



Tot plugin LDAP

Control de versiones	2
Introducción	3
Servicios disponibles en el plugin	3
Modelo de integración	3
Gobierno activo	3
Credenciales requeridas	3
Limitaciones	3
Configuración	4
Consideraciones	5
Especificidades para AD	5
Integración con Plugin de Ranger	6

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
2.0	29/01/2025	José González	Ana Melcón	Aclaraciones sobre la configuración, sobre todo centrado en las configuración necesaria para usar contra un Windows AD.

Introducción

Este plugin se usa en coordinación con los plugins de tecnologías de almacenamiento conectadas a tecnologías de gestor de identidades que implementen el protocolo 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 se representan como grupos y los firmantes de dichos DSA son miembros de dichos grupos.

Anjana Data crea y elimina los grupos de forma automática, al igual que incluye y excluye 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 ejecuta las operaciones descritas.

Credenciales requeridas

El plugin requiere de una credencial de conexión que será configurada en el YAML del plugin. Esta credencial requiere los siguientes permisos (cuyos nombres dependen de la tecnología usada):

- Creación, modificación y eliminación de OUs y grupos
- Modificación de miembros de grupos

Limitaciones

- El nombre del DSA con el que se va a crear el grupo se recomienda que no debe superar los 60 caracteres como norma general para evitar las limitaciones como la de Windows AD en particular.
- 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.

```
Unset
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 no obligatoria si se quiere buscar en “todas partes”.
 - **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 protocolo LDAP)
 - **attributes**:
 - **userCn**: el nombre del atributo que representa el nombre común de una entrada de usuario en LDAP. Por defecto: 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: person
 - **member**: el nombre del atributo que representa los miembros de una entrada. Por defecto: 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 y que se configura como en el ejemplo visto.
 - **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.

Consideraciones

Especificidades para AD

Los grandes cambios están en los atributos a utilizar en el protocolo LDAP para AD.

En **member** por lo general es necesario utilizar memberOf.

En **group** por lo general es necesario utilizar group.

En **extraGroupCn** por lo general es necesario usar sAMAccountName.

En *groupParam* es aconsejable rellenar los valores que se marcan en el ejemplo si se tiene una instalación estándar. Si no, pregunte a su departamento de IT cuáles son los valores. En caso de no saberlo se puede crear un grupo de forma manual y revisar esas propiedades.

Integración con 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 sAMAccountName 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.