



Tot plugin SQL Server

<b>Control de versiones</b>	<b>2</b>
<b>Modelo de integración</b>	<b>2</b>
Extracción de metadatos	3
Tipos soportados	3
Muestreo de datos	3
Creación de estructuras	4
<b>Credenciales requeridas</b>	<b>4</b>
Extracción de metadatos	4
Muestreo de datos	4
Creación de estructuras	4
Gestión de accesos	4
Gestión de accesos mediante Azure AD	4
<b>Despliegue</b>	<b>7</b>
<b>Configuración</b>	<b>7</b>
<b>ImAri disponibles</b>	<b>8</b>

## Control de versiones

Versión	Fecha de modificación	Responsable	Aprobador	Resumen de cambios
1.0	28/10/2022	Anjana Producto	Anjana Producto	Creación del documento

# Modelo de integración

## Extracción de metadatos

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.

## Tipos soportados

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

- Tabla de base de datos

## Muestreo de datos

Utilizando el driver JDBC se ejecuta una query sobre los campos definidos en el dataset en la cual adicionalmente se sustituyen los valores de los campos sensibles por asteriscos.

Aquellos campos que estén definidos en el metadato pero no se hayan incorporado en la estructura física (por ejemplo cuando se ha versionado pero no se ha cambiado el path del mismo) aparecerán como no disponibles.

## Creación de estructuras

El plugin permite crear las estructuras físicas siempre que el dataset 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.

## Credenciales requeridas

### Extracción de metadatos

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

- VIEW DEFINITION

### Muestreo de datos

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

- SELECT

### 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.

## Gestión de accesos

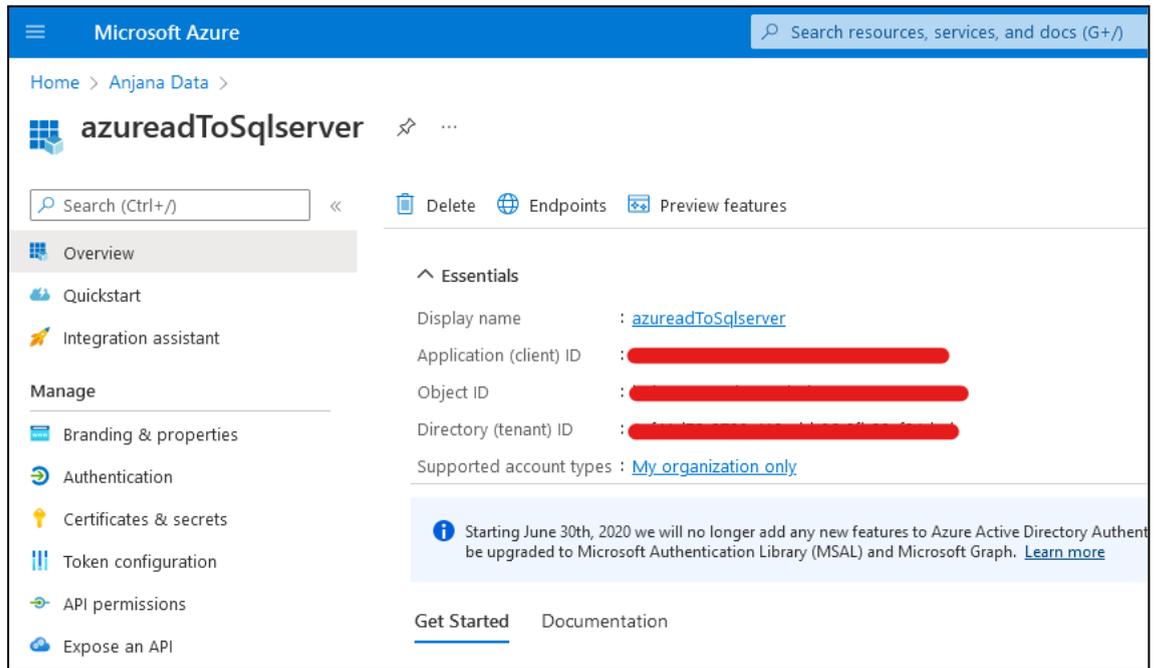
Usuario con los siguientes permisos necesarios sobre los catálogos, esquemas y tablas que se quieran gobernar.

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

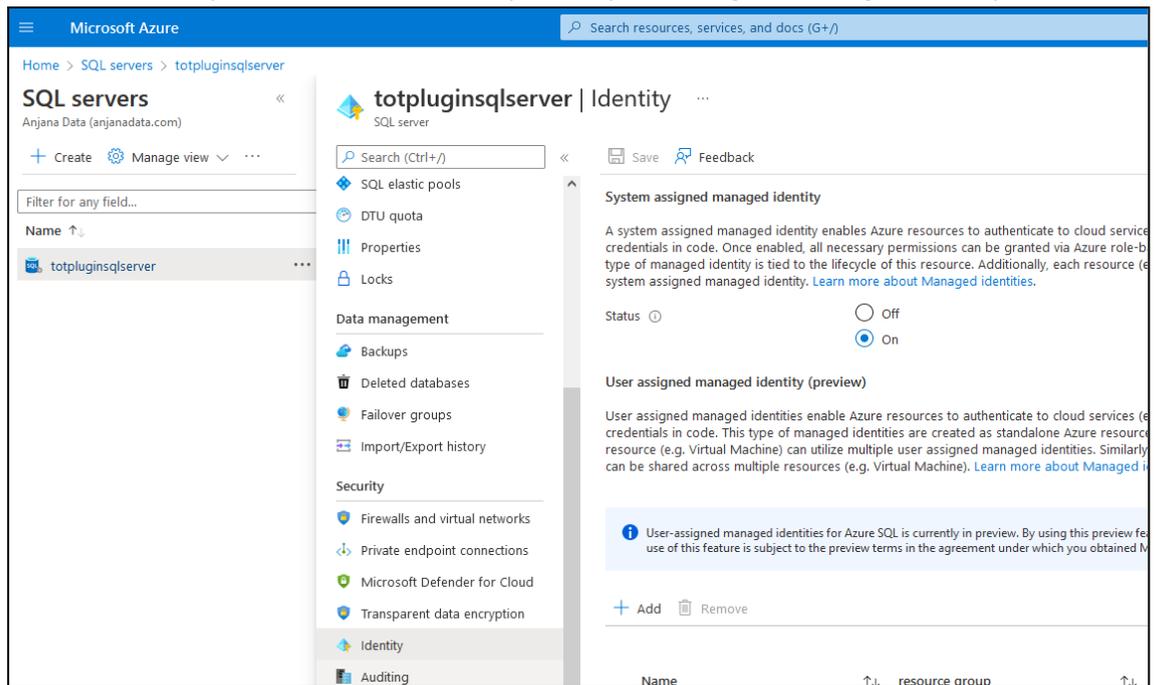
## Gestión de accesos mediante Azure AD

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

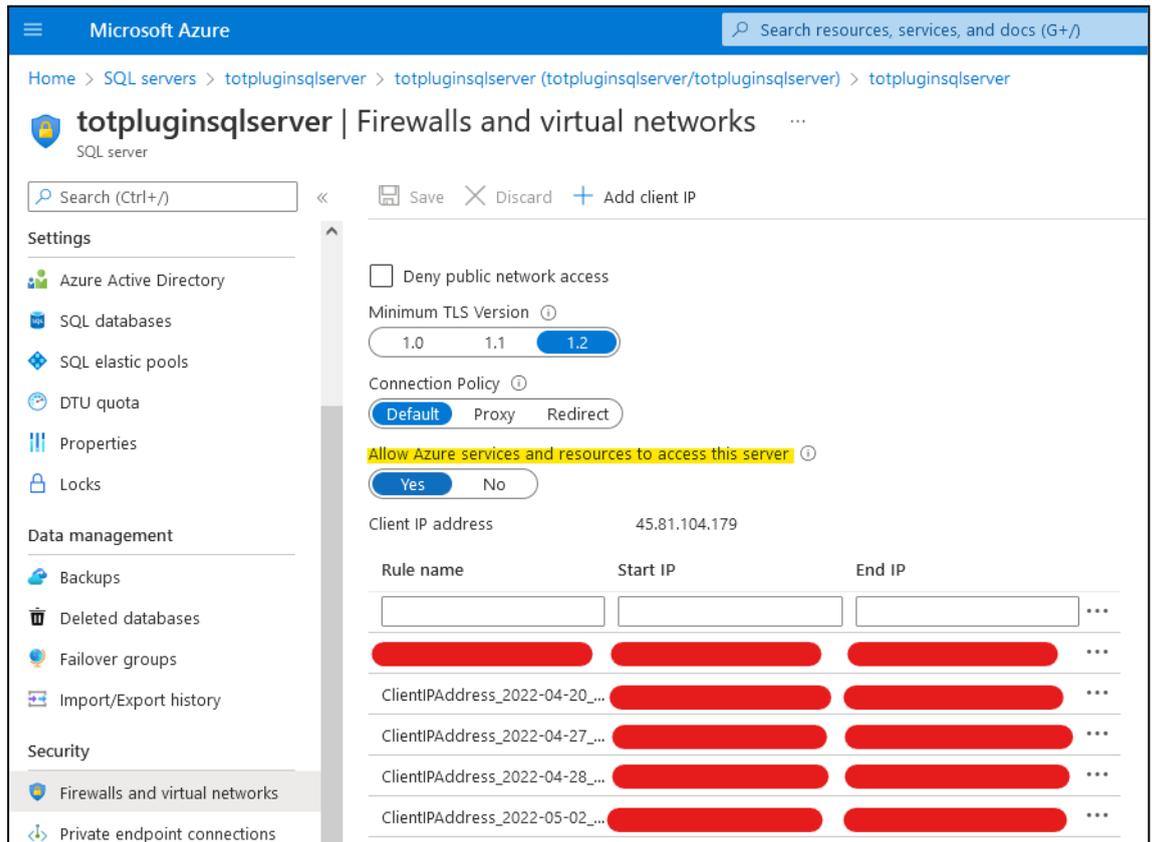
1. Crear una APP en Azure AD para que actúe de service principal y generar un secret



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

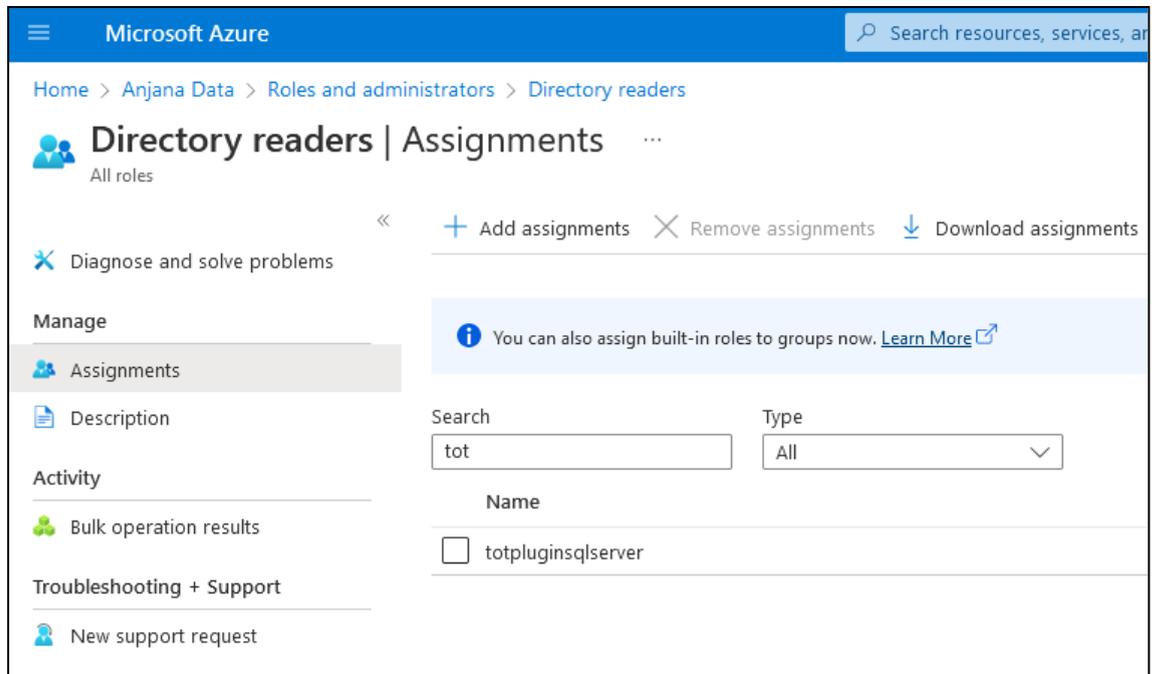


3. Permitir a los servicios de Azure a acceder al servidor SQL



The screenshot shows the Azure portal interface for configuring a firewall rule on a SQL server. The breadcrumb path is: Home > SQL servers > totpluginsqlserver > totpluginsqlserver (totpluginsqlserver/totpluginsqlserver) > totpluginsqlserver. The page title is 'totpluginsqlserver | Firewalls and virtual networks'. The left sidebar shows navigation options like Settings, Data management, and Security. The main content area shows the 'Firewalls and virtual networks' settings for the selected server. Key settings include: 'Deny public network access' (unchecked), 'Minimum TLS Version' set to 1.2, 'Connection Policy' set to Default, and 'Allow Azure services and resources to access this server' set to Yes. A table lists existing firewall rules, including several 'ClientIPAddress' rules with red bars indicating they are blocked.

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



The screenshot shows the 'Directory readers | Assignments' page in the Azure portal. The breadcrumb path is: Home > Anjana Data > Roles and administrators > Directory readers. The page title is 'Directory readers | Assignments'. The left sidebar shows navigation options like Manage, Activity, and Troubleshooting + Support. The main content area shows the 'Assignments' section with a search bar containing 'tot' and a 'Type' dropdown set to 'All'. A table lists assignments, with one entry for 'totpluginsqlserver' that is currently unchecked.

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

```
-- 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 del despliegue de plugins.

Doc: Anjana Data x.x - DOC - Tot despliegue de plugins

## Configuración

Se han de revisar las configuraciones comunes en el doc de configuraciones “Anjana Data - Microservices configuration”

Configuraciones específicas:

- Database url, username and password:
  - url: jdbc:sqlserver://<database\_host>:<port>;database=<database>
  - user: sa
  - password: <password>
  - using-catalogs: false
  - using-schemas: true
  - path-separator

Si “using-catalogs” y “using-schemas” están a false, solo muestran el schema por defecto o el elegido en la url de conexión.

using-schemas lista todas las tablas de todos los esquemas que tenga acceso

path-separator va a indicar el separador utilizado por parte de Anjana para el path.

El plugin transforma el path en una estructura correcta para SQL Server por lo que si no se especifica correctamente se intentará crear recursos erróneos produciéndose un error.

El parámetro groupPrefix indica el prefijo que tiene el nombre del grupo, su valor debe de ser el mismo que el plugin que haga las funciones de active directory.

Config file:

```
server:  
  port: 15005  
totplugin:  
  location: http://totpluginjdbcsqlserverserver:15005/plugin/sqlserver/api/v1  
server:  
  url: http://totserver:15000/tot/  
connection:  
  url: jdbc:sqlserver://rdbservice:1433;database=anjana  
  path-separator: "/"
```

```
using-catalogs: false
using-schemas: true
#Connection with user & password
user: sa
password: anjana
#Connection with ActiveDirectoryServicePrincipal
serverName: totpluginsqlserver.database.windows.net
databaseName: totpluginsqlserver
principalId: asdfasdas-asdf-asdf-14befd853df0
principalSecret: asdfasdf~asdfasdf.asdfasdfas.JK~bEG
aris:
- ari: "anja:totplugin:extract:/jdbc/mssqlserver/mssqlserver/"
- ari: "anja:totplugin:sample:/jdbc/mssqlserver/mssqlserver/"
- ari: "anja:totplugin:create:/jdbc/mssqlserver/mssqlserver/"
- ari: "anja:totplugin:im:/jdbc/mssqlserver/mssqlserver/"
  imAri: "anja:totplugin:im:/azure/ad/zoneazure/"
groupPrefix: Dsa_
```

## ImAri disponibles

- Azure
- Ldap

Por defecto el plugin considera que se conecta a un AzureAD y hace el enlace entre el usuario de Sql Server y AzureAD. Si se utilizara otro AD distinto hay que especificar la siguiente configuración:

```
totplugin:
  sql:
    query-pattern:
      createFromExternalProvider: "CREATE USER [DOMAIN\{0}] FROM EXTERNAL PROVIDER WITH
DEFAULT_SCHEMA = [{1}]"
```

Siendo DOMAIN el dominio del AD