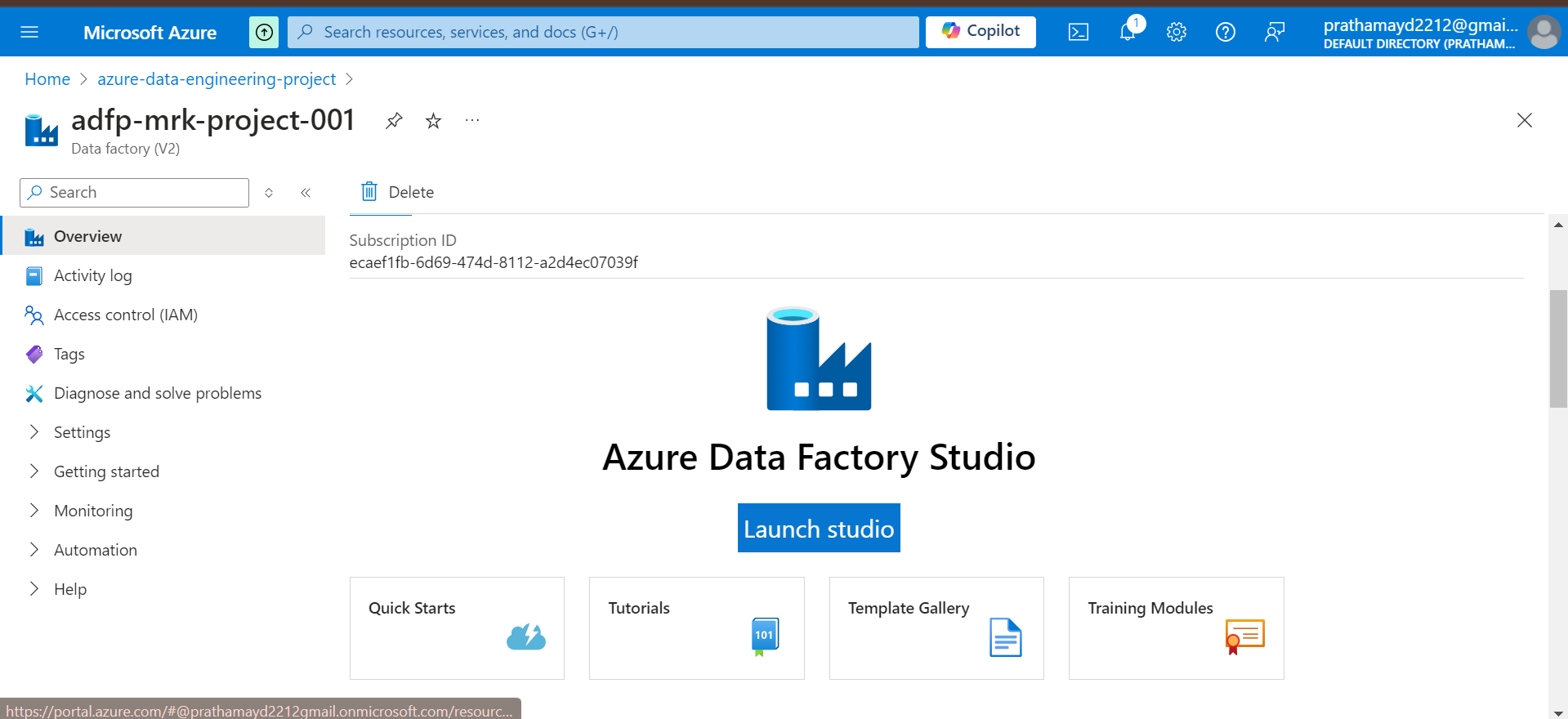
**Azure Data Engineering**

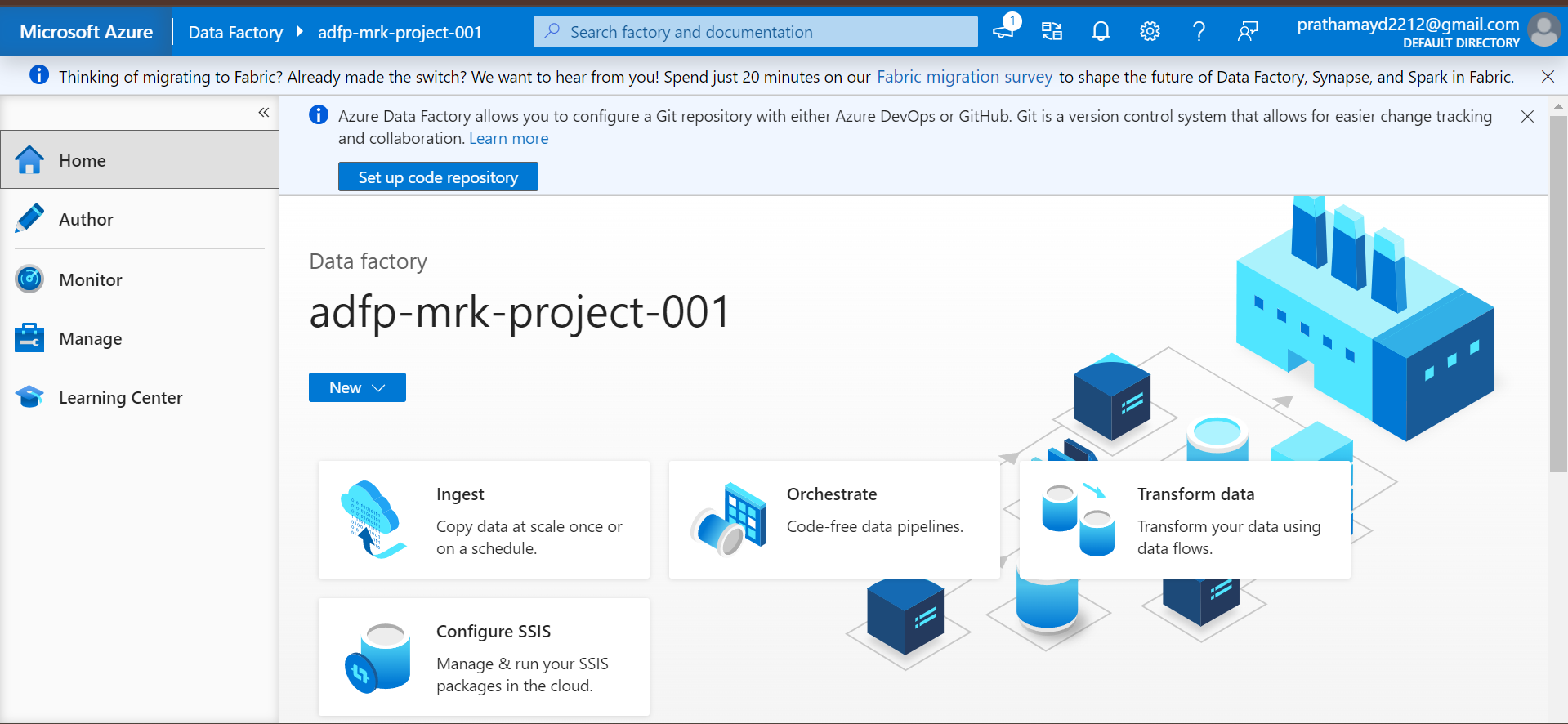
**Data Ingestion using ADF(Azure Data Factory):**

Navigate to your resource group and click on the Data factory resource and click on launch studio.

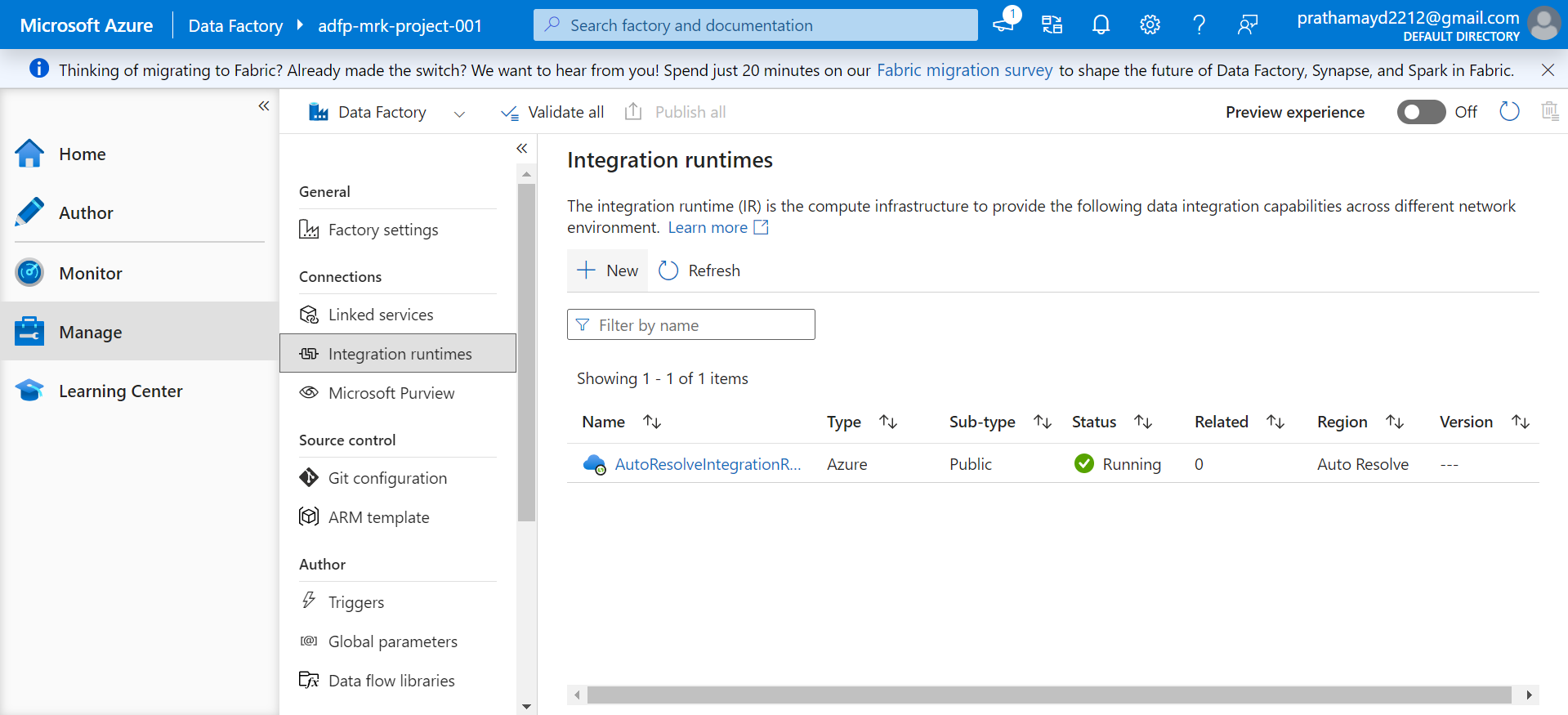


Now to connect to the on premiss sql server database, you need to install **self hosted integration runtime** on the device where the database is located. That is my laptop.

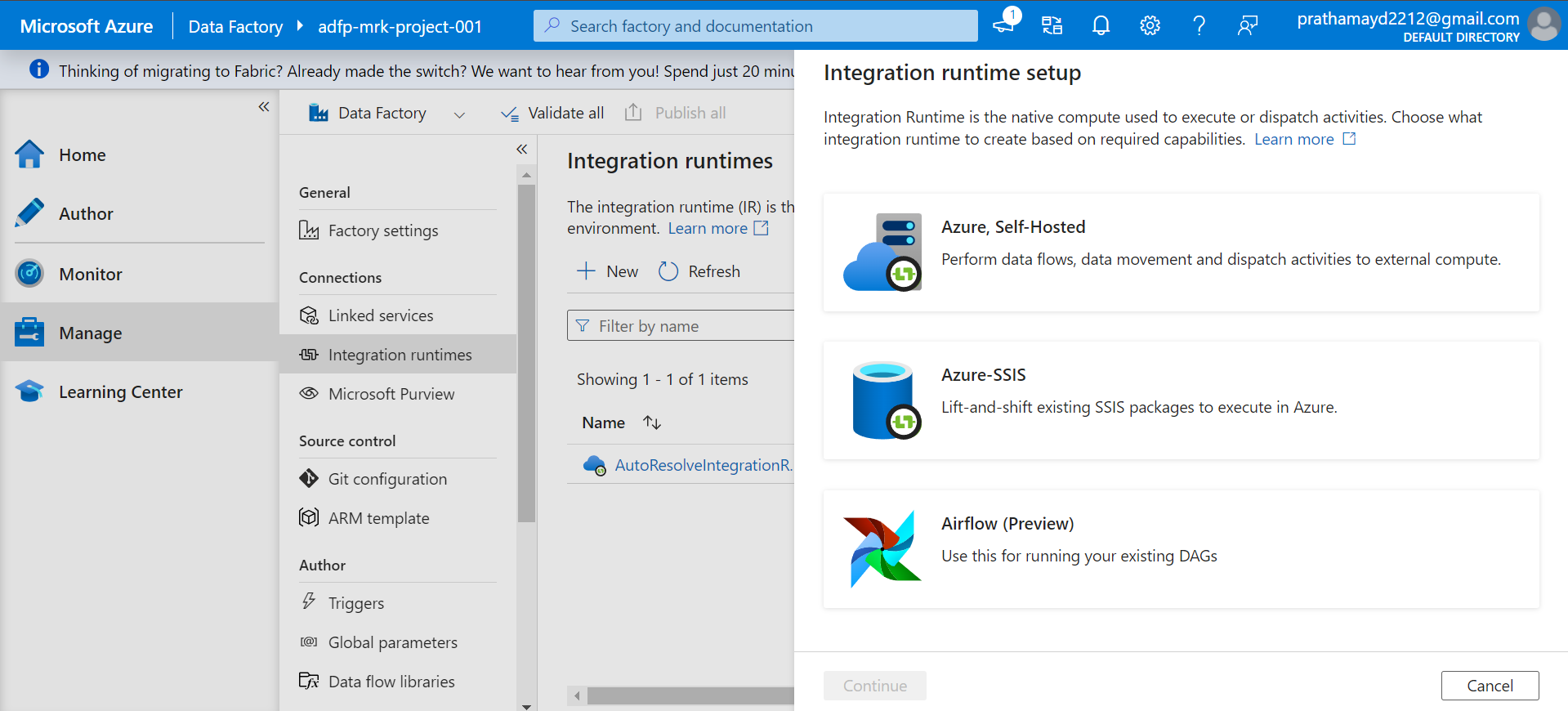
Installation of the Self Hosted integration runtime:



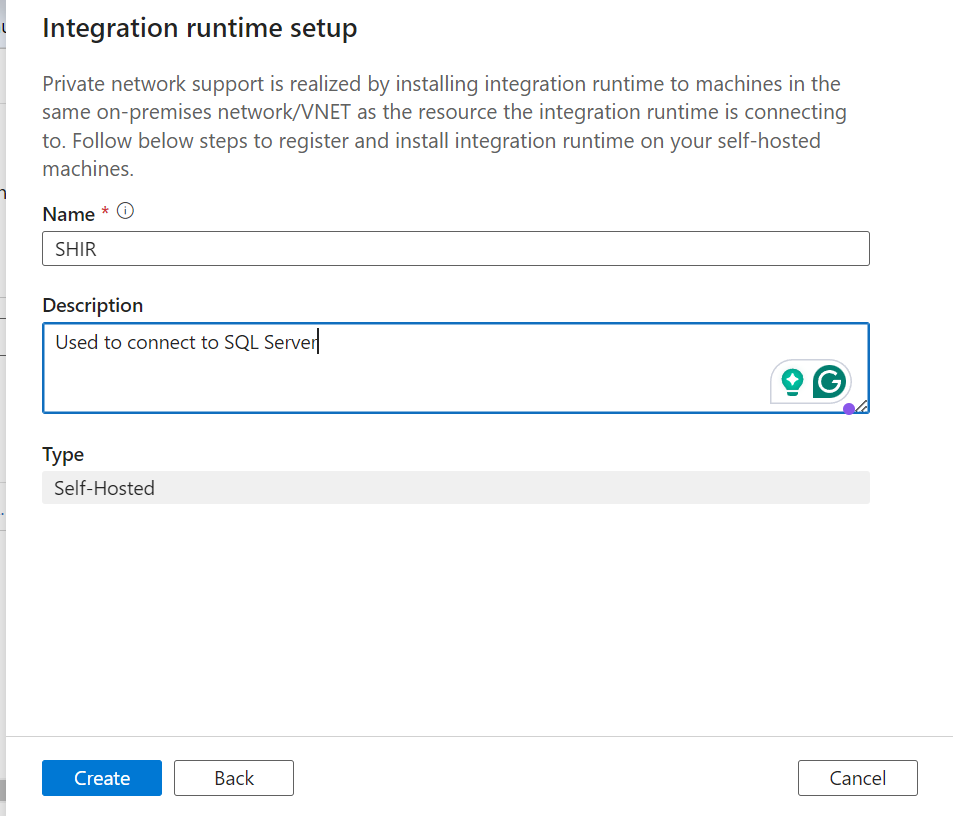
Managed 🡪Integrations runtime🡪new



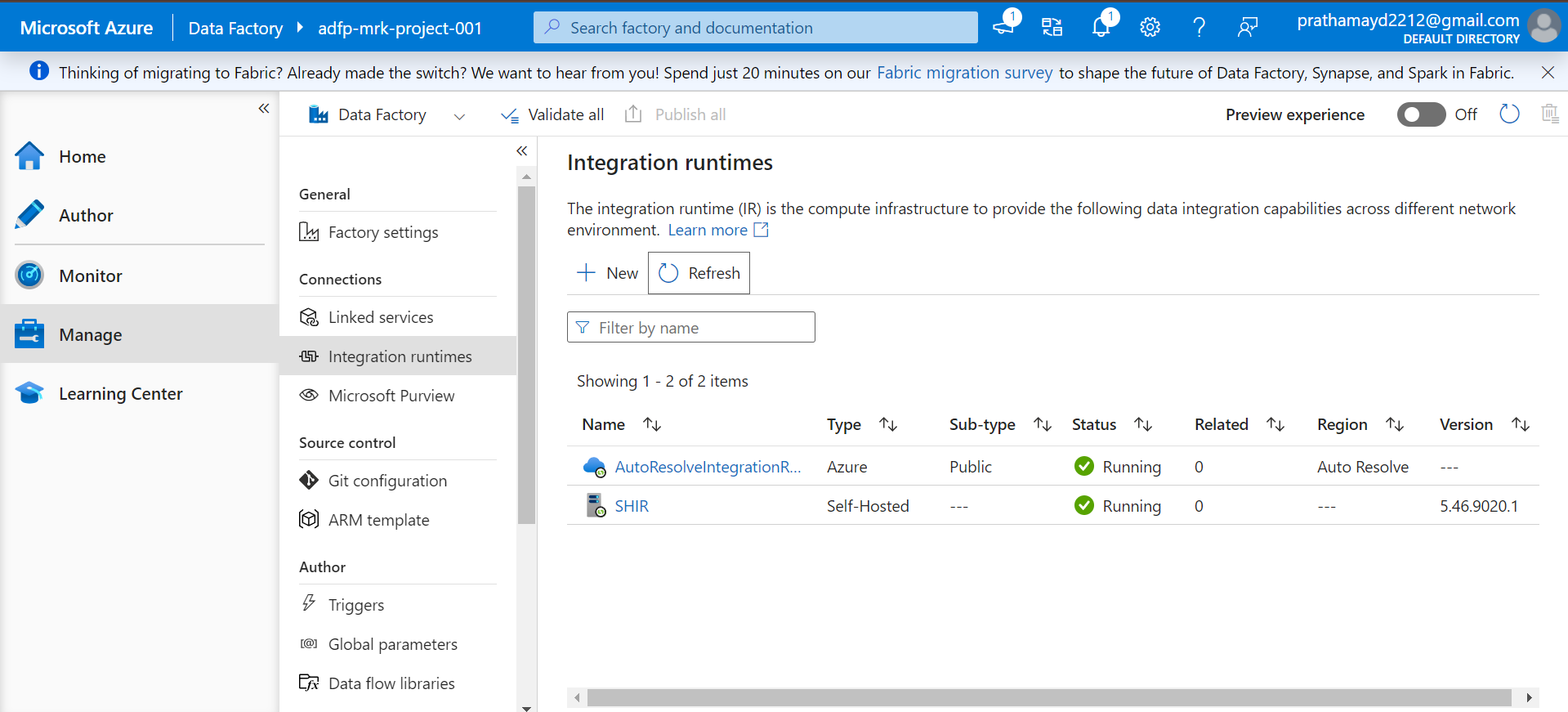
🡪Azure, Self Hosted 🡪 Self-Hosted



🡪Provide integration name 🡪Description🡪Create

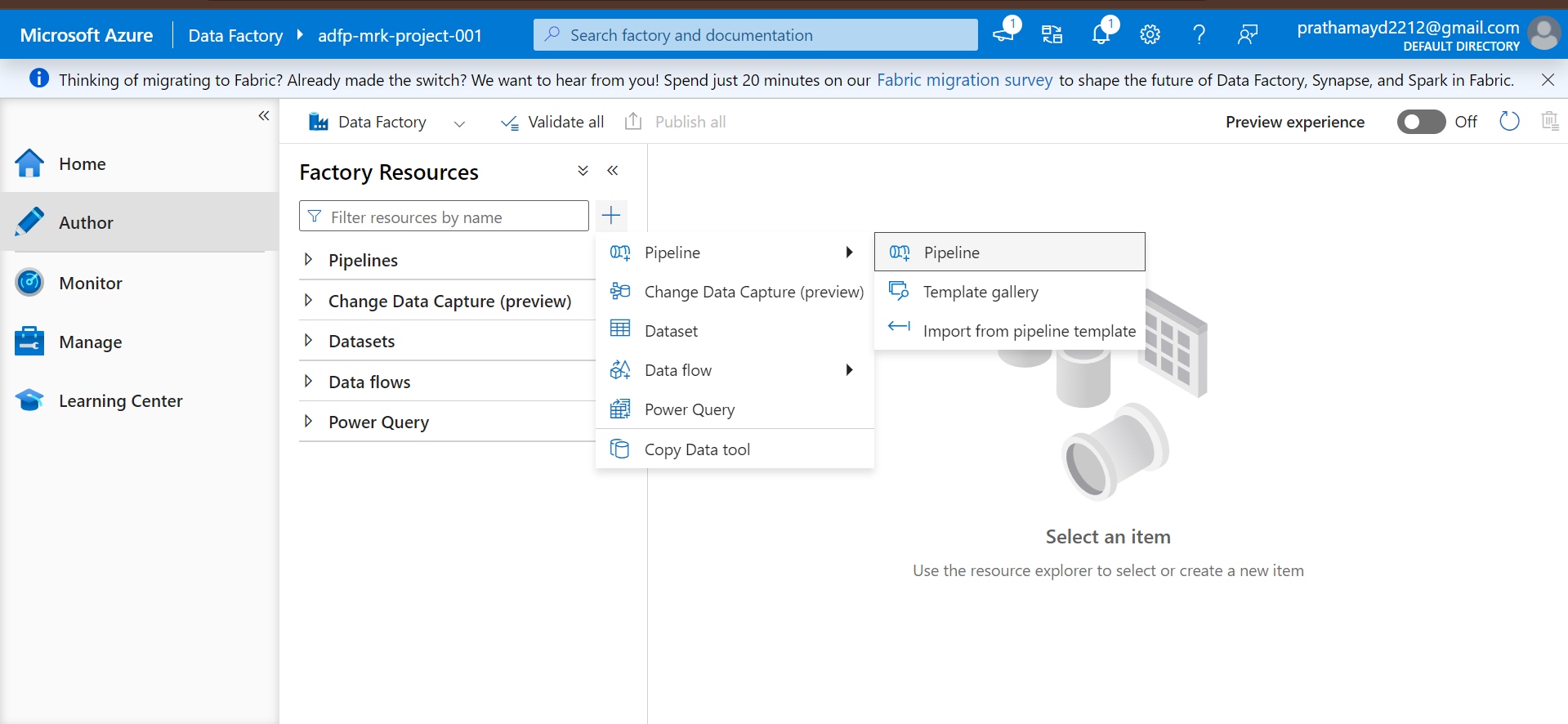


* Then you will get two options, 1- Express setup and 2- Manual Setup
* Select Express and install the setup.
* It will install the the (Self-Hosted) Express setup
* The integration runtime helps us to connect to sql server and integrate to move data from the database to ADF.
* Once the slef-host is installed, you will see that one more item is added to the list in your runtime tab.

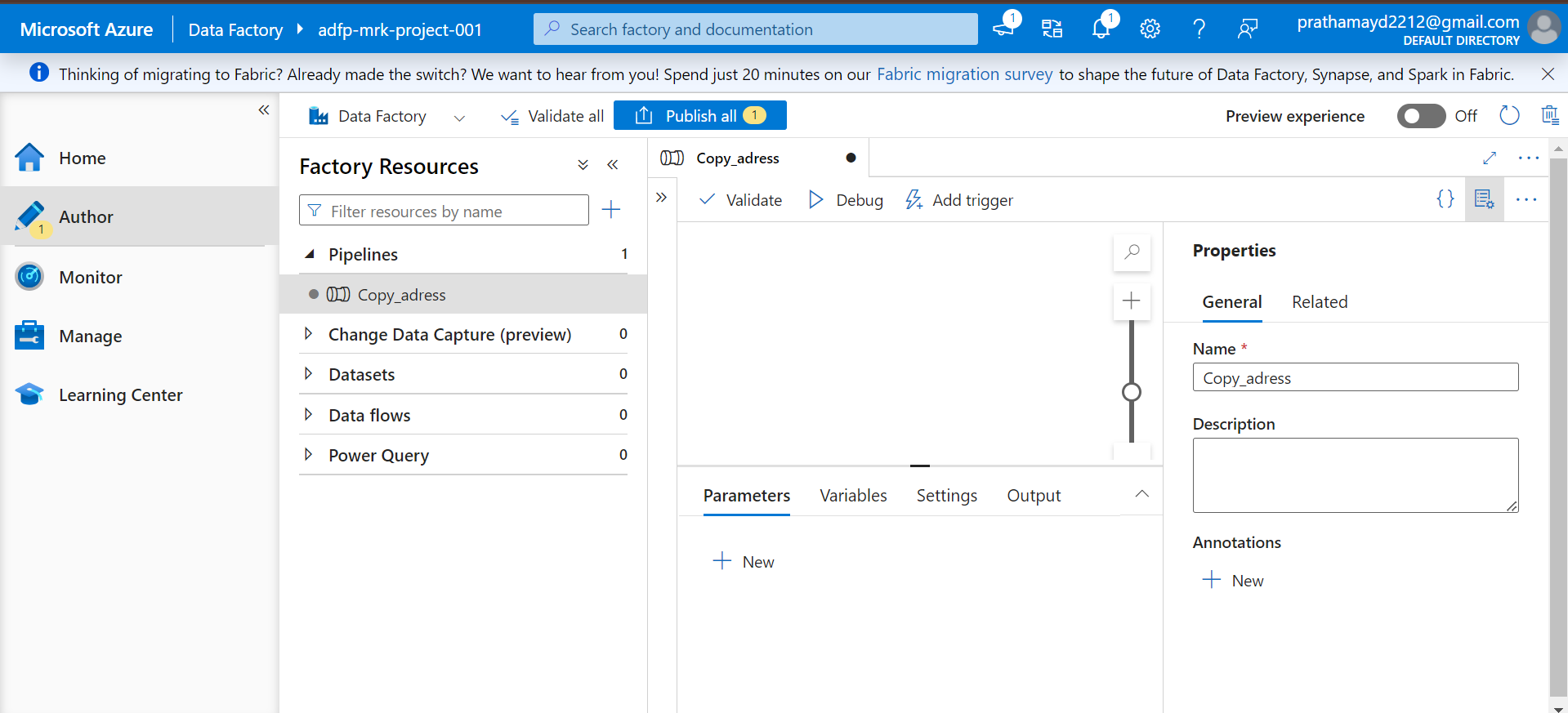


* Now we need to connect to the on premis sql server to load the data into Azure Data Factory.

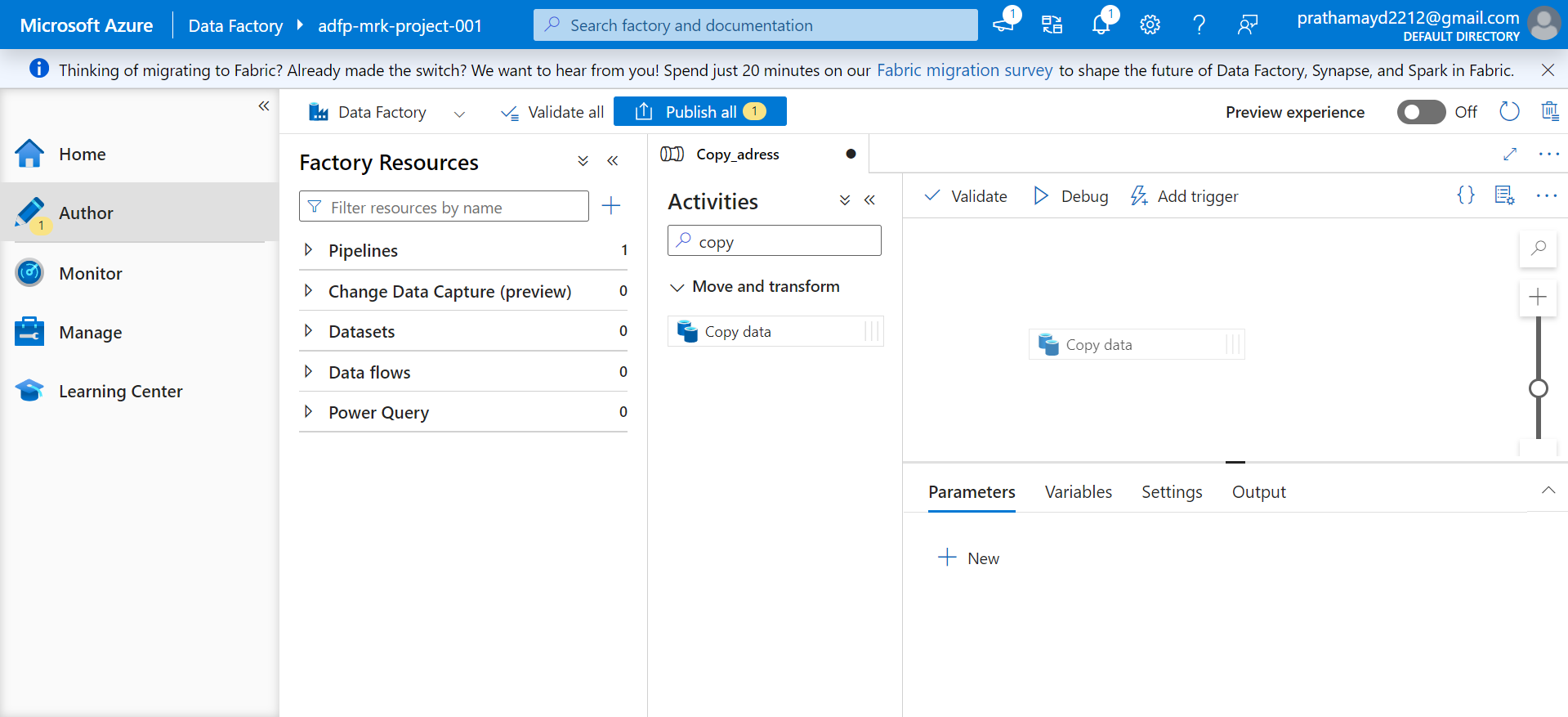
In ADF 🡪 Authors 🡪 Add 🡪 pipeline🡪 Pipeline



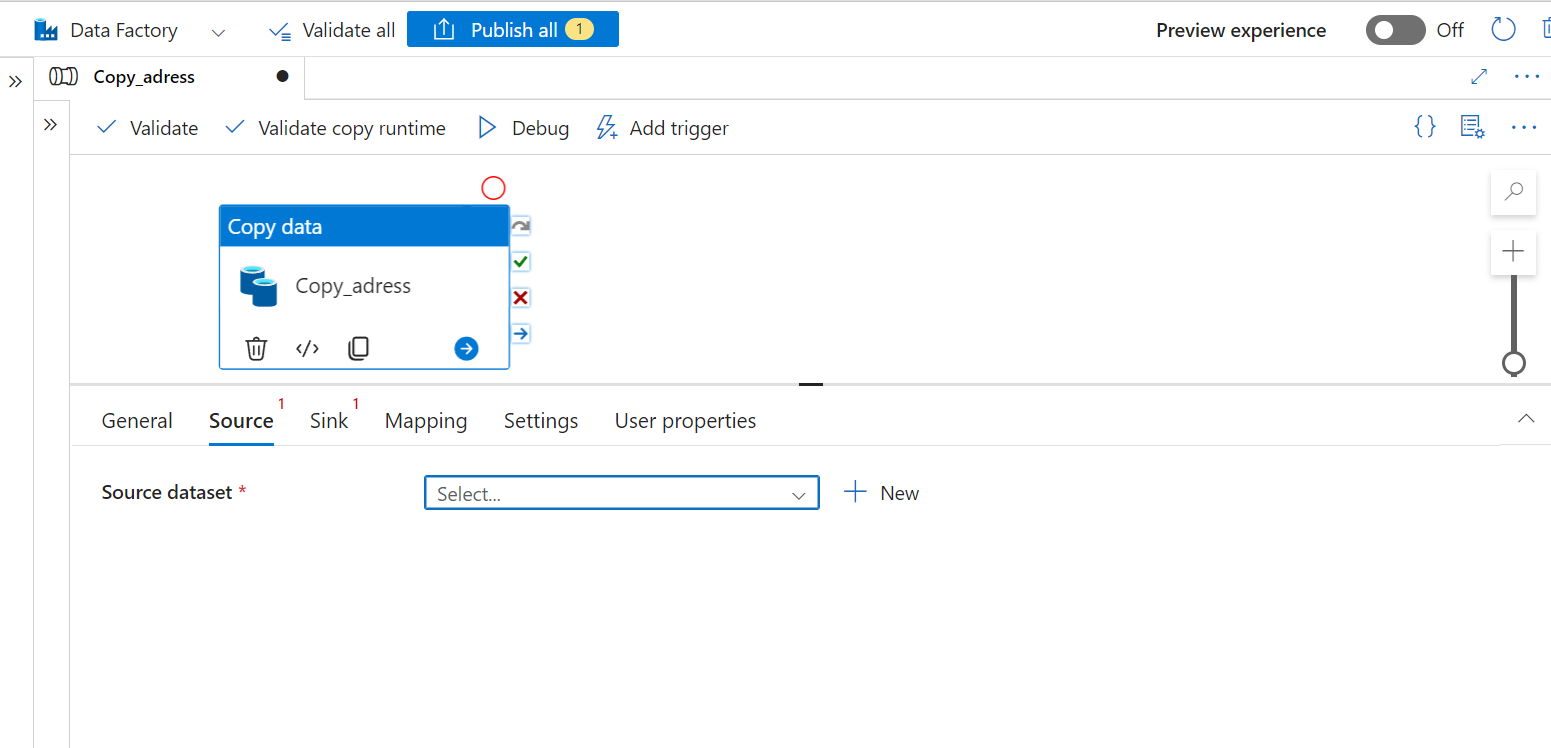
Change the pipeline name



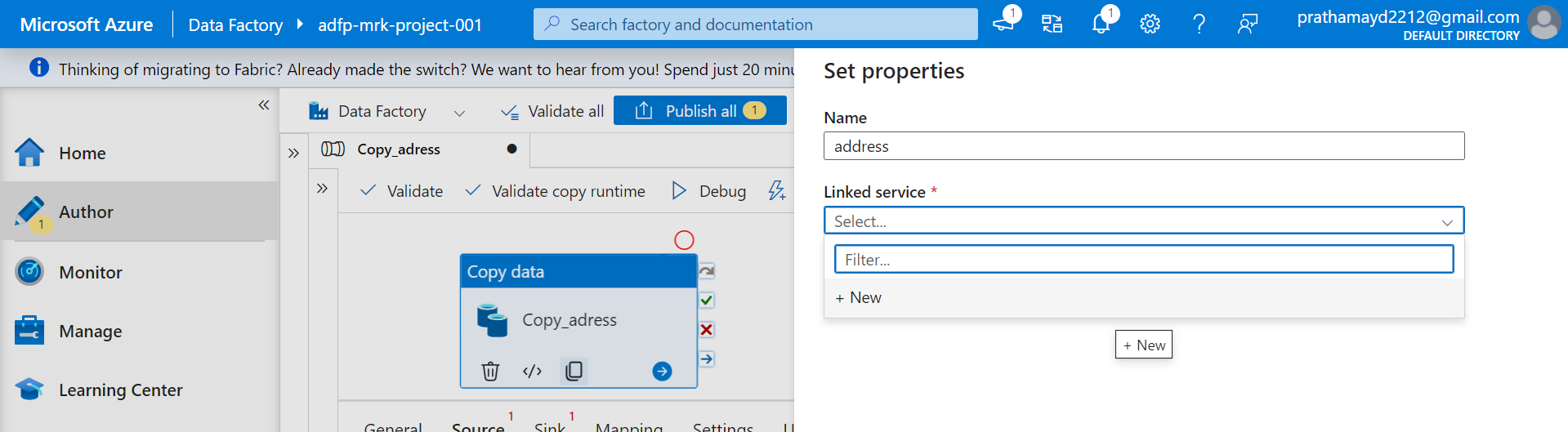
🡪Activity 🡪Search for the pipeline🡪 Drag and drop it in the dashboard

First we will copy only the address table and then rest of the tables

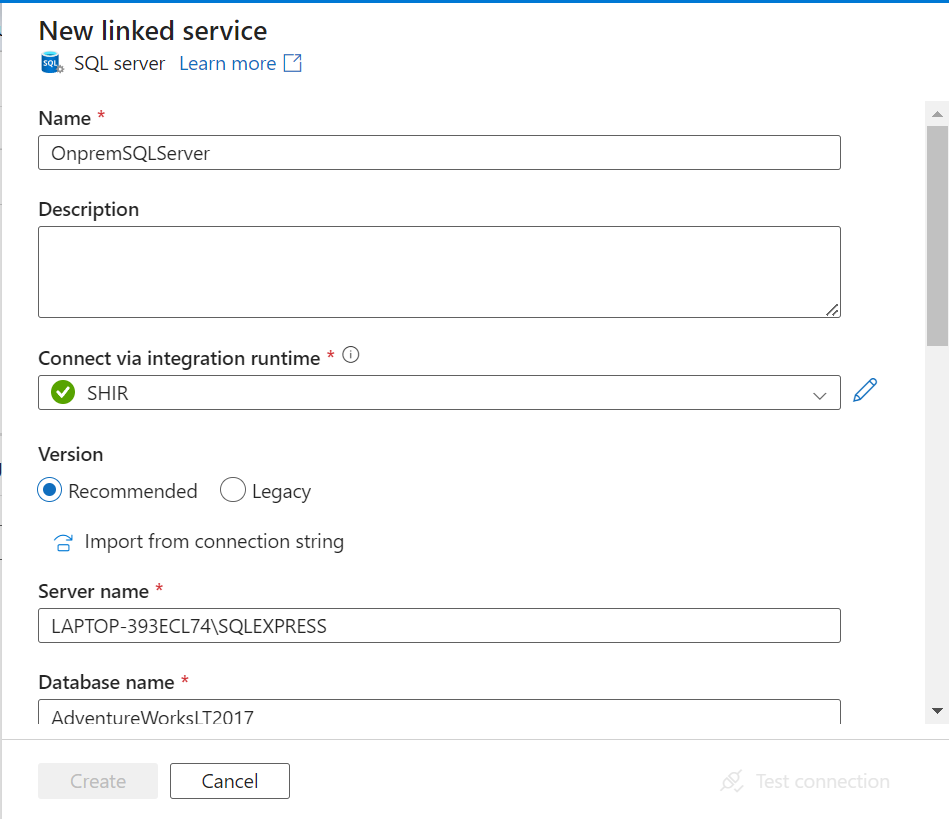
🡪Source🡪New🡪SQL Server

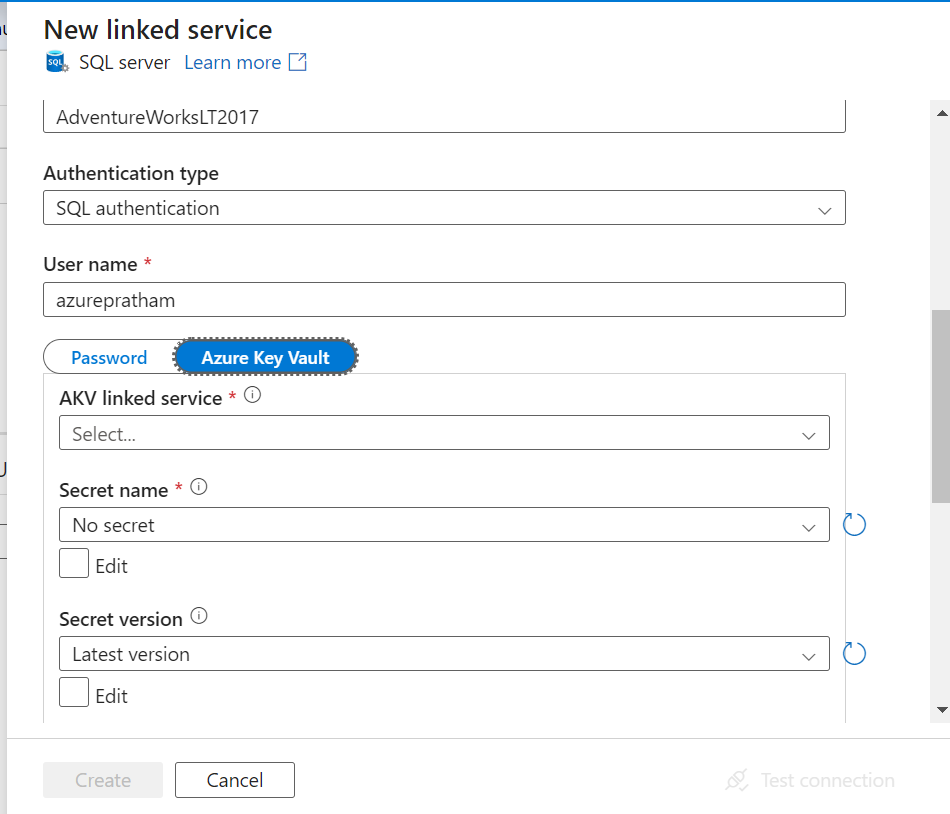


Select SQL server and give a new name, then add new linked service.

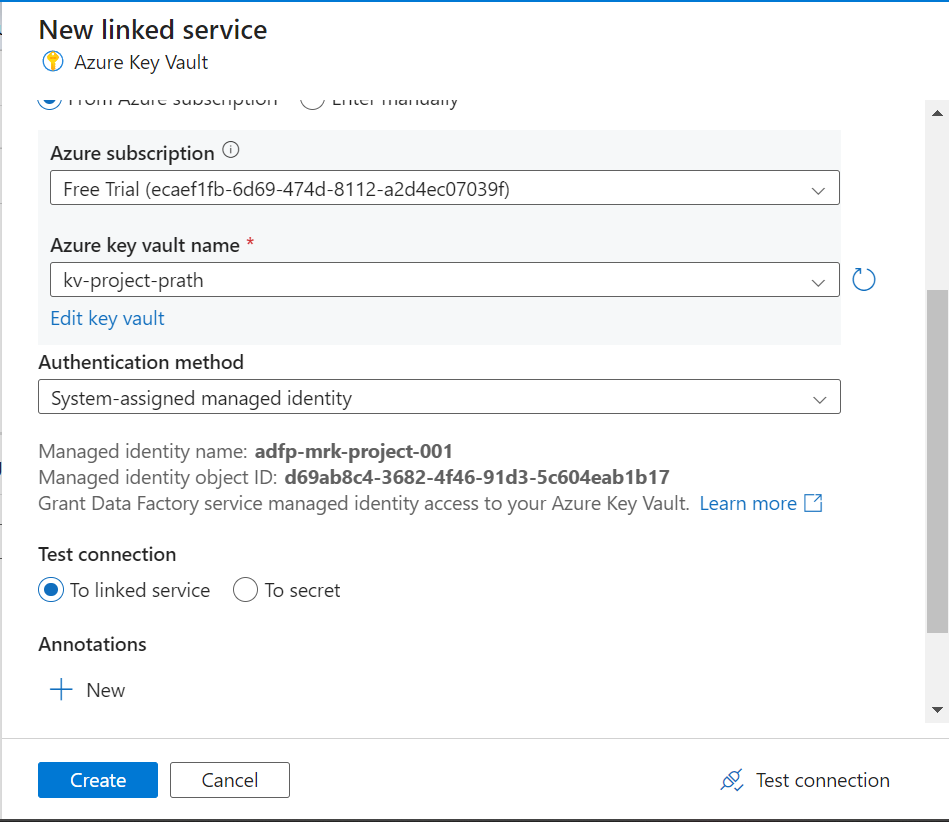


Provide all the details





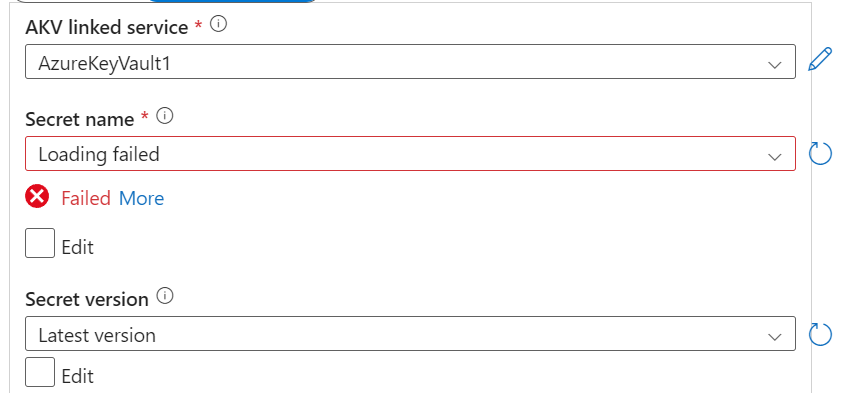
We can either write the password directly or we can provide the secret access, and for that we need to set up the permission to the key vault.



Provide all details and click on test connections on bottom right corner.

IF it shows Connection Successful then you are good to proceed. Click Create.

🡪Now you will see that the secret key shows Loading failed.



Now we need to provide reader permission to read the secret so that it can read the secret password.

**Additional configuration:**

**🡪Azure key vault 🡪 Access Policies**

**Follow the below steps if you do not have access to Access Policies:**

The message in the screenshot indicates that Access Policies are not available because the Key Vault is configured to use Role-Based Access Control (RBAC) instead of traditional access policies. In Azure, there are two ways to control access to a Key Vault:

1. Role-Based Access Control (RBAC)
2. Vault Access Policies

Since the Key Vault is using RBAC, you cannot modify access policies directly through the traditional Access Policies tab. Here's what you can do to solve this:

Solution Steps

1. Use Role-Based Access Control (RBAC) to Grant Access:

* Go to the Access control (IAM) section of your Key Vault.
* Click on + Add role assignment.
* Select a role like:
  + Key Vault Administrator: Full control over the Key Vault and its contents.
  + Key Vault Secrets User: Access to secrets but not keys or certificates.
  + Key Vault Secrets Officer: Similar to Secrets User but with more management permissions.
  + Key Vault Contributor: Broad access to manage keys, secrets, and certificates.
* Select the appropriate user, group, or service principal to assign the role.
* Save the changes.

This will grant the necessary access based on RBAC.

2. Switch Back to Access Policies (Optional):

If you want to manage access using the traditional Vault Access Policies, you can switch back to that model:

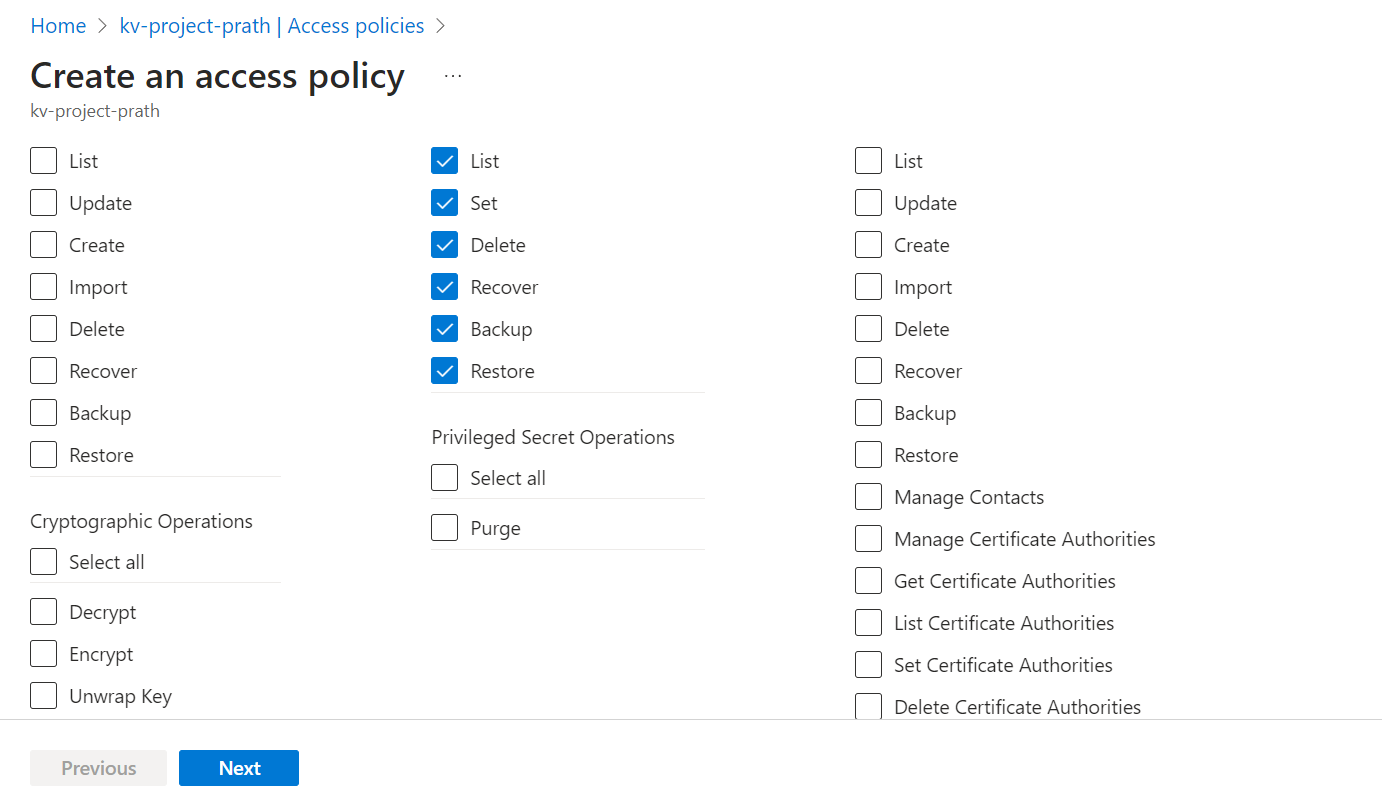
* In the Azure portal, go to your Key Vault.
* Under Settings, select Access configuration.
* Switch from Azure role-based access control (RBAC) to Vault access policy.

Note: Changing this setting will disable RBAC for Key Vault access, and you'll need to manually configure Access Policies again.

Azure Free Trial Considerations:

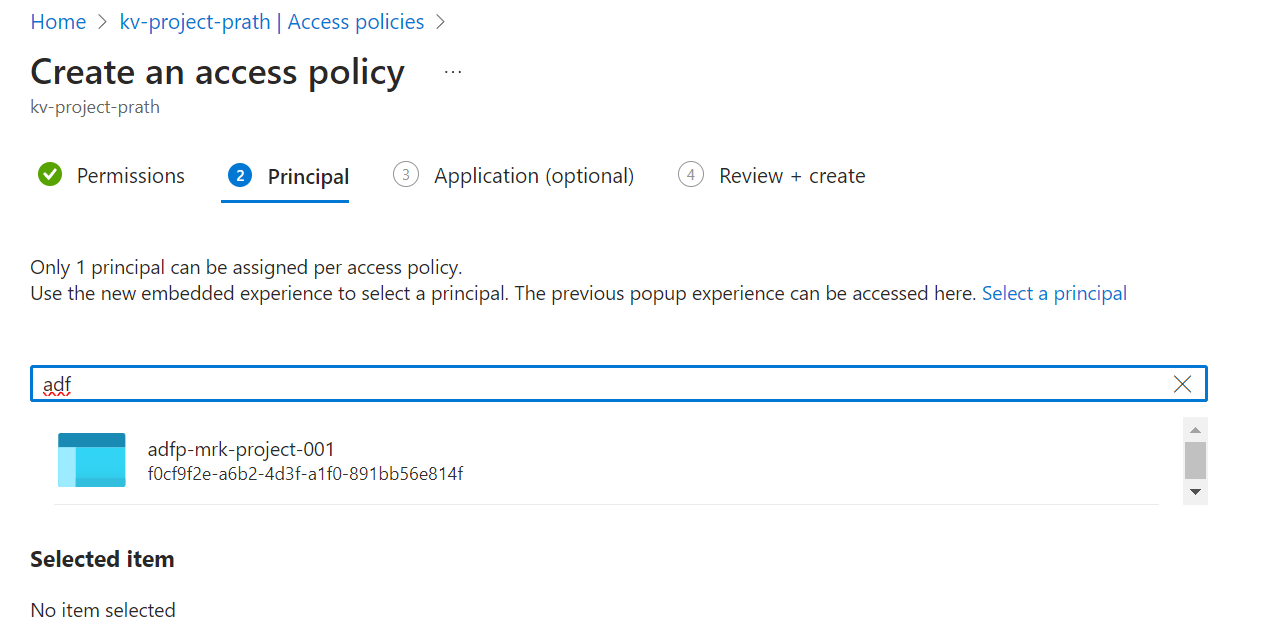
* The free trial account still supports both RBAC and Access Policies. There are no restrictions in a free trial preventing you from switching access methods.
* Ensure that your subscription is active and that your role (e.g., Owner or Contributor) has sufficient permissions to modify these settings.

**ACCESS policies 🡪Create🡪Secret Permissions(Select ALL) 🡪Next**

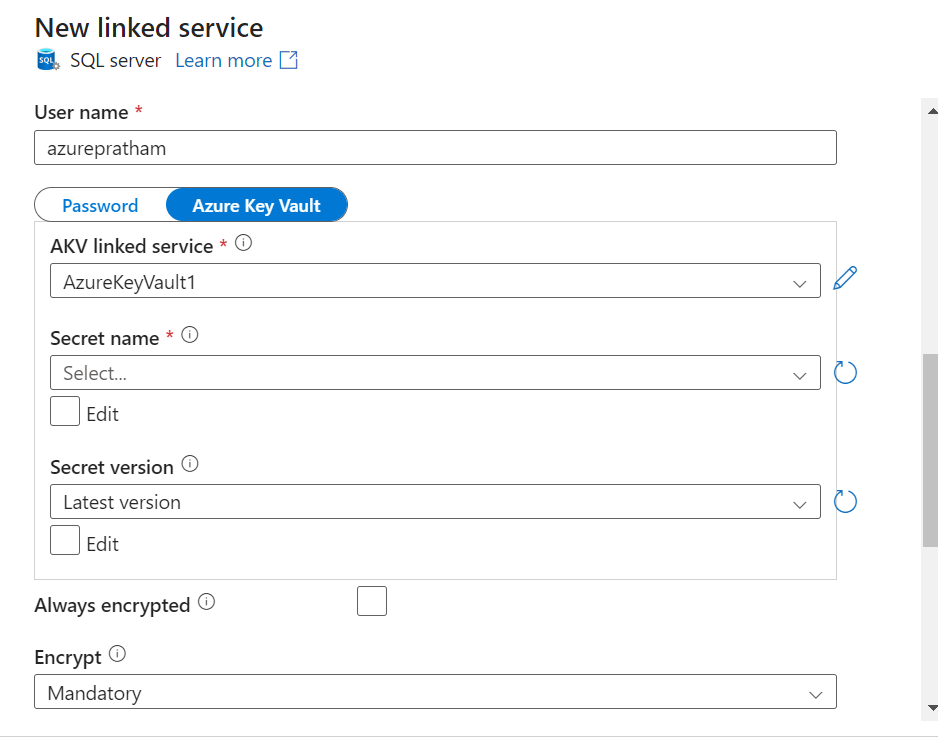
****

**Principles**

Enter Azure data factory name created by you and add it. **Create**

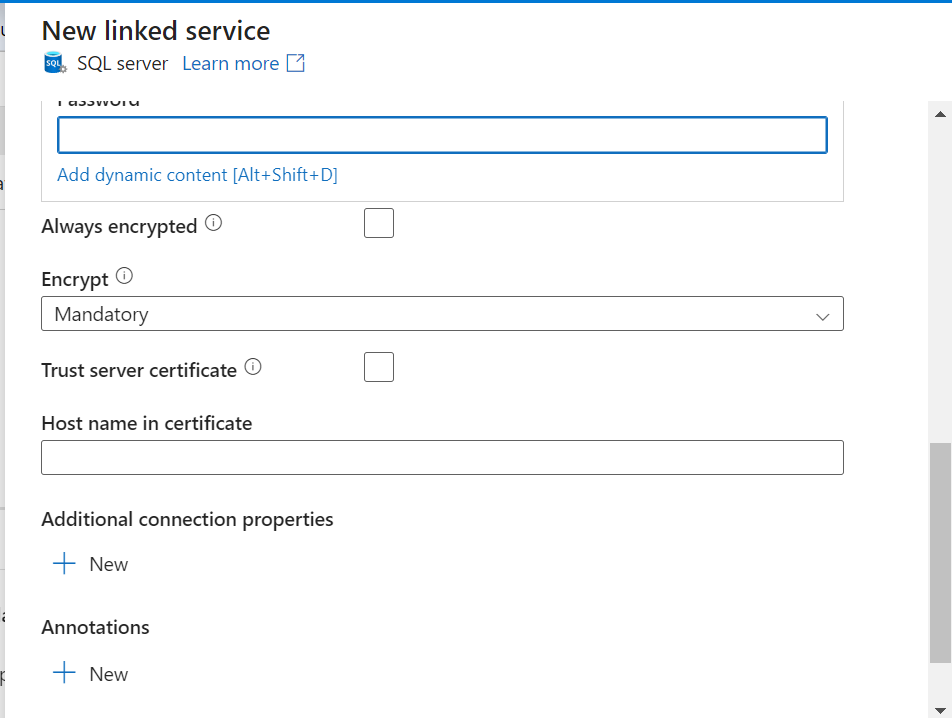
****

Once access policy is created go back to Azure Data Factory and refresh the Secret name and add the password over there

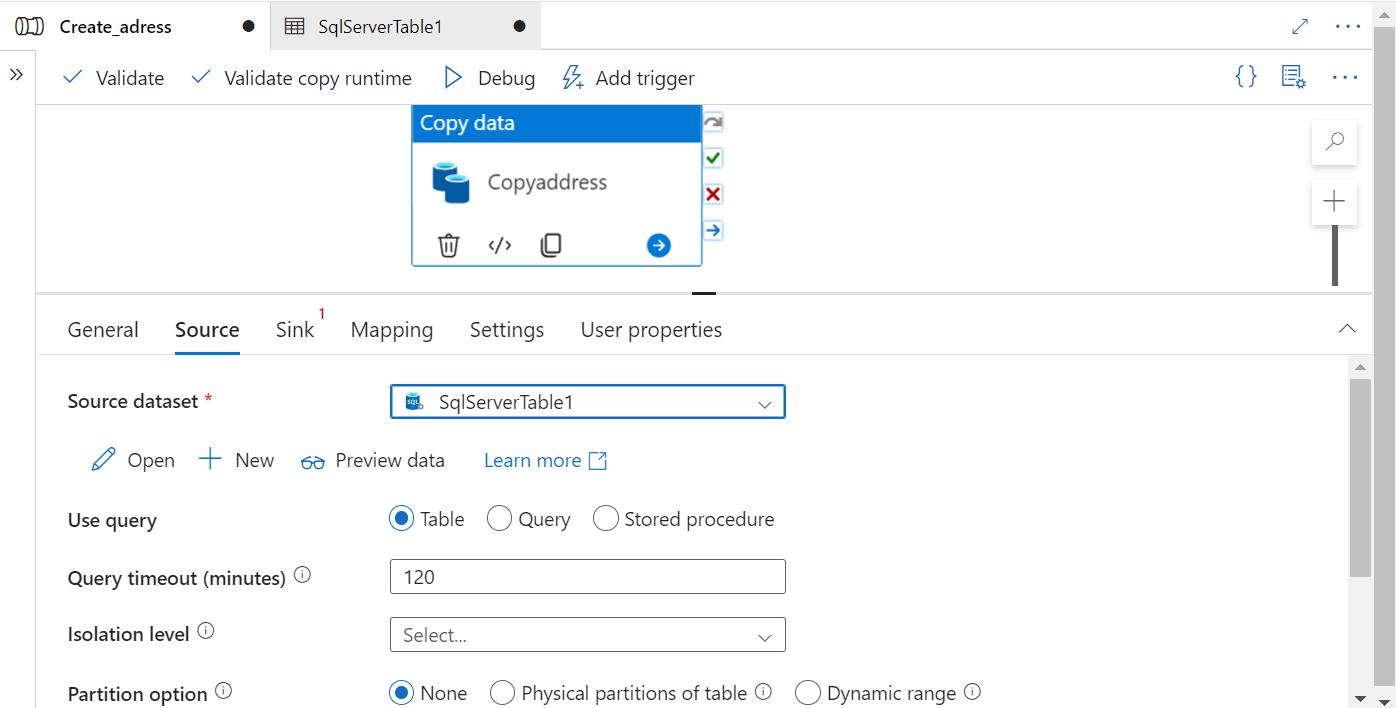


Click on test connection and then once it is successful, create

If you get any certification error then just check the Trust server certificate box and you will be good to go.



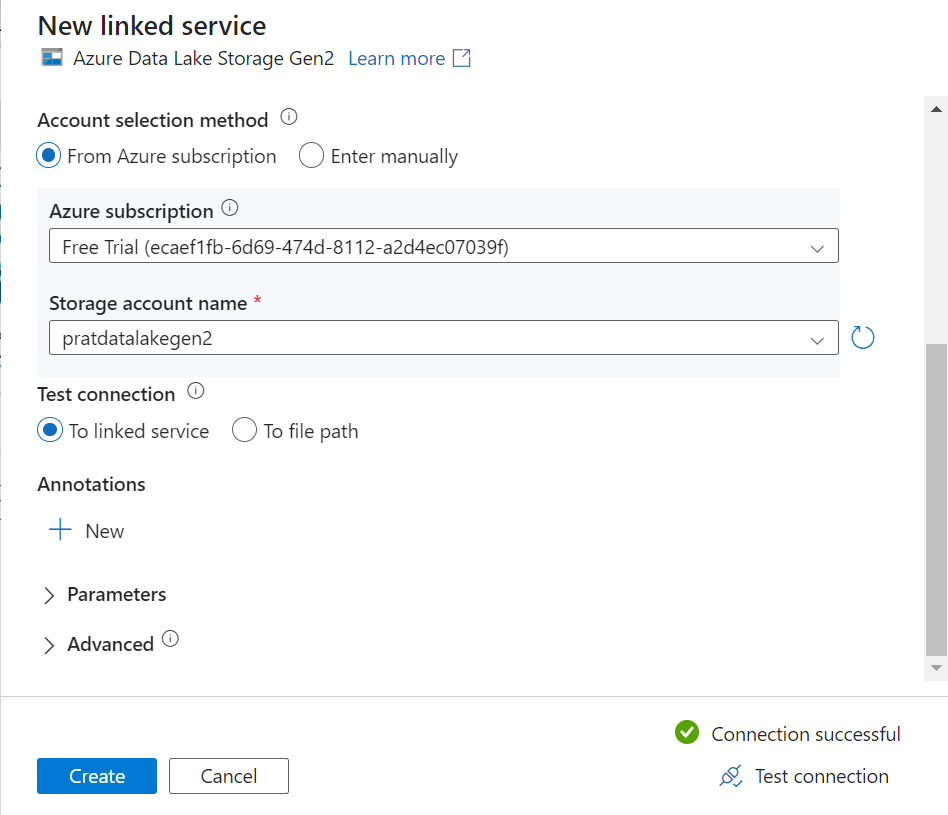
Choose the source here (NOTE:Name of the source has changed here)



Now click on Sink option to ingest the data.

Sink🡪 New 🡪 Azure Data Lake Storage Gen2 🡪 Parquet

Choose Parquet then link a new service with the Blob Storage.

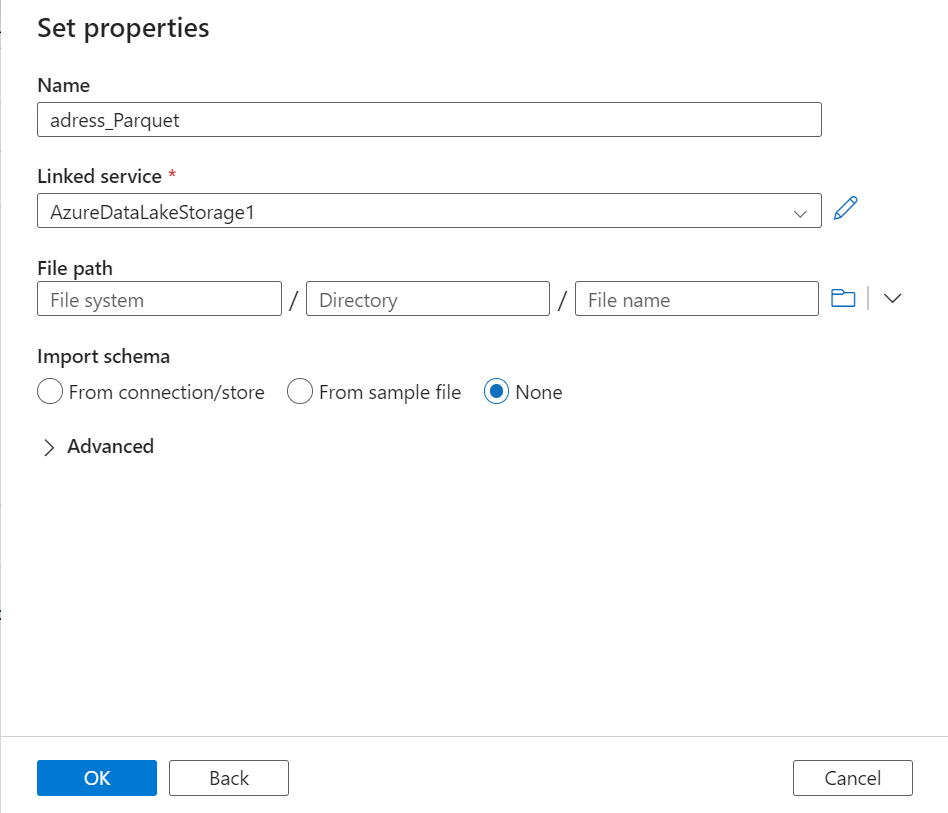


Enter the details and test connection.  
If connection fails to the blob storage, go to the storage resource and disable the soft delete if it was enabled.

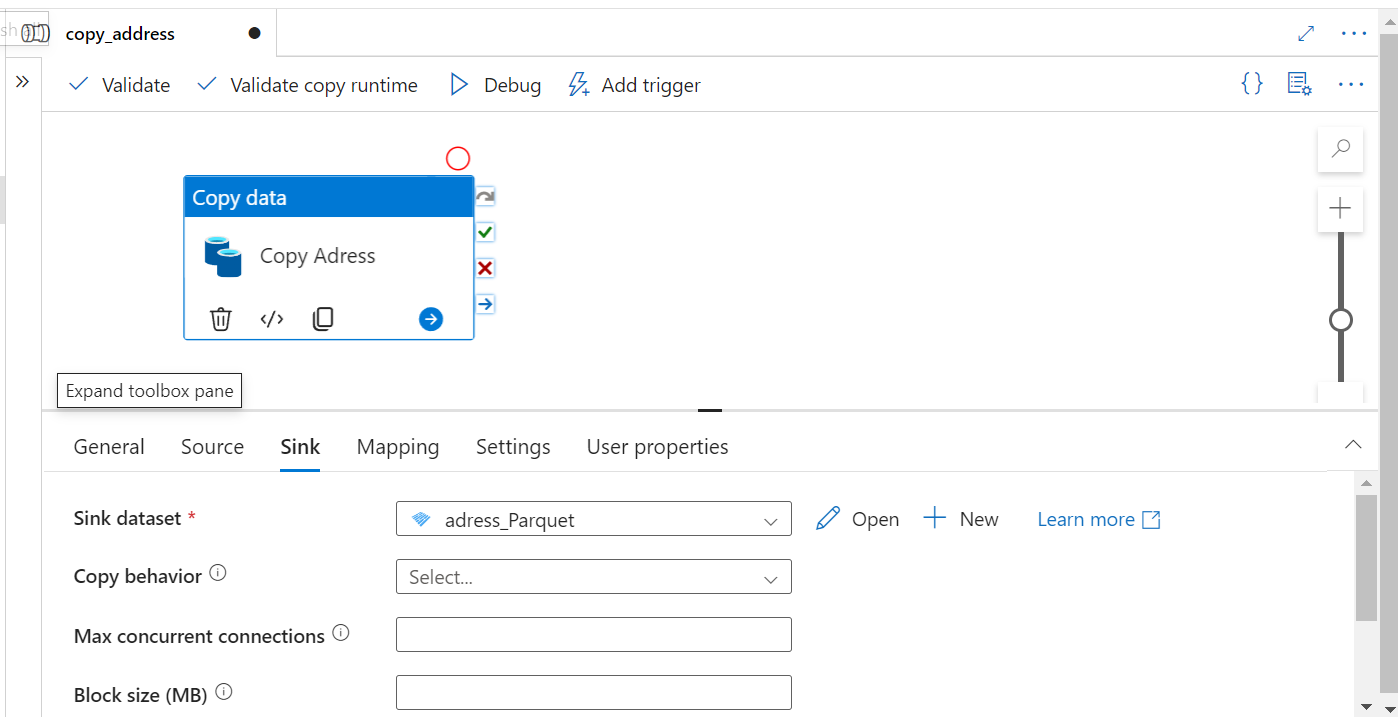
**CREATE**

**You will be navigated to this page and you need to set up the properties.**

**And Choose the container where you want to drop the address table.**

** Choose the bronze folder that was created earlier.**

**Once the pipeline is created we need to run the pipeline by clicking the debug option.**

****

Once the pipeline run is successful you will be able to see the data in the blob storage in the bronze container.

