Lab 03: Security for Data and Workspace

Introduction

In this lab, you will start by creating a new workspace, a Warehouse and Lakehouse. Then you will assign users to the various workspace roles and warehouse security features.

Objectives

After completing this lab, you will be better able to:

1. Manage Workspace roles
2. Manage items permissions
3. Access secured data sources from Lakehouse Endpoint, Spark, DataFlow Gen2
4. Apply granular security features for warehouse

Estimated time to complete this lab

180 minutes

Lab Prerequisites

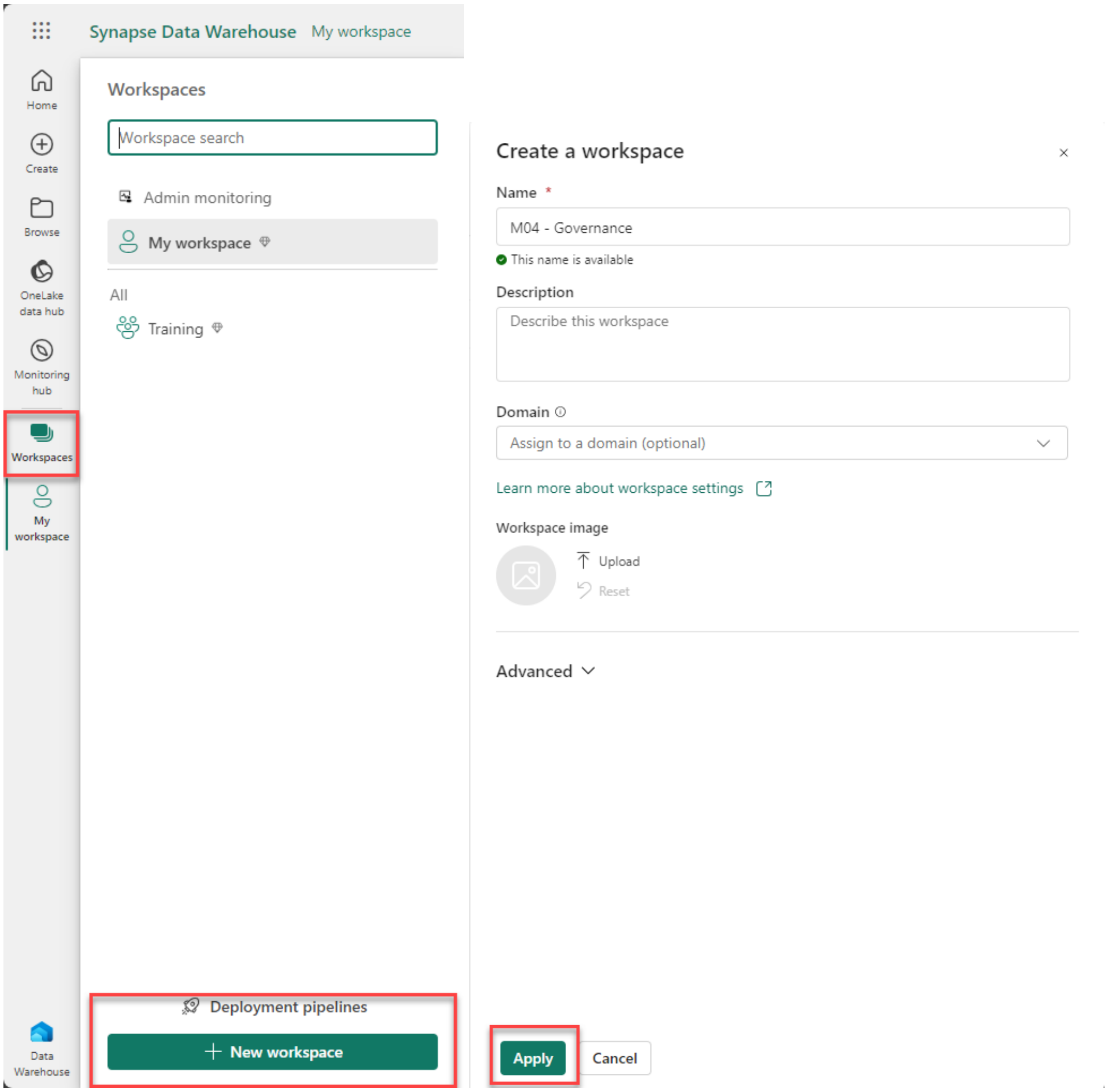
- A Fabric capacity or Fabric trial
- In Subsequent tasks, you will need more 2 accounts apart from the one you used to create the workspace.
- Azure Data Studio or SSMS (SQL Server Management Studio)

Contents

Task 1: Creating a new workspace

In this task, you will create a new workspace to be used in the remainder of the lab.

- Connect to the Microsoft Fabric environment (Analyze (powerbi.com))
- Now, select "Workspaces" in the left side menu and click "+ New workspace"



Create a workspace

Name *

M04 - Governance

This name is available

Description

Describe this workspace

Domain

Assign to a domain (optional)

Learn more about workspace settings

Workspace image

Upload

Reset

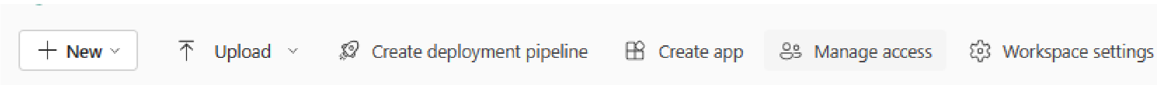
Advanced

- Provide the name as **M04 - Governance**.
- Click apply.

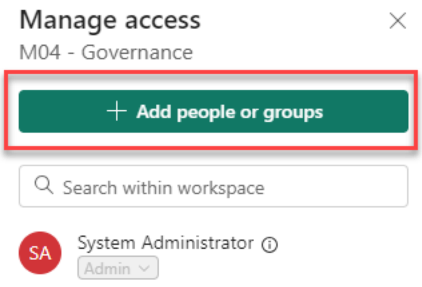
Task 2: Managing workspace permissions

In this task, you will assign permissions to different users.

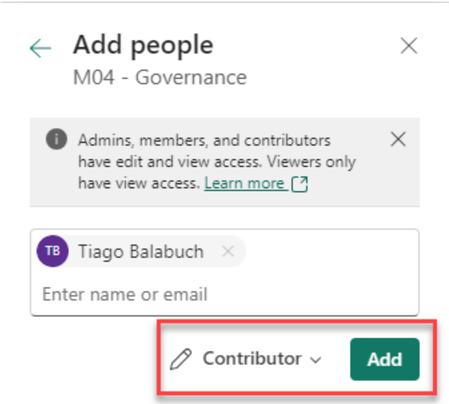
- Click "Manage access" from the top



Click "+ Add people or groups"



- Enter the name or email address - user01@yourcompany.com
- Choose "Contributor" permission from the dropdown list
- Click "Add"



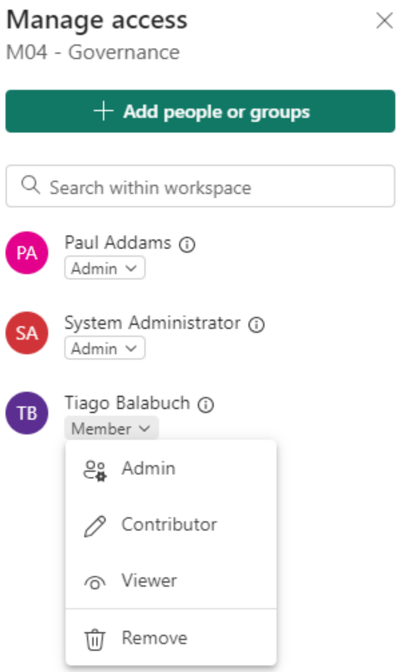
Admins, members, and contributors have edit and view access. Viewers only have view access. Learn more

TB Tiago Balabuch

Enter name or email

Contributor

- (Optional) Repeat the above steps for another user. But instead of "Contributor" choose "Admin" permission from the dropdown list and click "Add"
- Now, let's change permission for a user. Click "Manage access"
- Find the user user01@yourcompany.com.
- From the dropdown list, choose "Member". There is no need to save. It's automatically saves.



Manage access
M04 - Governance

Paul Addams
Admin

System Administrator
Admin

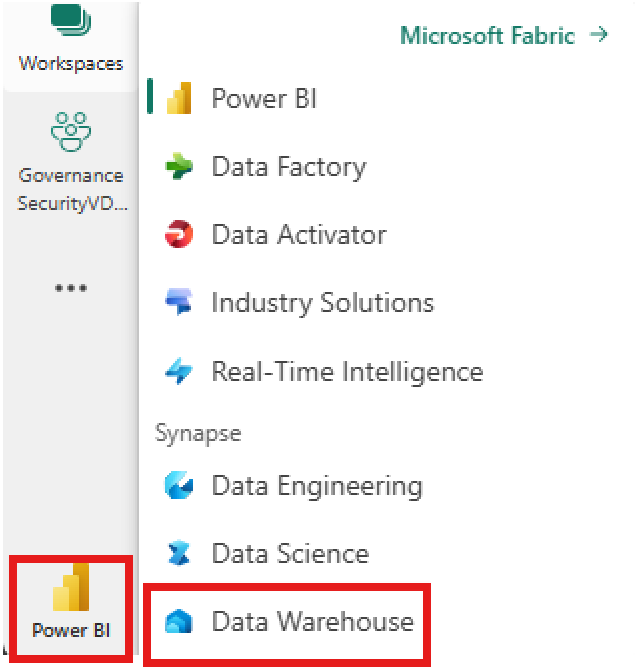
Tiago Balabuch
Member

- Follow similar steps above to remove permission from users (user01@yourcompany.com and user02@yourcompany.com)

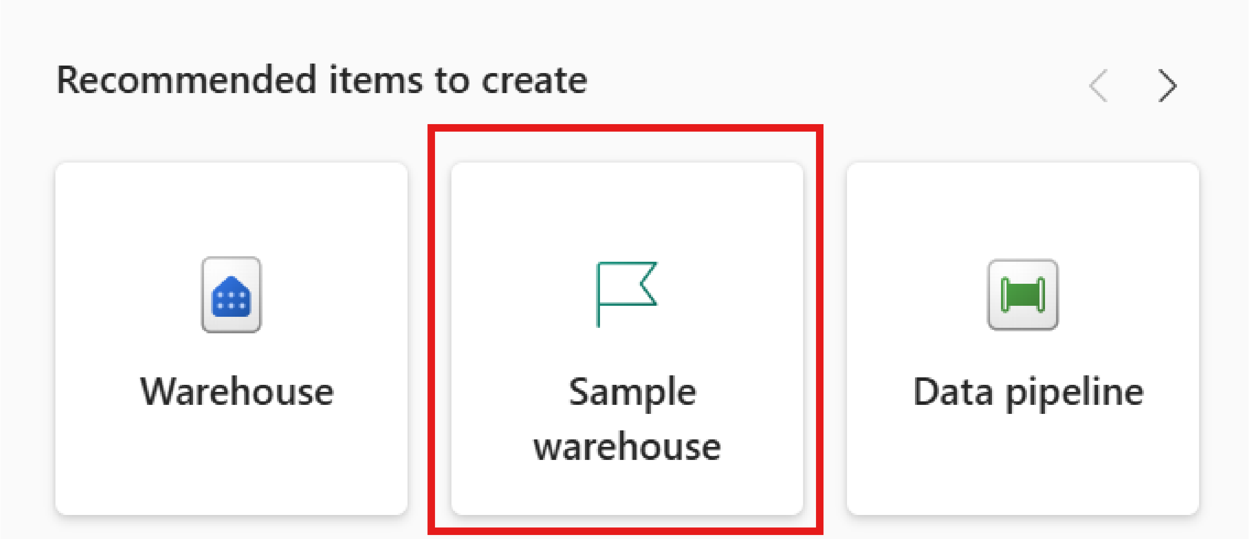
Task 3: Managing items permissions

In this task, you will manage item permission within the workspace.

- In the M04 - Governance workspace, switch to Data Warehouse experience

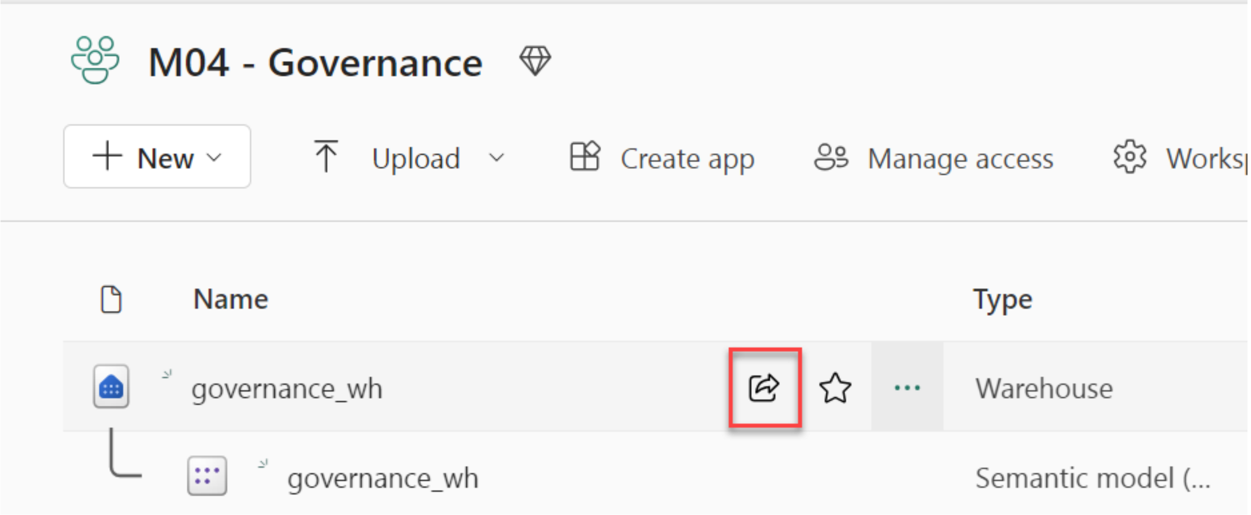


- On the right side under recommended items to create, click “Sample warehouse” as shown below

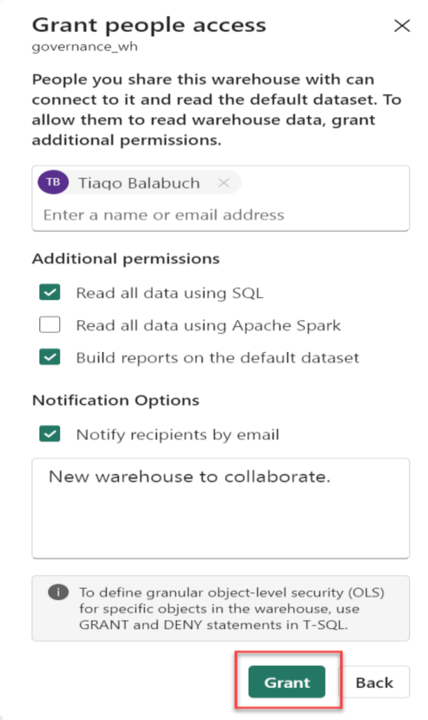


Provide a name for the new warehouse eg., governance_wh

- Go back to M04 - Governance workspace. In governance_wh warehouse click on the “Share” button.



- Enter the name or email address of the person/group you want to share. In this case user01@yourcompany.com
- By default, "Build reports on the default dataset" is selected.
- Additionally, select "Read all data using SQL"
- By default, "Notify recipients by email" is selected. Add a message to the user – "New warehouse to collaborate."
- Click "Grant"



Grant people access

governance_wh

People you share this warehouse with can connect to it and read the default dataset. To allow them to read warehouse data, grant additional permissions.

TB Tiago Balabuch

Enter a name or email address

Additional permissions

☑ Read all data using SQL

☐ Read all data using Apache Spark

☑ Build reports on the default dataset

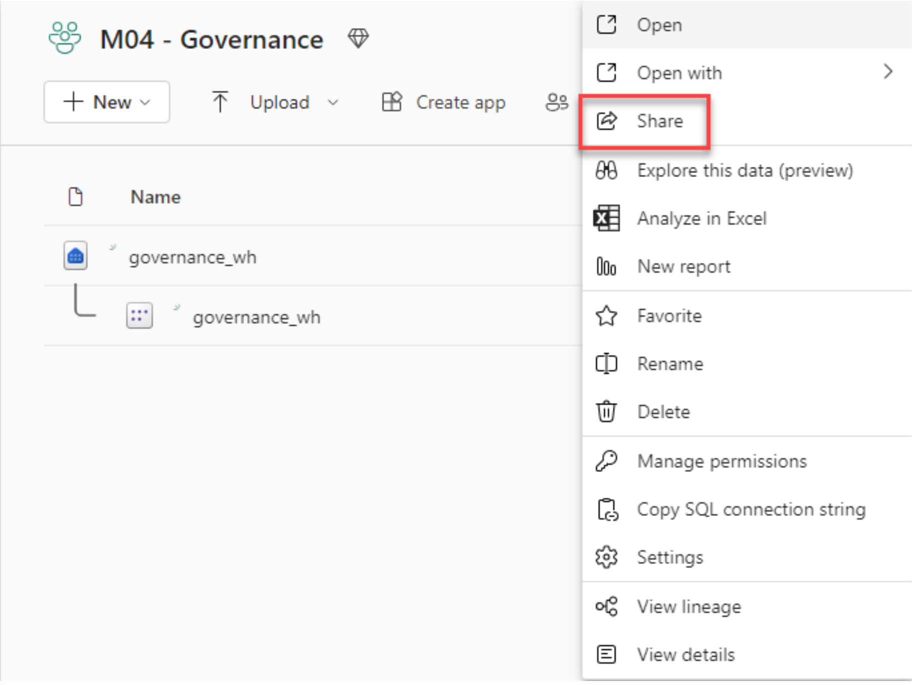
Notification Options

☑ Notify recipients by email

New warehouse to collaborate.

To define granular object-level security (OLS) for specific objects in the warehouse, use GRANT and DENY statements in T-SQL.

Again, in governance_wh warehouse click the ellipsis against the warehouse and from the menu, click "Share"



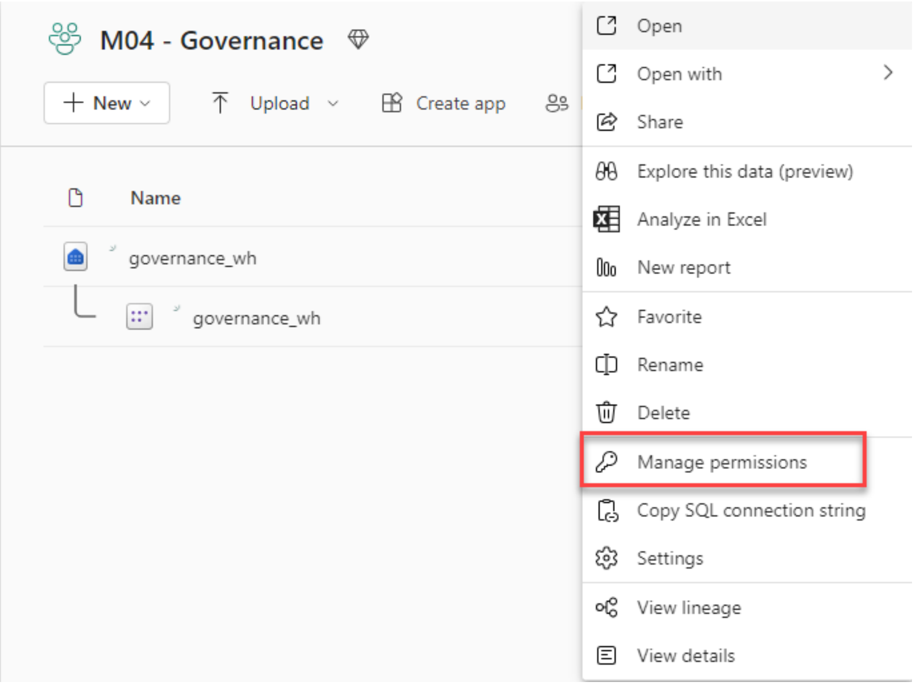
Enter the name or email address of the person/group you want to share. In this case user02@yourcompany.com

Unselect all permissions. This will grant only permission to connect to Warehouse. It will be used to grant more granular control.

By default, “Notify recipients by email” is selected.

Click “Grant”

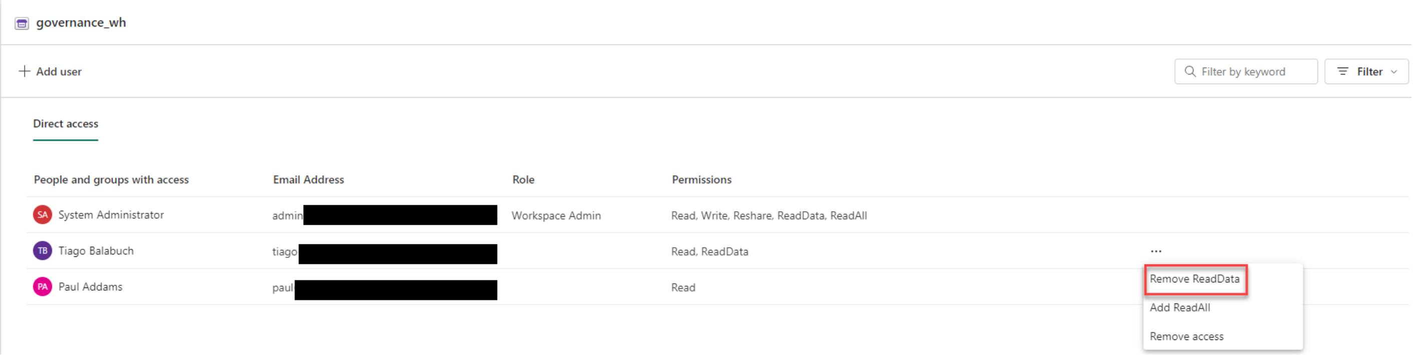
In governance_wh warehouse, click the ellipsis and from the menu, click “Manage permission”



Find the people or group you want and click the ellipsis. In this case user01@yourcompany.com

Click "Remove ReadData"

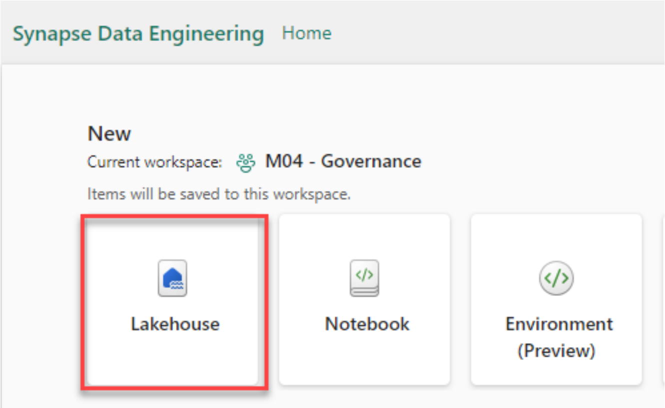
There is no need to save. It's automatically saved.



People and groups with access	Email Address	Role	Permissions
System Administrator	admin[redacted]	Workspace Admin	Read, Write, Reshare, ReadData, ReadAll
Tiago Balabuch	tiago[redacted]		Read, ReadData
Paul Addams	paul[redacted]		Read

Next, in the M04 - Governance workspace, switch to Data Engineering experience and click "Lakehouse"

In the new Lakehouse provide a name eg., governance_lh


Synapse Data Engineering
Home
New
Current workspace: M04 - Governance
Items will be saved to this workspace.
Lakehouse
Notebook
Environment (Preview)

Go back to M04 - Governance workspace

In governance_lh lakehouse click on the “Share” button.

Enter the name or email address of the person/group you want to share. In this case user01@yourcompany.com

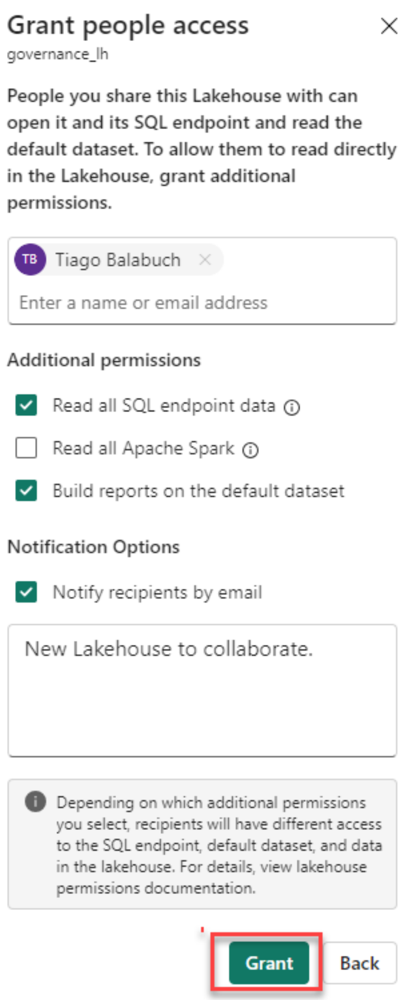
Select “Read all SQL endpoint data”.

Select “Build reports on the default dataset”.

By default, “Notify recipients by email” is selected.

Add a message to the user – “New Lakehouse to collaborate.”

Click “Grant”



Grant people access

governance_lh

People you share this Lakehouse with can open it and its SQL endpoint and read the default dataset. To allow them to read directly in the Lakehouse, grant additional permissions.

TB Tiago Balabuch

Enter a name or email address

Additional permissions

☑ Read all SQL endpoint data

☐ Read all Apache Spark

☑ Build reports on the default dataset

Notification Options

☑ Notify recipients by email

New Lakehouse to collaborate.

Depending on which additional permissions you select, recipients will have different access to the SQL endpoint, default dataset, and data in the lakehouse. For details, view lakehouse permissions documentation.

In governance_lh lakehouse, click in the ellipsis.

From the menu, click “Share”

Enter the name or email address of the person/group you want to share. In this case user02@yourcompany.com

Select “Read all Apache Spark” .

By default, “Notify recipients by email” is selected.

Add a message to the user – “New lakehouse to collaborate using Spark”

Click “Grant”

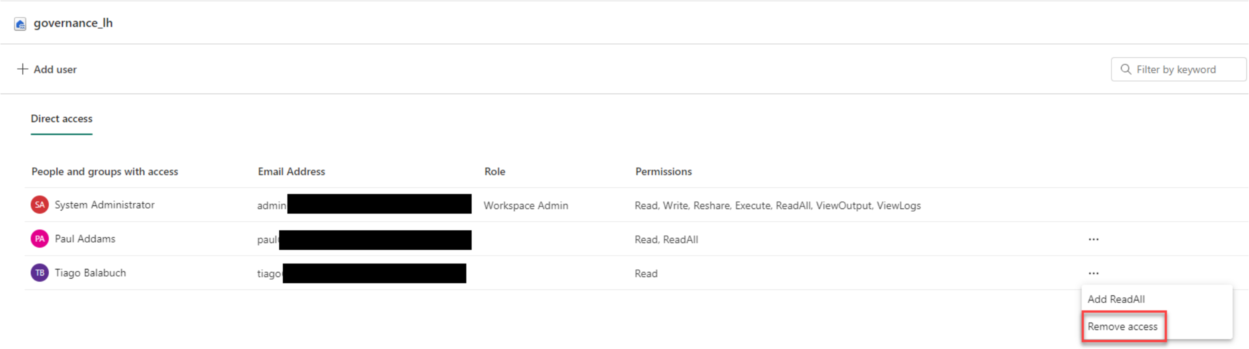
In governance_lh lakehouse, click the ellipsis.

From the menu, click “Manage permission”

Find the people or group you want and click the ellipsis. In this case user01@yourcompany.com and user02@yourcompany.com

Click “Remove access”

There is no need to save. It’s automatically saved.



governance_lh

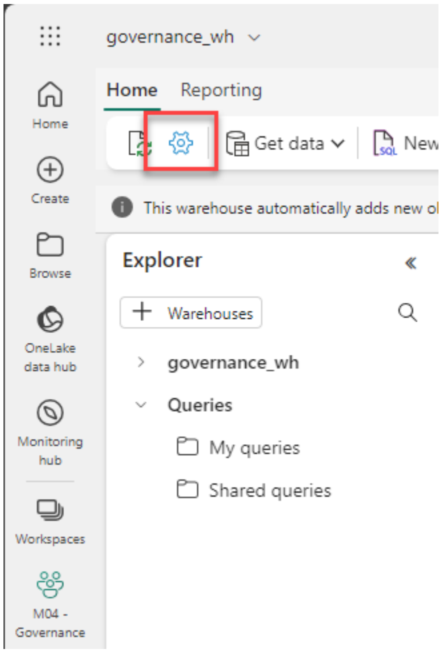
People and groups with access	Email Address	Role	Permissions	
SA System Administrator	admin[redacted]	Workspace Admin	Read, Write, Reshare, Execute, ReadAll, ViewOutput, ViewLogs	
PA Paul Addams	paul[redacted]		Read, ReadAll	...
TB Tiago Balabuch	tiago[redacted]		Read	...

Task 4: Granular permission

In this task, you will learn how to grant granular permissions in the warehouse objects.

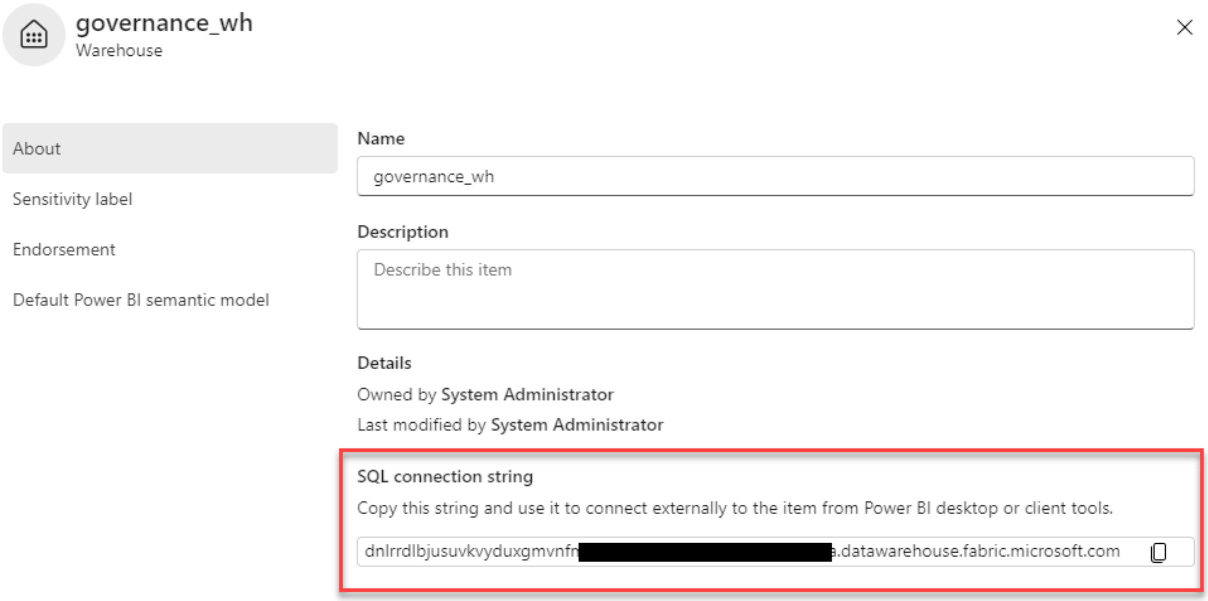
This step should be done by Workspace Admin. In the Governance workspace, select governance_wh.

Make sure “Home” menu is selected, and then, select settings (gear button)



This warehouse automatically adds new o

Copy the SQL connection string.



governance_wh
Warehouse

Name
governance_wh

Description
Describe this item

Details
Owned by System Administrator
Last modified by System Administrator

SQL connection string
Copy this string and use it to connect externally to the item from Power BI desktop or client tools.
dnlrrdlbjusuvkvyduxgmvnf[redacted].datawarehouse.fabric.microsoft.com

Open SQL Server Management Studio (SSMS) or Azure Data Studio

If you are using Azure Data Studio, make sure your account is linked.

[Explore Azure SQL resources with the Azure View - Azure Data Studio | Microsoft Learn]

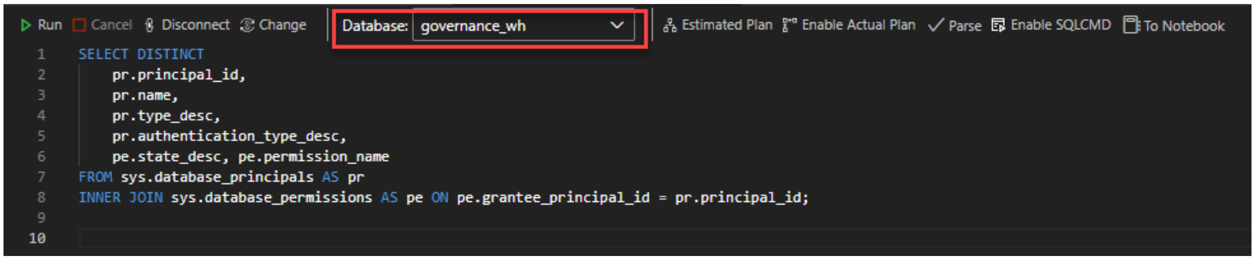
You have to use Microsoft Entra ID to authenticate.

Once you are connected to your warehouse, select governance_wh and create a new query

Copy and paste the following command:

```
SELECT DISTINCT
  pr.principal_id,
  pr.name,
  pr.type_desc,
  pr.authentication_type_desc,
  pe.state_desc, pe.permission_name
FROM sys.database_principals AS pr
INNER JOIN sys.database_permissions AS pe ON pe.grantee_principal_id = pr.principal_id;
```

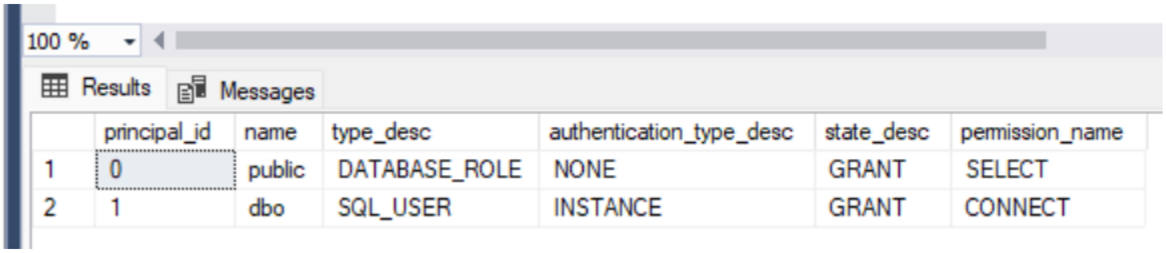
Run the query.



Database: governance_wh

```
SELECT DISTINCT
    pr.principal_id,
    pr.name,
    pr.type_desc,
    pr.authentication_type_desc,
    pe.state_desc, pe.permission_name
FROM sys.database_principals AS pr
INNER JOIN sys.database_permissions AS pe ON pe.grantee_principal_id = pr.principal_id;
```

The output does not show the users or the user permissions that are granted at the workspace level or item level.



	principal_id	name	type_desc	authentication_type_desc	state_desc	permission_name
1	0	public	DATABASE_ROLE	NONE	GRANT	SELECT
2	1	dbo	SQL_USER	INSTANCE	GRANT	CONNECT

Copy and paste the following query

```
GRANT SELECT ON OBJECT::dbo.Trip TO [<user01@yourcompany.com>];
```

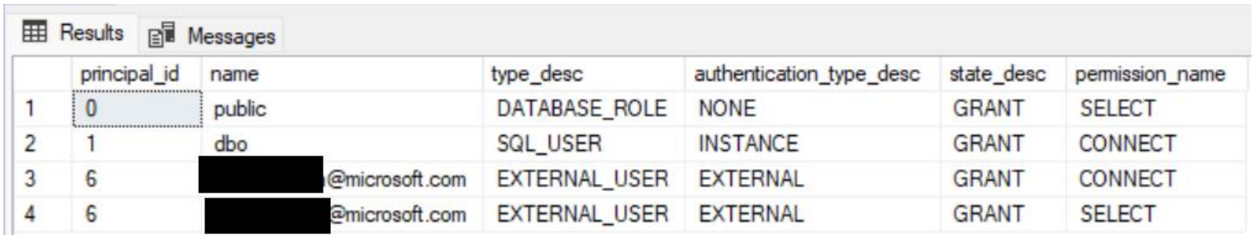
```
GO
```

Replace user01@yourcompany.com for the user you want to assign this permission.

You must keep the brackets "[ ]"

Run this query again to confirm that new permission was assigned correctly.

```
SELECT DISTINCT
  pr.principal_id,
  pr.name,
  pr.type_desc,
  pr.authentication_type_desc,
  pe.state_desc, pe.permission_name
FROM sys.database_principals AS pr
INNER JOIN sys.database_permissions AS pe ON pe.grantee_principal_id = pr.principal_id;
```



	principal_id	name	type_desc	authentication_type_desc	state_desc	permission_name
1	0	public	DATABASE_ROLE	NONE	GRANT	SELECT
2	1	dbo	SQL_USER	INSTANCE	GRANT	CONNECT
3	6	[redacted]@microsoft.com	EXTERNAL_USER	EXTERNAL	GRANT	CONNECT
4	6	[redacted]@microsoft.com	EXTERNAL_USER	EXTERNAL	GRANT	SELECT

Step 4.1 – Checking permission

NOTE: This step should be done by the user: user01@yourcompany.com

If you are using Azure Data Studio, make sure your account is linked.

Explore Azure SQL resources with the Azure View - Azure Data Studio | Microsoft Learn

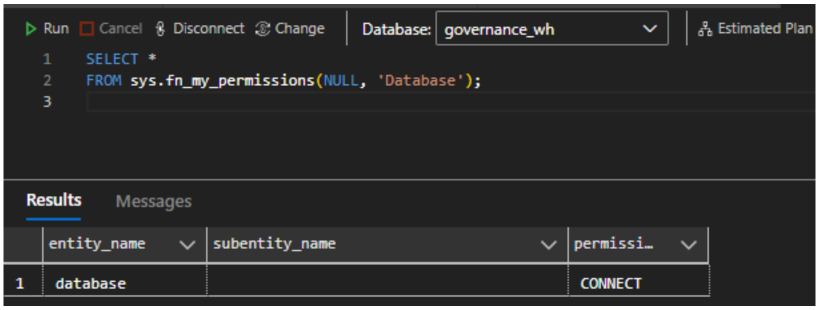
You have to use Microsoft Entra ID to authenticate.

Once you are connected to your warehouse, select governance_wh and create a new query

Copy and paste the following command in the new query

```
SELECT *
FROM sys.fn_my_permissions(NULL, 'Database');
```

Run the command.



```
SELECT *
FROM sys.fn_my_permissions(NULL, 'Database');
```

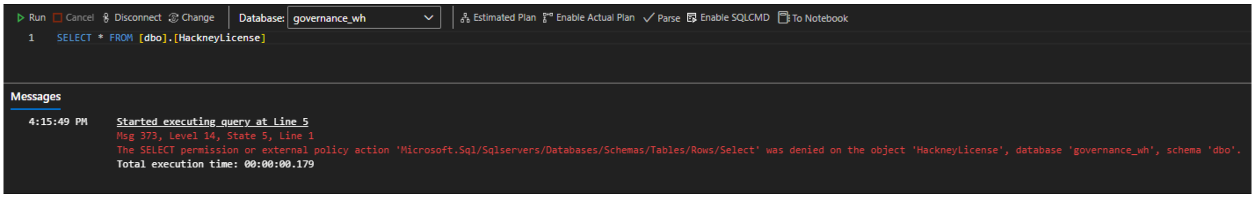
	entity_name	subentity_name	permissi…
1	database		CONNECT

This commands show User's database scoped permissions.

Copy and paste the following command

SELECT * FROM [dbo].[HackneyLicense]

This will return an error because the user has no permission to dbo.HackneyLicense table.



```
SELECT * FROM [dbo].[HackneyLicense]
```

```
4:15:49 PM     Started executing query at Line 5
               Msg 373, Level 14, State 5, Line 1
               The SELECT permission or external policy action 'Microsoft.Sql/Sqlservers/Databases/Schemas/Tables/Rows/Select' was denied on the object 'HackneyLicense', database 'governance_wh', schema 'dbo'.
               Total execution time: 00:00:00.179
```

Now copy and paste the following command.

SELECT TOP 10 * FROM [dbo].[Trip]

This table has more than 2 million of rows. Just bring top 10 to validate the permissions.

You can check your permissions using the following command.

SELECT *

FROM sys.fn_my_permissions('dbo.Trip', 'Object');

This command show the permissions on Trip table.

SELECT *

FROM sys.fn_my_permissions('dbo.HackneyLicense’, 'Object');

This command show the permissions on HackneyLicense table. As you noticed, there is no result, meaning that you don’t have permission on this table.

Step 4.2 – Changing permission

This step should be done using the Workspace Admin account.

If you are using Azure Data Studio, make sure your account is linked

You have to use Microsoft Entra ID to authenticate.

Once you are connected to your warehouse, select governance_wh and create a new query.

Copy and paste the following command:

```
REVOKE SELECT ON OBJECT::dbo.Trip TO [<user01@yourcompany.com>];

GO
```

It will revoke permission on Trip table to a specific user.

Replace user01@yourcompany.com for the user you want to assign this permission.

You must keep the brackets "[ ]"

Copy and paste the following command:

```
DENY SELECT ON OBJECT::dbo.Date TO [<user01@yourcompany.com>];

GO
```

This will deny SELECT permission to Date Table.

You can check these permissions using the following

```
SELECT DISTINCT

   pr.principal_id,

   pr.name,

   pr.type_desc,

   pr.authentication_type_desc,

   pe.state_desc, pe.permission_name

FROM sys.database_principals AS pr

INNER JOIN sys.database_permissions AS pe ON pe.grantee_principal_id = pr.principal_id;
```

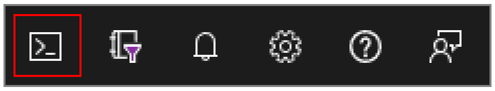
Task 5: Conditional Access

Fabric is accessible from public internet, in this task you will implement and test conditional Access to restrict login to fabric from specific IP range.

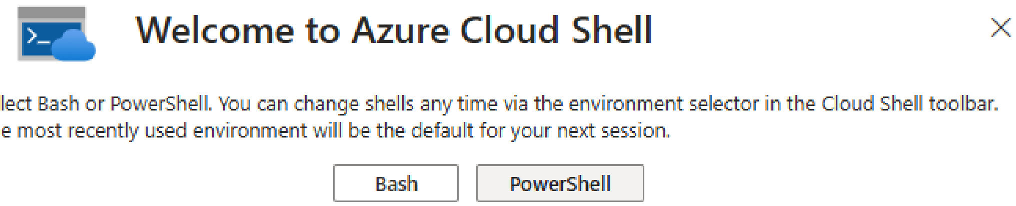
The first step is to create a Virtual Machine. In the below steps you will deploy two bicep files to deploy a VNET with the required subnets and deploy a VM.

Use the below steps to launch Azure Portal cloud shell

1. Launch Cloud Shell from the top navigation of the Azure portal.



2. Then choose PowerShell

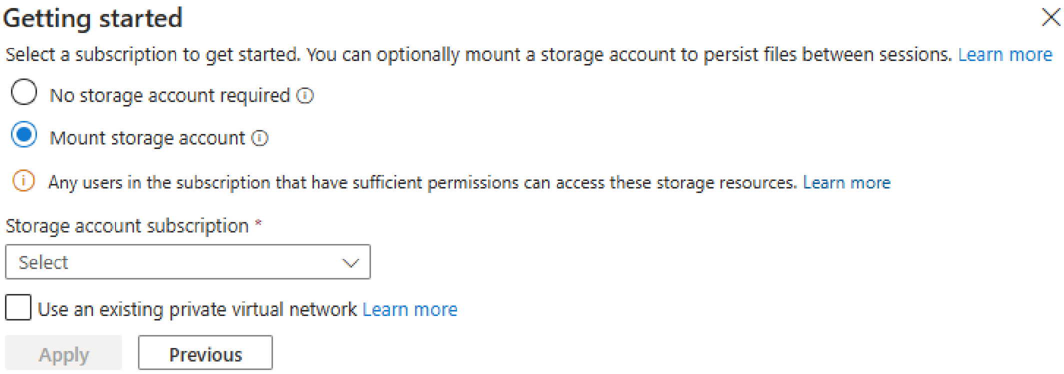


Welcome to Azure Cloud Shell

Select Bash or PowerShell. You can change shells any time via the environment selector in the Cloud Shell toolbar. The most recently used environment will be the default for your next session.

Bash PowerShell

3. The first time you start Cloud Shell you're prompted to mount an Azure Storage account for the Azure file share. Select "Mount storage account", select the appropriate subscription and click Apply



Getting started

Select a subscription to get started. You can optionally mount a storage account to persist files between sessions. Learn more

○ No storage account required ⓘ

● Mount storage account ⓘ

ⓘ Any users in the subscription that have sufficient permissions can access these storage resources. Learn more

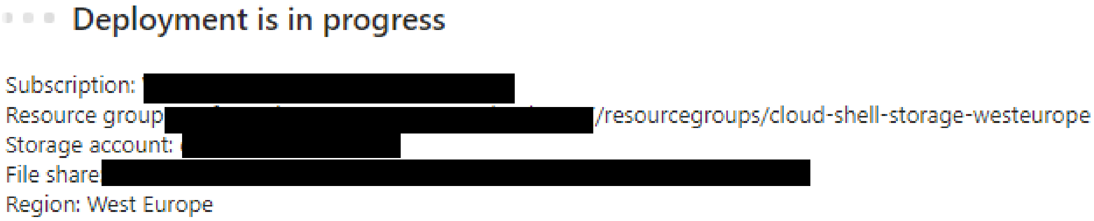
Storage account subscription *

Select

□ Use an existing private virtual network Learn more

Apply Previous

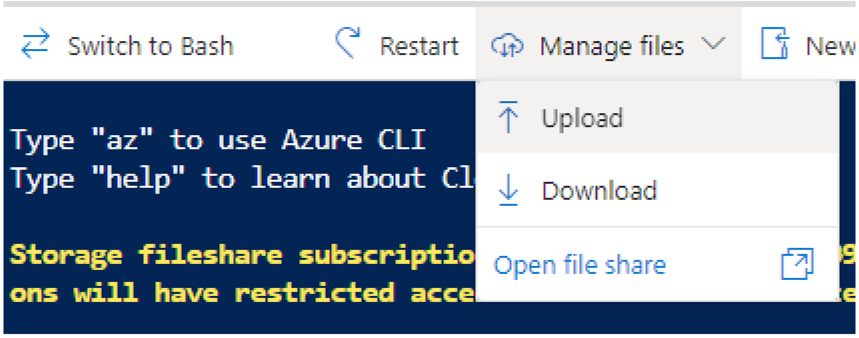
4. In the next step, select "We will create a storage account for you" and click Next. This will begin the deployment.



Deployment is in progress

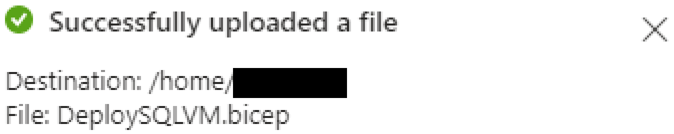
Subscription: [redacted]
Resource group [redacted]/resourcegroups/cloud-shell-storage-westeurope
Storage account: [redacted]
File share [redacted]
Region: West Europe

5. Once complete, you will see the cloudshell prompt
6. Download DeploySQLVM.bicep from here: [Fabric VBD - 7 - Governance and Security - SQLVM - All Documents;]() Download VNET.bicep from here: [Fabric VBD - 7 - Governance and Security - VNET - All Documents]()
7. Upload the bicep files VNET.bicep and DeploySQLVM.bicep by clicking on "Manage files" and selecting "Upload". Before uploading the DeploySQLVM.bicep, open the file (opening in notepad should be fine too) and provide a value for the password for the param adminPassword (line 44)
    1. NOTE: password must be between 8-123 characters long and must satisfy at least 3 of password complexity requirements from the following: 1) Contains an uppercase character 2) Contains a lowercase character 3) Contains a numeric digit 4) Contains a special character 5) Control characters are not allowed



```
Type "az" to use Azure CLI
Type "help" to learn about Cl
Storage fileshare subscriptio
ons will have restricted acce
```

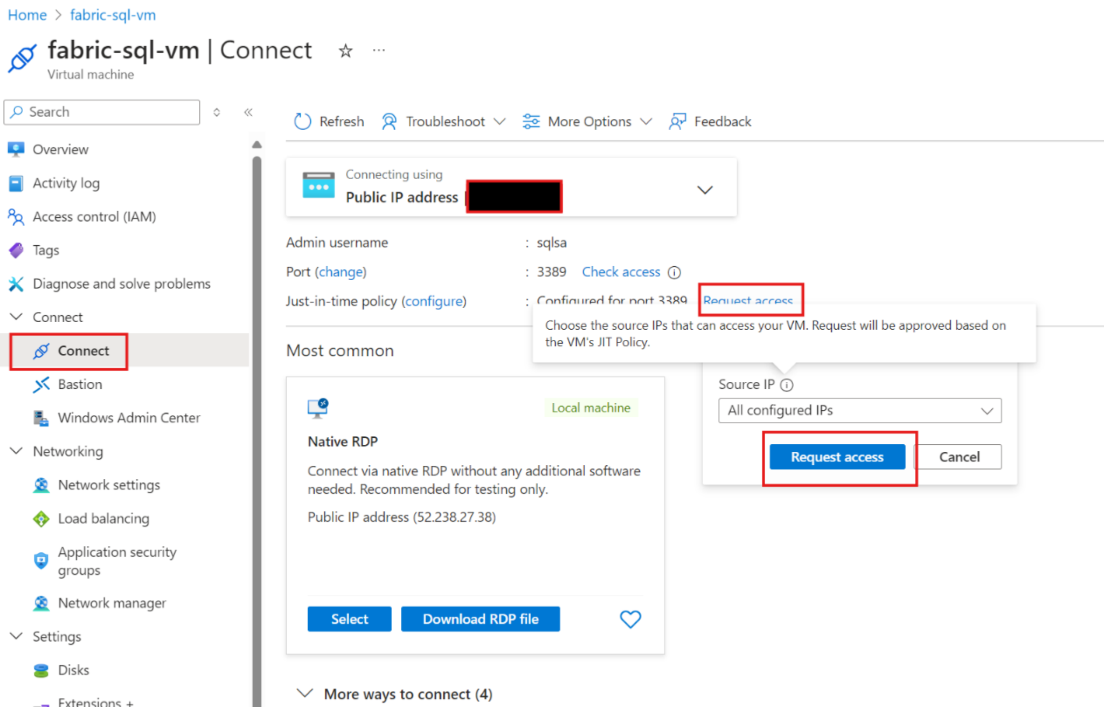
You should see a success message for each of the files you have uploaded



Successfully uploaded a file

Destination: /home/[redacted]
File: DeploySQLVM.bicep

8. If you are unable to connect to vm after inactivity, raise just in time request to regain access to it.

1. 

Connecting using
Public IP address [redacted]

Admin username : sqlsa

Port (change) : 3389 Check access

Just-in-time policy (configure) : Configured for port 3389 Request access

Choose the source IPs that can access your VM. Request will be approved based on the VM's JIT Policy.

Source IP: All configured IPs

Connect via native RDP without any additional software needed. Recommended for testing only.

Public IP address (52.238.27.38)

9. Run the below commands in the cloud shell to deploy the VNET and a SQL Server VM within the VNET. You may want to change the region name to suit your requirement. The below script does the following:

    a. Create a Resource Group that will house the VNET and the SQL Server VM
    b. Create a VNET with two subnets (PESubnet, VNETGatewaySubnet)
    c. Deploy the VM into the same resource group as the VNET (uses the PE Subnet).

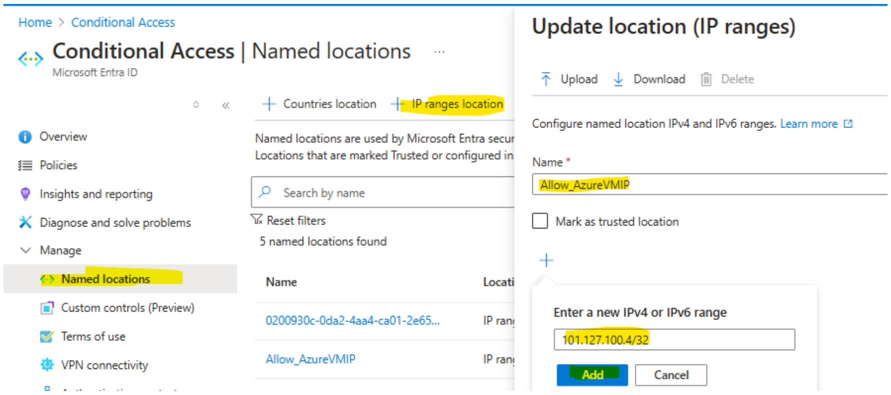
    Note: Preferably, do not change names like the resource group, VNET etc as these names are referenced in the SQL Server deployment bicep file and you may need to manually updates them

```
$SQLrgName = "fabric-sql-rg"
$region = "westeurope"
az group create --name $SQLrgName --location $region
az deployment group create --name deployVNET --resource-group $SQLrgName --
template-file  VNET.bicep
az deployment group create --name deploySQL --resource-group $SQLrgName --template-
file DeploySQLVM.bicep
```

After completing the above steps, the VNETs and the VM should be deployed

Next, we will implement conditional access using the steps below

1. Connect to Azure VM (for the credentials, refer to the step above where you would have provided the password for the admin account)
2. On your personal computer , Open the browser and get your public IP address by visiting - ipinfo.io/ip
3. Connect to Fabric Portal from your personal computer: https://app.fabric.microsoft.com/, you should be able to login using your account to Microsoft Fabric
4. Go to Microsoft Azure Portal
5. Search for ‘Microsoft Entra Named Location’ in search bar and navigate to ‘Named Locations’ view.
6. Click on ‘+ IP range location’ button to enter IP ranges and mark it as trusted location and key the Public IP which you copied in the above step and Key with /32. For example – 101.127.100.12/32



Named locations are used by Microsoft Entra secur
Locations that are marked Trusted or configured in

5 named locations found

Name	Locati
0200930c-0da2-4aa4-ca01-2e65...	IP ran
Allow_AzureVMIP	IP ran

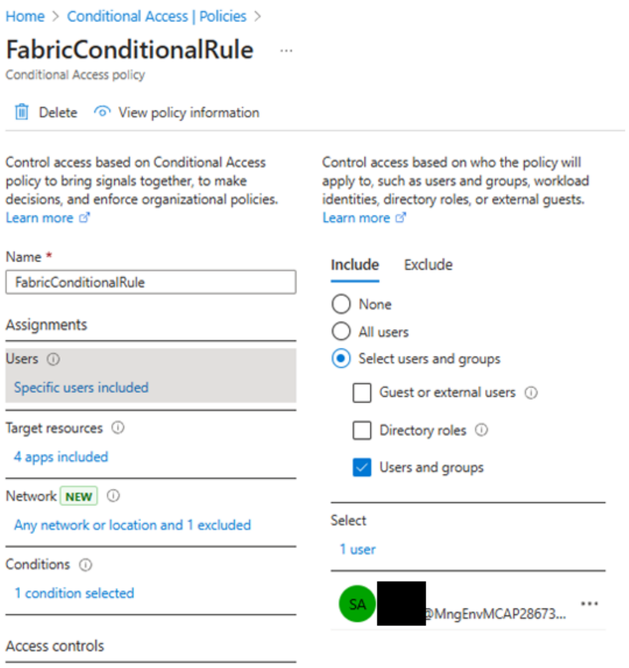
Configure named location IPv4 and IPv6 ranges.

Name * Allow_AzureVMIP

☐ Mark as trusted location

Enter a new IPv4 or IPv6 range 101.127.100.4/32

7. Type Conditional Access in Azure Portal Search Bar -> Hit Enter -> Click on Create New Policy -> under Assignments click on Users -> Select users and groups under Include section -> users and groups -> User / Assignment ->User or Workload identity(for which you are trying to setup conditional access for).



Home > Conditional Access | Policies >

FabricConditionalRule ...

Conditional Access policy

Delete View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

FabricConditionalRule

Assignments

Users

Specific users included

Target resources

4 apps included

Network NEW

Any network or location and 1 excluded

Conditions

1 condition selected

Access controls

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. Learn more

Include Exclude

○ None

○ All users

● Select users and groups

□ Guest or external users

□ Directory roles

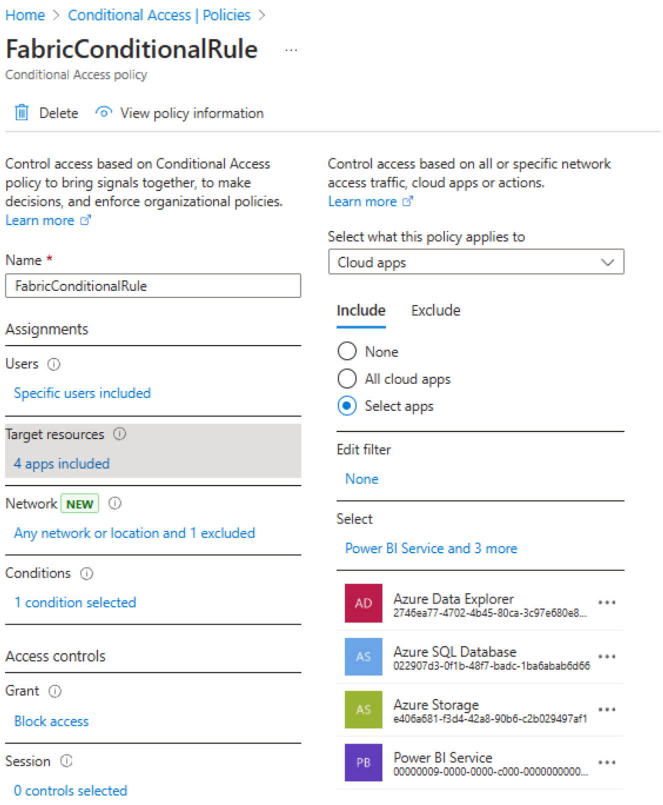
☑ Users and groups

Select

1 user

SA [redacted]@MngEnvMCAP28673... ...

8. Click the Target resources and click select and type these App names to add (Azure Data Explorer, Azure Sql Database, Azure Storage, Power BI Service). Once you restrict access to these 4 services, Fabric won't be accessible from public internet.
    - Note: If you do not see a service in the list, open a new duplicate azure portal tab -> Type Subscription in the Portal Search Bar and pick the subscription that you are working with for the labs -> On the left Pane, Under Settings pick Resource Providers -> In right pane "Filter by name", type the service name that you did not see in the list, select it and hit Register. For Azure Data Explorer, its kusto.



Home > Conditional Access | Policies >

FabricConditionalRule ...

Conditional Access policy

Delete View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

FabricConditionalRule

Assignments

Users

Specific users included

Target resources

4 apps included

Network NEW

Any network or location and 1 excluded

Conditions

1 condition selected

Access controls

Grant

Block access

Session

0 controls selected

Control access based on all or specific network access traffic, cloud apps or actions. Learn more

Select what this policy applies to

Cloud apps

Include | Exclude

○ None

○ All cloud apps

● Select apps

Edit filter

None

Select

Power BI Service and 3 more

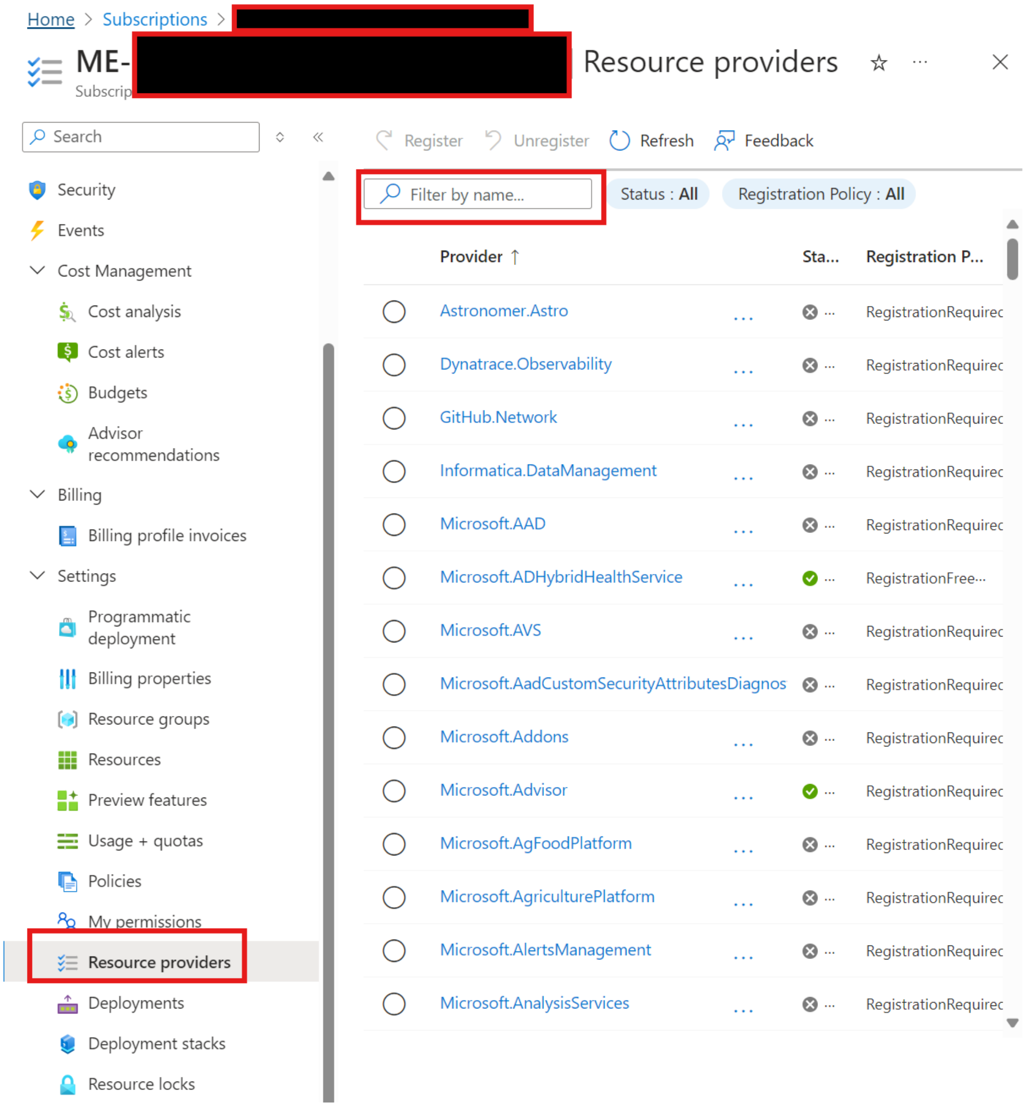
AD Azure Data Explorer
2746ea77-4702-4b45-80ca-3c97e680e8...

AS Azure SQL Database
022907d3-0f1b-48f7-badc-1ba6abab6d66

AS Azure Storage
e406a681-f3d4-42a8-90b6-c2b029497af1

PB Power BI Service
00000009-0000-0000-c000-0000000000...

- ○

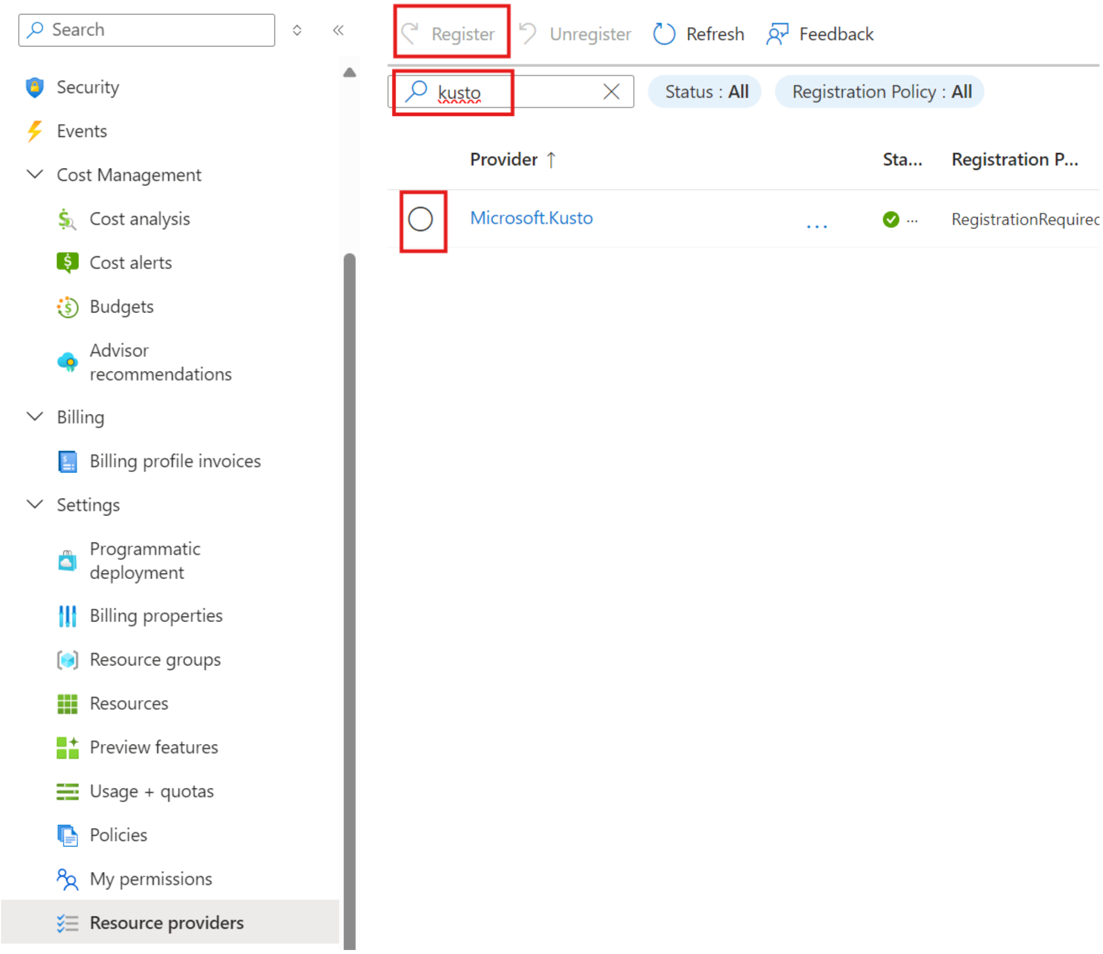


Home > Subscriptions > [redacted]

ME- [redacted] Resource providers

Subscrip

	Provider ↑		Sta...	Registration P...
○	Astronomer.Astro	...	⊗ ...	RegistrationRequirec
○	Dynatrace.Observability	...	⊗ ...	RegistrationRequirec
○	GitHub.Network	...	⊗ ...	RegistrationRequirec
○	Informatica.DataManagement	...	⊗ ...	RegistrationRequirec
○	Microsoft.AAD	...	⊗ ...	RegistrationRequirec
○	Microsoft.ADHybridHealthService	...	✓ ...	RegistrationFree...
○	Microsoft.AVS	...	⊗ ...	RegistrationRequirec
○	Microsoft.AadCustomSecurityAttributesDiagnos		⊗ ...	RegistrationRequirec
○	Microsoft.Addons	...	⊗ ...	RegistrationRequirec
○	Microsoft.Advisor	...	✓ ...	RegistrationRequirec
○	Microsoft.AgFoodPlatform	...	⊗ ...	RegistrationRequirec
○	Microsoft.AgriculturePlatform	...	⊗ ...	RegistrationRequirec
○	Microsoft.AlertsManagement	...	⊗ ...	RegistrationRequirec
○	Microsoft.AnalysisServices	...	⊗ ...	RegistrationRequirec

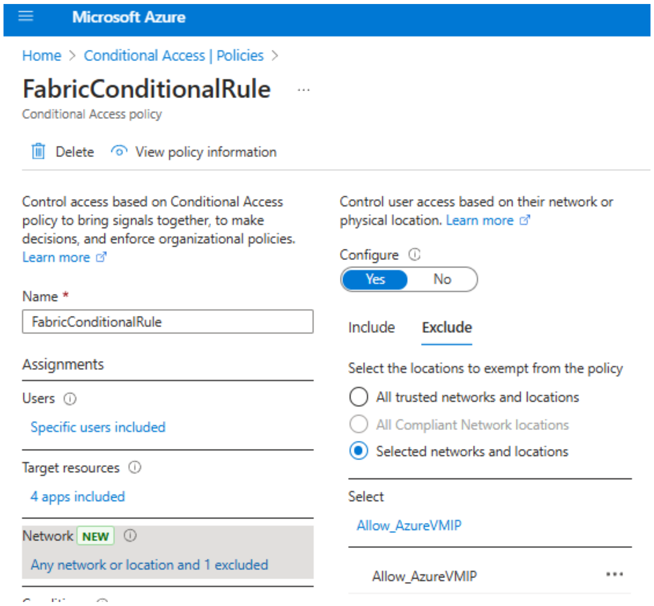


kusto

	Provider ↑		Sta...	Registration P...
○	Microsoft.Kusto	...	✓ ...	RegistrationRequirec

○

9. Click the Network > Configure “Yes” > Click on exclude and selected the selected networks and locations > Select the ‘+ IP range location’ you created in step 6 and hit save.



Microsoft Azure

Home > Conditional Access | Policies >

FabricConditionalRule ...

Conditional Access policy

Delete   View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

FabricConditionalRule

Assignments

Users

Specific users included

Target resources

4 apps included

Network NEW

Any network or location and 1 excluded

Control user access based on their network or physical location. Learn more

Configure

[✓ Yes] No

Include   Exclude

Select the locations to exempt from the policy

○ All trusted networks and locations

○ All Compliant Network locations

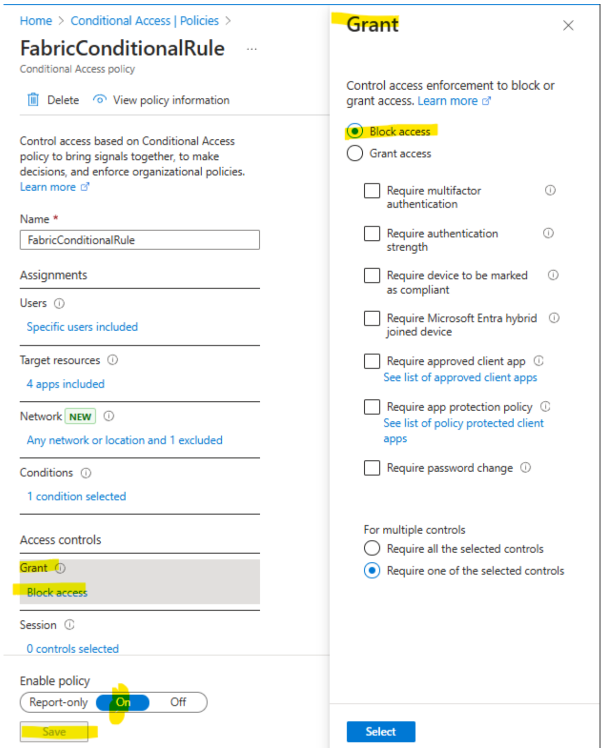
● Selected networks and locations

Select

Allow_AzureVMIP

Allow_AzureVMIP ...

10. Click on the Grant, enable Block access, and Enable Policy “On”. This will restrict access to Fabric, allowing it only from the Azure VM while preventing access from any other system using the specified user.



Home > Conditional Access | Policies >

FabricConditionalRule ...

Conditional Access policy

Delete   View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

FabricConditionalRule

Assignments

Users

Specific users included

Target resources

4 apps included

Network NEW

Any network or location and 1 excluded

Conditions

1 condition selected

Access controls

Grant

Block access

Session

0 controls selected

Enable policy

Report-only [✓ On] Off

Save

Grant

Control access enforcement to block or grant access. Learn more

● Block access

○ Grant access

☐ Require multifactor authentication

☐ Require authentication strength

☐ Require device to be marked as compliant

☐ Require Microsoft Entra hybrid joined device

☐ Require approved client app
See list of approved client apps

☐ Require app protection policy
See list of policy protected client apps

☐ Require password change

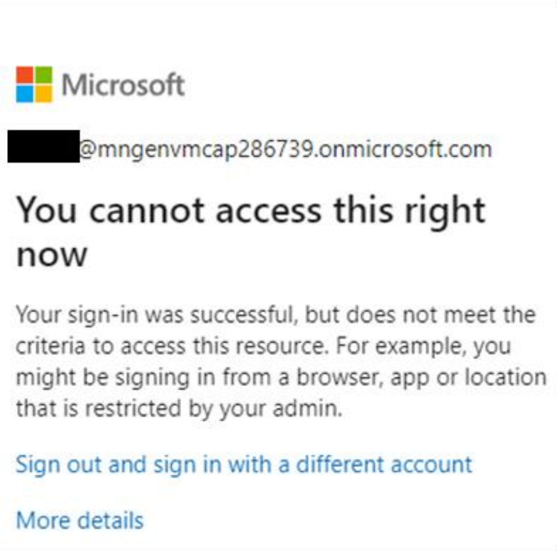
For multiple controls

○ Require all the selected controls

● Require one of the selected controls

Select

11. Restricting the specified user from accessing Microsoft Fabric from any system other than the designated Azure VM.



Microsoft

[redacted]@mngenvmcap286739.onmicrosoft.com

You cannot access this right now

Your sign-in was successful, but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app or location that is restricted by your admin.

Sign out and sign in with a different account

More details

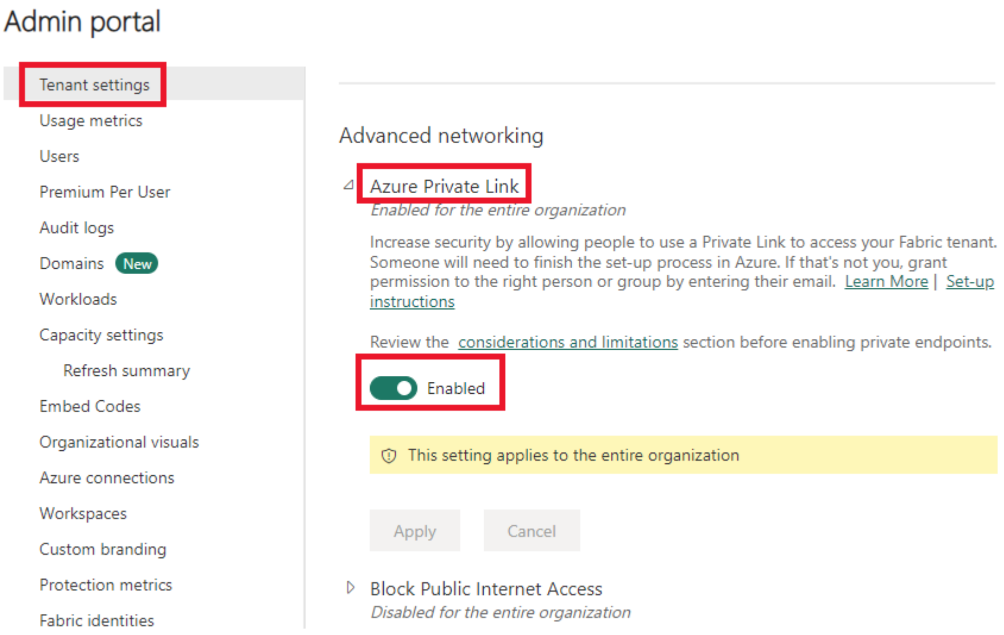
This concludes enabling Conditional Access in Fabric

Task 6: Set up and use private links

In previous task, we tested if a user is able to access fabric from specific ip location. In this task, we will let the user access fabric only when they are signing in from specific Network. For that we are going to setup private link/private endpoint connectivity.

To deploy the Private Link

1. At the Fabric tenant level, enable “Azure Private Link” as shown below. Toggling this to on may take 15 minutes to take effect



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

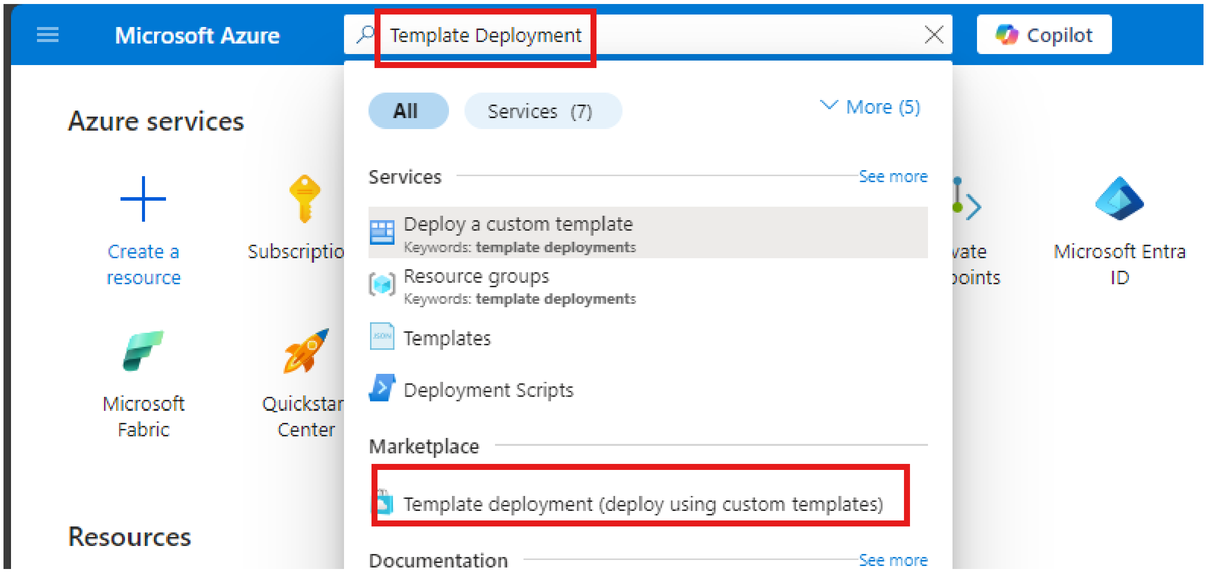
This setting applies to the entire organization

Apply Cancel

Block Public Internet Access

Disabled for the entire organization

2. Next, we will Create a Microsoft.PowerBI private link services for Power BI resource in the Azure portal. Sign in to the Azure portal.
3. Select Create a resource.
4. Type Template Deployment in Search bar, select template deployment(deploy using custom templates) .



5. On the Custom deployment page, select "Build your own template in the editor".
6. In the editor, create the following a Fabric resource using the ARM template as shown below, where:

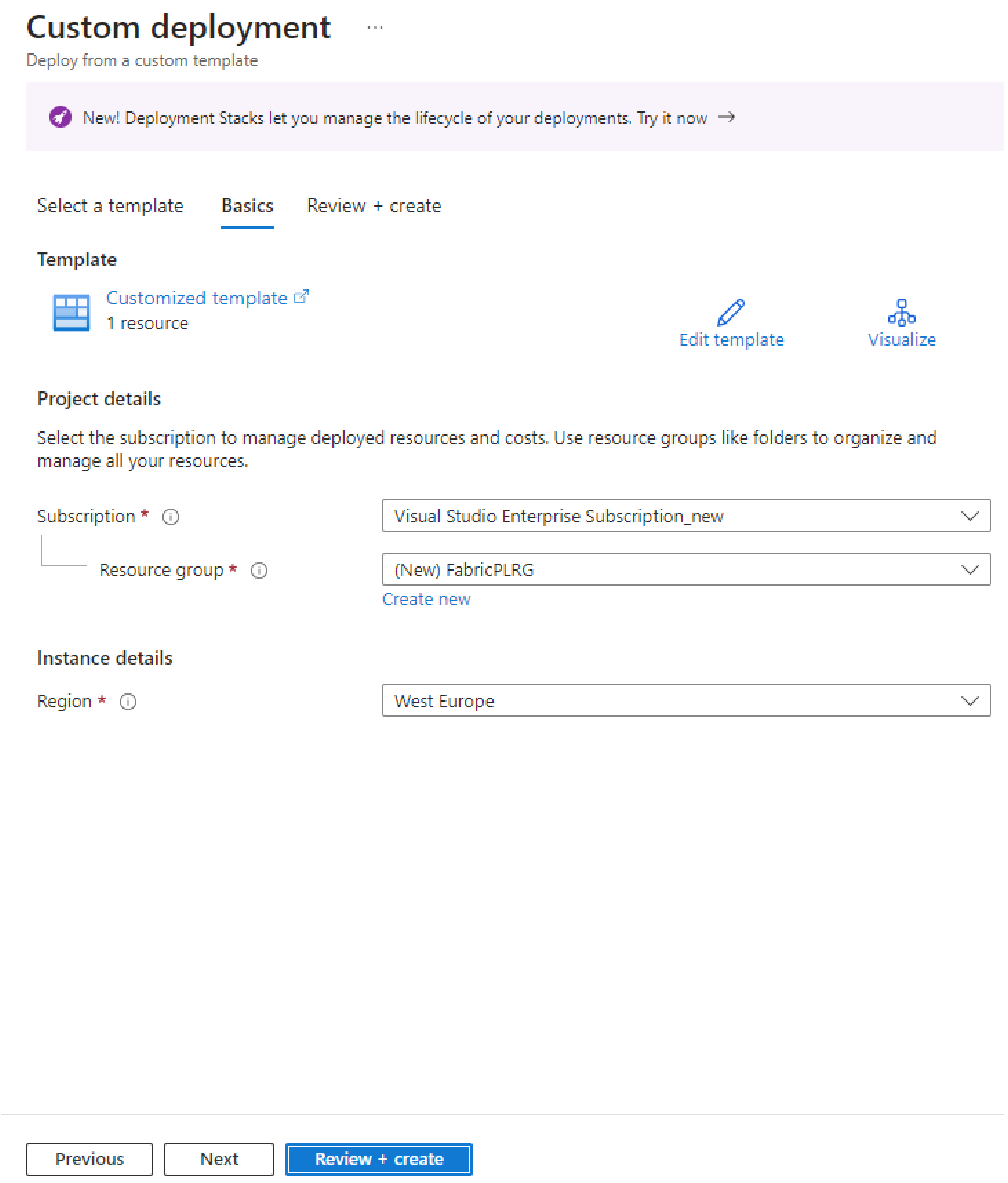
NOTE: Replace resource name and tenand id from below code smaple

<resource-name> is the name you choose for the Fabric Private Link resource. (eg., FabricPL)

<tenant-object-id> is your Microsoft Entra tenant ID. You can get this from Microsoft Entra ID service from Azure portal

```
{
  "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {},
  "resources": [
    {
      "type":"Microsoft.PowerBI/privateLinkServicesForPowerBI",
      "apiVersion": "2020-06-01",
      "name" : "<resource-name>",

      "location": "global",

      "properties" :

      {

        "tenantId": "<tenant-object-id>"

      }

    }

  ]

}
```

7. Save the template and provide the Resource group and Region details



Custom deployment ...

Deploy from a custom template

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

Select a template | Basics | Review + create

Template

Customized template

1 resource

Edit template

Visualize

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Visual Studio Enterprise Subscription_new

Resource group * : (New) FabricPLRG

Create new

Instance details

Region * : West Europe

Previous | Next | Review + create

8. Click on Review+Create -> create

Next, we will Create a Private Endpoint for Fabric in the Azure portal.

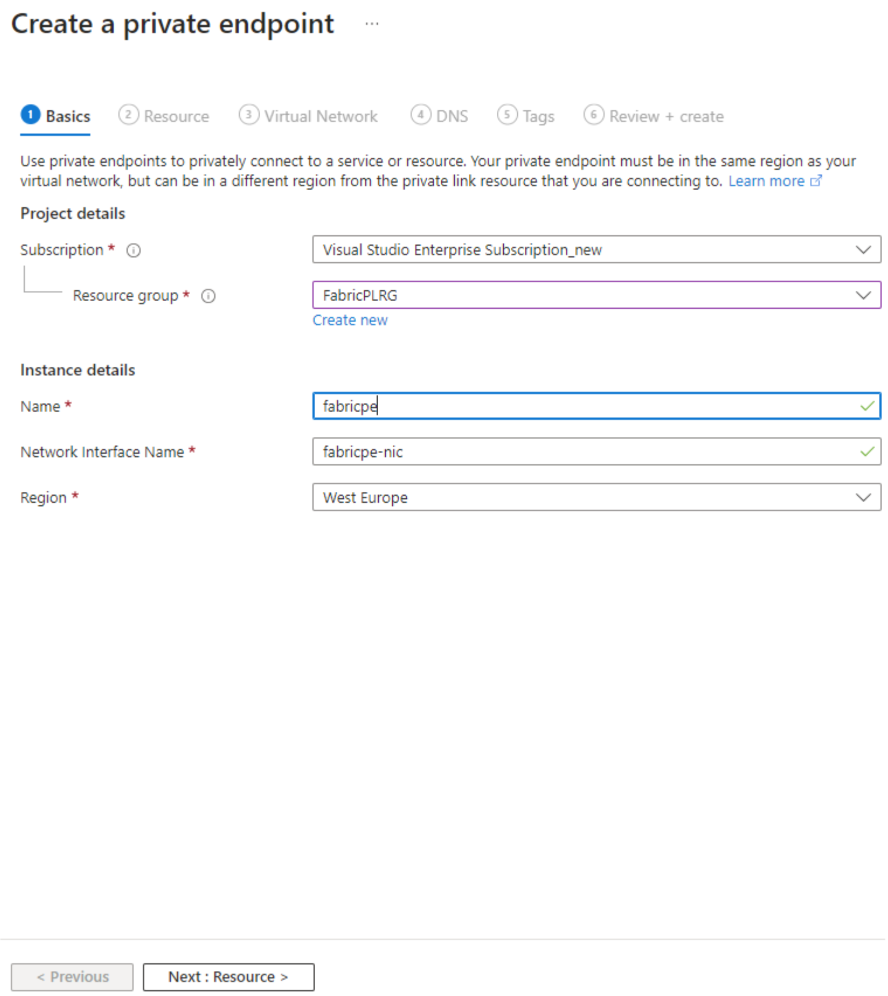
1. In the search box at the top of the portal, enter Private endpoint. Select Private endpoints.

2. Select + Create in Private endpoints.

3. On the Basics tab of Create a private endpoint, enter or select the following information:

Settings	Value
Subscription	Select your Azure Subscription.
Resource group	Select the resource group you created in the above step (while deploying the Private Link using the custom ARM template.
Name	Enter a unique name.
Region	Select the region you created for your virtual network in VNET in

4. The following image shows the Create a private endpoint - Basics window.


Create a private endpoint ···

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. Learn more

Project details

Subscription * : Visual Studio Enterprise Subscription_new

Resource group * : FabricPLRG

Create new

Instance details

Name * : fabricpe

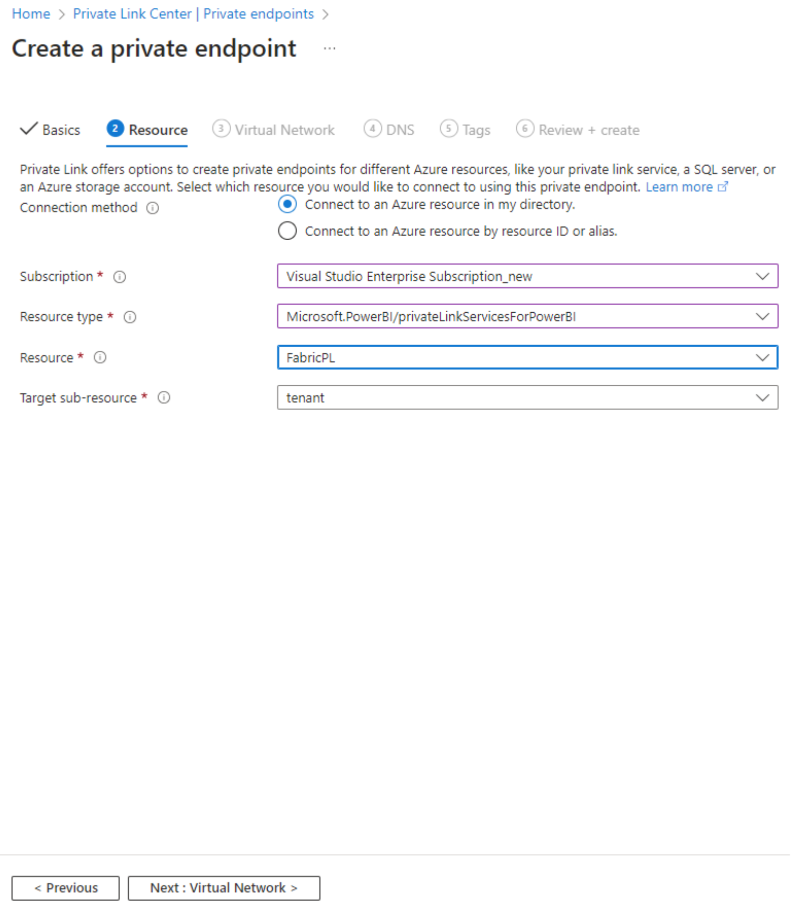
Network Interface Name * : fabricpe-nic

Region * : West Europe

5. Select Next: Resource. In the Resource pane, enter or select the following information:

Settings	Value
Connection method	Select connect to an Azure resource in my directory.
Subscription	Select your subscription.
Resource type	Select Microsoft.PowerBI/privateLinkServicesForPowerBI
Resource	Choose the Fabric resource you created earlier.
Target subresource	Tenant

The following image shows the Create a private endpoint - Resource window.



Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. Learn more

Connection method ⓘ ● Connect to an Azure resource in my directory.
○ Connect to an Azure resource by resource ID or alias.

Subscription * ⓘ Visual Studio Enterprise Subscription_new

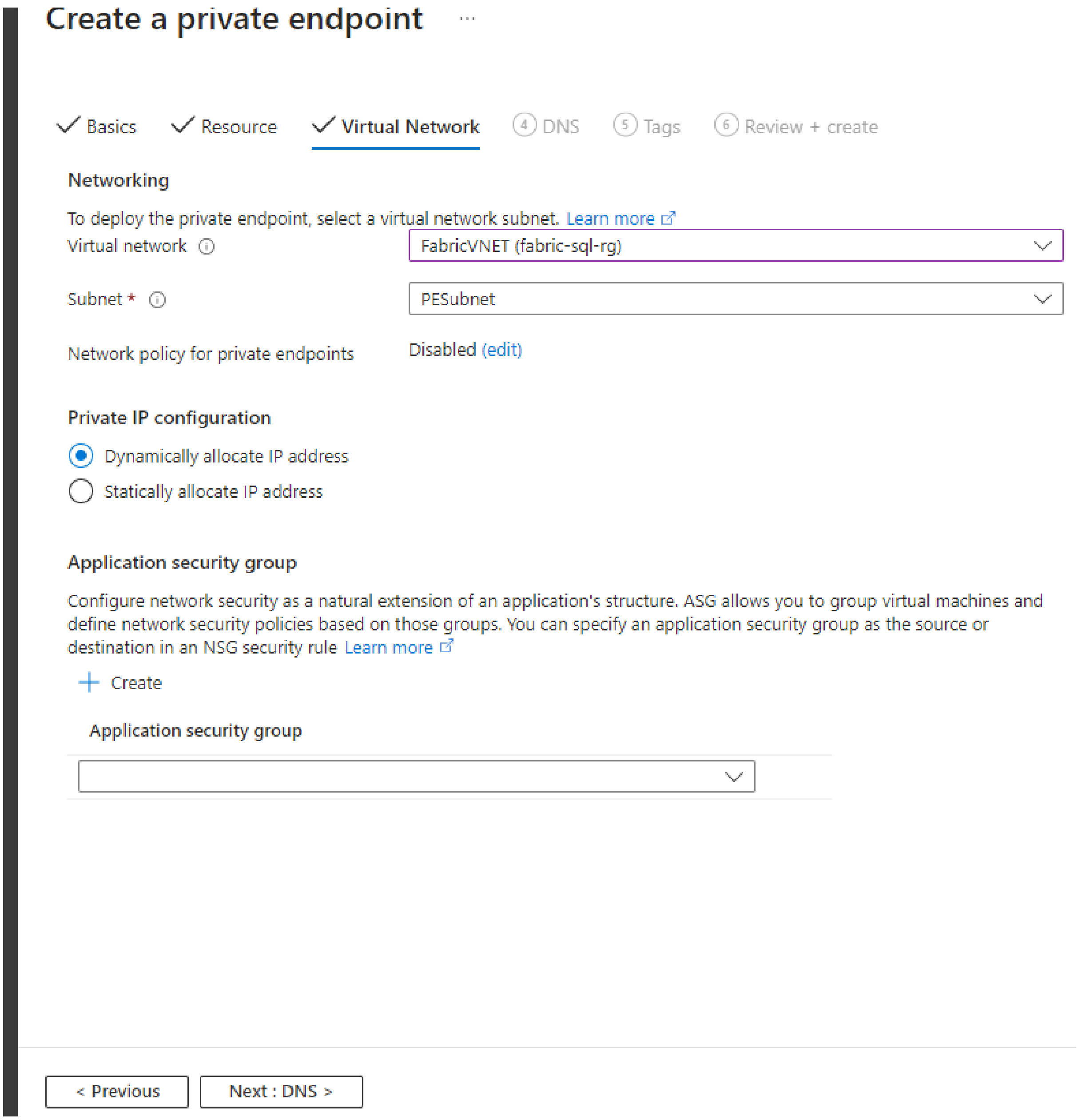
Resource type * ⓘ Microsoft.PowerBI/privateLinkServicesForPowerBI

Resource * ⓘ FabricPL

Target sub-resource * ⓘ tenant

6. Select **Next: Virtual Network**.

Settings	Value
Virtual network	Select *FabricVNET* which you created using VNET.bicep.
Subnet	Select *PESubnet* which you created using VNET.bicep.



Create a private endpoint ...

Networking

To deploy the private endpoint, select a virtual network subnet. Learn more

Virtual network: FabricVNET (fabric-sql-rg)

Subnet *: PESubnet

Network policy for private endpoints: Disabled (edit)

Private IP configuration

● Dynamically allocate IP address

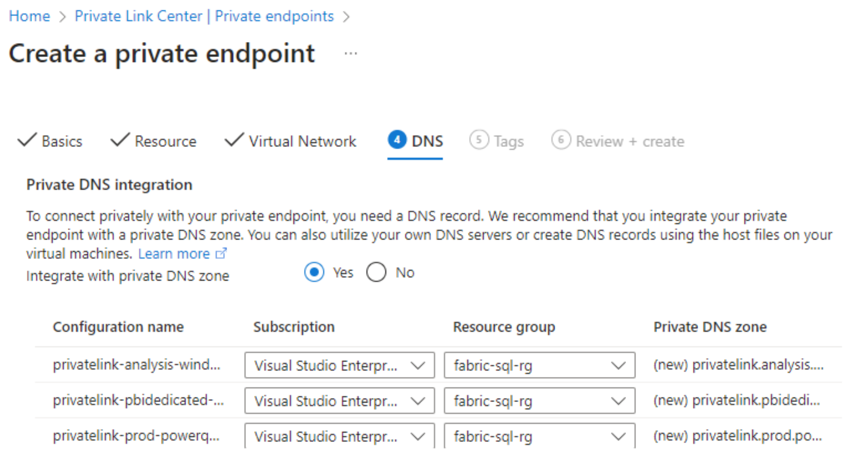
○ Statically allocate IP address

Application security group

Configure network security as a natural extension of an application's structure. ASG allows you to group virtual machines and define network security policies based on those groups. You can specify an application security group as the source or destination in an NSG security rule Learn more

7. Select Next:DNS

Settings	**Value**
Integrate with private DNS zone	Select **Yes**.
Private DNS Zone	Select *(New)privatelink.analysis.windows.net* *(New)privatelink.pbidedicated.windows.net* *(New)privatelink.prod.powerquery.microsoft.com*



Home > Private Link Center | Private endpoints >

Create a private endpoint ...

✓ Basics ✓ Resource ✓ Virtual Network 4 DNS 5 Tags 6 Review + create

Private DNS integration

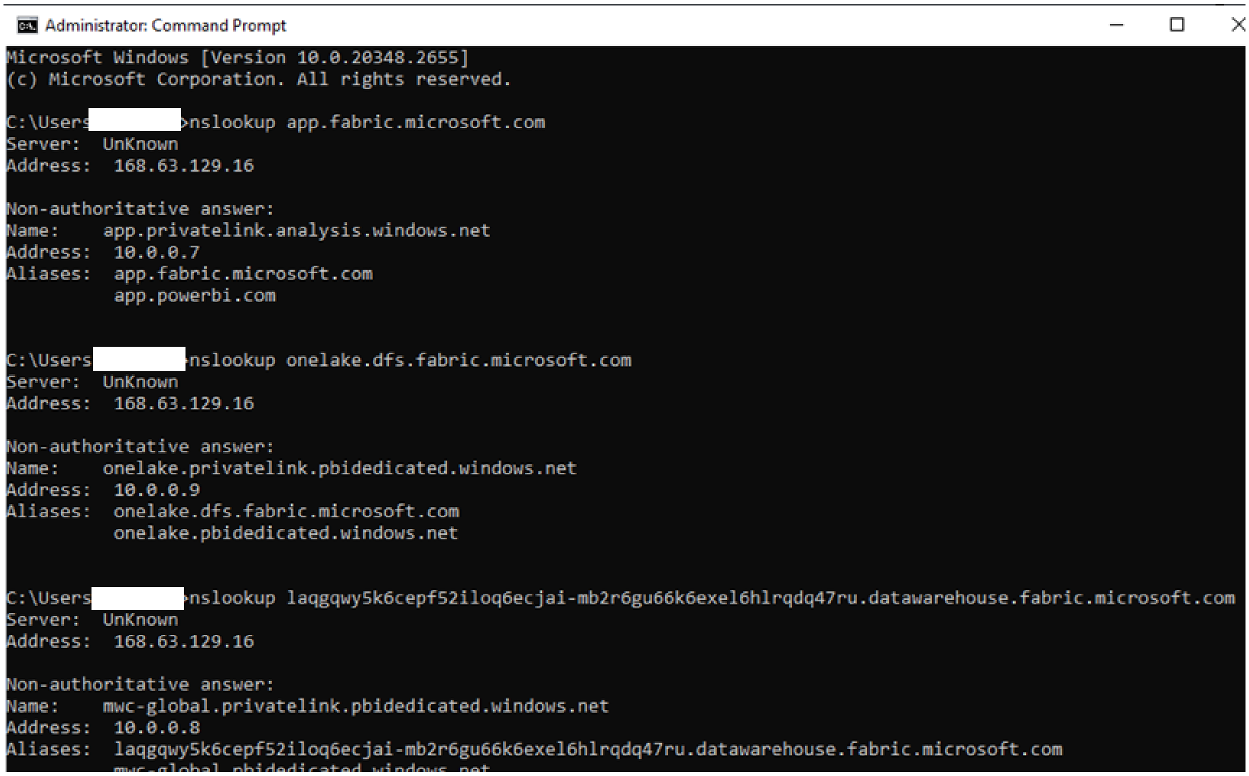
To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. Learn more

Integrate with private DNS zone ● Yes ○ No

Configuration name	Subscription	Resource group	Private DNS zone
privatelink-analysis-wind...	Visual Studio Enterpr...	fabric-sql-rg	(new) privatelink.analysis....
privatelink-pbidedicated-...	Visual Studio Enterpr...	fabric-sql-rg	(new) privatelink.pbidedi...
privatelink-prod-powerq...	Visual Studio Enterpr...	fabric-sql-rg	(new) privatelink.prod.po...

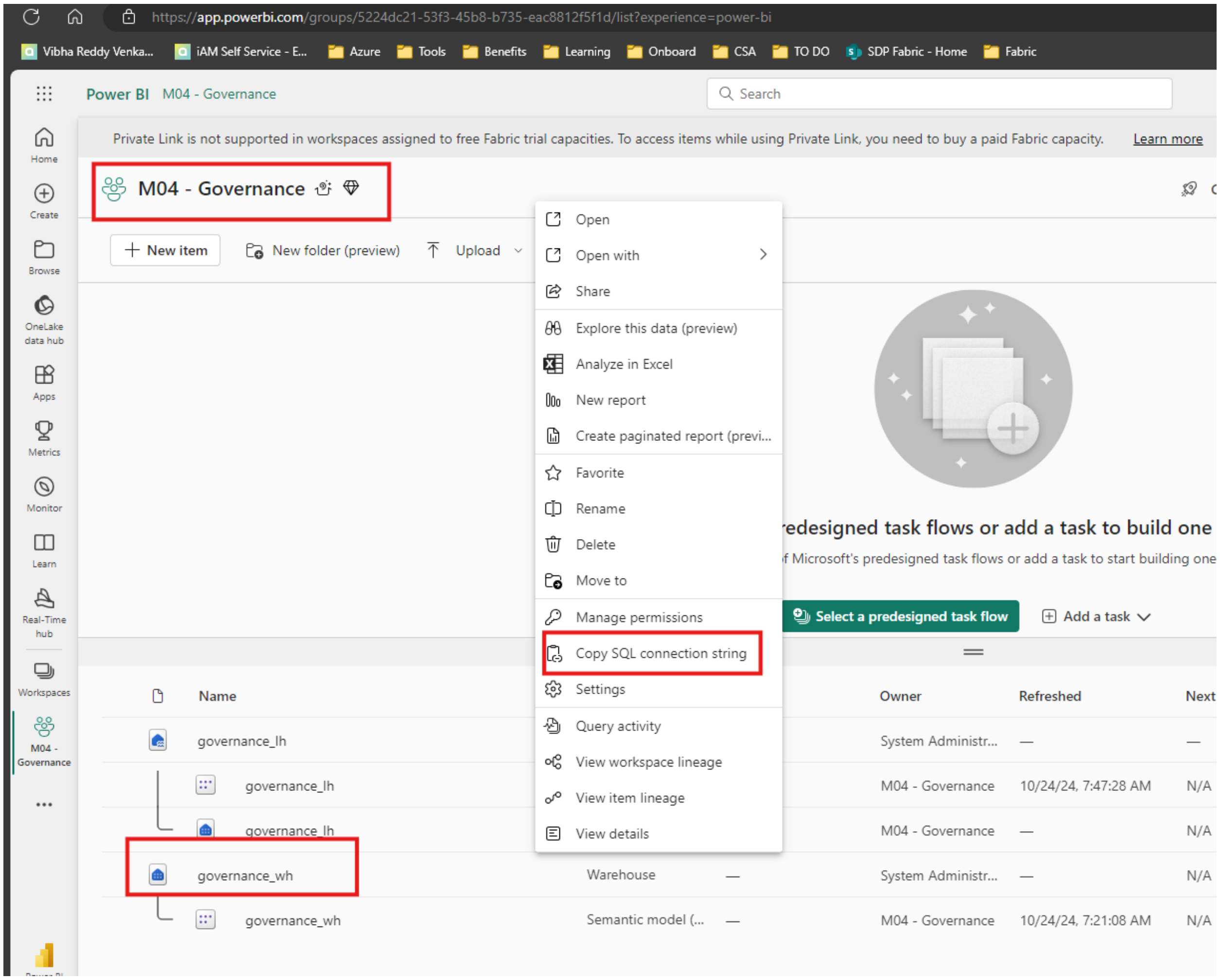
8. Click Next -> Review+Create -> create
   - Private Endpoint should be delpoyed

Once the deployment is complete, login to the Azure Sql VM that was deployed earlier in the lab, and run all the nslookup commands as show in the below snip to different endpoints, if you notice the address that was returned in the output is private ip address and not public one. This proves that all the traffic from the vm to fabric is via private endpoint. Please refer to second screenshot below to know how to retrieve datawarehouse sql connection string to enter in the 3rd nslookup command.



Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.20348.2655]
(c) Microsoft Corporation. All rights reserved.

C:\Users[redacted]>nslookup app.fabric.microsoft.com
Server:  UnKnown
Address:  168.63.129.16

Non-authoritative answer:
Name:    app.privatelink.analysis.windows.net
Address:  10.0.0.7
Aliases:  app.fabric.microsoft.com
          app.powerbi.com


C:\Users[redacted]nslookup onelake.dfs.fabric.microsoft.com
Server:  UnKnown
Address:  168.63.129.16

Non-authoritative answer:
Name:    onelake.privatelink.pbidedicated.windows.net
Address:  10.0.0.9
Aliases:  onelake.dfs.fabric.microsoft.com
          onelake.pbidedicated.windows.net


C:\Users[redacted]nslookup laqgqwy5k6cepf52iloq6ecjai-mb2r6gu66k6exel6hlrqdq47ru.datawarehouse.fabric.microsoft.com
Server:  UnKnown
Address:  168.63.129.16

Non-authoritative answer:
Name:    mwc-global.privatelink.pbidedicated.windows.net
Address:  10.0.0.8
Aliases:  laqgqwy5k6cepf52iloq6ecjai-mb2r6gu66k6exel6hlrqdq47ru.datawarehouse.fabric.microsoft.com
          mwc-global.pbidedicated.windows.net
```



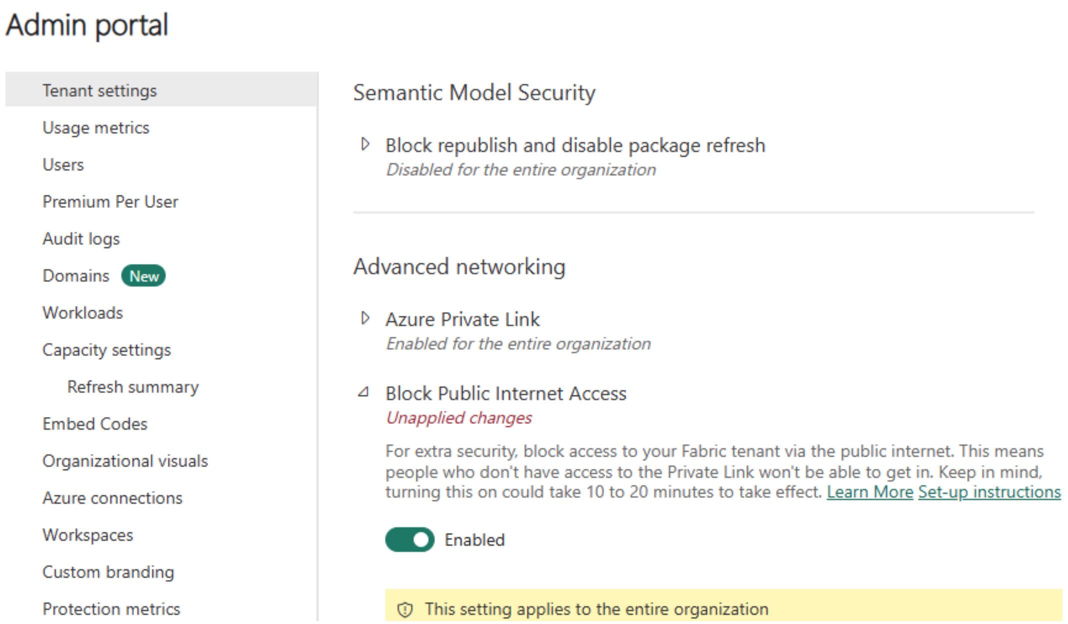
Private Link is not supported in workspaces assigned to free Fabric trial capacities. To access items while using Private Link, you need to buy a paid Fabric capacity.

redesigned task flows or add a task to build one

f Microsoft's predesigned task flows or add a task to start building one

Name			Owner	Refreshed	Next
governance_lh			System Administr...	—	—
governance_lh			M04 - Governance	10/24/24, 7:47:28 AM	N/A
governance_lh			M04 - Governance	—	N/A
governance_wh	Warehouse	—	System Administr...	—	N/A
governance_wh	Semantic model (...	—	M04 - Governance	10/24/24, 7:21:08 AM	N/A

1. As a next step, from the Fabric tenant settings, disable the Public Internet Access to Fabric from your machine



Semantic Model Security

Block republish and disable package refresh
Disabled for the entire organization

Advanced networking

Azure Private Link
Enabled for the entire organization

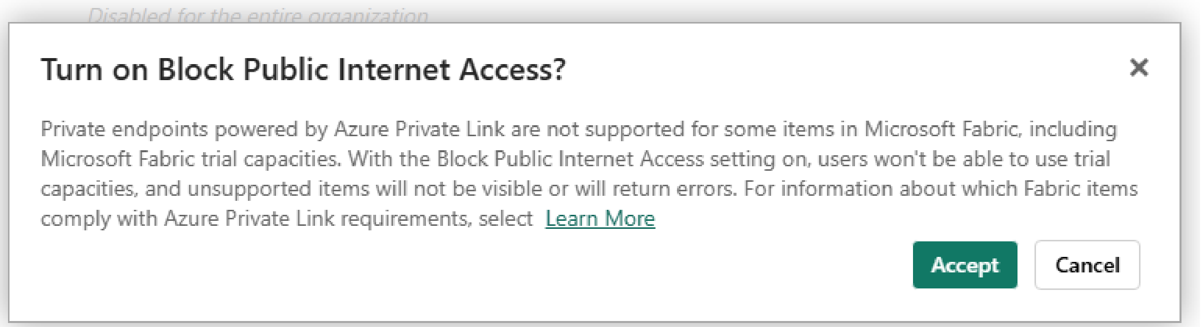
Block Public Internet Access
Unapplied changes

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

2. When you click "Apply" and "Accept" you will see the below:

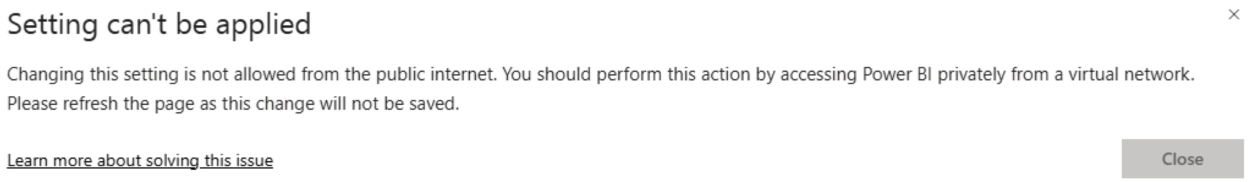


Disabled for the entire organization

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

3.

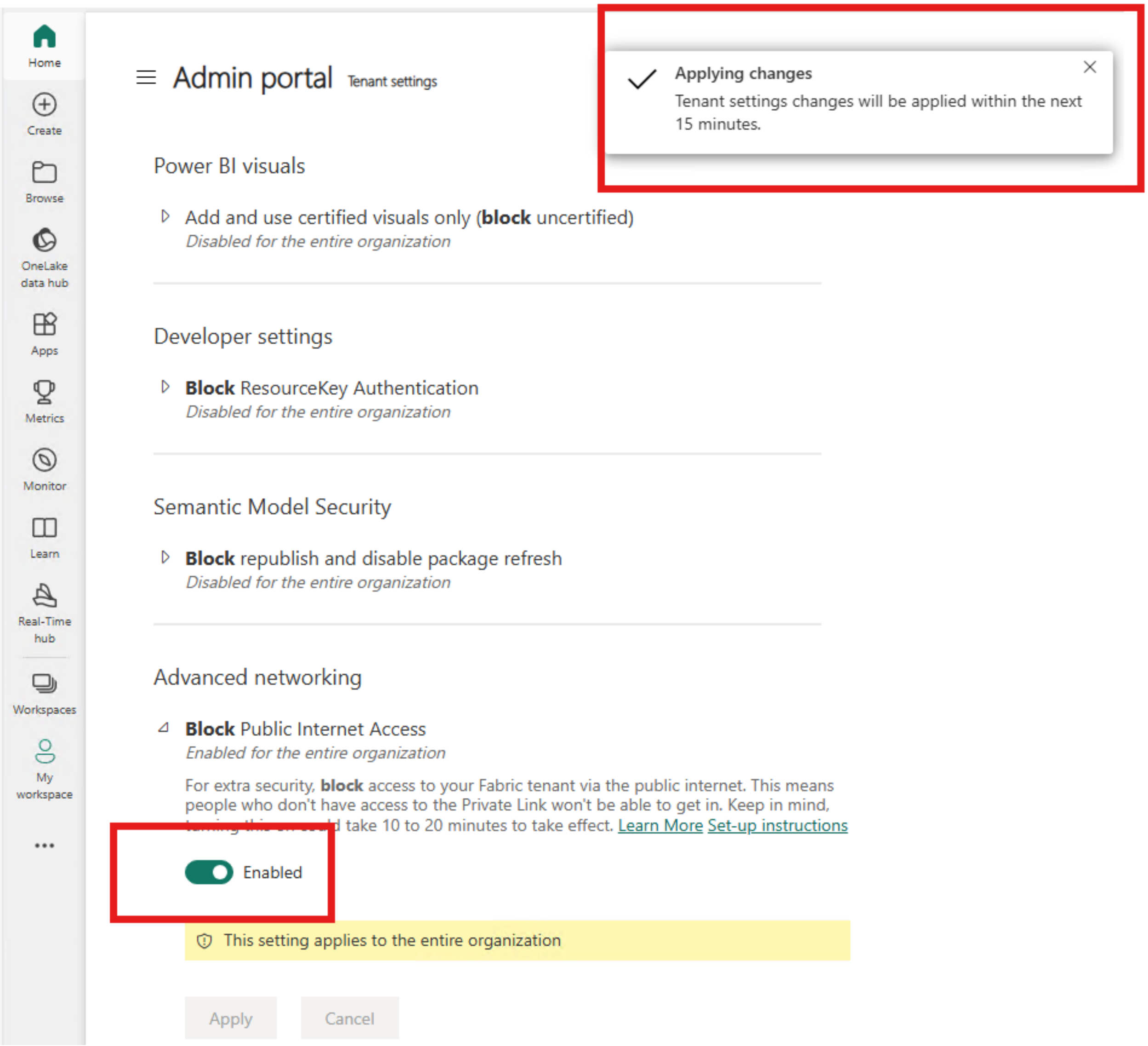


Setting can't be applied

Changing this setting is not allowed from the public internet. You should perform this action by accessing Power BI privately from a virtual network. Please refresh the page as this change will not be saved.

Learn more about solving this issue

4. From the VM where we tested the Private Endpoint, doing the same will not result in the above error. Thus disabling public network access to Fabric
Important: Remember to enable Public Internet Access before concluding the lab



Admin portal Tenant settings

✓ **Applying changes**
Tenant settings changes will be applied within the next 15 minutes.

Power BI visuals

▷ Add and use certified visuals only (**block** uncertified)
Disabled for the entire organization

Developer settings

▷ **Block** ResourceKey Authentication
Disabled for the entire organization

Semantic Model Security

▷ **Block** republish and disable package refresh
Disabled for the entire organization

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

Important: Remember to enable Public Internet Access before concluding the lab

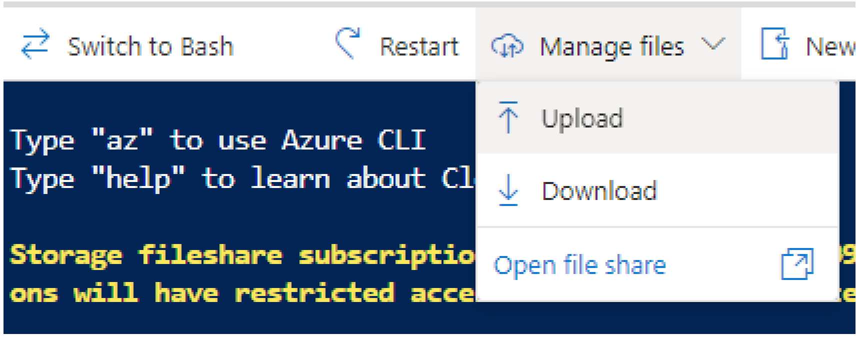
This concludes enabling Private Link and Private Endpoints in Fabric

Task 7: Trusted workspace access

In this task we will test how Fabric can access a ADLS Gen2 account that is behind a firewall. We will run a script that creates ADLS Gen2 account and deploys a container with it. ADLS Gen2 will have firewall settings enabled; you will then upload a file to test.

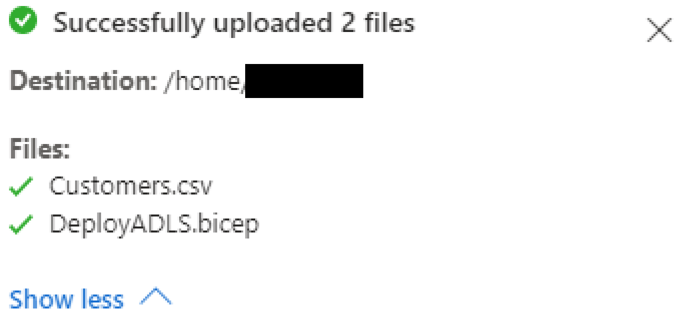
Follow steps 1 to 5 from Task 5 above. This will open the cloud shell. If you already have the cloud shell open continue to the next step

1. Upload the bicep file DeployADLS.bicep and Customers.csv (Fabric VBD - 7 - Governance and Security - ADLS - All Documents)by clicking on “Manage files” and selecting “Upload”.



```
Type "az" to use Azure CLI
Type "help" to learn about Cl
Storage fileshare subscriptio
ons will have restricted acce
```

You should see a success message for each of the files you have uploaded



Successfully uploaded 2 files

Destination: /home/[redacted]

Files:
✓ Customers.csv
✓ DeployADLS.bicep

2. Run the below commands in the cloud shell to deploy the ADLS Gen 2. You may want to change the region name to suit your requirement. The below script does the following:

   a) Create a Resource Group that will house the ADLS Gen2
   b) Deploy ADLS Gen2 into the same resource group.
   c) Set the IPaddress of your local machine as an exception to access the storage
   d) Create a container called samplecontainer

```
$ipaddr = Invoke-RestMethod -Uri "https://api.ipify.org"
$subscriptionId = "your subscription id"
$ADLSrgName = "your resource group name"
$region = "Region to deploy the RG and the ADLS Gen2 resource"

az group create --name $ADLSrgName --location $region
az deployment group create --name deployADLS --resource-group $ADLSrgName --template-file "DeployADLS.bicep" --parameters myIpAddress=$ipaddr
```

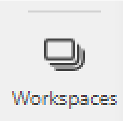
3. Upload customers.csv into the container (you may do so manually or use the script below)

```
$RESOURCE_GROUP=" your resource group name"
```

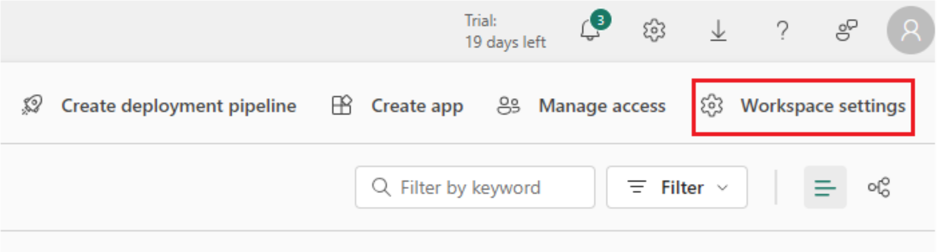
```
$STORAGE_ACCOUNT_NAME="storage account name created in the above step "
$CONTAINER_NAME="samplecontainer" – leave as is unless the container name was changed in the earlier step
$FILE_PATH="Customers.csv"
az storage blob upload --account-name $STORAGE_ACCOUNT_NAME --container-name $CONTAINER_NAME --file $FILE_PATH --overwrite
```

After completing the above steps, the ADLS Gen 2 account along with the sample file should be ready to use

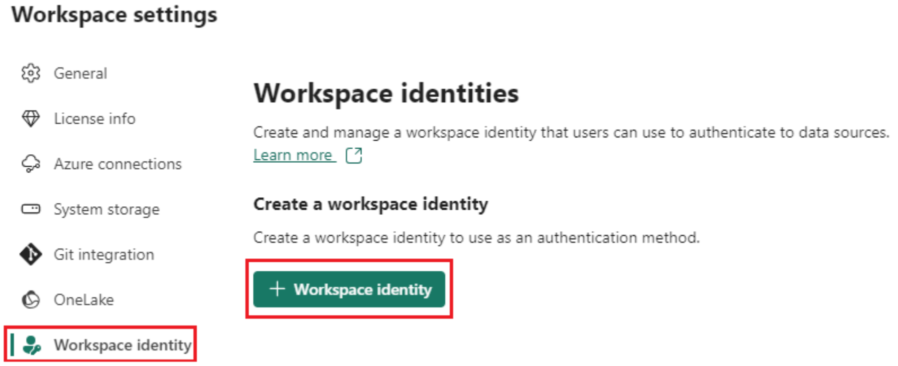
Next, we will create a workspace identity for the workspace from where we would like to setup the trusted workspace access. Sign into the Fabric portal



1. Navigate to the workspace by clicking on Workspaces on the left navigation
2. Click on Workspace settings on the right hand top corner



3. In the Workspace Settings dialog box, click Workspace Identity tab on the left navigation, and then click the green "+ Workspace Identity" button to create the workspace identity



Workspace settings

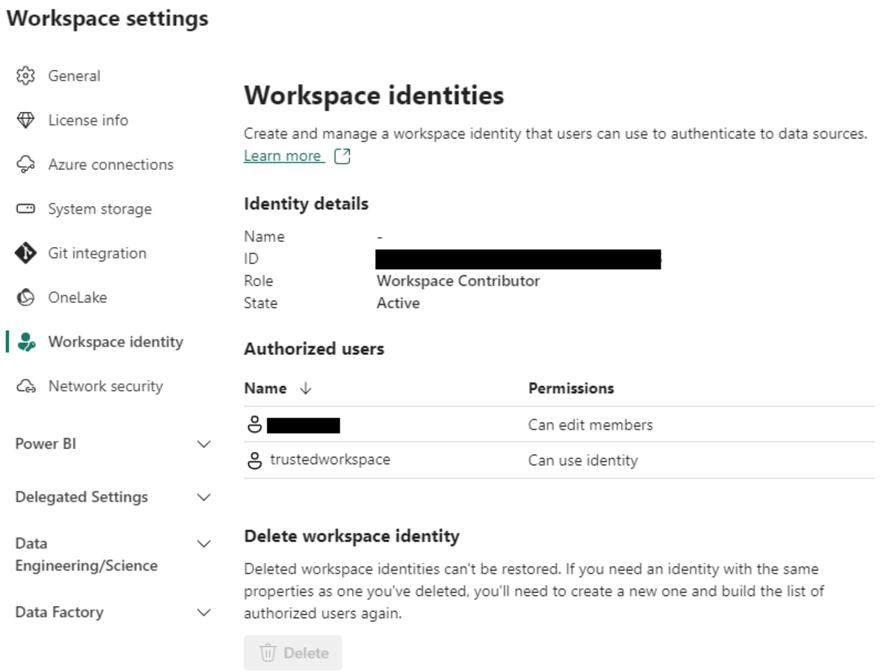
Workspace identities

Create and manage a workspace identity that users can use to authenticate to data sources.

Create a workspace identity

Create a workspace identity to use as an authentication method.

4. It will take a few seconds to create the the Workspace Identity and show the details of the same



Workspace identities

Create and manage a workspace identity that users can use to authenticate to data sources. Learn more

Identity details

Name	-
ID	[redacted]
Role	Workspace Contributor
State	Active

Authorized users

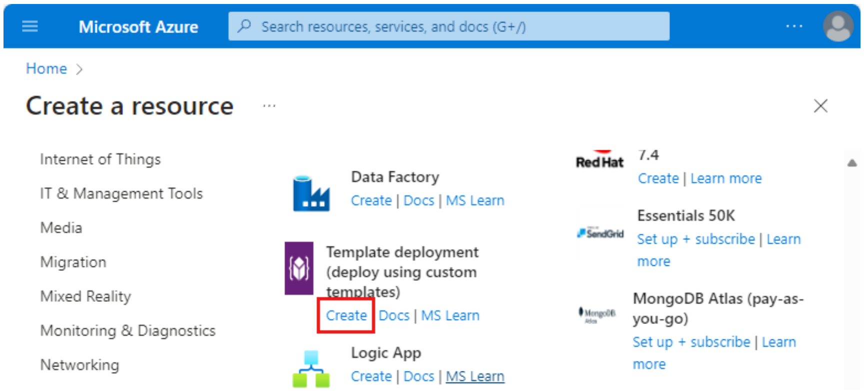
Name	Permissions
[redacted]	Can edit members
trustedworkspace	Can use identity

Delete workspace identity

Deleted workspace identities can't be restored. If you need an identity with the same properties as one you've deleted, you'll need to create a new one and build the list of authorized users again.

Next, we will configure the Resource instance rule from the Azure portal. Sign in to the Azure portal.

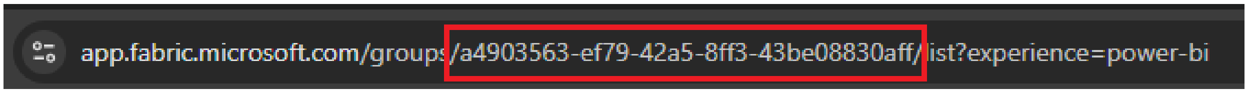
1. Select Create a resource.
2. Under Template deployment, select Create.



3. On the Custom deployment page, select “Build your own template in the editor”.
4. In the editor, create the following a Fabric resource using the ARM template as shown below, and modify the highlighted areas to match your requirements:

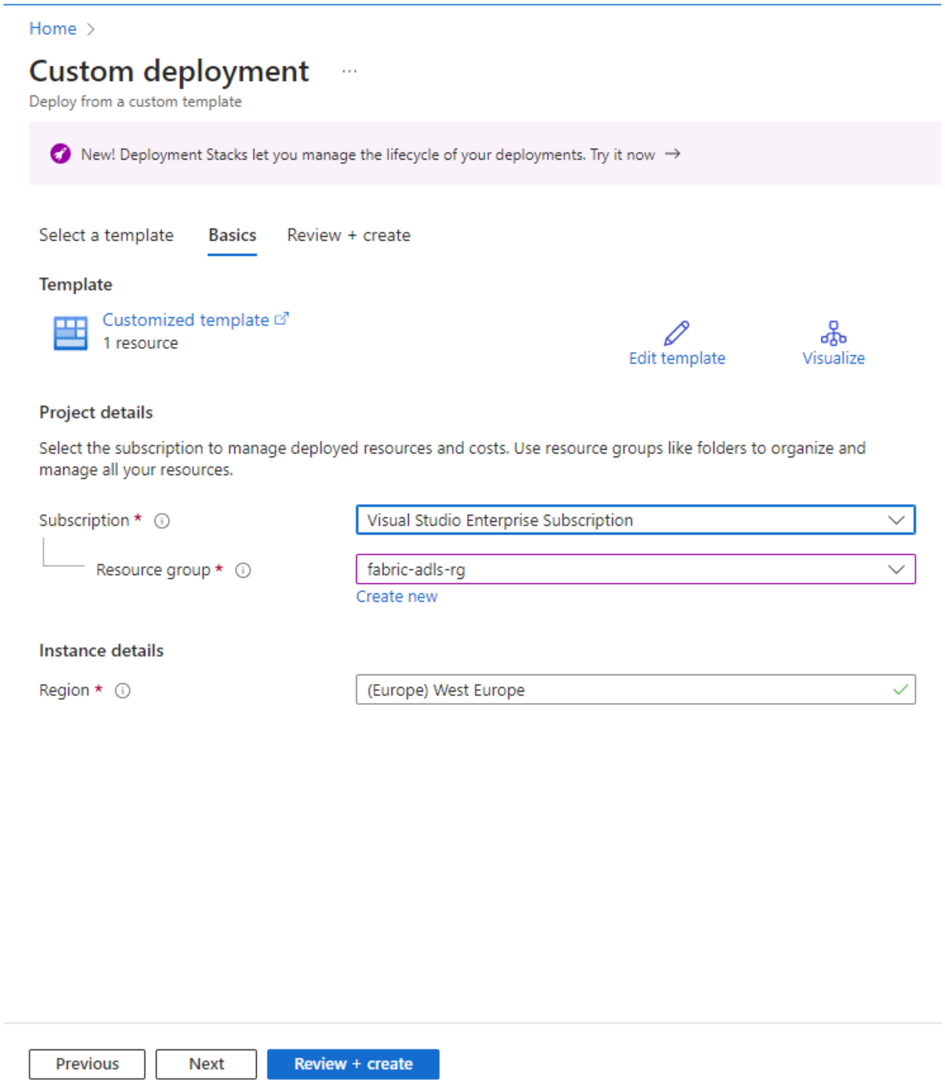
```
{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "resources": [
    {
      "type": "Microsoft.Storage/storageAccounts",
      "apiVersion": "2023-01-01",
      "name": "<storageaccountname>",
      "id": "/subscriptions/<subscription ID>/resourceGroups/<resourcegroup>/Microsoft.Storage/storageAccounts/<storageaccountname>",
      "location": "<Azure Region>",
      "kind": "StorageV2",
      "properties": {
        "networkAcls": {
          "resourceAccessRules": [
            {
              "tenantId": "<tenant ID>",
              "resourceId": "/subscriptions/"<subscription ID>"/resourcegroups/Fabric/providers/Microsoft.Fabric/workspaces/"<Fabric workspace ID>""
            }]
        }
      }
    }
  ]
}
```

You can get the Fabric workspace ID from the URL like shown below:



app.fabric.microsoft.com/groups/a4903563-ef79-42a5-8ff3-43be08830aff/list?experience=power-bi

7. Save the template and provide the Resource group (resource group that has the storage account) and Region details. If you provide a different resource group, you may encounter an error



Home >

Custom deployment ...

Deploy from a custom template

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

Template

Customized template
1 resource

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

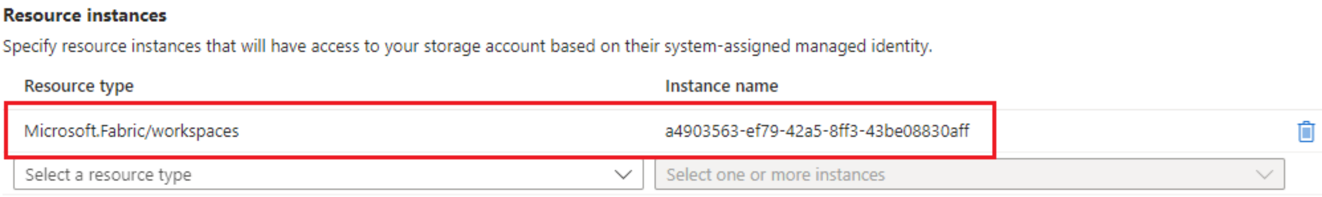
Subscription * : Visual Studio Enterprise Subscription

Resource group * : fabric-adls-rg

Instance details

Region * : (Europe) West Europe

8. Click on Review+Create and then create in order to complete the Custom Deployment
9. Once the deployment is complete, the ADLS Gen 2 should now have the rule configured like the below



Resource instances

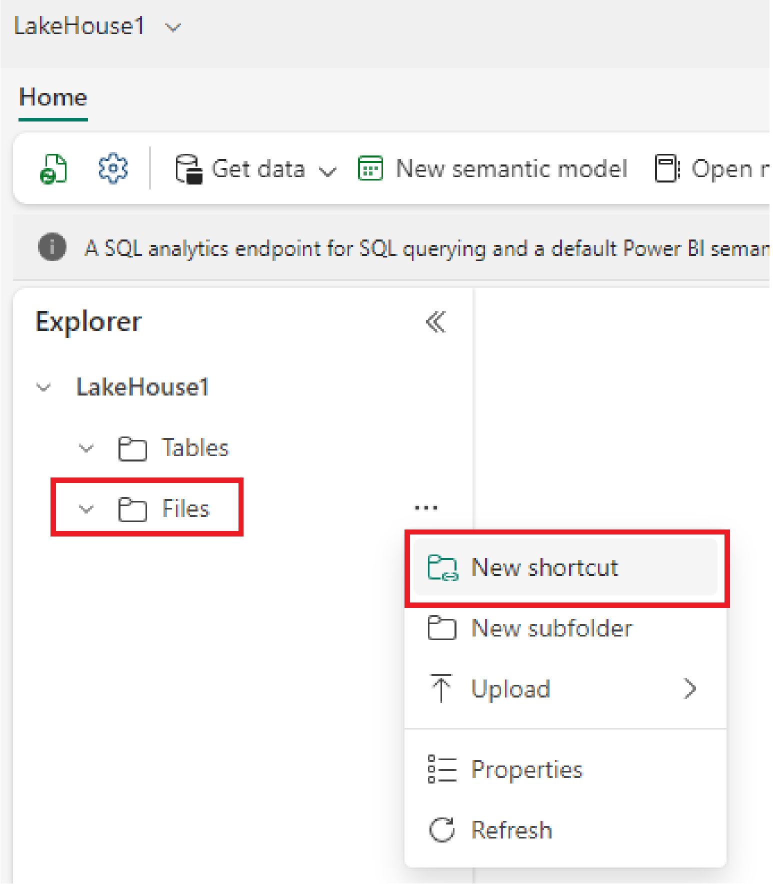
Specify resource instances that will have access to your storage account based on their system-assigned managed identity.

Resource type	Instance name
Microsoft.Fabric/workspaces	a4903563-ef79-42a5-8ff3-43be08830aff
Select a resource type	Select one or more instances

Next, we will create a shortcut from the Fabric workspace pointing to the Customers.csv file that was uploaded earlier

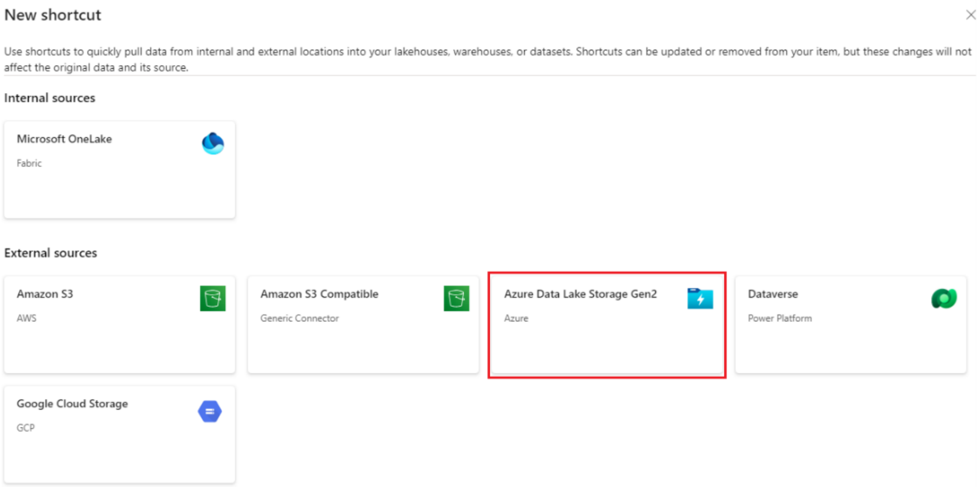
Prior to creating a shortcut, ensure that the user account you will use to create a shortcut has the "Blob Data Contributor" privileges on the storage account (else you may encounter a "Invalid Credentials" error while creating the connection)

1. From an already created LakeHouse, use the below steps to create the shortcut (if you do not have a lakehouse, create one)
2. In the Lakehouse, right-click the files folder and click on "New shortcut"



A SQL analytics endpoint for SQL querying and a default Power BI seman

3. In the new shortcut wizard select Azure Data Lake Storage Gen2 and create a new connection, fill out the details



New shortcut

Use shortcuts to quickly pull data from internal and external locations into your lakehouses, warehouses, or datasets. Shortcuts can be updated or removed from your item, but these changes will not affect the original data and its source.

Internal sources

Microsoft OneLake
Fabric

External sources

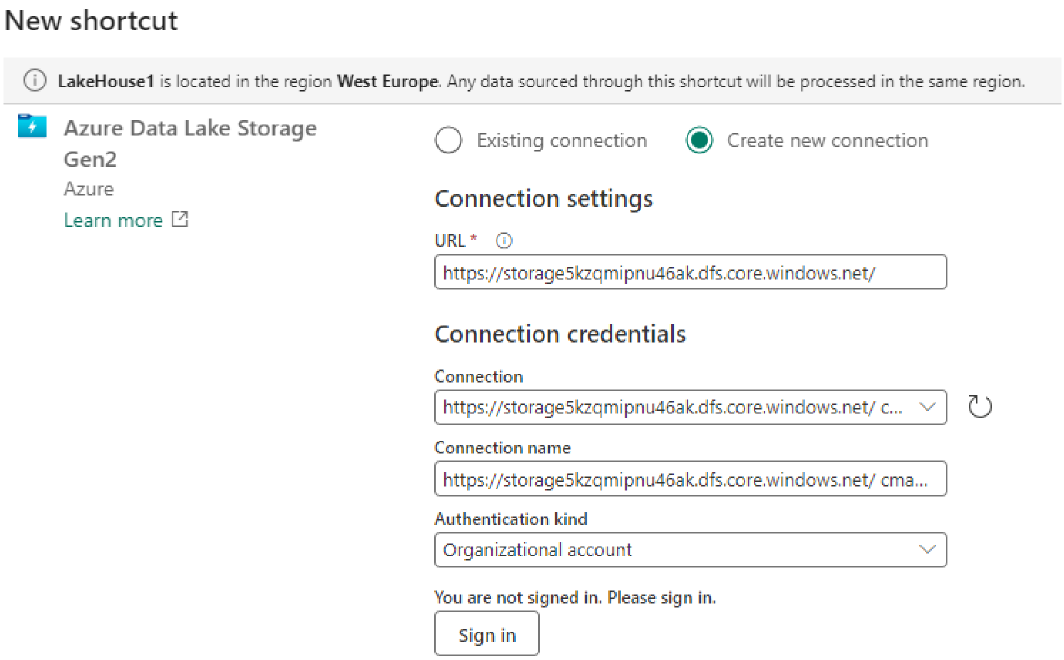
Amazon S3
AWS

Amazon S3 Compatible
Generic Connector

Azure Data Lake Storage Gen2
Azure

Dataverse
Power Platform

Google Cloud Storage
GCP



New shortcut

ⓘ **LakeHouse1** is located in the region **West Europe**. Any data sourced through this shortcut will be processed in the same region.

Azure Data Lake Storage Gen2
Azure
Learn more

○ Existing connection ● Create new connection

Connection settings

URL *: https://storage5kzqmipnu46ak.dfs.core.windows.net/

Connection credentials

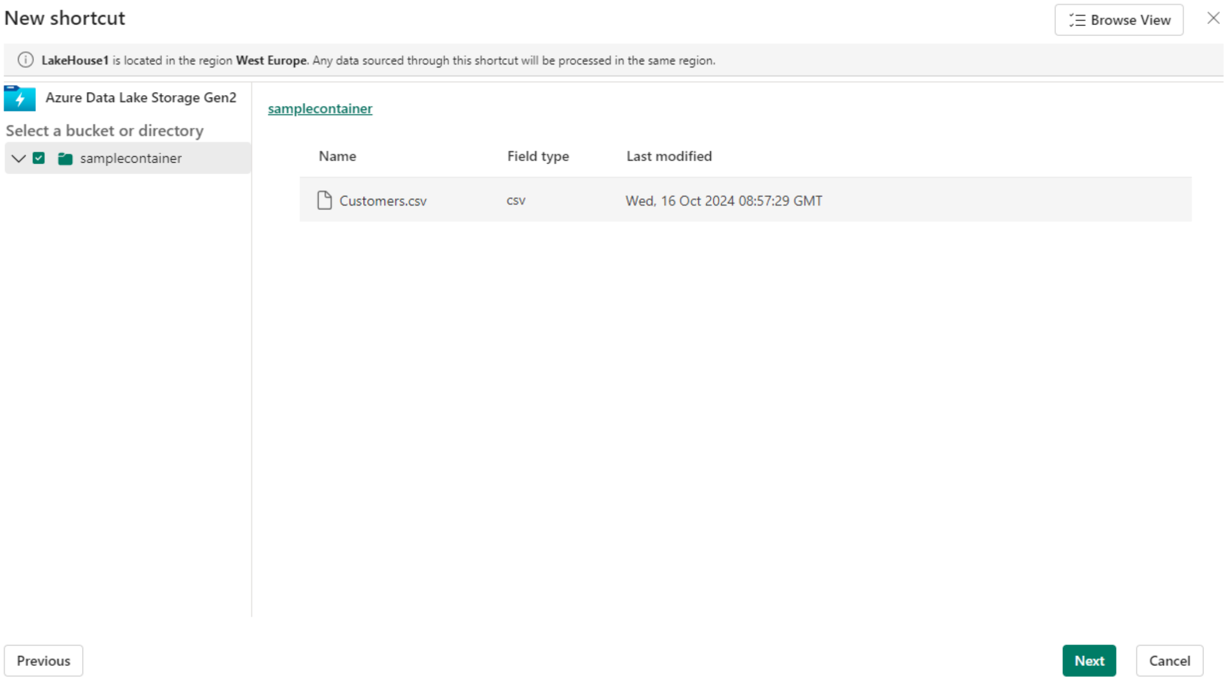
Connection: https://storage5kzqmipnu46ak.dfs.core.windows.net/ c...

Connection name: https://storage5kzqmipnu46ak.dfs.core.windows.net/ cma...

Authentication kind: Organizational account

You are not signed in. Please sign in.

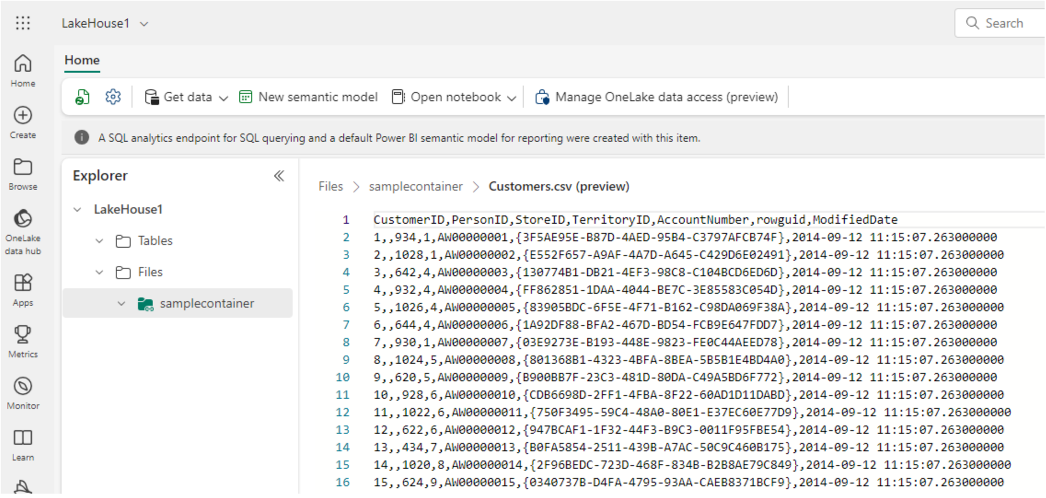
4. Once authenticated, select the Customers.csv from the samplecontainer and click Next



LakeHouse1 is located in the region West Europe. Any data sourced through this shortcut will be processed in the same region.

Name	Field type	Last modified
Customers.csv	csv	Wed, 16 Oct 2024 08:57:29 GMT

5. On the final screen click on Create to create the shortcut
6. Once, the shortcut is created, you should be able to view the contents of the file



A SQL analytics endpoint for SQL querying and a default Power BI semantic model for reporting were created with this item.

```
CustomerID,PersonID,StoreID,TerritoryID,AccountNumber,rowguid,ModifiedDate
1,,934,1,AW00000001,{3F5AE95E-B87D-4AED-95B4-C3797AFCB74F},2014-09-12 11:15:07.263000000
2,,1028,1,AW00000002,{E552F657-A9AF-4A7D-A645-C429D6E02491},2014-09-12 11:15:07.263000000
3,,642,4,AW00000003,{130774B1-DB21-4EF3-98C8-C104BCD6ED6D},2014-09-12 11:15:07.263000000
4,,932,4,AW00000004,{FF862851-1DAA-4044-BE7C-3E85583C054D},2014-09-12 11:15:07.263000000
5,,1026,4,AW00000005,{83905BDC-6F5E-4F71-B162-C98DA069F38A},2014-09-12 11:15:07.263000000
6,,644,4,AW00000006,{1A92DF88-BFA2-467D-BD54-FCB9E647FDD7},2014-09-12 11:15:07.263000000
7,,930,1,AW00000007,{03E9273E-B193-448E-9823-FE0C44AEED78},2014-09-12 11:15:07.263000000
8,,1024,5,AW00000008,{801368B1-4323-4BFA-8BEA-5B5B1E4BD4A0},2014-09-12 11:15:07.263000000
9,,620,5,AW00000009,{B900BB7F-23C3-481D-80DA-C49A5BD6F772},2014-09-12 11:15:07.263000000
10,,928,6,AW00000010,{CDB6698D-2FF1-4FBA-8F22-60AD1D11DABD},2014-09-12 11:15:07.263000000
11,,1022,6,AW00000011,{750F3495-59C4-48A0-80E1-E37EC60E77D9},2014-09-12 11:15:07.263000000
12,,622,6,AW00000012,{947BCAF1-1F32-44F3-B9C3-0011F95FBE54},2014-09-12 11:15:07.263000000
13,,434,7,AW00000013,{B0FA5854-2511-439B-A7AC-50C9C460B175},2014-09-12 11:15:07.263000000
14,,1020,8,AW00000014,{2F96BEDC-723D-468F-834B-B2B8AE79C849},2014-09-12 11:15:07.263000000
15,,624,9,AW00000015,{0340737B-D4FA-4795-93AA-CAEB8371BCF9},2014-09-12 11:15:07.263000000
```

This concludes enabling Trusted workspaces in Fabric

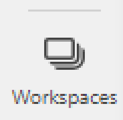
Task 8: Managed Private Endpoints

In this task, you will learn how to implement Managed Private Endpoints that allows secure and private access to data sources from Fabric Spark.

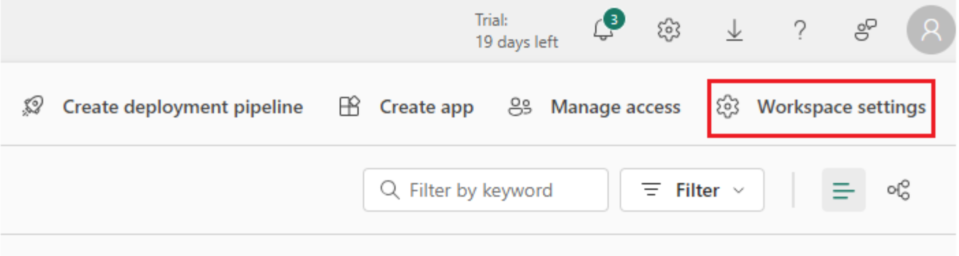
Using the previously deployed ADLS Gen 2 account, the following steps creates a Managed Private Endpoint to the same and uses a Spark notebook to access the Customers.csv

In the below steps. we will create the Managed Private Endpoint. Sign into the Fabric portal

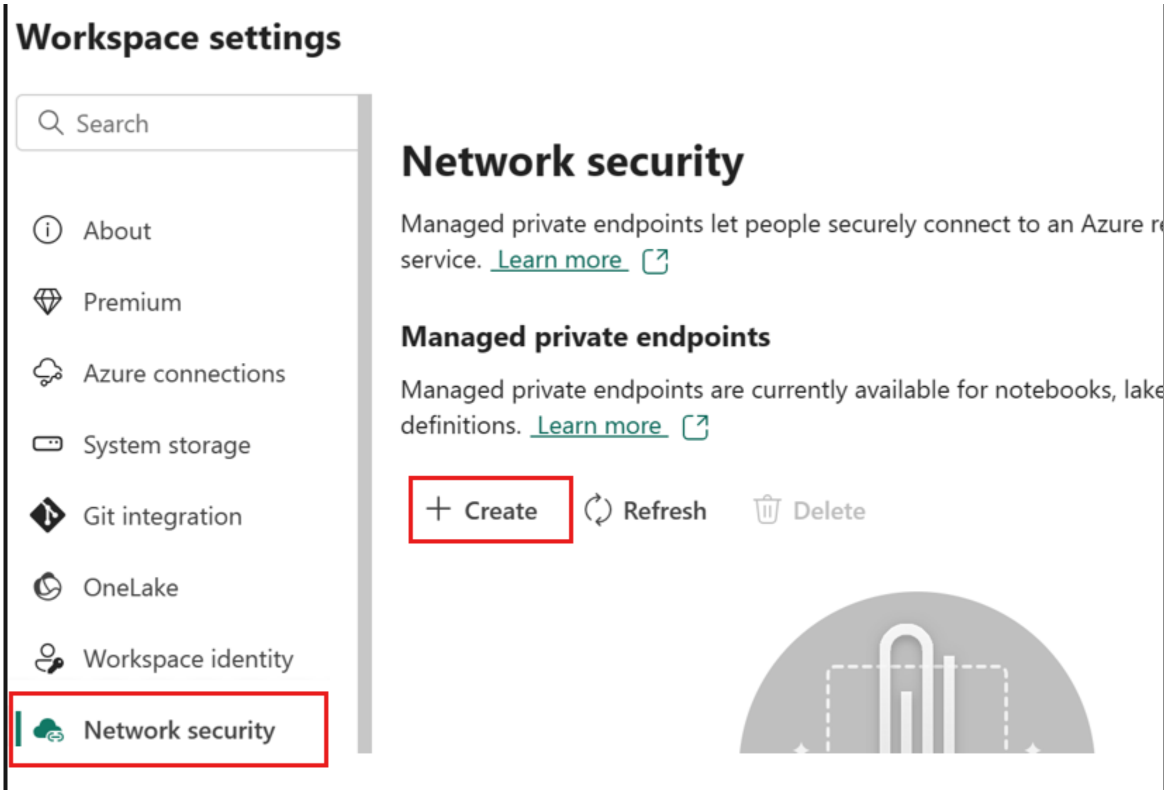
1. Navigate to the workspace by clicking on Workspaces on the left navigation



2. Click on Workspace settings on the right hand top corner



3. In the the workspace settings, select the Network security tab, and then select the Create option in the Managed Private Endpoint section.



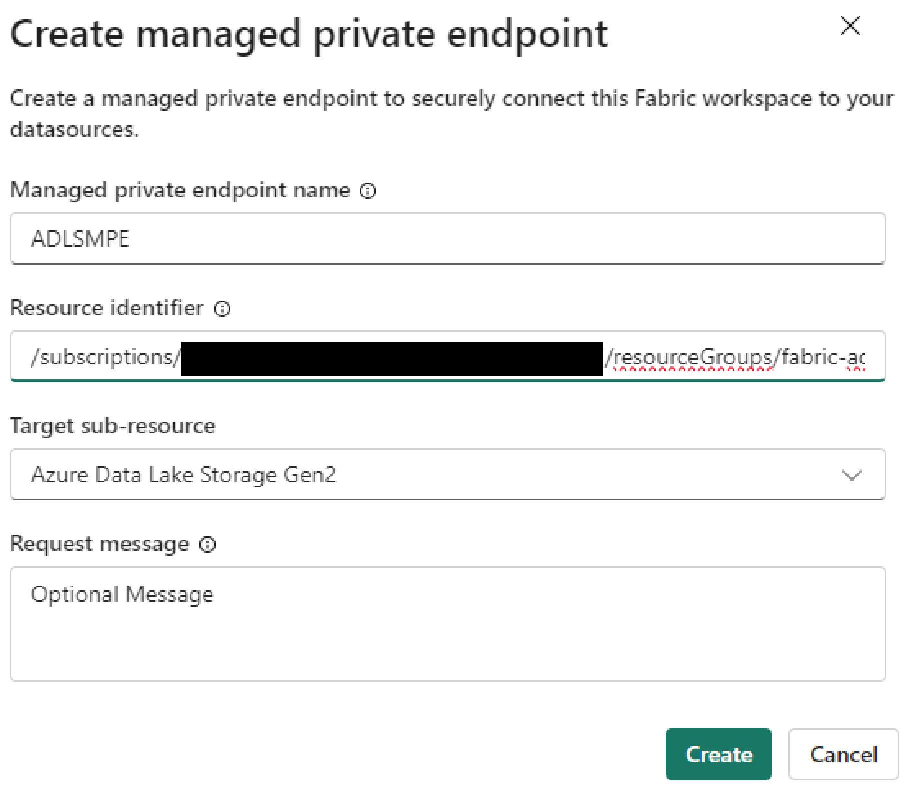
Network security

Managed private endpoints let people securely connect to an Azure r service. Learn more

Managed private endpoints

Managed private endpoints are currently available for notebooks, lake definitions. Learn more

4. The Create Managed Private endpoint dialog opens.



Create managed private endpoint

Create a managed private endpoint to securely connect this Fabric workspace to your datasources.

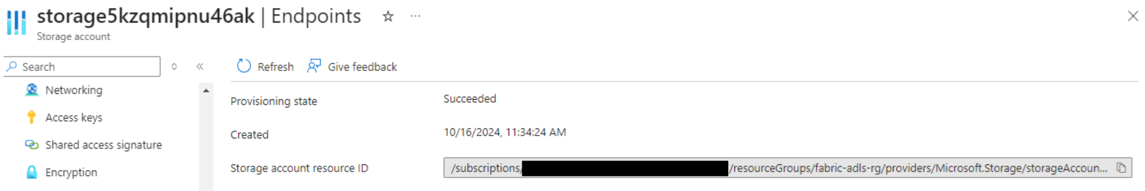
Managed private endpoint name: ADLSMPE

Resource identifier: /subscriptions/[redacted]/resourceGroups/fabric-ac

Target sub-resource: Azure Data Lake Storage Gen2

Request message: Optional Message

5. Specify a name for the private endpoint and copy in the resource identifier for the Azure resource. The resource identifier can be found in the endpoints tab on the Azure portal page for the storage account. When done, click Create



storage5kzqmipnu46ak | Endpoints

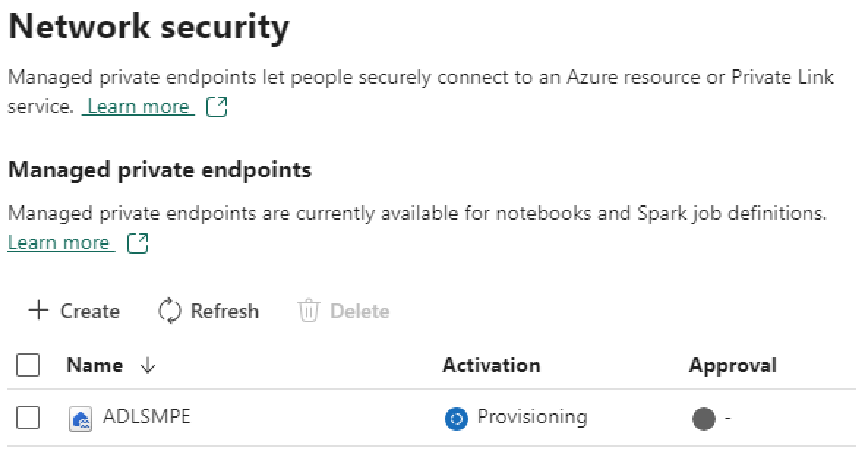
Storage account

Provisioning state: Succeeded

Created: 10/16/2024, 11:34:24 AM

Storage account resource ID: /subscriptions/[redacted]/resourceGroups/fabric-adls-rg/providers/Microsoft.Storage/storageAccoun...

6. The state will now show Provisioning



Network security

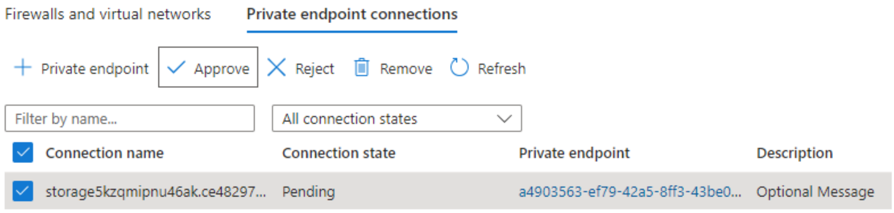
Managed private endpoints let people securely connect to an Azure resource or Private Link service. Learn more

Managed private endpoints

Managed private endpoints are currently available for notebooks and Spark job definitions. Learn more

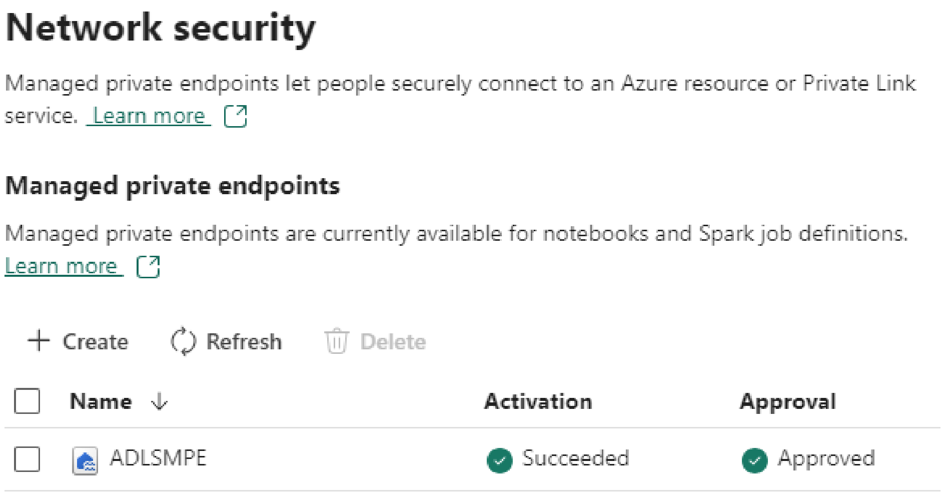
☐	Name	Activation	Approval
☐	ADLSMPE	Provisioning	● -

7. At this stage, head back to the ADLS Gen 2 account in the Azure portal, click on Networking and click on the Private Endpoints Connections tab. The request for creating the Private Endpoint from Fabric should show up here in Pending status here. Select the request and click Approve and click Yes in the Approve Connection dialog



☑	Connection name	Connection state	Private endpoint	Description
☑	storage5kzqmipnu46ak.ce48297...	Pending	a4903563-ef79-42a5-8ff3-43be0...	Optional Message

8. It may take about 2-3 minutes for the Activation status in the Fabric portal to change from Provisioning to Succeeded


Network security
Managed private endpoints let people securely connect to an Azure resource or Private Link service. Learn more
Managed private endpoints
Managed private endpoints are currently available for notebooks and Spark job definitions.
Learn more
+ Create
Refresh
Delete

□	Name ↓	Activation	Approval
□	ADLSMPE	✓ Succeeded	✓ Approved

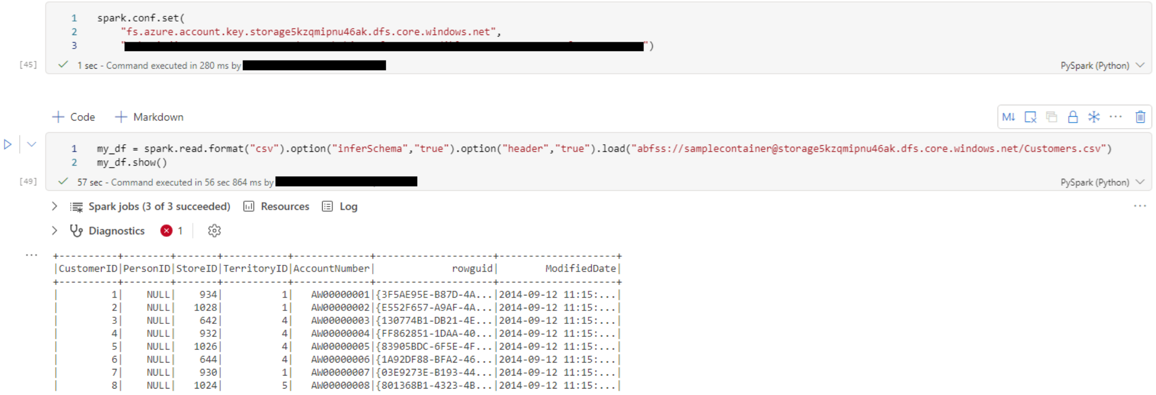
9. Next, create a notebook in your workspace by clicking on New Item and selecting Notebook
10. In the notebook, copy/paste the following line of code by replacing the <storage-account> with your storage account and the “<Account Key>” with the account key of your storage account. Note it is not recommended to use the account key but it is only being done here for demo purposes. Also note that running the cell for the first time will take 3-5 minutes as a Spark cluster needs to be setup

```
spark.conf.set(
    "fs.azure.account.key.<storage-account>.dfs.core.windows.net",
    "<Account Key>")
```

11. You can get the account key from the storage account by navigating to: Security+Networking → Access Keys → Under Key1 → Click on Show to show the key and then click on the Copy icon to copy the key
12. Next copy/paste the below script in a new cell in the notebook to load the Customers.CSV into a dataframe and display it

```
my_df = spark.read.format("csv").option("inferSchema","true").option("header","true").load("abfss://samplecontainer@ <storage-account>.dfs.core.windows.net/Customers.csv")
my_df.show()
```

13. The overall notebook execution should resemble the below



```
spark.conf.set(
    "fs.azure.account.key.storage5kzqmipnu46ak.dfs.core.windows.net",
    "[redacted]")
```

[45] ✓ 1 sec - Command executed in 280 ms by [redacted]

```
my_df = spark.read.format("csv").option("inferSchema","true").option("header","true").load("abfss://samplecontainer@storage5kzqmipnu46ak.dfs.core.windows.net/Customers.csv")
my_df.show()
```

[49] ✓ 57 sec - Command executed in 56 sec 864 ms by [redacted]

```
+----------+--------+-------+-----------+-------------+--------------------+--------------------+
|CustomerID|PersonID|StoreID|TerritoryID|AccountNumber|             rowguid|        ModifiedDate|
+----------+--------+-------+-----------+-------------+--------------------+--------------------+
|         1|    NULL|    934|          1|   AW00000001|{3F5AE95E-B87D-4A...|2014-09-12 11:15:...|
|         2|    NULL|   1028|          1|   AW00000002|{E552F657-A9AF-4A...|2014-09-12 11:15:...|
|         3|    NULL|    642|          4|   AW00000003|{130774B1-DB21-4E...|2014-09-12 11:15:...|
|         4|    NULL|    932|          4|   AW00000004|{FF862851-1DAA-40...|2014-09-12 11:15:...|
|         5|    NULL|   1026|          4|   AW00000005|{83905BDC-6F5E-4F...|2014-09-12 11:15:...|
|         6|    NULL|    644|          4|   AW00000006|{1A92DF88-BFA2-46...|2014-09-12 11:15:...|
|         7|    NULL|    930|          1|   AW00000007|{03E9273E-B193-44...|2014-09-12 11:15:...|
|         8|    NULL|   1024|          5|   AW00000008|{801368B1-4323-4B...|2014-09-12 11:15:...|
```

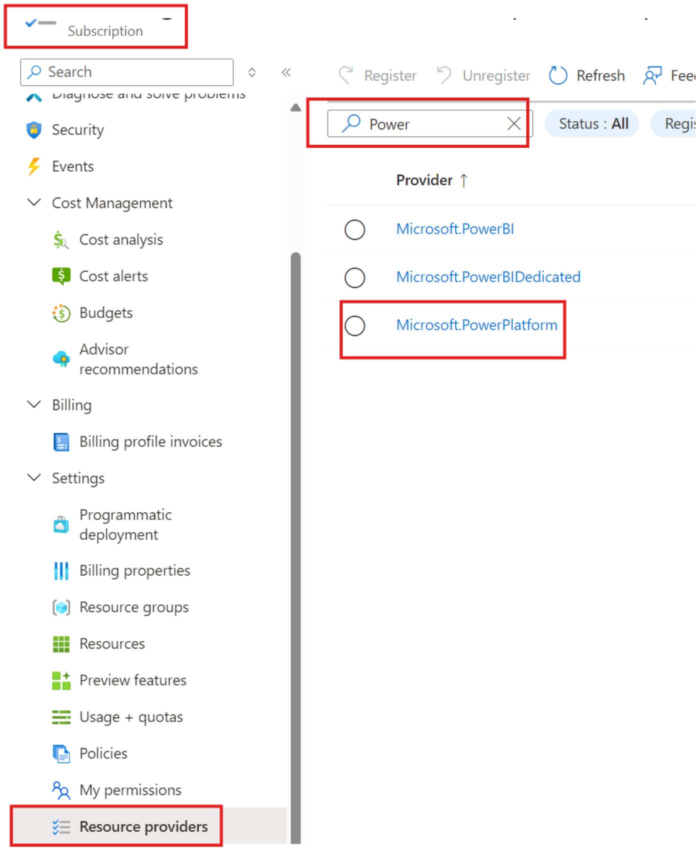
This concludes enabling Managed Private Endpoints in Fabric

Task 9: Managed VNET Gateway

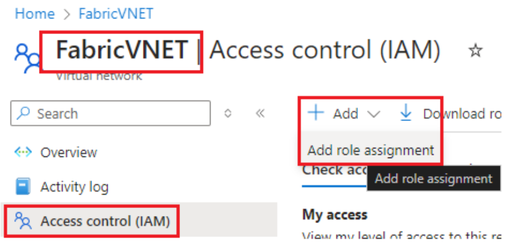
In this task, you will learn how to connect and query from secured data sources using Fabric DataFlow Gen2 via Managed Virtual Network.

Recall earlier in Task 2, we created a VNET with 2 subnets. We will use the VNETGatewaySubnet in this task to implement the Managed VNET Gateway. Since both sql vm subnet and vnetgateway subnet are on same vnet, both subnets can communicate with each other without any additional config.

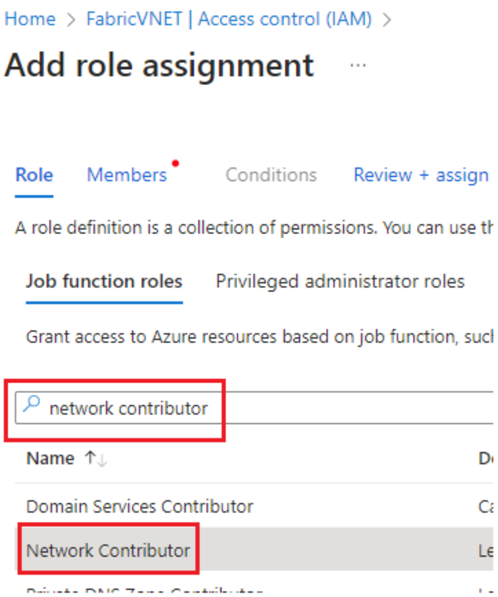
1. The first step is to register the Microsoft.PowerPlatform as a resource provider for the subscription that contains the VNet.
2. Sign in to the Azure portal.
3. Open your subscirption
4. Under Settings, Select Resource providers.
5. In the filter pane search for Microsoft.PowerPlatform and then hit Register.



6. In Azure portal Search bar, type FabricVNET and hit Enter
7. click on Access Control (IAM) On the left navigation.
8. Click on Add and select Add Role Assignment



9. In the Add role assignment dialog, select Network Contributor



Home > FabricVNET | Access control (IAM) >

Add role assignment ···

Role | Members | Conditions | Review + assign

A role definition is a collection of permissions. You can use th

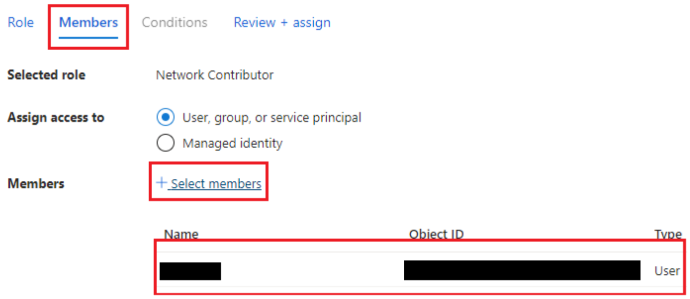
Job function roles | Privileged administrator roles

Grant access to Azure resources based on job function, sucl

network contributor

Name ↑↓	De
Domain Services Contributor	Ca
Network Contributor	Le

10. In the members tab, click on select members and search for your user account and add and click on Review + assign twice to assign the permission



Role | Members | Conditions | Review + assign

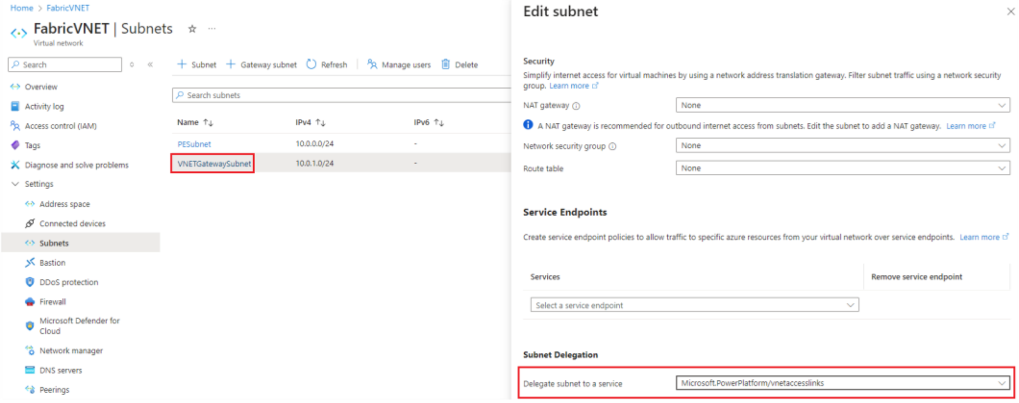
Selected role: Network Contributor

Assign access to: ● User, group, or service principal ○ Managed identity

Members: + Select members

Name	Object ID	Type
[redacted]	[redacted]	User

11. FabricVnet -> settings-> subnets -> VNETGateway subnet and click on the name to edit the subnet. Scroll down to the Subnet Delegation section and select Microsoft.PowerPlatform/vnetaccesslinks



Name ↑↓	IPv4 ↑↓	IPv6 ↑↓
PESubnet	10.0.0.0/24	-
VNETGatewaySubnet	10.0.1.0/24	-

Edit subnet

Security

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. Learn more

NAT gateway: None

A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. Learn more

Network security group: None

Route table: None

Service Endpoints

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more

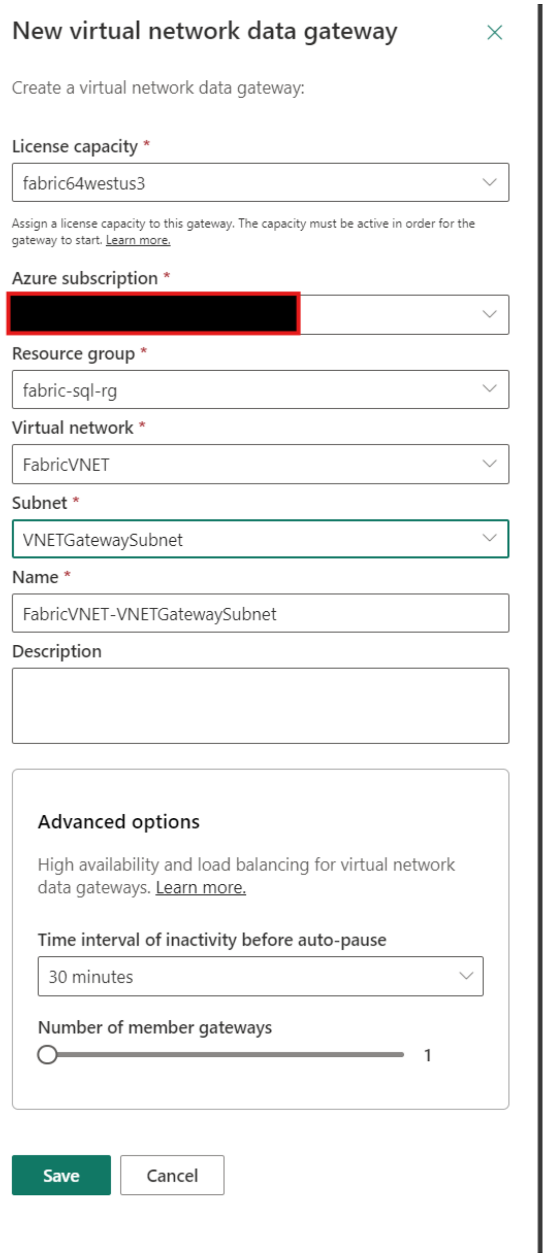
Services	Remove service endpoint
Select a service endpoint	

Subnet Delegation

Delegate subnet to a service: Microsoft.PowerPlatform/vnetaccesslinks

12. Click Save
13. Sign into the [Fabric portal](). In the top navigation bar, select the settings gear icon on the right.
14. From the drop down, select the Manage connections and gateways page.
15. Select Virtual network (VNet) data gateway > New.

16. Select the license capacity, subscription, resource group(where FabricVNET is deployed), VNet and the Subnet. Only subnets that are delegated to Microsoft Power Platform are displayed in the drop-down list.



New virtual network data gateway

Create a virtual network data gateway:

License capacity *: fabric64westus3

Assign a license capacity to this gateway. The capacity must be active in order for the gateway to start. Learn more.

Azure subscription *: [redacted]

Resource group *: fabric-sql-rg

Virtual network *: FabricVNET

Subnet *: VNETGatewaySubnet

Name *: FabricVNET-VNETGatewaySubnet

Description

Advanced options

High availability and load balancing for virtual network data gateways. Learn more.

Time interval of inactivity before auto-pause: 30 minutes

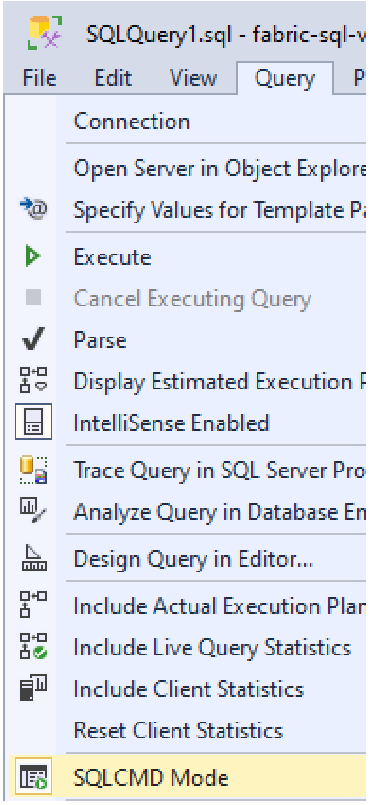
Number of member gateways: 1

By default, we provide a unique name for this data gateway, but you could optionally update it.

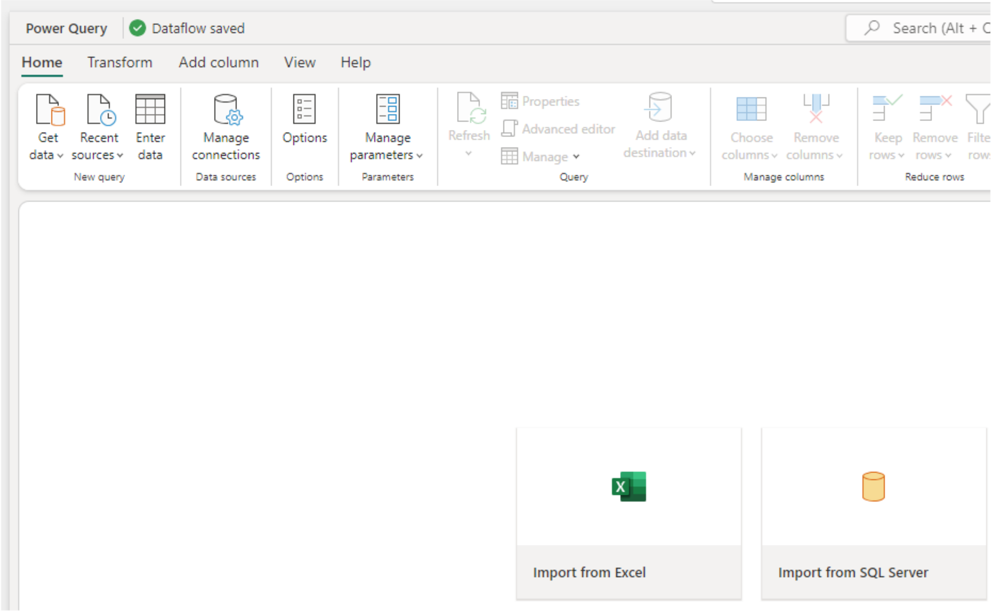
17. Select Save. This VNet data gateway is now displayed in your Virtual network data gateways tab. A VNet data gateway is a managed gateway that could be used for controlling access to this resource for Power platform users.

Lastly, we will create a Data Flow Gen2 item to connect to the SQL Server on the VM that was deployed in Task 4 using the VNET Gateway

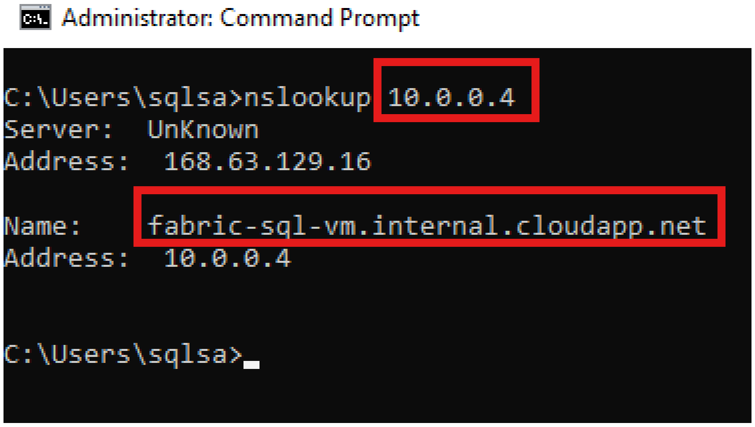
1. Login to the VM deployed in Task 4
2. Launch SQL Server Management Studio and connect to the SQL Server instance
3. Important: Enable SQLCMD Mode from Query Menu tab or by opening a new query window and pressing ALT + Q + M


SQLQuery1.sql - fabric-sql-v
File
Edit
View
Query
P
Connection
Open Server in Object Explore
Specify Values for Template Pa
Execute
Cancel Executing Query
Parse
Display Estimated Execution P
IntelliSense Enabled
Trace Query in SQL Server Pro
Analyze Query in Database En
Design Query in Editor...
Include Actual Execution Plan
Include Live Query Statistics
Include Client Statistics
Reset Client Statistics
SQLCMD Mode

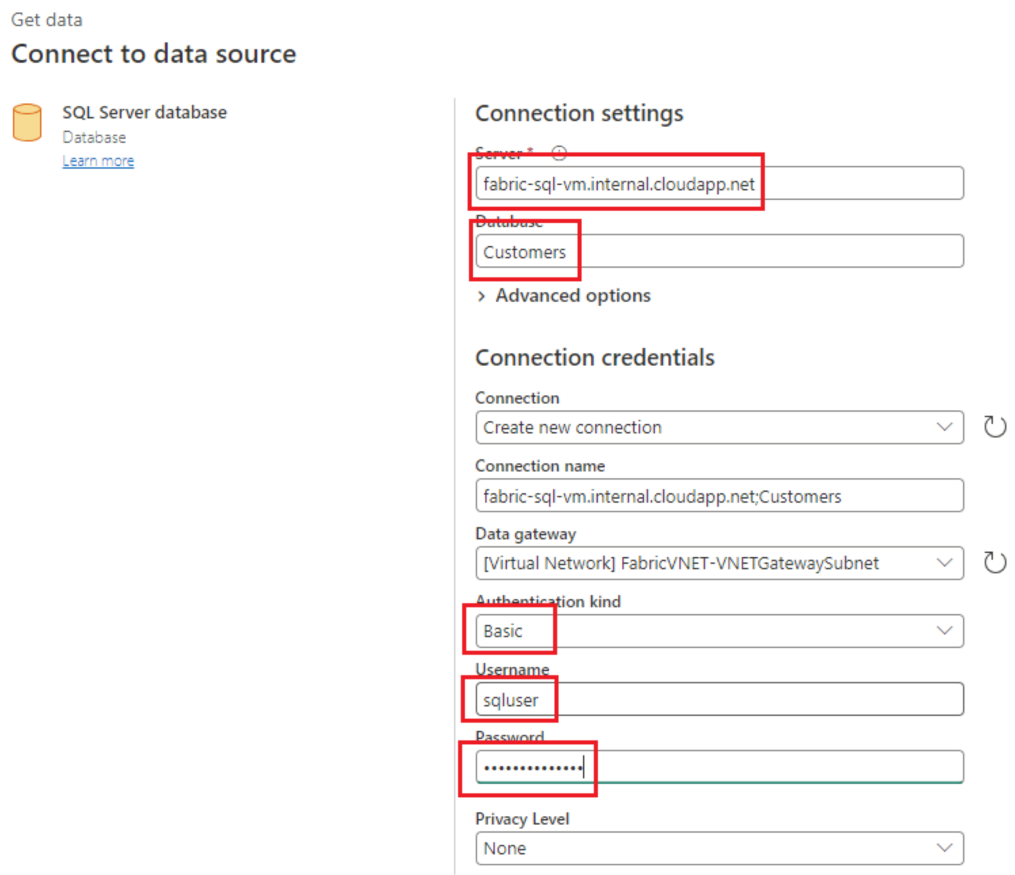
4. Copy text from PrepSQL.sql , provide a strong password in for sqluser in the script before executing the SQL Script.
   - **NOTE**: If SQLCMD Mode is enabled query should not throw an error. If you see an error in query make sure to run through step 3 again and rerun step4.
   - This script changes the authentication mode for SQL Server to Mixed Mode: Currently only windows authentication is enabled, doing this enables sql server authentication as well. VNET Gateway only support SQL Authenticated users.
   - Restarts the SQL Server instance: For Mixed Mode Authentication to take effect
   - Enables port 1433 on the windows firewall: For VNET Gateway to make Inbound connection into Sql Server
   - Creates a new database-Customers, new table -TblCustomers,new SQL Authenticated user, gives new user db_reader permission to the Customers database
5. In the Fabric workspace, click on New to create a new item and select Data Flow Gen2
6. Once the Data Flow Gen2 opens up, click Import from SQL Server



7. In the Connect to a data store dialog, provide the values as shown below and click next: Grab private ip of vm from Azure Portal, go to vm command prompt and do nslookup to get full servername(fabric-sql-vm.internal.cloudapp.net)


Administrator: Command Prompt

```
C:\Users\sqlsa>nslookup 10.0.0.4
Server:  UnKnown
Address:  168.63.129.16

Name:    fabric-sql-vm.internal.cloudapp.net
Address:  10.0.0.4


C:\Users\sqlsa>_
```



Get data

Connect to data source

SQL Server database
Database
Learn more

Connection settings

Server *: fabric-sql-vm.internal.cloudapp.net

Database: Customers

› Advanced options

Connection credentials

Connection: Create new connection

Connection name: fabric-sql-vm.internal.cloudapp.net;Customers

Data gateway: [Virtual Network] FabricVNET-VNETGatewaySubnet

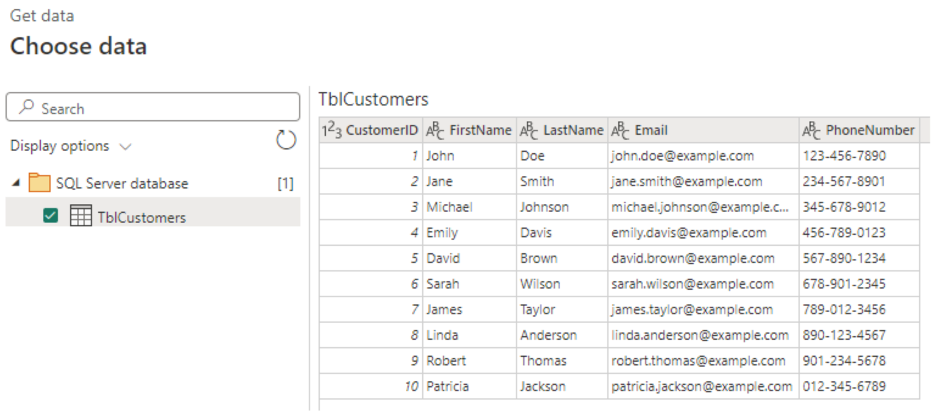
Authentication kind: Basic

Username: sqluser

Password: ••••••••••••••

Privacy Level: None

8. You should now be able to see the TblCustomers table and selecting that should show all the values of the table



Get data

Choose data

TblCustomers

CustomerID	FirstName	LastName	Email	PhoneNumber
1	John	Doe	john.doe@example.com	123-456-7890
2	Jane	Smith	jane.smith@example.com	234-567-8901
3	Michael	Johnson	michael.johnson@example.c...	345-678-9012
4	Emily	Davis	emily.davis@example.com	456-789-0123
5	David	Brown	david.brown@example.com	567-890-1234
6	Sarah	Wilson	sarah.wilson@example.com	678-901-2345
7	James	Taylor	james.taylor@example.com	789-012-3456
8	Linda	Anderson	linda.anderson@example.com	890-123-4567
9	Robert	Thomas	robert.thomas@example.com	901-234-5678
10	Patricia	Jackson	patricia.jackson@example.com	012-345-6789

9. Click on Create to create the dataflow and then click on Publish to publish the same

This concludes enabling Managed VNET Gateway in Fabric

Task 10: Row Level Security

In this task, you will learn how to implement Row Level Security within a Data Warehouse and test the implementation of the same

This step should be done using the Admin User

If you are using Azure Data Studio, make sure your account is linked

You have to use Microsoft Entra ID to authenticate.

Once you are connected to your warehouse, select governance_wh and create a new query

Copy and paste the following query to create a Sales table

```
CREATE TABLE dbo.Sales

(

  OrderID int,

  SalesRep varchar(100),

  Product varchar(10),

  Qty int

);
```

Run the command

Copy and paste the following command to insert some data (replace the 'user01@yourcompany.com' and user02@yourcompany.com' with valid user accounts)

```
INSERT INTO dbo.Sales

VALUES

  (1, 'user01@yourcompany.com', 'Valve', 5),

  (2, 'user01@yourcompany.com', 'Wheel', 2),

  (3, 'user01@yourcompany.com', 'Valve', 4),

  (4, 'user02@yourcompany.com', 'Bracket', 2),

  (5, 'user02@yourcompany.com', 'Wheel', 5),

  (6, 'user02@yourcompany.com', 'Seat', 5)
```

Copy and paste the following command to select from the same table. As you are an admin you will be able to see all rows.

```
SELECT * FROM dbo.Sales;
```

Now, let's grant permission to specific users

Run the following command

```
GRANT SELECT ON OBJECT::dbo.Sales TO [<user01@yourcompany.com>];

GRANT SELECT ON OBJECT::dbo.Sales TO [<user02@yourcompany.com>];

GO
```

Replace user01@yourcompany.com and user02@yourcompany.com for the user you want.

You must keep the brackets “[ ]”

Run the below script to create the security function.

```
CREATE SCHEMA security;

GO

CREATE FUNCTION security.fn_rls_sales_predicate(@salesRep AS nvarchar(100))

  RETURNS TABLE

WITH SCHEMABINDING

AS

  RETURN SELECT 1 AS result

WHERE @salesRep = USER_NAME() OR USER_NAME() =
'<workspaceadminuser@yourcompany.com>';
```

The function returns 1 when a row in the SalesRep column is the same as the user executing the query (@SalesRep = USER_NAME()) or if the user executing the query is the Manager user (USER_NAME() = 'workspaceadminuser@yourcompany.com'):

Replace <workspaceadminuser@yourcompany.com> for the workspace admin user and run the command.

Copy and paste the following command to create the security function.

```
CREATE SECURITY POLICY security.Sales_PolicyFilter

ADD FILTER PREDICATE security.fn_rls_sales_predicate(SalesRep)

ON dbo.Sales

WITH (STATE = ON)
```

Copy and paste the following command.

SELECT *

FROM dbo.Sales;

Run the command.

You are able to all rows.

Task 5.1 – Row level Security – User01

This step should be done using the user: user01@yourcompany.com

If you are using Azure Data Studio, make sure your account is linked.

You have to use Microsoft Entra ID to authenticate.

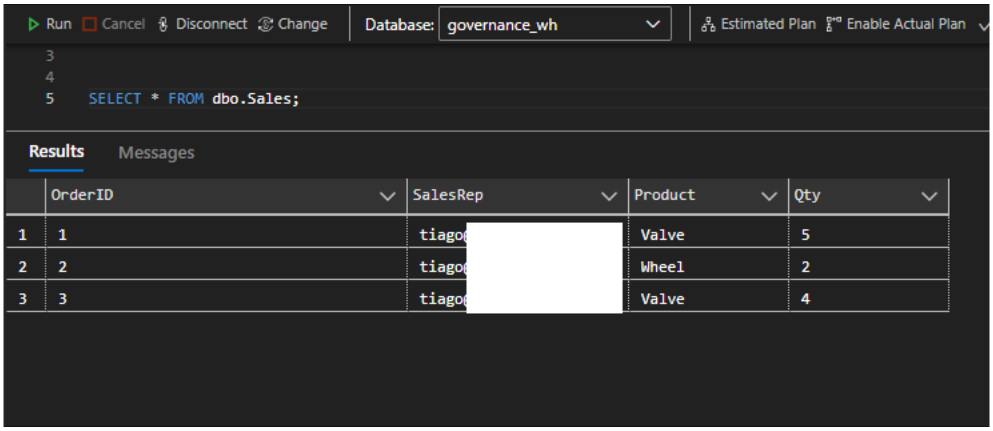
Once you are connected to your warehouse, select governance_wh and create a new query

Copy and paste the following command.

SELECT *

FROM dbo.Sales;

Run the command.



Database: governance_wh

```
SELECT * FROM dbo.Sales;
```

	OrderID	SalesRep	Product	Qty
1	1	tiago[redacted]	Valve	5
2	2	tiago[redacted]	Wheel	2
3	3	tiago[redacted]	Valve	4

You can only see rows that belong to the user: user01@yourcompany.com

Task 5.2 – Row level Security – User02

This step should be done using the user: user02@yourcompany.com

If you are using Azure Data Studio, make sure your account is linked.

You have to use Microsoft Entra ID to authenticate.

Once you are connected to your warehouse, select governance_wh and create a new query

Run the following command.

```
SELECT *

FROM dbo.Sales;
```

You can only see rows that belong to the user: user02@yourcompany.com

Task 6: Column level security

In this task, you will learn how to implement Column Level Security within a Data Warehouse and test the implementation of the same

This step should be done using the Admin User

If you are using Azure Data Studio, make sure your account is linked.

You have to use Microsoft Entra ID to authenticate.

Once you are connected to your warehouse, select governance_wh and create a new query

Replace user01@yourcompany.com for the user and run the command.

Run the following command

```
REVOKE SELECT ON OBJECT::dbo.Trip TO [<user01@yourcompany.com>];

GO
```

Run the following command

The statement is to ensure no other permission from the previous task will influence

```
GRANT SELECT ON dbo.Trip
  (  [DateID]
    ,[MedallionID]
    ,[PassengerCount]
    ,[PaymentType]
    ,[TotalAmount]
    )
TO [<user01@yourcompany.com>];
```

Step 6.1 – Querying columns – User01

This step should be done using the User01

If you are using Azure Data Studio, make sure your account is linked.

You have to use Microsoft Entra ID to authenticate.

Once you are connected to your warehouse, select governance_wh and create a new query

Run the following command

```
SELECT [DateID]
```

```
    ,[MedallionID]
    ,[PaymentType]
    ,[FareAmount]
    ,[SurchargeAmount]
    ,[TaxAmount]
    ,[TipAmount]
    ,[TollsAmount]
    ,[TotalAmount]
 FROM [dbo].[Trip]
```

This query will fail due to lack of permission.

Now, run the following command.

```
SELECT [DateID]
    ,[MedallionID]
    ,[PassengerCount]
    ,[PaymentType]
    ,[TotalAmount]
FROM [dbo].[Trip]
```

This query will complete successfully.

Task 7: Data Masking

In this task, you will learn how to implement Data Masing within a Data Warehouse and test the implementation of the same

This step should be done using the Admin User.

If you are using Azure Data Studio, make sure your account is linked.

You have to use Microsoft Entra ID to authenticate.

Once you are connected to your warehouse, select governance_wh and create a new query.

Run the following command to create a table and insert some data.

```
DROP TABLE IF EXISTS dbo.Person;

CREATE TABLE dbo.Person (PersonId   INT NOT NULL,

    Firstname VARCHAR(40) NOT NULL,

    Lastname VARCHAR(40) NOT NULL,

    Username VARCHAR(40) NOT NULL,

    UserLoginID BIGINT MASKED WITH (FUNCTION = 'random(50000, 75000)') NOT NULL,

    Email VARCHAR(50)  MASKED WITH (FUNCTION = 'email()') NOT NULL,

    UserPwd VARCHAR(50)  MASKED WITH (FUNCTION = 'default()') NOT NULL

  ) ;

  GO


INSERT INTO dbo.Person (PersonId, Firstname, Lastname, Username, UserLoginID, Email, UserPwd)

VALUES

 (1,'John','Smith','JSmith', 372036854775808, 'johnsmith@gmail.com','123456ABCDE'),

 (2,'Jane','Doe','JDoe', 372032254855106, 'janedoe@gmail.com','112233ZYXWV'),

 (3,'Walt','Disney','WDisney', 372031114679991, 'waltdisney@gmail.com','998877AZBYC');
```

Now, let’s grant access to this table to user01

Replace user01@yourcompany.com for the user and run the command.

```
GRANT SELECT ON OBJECT::dbo.Person TO [<user01@yourcompany.com>];
```

Step 7.1- Querying data – User01

This step should be done using the User01

If you are using Azure Data Studio, make sure your account is linked.

You have to use Microsoft Entra ID to authenticate.

Once you are connected to your warehouse, select governance_wh and create a new query

Run the following command

SELECT * FROM dbo.Person

You can see that the data is masked.

Step 7.2 – Removing data masking

This step should be done using the Admin User

If you are using Azure Data Studio, make sure your account is linked.

You have to use Microsoft Entra ID to authenticate.

Once you are connected to your warehouse, select governance_wh and create a new query

Run the following command

ALTER TABLE dbo.Person ALTER COLUMN [UserPwd] DROP MASKED

This command removes masking on UserPwd column.

Step 7.3 – Querying data without data masking

This step should be done using the User01

If you are using Azure Data Studio, make sure your account is linked.

You have to use Microsoft Entra ID to authenticate.

Once you are connected to your warehouse, select governance_wh and create a new query

Run the select against after masking has been removed from UserPwd column and know you will be able to see complete the complete Password

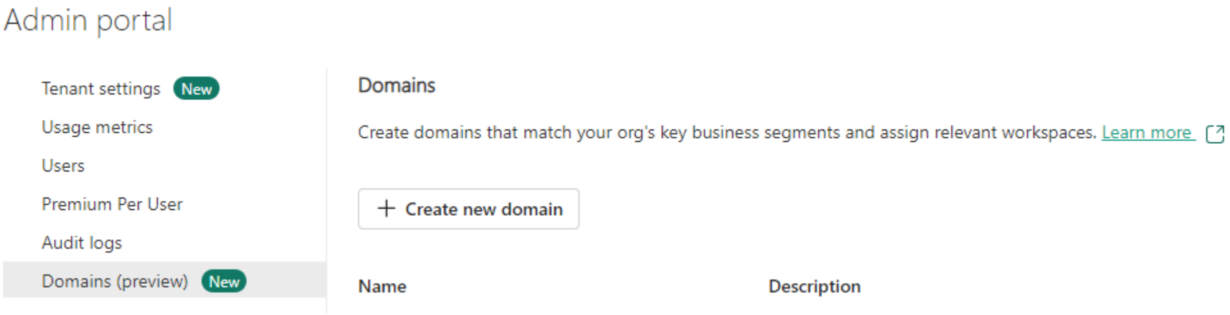
Run the following command

SELECT * FROM dbo.Person

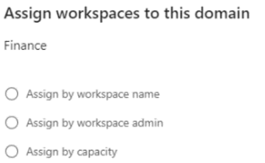
Task 8: Work with Domains (Optional)

In this task, we will explore the concept of Domains by creating them and associating workspaces with Domains and other capabilities of using domains

1. On the Admin portal click Domains and click Create new domain



2. Provide a name and description of your choice and click Apply
3. Once the domain is created, optionally, you can choose a cover image for the domain and apply
4. Optionally, you can also add Domain Admins by click on Domain Admins and adding a user. Similarly, you can also add a Domain Contributor user too
5. Finally, you can bulk add workspaces to this domain by clicking the Workspaces in this Domain and clicking Assign workspaces
6. In the resulting dialog box, explore the options to add workspaces using all the three options below:



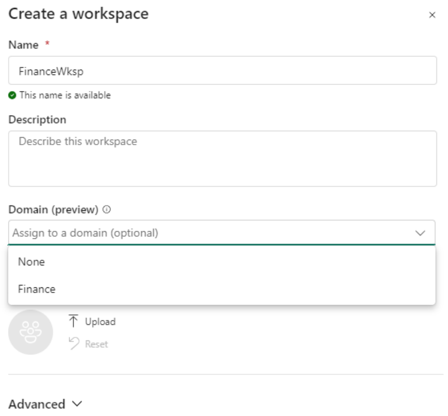
Assign workspaces to this domain

Finance

○ Assign by workspace name
○ Assign by workspace admin
○ Assign by capacity

7. Assign individual workspaces to domains:

a. It can be done during workspace creation time like the below:

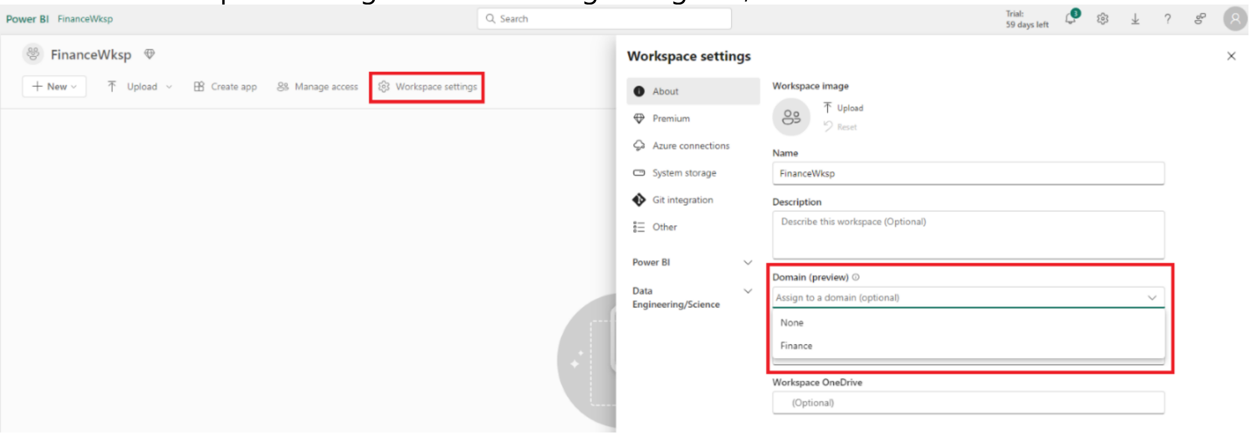

Create a workspace

Name *
FinanceWksp
This name is available

Description
Describe this workspace

Domain (preview)
Assign to a domain (optional)

b. Or if the workspace is already created, navigate to the workspace, click the workspace settings. In the resulting dialog box, select the domain


Workspace settings

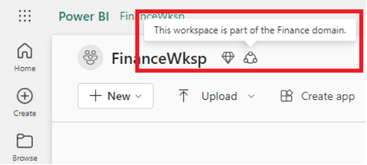
Name
FinanceWksp

Description
Describe this workspace (Optional)

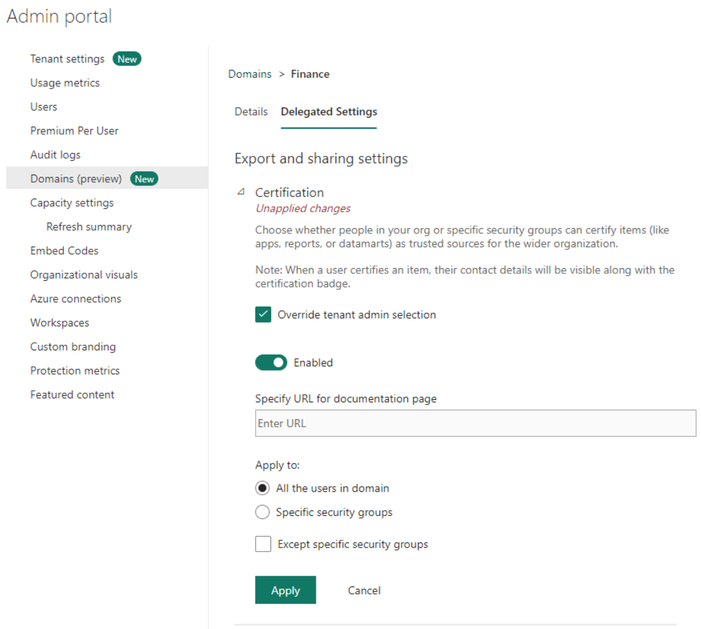
Domain (preview)
Assign to a domain (optional)

Workspace OneDrive
(Optional)

8. Once associated with a domain you will notice the workspace shows the domain icon and the domain name too


This workspace is part of the Finance domain.

9. Next, we will learn how to override tenant admin settings at the domain level by first enabling the override option at the tenant level
10. In the Admin portal, search for certification settings and toggle the Enable certification and apply it to the Entire organization
11. Also, ensure that the checkbox for Domain admins can enable/disable is checked on and click Apply



Export and sharing settings

Certification

Unapplied changes

Choose whether people in your org or specific security groups can certify items (like apps, reports, or datamarts) as trusted sources for the wider organization.

Note: When a user certifies an item, their contact details will be visible along with the certification badge.

☑ Override tenant admin selection

Enabled

Specify URL for documentation page

Enter URL

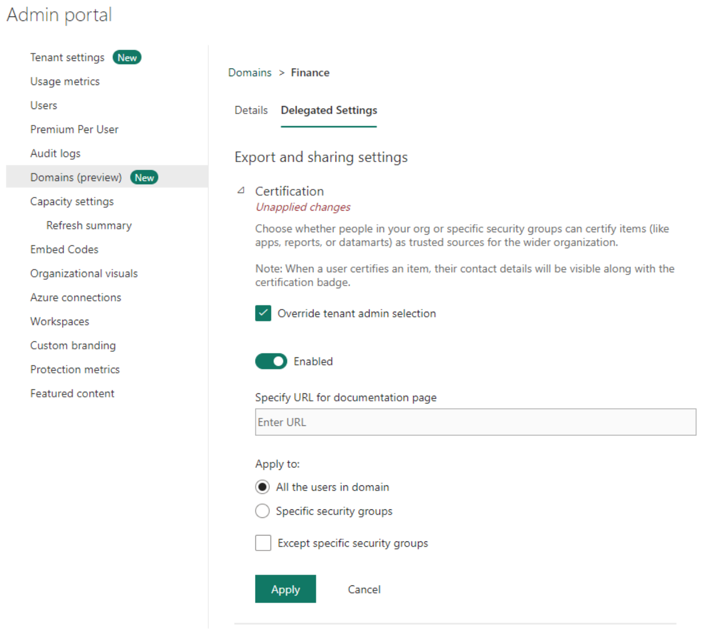
Apply to:

● All the users in domain

○ Specific security groups

□ Except specific security groups

12. From the Admin portal again, select Domains and open the Domain you created earlier
13. Click the Delegated Settings tab of the domain. You would see that you should be able to override the tenant admin settings for the Certification



Export and sharing settings

Certification

Unapplied changes

Choose whether people in your org or specific security groups can certify items (like apps, reports, or datamarts) as trusted sources for the wider organization.

Note: When a user certifies an item, their contact details will be visible along with the certification badge.

☑ Override tenant admin selection

Enabled

Specify URL for documentation page

Enter URL

Apply to:

● All the users in domain

○ Specific security groups

□ Except specific security groups

This is the end of the lab. Congratulations for finishing the lab!