depurador de Stackdriver
Genomics
...
Para obtener la lista completa, consulte los documentos

Google Cloud

Programa

- Administración de identidades y accesos (IAM) de Cloud
- Organización
- Funciones
- **Miembros**
- Cuentas de servicio
- Recomendaciones de Cloud IAM
- Cuestionario
- Lab

Google Cloud

Miembros

Usuarios

- Cuentas de Google: @gmail, @google
- Dominios de **G Suite**: Dominios alojados en Google (*mydomain*.com)
- Grupos de Google (*nombredelgrupo*@mydomain.com)
- GCP ***no*** crea ni administra usuarios o grupos
  - El administrador avanzado del **Administrador** de **G Suite** administra los usuarios y los grupos para una organización. El "**Administrador** de **G Suite**" es un producto diferente de GCP.

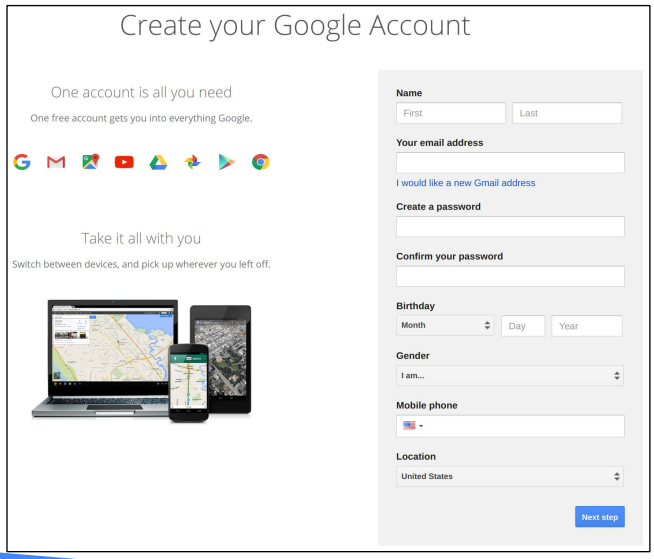
Cuentas de servicio

- Creadas y administradas en GCP

Google Cloud

example.com
groups.google.com/a/su-dominio.com
Característica de Groups for Business
groups.su-dominio.com

Acceso a GCP sin Gmail



- Simplemente, puede utilizar Gmail.
- Puede obtener una contraseña de Google sin Gmail.
- Existen beneficios por tener un dominio, incluidos los permisos de grupo.

Google Cloud

https://accounts.google.com/SignUpWithoutGmail?hl=es-419

Programa

- Administración de identidades y accesos (IAM) de Cloud
- Organización
- Funciones
- Miembros
- **Cuentas de servicio**
- Recomendaciones de Cloud IAM
- Cuestionario
- Lab

Google Cloud

Cuentas de servicio (1 de 2)

- Ofrecen una identidad para realizar interacciones de **servidor a servidor** en un proyecto sin proporcionar credenciales de usuario.
- Se utilizan para **autenticar** de un servicio a otro:
  - Los programas que se ejecutan dentro de las instancias de Compute Engine pueden adquirir automáticamente tokens de acceso con credenciales.
  - Se utilizan tokens para acceder a cualquier API de servicios en su proyecto y a cualquier otro servicio que otorgó acceso a esa cuenta de servicio.
  - Es conveniente cuando no se accede a los datos del usuario.

Google Cloud

Una cuenta de servicio es una identidad para que utilicen sus programas a fin de autenticar las API de Google Cloud Platform y obtener acceso a estas. Las cuentas de servicio autentican aplicaciones que se ejecutan en instancias de su máquina virtual para otros servicios de Google Cloud Platform. Por ejemplo, si escribe una aplicación que lee y escribe archivos en Cloud Storage, primero se debe autenticar para la API XML o la API JSON de Google Cloud Storage. Puede habilitar cuentas de servicio y otorgar acceso de lectura-escritura para la cuenta en la instancia en la que planea ejecutar su aplicación. Luego, programe la aplicación para obtener credenciales de la cuenta de servicio. Su aplicación se autentica sin inconvenientes con la API sin incorporar claves secretas ni credenciales a su instancia, imagen o código de aplicación.

Cuentas de servicio (2 de 2)

- Identificadas por una dirección de **correo electrónico**:
  - `123845678986-compute@project.gserviceaccount.com`
- Tres tipos de cuentas de servicio:
  - Creada por el usuario (personalizada)
  - Integrada
    - Cuentas de servicio predeterminadas de Compute Engine y App Engine
  - Cuenta de servicio de las API de Google
    - Ejecuta los procesos internos de Google en su nombre

Google Cloud

De manera predeterminada, todos los proyectos vienen con la cuenta de servicio predeterminada de Compute Engine. Cuando inicia una instancia nueva con gcloud, se habilita la cuenta de servicio predeterminada en esa instancia.

Aparte de la cuenta de servicio predeterminada, todos los proyectos vienen con una cuenta de servicio de las API de Google Cloud Platform, identificable por el correo electrónico:

{número-de-proyecto}@cloudservices.gserviceaccount.com

Esta es una cuenta de servicio diseñada específicamente para ejecutar los procesos internos de Google en su nombre. Esta cuenta no aparece en la sección Cuentas de servicio de Google Cloud Platform Console; sin embargo, de manera predeterminada, se le otorga automáticamente la función de Editor para el proyecto y aparece en la sección Cloud IAM de Google Cloud Platform Console. Esta cuenta de servicio se borra únicamente cuando se borra el proyecto. Sin embargo, puede cambiar las funciones otorgadas a esta cuenta, lo cual incluye revocar todo acceso a su proyecto. Ciertos recursos dependen de esta cuenta de servicio y los permisos de editor predeterminados otorgados a la cuenta de servicio. Por ejemplo, los grupos de instancias administradas y el ajuste de escala automático utilizan las credenciales de esta cuenta para crear, borrar y administrar instancias. Si usted revoca los permisos para la cuenta de servicio o modifica los permisos de tal manera que no otorga permisos para crear instancias, los grupos de instancias administrados y el ajuste de escala automático dejarán de funcionar. Por estos motivos, se recomienda que no

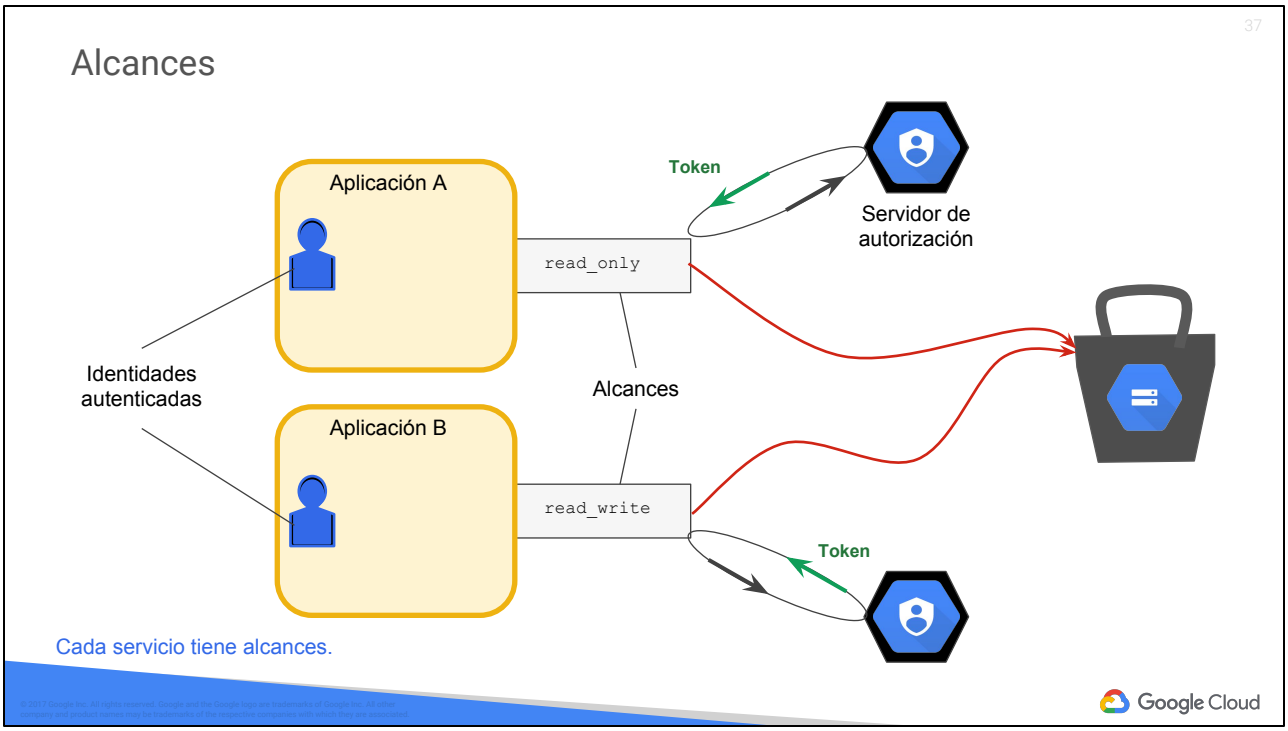
modifique las funciones de esta cuenta de servicio.

Como alternativa, también puede iniciar una instancia con una cuenta de servicio personalizada. Las cuentas de servicio personalizadas ofrecen más flexibilidad que la cuenta de servicio predeterminada, pero requieren mayor administración de su parte. Puede crear tantas cuentas de servicio personalizadas como necesite, asignar alcances de acceso arbitrario o funciones de Cloud IAM a estas y asignar las cuentas de servicio a cualquier instancia de máquina virtual.

Las cuentas de servicio predeterminadas de App Engine no se cubren en este curso. Para obtener más información, consulte: https://developers.google.com/identity/protocols/application-default-credentials.

Cuenta de servicio predeterminada de Compute Engine

- Creada automáticamente por proyecto con nombre y dirección de correo electrónico autogenerados:
  - El nombre tiene el sufijo `-compute`
    `39xxxx0965-compute@developer.gserviceaccount.com`
- Se agrega automáticamente como Editor del proyecto
- De manera predeterminada, habilitada en todas las instancias creadas con `gcloud` o GCP Console
  - Para anularla, especifique otra cuenta de servicio o inhabilite las cuentas de servicio destinadas a la instancia



https://cloud.google.com/storage/docs/authentication

OAuth utiliza alcances a fin de determinar si una identidad autenticada está autorizada para tener acceso a un recurso.

Las aplicaciones utilizan alcances en el proceso de acceso.

En el ejemplo, las aplicaciones A y B contienen identidades autenticadas (cuentas de servicio).
Ambas quieren utilizar un depósito de Cloud Storage.
Solicitan acceso desde los servidores de autorización de Google.
Se envía un token de acceso con el alcance.
La aplicación A solo puede leer desde el depósito.
La aplicación B puede leer y escribir.
Pero ninguna aplicación puede leer ni modificar las LCA (listas de control de acceso), porque esto requeriría el alcance full_access que no tienen.

Los alcances de acceso otorgan acceso solo si la API correspondiente se ha habilitado en el proyecto al que pertenece la cuenta de servicio. Por ejemplo, otorgar un alcance de acceso para Cloud Storage en una instancia de máquina virtual permite a la instancia llamar a la API de Firebase Cloud Storage solo si ha habilitado la API de Cloud Storage en el proyecto. Si la API no está habilitada en el proyecto, el alcance de acceso no tiene efecto. Además, si planea utilizar la cuenta de servicio para acceder a otro proyecto, debe otorgar a la cuenta de servicio las funciones de

Cloud IAM correspondientes en el proyecto objetivo.

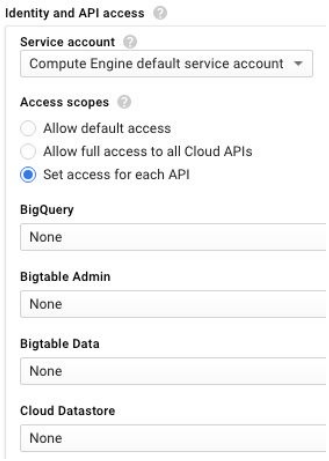
Las cuentas de servicio predeterminadas de Compute Engine se habilitan automáticamente con los siguientes alcances de acceso:
https://www.googleapis.com/auth/cloud.useraccounts.readonly
https://www.googleapis.com/auth/devstorage.read_only
https://www.googleapis.com/auth/logging.write
https://www.googleapis.com/auth/monitoring.write
https://www.googleapis.com/auth/service.management.readonly
https://www.googleapis.com/auth/servicecontrol

Cómo personalizar alcances para una VM

Puede crear una instancia con alcances personalizados para su caso práctico, con la cuenta de servicio predeterminada.

- Los alcances se pueden cambiar después de que se haya creado una instancia.

Para las cuentas de servicio creadas por el usuario, utilice en su lugar las funciones de Cloud IAM.



Google Cloud

Los alcances se pueden cambiar después de crear una instancia deteniéndola.

Las cuentas de servicio pueden utilizar alcances mediante SDK de Cloud. Los comandos gcloud y gsutil captan automáticamente los tokens y puede ejecutar de manera sencilla estos comandos en secuencias de comandos para automatizar los flujos de trabajo. También puede escribir códigos personalizados de aplicaciones o herramientas con las bibliotecas de cliente de Google, o bien escribir su propio código para consumir tokens.

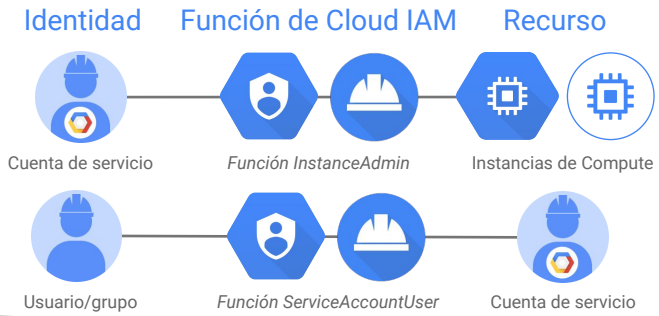
Estos alcances ofrecen el siguiente acceso:
Acceso de solo lectura a la API de Cloud User Accounts*
Acceso de solo lectura a la API JSON de Cloud Storage v1
Acceso de lectura/escritura a la API de Stackdriver Logging v2
Acceso de lectura/escritura a la API de Stackdriver Monitoring v3
Acceso de solo lectura a la API de Google Service Management v1*
Acceso de lectura-escritura a la API de Google Service Control v1*

Permisos de la cuenta de servicio

Las cuentas de servicio predeterminadas son compatibles con las funciones básicas (proyecto) y seleccionadas (Cloud IAM).

- Las cuentas de servicio creadas por el usuario utilizan solo las funciones de Cloud IAM.

Las funciones para las cuentas de servicio se pueden asignar a grupos o usuarios.



Google Cloud

Una de las características de la cuenta de servicio de Cloud IAM es que puede tratarla como un recurso o una identidad.

Cuentas de servicio como recurso

Cuando se trata una cuenta de servicio como un recurso, usted puede otorgar a un usuario el permiso para acceder a esa cuenta de servicio. Puede otorgar la función de Propietario, Editor, Lector o serviceAccountUser a un usuario para la cuenta de servicio. Por ejemplo, si desea permitir a un usuario crear una VM con la cuenta de servicio o autenticarse como cuenta de servicio, primero debe otorgar al usuario la función serviceAccountUser. En este caso, la cuenta de servicio es el recurso y usted otorga al usuario el permiso para utilizar este recurso de cuenta de servicio.

Cuentas de servicio como identidad

Puede otorgar una función a una cuenta de servicio para acceder a un recurso. En este caso, la cuenta de servicio es la identidad. Estos son algunos ejemplos:

- Se otorga a las cuentas de servicio predeterminadas de Compute Engine y App Engine las funciones de Editor en el proyecto cuando se crean, para que el código que se ejecuta en su instancia de VM o aplicación tenga los permisos necesarios. En este caso, las cuentas de servicio son identidades a las que se les otorga la función de Editor para un recurso (proyecto).
- Si desea permitir que su automatización acceda a un depósito de almacenamiento, usted otorga a la cuenta de servicio (que su automatización

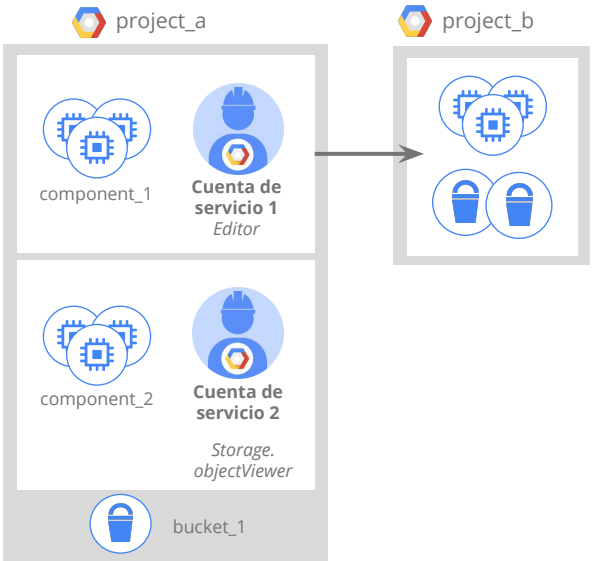
- utiliza) los permisos para leer el depósito de almacenamiento. En este caso, la cuenta de servicio es la identidad a la que otorga permisos para otro recurso (depósito de Cloud Storage).

Cómo otorgar a otro usuario la capacidad de actuar como cuenta de servicio

Si desea que otros usuarios puedan utilizar la cuenta de servicio, debe otorgar la función serviceAccountUser al usuario. Los usuarios con la función serviceAccountUser pueden actuar como cuenta de servicio para realizar operaciones, como crear y administrar instancias de Compute Engine que utilizan una cuenta de servicio. Para obtener información sobre cómo hacer esto, consulte la documentación de Compute Engine. Los usuarios que son serviceAccountUsers para una cuenta de servicio pueden acceder a todos los recursos a los cuales la cuenta de servicio tiene acceso. Por lo tanto, tenga cuidado cuando otorgue la función serviceAccountUser a un usuario.

Ejemplo: cuentas de servicio y Cloud IAM

- A las VM que ejecutan component_1 se les otorga acceso de Editor a project_b con la *Cuenta de servicio 1*
- A las VM que ejecutan component_2 se les otorga el acceso objectViewer a bucket_1 *con la Cuenta de Servicio 2*
- Los permisos de cuenta de servicio se pueden cambiar sin crear de nuevo las VM.



Google Cloud

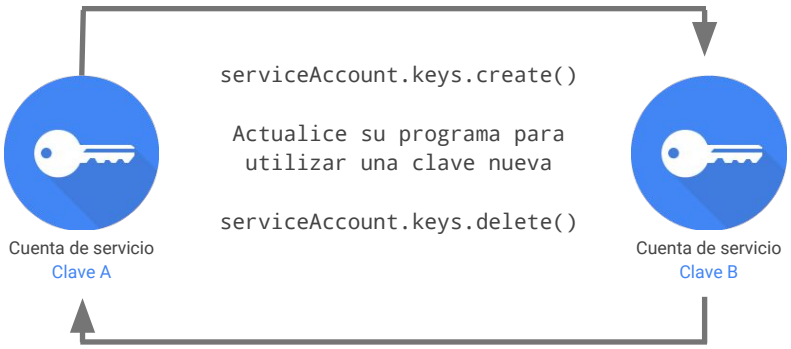
Puede otorgar distintas identidades a diferentes grupos de VM en su proyecto. Esto facilita la administración de diferentes permisos para cada grupo. Por ejemplo, si un componente en su aplicación necesita tener la función de Editor en otro proyecto, puede tener una cuenta de servicio con este permiso que utilicen solo las VM que ejecutan el componente. Se puede asignar a otras VM los permisos que requieren sus funcionalidades. De esta manera, puede definir el alcance de los permisos para las VM. También puede cambiar los permisos de las cuentas de servicio sin tener que volver a crear las VM.

Cloud IAM también le permite dividir un proyecto en diferentes microservicios, cada uno con acceso a diferentes recursos, al crear cuentas de servicio para representar a todos. Usted asigna las cuentas de servicio a las VM cuando se crean y no necesita asegurarse de que las credenciales se administren de manera correcta.
Google Cloud Platform administra la seguridad por usted.

Cuentas de servicio y claves

Las cuentas de servicio realizan autenticaciones con claves

- Google administra las claves y su rotación para Compute Engine y App Engine
- Como alternativa, cree, administre y rote claves usted mismo



Google Cloud

Los usuarios requieren un nombre de usuario y una contraseña para autenticarse. Las aplicaciones utilizan una clave. Se pueden generar una o más claves para cada cuenta de servicio de Cloud IAM. Las claves son confidenciales y se deben administrar cuidadosamente porque le dan acceso a recursos. Cuando ejecuta aplicaciones en Compute Engine o App Engine, Google administra las claves por usted y las rota automáticamente. Nunca tiene el riesgo de perder/exponer sus claves. Cuando ejecuta aplicaciones en otro lugar, puede generar y descargar las claves a utilizar en su código. Se recomienda mantener su seguridad y rotarlas.

Una cuenta de servicio es una identidad y un recurso. Una cuenta de servicio se utiliza como una identidad para autenticar su aplicación; por ejemplo, una VM de Compute Engine que se ejecute como cuenta de servicio. Para dar acceso a la VM a los recursos necesarios, necesita otorgar las funciones correspondientes de Cloud IAM a la cuenta de servicio. Al mismo tiempo, necesita controlar quién puede crear las VM con la cuenta de servicio, de modo que una VM al azar no pueda asumir la identidad. En este caso, la cuenta de servicio es el recurso al que se dará el permiso. Asigne la función ServiceAccountUser a los usuarios en los que confíe para utilizar la cuenta de servicio.

Programa

- Administración de identidades y accesos (IAM) de Cloud
- Organización
- Funciones
- Miembros
- Cuentas de servicio
- **Recomendaciones de Cloud IAM**
- Cuestionario
- Lab

Google Cloud

Jerarquía de recursos

- Utilice proyectos para agrupar los recursos que comparten el mismo límite de confianza.
- Verifique la política otorgada para cada recurso y asegúrese de comprender la herencia.
- Utilice el “principio de privilegios mínimos” cuando otorgue funciones.
- Audite las políticas en los registros de auditoría de Cloud: `setiampolicy`.
- Audite la pertenencia de los grupos utilizada en las políticas.

Google Cloud

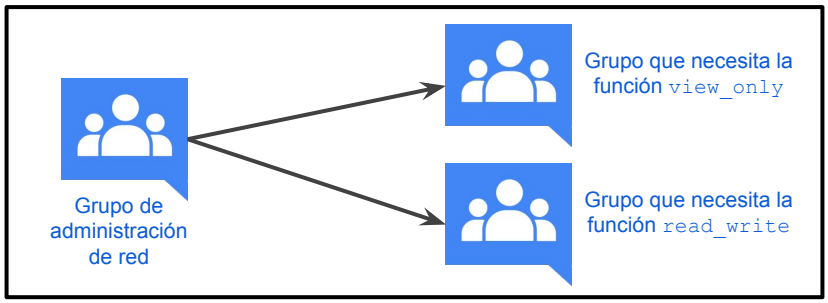
1. Duplique la jerarquía de políticas de Cloud IAM en la estructura de su organización.
2. Utilice los proyectos de Google Cloud Platform para agrupar los recursos que comparten el mismo límite de confianza. Por ejemplo, los recursos para el mismo producto o microservicio pueden pertenecer al mismo proyecto de Google Cloud Platform.
3. Establezca políticas a nivel de la organización y en el nivel del proyecto en lugar del nivel del recurso.
4. Verifique la política otorgada para cada recurso y comprenda la herencia jerárquica.
5. Si necesita otorgar una función a un usuario o grupo que abarca varios proyectos, establezca esa función a nivel de la organización en lugar de a nivel del proyecto.
6. Utilice etiquetas para anotar, agrupar y filtrar recursos.
7. Si desea limitar la creación del proyecto en su organización, modifique la política al nivel de la organización para otorgar la función de Creador del proyecto a un grupo que administre.
8. Utilice el principio de seguridad de privilegios mínimos para otorgar funciones.
9. Otorgue funciones con el alcance mínimo necesario.
10. Audite sus políticas para garantizar el cumplimiento. Los registros de auditoría de Cloud contienen todas las llamadas a `setiampolicy` para que pueda hacer un seguimiento de cuándo se implementaron las políticas.
11. Audite la propiedad y la pertenencia de los grupos de Google utilizados en las políticas.

1. Otorgue funciones con el alcance mínimo necesario. Por ejemplo, si un usuario solo necesita acceso para publicar mensajes en un tema de Pub/Sub, otorgue la función de Publicador al usuario para ese tema.

Grupos

Otorgue funciones a los grupos de Google en lugar de a personas:

- Actualice la pertenencia al grupo en lugar de cambiar la política de Cloud IAM.
- Audite la pertenencia de los grupos utilizada en las políticas.
- Controle la propiedad del grupo de Google utilizada en las políticas de Cloud IAM.



- Utilice varios grupos para tener un mejor control.
- Los grupos no solo se relacionan con funciones de trabajo.
- Los grupos pueden existir con el propósito de asignar funciones.

Google Cloud

En el diagrama, se creó un solo grupo que se relacionaba con una función de trabajo, “administrador de red”. Sin embargo, la administración de Cloud IAM se dio cuenta en seguida de que había diferentes subgrupos que requerían diferentes permisos. En este ejemplo, la configuración estándar se mantiene en archivos de un depósito. Algunos administradores de red necesitan acceso para ver estos archivos. Unas pocas personas seleccionadas tienen la autoridad para editar y borrar estos archivos.

El grupo original se continúa utilizando para correos grupales y aquellas funciones que todo administrador de red necesita, pero los otros grupos y sus pertenencias se establecieron solo para asignar funciones adicionales de Cloud IAM. Cuando se agregan y borran personas de los tres grupos, se controla su acceso total.

1. Otorgue funciones a un grupo de Google en lugar de a usuarios individuales cuando sea posible. Es más sencillo agregar miembros a un grupo de Google y quitarlos en lugar de actualizar la política de Cloud IAM para agregar o quitar usuarios.
2. Si necesita otorgar varias funciones para permitir la realización de una tarea particular, cree un grupo de Google, otorgue las funciones a ese grupo y, luego, agregue usuarios a ese grupo.
3. Controle la propiedad del grupo de Google utilizada en las políticas de Cloud IAM.

Cuentas de servicio

- Tenga cuidado cuando otorgue la función `serviceAccountUser`.
- Cuando cree una cuenta de servicio, asígnele un nombre visible que identifique claramente su propósito.
- Establezca una nomenclatura para las cuentas de servicio.
- Establezca políticas y métodos de rotación de claves.
- Realice una auditoría con el método `serviceAccount.keys.list()`.

Google Cloud

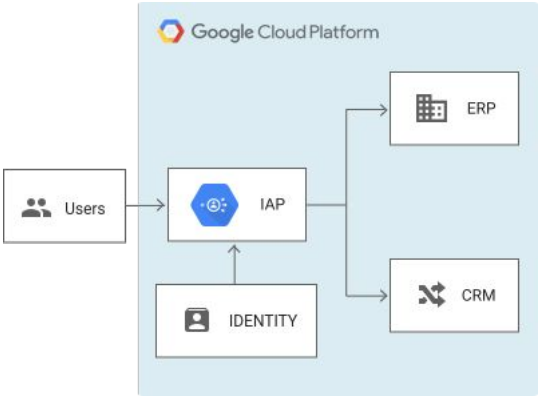
1. Restrinja quién puede actuar como cuenta de servicio. Los usuarios que son serviceAccountUsers para una cuenta de servicio pueden acceder a todos los recursos a los cuales la cuenta de servicio tiene acceso. Por lo tanto, tenga cuidado cuando otorgue la función serviceAccountUser a un usuario.
2. Otorgue a la cuenta de servicio solo el conjunto mínimo de permisos requeridos para alcanzar su objetivo.
3. Cree cuentas de servicio correspondientes a cada servicio con solo los permisos requeridos para ese servicio.
4. Utilice el nombre visible de una cuenta de servicio para hacer un seguimiento de las cuentas de servicio. Cuando cree una cuenta de servicio, cree su nombre visible con la finalidad de la cuenta de servicio.
5. Defina una nomenclatura para las cuentas de servicio.
6. Implemente procesos para automatizar la rotación de claves de cuentas de servicio administradas por el usuario.
7. Aproveche la API de cuentas de servicio de Cloud IAM para implementar la rotación de claves.
8. Audite las cuentas de servicio y las claves con el método de serviceAccount.keys.list() o la página del Lector de registros en la Consola.
9. No ejecute instancias en App Engine ni Compute Engine para borrar cuentas de servicio que están en uso.

Cloud Identity-Aware Proxy (Cloud IAP)

Implemente políticas de control de acceso para aplicaciones y recursos:

- Control de acceso basado en la identidad
- Capa de autorización central para aplicaciones a las que se accede por HTTPS

Se aplica la política de Cloud IAM después de la autenticación.



Google Cloud

Cloud IAP le permite establecer una capa de autorización central para las aplicaciones a las que se accede por HTTPS, de modo que puede utilizar un modelo de control de acceso a nivel de la aplicación en lugar de depender de firewalls a nivel de red.

Los usuarios y los grupos con la función correcta de Cloud IAM pueden acceder a las aplicaciones y los recursos protegidos por Cloud IAP solo mediante el proxy. Cuando otorga a un usuario el acceso a una aplicación o recurso mediante Cloud IAP, está sujeto a los controles de acceso fino implementados por el producto en uso sin requerir una VPN. Cloud IAP realiza verificaciones de autenticación y autorización cuando un usuario intenta acceder a un recurso protegido por Cloud IAP.

Cloud IAP protege la autenticación y la autorización de todas las solicitudes a HTTPS de Cloud Load Balancing o App Engine. Cloud IAP no protege contra lo siguiente:

- Actividad en el interior de su VM, por ejemplo, si alguien accede a la VM a través de SSH. Esto incluye el entorno flexible de App Engine, cuando se habilita el acceso directo de SSH a su VM.
- La actividad dentro de un proyecto, por ejemplo, otra VM dentro del proyecto.

Para obtener más información, consulte:
https://cloud.google.com/iap/docs/concepts-overview

Programa

- Administración de identidades y accesos (IAM) de Cloud
- Organización
- Funciones
- Miembros
- Cuentas de servicio
- Recomendaciones de Cloud IAM
- **Cuestionario**
- Lab

Google Cloud

Cuestionario

¿Qué abstracción se utiliza principalmente para administrar el acceso del usuario en Cloud IAM?

1. Concesiones: una abstracción de derechos periódicos
2. Funciones: una abstracción de funciones de trabajo
3. Credenciales: una abstracción de un token de autorización
4. Privilegios: una abstracción de derechos de acceso

Cuestionario

¿Qué abstracción se utiliza principalmente para administrar el acceso del usuario en Cloud IAM?

1. Concesiones: una abstracción de derechos periódicos
2. Funciones: una abstracción de funciones de trabajo*
3. Credenciales: una abstracción de un token de autorización
4. Privilegios: una abstracción de derechos de acceso

Explicación:
La administración de Cloud IAM utiliza funciones predefinidas para el control del acceso del usuario. Las funciones se definen mediante permisos más detallados. Sin embargo, los permisos no se aplican a los usuarios directamente; solo mediante las funciones que se asignan a ellos.

Cuestionario

¿Cómo se crea una identidad de usuario en Cloud IAM?

1. Las identidades de usuario se crean desde la Consola de Cloud Identity que es visible solo para los administradores avanzados de GCP.
2. Las identidades de usuario se crean desde el área de Cloud IAM en GCP Console o con el comando gcloud.
3. Las identidades de usuario se crean mediante un dominio de Active Directory federado.
4. Las identidades de usuario se crean fuera de GCP en un dominio administrado por Google.

Cuestionario

¿Cómo se crea una identidad de usuario en Cloud IAM?

1. Las identidades de usuario se crean desde la Consola de Cloud Identity que es visible solo para los administradores avanzados de GCP.
2. Las identidades de usuario se crean desde el área de Cloud IAM en GCP Console o con el comando gcloud.
3. Las identidades de usuario se crean mediante un dominio de Active Directory federado.
4. Las identidades de usuario se crean fuera de GCP en un dominio administrado por Google. *

Explicación:
El acceso de Cloud IAM se crea a partir de un sistema de administración de acceso y autorización de identidades que todos los productos de Google Cloud utilizan, no solo GCP.

Cuestionario

¿Qué tecnología se puede utilizar junto con Cloud IAM para ofrecer otra capa de control de acceso y seguridad en GCP?

1. Aprendizaje automático, específicamente, detección de intrusos
2. Software contra vulnerabilidades de seguridad y de antivirus integrado a las VM de GCP
3. Herramientas de redes, específicamente, reglas de firewall
4. Limitación dinámica de peticiones de recursos por usuario

Cuestionario

¿Qué tecnología se puede utilizar junto con Cloud IAM para ofrecer otra capa de control de acceso y seguridad en GCP?

1. Aprendizaje automático, específicamente, detección de intrusos
2. Software contra vulnerabilidades de seguridad y de antivirus integrado a las VM de GCP
3. Herramientas de redes, específicamente, reglas de firewall*
4. Limitación dinámica de peticiones de recursos por usuario

Explicación:
Debido a que GCP es un conjunto de servicios en red, puede administrar un acceso fino a los recursos limitando el acceso a la red. Ejemplo: con las funciones de Cloud IAM, puede otorgar a un grupo de usuarios el acceso a una VM particular que ejecute una aplicación. Con las reglas de firewall, podría permitir el acceso a la VM solo desde rangos de IP específicos, de modo que los usuarios puedan obtener el acceso a la VM solamente desde la red corporativa y no desde otra ubicación.

Programa

- Administración de identidades y accesos (IAM) de Cloud
- Organización
- Funciones
- Miembros
- Cuentas de servicio
- Recomendaciones de Cloud IAM
- Cuestionario
- **Lab**

Google Cloud

Lab: Cloud IAM

Objetivos

En este lab, aprenderá a realizar las siguientes tareas:

- Utilizar Cloud IAM para implementar un control de acceso
- Restringir el acceso a características o recursos específicos
- Utilizar la función de usuario de cuenta de servicio

Duración: 30 minutos

Acceso: 60 minutos

Repaso del lab

En este lab, realizó las siguientes actividades:

- Otorgó y revocó las siguientes funciones de Cloud IAM:
  - Usuario, Username 2
  - Usuario de la cuenta de servicio

Pudo adjudicar las credenciales de Usuario de cuenta de servicio e "integrarlas" a una VM a fin de crear hosts de bastión autorizados para un fin específico.

Más recursos

Cómo utilizar cuentas de servicio
https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances

Cómo autorizar solicitudes a Google Compute Engine
https://cloud.google.com/compute/docs/api/how-tos/authorization

Cómo utilizar OAuth 2.0 para acceder a las API de Google
https://developers.google.com/identity/protocols/OAuth2