Module 3 - Lab 7: Restrict network access to PaaS resources with virtual network service endpoints

Virtual network service endpoints enable you to limit network access to some Azure service resources to a virtual network subnet. You can also remove internet access to the resources. Service endpoints provide direct connection from your virtual network to supported Azure services, allowing you to use your virtual network's private address space to access the Azure services. Traffic destined to Azure resources through service endpoints always stays on the Microsoft Azure backbone network. In this lab, you learn how to:

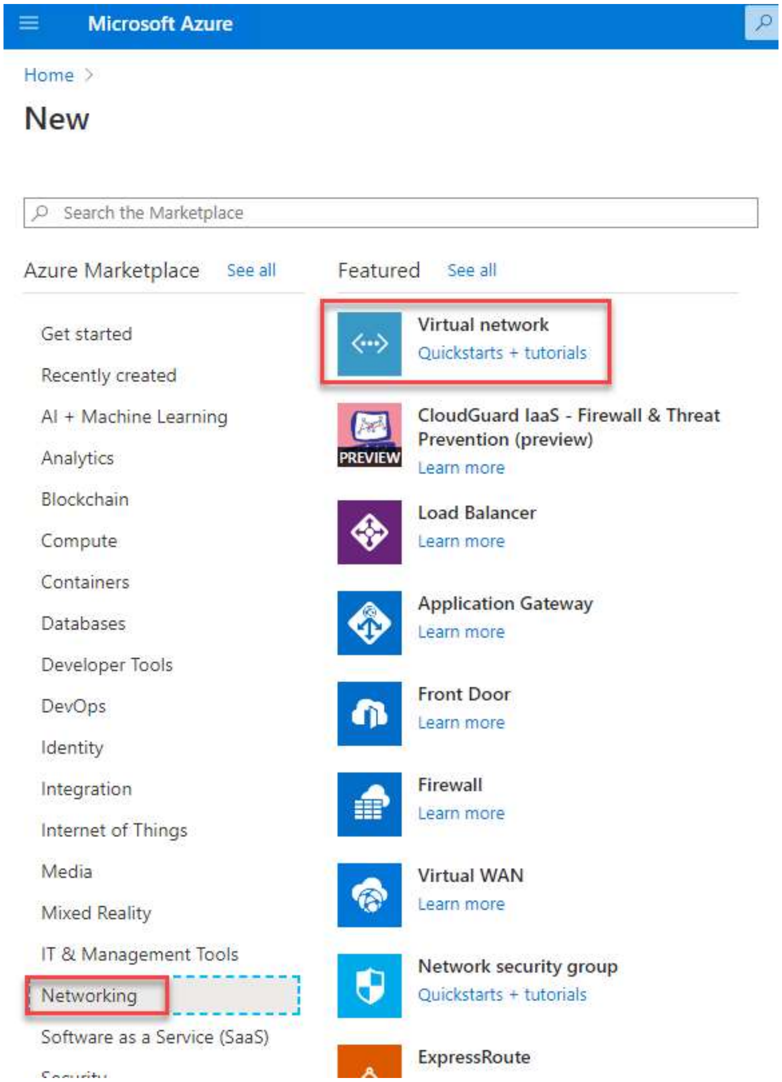
- Create a virtual network with one subnet
- Add a subnet and enable a service endpoint
- Create an Azure resource and allow network access to it from only a subnet
- Deploy a virtual machine (VM) to each subnet
- Confirm access to a resource from a subnet
- Confirm access is denied to a resource from a subnet and the internet

Task 1: Create a virtual network

□ 1. Log in to the Azure portal **https://portal.azure.com** with the username **sheikhnasir5WOVJ@gdcs0.com** and password **vSPRTEL86Al6MxYD**

□ 2. Select **+ Create a resource** on the upper, left corner of the Azure portal.

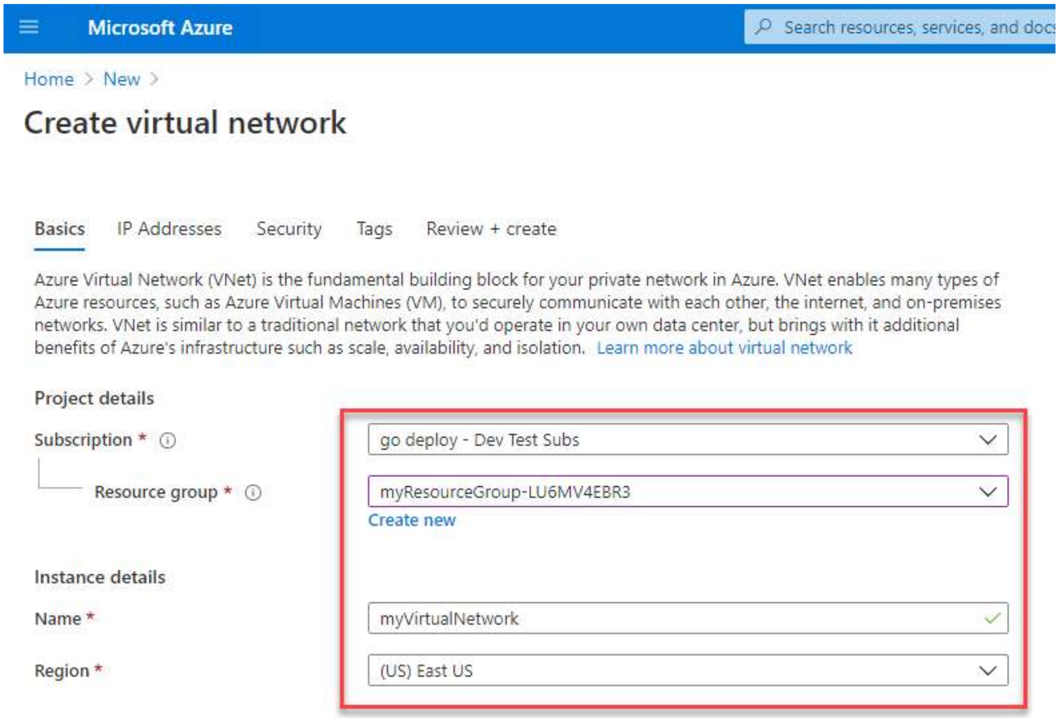
□ 3. Select **Networking**, and then select **Virtual network**.



□ 4. Enter, or select, the following information

Setting	Value
Subscription	Select your subscription
Resource group	Select myResourceGroup
Name	**myVirtualNetwork**

Setting	Value
Location	Select **East US**



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 * : go deploy - Dev Test Subs

Resource group * : myResourceGroup-LU6MV4EBR3

Create new

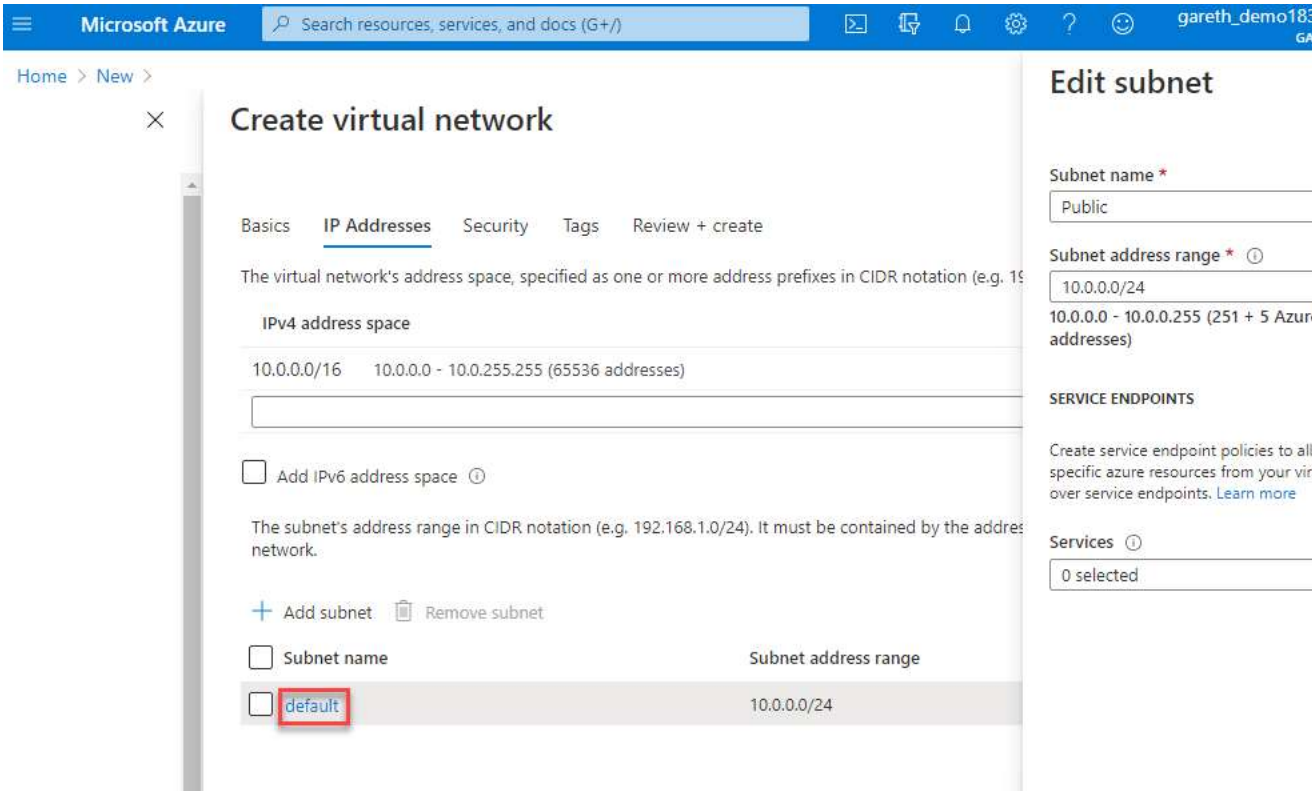
Instance details

Name * : myVirtualNetwork

Region * : (US) East US

Select the **IP Addresses** tab

Setting	Value
Address space	10.0.0.0/16
Subnet Name	Public *(Select the default Subnet name to change)*
Subnet Address range	10.0.0.0/24
Service endpoints	None selected then click **Save**



Create virtual network

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 19

IPv4 address space

10.0.0.0/16 10.0.0.0 - 10.0.255.255 (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 addres network.

□ Subnet name	Subnet address range
□ default	10.0.0.0/24

Edit subnet

Subnet name * : Public

Subnet address range * : 10.0.0.0/24

10.0.0.0 - 10.0.0.255 (251 + 5 Azur addresses)

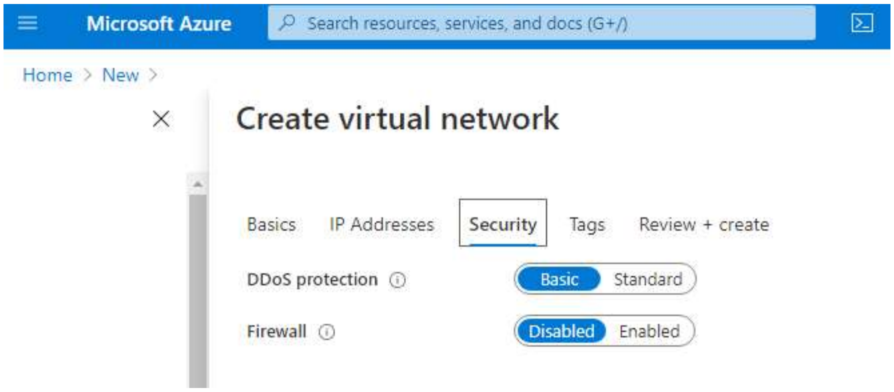
SERVICE ENDPOINTS

Create service endpoint policies to all specific azure resources from your vir over service endpoints. Learn more

Services : 0 selected

Select the **Security** tab

Setting	Value
DDoS protection	Disabled
Firewall	Disabled



Create virtual network

DDoS protection ⓘ [✓ Basic] Standard

Firewall ⓘ [✓ Disabled] Enabled

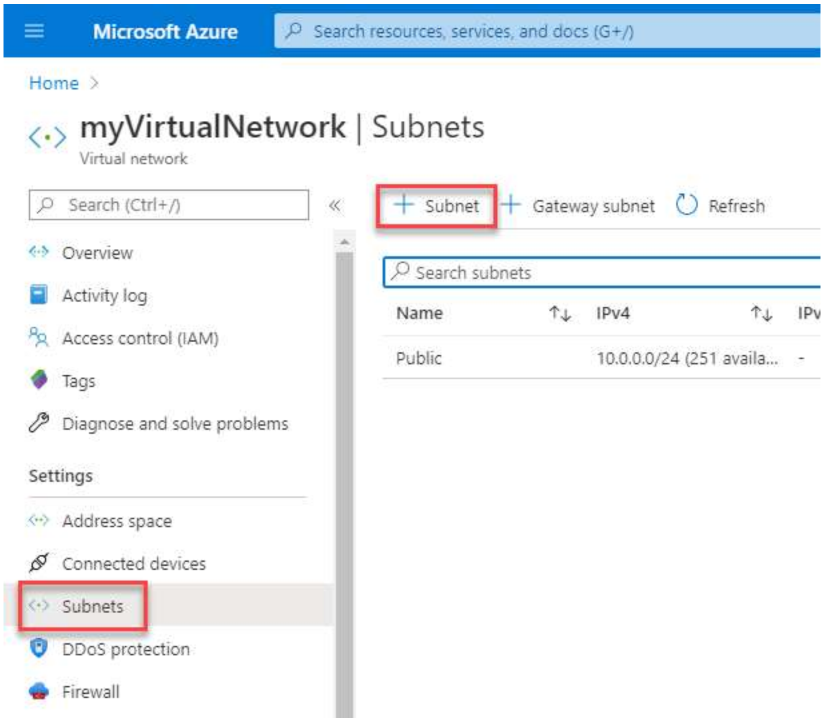
□ 5. Click **Review + create** then select **Create**:

Task 2: Enable a service endpoint

> Service endpoints are enabled per service, per subnet. Create a subnet and enable a service endpoint for the subnet.

□ 1. In the **Search resources, services, and docs** box at the top of the portal, enter **myVirtualNetwork**. When **myVirtualNetwork** appears in the search results, select it.

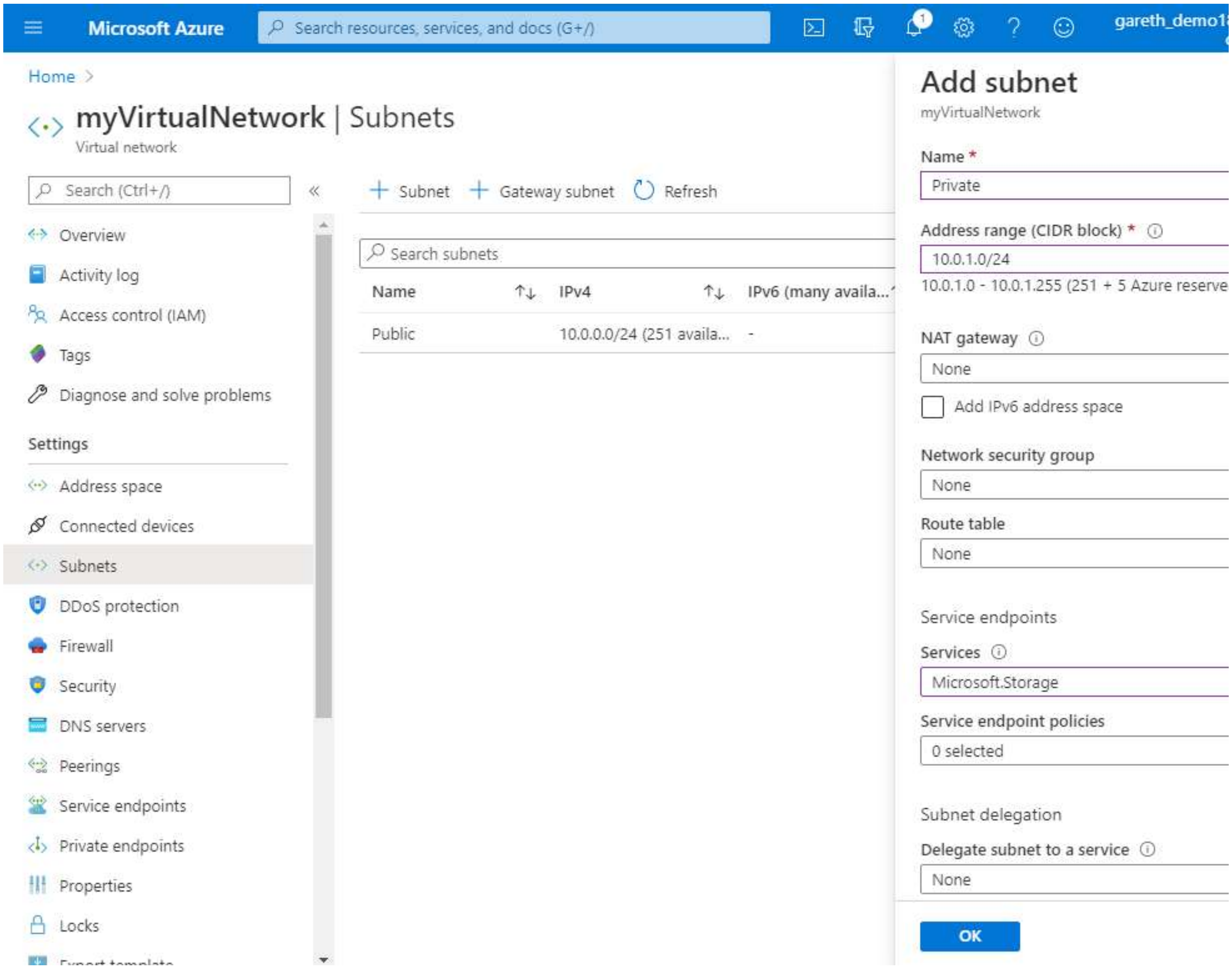
□ 2. Add a subnet to the virtual network. Under **Settings**, select **Subnets**, and then select **+ Subnet**, as shown in the following picture:



Name	IPv4	IPv
Public	10.0.0.0/24 (251 availa...	-

□ 3. Under **Add subnet**, select or enter the following information, and then select **Save**:

Setting	Value
Name	Private
Address range	10.0.1.0/24
Service endpoints	Select **Microsoft.Storage** under **Services**



Name	IPv4	IPv6 (many availa...
Public	10.0.0.0/24 (251 availa...	-

Add subnet

myVirtualNetwork

Name *: Private

Address range (CIDR block) *: 10.0.1.0/24

10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserve

NAT gateway: None

□ Add IPv6 address space

Network security group: None

Route table: None

Service endpoints

Services: Microsoft.Storage

Service endpoint policies: 0 selected

Subnet delegation

Delegate subnet to a service: None

OK

Task 3: Restrict network access for a subnet

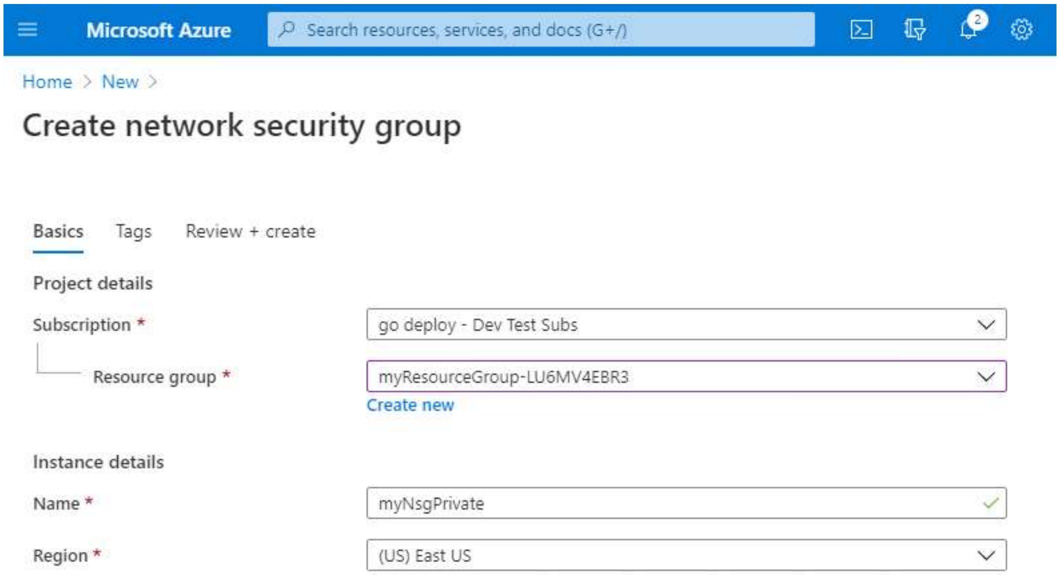
> By default, all VMs in a subnet can communicate with all resources. You can limit communication to and from all resources in a subnet by creating a network security group, and associating it to the subnet.

□ 1. Select **+ Create a resource** on the upper, left corner of the Azure portal.

□ 2. Select **Networking**, and then select **Network security group**.

□ 3. Under **Create a network security group**, enter, or select, the following information, and then click **Review + create** and then select **Create**:

Setting	Value
Subscription	Select your subscription
Resource group	Select myResourceGroup
Name	myNsgPrivate
Location	Select **East US**



Create network security group

Project details

Subscription * go deploy - Dev Test Subs

Resource group * myResourceGroup-LU6MV4EBR3

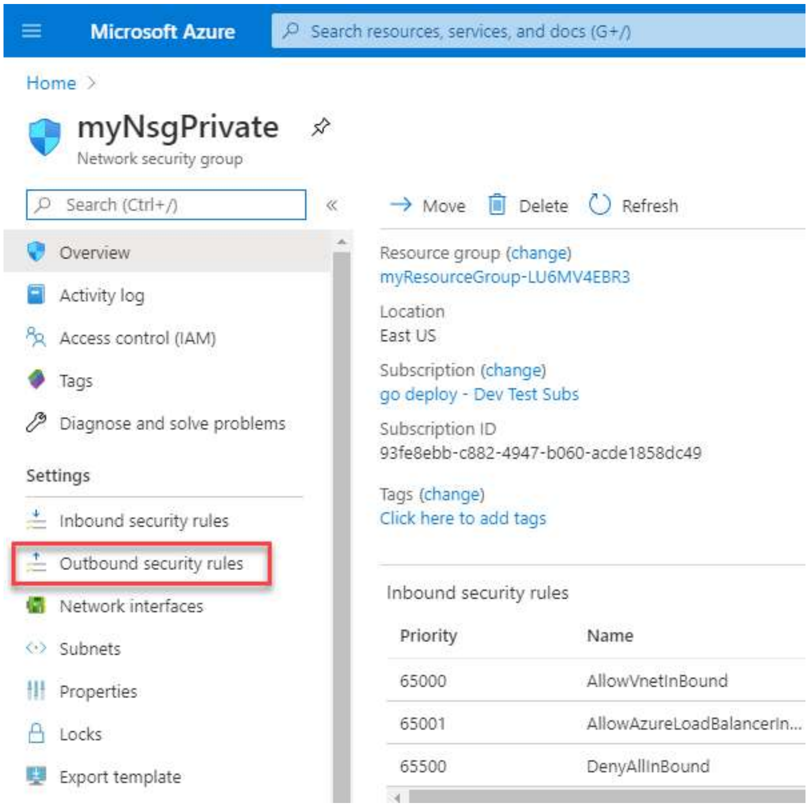
Instance details

Name * myNsgPrivate

Region * (US) East US

□ 4. Wait for the resource to deploy and then select **Go to Resource**.

□ 5. Under **Settings**, select **Outbound security rules**.



myNsgPrivate

Network security group

Resource group (change)
myResourceGroup-LU6MV4EBR3

Location
East US

Subscription (change)
go deploy - Dev Test Subs

Subscription ID
93fe8ebb-c882-4947-b060-acde1858dc49

Tags (change)
Click here to add tags

Inbound security rules

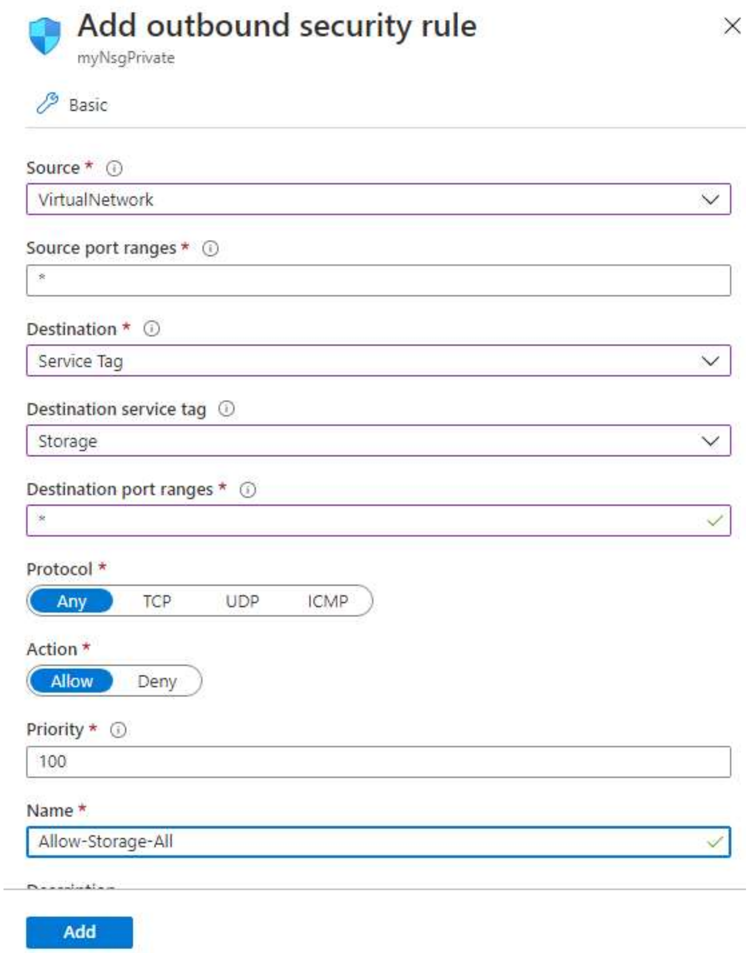
Priority	Name
65000	AllowVnetInBound
65001	AllowAzureLoadBalancerIn...
65500	DenyAllInBound

□ 6. Select **+ Add**.

□ 7. Create a rule that allows outbound communication to the Azure Storage service. Enter, or select, the following information, and then select **Add**:

Setting	Value
Source	Select **VirtualNetwork**
Source port ranges	*
Destination	Select **Service Tag**
Destination service tag	Select **Storage**
Destination port ranges	*
Protocol	Any
Action	Allow

Setting	Value
Priority	100
Name	Allow-Storage-All



Add outbound security rule

myNsgPrivate

Basic

Source * : VirtualNetwork

Source port ranges * : *

Destination * : Service Tag

Destination service tag : Storage

Destination port ranges * : *

Protocol * : [✓ Any] TCP UDP ICMP

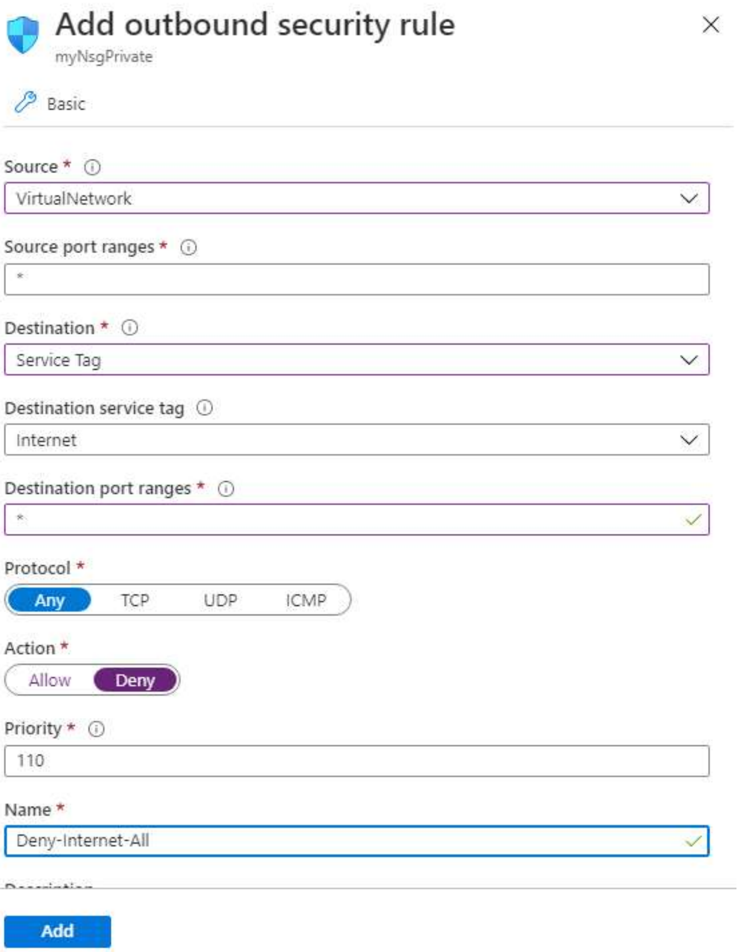
Action * : [✓ Allow] Deny

Priority * : 100

Name * : Allow-Storage-All

□ 8. Create another outbound security rule that denies communication to the internet. This rule overrides a default rule in all network security groups that allows outbound internet communication. Complete steps 5-7 again, using the following values:

Setting	Value
Source	Select **VirtualNetwork**
Source port ranges	*
Destination	Select **Service Tag**
Destination service tag	Select **Internet**
Destination port ranges	*
Protocol	Any
Action	Deny
Priority	110
Name	Deny-Internet-All



Add outbound security rule

myNsgPrivate

Basic

Source * VirtualNetwork

Source port ranges * *

Destination * Service Tag

Destination service tag Internet

Destination port ranges * *

Protocol * [✓ Any] TCP UDP ICMP

Action * Allow [✓ Deny]

Priority * 110

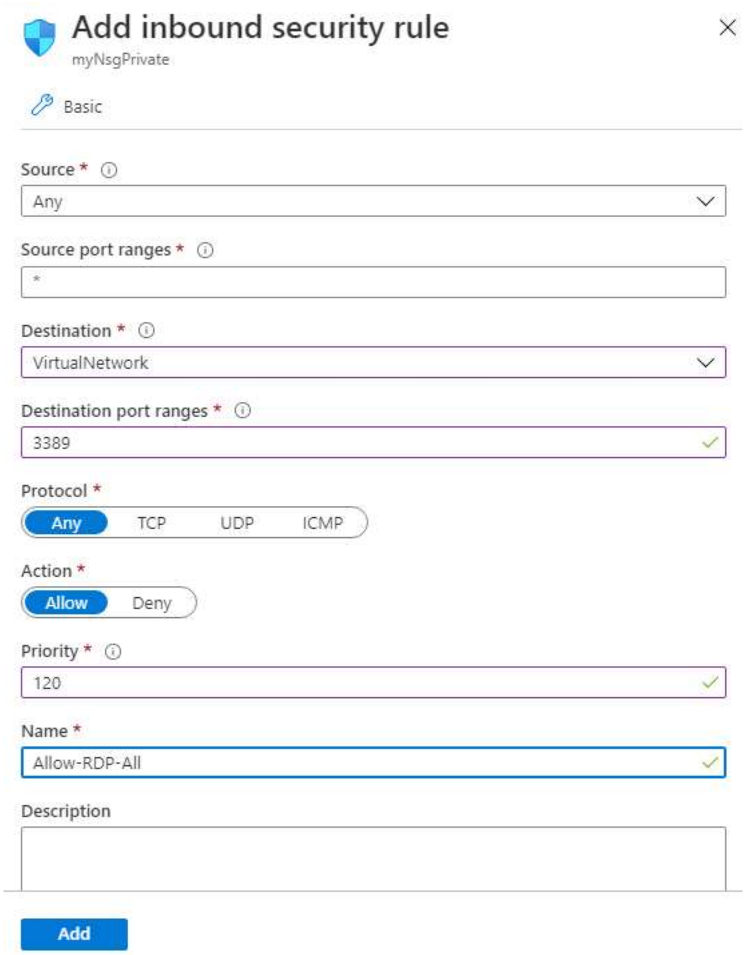
Name * Deny-Internet-All

□ 9. Under **Settings**, select **Inbound security rules**.

□ 10. Select **+ Add**.

□ 11. Create an inbound security rule that allows Remote Desktop Protocol (RDP) traffic to the subnet from anywhere. The rule overrides a default security rule that denies all inbound traffic from the internet. Remote desktop connections are allowed to the subnet so that connectivity can be tested in a later step. Under **Settings**, select **Inbound security rules**, select **+Add**, enter the following values, and then select **Add**:

Setting	**Value**
Source	Any
Source port ranges	*
Destination	Select **VirtualNetwork**
Destination port ranges	3389
Protocol	Any
Action	Allow
Priority	120
Name	**Allow-RDP-All**


Add inbound security rule
myNsgPrivate

Basic

Source * Any

Source port ranges * *

Destination * VirtualNetwork

Destination port ranges * 3389

Protocol * ● Any ○ TCP ○ UDP ○ ICMP

Action * ● Allow ○ Deny

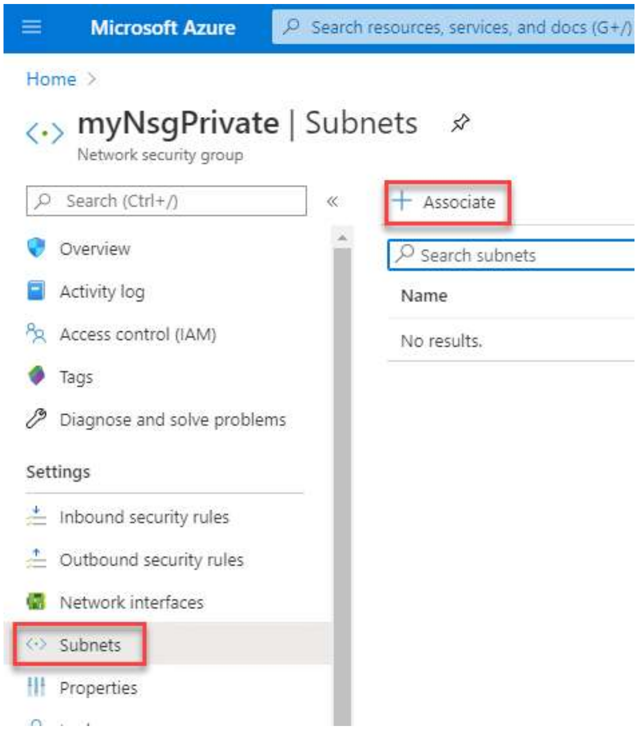
Priority * 120

Name * Allow-RDP-All

Description

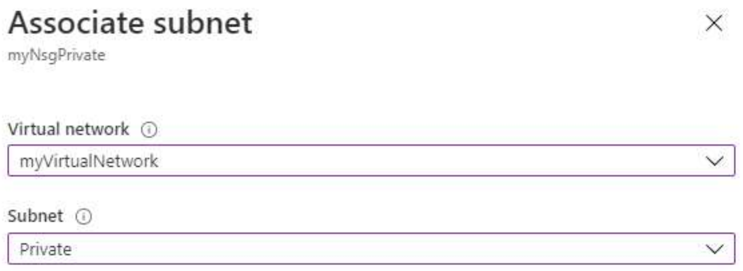
□ 12. Under **Settings**, select **Subnets**.

□ 13. Select **+ Associate**



□ 14. Under **Associate subnet**, select **Virtual network** and then select **myVirtualNetwork** under **Choose a virtual network**.

□ 15. Under **Choose subnet**, select **Private**, and then select **OK**.



Associate subnet

myNsgPrivate

Virtual network ⓘ

myVirtualNetwork

Subnet ⓘ

Private

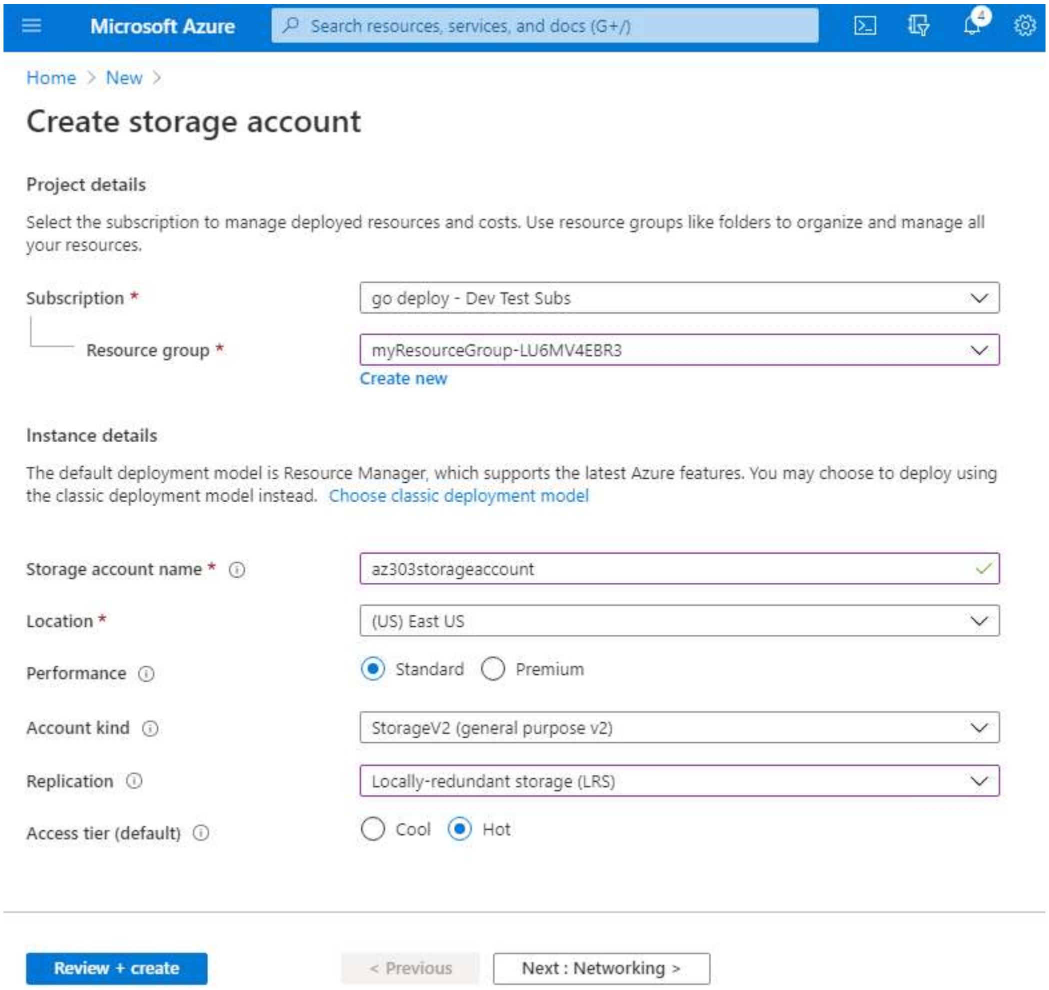
Task 4: Restrict network access to a resource

> The steps necessary to restrict network access to resources created through Azure services enabled for service endpoints varies across services. See the documentation for individual services for specific steps for each service. The remainder of this tutorial includes steps to restrict network access for an Azure Storage account, as an example.

□ 1. . In the **Search resources, services, and docs** search engine at the top of the azure portal, enter **storage accounts** and select it.

□ 2. Select **+Create** and Enter, or select, the following information, accept the remaining defaults, and then click **Review + create** and then select **Create**:

Setting	Value
Subscription	Select your subscription
Resource group	Select **Use existing** and select myResourceGroup
Name	Enter a name that is unique across all Azure locations, between 3-24 characters in length, using only numbers and lower-case letters.
Performance	Standard (general purpose v2)
Region	Select **East US**
Redundancy	Locally-redundant storage (LRS)



Create storage account

Project details

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

Subscription * : go deploy - Dev Test Subs

Resource group * : myResourceGroup-LU6MV4EBR3

Create new

Instance details

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. Choose classic deployment model

Storage account name * ⓘ : az303storageaccount

Location * : (US) East US

Performance ⓘ : ● Standard ○ Premium

Account kind ⓘ : StorageV2 (general purpose v2)

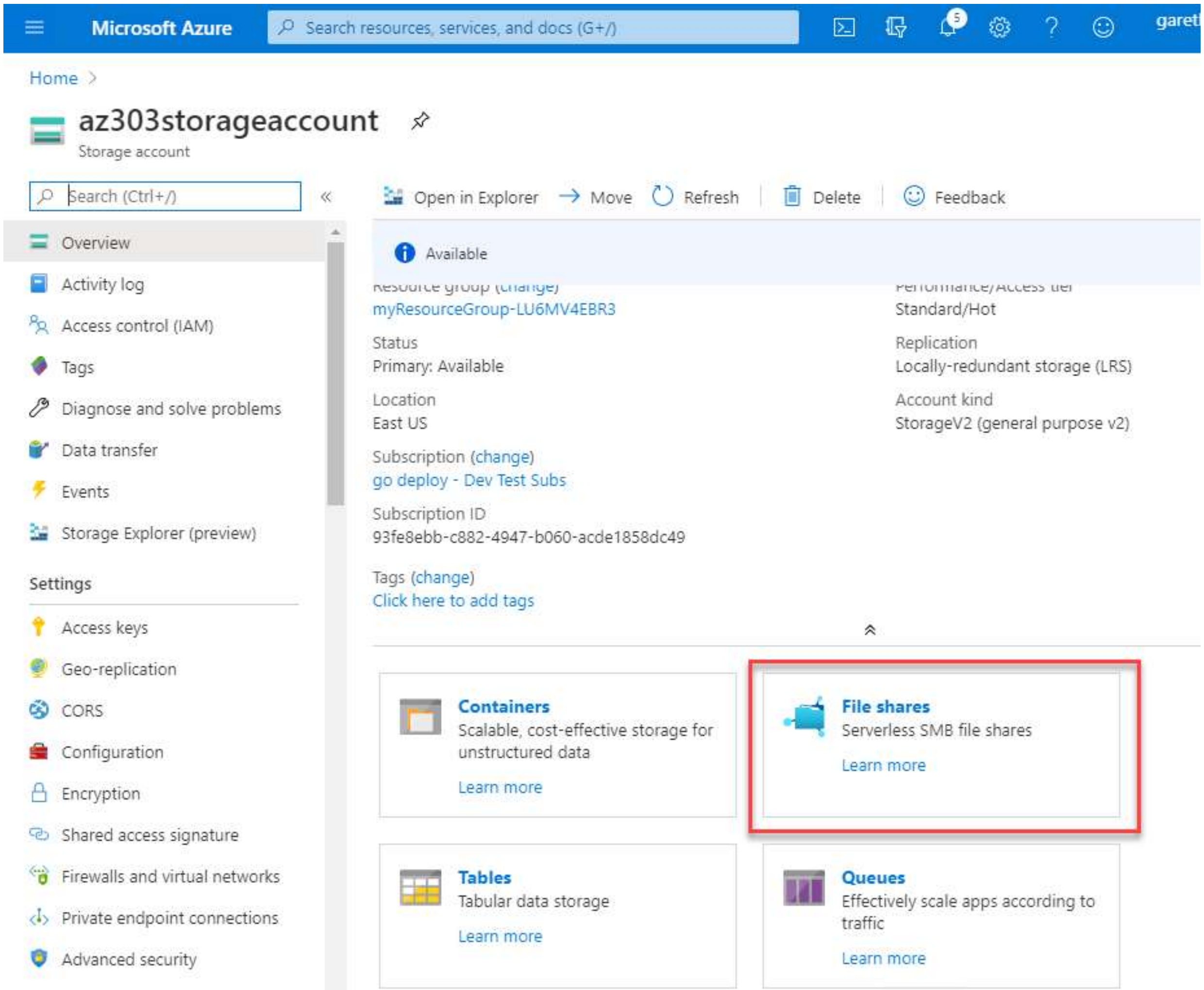
Replication ⓘ : Locally-redundant storage (LRS)

Access tier (default) ⓘ : ○ Cool ● Hot

Task 5: Create a file share in the storage account

□ 1. Wait for the resource to deploy and then select **Go to resource**

□ 2. Select **File shares**, as shown in the following picture:



Resource group (change)
myResourceGroup-LU6MV4EBR3

Status
Primary: Available

Location
East US

Subscription (change)
go deploy - Dev Test Subs

Subscription ID
93fe8ebb-c882-4947-b060-acde1858dc49

Tags (change)
Click here to add tags

Performance/Access tier
Standard/Hot

Replication
Locally-redundant storage (LRS)

Account kind
StorageV2 (general purpose v2)

Containers
Scalable, cost-effective storage for unstructured data
Learn more

File shares
Serverless SMB file shares
Learn more

Tables
Tabular data storage
Learn more

Queues
Effectively scale apps according to traffic
Learn more

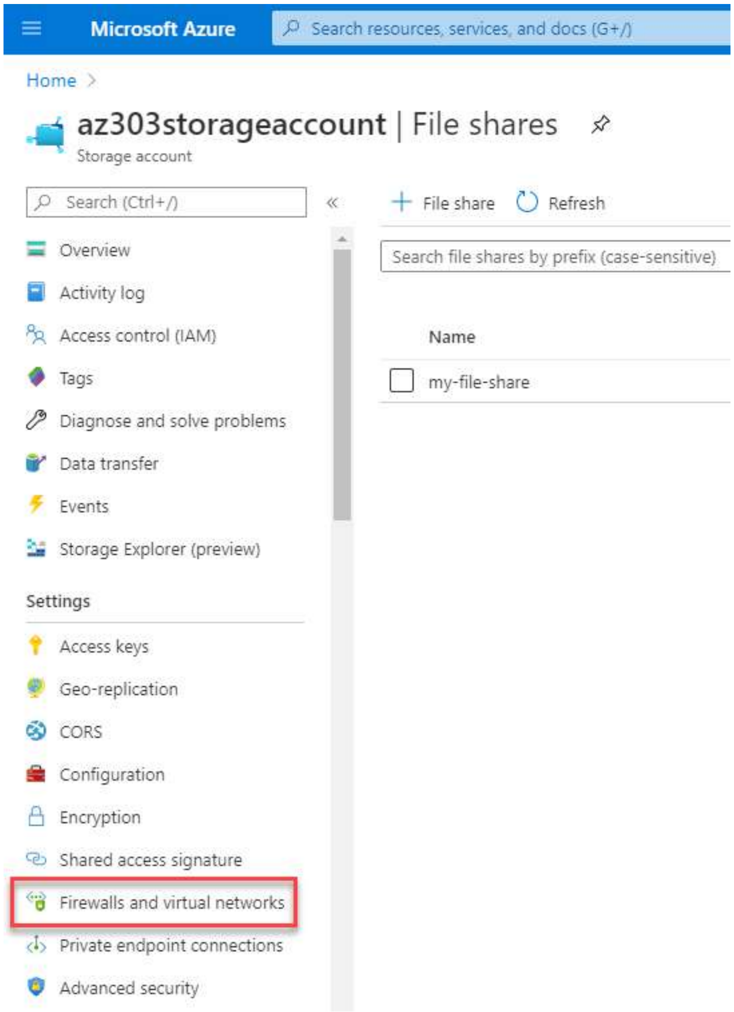
□ 3. Select **+ File share**.

□ 4. Enter my-file-share under **Name**, and then select **Create**.

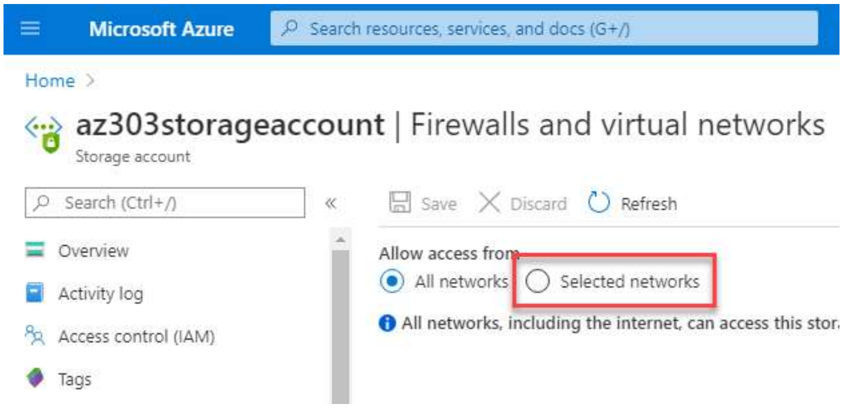
Task 6: Restrict network access to a subnet

By default, storage accounts accept network connections from clients in any network, including the internet. Deny network access from the internet, and all other subnets in all virtual networks, except for the *Private* subnet in the *myVirtualNetwork* virtual network.

□ 1. Under **Security + networking** for the storage account, select **Networking**.



□ 2. Select **Selected networks**.

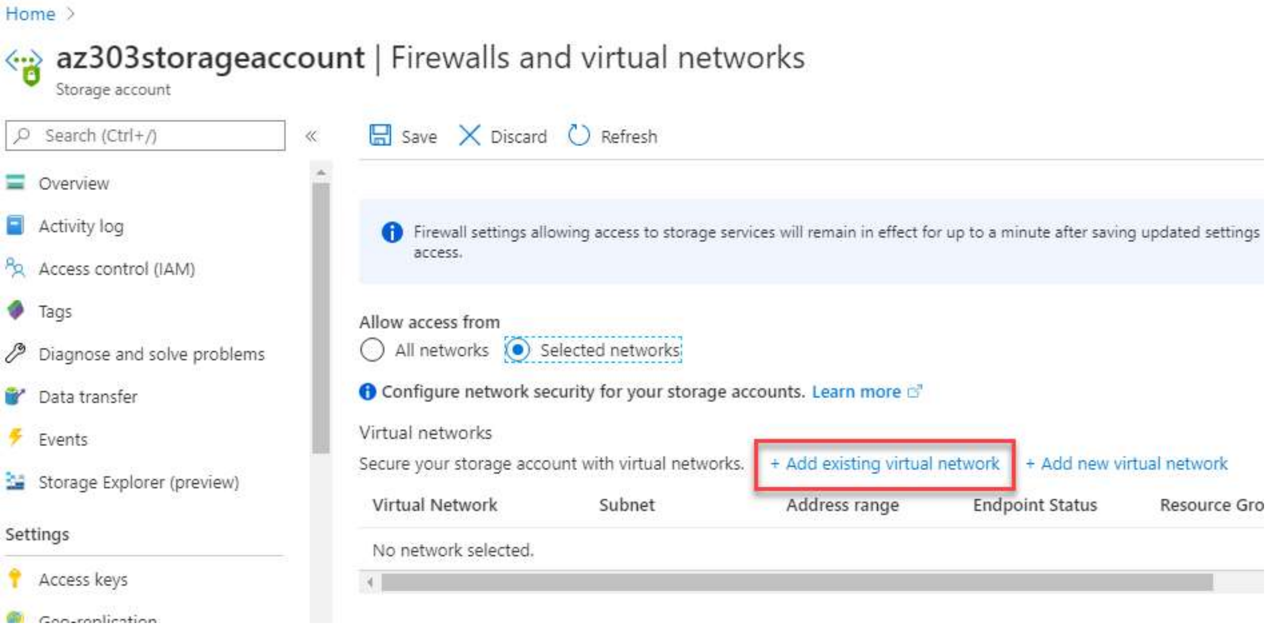


Allow access from

● All networks ○ Selected networks

All networks, including the internet, can access this stor

□ 3. Select **+ Add existing virtual network**.



az303storageaccount | Firewalls and virtual networks

Storage account

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

Allow access from

○ All networks ● Selected networks

Configure network security for your storage accounts. Learn more

Virtual networks

Secure your storage account with virtual networks. + Add existing virtual network + Add new virtual network

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

□ 4. Under **Add networks**, select the following values, and then select **Add**:

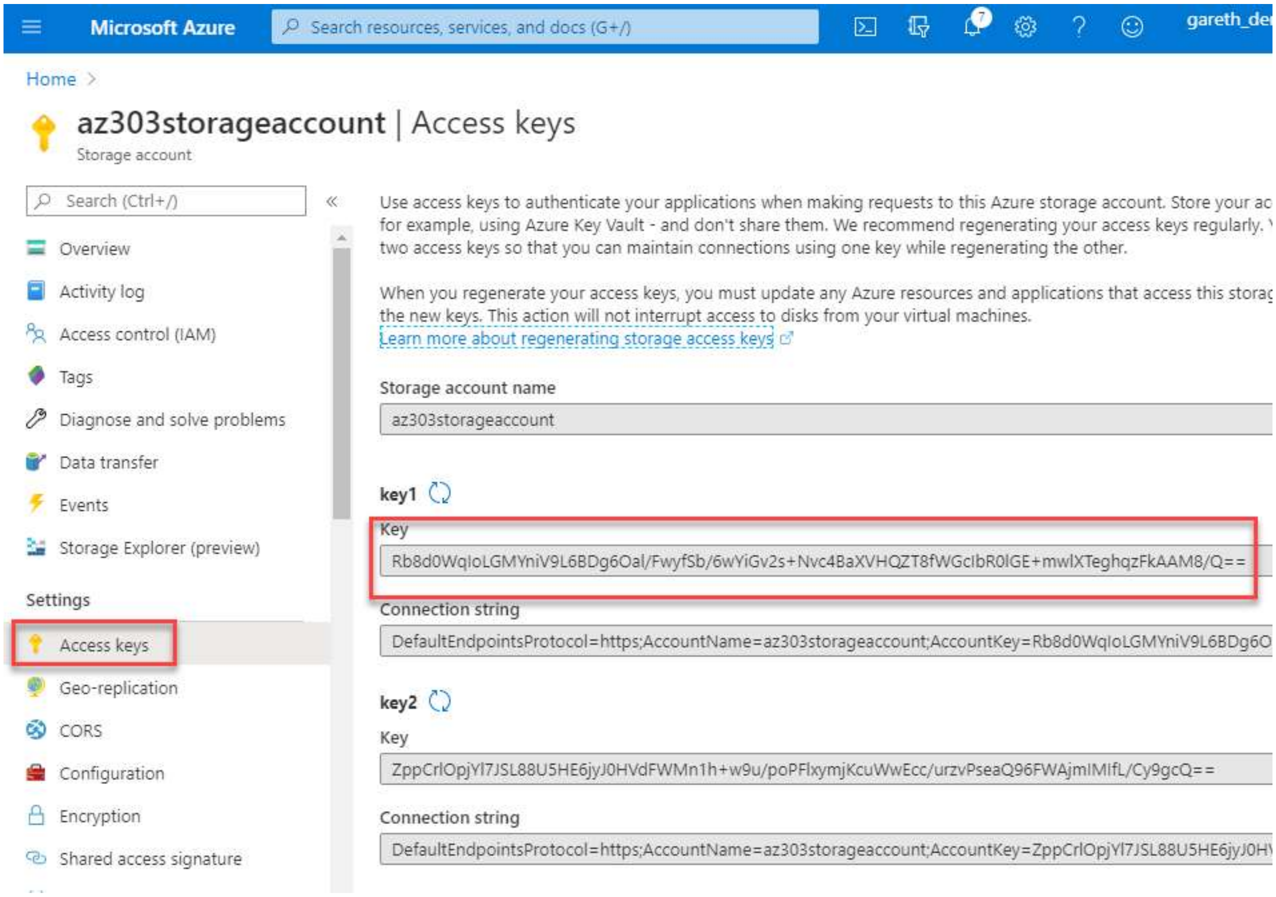
Setting	Value
Subscription	Select your subscription.
Virtual networks	Select **myVirtualNetwork**, under **Virtual networks**
Subnets	Select **Private**, under **Subnets**

□ 5. Select **Save**.

□ 6. Close the **Firewalls and virtual networks** box.

□ 7. Under **SETTINGS** for the storage account, select **Access keys**, as shown in the following picture:

□ 8. Note the **Key** value, as you'll have to manually enter it in a later step when mapping the file share to a drive letter in a VM.



az303storageaccount | Access keys

Storage account

Use access keys to authenticate your applications when making requests to this Azure storage account. Store your ac for example, using Azure Key Vault - and don't share them. We recommend regenerating your access keys regularly. two access keys so that you can maintain connections using one key while regenerating the other.

When you regenerate your access keys, you must update any Azure resources and applications that access this storag the new keys. This action will not interrupt access to disks from your virtual machines.

Learn more about regenerating storage access keys

Storage account name: az303storageaccount

key1

Key: Rb8d0WqIoLGMYniV9L6BDg6Oal/FwyfSb/6wYiGv2s+Nvc4BaXVHQZT8fWGcIbR0lGE+mwlXTeghqzFkAAM8/Q==

Connection string: DefaultEndpointsProtocol=https;AccountName=az303storageaccount;AccountKey=Rb8d0WqIoLGMYniV9L6BDg6O

key2

Key: ZppCrlOpjYl7JSL88U5HE6jyJ0HVdFWMn1h+w9u/poPFlxymjKcuWwEcc/urzvPseaQ96FWAjmIMIfL/Cy9gcQ==

Connection string: DefaultEndpointsProtocol=https;AccountName=az303storageaccount;AccountKey=ZppCrlOpjYl7JSL88U5HE6jyJ0H

Task 7: Create virtual machines

> To test network access to a storage account, deploy a VM to each subnet.

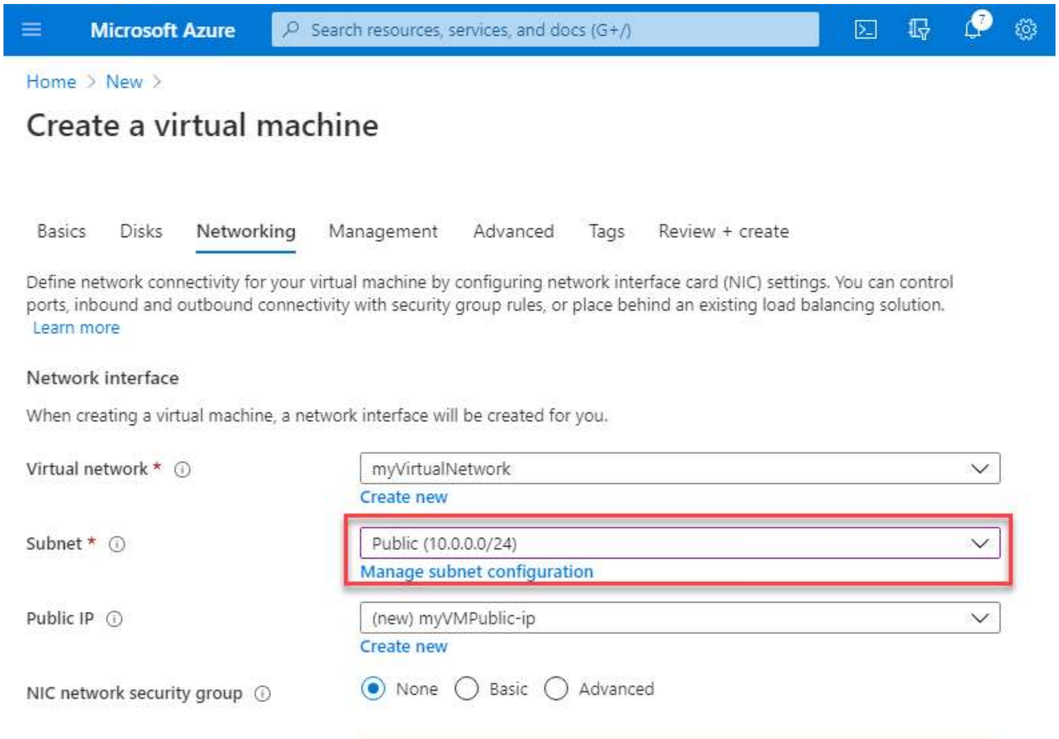
☐ 1. Select **+ Create a resource** found on the upper, left corner of the Azure portal.

☐ 2. Select **Compute**, and then select **Virtual Machine**.

☐ 3. Enter, or select, the following information and then select **OK**:

Setting	Value
Subscription	Select your subscription.
Resource group	Select myResourceGroup
Name	**myVmPublic**
Location	Select **East US**.
Image	**Windows Server 2016 Datacenter Gen2**.
User name	**localadmin**
Password	**vSPRTEL86Al6MxYD**

☐ 4. Select the **Networking** tab and then select **myVirtualNetwork**. Then select **Subnet**, and select **Public**, as shown in the following picture:



Create a virtual machine

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.

Network interface

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

Virtual network * : myVirtualNetwork

Subnet * : Public (10.0.0.0/24)

Public IP : (new) myVMPublic-ip

NIC network security group : ● None ○ Basic ○ Advanced

☐ 5. Under **NIC Network Security Group**, select **Advanced**. The portal automatically creates a network security group for you that allows port 3389, which you'll need open to connect to the virtual machine in a later step. Click **Review + create**.

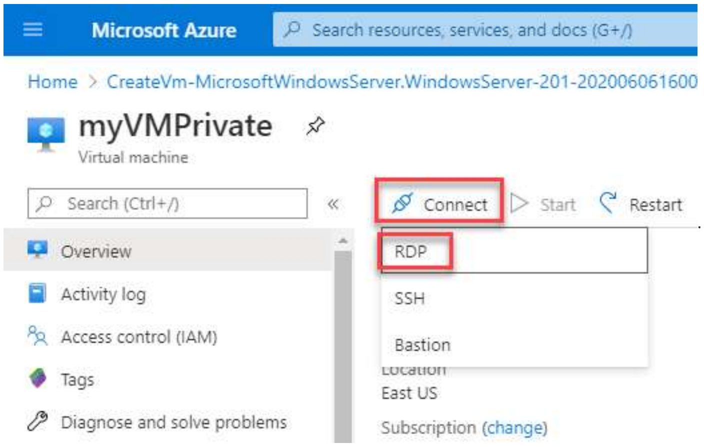
☐ 6. On the **Review** page, select **Create** to start the virtual machine deployment. The VM takes a few minutes to deploy, but you can continue to the next step while the VM is creating.

☐ 7. Complete steps 1-7 again, but in step 3, name the virtual machine **myVmPrivate** and in step 5, select the **Private** subnet and **None** for **NIC Network Security Groups**

> ⚠ **Note**: The VM takes a few minutes to deploy. Do not continue to the next step until it finishes creating and its settings open in the portal.

Task 8: Create the second virtual machine

☐ 1. Once the *myVmPrivate* VM finishes creating, Azure opens the settings for it. Connect to the VM by selecting the **Connect** button and selecting **RDP**, as shown in the following picture:



□ 2. After selecting the **Connect > RDP** button, click **Download RDP File** and a Remote Desktop Protocol (.rdp) file is created and downloaded to your computer.

□ 3. Open the downloaded rdp file. If prompted, select **Connect**. Enter the user name **localadmin** and password **vSPRTEL86AI6MxYD**

□ 4. Select **OK**.

□ 5. You may receive a certificate warning during the sign-in process. If you receive the warning, select **Yes** or **Continue**, to proceed with the connection.

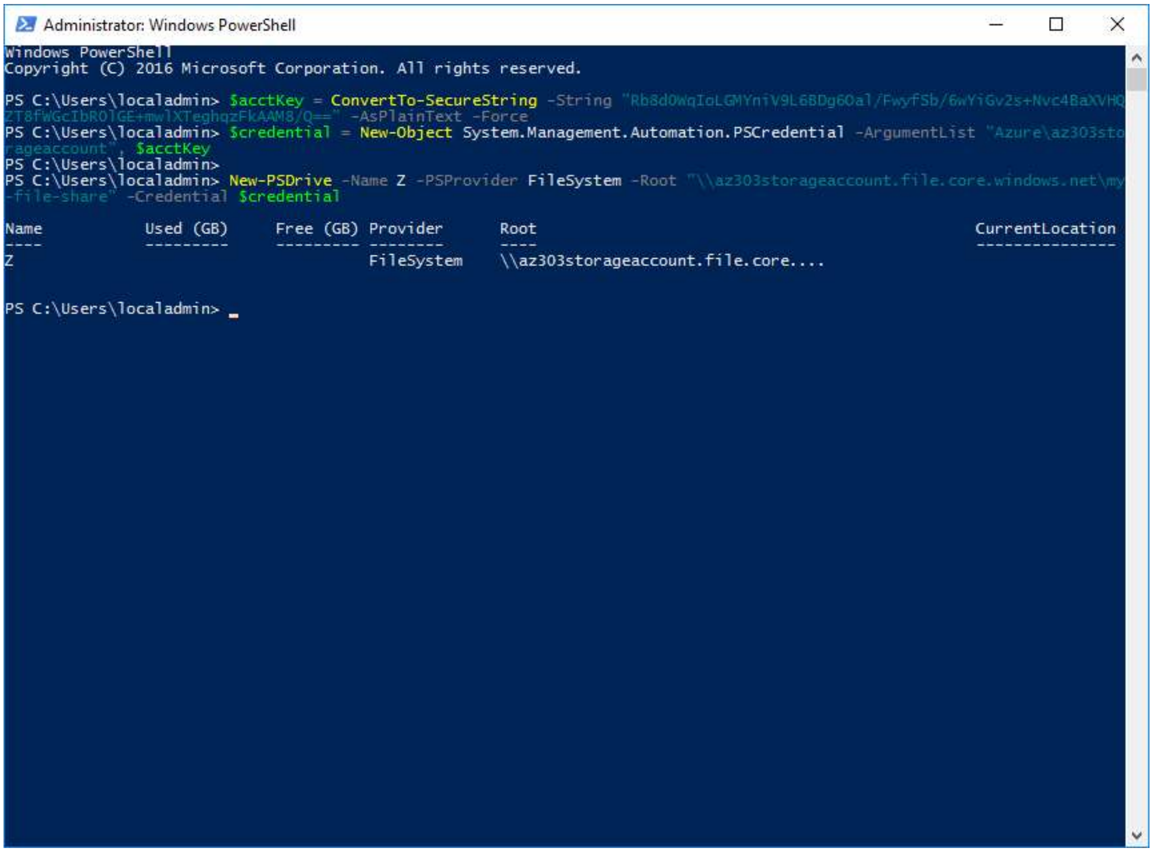
□ 6. On the *myVmPrivate* VM, map the Azure file share to drive Z using PowerShell ISE. Before running the commands that follow, replace <storage-account-key> and storage-account-name with values you supplied and retrieved in the Create a storage account task.

```
$acctKey = ConvertTo-SecureString -String "<storage-account-key>" -AsPlainText -Force
$credential = New-Object System.Management.Automation.PSCredential -ArgumentList "Azure\storage-account-name", $acctKey
New-PSDrive -Name Z -PSProvider FileSystem -Root "\\storage-account-name.file.core.windows.net\my-file-share" -Credential $credential
```

PowerShell returns output similar to the following example output:

```
Name           Used (GB)     Free (GB) Provider      Root
----           ---------     --------- --------      ----
Z                                      FileSystem    \\vnt.file.core.windows.net\my-f...
```

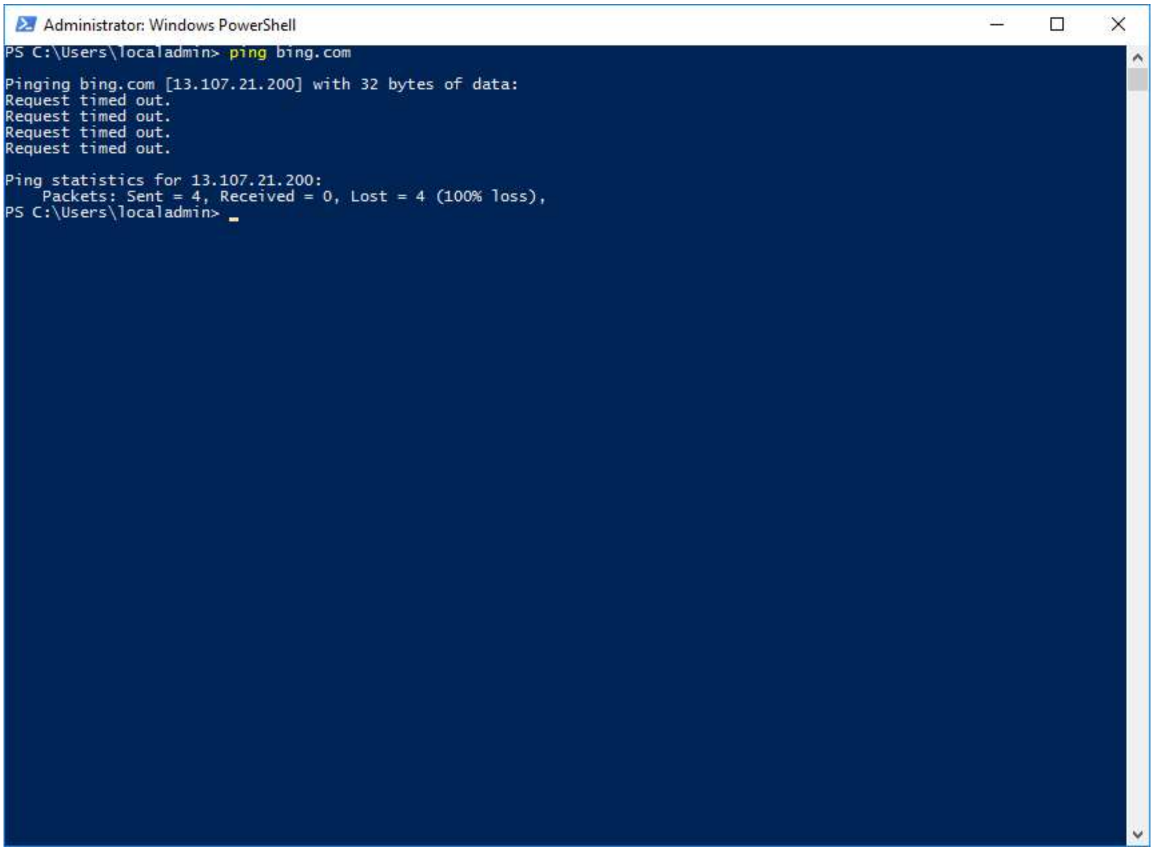
The Azure file share successfully mapped to the Z drive.



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\localadmin> $acctKey = ConvertTo-SecureString -String "Rb8d0WqIoLGMYniV9L6BDg6Oal/FwyfSb/6wYiGv2s+Nvc4BaXVHQ
ZT8fWGcIbR0lGE+mwlXTeghqzFkAAM8/Q==" -AsPlainText -Force
PS C:\Users\localadmin> $credential = New-Object System.Management.Automation.PSCredential -ArgumentList "Azure\az303sto
rageaccount", $acctKey
PS C:\Users\localadmin>
PS C:\Users\localadmin> New-PSDrive -Name Z -PSProvider FileSystem -Root "\\az303storageaccount.file.core.windows.net\my
-file-share" -Credential $credential

Name           Used (GB)     Free (GB) Provider      Root                                               CurrentLocation
----           ---------     --------- --------      ----                                               ---------------
Z                                      FileSystem    \\az303storageaccount.file.core....


PS C:\Users\localadmin> _
```

□ 7. Confirm that the VM has no outbound connectivity to the internet from a command prompt: **ping bing.com**

You receive no replies, because the network security group associated to the *Private* subnet does not allow outbound access to the internet.



```
PS C:\Users\localadmin> ping bing.com

Pinging bing.com [13.107.21.200] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 13.107.21.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\localadmin> _
```

☐ 8. Close the remote desktop session to the *myVmPrivate* VM.

Task 9: Confirm access is denied to storage account

☐ 1. Enter *myVmPublic* In the **Search resources, services, and docs** box at the top of the portal.

☐ 2. When **myVmPublic** appears in the search results, select it.

☐ 3. Complete steps 1-6 in the previous task for the *myVmPublic* VM.

After a short wait, you receive a `New-PSDrive : Access is denied` error. Access is denied because the *myVmPublic* VM is deployed in the *Public* subnet. The *Public* subnet does not have a service endpoint enabled for Azure Storage. The storage account only allows network access from the *Private* subnet, not the *Public* subnet.

☐ 4. Close the remote desktop session to the *myVmPublic* VM.

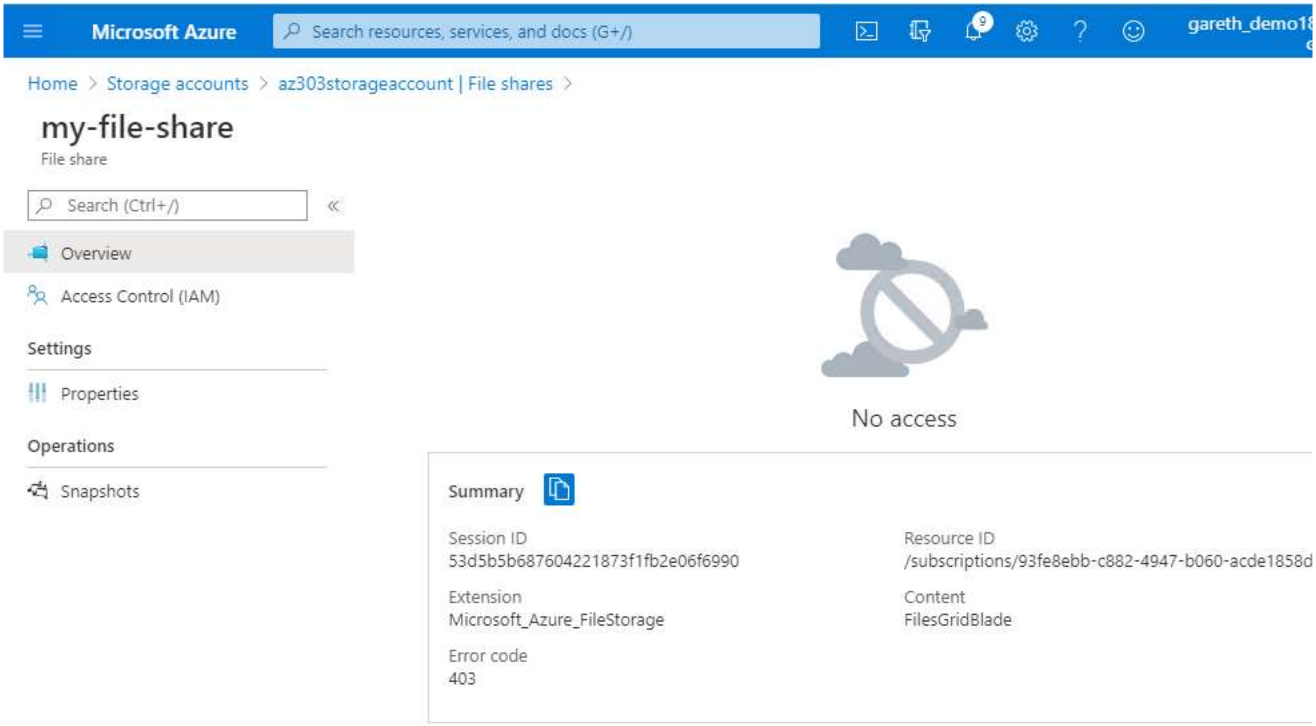
☐ 5. From your computer, browse to the Azure portal **https://portal.azure.com**

☐ 6. Enter the name of the storage account you created in the **Search resources, services, and docs** box. When the name of your storage account appears in the search results, select it.

☐ 7. Select **Files Shares**.

☐ 8. You receive the error shown in the following picture:

Access is denied, because your computer is not in the *Private* subnet of the *MyVirtualNetwork* virtual network.



No access

Summary

Session ID
53d5b5b687604221873f1fb2e06f6990

Resource ID
/subscriptions/93fe8ebb-c882-4947-b060-acde1858d

Extension
Microsoft_Azure_FileStorage

Content
FilesGridBlade

Error code
403