Tot plugin SQL Server

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
1.2	05/12/2023	Anjana Producto	Anjana Producto	Añadido el detalle para la funcionalidad de la Edición de objetos de la integración
1.3	16/12/2023	Anjana Producto	Anjana Producto	Añadida la query para el borrado del usuario externo (el grupo del plugin IM)
2.0	29/01/2025	José González	Ana Melcón, Antonio Gómez, Lucía Engo, Alberto Montero	Revisión de textos para integración con Plugin de LDAP/AD

Modelo de integración

Extracción de metadatos

Para la extracción de metadata de un objeto se utilizan los métodos que ofrece el driver de JDBC mediante los cuales se accede a la definición de esquemas y tablas.

Extrae los siguientes atributos que deben llamarse igual en la tabla attribute_definition, campo name para que aparezcan en la plantilla.

- **catalog** con el valor de catalog en la base de datos
- **schema** con el valor de schema en la base de datos
- **physicalName** y name con el mismo valor, el nombre de la tabla
- **path** con la concatenación de los valores de catalog, schema and table
- **infrastructure** con el valor seleccionado
- **technology** con el valor seleccionado
- **zone** con el valor seleccionado

En caso de extraer el metadato para crear un dataset, también se extraerán los siguientes atributos relativos a los campos del recurso pedido para poder rellenar la información de su estructura:

- **physicalName** y **name** con el mismo valor, el nombre del campo
- **defaultValue** con el valor por defecto que se haya establecido al field
- **fieldDataType** con el tipo de dato asignado al field, si se ha establecido
- **length** con la longitud del campo, si se ha establecido.
- **incrementalField**
- **position** con el valor de la posición que ocupa el field
- **precision** con el valor de la precisión del campo, si se ha establecido
- **nullable** indicando si el field es anulable o no (valor booleano)
- **pk** indicando si el field es una clave primaria (valor boolean)
- **description** la descripción del dataset-field

Los atributos a crear en Anjana deben de tener los siguientes tipos:

Nombre de atributo	**Tipo de atributo**
catalog	INPUT_TEXT
schema	INPUT_TEXT
physicalName	INPUT_TEXT
path	INPUT_TEXT
infrastructure	SELECT
technology	SELECT
zone	SELECT
name	INPUT_TEXT
defaulValue	INPUT_TEXT

fieldDataType	INPUT_TEXT
length	INPUT_NUMBER
incrementalField	INPUT_CHECKBOX
position	INPUT_NUMBER
precision	INPUT_NUMBER
nullable	INPUT_CHECKBOX
pk	INPUT_CHECKBOX
description	ENRICHED_TEXT_AREA_INTERNATIONAL

El plugin es capaz de realizar la extracción de metadatos de los siguientes tipos de elementos y es configurable:

- Tabla de base de datos
- Vistas de base de datos

Muestreo de datos

Utilizando el driver JDBC se ejecuta una query con límite de registros sobre los campos definidos en el dataset en la que, adicionalmente, se sustituyen los valores de los campos sensibles por asteriscos.

Aquellos campos que se modifiquen después de crear el objeto en Anjana (es decir, que estén definidos en el metadato pero no se hayan incorporado en la estructura física) aparecerán como no disponibles en el muestreo.

Creación de estructuras

El plugin permite crear las estructuras físicas siempre que el objeto sea gobernado. Cuando esto ocurra y se valide el workflow asociado se creará la estructura en el path indicado del dataset. Una vez creado no se modificará aunque se generen nuevas versiones del dataset a no ser que se especifique un nuevo path.

Gestión de accesos

El plugin permite gestionar el acceso a aquellas estructuras que se gobiernen. Mediante el uso de roles y asociar permisos de SELECT sobre las estructuras al rol.

El plugin además permite gestionar la activación o desactivación de entidades no nativas, de modo que cuando una entidad no nativa se active se darán los permisos correspondientes en las tablas y cuando se desactive se eliminarán los permisos.

Dependiendo de la tecnología usada para gestionar los grupos se generan estos grupos de diferentes maneras:

- Entra ID
- Windows AD / LDAP
- Por defecto

Versiones soportadas

Soporte desde SQL Server 2014 a SQL Server 2012 y todas las versiones Cloud gracias al driver JDBC versión 12.6. Para más información consultar la matriz de compatibilidades de Microsoft.

Credenciales requeridas

Extracción de metadatos

Usuario o rol con permisos VIEW DEFINITION sobre las tablas o vistas de las que se quiera extraer el metadato.

También se puede aplicar sobre esquemas o base de datos directamente y aplicará a todo lo que contiene.

Query recomendada:

```
Unset
USE YourDatabase;
GRANT VIEW DEFINITION TO YourUsername;
```

Muestreo de datos

Usuario o rol con permisos SELECT sobre las tablas o vistas que se quieran obtener un muestreo de datos.

También se puede aplicar sobre esquemas o base de datos directamente y aplicará a todo lo que contiene.

Query recomendada:

```
Unset
USE YourDatabase;
GRANT SELECT ON SCHEMA::dbo TO YourUsername;
```

Creación de estructuras

Usuario con los siguientes permisos/roles necesarios sobre los catálogos, esquemas y tablas que se quieran gobernar.

- CREATE TABLE

Los nombres utilizados para crear los recursos en SQL Server están sujetos a las restricciones impuestas por el mismo SQL Server para cada uno de ellos.

Query recomendada:

```
Unset
USE YourDatabase;
GRANT CREATE TABLE TO YourUsername;
GRANT CREATE VIEW TO YourUsername;
```

Gestión de accesos

Usuario con los siguientes permisos necesarios sobre los catálogos, esquemas y tablas que se quieran gobernar.

- CREATE ROLE
- ALTER ANY ROLE
- CONTROL (opcional si la propiedad del rol se cede a tercero)
- SELECT ON OBJECT

Gestión de accesos mediante Windows AD

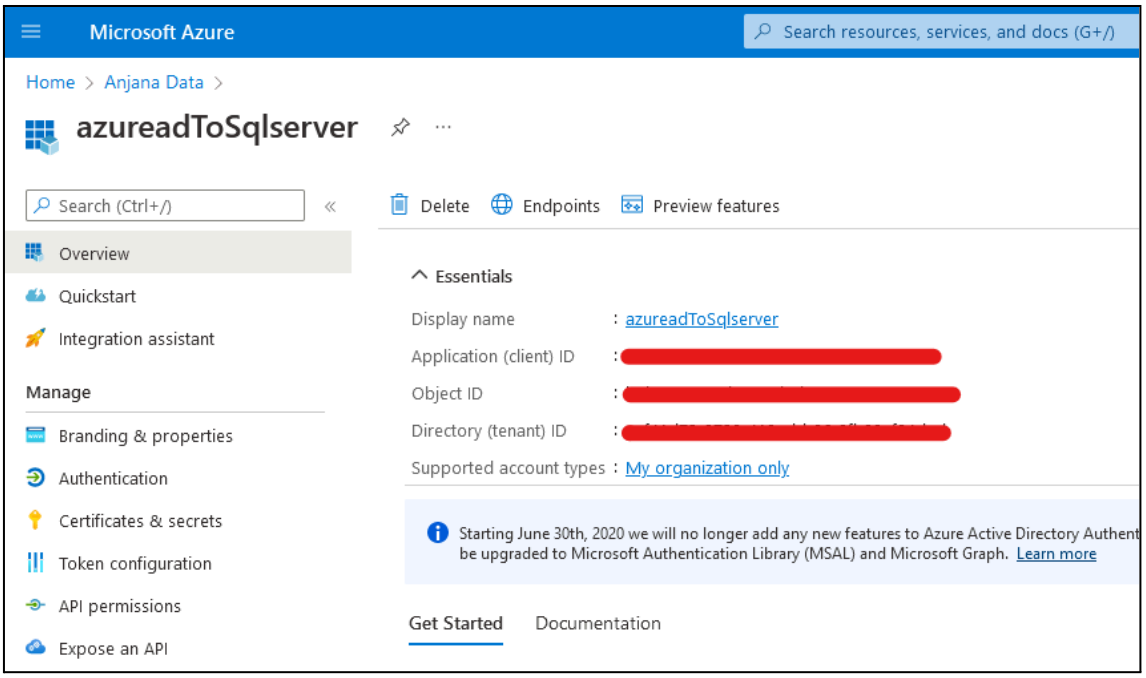
Para el usuario usado para la conexión del Plugin si se usa SQLServer con Windows AD se puede gestionar con estas queries:

```
Unset
-- Agregar al rol securityadmin
ALTER SERVER ROLE securityadmin ADD MEMBER [nombre_usuario];

-- Otorgar permisos a nivel de base de datos
USE [nombre_base_datos];
GRANT ALTER ANY USER TO [nombre_usuario];
GRANT CONTROL ON DATABASE::[nombre_base_datos] TO [nombre_usuario];

-- Agregar al rol db_owner
ALTER ROLE db_owner ADD MEMBER [nombre_usuario];
```

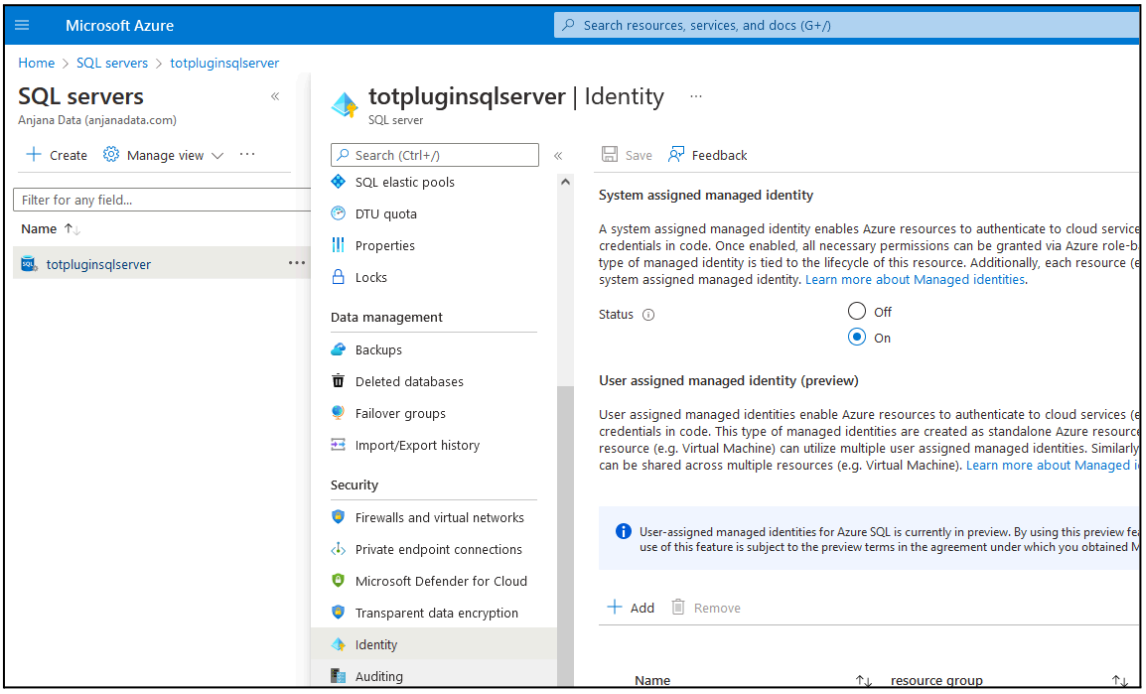
Gestión de accesos mediante Azure AD

Si el gobierno activo se va a realizar con Azure AD hay que realizar los siguientes pasos:

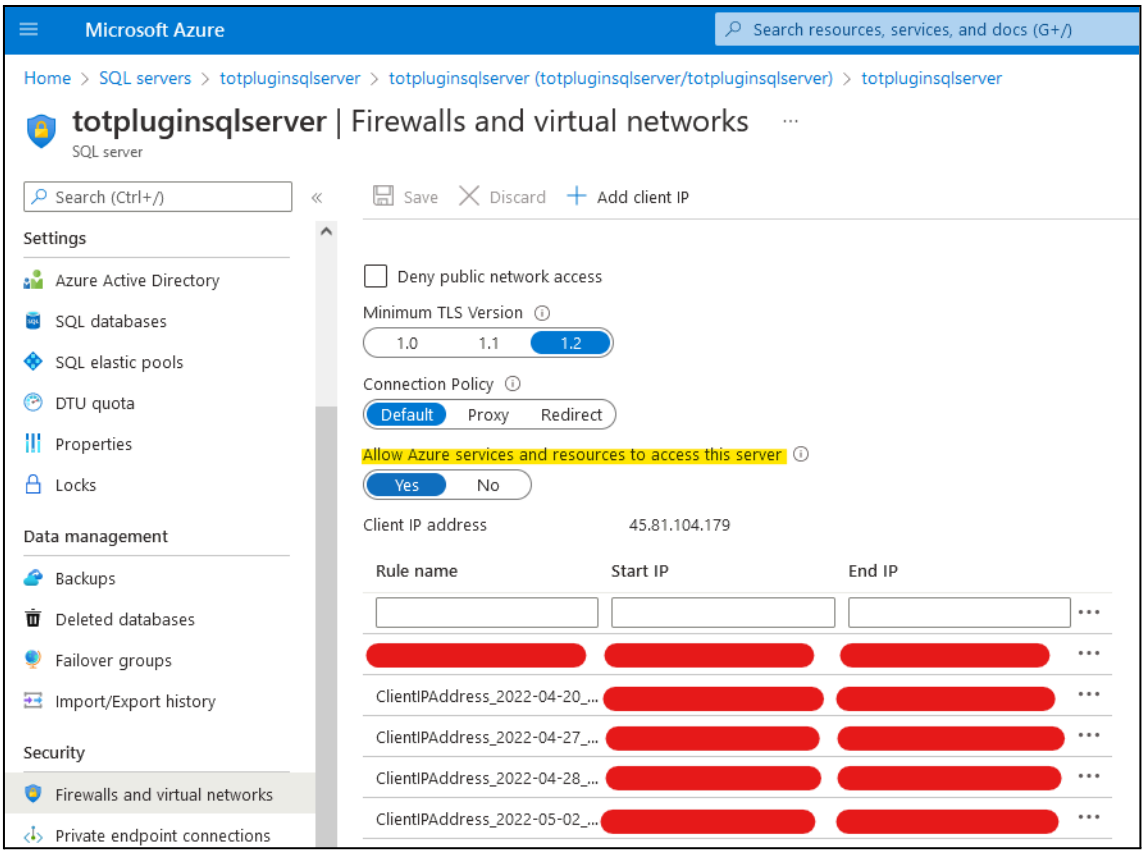
1. Crear una APP en Azure AD para que actúe de service principal y generar un secret



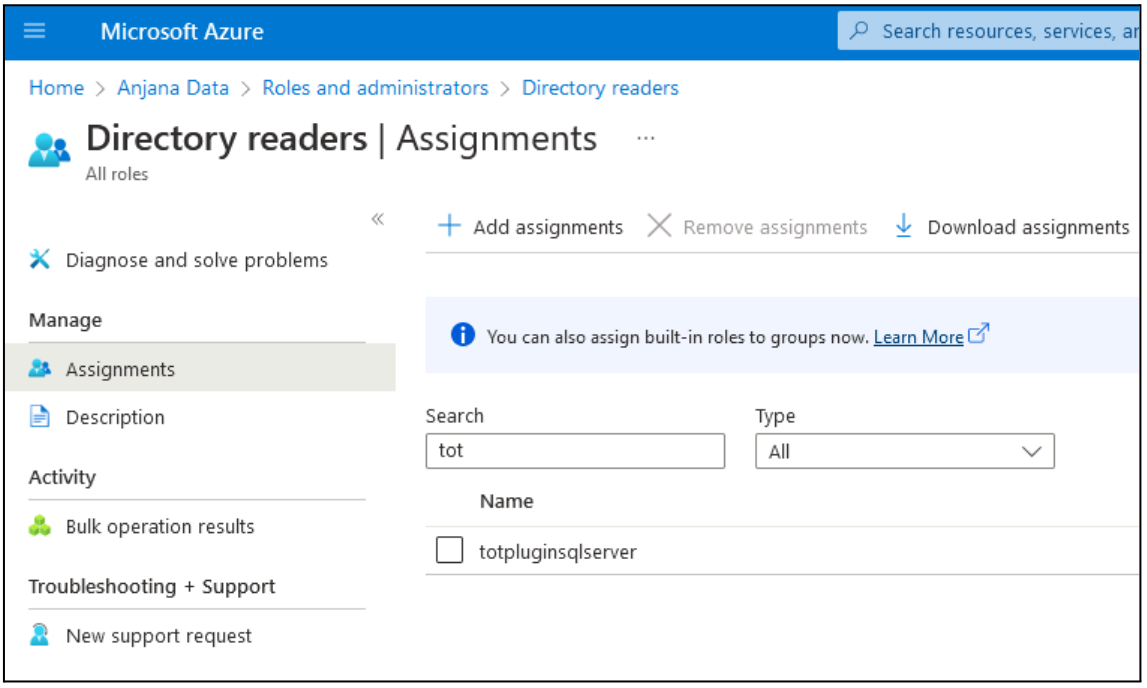
2. Activar en Identity del servidor de SQL la opción “System assigned managed identity”



3. Permitir a los servicios de Azure a acceder al servidor SQL



4. Dar permiso a la identidad del servidor SQL a acceder al directorio de Azure AD



5. En SQL hay que darle permisos al service principal de la APP que usamos en el plugin de Azure AD

```
Unset
-- LOGIN
CREATE USER [<app-name>] FROM EXTERNAL PROVIDER;

-- ADD PERMISSIONS TO [<app-name>]
ALTER ROLE db_XXXX ADD MEMBER [<app-name>];

GO
```

Despliegue

Se ha de seguir el manual genérico de Tot despliegue de plugins.

Configuración

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

Todas las propiedades tienen valores por defecto que se indican en los ejemplos, excepto los parámetros de credenciales.

```
Unset
server:
 port: 15005
```

Esta propiedad indica el puerto en el que se va a desplegar el plugin

```
Unset
totplugin:
  connection:
    url: jdbc:sqlserver://rdbservice:1433;database=<db>
    user: <user>
    password: <pwd>
    serverName: totpluginsqlserver.database.windows.net
    databaseName: totpluginsqlserver
    principalId: asdfasdas-asdf-asdf-asdf-14befd853df0
    principalSecret: asdfasdf~asdfasdf.asdfasdfas.JK~bEG
```

Los parámetros de credenciales se dividen en dos bloques:

- Url, databaseName, user y password, son credenciales de conexión a la BD, se deben usar cuando se conecte contra un SQL Server.
- ServerName, databaseName, principalId y principalSecret son credenciales contra un Azure SQL Server.

No deberían estar ambos bloques rellenos a la vez, en caso de que se haga, se ignorará todo lo relacionado con Azure y solo se intentará conectar al SQL Server.

```
Unset
totplugin:
 connection:
   path-separator: "/"
   using-catalogs: false
   using-schemas: true
   sampleRows: 15
   imType: EID
   imDomain:
   forceSync: false
   exportationTypes:
     - TABLE
     - VIEW
 rolePrefix: "_role"
 azureCountRetry: 5
 azureWaitRetry: 15
```

El siguiente bloque de configuración es sobre cómo se interpreta la información de Anjana y cómo se navega por el SQL Server.

“using-catalogs” y “using-schemas” determina el nivel desde el que se gobierna el SQL Server y cómo se interpretan los path de las estructuras que se quieren gobernar desde Anjana, si ambos están a false solo muestran el schema por defecto o el elegido en la url de conexión. (EX: using-catalogs a false y using-schemas a true indican que se quiere gobernar todos los esquemas que se tenga acceso y siempre dentro del mismo catálogo o base de datos)

“path-separator” va a indicar el separador utilizado por parte de Anjana para el path. (EX: Si es “/” la tabla empleados en el esquema de hr se espera que llegue desde anjana como hr/empleados). El plugin transforma el path en una estructura correcta para SQL Server por lo que, si no se especifica correctamente, se intentarán crear recursos erróneos produciéndose un error.

“sampleRows” indica el número de filas que se recuperan para la funcionalidad de sampleo de datos.

“imType” indica que tipo de gestor de identidades externo a SQLServer se usa, los posibles valores son:

- EID para EntraID (antiguo AzureAD), por defecto se usa este
- AD para Windows AD o LDAP
- NONE para usar SQLServer puro

“imDomain” se usa para indicar sobre que dominio del gestor de identidades se va a trabajar, no llevar valor por defecto y no es necesario usarlo si en “imType” coge valor *NONE.*

“forceSync” se usa para forzar la sincronización entre SQLServer y AD/EID para entornos que puedan tener por su naturaleza o configuración cierto retraso entre las sincronización entre las tecnologías. Por defecto a false.

“exportationTypes” contiene una lista de tipos de tabla que se pueden exportar, siendo los valores aceptados TABLE y VIEW. Al menos una debe de estar y el valor por defecto son ambas.

Al crear roles nuevos en SQL Server para asignar permisos sobre las que tablas que se quiera gobernar con ese rol se usa “rolePrefix” para indicar el sufijo que se quiere sobre el nombre del rol. Si no se quiere que tenga un sufijo es necesario incluir la variable en el yml sin ponerle valor.

En el proceso de creación de un rol y sus permisos existen una serie de reintentos y espera entre los reintentos, para configurar dichos reintentos se usan “azureCountRetry” y “azureWaitRetry”

ImAri disponibles

- Azure
- Ldap