Tot plugin Azure AD

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
1.1	31/01/2024	Anjana Producto	Anjana Producto	Añadida limitación con respecto a los nombres de los DSAs
1.2	14/03/2024	Anjana Producto	Anjana Producto	Se añade la información de edición de objetos

Introducción

Este plugin se usa en coordinación con los plugins de tecnologías de almacenamiento conectadas a Azure AD 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.

Modelo de integración

Gobierno activo

De forma general los DSA de Anjana Data serán representados como grupos en Azure AD, y los firmantes de dichos DSA serán miembros de dichos grupos.

Edición de objetos

El plugin de Azure Storage permite gestionar la activación o desactivación de entidades no nativas, para ello necesita que este plugin recupere la información de los grupos necesarios.

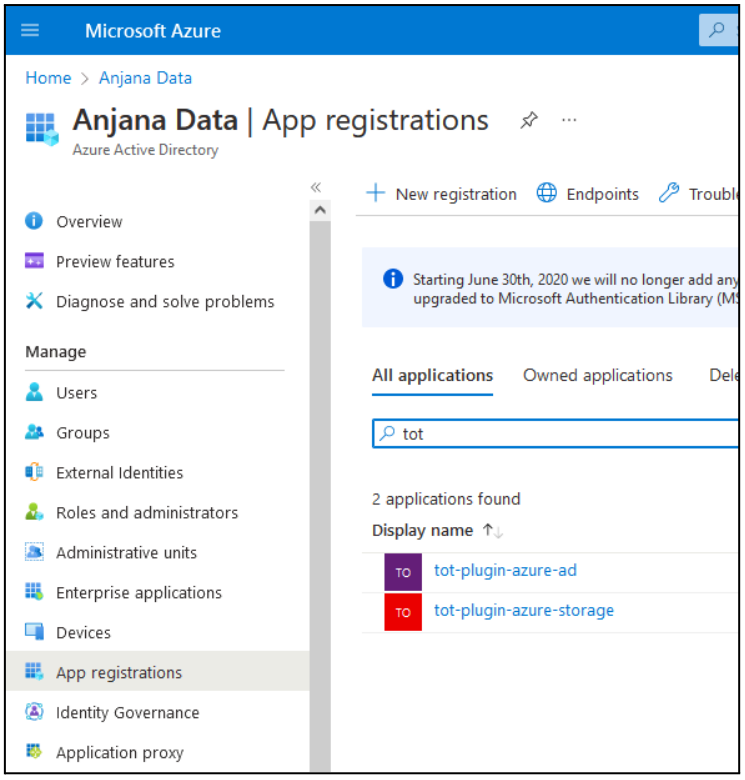
Credenciales requeridas

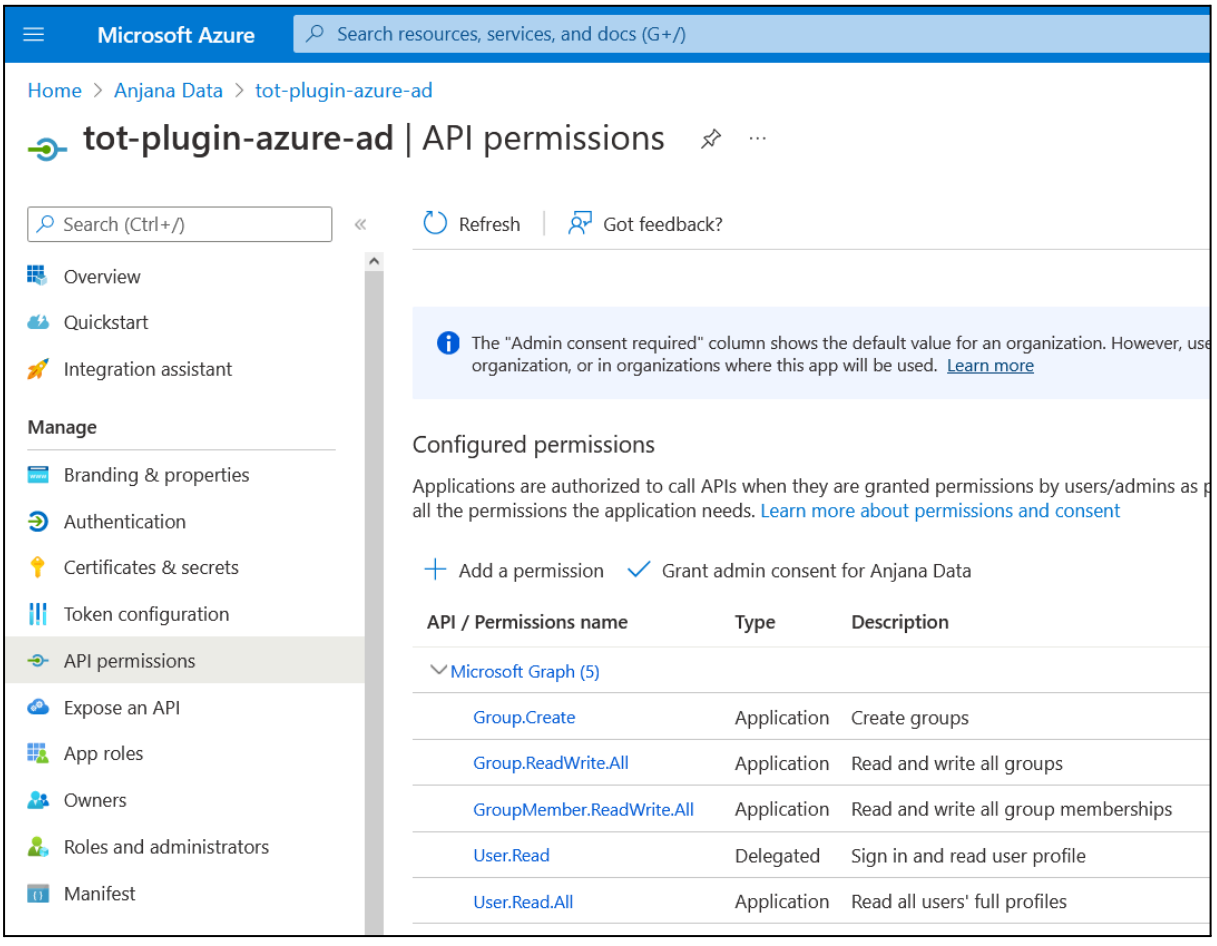
Es necesario registrar una aplicación en Azure AD y generar el necesario clientID y secret para que el plugin pueda autenticar y adquirir los permisos necesarios para cada funcionalidad.

Gobierno activo

La acciones realizadas por este plugin son las siguientes:

- Crear grupos: Se crearán grupos que representen a DSAs que pasen a estado aprobado. Para ello es necesario que la aplicación registrada tenga el permiso de “Group.Create” para poder crear los grupos.
- Lectura usuarios: Se requiere la lectura de los campos para realizar la membresía. Para ello la aplicación requiere el permiso “User.Read”.
- Añadir/Eliminar usuarios en grupos: En los grupos creados por el plugin se van a añadir y eliminar usuarios (el plugin no crea ni borra usuarios del Active Directory) en base a las adherencias y desadherencias sobre el DSA. Para ello la aplicación requiere los permisos “User.Read” para poder localizar los usuarios y “GroupMember.ReadWrite.All” para poder modificar los miembros del grupo con los usuarios localizados.
- Eliminar grupos: El plugin eliminará aquellos grupos que representen a DSA que pasen a estados expirados de forma automática en Anjana. Para ello la aplicación requiere el permiso “Group.ReadWrite.All” para poder borrar grupos.


Microsoft Azure
Home > Anjana Data
Anjana Data | App registrations
Azure Active Directory
Overview
Preview features
Diagnose and solve problems
Manage
Users
Groups
External Identities
Roles and administrators
Administrative units
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
New registration
Endpoints
Starting June 30th, 2020 we will no longer add any
upgraded to Microsoft Authentication Library (MS
All applications
Owned applications
tot
2 applications found
Display name
TO
tot-plugin-azure-ad
TO
tot-plugin-azure-storage


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Anjana Data > tot-plugin-azure-ad
tot-plugin-azure-ad | API permissions
Search (Ctrl+/)
Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Refresh
Got feedback?
The "Admin consent required" column shows the default value for an organization. However, use
organization, or in organizations where this app will be used. Learn more
Configured permissions
Applications are authorized to call APIs when they are granted permissions by users/admins as p
all the permissions the application needs. Learn more about permissions and consent
Add a permission
Grant admin consent for Anjana Data
API / Permissions name
Type
Description
Microsoft Graph (5)
Group.Create
Application
Create groups
Group.ReadWrite.All
Application
Read and write all groups
GroupMember.ReadWrite.All
Application
Read and write all group memberships
User.Read
Delegated
Sign in and read user profile
User.Read.All
Application
Read all users' full profiles

Edición de objetos

La acciones realizadas por este plugin son las siguientes:

- Leer grupos: Se hará una petición para leer los datos de los grupos que representen a DSAs. Para ello es necesario que la aplicación registrada tenga el permiso de “Group.Read.All” para poder leer los grupos.

Limitaciones Azure

El número máximo de usuarios en un grupo es de 100. Lo que significa que en un DSA que gobierne objetos en Azure no puede tener más de 100 personas adheridas (incluyendo owners), a partir de la 100 no se podrá aplicar gobierno activo.

El nombre del DSA (incluyendo el prefijo configurable) no debe contener los siguientes caracteres '@’, ‘(’, ‘)’, ‘\’, ‘[’, ‘]’, ‘;’, ‘:’, ‘<’, ‘>’ ni espacios en blanco ni superar los 64 caracteres (incluyendo el sufijo con la versión del dsa que incluye el plugin). Esta limitación sólo aplica si el DSA no tiene rellenado el campo del nombre físico y se espera que cree el grupo automáticamente.

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: 15009

totplugin:
   server:
    urls:
     - http://totserver:15000/tot/

   keep-alive-seconds: 60
 aris:
   - ari: "anja:totplugin:im:/microsoft/azure/ad/"
 connection:
   pathSeparator: "/"
   clientId: <clientId>
   tenantId: <tenantId>
   secret: <secret>
   scopes: "https://graph.microsoft.com/.default"
 groupPrefix: Dsa_

eureka:
 client:
   serviceUrl:
     defaultZone: http://totserver:15000/tot/eureka
```

- port: El puerto en el que se va a desplegar el plugin.

- keep-alive-seconds: Tiempo de espera entre intentos de registro del plugin
- pathSeparator: El símbolo que se usa como separador de path
- clientId: El id de la aplicación registrada para conectarse con Azure AD.
- tenantId: El tenant id de la suscripción de la cuenta de Azure.
- secret: La contraseña de la aplicación registrada para conectarse con Azure AD.
- scopes: El scope al que el plugin interactúa con Azure, en este caso con el graph de microsoft que es el encargado de los grupos y usuarios.
- groupPrefix: El prefijo que se concatena a los nombres de los grupos. El nombre completo del grupo lo formará el prefijo más el nombre y la versión.