

Lab: Integrating Microsoft Purview with Microsoft Fabric and Implementing Data Catalog

Objective:

This lab aims to demonstrate the integration of Microsoft Purview with Microsoft Fabric, enabling automatic metadata discovery, data lineage tracking, and the creation of a centralized data catalog for Fabric assets. Participants will learn how to connect Fabric to Purview, scan Fabric workspaces, browse the catalog, and understand the benefits of a unified data governance solution.

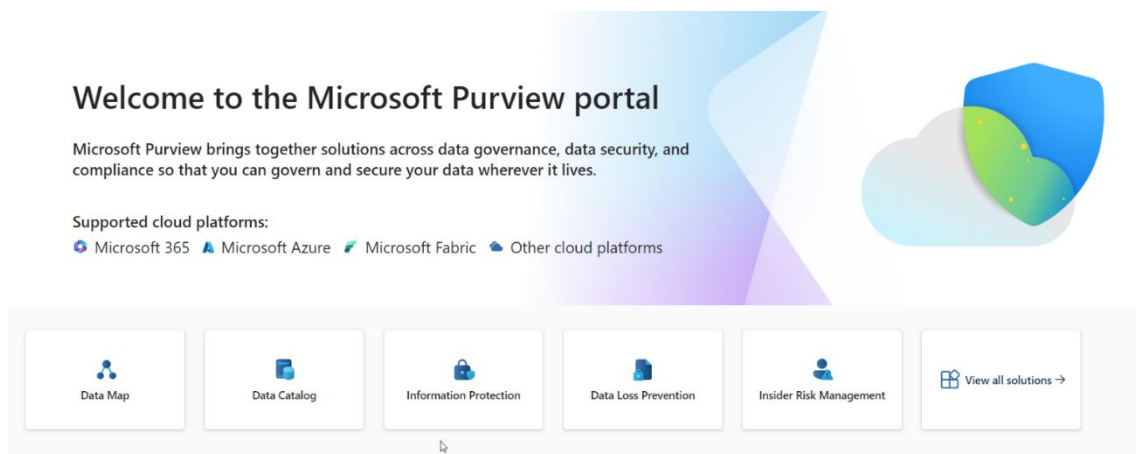
Tasks:

1. Connect Microsoft Fabric to Microsoft Purview
2. Scan Fabric Workspaces and Ingest Metadata

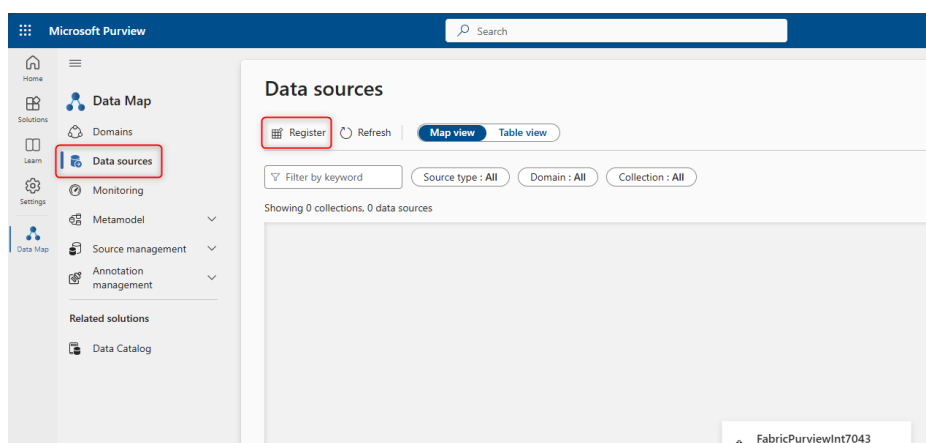
Task 1: Connect Microsoft Fabric to Microsoft Purview

Register Fabric tenant:

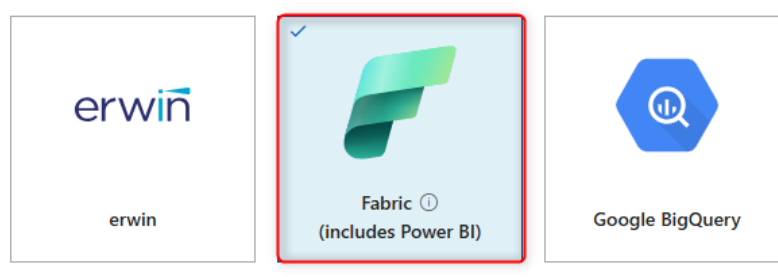
1. Open the new purview portal (purview.microsoft.com) in a browser window.
2. While you are in the Microsoft Purview Home page, Select **Data Map**



3. On the left side navigation pane, select **Data Sources** and then select **Register**.



4. Select **Fabric** as your data source and click on **Continue**.



5. Give your Fabric instance a friendly name
 - a. Data source name – FabricDatasource.
 - b. Select **Register**. The data source is added successfully.

Register data source (Fabric)

Data source name *

Fabric-DataSource

Tenant ID *


2c9aff69-db95-4dd0-8e23-de858458994a

Domain *

 FabricPurviewInt

Collection * ⓘ

Select domain only

 All items in this data source will belong to the collection that you select.

Authenticate to Fabric tenant (No Required)

1. Switch back to Azure portal - <https://portal.azure.com/>, search for **Microsoft Entra ID**.
2. Expand **Manage** and select **Groups**
3. Select **New group**.
4. Enter the below details and click on **Create**.
 - a. Group Type: **Security**
 - b. Group Name – Security11
5. Refresh the page to the newly created group in the list.
6. On the Newly created Group page navigate to **members** on the left hand pane, click on add members, Select You Microsoft Purview Managed Identity (the Microsoft Purview Account name that you created). Click on **Select**.
7. You will get a success notification that 1 member selected.

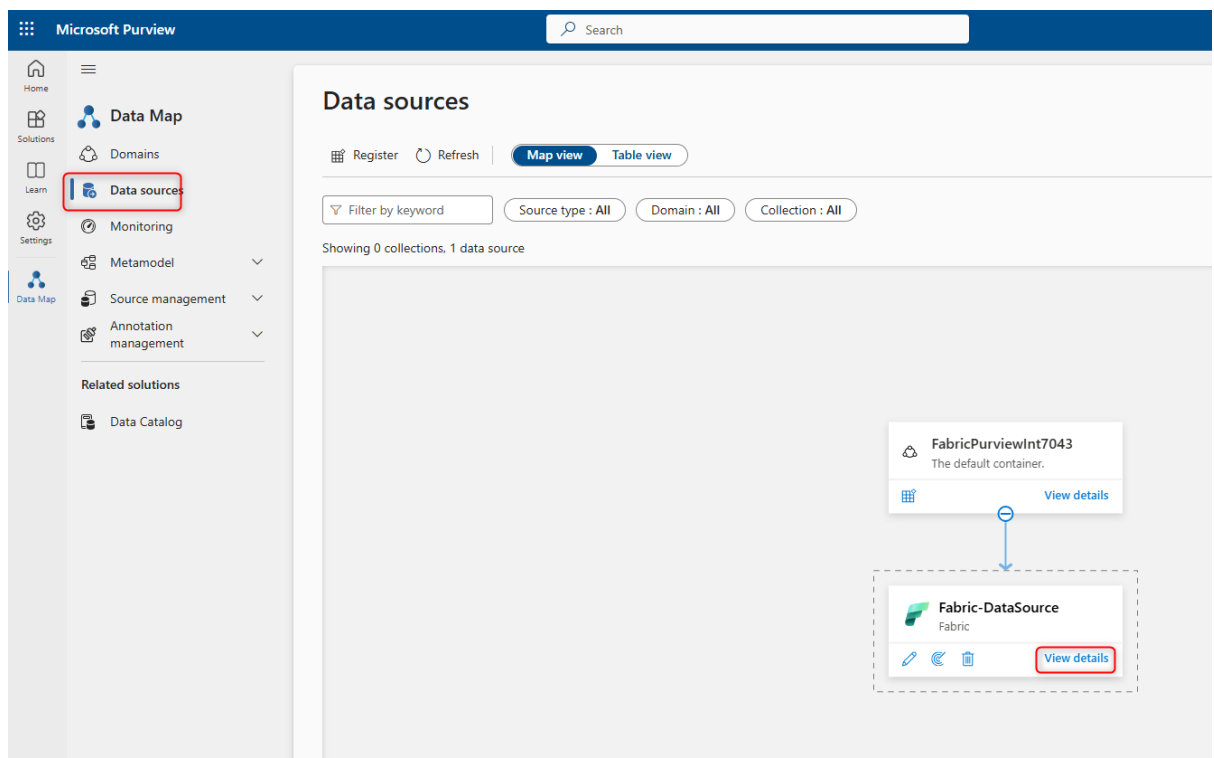
Associate the security group with the Fabric tenant (Not Required)

1. Switch back to Fabric Portal.
2. Select the **Settings** icon and Select **Admin Portal**.
3. Select the **Tenant settings** page. Search for **Admin API settings** and then search for **Service principals can access read-only admin APIs**. Enable the toggle if it is not enabled. Add your Security group and select **Apply**
4. Perform the below steps and add security group

- a. Enhance admin APIs responses with detailed metadata
- b. Enhance admin APIs responses with DAX and mashup expressions

Task 2: Scan Fabric Workspaces and Ingest Metadata

1. Switch back to Microsoft Purview Portal.
2. Navigate to **Data sources** > Select your **Fabric Datasource**. Select **View Details**



3. Click on **New Scan**.
4. Enter/Update the below details and click on **Continue**.
 - a. Name – FabricPurviewScan
 - b. Credential – **Microsoft Purview MSI (System)**
 - c. Select **Test Connection**

Scan "Fabric-DataSource"

i In addition to Power BI items, other Fabric items can also be scanned in Fabric tenants. [Learn more](#)

Name *

FabricPurviewScan **1**

Personal workspaces *

☒ Include ☐ Exclude

i Changes to the scan configuration will reset the upcoming scan to be a full scan for this data source. [Learn more](#)

Connect with integration runtime * ⓘ

☒ Azure AutoResolveIntegrationRuntime

Credential *

Microsoft Purview MSI (system) **2**

💡 Before you set up your scan you must give the managed identity of the Microsoft Purview account permissions to connect to your Fabric. [Show more](#) ▼

Continue

3 ☒ Success [View report](#)

☐ Test connection

Cancel

5. On the **Scope your scan** page select **Yes(Purview)** to and click on **Continue**.

Scope your scan

☒ Yes (Preview) ☐ No







i You can specify the scope for your scan by selecting the workspaces or manually input the item paths for the workspaces. [Learn more](#) ⓘ

Refresh

Select Fabric workspace

☒ From Fabric tenant ☐ Enter manually

Search

- ▼  **Fabric-DataSource**
 -  Fabric Workspace
 -  PersonalWorkspace FabricPurviewInt
 -  PersonalWorkspace Microsoft Service Account
 -  PersonalWorkspace MOD Administrator
 -  Test

Select all

Add to list

Selected scope

Search

No records found.

Clear

Continue


Back





Cancel

6. On the **Set a scan trigger**, Select **Once** and click on **Continue**.
7. On **Review new scan**, select **Save and run** to launch your scan.
8. The scan is created.

Data Map > Data sources >

Fabric-DataSource FabricPurviewInt


 Fabric

 New scan  Edit data source  Delete data source  Refresh

Overview Scans

Data source ID: <https://app.fabric.microsoft.com/home?ctid=2c9aff69-db95-4dd0-8e23-de858458994a>

Registered on
07/24/2024, 6:26:19 AM


Collection path
 FabricPurviewInt

Scans
1

Discovered assets ⓘ
0

Classified assets ⓘ
0

Recent scans


Scan name	Last run status	Scan rule set	Last scan time
Scan-fVK	 Queued	-	07/25/2024, 10:57 AM





[→ See all applied scans](#)

9. The scan takes a while to complete

Data Map > Data sources >

Fabric-DataSource FabricPurviewInt

 Fabric

 New scan  Edit data source  Delete data source  Refresh

Overview Scans


Data source ID: <https://app.fabric.microsoft.com/home?ctid=2c9aff69-db95-4dd0-8e23-de858458994a>

Scans
1

Discovered assets ⓘ
5

Classified assets ⓘ
0

Recent scans

Scan name	Last run status	Scan rule set	Last scan time
Scan-fVK	 Completed	-	07/25/2024, 10:57 AM

[→ See all applied scans](#)