



Integración GCP

| | |
|---------------------------------------|-----------|
| Control de versiones | 2 |
| Modelo de integración | 3 |
| Autenticación y autorización (Oauth2) | 3 |
| Configuración de autenticación | 3 |
| Configuración de autorización | 3 |
| Gobierno activo | 4 |
| Nomenclatura de los grupos y UO | 4 |
| Grupos en Gsuite | 4 |
| Roles GCP | 4 |
| Credenciales requeridas | 5 |
| Autenticación y autorización (Oauth2) | 5 |
| API's necesarias | 5 |
| Provisión de credencial | 5 |
| Asignación de roles en GCP y Gsuite | 16 |
| Funciones en GCP | 16 |
| Grupos en Gsuite | 17 |
| Gobierno activo | 18 |
| Emulación SSO vía Oauth2 | 18 |

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

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

```
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: *****.com  
        client-secret: *****  
        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

```
security:  
  ...  
  authorization:  
    google-api:  
      providers:  
        google:  
          json-content: '  
            {  
              "type": "service_account",
```

```
"project_id": "AAAAAAA",
"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-aaabbccc.json # absolute path --> /xxxxxx.json
delegated: persona@dominio.com
customer: CCC000
group-org-unit-separator: "/"
role-org-unit-separator: "-"
groupPrefix: "prefix-"
```

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.

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

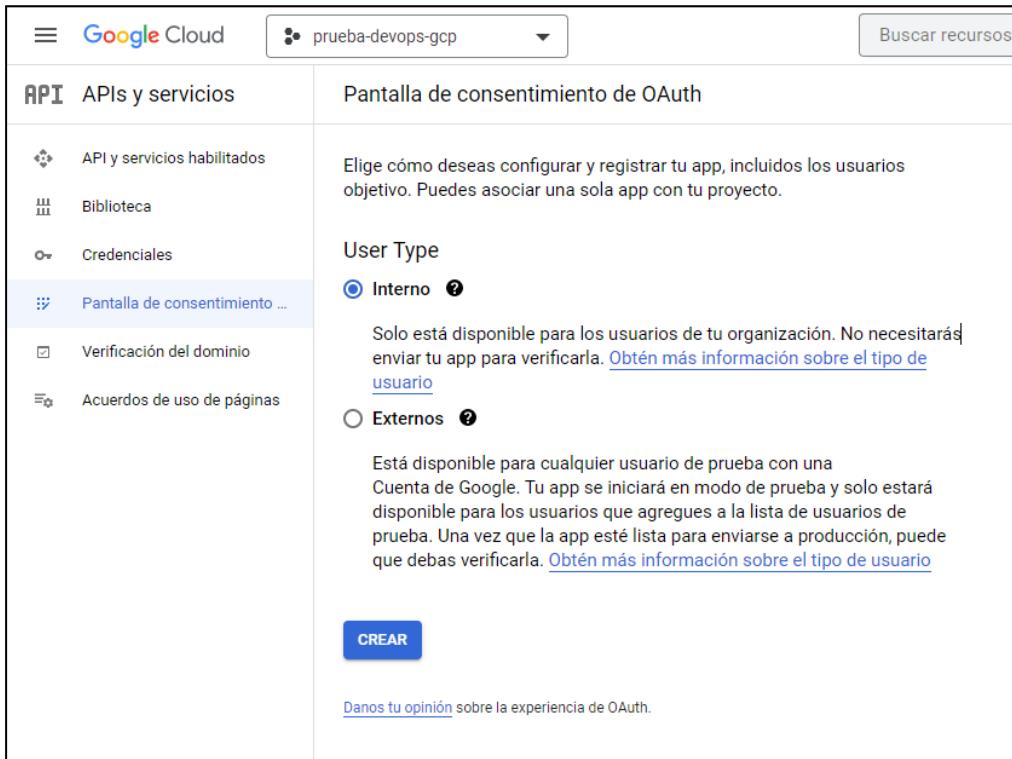
- OAuth 2.0 Client ID type web application with authorized url pointed to POC installation point (<https://<hostname>:<port>/anjana/login>) and <https://<hostname>:<port>/anjana/authorized>), default package has configured apache self signed certificate listening con 8443 port. Documentation at <https://developers.google.com/identity/protocols/oauth2/web-server>
- 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

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.

- .../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



The screenshot shows the Google Cloud Platform interface for managing APIs and services. The left sidebar lists several options: 'API y servicios habilitados' (selected), 'Biblioteca', 'Credenciales', 'Pantalla de consentimiento de OAuth' (selected), 'Verificación del dominio', and 'Acuerdos de uso de páginas'. The main content area is titled 'Pantalla de consentimiento de OAuth' and displays the configuration for this screen. It includes sections for 'User Type' where 'Interno' is selected, and 'Externos'. A note states that 'Interno' is available for organization users and 'Externos' is for testing with a Google account. A 'CREAR' button is at the bottom.

| | |
|-----------------------------|--|
| API APIs y servicios | Editar el registro de la app <input checked="" type="checkbox"/> API y servicios habilitados <input type="checkbox"/> Biblioteca <input type="checkbox"/> Credenciales <input checked="" type="checkbox"/> Pantalla de consentimiento ... <input checked="" type="checkbox"/> Verificación del dominio <input type="checkbox"/> Acuerdos de uso de páginas |
|-----------------------------|--|

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

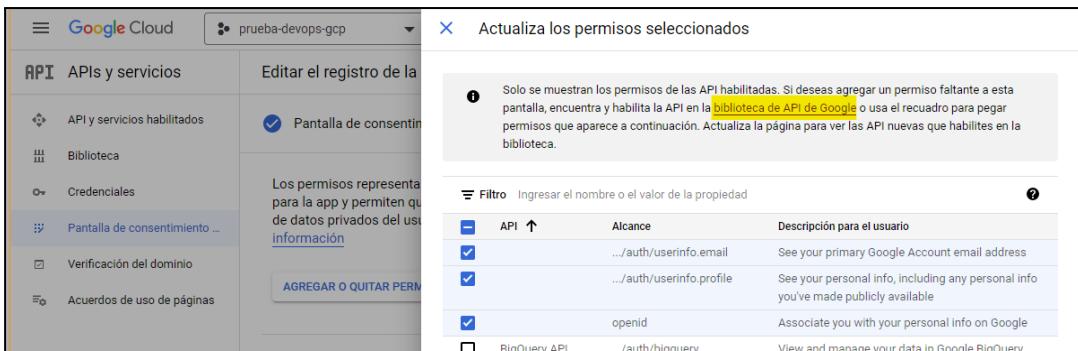
Información de contacto del desarrollador

Direcciones de correo electrónico *

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

GUARDAR Y CONTINUAR **CANCELAR**

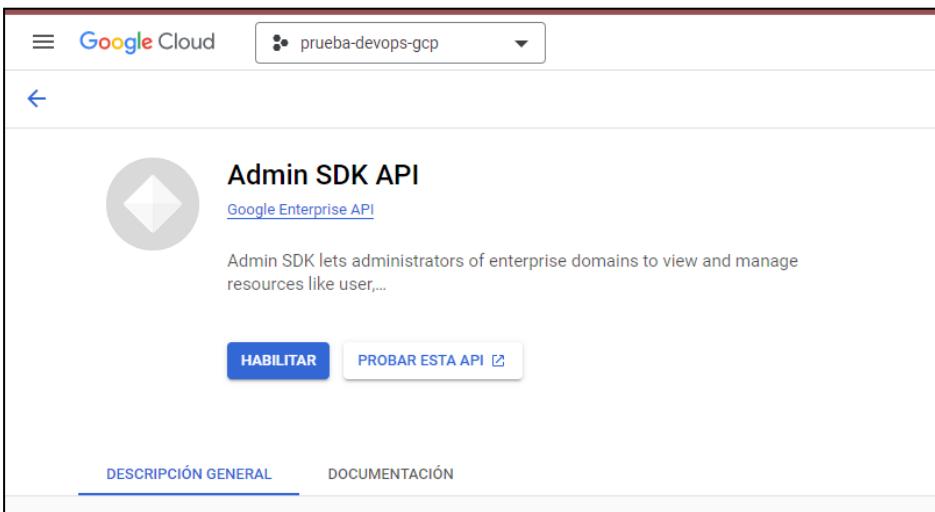
Varias API's están deshabilitadas por defecto y hay que habilitarlas en el siguiente link de la biblioteca de API's.



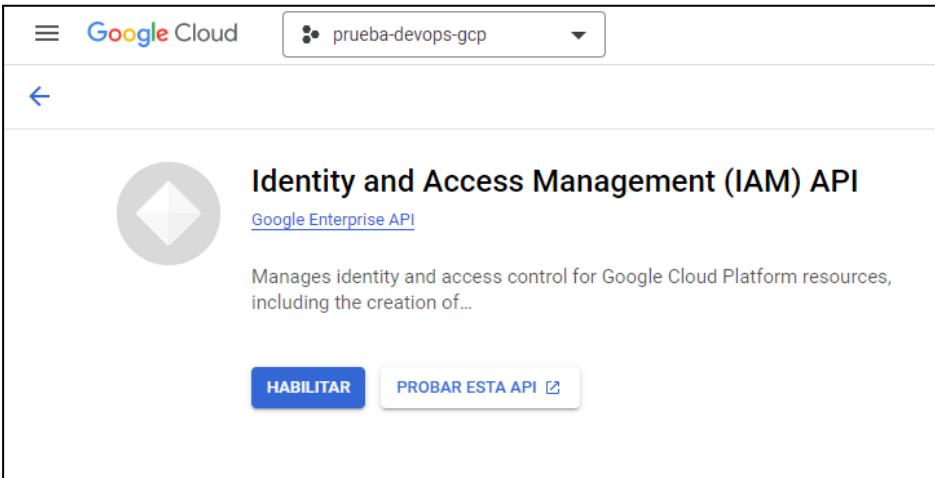
The screenshot shows the Google Cloud API library interface. On the left, there's a sidebar with options like 'APIs y servicios habilitados', 'Biblioteca', 'Credenciales', 'Pantalla de consentimiento ...', 'Verificación del dominio', and 'Acuerdos de uso de páginas'. The main area is titled 'Actualiza los permisos seleccionados' and contains a note about enabling APIs. A table lists selected permissions:

| 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"/> | /auth/biquery | View and manage your data in Google BigQuery |

Buscamos las siguientes API y las habilitamos



The screenshot shows the 'Admin SDK API' page in the Google Cloud library. It includes a brief description: 'Admin SDK lets administrators of enterprise domains to view and manage resources like user,...'. Below the description are two buttons: 'HABILITAR' (Enable) and 'PROBAR ESTA API' (Try this API). At the bottom, there are links for 'DESCRIPCIÓN GENERAL' and 'DOCUMENTACIÓN'.



The screenshot shows the 'Identity and Access Management (IAM) API' page in the Google Cloud library. It includes a brief description: 'Manages identity and access control for Google Cloud Platform resources, including the creation of...'. Below the description are two buttons: 'HABILITAR' (Enable) and 'PROBAR ESTA API' (Try this API).



The screenshot shows the Google Cloud API library interface. At the top, it says "Google Cloud" and "prueba-devops-gcp". Below that is a back arrow and the title "Cloud Resource Manager API". A circular icon with a diamond shape is next to the title. Below the title, it says "Google Enterprise API". A brief description follows: "Creates, reads, and updates metadata for Google Cloud Platform resource containers." Two buttons are at the bottom: "HABILITAR" (Enable) and "PROBAR ESTA API" (Try this API).

Una vez habilitados, en la pantalla de permisos, añadimos todos los siguientes



The screenshot shows the "Permissions" section of the Google Cloud API library. On the left, there's a sidebar with "APIs y servicios" (APIs and services) listed: "API y servicios habilitados" (Enabled APIs and services), "Biblioteca" (Library), "Credenciales" (Credentials), "Pantalla de consentimiento ..." (Consent screen), "Verificación del dominio" (Domain verification), and "Acuerdos de uso de páginas" (Page usage agreements). The "Pantalla de consentimiento ..." item is selected and highlighted in blue.

Tus permisos no sensibles

This section lists permissions for the "Cloud Resource Manager API".

| API ↑ | Alcance | Descripción para el usuario |
|--|---|--|
| Cloud Resource Manager API | .../auth/cloudplatformprojects.readonly | See your Cloud Platform projects |
| Identity and Access Management (IAM) API | .../auth/iam | Permitir gestionar políticas de administración de identidades y acceso |

Tus permisos sensibles

This section lists sensitive permissions for the "Cloud Resource Manager API".

| API ↑ | Alcance | Descripción para el usuario |
|--|--|--|
| Admin SDK API | .../auth/admin.directory.user.alias.readonly | Permitir 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 | Permitir ver dominios relacionados con tu |
| Admin SDK API | .../auth/admin.directory.group.readonly | Permitir visualizar grupos en tu dominio |
| Admin SDK API | .../auth/admin.directory.group.member.readonly | Permitir 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.read-only | Ver tus datos en los servicios de Google y ver 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 | Permitir 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 | Credenciales |
|---|---|
| <ul style="list-style-type: none"> <input checked="" type="checkbox"/> API y servicios habilitados <input type="checkbox"/> Biblioteca <input checked="" type="checkbox"/> Credenciales <input type="checkbox"/> Pantalla de consentimiento ... <input type="checkbox"/> Verificación del dominio <input type="checkbox"/> Acuerdos de uso de páginas | <p>+ CREAR CREDENCIALES BORRAR</p> <p>Clave de API Identifica tu proyecto con una clave de API simple para verificar la cuota y el acceso</p> <p>ID de cliente de OAuth Solicita el consentimiento del usuario para que tu app pueda acceder a sus datos</p> <p>Cuenta de servicio Habilita la autenticación de servidor a servidor en el nivel de la app mediante cuentas robot</p> <p>ID de clientes OAuth Ayúdame a elegir Responde algunas preguntas para decidir qué tipo de credencial usar</p> <p>Cuentas de servicio <input type="checkbox"/> Correo electrónico No hay cuentas de servicio para mostrar</p> |

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**

Copiamos y pegamos y guardamos 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

Información: 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: [Copiar](#)

Tu secreto del cliente: [Copiar](#)

[DESCARGAR JSON](#)

[ACEPTAR](#)

| API APIs y servicios | | Credenciales | + CREAR CREDENCIALES | BORRAR | |
|--|--|--|----------------------|----------------|---|
| API y servicios habilitados | | | | | |
| Biblioteca | | | | | |
| Credenciales | | | | | |
| Pantalla de consentimiento ... | | | | | |
| Verificación del dominio | | | | | |
| Acuerdos de uso de páginas | | | | | |
| | | Claves de API | | | |
| | | <input type="checkbox"/> Nombre | Fecha de creación ↓ | Restricciones | Acción |
| | | No hay claves de API para mostrar | | | |
| | | ID de clientes OAuth 2.0 | | | |
| | | <input type="checkbox"/> Nombre | Fecha de creación ↓ | Tipo | ID de cliente |
| | | <input checked="" type="checkbox"/> Prueba-web | 26 oct 2022 | Aplicación web | 134988388008-18s6... Copiar |
| | | | | | |

3. Crear la cuenta de servicio

| Google Cloud | | prueba-devops-gcp | Buscar recursos, documentos, productos y más | | | |
|---|--|--|--|----------|--------------------|-------------|
| IAM y administración | | Cuentas de servicio | + CREAR CUENTA DE SERVICIO | BORRAR | ADMINISTRAR ACCESO | ACTUALIZAR |
| IAM | | Cuentas de servicio del proyecto "prueba-devops-gcp" | | | | |
| Identidad y organización | | Una cuenta de servicio representa una identidad de servicio de Google Cloud, como el código en ejecución en las VM de Compute Engine, las apps de App Engine o los sistemas que... | | | | |
| Solucionador de problemas ... | | Las políticas de la organización se pueden usar para asegurar las cuentas de servicio y bloquear sus características riesgosas, como el otorgamiento automático de IAM, la creaci... | | | | |
| Analizador de políticas | | Filtro: Ingresar el nombre o el valor de la propiedad | | | | |
| Políticas de la organización | | <input type="checkbox"/> Correo electrónico | Estado | Nombre ↑ | Descripción | ID de clave |
| Cuentas de servicio | | No hay filas para mostrar | | | | |

IAM y administración

Crear cuenta de servicio

1 Detalles de la cuenta de servicio

Nombre de la cuenta de servicio Mostrar nombre de esta cuenta de servicio

ID de la cuenta de servicio * X C

Dirección de correo electrónico: prueba-cuenta@prueba-devops-gcp.iam.gserviceaccount.com

Descripción de la cuenta de servicio
Describe lo que hará esta cuenta de servicio

CREAR Y CONTINUAR

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

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

LISTO **CANCELAR**

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 Condición de IAM (opcional) ?

Acceso de lectura a todas las funciones personalizadas del proyecto.

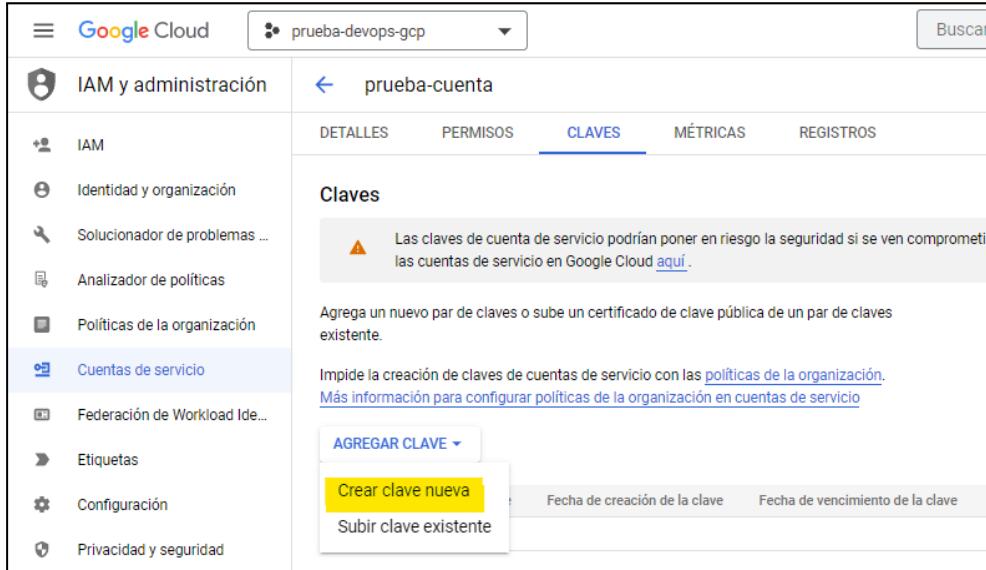
3 Otorga a usuarios acceso a esta cuenta de servicio (opcional)

LISTO **CANCELAR**

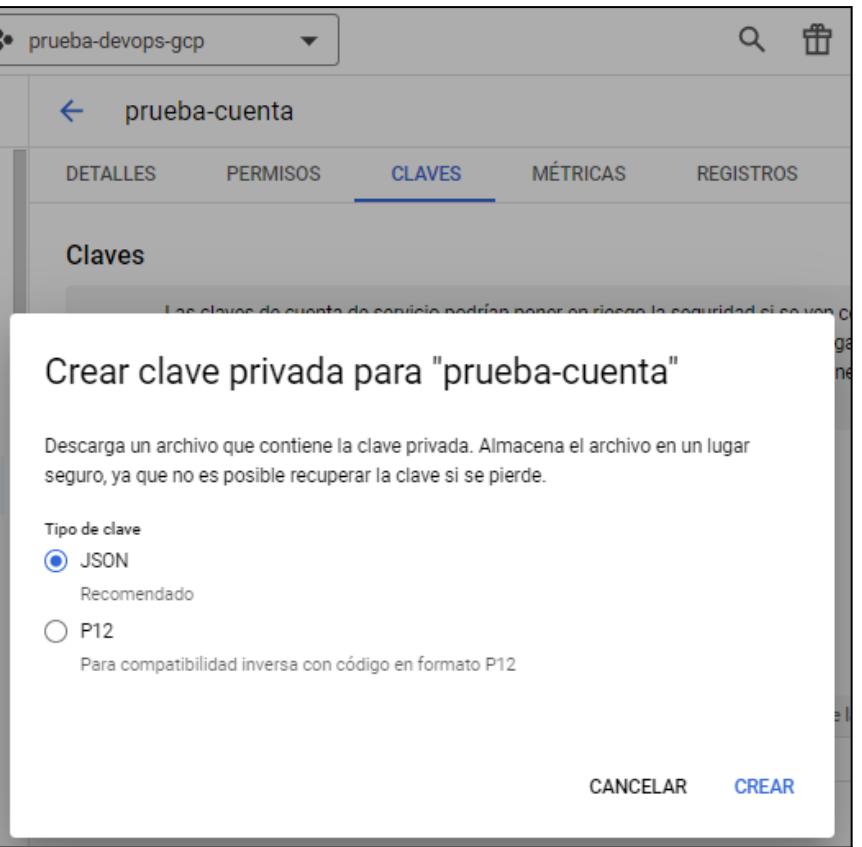


The screenshot shows the Google Cloud IAM & administration interface. The left sidebar is titled "Menú de navegación" and includes options like IAM, Identidad y organización, Solucionador de problemas, Analizador de políticas, Políticas de la organización, and Cuentas de servicio. The main area is titled "Cuentas de servicio" and shows a table with one row for "prueba-cuenta@prueba-devops-gcp.iam.gserviceaccount.com". The table columns are Estado, Nombre, Descripción, ID de clave, Fecha de creación de la clave, and ID de cliente de OAuth 2.

Tenemos que crear una clave de la cuenta de servicio



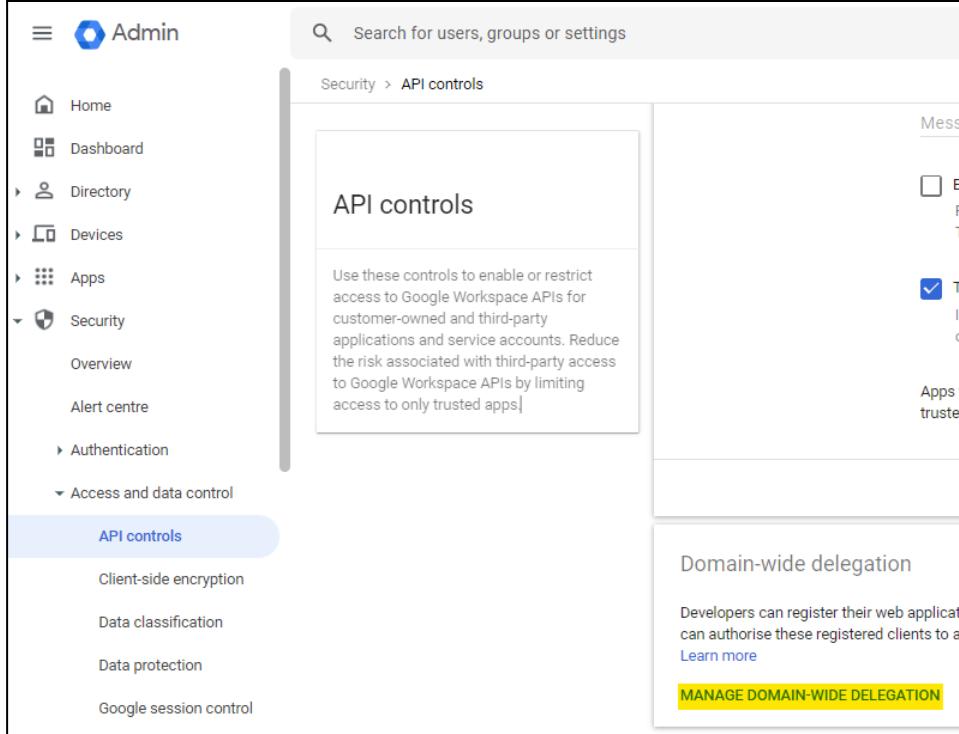
The screenshot shows the "Claves" tab in the service account details page. The left sidebar has the same navigation as the previous screenshot. The main area has tabs for DETALLES, PERMISOS, CLAVES (which is selected), MÉTRICAS, and REGISTROS. The "Claves" section contains a warning about the risks of exposing service account keys. It also has a button to "AGREGAR CLAVE" with options for "Crear clave nueva" or "Subir clave existente".



The screenshot shows a modal dialog box titled "Crear clave privada para "prueba-cuenta"". It contains instructions to download the private key file and store it securely. It offers two options for key type: "JSON" (selected) and "P12". The "JSON" option is described as "Recomendado" (Recommended). At the bottom right are "CANCELAR" and "CREAR" buttons.

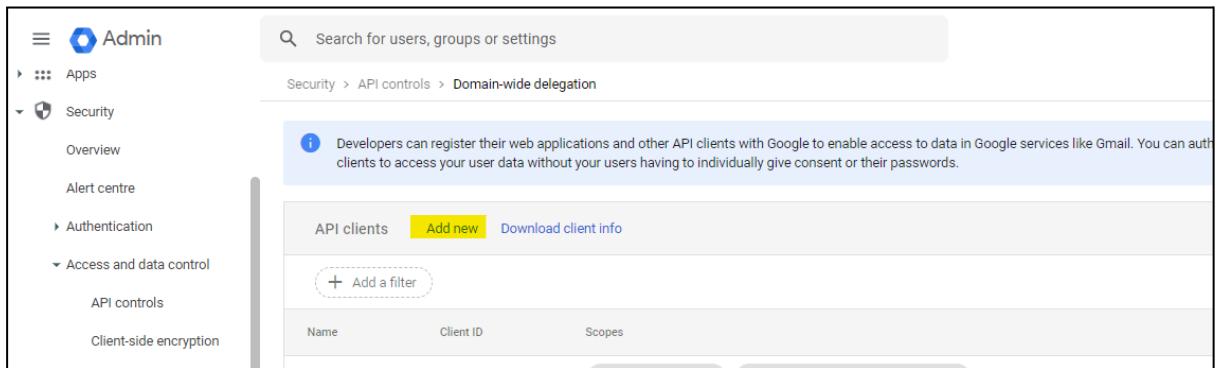
Se te descargará un archivo JSON en tu propio ordenador

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



The screenshot shows the 'API controls' section under 'Domain-wide delegation'. It includes a note about developers registering web applications to access Google services like Gmail. A yellow button labeled 'MANAGE DOMAIN-WIDE DELEGATION' is visible.

Una vez dentro, debemos de añadir un API client nuevo



The screenshot shows the 'API clients' page with a prominent yellow 'Add new' button. The left sidebar shows the navigation path: Admin > Security > API controls > Domain-wide delegation.

Una vez en el menú, añadimos el client ID de la cuenta de servicio que hemos creado anteriormente, y añadimos 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 your Google Cloud Platform resources.

Add a new client ID

| API clients | Add new |
|----------------|-----------------------|
| + Add a filter | |
| Name | Client ID |
| Auth-prueba | 104390216870416224641 |
| anjanadata | 105380302 |
| anjanadata | 117127555 |
| anjanadata | 114573386 |

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.user.readonly>

[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:

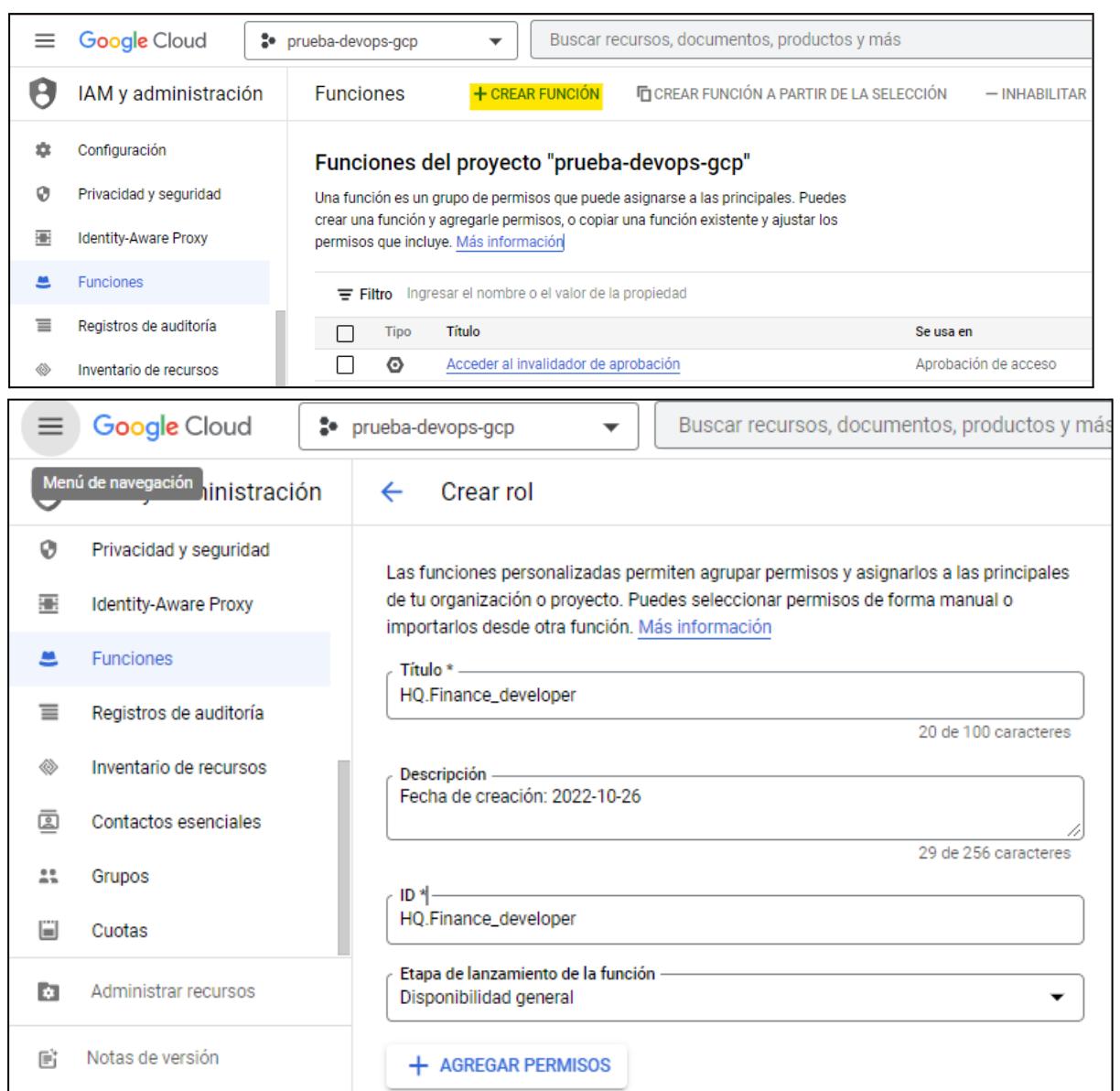
- Funciones de GCP
- Grupo en Gsuite

Funciones en GCP

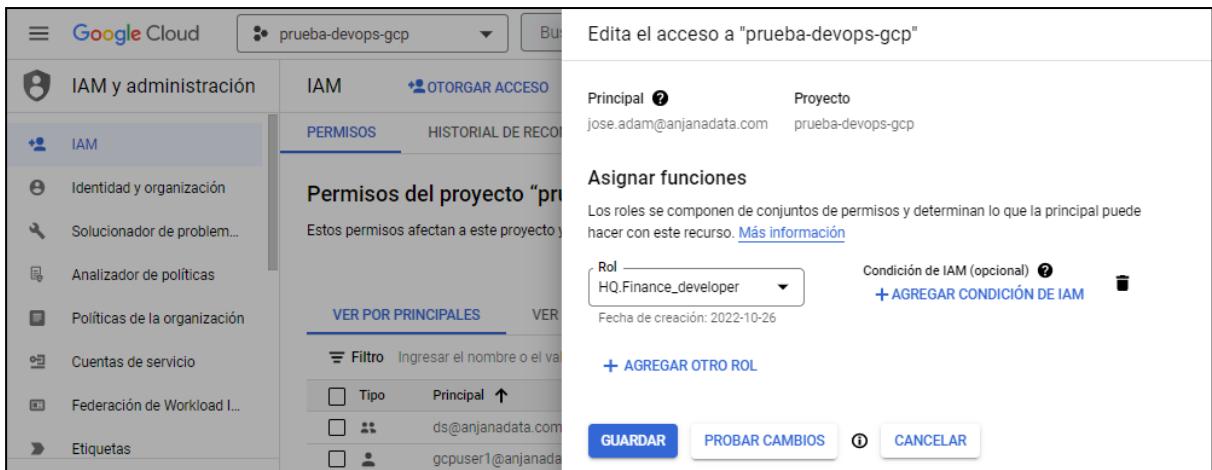
A diferencia de los grupos de Gsuite, este no genera ninguna cuenta de correo electrónico nuevo y se gestiona a través de GCP.

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



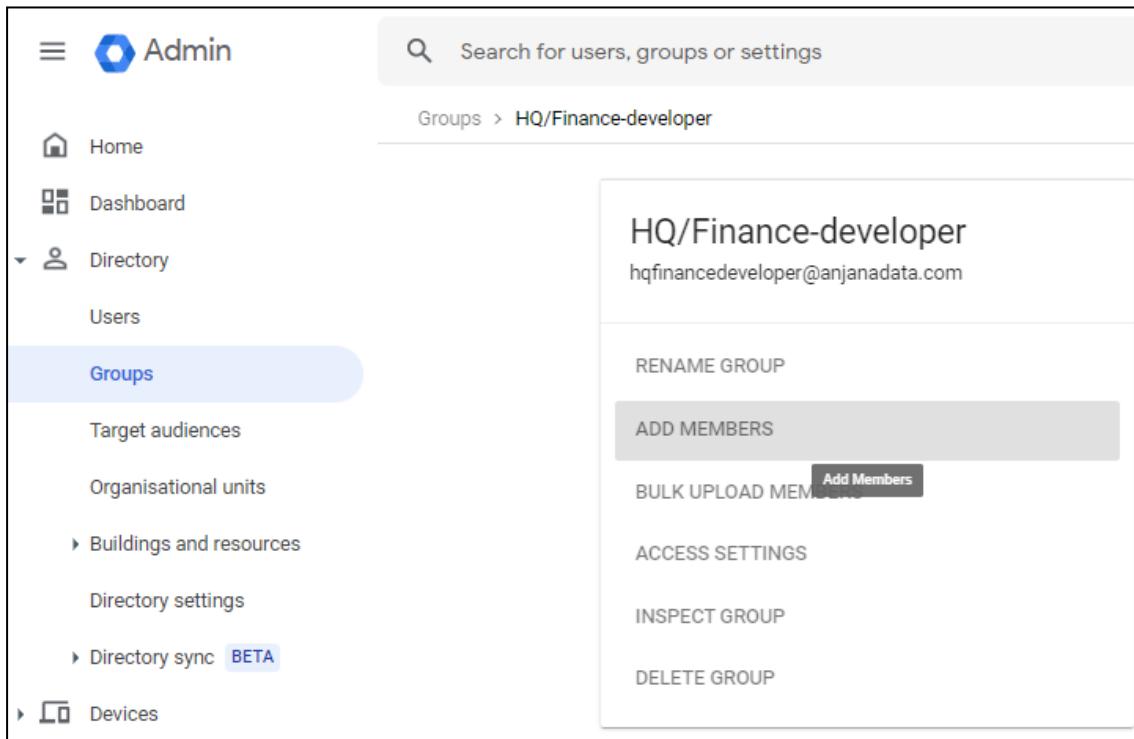
2. Se asigna la nueva función custom a un usuario en IAM



The screenshot shows the Google Cloud IAM interface for the project "prueba-devops-gcp". On the left, the navigation menu includes "IAM y administración" and "IAM". The main panel displays the "PERMISOS" tab under "Permisos del proyecto". It lists a single principal, "jose.adam@anjanadata.com", with the role "HQ.Finance_developer". A note indicates that roles are composed of permission sets and determine what the principal can do. Buttons for "GUARDAR", "PROBAR CAMBIOS", and "CANCELAR" are at the bottom.

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.



The screenshot shows the Google Workspace Admin console under the "Admin" section. The left sidebar has "Groups" selected. The main area shows a group named "HQ/Finance-developer" with the email address "hqfinancedeveloper@anjanadata.com". A sidebar on the right provides options for "RENAME GROUP", "ADD MEMBERS" (with a "BULK UPLOAD MEMBERS" button), "ACCESS SETTINGS", "INSPECT GROUP", and "DELETE GROUP".

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.