Microsoft Cloud Workshop

Traffic Routing & Network Security

Hands-on lab step-by-step

August 2018

Traffic Routing & Network Security hands-on lab step-by-step

Abstract and learning objectives

The student will build a series of resources that will present a logical network, covering Azure native networking services in Azure. All step-by-step configurations will be done via the portal to build familiarity.

Attendees will be better able to understand all the proper technical terminology surrounding Azure Networking as well as design robust networking in Azure.

Networking References

1) Azure Virtual Network Overview
2) Azure Virtual Network FAQ
3) IP Addresses
    a. Public IP Addresses
    b. Internal IP Addresses
4) DNS
    a. Azure DNS
    b. Name Resolution for Azure VNets
5) Connectivity for Azure Virtual Networks
    a. Site-to-Site VPN
    b. VNet-to-VNet VPN
    c. Point-to-Site VPN
    d. Regional VNet Peering
    e. Global VNet Peering
    f. ExpressRoute Overview
6) Load Balancers
    a. Azure Load Balancer
    b. Azure Traffic Manager
    c. Azure Application Gateway
7) Network Security Strategies
    a. DMZ Between Azure and On-Premises
    b. DMZ Between Azure and the Internet
    c. Network Security Groups
    d. User Defined Routes
    e. Virtual Network Service Tunneling
    f. Web Application Firewall
    g. Service Endpoints
    h. Network Virtual Appliances
8) Monitoring
    a. Network Watcher
    b. Network Performance Monitor Overview & Solution
    c. ExpressRoute Monitor
    d. DNS Analytics
    e. Service Endpoint Monitoring

Filter Network Traffic with a Network Security Group

Task 1: Create a Virtual Network

1. Select **+ Create a resource** on the upper, left corner of the Azure portal.
2. Select **Networking**, and then select **Virtual network**.
3. Enter, or select, the following information, accept the defaults for the remaining settings, and then select **Create**:

Setting	**Value**
Name	myVirtualNetwork
Address space	10.0.0.0/16
Subscription	Select your subscription.
Resource group	Select **Create new** and enter *myResourceGroup*.
Location	Select **East US**.
Subnet- Name	mySubnet
Subnet - Address range	10.0.0.0/24

Task 2: Create Application Security Groups

An application security group enables you to group together servers with similar functions, such as web servers.

1. Select **+ Create a resource** on the upper, left corner of the Azure portal.
2. In the **Search the Marketplace** box, enter *Application security group*. When **Application security group** appears in the search results, select it, select **Application security group** again under **Everything**, and then select **Create**.
3. Enter, or select, the following information, and then select **Create**:

Setting	**Value**
Name	myAsgWebServers
Subscription	Select your subscription.
Resource group	Select **Use existing** and then select **myResourceGroup**.
Location	East US

4. Complete step 3 again, specifying the following values:

Setting	**Value**
Name	myAsgMgmtServers
Subscription	Select your subscription.
Resource group	Select **Use existing** and then select **myResourceGroup**.
Location	East US

Task 3: Create a Network Security Group

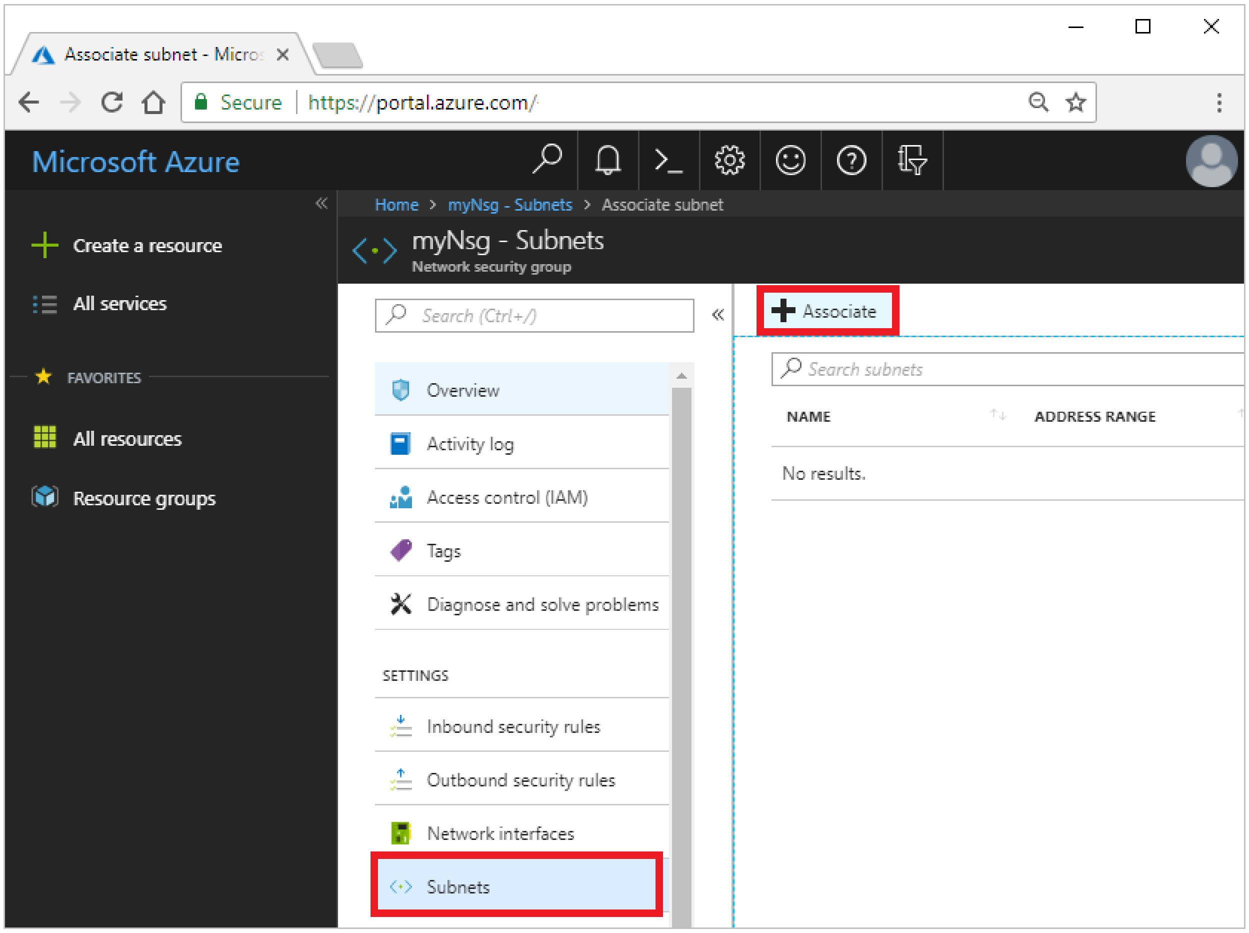
1. Select **+ Create a resource** on the upper, left corner of the Azure portal.
2. Select **Networking**, and then select **Network security group**.
3. Enter, or select, the following information, and then select **Create**:

Setting	**Value**
Name	myNsg
Subscription	Select your subscription.

Setting	Value
Resource group	Select **Use existing** and then select *myResourceGroup*.
Location	East US

Task 4: Associate Network Security Group to Subnet

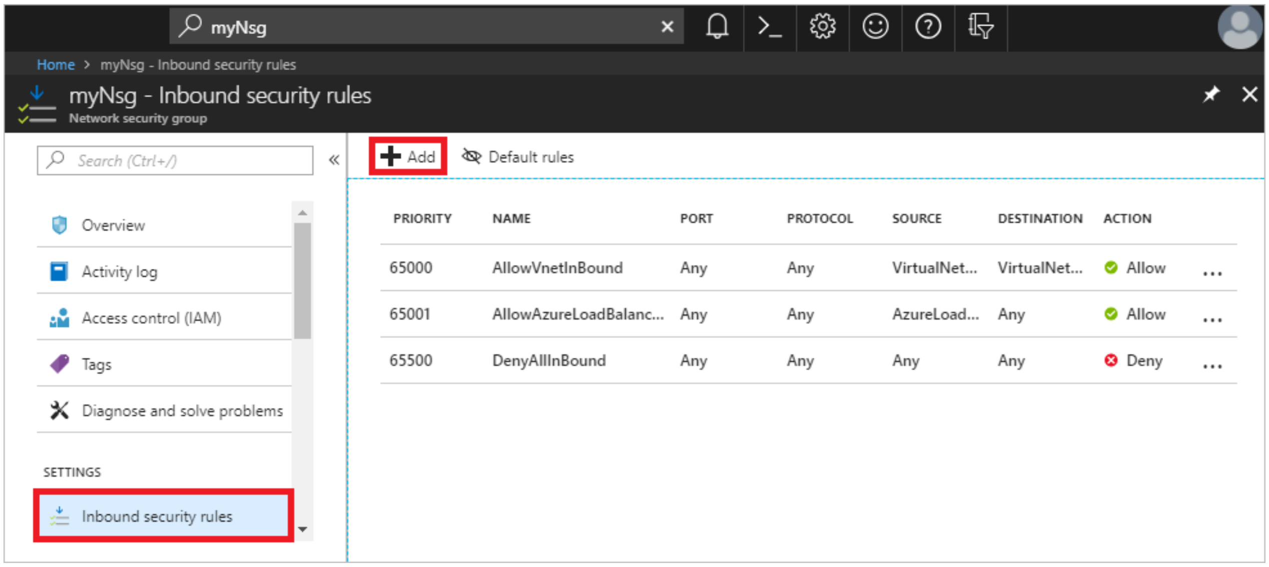
1. In the *Search resources, services, and docs* box at the top of the portal, begin typing *myNsg*. When **myNsg** appears in the search results, select it.
2. Under **SETTINGS**, select **Subnets** and then select **+ Associate**, as shown in the following picture:



3. Under **Associate subnet**, select **Virtual network** and then select **myVirtualNetwork**. Select **Subnet**, select **mySubnet**, and then select **OK**.

Task 5: Create Security Rules

1. Under **SETTINGS**, select **Inbound security rules** and then select **+ Add**, as shown in the following picture:



PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetInBound	Any	Any	VirtualNet...	VirtualNet...	Allow
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoad...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

2. Create a security rule that allows ports 80 and 443 to the **myAsgWebServers** application security group. Under **Add inbound security rule**, enter, or select the following values, accept the remaining defaults, and then select **Add**:

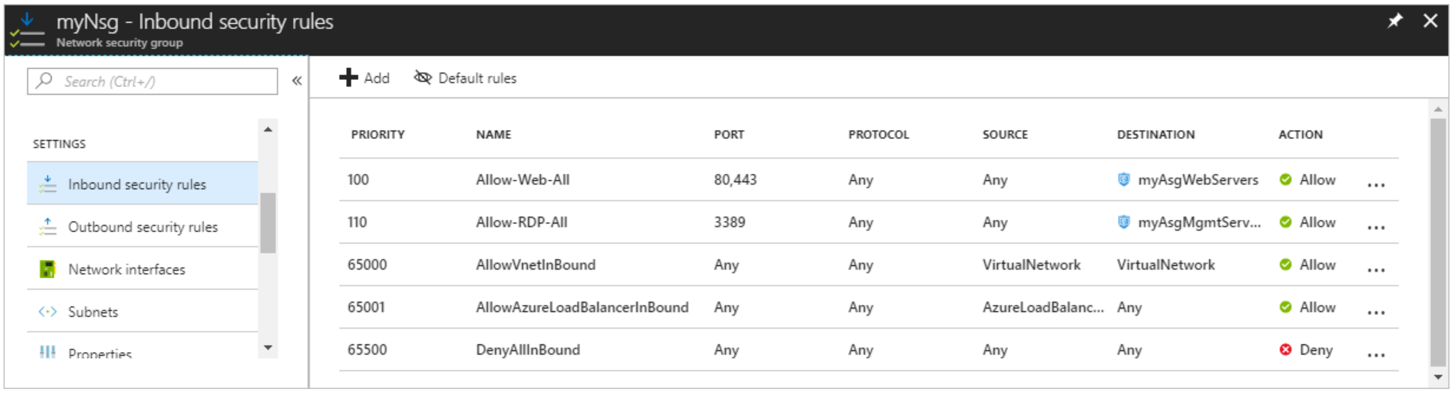
Setting	**Value**
Destination	Select **Application security group**, and then select **myAsgWebServers** for **Application security group**.
Destination port ranges	Enter 80,443
Protocol	Select TCP
Name	Allow-Web-All

3. Complete step 2 again, using the following values:

Setting	**Value**
Destination	Select **Application security group**, and then select **myAsgMgmtServers** for **Application security group**.
Destination port ranges	Enter 3389
Protocol	Select TCP
Priority	Enter 110
Name	Allow-RDP-All

4. In this tutorial, RDP (port 3389) is exposed to the internet for the VM that is assigned to the *myAsgMgmtServers* application security group. For production environments, instead of exposing port 3389 to the internet, it's recommended that you connect to Azure resources that you want to manage using a VPN or private network connection.

Once you've completed steps 1-3, review the rules you created. Your list should look like the list in the following picture:



PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	Allow-Web-All	80,443	Any	Any	myAsgWebServers	Allow
110	Allow-RDP-All	3389	Any	Any	myAsgMgmtServ...	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalanc...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Task 6: Create the First VM

1. Select **+ Create a resource** found on the upper, left corner of the Azure portal.
2. Select **Compute**, and then select **Windows Server 2016 Datacenter**.
3. Enter, or select, the following information, accept the defaults for the remaining settings, and then select **OK**:

Setting	**Value**
Name	myVmWeb
User name	Enter a user name of your choosing.
Password	Enter a password of your choosing. The password must be at least 12 characters long and meet the defined complexity requirements.
Subscription	Select your subscription.
Resource group	Select **Use existing** and select **myResourceGroup**.
Location	Select **East US**

4. Select a size for the VM and then select **Select**.
5. Under **Settings**, select the following values, accept the remaining defaults, and then select **OK**:

Setting	**Value**
Virtual network	Select **myVirtualNetwork**
Network Security Group	Select **Advanced**.
Network security group (firewall)	Select **(new) myVmWeb-nsg**, and then under **Choose network security grou**

6. Under **Create** of the **Summary**, select **Create** to start VM deployment.

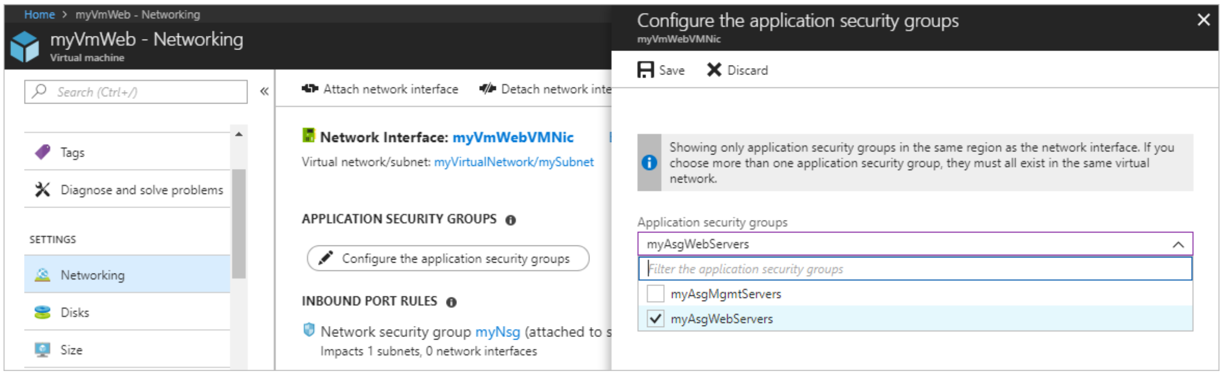
Task 7: Create the Second VM

Complete steps 1-6 again, but in step 3, name the VM *myVmMgmt*. The VM takes a few minutes to deploy. Do not continue to the next step until the VM is deployed.

Task 8: Associate Network Interfaces to a Network Security Group

When the portal created the VMs, it created a network interface for each VM, and attached the network interface to the VM. Add the network interface for each VM to one of the application security groups you created previously:

1. In the *Search resources, services, and docs* box at the top of the portal, begin typing *myVmWeb*. When the **myVmWeb** VM appears in the search results, select it.
2. Under **SETTINGS**, select **Networking**. Select **Configure the application security groups**, select **myAsgWebServers** for **Application security groups**, and then select **Save**, as shown in the following picture:



Network Interface: myVmWebVMNic

Virtual network/subnet: myVirtualNetwork/mySubnet

Network security group myNsg (attached to s

Impacts 1 subnets, 0 network interfaces

Showing only application security groups in the same region as the network interface. If you choose more than one application security group, they must all exist in the same virtual network.

Application security groups: myAsgWebServers

☐ myAsgMgmtServers

☑ myAsgWebServers

Home > myVmWeb - Networking
myVmWeb - Networking
Virtual machine
Search (Ctrl+/)
Tags
Diagnose and solve problems
SETTINGS
Networking
Disks
Size
Attach network interface
Detach network inte
APPLICATION SECURITY GROUPS
Configure the application security groups
INBOUND PORT RULES
Configure the application security groups
myVmWebVMNic
Save
Discard
Filter the application security groups

3. Complete steps 1 and 2 again, searching for the **myVmMgmt** VM and selecting the **myAsgMgmtServers** ASG.

Task 9: Test Traffic Filters

1. Connect to the *myVmMgmt* VM. Enter *myVmMgmt* in the search box at the top of the portal. When **myVmMgmt** appears in the search results, select it. Select the **Connect** button.
2. Select **Download RDP file**.
3. Open the downloaded rdp file and select **Connect**. Enter the user name and password you specified when creating the VM. You may need to select **More choices**, then **Use a different account**, to specify the credentials you entered when you created the VM.
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.

The connection succeeds, because port 3389 is allowed inbound from the internet to the *myAsgMgmtServers* application security group that the network interface attached to the *myVmMgmt* VM is in.

6. Connect to the *myVmWeb* VM from the *myVmMgmt* VM by entering the following command in a PowerShell session:

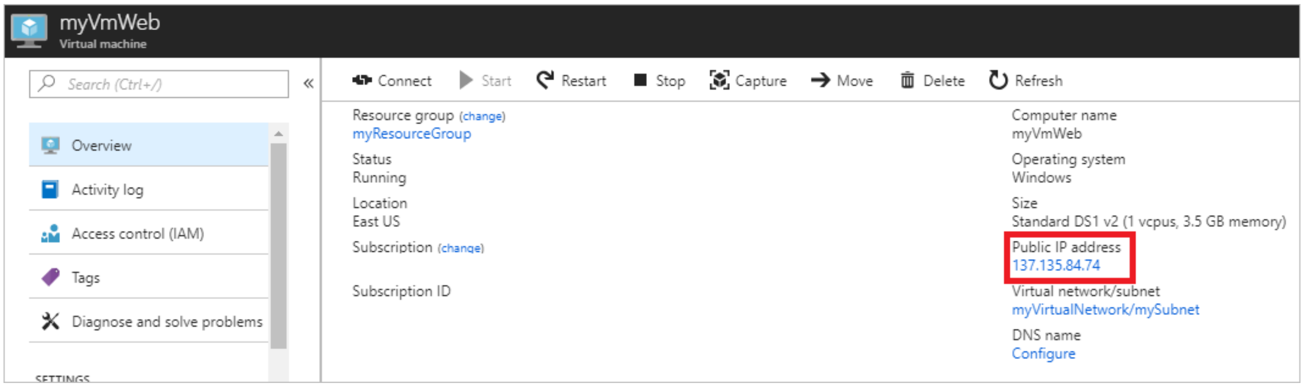
```
mstsc /v:myVmWeb
```

You are able to connect to the myVmWeb VM from the myVmMgmt VM because VMs in the same virtual network can communicate with each other over any port, by default. You can't however, create a remote desktop connection to the *myVmWeb*VM from the internet, because the security rule for the *myAsgWebServers* doesn't allow port 3389 inbound from the internet and inbound traffic from the Internet is denied to all resources, by default.

7. To install Microsoft IIS on the *myVmWeb* VM, enter the following command from a PowerShell session on the *myVmWeb* VM:

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

8. After the IIS installation is complete, disconnect from the *myVmWeb* VM, which leaves you in the *myVmMgmt* VM remote desktop connection.
9. Disconnect from the *myVmMgmt* VM.
10. In the *Search resources, services, and docs* box at the top of the Azure portal, begin typing *myVmWeb* from your computer. When **myVmWeb** appears in the search results, select it. Note the **Public IP address** for your VM. The address shown in the following picture is 137.135.84.74, but your address is different:



Resource group (change)
myResourceGroup
Status
Running
Location
East US
Subscription (change)
Subscription ID

Computer name
myVmWeb
Operating system
Windows
Size
Standard DS1 v2 (1 vcpus, 3.5 GB memory)
Public IP address
137.135.84.74
Virtual network/subnet
myVirtualNetwork/mySubnet
DNS name
Configure

11. To confirm that you can access the *myVmWeb* web server from the internet, open an internet browser on your computer and browse to `http://<public-ip-address-from-previous-step>`. You see the IIS welcome screen, because port 80 is allowed inbound from the internet to

the *myAsgWebServers* application security group that the network interface attached to the *myVmWeb* VM is in.

Task 10: Clean Up Resources

When no longer needed, delete the resource group and all of the resources it contains:

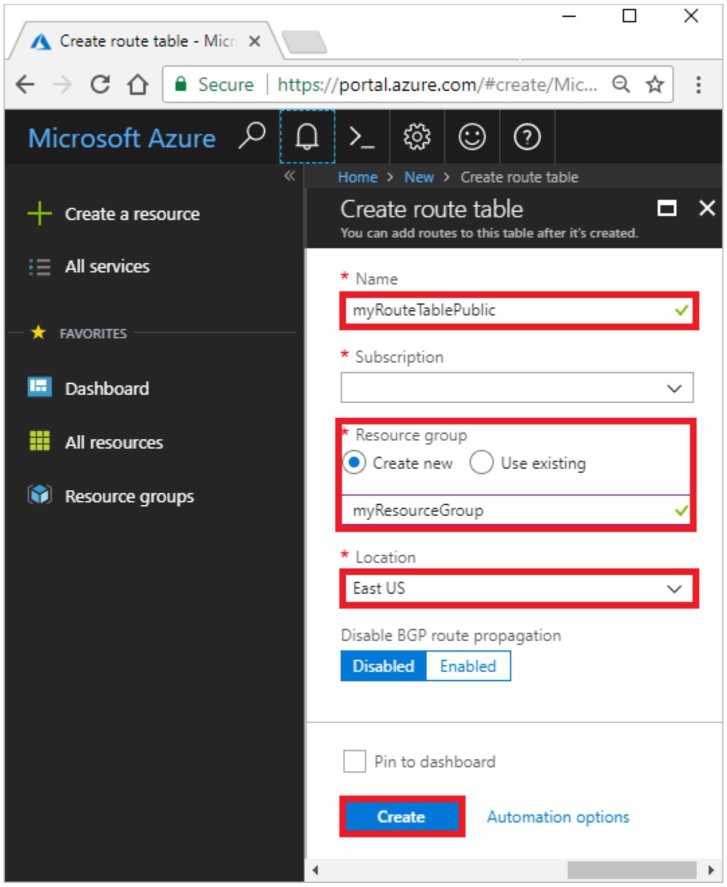
1. Enter *myResourceGroup* in the **Search** box at the top of the portal. When you see **myResourceGroup** in the search results, select it.
2. Select **Delete resource group**.
3. Enter *myResourceGroup* for **TYPE THE RESOURCE GROUP NAME:** and select **Delete**.

Route Network Traffic with a Route Table

Task 1: Create a Route Table

1. Select **+ Create a resource** on the upper, left corner of the Azure portal.
2. Select **Networking**, and then select **Route table**.
3. Enter, or select, the following information, accept the default for the remaining setting, and then select **Create**:

Setting	**Value**
Name	myRouteTablePublic
Subscription	Select your subscription.
Resource group	Select **Create new** and enter *myResourceGroup*.
Location	East US



Create route table

You can add routes to this table after it's created.

* Name: myRouteTablePublic

* Subscription:

* Resource group: ● Create new ○ Use existing

myResourceGroup

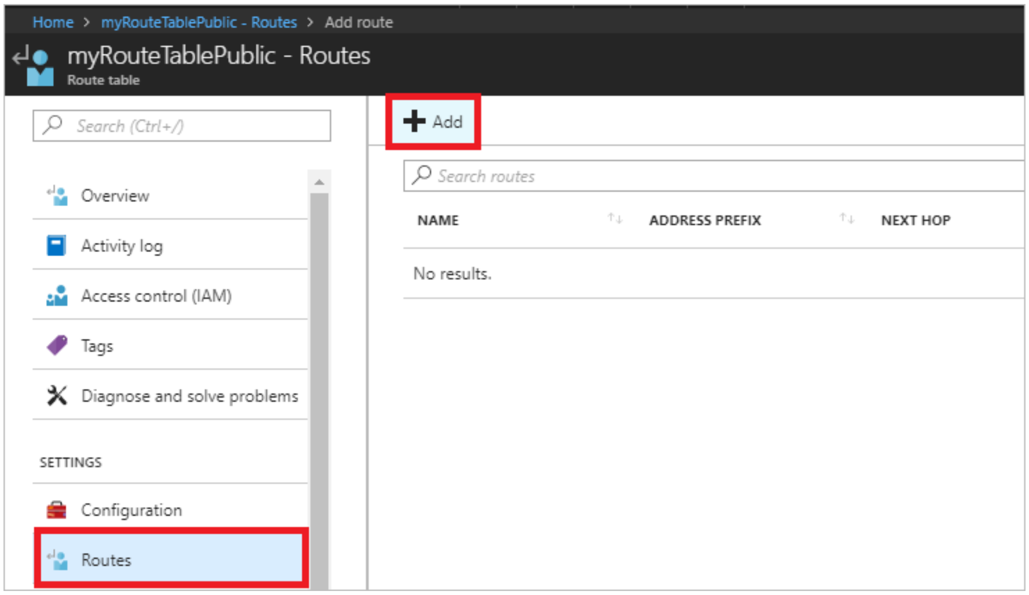
* Location: East US

Disable BGP route propagation: [✓ Disabled] Enabled

□ Pin to dashboard

Task 2: Create a Route

1. In the *Search resources, services, and docs* box at the top of the portal, begin typing *myRouteTablePublic*. When **myRouteTablePublic** appears in the search results, select it.
2. Under **SETTINGS**, select **Routes** and then select **+ Add**, as shown in the following picture:



myRouteTablePublic - Routes

Route table

NAME	ADDRESS PREFIX	NEXT HOP
No results.		

3. Under **Add route**, enter, or select, the following information, accept the default for the remaining settings, and then select **Create**:

Setting	**Value**
Route name	ToPrivateSubnet
Address prefix	10.0.1.0/24
Next hop type	Select **Virtual appliance**.
Next hop address	10.0.2.4

Task 3: Associate a Route Table to a Subnet

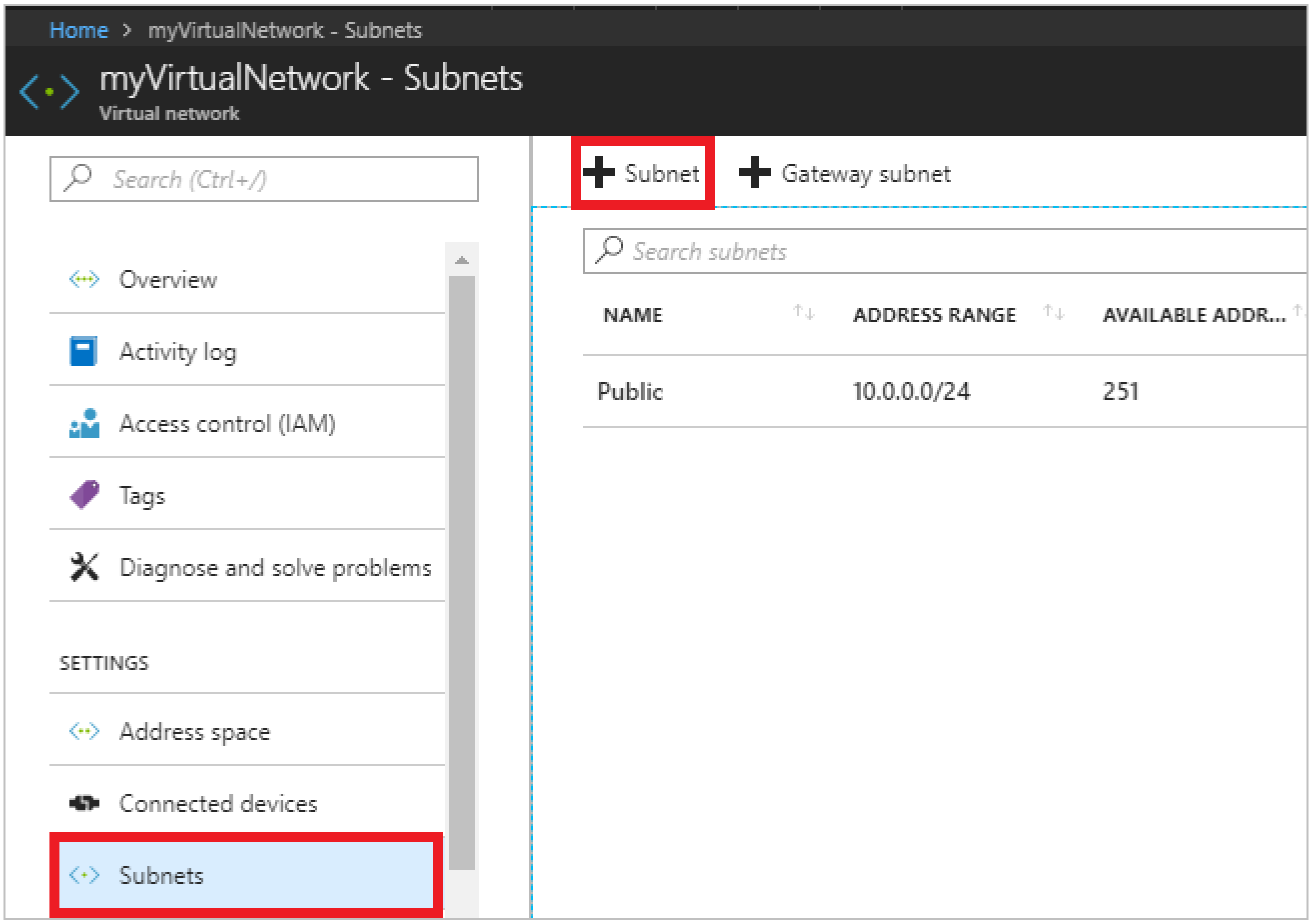
Before you can associate a route table to a subnet, you have to create a virtual network and subnet, then you can associate the route table to a subnet:

1. Select **+ Create a resource** on the upper, left corner of the Azure portal.
2. Select **Networking**, and then select **Virtual network**.
3. Under **Create virtual network**, Enter, or select, the following information, accept the default for the remaining settings, and then select **Create**:

Setting	**Value**
Name	myVirtualNetwork
Address space	10.0.0.0/16
Subscription	Select your subscription.
Resource group	Select **Use existing** and then select **myResourceGroup**.
Location	Select *East US*

Setting	**Value**
Subnet name	Public
Address range	10.0.0.0/24

4. In the **Search resources, services, and docs** box at the top of the portal, begin typing *myVirtualNetwork*. When **myVirtualNetwork**appears in the search results, select it.
5. Under **SETTINGS**, select **Subnets** and then select **+ Subnet**, as shown in the following picture:



NAME	ADDRESS RANGE	AVAILABLE ADDR...
Public	10.0.0.0/24	251

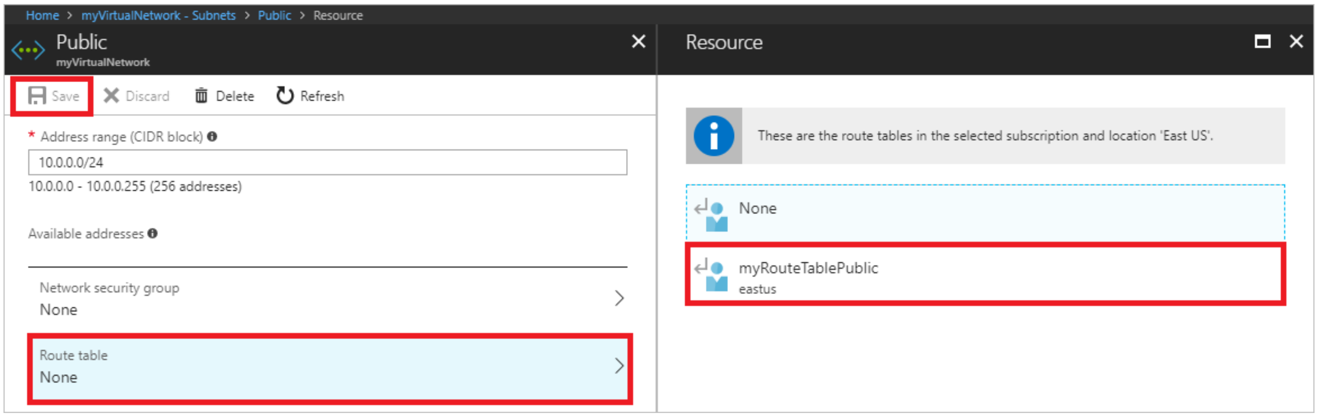
6. Select or enter the following information, then select **OK**:

Setting	**Value**
Name	Private
Address space	10.0.1.0/24

7. Complete steps 5 and 6 again, providing the following information:

Setting	**Value**
Name	DMZ
Address space	10.0.2.0/24

8. The **myVirtualNetwork - Subnets** box is displayed after completing the previous step. Under **SETTINGS**, select **Subnets** and then select **Public**.
9. As shown in the following picture, select **Route table**, select **MyRouteTablePublic**, and then select **Save**:



* Address range (CIDR block)
10.0.0.0/24
10.0.0.0 - 10.0.0.255 (256 addresses)

Available addresses

Network security group
None

Route table
None

These are the route tables in the selected subscription and location 'East US'.

None

myRouteTablePublic
eastus

Task 4: Create a NVA

An NVA is a VM that performs a network function, such as routing, firewalling, or WAN optimization.

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

2. Select **Compute**, and then select **Windows Server 2016 Datacenter**. You can select a different operating system, but the remaining steps assume you selected **Windows Server 2016 Datacenter**.
3. Select or enter the following information for **Basics**, then select **OK**:

Setting	**Value**
Name	myVmNva
User name	Enter a user name of your choosing.
Password	Enter a password of your choosing. The password must be at least 12 characters long and meet the c requirements.
Resource group	Select **Use existing** and then select *myResourceGroup*.
Location	Select **East US**.

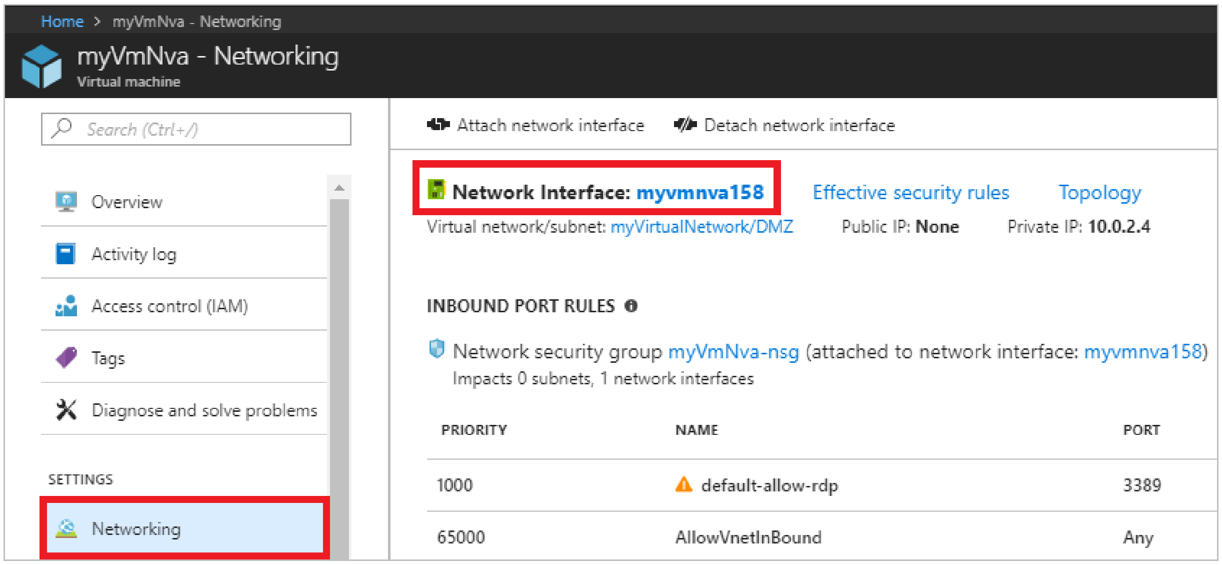
4. Select a VM size under **Choose a size**.
5. Select or enter the following information for **Settings**, then select **OK**:

Setting	**Value**
Virtual network	myVirtualNetwork - If it's not selected, select **Virtual network**, then select **myVirtualNetwork** under **Choose virtual network**.
Subnet	Select **Subnet** and then select **DMZ** under **Choose subnet**.
Public IP address	Select **Public IP address** and select **None** under **Choose public IP address**. No public IP address is assigned to this VM since it won't be connected to from the internet.

6. Under **Create** in the **Summary**, select **Create** to start the VM deployment.

   The VM takes a few minutes to create. Do not continue to the next step until Azure finishes creating the VM and opens a box with information about the VM.

7. In the box that opened for the VM after it was created, under **SETTINGS**, select **Networking**, and then select **myvmnva158** (the network interface Azure created for your VM has a different number after **myvmnva**), as shown in the following picture:



Network Interface: myvmnva158

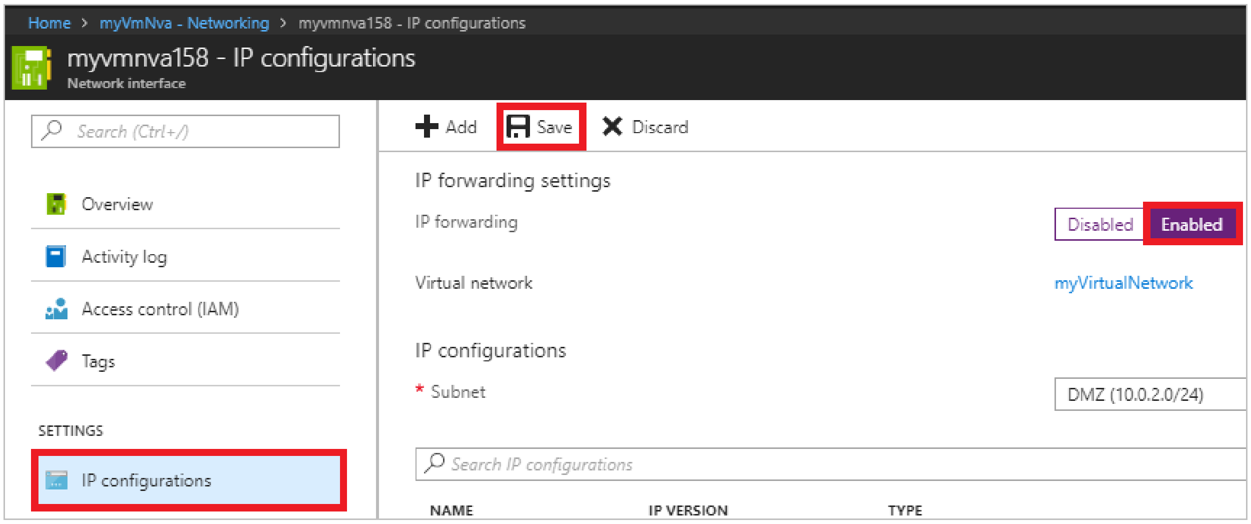
Virtual network/subnet: myVirtualNetwork/DMZ Public IP: None Private IP: 10.0.2.4

INBOUND PORT RULES

Network security group myVmNva-nsg (attached to network interface: myvmnva158)
Impacts 0 subnets, 1 network interfaces

PRIORITY	NAME	PORT
1000	⚠ default-allow-rdp	3389
65000	AllowVnetInBound	Any

8. For a network interface to be able to forward network traffic sent to it, that is not destined for its own IP address, IP forwarding must be enabled for the network interface. Under **SETTINGS**, select **IP configurations**, select **Enabled** for **IP forwarding**, and then select **Save**, as shown in the following picture:



IP forwarding settings

IP forwarding: Disabled [✓ Enabled]

Virtual network: myVirtualNetwork

IP configurations

* Subnet: DMZ (10.0.2.0/24)

NAME	IP VERSION	TYPE

Task 5: Create Virtual Machines

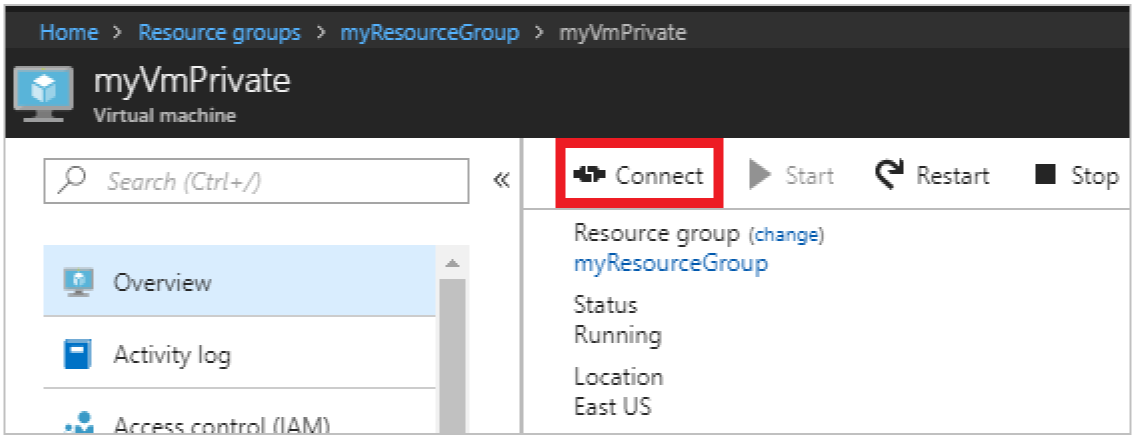
Create two VMs in the virtual network, so that you can validate that traffic from the *Public* subnet is routed to the *Private* subnet through the NVA in a later step. Complete steps 1-6 of Create a NVA. Use the same settings in steps 3 and 5, except for the following changes:

Virtual machine name	Subnet	Public IP address
myVmPublic	Public	Accept portal default
myVmPrivate	Private	Accept portal default

You can create the *myVmPrivate* VM while Azure creates the *myVmPublic* VM. Do not continue with the following steps until Azure finishes creating both VMs.

Task 6: Route Traffic Through a NVA

1. In the *Search* box at the top of the portal, begin typing *myVmPrivate*. When the **myVmPrivate** VM appears in the search results, select it.
2. Create a remote desktop connection to the *myVmPrivate* VM by selecting **Connect**, as shown in the following picture:



3. To connect to the VM, open the downloaded RDP file. If prompted, select **Connect**.
4. Enter the user name and password you specified when creating the VM (you may need to select **More choices**, then **Use a different account**, to specify the credentials you entered when you created the VM), then select **OK**.
5. You may receive a certificate warning during the sign-in process. Select **Yes** to proceed with the connection.

6. In a later step, the trace route tool is used to test routing. Trace route uses the Internet Control Message Protocol (ICMP), which is denied through the Windows Firewall. Enable ICMP through the Windows firewall by entering the following command from PowerShell on the *myVmPrivate* VM:

   ```
   New-NetFirewallRule -DisplayName “Allow ICMPv4-In” -Protocol ICMPv4
   ```

   Though trace route is used to test routing in this tutorial, allowing ICMP through the Windows Firewall for production deployments is not recommended.

7. You enabled IP forwarding within Azure for the VM's network interface in Enable IP Forwarding above. Within the VM, the operating system, or an application running within the VM, must also be able to forward network traffic. Enable IP forwarding within the operating system of the *myVmNva* VM:

   From a command prompt on the *myVmPrivate* VM, remote desktop to the *myVmNva* VM:

   ```
   mstsc /v:myvmnva
   ```

   To enable IP forwarding within the operating system, enter the following command in PowerShell from the *myVmNva* VM:

   ```
   Set-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters -Name
   IpEnableRouter -Value 1
   ```

   Restart the *myVmNva* VM, which also disconnects the remote desktop session.

8. While still connected to the *myVmPrivate* VM, create a remote desktop session to the *myVmPublic* VM, after the *myVmNva* VM restarts:

   ```
   mstsc /v:myVmPublic
   ```

   Enable ICMP through the Windows firewall by entering the following command from PowerShell on the *myVmPublic* VM:

   ```
   New-NetFirewallRule -DisplayName “Allow ICMPv4-In” -Protocol ICMPv4
   ```

9. To test routing of network traffic to the *myVmPrivate* VM from the *myVmPublic* VM, enter the following command from PowerShell on the *myVmPublic* VM:

```
tracert myVmPrivate
```

The response is similar to the following example:

```
Tracing route to myVmPrivate.vpgub4nqnocezhjgurw44dnxrc.bx.internal.cloudapp.net
[10.0.1.4]
over a maximum of 30 hops:

1    <1 ms     *        1 ms  10.0.2.4
2     1 ms     1 ms     1 ms  10.0.1.4

Trace complete.
```

You can see that the first hop is 10.0.2.4, which is the NVA's private IP address. The second hop is 10.0.1.4, the private IP address of the *myVmPrivate* VM. The route added to the *myRouteTablePublic* route table and associated to the *Public* subnet caused Azure to route the traffic through the NVA, rather than directly to the *Private* subnet.

10. Close the remote desktop session to the *myVmPublic* VM, which leaves you still connected to the *myVmPrivate* VM.
11. To test routing of network traffic to the *myVmPublic* VM from the *myVmPrivate* VM, enter the following command from a command prompt on the *myVmPrivate* VM:

```
tracert myVmPublic
```

The response is similar to the following example:

```
Tracing route to myVmPublic.vpgub4nqnocezhjgurw44dnxrc.bx.internal.cloudapp.net
[10.0.0.4]
over a maximum of 30 hops:

1     1 ms     1 ms     1 ms  10.0.0.4

Trace complete.
```

You can see that traffic is routed directly from the *myVmPrivate* VM to the *myVmPublic* VM. By default, Azure routes traffic directly between subnets.

12. Close the remote desktop session to the *myVmPrivate* VM.

Task 6: Clean Up Resources

When no longer needed, delete the resource group and all resources it contains:

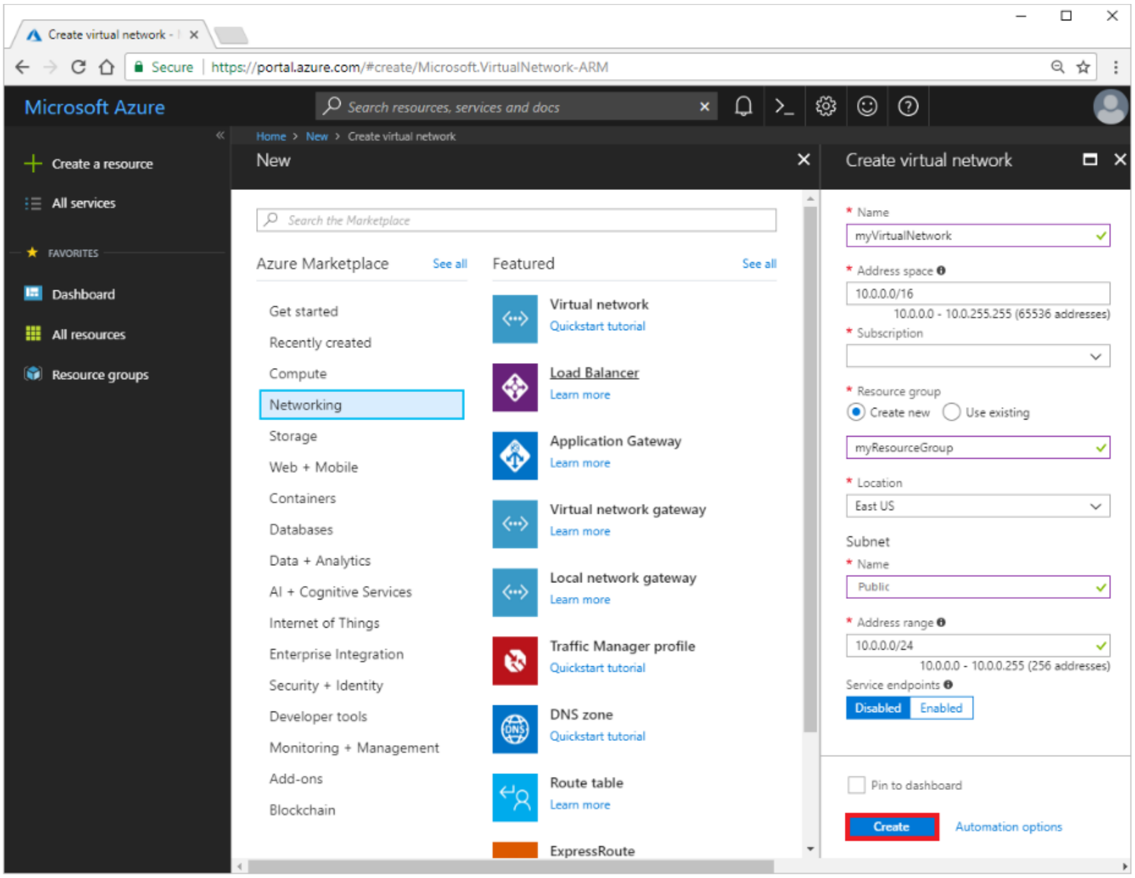
1. Enter *myResourceGroup* in the **Search** box at the top of the portal. When you see **myResourceGroup** in the search results, select it.
2. Select **Delete resource group**.
3. Enter *myResourceGroup* for **TYPE THE RESOURCE GROUP NAME:** and select **Delete**.

Restrict Network Access to PaaS Resources with Virtual Network Service Endpoints

Task 1: Create a Virtual Network

1. Select **+ Create a resource** on the upper, left corner of the Azure portal.
2. Select **Networking**, and then select **Virtual network**.
3. Enter, or select, the following information, and then select **Create**:

Setting	**Value**
Name	myVirtualNetwork
Address space	10.0.0.0/16
Subscription	Select your subscription
Resource group	Select **Create new** and enter *myResourceGroup*.
Location	Select **East US**
Subnet Name	Public
Subnet Address range	10.0.0.0/24
Service endpoints	Disabled



* Name: myVirtualNetwork

* Address space: 10.0.0.0/16 (10.0.0.0 - 10.0.255.255 (65536 addresses))

* Subscription:

* Resource group: ● Create new ○ Use existing — myResourceGroup

* Location: East US

Subnet

* Name: Public

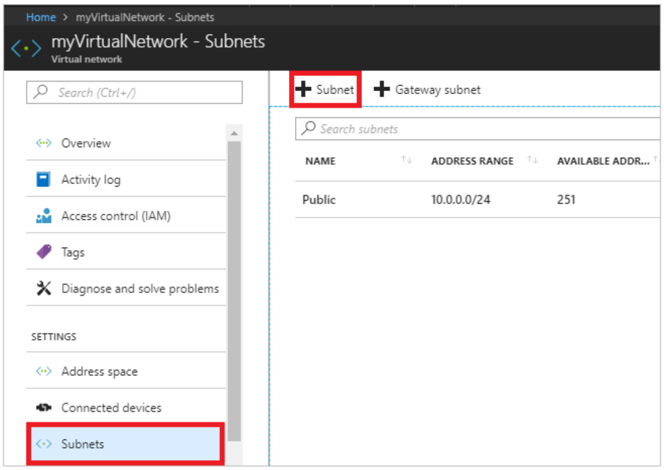
* Address range: 10.0.0.0/24 (10.0.0.0 - 10.0.0.255 (256 addresses))

Service endpoints: [✓ Disabled] Enabled

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	ADDRESS RANGE	AVAILABLE ADDR...
Public	10.0.0.0/24	251

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

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

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 select **Create**:

Setting	**Value**
Name	myNsgPrivate
Subscription	Select your subscription
Resource group	Select **Use existing** and select *myResourceGroup*.
Location	Select **East US**

4. After the network security group is created, enter *myNsgPrivate*, in the **Search resources, services, and docs** box at the top of the portal. When **myNsgPrivate** appears in the search results, select it.
5. Under **SETTINGS**, select **Outbound security rules**.
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 **OK**:

Setting	**Value**
Source	Select **VirtualNetwork**
Source port ranges	*
Destination	Select **Service Tag**
Destination service tag	Select **Storage**
Destination port ranges	*
Protocol	Any
Action	Allow
Priority	100
Name	Allow-Storage-All

8. Create a rule that denies outbound communication to the internet. This rule overrides a default rule in all network security groups that allows outbound internet communication. Complete steps 6 and 7 again, using the following values:

Setting	**Value**
Source	Select **VirtualNetwork**
Source port ranges	*
Destination	Select **Service Tag**

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

9. Under **SETTINGS**, select **Inbound security rules**.
10. Select **+ Add**.
11. Create a rule that allows Remote Desktop Protocol (RDP) traffic inbound 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. Complete steps 6 and 7 again, using the following values:

Setting	**Value**
Source	Any
Source port ranges	*
Destination	Select **Service Tag**
Destination service tag	Select **VirtualNetwork**
Destination port ranges	3389

Setting	Value
Protocol	Any
Action	Allow
Priority	120
Name	Allow-RDP-All

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**.

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.

Task 5: Create a Storage Account

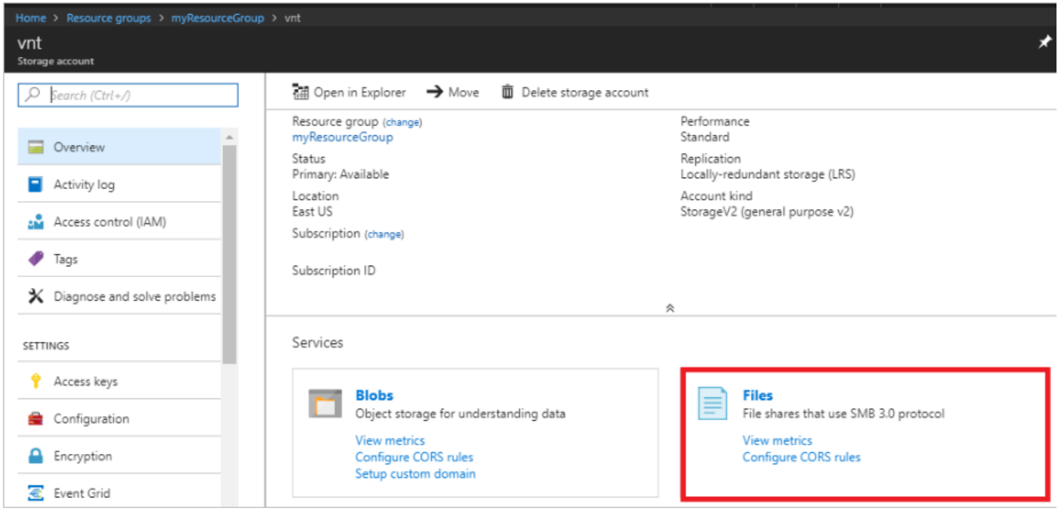
1. Select **+ Create a resource** on the upper, left corner of the Azure portal.
2. Select **Storage**, and then select **Storage account - blob, file, table, queue**.
3. Enter, or select, the following information, accept the remaining defaults, and then select **Create**:

Setting	Value
Name	Enter a name that is unique across all Azure locations, between 3-24 characters in length, using only numbers and lower-case letters.
Account kind	StorageV2 (general purpose v2)

Setting	**Value**
Replication	Locally-redundant storage (LRS)
Subscription	Select your subscription
Resource group	Select **Use existing** and select *myResourceGroup*.
Location	Select **East US**

Task 6: Create a file share in the storage account

1. After the storage account is created, enter the name of the storage account in the **Search resources, services, and docs** box, at the top of the portal. When the name of your storage account appears in the search results, select it.
2. Select **Files**, as shown in the following picture:



Resource group (change)
myResourceGroup
Status
Primary: Available
Location
East US
Subscription (change)
Subscription ID

Performance
Standard
Replication
Locally-redundant storage (LRS)
Account kind
StorageV2 (general purpose v2)

Blobs
Object storage for understanding data

Files
File shares that use SMB 3.0 protocol

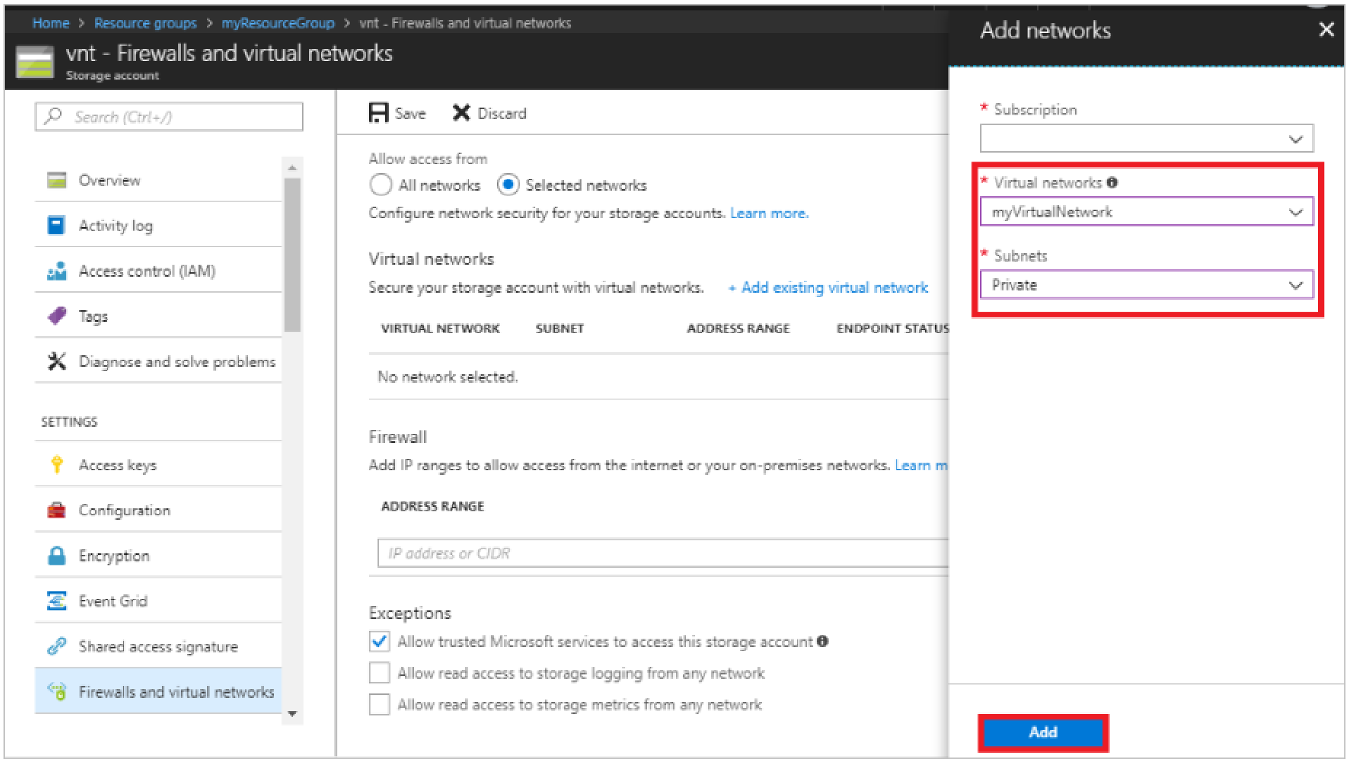
3. Select **+ File share**, under **File service**.
4. Enter *my-file-share* under **Name**, and then select **OK**.
5. Close the **File service** box.

Task 7: 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 **SETTINGS** for the storage account, select **Firewalls and virtual networks**.
2. Under **Virtual networks**, select **Selected networks**.
3. Select **Add existing virtual network**.
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**


Home > Resource groups > myResourceGroup > vnt - Firewalls and virtual networks
vnt - Firewalls and virtual networks
Storage account
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
SETTINGS
Access keys
Configuration
Encryption
Event Grid
Shared access signature
Firewalls and virtual networks
Save
Discard
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
VIRTUAL NETWORK
SUBNET
ADDRESS RANGE
ENDPOINT STATUS
No network selected.
Firewall
Add IP ranges to allow access from the internet or your on-premises networks. Learn m
ADDRESS RANGE
IP address or CIDR
Exceptions
Allow trusted Microsoft services to access this storage account
Allow read access to storage logging from any network
Allow read access to storage metrics from any network
Add networks
* Subscription
* Virtual networks
* Subnets
Add

Allow access from: ○ All networks ● Selected networks

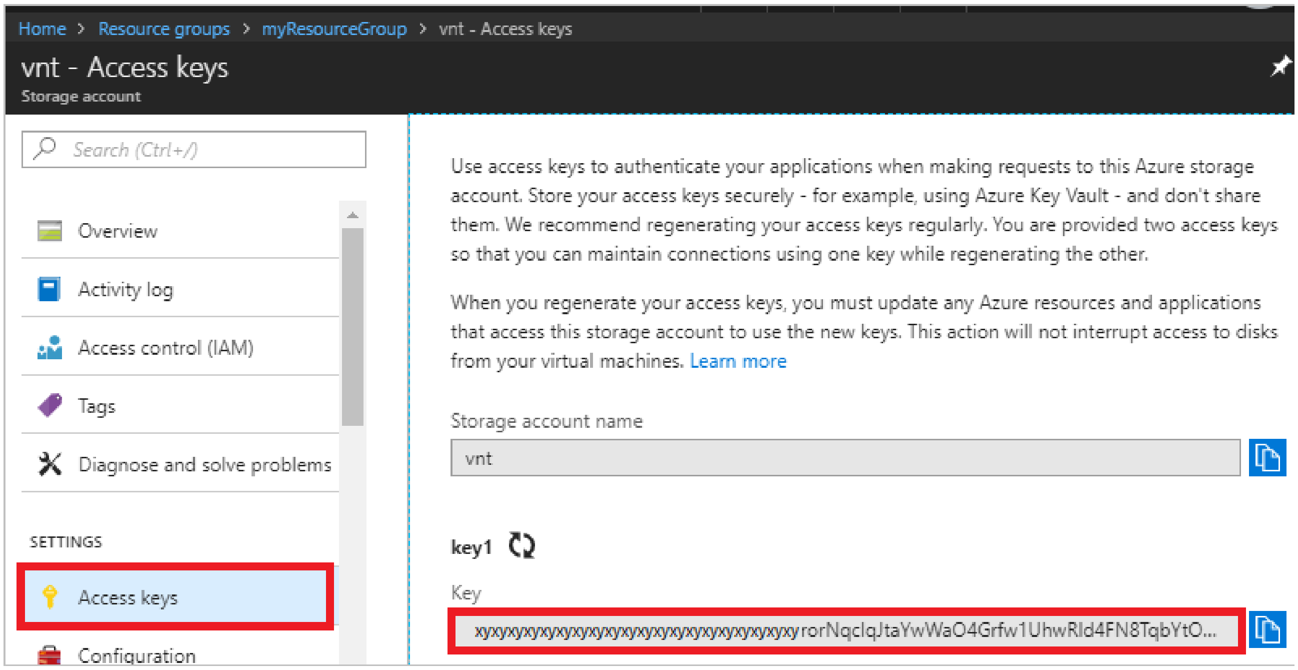
☑ Allow trusted Microsoft services to access this storage account
☐ Allow read access to storage logging from any network
☐ Allow read access to storage metrics from any network

* Virtual networks: myVirtualNetwork

* Subnets: Private

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:



Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys securely - for example, using Azure Key Vault - and don't share them. We recommend regenerating your access keys regularly. You are provided 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 storage account to use the new keys. This action will not interrupt access to disks from your virtual machines. Learn more

Storage account name: vnt

key1

Key: xyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyrorNqclqJtaYwWaO4Grfw1UhwRld4FN8TqbYtO...

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.

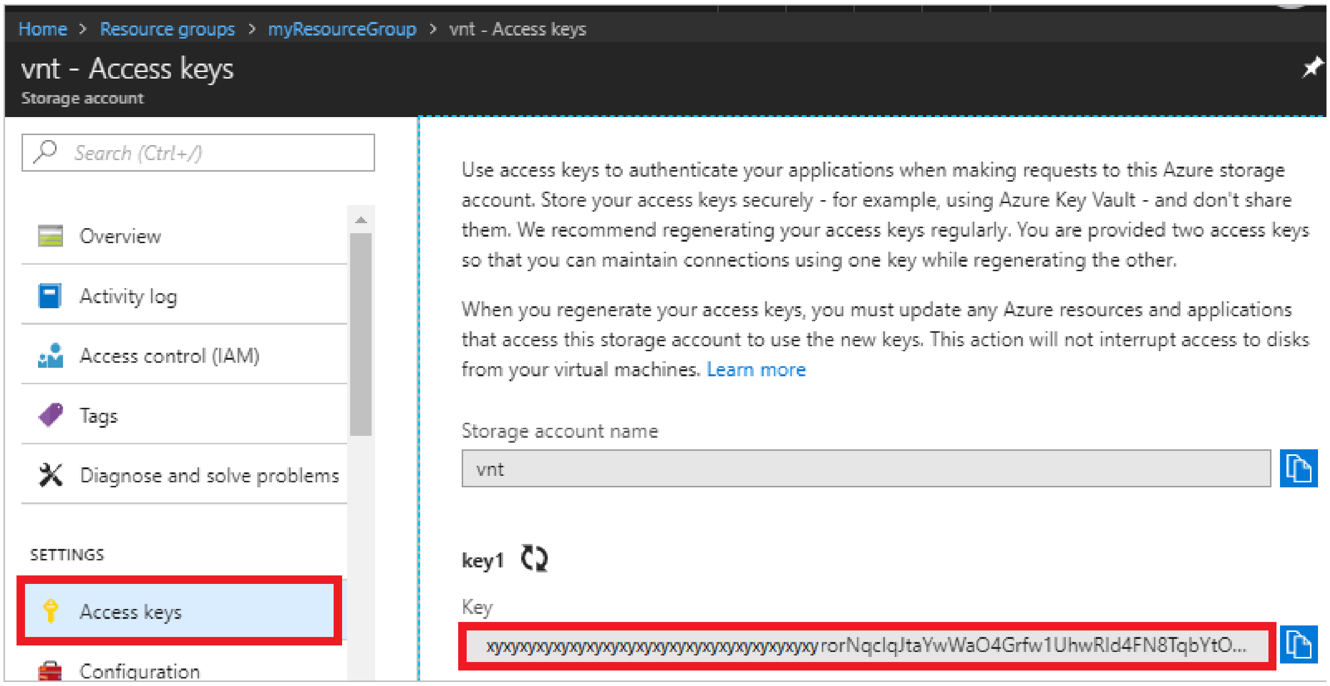
Task 8: Create the First Virtual Machine

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 **Windows Server 2016 Datacenter**.
3. Enter, or select, the following information, and then select **OK**:

Setting	**Value**
Name	myVmPublic
User name	Enter a user name of your choosing.
Password	Enter a password of your choosing. The password must be at least 12 characters long and meet the defined complexity requirements.
Subscription	Select your subscription.

Setting	Value
Resource group	Select **Use existing** and select **myResourceGroup**.
Location	Select **East US**.



Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys securely - for example, using Azure Key Vault - and don't share them. We recommend regenerating your access keys regularly. You are provided 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 storage account to use the new keys. This action will not interrupt access to disks from your virtual machines. Learn more

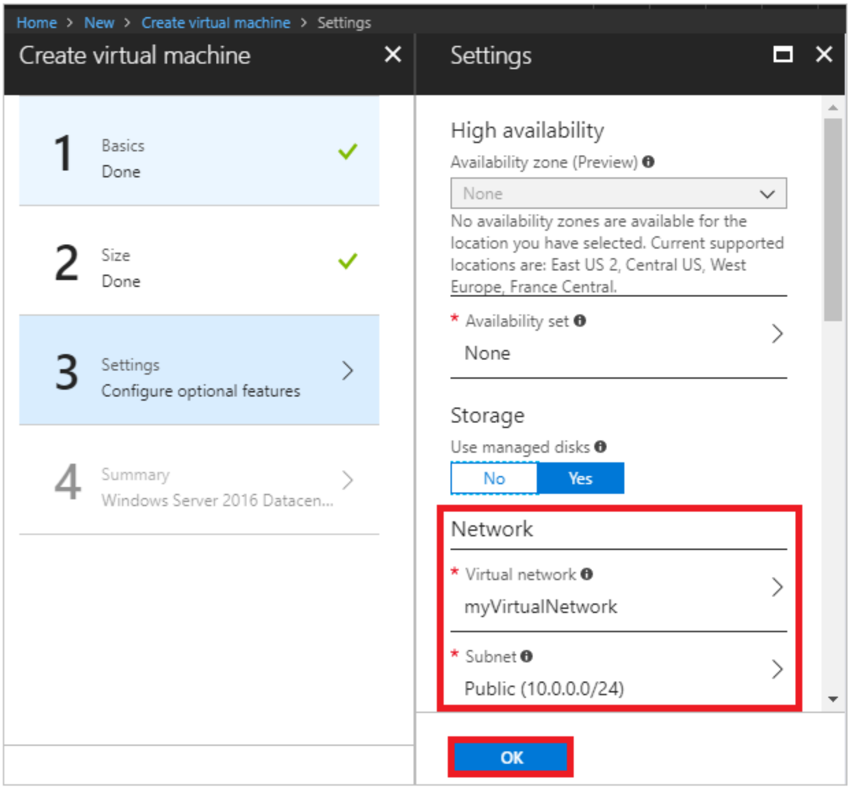
Storage account name: vnt

key1

Key: xyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxy rorNqclqJtaYwWaO4Grfw1UhwRld4FN8TqbYtO...

4. Select a size for the virtual machine and then select **Select**.

5. Under **Settings**, select **Network** and then select **myVirtualNetwork**. Then select **Subnet**, and select **Public**, as shown in the following picture:



Home > New > Create virtual machine > Settings

Create virtual machine

1 Basics
Done

2 Size
Done

3 Settings
Configure optional features

4 Summary
Windows Server 2016 Datacen...

Settings

High availability

Availability zone (Preview): None

No availability zones are available for the location you have selected. Current supported locations are: East US 2, Central US, West Europe, France Central.

* Availability set: None

Storage

Use managed disks: No | Yes

Network

* Virtual network: myVirtualNetwork

* Subnet: Public (10.0.0.0/24)

OK

6. On the **Summary** 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.

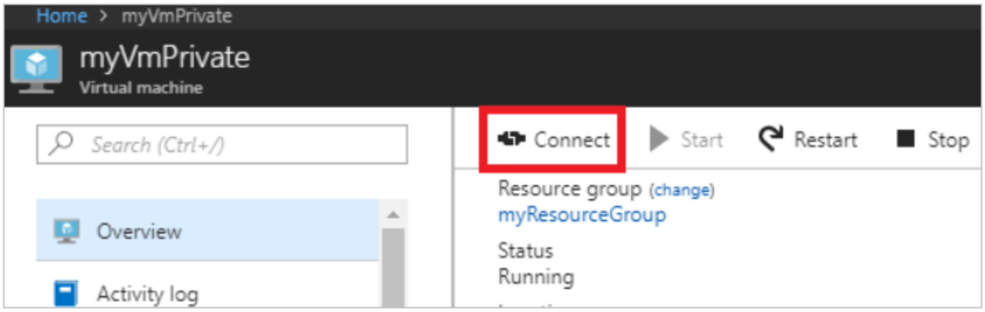
Task 9: Create the second virtual machine

Complete steps 1-6 again, but in step 3, name the virtual machine *myVmPrivate* and in step 5, select the **Private** subnet.

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 10: Confirm access to storage account

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



2. After selecting the **Connect** button, 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 and password you specified when creating the VM. You may need to select **More choices**, then **Use a different account**, to specify the credentials you entered when you created the VM.
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. Before running the commands that follow, replace `<storage-account-key>` and `<storage-account-name>` with values you supplied and retrieved in when you created your storage account.

```
$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.

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.

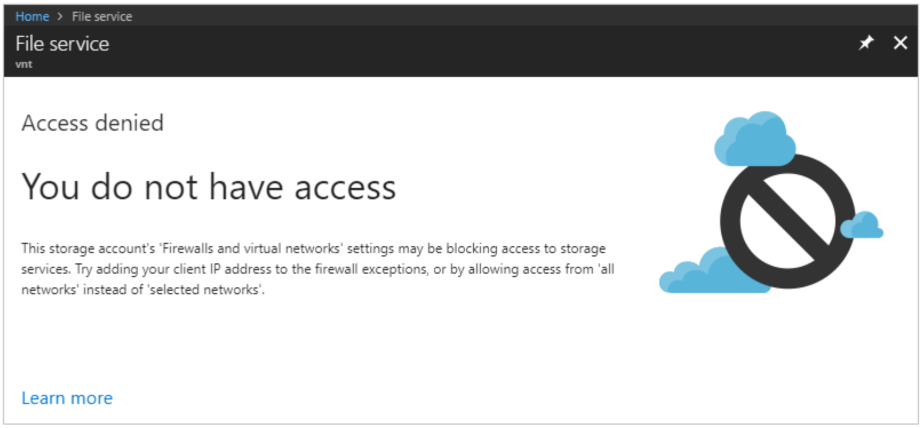
8. Close the remote desktop session to the *myVmPrivate* VM.

Task 11: 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 Confirm access to storage account for the *myVmPublic* VM.

   Access is denied and 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.
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**.
8. You receive the error shown in the following picture:



Access denied

You do not have access

This storage account's 'Firewalls and virtual networks' settings may be blocking access to storage services. Try adding your client IP address to the firewall exceptions, or by allowing access from 'all networks' instead of 'selected networks'.

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

Task 12: Clean up resources

When no longer needed, delete the resource group and all resources it contains:

1. Enter *myResourceGroup* in the **Search** box at the top of the portal. When you see **myResourceGroup** in the search results, select it.
2. Select **Delete resource group**.
3. Enter *myResourceGroup* for **TYPE THE RESOURCE GROUP NAME:** and select **Delete**.