Identity and Access Management

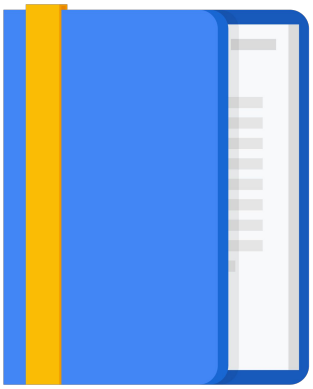
Mylene Biddle

En este módulo, analizaremos Identity and Access Management (o IAM).

IAM es un sistema sofisticado basado en nombres de direcciones de tipo de correo electrónico, roles de tipo de trabajo y permisos detallados. Si ya conoce IAM por otras implementaciones, descubra los cambios que aplicó Google para hacerlo más seguro y facilitar su administración.

Temario

- Identity and Access Management (IAM)
- Organización
- Roles
- Miembros
- Cuentas de servicio
- Prácticas recomendadas de IAM
- Lab

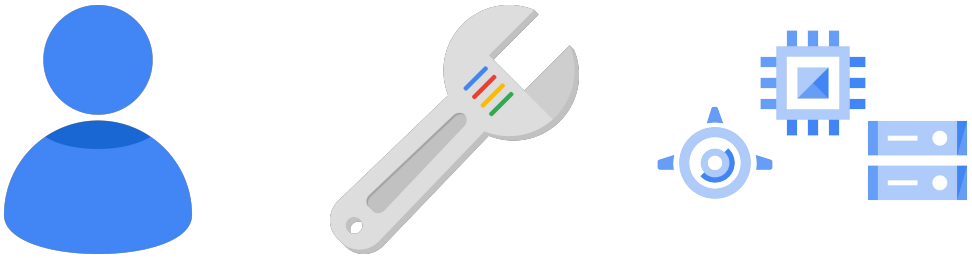


Comenzaré con una presentación de IAM desde una perspectiva general. Luego, analizaremos cada uno de sus componentes, que son las organizaciones, los roles, los miembros y las cuentas de servicio. También presentaré algunas prácticas recomendadas que lo ayudarán a aplicar estos conceptos en su trabajo diario.

Por último, obtendrá experiencia práctica con la IAM por medio de un lab.

Comencemos con la descripción general de Identity and Access Management.

Identity and Access Management

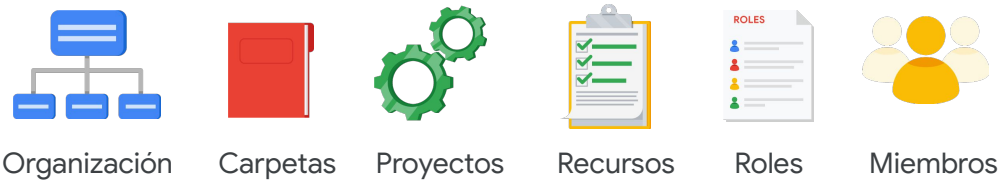


¿Qué es Identity and Access Management? Es una forma de identificar quién puede hacer qué, en qué recurso.

“Quién” puede ser una persona, un grupo o una aplicación. El “qué” se refiere a privilegios o acciones específicos, y el recurso puede ser cualquier servicio de Google Cloud.

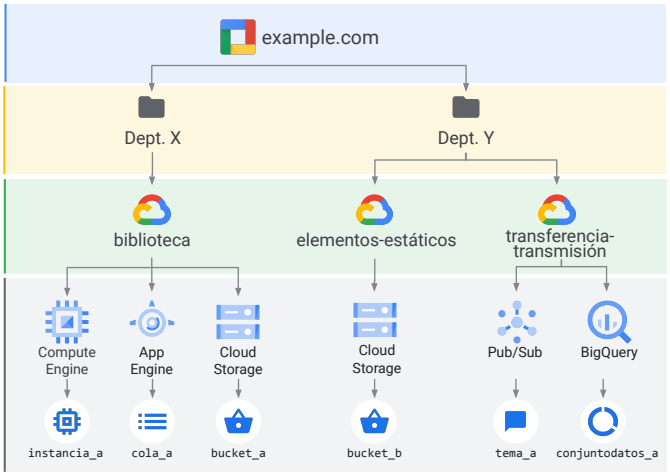
Por ejemplo, podría otorgarle el privilegio o rol de Visualizador de Compute. Esto le proporciona acceso de solo lectura para obtener y enumerar recursos de Compute Engine sin poder leer los datos almacenados en ellos.

Objetos de IAM



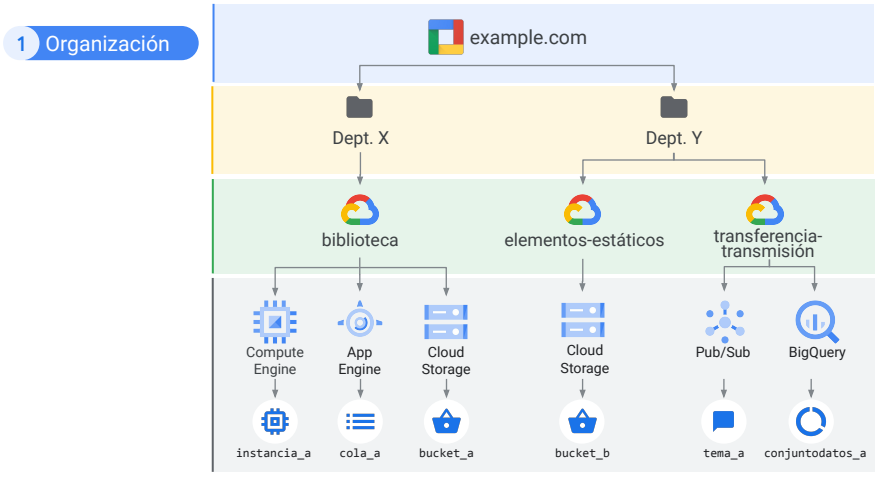
IAM se compone de diferentes objetos, como se muestra en esta diapositiva. Revisaremos cada uno de ellos en este módulo. Para comprender mejor estos objetos, analicemos las políticas y la jerarquía de recursos de IAM.

Jerarquía de recursos de IAM



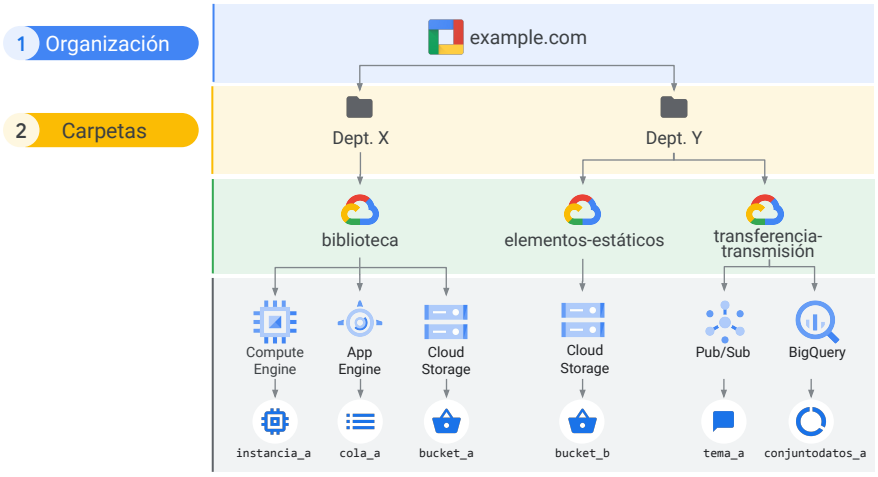
Los recursos de Google Cloud están organizados de forma jerárquica, como se muestra en esta estructura de árbol.

Jerarquía de recursos de IAM



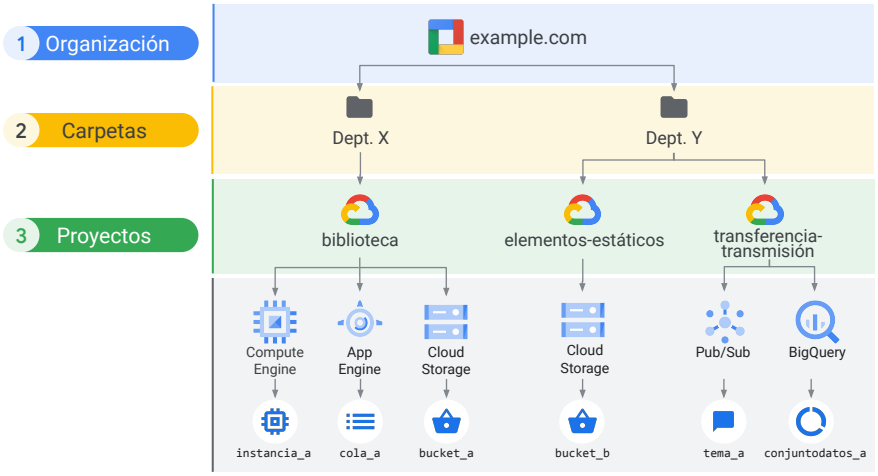
El nodo de la organización es el nodo raíz en esta jerarquía,

Jerarquía de recursos de IAM



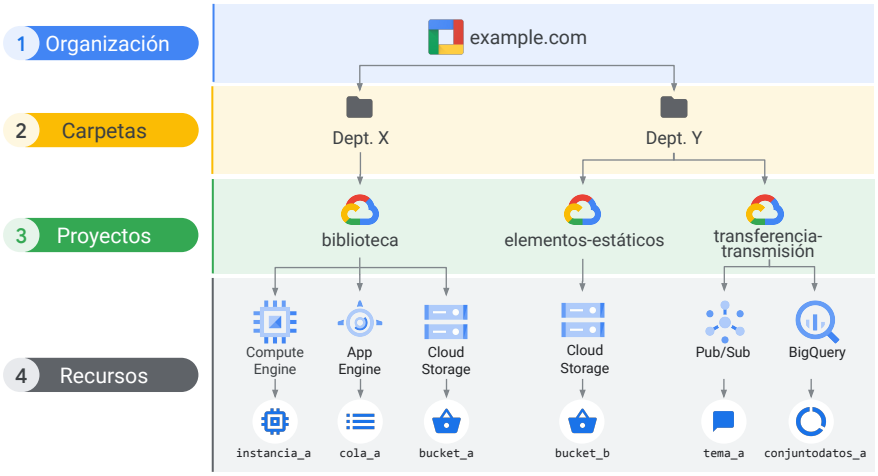
las carpetas son elementos secundarios de la organización,

Jerarquía de recursos de IAM



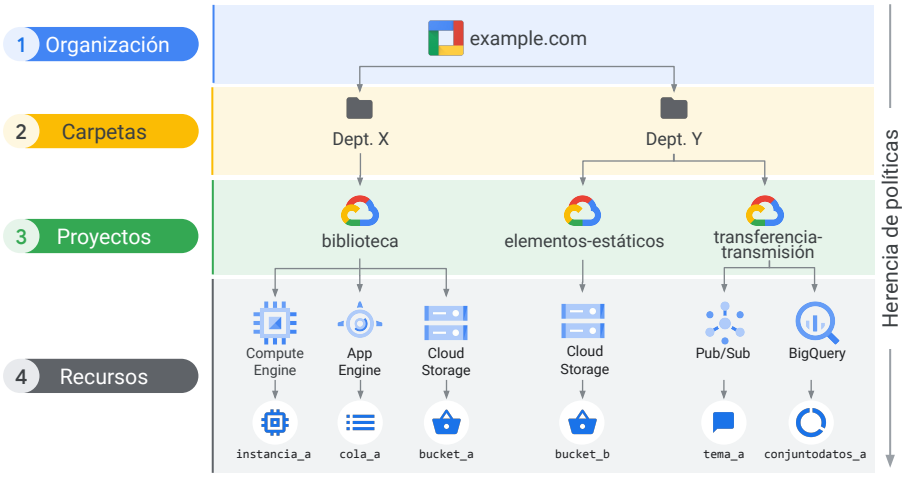
los proyectos son elementos secundarios de las carpetas

Jerarquía de recursos de IAM



y los recursos individuales son elementos secundarios de los proyectos. Cada recurso tiene exactamente un elemento superior.

Jerarquía de recursos de IAM



El recurso de organización representa a su empresa. Todos los recursos en la organización heredan los roles de IAM otorgados en este nivel.

El recurso de carpeta podría representar su departamento. Todos los recursos que contiene la carpeta heredan los roles de IAM otorgados en este nivel.

Los proyectos representan un límite de confianza dentro de su empresa. Los servicios dentro del mismo proyecto tienen el mismo nivel de confianza predeterminado.

Temario

Identity and Access Management (IAM)

Organización

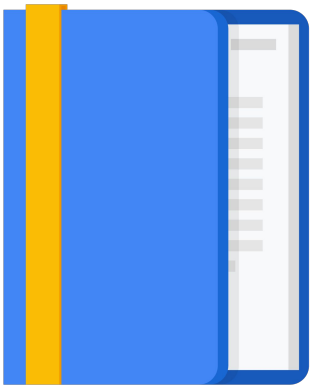
Roles

Miembros

Cuentas de servicio

Prácticas recomendadas de IAM

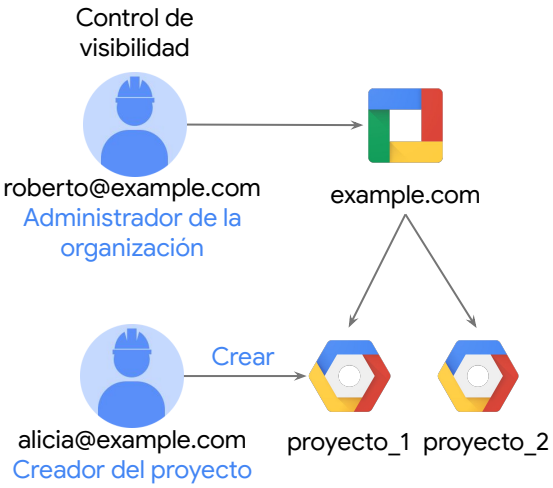
Lab



Revisemos con más detalle el nodo de organización.

Nodo de la organización

- El nodo de la organización es un nodo raíz de los recursos de Google Cloud.
- Roles de la organización:
  - Administrador de la organización: Controla todos los recursos de la nube; útil para auditorías
  - Creador del proyecto: Controla la creación de proyectos; control sobre quiénes pueden crear proyectos



Como mencioné, el recurso de organización es el nodo raíz en la jerarquía de recursos de GCP. Este tiene muchos roles, como el de Administrador de la organización.

El Administrador de la organización le otorga a un usuario, como Roberto, acceso para administrar todos los recursos que pertenecen a su organización, lo que es útil en auditorías.

También existe el rol de Creador de proyectos, que permite que un usuario, como Alicia, cree proyectos dentro de su organización. Aquí muestro el rol de creador del proyecto porque también se puede aplicar a nivel de la organización, y después lo heredarán todos los proyectos dentro de la organización.

Cree y administre organizaciones

- Se constituyen cuando se crea un proyecto de Google Cloud con una cuenta de **Google Workspace** o **Cloud Identity**
- **El administrador avanzado de Workspace** o **Cloud Identity** puede realizar las siguientes acciones:
  - Asignar el rol de **administrador de la organización** a algunos usuarios
  - Ser el punto de contacto en caso de problemas de recuperación
  - Controlar el ciclo de vida de las cuentas de Workspace o Cloud Identity y el de los recursos de la organización
- **El Administrador de la organización puede realizar las siguientes acciones:**
  - Definir políticas de IAM
  - Determinar la estructura de la jerarquía de recursos
  - Delegar la responsabilidad de los componentes fundamentales, como las Herramientas de redes, la facturación y la jerarquía de recursos, mediante roles de IAM

G Suite ahora es Google Workspace

El recurso de organización está estrechamente asociado con una cuenta de Google Workspace o Cloud Identity.

Cree y administre organizaciones

- Se constituyen cuando se crea un proyecto de Google Cloud con una cuenta de **Google Workspace** o **Cloud Identity**
- **El administrador avanzado de Workspace** o **Cloud Identity** puede realizar las siguientes acciones:
  - Asignar el rol de **administrador de la organización** a algunos usuarios
  - Ser el punto de contacto en caso de problemas de recuperación
  - Controlar el ciclo de vida de las cuentas de Workspace o Cloud Identity y el de los recursos de la organización
- **El Administrador de la organización puede realizar las siguientes acciones:**
  - Definir políticas de IAM
  - Determinar la estructura de la jerarquía de recursos
  - Delegar la responsabilidad de los componentes fundamentales, como las Herramientas de redes, la facturación y la jerarquía de recursos, mediante roles de IAM

G Suite ahora es Google Workspace

Cuando un usuario con una cuenta de Workspace o Cloud Identity crea un proyecto de Google Cloud, se le aprovisiona automáticamente un recurso de organización. Luego, Google Cloud informa de su disponibilidad a los administradores avanzados de Workspace o Cloud Identity. Estas cuentas de administrador avanzado deben usarse con cuidado, ya que tienen un amplio control sobre su organización y todos sus recursos subyacentes.

Los administradores avanzados de Workspace o Cloud Identity y el Administrador de la organización de Google Cloud son roles clave durante el proceso de configuración y para controlar el ciclo de vida del recurso de organización. En general, los dos roles se le asignan a distintos usuarios o grupos, aunque esto depende de la estructura y las necesidades de la organización.

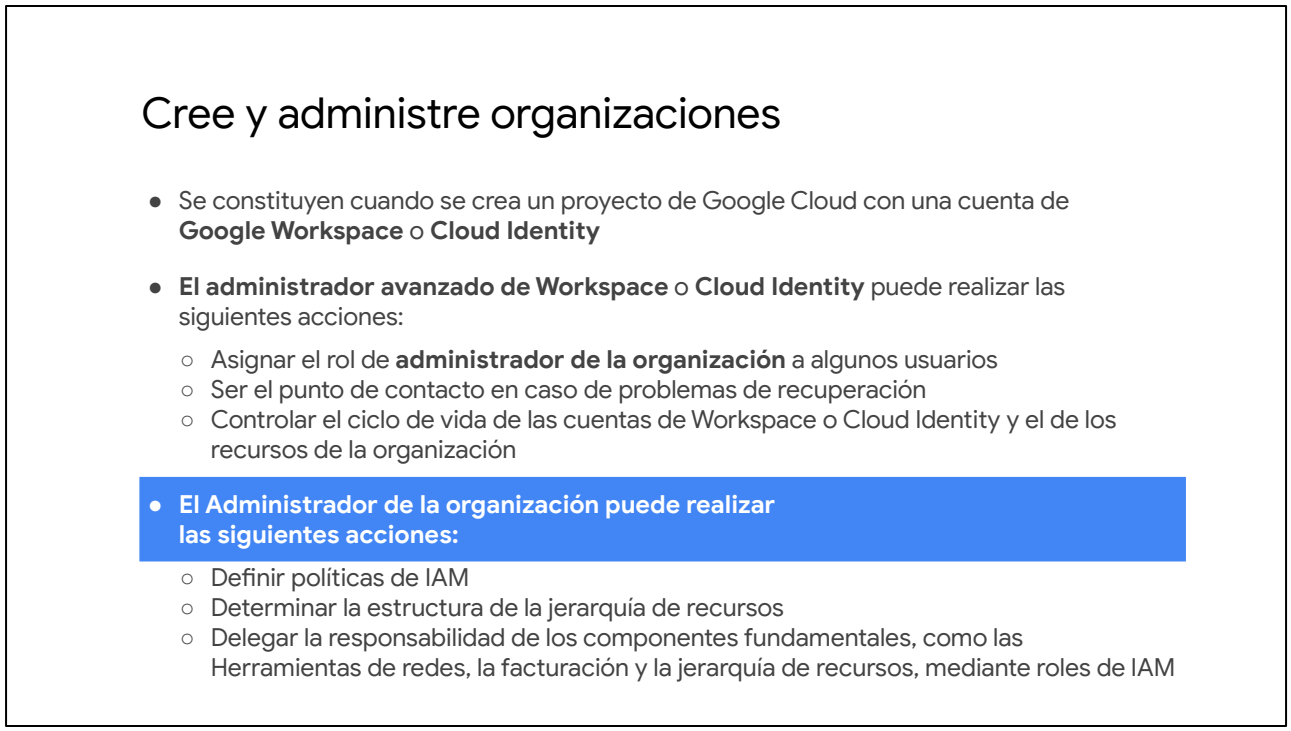
Cree y administre organizaciones

- Se constituyen cuando se crea un proyecto de Google Cloud con una cuenta de **Google Workspace** o **Cloud Identity**
- **El administrador avanzado de Workspace** o **Cloud Identity** puede realizar las siguientes acciones:
  - Asignar el rol de **administrador de la organización** a algunos usuarios
  - Ser el punto de contacto en caso de problemas de recuperación
  - Controlar el ciclo de vida de las cuentas de Workspace o Cloud Identity y el de los recursos de la organización
- **El Administrador de la organización puede realizar las siguientes acciones:**
  - Definir políticas de IAM
  - Determinar la estructura de la jerarquía de recursos
  - Delegar la responsabilidad de los componentes fundamentales, como las Herramientas de redes, la facturación y la jerarquía de recursos, mediante roles de IAM

G Suite ahora es Google Workspace

En el contexto de la configuración de la organización de Google Cloud, el administrador avanzado de Workspace o Cloud Identity tiene las siguientes responsabilidades:

- Asignar el rol de administrador de la organización a algunos usuarios
- Ser un punto de contacto en caso de problemas de recuperación
- Controlar el ciclo de vida de la cuenta de Workspace o Cloud Identity y del recurso de organización

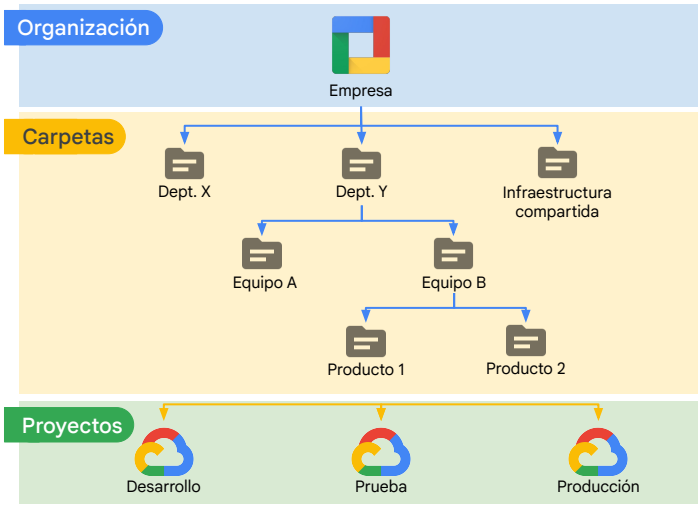


Las responsabilidades del rol de administrador de la organización son las siguientes:

- Definir políticas de IAM
- Determinar la estructura de la jerarquía de recursos
- Delegar la responsabilidad de los componentes fundamentales, como las Herramientas de redes, la facturación y la jerarquía de recursos, mediante roles de IAM

De acuerdo con el principio de privilegio mínimo, este rol no incluye el permiso para realizar otras acciones, como crear carpetas. Para obtener estos permisos, un Administrador de la organización debe asignarle roles adicionales a su cuenta. Para saber más sobre la creación y administración de organizaciones, consulte la guía práctica que aparece en la sección de vínculos de este video: [https://cloud.google.com/resource-manager/docs/creating-managing-organization#adding_an_organization_admin]

Carpetas



Proporcionan un mecanismo de agrupación y límites de aislamiento adicionales entre proyectos:

- Diferentes entidades legales
- Departamentos
- Equipos

Las carpetas permiten delegar derechos de administración.

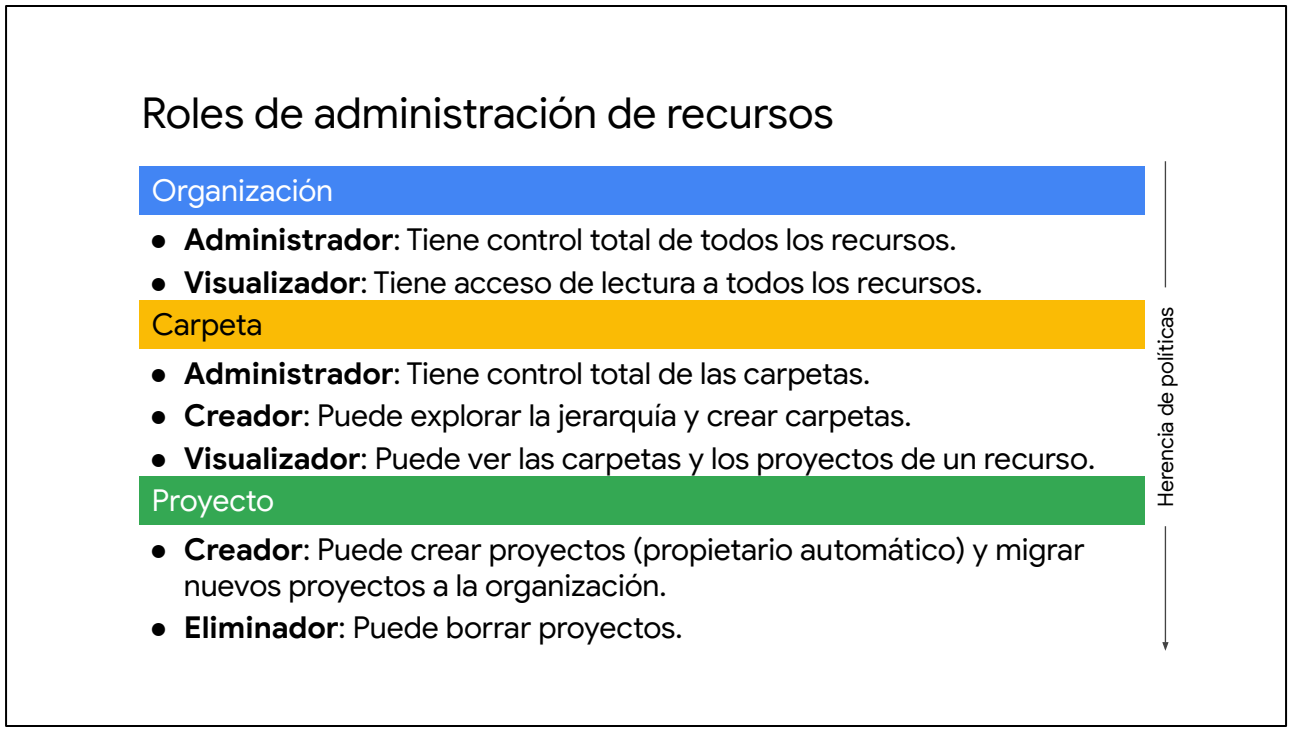
Veamos las carpetas con más detalle porque se pueden considerar como suborganizaciones dentro de la organización.

Tienen un mecanismo de agrupamiento adicional y un límite de aislamiento entre proyectos. Se pueden usar para diferenciar distintos departamentos, equipos y entidades legales dentro de una empresa. Por ejemplo, un primer nivel de carpetas podría usarse para representar los principales departamentos de su organización, como el X y el Y.

Como pueden contener proyectos y otras carpetas, cada carpeta podría incluir otras subcarpetas para representar diferentes equipos, como el A y el B.

Cada carpeta de equipo puede contener subcarpetas adicionales para representar diferentes aplicaciones, como el producto 1 y el 2.

Las carpetas permiten la delegación de derechos de administración; así, por ejemplo, cada jefe de un departamento puede obtener la propiedad total de todos los recursos de GCP que pertenecen a su departamento. Del mismo modo, el acceso a los recursos puede estar limitado por carpeta, por lo que los usuarios de un departamento solo pueden acceder y crear recursos de GCP dentro de esa carpeta.



Veamos otros roles de administración de recursos teniendo en cuenta que las políticas se heredan desde arriba hacia abajo.

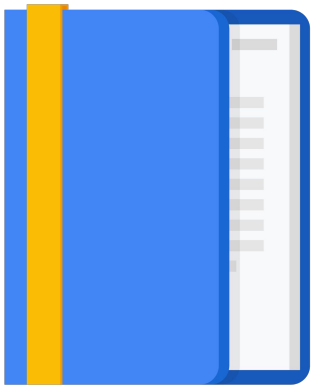
El nodo de organización también tiene un rol de Visualizador que otorga acceso de lectura a todos los recursos dentro de una organización.

El nodo de carpeta tiene varios roles que se asemejan a los de la organización, pero se aplican a los recursos que están dentro de una carpeta. Existe un rol de Administrador que proporciona control total sobre las carpetas, un rol de Creador para explorar la jerarquía y crear carpetas, y un rol de Visualizador que permite ver las carpetas y los proyectos de un recurso.

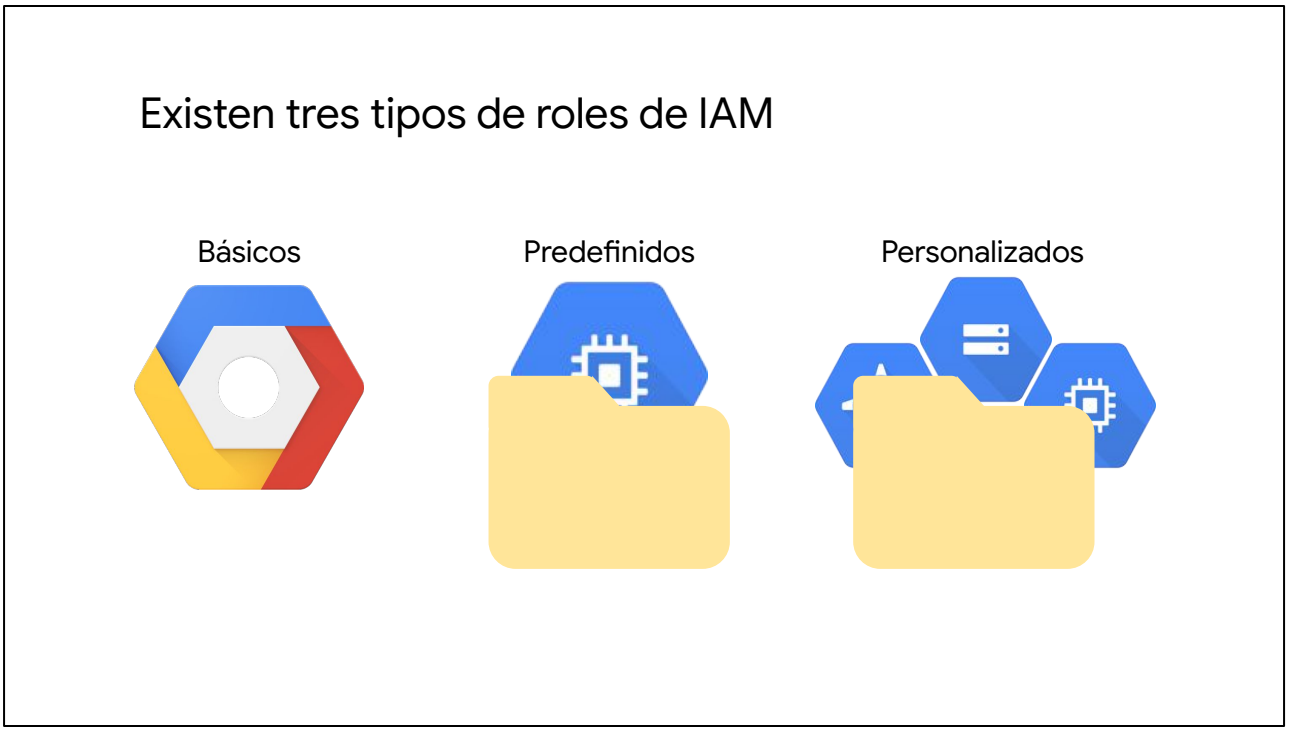
Del mismo modo, para los proyectos hay un rol de Creador que permite que un usuario cree proyectos nuevos, lo que lo convierte automáticamente en el propietario. También hay un rol de Eliminador de proyectos, que otorga el privilegio de eliminar proyectos.

Temario

- Identity and Access Management (IAM)
- Organización
- **Roles**
- Miembros
- Cuentas de servicio
- Prácticas recomendadas de IAM
- Lab



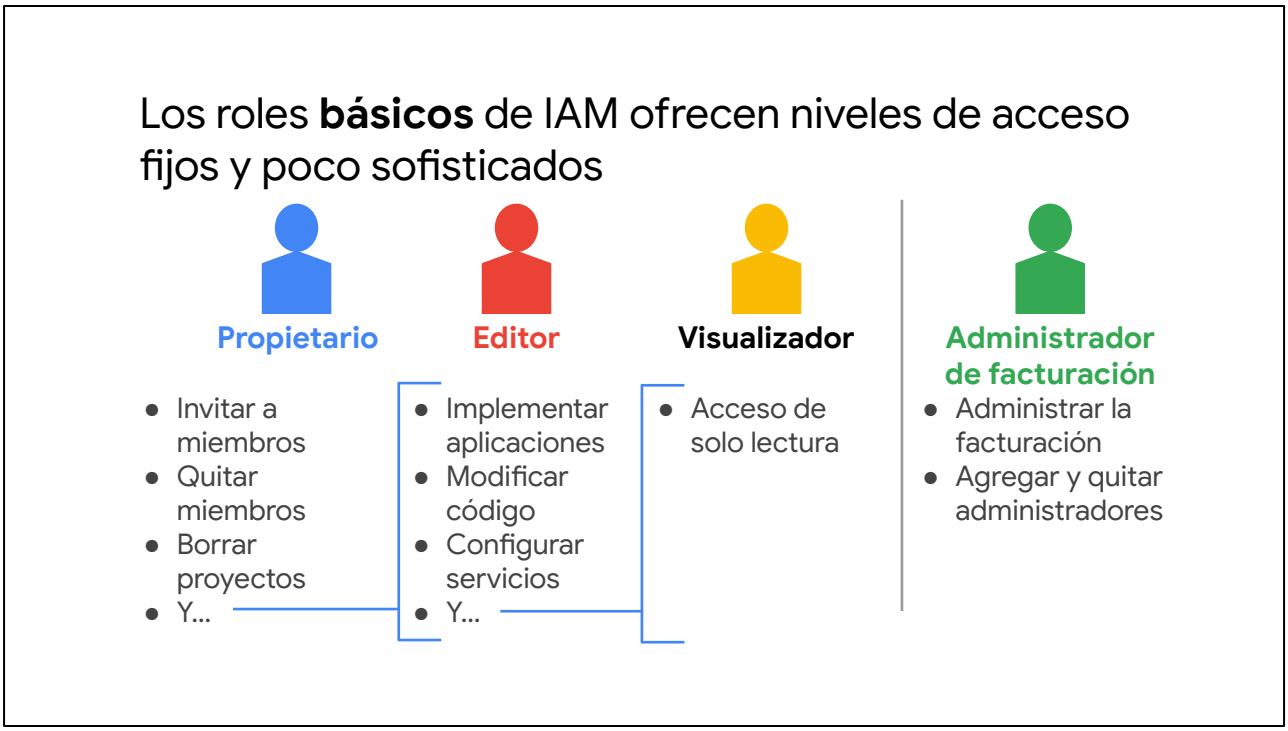
Hablemos sobre los roles, que definen “[quién] puede hacer qué en qué recurso” en IAM.



Existen tres tipos de roles de Cloud IAM: los básicos, los predefinidos y los personalizados.

Los roles básicos son los originales que estaban disponibles en Cloud Console, pero son amplios.

Si los aplica a un proyecto de Google Cloud, afectarán a todos los recursos del proyecto.



En otras palabras, los roles básicos de IAM ofrecen niveles de acceso fijos y poco sofisticados.

Los roles básicos son los de Propietario, Editor y Visualizador.

- El Propietario tiene acceso administrativo total y puede agregar y quitar miembros, así como borrar proyectos.
- El rol de Editor otorga acceso para realizar modificaciones y borrar datos. Esto permite que un desarrollador implemente aplicaciones y modifique o configure sus recursos.
- El rol de Visualizador brinda acceso de solo lectura.

Todos estos roles son concéntricos; es decir, el rol de Propietario incluye los permisos del rol de Editor, y este último incluye los permisos del rol de Visualizador.

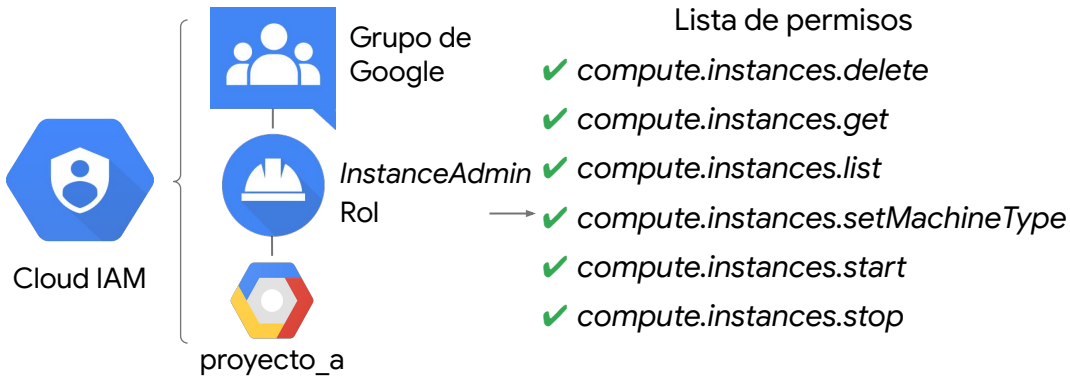
También existe un rol de Administrador de facturación que administra la facturación y agrega o quita administradores, pero no puede cambiar los recursos del proyecto.

Cada proyecto puede tener varios propietarios, editores, visualizadores y administradores de facturación.

Los servicios de GCP ofrecen sus propios conjuntos de roles predefinidos y establecen en qué circunstancias se pueden aplicar. De esta forma, se otorga a los miembros acceso detallado a recursos específicos de GCP y se impide el acceso no deseado a otros recursos.

Estos roles son *colecciones* de permisos porque seguramente necesitará más de un permiso para realizar cualquier operación importante.

Los roles **predefinidos** de IAM ofrecen permisos más detallados para servicios específicos



Por ejemplo, como se muestra aquí, se le otorga a un grupo de usuarios el rol de InstanceAdmin en el proyecto_a. Esto les otorga todos los permisos de Compute Engine que aparecen en el lado derecho y muchos más. Ahora bien, agrupar estos permisos en un rol hace que sean más fáciles de administrar. Además, estos son clases y métodos en las API.

Por ejemplo, compute.instances.start se puede desglosar en el servicio, el recurso y el verbo que indican que este permiso se usa para iniciar una instancia detenida de Compute Engine.

Normalmente, estos permisos se alinean con la API de REST que se corresponde con la acción.

Funciones de IAM de Compute Engine

Título de la función	Descripción
Administrador de Compute	Tiene control total de todos los recursos de Compute Engine (compute.*).
Administrador de la red	Tiene los permisos para crear, modificar y borrar recursos de herramientas de redes, excepto reglas de firewall y certificados SSL.
Administrador de almacenamiento	Tiene los permisos para crear, modificar y borrar imágenes, instantáneas y discos.

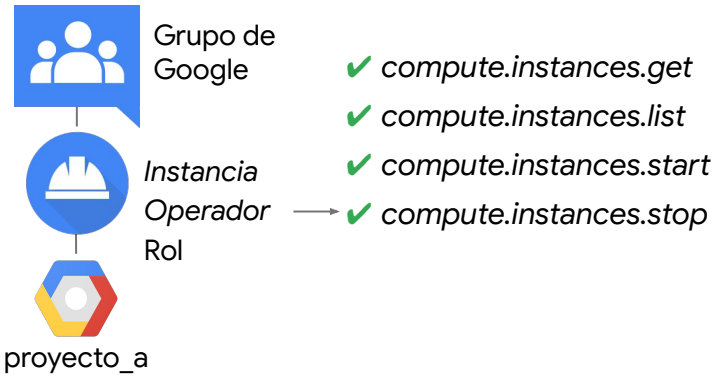
Compute Engine tiene varios roles de IAM predefinidos. Analicemos tres de ellos:

- El rol de Administrador de Compute otorga control total de todos los recursos de Compute Engine. Esto incluye todos los permisos que comienzan con *Compute*, lo que significa que se permite cada acción para cualquier tipo de recurso de Compute Engine.
- El rol de Administrador de red contiene permisos para crear, modificar y borrar recursos de red, *excepto* reglas de firewall y certificados SSL. En otras palabras, el rol de administrador de red permite el acceso de solo lectura a las reglas de firewall, certificados SSL y, también, instancias para ver sus direcciones IP efímeras.
- El rol de Administrador de almacenamiento contiene permisos para crear, modificar y borrar imágenes, instantáneas y discos.

Por ejemplo, si una persona de su empresa administra las imágenes del proyecto y usted no desea que tenga el rol de editor, otórguele a su cuenta el rol de Administrador de almacenamiento en el proyecto.
Para obtener la lista completa de roles predefinidos de Compute Engine, consulte la sección de vínculos de este video:
[https://cloud.google.com/compute/docs/access/iam#iam_roles]

El propósito de los roles es representar funciones abstractas y se personalizan para alinearse con trabajos reales. Pero ¿qué pasa si uno de estos roles no tiene suficientes permisos o usted necesita algo aún más detallado?

Los roles **personalizados** de IAM le permiten definir un conjunto preciso de permisos



Eso es lo que permiten los roles personalizados. Muchas empresas usan el modelo de “privilegio mínimo”, en el que cada persona de su organización obtiene la cantidad mínima de privilegios necesarios para realizar el trabajo.

Imaginemos que desea definir un rol de “Operador de instancia” para permitir que algunos usuarios inicien y detengan máquinas virtuales de Compute Engine, pero no las puedan volver a configurar. Los roles personalizados le permiten hacerlo.

Demostración

Roles personalizados

Philipp Maier

Le mostraré cómo crear un rol personalizado en GCP.
Mi objetivo es crear un rol de Operador de instancias para que algunos usuarios puedan iniciar y detener máquinas virtuales de Compute Engine, pero no las puedan volver a configurar.

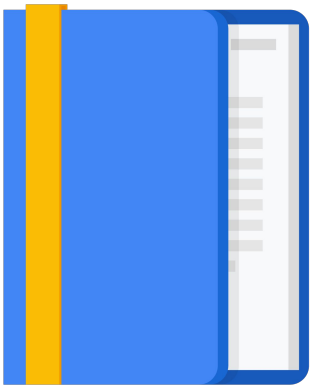
[Demostración]

Así de fácil es crear un rol personalizado en GCP. De forma alternativa, pude iniciar con el rol de Administrador de instancias como base y quitar los permisos que no deseo que tenga el rol.

Recuerde que Google no realiza mantenimiento a los roles personalizados. Esto significa que, cuando se agregan permisos, atributos o servicios nuevos a GCP, sus roles personalizados no se actualizan automáticamente.

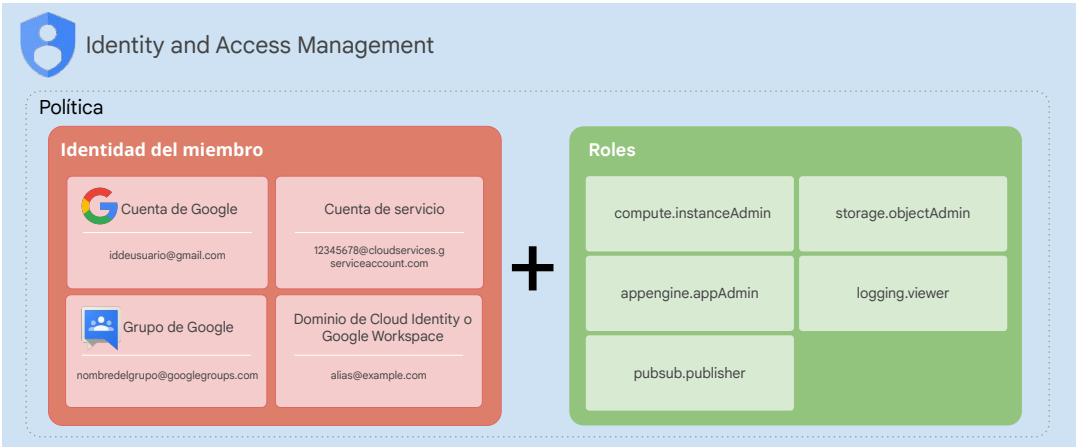
Temario

Identity and Access Management (IAM)
Organización
Roles
Miembros
Cuentas de servicio
Prácticas recomendadas de IAM
Lab



Analicemos los miembros, que definen la parte de “quién” en “quién puede hacer qué en un recurso”.

Miembros



Nota: Usted *no puede* usar IAM para crear ni administrar sus usuarios o grupos.

Existen cinco tipos diferentes de miembros: Cuentas de Google, cuentas de servicio, Grupos de Google, dominios de Google Workspace y dominios de Cloud Identity.

Una Cuenta de Google representa a un desarrollador, un administrador o cualquier otra persona que interactúe con Google Cloud. Cualquier dirección de correo electrónico asociada a una Cuenta de Google puede ser una identidad, incluidos gmail.com y otros dominios. Los usuarios nuevos se pueden registrar para obtener una Cuenta de Google en la página de registro de Cuentas de Google, sin recibir un correo electrónico a través de Gmail.

Una cuenta de servicio es una cuenta que pertenece a su aplicación en lugar de un usuario final individual. Cuando ejecuta código alojado en Google Cloud, debe especificar la cuenta con la que se ejecutará. Puede crear tantas cuentas de servicio como sea necesario para representar los diferentes componentes lógicos de su aplicación.

Un Grupo de Google es una colección de Cuentas de Google y cuentas de servicio que posee un nombre. Cada grupo tiene una única dirección de correo electrónico asociada. Los Grupos de Google son una forma conveniente de aplicar una política de acceso a un grupo de usuarios. Puede otorgar y cambiar los controles de acceso de un grupo completo de una sola vez, en lugar de hacerlo para usuarios individuales

o cuentas de servicio uno por uno.

Un dominio de Google Workspace representa un grupo virtual de todas las Cuentas de Google que se crearon en la cuenta de Workspace de una organización. Los dominios de Workspace representan el nombre de dominio de Internet de su organización, como example.com y, cuando agrega un usuario a su dominio de Workspace, se crea una nueva Cuenta de Google para el usuario dentro de este grupo virtual, como username@example.com.

Los clientes de Google Cloud que no son clientes de Workspace pueden obtener las mismas capacidades a través de Cloud Identity. Cloud Identity le permite administrar usuarios y grupos con la Consola del administrador de Google, pero no recibe ni paga por productos de colaboración de Workspace, como Gmail, Documentos, Drive y Calendario.

Es importante tener en cuenta que no puede usar IAM para crear ni administrar sus usuarios o grupos. En lugar de eso, puede usar Cloud Identity o Workspace para crear y administrar usuarios.

[Cloud Identity: https://support.google.com/cloudidentity/answer/7319251?hl=es-419]

Políticas de IAM

- Una política consta de una lista de vinculaciones.

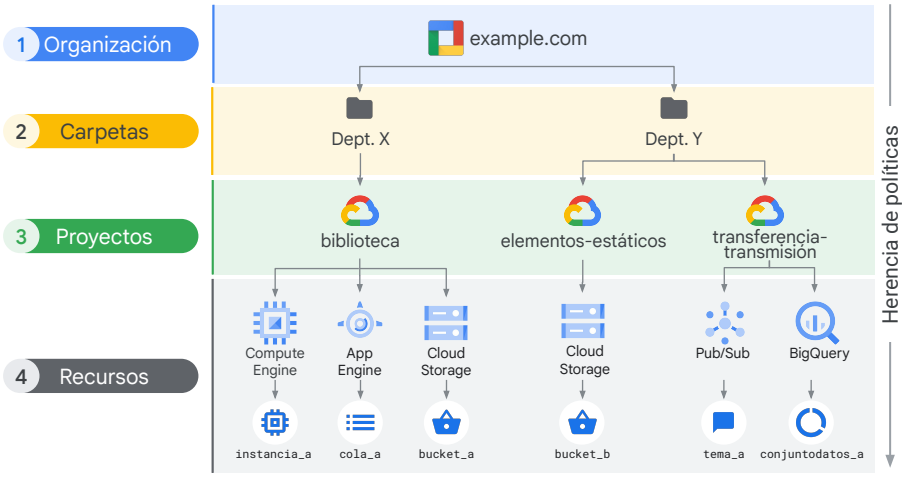
Una política consta de una lista de vinculaciones.

Políticas de IAM

- Una política consta de una lista de vinculaciones.
- Cada una de ellas vincula una lista de miembros a una función.

Una vinculación vincula una lista de miembros a un rol, y los miembros pueden ser cuentas de usuario, grupos o dominios de Google, o bien cuentas de servicio. Un rol es una lista identificada de permisos definidos por IAM. Repasemos la jerarquía de recursos de IAM.

Jerarquía de recursos de IAM



Una política es una colección de sentencias de acceso asociadas a un recurso.

Cada política contiene un conjunto de roles y miembros de roles, con recursos que heredan políticas de su elemento superior. Imagínelo de la siguiente manera: las políticas de recursos consisten en *una unión entre el elemento superior y el recurso*, en las que una política superior *menos* restrictiva siempre anulará a una política de recursos *más* restrictiva.

La jerarquía de políticas de IAM siempre sigue la misma ruta que la jerarquía de recursos de Google Cloud. Esto significa que, si cambia la jerarquía de recursos, la de políticas también cambia. Por ejemplo, cuando migra un proyecto a una organización diferente, se actualizará la política de IAM del proyecto para heredar la de la nueva organización.

Además, las políticas secundarias no pueden restringir el acceso otorgado en el nivel superior. Por ejemplo, si le otorgamos el rol de Editor al Departamento X y a usted el rol de Visualizador a nivel del proyecto de la biblioteca, seguirá teniendo el rol de Editor para ese proyecto. Por lo tanto, la práctica recomendada es seguir el principio de privilegio mínimo. Este se aplica a identidades, roles y recursos. Seleccione siempre el permiso con el menor alcance necesario para realizar la tarea, con el fin de reducir la exposición a riesgos.

También puede usar un recomendador de roles para identificar y quitar permisos excesivos de los principales, lo que mejora la configuración de seguridad de sus

recursos. Cada recomendación de rol sugiere que quite o reemplace un rol que otorgue permisos excesivos a los miembros. A gran escala, estas recomendaciones le permiten aplicar el principio de privilegio mínimo, ya que garantizan que las principales solo tengan los permisos que en verdad necesitan. El recomendador identifica los permisos no usados mediante las estadísticas de las políticas. Las estadísticas de políticas son resultados basados en el AA sobre el uso de permisos en el proyecto, la carpeta o la organización.

[Recomendaciones de roles:
https://cloud.google.com/iam/docs/recommender-overview]

Condiciones de IAM

Aplican control de acceso condicional y basado en atributos para los recursos de Google Cloud.

- Otorgan acceso a recursos para identidades (miembros) solo si se cumplen las condiciones configuradas.
- Se especifican en las vinculaciones de roles de la política de IAM de un recurso.

Las condiciones de IAM le permiten definir y aplicar el control de acceso condicional basado en atributos para los recursos de Google Cloud.

Con las Condiciones de IAM, puede optar por otorgarles a las identidades (miembros) acceso a recursos solo si se cumplen las condiciones configuradas. Esto puede hacerse a fin de configurar el acceso temporal de los usuarios en el caso de un problema de producción o para limitar el acceso a los recursos solo a los empleados que realizan solicitudes desde su oficina corporativa.

Las condiciones se especifican en las vinculaciones de roles de la política de IAM de un recurso. Cuando existe una condición, la solicitud de acceso solo se otorga si la expresión de la condición se evalúa como `verdadera`. Cada expresión de condición se define como un conjunto de declaraciones lógicas que le permiten especificar uno o más atributos que se deben verificar.

Políticas de la organización

Una política de la organización tiene las siguientes características:

- Es una configuración de restricciones.

Una política de la organización es una configuración de restricciones,

Políticas de la organización

Una política de la organización tiene las siguientes características:

- Es una configuración de restricciones.
- Se define por la configuración de una restricción con restricciones deseadas.

que se define por la configuración de una restricción con las restricciones deseadas para esa organización.

Políticas de la organización

Una política de la organización tiene las siguientes características:

- Es una configuración de restricciones.
- Se define por la configuración de una restricción con restricciones deseadas.
- Se aplica al nodo de organización, carpetas o proyectos.

Se puede aplicar al nodo de organización y a todos los proyectos o las carpetas dentro de ese nodo. Los descendientes del nodo de jerarquía de recursos objetivo heredan la política de la organización que se aplicó a los elementos superiores.

Se pueden hacer excepciones a estas políticas, pero solo de parte de un usuario con el rol de administrador de políticas de la organización.

¿Qué pasa si ya tengo un directorio corporativo diferente?

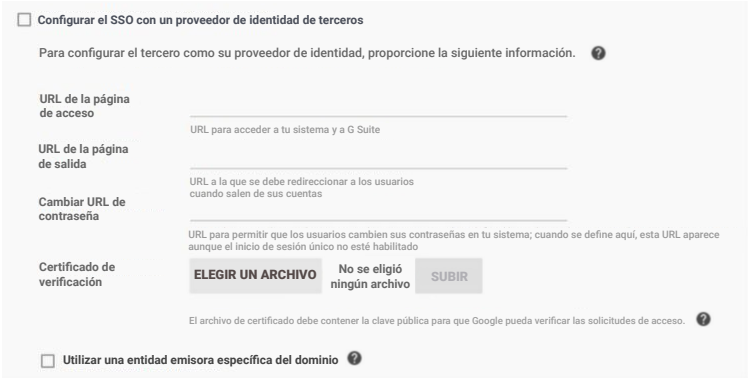
¿Qué pasa si ya tiene un directorio corporativo diferente? ¿Cómo puede llevar a sus usuarios y grupos a Google Cloud?

Con Google Cloud Directory Sync, sus administradores pueden acceder a recursos de Google Cloud y administrarlos con los mismos nombres de usuario y contraseñas que ya usaban. Esta herramienta sincroniza a usuarios y grupos de su sistema de Active Directory o LDAP con los usuarios y grupos de su dominio de Cloud Identity.

La sincronización es unilateral, esto significa que no se modifica la información de su Active Directory o mapa de LDAP. Google Cloud Directory Sync se diseñó para ejecutar sincronizaciones programadas sin supervisión, después de que se configuran sus reglas de sincronización.

Inicio de sesión único (SSO)

- Use Cloud Identity para configurar SSO SAML.
- Si SAML2 no es compatible, use una solución de terceros (ADFS, Okta o Ping).



Google Cloud también ofrece autenticación con inicio de sesión único.

Si tiene su sistema de identidad, puede seguir usando su sistema y procesos propios con SSO configurado. Cuando se requiera la autenticación de un usuario, Google lo redireccionará a su sistema. Si el usuario se autentica en su sistema, se otorga el acceso a Google Cloud; de lo contrario, se le pide al usuario que acceda.

De esta forma, también podrá revocar el acceso a Google Cloud.

Si su sistema de autenticación actual es compatible con SAML2, para realizar la configuración de SSO solo necesita 3 vínculos y un certificado, como se muestra en esta diapositiva. De lo contrario, puede usar una solución de terceros, como ADFS, Okta o Ping.

Para obtener más información sobre su sistema de administración de identidad existente, consulte la sección de vínculos de este video.

[https://cloud.google.com/blog/products/identity-security/using-your-existing-identity-management-system-with-google-cloud-platform]

Acceso a Google Cloud sin Gmail

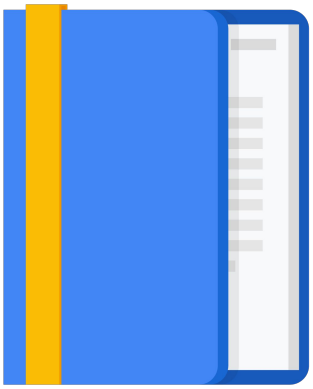
- Puede obtener una contraseña de Google sin Gmail.
- Hay beneficios por tener un dominio, incluidos los permisos de grupo.

Además, si desea usar una Cuenta de Google, pero no desea recibir correo electrónico a través de Gmail, puede crear una cuenta sin este servicio. Para obtener más información sobre el tema, consulte la sección de vínculos de este video.

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

Temario

Identity and Access Management (IAM)
Organización
Roles
Miembros
Cuentas de servicio
Prácticas recomendadas de IAM
Lab



Como mencioné antes, otro tipo de miembro es una cuenta de servicio.

Las cuentas de servicio proporcionan una identidad para llevar a cabo interacciones de servidor a servidor

- Los programas que ejecutan instancias de Compute Engine pueden adquirir tokens de acceso con credenciales automáticamente.
- Los tokens se usan para acceder a cualquier API de servicio en su proyecto y a cualquier otro servicio que otorgó acceso a esa cuenta de servicio.
- Las cuentas de servicio son convenientes cuando no tiene que acceder a los datos del usuario.

Una cuenta de servicio es una cuenta que pertenece a su aplicación en lugar de un usuario final individual. Esto proporciona una identidad para realizar interacciones servidor a servidor en un proyecto sin entregar credenciales de usuario.

Por ejemplo, si escribe una aplicación que interactúa con Google Cloud Storage, primero se debe autenticar en la API de XML o API de JSON Google Cloud Storage.

Puede habilitar cuentas de servicio y otorgar acceso de solo lectura a la cuenta en la instancia en la que piensa ejecutar su aplicación.

Luego, programe la aplicación para obtener credenciales desde la cuenta de servicio. Su aplicación se autentica sin problemas en la API y no incorpora claves secretas ni credenciales en su instancia, imagen o código de la aplicación.

Las cuentas de servicio se identifican mediante una dirección de correo electrónico

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

Las cuentas de servicio se identifican mediante una dirección de correo electrónico, como en este ejemplo.

Existen tres tipos de cuentas de servicio: creadas por usuarios o personalizadas, integradas y cuentas de servicio de las API de Google.

De forma predeterminada, todos los proyectos incluyen la cuenta de servicio predeterminada integrada de Compute Engine.

Además de la cuenta de servicio predeterminada, todos los proyectos incluyen una cuenta de servicio de la API de Google Cloud, que se puede identificar por el correo electrónico project-number@cloudservices.gserviceaccount.com. Esta es una cuenta de servicio diseñada específicamente para ejecutar procesos internos de Google en su nombre, y se le otorga automáticamente el rol de Editor en el proyecto.

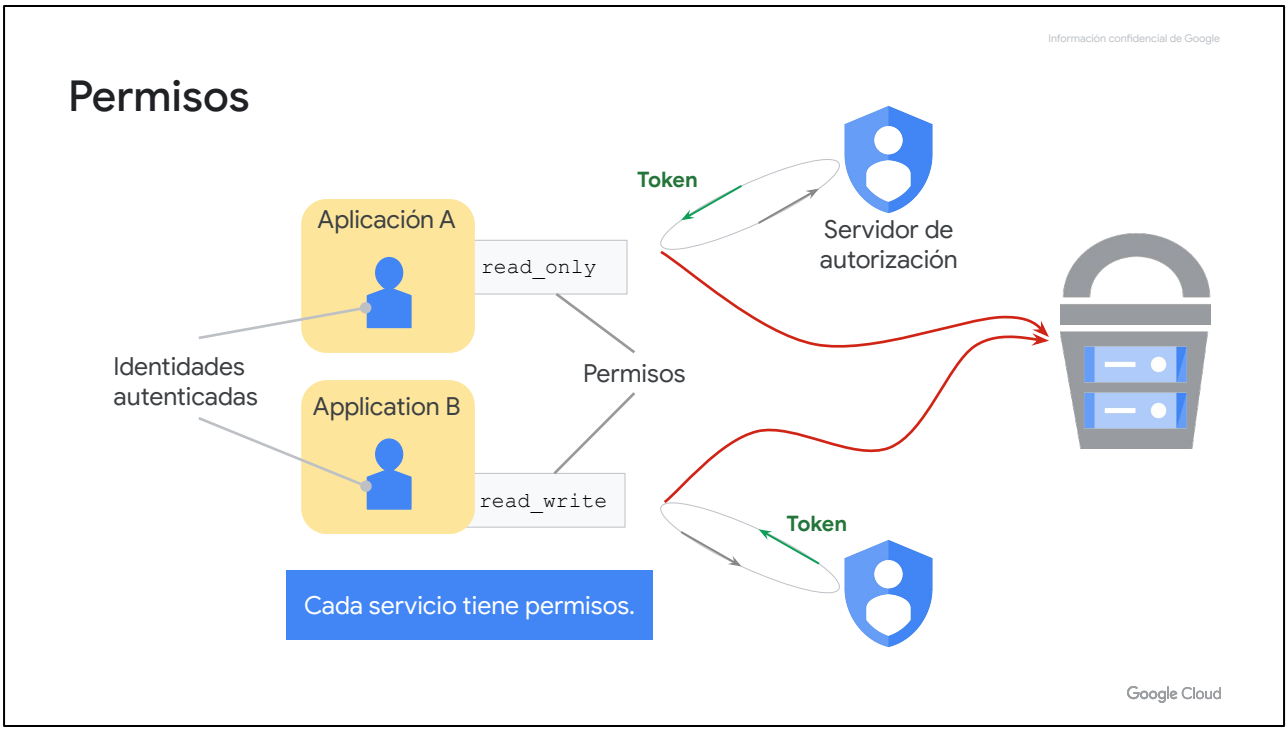
Como alternativa, también puede comenzar una instancia con una cuenta de servicio personalizada. Las cuentas de servicio personalizadas proporcionan más flexibilidad que las predeterminadas, pero requieren más administración de su parte. Puede crear la cantidad de cuentas de servicio personalizadas que necesite, asignarles cualquier permiso de acceso arbitrario o rol de IAM y asignarlas a cualquier instancia de máquina virtual.

Cuenta de servicio predeterminada de Compute Engine

- Creada por proyecto con un nombre y una dirección de correo electrónico generados automáticamente:
  - El nombre tiene el sufijo -compute `39xxxx0965-compute@developer.gserviceaccount.com`
- Se agrega automáticamente como Editor del proyecto.
- De forma predeterminada, se habilita en todas las instancias creadas con `gcloud` o Cloud Console.

Analicemos la cuenta de servicio predeterminada de Compute Engine. Como mencioné, esta cuenta se crea automáticamente por proyecto. Se puede identificar con el correo electrónico project-number-compute@developer.gserviceaccount.com y se le otorga automáticamente el rol de Editor en el proyecto.

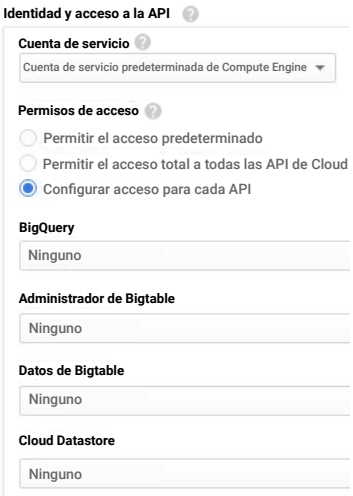
Cuando inicia una nueva instancia con gcloud, la cuenta de servicio predeterminada se habilita en ella. Puede anular este comportamiento si especifica otra cuenta de servicio o inhabilita las cuentas de servicio para la instancia.



La autorización es el proceso que determina qué permisos tiene una identidad autenticada en un conjunto de recursos especificados. Los permisos se usan para determinar si una identidad autenticada está autorizada.

En este ejemplo, las Aplicaciones A y B contienen identidades autenticadas (o cuentas de servicio). Supongamos que ambas aplicaciones desean usar un bucket de Cloud Storage. Cada una solicita acceso al servidor de autorización de Google y, a cambio, reciben un token de acceso. La Aplicación A recibe un token de acceso con permiso de solo lectura, por lo que solo puede leer desde el bucket de Cloud Storage. Por el contrario, la Aplicación B recibe un token de acceso con permiso de lectura y escritura, de modo que puede leer y modificar datos en el bucket de Cloud Storage.

Personalización de permisos para una VM



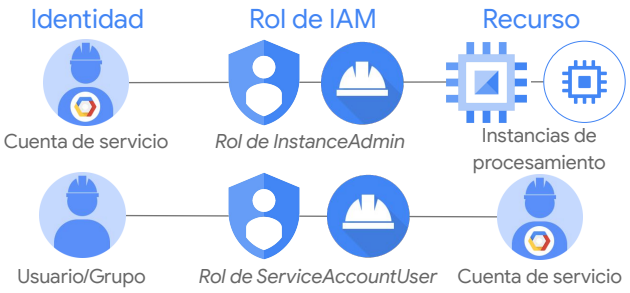
- Los permisos se pueden cambiar después de que se crea una instancia.
- Para las cuentas de servicio creadas por usuarios, use los roles de IAM en su lugar.

Los permisos se pueden personalizar cuando crea una instancia con la cuenta de servicio predeterminada, como se muestra en esta captura de pantalla. Además, se pueden cambiar después de que se crea una instancia si la detiene. Los permisos de acceso son el método heredado de especificar permisos para su VM. Antes de que existieran los roles de IAM, los permisos de acceso eran el único mecanismo para otorgarles permisos a cuentas de servicio.

Use los roles de IAM para especificar permisos en las cuentas de servicio creadas por el usuario.

Permisos de las cuentas de servicio

- Cuentas de servicio predeterminadas: roles básicos y predefinidos
- Cuentas de servicio creadas por usuarios: roles predefinidos
- Los roles para las cuentas de servicio se pueden asignar a grupos o usuarios

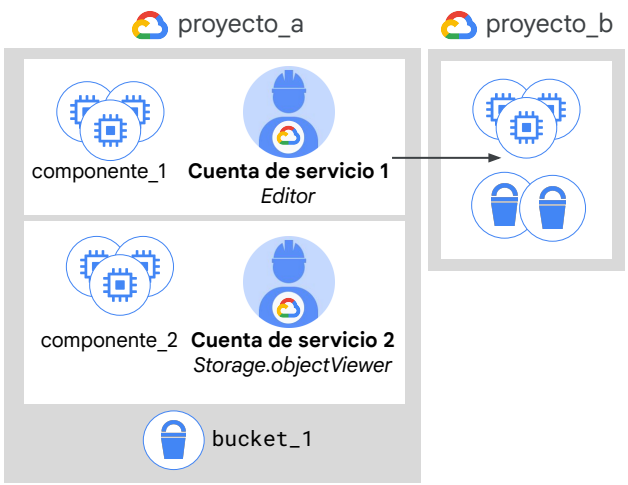


Los roles de las cuentas de servicio también se pueden asignar a grupos o usuarios. Observemos el ejemplo que aparece en esta diapositiva. Primero, usted crea una cuenta de servicio que tiene el rol InstanceAdmin, el cual tiene permisos para crear, modificar y borrar instancias y discos de máquina virtual. Luego, usted considera que esta cuenta de servicio es el recurso y, para decidir quién puede usarla, les otorga a usuarios o a un grupo el rol de usuario de cuenta de servicio. Esto permite que los usuarios se presenten como esa cuenta de servicio para crear, modificar y borrar instancias y discos de máquina virtual.

Los usuarios de cuenta de servicio (para una cuenta de servicio) pueden acceder a todos los recursos a los que tiene acceso esta cuenta. Por lo tanto, tenga cuidado cuando otorgue este rol a un usuario o grupo.

Ejemplo: IAM y cuentas de servicio

- A las VM que ejecutan el componente_1 se les otorga acceso de editor al proyecto_b por medio de la ***cuenta de servicio 1***.
- A las VM que ejecutan el componente_2 se les otorga acceso de objectViewer al bucket_1 por medio de la ***cuenta de servicio 2***.
- Los permisos de la cuenta de servicio se pueden cambiar sin necesidad de volver a crear VM.



A continuación, se muestra otro ejemplo. A las VM que ejecutan el componente_1 se les otorga acceso de editor al proyecto_b por medio de la cuenta de servicio 1. A las VM que ejecutan el componente_2 se les otorga acceso de objectViewer al bucket_1 por medio de una cuenta de servicio 2 aislada. De este modo, puede definir permisos para las VM sin volver a crearlas.

En términos sencillos, IAM le permite dividir un proyecto en diferentes microservicios, cada uno con acceso a recursos distintos, mediante la creación de cuentas de servicio para representar a cada uno de ellos. Si bien usted asigna las cuentas de servicio a las VM cuando se crean, no tiene que asegurarse de la correcta administración de las credenciales, ya que Google Cloud administra la seguridad por usted.

Es posible que se pregunte: ¿Cómo se autentican las cuentas de servicio?

Existen dos tipos de cuentas de servicio de Google

Cuentas de servicio administradas por Google

- Todas las cuentas de servicio tienen claves administradas por Google.
- Google almacena la parte privada y pública de la clave.
- Cada clave pública se puede usar para acceder durante un máximo de dos semanas.
- Nunca se puede acceder directamente a las claves privadas.

Cuentas de servicio administradas por el usuario

- Google solo almacena la sección pública de una clave administrada por el usuario.
- Los usuarios son responsables de la seguridad de la clave privada.
- Se pueden crear hasta 10 claves de cuenta de servicio administrado por el usuario por servicio.
- Se pueden administrar a través de la API de IAM, `gcloud` o Console.

Existen dos tipos de cuentas de servicio de Google.

De forma predeterminada, cuando usa cuentas de servicio dentro de Google Cloud (por ejemplo, desde Compute Engine o App Engine), Google administra automáticamente las claves para las cuentas de servicio. Sin embargo, si desea usar cuentas de servicio fuera de Google Cloud o quiere definir un período de rotación diferente, también es posible crear y administrar manualmente sus propias claves de cuenta de servicio.

Existen dos tipos de cuentas de servicio de Google

Cuentas de servicio administradas por Google

- Todas las cuentas de servicio tienen claves administradas por Google.
- Google almacena la parte privada y pública de la clave.
- Cada clave pública se puede usar para acceder durante un máximo de dos semanas.
- Nunca se puede acceder directamente a las claves privadas.

Cuentas de servicio administradas por el usuario

- Google solo almacena la sección pública de una clave administrada por el usuario.
- Los usuarios son responsables de la seguridad de la clave privada.
- Se pueden crear hasta 10 claves de cuenta de servicio administrado por el usuario por servicio.
- Se pueden administrar a través de la API de IAM, `gcloud` o Console.

Todas las cuentas de servicio tienen pares de claves administradas por Google.

Con las claves de cuenta de servicio administradas por Google, el servicio almacena las secciones pública y privada de la clave, y las rota con regularidad.

Cada clave pública se puede usar para acceder durante un máximo de dos semanas.

Su clave privada siempre se guarda de forma segura en un depósito y nunca se puede acceder a ella directamente.

Existen dos tipos de cuentas de servicio de Google

Cuentas de servicio administradas por Google

- Todas las cuentas de servicio tienen claves administradas por Google.
- Google almacena la parte privada y pública de la clave.
- Cada clave pública se puede usar para acceder durante un máximo de dos semanas.
- Nunca se puede acceder directamente a las claves privadas.

Cuentas de servicio administradas por el usuario

- Google solo almacena la sección pública de una clave administrada por el usuario.
- Los usuarios son responsables de la seguridad de la clave privada.
- Se pueden crear hasta 10 claves de cuenta de servicio administrado por el usuario por servicio.
- Se pueden administrar a través de la API de IAM, `gcloud` o Console.

Puede crear uno o más pares de claves administradas por el usuario (también conocidas como claves “externas”) que se pueden usar desde fuera de Google Cloud. Google solo almacena la sección pública de una clave administrada por el usuario.

El usuario es responsable de la seguridad de la clave privada y de realizar otras operaciones administrativas, como la rotación de claves, de forma manual o programática.

Los usuarios pueden crear hasta 10 claves de cuentas de servicio por cuenta de servicio a fin de facilitar la rotación de claves.

Las claves administradas por el usuario se pueden administrar mediante la API de IAM, la herramienta de línea de comandos de gcloud o la página de cuentas de servicio de Cloud Console.

Es fundamental que proteja sus claves administradas por el usuario. Esto es responsabilidad del creador

Recuerde: Google no guarda sus claves privadas administradas por el usuario, por lo que, si las pierde, no puede ayudarlo a recuperarlas.

Google no guarda sus claves privadas administradas por el usuario, así que, si las pierde, no podrá ayudarlo a recuperarlas.

Es responsable de proteger estas claves y, además, de realizar la rotación de claves.

Las claves administradas por el usuario solo se deben usar como último recurso. Considere otras alternativas, como las credenciales de cuentas de servicio de corta duración (tokens), o los permisos de robo de identidad de la cuenta de servicio.

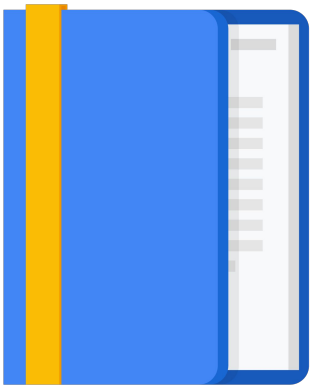
Use la herramienta de línea de comandos de gcloud para especificar rápidamente todas las claves asociadas a una cuenta de servicio

```
gcloud iam service-accounts keys list --iam-account user@email.com
```


La línea de comandos de `gcloud` de esta diapositiva es una forma fácil y rápida de mostrar todas las claves asociadas con una cuenta de servicio en particular.

Temario

Identity and Access Management (IAM)
Organización
Roles
Miembros
Cuentas de servicio
Prácticas recomendadas de IAM
Lab



Hablemos sobre algunas prácticas recomendadas de IAM que lo ayudarán a aplicar estos conceptos que acaba de aprender en su trabajo diario.

Aproveche y comprenda la jerarquía de recursos.

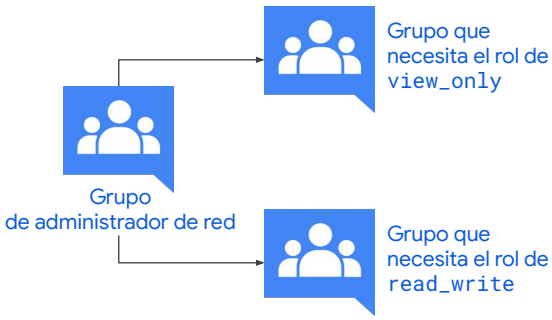
- Use proyectos para agrupar recursos que compartan el mismo límite de confianza.
- Verifique la política otorgada en cada recurso y asegúrese de que comprende la herencia.
- Use los “principios de privilegio mínimo” cuando otorgue roles.
- Realice auditorías de políticas en Registros de auditoría de Cloud: setiampolicy.
- Audite la pertenencia de los grupos que se usan en las políticas.

Primero, debe aprovechar y comprender la jerarquía de recursos.

- Específicamente, use proyectos para agrupar recursos que compartan el mismo límite de confianza.
- Verifique la política otorgada en cada recurso y asegúrese de que reconoce la herencia.
- Debido a la herencia, use el “principio de privilegio mínimo” cuando otorgue roles.
- Por último, audite las políticas con los Registros de auditoría de Cloud y audite la pertenencia a los grupos que se usan en las políticas.

Otorgue roles a Grupos de Google en lugar de a personas

- Actualice la pertenencia a un grupo en lugar de cambiar la política de IAM.
- Audite la pertenencia de los grupos que se usan en las políticas.
- Controle la propiedad del Grupo de Google que se usa en las políticas de IAM.



Le recomiendo otorgar roles a grupos en lugar de a personas. Esto le permite actualizar la pertenencia a un grupo en lugar de cambiar la política de IAM. Si lo hace, asegúrese de realizar auditorías de la pertenencia a grupos que se usan en políticas y controlar la propiedad del Grupo de Google que se usa en las políticas de IAM.

También puede usar varios grupos para tener un mayor control. En el ejemplo de esta diapositiva, hay un grupo de administradores de red. Algunos de esos miembros también necesitan un rol de read_write para un bucket de Cloud Storage, pero otros solo necesitan el rol de read_only. Cuando agrega y quita personas de los tres grupos, controla su acceso total. Por lo tanto, los grupos no solo se asocian con roles de trabajo, sino que pueden existir con el propósito de asignar roles.

Cuentas de servicio

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

Estas son algunas prácticas recomendadas para usar cuentas de servicio:

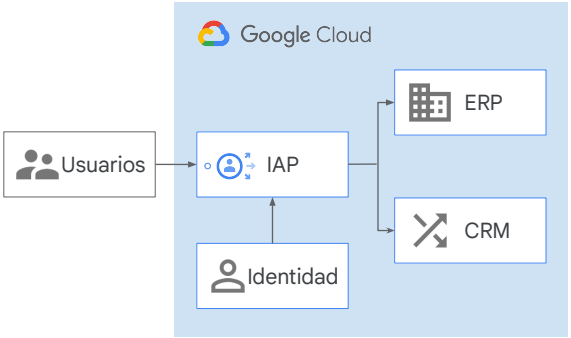
- Como mencionamos antes, debe tener cuidado cuando otorgue el rol de los usuarios de cuentas de servicio, porque brinda acceso a todos los recursos a los que tiene acceso la cuenta de servicio.
- Además, cuando cree una cuenta de servicio, otórguele un nombre visible que identifique claramente su propósito, de ser posible, con una convención de nombres establecida.
- En cuanto a las claves, establezca políticas y métodos de rotación de claves, y claves de auditoría con el método serviceAccount.keys.list().

Identity-Aware Proxy (IAP)

Aplique políticas de control de acceso para las aplicaciones y los recursos:

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

La política de IAM se aplica después de la autenticación.



Por último, le recomiendo usar Identity-Aware Proxy, o IAP. IAP le permite establecer una capa de autorización central para las aplicaciones a las que se accede mediante HTTPS, por lo que puede usar un modelo de control de acceso a nivel de aplicación en lugar de firewalls a nivel de red.

Solo los usuarios y grupos con el rol de IAM correcto pueden acceder a las aplicaciones y los recursos con la protección de IAP a través de un proxy. Cuando otorga a un usuario acceso a una aplicación o un recurso mediante IAP, estará sujeto a los controles de acceso detallados que implementa el producto en uso sin necesidad de una VPN. IAP realiza verificaciones de autenticación y autorización cuando un usuario trata de acceder a un recurso con la protección de IAP, como se muestra en el lado derecho.

Para obtener más información sobre IAP, consulte la sección de vínculos de este video.

[https://cloud.google.com/iap/docs/concepts-overview]

Lab

Cloud IAM

Es hora de aplicar lo que aprendió.

En este lab, otorgará y revocará roles para cambiar el acceso. Específicamente, usará Cloud IAM para implementar control de acceso, restringir el acceso a funciones y recursos específicos, y usar el rol de usuario de la cuenta de servicio.

Cuando realice cambios en los roles de IAM, GCP Console se actualizará más rápido que el sistema. Por lo tanto, es posible que experimente algunos retrasos breves cuando realice cambios en el rol de un miembro.

Repaso del lab

Cloud IAM

En este lab, otorgó y revocó roles de IAM, primero a un usuario (Nombre de usuario 2) y, luego, a un usuario de cuenta de servicio. Cuando accedió a ambos usuarios, pudo ver los resultados de los cambios que realizó.

Puede continuar con un recorrido por el lab, pero recuerde que la interfaz de usuario de GCP puede cambiar, por lo que su entorno podría verse un poco diferente.

Repaso

Identity and Access Management

En este módulo, abordamos Identity and Access Management junto con sus componentes y prácticas recomendadas. IAM se basa en otros servicios de Google Cloud Identity.

La creación y administración de identidades corporativas ocurre a través del administrador de Workspace o la interfaz de Cloud Identity y, normalmente, las controla una persona independiente del administrador de Google Cloud.

Los Grupos de Google son un buen método para que estas dos funciones empresariales colaboren. Usted establece los roles y los asigna al grupo y, luego, el administrador de Workspace administra la pertenencia al grupo.

Por último, recuerde que las cuentas de servicio son muy flexibles y le permiten compilar en su aplicación un nivel de control basado en la infraestructura.