



Tot plugin GCP IAM

Control de versiones	2
Modelo de integración	3
Gobierno activo	3
Credenciales requeridas	3
Crear la cuenta de servicio	3
Gobierno activo	5
Ejemplo de configuración	6

Control de versiones

Versión	Fecha de modificación	Responsable	Aprobador	Resumen de cambios
1.0	28/10/2022	Anjana Producto	Anjana Producto	Creación del documento

Modelo de integración

Gobierno activo

Para gestionar los permisos y roles, el plugin se conecta a una instancia de Google IAM¹, la cual da acceso a una API que proporciona Google en su plataforma Cloud que gestiona el control de acceso e identidades sobre los recursos de la propia plataforma.

El contrato está representado por un rol custom con los permisos genéricos de acceso a la tecnología preconcedidos, los usuarios se asocian a dicho rol (adquieren dichos permisos) usando políticas en las cuales se termina de especificar el grano fino a nivel elemento en las tecnologías que lo permitan.

Las acciones que se aplican sobre GCP son la siguientes:

- Creación/modificación/eliminación de roles custom.
- Asignación de roles a usuarios mediante políticas IAM con condiciones de aplicabilidad (para gestionar acceso a nivel elemento). En el plugin GCP IAM se recupera el nombre de los roles y es en otros plugins como el de GCP FILES donde se asignan/eliminan dichos roles para los usuarios.

Credenciales requeridas

Las credenciales requeridas se deberán configurar en el fichero yaml que utilizaremos para arrancar el servicio en la propiedad “totplugin.connection.credentialsContent”

Crear la cuenta de servicio

Para GCP será necesario crear una cuenta de servicio en IAM para cada plugin de forma individual y tras eso asignarle los permisos necesarios para la ejecución de las tareas específicas de cada plugin.

—   gcp-bigquery@anjana-data-
qa.iam.gserviceaccount.com gcp-bigquery

—   gcp-storage@anjana-data-
qa.iam.gserviceaccount.com gcp-storage

—   gpc-iam@anjana-data-
qa.iam.gserviceaccount.com gpc-iam

¹ Documentación Google IAM: <https://cloud.google.com/iam/docs>

Para personalizar los permisos de forma más acorde será necesaria la creación de roles personalizados en los cuáles se engloban los permisos que luego son asociados a las cuentas de servicio.

IAM y administración

- IAM**
- Identidad y organización
- Solucionador de problemas ...
- Analizador de políticas
- Políticas de la organización
- Cuentas de servicio
- Federación de Workload Ide...
- Etiquetas
- Configuración
- Privacidad y seguridad
- Identity-Aware Proxy
- Funciones**
- Registros de auditoría
- Inventario de recursos
- Contactos esenciales
- Grupos
- Cuotas

Administrador de recursos

Crear rol

Las funciones personalizadas permiten agrupar permisos y asignarlos a las principales de tu organización o proyecto. Puedes seleccionar permisos de forma manual o importarlos desde otra función. [Más información](#)

Título * 18 de 100 caracteres

Descripción 29 de 256 caracteres

ID *

Etapa de lanzamiento de la función

AGREGAR PERMISOS

No hay permisos asignados

Permiso	Estado
No hay filas para mostrar	

Es posible que algunos permisos estén asociados con terceros y que estos los revisen. Estos permisos contienen el servicio y nombre de dominio del tercero en el prefijo del permiso.

CREAR **CANCELAR**

Gobierno activo

Los permisos utilizados son los siguientes:

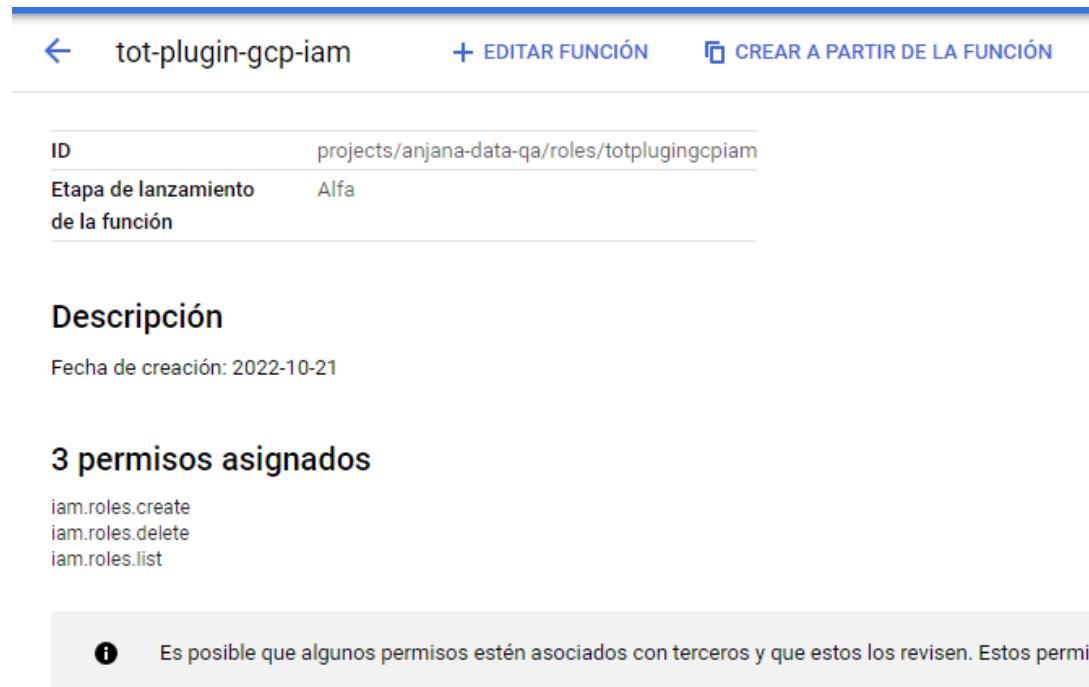
- `iam.roles.create`
- `iam.roles.delete`
- `iam.roles.list`

Apis requeridas en proyecto:

- Identity and Access Management (IAM) API

- Admin API SDK

En resumen los permisos utilizados para el rol personalizado serán los siguientes:



The screenshot shows the 'tot-plugin-gcp-iam' role configuration page. It includes the role's ID, launch stage, and a description section with creation date. It lists three assigned permissions: iam.roles.create, iam.roles.delete, and iam.roles.list. A note indicates that some permissions might be associated with external accounts.

ID	projects/anjana-data-qa/roles/totpluggingcpiam
Etapa de lanzamiento de la función	Alfa

Descripción

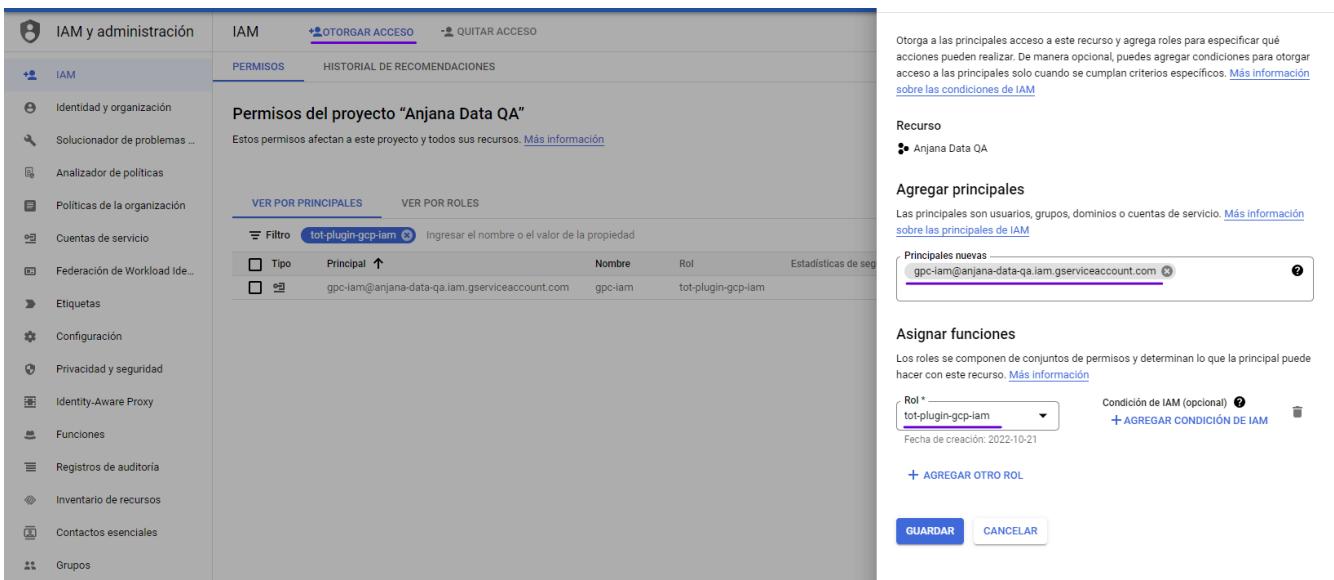
Fecha de creación: 2022-10-21

3 permisos asignados

iam.roles.create
iam.roles.delete
iam.roles.list

Es posible que algunos permisos estén asociados con terceros y que estos los revisen. Estos permisos no se incluirán en tu cuenta de servicio.

Para asignar los permisos a la cuenta de servicio de iam tendremos que:



The screenshot shows the IAM & administración interface under the IAM tab. It displays the 'PERMISOS' section for the project 'Anjana Data QA'. A table lists a single principal ('gpc-iam@anjana-data-qa.iam.gserviceaccount.com') with the role 'tot-plugin-gcp-iam'. The 'Asignar funciones' section is visible on the right, showing the selected role and a condition for the IAM service account.

Tipo	Principal	Nombre	Rol
<input type="checkbox"/>	gpc-iam@anjana-data-qa.iam.gserviceaccount.com	gpc-iam	tot-plugin-gcp-iam

Ejemplo de configuración

Se han de revisar las configuraciones comunes en el doc de configuraciones “Anjana Data - Microservices configuration”

Configuraciones específicas:

- connection:
 - credentialsContent: Credenciales de acceso a GCP.
 - project: Nombre del proyecto

```
server:
  port: 15010

totplugin:
  location: http://totpluggingcpiamserver:15010/plugin/gcp/iam/api/v1
  server:
    url: http://totserver:15000/tot/
  aris:
    - ari: "anja:totplugin:im:/Google/gcpIam/devQA/"
  groupPrefix: Dsa_
  connection:
    project: "projects/anjana-data-qa"
    credentialsContent: |
      {
        "type": "service_account",
        "project_id": "anjana-data",
        "private_key_id": "*****",
        "private_key": "-----BEGIN PRIVATE KEY-----\n-----END PRIVATE KEY-----\n",
        "client_email": "gpc-iam@****.com",
        "client_id": "*****",
        "auth_uri": "https://accounts.google.com/o/oauth2/auth",
        "token_uri": "https://oauth2.googleapis.com/token",
        "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
        "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/gpc-iam%40****.com"
      }
```