

1. Create resource group for network "rg-ntt-network-dev01"

## Create a resource group ...

Basics

Tags

Review + create

 [Automation Link](#)

### Basics

Subscription	Azure subscription 1
Resource group name	rg-ntt-network-dev01
Region	East US

### Tags

None

1. Create VNet "vnet-nttdomain-dev01"

# Create virtual network ...

 Validation passed

- Basics
- Security
- IP addresses
- Tags
- Review + create

[View automation template](#)

## Basics

Subscription	Azure subscription 1
Resource Group	rg-ntt-network-dev01
Name	vnet-nttdomain-dev01
Region	East US

## Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

## IP addresses

Address space	10.0.0.0/16 (65,536 addresses)
---------------	--------------------------------

3. Create subnet for "EntraDomainServicesSubnet"
- a. Create this subnet in the same VNet "vnet-nttdomain-dev01"

## Add a subnet



Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose ⓘ

Name \* ⓘ

### IPv4

Include an IPv4 address space ☒

IPv4 address range ⓘ   
10.0.0.0 - 10.0.255.255

Starting address \* ⓘ

Size ⓘ

Subnet address range ⓘ 10.0.4.0 - 10.0.4.255

### IPv6

Include an IPv6 address space ☐ This virtual network has no IPv6 address ranges.

### Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Enable private subnet (no default outbound access) ☒

**i** After March 31, 2026, private subnet will be the default selection for new virtual networks. [Learn more](#)

- b. Create new resource group "rg-nttentrado mainservices-dev01"

# Create a resource group ...

Basics   Tags   Review + create

**Resource group** - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

Subscription \* ⓘ

Azure subscription 1

Resource group name \* ⓘ

rg-nttentradoainservices-dev01

Region \* ⓘ

(US) East US

c. Go inside and create Microsoft Entra Domain Services

# Create Microsoft Entra Domain Services ...

\* Basics   \* Networking   Administration   Synchronization   Security Settings   Tags   Review + create

Microsoft Entra Domain Services provides managed domain services such as domain join, group policy, LDAP, and Kerberos/NTLM authentication. You can use Microsoft Entra Domain Services without needing to manage, patch, or service domain controllers in the cloud. For ease and simplicity, defaults have been specified to provide a one-click deployment. [Learn more](#)

### Project details

When choosing the basic information needed for Microsoft Entra Domain Services, keep in mind that the subscription, resource group, DNS domain name, and location cannot be changed after creation.

Subscription \*

Azure subscription 1

Resource group \* ⓘ

rg-nttentradoainservices-dev01

Create new

Help me choose the subscription and resource group

DNS domain name \* ⓘ

nttentradoain.onmicrosoft.com

Help me choose the DNS name

Region \* ⓘ

(US) East US

SKU \* ⓘ

Enterprise

Help me choose a SKU

# Create Microsoft Entra Domain Services ...

\* Basics   \* **Networking**   Administration   Synchronization   Security Settings   Tags   Review + create

Microsoft Entra Domain Services uses a dedicated subnet within a virtual network to hold all of its resources. If using an existing network, ensure that the network configuration does not block the ports required for Microsoft Entra Domain Services to run. [Learn more](#)

Virtual network \* ⓘ 

vnet-nttdomain-dev01



[Create new](#)

▼ Help me choose the virtual network and address


Subnet \* ⓘ 

EntraDomainServicesSubnet (10.0.4.0/24)

[Manage](#)

 Your subnet should contain one of the private IP Address Spaces: 192.168.0.0/16, 172.16.0.0/12, or 10.0.0.0/8. While you can create public IPs, we recommend considering the associated risks before proceeding. [Learn more](#) 

▼ Help me choose the subnet and NSG

 A network security group will be automatically created and associated to the subnet to protect Microsoft Entra Domain Services. The network security group will be configured according to [guidelines for configuring NSGs](#).

## Create Microsoft Entra Domain Services ...

\* Basics \* Networking Administration Synchronization Security Settings Tags Review + create

Use these settings to specify which users should have administrative privileges and be notified of problems on your managed domain. [Learn more](#)

AAD DC Administrators ⓘ

[Manage group membership](#)

∨ Help me choose AAD DC Admins

Notifications

These groups will be notified when you have an alert of warning or critical severity

- ☒ All Global Administrators of the Microsoft Entra ID directory.
- ☒ Members of the AAD DC Administrators group.

Additional email recipients:

∨ Help me choose who gets notifications

## Create Microsoft Entra Domain Services ...

\* Basics \* Networking Administration Synchronization Security Settings Tags Review + create

Microsoft Entra Domain Services provides a one-way synchronization from Microsoft Entra ID to the managed domain. In addition, only certain attributes are synchronized down to the managed domain, along with groups, group memberships, and passwords. [Learn more](#)

Synchronization type

☒ All ☐ Cloud-only

Synchronization filter

☐ Filter by group entitlements

∨ Help me choose the synchronization settings

\* Basics \* Networking Administration Synchronization **Security Settings** Tags Review + create

Microsoft Entra Domain Services has multiple security settings that can be used to harden the domain service. When choosing to enable or disable a security setting, it is important to first understand the impact on the workloads using the domain service. [Learn more](#)

NTLM v1 authentication

Disable Enable

✓ Help me choose strong ciphers

NTLM password synchronization

Disable Enable

Password synchronization from on-premises

Disable Enable

✓ Help me choose password synchronization settings

Kerberos RC4 encryption

Disable Enable

Kerberos armoring

Disable Enable

✓ Help me choose kerberos RC4 encryption and armoring

LDAP signing

Disable Enable

LDAP channel binding

Disable Enable

✓ Help me choose LDAP signing and channel binding

- d. Click review + create
4. Get the DNS IP Address from Microsoft Entra Domain Services and Configured DNS Server settings for managed domain service IP in virtual networks "vnet-nttdomain-dev01"
  - a. Go to the resource group "rg-nttentradoainservices-dev01" > open Microsoft Entra Domain Services "nttentradoain.onmicrosoft.com" > Settings > Properties > take note the IP addresses > go to your VNet > settings > DNS > Update DNS Server IP Address; OR run the configuration diagnostics



## nttentradomain.onmicrosoft.com | Properties



Microsoft Entra Domain Services

- Overview
- Activity log
- Access control (IAM)
- Tags
- Resource visualizer
- Settings
- Properties**
- Secure LDAP
- Synchronization
- Custom attributes
- Replica sets
- Trusts

### DNS domain name

nttentradomain.onmicrosoft.com

### Locations

East US

### Virtual Networks/Subnets

[East US/vnet-nttdomain-dev01/vnet-nttdomain-dev01/EntraDomainServicesSubnet](#)

### Network security groups

[East US/aadds-nsg](#)

### IP addresses

East US/10.0.4.4 10.0.4.5

### Secure LDAP

Disabled

### Secure LDAP external IP addresses

East US/20.169.218.227



## vnet-nttdomain-dev01 | DNS



Virtual network

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Settings

### DNS server

All VMs that are connected to the virtual network register with the DNS servers that you specify for the virtual network. [Learn more](#)

DNS server	Custom ( <a href="#">Change</a> )
Custom DNS servers	10.0.4.4 10.0.4.5

### DNS private resolver

[Home](#) > [Resource Manager](#) | [Resource groups](#) > [rg-nttentradomain-services-dev01](#) > [nttentradomain.onmicrosoft.com](#)



## nttentradomain.onmicrosoft.com | Configuration diagnostics



Run

- Overview
- Activity log
- Access control (IAM)
- Tags
- Resource visualizer
- Settings
- Properties**
- Secure LDAP
- Synchronization
- Custom attributes

Diagnostics for the Microsoft Entra Domain Services

**⚠** Diagnostics completed with one or more warnings at 11/28/2025, 11:17:05 AM.

Validation	Result
East US/vnet-nttdomain-dev01/EntraDomainServicesSubnet	OK
DNS records	Warning
Issues found	
• DNS server settings for managed domain service IPs 10.0.4.4, 10.0.4.5 need to be configured for virtual networks <a href="#">East US/vnet-nttdomain-dev01</a>	
<a href="#">Fix</a>	



## 5. Create Subnet for "GatewaySubnet"

### Add a subnet ✕

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose ⓘ

Virtual Network Gateway

Name \* ⓘ

GatewaySubnet

#### IPv4

Include an IPv4 address space



IPv4 address range ⓘ

10.0.0.0/16

10.0.0.0 - 10.0.255.255

Starting address \* ⓘ

10.0.250.0

Size ⓘ

/24 (256 addresses)

Subnet address range ⓘ

10.0.250.0 - 10.0.250.255

#### IPv6

Include an IPv6 address space



This virtual network has no IPv6 address ranges.

#### Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Enable private subnet (no default outbound access)



## 4. Create Virtual Network Gateway "vnetgateway-nttdomain-dev01"

# Create virtual network gateway ...

✓ Validation passed

Basics   Tags   Review + create

## Basics

Subscription	Azure subscription 1
Resource group	rg-ntt-network-dev01
Name	vnetgateway-nttdomain-dev01
Region	East US
SKU	VpnGw2AZ
Generation	Generation2
Virtual network	vnet-nttdomain-dev01
Subnet	GatewaySubnet (10.0.250.0/24)
Gateway type	Vpn
VPN type	RouteBased
Enable active-active mode	Disabled
Enable Advanced Connectivity	Disabled
Configure BGP	Disabled
Public IP address	vnetgateway-publicip-nttdomain-dev01

## Tags

None

4. Creating the root certificate & client certificates (Reference: <https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site>)
  - a. This certificate is very important for our point-to-site configuration later
  - b. On your local computer (I assume MyPC), easier way is opening PowerShell ISE
  - c. Copy, Paste, and run the PowerShell code in PowerShell ISE Editor (with current user login):
  - d. If you facing UnauthorizedAccess error, you need to run this command "Set-ExecutionPolicy -ExecutionPolicy ByPass"

#

##

###

# STEP 0 - Set parameters. Create the directory and change location

```
$Path = "C:\Temp"
```

```
$DirName = "vnetgateway-nttdomain-dev01-CertDirectory"
```

```
$CertPassword = "100%VNetGW@12345"
```

```
$PreDefinedCertFileName_String = "vnetgateway-nttdomain-dev01-"
```

```
$CertificatePath = "Cert\CurrentUser\My"
```

# Testing Certificate Path, remove the existing (Commenting if it is not needed)

```
$ExistingCertificateList = Get-ChildItem -Path $CertificatePath
```

```
foreach($Specific_ExistingCertificateList in $ExistingCertificateList){
```

```
    Write-Host "Detected Existing Certificate (RELATED TO THIS CERT NAME ONLY):"
```

```
    Write-Host $Specific_ExistingCertificateList.Subject
```

```
    Write-Host $Specific_ExistingCertificateList.PSPath
```

```
    if(($Specific_ExistingCertificateList.Subject -eq "CN= $($PreDefinedCertFileName_String)P2SVPNClient") -  
or ($Specific_ExistingCertificateList.Subject -eq "CN= $($PreDefinedCertFileName_String)P2SRootCert")){
```

```
        $true
```

```
        Remove-Item -Path $Specific_ExistingCertificateList.PSPath -Recurse -Force
```

```
    }else{
```

```
        $false
```

```
    }
```

```
}
```

# Checking the certificate local directories (Commenting if it is not needed)

```
if(Test-Path -Path "$($Path)\ $($DirName)"){
```

```
    Remove-Item -Path "$($Path)\ $($DirName)" -Recurse -Force
```

```
}
```

```
New-Item -ItemType Directory -Path $Path -Name $DirName -Force
Set-Location -Path "$($Path)\$($DirName)"
```

```
###
```

```
##
```

```
#
```

```
#
```

```
##
```

```
###
```

```
# STEP 1 - To Create Root Certificate
```

```
# Create the self-signed Root CA (same as OpenSSL x509 root)
```

```
$rootCert = New-SelfSignedCertificate `
    -Type Custom `
    -KeyExportPolicy Exportable `
    -KeyLength 2048 `
    -KeyAlgorithm RSA `
    -KeySpec Signature `
    -HashAlgorithm SHA256 `
    -Subject "CN=$($PreDefinedCertFileName_String)P2SRootCert" `
    -CertStoreLocation "$($CertificatePath)" `
    -KeyUsageProperty Sign `
    -KeyUsage CertSign, CRLSign `
    -NotAfter (Get-Date).AddMonths(24)
```

```
# Export private key + certificate (PFX)
```

```
$Password = ConvertTo-SecureString -String $CertPassword -Force -AsPlainText
```

```
Export-PfxCertificate -Cert $rootCert -FilePath "$($PreDefinedCertFileName_String)P2SRootCA.pfx" -  
Password $Password -Force
```

```
#Export certificate only (CRT/PEM)
```

```
Export-Certificate -Cert $rootCert -FilePath "$($PreDefinedCertFileName_String)P2SRootCA.cer" -Force
```

```
certutil -encode "$($PreDefinedCertFileName_String)P2SRootCA.cer"  
"$($PreDefinedCertFileName_String)P2SRootCA.pem"
```

```
###
```

```
##
```

```
#
```

```
#
```

```
##
```

```
###
```

```
# STEP 2 - To Create Client Certificate signed by the root certificate (created in STEP 1)
```

```
# Create the client certificate request
```

```
$clientReq = New-SelfSignedCertificate `  
-Type Custom `  
-KeyExportPolicy Exportable `  
-KeyLength 2048 `  
-KeyAlgorithm RSA `  
-HashAlgorithm SHA256 `  
-NotAfter (Get-Date).AddMonths(24) `  
-KeySpec Signature `  
-Subject "CN=$($PreDefinedCertFileName_String)P2SVPNClient" `
```

```
-DnsName "$($PreDefinedCertFileName_String)P2SVPNClient" `
-CertStoreLocation "$($CertificatePath)" `
-Signer $rootCert `
-TextExtension @"(2.5.29.37={text}1.3.6.1.5.5.7.3.2)"
```

# Export PFX

```
Export-PfxCertificate -Cert $clientReq -FilePath "$($PreDefinedCertFileName_String)P2SVPNClient.pfx" -
Password $Password -Force
```

# Export public certificate

```
Export-Certificate -Cert $clientReq -FilePath "$($PreDefinedCertFileName_String)P2SVPNClient.cer" -Force
```

```
certutil -encode "$($PreDefinedCertFileName_String)P2SVPNClient.cer"
"$($PreDefinedCertFileName_String)P2SVPNClient.crt"
```

###

##

#

```

RootClientCertGenerate_AzGateway_P2S.ps1 X
1 #
2 ##
3 ###
4
5 # STEP 0 - Set parameters. Create the directory and change location
6
7 $Path = "C:\Temp"
8 $DirName = "vnetgateway-nttdomain-dev01-CertDirectory"
9 $CertPassword = "100%VNetGW@12345"
10 $PreDefinedCertFileName_String = "vnetgateway-nttdomain-dev01-"
11 $CertificatePath = "Cert:\CurrentUser\My"
12
13 # Testing Certificate Path, remove the existing (Commenting if it is not needed)
14 $ExistingCertificateList = Get-Childitem -Path $CertificatePath
15 if($ExistingCertificateList.Count -gt 0) {
16     foreach($ExistingCertificate in $ExistingCertificateList) {
17         Remove-Item $ExistingCertificate
18     }
19 }
20
21 PS C:\Temp\vnetgateway-nttdomain-dev01-CertDirectory> C:\Users\ABRFA\OneDrive - VAT\Documents\NurFaizM_Work\Project\DeCap\RootClientCertGenerate_AzGateway
Detected Existing Certificate (RELATED TO THIS CERT NAME ONLY):
CN=vnetgateway-nttdomain-dev01-P2SVPNCClient
Microsoft.PowerShell.Security\Certificate::CurrentUser\My\9AA1FDC95251891DD530AF1F60E5E7FE264E871B
True
Detected Existing Certificate (RELATED TO THIS CERT NAME ONLY):
CN=vnetgateway-nttdomain-dev01-P2SRootCert
Microsoft.PowerShell.Security\Certificate::CurrentUser\My\866550CC4B2EABA26D739B4358645943F80F76BB
True

Directory: C:\Temp

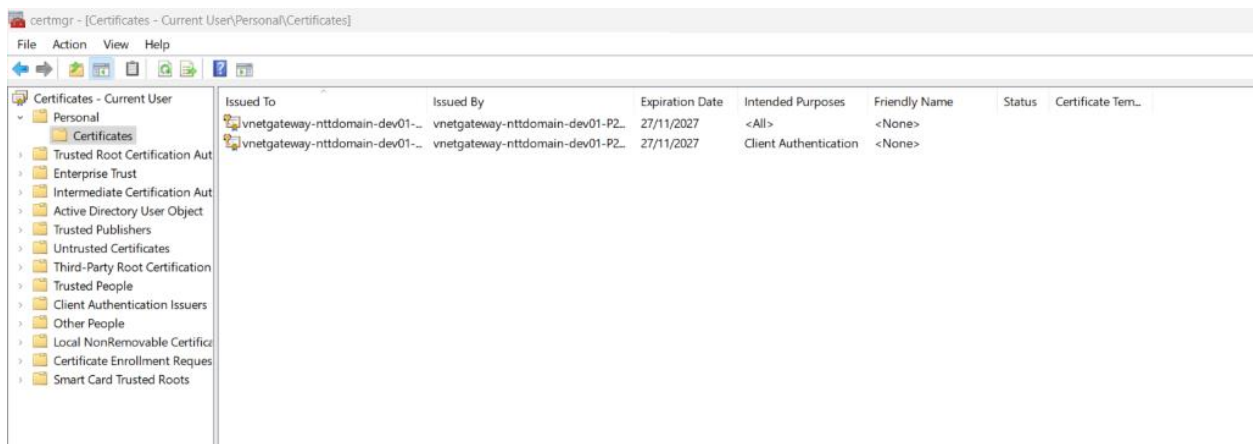
Mode                LastWriteTime         Length Name
----                -
d-----          27/11/2025   2:54 PM                vnetgateway-nttdomain-dev01-CertDirectory

Directory: C:\Temp\vnetgateway-nttdomain-dev01-CertDirectory

Mode                LastWriteTime         Length Name
----                -
-a-----          27/11/2025   2:54 PM        2652 vnetgateway-nttdomain-dev01-P2SRootCA.pfx
-a-----          27/11/2025   2:54 PM         803 vnetgateway-nttdomain-dev01-P2SRootCA.cer
Input Length = 803
Output Length = 1162
CertUtil: -encode command completed successfully.
-a-----          27/11/2025   2:54 PM        3604 vnetgateway-nttdomain-dev01-P2SVPNCClient.pfx
-a-----          27/11/2025   2:54 PM         913 vnetgateway-nttdomain-dev01-P2SVPNCClient.cer
Input Length = 913
Output Length = 1316
CertUtil: -encode command completed successfully.

```

5. Verify the cert is create in certificate manager of current users (Go to start > search for certmgr.msc > Certificates – Current User > Personal > Certificates)



6. Configuring the Point-to-site connection
  - a. Reference = <https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-certificate-gateway>
  - b. Export the root cert "vnetgateway-nttdomain-dev01-P2SRootCert". From the certificate manager of current users (Go to start > search for certmgr.msc > Certificates – Current

User > Personal > Certificates), right click > all tasks > export of this certificate "vnetgateway-nttdomain-dev01-P2SRootCert" > from the certificate export wizard: click next > select No, do not export the private key and click next > Select Base-64 encoded X.509 (.CER) for the file format and click next > Browse the location to export file and set file name > click next > click finish.

- c. Go back to the location of certificate that we've export (e.g: C:\Temp\vnetgateway-nttdomain-dev01-CertDirectory) and open it with notepad. You should see certificate like below:

```
File Edit View

|-----BEGIN CERTIFICATE-----
MIIDHzCCAgegAwIBAgIQK8j2CGZQK59Ls4SPQ+ea0zANBgkqhkiG9w0BAQsFADAy
MTAwLgYDVQQDDCk2bmV0Z2F0ZXdhcS1udHRkb21haW4tZGV2MDEtUDJUm9vdENl
cnQwHhcNMjUxMTI3MDY0NDMyWjcNMjUxMTI3MDY1NDMzWjAUMTAwLgYDVQQDDCk2
bmV0Z2F0ZXdhcS1udHRkb21haW4tZGV2MDEtUDJUm9vdENlcnQwggeEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQQDQy1S7RBF0Js7EhKtF/MimpB51mwPqwviD
/+X2dVpUpRxxXQ2tPGwVed91kJbrQuwy8J9ZLUX+aNnH3GUwnV8Z9GdhC+r/scOb
OdFaKcmie33WQcUCeIo0RVKHqW/0+GCHY6w/ct7ua6QiPX208AoktoEb6jG4y2wQ
g7YV3UJkASj57EKMMtdvXzuQRaRpgTsyYKVad10Jb9INpgH0kbCGzwKwxrWdEIhd
IDrreku7xya23EWQ8hPhBXDJJoILlcmSZU53uIiVGB1kaKrQY124XszulMSnMr3EQ
W9qnuYa+HNM/9o0KJKzUVvFzS1jK5IzKoO+bVehqdpYfKXNxmTABAgMBAAGjMTAv
MA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUpozAQp6fH+B665dT9bzAuH7s60Aw
DQYJKoZIhvcNAQELBQADggEBABaQ1Wgi+IAgiXkNByrnW394+Go0tZvFaG09KHSO
UjQPdtrPu9cVo2Bm+7KFcV/jijo8dB1cPra9fu6IUi9RrR5QMbWYqzfcZdwbg43/
vaY3uFQrcxgzYnfUH+YhHFKSMYnwzQCG209kEwg4St6EydqrGr6ZqxiBDEpPR6kx
jH83v5abaDCvar1ZmdBRHB+rhs8rBk6bEFkIZs1turvyMyDzLz5mBBZmGVE1K4T6
jI4fnm8V7/SB1XI4y1dN1tCIqKxr74BpEeMJooQF1t00UjpiSXF8YE6efxhpRtT
yRsCmtwXoB8zikDC0900GODpBP0ReNm2idCoGKjcgJJUkpA=
-----END CERTIFICATE-----
```

- d. Go back to your Virtual Network Gateway > Settings > Point-to-Site- Configuration > Click Configure Now:
  - i. Enter the custom our defined private IP range that will be using in P2S client (e.g 172.16.201.0/24) in Address Pool
    1. The P2S client address pool must NOT overlap with:
      - a. Your VNet (e.g. 10.0.0.0/16 or whatever you use)
      - b. The GatewaySubnet (10.0.250.0/24)
      - c. On-premises networks (if hybrid)
      - d. Other P2S pools (if multiple gateways)



- ii. Tunnel type set OpenVPN (SSL)
- iii. Authentication type = Azure Certificate
- iv. Root Certificates (Name = Set same Root certificate name that we export on previous step, Public Certificate Data = Copy from the certificate data that we open with notepad)
- v. Click save and download the VPN client

**vnetgateway-nttdomain-dev01 | Point-to-site configuration** ☆ ...

Virtual network gateway

Search [ ] Save Discard Delete Download VPN client

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Configuration

Connections

Point-to-site configuration

NAT Rules

Maintenance

Properties

Locks

Monitoring

Automation

Help

Address pool \*

172.16.201.0/24 ✓

Tunnel type

OpenVPN (SSL) ▾

Authentication type

Azure certificate ▾

Root certificates

Name	Public certificate data
vnetgateway-nttdomain-dev01-P25RootCert ✓	MIIDHzCCAgegAwIBAgIQK8j2CGZQK59Ls45PQ+ea0zANBgkqhkiG9w0BAQsFA... ✓

Revoked certificates

Name	Thumbprint

Additional routes to advertise

**vnetgateway-nttdomain-dev01 | Point-to-site configuration** ☆ ...

Virtual network gateway

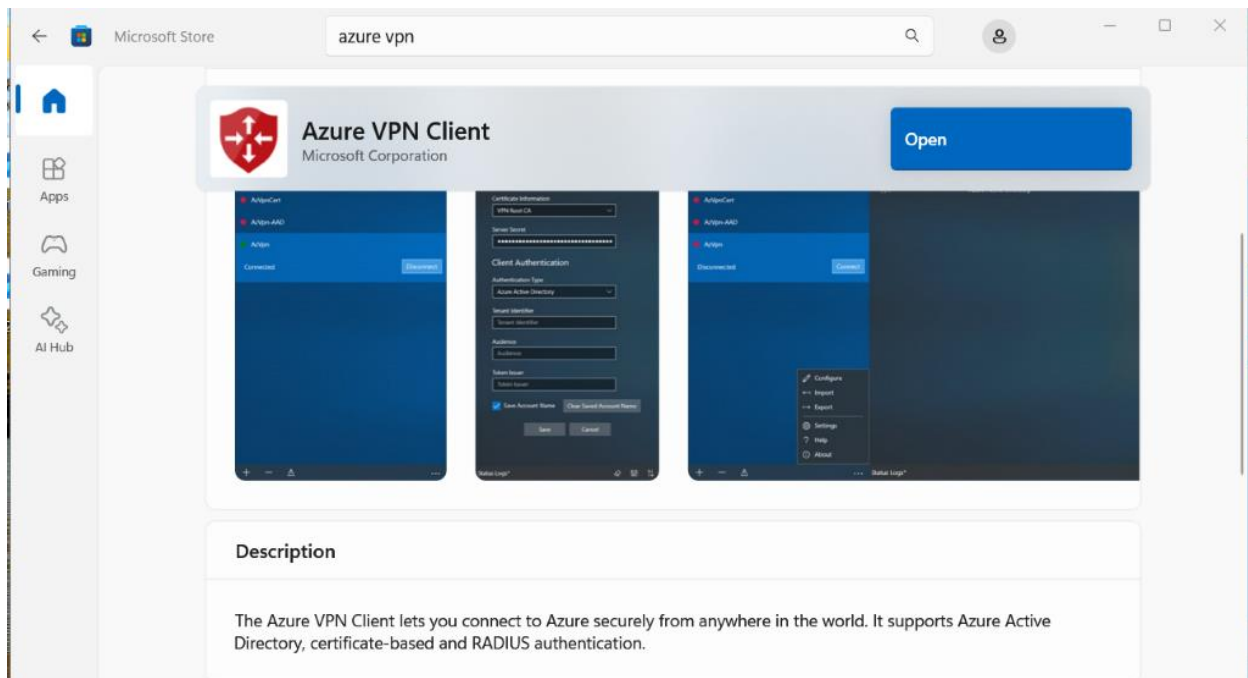
Search [ ] Save Discard Delete Download VPN client

- e. Testing the Azure VPN Client:
  - i. Once you have download the VPN client from the Azure Point-To-Site, you may extract it. It should look like below. Inside the folder should have the AzureVPN folder and inside that we have the VPN profiles

✓ Today

AzureVPN	27/11/2025 3:40 PM
Generic	27/11/2025 3:40 PM
OpenVPN	27/11/2025 3:40 PM

- ii. If no Azure VPN installer, we can get it from Microsoft Store



- iii. (Assume we are in client computer) Once Azure VPN Client Install, then we need to configure it. First import the client certificate (\*.pfx) on the client side. **IMPORTANT:** Client certificate must be import into any client side (Can use automation / GPO / Policies to do that). When import the client certificate, it may asking for the password, please enter password that we set in the script earlier.
- iv. From azure VPN Client click + icon > click import

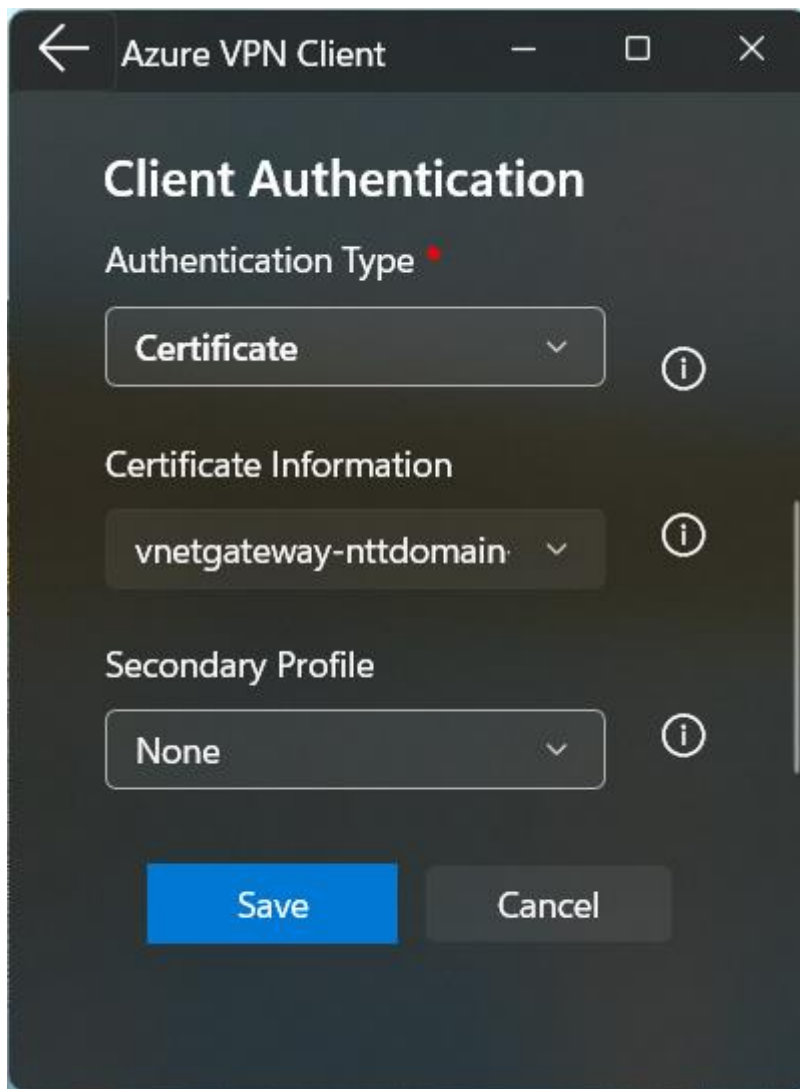


- v. Go to VPN Profiles that we've download previously (inside AzureVPN folder), you will see azurevpnconfig.xml > select and click Open. You will see connection name, server validation information

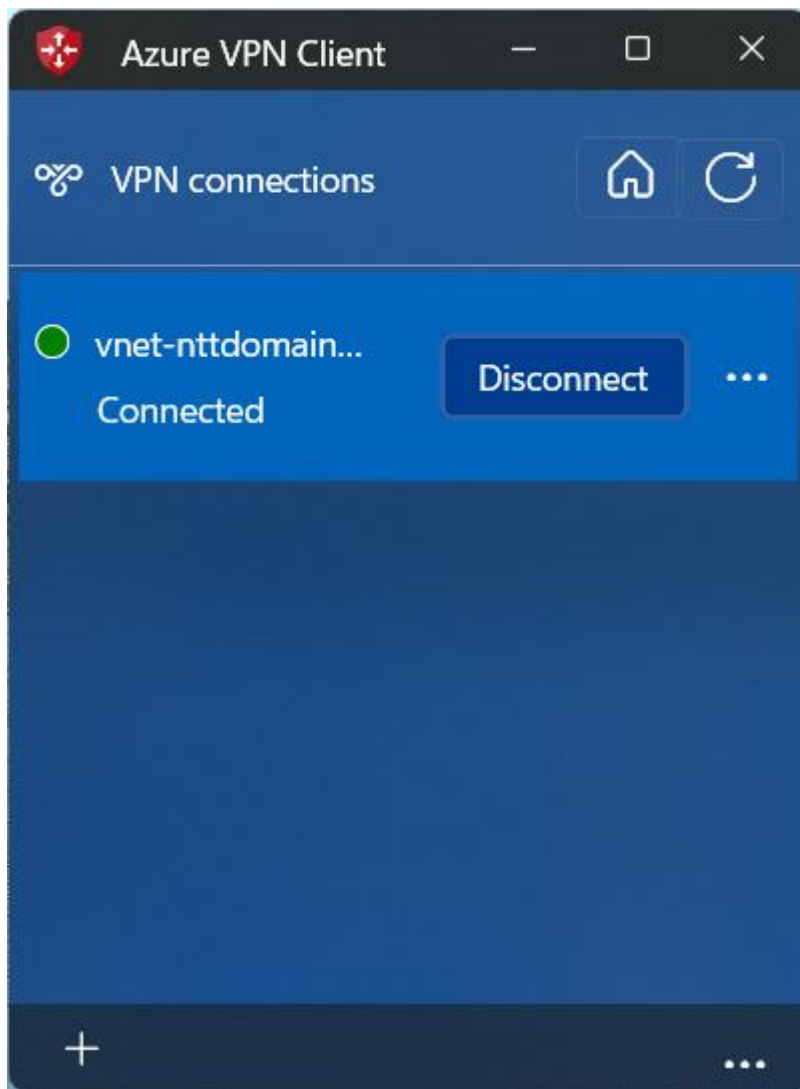
The screenshot shows the 'Azure VPN Client' configuration window. It has a dark theme and a title bar with a back arrow, the text 'Azure VPN Client', and standard window controls (minimize, maximize, close). The window contains the following elements:

- Connection Name**: A text input field with a red asterisk, containing the value 'vnet-nttdomain-dev01'.
- VPN Server**: A text input field with a red asterisk, containing the value 'azuregateway-a4570077-1b5'. To its right is an information icon (i in a circle).
- Server Validation**: A section header.
- Certificate Information**: A section header with a red asterisk.
- Certificate Selection**: A dropdown menu showing 'DigiCert Global Root G2' with a downward arrow. To its right is an information icon (i in a circle).
- Buttons**: At the bottom, there are two buttons: a blue 'Save' button and a grey 'Cancel' button.

- vi. Scroll down until client authentication. Authentication type (certificate) > Certificate Information (Choose the client certificate name that we've successfully import earlier) > Click Save



- vii. From your home network, please try to connect. It should be connected



- viii. Open command prompt and do ipconfig. You should see the adapter (Azure VPN) that we connected and the IP address should be within the address pool that we've assigned in point-to-site configuration (172.16.201.0/24):

```
PPP adapter vnet-nttdomain-dev01:

Connection-specific DNS Suffix  . : 
IPv4 Address. . . . .           : 172.16.201.2
Subnet Mask . . . . .           : 255.255.255.255
Default Gateway . . . . .       :
```

7. Create a new subnet "PrivateEndpointSubnet"

## Add a subnet



Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose <sup>①</sup> Default

Name \* <sup>①</sup> PrivateEndpointSubnet

### IPv4

Include an IPv4 address space ☒

IPv4 address range <sup>①</sup> 10.0.0.0/16

10.0.0.0 - 10.0.255.255

Starting address \* <sup>①</sup> 10.0.2.0

Size <sup>①</sup> /24 (256 addresses)

Subnet address range <sup>①</sup> 10.0.2.0 - 10.0.2.255

### IPv6

Include an IPv6 address space ☐ This virtual network has no IPv6 address ranges.

### Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Enable private subnet (no default outbound access) ☒

8. Create Azure Machine Learning resource group "rg-ntt-azuremachinelearning-dev01"

# Create a resource group ...

Basics

Tags

Review + create

[Automation Link](#)

## Basics

Subscription	Azure subscription 1
Resource group name	rg-ntt-azuremachinelearning-dev01
Region	East US

## Tags

None

9. Create Azure Machine Learning
  - a. Go inside resource group "rg-ntt-azuremachinelearning-dev01"
  - b. Click create new resources > search for azure machine learning > click create > click azure machine learning



🔍 azure machine learning ✕

Pricing :

☐ Azure benefit eligible only ⓘ ☐ Azure services only

🌟 **New!** Get AI-generated suggestions for 'azure machine learning'

Showing 1 to 20 of 1743 results for 'azure machine learning'. [Clear search](#)



## Azure Machine Learning

Microsoft

Azure Service

Enterprise-grade machine learning to build and deploy models faster

Create ▾



Azure Machine Learning



## VM Watira Machine Learning

Sahara Watira for Digital Transfo...

Virtual Machine

Machine learning with cyber security

Starts at  
**\$28.935/hour**

Create ▾



# Azure Machine Learning ...

Create a machine learning workspace

**Basics**   Inbound Access   Outbound Access   Encryption   Identity   Tags   Review + create

## Resource details

Every workspace must be assigned to an Azure subscription, which is where billing happens. You use resource groups like folders to organize and manage resources, including the workspace you're about to create.

[Learn more about Azure resource groups](#)

Subscription *	<div>Azure subscription 1</div>
Resource group *	<div>rg-ntt-azuremachinelearning-dev01</div>

[Create new](#)

## Workspace details

Configure your basic workspace settings like its storage connection, authentication, container, and more. [Learn more](#)

Name *	<div>azmlws-workspace-dev01</div>
Region *	<div>East US</div>
Storage account *	<div>(new) azmlwsstorageacctdev01</div>
Key vault *	<div>(new) azmlwskeyvaultdev01</div>
Application insights *	<div>(new) azmlwsappsinsightdev01</div>
Container registry	<div>(new) azmlwscontainerregistrydev01</div>

[Create new](#)

# Azure Machine Learning ...

Create a machine learning workspace

Basics Inbound Access Outbound Access Encryption Identity Tags Review + create

Public network access allows access to this resource through the internet using a public IP address. An application

Public network access \* ☒ Disabled  
☐ All networks

**i** All networks, including the internet, can access this resource.

## Workspace Inbound access

Name	Subscription
Click on add to create a private endpoint	
<a href="#">+</a> Add	

(Outbound Access) If choosing Allow Internet Outbound then no need for user defined outbound rule (we can create later if needed)

# Azure Machine Learning ...

Create a machine learning workspace

Basics   Inbound Access   **Outbound Access**   Encryption   Identity   Tags   Review + create

## Network isolation

Choose the type of network isolation you need for your workspace, from not isolated at all to an entirely separate virtual network managed by Azure Machine Learning. [Learn more about managed network isolation](#)

☐ **Public**

- Compute can access public resources
- Outbound data movement is unrestricted

☒ **Allow Internet Outbound**

- Compute can access private resources
- Outbound data movement is unrestricted

☐ **Allow Only Approved Outbound**

- Compute can access allowlisted resources only
- Outbound data movement is restricted to approved targets

## Workspace Outbound access

☐ Provision managed virtual network ⓘ

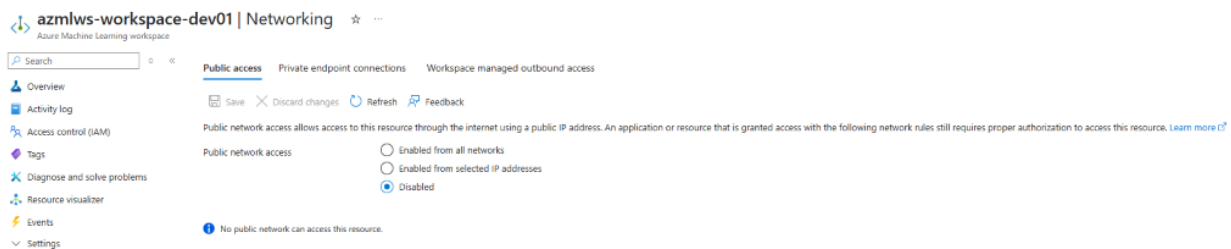
+ Add user-defined outbound rules

Connection Name	Status	Destination Type
> Required outbound rules		

c. Click review + create

## 10. Create private endpoint for workspace

- Go to resource group "rg-ntt-azuremachinelearning-dev01" > open azure machine learning workspace "azmlws-workspace-dev01" > Settings > networking
- Public access tabs > Disable public access



c. Private endpoints connections > click + Private endpoint

# Create a private endpoint ...

- 1 Basics
- 2 Resource
- 3 Virtual Network
- 4 DNS
- 5 Tags
- 6 Review + create

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 \* ⓘ

Azure subscription 1

Resource group \* ⓘ

rg-ntt-azuremachinelearning-dev01

Create new

## Instance details

Name \*

azmlws-workspace-pe-dev01

Network Interface Name \*

azmlws-workspace-pe-dev01-nic

Region \*

East US

# Create a private endpoint ...

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

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](#)

Subscription

Azure subscription 1 (89fd8d45-9f83-4f18-af2f-d99dac4acf15)

Resource type

Microsoft.MachineLearningServices/workspaces

Resource

azmlws-workspace-dev01


Target sub-resource \* ⓘ

amlworkspace

## Create a private endpoint ...

✓ Basics   ✓ Resource   **3 Virtual Network**   ④ DNS   ⑤ Tags   ⑥ Review + create

### Networking

To deploy the private endpoint, select a virtual network subnet. [Learn more](#) 

Virtual network ⓘ

Subnet \* ⓘ


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](#) 

[+](#) Create

Application security group

Please take note the private DNS zone for later testing:

Private DNS zone

privatelink.api.azureml.ms

privatelink.notebooks.azure.net

# 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-api-azureml-ms	Azure subscription 1	rg-ntt-azuremachinel...	(new) privatelink.api.azur...
privatelink-notebooks-az...	Azure subscription 1	rg-ntt-azuremachinel...	(new) privatelink.noteboo...

d. Click review + create

## 11. Create private endpoint for storage

- a. Go to resource group > rg-ntt-azuremachinelearning-dev01 > click storage account azmlwsstorageacctdev01 > Security + networking > networking
- b. Disable public access

Home > Resource Manager | Resource groups > rg-ntt-azuremachinelearning-dev01 > azmlwsstorageacctdev01 | Networking >

## Public network access ...

Configure what inbound access is enabled through this resource's public endpoint. [Learn more](#)

Public network access \* ⓘ

☐ Enable  
Allow inbound and outbound access with the option to restrict select inbound access resource access configurations for this resource.

☒ Disable  
Restrict inbound access while allowing outbound access.

☐ Secured by perimeter (Most restricted)  
Restrict inbound and outbound access using a network security perimeter. Secure by perimeter offers the greatest level of inbound and outbound restriction to secure your resource.

▲ Disabling public network access will make this resource not available publicly. [Learn more](#)

Public network access scope \* ⓘ

☐ Enable from all networks

☐ Enable from selected networks

# Create a private endpoint ...

- 1 Basics
- 2 Resource
- 3 Virtual Network
- 4 DNS
- 5 Tags
- 6 Review + create

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 \* ⓘ

Azure subscription 1

Resource group \* ⓘ

rg-ntt-azuremachinelearning-dev01

Create new

## Instance details

Name \*

azmlws-storage-pe-dev01

Network Interface Name \*

azmlws-storage-pe-dev01-nic

Region \*

East US

Repeat the same step for target sub-resource that we need based on business requirement



# Create a private endpoint ...

✓ Basics   **2 Resource**   ③ Virtual Network   ④ DNS   ⑤ Tags   ⑥ Review + create

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](#)

Subscription      Azure subscription 1 (89fd8d45-9f83-4f18-af2f-d99dac4acf15)

Resource type      Microsoft.Storage/storageAccounts

Resource      azmlwsstorageacctdev01

Target sub-resource \* ⓘ

blob

blob

table

queue

file

web

dfs

## Create a private endpoint ...

✓ Basics   ✓ Resource   **3 Virtual Network**   ④ DNS   ⑤ Tags   ⑥ Review + create

### Networking

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network ⓘ	vnet-nttdomain-dev01 (rg-ntt-network-dev01) ▼
Subnet * ⓘ	PrivateEndpointSubnet ▼
Network policy for private endpoints	Disabled <a href="#">(edit)</a>

### 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](#)

[+](#) Create

Application security group

▼

Please take note on the private DNS zone for testing later (example blob)

privatelink.blob.core.windows.net

## Create a private endpoint ...

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

### Private DNS integration

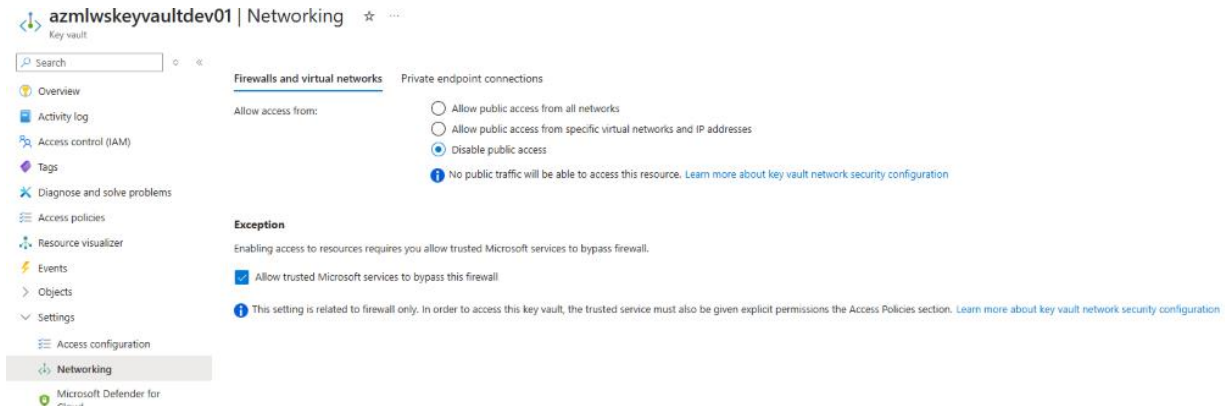
To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. [Learn more](#)

Integrate with private DNS zone   ☒ Yes   ☐ No

Configuration name	Subscription	Resource group	Private DNS zone
privatelink-blob-core-win...	Azure subscription 1 ▼	rg-ntt-azuremachinel... ▼	(new) privatelink.blob.cor...

## 12. Create private endpoint for keyvault

- Go to resource group > rg-ntt-azuremachinelearning-dev01 > click keyvault azmlwskeyvaultdev01 > Settings > Networking
- Firewalls and virtual networks = disable public access



- Private endpoints connection > create

## Create a private endpoint

- Basics
- Resource
- Virtual Network
- DNS
- Tags
- Review + create

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 *	Azure subscription 1
Resource group *	rg-ntt-azuremachinelearning-dev01

[Create new](#)

### Instance details

Name *	azmlws-keyvault-pe-dev01
Network Interface Name *	azmlws-keyvault-pe-dev01-nic
Region *	East US

## Create a private endpoint ...

✓ Basics **2 Resource** ③ Virtual Network ④ DNS ⑤ Tags ⑥ Review + create

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 ①

☒ Connect to an Azure resource in my directory.  
☐ Connect to an Azure resource by resource ID or alias.

Subscription \* ①

Resource type \* ①

Resource \* ①

Target sub-resource \* ①

## Create a private endpoint ...

✓ Basics ✓ Resource **3 Virtual Network** ④ DNS ⑤ Tags ⑥ Review + create

### Networking

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network ①

Subnet \* ①

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](#)

+ Create

Application security group


Please take note on the private DNS zone for testing later

privatelink.vaultcore.azure.net



## 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-vaultcore-azur...	Azure subscription 1 	rg-ntt-azuremachinel... 	(new) privatelink.vaultcor...

### 13. Create private endpoints for container registry

- Go to resource group > rg-ntt-azuremachinelearning-dev01 > azmlwscontainerregistrydev01 > Settings > Networking
- Public access = Disabled

Search 🔍 ◊ <<

- Overview
- Activity log
- Access control (IAM)
- Tags
- Quick start
- Resource visualizer
- Events
- Settings
  - Access keys
  - Encryption
  - Identity
  - Networking**

**Public access** Private access

Save ✕ Discard ↺ Refresh

Public network access:

- ☐ All networks  
☐ Selected networks  
☒ Disabled

#### Firewall exception

☒ Allow trusted Microsoft services to access this container registry ⓘ

c. Private access = create a private endpoints

## Create a private endpoint ...

**1 Basics** (2) Resource (3) Virtual Network (4) DNS (5) Tags (6) Review + create

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 \* ⓘ Azure subscription 1 ▼  
Resource group \* ⓘ rg-ntt-azuremachinelearning-dev01 ▼  
[Create new](#)

#### Instance details

Name \* azmlws-containerregistry-pe-dev01 ✓  
Network Interface Name \* azmlws-containerregistry-pe-dev01-nic ✓  
Region \* East US ▼

# Create a private endpoint ...

- ✓ Basics
- 2 Resource**
- 3 Virtual Network
- 4 DNS
- 5 Tags
- 6 Review + create

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](#)

Subscription	Azure subscription 1 (89fd8d45-9f83-4f18-af2f-d99dac4acf15)
Resource type	Microsoft.ContainerRegistry/registries
Resource	azmlwscontainerregistrydev01
Target sub-resource * ⓘ	<div>registry</div>

# Create a private endpoint ...

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

## Networking

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network ⓘ	<div>vnet-nttdomain-dev01 (rg-ntt-network-dev01)</div>
Subnet * ⓘ	<div>PrivateEndpointSubnet</div>
Network policy for private endpoints	Disabled <a href="#">(edit)</a>

## 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](#)

[+ Create](#)

Application security group

Please take note on the private DNS zone for testing later

privatelink.azurecr.io

## 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-azurecr-io	Azure subscription 1	rg-ntt-azuremachinel...	(new) privatelink.azurecr.io

## 14. Create private endpoints for application insight

- Go to resource group > rg-ntt-azuremachinelearning-dev01 > azmlwsappsinsightdev01 > Configure > Network Isolation
- Public access = disabled

Home > Resource Manager | Resource groups > rg-ntt-azuremachinelearning-dev01 > azmlwsappsinsightdev01

azmlwsappsinsightdev01 | Network Isolation

Public access Private access

Allow access to this resource through the internet using a public IP address or by using a network security perimeter to manage inbound and outbound access rules centrally. [Learn More](#)

Network security perimeter is not available on Application Insights resources. Please use the associated workspace to configure network security perimeter access. [Click here to go to workspace](#)

Ingestion access ☐ Enabled from all networks ☒ Restricted public inbound, enabled public outbound

Query access ☐ Enabled from all networks ☒ Restricted public inbound, enabled public outbound

Save Cancel

- Private access = create private endpoints

Home > Resource Manager | Resource groups > rg-ntt-azuremachinelearning-dev01 > azmlwsappsinsightdev01

azmlwsappsinsightdev01 | Network Isolation

Public access Private access

+ Add Refresh Remove

This resource can be accessed over a Private Link using the Azure Monitor Private Link Scopes (AMPLS) it is added to. To add this resource after adding Private Link scopes, you may also choose to block access from public networks that don't connect through a Private Link. If you choose to block access from public networks, only networks connected to the listed Private Link scopes will be able to reach this resource.

Azure Monitor Private Link Scopes

Filter by name:

Name

No results

Select a scope

Browse Recent

Scope	Resource type	Location
AzureMonitor-AzMWWorkspaceDev02	Azure Monitor Private Link Sco...	Global



15. Create a compute cluster for container registry, else you will see this error

*Container registry Code: ImageBuildComputeNotValid Message: If Container Registry is behind the virtual network, Container Registry cannot build your image. Set the imageBuildCompute property to build your image. See <https://docs.microsoft.com/azure/machine-learning/how-to-secure-workspace-vnet#enable-azure-container-registry-acr>*

- a. AzureML uses the compute cluster to build the docker image. So we need to create a compute cluster (Reference: <https://learn.microsoft.com/en-us/azure/machine-learning/how-to-secure-workspace-vnet?view=azureml-api-2&tabs=required%2Cpe%2Ccli#enable-azure-container-registry-acr>)
- b. Open cloud shell on your azure portal > Verify the aml compute cluster (use this command): **az ml compute list -g rg-ntt-azuremachinelearning-dev01 -w azmlws-workspace-dev01 --query "[{name:name,type:type}]"**

```
PS /home/ntt> az ml compute list -g rg-ntt-azuremachinelearning-dev01 -w azmlws-workspace-dev01 --query "[{name:name,type:type}]"
[]
PS /home/ntt>
```

- c. If see blank array meaning that n aml compute cluster, we have to create it. Use this command to verify the container registry = **az ml workspace show -n azmlws-workspace-dev01 -g rg-ntt-azuremachinelearning-dev01 --query 'container\_registry'**

```
Switch to Bash Restart Manage files New session Editor Web preview Settings Help
PS /home/ntt> az ml workspace show -n azmlws-workspace-dev01 -g rg-ntt-azuremachinelearning-dev01 --query 'container_registry'
"/subscriptions/89f8845-9f83-4f18-af2f-d9dac4acf15/resourceGroups/rg-ntt-azuremachinelearning-dev01/providers/Microsoft.ContainerRegistry/registries/azmlwscontainerregistrydev01"
PS /home/ntt>
```

- d. Set up an image-build AML compute, create an Azure Machine Learning AML compute cluster in the same VNet as your workspace-dependent resources. This cluster can then be set as the default image-build compute and will be used to build every image in your workspace from that point onwards:
  - i. **PS /home/ntt> az ml compute create -n azmlwsomputeclusterdev01 -g rg-ntt-azuremachinelearning-dev01 -w azmlws-workspace-dev01 --type AmlCompute --size Standard\_DS3\_v2 --min-instances 0 --max-instances 1**

```

PS /home/ntt> az ml compute delete -n azmlwscomputeclusterdev01 -g rg-ntt-azuremachinelearning-dev01 -w azmlws-workspace-dev01 --yes
PS /home/ntt> az ml compute create -n azmlwscomputeclusterdev01 -g rg-ntt-azuremachinelearning-dev01 -w azmlws-workspace-dev01 --type AmlCompute --size Standard_DS3_v2 --min-instances 0 --max-instances 1
{
  "enable_node_public_ip": true,
  "id": "/subscriptions/89fd8d45-9f83-4f18-af2f-d99dac4acf15/resourceGroups/rg-ntt-azuremachinelearning-dev01/providers/Microsoft.MachineLearningServices/workspaces/azmlws-workspace-dev01/computes/azmlwscomputeclusterdev01",
  "idle_time_before_scale_down": 120,
  "location": "eastus",
  "max_instances": 1,
  "min_instances": 0,
  "name": "azmlwscomputeclusterdev01",
  "network_settings": {},
  "provisioning_state": "Succeeded",
  "resourceGroup": "rg-ntt-azuremachinelearning-dev01",
  "size": "Standard_DS3_v2",
  "ssh_public_access_enabled": true,
  "tier": "dedicated",
  "type": "amlcompute"
}
PS /home/ntt>

```

- ii. Final verify the aml compute cluster (use this command): **az ml compute list -g rg-ntt-azuremachinelearning-dev01 -w azmlws-workspace-dev01 --query "[].{name:name,type:type}"**

```

PS /home/ntt> az ml compute list -g rg-ntt-azuremachinelearning-dev01 -w azmlws-workspace-dev01 --query "[].{name:name,type:type}"
[
  {
    "name": "azmlwscomputeclusterdev01",
    "type": "amlcompute"
  }
]
PS /home/ntt>

```

## 16. Create private DNS resolver

- a. Search for DNS Private Resolver > Create. During creation you will create another 2 subnet for DnsResolver subnet inbound and outbound. Make sure to create under the same VNet else you need to make connection between VNet-to-VNet

# Create a DNS private resolver ...

- Basics
- Inbound Endpoints
- Outbound Endpoints
- Ruleset
- Tags
- Review + Create

## Instance details

Private resolver is a regional service. Only virtual networks and rulesets in the same region can use this private resolver.

Name \*

ntt-network-dnsprivateresolver-dev01

Region \*

(US) East US

**i** DNS private resolver and virtual network must exist in the same location, so the region selected here will affect the available virtual networks for selection.

## Virtual Network

Select a virtual network for your private resolver and endpoints. [Learn more](#)

Virtual Network \* **i**

vnet-nttdomain-dev01 (rg-ntt-network-dev01)

[Home](#) > [DNS private resolvers](#) >

## Create a DNS private resolver ...

- Basics
- Inbound Endpoints
- Outbound Endpoints
- Ruleset
- Tags
- Review + Create

Inbound endpoints can receive domain name resolution requests. [Learn more](#)

+ Add an endpoint

Endpoint name	Subnet

## Add an inbound endpoint

Inbound endpoints can receive domain name resolution requests. [Learn more](#)

Endpoint name \*

ntt-network-dnsprivateresolver-inbound-dev01

Subnet \* **i**

DnsResolverSubnet (10.0.1.0/27)

Create new

IP address assignment \*

☒ Dynamic

☐ Static

[Home](#) > [DNS private resolvers](#) >

## Create a DNS private resolver ...

- Basics
- Inbound Endpoints
- Outbound Endpoints
- Ruleset
- Tags
- Review + Create

Outbound endpoints can forward domain name resolution requests to the DNS servers specified in rulesets. To complete your configuration, create rulesets later that point to this endpoint. [Learn more](#)

+ Add an endpoint

Endpoint name	Subnet

## Add an outbound endpoint

Outbound endpoints can forward domain name resolution (DNS) requests. Create a ruleset to specify DNS servers and select this endpoint to use it for DNS forwarding. [Learn more](#)

Endpoint name \*

ntt-network-dnsprivateresolver-outbound-dev01

Subnet \* **i**

DnsPrivateResolverOutbound (10.0.0.0/28) [...]

Create new

**i** To complete your configuration, create rulesets later that point to these endpoints. [Learn more](#)

<input type="checkbox"/>	DnsResolverSubnet	10.0.1.0/27	-	26	Microsoft....	-	-		
<input type="checkbox"/>	DnsPrivateResolverOutbound	10.0.0.0/28	-	11	Microsoft....	-	-		

- b. Click review + create. Later step we do DNS forwarding ruleset. To do that you need to make sure you already have DNS Server VM / On-Premises / Microsoft Entra Domain Services

## 17. Testing accessing azure machine learning

- a. Go to <https://ml.azure.com/>
- b. Login > click workspace > you should see the workspace name that we've create BUT it should show as private
- c. Click to open the workspace azmlws-workspace-dev01

Microsoft Foundry | Azure Machine Learning

Search All workspaces

Default Directory > Workspaces

### Workspaces

A workspace provides a centralized place to keep track of all the artifacts you create while performing machine learning experiments.

[+ New](#) [Refresh](#) [Edit workspace](#) [Reset view](#)

Search Filter Columns

Name ↑	Resource group	Region	Subscription	Created on
azmlws-workspace-dev01	Private rg-nitt-azurermachinelearning-dev01	eastus	Azure subscription 1	Nov 27, 2025 9:04 PM

- d. (Assume you are in public network) when you open the workspace you should see error that you are not allow to access private resources from public network – meaning that the test was success.




### Error loading workspace

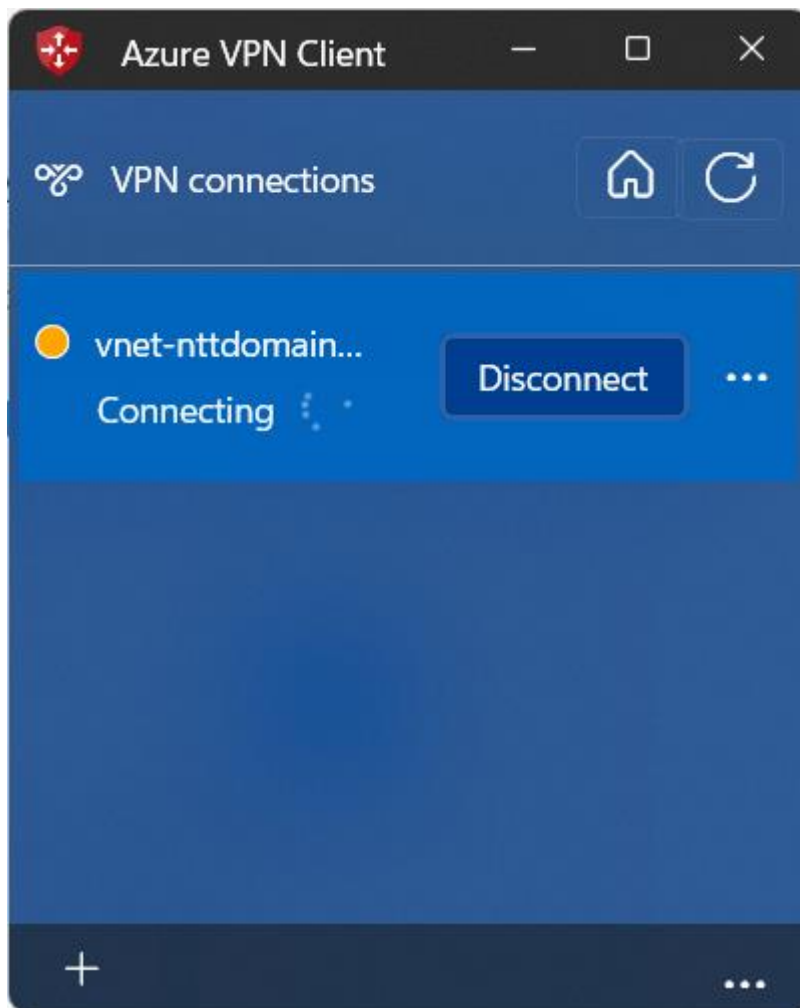
You are attempting to access a restricted resource from an unauthorized network location. Please contact your administrator or follow the troubleshooting instructions [here](#).

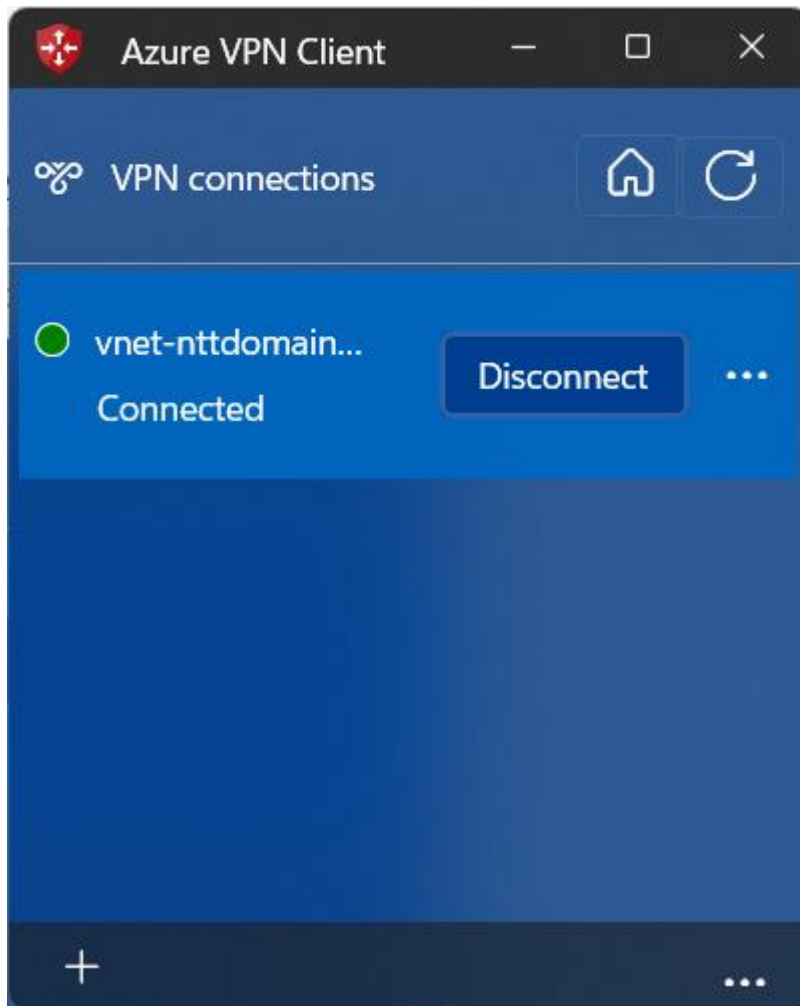
[← Back to all workspaces](#)

### Workspace Diagnostics

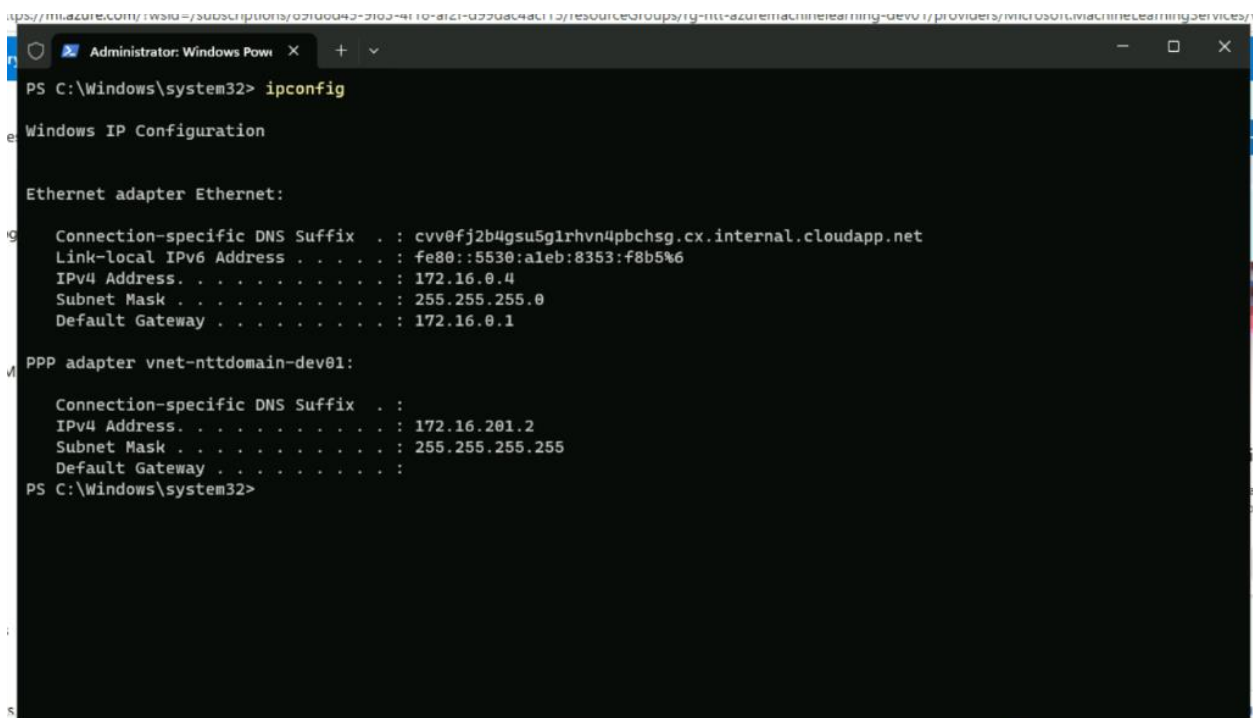
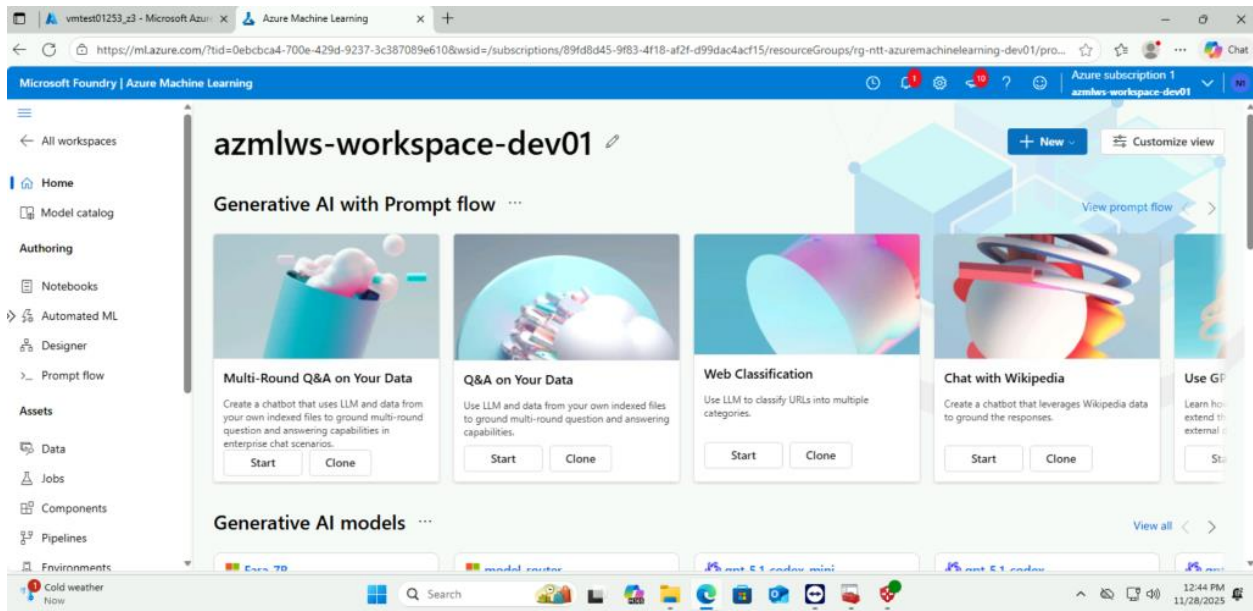
Hold on while we run workspace diagnostics 

- e. To make it work we need to connect to azure VPN that we've configured (Azure VPN Gateways + P2S). The outcome we should be able to open the private workspace



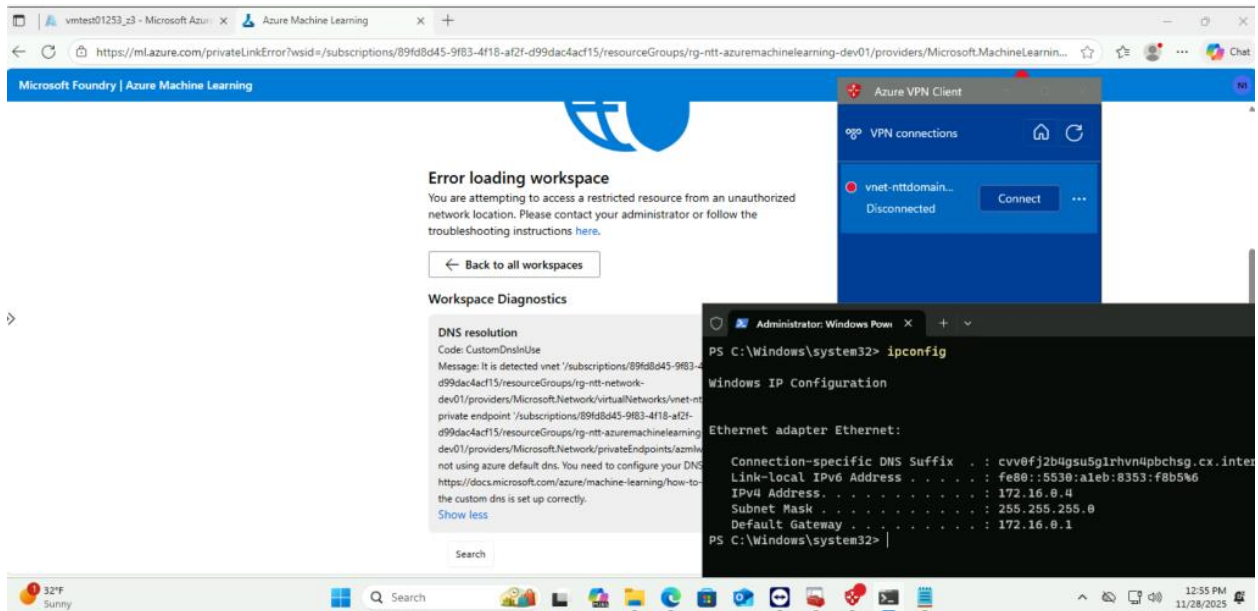


- f. Open <https://ml.azure.com>
- g. Open the private workspace (NOTES: You may facing access issue maybe local or domain firewall, DNS private resolver issue, DNS forwarding ruleset issue, NSG issue)

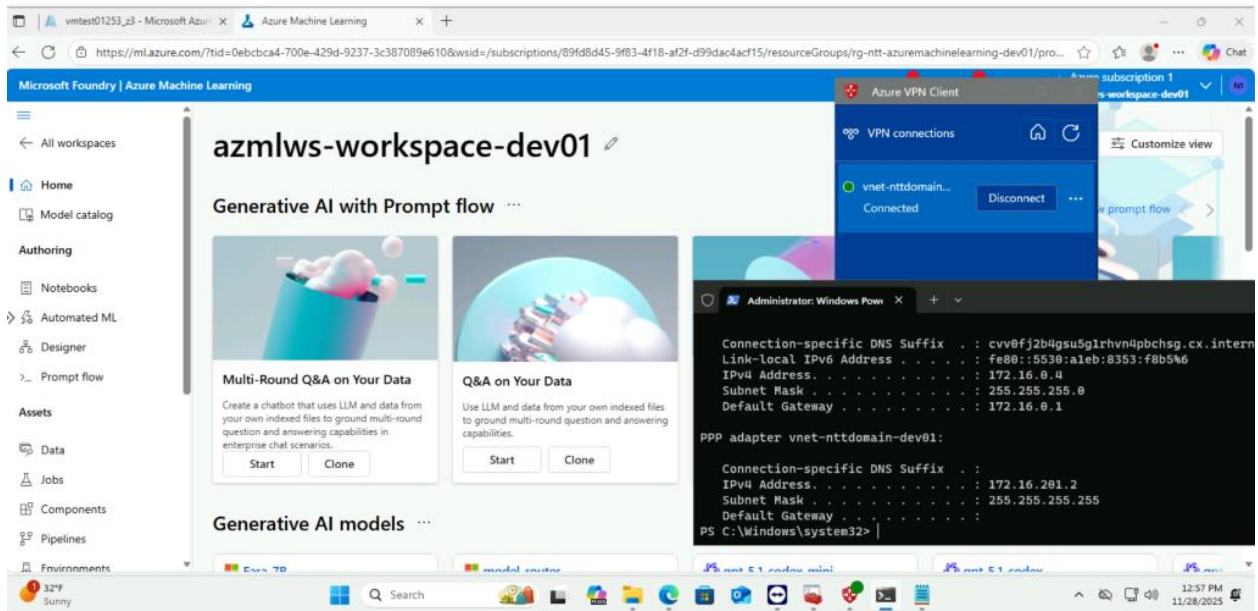


If not connect to VPN – So it is expected that we cannot access to our Azure Machine Learning Workspace:

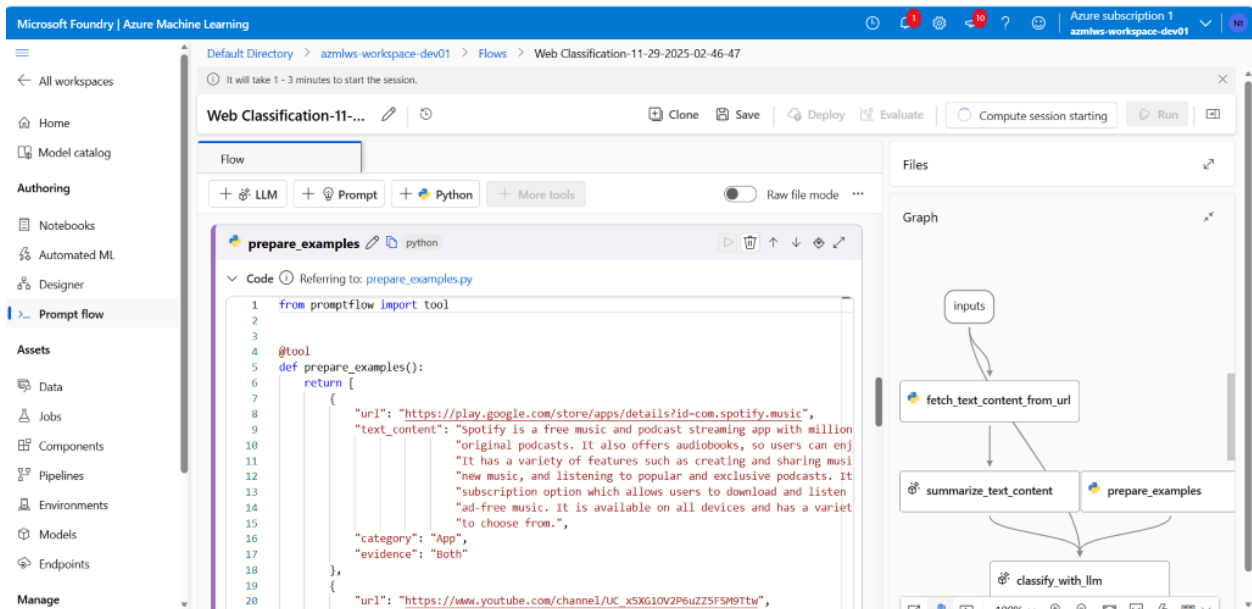
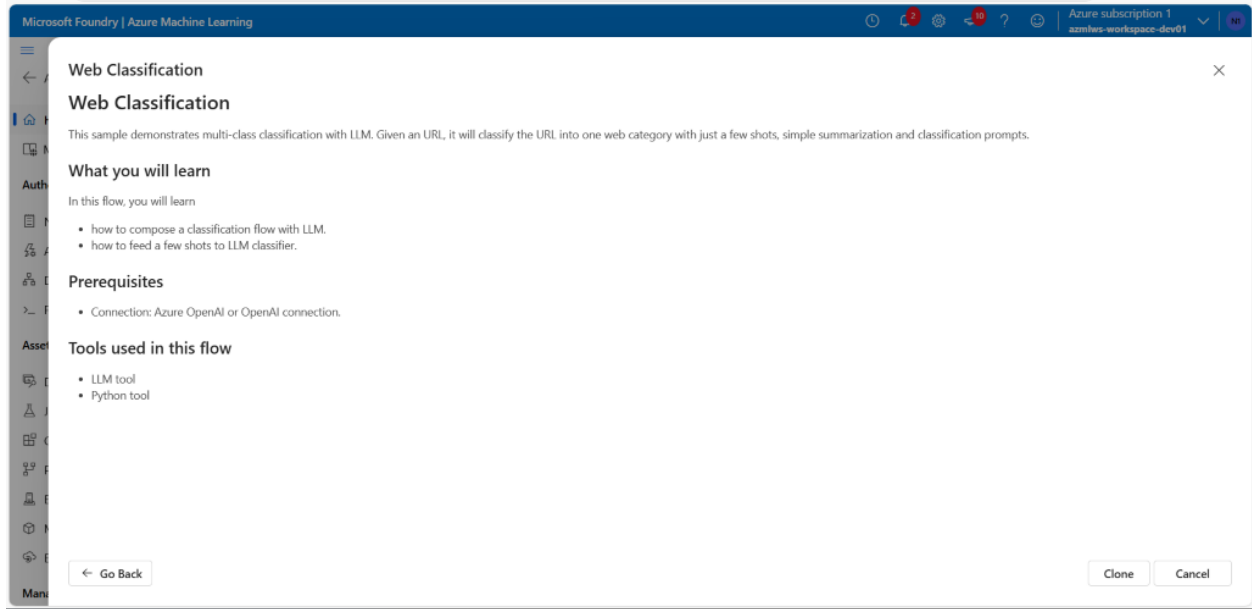




If connect to VPN – It is expected that we should be able to connect to VPN:



Testing azure machine learning workspace by running web classification project:



Microsoft Foundry | Azure Machine Learning

Default Directory > azmlws-workspace-dev01 > Notebooks

All workspaces

Home

Model catalog

Authoring

Notebooks

Automated ML

Designer

Prompt flow

Assets

Data

Jobs

Components

Pipelines

Environments

Models

Endpoints

Manage

Notebooks

Files

Samples

Users

nttraining1

promptflow

Web Classification-11-28-20

Web Classification-11-29-20

Notebooks is your space to add, browse, and edit files.

You can add files of any type, including Jupyter Notebooks (.ipynb). The files you see here are stored in the workspace file share, and are accessible and shared within the workspace.

In order to run notebooks and scripts, you must connect to an Azure Machine Learning compute resource. Once a notebook or terminal is connected, you can access all workspace assets including experiment details, data, models, and more. [Learn more](#)

+ Files

Create compute

[View Azure Machine Learning tutorials](#)

Microsoft Foundry | Azure Machine Learning

Default Directory > azmlws-workspace-dev01 > Environments

Notebooks

Automated ML

Designer

Prompt flow

Assets

Data

Jobs

Components

Pipelines

Environments

Models

Endpoints

Manage

Compute

Monitoring

Data Labeling

Linked Services

Connections

Environments

Curated environments

Custom environments

Curated environments are predefined environments that offer good starting points for building your own environments. Curated environments are backed by cached Docker images, providing a reduced run preparation cost. [Learn more about curated environments](#)

Refresh

Reset view

Search

Filter

Columns

Name	Source	Version	Created	Tags	Description
model-management61	azureml	61	Nov 25, 2025 10:51 PM	Preview	Environment
sklearn-1.5.35	azureml	35	Nov 25, 2025 9:55 PM	OpenMpi : 4.1.0 OS : Ubuntu20.04 Preview Python : 3.10	An environn
lightgbm-3.3.70	azureml	70	Nov 25, 2025 9:54 PM	LightGBM : 4.6 OpenMpi : 5.0 OS : Ubuntu24.04 Preview	An environn
component68	azureml	68	Nov 25, 2025 8:20 PM	OS : Ubuntu22.04 Python : 3.9	An environn
python-sdk-v240	azureml	40	Nov 25, 2025 8:08 PM	Preview	Environment
mlflow-model-inference15	azureml	15	Nov 25, 2025 8:07 PM	Inference OS : Ubuntu22.04 Preview	AzureML ML

25/Page

Microsoft Foundry | Azure Machine Learning

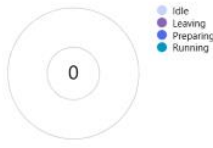
Default Directory > azmlws-workspace-dev01 > azmlwscomputeclusterdev01 > Compute

### azmlwscomputeclusterdev01

Details Nodes Jobs Monitoring (preview)

Refresh Delete Diagnose

#### Cluster node status



#### Cluster state

**Allocation state**  
Succeeded (0 nodes)

**Allocation state transition time**  
28/11/2025, 12:02:34 am

**Created on**  
27/11/2025, 11:54:53 pm

**Current node count**  
0

#### Attributes

**Compute name**  
azmlwscomputeclusterdev01

**Resource ID**  
--

**Compute type**  
Machine Learning compute

#### Resource properties

**Virtual machine size**  
Standard\_DS3\_v2 (4 cores, 14 GB RAM, 28 GB disk)

**Processing unit**  
[CPU - General purpose](#)

**Estimated cost**  
--

Microsoft Foundry | Azure Machine Learning

Default Directory > azmlws-workspace-dev01

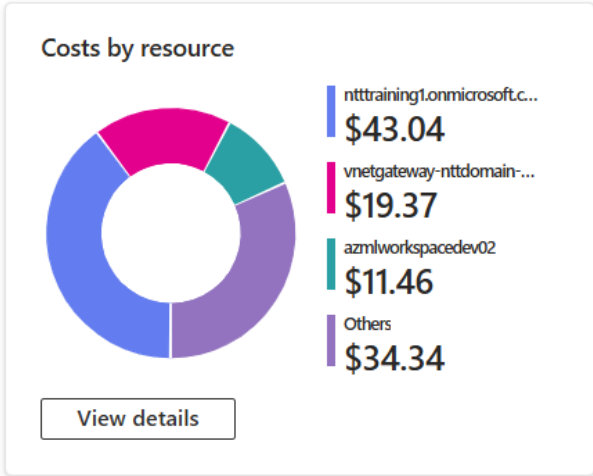
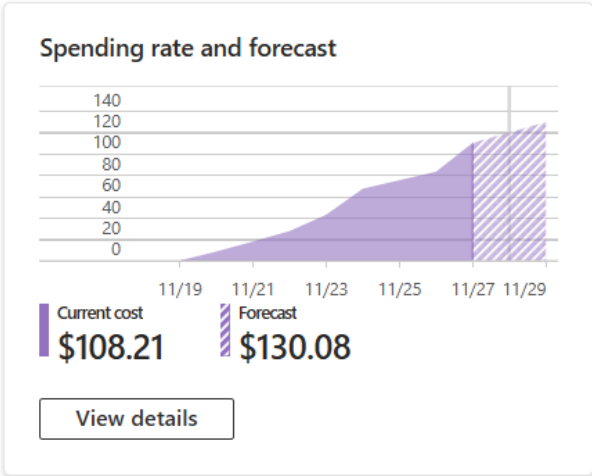
### Connections

+ Connect Refresh Delete Edit Reset view

Search Filter Columns

Name	Authentication type	Added by	☆	Type
azureml_globaldatasets	SAS	779301c0-18b2-4cdc-8...		Azure Blob Storage
workspaceartifactstore	Account key	System		Azure Blob Storage
workspaceblobstore	Account key	System		Azure Blob Storage

Finally I spend USD108.21 to complete this project



The best part is my secure score is 100%