Integración GCP

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=${security.authentication.oidc.pr
oviders.google.client-id}&response_type=code&scope=${security.authentication.oidc.provid
ers.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.pr
oviders.google.client-id}&response_type=code&scope=${security.authentication.oidc.provid
ers.google.scopes}&redirect_uri=${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": "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-"
```

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 rol[1].
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-separator[2].

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

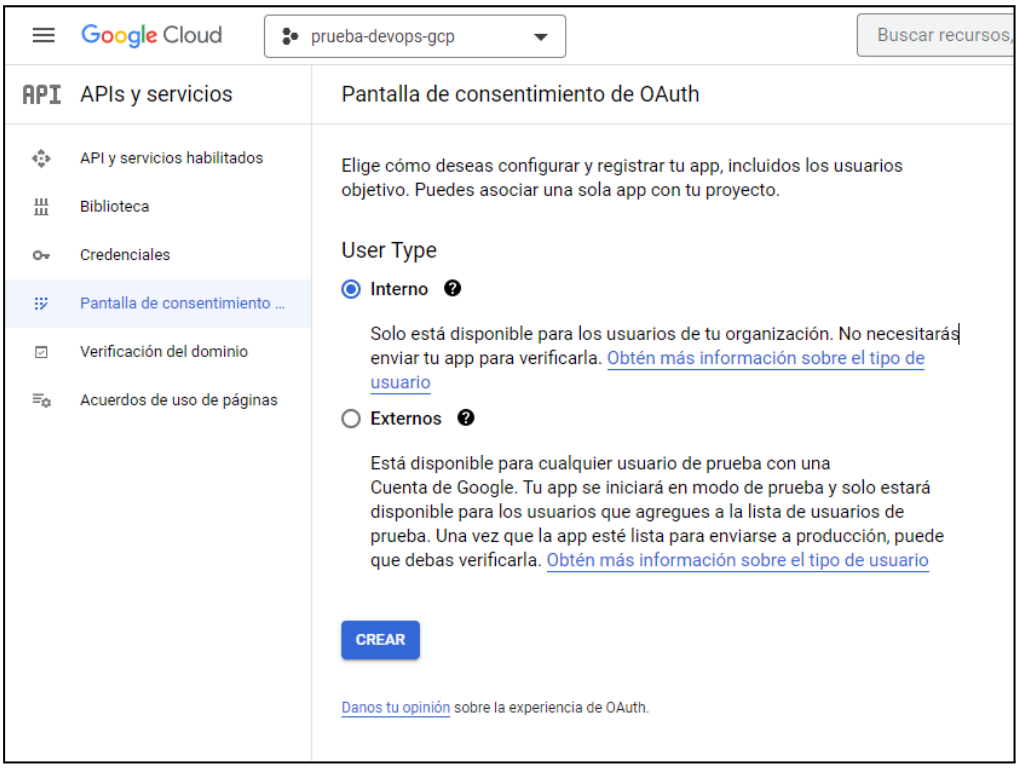
- OAuth 2.0 Client type service account with domain delegation and following permissions (DOC https://developers.google.com/admin-sdk/directory/v1/guides/delegation):
    - GCP roles (en la cuenta de servicio a usar en Zeus)
        - Role Viewer
        - Identity Platform Viewer
        - Identity 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

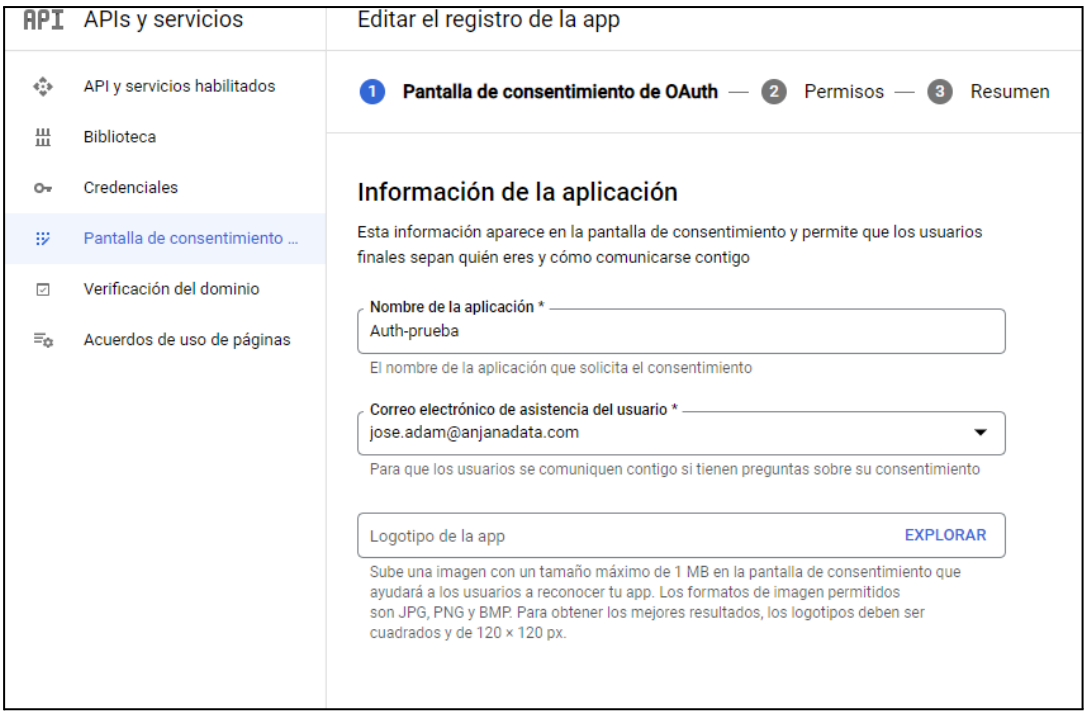
[1] Independientemente de los separadores usados en los repositorios de identidades el producto normalizará al formato estándar, por lo que en la configuración del producto ha de usarse siempre los separadores “/” y “-” para conformar el alias, por ejemplo “UO/UO…./UO-role”.
[2] Los separadores por defecto 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

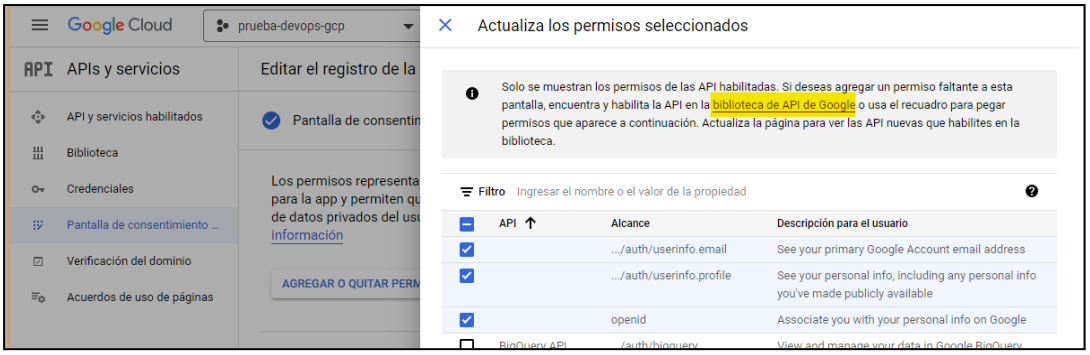
- Gsuite scopes (afecta en gsuite en el registro de la aplicación web en control de api's)
  - Openid
    - https://www.googleapis.com/auth/admin.directory.user.readonly
    - https://www.googleapis.com/auth/admin.directory.group.readonly
    - https://www.googleapis.com/auth/admin.directory.group.member.readonly
    - 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

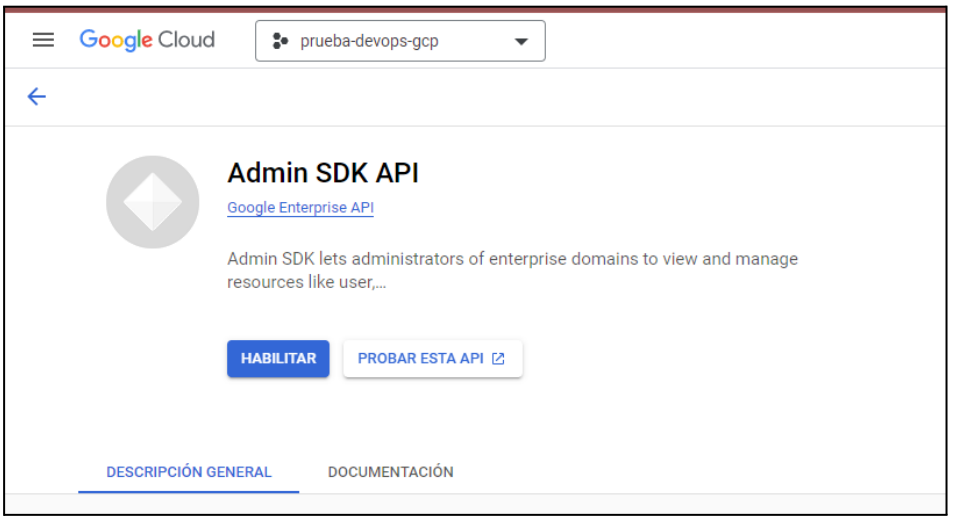


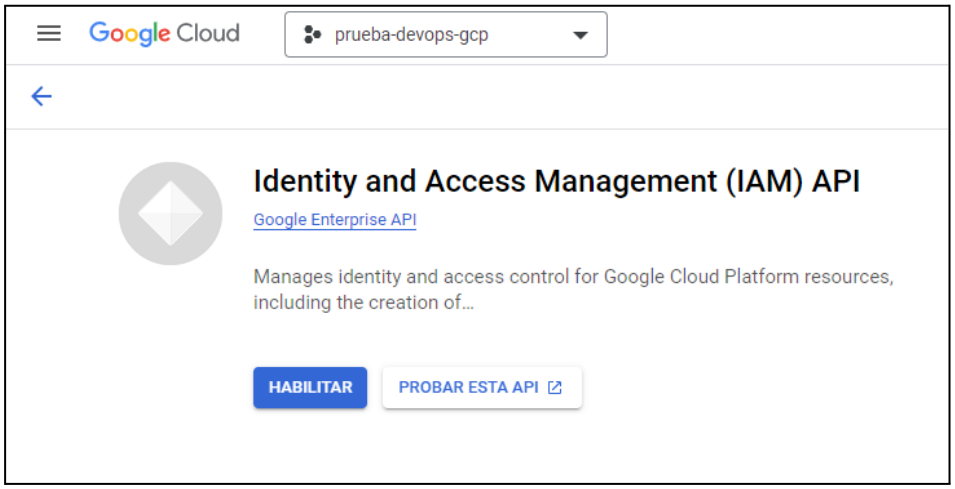


Varias API's están deshabilitadas por defecto y hay que habilitarlas en el siguiente link de la biblioteca de API's.

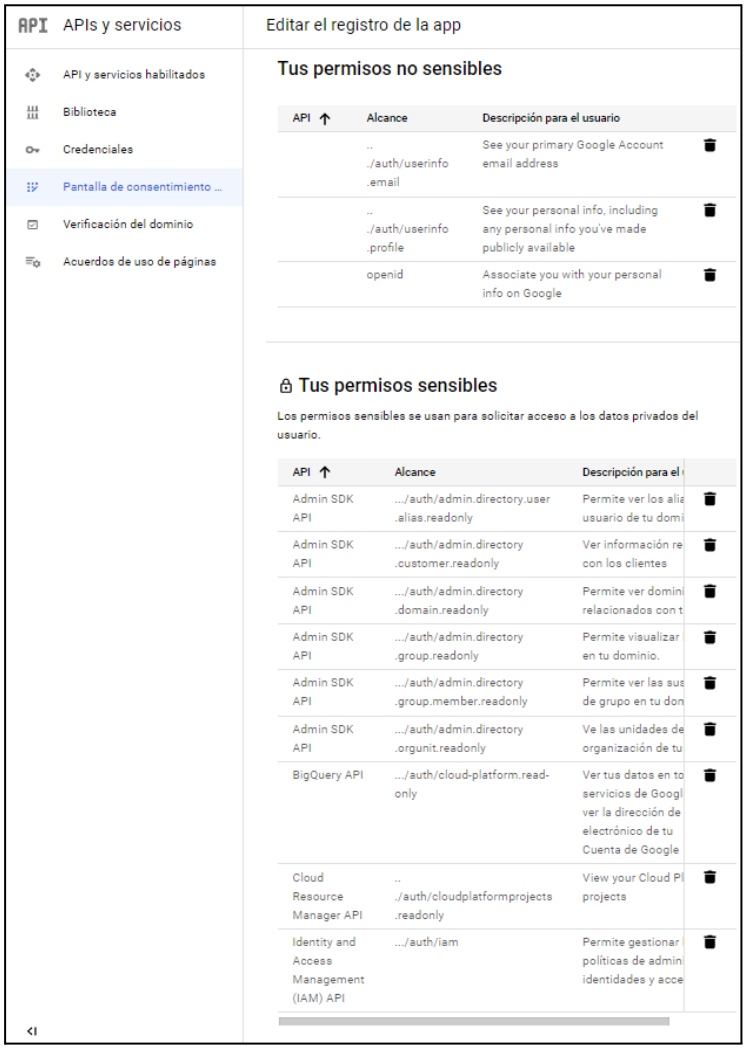


Buscamos las siguientes API y las habilitamos

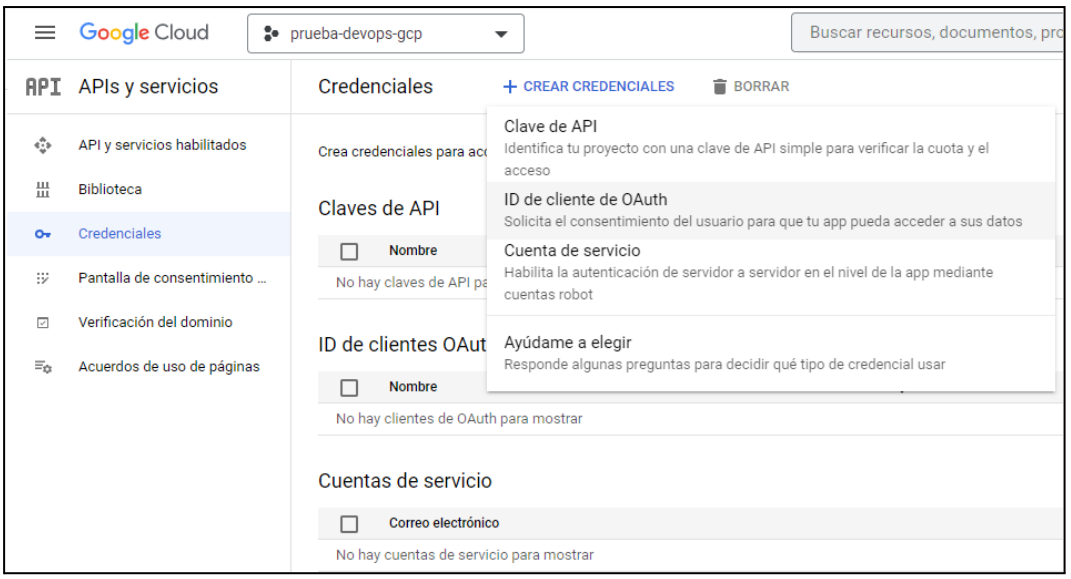


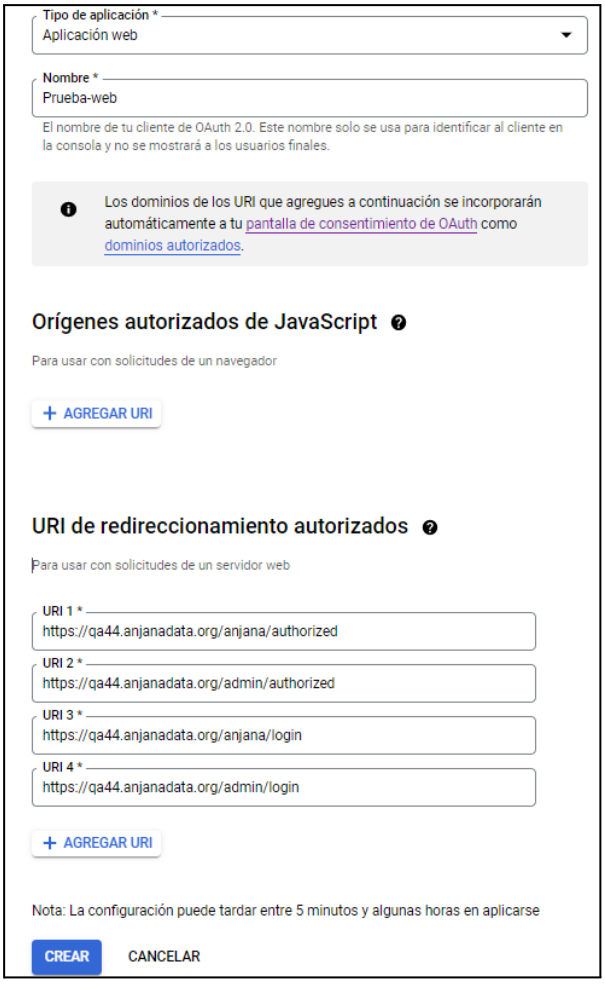


Una vez habilitados, en la pantalla de permisos, añadimos todos los siguientes

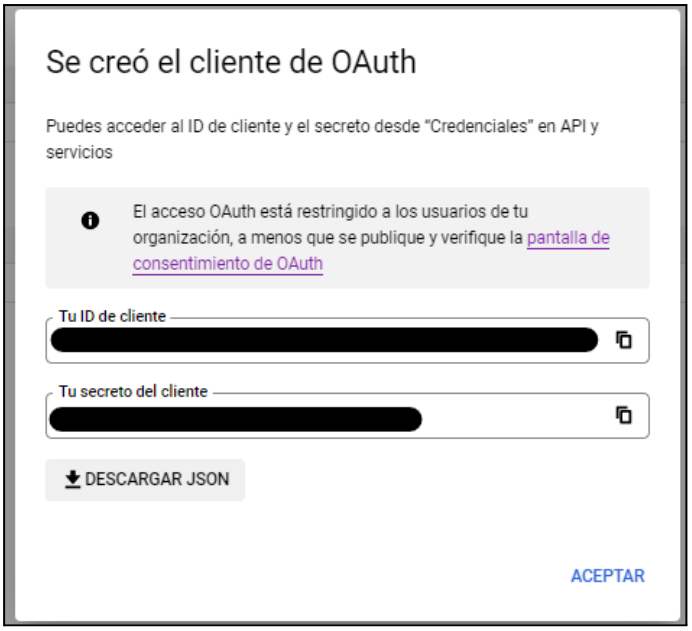


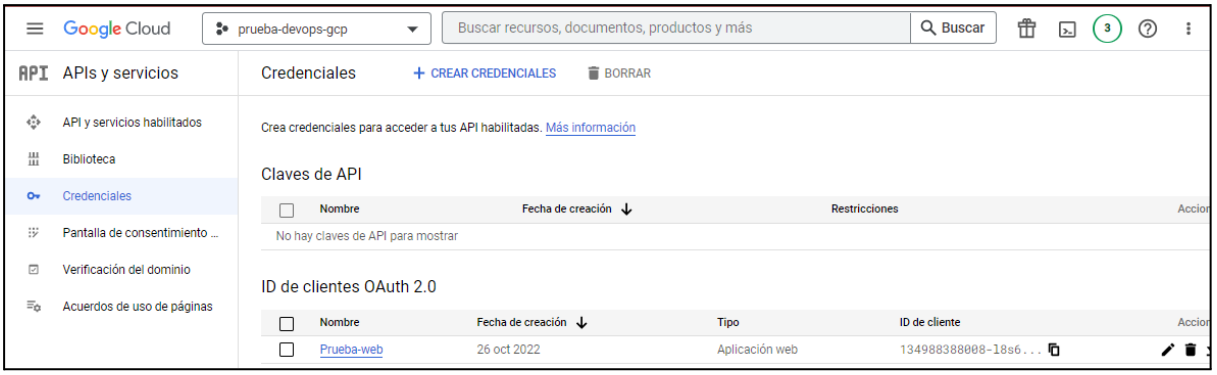
2. Crear ID de cliente OAuth



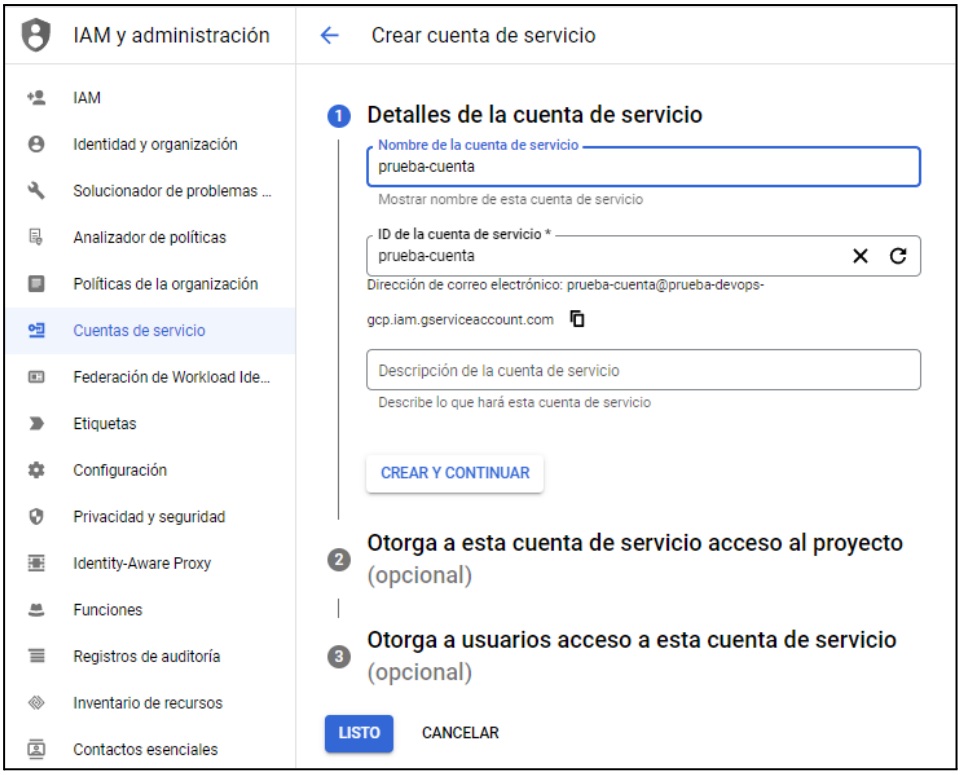


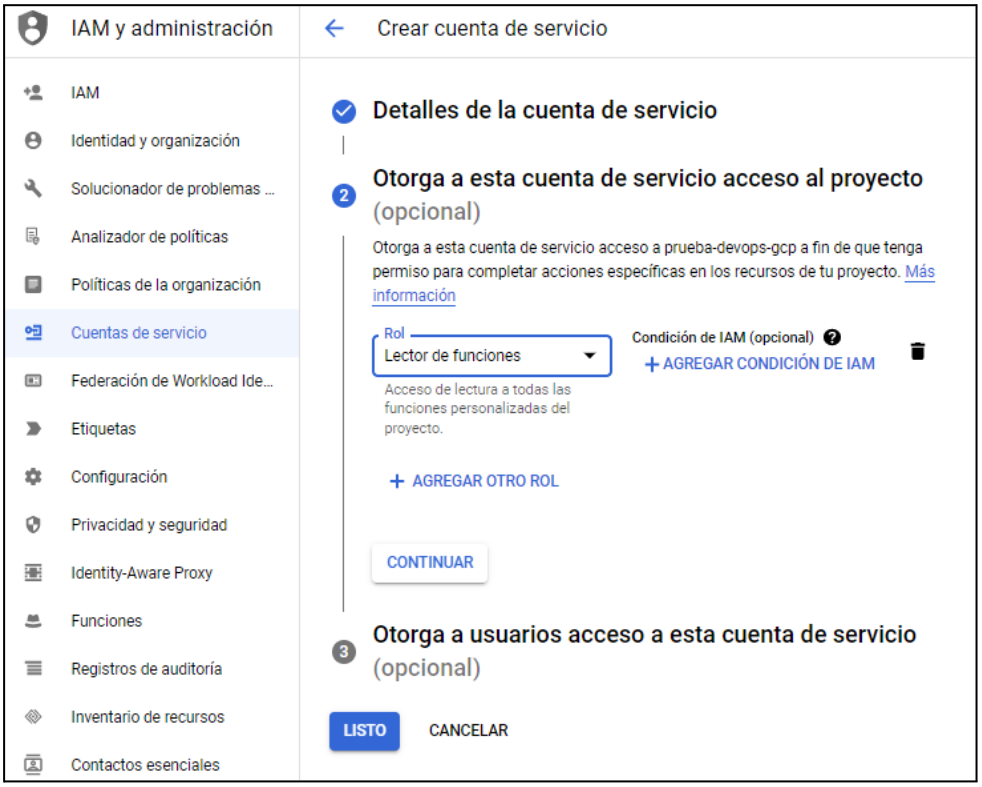
Copiamos y pegamos y guardamos el JSON de las credenciales

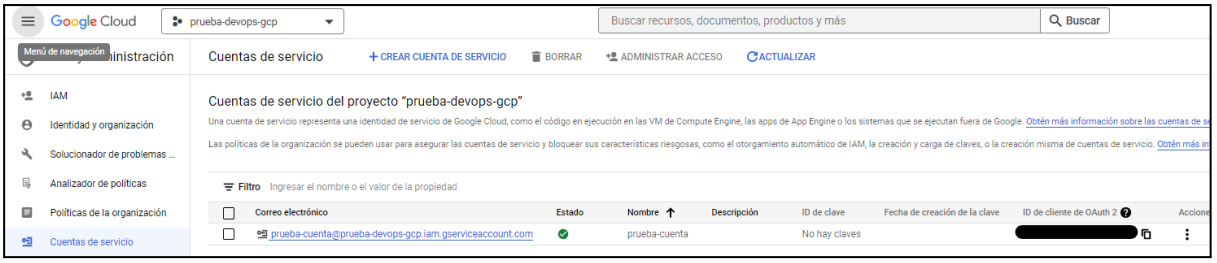




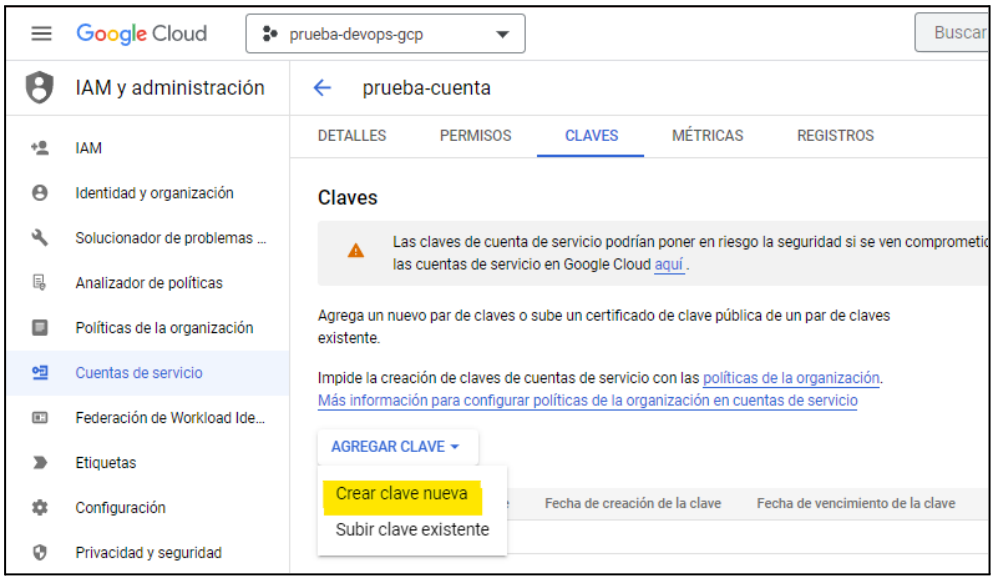
3. Crear la cuenta de servicio

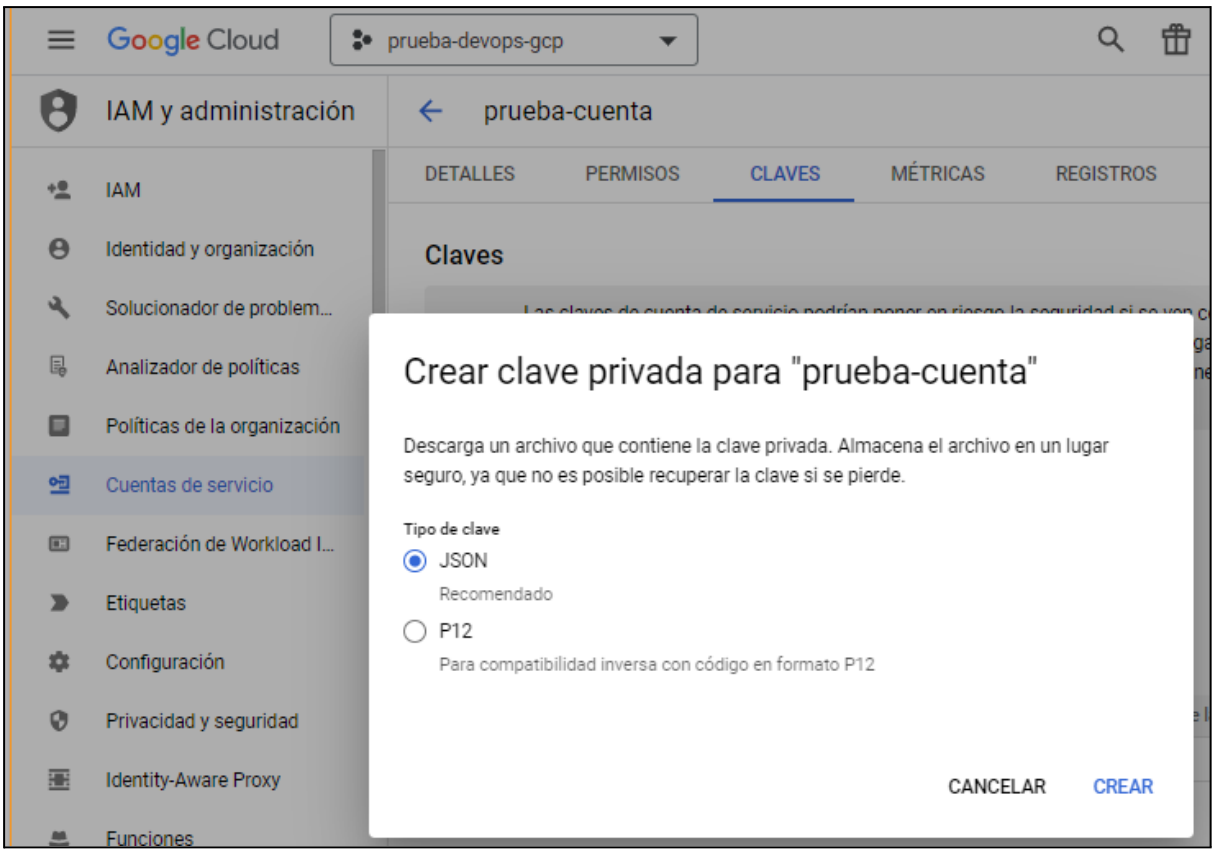

IAM y administración
Crear cuenta de servicio
IAM
Identidad y organización
Solucionador de problemas ...
Analizador de políticas
Políticas de la organización
Cuentas de servicio
Federación de Workload Ide...
Etiquetas
Configuración
Privacidad y seguridad
Identity-Aware Proxy
Funciones
Registros de auditoría
Inventario de recursos
Contactos esenciales
1 Detalles de la cuenta de servicio
Nombre de la cuenta de servicio
prueba-cuenta
Mostrar nombre de esta cuenta de servicio
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
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
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
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
Acceso de lectura a todas las funciones personalizadas del proyecto.
Condición de IAM (opcional)
+ AGREGAR CONDICIÓN DE IAM
+ AGREGAR OTRO ROL
CONTINUAR
3 Otorga a usuarios acceso a esta cuenta de servicio (opcional)
LISTO
CANCELAR



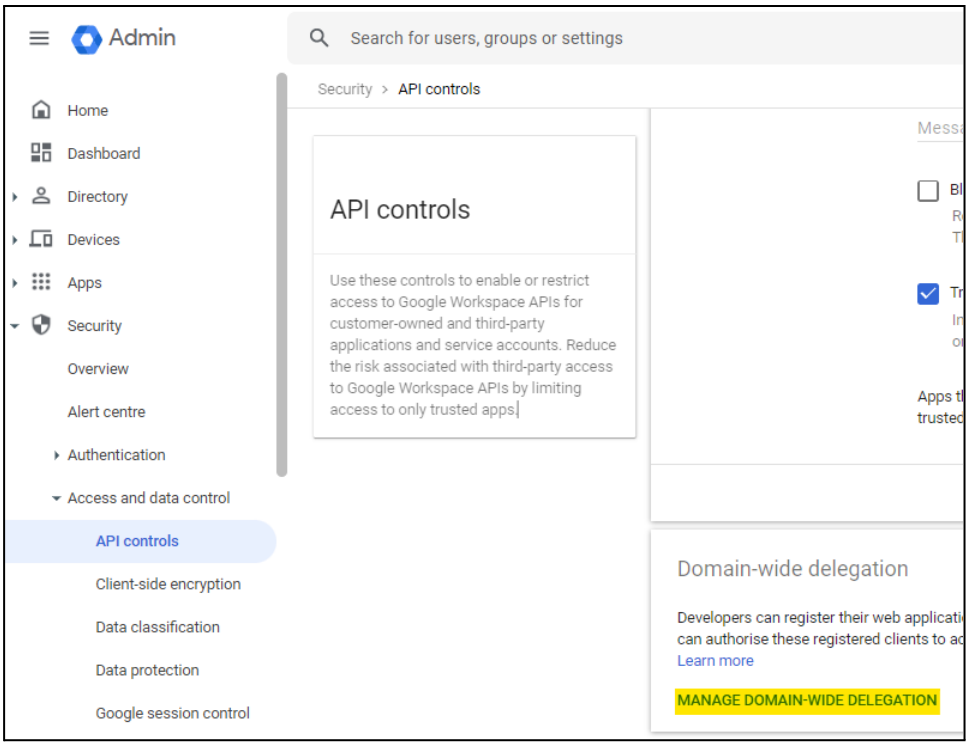
Tenemos que crear una clave de la cuenta de servicio



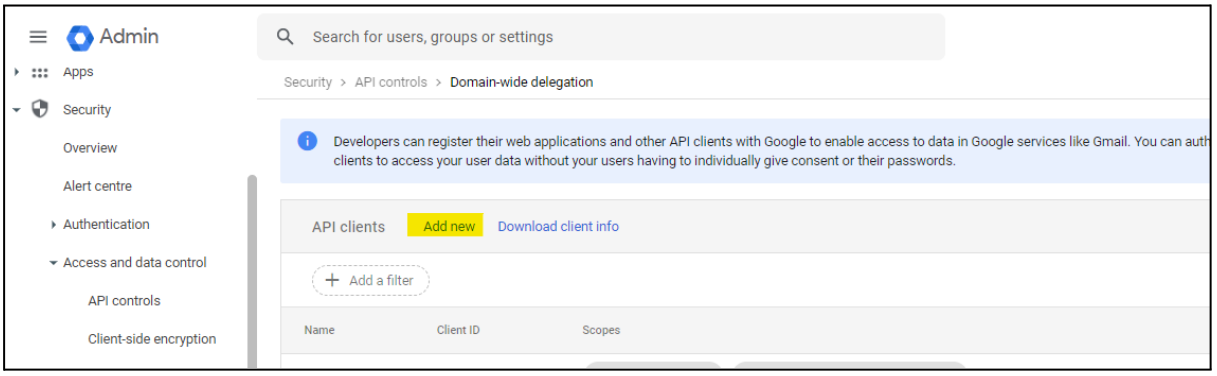


Se te descargará un archivo JSON en tu propio ordenador

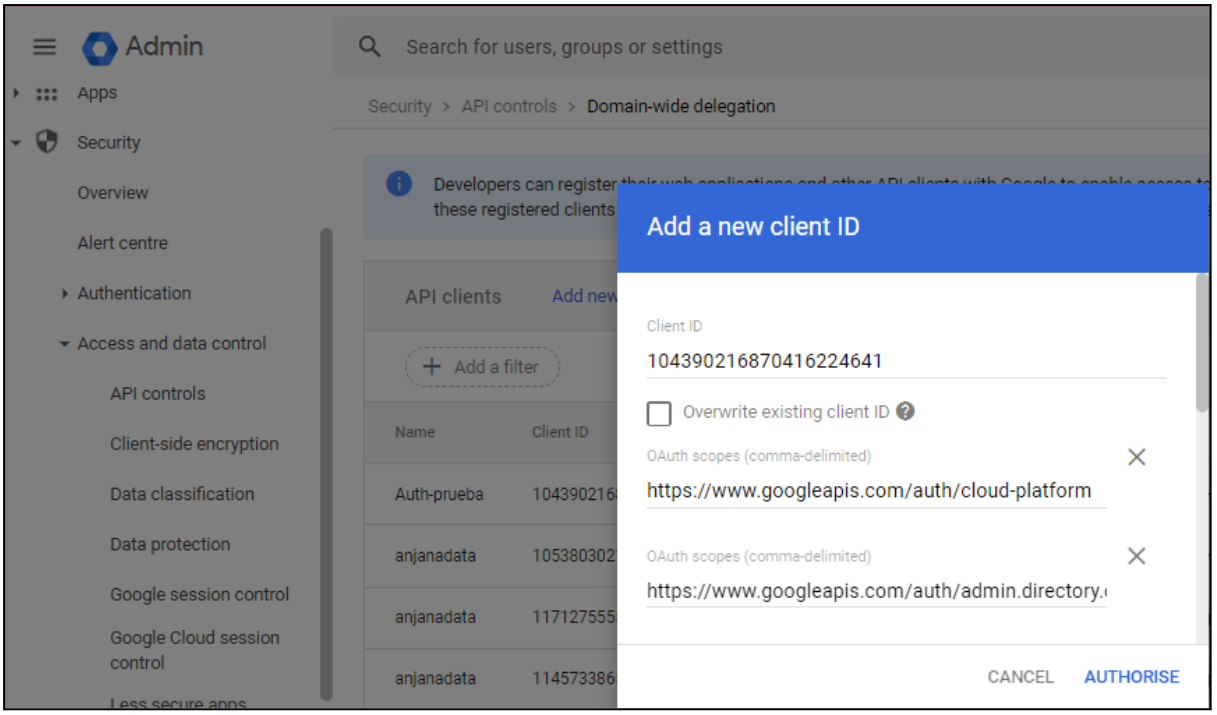
4. En Gsuite->seguridad->Control de accesos->Control de API registrar la cuenta de servicio y darle permisos en los scopes necesarios

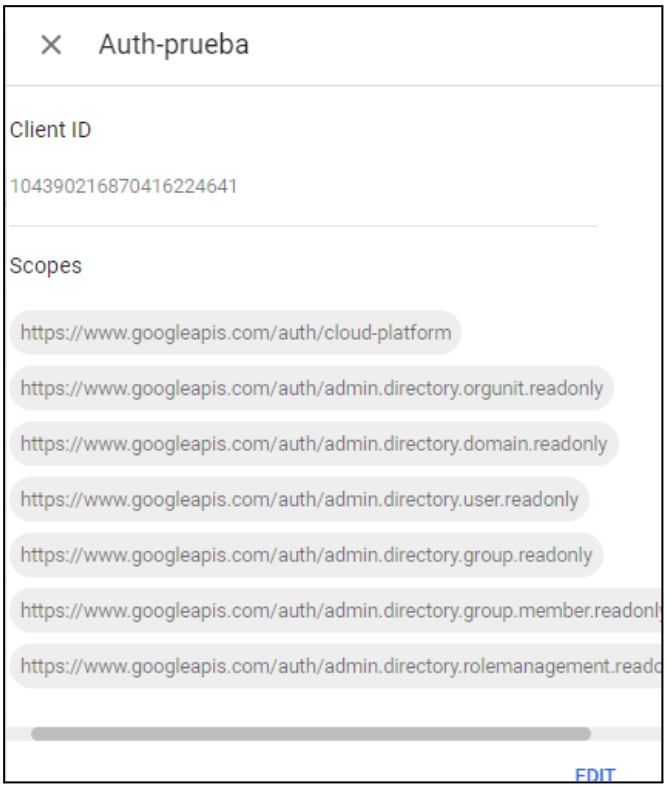


Una vez dentro, debemos de añadir un API client nuevo



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
Apps
Security
Overview
Alert centre
Authentication
Access and data control
API controls
Client-side encryption
Data classification
Data protection
Google session control
Google Cloud session control
Security > API controls > Domain-wide delegation
Developers can register
these registered clients
API clients
Add a filter
Name
Client ID
Auth-prueba
anjanadata
anjanadata
anjanadata
Add a new client ID
Client ID
10439021687041622464 1
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.readonl
https://www.googleapis.com/auth/admin.directory.rolemanagement.readc
EDIT

Asignación de roles en GCP y Gsuite

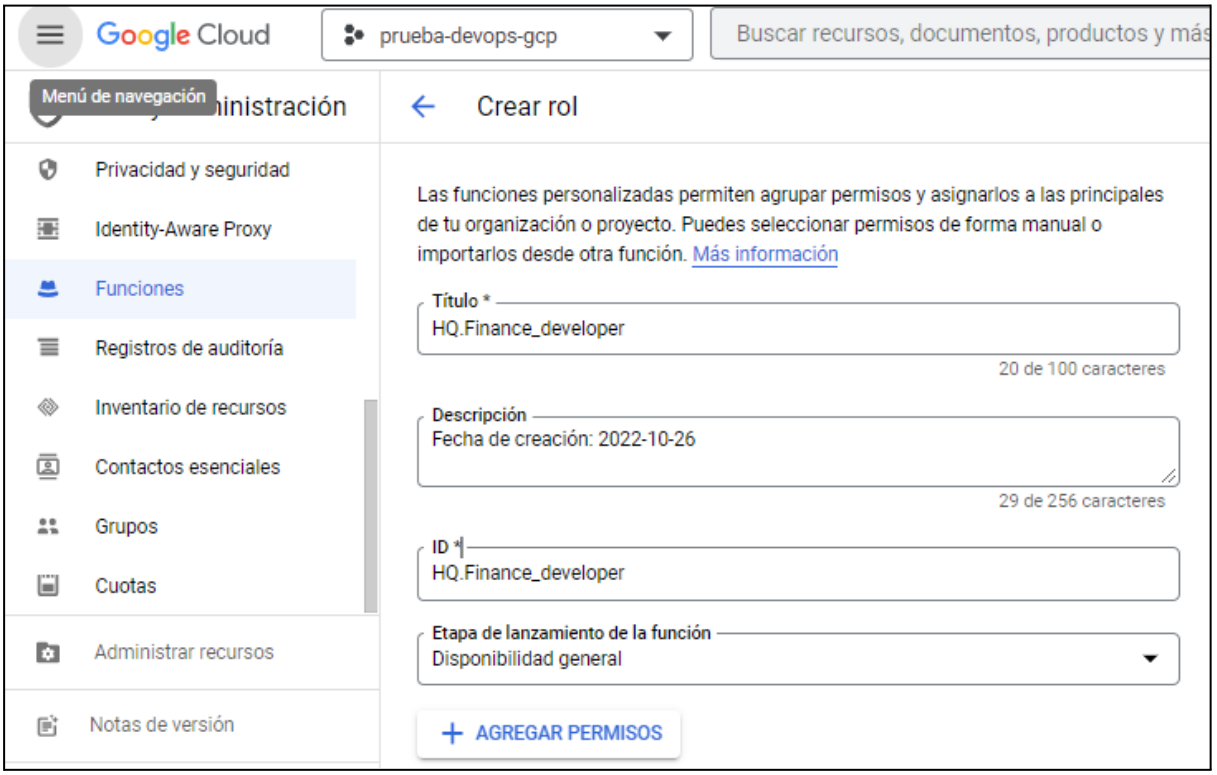
En el cloud de Google podemos dar membresías a roles de dos maneras distintas:

- Funciones de GCP
- Grupo en Gsuite

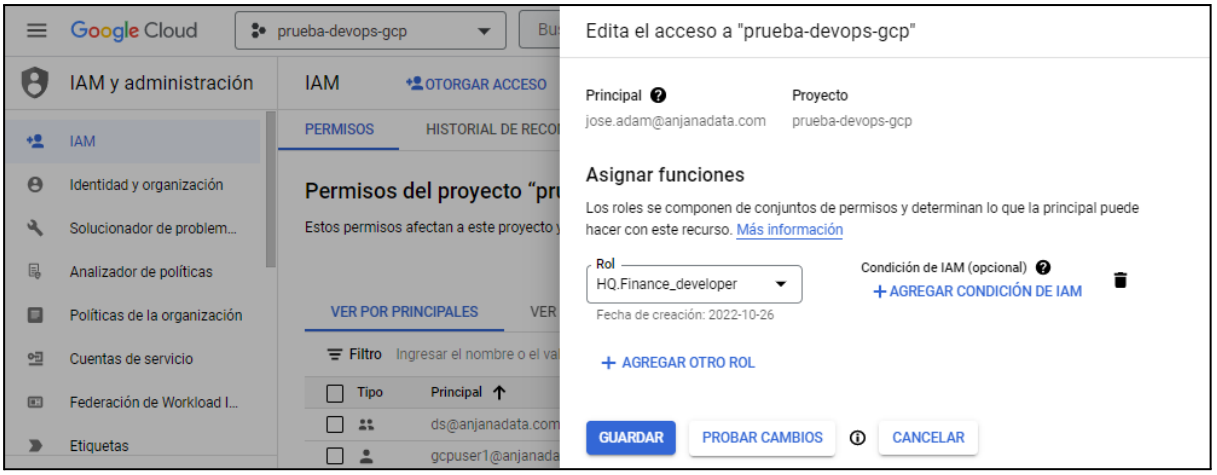
Funciones en GCP

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

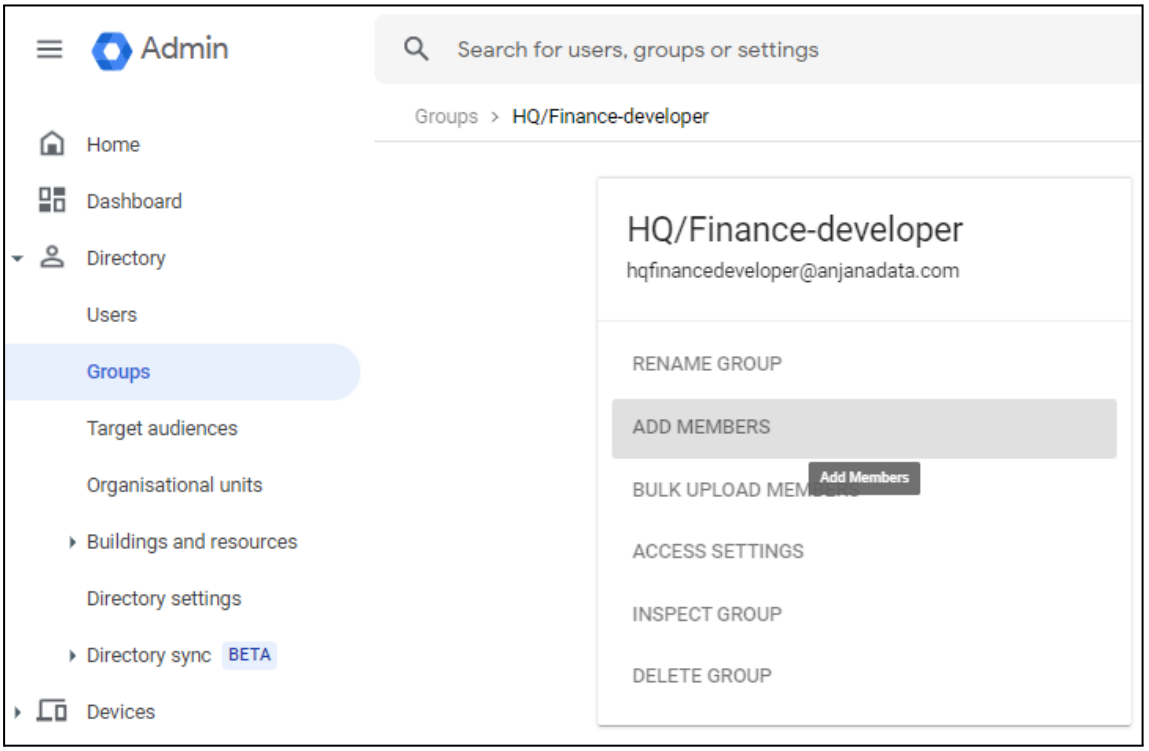


2. Se asigna la nueva función custom a un usuario en IAM



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.