

Workflow for enabling Privatelink for Fabric instance

Workflow for enabling Privatelink for Fabric instance

Step	Executor	Procedure	Permission needed
1	M365 admin	Access https://portal.office.com/adminportal/home?#/rbac/directory Lookup “Fabric Administrator “ and grant the Azure Subscription Owner with this role	M365 system admin
2	BU	Azure portal > Subscription > Settings > Resource providers Search and register “Microsoft.Fabric”	Subscription Owner/Contributor
3	BU	Azure portal > Search “Microsoft.Fabric” Create Fabric Instance, select the same Region where BU’s data residency	Subscription/Resource Group Owner/Contributor
4	BU	Access https://app.fabric.microsoft.com/ Right upper Gear icon > tenant settings> Search and enable “ Azure Private Link ”	Fabric Administrator
5	BU	Login Azure Portal, switch subscription to BU’s sub > Search “Deploy a custom template”. Follow Step 2 “ Create a Microsoft.PowerBI private link services for Power BI resource in the Azure portal ”	Subscription Owner + Fabric Administrator
6	BU	Login Azure Portal, follow Step 3 “ Create a virtual network ” to Step 7 “ Access Fabric privately from the virtual machine ” You can skip VNET, VM, Bastion workflow if you already have them	Subscription/Resource Group Owner/Contributor

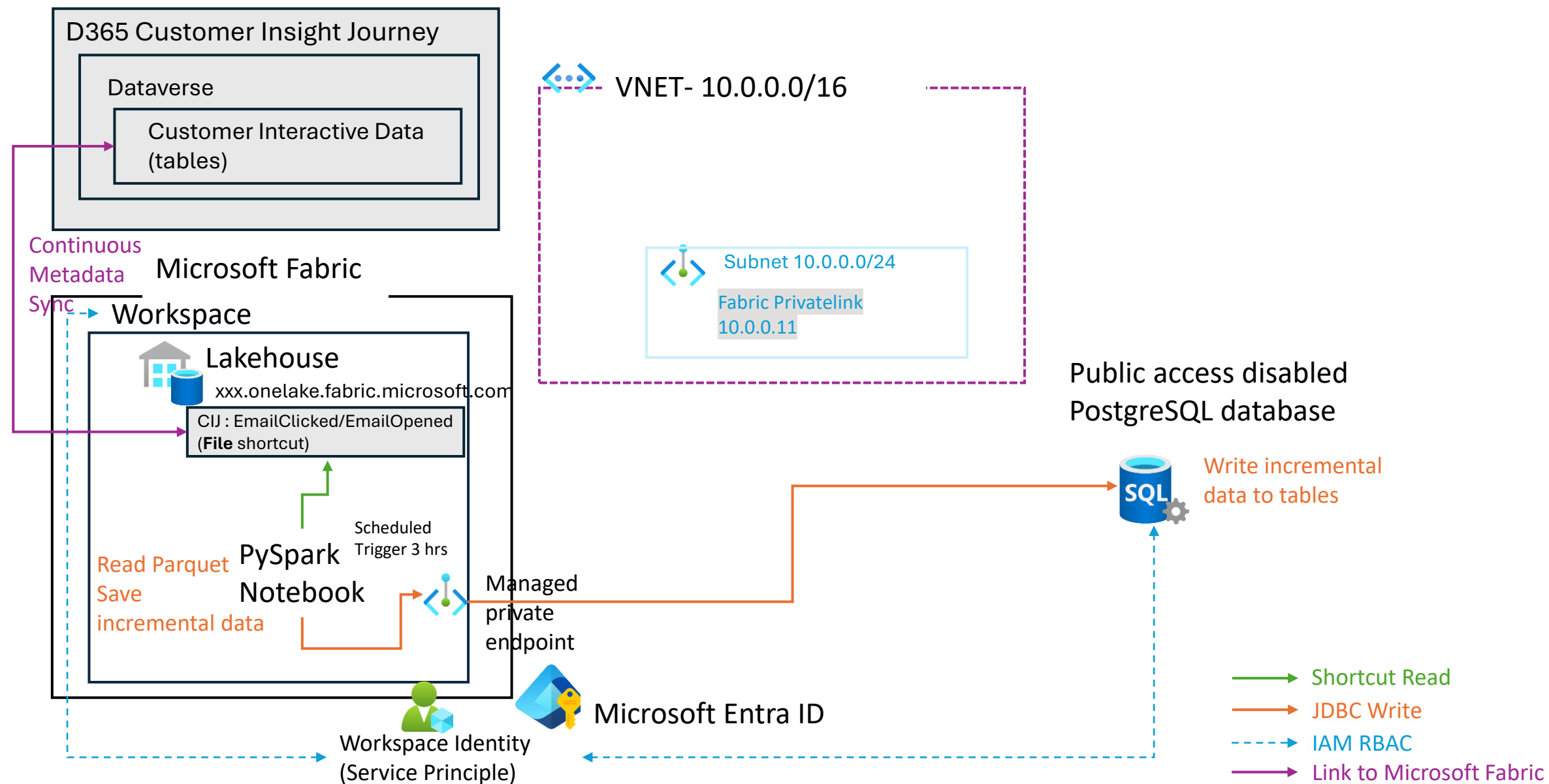
Workflow for enabling Privatelink for Fabric instance

Step	Executor	Procedure	Permission needed
7	BU	Access to https://app.fabric.microsoft.com/home Click “Power BI” icon > Workspaces > Create workspace - Workspace settings > License info > binding with your Fabric instance - Workspace settings > Workspace identity > enable identity	Subscription Owner + Fabric admin
8	BU	Login PowerApps Portal, https://make.powerapps.com/ , > select D365CIJ environment > Tables > Analyze > click “ Link to Microsoft Fabric ” - Select the Fabric workspace - Wait for completion is necessary	D365 system admin+ Fabric admin
9	BU	Use a VM to access https://app.fabric.microsoft.com/ Right upper Gear icon > tenant settings> Search and enable “ Block Public Internet Access ”	Fabric Administrator
10	BU	Wait for 15-20mins, access to https://app.fabric.microsoft.com/ via internet, to validate the Fabric entry point is blocked for public access	Any tenant user
11	BU	Access to https://app.fabric.microsoft.com/ via VM, to validate the Fabric entry point is accessible from VNET	Any tenant user from a VM

If any BU need to perform step8 again for another D365CIJ environment, need to ask Fabric Administrator to perform step 9 for disabling the “Block Public Internet Access”. Otherwise, step 8 will be failed

Workflow for setup Fabric shortcut for Dataverse

Fabric notebook read shortcut and write to PostgreSQL



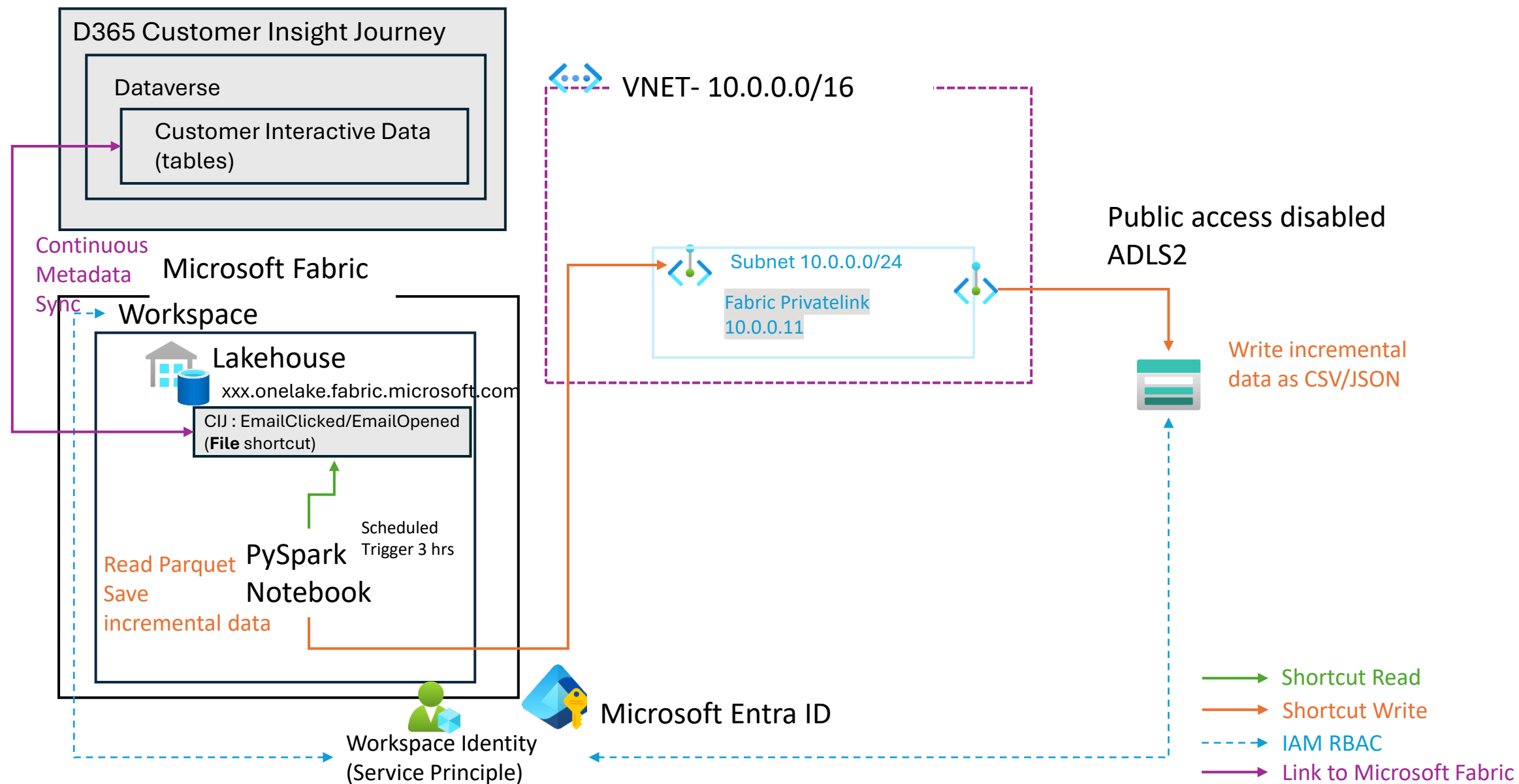
Workflow for Fabric notebook (PostgreSQL)

Step	Executor	Procedure	Permission needed
0	BU	<p>Access to https://app.fabric.microsoft.com/home</p> <p>Click “Power BI” icon > Workspaces > Select your workspace</p> <ul style="list-style-type: none"> - You will find a lakehouse named “Dataverse_xxx” is created by “Link to Microsoft Fabric”, you can delete this lakehouse - Create a new lakehouse, click “+New item” button, select lakehouse 	Fabric workspace contributor
1	BU	<p>Go to lakehouse page > click “...” icon next to “Files” > New shortcut > Dataverse</p> <ul style="list-style-type: none"> - Enter your D365 CIJ environment domain - Sign on your D365 system admin for “connection credentials” - Select the tables you needed “Customer Insights Journeys/EmailClicked / EmailOpened” 	Fabric admin + D365 system admin
2	BU	<p>Azure portal > your_postgresql > IAM</p> <p>Grant contributor role to your workspace identity</p>	SubscriptionOwner/Contributor
3	BU	<p>Azure portal > your_postgresql > Overview > click JSON View > Copy Resource ID</p> <p>Fabric Workspace > Workspace settings > Network Security > Create > paste your PostgreSQL Resource ID to Resource identifier, pick sub-resource “PostgreSQL”</p> <p>Azure portal > your_postgresql > Network > Click the private endpoint with “Pending” status, click “Approve”</p>	Subscription/Resource Group Owner/Contributor
4	BU	<p>Azure portal > your_postgresql > Security > Authentication ></p> <ul style="list-style-type: none"> - Microsoft Entra Admins : add your workspace identity - Authentication = PostgreSQL and Microsoft Entra authentication 	PostgreSQL Contributor
5	BU	<p>Azure portal > Microsoft Entra ID > Manage > App Registration > All applications > select your workspace name > Manage > Certificates & Secrets > + New client secrets, copy the secret value, not secret ID.</p> <p>Go to Overview, copy tenant ID and client ID,</p> <p>Azure portal > Azure Key Vault > create secret for AZURE-CLIENT-ID/ AZURE-TENANT-ID/ AZURE-CLIENT-SECRET</p> <p>Azure portal > Azure Key Vault > IAM > grant workspace identity with “Key Vault Secrets User “ role</p>	Subscription Owner AKV Admin

Workflow for Fabric notebook (PostgreSQL)

Step	Executor	Procedure	Permission needed
6	BU	Create database named “fabricoutput” in your PostgreSQL	PostgreSQL admin
7	BU	Fabric Workspace > left lower corner, change to “Data Engineering” icon > import notebook > upload both “sink_delta_emailClicked_PostgreSQL.ipynb” and “sink_delta_emailOpened_PostgreSQL.ipynb”	Fabric Workspace Contributor
8	BU	Fabric Workspace > click the notebook “sink_delta_emailClicked_PostgreSQL”, remove existing lakehouse if any , click Lakehouse+ button, select your lakehouse,	
9	BU	Edit the notebook, AKV_ENDPOINT = https://xxx.vault.azure.net/ jdbc_url = "jdbc:postgresql://xxx.postgres.database.azure.com:5432/fabricoutput" cutoffdate = "2024-05-09 09:46:55“ any record’s timestamp before this cutoffdate will be ignored, will not be ingested to PostgreSQL	
10	BU	Fabric Workspace > click the “...” button next to the notebook “sink_delta_emailClicked_PostgreSQL” > Settings > Schedule > set your scheduled running period	
11	BU	Repeat steps 8-10 for the notebook “sink_delta_emailOpened_PostgreSQL”	
12	BU	The data will be stored in PostgreSQL database:“fabricoutput”, tables: “emailopened” and “emailclicked”	
13	BU	Testing routines 1. Open the notebook 2. Click Connect > New standard session > wait for session connected (8mins) > click “Run all” 3. To repeat the test , you need to unfreeze cell #4 “# just for debug”, change the cutoffdate value in cell #1 to the date you needed, unfreeze this cell #4 and then run this cell only then lasttimestamp will be reset. Freeze this cell again before you execute “Run all”	

Fabric notebook read shortcut and write to ADLS2



Workflow for Fabric notebook (ADLS2)

Step	Executor	Procedure	Permission needed
0	BU	Access to https://app.fabric.microsoft.com/home Click “Power BI” icon > Workspaces > Select your workspace <ul style="list-style-type: none">- You will find a lakehouse named “Dataverse_xxx” is created by “Link to Microsoft Fabric”, you can delete this lakehouse- Create a new lakehouse, click “+New item” button, select lakehouse	Fabric workspace contributor
1	BU	Go to lakehouse page > click “...” icon next to “Files” > New shortcut > Dataverse <ul style="list-style-type: none">- Enter your D365 CIJ environment domain- Sign on your D365 system admin for “connection credentials”- Select the tables you needed “Customer Insights Journeys/EmailClicked / EmailOpened”	Fabric admin + D365 system admin
2	BU	Azure portal > Your_Storage_account_ADLS2 > IAM Grant storage account blob contributor role to your workspace identity	Subscription/Resource Group Owner/Contributor
3	BU	Azure portal >> Your_Storage_account_ADLS2 > Network Assume you have the private endpoint in the VNET that also has FabricLink endpoint created.	Subscription/Resource Group Owner/Contributor
4	BU	Azure portal > Microsoft Entra ID > Manage > App Registration > All applications > select your workspace name > Manage > Certificates & Secrets > + New client secrets, copy the secret value, not secret ID. Go to Overview, copy tenant ID and client ID,	Subscription Owner

Workflow for Fabric notebook (ADLS2)

Step	Executor	Procedure	Permission needed
5	BU	<ol style="list-style-type: none"> 1. Azure portal > Your_Storage_account_ADLS2 > Endpoints 2. Copy Data Lake Storage endpoint https://xxx.dfs.core.windows.net/ 3. Fabric Workspace > your_lakehouse > click “...” icon next to “Files” > New shortcut > ADLS2 4. Paste your ADLS2 dfs endpoint, create connection, select Service Principal, fill in your tenant ID, client ID and client secret 5. Select your destination container and sub-folder in your ADLS2 (e.g. fabricoutput\emailclicked) 6. Give a name for this shortcut as “adls2_emailclicked” 7. Repeat step 1 for create new shortcut for “fabricoutput\emailopened” 	Subscription/Resource Group Owner/Contributor + Fabric Workspace Contributor
6	BU	Fabric Workspace > left lower corner, change to “Data Engineering” icon > import notebook > upload both “sink_delta_emailClicked_ADLS2.ipynb” and “sink_delta_emailOpened_ADLS2.ipynb”	Fabric Workspace Contributor
7	BU	Fabric Workspace > click the notebook “sink_delta_emailClicked_ADLS2” , remove existing lakehouse if any , click Lakehouse+ button, select your lakehouse,	
8	BU	Fabric Workspace > click the “...” button next to the notebook “sink_delta_emailClicked_PostgreSQL” > Settings > Schedule > set your scheduled running period	
9	BU	Repeat step 7-8 for the notebook “sink_delta_emailOpened_PostgreSQL”	
10	BU	The data will be stored in ADLS2 container “fabricoutput” with path “\emailopened” and “\emailclicked”	
11	BU	Testing routines <ol style="list-style-type: none"> 1. Open the notebook 2. Click Connect > New standard session > wait for session connected (8mins) > click “Run all” 3. To repeat the test , you need to delete the folders inside fabricoutput container 	

References

[Set up and use private links for secure access to Fabric - Microsoft Fabric | Microsoft Learn](#)

[Link your Dataverse environment to Microsoft Fabric and unlock deep insights - Power Apps | Microsoft Learn](#)

Screenshots : PrivateLink

Privatelink Step 1

Microsoft 365 admin center

Search

Home

Users

Teams & groups

Roles

Role assignments

Administrative units

Resources

Marketplace

Billing

Copilot

Support

Settings

Setup

Reports

Home > Role assignments

Role assignments

Microsoft Entra ID Exchange Intune Billing

Assign Microsoft Entra (Microsoft Entra ID) built-in roles to users who need access to other admin centers and resources in Microsoft Entra ID, such as users, groups, and apps that use Microsoft Graph API.

[Learn more about roles in Microsoft 365](#)

Add to favorites

Assign admins

Run As

Compare roles

<input checked="" type="checkbox"/>	Name ↑	Description
<input checked="" type="checkbox"/>	Fabric Administrator	Full access to Microsoft Fabric man...

Show all roles

Fabric Administrator

Run As

General Assigned Permissions

[Learn more about assigning admin roles](#)

Add users

Add groups

<input checked="" type="checkbox"/>	Admin name	Last sign-in	Scope
-------------------------------------	------------	--------------	-------

Nobody has been assigned to this role yet.

Select 'Add users' or 'Add groups' to get started.

Privatelink

Step 4

Microsoft Fabric

Search

Home

Create

Browse

OneLake data hub

Apps

Metrics

Monitor

Workspaces

Data Science Team

Dyn365CU

...

Admin portal

Tenant settings

Usage metrics

Users

Premium Per User

Audit logs

Domains New

Workloads

Capacity settings

Refresh summary

Embed Codes

Organizational visuals

Azure connections

Workspaces

Custom branding

Protection metrics

Fabric identities

Featured content

Help + support

Export and sharing settings

▷ Publish to web

Disabled for the entire organization

Advanced networking

⚡ Azure **Private** Link

Enabled for the entire organization

Increase security by allowing people to use a **Private** Link to access your Fabric tenant. Someone will need to finish the set-up process in Azure. If that's not you, grant permission to the right person or group by entering their email. [Learn More](#) | [Set-up instructions](#)

Review the [considerations and limitations](#) section before enabling **private** endpoints.

☒

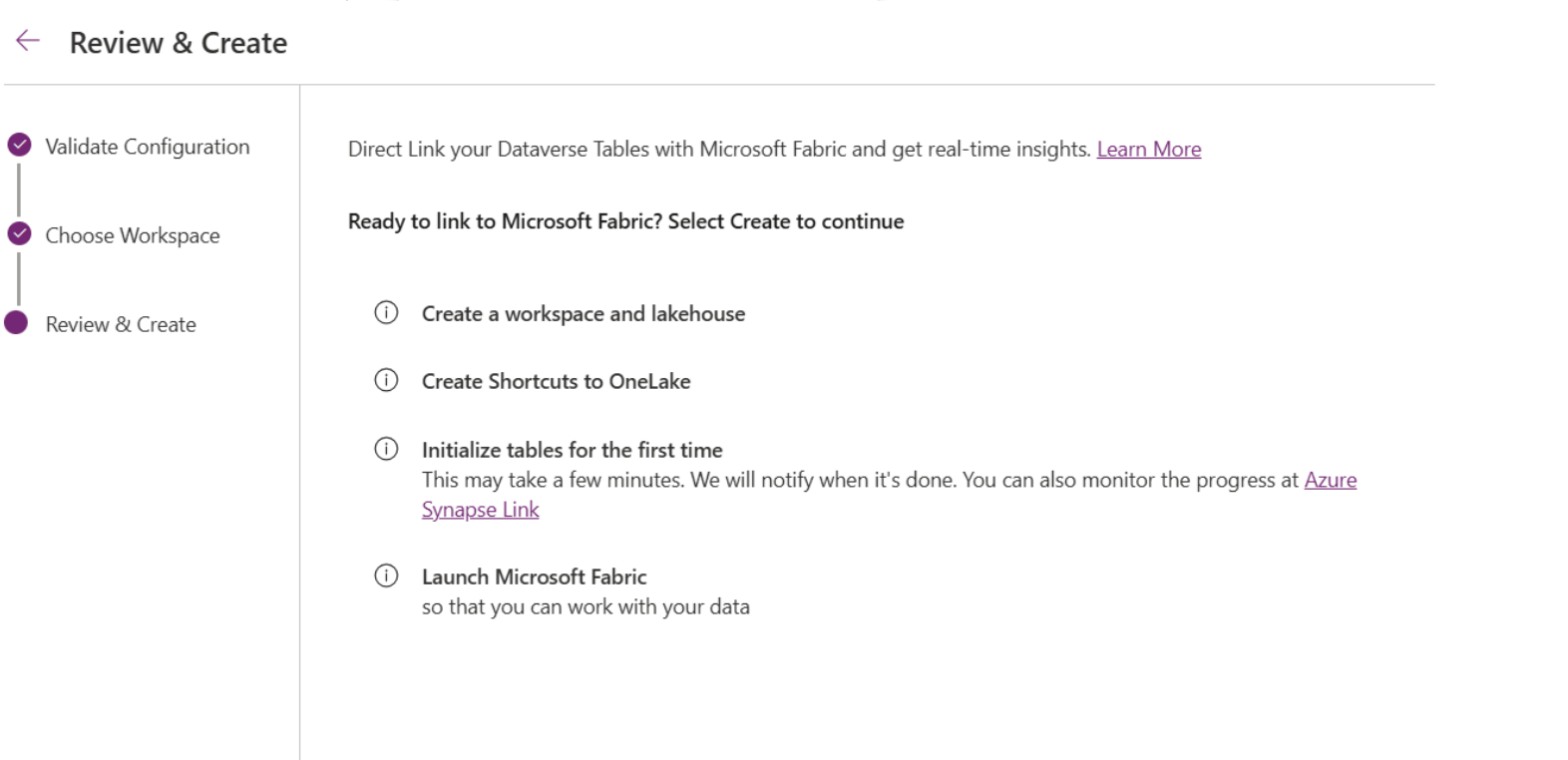
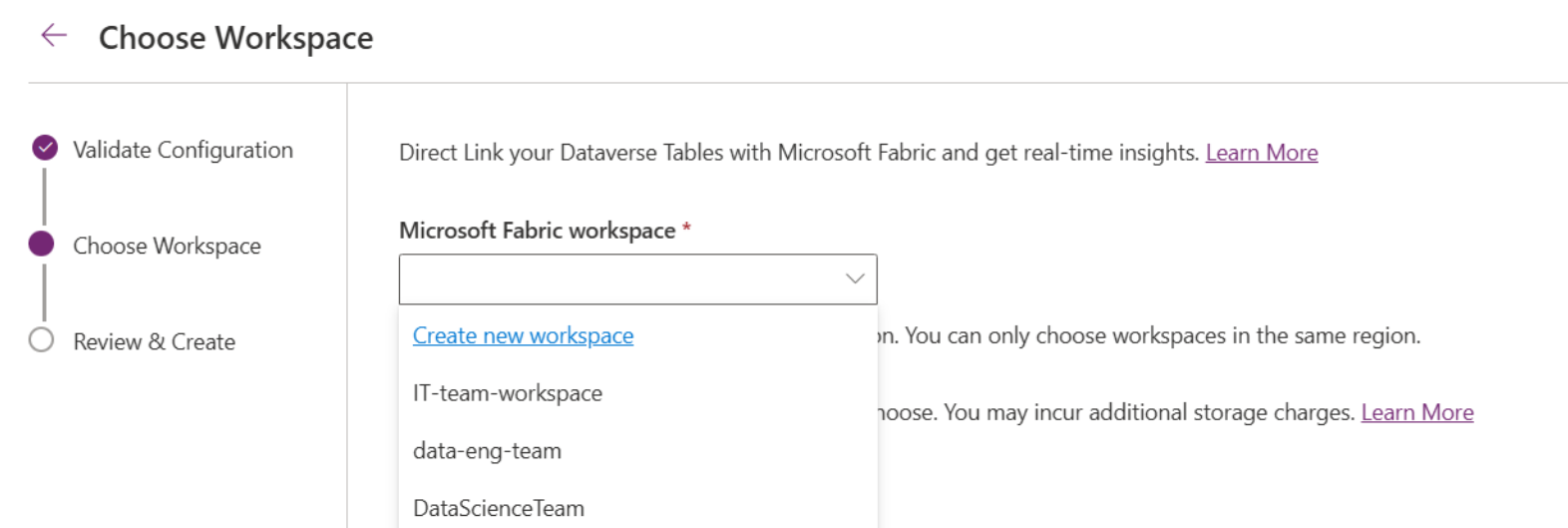
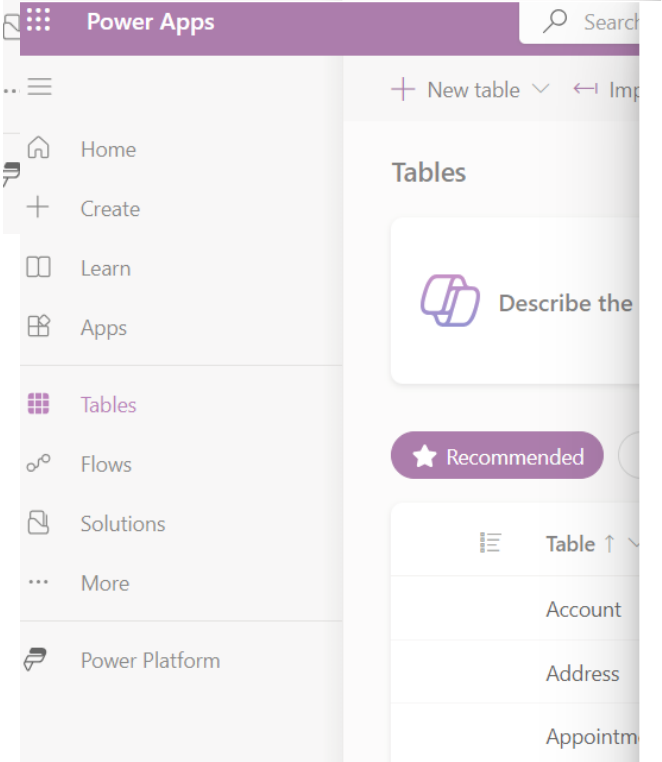
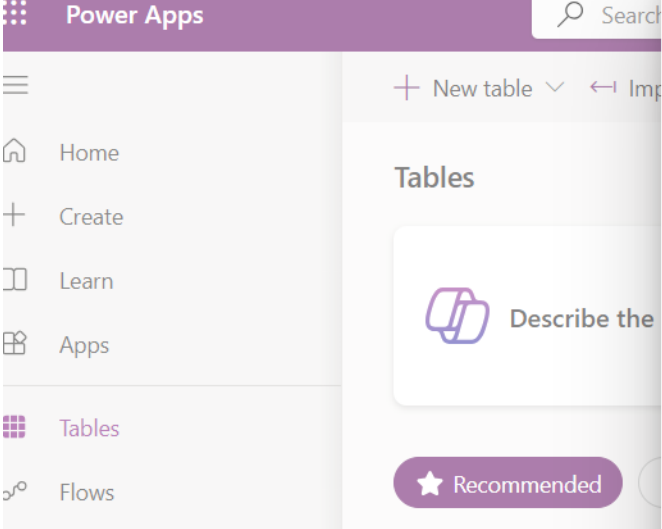
 Enabled

⚠ This setting applies to the entire organization

Apply

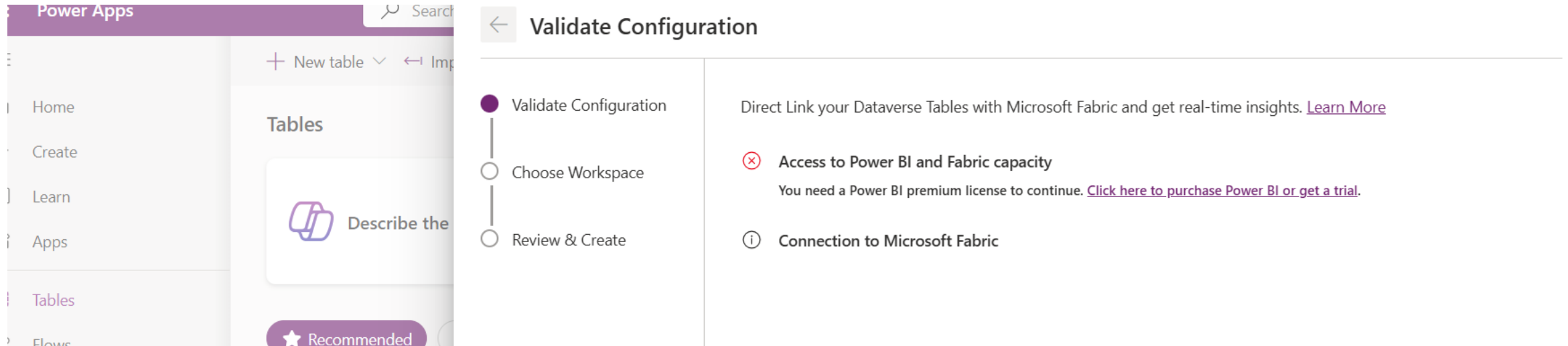
Cancel

Privatelink
Step 8



Block **Public** Internet Access Enabled for the entire organization

If you disable public access, you cannot setup any "Link to Microsoft Fabric"



The screenshot displays the Power Apps interface. On the left, the 'Power Apps' sidebar is visible with options like Home, Create, Learn, Apps, Tables, and Flows. The main area shows the 'Validate Configuration' screen. A progress bar on the left indicates the steps: 'Validate Configuration' (selected), 'Choose Workspace', and 'Review & Create'. The right pane shows the configuration details for 'Direct Link your Dataverse Tables with Microsoft Fabric and get real-time insights. [Learn More](#)'. Two configuration items are listed:

- Access to Power BI and Fabric capacity** (marked with a red 'x' icon): You need a Power BI premium license to continue. [Click here to purchase Power BI or get a trial.](#)
- Connection to Microsoft Fabric** (marked with an 'i' icon):

Block **Public** Internet Access

Enabled for the entire organization

Turn on Block Public Internet Access?


Private endpoints powered by Azure Private Link are not supported for some items in Microsoft Fabric, including Microsoft Fabric trial capacities. With the Block Public Internet Access setting on, users won't be able to use trial capacities, and unsupported items will not be visible or will return errors. For information about which Fabric items comply with Azure Private Link requirements, select [Learn More](#)

Advanced networking

Block **Public** Internet Access *Enabled for the entire organization*

For extra security, block access to your Fabric tenant via the **public** internet. This means people who don't have access to the Private Link won't be able to get in. Keep in mind, turning this on could take 10 to 20 minutes to take effect. [Learn More](#) [Set-up instructions](#)

☒ Enabled

 This setting applies to the entire organization

Apply

Cancel

Privatelink Step 9

Screenshots : Fabric Shortcut

ADLS2/PostgreSQL: Step 1

New shortcut

d365cij is located in the region **East US**. Any data sourced through this shortcut will be processed in the same region.

Dataverse
Power Platform

Connection settings
Environment domain

Connection credentials
Connection

Authentication kind: Organizational account

New shortcut

d365cij is located in the region **East US**. Any data sourced through this shortcut will be processed in the same region.

Dataverse
Select a bucket or directory

- > Customer Insights Journeys
- > CDS2
- ✓ msdyn_analytics
- ✓ Customer Insights Journeys (Preview)
 - > ☐ ActionEvent
 - > ☐ BotEmailLinkClicked
 - > ☐ EmailBounced
 - > ☒ EmailClicked
 - > ☐ EmailDelivered
 - > ☒ EmailOpened
 - > ☐ EmailSent
 - > ☐ EmailSoftBounced
 - > ☐ EventCheckIn
 - > ☐ FormSubmitted
 - > ☐ FormVisited

Customer Insights Journeys (Preview)

Name	Field type	Last modified
ActionEvent	Folder	—
BotEmailLinkClicked	Folder	—
EmailBounced	Folder	—
EmailClicked	Folder	—
EmailDelivered	Folder	—
EmailOpened	Folder	—
EmailSent	Folder	—
EmailSoftBounced	Folder	—
EventCheckIn	Folder	—
FormSubmitted	Folder	—

Previous

Next

Cancel

PostgreSQL: Step 4

denlaipostgresqlwestus3 | Authentication

Azure Database for PostgreSQL flexible server

Search

Compute + storage

Networking

Databases

Connect

Server parameters

Replication

Maintenance

High availability

Backup and restore

Advisor recommendations

Locks

Power Platform

Security

Authentication

Microsoft Defender for Cloud

Identity

Intelligent Performance

Monitoring

Automation

Help

Save Discard Feedback

Authentication

ⓘ Azure Active Directory (Azure AD) is now Microsoft Entra ID. [Learn more](#)

Select the authentication methods you would like to support for accessing this PostgreSQL server. PostgreSQL password authentication allows you to create roles and users. Enabling Microsoft Entra authentication allows you to create ROLES based on your Microsoft Entra accounts and generate an authentication token with a Microsoft Entra ID token.

Assign access to *

☐ PostgreSQL authentication only

☐ Microsoft Entra authentication only

☒ PostgreSQL and Microsoft Entra authentication

Admin username * ⓘ

den

[Reset password](#)

Microsoft Entra Admins

Once enabled for Microsoft Entra authentication support, Microsoft Entra admins can be added as security principals that have permissions to add or change server parameters.

+ Add Microsoft Entra Admins ⓘ

Name	Object ID	Type	Actions
denlai@denlailabs.net	76203cc0-...ca51b	User ⓘ	Delete
IT-team-workspace	ab585d50-...2d55	ServicePrincipal ⓘ	Delete

PostgreSQL: Step 5

[Home](#) > [DenLai Labs | App registrations](#) >



Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Diagnose and solve problems

▼ Manage

Branding & properties

Authentication

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

^ Essentials

Display name : [IT-team-workspace](#)

Application (client) ID : 19c6dbd8-[REDACTED]300420d7427

Object ID : cbcabc[REDACTED]c6-ae5694859f2e

Directory (tenant) ID : 9fd8775f-acbf-40a6-a[REDACTED]c

Supported account types : [My organization only](#)

Certificates (0)

Client secrets (1)

Federated credentials (1)

rectory

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to a:

New client secret

Description	Expires	Value ⓘ
notebook_secret	03/09/2026	8N_*****

PostgreSQL:

Step 5

Home > fabricd365-akv-westus2

fabricd365-akv-westus2 | Secrets

Key vault

Search << + Generate/Import Refresh Restore Backup View sample code Manage deleted secrets

The secret 'AZURE-CLIENT-SECRET' has been successfully created.

Name	Type	Status
AZURE-CLIENT-SECRET		✓ Enabled
AZURE-TENANT-ID		✓ Enabled
AZURE-CLIENT-ID		✓ Enabled

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Access policies
Events
Objects
Keys
Secrets

```
1
2 import os
3 #change to your service principle (Workspace identity) ClientID, tenantID and clientsecret
4 #customer should setup Azure Key Vault and store secret in AKV instead of hardcoding here
5 #https://www.datasarva.com/fabric-notebook-azurekeyvault/
6 os.environ["AZURE_CLIENT_ID"] = mssparkutils.credentials.getSecret('https://f[REDACTED]vault.azure.net/', 'AZURE-CLIENT-ID')
7 os.environ["AZURE_TENANT_ID"] = mssparkutils.credentials.getSecret('https://f[REDACTED]vault.azure.net/', 'AZURE-TENANT-ID')
8 os.environ["AZURE_CLIENT_SECRET"] = mssparkutils.credentials.getSecret('https://f[REDACTED]us2.vault.azure.net/', 'AZURE-CLIENT-SECRET')
```

ADLS2 Step 6 PostgreSQL Step 7

ork

https://app.fabric.microsoft.com/home?experience=data-engineering

Synapse Data Engineering Home

Welcome to Microsoft Fabric

Get started with Synapse Data Engineering

Recommended items to create

Lakehouse

Notebook

Environment

Spark Job Definition

Data pipeline

Import notebook

Current workspace: IT-team-workspace
Items will be saved to this workspace.

Learn more about Synapse Data Engineering

What's a lakehouse?

Get started with data engineering

[Open](#)

Get data experience in lakehouse

Get started with data engineering

[Open](#)

Get started with Spark Job De

Get started with data engineering

[Open](#)

ADLS2 Step 7
PostgreSQL Step 8

sink_delta_emailClicked_ADLS2 | Saved

Search

Home | Edit | Run | View

Run all

Connect

PySpark (Python)

← All sources

⏪

Lakehouses

+ Lakehouse

d365dataverse

Tables

Files

EmailClicked

EmailOpened

adls2_emailclicked

adls2_emailopened

Other people in your organization n

-- SourceSystem: 1
-- State: string (
-- TargetUrl: stri
-- Timestamp: time
-- UsageType: stri
-- Version: intege
-- VisitDuration:
-- VisitorAnonymou
-- VisitorId: stri
-- VisitorReturnin

1 # Get a list
2 columns = df.
3 print("Columr

[4] ✓

Columns: ['AccountI
'CountryIsoCode', 'C

ADLS2 Step 8

PostgreSQL Step 10

Power BI IT-team-workspace

Search

IT-team-workspace

+ New item New folder (preview) Upload

Name	Type
d365dataverse	Lakehouse
d365dataverse	Semantic model
d365dataverse	SQL analytics endpoint
sink_delta_emailClicked_ADLS2	Notebook
sink_delta_emailClicked_postgresql	Notebook
sink_delta_emailOpened_ADLS2	Notebook
sink_delta_emailOpened_postgresql	Notebook

sink_delta_emailOpened_postgresql Notebook

About Endorsement **Schedule**

Other people in your organization may have access to this notebook in this workspace. Carefully review this item before scheduling it.

No previous history

The scheduled refresh is turned off

Schedule

Scheduled run

☒ On ☐ Off

Repeat

By the minute

Every

15 minute(s)

Start date and time

dd/mm/yyyy --:--

End date and time

dd/mm/yyyy --:--

Time zone

(UTC+08:00) Beijing, Chongqing, Hong Kong

PostgreSQL: Step 13

```
1 # just for debug
```

Run all above this cell

Run this cell and all below

Run selected code



Unfreeze cell

```
StructType([  
    tField("lasttimestamp", StringTy
```

```
the DataFrame  
cutoffdate,)]  
df = spark.createDataFrame(data,
```

```
10 # Write DataFrame to PostgreSQL  
11 write_ts_df.write \  
12     .format("jdbc") \  
13     .option("url", jdbc_url) \  
14     .option("driver", "org.postgresql.Driver")
```