



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"

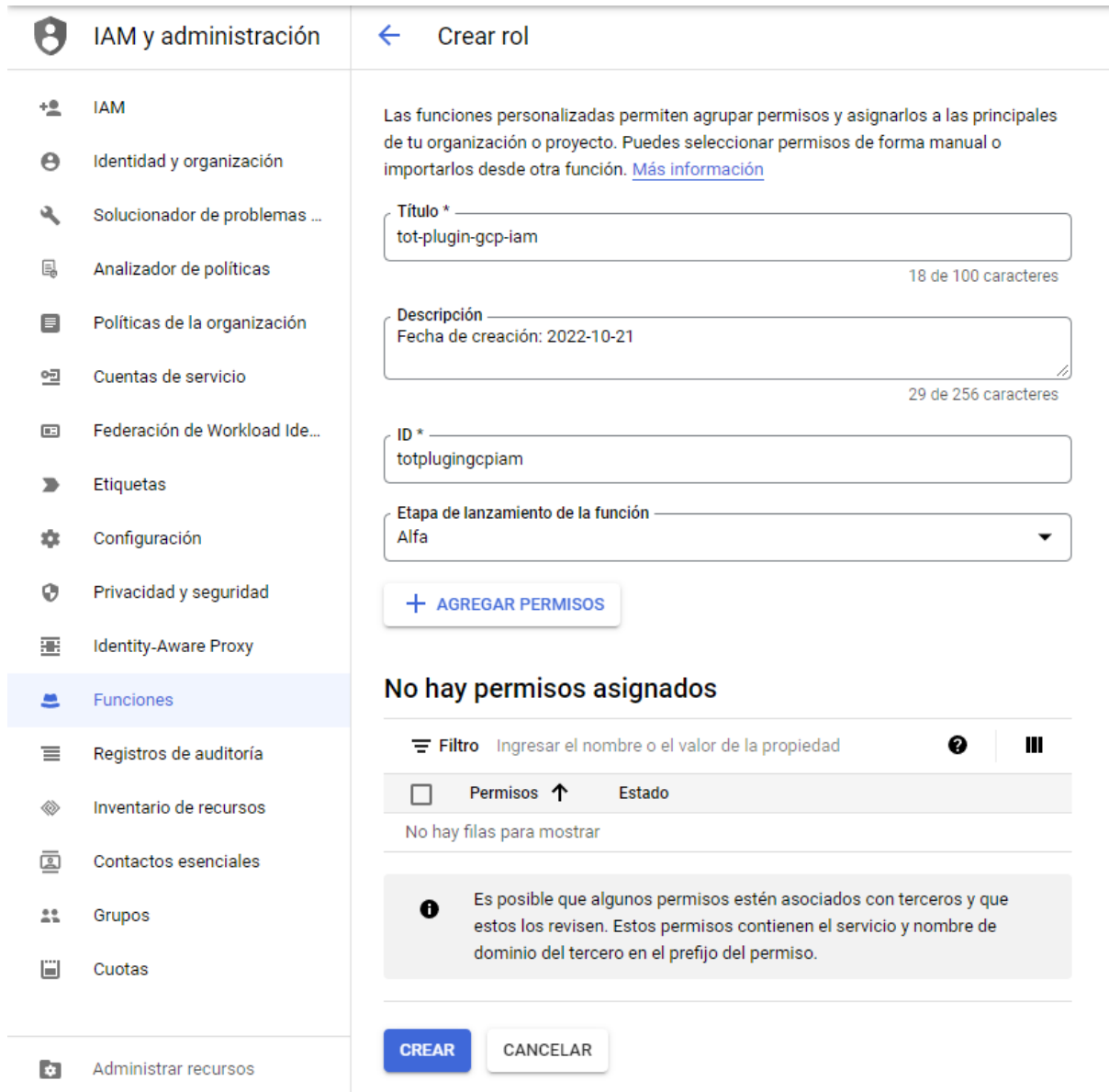
Crear la cuenta de servicio

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.

	<code>gcp-bigquery@anjana-data-qa.iam.gserviceaccount.com</code>	<code>gcp-bigquery</code>
	<code>gcp-storage@anjana-data-qa.iam.gserviceaccount.com</code>	<code>gcp-storage</code>
	<code>gpc-iam@anjana-data-qa.iam.gserviceaccount.com</code>	<code>gpc-iam</code>

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 ← 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 *
tot-plugin-gcp-iam
18 de 100 caracteres

Descripción
Fecha de creación: 2022-10-21
29 de 256 caracteres

ID *
totpluggingcpiam

Etapa de lanzamiento de la función
Alfa

+ AGREGAR PERMISOS

No hay permisos asignados

Filtro Ingresar el nombre o el valor de la propiedad ?

Permisos ↑ 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:

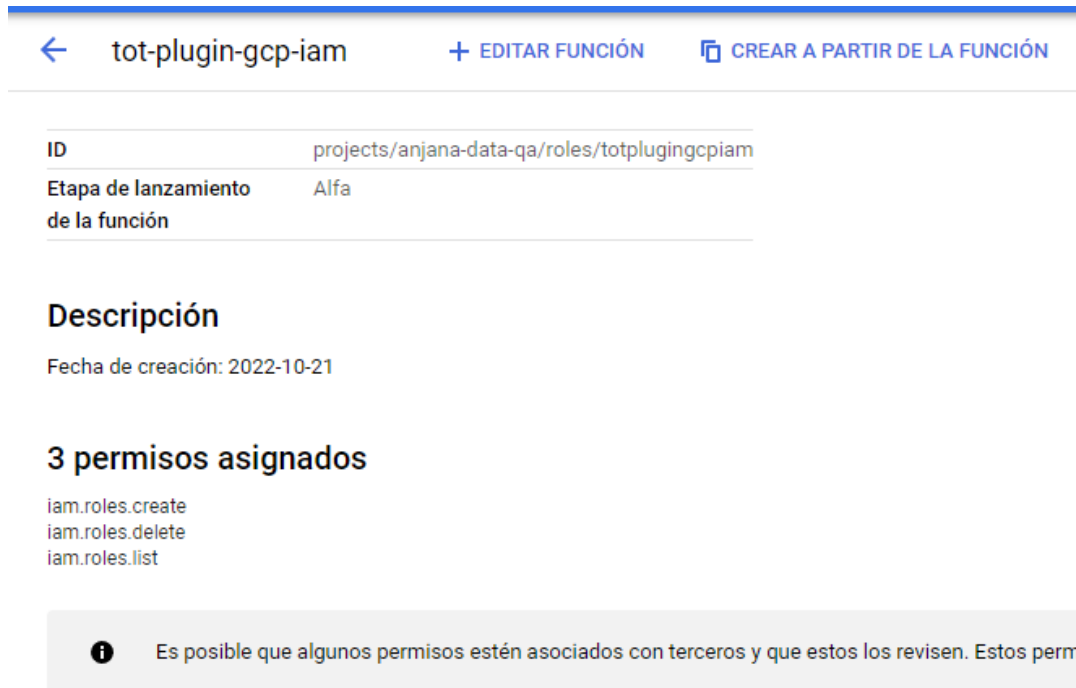
- iam.roles.create
- iam.roles.delete
- iam.roles.list

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:



← tot-plugin-gcp-iam + EDITAR FUNCIÓN CREAR A PARTIR DE LA FUNCIÓN

ID: projects/anjana-data-qa/roles/totpluggingcpiam

Etapa de lanzamiento de la función: Alfa

Descripción

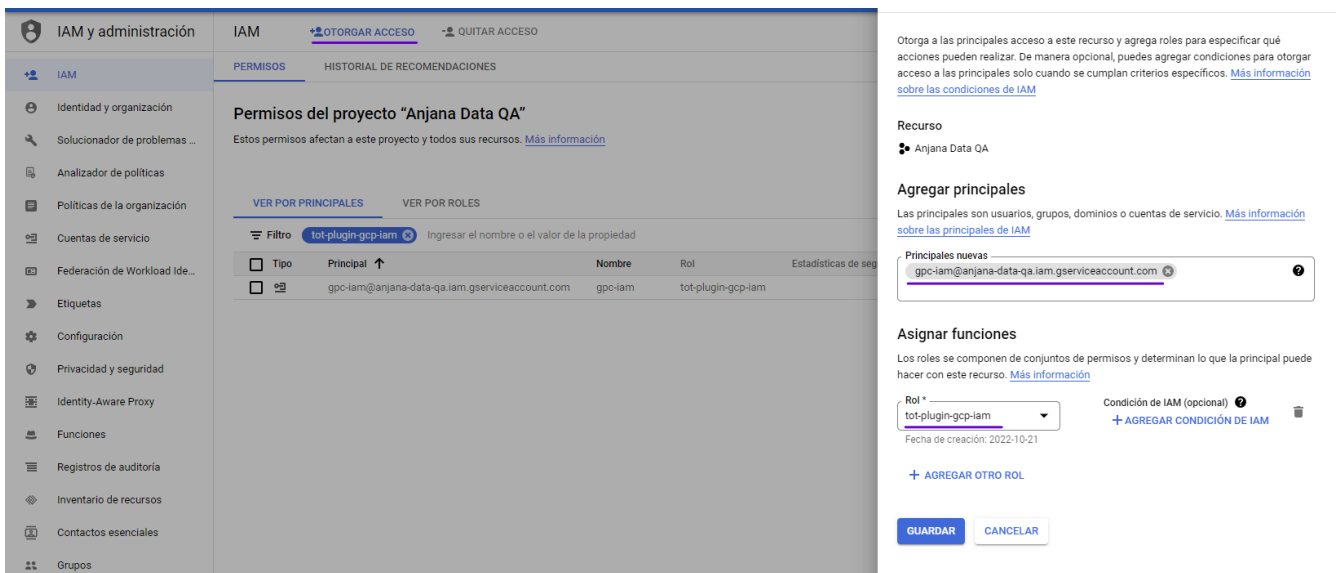
Fecha de creación: 2022-10-21

3 permisos asignados

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

i Es posible que algunos permisos estén asociados con terceros y que estos los revisen. Estos perm...

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



IAM y administración IAM + OTORGAR ACCESO - QUITAR ACCESO

PERMISOS HISTORIAL DE RECOMENDACIONES

Permisos del proyecto "Anjana Data QA"

Estos permisos afectan a este proyecto y todos sus recursos. [Más información](#)

VER POR PRINCIPALES VER POR ROLES

Filtro: tot-plugin-gcp-iam Ingresar el nombre o el valor de la propiedad

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

Otorga a las principales acceso a este recurso y agrega roles para especificar qué acciones pueden realizar. De manera opcional, puedes agregar condiciones para otorgar acceso a las principales solo cuando se cumplan criterios específicos. [Más información sobre las condiciones de IAM](#)

Recurso: Anjana Data QA

Agregar principales

Las principales son usuarios, grupos, dominios o cuentas de servicio. [Más información sobre las principales de IAM](#)

Principales nuevas: gcp-iam@anjana-data-qa.iam.gserviceaccount.com

Asignar funciones

Los roles se componen de conjuntos de permisos y determinan lo que la principal puede hacer con este recurso. [Más información](#)

Rol: tot-plugin-gcp-iam Condición de IAM (opcional) + AGREGAR CONDICIÓN DE IAM

Fecha de creación: 2022-10-21

+ AGREGAR OTRO ROL

GUARDAR CANCELAR

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"
      }

```