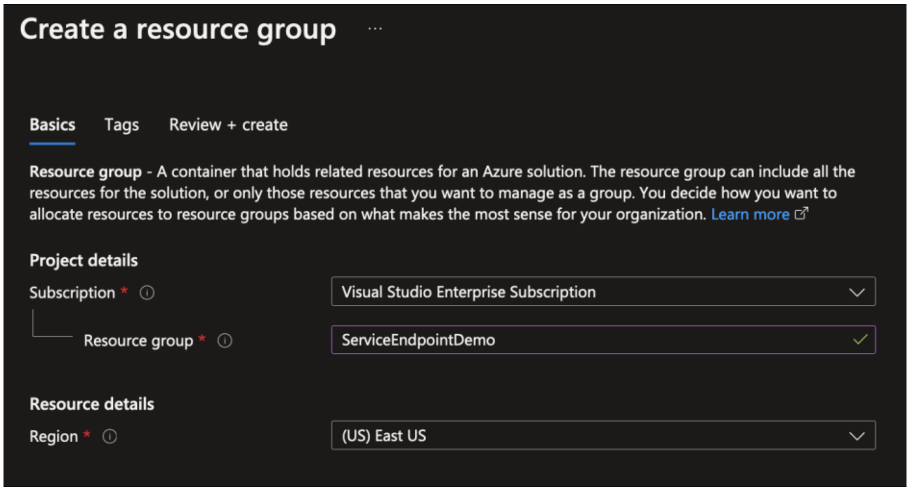
Azure Service Endpoint

Create a new Resource Group:

Login to Azure portal (https://portal.azure.com/) and then create a new RG



Create a resource group ···

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

Project details

Subscription * : Visual Studio Enterprise Subscription

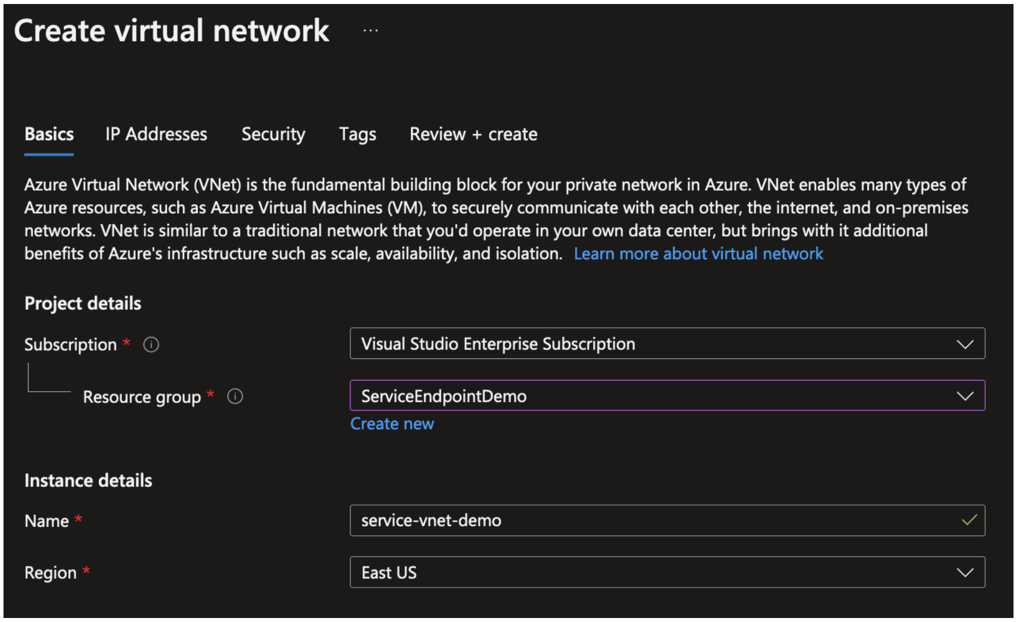
Resource group * : ServiceEndpointDemo

Resource details

Region * : (US) East US

Create a new Virtual Network:

Create a new VNet in the same RG where we have created the new Service Endpoint plan



Create virtual network ···

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. Learn more about virtual network

Project details

Subscription * : Visual Studio Enterprise Subscription

Resource group * : ServiceEndpointDemo

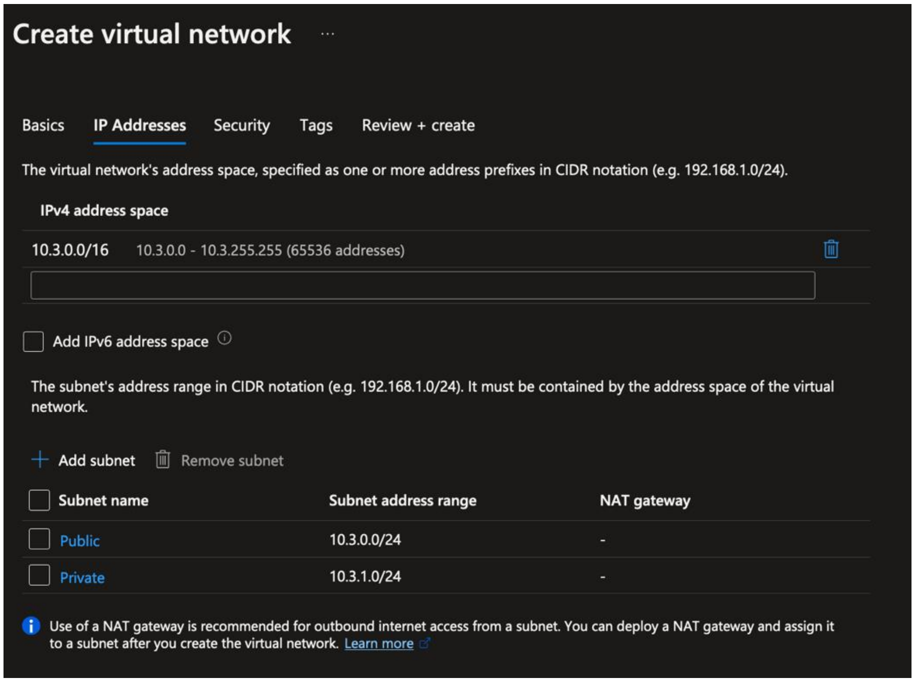
Create new

Instance details

Name * : service-vnet-demo

Region * : East US

Create 2 Subnet as one for Public and other for Private endpoint.



Create virtual network ···

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

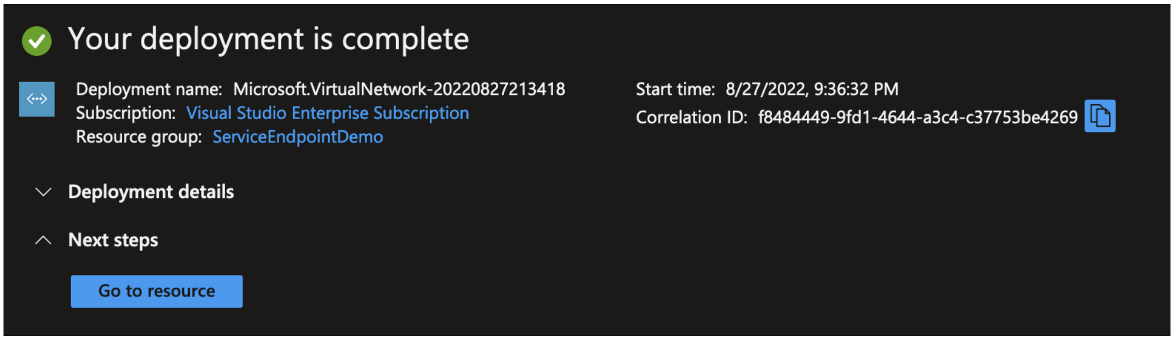
IPv4 address space	
10.3.0.0/16	10.3.0.0 - 10.3.255.255 (65536 addresses)

□ Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

□ Subnet name	Subnet address range	NAT gateway
□ Public	10.3.0.0/24	-
□ Private	10.3.1.0/24	-

ⓘ Use of a NAT gateway is recommended for outbound internet access from a subnet. You can deploy a NAT gateway and assign it to a subnet after you create the virtual network. Learn more

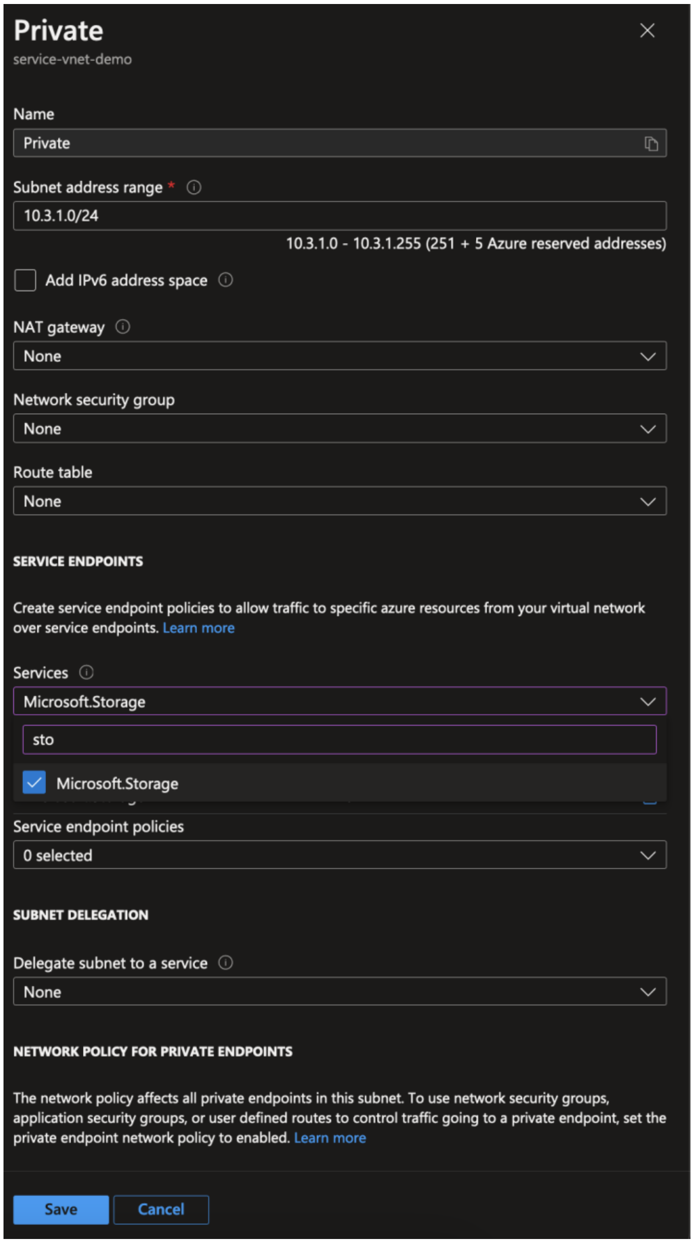


Your deployment is complete

Deployment name: Microsoft.VirtualNetwork-20220827213418
Subscription: Visual Studio Enterprise Subscription
Resource group: ServiceEndpointDemo

Start time: 8/27/2022, 9:36:32 PM
Correlation ID: f8484449-9fd1-4644-a3c4-c37753be4269

Once the Vnet is created, we need to enable the Service Endpoint for the Storage account so that the traffic goes only to the Storage account and not the external Internet.



Private

service-vnet-demo

Name

Private

Subnet address range *

10.3.1.0/24

10.3.1.0 - 10.3.1.255 (251 + 5 Azure reserved addresses)

□ Add IPv6 address space

NAT gateway

None

Network security group

None

Route table

None

SERVICE ENDPOINTS

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

Services

Microsoft.Storage

sto

☑ Microsoft.Storage

Service endpoint policies

0 selected

SUBNET DELEGATION

Delegate subnet to a service

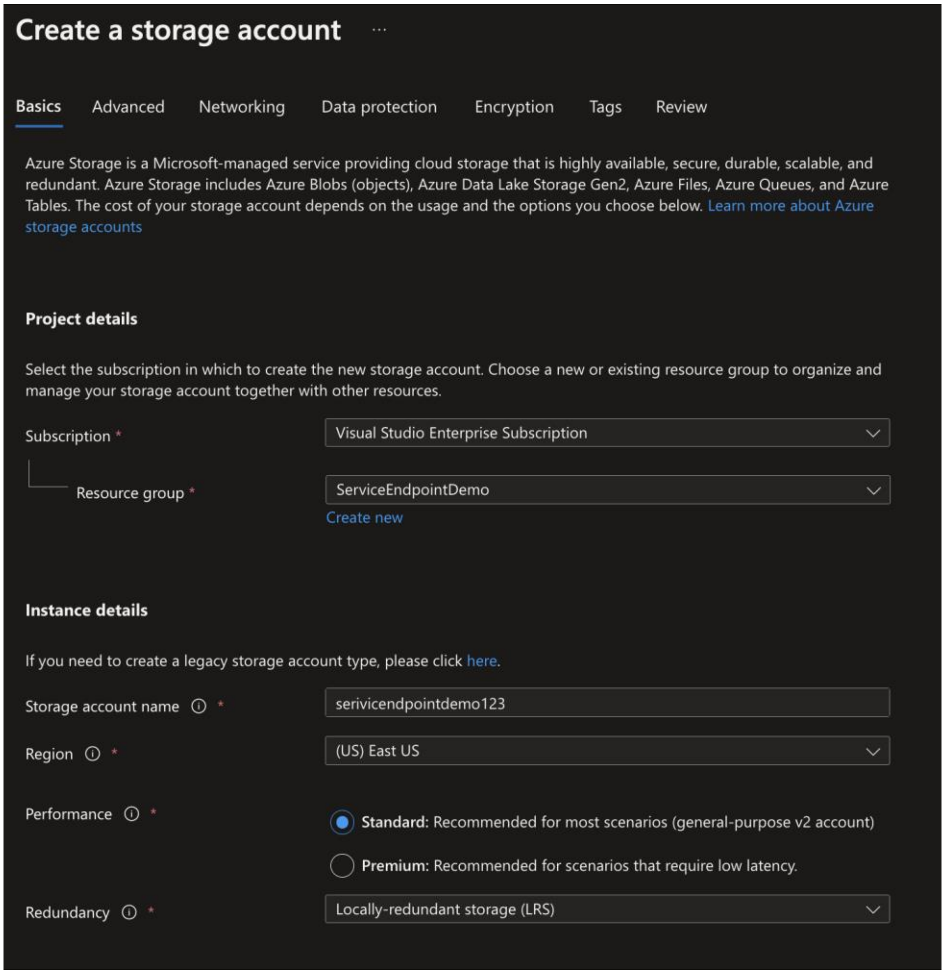
None

NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. To use network security groups, application security groups, or user defined routes to control traffic going to a private endpoint, set the private endpoint network policy to enabled. Learn more

Create a new Storage Account:

Create a new Storage Account in the same RG where we need to create a Service Endpoint.



Create a storage account ···

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. Learn more about Azure storage accounts

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription *: Visual Studio Enterprise Subscription

Resource group *: ServiceEndpointDemo

Create new

Instance details

If you need to create a legacy storage account type, please click here.

Storage account name ⓘ *: serivicendpointdemo123

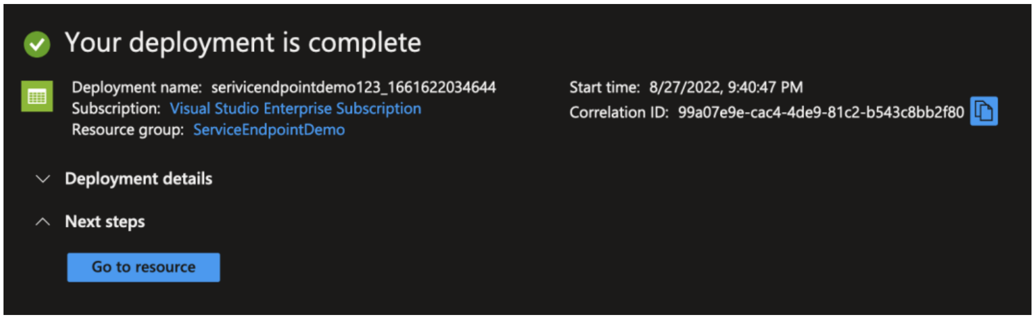
Region ⓘ *: (US) East US

Performance ⓘ *:

● **Standard:** Recommended for most scenarios (general-purpose v2 account)

○ **Premium:** Recommended for scenarios that require low latency.

Redundancy ⓘ *: Locally-redundant storage (LRS)

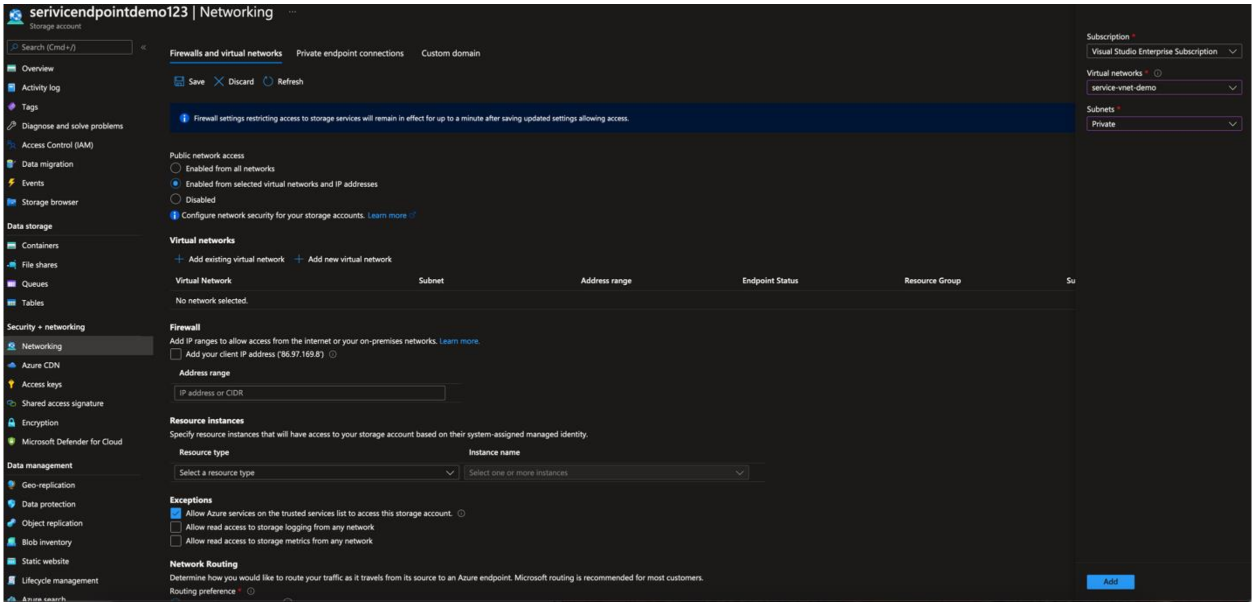


Your deployment is complete

Deployment name: serivicendpointdemo123_1661622034644
Subscription: Visual Studio Enterprise Subscription
Resource group: ServiceEndpointDemo

Start time: 8/27/2022, 9:40:47 PM
Correlation ID: 99a07e9e-cac4-4de9-81c2-b543c8bb2f80

Once the Storage account is created then try to disable the internet traffic and then allow only the subnet where we created the End point.



Firewall settings restricting access to storage services will remain in effect for up to a minute after saving updated settings allowing access.

Public network access

○ Enabled from all networks
● Enabled from selected virtual networks and IP addresses
○ Disabled

Configure network security for your storage accounts. Learn more

Virtual networks

+ Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group	Su
No network selected.					

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. Learn more.

□ Add your client IP address ('86.97.169.8')

Address range: IP address or CIDR

Resource instances

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

Resource type: Select a resource type
Instance name: Select one or more instances

Exceptions

☑ Allow Azure services on the trusted services list to access this storage account.
□ Allow read access to storage logging from any network
□ Allow read access to storage metrics from any network

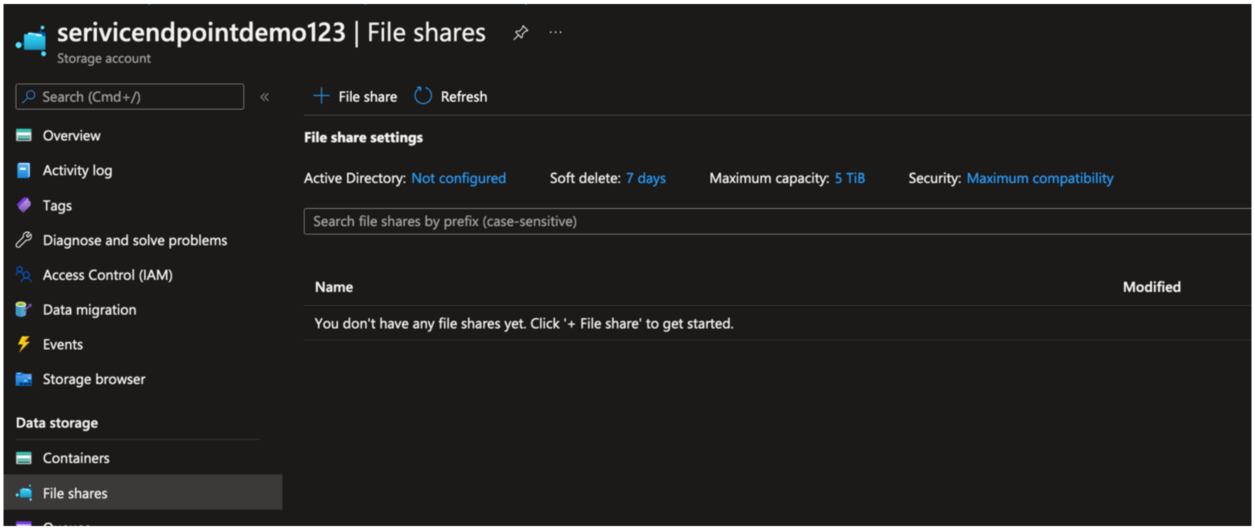
Network Routing

Determine how you would like to route your traffic as it travels from its source to an Azure endpoint. Microsoft routing is recommended for most customers.

Routing preference *

Subscription *: Visual Studio Enterprise Subscription
Virtual networks *: service-vnet-demo
Subnets *: Private

Next, create a new file share to check if we can access this file share outside in the internet.

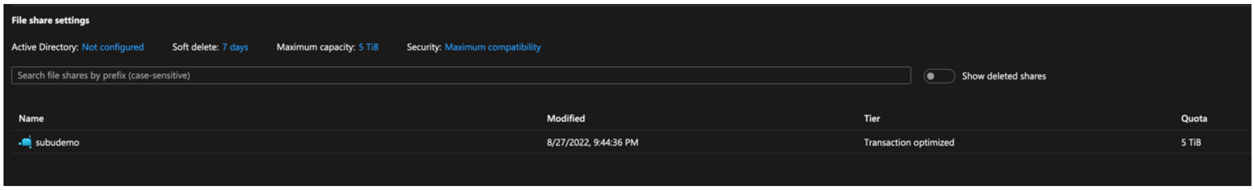


File share settings

Active Directory: Not configured Soft delete: 7 days Maximum capacity: 5 TiB Security: Maximum compatibility

Search file shares by prefix (case-sensitive)

Name	Modified
You don't have any file shares yet. Click '+ File share' to get started.	



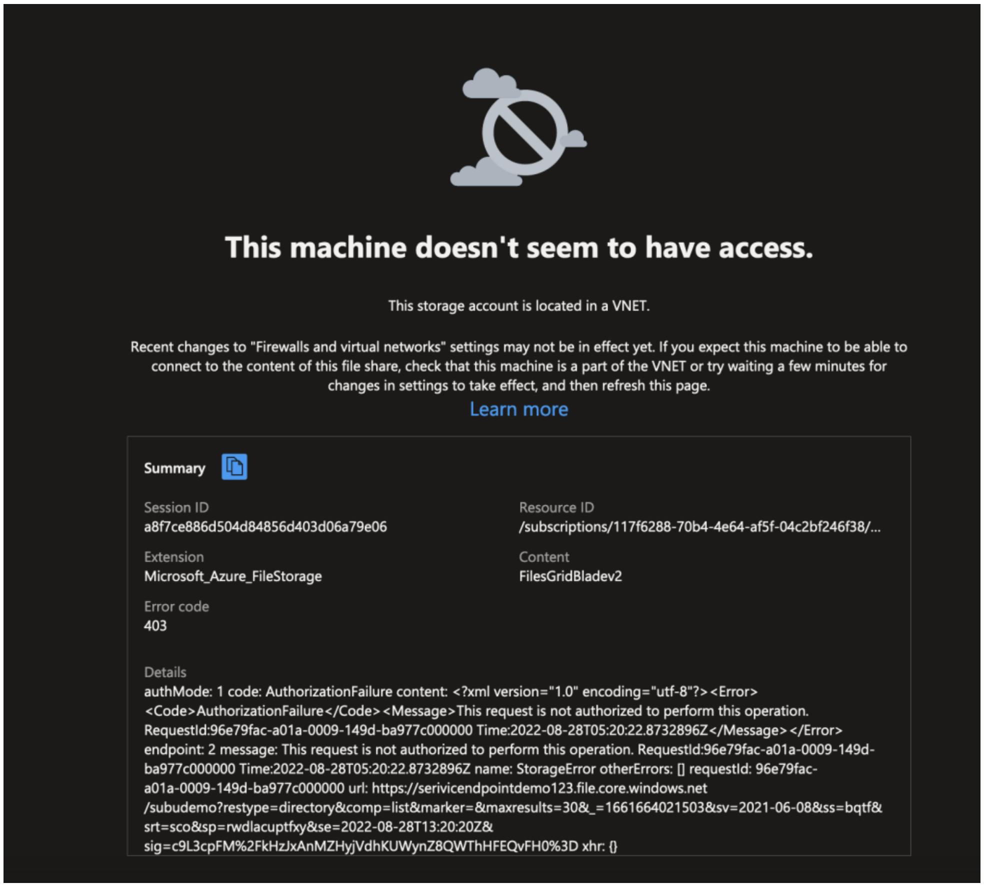
File share settings

Active Directory: Not configured Soft delete: 7 days Maximum capacity: 5 TiB Security: Maximum compatibility

Search file shares by prefix (case-sensitive)

Name	Modified	Tier	Quota
subudemo	8/27/2022, 9:44:36 PM	Transaction optimized	5 TiB

Now, take the script from the file server to connect to the file share and then we can see if its allowed or not.



This machine doesn't seem to have access.

This storage account is located in a VNET.

Recent changes to "Firewalls and virtual networks" settings may not be in effect yet. If you expect this machine to be able to connect to the content of this file share, check that this machine is a part of the VNET or try waiting a few minutes for changes in settings to take effect, and then refresh this page.

Learn more

Summary

Session ID
a8f7ce886d504d84856d403d06a79e06

Resource ID
/subscriptions/117f6288-70b4-4e64-af5f-04c2bf246f38/...

Extension
Microsoft_Azure_FileStorage

Content
FilesGridBladev2

Error code
403

Details

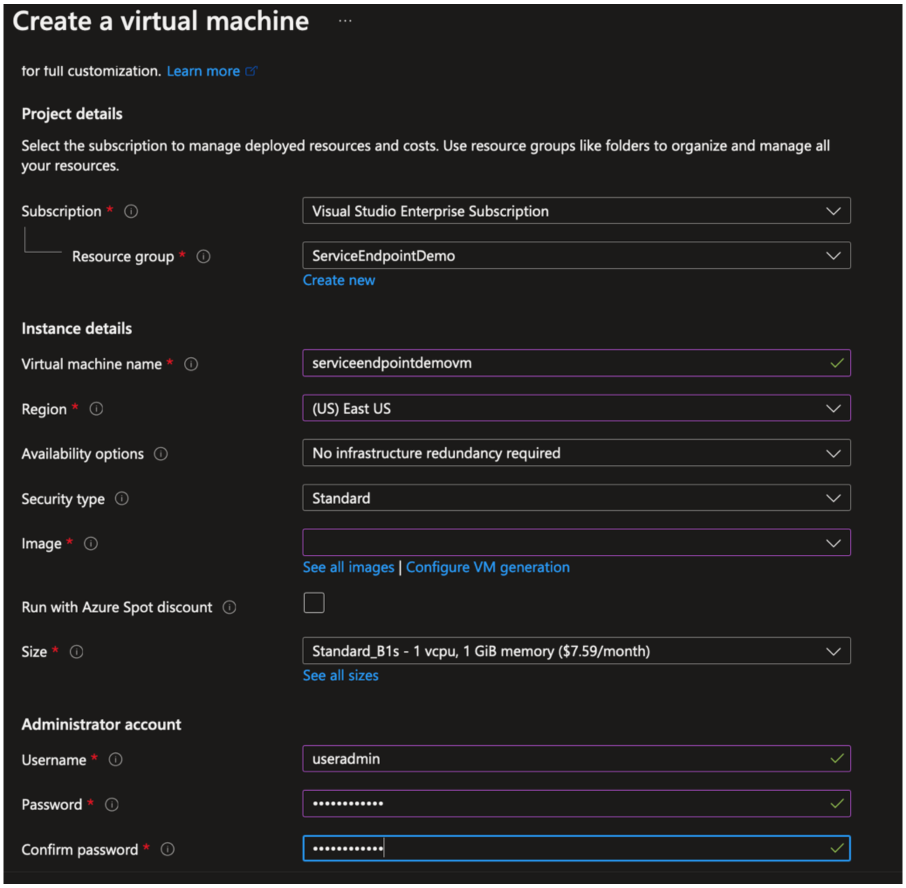
```
authMode: 1 code: AuthorizationFailure content: <?xml version="1.0" encoding="utf-8"?><Error>
<Code>AuthorizationFailure</Code><Message>This request is not authorized to perform this operation.
RequestId:96e79fac-a01a-0009-149d-ba977c000000 Time:2022-08-28T05:20:22.8732896Z</Message></Error>
endpoint: 2 message: This request is not authorized to perform this operation. RequestId:96e79fac-a01a-0009-149d-
ba977c000000 Time:2022-08-28T05:20:22.8732896Z name: StorageError otherErrors: [] requestId: 96e79fac-
a01a-0009-149d-ba977c000000 url: https://serivicendpointdemo123.file.core.windows.net
/subudemo?restype=directory&comp=list&marker=&maxresults=30&_=1661664021503&sv=2021-06-08&ss=bqtf&
srt=sco&sp=rwdlacuptfxy&se=2022-08-28T13:20:20Z&
sig=c9L3cpFM%2FkHzJxAnMZHyjVdhKUWynZ8QWThHFEQvFH0%3D xhr: {}
```

If you see the error, it clearly says that only the Vnet has access to the Storage account.

Now let’s create a new VM and try to access that to the file server.

<u>Create a new VM to test the Service End point:</u>

Create a new VM and add the same VNet and Storage Account to this VM so that we will be able to test the VM accordingly.



Create a virtual machine ···

for full customization. Learn more

Project details

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

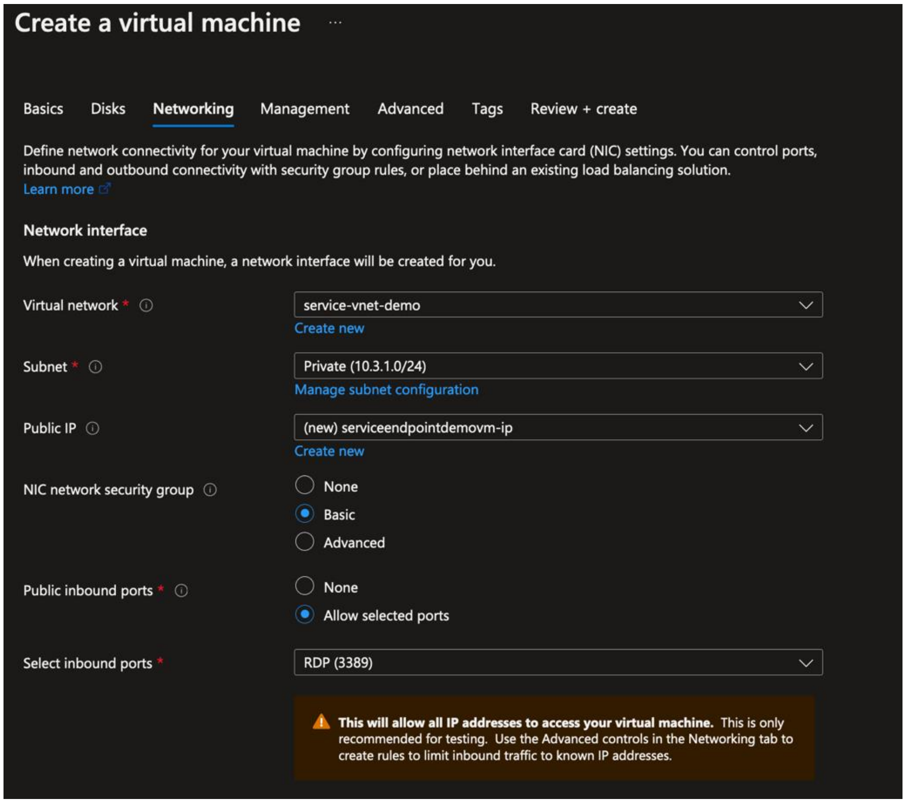
Subscription * ⓘ	Visual Studio Enterprise Subscription
Resource group * ⓘ	ServiceEndpointDemo Create new

Instance details

Virtual machine name * ⓘ	serviceendpointdemovm ✓
Region * ⓘ	(US) East US
Availability options ⓘ	No infrastructure redundancy required
Security type ⓘ	Standard
Image * ⓘ	 See all images | Configure VM generation
Run with Azure Spot discount ⓘ	□
Size * ⓘ	Standard_B1s - 1 vcpu, 1 GiB memory ($7.59/month) See all sizes

Administrator account

Username * ⓘ	useradmin ✓
Password * ⓘ	•••••••••••• ✓
Confirm password * ⓘ	•••••••••••• ✓



Create a virtual machine ···

Basics Disks **Networking** Management Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
Learn more

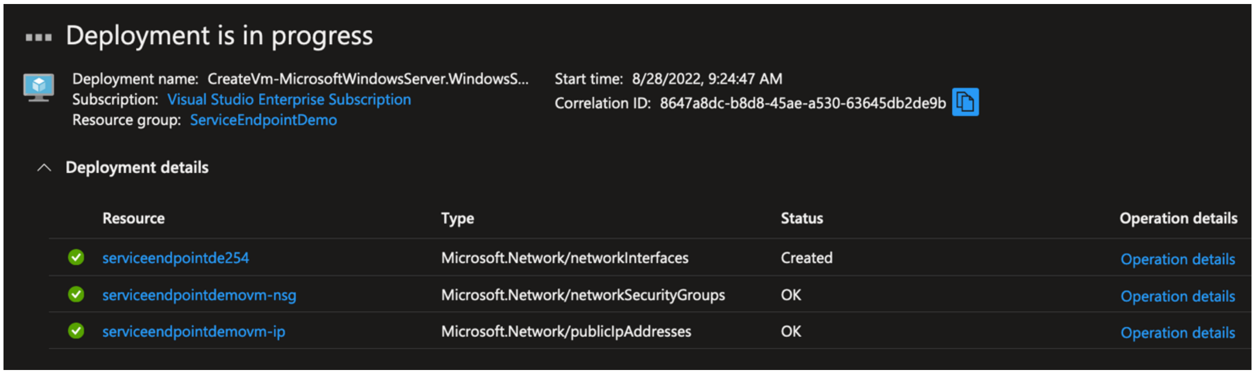
Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ	service-vnet-demo Create new
Subnet * ⓘ	Private (10.3.1.0/24) Manage subnet configuration
Public IP ⓘ	(new) serviceendpointdemovm-ip Create new
NIC network security group ⓘ	○ None ● Basic ○ Advanced
Public inbound ports * ⓘ	○ None ● Allow selected ports
Select inbound ports *	RDP (3389)

⚠ **This will allow all IP addresses to access your virtual machine.** This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Use the same Vnet where we created the Service End Point.



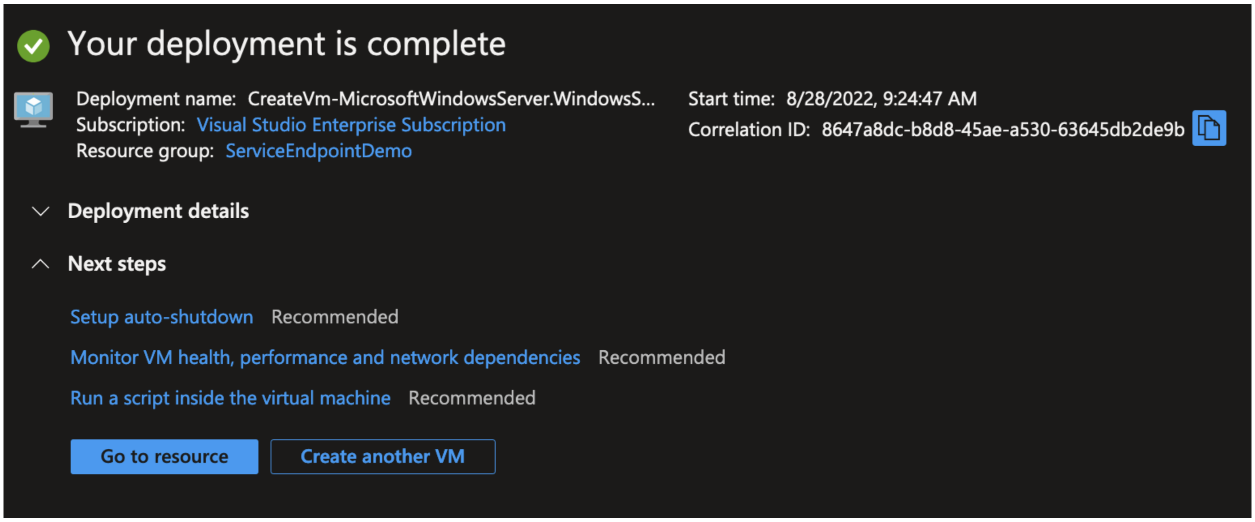
Deployment is in progress

Deployment name: CreateVm-MicrosoftWindowsServer.WindowsS...
Subscription: Visual Studio Enterprise Subscription
Resource group: ServiceEndpointDemo

Start time: 8/28/2022, 9:24:47 AM
Correlation ID: 8647a8dc-b8d8-45ae-a530-63645db2de9b

^ Deployment details

	Resource	Type	Status	Operation details
✓	serviceendpointde254	Microsoft.Network/networkInterfaces	Created	Operation details
✓	serviceendpointdemovm-nsg	Microsoft.Network/networkSecurityGroups	OK	Operation details
✓	serviceendpointdemovm-ip	Microsoft.Network/publicIpAddresses	OK	Operation details



Your deployment is complete

Deployment name: CreateVm-MicrosoftWindowsServer.WindowsS...
Subscription: Visual Studio Enterprise Subscription
Resource group: ServiceEndpointDemo

Start time: 8/28/2022, 9:24:47 AM
Correlation ID: 8647a8dc-b8d8-45ae-a530-63645db2de9b

Deployment details

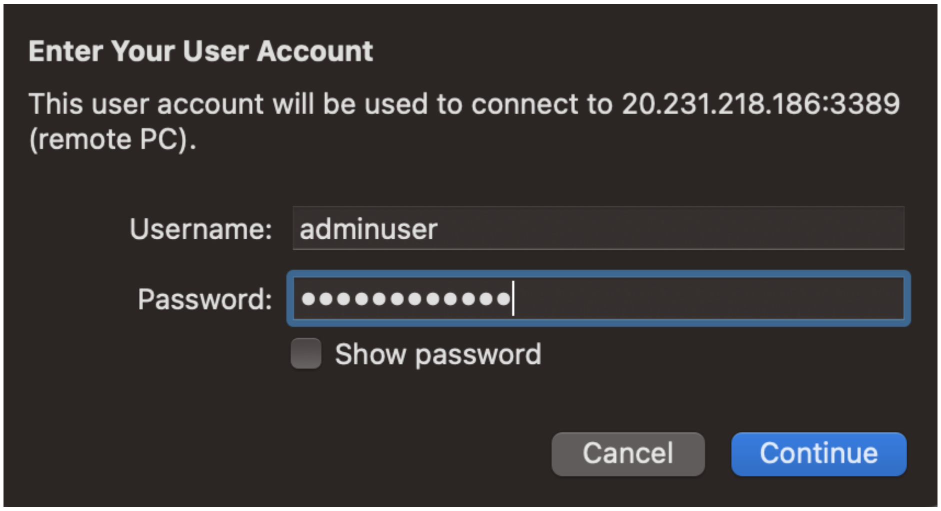
Next steps

Setup auto-shutdown Recommended

Monitor VM health, performance and network dependencies Recommended

Run a script inside the virtual machine Recommended

Now connect to the RDP to check the file server using the username and password.



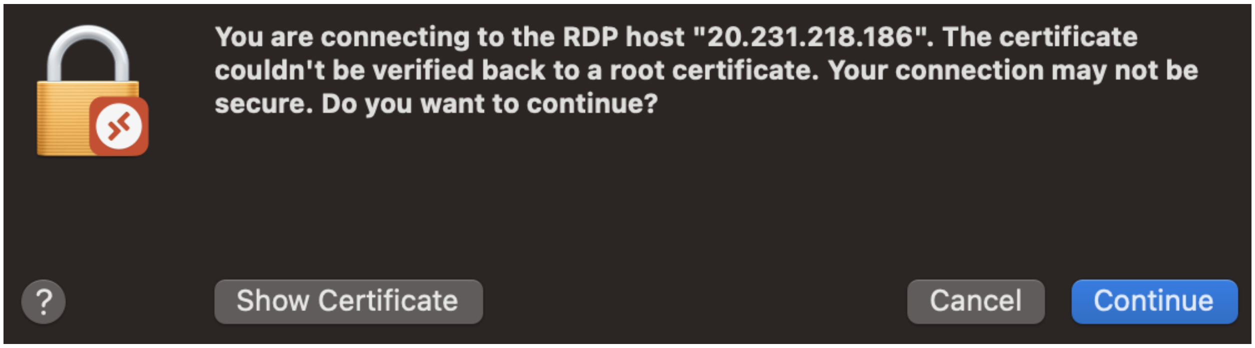
Enter Your User Account

This user account will be used to connect to 20.231.218.186:3389 (remote PC).

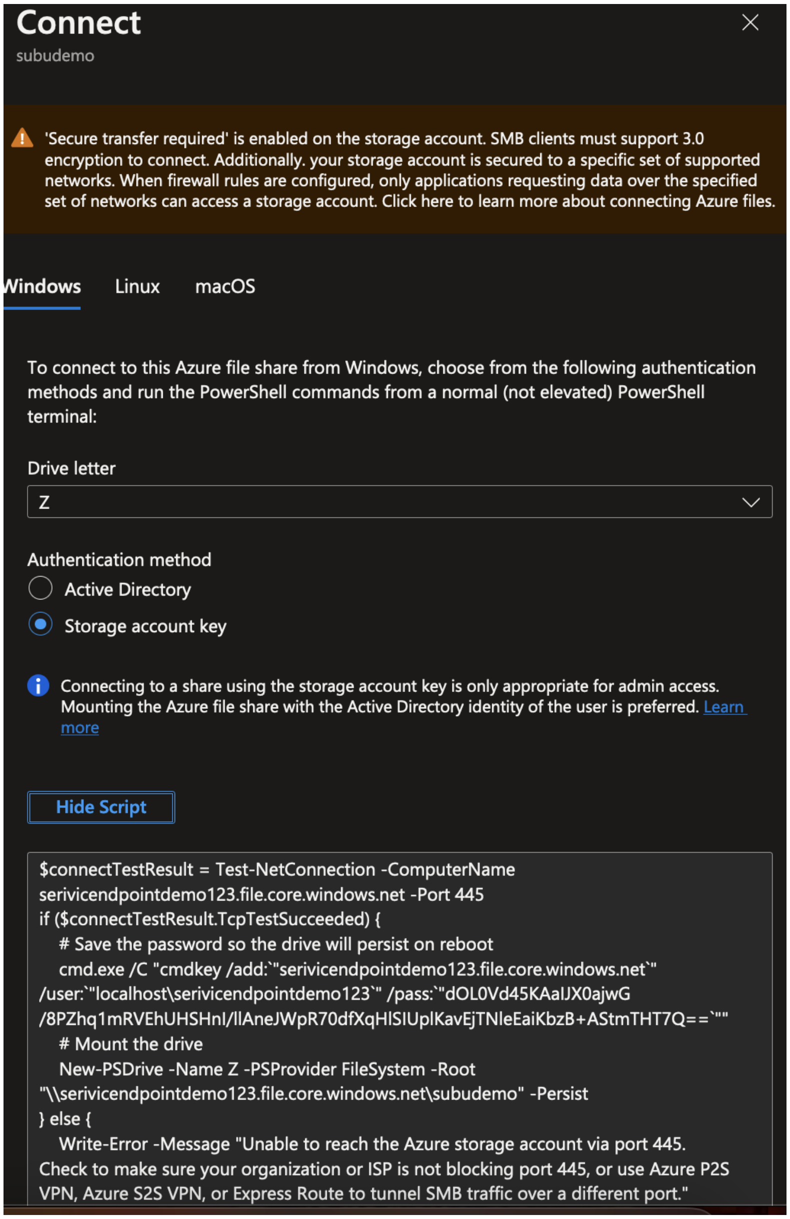
Username: adminuser

Password: ●●●●●●●●●●●●

□ Show password



You are connecting to the RDP host "20.231.218.186". The certificate couldn't be verified back to a root certificate. Your connection may not be secure. Do you want to continue?



Connect

subudemo

'Secure transfer required' is enabled on the storage account. SMB clients must support 3.0 encryption to connect. Additionally. your storage account is secured to a specific set of supported networks. When firewall rules are configured, only applications requesting data over the specified set of networks can access a storage account. Click here to learn more about connecting Azure files.

To connect to this Azure file share from Windows, choose from the following authentication methods and run the PowerShell commands from a normal (not elevated) PowerShell terminal:

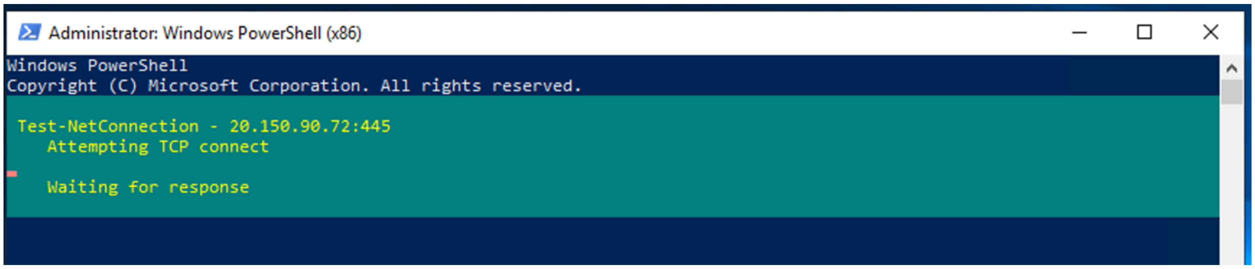
Drive letter: Z

Authentication method
○ Active Directory
● Storage account key

Connecting to a share using the storage account key is only appropriate for admin access. Mounting the Azure file share with the Active Directory identity of the user is preferred. Learn more

```
$connectTestResult = Test-NetConnection -ComputerName
serivicendpointdemo123.file.core.windows.net -Port 445
if ($connectTestResult.TcpTestSucceeded) {
   # Save the password so the drive will persist on reboot
   cmd.exe /C "cmdkey /add:`"serivicendpointdemo123.file.core.windows.net`"
/user:`"localhost\serivicendpointdemo123`" /pass:`"dOL0Vd45KAaIJX0ajwG
/8PZhq1mRVEhUHSHnI/llAneJWpR70dfXqHlSIUplKavEjTNleEaiKbzB+AStmTHT7Q==`""
   # Mount the drive
   New-PSDrive -Name Z -PSProvider FileSystem -Root
"\\serivicendpointdemo123.file.core.windows.net\subudemo" -Persist
} else {
   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, or use Azure P2S
VPN, Azure S2S VPN, or Express Route to tunnel SMB traffic over a different port."
```

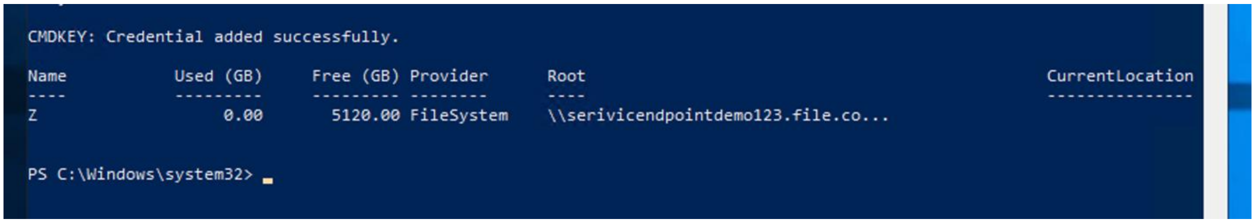
Now in the VM run the PowerShell script to connect the file server since the subnet is on the Vnet created on the subnet which we enabled the service end point.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

 Test-NetConnection - 20.150.90.72:445
    Attempting TCP connect

    Waiting for response
```



```
CMDKEY: Credential added successfully.

Name           Used (GB)     Free (GB) Provider      Root                                               CurrentLocation
----           ---------     --------- --------      ----                                               ---------------
Z                   0.00       5120.00 FileSystem    \\serivicendpointdemo123.file.co...

PS C:\Windows\system32> 
```

So by this we can understand that the Service End point works only for the Subnet where its active and other areas we cannot do it.