



Tot plugin PowerBI

Control de versiones	3
Servicios disponibles en el plugin	4
Modelo de integración	4
Extracción de metadatos	4
Gestión de accesos (En Roadmap)	5
Credenciales requeridas	5
Extracción de metadatos	5
Gestión de accesos (En Roadmap)	7
Configuración	7
Anexos	8
Asignación grupo a Report	8
Asignación de grupos a Dashboard	10
Asignación de grupo a Modelo Semántico	12
Asignación de grupo a APP	14

Control de versiones

Versión	Fecha modificación	Responsable	Aprobador	Resumen de cambios
1.0	30/08/2024	Jose Angel González	Ana Melcón	Creación del documento
2.0	24/12/2024	Alberto Montero	Ana Melcón	Se añade punto 3

Servicios disponibles en el plugin

- Listado y extracción de metadatos
- Gestión de accesos (delegada sobre AzureAD)(en Roadmap)

Modelo de integración

Extracción de metadatos

Para la extracción de metadata de un objeto se utilizan las APIs:

- <https://learn.microsoft.com/en-us/rest/api/power-bi/admin/groups-get-groups-as-admin>
- <https://learn.microsoft.com/en-us/rest/api/power-bi/admin/apps-get-apps-as-admin>

Con estas APIs el plugin es capaz de extraer los siguientes tipos de objeto de PowerBI:

- APP
- Dataset (modelo de datos)
- Report
- Dashboard

El plugin extrae los siguientes atributos, que deben llamarse igual en la tabla attribute_definition, (campo name) para que aparezcan en la plantilla:

Nombre de atributo	Tipo de atributo	Descripción
physicalName, name	INPUT_TEXT	nombre del objeto
path	INPUT_TEXT	ruta al objeto
infrastructure	SELECT	valor seleccionado
technology	SELECT	valor seleccionado
zone	SELECT	valor seleccionado

Además, la propia API de Azure permite extraer más atributos de los objetos con lo que, si se incluyen estos atributos en la plantilla del objeto, la extracción completará su valor. En caso de duda del valor devuelto para un atributo, el tipo INPUT_TEXT siempre aceptará insertar cualquier valor.

NOTA: El atributo ID presente en todos los objetos de PowerBI no puede ser configurado en Anjana Data por el momento al ser un identificador interno de la aplicación

Para más detalles sobre los atributos que potencialmente se pueden extraer de cada objeto consultar los siguientes enlaces.

Dashboard:

<https://learn.microsoft.com/en-us/rest/api/power-bi/admin/groups-get-groups-as-admin#admindashboard>

Dataset (modelo de datos) :

<https://learn.microsoft.com/en-us/rest/api/power-bi/admin/groups-get-groups-as-admin#admindataset>

App:

<https://learn.microsoft.com/en-us/rest/api/power-bi/admin/apps-get-apps-as-admin#adminapp>

Report:

<https://learn.microsoft.com/en-us/rest/api/power-bi/admin/groups-get-groups-as-admin#adminreport>

Gestión de accesos (En Roadmap)

Dado que la API de PowerBI no tiene accesible la gestión de accesos, la única manera de hacerlo posible es mediante la delegación de estos a través de AzureAD. Para ello habrá dos actuaciones manuales requeridas para que este mecanismo funcione:

1. Asignación de permisos:
 - a. Crear un DSA y añadir objetos de Power BI.
 - i. En el campo `physical_name` deberá informarse el nombre del grupo.
 - b. Este grupo habrá que asignarlo a cada objeto de Power BI (mirar [Anexos](#))
2. Sincronización:
 - a. El proceso de sincronización entre Azure y PowerBI no es automático ni instantáneo.
 - b. Forzarlo si es posible

Credenciales requeridas

Extracción de metadatos

Se necesitan los siguientes permisos:

- Tenant.Read.All

Estos permisos se deben dar sobre el service principal que se vaya a usar para el cometido del plugin. Estos permisos no pueden ser consentimiento de Administración si no que tienen que ser permisos delegados:

1. Configuración del App Registration
 - a. Ir al Azure Portal.
 - b. Navegar a Azure Active Directory > App registrations > + New registration.
 - c. Proporcionar un nombre para la aplicación y seleccionar el tipo de cuenta (lo más común es Accounts in this organizational directory only).
2. Configurar los Permisos API
 - a. Dentro de la App Registration, navegar a API permissions.
 - b. Hacer clic en + Add a permission.
 - c. Seleccionar Microsoft Power BI.
 - d. Seleccionar **Delegated permissions** (no Application permissions).
 - e. Buscar y seleccionar los permisos que la aplicación necesita mencionados anteriormente.
3. Generar un grupo de seguridad en Azure específico para consumir las APIs de PowerBI
 - a. Meter dentro del grupo la APP generada

- b. Meter al grupo dentro de la siguiente opción existente en PowerBI (ver captura)

Configuración de la **API** de administración

- 4 Las entidades de servicio pueden acceder a las **API** de administración de solo lectura
Habilitado para un subconjunto de la organización

Las aplicaciones web registradas en Microsoft Entra ID pueden usar entidades de servicio, en lugar de credenciales de usuario, para autenticarse en las **API** de administración de solo lectura.

- Para permitir que una aplicación use una entidad de servicio como método de autenticación, la entidad de servicio debe agregarse a un grupo de seguridad permitido. Las entidades de servicio incluidas en los grupos de seguridad permitidos tendrán acceso de solo lectura a toda la información disponible a través de las **API** de administración, que puede incluir nombres de usuario y correos electrónicos, y metadatos detallados sobre modelos semánticos e informes. [Más información](#)

☒ Habilitado


Aplicar a:

☐ Toda la organización

☒ Grupos de seguridad específicos

g gr-gob-azure-poc-purview-readers-pro x

g gr-gob-azure-powerbi-contributors x



☐ Excepto grupos de seguridad específicos

- c. Meter en Powerbi a la Aplicación generada en el punto 1 dentro del grupo de seguridad

NOTA: En la mayoría de escenarios no es necesario la concesión de permisos delegados (*Tenant.Read.All*) siempre y cuando cumplamos con el punto 3 anteriormente descrito

Los endpoint utilizados para realizar la extracción de los objetos de PowerBI son los siguientes:

- APP

<https://learn.microsoft.com/en-us/rest/api/power-bi/admin/apps-get-apps-as-admin>

- Dataset (modelo de datos)

<https://learn.microsoft.com/en-us/rest/api/power-bi/admin/datasets-get-datasets-as-admin>

- Report

<https://learn.microsoft.com/en-us/rest/api/power-bi/admin/reports-get-reports-as-admin>

- Dashboard

<https://learn.microsoft.com/en-us/rest/api/power-bi/admin/dashboards-get-dashboards-as-admin>

Gestión de accesos (En Roadmap)

Para la gestión de accesos el usuario encargado de la asignación de un grupo a un objeto de PowerBI (dentro de la aplicación de PowerBI) deberá tener permiso de **Owner o Member sobre el Workspace** donde reside el objeto o desde el que se publica una App.

Configuración

Para la configuración del plugin será necesario tener disponible las siguientes propiedades:

- *TenantId*: tenant sobre el que se va a actuar en la integración
- *ClientId*: *Id de la aplicación que se ha registrado (ver apartado [Credenciales Requeridas](#))*
- *ClientSecret*(*el value no el Id del secret*): serán las claves de acceso con las que se comunicará el plugin, estas deben de ser de un service principal

Además será necesario tipar en el YAML una conversión de subtipos de objeto de Anjana con los tipos de objeto PowerBI que se pueden extraer, deberán estar escritos de la misma manera que aparecen en la tabla `object_subtype` del esquema anjana de base de datos. Los tipos de objeto son los descritos en [Modelo de integración](#).

Ejemplo YML de configuración del plugin.








```
server:
  port: 15016

totplugin:
  server:
    urls:
      - http://tot1server:15000/tot/
  aris:
    - ari: "anja:totplugin:extract:/Azure/PowerBI/Cliente/"
  connection:
    tenant: <tenant-id>
    clientId: <client-id>
    clientSecret: <client-secret>
  mapping:
    app: POWERBI-APP
    dashboard: POWERBI-DASHBOARD
    report: POWERBI-REPORT
    semantic-model: POWERBI-MODEL

eureka:
  instance:
    hostname: totpluginpowerbi1server
  client:
    serviceUrl:
      defaultZone: http://hecate1server:15000/tot/eureka
```

Anexos

Asignación grupo a Report

	Name		Type	Owner
	Carga_Incremental_Todo_Imported_Mism...	 	Report 1	Wkp1
	Carga_Incremental_Todo_Imported_Mismo_Modelo_No		Explore this data (preview)	Wkp1
	Prueba_composite_model_and_roles_demo_limpio		Analyze in Excel	Wkp1
	Prueba_composite_model_and_roles_demo_limpio		Delete	Wkp1
			Quick insights	
			Save a copy	
			Settings	
			View usage metrics report	
			View lineage	
			Create paginated report	
			Manage permissions 2	
			Move to	

Related content

Dashboards

Workbooks

Semantic models

+ Add user

1

Links

Direct access

2

Ending

Shared views

People and groups with access

Email Address

LM

Link: Microsoft Customer

NA

Microsoft Analytics

Grant people access

X

Q dsa

3

D

Dsa_18SeptSqlServer_v0

D

Dsa_ActorSqlServerAd_v1

D

Dsa_azure_ad_10685_v0

D

Dsa_AZURE_EXP_v0

D

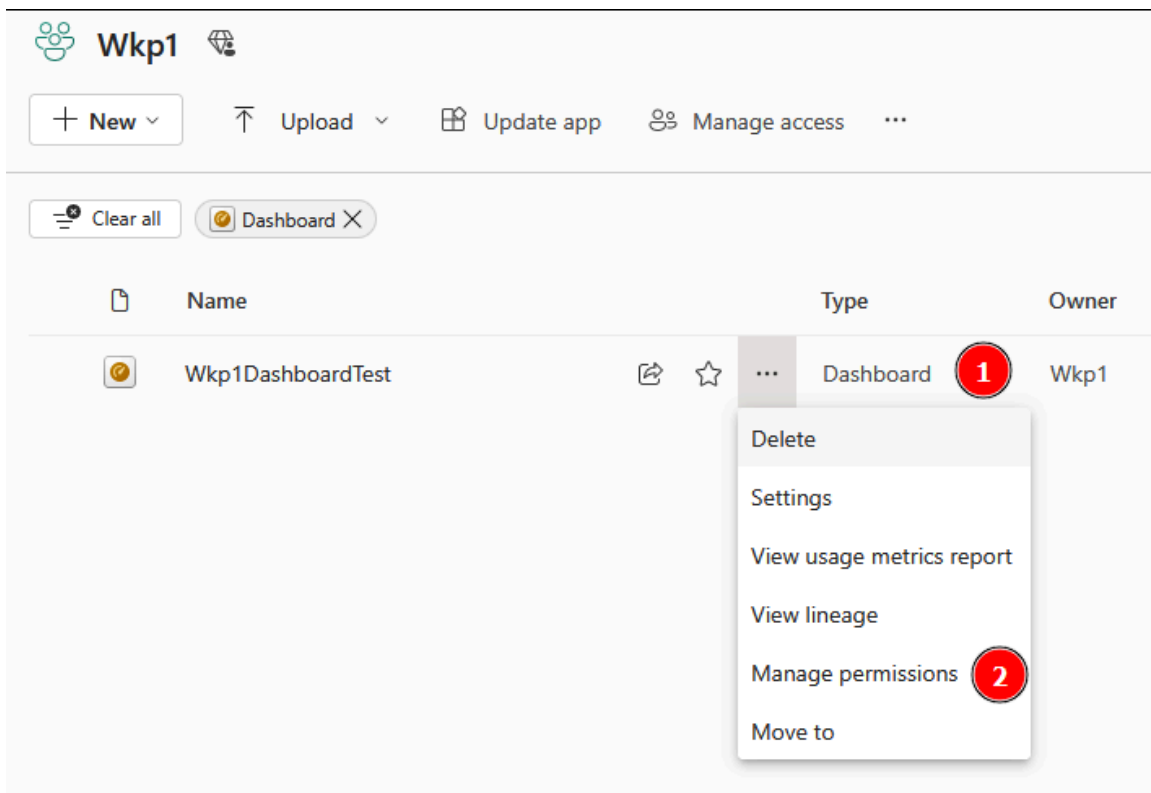
Dsa_AzureBeaCOCO_v0

4

Grant access

Cancel

Asignación de grupos a Dashboard



The screenshot displays the 'Wkp1' dashboard management interface. At the top, there are buttons for '+ New', 'Upload', 'Update app', 'Manage access', and a menu icon. Below these, there are filters for 'Clear all' and 'Dashboard'. A table lists the dashboards with columns for Name, Type, and Owner. The first entry is 'Wkp1DashboardTest', which is a 'Dashboard' owned by 'Wkp1'. A context menu is open for this entry, showing options: Delete, Settings, View usage metrics report, View lineage, Manage permissions (highlighted with a red circle '2'), and Move to. A red circle '1' is also placed over the 'Dashboard' type and the 'Wkp1' owner text.

Name	Type	Owner
Wkp1DashboardTest	Dashboard	Wkp1

- Delete
- Settings
- View usage metrics report
- View lineage
- Manage permissions
- Move to

+ Add user

1

2

Direct access

Pending

People and groups with access

Email Address

Grant people access

Q dsa

3

Enter a name or email address

D Dsa_18SeptSqlServer_v0

D Dsa_ActorSqlServerAd_v1

D Dsa_azure_ad_10685_v0

D Dsa_AZURE_EXP_v0








D Dsa_AzureBeaCOCO_v0

4

Grant access

Cancel

Asignación de grupo a Modelo Semántico

	Name	Type	Owner
	Carga_Incremental_Todo_Imported_Mismo_Modelo_No_Co...	Report	Wkp1Pro
	Carga_Incremental_Todo_Imported_Mism...  	...	Semantic model 1 Wkp1Pro
	Prueba_composite_model_and_roles_demo_limpio	Explore this data (preview)	Wkp1Pro
	Prueba_composite_model_and_roles_demo_limpio	Analyze in Excel	Wkp1Pro
		Create report	
		Auto-create report	
		Create paginated report	
		Delete	
		Quick insights	
		Security	
		Rename	
		Open data model	
		Settings	
		Download this file	
		Manage permissions 2	

+ Add user

1

Links

Direct access

2

People and groups with access

Email Address

Grant people access

X

Q dsa

3

D Dsa_18SeptSqlServer_v0

D Dsa_ActorSqlServerAd_v1

D Dsa_azure_ad_10685_v0

D Dsa_AZURE_EXP_v0

D Dsa_AzureBeaCOCO_v0

Add a message (Optional)

4





Grant access

Cancel

Asignación de grupo a APP

Apps

Apps are collections of dashboards and reports in one easy-to-find place.

	Name		Publisher
	Wkp1App	1 	Luis Moran Cuenca
	Microsoft Fabric Capacity Metrics	<div><div>Edit</div><div>Delete</div><div>2 Manage permissions</div><div>Settings</div></div>	

Wkp1App

1

+

Add user

Manage audiences

2

Direct access

Pending requests

Pending invitations

People and groups with access	Email Address	Audiences	Options
<div><div></div><div>Workspace users</div></div>		All	
<div><div></div><div></div></div>		Wkp1App	...
<div><div></div><div></div></div>		Wkp1App	...
<div><div></div><div></div></div>		Wkp1App	...

Grant access

×

Add a person or security group to an audience to give them access to this app.

Audience

3

Wkp1App

Add people

4

D

Dsa_18SeptSqlServer_v0

Enter a name or email

5

Grant access

Cancel