Integración Azure

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 para “Web apps”, descrito por el fabricante en la siguiente documentación:
https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-flow
https://docs.microsoft.com/en-us/azure/active-directory/develop/app-sign-in-flow
https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-flows-app-scenarios

Para la recuperación de información relativa a perfil de usuario y grupos de autorización se explota la API Microsoft Graph:
https://docs.microsoft.com/en-us/graph/overview

Es importante considerar que la capacidad de uso de esta API corresponde directamente con la cuota que Microsoft le tiene asignada a la cuenta del cliente con su licencia. De forma general Microsoft limita las peticiones a:

- Límite al Resource Manager
  https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/request-limits-and-throttling
- Límite a la API Graph (15 llamadas en lapso de 5 segundos)
  https://learn.microsoft.com/en-us/azure/governance/resource-graph/concepts/guidance-for-throttled-requests#understand-throttling-headers

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.

Configuración de autenticación

En la propiedad *security.authentication* se configuran los distintos proveedores de autenticación que se utilizan.
En el caso de Azure es necesario configurar las siguientes propiedades:

```
security:
 authentication:
    oidc:
      providers:
        azure:
          name: Anjana Azure
            authorize-url:
https://login.microsoftonline.com/aef41d72-8720-418a-bb06-9fb98ef04ded/
oauth2/v2.0/authorize?client_id=${security.authentication.oidc.provider
```

```
s.azure.client-id}&response_type=code&response_mode=query&scope=${secur
ity.authentication.oidc.providers.azure.scopes}&redirect_uri=${security
.authentication.oidc.providers.azure.redirect-uri}
            authorize-url-portuno:
https://login.microsoftonline.com/aef41d72-8720-418a-bb06-9fb98ef04ded/
oauth2/v2.0/authorize?client_id=${security.authentication.oidc.provider
s.azure.client-id}&response_type=code&response_mode=query&scope=${secur
ity.authentication.oidc.providers.azure.scopes}&redirect_uri=${security
.authentication.oidc.providers.azure.redirect-uri-portuno}
            token-url:
https://login.microsoftonline.com/<tenant>/oauth2/v2.0/token
            scopes: openid profile email user.read
            client-id: <client-id>
            client-secret: <client-secret>
            client-authentication-method: POST
            redirect-uri:
https://anjana.client.com:8443/anjana/authorized
            redirect-uri-portuno:
https://anjana.client.com:8443/admin/authorized
            username-claim: preferred_username
            workflowType: IMPLICIT
            type: AZURE
```

- name: el nombre que se mostrará en la pantalla de login

Configuración de autorización

En la propiedad *security.authorization* se configuran los distintos proveedores de autorización que se utilizan.
En el caso de Azure es necesario configurar las siguientes propiedades:

```
security:
 authorization:
    azure-active-directory:
      providers:
        azure:
          scopes: https://graph.microsoft.com/.default
          client-id: <clientId>
          client-secret: <clientSecret>
          tenant-id: <tenantId>
          national-cloud: Global
          groupOrgUnitSeparator: "/"
          roleOrgUnitSeparator: "-"
          groupPrefix: "prefix-"
```

- groupOrgUnitSeparator: 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.
- roleOrgUnitSeparator: 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

El plugin a desplegar el cual realizará la parte de las tareas de gobierno activo que tengan que provisionar elementos sobre Azure AD es “Tot plugin Azure AD”.
Para la provisión de grupos de usuarios a los que posteriormente se asignan permisos de acceso a recursos de datos gobernados por el producto se explota la API Microsoft Graph:
https://docs.microsoft.com/en-us/graph/overview

Nomenclatura de los grupos

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[1].
Como se puede observar hay dos separadores:

- El separador de jerarquía de la unidad organizativa: ‘/’ , cuyo valor es configurable con la propiedad del yml: roles.separator-organizational-unit.
- El separador de la unidad organizativa y el rol: ‘-’ , cuyo valor es configurable con la propiedad del yml: roles.separator-role.

Credenciales requeridas

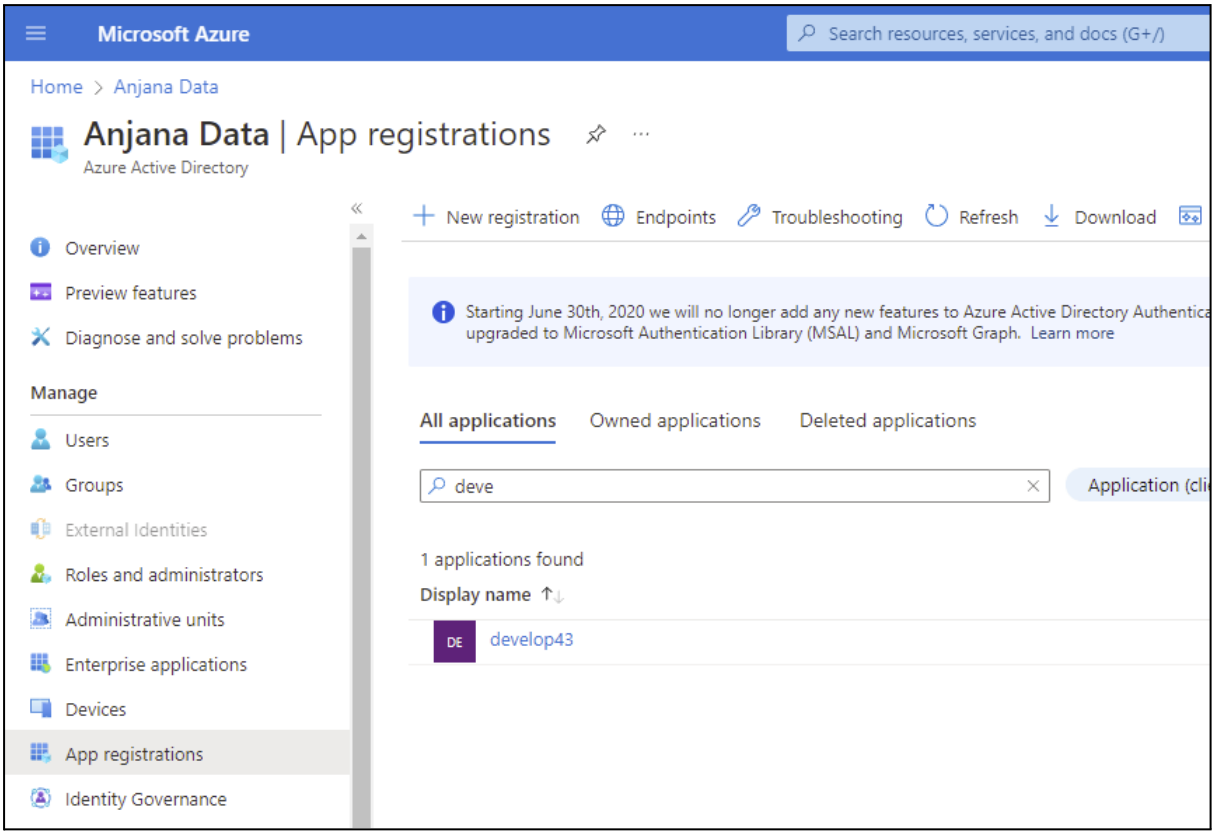
La credencial puede ser única aglutinando los permisos de ambas, pero se recomienda mantenerlas por separado de cara a facilitar la monitorización y auditoría de la actividad ejercida por las mismas.

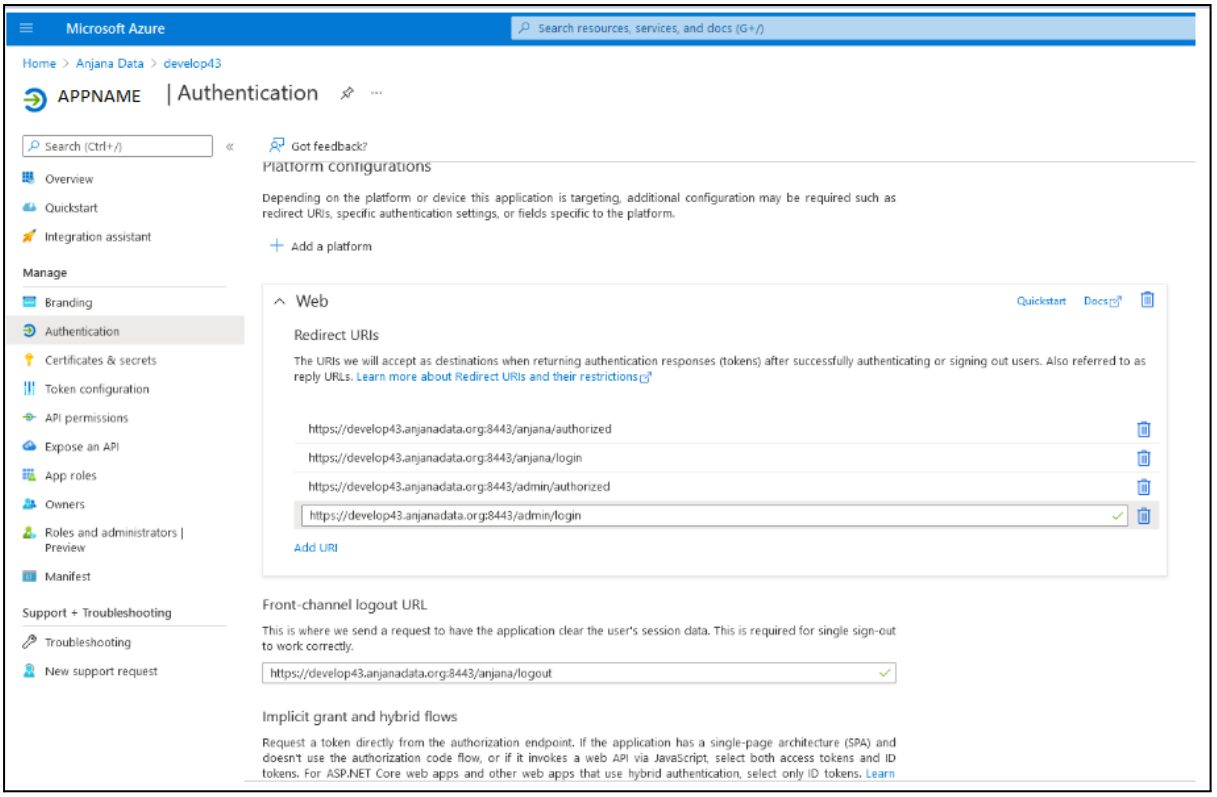
[1] Independientemente de los separadores usados en los repositorios de identidades el producto normalizará al formato estándar, por lo que en la configuración del producto ha de usarse siempre los separadores “/” y “-” para conformar el alias, por ejemplo “UO/UO…./UO-role”.

Autenticación y autorización (Oauth2)

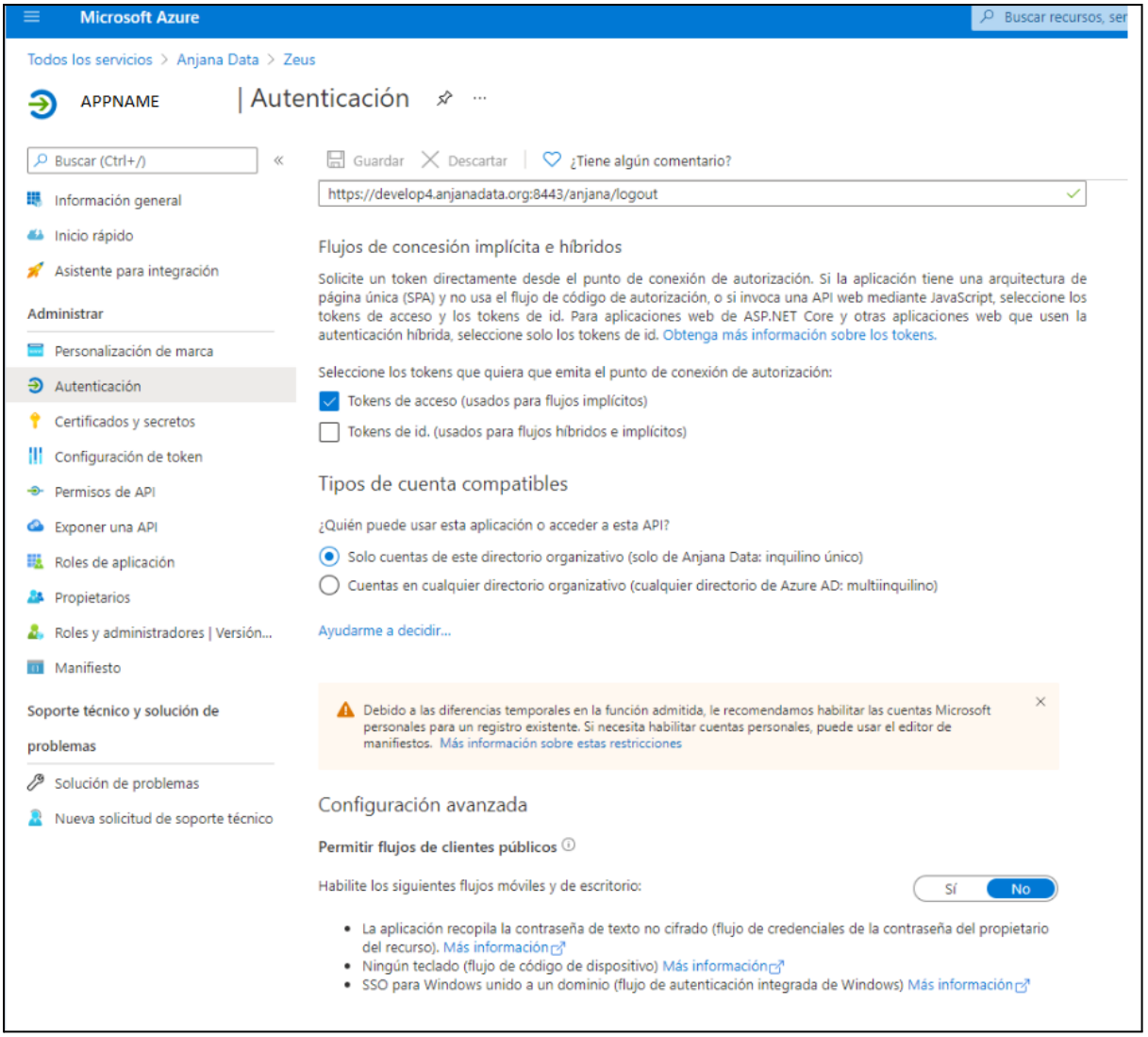
La funcionalidad está directamente embebida en el microservicio de gestión de autenticación y autorización Zeus, se habilita y configura mediante el fichero de configuración de dicho microservicio.

- Para la autenticación web se deben configurar las url acorde al nombre de dominio que enrute hasta el frontal de Anjana Data, es necesario dar de alta dos URL, más la de log out:
    - https://<host>:<port>/anjana/authorized
    - https://<host>:<port>/anjana/login
    - https://<host>:<port>/anjana/logout

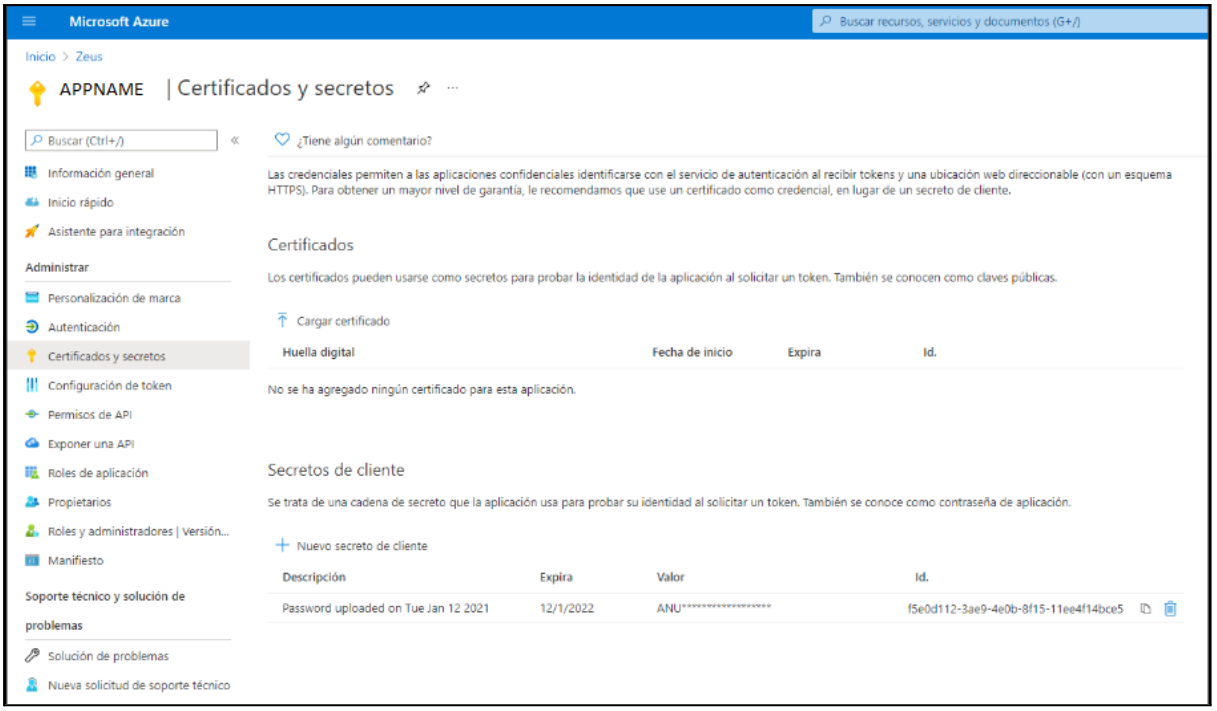




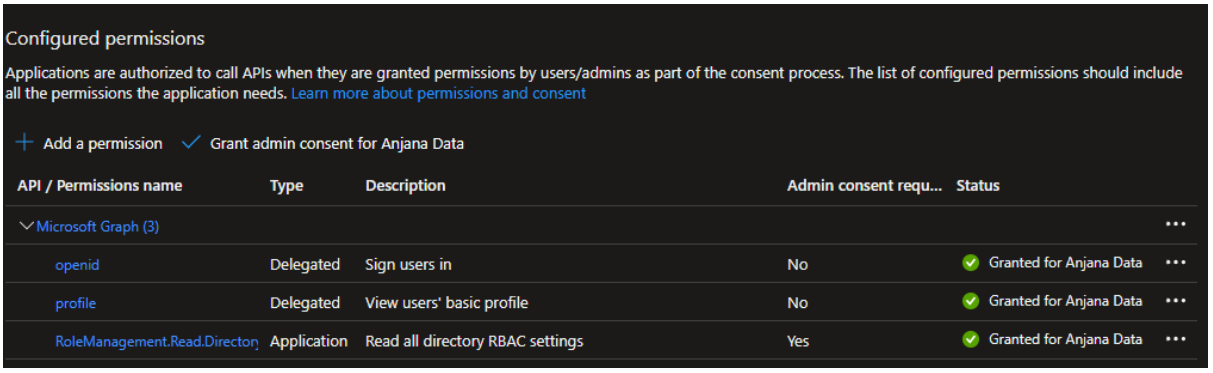
- En base a necesidad ajustar las opciones, generalmente son las siguientes:



- Tras ello es necesario crear cliente y secreto que posteriormente será configurado en producto:



- Asignar permisos de lectura necesarios para recopilar la información del usuario y sus membresías que serán mapeadas de forma automática a roles y unidades organizativas en el producto:



- Asignar usuarios a los grupos de Azure AD.

Gobierno activo

El plugin a desplegar el cual realizará la parte de las tareas de gobierno activo que tengan que provisionar elementos sobre Azure AD es “Tot plugin Azure AD”, en su documentación queda descrita la credencial requerida.

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.