

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

X

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 ⓘ

Default

Name * ⓘ

EntraDomainServicesSubnet

IPv4

Include an IPv4 address space



IPv4 address range ⓘ

10.0.0.0/16



10.0.0.0 - 10.0.255.255

Starting address * ⓘ

10.0.4.0

Size ⓘ

/24 (256 addresses)



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-nttentrardomainservices-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-nttentradomainservices-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-nttentradomainservices-dev01

Help me choose the subscription and resource group

DNS domain name * ⓘ	nttentradomain.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-ntdomain-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](#) X

⌄ Help me choose the subnet and NSG

ℹ 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:

[Add another email to be contacted at](#)

▽ 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

Help me choose strong ciphers

NTLM password synchronization

Password synchronization from on-premises

Help me choose password synchronization settings

Kerberos RC4 encryption

Kerberos armoring

Help me choose kerberos RC4 encryption and armoring

LDAP signing

LDAP channel binding

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-nttentradomainservices-dev01" > open Microsoft Entra Domain Services "nttentradomain.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

nttentrardomain.onmicrosoft.com | Properties

Microsoft Entra Domain Services

Search ◇ ◀ ↴

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

DNS domain name
nttentrardomain.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

Search ◇ ◀ ↴

- 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 (Change)
Custom DNS servers	10.0.4.4 10.0.4.5

DNS private resolver

Home > Resource Manager | Resource groups > rg-nttentrardomservices-dev01 > nttentrardomain.onmicrosoft.com

nttentrardomain.onmicrosoft.com | Configuration diagnostics

Microsoft Entra Domain Services

Search ◇ ◀ ↴ 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 East US/vnet-nttdomain-dev01

[Fix](#)

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.PSPPath

    if(($Specific_ExistingCertificateList.Subject -eq "CN=$($PreDefinedCertFileName_String)P2SVPNClient") -or ($Specific_ExistingCertificateList.Subject -eq "CN=$($PreDefinedCertFileName_String)P2SRootCert")){
        $true
        Remove-Item -Path $Specific_ExistingCertificateList.PSPPath -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 $CertificatePath
15 #foreach ($SpecificExistingCertificate in $ExistingCertificateList){$_.Delete()}

PS C:\Temp\vnetgateway-nttdomain-dev01-CertDirectory> C:\Users\ABRFA\OneDrive - VAT\Documents\NurFaiz_M_Work\Project\DeCap\RootClientCertGenerate_AzGateway
Detected Existing Certificate (RELATED TO THIS CERT NAME ONLY):
CN=vnetgateway-nttdomain-dev01-P2SVPNClient
Microsoft.PowerShell.Security\Certificate::CurrentUser\My\9AAIFDC95251891DD530AF1F60E5E7FE264E871B
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

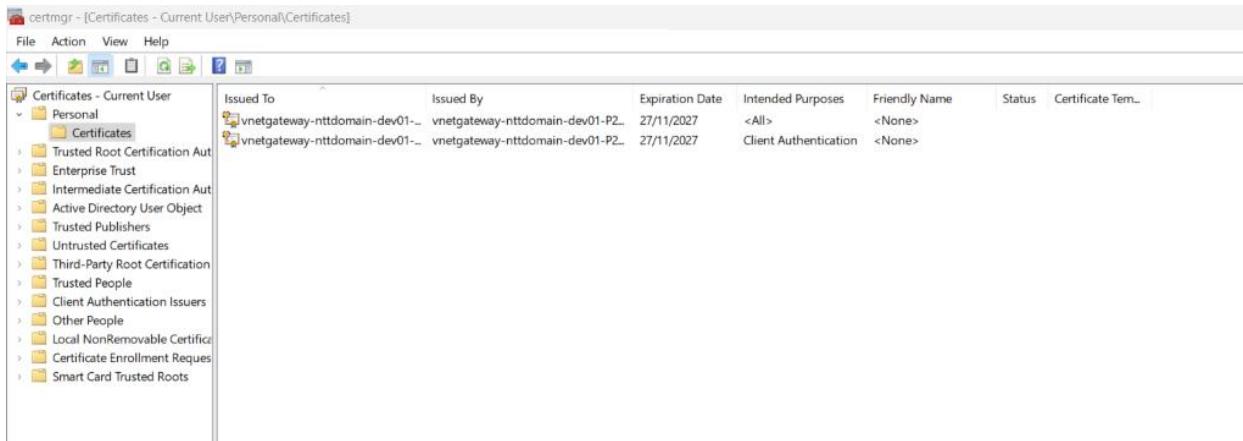
Mode                LastWriteTime         Length Name
----                <-----              ----- 
d----      27/11/2025   2:54 PM          vnetgateway-nttdomain-dev01-CertDirectory

    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-P2SVPNClient.pfx
-a---      27/11/2025   2:54 PM          913 vnetgateway-nttdomain-dev01-P2SVPNClient.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

- Reference = <https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-certificate-gateway>
- 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
MTAwLgYDVQQDDCd2bmV0Z2F0ZXdheS1udHRkb21haW4tZGV2MDEtUDJTUm9vdEN1
cnQwHhcNmjUxMTI3MDY0NDMyWhcNMjcxMTI3MDY1NDMzWjAyMTAwLgYDVQQDDCd2
bmV0Z2F0ZXdheS1udHRkb21haW4tZGV2MDEtUDJTUm9vdEN1cnQwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDQy1S7RBF0Js7EhKtF/MimpB51mwPqwviD
/+X2dVpUpRxhXQ2tPGwVed91kJbrQuwy8J9ZLUx+aNnH3GUwnV8Z9GdhC+r/scOb
OdFaKcmie33WQcUCeIo0RVKHqw/0+GCHY6w/ct7ua6QiPX208AoktoEb6jG4y2wQ
g7YV3UJkASj57EKMMtdvXzuQRaRpgTsyYKVad10Jb9INpgH0kbCGzwKwxrWdEIhd
IDrreku7xya23EWQ8hPhBXDJoIL1cmSZU53uIIvGB1kaKrqY124Xszu1MSnMr3EQ
W9qnuYa+HNM/9o0KJKzUVvFzS1jK5IzKo0+bVehqdpfKXNxmtABAgMBAAGjMTAv
MA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUpozAQp6fH+B665dT9bzAuH7s60Aw
DQYJKoZIhvcNAQELBQADggEBABAQlWgi+IAgiXkNBByrnW394+Go0tZvFaG09KHS0
UjQPdtrPu9cVo2Bm+7KFcV/jijo8dB1cPra9fu6IUi9RrR5QMbwYqzfcZdwbg43/
vaY3uFQrcxgzYnfUH+YhHFKSMYnwzQCG209kEwg4St6EydqrGr6ZqxiBDEpPR6kx
jh83v5abaDCvar1ZmdBRHB+rhs8rBk6bEFkIZslturvyMyDzLz5mBBZmGVE1K4T6
jI4fnm8V7/SB1XI4y1dN1tCIqKxr74BpEeMJooQF1t0OUjpiSXFP8YE6efxhpRtT
yRsCmtwXoB8zikDC0900G0DpBP0ReNm2idCoGKjcgJJUkpA=
-----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

Address pool * 172.16.201.0/24

Tunnel type OpenVPN (SSL)

Authentication type Azure certificate

Root certificates

Name	Public certificate data
vnetgateway-nttdomain-dev01-P2SRootCert	MIIDHzCCA... (with a green checkmark)

Revoked certificates

Name	Thumbprint

Additional routes to advertise

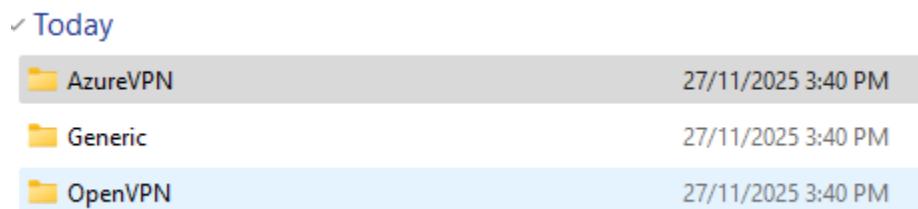
vnetgateway-nttdomain-dev01 | Point-to-site configuration

Virtual network gateway

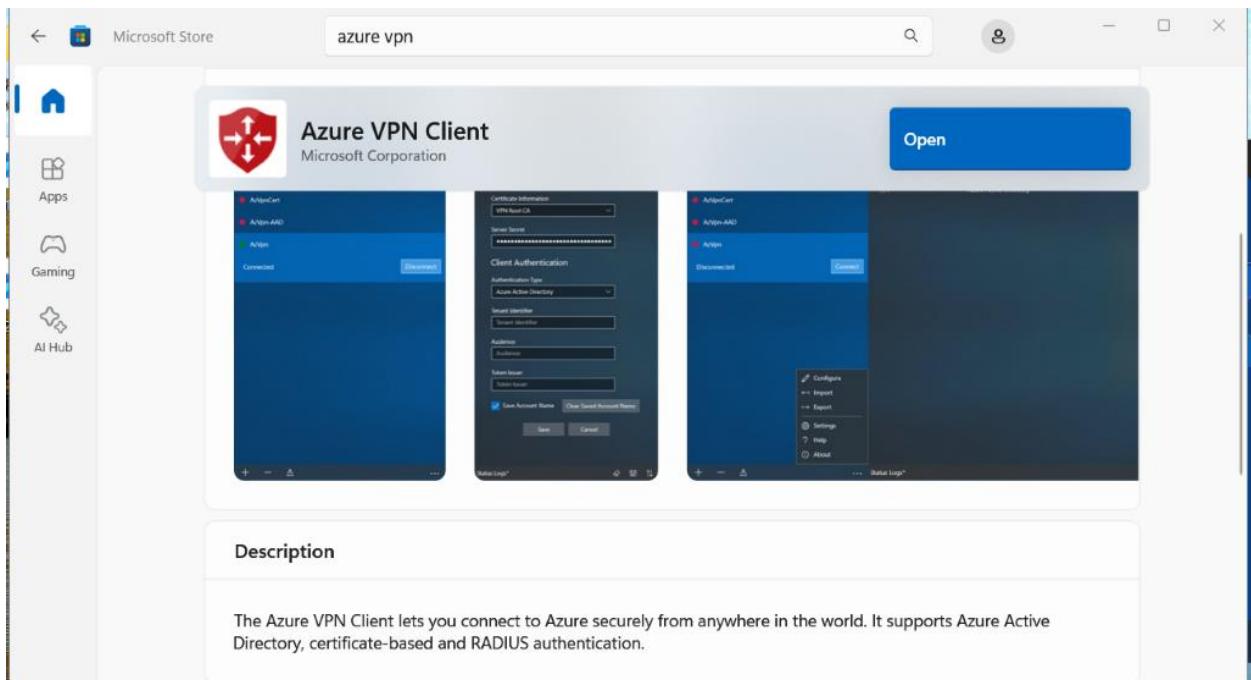
Search Save Discard Delete Download VPN client

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



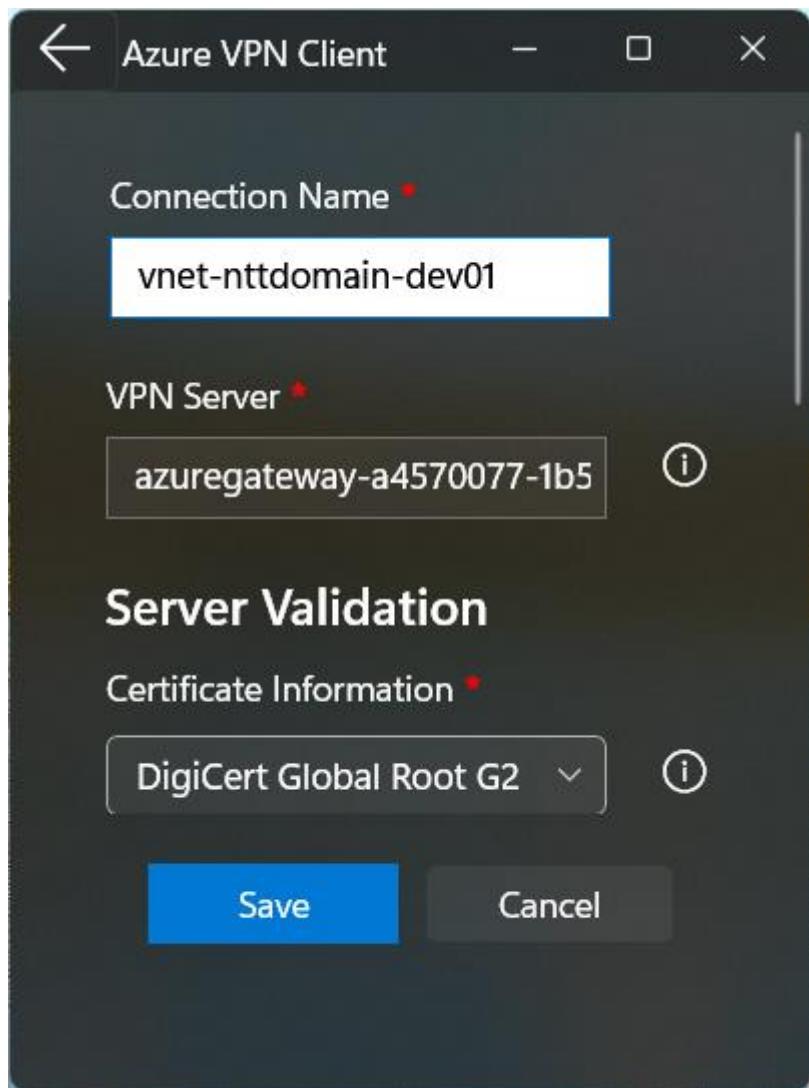
- ii. If no Azure VPN installer, we can get it from Microsoft Store



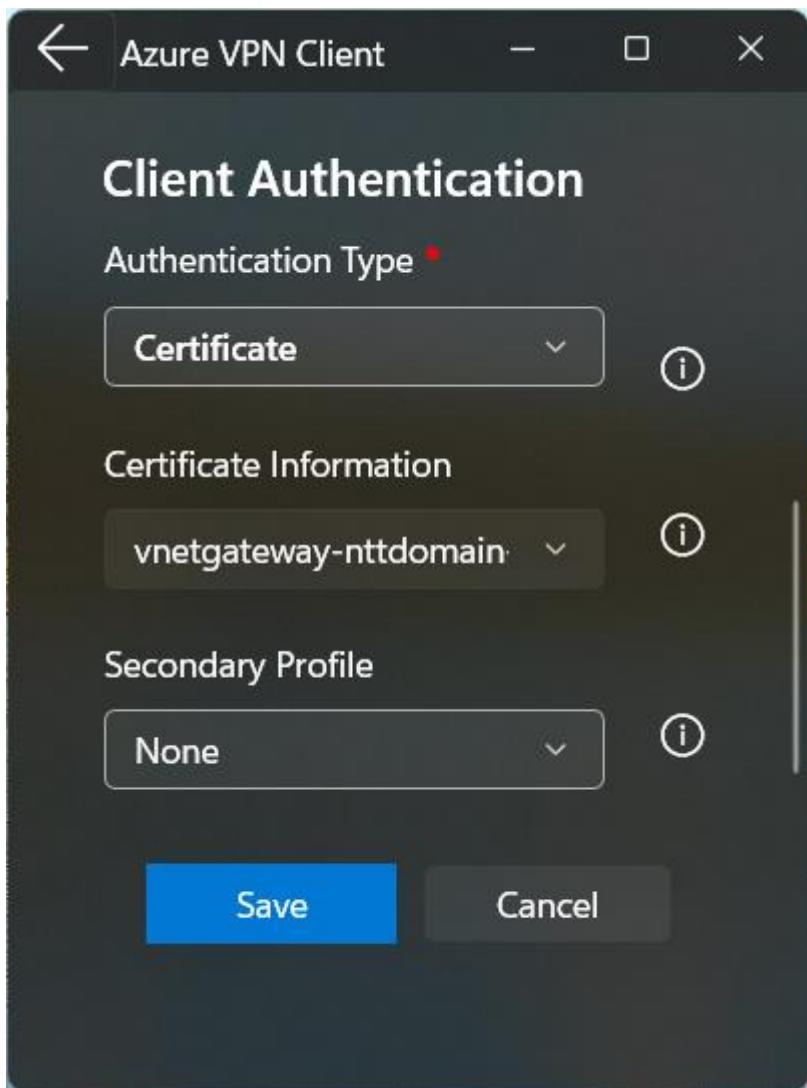
- iii. (Assume we are in client computer) Once Azure VPN Client Install, then we need to configure it. First import the client certificate (*.pfx) on the client side. IMPORTANT: Client certificate must be import into any client side (Can use automation / GPO / Policies to do that). When import the client 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



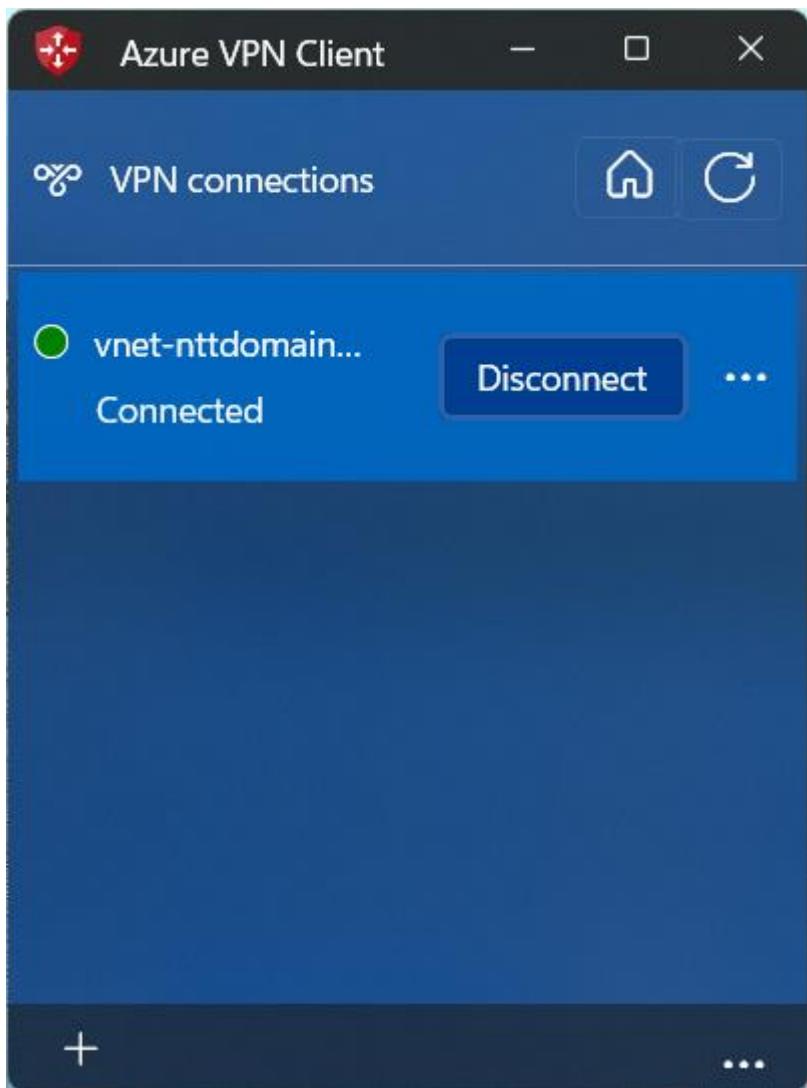
- v. Go to VPN Profiles that we've download previously (inside AzureVPN folder), you will see azurevpnconfig.xml > select and click Open. You will see connection name, server validation information



- 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 shpuld 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

X

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 ⓘ

Default

Name * ⓘ

PrivateEndpointSubnet

IPv4

Include an IPv4 address space



IPv4 address range ⓘ

10.0.0.0/16

10.0.0.0 - 10.0.255.255

Starting address * ⓘ

10.0.2.0

Size ⓘ

/24 (256 addresses)

Subnet address range ⓘ

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 learn'

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  



Koç Lea

Koç
Lea
Koç
Man
Build
learn
Learn

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 *	<input type="text" value="Azure subscription 1"/>	▼
Resource group *	<input type="text" value="rg-ntt-azuremachinelearning-dev01"/>	▼
	Create new	

Workspace details

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

Name *	<input type="text" value="azmlws-workspace-dev01"/>	✓
Region *	<input type="text" value="East US"/>	▼
Storage account *	<input type="text" value="(new) azmlwsstorageacctdev01"/>	▼
	Create new	
Key vault *	<input type="text" value="(new) azmlwskeyvaultdev01"/>	▼
	Create new	
Application insights *	<input type="text" value="(new) azmlwsappinsightdev01"/>	▼
	Create new	
Container registry	<input type="text" value="(new) azmlwscontainerregistrydev01"/>	▼
	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 can connect to this endpoint from anywhere on the internet.

Public network access *

Disabled

All networks

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

Workspace Inbound access

Name	Subscription
Click on add to create a private endpoint	
 Add	

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

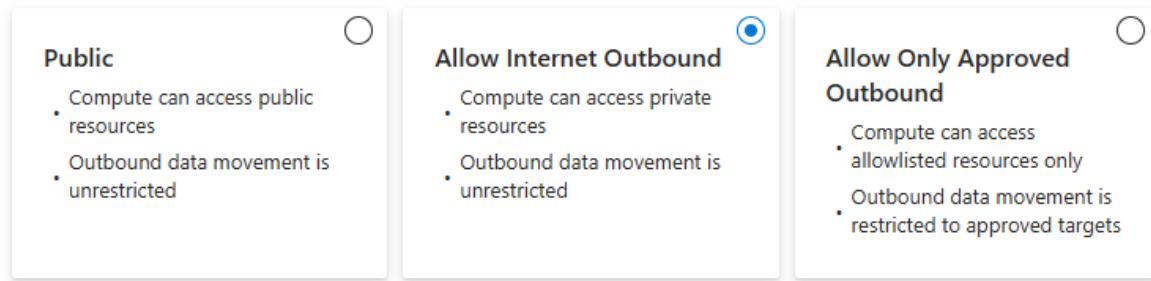
Azure Machine Learning

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](#)



Workspace Outbound access

Provision managed virtual network ①

[+ Add user-defined outbound rules](#)

Connection Name	Status	Destination Type
Required outbound rules		

c. Click review + create

10. Create private endpoint for workspace

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

The screenshot shows the 'Networking' settings for the 'azmlws-workspace-dev01' workspace. The 'Public access' tab is selected. Under 'Public network access', the 'Disabled' option is selected, indicating no public network can access the resource. The left sidebar shows other settings like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Events, and Settings.

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 ⓘ

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

Subnet * ⓘ

PrivateEndpointSubnet

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 **DNS** Tags 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-azurermachine... (new)	privatelink.api.azure...
privatelink-notebooks-az...	Azure subscription 1	rg-ntt-azurermachine... (new)	privatelink.noteboo...

d. Click review + create

11. Create private endpoint for storage

a. Go to resource group > rg-ntt-azurermachinelearning-dev01 > click storage account azmlwsstorageacctdev01 > Security + networking > networking

b. Disable public access

Home > Resource Manager | Resource groups > rg-ntt-azurermachinelearning-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 using 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

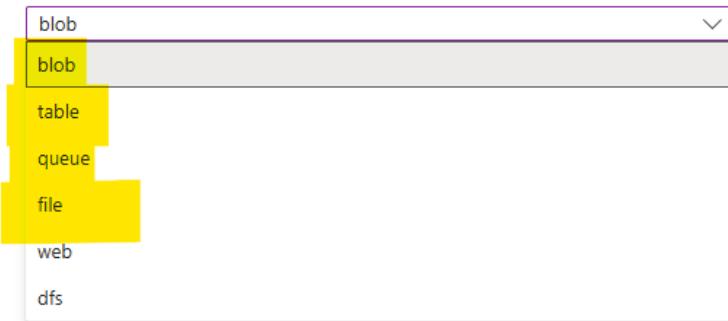
Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

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

Resource type Microsoft.Storage/storageAccounts

Resource azmlwsstorageacctdev01

Target sub-resource * ⓘ



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 [\(edit\)](#)

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 (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...

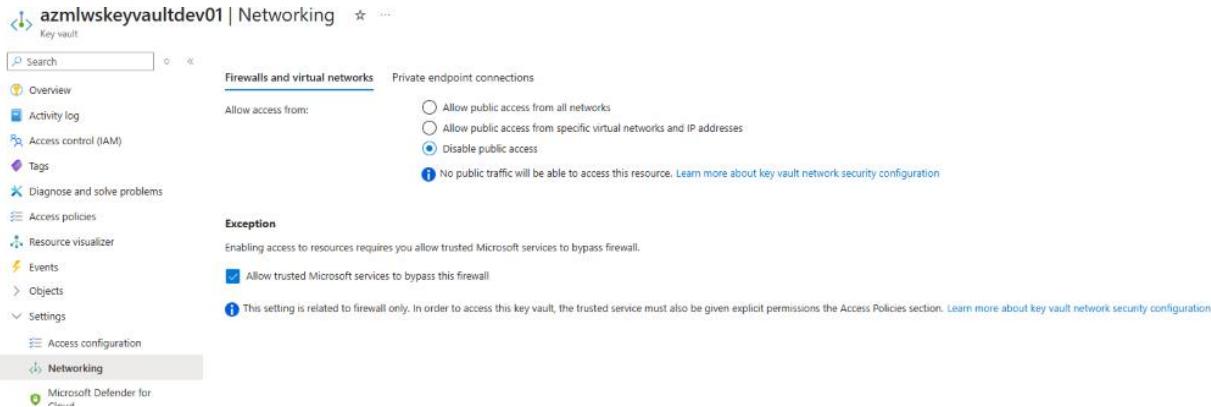
Azure subscription 1

rg-ntt-azurermachinel...

(new) privatelink.blob.cor...

12. Create private endpoint for keyvault

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



azmlwskeyvaultdev01 | Networking

Key vault

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

Access configuration Networking Microsoft Defender for

Firewalls and virtual networks Private endpoint connections

Allow access from:

- Allow public access from all networks
- Allow public access from specific virtual networks and IP addresses
- Disable public access

No public traffic will be able to access this resource. Learn more about key vault network security configuration

Exception

Enabling access to resources requires you allow trusted Microsoft services to bypass firewall.

Allow trusted Microsoft services to bypass this firewall

This setting is related to firewall only. In order to access this key vault, the trusted service must also be given explicit permissions the Access Policies section. Learn more about key vault network security configuration

- c. Private endpoints connection > create

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 *

Resource group * [Create new](#)

Instance details

Name *

Network Interface Name *

Region *

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 [?](#)

Connect to an Azure resource in my directory.

Connect to an Azure resource by resource ID or alias.

Subscription * [?](#)

Azure subscription 1

Resource type * [?](#)

Microsoft.KeyVault/vaults

Resource * [?](#)

azmlwskeyvaultdev01

Target sub-resource * [?](#)

vault

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 [\(edit\)](#)

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 ...

The screenshot shows the 'Create a private endpoint' wizard at the 'DNS' step. The steps are: Basics, Resource, Virtual Network, DNS (selected), Tags, Review + create. Under 'Private DNS integration', it says: '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.' A link 'Learn more' is provided. Below, 'Integrate with private DNS zone' has 'Yes' selected. Configuration details show: Configuration name: privatelink-vaultcore-azur..., Subscription: Azure subscription 1, Resource group: rg-ntt-azuremachine... (new), Private DNS zone: (new) privatelink.vaultcor...

13. Create private endpoints for container registry

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

The screenshot shows the Azure Container Registry settings for the resource 'azmlwscontainerregistrydev01'. The 'Networking' tab is active. In the 'Public access' section, the 'Disabled' option is selected. Under 'Firewall exception', there is a checked checkbox for 'Allow trusted Microsoft services to access this container registry'. Other tabs like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Quick start', 'Resource visualizer', 'Events', and 'Settings' are also visible.

c. Private access = create a private endpoint

Create a private endpoint ...

The screenshot shows the 'Create a private endpoint' wizard. Step 1: Basics is selected. Project details are set: Subscription is 'Azure subscription 1' and Resource group is 'rg-ntt-azuremachinelearning-dev01'. Below are sections for Instance details: Name is 'azmlws-containerregistry-pe-dev01', Network Interface Name is 'azmlws-containerregistry-pe-dev01-nic', and Region is 'East US'. Steps 2 through 6 are also listed at the top.

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 * ⓘ

registry



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 [\(edit\)](#)

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.azurecr.io

Create a private endpoint ...

Basics Resource Virtual Network **DNS** Tags 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

azmlwsappsinsightdev01 | Network Isolation

Public access

Ingestion access: Enabled from all networks
 Query access: Enabled from all networks

Public network access

Public network access: Restricted public inbound, enabled public outbound

- Private access = create private endpoints

azmlwsappsinsightdev01 | Network Isolation

Private access

Select a scope

Scope	Resource type	Location
AzureMonitorAzMWSpaceDev02	Azure Monitor Private Link Sco...	Global

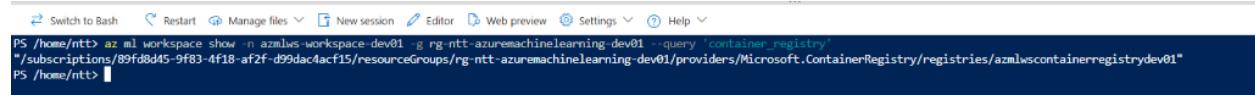
15. Create a compute cluster for container registry, else you will see this error

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=azmls-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 no 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'`



```
PS /home/ntt> az ml workspace show -n azmlws-workspace-dev01 -g rg-ntt-azuremachinelearning-dev01 --query 'container_registry'  
"/subscriptions/89fd8d45-9f83-4f18-af2f-d99dac4acf15/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 azmlwscomputeclusterdev01 -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

- 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 *

Region * ▾

(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) ▾

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 *

Subnet * (i)

[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 *

Subnet * (i)

[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

Name ↑	Resource group	Region	Subscription	Created on
azmlws-workspace-dev01	rg-ntt-azuremachinelearning-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

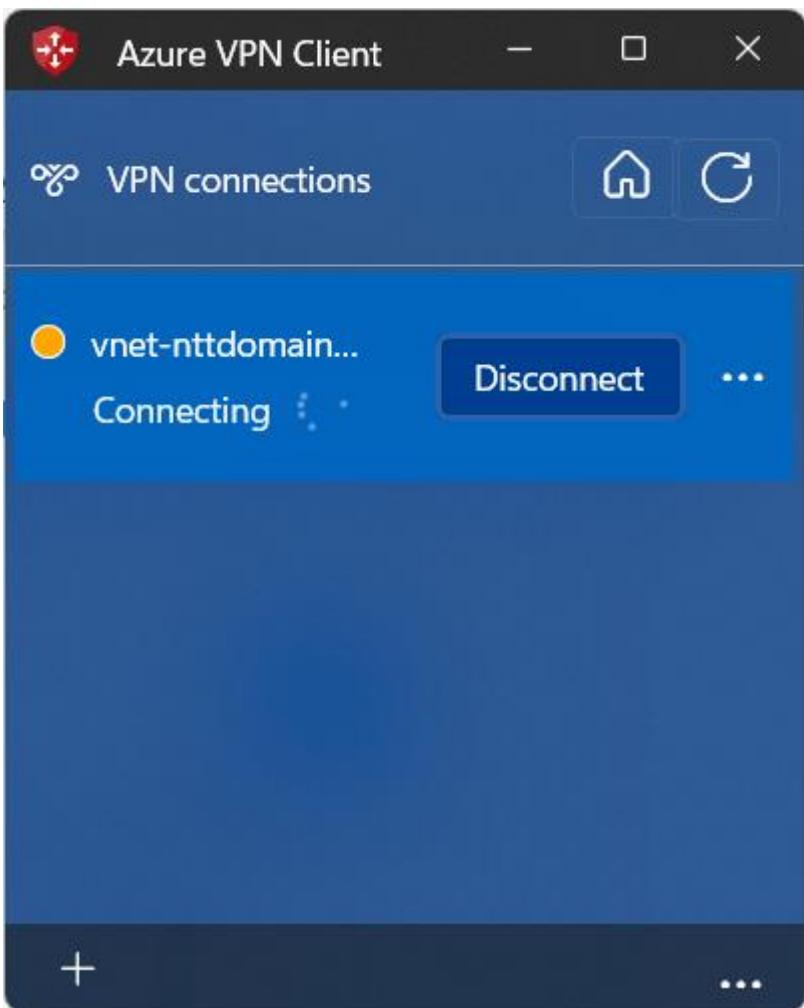
You are attempting to access a restricted resource from an unauthorized network location. Please contact your administrator or follow the troubleshooting instructions [here](#).

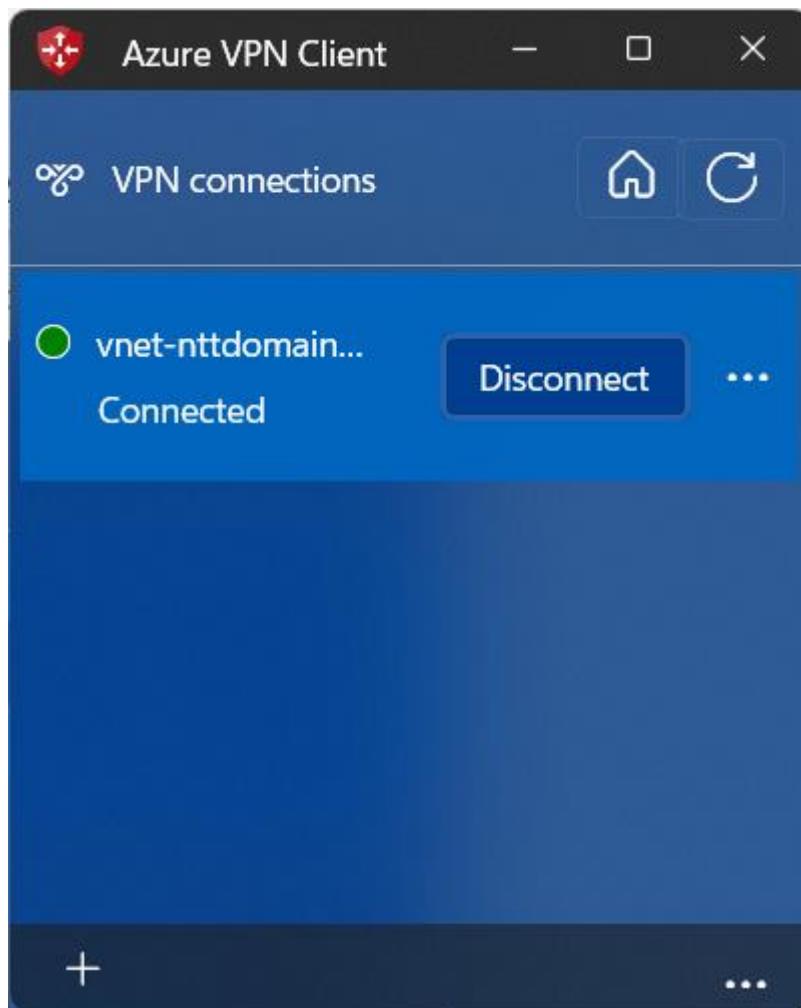
[← Back to all workspaces](#)

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)

The screenshot shows the Microsoft Foundry | Azure Machine Learning interface. The workspace is named 'azmlws-workspace-dev01'. On the left, there's a sidebar with navigation links like Home, Model catalog, Authoring, Notebooks, Automated ML, Designer, Prompt flow, Assets, Data, Jobs, Components, Pipelines, and Environments. The main area displays several AI models: 'Multi-Round Q&A on Your Data', 'Q&A on Your Data', 'Web Classification', 'Chat with Wikipedia', and 'Use GP'. Below these, there's a section for 'Generative AI models' with a 'View all' link. The taskbar at the bottom shows various pinned icons.

```
Administrator: Windows PowerShell X + v
PS C:\Windows\system32> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

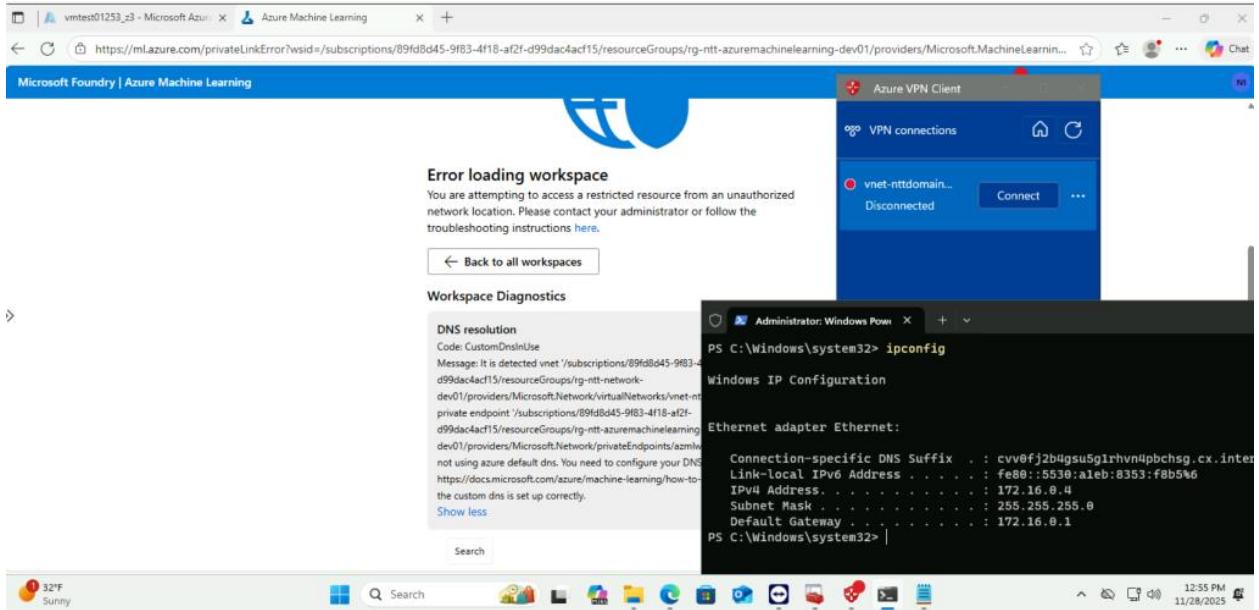
Connection-specific DNS Suffix . : cvv0fj2b4gsu5g1rvn4pbchsg.cx.internal.cloudapp.net
Link-local IPv6 Address . . . . . : fe80::5530:aleb:8353:f8b5%6
IPv4 Address. . . . . : 172.16.0.4
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.0.1

PPP adapter vnet-nttdomain-dev01:

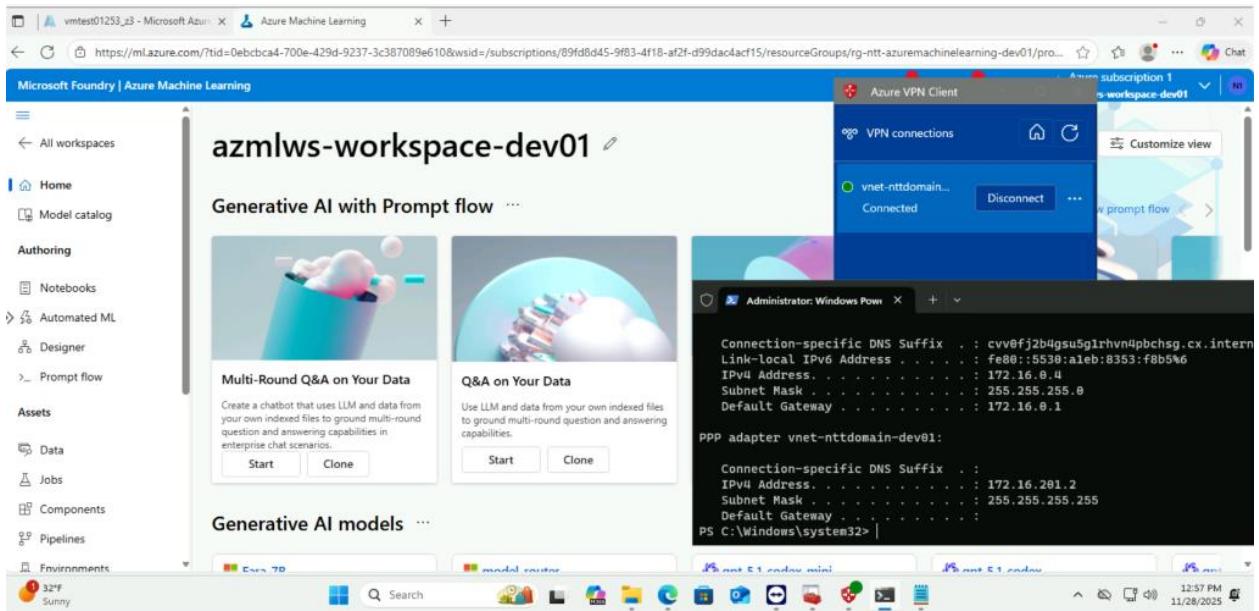
Connection-specific DNS Suffix . :
IPv4 Address. . . . . : 172.16.201.2
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . :

PS C:\Windows\system32>
```

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

Web Classification

Web Classification

This sample demonstrates multi-class classification with LLM. Given an URL, it will classify the URL into one web category with just a few shots, simple summarization and classification prompts.

What you will learn

In this flow, you will learn

- how to compose a classification flow with LLM.
- how to feed a few shots to LLM classifier.

Prerequisites

- Connection: Azure OpenAI or OpenAI connection.

Tools used in this flow

- LLM tool
- Python tool

[Go Back](#) [Clone](#) [Cancel](#)

Microsoft Foundry | Azure Machine Learning

Default Directory > azmlws-workspace-dev01 > Flows > Web Classification-11-29-2025-02-46-47

It will take 1 - 3 minutes to start the session.

Web Classification-11...

Flow

+ LLM + Prompt + Python + More tools

Raw file mode

Code Referring to: `prepare_examples.py`

```

from promptflow import tool

@tool
def prepare_examples():
    return [
        {
            "url": "https://play.google.com/store/apps/details?id=com.spotify.music",
            "text_content": "Spotify is a free music and podcast streaming app with millions of original podcasts. It also offers audiobooks, so users can enjoy new music, and listening to popular and exclusive podcasts. It has a variety of features such as creating and sharing playlists, and a subscription option which allows users to download and listen to ad-free music. It is available on all devices and has a variety of categories to choose from.",
            "category": "App",
            "evidence": "Both"
        },
        {
            "url": "https://www.youtube.com/channel/UC_x5XG1OV2P6uzZFSM9Ttw",
            "text_content": "YouTube is a video sharing platform that allows users to upload, share, and watch videos. It has a wide range of content, including music videos, vlogs, documentaries, and educational videos. YouTube is one of the most popular websites in the world and is used by billions of people every day.", "category": "Video", "evidence": "Both"
        }
    ]

```

Files

Graph

```

graph TD
    inputs((inputs)) --> fetch[fetch_text_content_from_url]
    fetch --> summarize(summarize_text_content)
    fetch --> prepare[prepare_examples]
    summarize --> classify(classify_with_llm)
    prepare --> classify

```

Microsoft Foundry | Azure Machine Learning

Default Directory > azmlws-workspace-dev01 > Notebooks

Notebooks

Files Samples



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

Navigation sidebar:

- All workspaces
- Home
- Model catalog
- Authoring
 - Notebooks
 - Automated ML
 - Designer
 - Prompt flow
- Assets
 - Data
 - Jobs
 - Components
 - Pipelines
 - Environments
 - Models
 - Endpoints
- Manage

Microsoft Foundry | Azure Machine Learning

Default Directory > azmlws-workspace-dev01 > Environments

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

Name	Source	Version	Created	Tags	Description
model-management:61	azureml	61	Nov 25, 2025 10:51 PM	Preview	Environment
sklearn-1:5:35	azureml	35	Nov 25, 2025 9:55 PM	OpenMp : 4.1.0 OS : Ubuntu20.04 Preview Python : 3.10	An environment
lightgbm-3:3:70	azureml	70	Nov 25, 2025 9:54 PM	LightGBM : 4.6 OpenMp : 5.0 OS : Ubuntu24.04 Preview	An environment
component:68	azureml	68	Nov 25, 2025 8:20 PM	OS : Ubuntu22.04 Python : 3.9	An environment
python-sdk-v2:40	azureml	40	Nov 25, 2025 8:08 PM	Preview	Environment
mlflow-model-inference:15	azmlml	15	Nov 25, 2025 8:07 PM	Inference OS : Ubuntu22.04 Preview	AzureML MI

Prev Next 25/Page

Navigation sidebar:

- Notebooks
- Automated ML
- Designer
- Prompt flow
- Assets
- Data
- Jobs
- Components
- Pipelines
- Environments
- Models
- Endpoints
- Manage
- Compute
- Monitoring
- Data Labeling
- Linked Services
- Connections

Microsoft Foundry | Azure Machine Learning

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

azmlwscomputeclusterdev01

Details Nodes Jobs Monitoring (preview)

Assets Data Jobs Components Pipelines Environments Models Endpoints Manage Compute Monitoring Data Labeling Linked Services PREVIEW Connections

Cluster node status

0

Idle Leaving Preparing Running

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

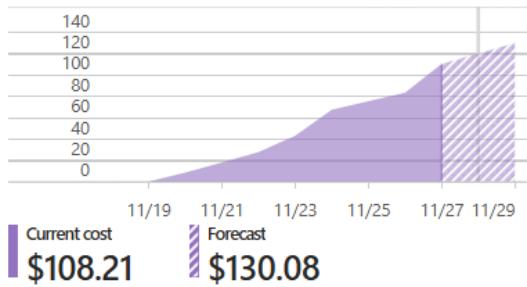
Search Filter Columns

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

Assets Data Jobs Components Pipelines Environments Models Endpoints Manage Compute Monitoring Data Labeling Linked Services PREVIEW Connections

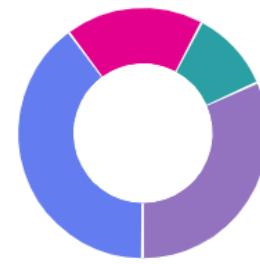
Finally I spend USD108.21 to complete this project

Spending rate and forecast



[View details](#)

Costs by resource



[View details](#)

The best part is my secure score is 100%