



Integración GCP

Control de versiones	2
Modelo de integración	3
Autenticación y autorización (Oauth2)	3
Configuración de autenticación	3
Configuración de autorización	4
Gobierno activo	5
Nomenclatura de los grupos y UO	5
Grupos en Gsuite	5
Roles GCP	5
Credenciales requeridas	5
Autenticación y autorización (Oauth2)	6
API's necesarias	6
Provisión de credencial	6
Asignación de roles en GCP y Gsuite	17
Funciones en GCP	17
Grupos en Gsuite	18
Gobierno activo	19
Emulación SSO vía Oauth2	19

Control de versiones

Versión	Fecha de modificación	Responsable	Aprobador	Resumen de cambios
1.0	22/11/2023	Anjana Producto	Anjana Producto	Creación del documento. Compatibilidad con la v4.5 de todos los módulos de Anjana

Modelo de integración

Autenticación y autorización (Oauth2)

Anjana Data se integra mediante circuito estándar Oauth2 para “Web apps” el cual se describe por el fabricante en la siguiente documentación:

<https://developers.google.com/identity/protocols/oauth2/web-server>

La funcionalidad está directamente embebida en el microservicio de gestión de autenticación y autorización Zeus, se habilita y configura mediante el fichero de configuración de dicho microservicio.

Este microservicio está preparado para reconocer como grupos tanto los grupos provenientes de Gsuite como los roles custom creados en GCP siendo ambos mapeados para asignar la autorización correspondiente al usuario en Anjana Data.

Configuración de autenticación

En la propiedad *security.authentication* se configuran los distintos proveedores de autenticación que se utilizan.

En el caso de GCP es necesario configurar las siguientes propiedades:

```
security:
  authentication:
    oidc:
      google:
        name: Anjana google
        authorize-url:
https://accounts.google.com/o/oauth2/v2/auth?client_id=${security.authentication.oidc.providers.google.client-id}&response_type=code&scope=${security.authentication.oidc.providers.google.scopes}&redirect_uri=${security.authentication.oidc.providers.google.redirect-uri}
        authorize-url-portuno:
https://accounts.google.com/o/oauth2/v2/auth?client_id=${security.authentication.oidc.providers.google.client-id}&response_type=code&scope=${security.authentication.oidc.providers.google.scopes}&redirect_uri=${security.authentication.oidc.providers.google.redirect-uri-portuno}
        }
        token-url: https://oauth2.googleapis.com/token
        scopes: openid email
        client-id: <clientId>
        client-secret: <clientSecret>
        client-authentication-method: BASIC
        redirect-uri: https://client.anjanadata.org/anjana/authorized
        redirect-uri-portuno:
https://client.anjanadata.org/admin/authorized
        username-claim: email
        type: GOOGLE
```

Configuración de autorización

En la propiedad `security.authorization` se configuran los distintos proveedores de autorización que se utilizan.

En el caso de GCP es necesario configurar las siguientes propiedades:

```
security:
  authorization:
    google-api:
      providers:
        google:
          json-content: '
{
  "type": "service_account",
  "project_id": "AAAAAAAAAA",
  "private_key_id": "*****",
  "private_key": "-----BEGIN PRIVATE KEY-----END
PRIVATE KEY-----",
  "client_email": "*****.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/*****.com"
}'
          json-path: /opt/AAAAA-aaabbbccc.json # absolute path -->
/xxxxxx.json
          delegated: persona@dominio.com
          customer: CCC000
          group-org-unit-separator: "/"
          role-org-unit-separator: "-"
          groupPrefix: "prefix-"
```

- `group-org-unit-separator`: separador de partes de unidad organizativa en un grupo (nunca valor ""). Esta propiedad, por tanto, debe tener valor o no ser definida)
En caso de configurar un separador distinto a '/', en el provider las OUs no se puede usar '/' como parte de un nombre de OU)
- `role-org-unit-separator`: separador del rol del resto de la cadena en un grupo (nunca valor ""). Esta propiedad, por tanto, debe tener valor o no ser definida)
- `groupPrefix`: prefijo que contengan los grupos (nunca valor ""). Esta propiedad, por tanto, debe tener valor o no ser definida)

Gobierno activo

De forma general los DSA de Anjana Data serán representados como roles custom y los firmantes de dichos DSA son asociados a dichos roles mediante políticas en cada una de las tecnologías en las cuales adicionalmente se aplicarán condiciones para habilitar el acceso a recursos específicos.

Nomenclatura de los grupos y UO

Para asignar unidades organizativas y grupos a los usuarios se pueden usar dos mecanismos diferentes, se pueden crear grupos en gsuite o roles en GCP, el producto intentará recuperar ambas asignaciones y las agrega como solo una.

Grupos en Gsuite

El nombre del grupo debe contener el alias de la unidad organizativa y el rol que aplica a dicha unidad organizativa.

Un ejemplo de un nombre de un grupo sería : HQ/Legal-architect , donde HQ/Legal es el alias de la unidad organizativa y architect el rol.

Como se puede observar hay dos separadores:

- El separador de jerarquía de la unidad organizativa: '/', cuyo valor es configurable gracias a la propiedad del yml: group-org-unit-separator.
- El separador de la unidad organizativa y el rol: '-', cuyo valor es configurable gracias a la propiedad del yml: group-actor-separator.

Roles GCP

El **ID del rol** (en el nombre se puede poner lo que se quiera) debe contener el alias de la unidad organizativa y el rol que aplica a dicha unidad organizativa.

Un ejemplo de un nombre de un grupo sería : HQ.Legal_architect , donde HQ.Legal es el alias de la unidad organizativa y architect el rol¹.

Como se puede observar hay dos separadores:

- El separador de jerarquía de la unidad organizativa: '.', cuyo valor es configurable gracias a la propiedad del yml: role-org-unit-separator.
- El separador de la unidad organizativa y el rol: '_', cuyo valor es configurable gracias a la propiedad del yml: role-actor-separator².

Credenciales requeridas

La credencial puede ser única aglutinando los permisos requeridos por todos los plugins a desplegar, pero se recomienda mantenerla por separado de cara a facilitar la monitorización y auditoría de la actividad ejercida por cada una de las mismas.

¹ Independientemente de los separadores usados en los repositorios de identidades el producto normalizará al formato estándar, por lo que en la configuración del producto ha de usarse siempre los separadores "/" y "-" para conformar el alias, por ejemplo "UO/UO..../UO-role".

² Los separadores por defecto son diferentes para roles y grupos puesto que los caracteres permitidos en roles son más estrictos que en grupos, puede unificarse si se desea usando los separadores de roles también en grupos.

Autenticación y autorización (Oauth2)

En la actualidad es necesario habilitar acceso tanto en GCP como en Gsuite para poder recuperar la información del usuario y los grupos o roles custom a los que pertenece, para ello es necesario habilitar API específicas de ambos y configurar la delegación de acceso de la cuenta de servicio a usar para que pueda acceder a los scope requeridos de Gsuite.

API's necesarias

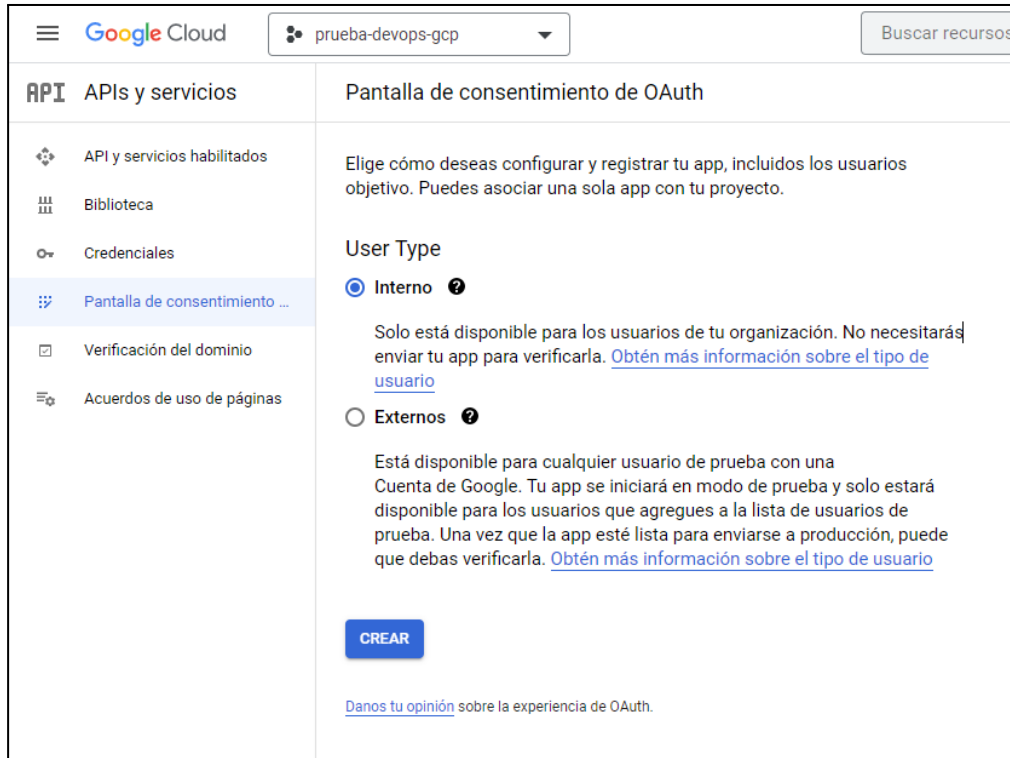
1. Admin SDK API
2. Identity and Access Management (IAM) API
3. Cloud Resource Manager API

Provisión de credencial

- OAuth 2.0 Client ID type web application with authorized url pointed to POC installation point (<https://<hostname>:<port>/anjana/login> and <https://<hostname>:<port>/anjana/authorized>), default package has configured apache self signed certificate listening con 8443 port. Documentation at <https://developers.google.com/identity/protocols/oauth2/web-server>
- OAuth 2.0 Client type service account with domain delegation and following permissions (DOC <https://developers.google.com/admin-sdk/directory/v1/guides/delegation>):
 - GCP roles (en la cuenta de servicio a usar en Zeus)
 - Role Viewer
 - Identity Platform Viewer
 - Identity Toolkit Viewer
 - Google Cloud Managed Identities Viewer
 - Functions Viewer
 - Permisos a nivel APP (afecta al registrar la nueva aplicación web)
 - Admin SDK API
 - .../auth/admin.directory.user.readonly
 - .../auth/admin.directory.user.alias.readonly
 - .../auth/admin.directory.customer.readonly
 - .../auth/admin.directory.domain.readonly
 - .../auth/admin.directory.group.readonly
 - .../auth/admin.directory.group.member.readonly
 - .../auth/admin.directory.orgunit.readonly
 - .../auth/iam
 - Gsuite scopes (afecta en gsuite en el registro de la aplicación web en control de api's)
 - Openid
 - <https://www.googleapis.com/auth/admin.directory.user.readonly>
 - <https://www.googleapis.com/auth/admin.directory.group.readonly>
 - <https://www.googleapis.com/auth/admin.directory.group.member.readonly>
 - <https://www.googleapis.com/auth/admin.directory.domain.readonly>
 - <https://www.googleapis.com/auth/admin.directory.orgunit.readonly>
 - <https://www.googleapis.com/auth/cloud-platform>

- <https://www.googleapis.com/auth/admin.directory.rolemanagement.readonly>

1. Registrar una web application



Google Cloud prueba-devops-gcp Buscar recursos

API APIs y servicios

- API y servicios habilitados
- Biblioteca
- Credenciales
- Pantalla de consentimiento ...**
- Verificación del dominio
- Acuerdos de uso de páginas

Pantalla de consentimiento de OAuth

Elige cómo deseas configurar y registrar tu app, incluidos los usuarios objetivo. Puedes asociar una sola app con tu proyecto.

User Type

Interno ?

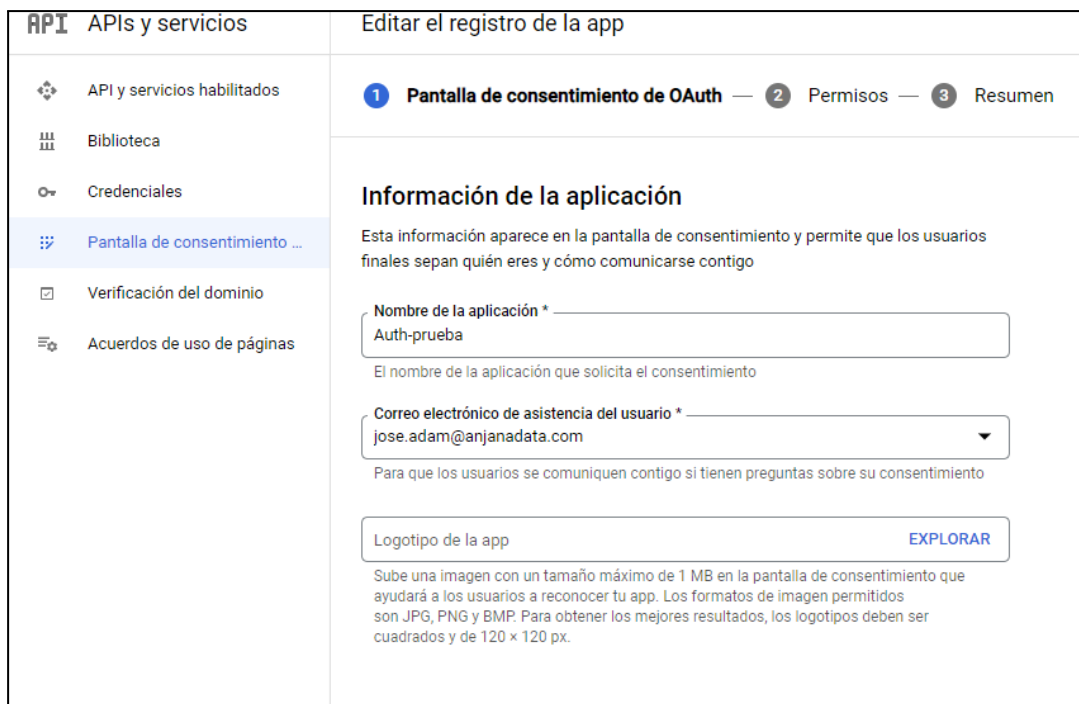
Solo está disponible para los usuarios de tu organización. No necesitarás enviar tu app para verificarla. [Obtén más información sobre el tipo de usuario](#)

Externos ?

Está disponible para cualquier usuario de prueba con una Cuenta de Google. Tu app se iniciará en modo de prueba y solo estará disponible para los usuarios que agregues a la lista de usuarios de prueba. Una vez que la app esté lista para enviarse a producción, puede que debas verificarla. [Obtén más información sobre el tipo de usuario](#)

CREAR

[Danos tu opinión](#) sobre la experiencia de OAuth.



API APIs y servicios

- API y servicios habilitados
- Biblioteca
- Credenciales
- Pantalla de consentimiento ...**
- Verificación del dominio
- Acuerdos de uso de páginas

Editar el registro de la app

1 **Pantalla de consentimiento de OAuth** — 2 Permisos — 3 Resumen

Información de la aplicación

Esta información aparece en la pantalla de consentimiento y permite que los usuarios finales sepan quién eres y cómo comunicarse contigo

Nombre de la aplicación *

El nombre de la aplicación que solicita el consentimiento

Correo electrónico de asistencia del usuario *

Para que los usuarios se comuniquen contigo si tienen preguntas sobre su consentimiento

Logotipo de la app

Sube una imagen con un tamaño máximo de 1 MB en la pantalla de consentimiento que ayudará a los usuarios a reconocer tu app. Los formatos de imagen permitidos son JPG, PNG y BMP. Para obtener los mejores resultados, los logotipos deben ser cuadrados y de 120 x 120 px.

Dominios autorizados ?

Cuando un dominio se usa en la pantalla de consentimiento o en la configuración del cliente de OAuth, debe contar con un registro previo aquí. Si debes verificar la app, ve [Google Search Console](#) para comprobar si tus dominios están autorizados. [Más información](#) sobre el límite de dominios autorizados.

Dominio autorizado 1 *

[+ AGREGAR UN DOMINIO](#)

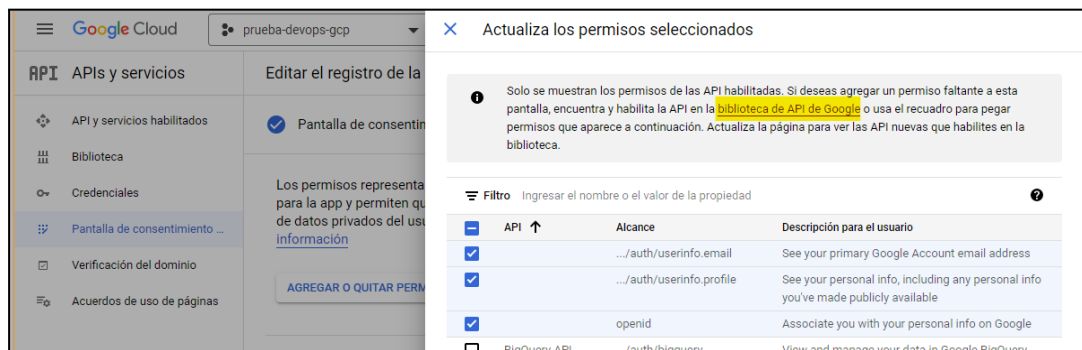
Información de contacto del desarrollador

Direcciones de correo electrónico *

Google enviará notificaciones sobre cualquier cambio en tu proyecto a estas direcciones de correo electrónico.

[GUARDAR Y CONTINUAR](#) [CANCELAR](#)

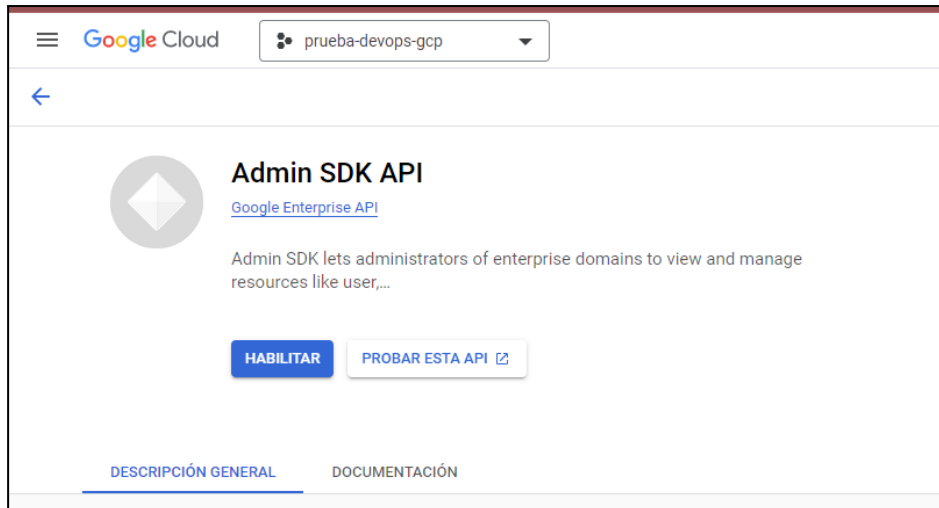
Varias API's están deshabilitadas por defecto y hay que habilitarlas en el siguiente link de la biblioteca de API's.



The screenshot shows the Google Cloud console interface for configuring API permissions. On the left, a sidebar lists 'API y servicios' with options like 'API y servicios habilitados', 'Biblioteca', 'Credenciales', 'Pantalla de consentimiento...', 'Verificación del dominio', and 'Acuerdos de uso de páginas'. The main area is titled 'Actualizar los permisos seleccionados' and contains a table of permissions. A message at the top states: 'Solo se muestran los permisos de las API habilitadas. Si deseas agregar un permiso faltante a esta pantalla, encuentra y habilita la API en la biblioteca de API de Google o usa el recuadro para pegar permisos que aparece a continuación. Actualiza la página para ver las API nuevas que habilites en la biblioteca.'


API	Alcance	Descripción para el usuario
<input checked="" type="checkbox"/>	.../auth/userinfo.email	See your primary Google Account email address
<input checked="" type="checkbox"/>	.../auth/userinfo.profile	See your personal info, including any personal info you've made publicly available
<input checked="" type="checkbox"/>	openid	Associate you with your personal info on Google
<input type="checkbox"/>	BinQuery API	View and manage your data in Google BinQuery

Se habilitan las siguientes API:



Google Cloud prueba-devops-gcp

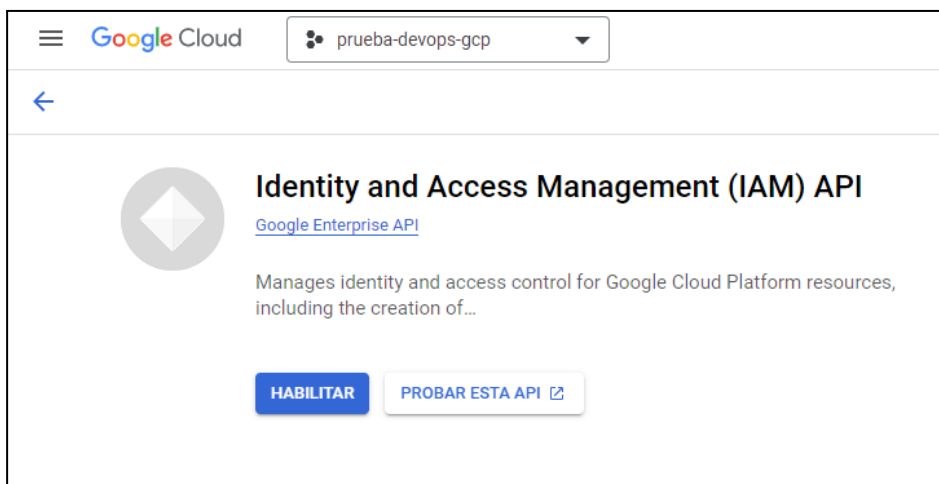
←

 **Admin SDK API**
[Google Enterprise API](#)

Admin SDK lets administrators of enterprise domains to view and manage resources like user,...


HABILITAR [PROBAR ESTA API ↗](#)

[DESCRIPCIÓN GENERAL](#) [DOCUMENTACIÓN](#)



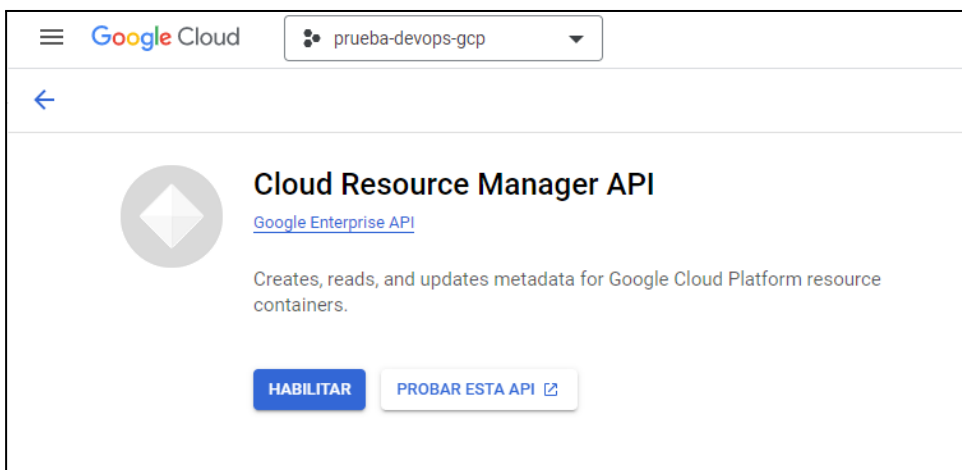
Google Cloud prueba-devops-gcp

←

 **Identity and Access Management (IAM) API**
[Google Enterprise API](#)


Manages identity and access control for Google Cloud Platform resources, including the creation of...

HABILITAR [PROBAR ESTA API ↗](#)



Google Cloud prueba-devops-gcp

←

 **Cloud Resource Manager API**
[Google Enterprise API](#)

Creates, reads, and updates metadata for Google Cloud Platform resource containers.

HABILITAR [PROBAR ESTA API ↗](#)

Una vez habilitados, en la pantalla de permisos, se añaden los siguientes.

API APIs y servicios
Editar el registro de la app

- API y servicios habilitados
- Biblioteca
- Credenciales
- Pantalla de consentimiento ...
- Verificación del dominio
- Acuerdos de uso de páginas

Tus permisos no sensibles

API ↑	Alcance	Descripción para el usuario	
...	./auth/userinfo.email	See your primary Google Account email address	🗑️
...	./auth/userinfo.profile	See your personal info, including any personal info you've made publicly available	🗑️
openid		Associate you with your personal info on Google	🗑️

Tus permisos sensibles

Los permisos sensibles se usan para solicitar acceso a los datos privados del usuario.

API ↑	Alcance	Descripción para el	
Admin SDK API	.../auth/admin.directory.user.alias.readonly	Permite ver los alias de usuario de tu dominio.	🗑️
Admin SDK API	.../auth/admin.directory.customer.readonly	Ver información relacionada con los clientes.	🗑️
Admin SDK API	.../auth/admin.directory.domain.readonly	Permite ver dominios relacionados con tu dominio.	🗑️
Admin SDK API	.../auth/admin.directory.group.readonly	Permite visualizar grupos en tu dominio.	🗑️
Admin SDK API	.../auth/admin.directory.group.member.readonly	Permite ver las suscripciones de grupo en tu dominio.	🗑️
Admin SDK API	.../auth/admin.directory.orgunit.readonly	Ver las unidades de organización de tu dominio.	🗑️
BigQuery API	.../auth/cloud-platform.readonly	Ver tus datos en los servicios de Google, como la dirección de correo electrónico de tu Cuenta de Google.	🗑️
Cloud Resource Manager API	./auth/cloudplatformprojects.readonly	View your Cloud Platform projects.	🗑️
Identity and Access Management (IAM) API	.../auth/iam	Permite gestionar políticas de administración de identidades y acceso.	🗑️

2. Crear ID de cliente OAuth

Google Cloud
prueba-devops-gcp
Buscar recursos, documentos, pro...

- API APIs y servicios
- API y servicios habilitados
- Biblioteca
- Credenciales
- Pantalla de consentimiento ...
- Verificación del dominio
- Acuerdos de uso de páginas

Credenciales
+ CREAR CREDENCIALES
🗑️ BORRAR

Clave de API

Identifica tu proyecto con una clave de API simple para verificar la cuota y el acceso

ID de cliente de OAuth

Solicita el consentimiento del usuario para que tu app pueda acceder a sus datos

Cuenta de servicio

Habilita la autenticación de servidor a servidor en el nivel de la app mediante cuentas robot

Ayúdame a elegir

Responde algunas preguntas para decidir qué tipo de credencial usar

Tipo de aplicación *
Aplicación web

Nombre *
Prueba-web

El nombre de tu cliente de OAuth 2.0. Este nombre solo se usa para identificar al cliente en la consola y no se mostrará a los usuarios finales.

Los dominios de los URI que agregues a continuación se incorporarán automáticamente a tu [pantalla de consentimiento de OAuth](#) como [dominios autorizados](#).

Orígenes autorizados de JavaScript

Para usar con solicitudes de un navegador

+ AGREGAR URI

URI de redireccionamiento autorizados

Para usar con solicitudes de un servidor web

URI 1 *
https://qa44.anjanadata.org/anjana/authorized

URI 2 *
https://qa44.anjanadata.org/admin/authorized

URI 3 *
https://qa44.anjanadata.org/anjana/login

URI 4 *
https://qa44.anjanadata.org/admin/login

+ AGREGAR URI

Nota: La configuración puede tardar entre 5 minutos y algunas horas en aplicarse

CREAR CANCELAR

Se copia y pega y se guarda el JSON de las credenciales.

Se creó el cliente de OAuth

Puedes acceder al ID de cliente y el secreto desde "Credenciales" en API y servicios

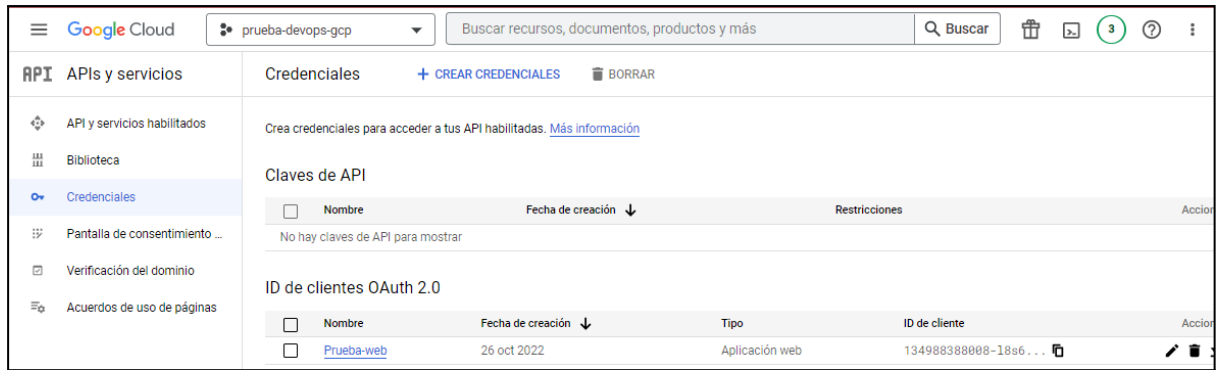
El acceso OAuth está restringido a los usuarios de tu organización, a menos que se publique y verifique la [pantalla de consentimiento de OAuth](#)

Tu ID de cliente

Tu secreto del cliente

DESCARGAR JSON

ACEPTAR

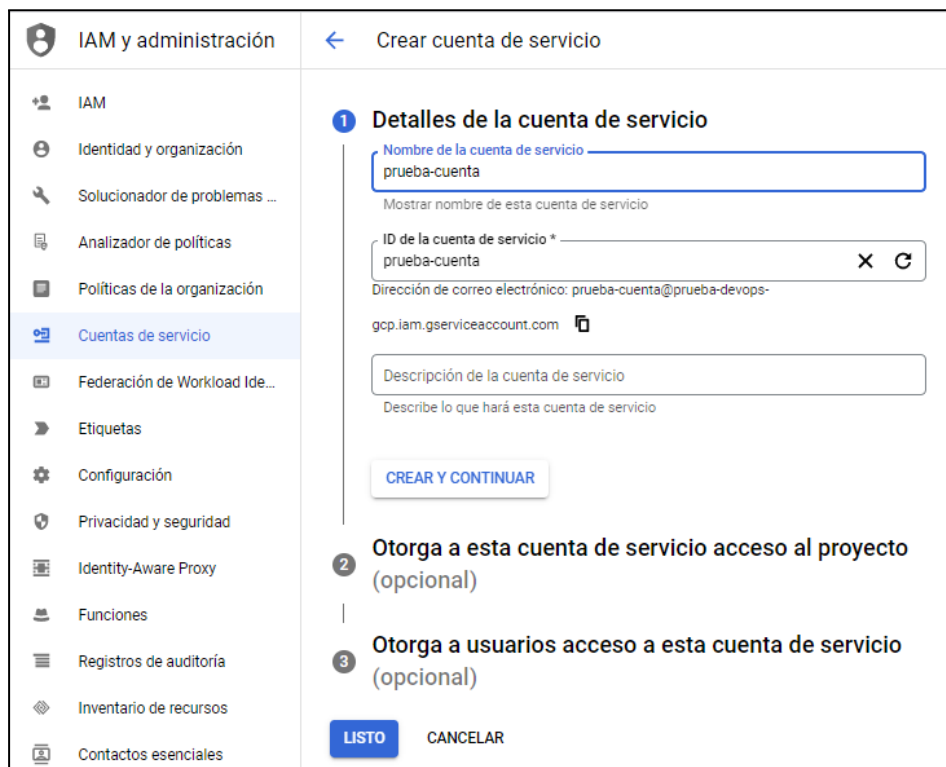


The screenshot shows the Google Cloud console interface for the project 'prueba-devops-gcp'. The left sidebar is under 'APIs y servicios' with 'Credenciales' selected. The main content area shows 'Credenciales' with a '+ CREAR CREDENCIALES' button and a 'BORRAR' button. Below this, there is a section for 'Claves de API' which is currently empty, and a section for 'ID de clientes OAuth 2.0' containing one entry: 'Prueba-web' created on 26 oct 2022, of type 'Aplicación web' with client ID '134988388008-18s6...'. The top navigation bar includes the Google Cloud logo, the project name, a search bar, and notification icons.

3. Crear la cuenta de servicio



The screenshot shows the Google Cloud console interface for the project 'prueba-devops-gcp' under the 'IAM y administración' section. The 'Cuentas de servicio' page is active, featuring a '+ CREAR CUENTA DE SERVICIO' button in yellow. The page includes a description of service accounts and a table with columns: 'Correo electrónico', 'Estado', 'Nombre', 'Descripción', 'ID de clave', 'Fecha de creación de la clave', and 'ID de cliente de OAuth'. The table is currently empty. The left sidebar shows 'Cuentas de servicio' selected under 'IAM y administración'.



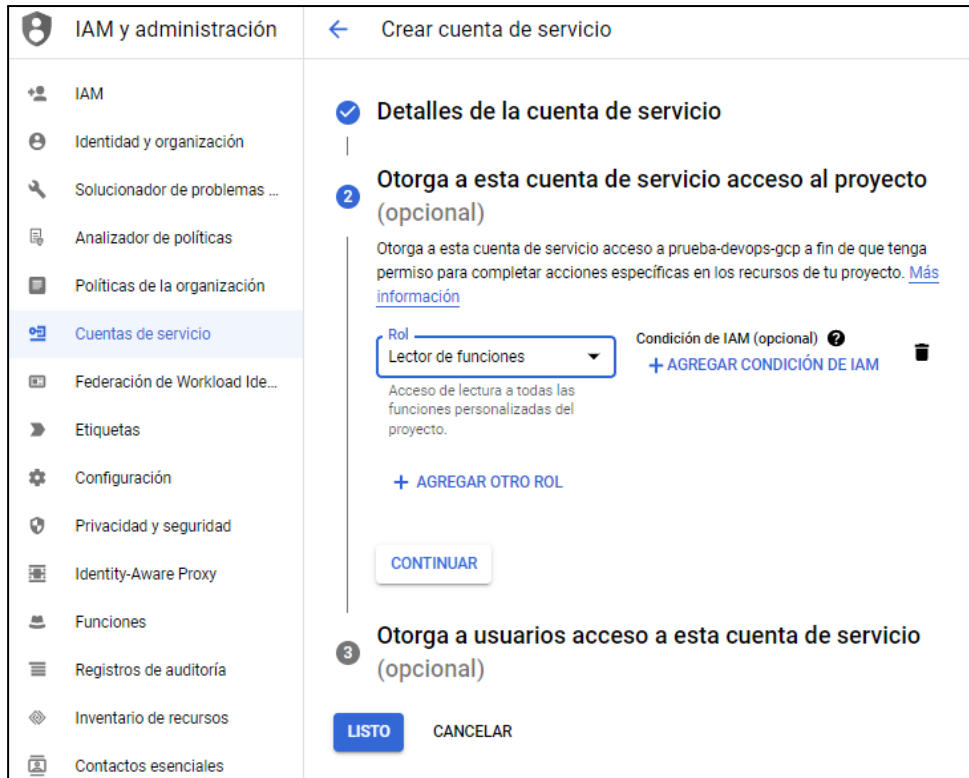
The screenshot shows the 'Crear cuenta de servicio' form in the Google Cloud console. The form is titled '1 Detalles de la cuenta de servicio' and contains the following fields:

- Nombre de la cuenta de servicio:** 'prueba-cuenta'
- ID de la cuenta de servicio *:** 'prueba-cuenta'
- Dirección de correo electrónico:** 'prueba-cuenta@prueba-devops-gcp.iam.gserviceaccount.com'
- Descripción de la cuenta de servicio:** (empty)

 Below the form is a 'CREAR Y CONTINUAR' button. The next steps are:

- Otorga a esta cuenta de servicio acceso al proyecto (opcional)
- Otorga a usuarios acceso a esta cuenta de servicio (opcional)

 At the bottom, there are 'LISTO' and 'CANCELAR' buttons. The left sidebar shows 'Cuentas de servicio' selected under 'IAM y administración'.



Crear cuenta de servicio

1 **Detalles de la cuenta de servicio**

2 **Otorga a esta cuenta de servicio acceso al proyecto (opcional)**

Otorga a esta cuenta de servicio acceso a prueba-devops-gcp a fin de que tenga permiso para completar acciones específicas en los recursos de tu proyecto. [Más información](#)

Rol: **Lector de funciones** Condición de IAM (opcional) **+ AGREGAR CONDICIÓN DE IAM**

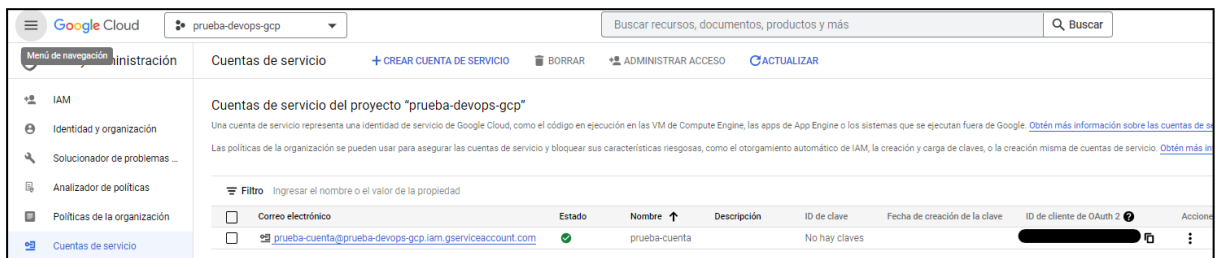
Acceso de lectura a todas las funciones personalizadas del proyecto.

+ AGREGAR OTRO ROL

CONTINUAR

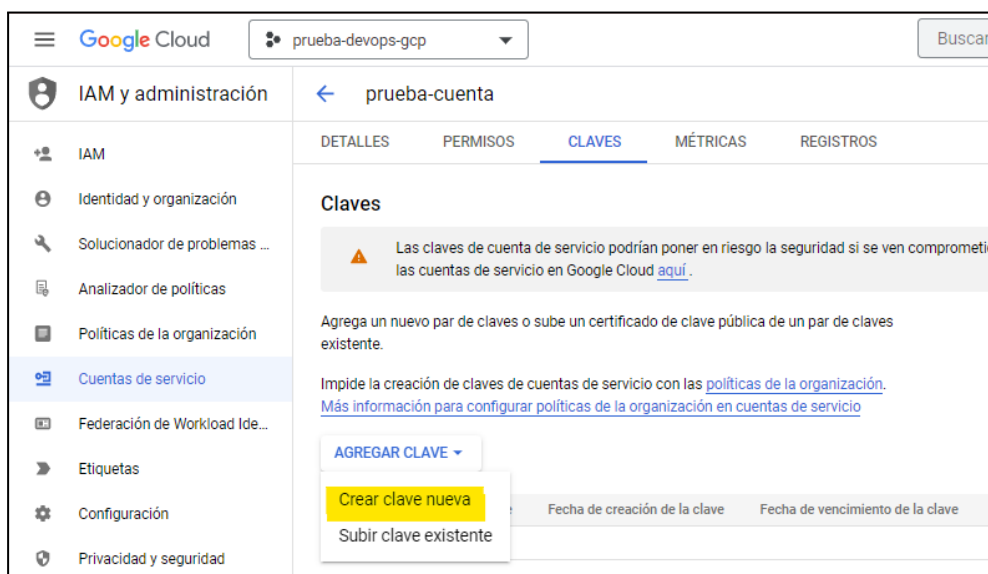
3 **Otorga a usuarios acceso a esta cuenta de servicio (opcional)**

LISTO CANCELAR



Correo electrónico	Estado	Nombre	Descripción	ID de clave	Fecha de creación de la clave	ID de cliente de OAuth 2	Acciones
<input type="checkbox"/> prueba-cuenta@prueba-devops-gcp.iam.gserviceaccount.com	OK	prueba-cuenta		No hay claves			

Hay que crear una clave de la cuenta de servicio



Google Cloud prueba-devops-gcp

prueba-cuenta

DETALLES PERMISOS **CLAVES** MÉTRICAS REGISTROS

Claves

⚠ Las claves de cuenta de servicio podrían poner en riesgo la seguridad si se ven comprometidas. [Las cuentas de servicio en Google Cloud aquí.](#)

Agrega un nuevo par de claves o sube un certificado de clave pública de un par de claves existente.

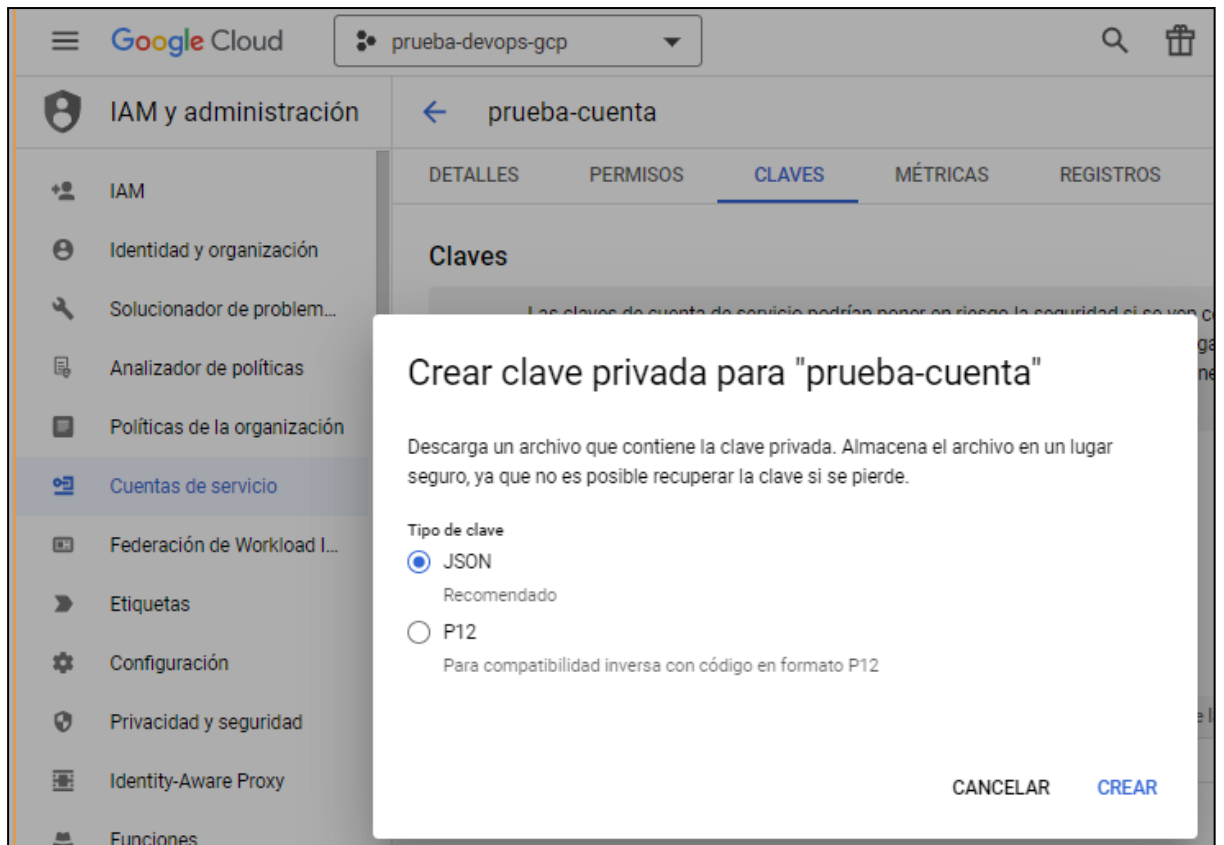
Impide la creación de claves de cuentas de servicio con las [políticas de la organización](#). [Más información para configurar políticas de la organización en cuentas de servicio](#)

AGREGAR CLAVE

Crear clave nueva

Subir clave existente

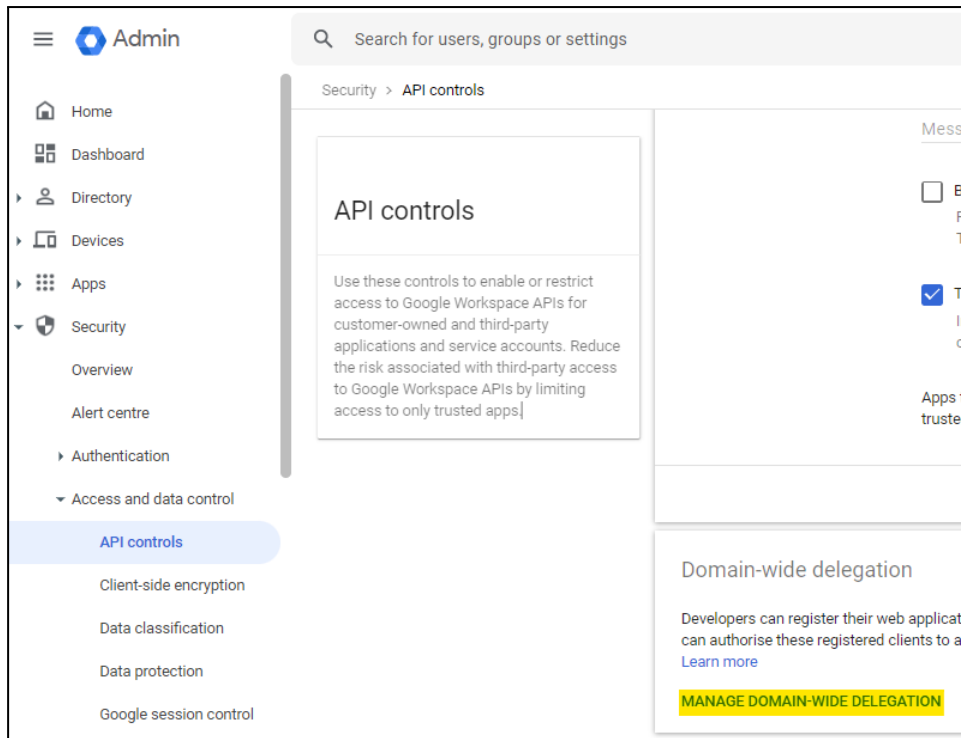
Fecha de creación de la clave Fecha de vencimiento de la clave



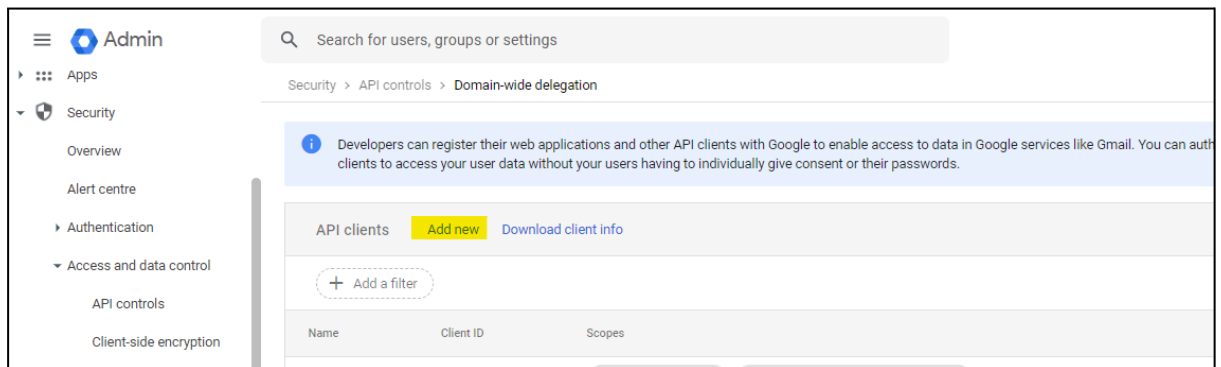
Se descargará un archivo JSON

4. Registrar la cuenta de servicio

En Gsuite->seguridad->Control de accesos->Control de API registrar la cuenta de servicio y dar permisos en los scopes necesarios:



Una vez dentro, hay que añadir un API client nuevo



Una vez en el menú, se añade el client ID de la cuenta de servicio que se ha creado anteriormente, y se añaden los siguientes scopes:

Admin

Search for users, groups or settings

Security > API controls > Domain-wide delegation

Developers can register their web applications and other API clients with Google to enable access to these registered clients

API clients [Add new](#)

+ Add a filter

Name	Client ID
Auth-prueba	104390216870416224641
anjanadata	105380302
anjanadata	117127555
anjanadata	114573386

Add a new client ID

Client ID

104390216870416224641

Overwrite existing client ID ?

OAuth scopes (comma-delimited) ×

<https://www.googleapis.com/auth/cloud-platform>

OAuth scopes (comma-delimited) ×

<https://www.googleapis.com/auth/admin.directory.>

CANCEL [AUTHORISE](#)

✕ Auth-prueba

Client ID

104390216870416224641

Scopes

<https://www.googleapis.com/auth/cloud-platform>

<https://www.googleapis.com/auth/admin.directory.orgunit.readonly>

<https://www.googleapis.com/auth/admin.directory.domain.readonly>

<https://www.googleapis.com/auth/admin.directory.user.readonly>

<https://www.googleapis.com/auth/admin.directory.group.readonly>

<https://www.googleapis.com/auth/admin.directory.group.member.readonly>

<https://www.googleapis.com/auth/admin.directory.rolemanagement.readonly>

[EDIT](#)

Asignación de roles en GCP y Gsuite

En el cloud de Google podemos dar membresías a roles de dos maneras distintas:

- Funciones de GCP
- Grupo en Gsuite

Funciones en GCP

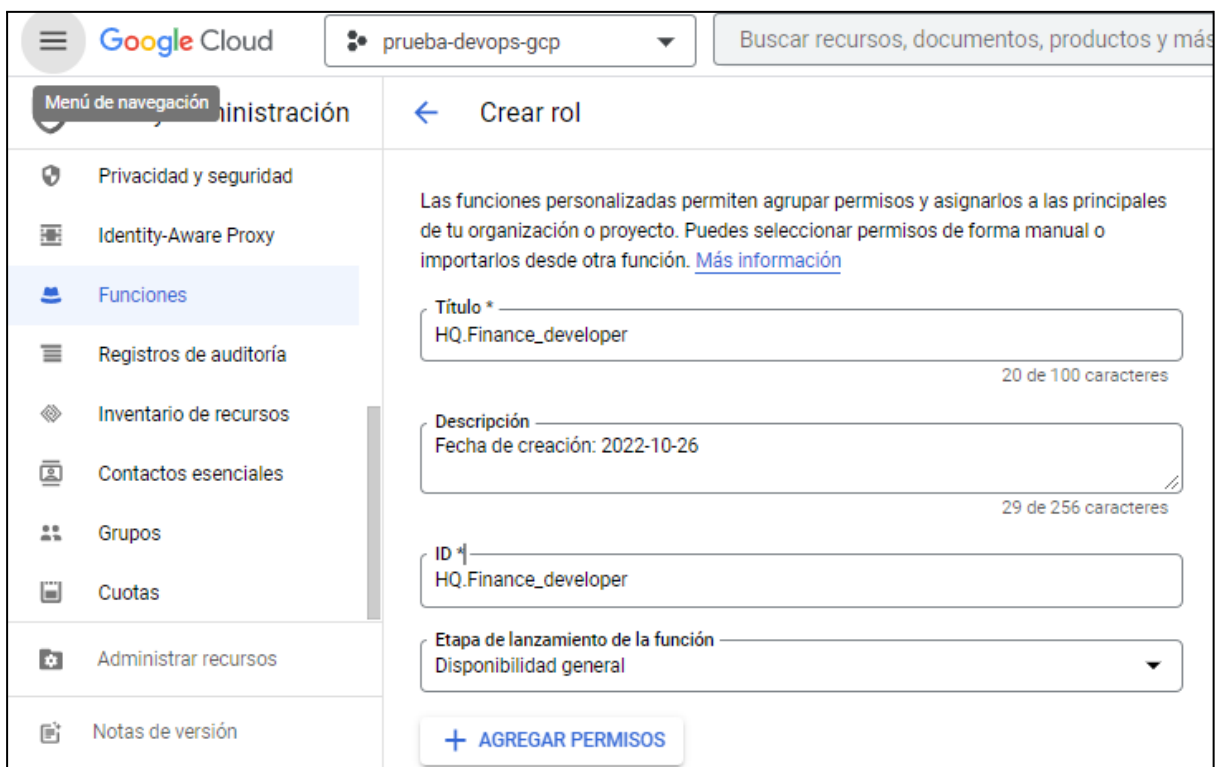
A diferencia de los grupos de Gsuite, este no genera ninguna cuenta de correo electrónico nuevo y se gestiona a través de GCP.

El procedimiento es el siguiente:

1. Se crea una función custom con la etapa "Disponibilidad general", hay que recordar que al valor que se tomará como referencia es el ID y no el nombre



The screenshot shows the Google Cloud IAM console for project 'prueba-devops-gcp'. The left sidebar contains navigation options: IAM y administración, Configuración, Privacidad y seguridad, Identity-Aware Proxy, Funciones (selected), Registros de auditoría, and Inventario de recursos. The main content area is titled 'Funciones del proyecto "prueba-devops-gcp"'. It includes a '+ CREAR FUNCIÓN' button and a description: 'Una función es un grupo de permisos que puede asignarse a las principales. Puedes crear una función y agregarle permisos, o copiar una función existente y ajustar los permisos que incluye. [Más información](#)'. Below this is a 'Filtro' input field and a table with columns 'Tipo', 'Título', and 'Se usa en'. One function is listed: 'Acceder al invalidador de aprobación' with the title 'Aprobación de acceso'.

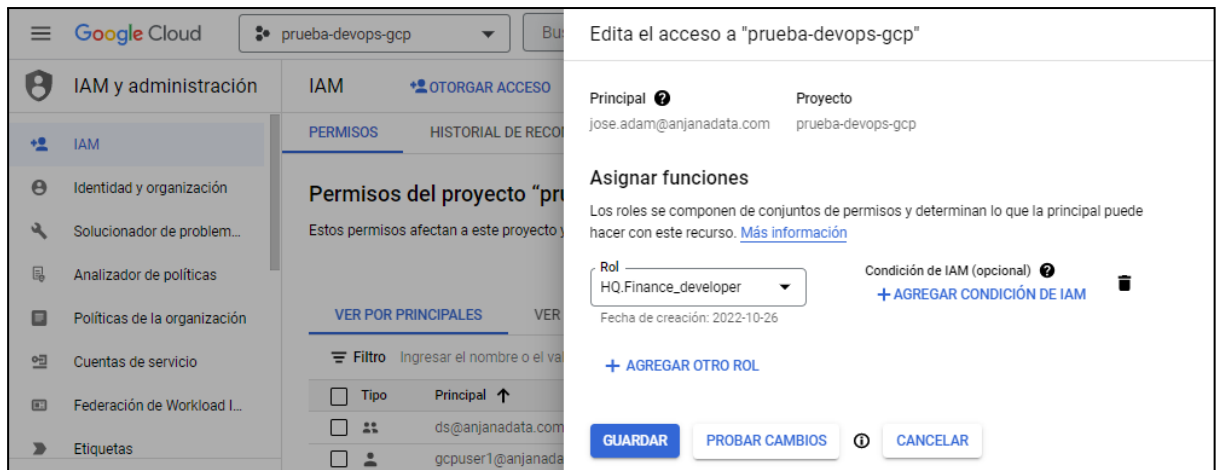


The screenshot shows the 'Crear rol' (Create role) form in the Google Cloud IAM console. The left sidebar is partially visible with 'Funciones' selected. The main content area is titled 'Crear rol' and includes the following fields:

- Título ***: HQ.Finance_developer (20 de 100 caracteres)
- Descripción**: Fecha de creación: 2022-10-26 (29 de 256 caracteres)
- ID ***: HQ.Finance_developer
- Etapa de lanzamiento de la función**: Disponibilidad general (dropdown menu)

 At the bottom of the form is a '+ AGREGAR PERMISOS' button.

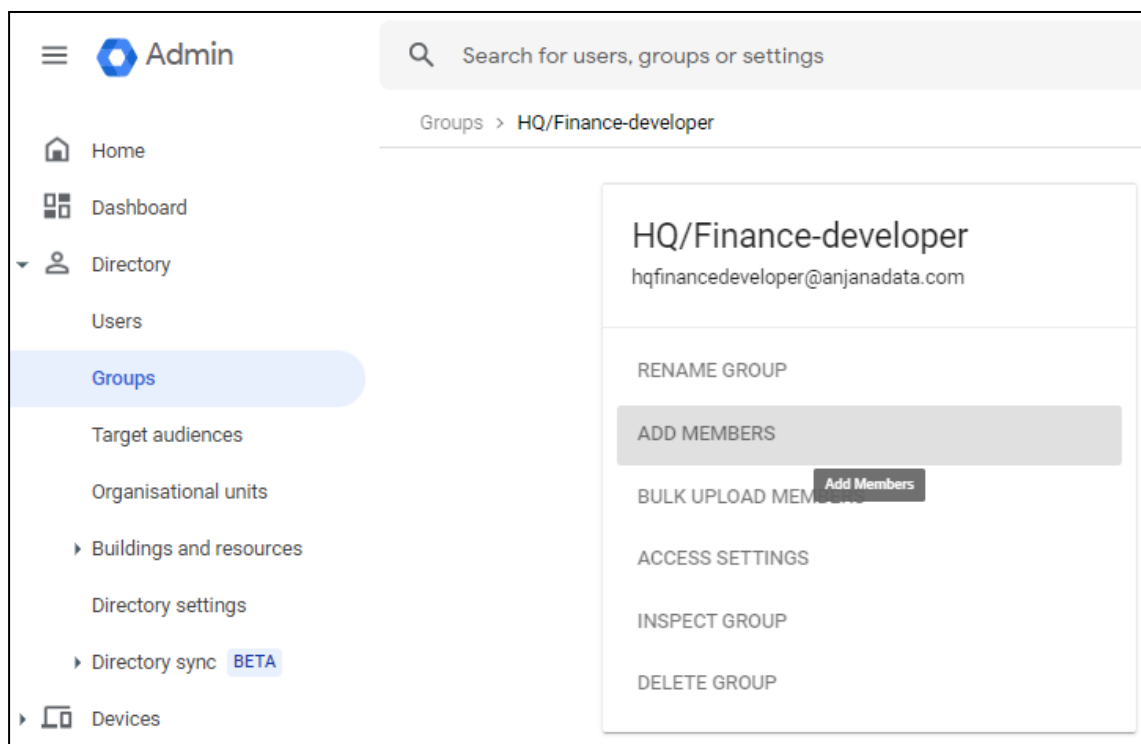
2. Se asigna la nueva función custom a un usuario en IAM



Grupos en Gsuite

Al crear un nuevo grupo en Gsuite, se genera una nueva cuenta de correo electrónico.

El procedimiento en el caso de los grupos de Gsuite es tan sencillo como crear un grupo y añadir los usuarios que quieras que obtengan esa membresía.



Gobierno activo

El plugin a desplegar el cual realizará la parte de las tareas de gobierno activo que tengan que provisionar roles custom sobre GCP es "Tot plugin GCP IAM", la credencial requerida está descrita en su documentación asociada. El resto de plugins disponibles de tecnologías integradas con GCP IAM aplicaran políticas de acceso en sus respectivas tecnologías para que dicho rol posea acceso a los recursos cubiertos por el contrato.

El plugin de gobierno activo sobre esta plataforma trabaja exclusivamente creando y asignando roles ya que tienen la suficiente funcionalidad y simplifica la administración al no generar grupos en Gsuite.

Emulación SSO vía Oauth2

El protocolo Oauth2 observa la autenticación transparente en caso de que sea posible, para lo cual solo es necesario redirigir al usuario a <https://<host>/anjana/login?provider=<identificador de provider en zeus>>, si el usuario ya está logado en dicho provider y las políticas configuradas en dicho provider hacen que no se requiera validar nuevamente la credencial, el usuario será autenticado en Anjana Data de forma totalmente transparente.