Tot plugin LDAP

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

Introducción

Este plugin se usa en coordinación con los plugins de tecnologías de almacenamiento conectadas a LDAP para provisionar los grupos que representan a los DSA y adicionalmente gestiona las membresías que representan la aceptación de los DSA por parte de los usuarios.

Servicios disponibles en el plugin

- Crear grupos: Permite crear grupos con usuarios.
- Asignar/desasignar usuarios: Sirve para añadir o eliminar usuarios en los grupos creados por el plugin.
- Eliminar grupos: Eliminar grupos previamente creados.

Modelo de integración

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.

Anjana Data creará y eliminará los grupos de forma automática, al igual que incluirá y excluirá a usuarios de cada grupo con el objetivo de materializar la adhesión o desadherencia de un usuario a un DSA.

Anjana Data interactúa con el gestor de identidades vía protocolo LDAP, mediante el cual ejecutará las operaciones descritas.

Credenciales requeridas

El plugin requiere de una credencial con los siguiente permisos:

- Creación, modificación y eliminación de OUs y grupos (`groupOfNames`)
- Modificación de miembros de grupos

Si se usa como instancia de plugin complemento para otra instancia de otro plugin diferente hay que tener en cuenta que cada tecnología es diferente, por lo tanto, la configuración de cada uno de ellos puede variar.

Limitaciones

- El nombre del DSA con el que se va a crear el grupo no debe superar los 60 caracteres, aunque se deberá revisar las limitaciones de la implementación AD en particular que se tiene implementado en caso de que varíe.

- En la ruta de la rama generada con la configuración de base + baseUser no deben existir usuarios con el mismo valor de username, aunque estén en sub ramas distintas.
- El nombre de la clase con la que se crean por defecto los grupos es groupOfNames. Como se explica más adelante, ese tipo de clase no permite crear grupos sin usuarios por lo que si, debido a la configuración, no hay usuarios asignados como owners en el DSA, la creación del grupo en LDAP fallará.
  No obstante, existen otros tipos de clases que sí permiten crear el grupo en LDAP sin incluir usuarios como el tipo group.

Configuración

Aquí se incluye el detalle de la configuración específica del plugin.
En la Guía de Configuración técnica se explica la configuración común.

```
server:
  port: 15015

totplugin:
  server:
    urls:
      - http://<totserver>:<totport>/tot/
  aris:
    - ari: "anja:totplugin:im:/ldap/ldap/ldap/"
  connection:
    url: ldap://ldapservice:10389
    base: dc=anjanadata,dc=org
    baseUser: ou=people
    baseGroup: ou=groups
    user: uid=admin,ou=system
    password: anjana
  ldap:
    attributes:
      userCn: cn
      user: person
      member: member
      groupCn: cn
      extraGroupCn:
        - sAMAccountName
      group: group
      groupCaseTransformation: LOWER
      groupParam:
         instanceType: 4
         groupType: -214748646
         objectCategory:
cn=group,cn=schema,cn=configuration,dc=cdp,dc=local

eureka:
  client:
    serviceUrl:
       defaultZone: http://<totserver>:<totport>/tot/eureka
```

- *TotPlugin* (apartado con la configuración específica del plugin):

- *Connection* (apartado con la configuración relativa a las credenciales de conexión con LDAP):
  - *url:* url completa de acceso a ldap (ip y puerto).
  - *base:* especifica el nombre por el que empieza la búsqueda del ldap.
  - *baseUser:* dn que junto con la propiedad base se usa para determinar desde qué rama se buscarán los usuarios para incluirlos o eliminarlos de grupos. Variable opcional
  - *baseGroup:* dn desde el que se crearan los grupos que representan a los DSA
  - *user:* usuario para conectarse con el repositorio.
  - *password:* contraseña del usuario de ldap.
- *Ldap* (apartado con la configuración de algunos atributos del árbol de jerarquía del LDAP)
  - *attributes*:
    - *userCn:* el nombre del atributo que representa el nombre común de una entrada de usuario en el LDAP, por defecto es cn
    - user: el nombre de la clase que tienen los usuarios, usada como filtro para buscar usuarios antes de añadirlos o quitarlos de grupos, por defecto es person
    - *member:* el nombre del atributo que representa los miembros de una entrada, por defecto es member
    - groupCn: el nombre del atributo que representa el nombre común de una entrada de grupo en el LDAP. Por defecto: cn
    - *group*: el nombre de la clase con la que crear los grupos. Por defecto: groupOfNames
    - *groupParam*: lista de parámetros extra que se quieren insertar en el grupo al crearlo. Parámetro opcional
    - extraGroupCn: lista de atributos en las que se tiene que incluir el mismo valor que en el atributo groupCn. Parámetro opcional
    - groupCaseTransformation: La transformación que se quiere hacer al nombre del grupo cuando no existe un physical name, puede ser UPPER (convertir todo a mayúsculas), LOWER (convertir todo a minúsculas) o NONE (no hacer ninguna transformación). Por defecto: NONE.

Plugin de Ranger

En el caso de que se utilice el plugin de Tot LDAP en conjunto con Ranger y Active Directory, se debe tener en cuenta que se necesita un mecanismo para sincronizar los cambios realizados en los grupos de Active Directory y grupos que usa HDFS, por ejemplo SSSD.

Para ese caso que se requiera tener el identificador del grupo (el common name) en más de un sitio (por ejemplo el sAMAaccountName porque el mecanismo para sincronizar los cambios realizados en los grupos de Active Directory y grupos que usa HDFS lea ese atributo para la sincronización) se puede usar el extraGroupCn como se detalla en el ejemplo de configuración de arriba.

Es decir, si el usuario X se ha adherido a un DSA D, el resultado que se observará en Active Directory es la creación de un grupo D con un miembro, X.

Del mismo modo en Ranger se creará de una política con el grupo D y en HDFS al ejecutar por ejemplo *"hdfs groups X"* debe aparecer el grupo D.