Integración Azure

Control de versiones

Versión	Fecha de modificación	Responsable	Aprobador	Resumen de cambios
1.0	28/10/2022	Anjana Producto	Anjana Producto	Creación del documento
2.0	16/03/2023	Anjana Producto	Anjana Producto	Corrección de la variable client-secret en la Configuración de autenticación

Modelo de integración

Autenticación y autorización (Oauth2)

Anjana Data se integra mediante circuito estándar para “Web apps” el cual se describe 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

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.oidc.providers* colgarán los distintos proveedores de autenticación que tengamos. En el caso de Azure debemos poner las siguientes propiedades:

- name: Azure AD
    - *El nombre que se mostrará en la pantalla de login*
- authorize-url: https://login.microsoftonline.com/<tenant>/oauth2/v2.0/authorize?client_id=${security.authentication.oidc.providers.azure.client-id}&response_type=code&response_mode=query&scope=${security.authentication.oidc.providers.azure.scopes}&redirect_uri=${security.authentication.oidc.providers.azure.redirect-uri}
- authorize-url-portuno: https://login.microsoftonline.com/<tenant>/oauth2/v2.0/authorize?client_id=${security.authentication.oidc.providers.azure.client-id}&response_type=code&response_mode=query&scope=${security.authentication.oidc.providers.azure.scopes}&redirect_uri=${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://<front-anjana>/anjana/authorized
- redirect-uri-portuno: https://<front-anjana>/admin/authorized
- username-claim: preferred_username
- type: AZURE

Ej.

```yaml
security:
  ...
  authentication:
    oidc:
      providers:
        azure:
          name: Anjana Azure
          authorize-url: https://login.microsoftonline.com/11111111-2222-3333-4444-55
          authorize-url-portuno: https://login.microsoftonline.com/11111111-2222-3333
          token-url: https://login.microsoftonline.com/11111111-2222-3333-4444-555555
          scopes: openid profile email user.read
          client-id: aaaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee
          client-secret: AAAAAA.BBBBBBB_CCCCCCCCC~-.DDDDDDDDDD
          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
          type: AZURE
```

Configuración de autorización

En la propiedad *security.authorization* colgarán los distintos proveedores de autenticación que tengamos. En el caso de Azure debemos poner sus propiedades en security.authorization.azure-active-directory.providers.azure:

- tenant-id: 11111111-2222-3333-4444-5555555555555
- client-id: aaaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee
- client-secret: AAAAAA.BBBBBB_CCCCCCCCCC~-.DDDDDDDDDDDDDDD
- scopes: https://graph.microsoft.com/.default
- national-cloud: Global # One of: Global Germany China or UsGovernment. Global is default
- 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)

```yaml
security:
  ...
  authorization:
    azure-active-directory:
      providers:
        azure:
          tenant-id: 11111111-2222-3333-4444-5555555555555
          client-id: aaaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee
          client-secret: AAAAAA.BBBBBBB_CCCCCCCCC~-.DDDDDDDDDDD
          scopes: https://graph.microsoft.com/.default
          national-cloud: Global # One of: Global Germany China or UsGovernment. Global is default
```

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 AzureAD”.
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.
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: roles.separator-organizational-unit.
-El separador de la unidad organizativa y el rol -> ‘-’ , cuyo valor es configurable gracias a 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.

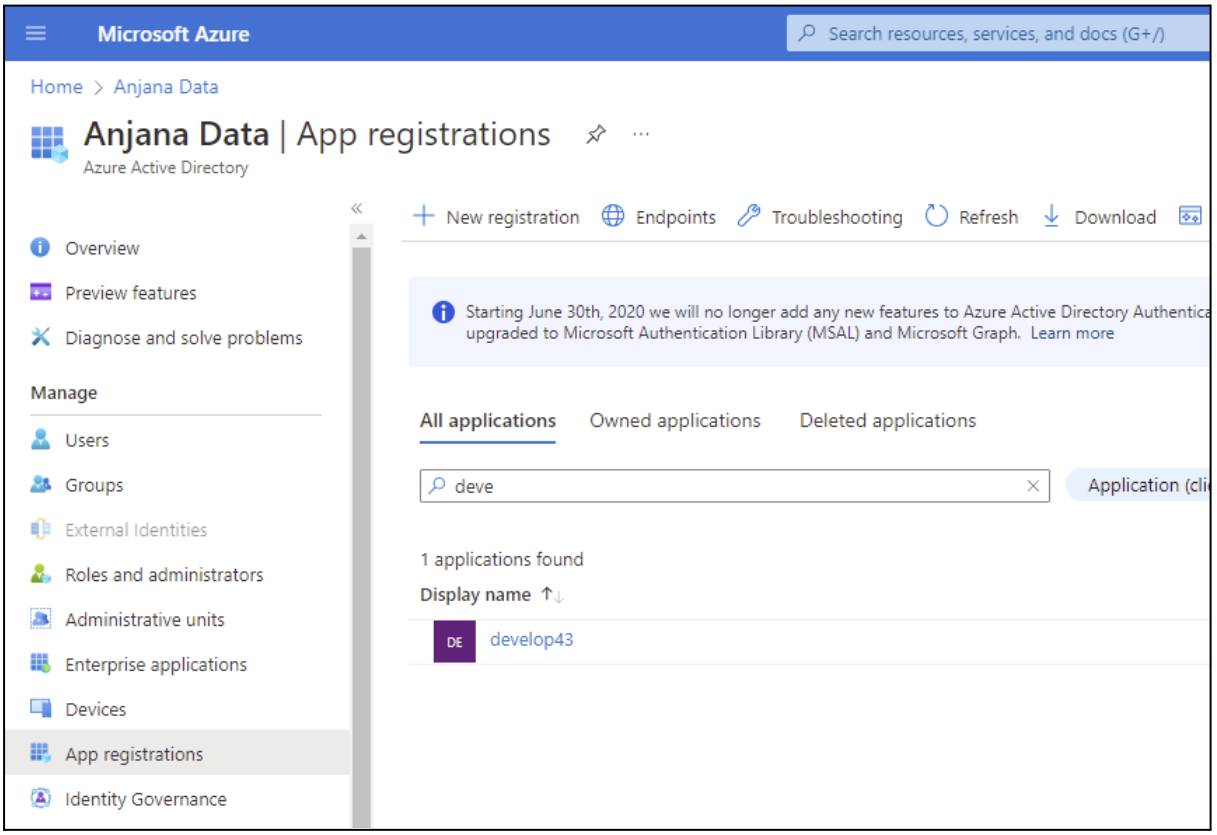
Autenticación y autorización (Oauth2)

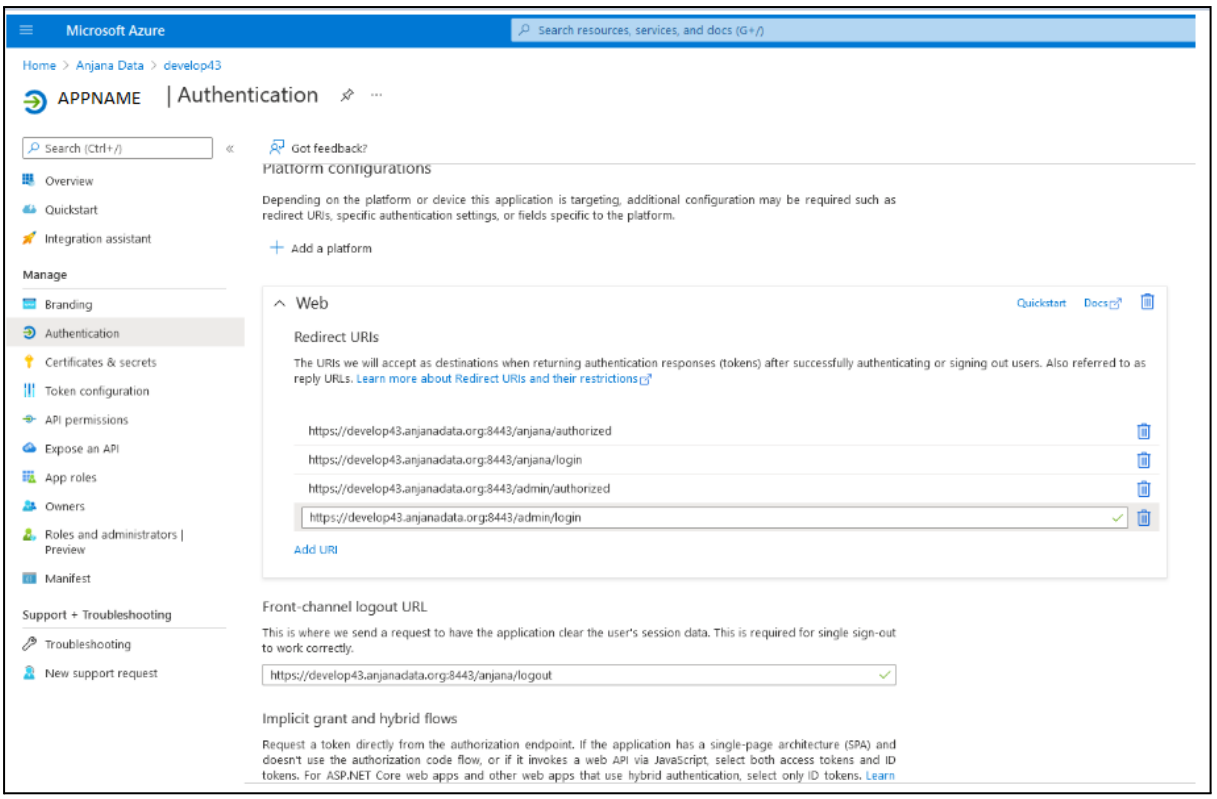
La funcionalidad está directamente embebida en el microservicio de gestión de autenticación y autorización Zeus, se habilita y configura mediante el fichero de configuración de dicho microservicio.

Es necesario registrar una nueva aplicación con las siguientes propiedades.

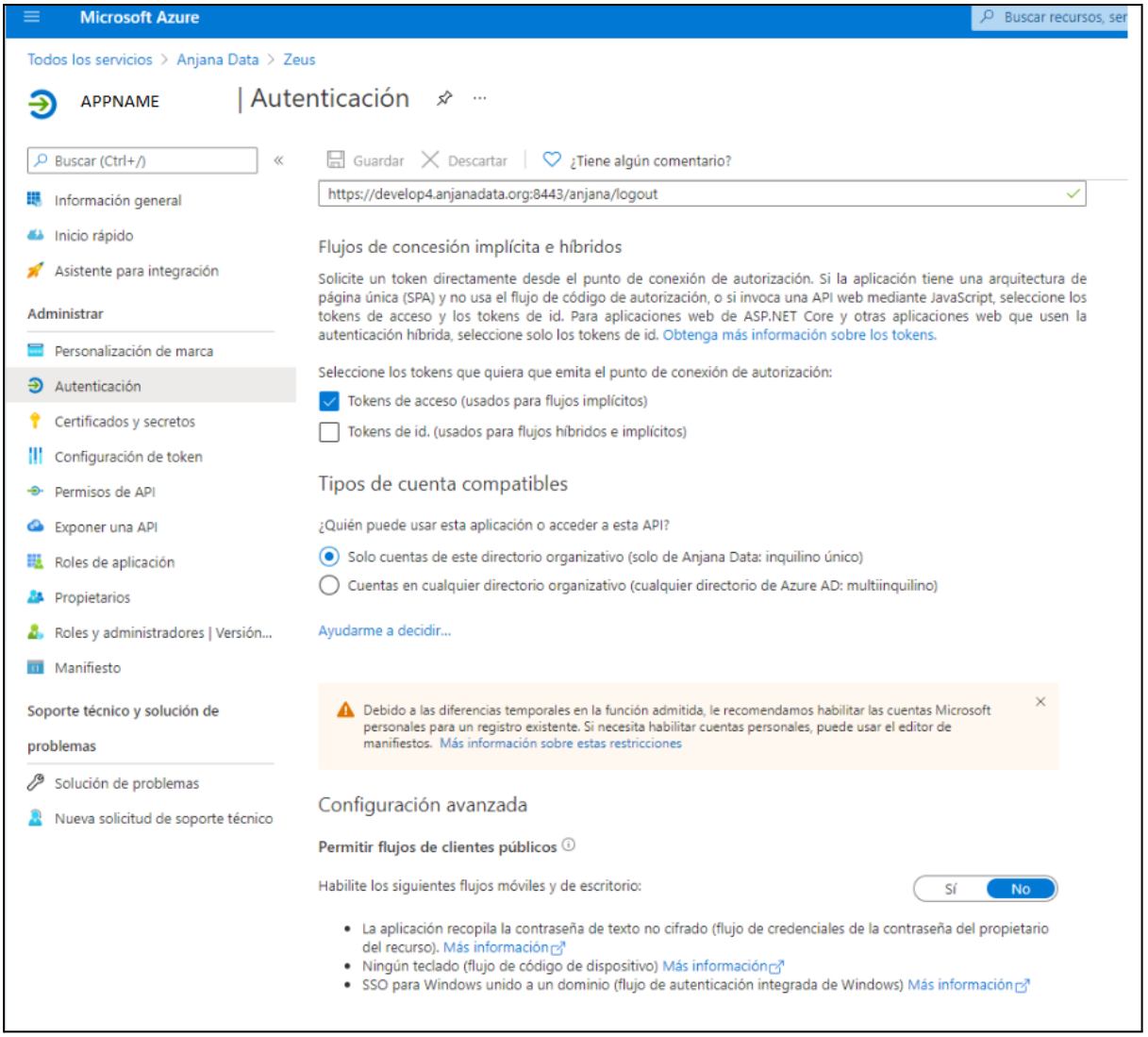
Autenticación web en la cual configuraremos las url acordes al nombre de dominio que enrute hasta el frontal de Anjana Data, es necesario dar de alta dos URL, más la de log out:

- https://<host>:<port>/anjana/authorized
- https://<host>:<port>/anjana/login
- https://<host>:<port>/anjana/logout

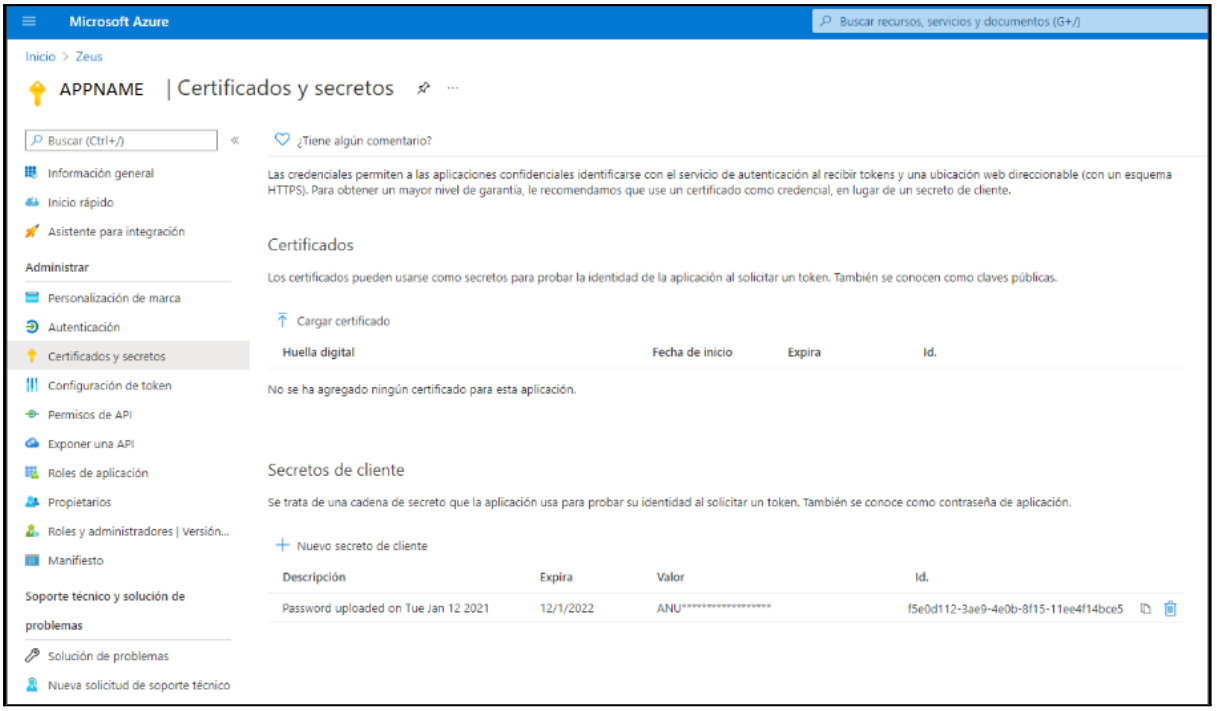




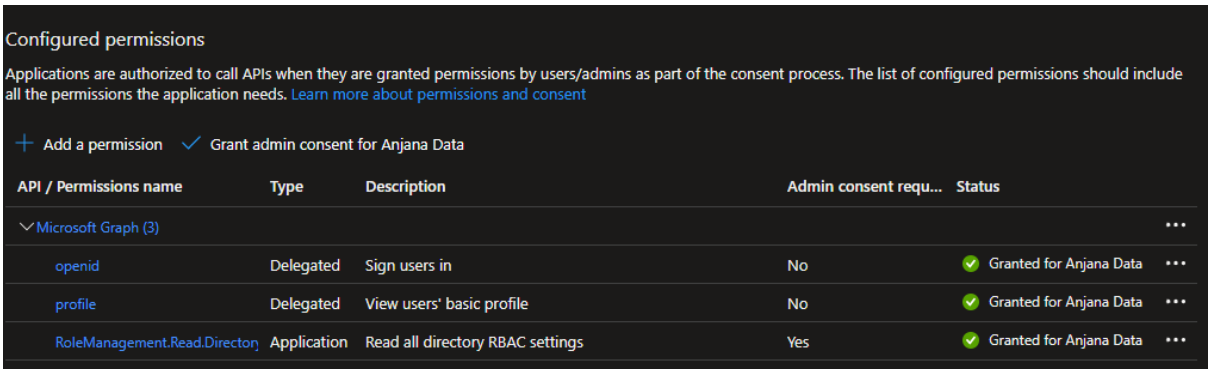
En base a necesidad ajustar las opciones, generalmente son las siguientes:



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 las cuales 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 AzureAD”, 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.