

HOW TO CONFIGURE PRIVATE ENDPOINT WITH AZURE SERVICES

- In the search box at the top of the portal, enter Private link. Select Private link services in the search results.
- Select + Create.
- In the Basics tab, enter or select the following information:

[Dashboard](#) >

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 * ⓘ

Free Trial

▼

Resource group * ⓘ

(New) demo-RG

▼

[Create new](#)

Instance details

Name *

demo-endpoint

✓

Network Interface Name *

demo-endpoint-nic

✓

Region *

Central India

▼

- Select Next: Outbound settings.
- In the resource tab, enter or select the following information: (for demonstration we are creating a storage endpoint)

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 ⓘ	<input checked="" type="radio"/> Connect to an Azure resource in my directory. <input type="radio"/> Connect to an Azure resource by resource ID or alias.
Subscription * ⓘ	Free Trial ▼
Resource type * ⓘ	Microsoft.Storage/storageAccounts ▼
Resource * ⓘ	qwerty123456 ▼
Target sub-resource * ⓘ	queue ▼

- In connection method we can also connect using alias (Any HTTPS endpoint that returns a valid Azure Analysis Services server name can serve as an alias. The endpoint must support HTTPS over port 443 and the port must not be specified in the URI.)
- Before going to the next tab create a virtual network in the same region of the private endpoint. here, we created a virtual network named “qwerty1234”
- Select Next: Virtual Network.
- In Virtual Network, enter or select the following information.

Create a private endpoint ...

Networking

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

Virtual network * ⓘ	qwerty1234 (DefaultResourceGroup-EUS) ▼
Subnet * ⓘ	default ▼

Network policy for private endpoints Disabled ([edit](#))

Private IP configuration

☒ Dynamically allocate IP address
☐ Statically allocate IP address

Application security group

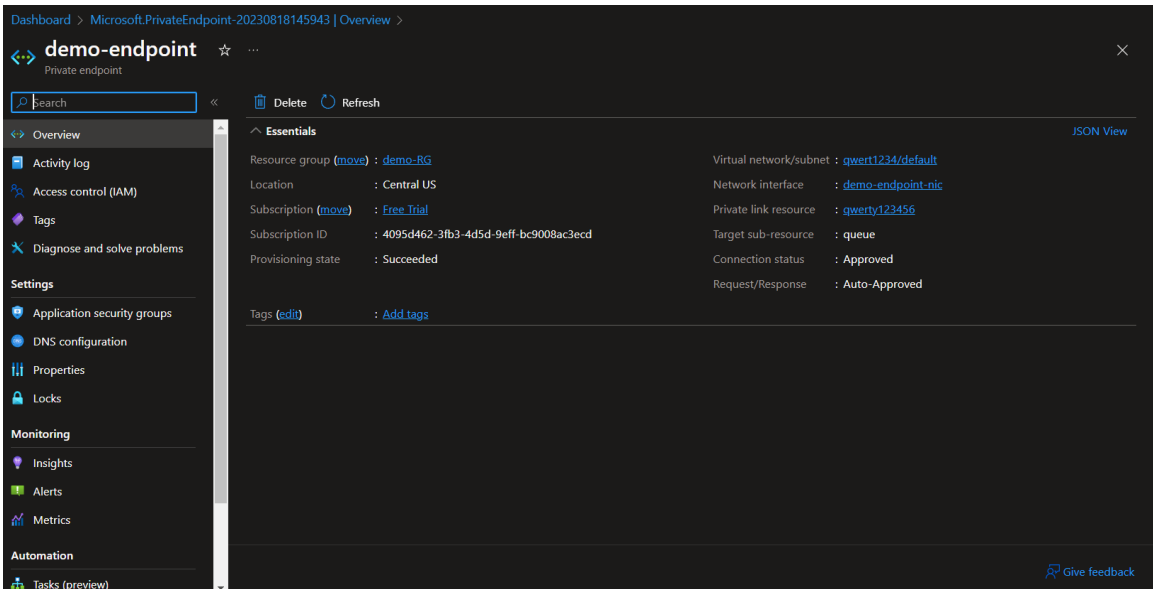
Configure network security as a natural extension of an application's structure. ASG allows you to group virtual machines and define network security policies based on those groups. You can specify an application security group as the source or destination in an NSG security rule. [Learn more](#)

[+ Create](#)

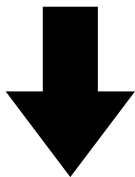
Application security group

(new) demo-nsg	
----------------	--

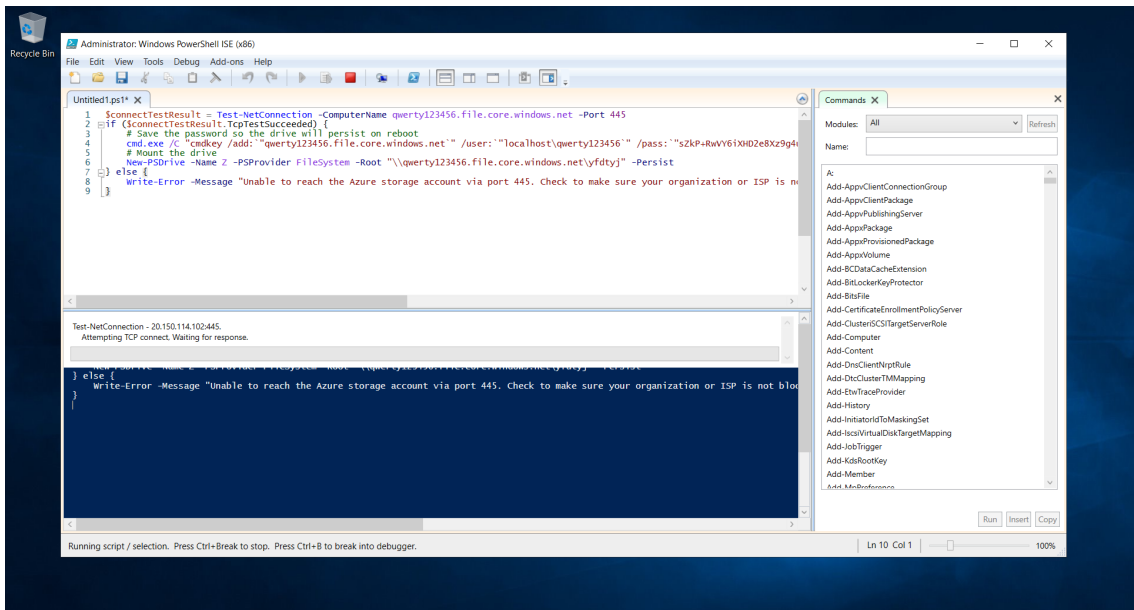
- If we are allocating static private IP then we must manually enter IP for the endpoint
- Select Review + create.
- Select Create.



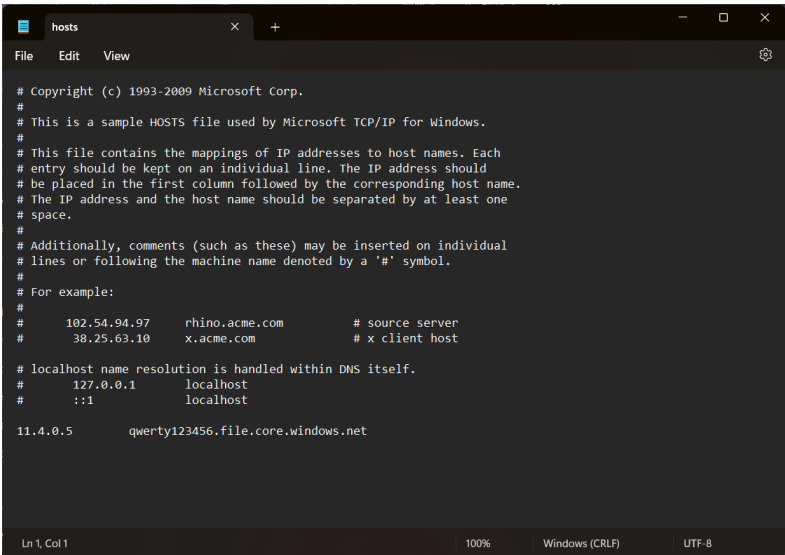
- An endpoint has been created successfully . Now to test the private endpoint,



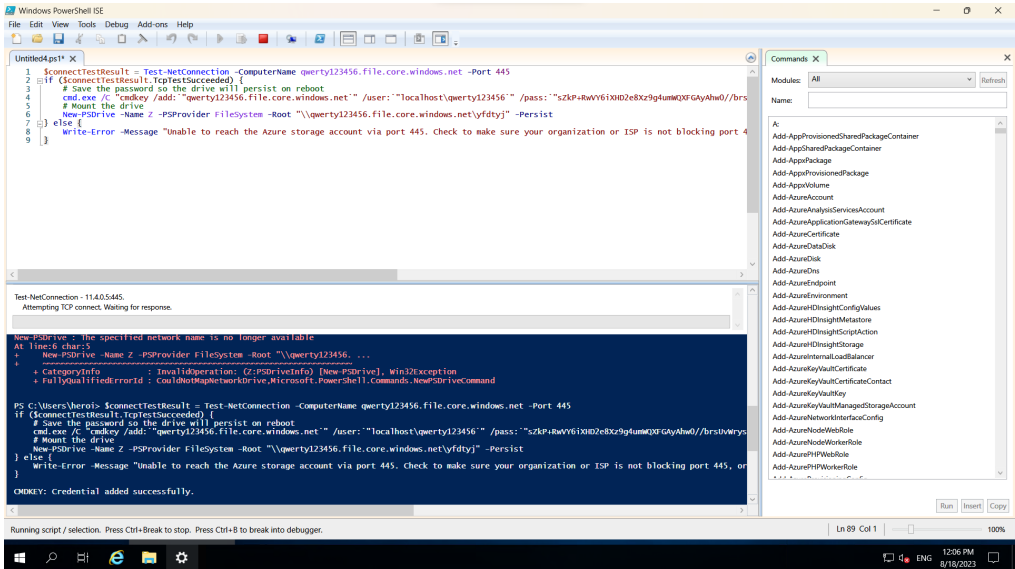
- before adding the private IP in hosts



- The disk is attached using a public IP (20.150.114.102)
- After adding the private IP in hosts



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10       x.acme.com           # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
#
11.4.0.5       qerty123456.file.core.windows.net
```



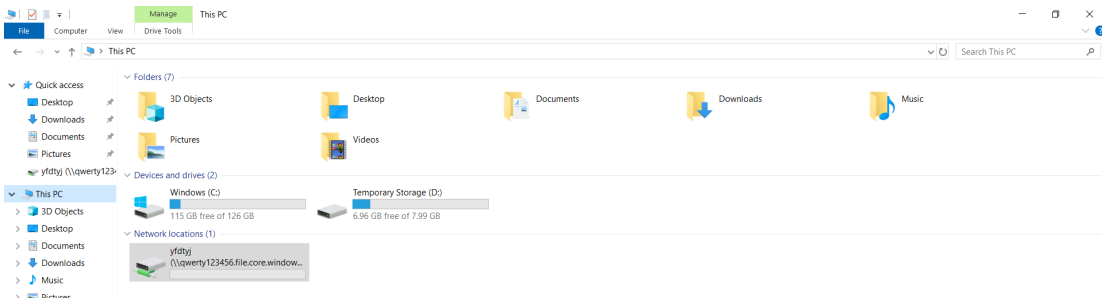
```
1 $connectTestResult = Test-NetConnection -ComputerName qerty123456.file.core.windows.net -Port 445
2 if ($connectTestResult.TcpTestSucceeded) {
3     # Save the password so the drive will persist on reboot
4     cmd.exe /c "cmdkey /add: qerty123456.file.core.windows.net /user:"localhost\qerty123456" /pass:"szkP+hwY6ixm2eKx3gltumq8GdyAhnd0/hrs
5 } else {
6     New-PSDrive -Name Z -PSProvider filesystem -Root "\\qerty123456.file.core.windows.net\yfdtyj" -Persist
7     Write-Error -Message "Unable to reach the Azure storage account via port 445. Check to make sure your organization or ISP is not blocking port 445."
8 }
9
```

Test-NetConnection - 11.4.0.5:445.
Attempting TCP connect. Waiting for response.

new-PSDrive : The specified network name is no longer available
At line:6 char:5
+ New-PSDrive -Name Z -PSProvider filesystem -Root "\\qerty123456...
+ ~~~~~
+ CategoryInfo : InvalidOperation (Z:PSDriveInfo) (New-PSDrive, Win32Exception)
+ FullyQualifiedErrorId : CouldNotMapNetworkDriveMicrosoft.PowerShell.Commands.NewDriveCommand

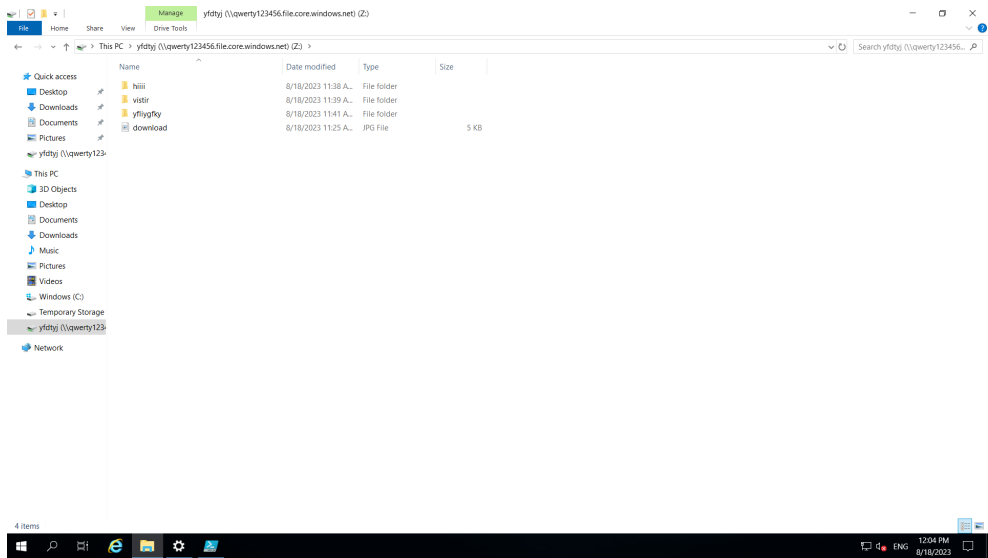
PS C:\Users\heroi> \$connectTestResult = Test-NetConnection -ComputerName qerty123456.file.core.windows.net -Port 445
if (\$connectTestResult.TcpTestSucceeded) {
 # Save the password so the drive will persist on reboot
 cmd.exe /c "cmdkey /add: qerty123456.file.core.windows.net /user:"localhost\qerty123456" /pass:"szkP+hwY6ixm2eKx3gltumq8GdyAhnd0/hrs
} else {
 New-PSDrive -Name Z -PSProvider filesystem -Root "\\qerty123456.file.core.windows.net\yfdtyj" -Persist
 Write-Error -Message "Unable to reach the Azure storage account via port 445. Check to make sure your organization or ISP is not blocking port 445."
}
cmdkey: credential added successfully.

- The connection is through the private endpoint IP and the drive is mounted successfully to the computer





- Any changes made in the drive is show in Azure portal and can be monitored by Admin



Home > Storage accounts > qwerty123456 | File shares > yfdtyj

yfdtyj | Browse

SMB File share

Search

Connect Upload Add directory Refresh Delete share Change tier Edit quota

Overview

Diagnose and solve problems

Access Control (IAM)

Browse

Operations

Snapshots

Backup

Authentication method: Access key (Switch to Azure AD User Account)

Search files by prefix

Name	Type	Size	
hiii	Directory		...
vistir	Directory		...
yfliygiky	Directory		...
download.jpg	File	4.46 KIB	...

