Integración LDAP

Control de versiones

Versión	Fecha de modificación	Responsable	Aprobador	Resumen de cambios
1.0	22/09/2023	Anjana Producto	Anjana Producto	Creación del documento

Modelo de integración

Autenticación y autorización (Oauth2)

Anjana Data interactúa con el gestor de identidades vía protocolo LDAP, mediante el cual validará la credencial facilitada por el usuario y recuperará la información del usuario y los grupos a los que pertenece.

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.

Mecanismo de autenticación LDAP implementado

- https://docs.ldap.com/specs/rfc4513.txt
- https://ldap.com/ldapv3-wire-protocol-reference-bind/

Mecanismo de autorización LDAP utilizado para leer el perfil de usuario

- https://ldap.com/ldapv3-wire-protocol-reference-search/

Configuración de autenticación

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

```
security:
  authentication:
    ldap:
      user-authentication: USER_CONNECTION
      url: ldap://ldap service:10389
      base-dn: dc=anjanadata,dc=org
      connection-user-dn: uid=admin,ou=system
      connection-user-password: <pwd>
      user-structural-class: person
      user-search-attribute: cn
      user-search-filter: (cn={0})
```

Configuración de autorización

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

```
security:
  authorization:
    ldap:
     url: ldap://ldapservice:10389
      base-dn: dc=anjanadata,dc=org
```

```
connection-user-dn: uid=admin,ou=system
connection-user-password: <pwd>
user-structural-class: person
user-search-attribute: cn
group-structural-class: groupOfNames
group-search-attribute: cn
member-of-patch-filter: member={0}
membership-user-group: member
root-ous:
  -
    name: groups
ou-structural-class: organizationalUnit
ou-search-attribute: ou
```

Gobierno activo

De forma general los DSA de Anjana Data serán representados como grupos y los firmantes de dichos DSA serán miembros de dichos grupos. Los plugins de Tot asignan permisos en las tecnologías conectadas a dicho LDAP mapeando dichos permisos directamente contra estos grupos que representan a los DSA.

Credenciales requeridas

Autenticación y autorización

Es necesario una credencial que permita:

- Realizar validación de credenciales de usuario (bind)
- Recuperar información de usuario
- Recuperar información de grupos de usuarios e integrantes de los mismos.

Mecanismo de autenticación LDAP implementado

- https://docs.ldap.com/specs/rfc4513.txt
- https://ldap.com/ldapv3-wire-protocol-reference-bind/

Mecanismo de autorización LDAP utilizado para leer el perfil de usuario

- https://ldap.com/ldapv3-wire-protocol-reference-search/

Gobierno activo

Credencial requerida documentada en plugin “Tot plugin LDAP”