**Labs Day 4**

**Lab 1A Create a virtual network using the Azure portal**

* ‎A virtual network enables Azure resources, like virtual machines (VMs), to communicate privately with each other, and with the internet. In this quickstart, you learn how to create a virtual network. After creating a virtual network, you deploy two VMs into the virtual network. You then connect to the VMs from the internet, and communicate privately between the two VMs.
* **The Resource Group Identified in the labs might already exist, so you may need to use another name**

**Task 1 Sign in to Azure**

Sign in to the [Azure portal](https://portal.azure.com/).

**Task 2 Create a virtual network**

1. On the upper-left side of the screen, select **Create a resource** > **Networking** > **Virtual network**.
2. In **Create virtual network**, enter or select this information:

| **Setting** | **Value** |
| --- | --- |
| Name | Enter *myVirtualNetwork*. |
| Address space | Enter *10.1.0.0/16*. |
| Subscription | Select your subscription. |
| Resource group | Select **Create new**, enter *myResourceGroup*, then select **OK**. |
| Location | Select **East US**. |
| Subnet - Name | Enter *myVirtualSubnet*. |
| Subnet - Address range | Enter *10.1.0.0/24*. |

1. Leave the rest of the defaults and select **Create**.

**Task 3 Create virtual machines**

Create two VMs in the virtual network:

**Create the first VM**

1. On the upper-left side of the screen, select **Create a resource** > **Compute** > **Windows Server 2016 Datacenter**.
2. In **Create a virtual machine - Basics**, enter or select this information:

| **Setting** | **Value** |
| --- | --- |
| **PROJECT DETAILS** |  |
| Subscription | Select your subscription. |
| Resource group | Select **MyResourceGroup**. You created it in the last section. |
| **INSTANCE DETAILS** |  |
| Virtual machine name | Enter *myVm1*. |
| Region | Select **East US**. |
| Availability options | Leave the default **No infrastructure redundancy required**. |
| Image | Leave the default **Windows Server 2016 Datacenter**. |
| Size | Leave the default **Standard DS1 v2**. |
| **ADMINISTRATOR ACCOUNT** |  |
| Username | Enter a user name of your choosing. Try **azureuser** |
| Password | Enter a password of your choosing. The password must be at least 12 characters long and meet the [defined complexity requirements](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/faq?toc=%2fazure%2fvirtual-network%2ftoc.json#what-are-the-password-requirements-when-creating-a-vm). Try **Pa55w.rd1234** |
| Confirm Password | Reenter password. |
| **INBOUND PORT RULES** |  |
| Public inbound ports | Leave the default **None**. |
| **SAVE MONEY** |  |
| Already have a Windows license? | Leave the default **No**. |

1. Select **Next : Disks**.
2. In **Create a virtual machine - Disks**, leave the defaults and select **Next : Networking**.
3. In **Create a virtual machine - Networking**, select this information:

| **Setting** | **Value** |
| --- | --- |
| Virtual network | Leave the default **myVirtualNetwork**. |
| Subnet | Leave the default **myVirtualSubnet (10.1.0.0/24)**. |
| Public IP | Leave the default **(new) myVm1-ip**. |
| Network security ports | Select **Allow selected ports**. |
| Select inbound ports | Select **HTTP** and **RDP**. |

1. Select **Next : Management**.
2. In **Create a virtual machine - Management**, for **Diagnostics storage account**, select **Create New**.
3. In **Create storage account**, enter or select this information:

| **Setting** | **Value** |
| --- | --- |
| Name | Enter a unique name |
| Account kind | Leave the default **Storage (general purpose v1)**. |
| Performance | Leave the default **Standard**. |
| Replication | Leave the default **Locally-redundant storage (LRS)**. |

1. Select **OK**
2. Select **Review + create**. You're taken to the **Review + create** page and Azure validates your configuration.
3. When you see that **Validation passed**, select **Create**.

**Task 4 Create the second VM**

1. Complete steps 1 and 9 from above.

**Note**

In step 2, for the **Virtual machine name**, enter *myVm2*.

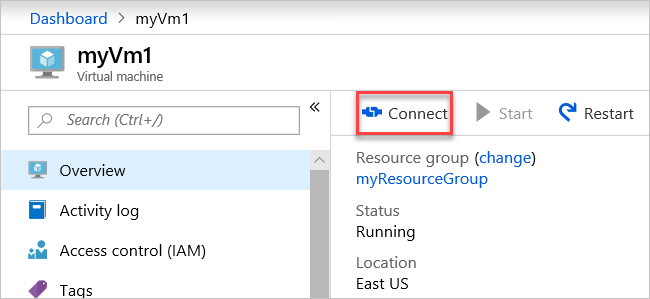
In step 7, for **Diagnostics storage account**, make sure you select the existing storage account created during the previous virtual machine deployment.

1. Select **Review + create**. You're taken to the **Review + create** page and Azure validates your configuration.
2. When you see that **Validation passed**, select **Create**.

**Task 5 Connect to a VM from the internet**

After you've created *myVm1*, connect to it over the internet.

1. In the portal's search bar, enter *myVm1*.
2. Select the **Connect** button.



After selecting the **Connect** button, **Connect to virtual machine** opens.

1. Select **Download RDP File**. Azure creates a Remote Desktop Protocol (*.rdp*) file and downloads it to your computer.
2. Open the downloaded *.rdp* file.
   1. If prompted, select **Connect**.
   2. Enter the user name and password you specified when creating the VM.

**Note**

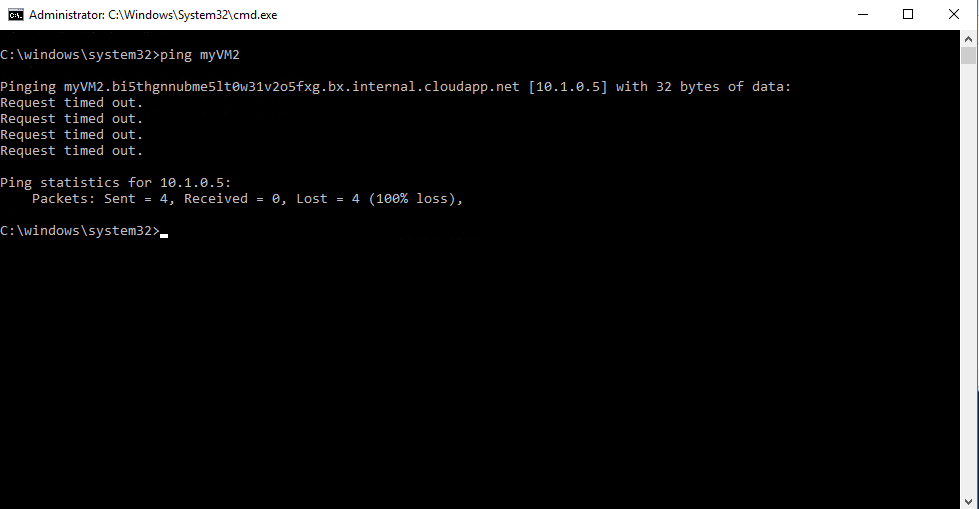
You may need to select **More choices** > **Use a different account**, to specify the credentials you entered when you created the VM.

1. Select **OK**.
2. You may receive a certificate warning during the sign in process. If you receive a certificate warning, select **Yes** or **Continue**.

**Task 6 Communicate between VMs**

1. In the Remote Desktop of *myVm1*, open PowerShell.
2. Enter ping myVm2.

You'll get back something like this message:



The ping fails, because ping uses the Internet Control Message Protocol (ICMP). By default, ICMP isn't allowed through the Windows firewall.

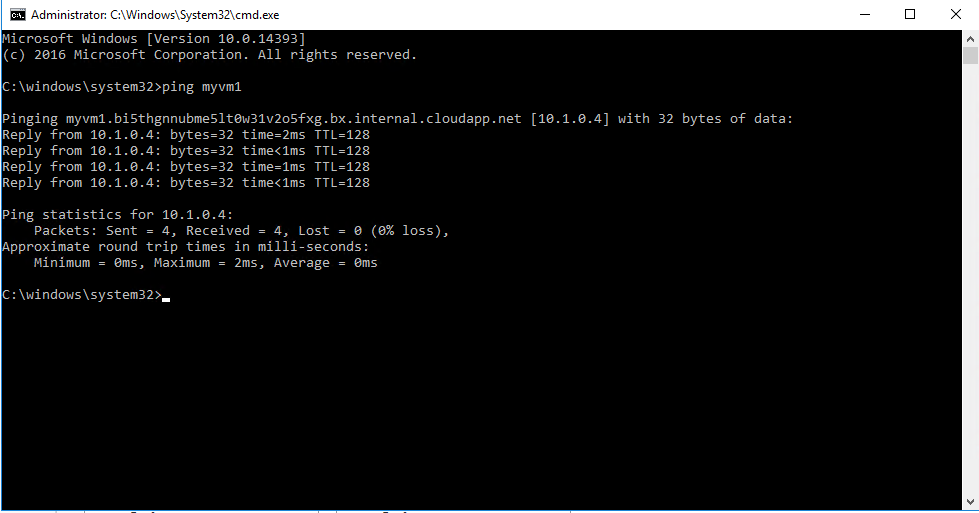
1. To allow *myVm2* to ping *myVm1* in a later step, enter this command:

PowerShell

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

That command allows ICMP inbound through the Windows firewall:

1. Close the remote desktop connection to *myVm1*.
2. Connect to *myVm2*.
3. From a command prompt, enter ping myvm1.



You receive replies from *myVm1*, because you allowed ICMP through the Windows firewall on the *myVm1* VM in a previous step.

1. Close the remote desktop connection to *myVm2*.

**Task 7 Clean up resources**

When you're done with the virtual network, and the VMs, delete the resource group and all of the resources it contains:

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

**Lab 1B** **Route network traffic with a route table using the Azure portal**

‎Azure routes traffic between all subnets within a virtual network, by default. You can create your own routes to override Azure's default routing. The ability to create custom routes is helpful if, for example, you want to route traffic between subnets through a network virtual appliance (NVA). In this lab, you learn how to:

* Create a route table
* Create a route
* Create a virtual network with multiple subnets
* Associate a route table to a subnet
* Create an NVA that routes traffic
* Deploy virtual machines (VM) into different subnets
* Route traffic from one subnet to another through an NVA

If you prefer, you can finish this tutorial using the [Azure CLI](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table-cli) or [Azure PowerShell](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table-powershell).

If you don't have an Azure subscription, create a [free account](https://azure.microsoft.com/free/?WT.mc_id=A261C142F) before you begin.

**Task 1 Sign in to Azure**

Sign in to the [Azure portal](https://portal.azure.com/).

**Task 2 Create a route table**

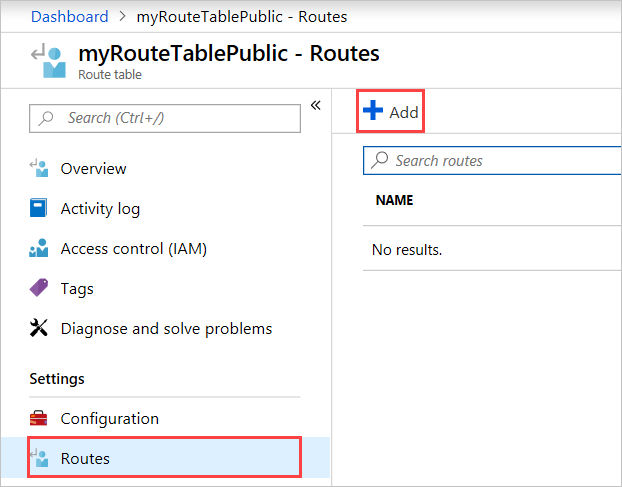
1. On the upper-left side of the screen, select **Create a resource** > **Networking** > **Route table**.
2. In **Create route table**, enter or select this information:

| **Setting** | **Value** |
| --- | --- |
| Name | Enter *myRouteTablePublic*. |
| Subscription | Select your subscription. |
| Resource group | Select **Create new**, enter *myResourceGroup or another name if this one is already being used*, and select *OK*. |
| Location | Leave the default **East US**. |
| BGP route propagation | Leave the default **Enabled**. |

1. Select **Create**.

**Task 3 Create a route**

1. In the portal's search bar, enter *myRouteTablePublic*.
2. When **myRouteTablePublic** appears in the search results, select it.
3. In **myRouteTablePublic** under **Settings**, select **Routes** > **+ Add**.



1. In **Add route**, enter or select this information:

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

1. Select **OK**.

**Task 4 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.

**Create a virtual network**

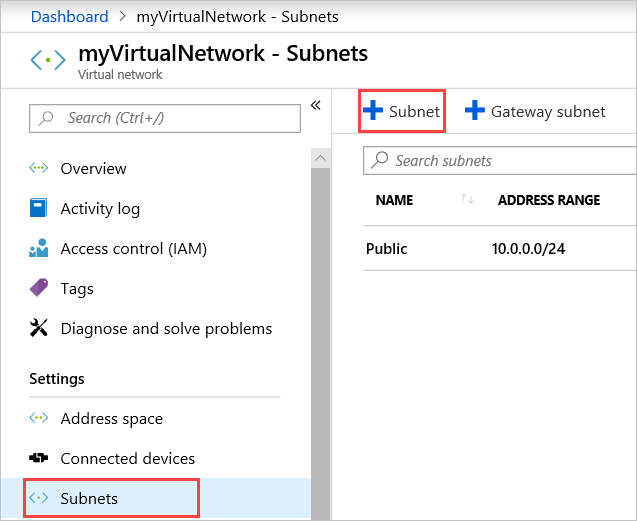
1. On the upper-left side of the screen, select **Create a resource** > **Networking** > **Virtual network**.
2. In **Create virtual network**, enter or select this information:

| **Setting** | **Value** |
| --- | --- |
| Name | Enter *myVirtualNetwork*. |
| Address space | Enter *10.0.0.0/16*. |
| Subscription | Select your subscription. |
| Resource group | Select ***Select existing*** > **Resource Group** that was used earlier |
| Location | Leave the default **East US**. |
| Subnet – Name | Enter *Public*. |
| Subnet - Address range | Enter *10.0.0.0/24*. |

1. Leave the rest of the defaults and select **Create**.

**Task 5 Add subnets to the virtual network**

1. In the portal's search bar, enter *myVirtualNetwork*.
2. When **myVirtualNetwork** appears in the search results, select it.
3. In **myVirtualNetwork**, under **Settings**, select **Subnets** > **+ Subnet**.



1. In **Add subnet**, enter this information:

| **Setting** | **Value** |
| --- | --- |
| Name | Enter *Private*. |
| Address range | Enter *10.0.1.0/24*. |

1. Leave the rest of the defaults and select **OK**.
2. Select **+ Subnet** again. This time, enter this information:

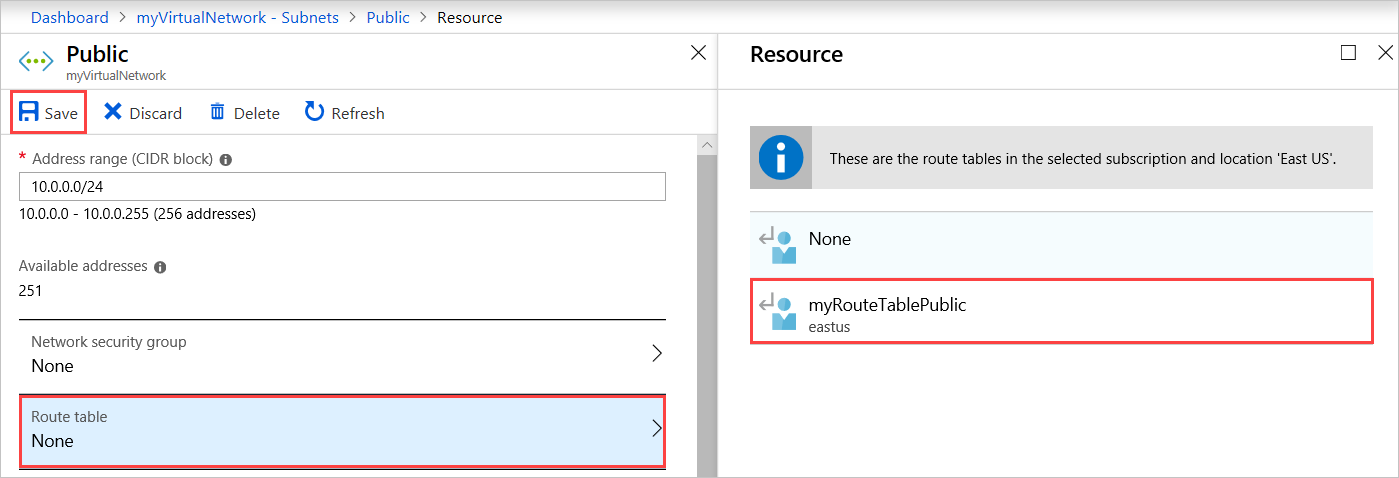
| **Setting** | **Value** |
| --- | --- |
| Name | Enter *DMZ*. |
| Address space | Enter *10.0.2.0/24*. |

1. Like the last time, leave the rest of the defaults and select **OK**.

Azure shows the three subnets: **Public**, **Private**, and **DMZ**.

**Associate myRouteTablePublic to your Public subnet**

1. Select **Public**.
2. In **Public**, select **Route table** > **MyRouteTablePublic** > **Save**.



**Task 6 Create an NVA**

NVAs are VMs that help with network functions like routing and firewall optimization. You can select a different operating system if you want. This tutorial assumes you're using **Windows Server 2016 Datacenter**.

1. On the upper-left side of the screen, select **Create a resource** > **Compute** > **Windows Server 2016 Datacenter**.
2. In **Create a virtual machine - Basics**, enter or select this information:

| **Setting** | **Value** |
| --- | --- |
| **PROJECT DETAILS** |  |
| Subscription | Select your subscription. |
| Resource group | Select **myResourceGroup** or the name of the previously used **Resource Group** |
| **INSTANCE DETAILS** |  |
| Virtual machine name | Enter *myVmNva*. |
| Region | Select **East US**. |
| Availability options | Leave the default **No infrastructure redundancy required**. |
| Image | Leave the default **Windows Server 2016 Datacenter**. |
| Size | Leave the default **Standard DS1 v2**. |
| **ADMINISTRATOR ACCOUNT** |  |
| Username | 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](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/faq?toc=%2fazure%2fvirtual-network%2ftoc.json#what-are-the-password-requirements-when-creating-a-vm). |
| Confirm Password | Reenter password. |
| **INBOUND PORT RULES** |  |
| Public inbound ports | Leave the default **None**. |
| **SAVE MONEY** |  |
| Already have a Windows license? | Leave the default **No**. |

1. Select **Next : Disks**.
2. In **Create a virtual machine - Disks**, accept the defaults.
3. Select **Next : Networking**.
4. In **Create a virtual machine - Networking**, select this information:

| **Setting** | **Value** |
| --- | --- |
| Virtual network | Leave the default **myVirtualNetwork**. |
| Subnet | Select **DMZ (10.0.2.0/24)**. |
| Public IP | Select **None**. You don't need a public IP address. The VM won't connect over the internet. |

1. Leave the rest of the defaults and select **Next : Management**.
2. In **Create a virtual machine - Management**, for **Diagnostics storage account**, select **Create New**.
3. In **Create storage account**, enter or select this information:

| **Setting** | **Value** |
| --- | --- |
| Name | Enter *mynvastorageaccount* and a random number to make the name unique. |
| Account kind | Leave the default **Storage (general purpose v1)**. |
| Performance | Leave the default **Standard**. |
| Replication | Leave the default **Locally-redundant storage (LRS)**. |

1. Select **OK**
2. Select **Review + create**. You're taken to the **Review + create** page and Azure validates your configuration.
3. When you see that **Validation passed**, select **Create**.

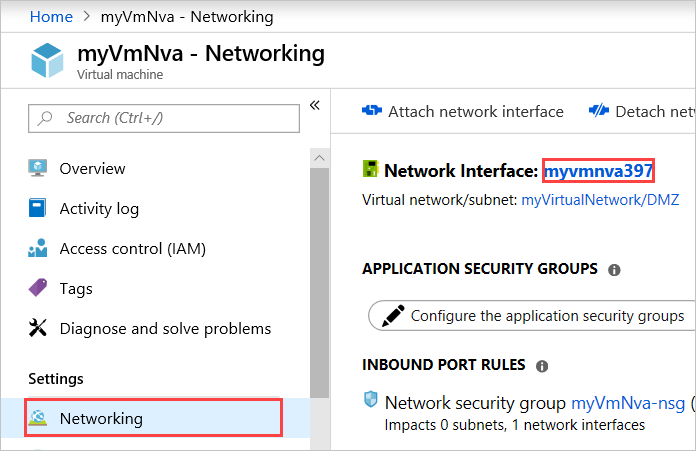
The VM takes a few minutes to create. Don't keep going until Azure finishes creating the VM. The **Your deployment is underway** page will show you deployment details.

1. When your VM is ready, select **Go to resource**.

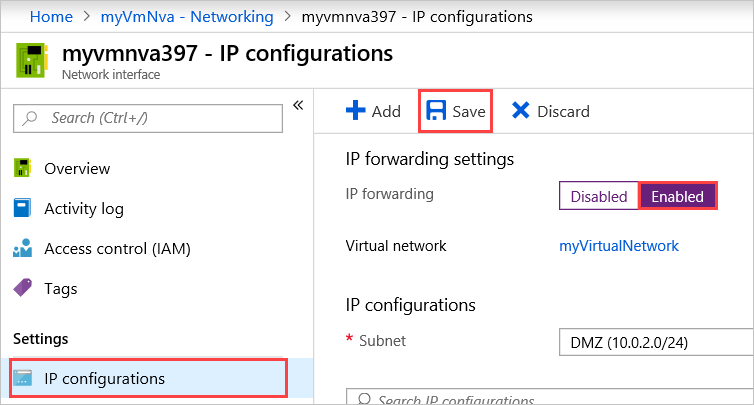
**Task 7 Turn on IP forwarding**

Turn on IP forwarding for *myVmNva*. When Azure sends network traffic to *myVmNva*, if the traffic is destined for a different IP address, IP forwarding will send the traffic to the correct location.

1. On **myVmNva**, under **Settings**, select **Networking**.
2. Select **myvmnva<random\_number>**. That's the network interface Azure created for your VM. It will have a string of numbers to make it unique for you.



1. Under **Settings**, select **IP configurations**.
2. On **myvmnva - IP configurations**, for **IP forwarding**, select **Enabled** and then select **Save**.



**Task 8 Create public and private virtual machines**

Create a VM in the *Public* subnet and another VM in the *Private* subnet in the *myVirtualNetwork* virtual network using the settings in the following table. Later, you'll use them to see that Azure routes the *Public* subnet traffic to the *Private* subnet through the NVA.

| **Setting** | **Value** |
| --- | --- |
| **PUBLIC VM** |  |
| BASICS |  |
| Virtual machine name | Enter *myVmPublic*. |
| NETWORKING |  |
| Subnet | Select **Public (10.0.0.0/24)**. |
| Public IP address | Accept the default. |
| Public inbound ports | Select **Allow selected ports**. |
| Select inbound ports | Select **HTTP** and **RDP**. |
| MANAGEMENT |  |
| Diagnostics storage account | Leave the default **mynvastorageaccount**. |
| **PRIVATE VM** |  |
| BASICS |  |
| Virtual machine name | Enter *myVmPrivate*. |
| NETWORKING |  |
| Subnet | Select **Private (10.0.1.0/24)**. |
| Public IP address | Accept the default. |
| Public inbound ports | Select **Allow selected ports**. |
| Select inbound ports | Select **HTTP** and **RDP**. |
| MANAGEMENT |  |
| Diagnostics storage account | Leave the default **mynvastorageaccount**. |

You can create the *myVmPrivate* VM while Azure creates the *myVmPublic* VM. Don't continue with the rest of the steps until Azure finishes creating both VMs.

**Route traffic through an NVA**

**Task 9 Sign in to myVmPrivate over remote desktop**

1. In the portal's search bar, enter *myVmPrivate*.
2. When the **myVmPrivate** VM appears in the search results, select it.
3. Select **Connect** to create a remote desktop connection to the *myVmPrivate* VM.
4. In **Connect to virtual machine**, select **Download RDP File**. Azure creates a Remote Desktop Protocol (*.rdp*) file and downloads it to your computer.
5. Open the downloaded *.rdp* file.
   1. If prompted, select **Connect**.
   2. Enter the user name and password you specified when creating the Private VM.
   3. You may need to select **More choices** > **Use a different account**, to use the Private VM credentials.
6. Select **OK**.

You may receive a certificate warning during the sign in process.

1. Select **Yes** to connect to the VM.

**Task 10 Enable ICPM through the Windows firewall**

In a later step, you'll use the trace route tool to test routing. Trace route uses the Internet Control Message Protocol (ICMP), which the Windows Firewall denies by default. Enable ICMP through the Windows firewall.

1. In the Remote Desktop of *myVmPrivate*, open PowerShell.
2. Enter this command:

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

You're using trace route to test routing in this tutorial. For production environments, we don't recommend allowing ICMP through the Windows Firewall.

**Task 11 Turn on IP forwarding within myVmNva**

You [turned on IP forwarding](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table-portal#turn-on-ip-forwarding) for the VM's network interface using Azure. The VM's operating system also has to forward network traffic. Turn on IP forwarding for *myVmNva* VM's operating system with these commands.

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

mstsc /v:myvmnva

1. From PowerShell on the *myVmNva*, enter this command to turn on IP forwarding:

PowerShell Copy

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

1. Restart the *myVmNva* VM. From the taskbar, select **Start button** > **Power button**, **Other (Planned)** > **Continue**.

That also disconnects the remote desktop session.

1. After the *myVmNva* VM restarts, create a remote desktop session to the *myVmPublic* VM. While still connected to the *myVmPrivate* VM, open a command prompt and run this command:

mstsc /v:myVmPublic

1. In the Remote Desktop of *myVmPublic*, open PowerShell.
2. Enable ICMP through the Windows firewall by entering this command:

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

**Task 12 Test the routing of network traffic**

First, let's test routing of network traffic from the *myVmPublic* VM to the *myVmPrivate* VM.

1. From PowerShell on the *myVmPublic* VM, enter this command:

tracert myVmPrivate

The response is similar to this 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 the first hop is to 10.0.2.4. It's NVA's private IP address. The second hop is to the private IP address of the *myVmPrivate* VM: 10.0.1.4. Earlier, you added the route to the *myRouteTablePublic* route table and associated it to the *Public* subnet. As a result, Azure sent the traffic through the NVA and not directly to the *Private* subnet.

1. Close the remote desktop session to the *myVmPublic* VM, which leaves you still connected to the *myVmPrivate* VM.
2. From a command prompt on the *myVmPrivate* VM, enter this command:

tracert myVmPublic

It tests the routing of network traffic from the *myVmPrivate* VM to the *myVmPublic* VM. The response is similar to this 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 Azure routes traffic directly from the *myVmPrivate* VM to the *myVmPublic* VM. By default, Azure routes traffic directly between subnets.

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

**Task 13 Clean up resources**

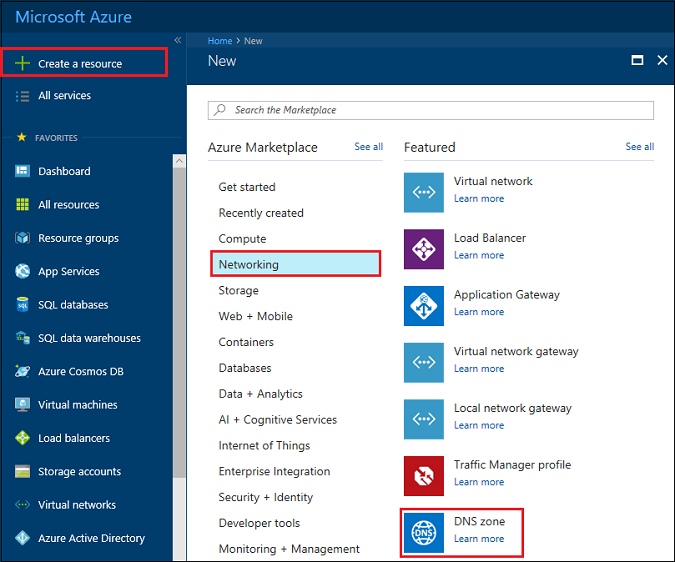
When no longer needed, delete the resource group and all resources it has:

1. In the portal's search bar, enter *myResourceGroup or the name of the Resource Group used*.
2. When you see your **ResourceGroup** in the search results, select it.
3. Select **Delete resource group**.
4. Enter *myResourceGroup* for **TYPE THE RESOURCE GROUP NAME:** and select **Delete**.

**Lab 2A** **OPTIONAL** **How to manage DNS Zones in the Azure portal**

* ‎**Note** You must have a domain name in order to do this lab
* **Task 1 Create a DNS zone**

1. Sign in to the Azure portal
2. On the Hub menu, navigate to **Create a resource > Networking > DNS zone** to open the **Create DNS zone** blade.



1. On the **Create DNS zone** blade enter the following values, then click **Create**:

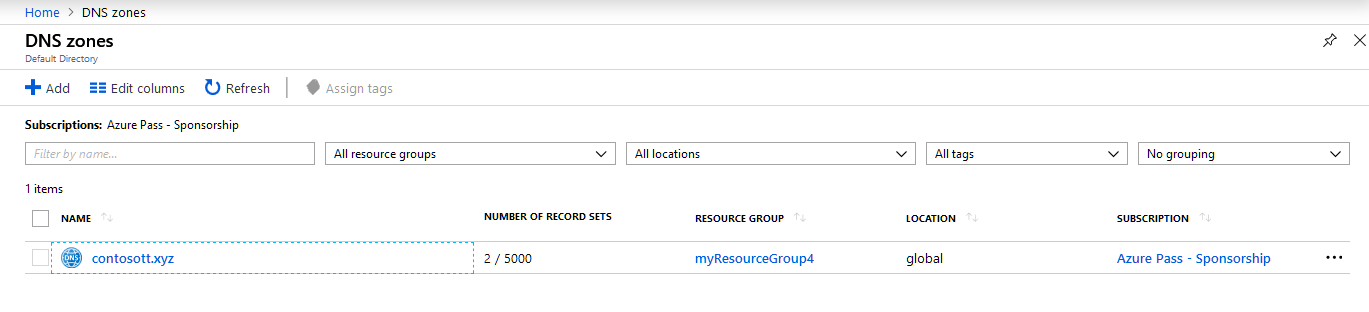
| **Setting** | **Value** | **Details** |
| --- | --- | --- |
| **Name** | A unique name  **contosoTT.xyz** | The name of the DNS zone |
| **Subscription** | [Your subscription] | Select a subscription to create the DNS zone in. |
| **Resource group** | **Create new:** contosoDNSRG | Create a resource group.  The resource group name must be unique within the subscription you selected. |
| **Location** | East US |  |

Note

The resource group refers to the location of the resource group, and has no impact on the DNS zone. The DNS zone location is always "global", and is not shown.

**Task 2 List DNS zones**

In the Azure portal, navigate to **All services** > **DNS zones**. Each DNS zone is its own resource, and information such as number of record-sets and name servers are viewable from this view. The column **NAME SERVERS** is not in the default view. To add it, click **Columns**, select **Name servers**, and then click **Done**.



**Task 3 Delete a DNS zone**

Navigate to a DNS zone in the portal. On the **DNS zone** blade, click **Delete zone**. You are then prompted to confirm you are wanting to delete the DNS zone. Deleting a DNS zone also deletes all records that are contained in the zone.

**Lab 2B** **Manage DNS records and record sets by using the Azure portal**

* ‎This lab shows you how to manage record sets and records for your DNS zone by using the Azure portal.

It's important to understand the difference between DNS record sets and individual DNS records. A record set is a collection of records in a zone that have the same name and are the same type. For more information, see [Create DNS record sets and records by using the Azure portal](https://docs.microsoft.com/en-us/azure/dns/dns-getstarted-create-recordset-portal).

**Create a new record set and record**

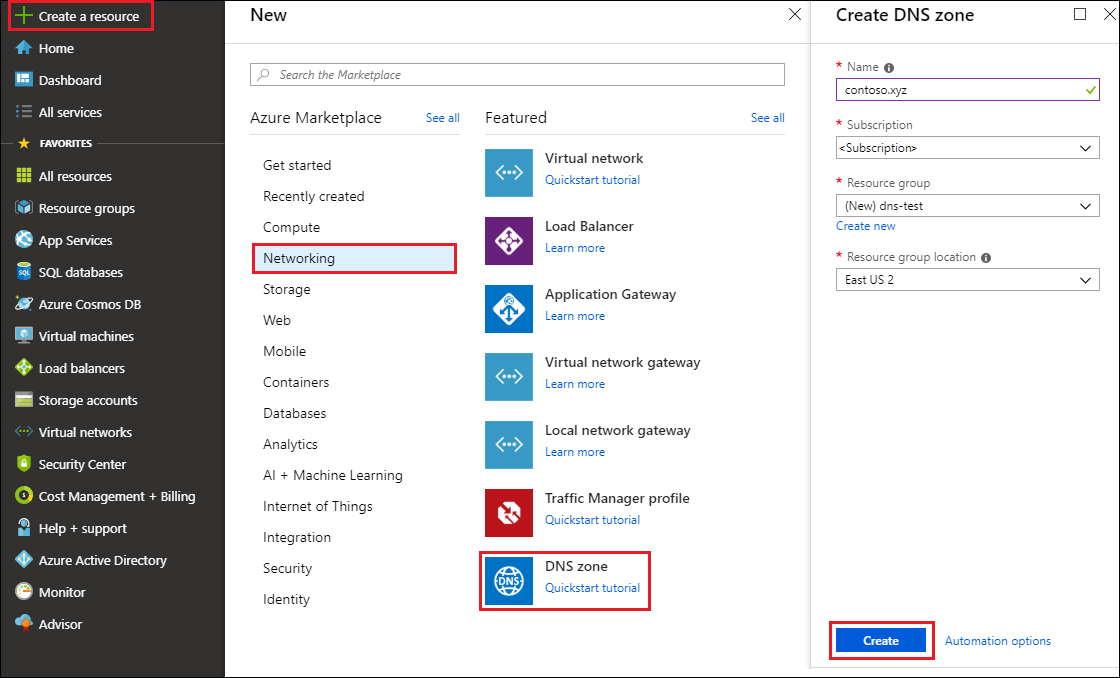
# Configure Azure DNS for name resolution by using the portal

## Task 1 Create a DNS zone

A DNS zone contains the DNS entries for a domain. To start hosting your domain in Azure DNS, you create a DNS zone for that domain name.

**To create the DNS zone:**

1. At upper left, select **Create a resource**, then **Networking**, and then **DNS zone**.
2. On the **Create DNS zone** page, type or select the following values:
   * **Name**: Type contoso.xyz, or another unique name for this lab example. The DNS zone name can be any value that is not already configured on the Azure DNS servers. A real-world value would be a domain that you bought from a domain name registrar.
   * **Resource group**: Select **Create new**, enter dns-test, and select **OK**. The resource group name must be unique within the Azure subscription.
3. Select **Create**.



It may take a few minutes to create the zone.

## Task 2 Create a DNS record

You create DNS entries or records for your domain inside the DNS zone. Create a new address record or 'A' record to resolve a host name to an IPv4 address.

**To create an 'A' record:**

1. In the Azure portal, under **All resources**, open the **contoso.xyz** DNS zone in the **dns-test** resource group. You can enter contoso.xyz in the **Filter by name** box to find it more easily.
2. At the top of the **DNS zone** page, select **+ Record set**.
3. On the **Add record set** page, type or select the following values:
   * **Name**: Type www. The record name is the host name that you want to resolve to the specified IP address.
   * **Type**: Select **A**. 'A' records are the most common, but there are other record types for mail servers ('MX'), IP v6 addresses ('AAAA'), and so on.
   * **TTL**: Type 1. Time-to-live of the DNS request specifies how long DNS servers and clients can cache a response.
   * **TTL unit**: Select **Hours**. This is the time unit for the **TTL** value.
   * **IP address**: For this lab, type 10.10.10.10. This value is the IP address the record name resolves to. In a real-world scenario, you would enter the public IP address for your web server.

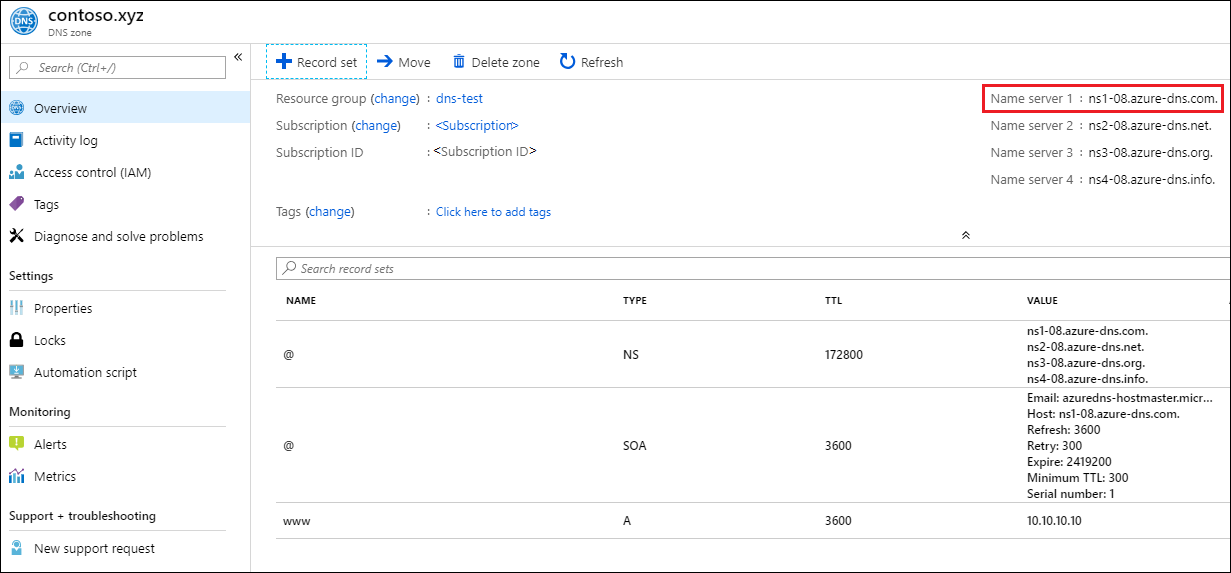
Since this lab doesn't use a real domain, there's no need to configure the Azure DNS name servers at a domain name registrar. With a real domain, you'll want anyone on the internet to resolve the host name to connect to your web server or app. You'll visit your domain name registrar to replace the name server records with the Azure DNS name servers. For more information, see [Tutorial: Host your domain in Azure DNS](https://docs.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns#delegate-the-domain).

## Task 3 Test the name resolution

Now that you have a test DNS zone with a test 'A' record, you can test the name resolution with a tool called nslookup.

**To test DNS name resolution:**

1. In the Azure portal, under **All resources**, open the **contoso.xyz** DNS zone in the **dns-test** resource group. You can enter contoso.xyz in the **Filter by name** box to find it more easily.
2. Copy one of the name server names from the name server list on the **Overview** page.

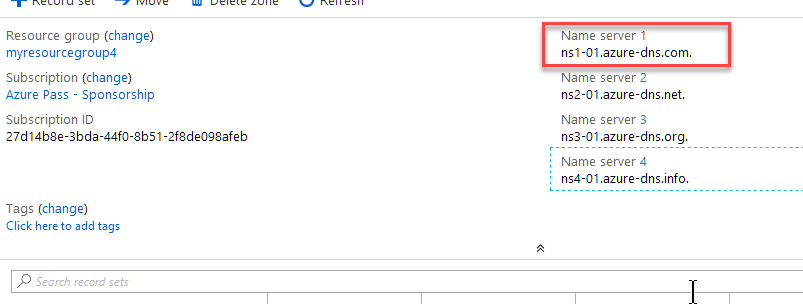


Note

In a real-world scenario, you copy all four name server names, including trailing periods, and use them for the new Azure DNS name server names at your domain registrar. For more information, see [Delegate a domain to Azure DNS](https://docs.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns)

1. Open a command prompt, and run the following command:

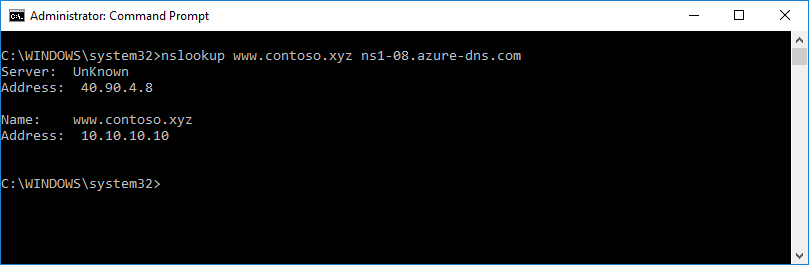
nslookup <host name> <name server name>



For example:

nslookup www.contoso.xyz ns1-08.azure-dns.com.

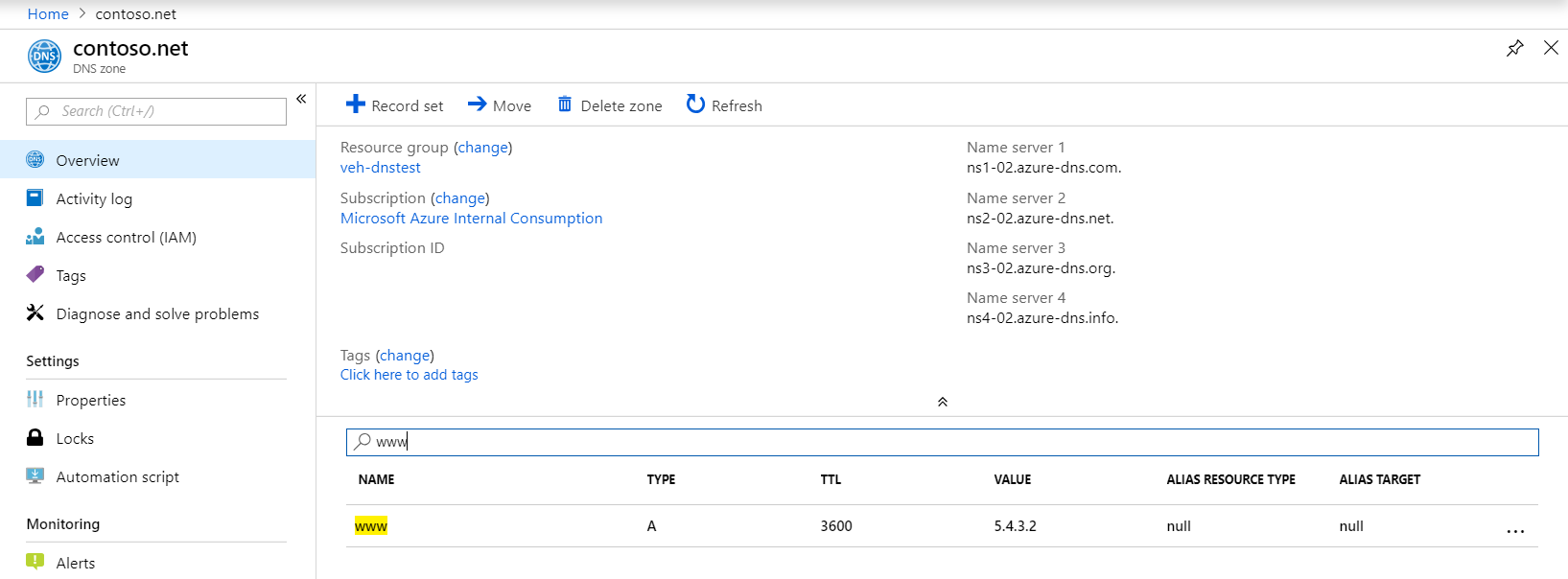
You should see something like the following screen:



The host name used resolves to **10.10.10.10**, just as you configured it. This result verifies that name resolution is working correctly.

**Task 4 View a record set**

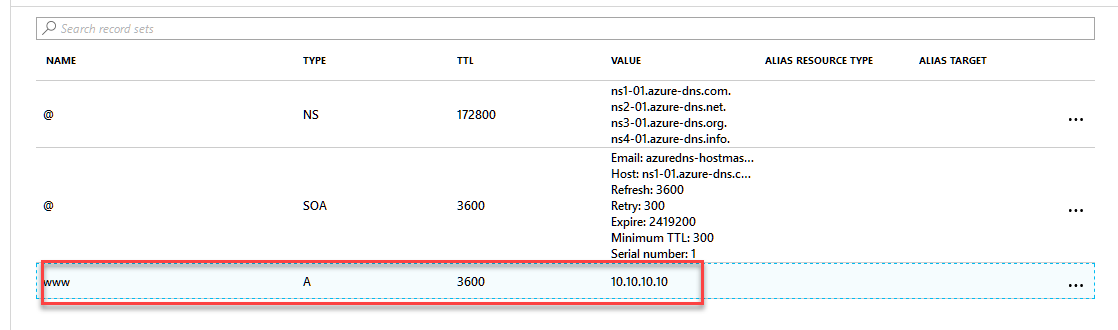
1. In the Azure portal, go to the **DNS zone** blade.
2. Search for the record set and select it. This opens the record set properties.



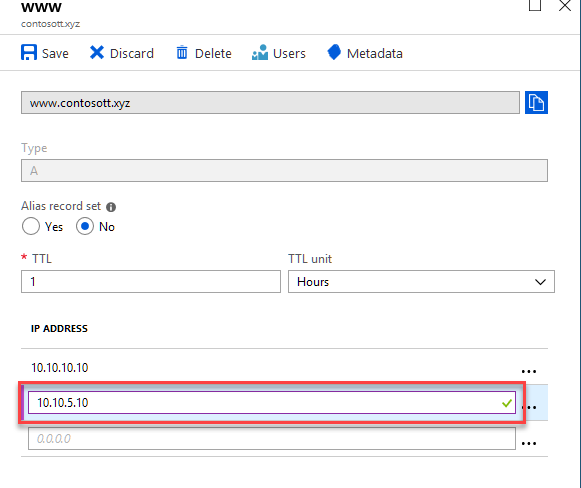
**Task 5 Update a record**

You can add up to 20 records to any record set. A record set cannot contain two identical records. Empty record sets (with zero records) can be created, but do not appear on the Azure DNS name servers. Record sets of type CNAME can contain one record at most.

1. On the **Record set properties** blade for your DNS zone, click the record set that you change or add a property value.



1. Modify the record set properties that need to be changed.



1. Click **Save** at the top of the blade to save your settings. Then close the blade.
2. In the corner, you will see that the record is saved

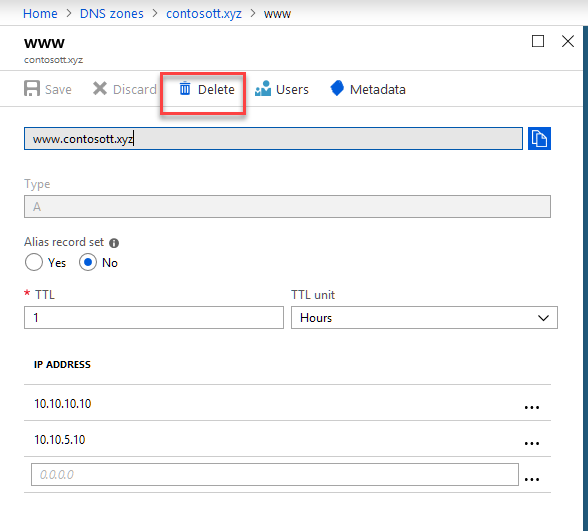


After the record has been saved, the values on the **DNS zone** blade will reflect the new record.

**Task 6 Delete a record set**

You can use the Azure portal to remove records from a record set. Note that removing the last record from a record set does not delete the record set.

1. On the **Record set properties** blade for your record set, search for the record.
2. Click the record that you want to remove. Then select **Delete**.



1. Click **Yes** to confirm the deletion.
2. After the record has been removed, the values for the record on the **DNS zone** blade will reflect the removal.

**Lab 3A** **Restrict network access to PaaS resources with** **Virtual network service endpoints using the Azure portal**

* ‎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

***The Resource Group named myResourceGroup is used throughout this lab. If you already have a resource group name myResourceGroup, just use another unique name and ensure you change the name where required in the lab steps.***

**Task 1 Log in to Azure**

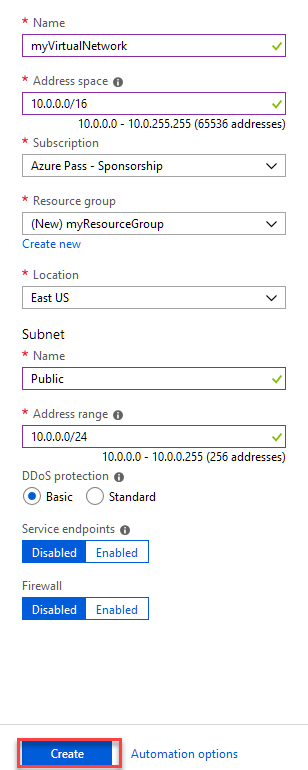
Log in to the Azure portal at [https://portal.azure.com](https://portal.azure.com/).

**Task 2 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 |

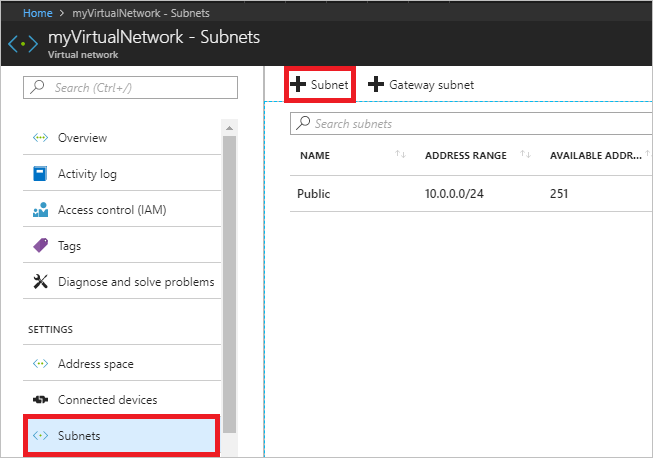
1. Then Click **Create**



**Task 3 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:



1. 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** |

Caution

Before enabling a service endpoint for an existing subnet that has resources in it, see [Change subnet settings](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-subnet#change-subnet-settings).

**Task 4 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  Type | Select **East US**  Resource Manager |

1. 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.
2. Under **SETTINGS**, select **Outbound security rules**.
3. Select **+ Add**.
4. 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 |
| Priority | 100 |
| Name | Allow-Storage-All |

1. 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 |

1. Under **SETTINGS**, select **Inbound security rules**.
2. Select **+ Add**.
3. 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 |

1. Under **SETTINGS**, select **Subnets**.
2. Select **+ Associate**
3. Under **Associate subnet**, select **Virtual network** and then select **myVirtualNetwork** under **Choose a virtual network**.
4. Under **Choose subnet**, select **Private**, and then select **OK**.

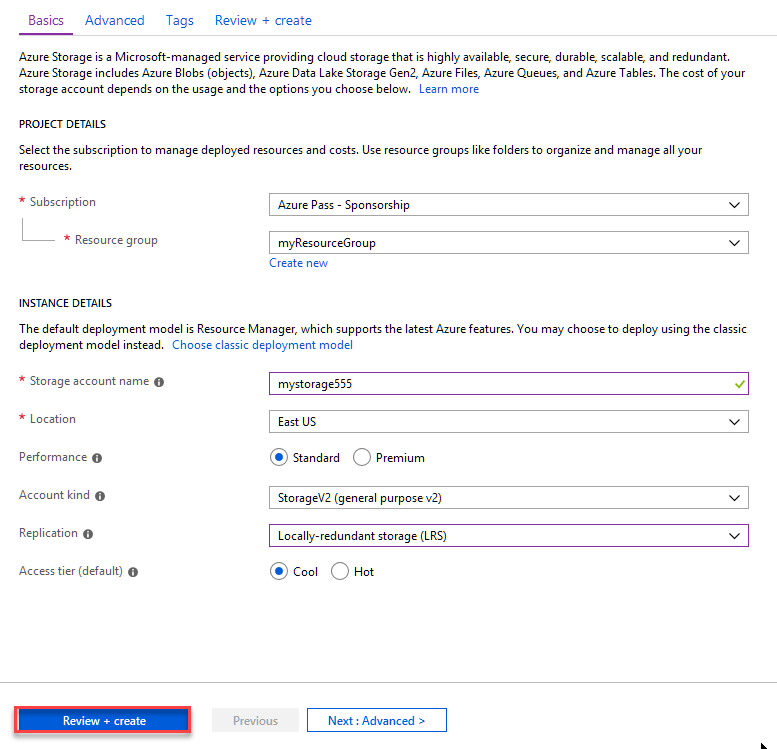
**Task 5 Restrict network access to a resource**

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.

**Create a storage account**

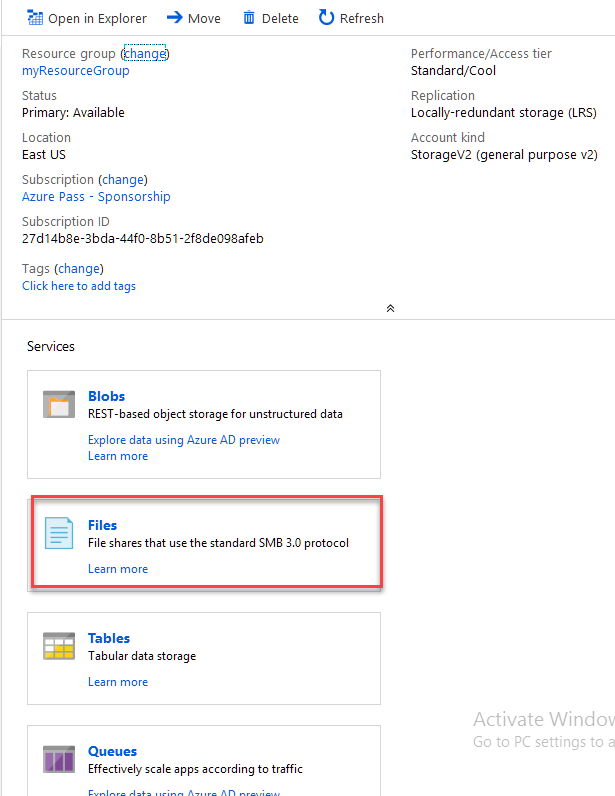
1. Select **+ Create a resource** on the upper, left corner of the Azure portal.
2. Select **Storage**, and then select **Storage account - blob, file, table, queue**
3. Then select **Create**.
4. Enter, or select, the following information, accept the remaining defaults, and then select **Review+Create** then **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) |
| Location | Select **East US** |
| Replication | Locally-redundant storage (LRS) |
| Subscription | Select your subscription |
| Resource group | Select **Use existing** and select *myResourceGroup*. |



**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:



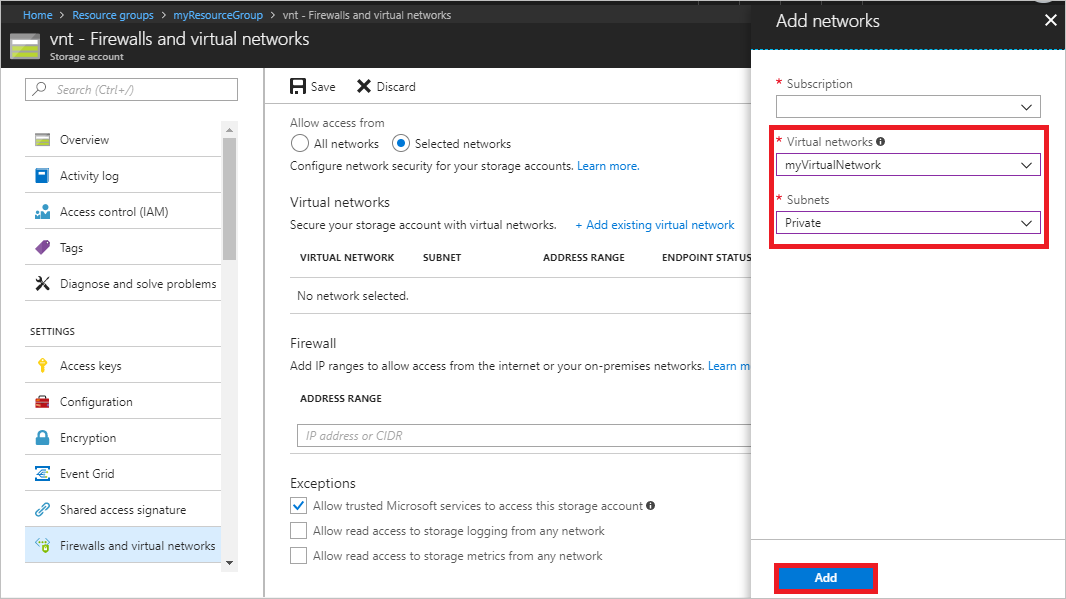
1. Select **+ File share**.
2. Enter *my-file-share* under **Name**, and then select **Create**.

**Task 7 Restrict network access to a subnet**

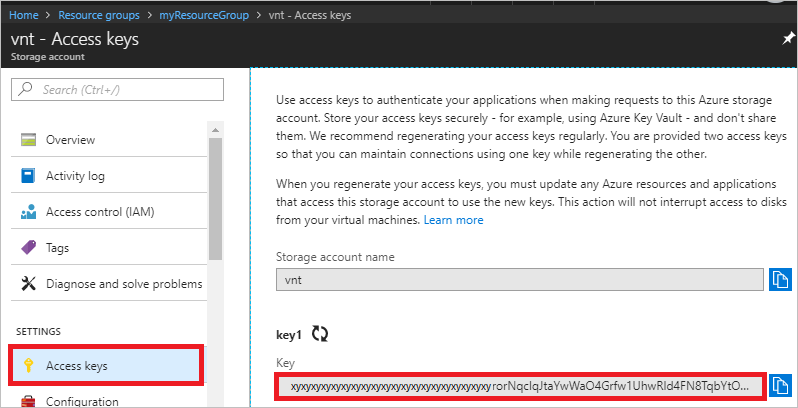
By default, storage accounts accept network connections from clients in any network, including the internet. Deny network access from the internet, and all other subnets in all virtual networks, except for the *Private* subnet in the *myVirtualNetwork* virtual network.

1. Under **SETTINGS** for the storage account, select **Firewalls and virtual networks**.
2. 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** |



1. Select **Save**.
2. Close the **Firewalls and virtual networks** box.
3. Under **SETTINGS** for the storage account, select **Access keys**, as shown in the following picture:



1. 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 virtual machines**

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

**Create the first virtual machine**

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**, then select **Create.**
3. Enter, or select, the following information and then select Review + Create:

| **Setting** | **Value** |
| --- | --- |
| Name | myVmPublic |
| User name | Enter a user name of your choosing like azureuser. |
| Password | Enter a password of your choosing. The password must be at least 12 characters long and meet the [defined complexity requirements](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/faq?toc=%2fazure%2fvirtual-network%2ftoc.json#what-are-the-password-requirements-when-creating-a-vm). Try **Pa55w.rd1234** |
| Subscription | Select your subscription. |
| Resource group | Select **Use existing** and select **myResourceGroup**. |
| Location | Select **East US**. |

1. Select the **Networking** tab, then select on the **Network Security Group** radio buttons, select **Basic**. Select port 3389, which you'll need open to connect to the virtual machine in a later step.
2. Select the **Public** subnet
3. Select **Review + Create**, then 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.

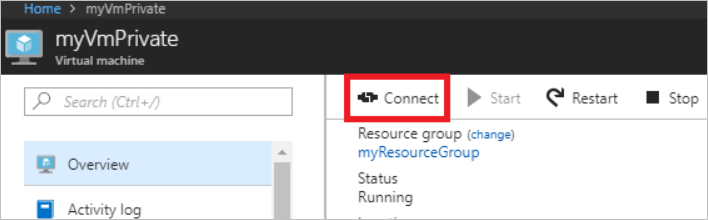
**Create the second virtual machine**

Complete steps 1-7 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 9 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:



1. After selecting the **Connect** button, a Remote Desktop Protocol (.rdp) file is created and downloaded to your computer.
2. 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.
3. Select **OK**.
4. 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.
5. 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 [Create a storage account](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-restrict-network-access-to-resources#create-a-storage-account).

PowerShell

$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:

PowerShell

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.

1. Ping
2. 8.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.

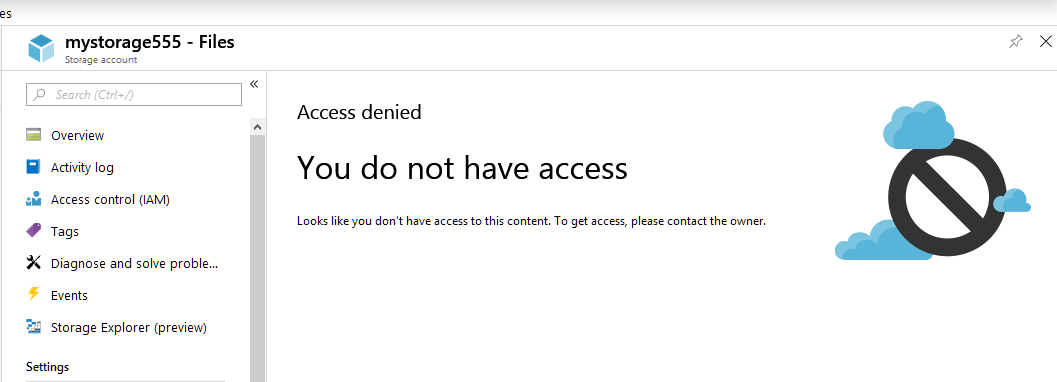
1. Close the remote desktop session VM.

**Task 10 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 and connect to it.
3. Complete steps 1-6 in [Confirm access to storage account](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-restrict-network-access-to-resources#confirm-access-to-storage-account) 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.

1. Close the remote desktop session to the *myVmPublic* VM.
2. From your computer, browse to the Azure [portal](https://portal.azure.com/).
3. 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.
4. Select **Files**.
5. 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.

**Lab 4A** **Configure a VNet-to-VNet VPN gateway connection by using the Azure portal**

* ‎ This lab shows you how to connect VNets by using the VNet-to-VNet connection type. In the lab, the virtual networks are in the same subscription, but in different resource groups. If your VNets are in different subscriptions, you can't create the connection in the portal.

Below are the values that will be used for each Virtual Network, Address Space, Subnet, and Gateway they will created or added.

**Values for TestVNet1:**

* VNet Name: TestVNet1
* Resource Group: TestRG1
* Location: East US
* TestVNet1: 10.11.0.0/16 & 10.12.0.0/16
* FrontEnd: 10.11.0.0/24
* BackEnd: 10.12.0.0/24
* GatewaySubnet: 10.12.255.0/27
* GatewayName: VNet1GW
* Public IP: VNet1GWIP
* VPNType: RouteBased
* Connection(1to4): VNet1toVNet4
* ConnectionType: VNet2VNet

**Values for TestVNet4:**

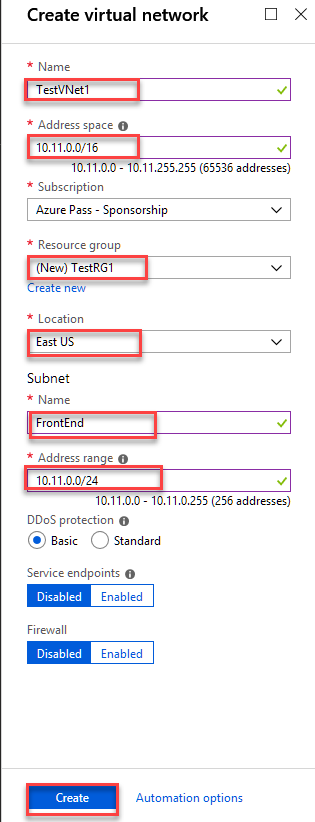
* VNet Name: TestVNet4
* TestVNet2: 10.41.0.0/16 & 10.42.0.0/16
* FrontEnd: 10.41.0.0/24
* BackEnd: 10.42.0.0/24
* GatewaySubnet: 10.42.255.0/27
* Resource Group: TestRG4
* Location: West US
* GatewayName: VNet4GW
* Public IP: VNet4GWIP
* VPNType: RouteBased
* Connection: VNet4toVNet1
* ConnectionType: VNet2VNet

**Task 1 Create and configure TestVNet1**

**Note**

For the VNet to connect to an on-premises location, coordinate with your on-premises network administrator to carve out an IP address range that you can use specifically for this virtual network. If a duplicate address range exists on both sides of the VPN connection, traffic will route in an unexpected way. Additionally, if you want to connect this VNet to another VNet, the address space cannot overlap with other VNet. Plan your network configuration accordingly.

1. Sign in to the [Azure portal](http://portal.azure.com/) and select **Create a resource**. The **New** page opens.
2. In the **Search the marketplace** field, enter *virtual network* and select **Virtual network** from the returned list. The **Virtual network** page opens.
3. From the **Select a deployment model** list near the bottom of the page, select **Resource Manager**, and then select **Create**. The **Create virtual network** page opens.
4. On the **Create virtual network** page, configure the VNet settings as shown in the picture. When you fill in the fields, the red exclamation mark becomes a green check mark when the characters you enter in the field are validated. Some values are autofilled, which you can replace with the ones in the picture:

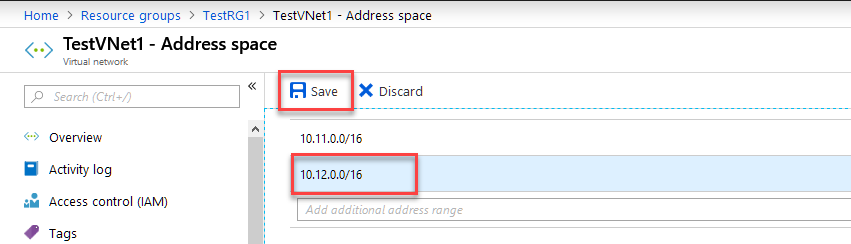


**Task 2 Add additional address space and create subnets**

You can add additional address space and create subnets once your VNet has been created.

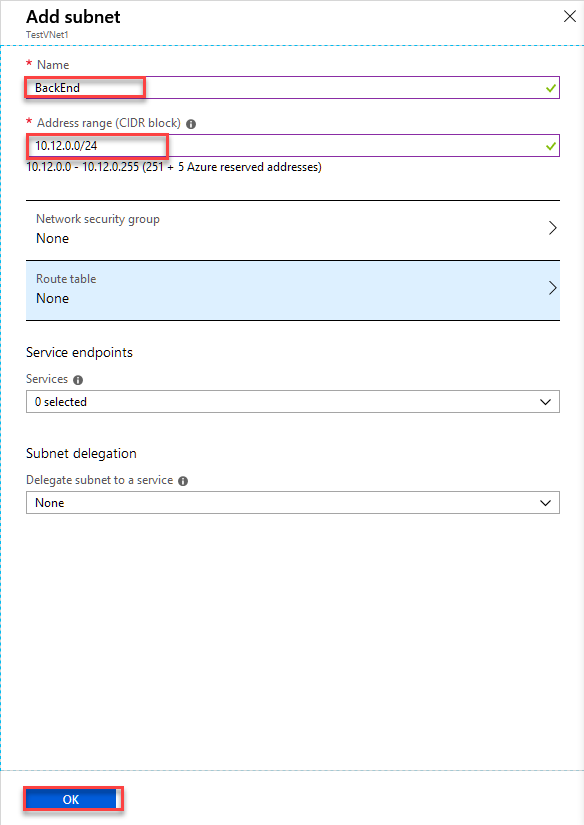
**To add additional address space**

1. To add additional address ranges to your address space, in the **Settings** section of your virtual network page, select **Address space**. The **Address space** page appears.
2. Add the additional address range, and then select **Save** at the top of the page.



**Task 3 To create additional subnets**

1. To create subnets, in the **Settings** section of your virtual network page, select **Subnets**. The **Subnets** page appears.
2. Select **+Subnet** to open the **Add subnet** page. Enter the **Name** of your new subnet and specify the **Address range** as shown in the picture.



1. To save your changes, select **OK** at the bottom of the page.

**Task 4 Create a gateway subnet**

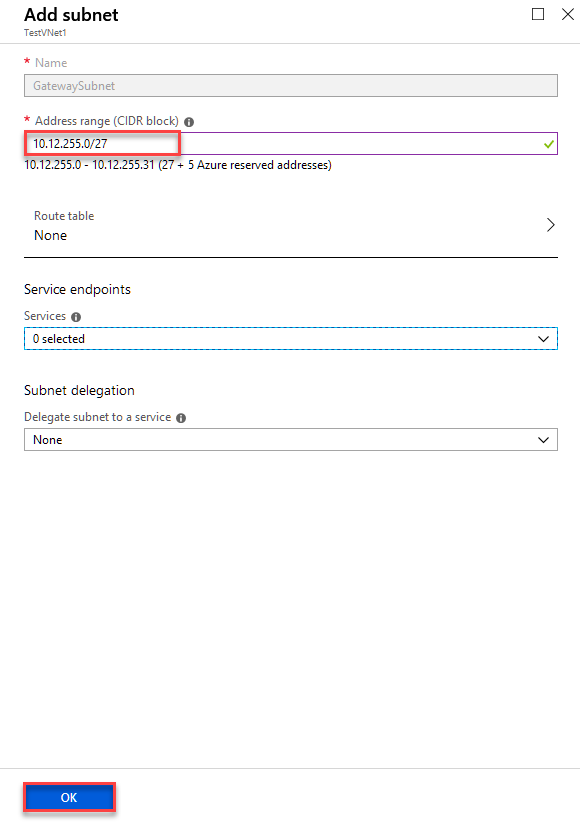
Before creating a virtual network gateway for your virtual network, you first need to create the gateway subnet. The gateway subnet contains the IP addresses that are used by the virtual network gateway. If possible, it's best to create a gateway subnet by using a CIDR block of /28 or /27 to provide enough IP addresses to accommodate future additional configuration requirements.

**Important**

When working with gateway subnets, avoid associating a network security group (NSG) to the gateway subnet. Associating a network security group to this subnet may cause your VPN gateway to stop functioning as expected.

**To create a gateway subnet**

1. On the **Subnets** page, select **+Gateway subnet** to open the **Add subnet** page.
2. The **Name** for your subnet is automatically autofilled with the value *GatewaySubnet*. This value is required for Azure to recognize the subnet as the gateway subnet. Adjust the autofilled **Address range** values to match your configuration requirements, then select **OK** to create the subnet.

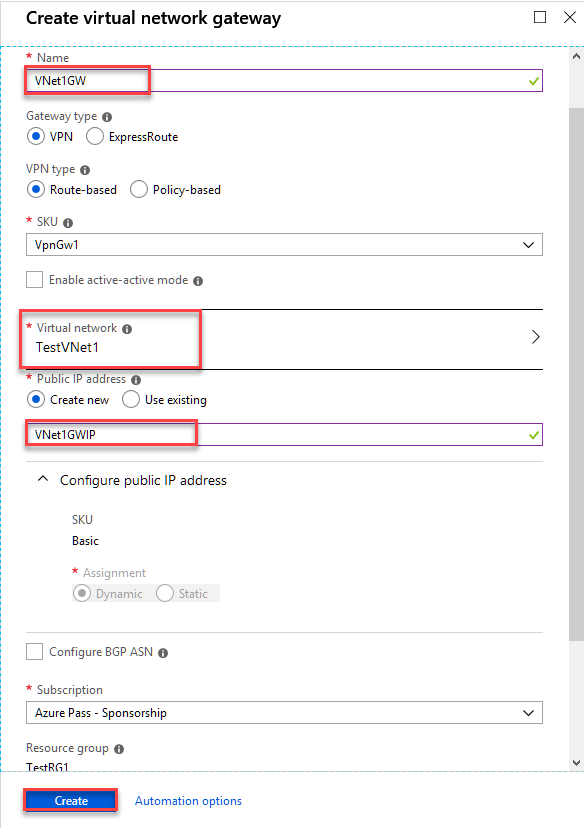


**Task 5 Create a virtual network gateway**

In this step, you create the virtual network gateway for your VNet. Creating a gateway can often take 45 minutes or more, depending on the selected gateway SKU.

**To create a virtual network gateway**

1. Sign in to the Azure portal and select **Create a resource**. The **New** page opens.
2. In the **Search the marketplace field**, enter *virtual network gateway*, and select **Virtual network gateway** from the search list.
3. On the **Virtual network gateway** page, select **Create** to open the **Create virtual network gateway** page.
4. On the **Create virtual network gateway** page, fill in the values for your virtual network gateway that are in the picture:



1. Verify the settings and select **Create** to begin creating the VPN gateway. The settings are validated and you'll see the **Deploying Virtual network gateway** tile on the dashboard. Creating a gateway can take up to 45 minutes. You may need to refresh your portal page to see the completed status.
2. After you create the gateway, verify the IP address that's been assigned to it by viewing the virtual network in the portal. The gateway appears as a connected device. You can select the connected device (your virtual network gateway) to view more information.

**Create and configure TestVNet4**

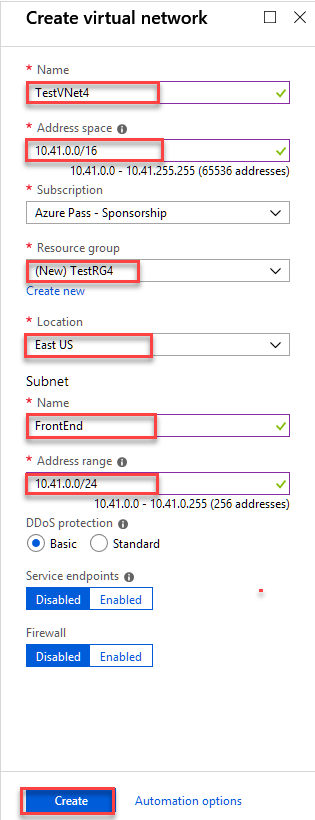
After you've configured TestVNet1, create TestVNet4 by repeating the previous steps and replacing the values with TestVNet4 values. You don't need to wait until the virtual network gateway for TestVNet1 has finished creating before you configure TestVNet4.

**Task 6 Create and configure TestVNet4**

**Note**

For the VNet to connect to an on-premises location, coordinate with your on-premises network administrator to carve out an IP address range that you can use specifically for this virtual network. If a duplicate address range exists on both sides of the VPN connection, traffic will route in an unexpected way. Additionally, if you want to connect this VNet to another VNet, the address space cannot overlap with other VNet. Plan your network configuration accordingly.

* 1. In the **Search the marketplace** field, enter *virtual network* and select **Virtual network** from the returned list. The **Virtual network** page opens.
  2. From the **Select a deployment model** list near the bottom of the page, select **Resource Manager**, and then select **Create**. The **Create virtual network** page opens.
  3. On the **Create virtual network** page, configure the VNet settings as shown in the picture. When you fill in the fields, the red exclamation mark becomes a green check mark when the characters you enter in the field are validated. Some values are autofilled, which you can replace with the ones in the picture:

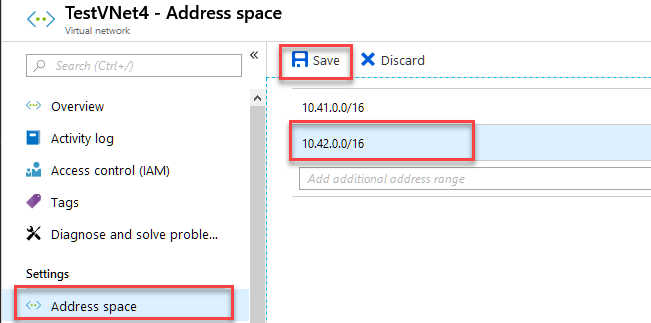


**Task 7 Add additional address space and create subnets**

You can add additional address space and create subnets once your VNet has been created.

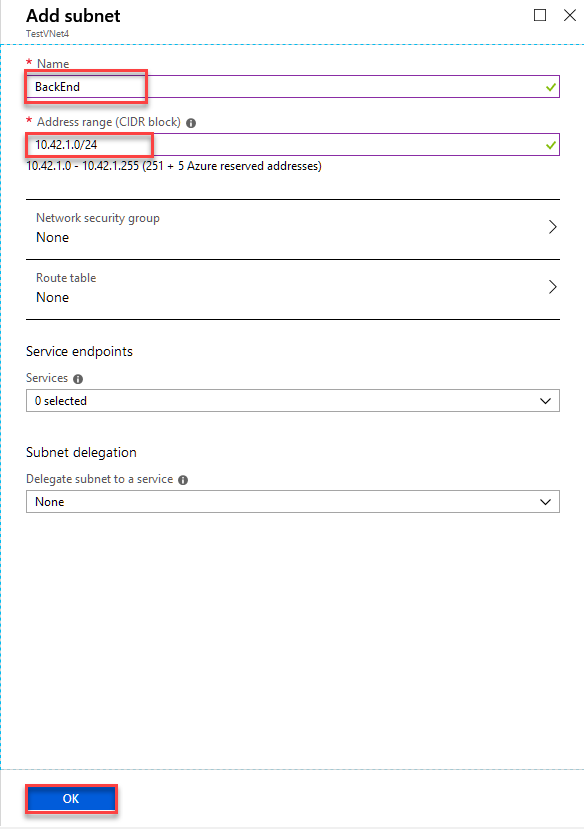
**To add additional address space**

1. To add additional address ranges to your address space, in the **Settings** section of your virtual network page, select **Address space**. The **Address space** page appears.
2. Add the additional address range, and then select **Save** at the top of the page.



**Task 8 To create additional subnets**

1. To create subnets, in the **Settings** section of your virtual network page, select **Subnets**. The **Subnets** page appears.
2. Select **+Subnet** to open the **Add subnet** page. Enter the **Name** of your new subnet and specify the **Address range** as shown in the picture.



1. To save your changes, select **OK** at the bottom of the page.

**Task 9 Create a gateway subnet**

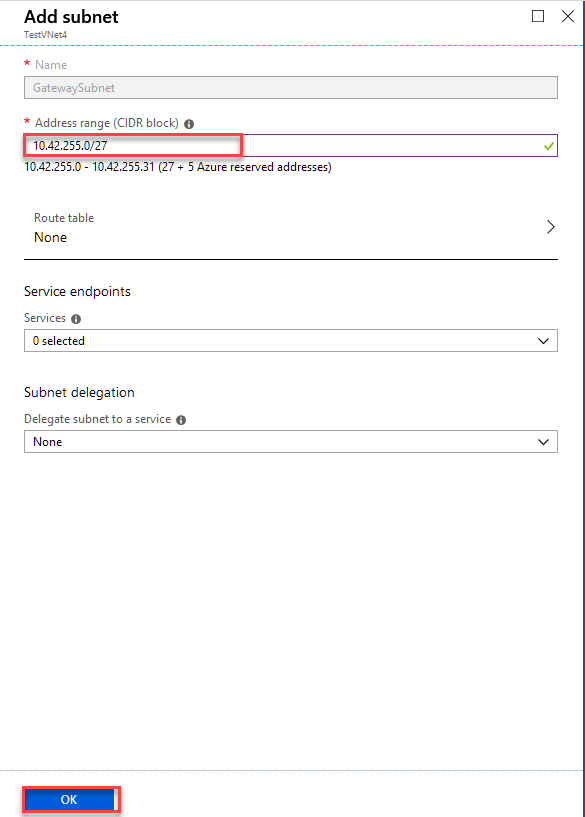
Before creating a virtual network gateway for your virtual network, you first need to create the gateway subnet. The gateway subnet contains the IP addresses that are used by the virtual network gateway. If possible, it's best to create a gateway subnet by using a CIDR block of /28 or /27 to provide enough IP addresses to accommodate future additional configuration requirements.

**Important**

When working with gateway subnets, avoid associating a network security group (NSG) to the gateway subnet. Associating a network security group to this subnet may cause your VPN gateway to stop functioning as expected.

**To create a gateway subnet**

1. On the **Subnets** page, select **+Gateway subnet** to open the **Add subnet** page.
2. The **Name** for your subnet is automatically autofilled with the value *GatewaySubnet*. This value is required for Azure to recognize the subnet as the gateway subnet. Adjust the autofilled **Address range** values to match your configuration requirements, then select **OK** to create the subnet.

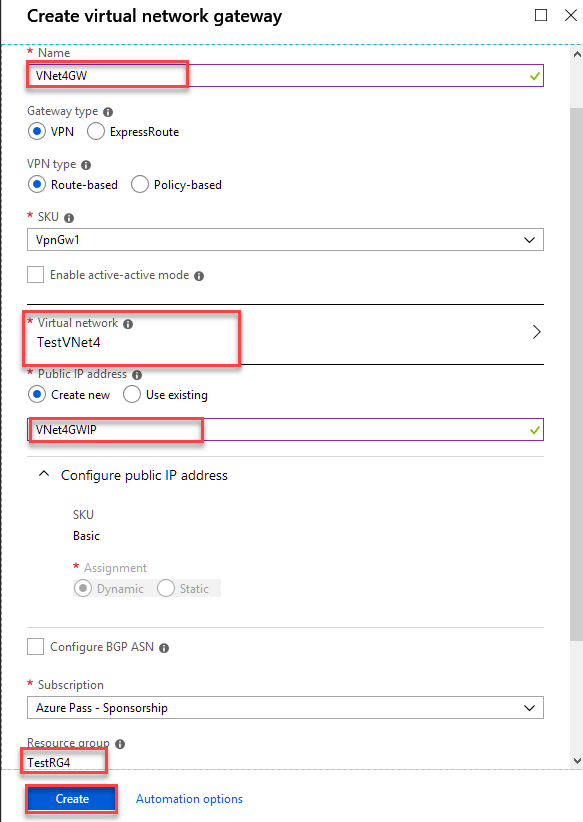


**Task 10 Create a virtual network gateway**

In this step, you create the virtual network gateway for your VNet. Creating a gateway can often take 45 minutes or more, depending on the selected gateway SKU.

**To create a virtual network gateway**

1. Sign in to the Azure portal and select **Create a resource**. The **New** page opens.
2. In the **Search the marketplace field**, enter *virtual network gateway*, and select **Virtual network gateway** from the search list.
3. On the **Virtual network gateway** page, select **Create** to open the **Create virtual network gateway** page.
4. On the **Create virtual network gateway** page, fill in the values for your virtual network gateway that are in the picture:

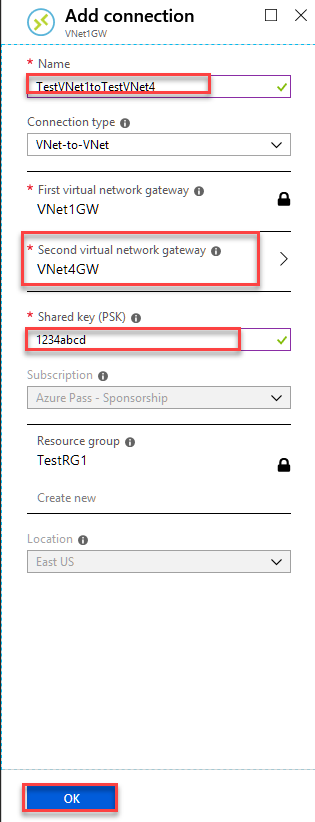


1. Verify the settings and select **Create** to begin creating the VPN gateway. The settings are validated and you'll see the **Deploying Virtual network gateway** tile on the dashboard. Creating a gateway can take up to 45 minutes. You may need to refresh your portal page to see the completed status.
2. After you create the gateway, verify the IP address that's been assigned to it by viewing the virtual network in the portal. The gateway appears as a connected device. You can select the connected device (your virtual network gateway) to view more information.

**Task 11 Configure the TestVNet1 gateway connection**

When the virtual network gateways for both TestVNet1 and TestVNet4 have completed, you can create your virtual network gateway connections. In this section, you create a connection from VNet1 to VNet4. These steps work only for VNets in the same subscription. If your VNets are in different subscriptions, you must use [PowerShell](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-vnet-vnet-rm-ps) to make the connection. However, if your VNets are in different resource groups in the same subscription, you can connect them by using the portal.

1. In the Azure portal, select **All resources**, enter *virtual network gateway* in the search box, and then navigate to the virtual network gateway for your VNet. For example, **TestVNet1GW**. Select it to open the **Virtual network gateway** page.
2. Under **Settings**, select **Connections**, and then select **Add** to open the **Add connection** page.
3. On the **Add connection** page, fill in the values for your connection:
   * **Name**: Enter a name for your connection. For example, *TestVNet1toTestVNet4*.
   * **Connection type**: Select **VNet-to-VNet** from the drop-down.
   * **First virtual network gateway**: This field value is automatically filled in because you're creating this connection from the specified virtual network gateway.
   * **Second virtual network gateway**: This field is the virtual network gateway of the VNet that you want to create a connection to. Select **Choose another virtual network gateway** to open the **Choose virtual network gateway** page.
     + View the virtual network gateways that are listed on this page. Notice that only virtual network gateways that are in your subscription are listed. If you want to connect to a virtual network gateway that isn't in your subscription, use the [PowerShell](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-vnet-vnet-rm-ps).
     + Select the virtual network gateway to which you want to connect.
     + **Shared key (PSK)**: In this field, enter a shared key for your connection. You can generate or create this key yourself. In a site-to-site connection, the key you use is the same for your on-premises device and your virtual network gateway connection. The concept is similar here, except that rather than connecting to a VPN device, you're connecting to another virtual network gateway.
4. Select **OK** to save your changes.



**Task 11 Test the Connection**

* 1. Wait a few minutes and then Run the following powershell command

Get-AzureRmVirtualNetworkGatewayConnection -Name TestVNet1toTestVNet4 -ResourceGroupName TestRG1



**Note** It might a take a few minutes to show connected.

**Lab 4B** **Connect virtual networks with virtual network peering using the Azure portal**

* ‎**Task 1** **Log in to Azure**

Log in to the Azure portal at [https://portal.azure.com](https://portal.azure.com/).

**Task 2 Create virtual networks**

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**:

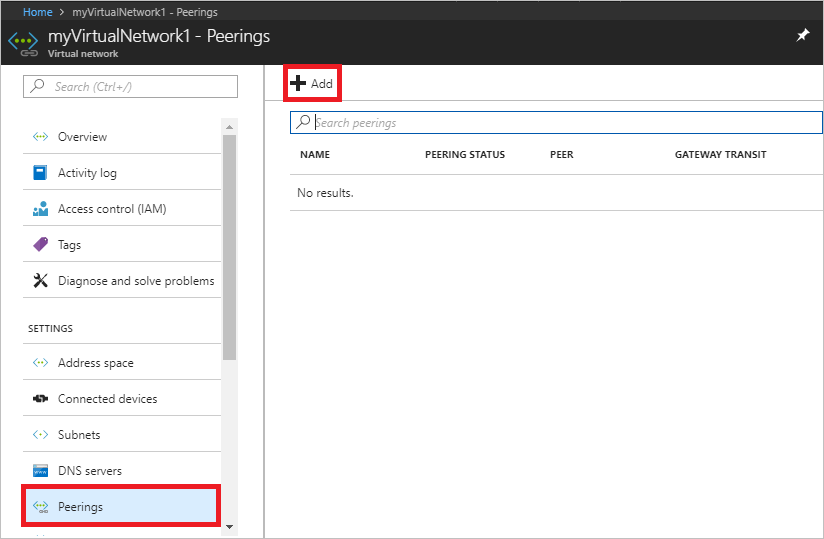
| **Setting** | **Value** |
| --- | --- |
| Name | myVirtualNetwork1 |
| Address space | 10.0.0.0/16 |
| Subscription | Select your subscription. |
| Resource group | Select **Create new** and enter *myResourceGroup*. |
| Location | Select **East US**. |
| Subnet Name | Subnet1 |
| Subnet Address range | 10.0.0.0/24 |

1. Complete steps 1-3 again, with the following changes:

| **Setting** | **Value** |
| --- | --- |
| Name | myVirtualNetwork2 |
| Address space | 10.1.0.0/16 |
| Resource group  Subnet Name | Select **Use existing** and then select **myResourceGroup**.  Subnet1 |
| Subnet Address range | 10.1.0.0/24 |

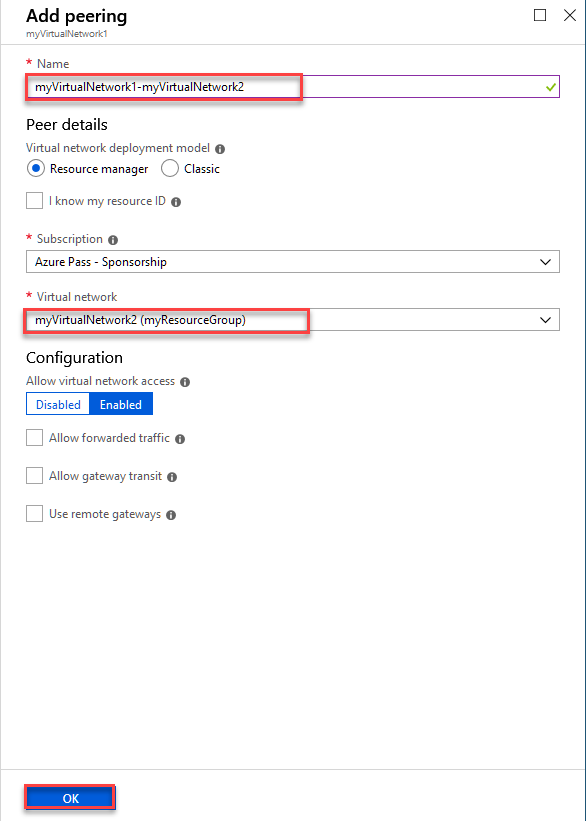
**Task 3 Peer virtual networks**

1. In the Search box at the top of the Azure portal, begin typing *MyVirtualNetwork1*. When **myVirtualNetwork1** appears in the search results, select it.
2. Select **Peerings**, under **SETTINGS**, and then select **+ Add**, as shown in the following picture:

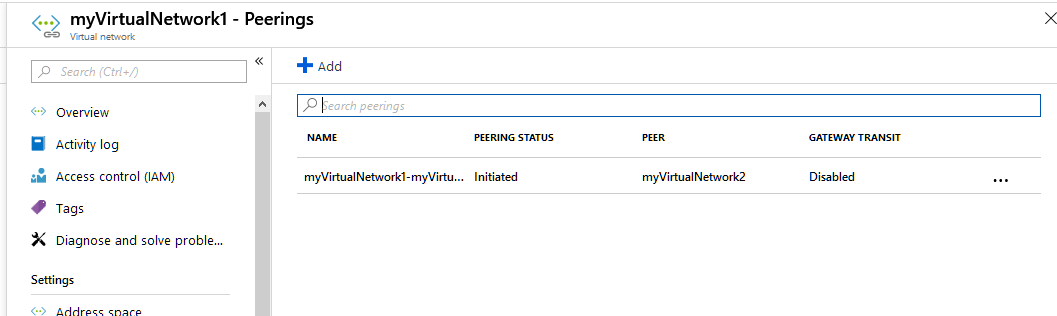


1. Enter, or select, the following information, accept the defaults for the remaining settings, and then select **OK**.

| **Setting** | **Value** |
| --- | --- |
| Name | myVirtualNetwork1-myVirtualNetwork2 |
| Subscription | Select your subscription. |
| Virtual network | myVirtualNetwork2 - To select the *myVirtualNetwork2* virtual network, select **Virtual network**, then select **myVirtualNetwork2**. You can select a virtual network in the same region or in a different region. |



1. The **PEERING STATUS** is *Initiated*, as shown in the following picture:



1. If you don't see the status, refresh your browser.
2. In the **Search** box at the top of the Azure portal, begin typing *MyVirtualNetwork2*. When **myVirtualNetwork2** appears in the search results, select it.
3. Complete steps 2-3 again for *myVirtualNetwork2*, with the following changes, and then select **OK**:

| **Setting** | **Value** |
| --- | --- |
| Name | myVirtualNetwork2-myVirtualNetwork1 |
| Virtual network | myVirtualNetwork1 |

1. The **PEERING STATUS** is *Connected*. Azure also changed the peering status for the *myVirtualNetwork2-myVirtualNetwork1* peering from *Initiated* to *Connected.* Virtual network peering is not fully established until the peering status for both virtual networks is *Connected.*

**Task 4 Create virtual machines**

Create a VM in each virtual network so that you can communicate between them in a later step.

**Create the first VM**

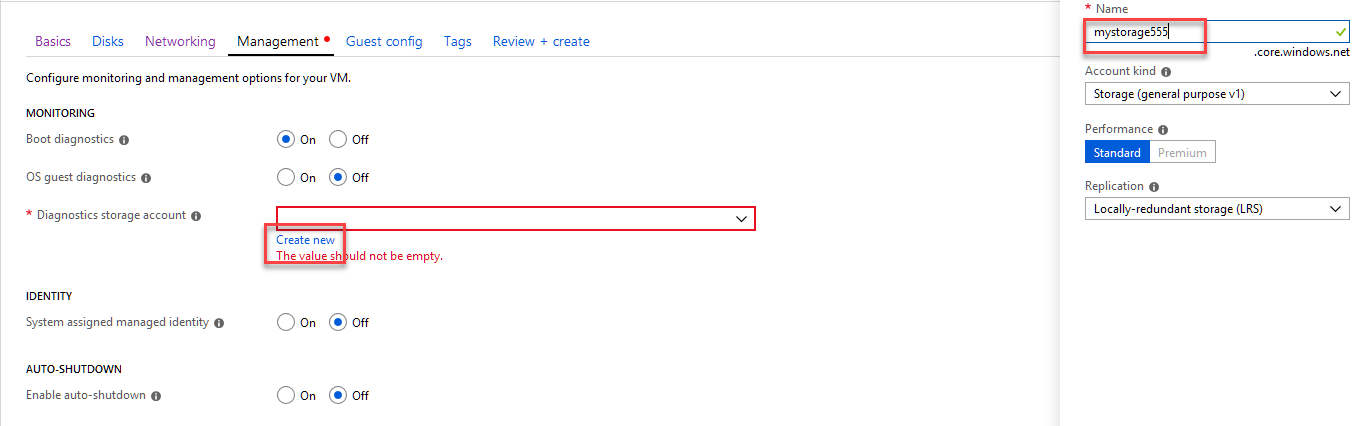
1. Select **+ Create a resource** on the upper, left corner of the Azure portal.
2. Select **Compute**, and then select **Windows Server 2016 Datacenter**. You can select a different operating system, but the remaining steps assume you selected **Windows Server 2016 Datacenter**.
3. Enter, or select, the following information for **Basics**:

| **Setting** | **Value** |
| --- | --- |
| Name | myVm1 |
| 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](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/faq?toc=%2fazure%2fvirtual-network%2ftoc.json#what-are-the-password-requirements-when-creating-a-vm). |
| Resource group | Select **Use existing** and then select **myResourceGroup**. |
| Location | Select **East US**. |

1. Then select the **Networking** tab and select the following values.

| **Setting** | **Value** |
| --- | --- |
| Virtual network | myVirtualNetwork1 - If it's not already selected, select **Virtual network** and then select **myVirtualNetwork1** under **Choose virtual network**. |
| Subnet  Public Inbound Ports | Subnet1 - If it's not already selected, select **Subnet** and then select **Subnet1** under **Choose subnet**.  Open Port 3389 for RDP |

1. Under **Create** in the **Summary**, select **Create** to start the VM deployment.
2. If a Validation Error occurs it is probably beucase of the Management configuration which can be fixed by the following picture:



**Task 5 Create the second VM**

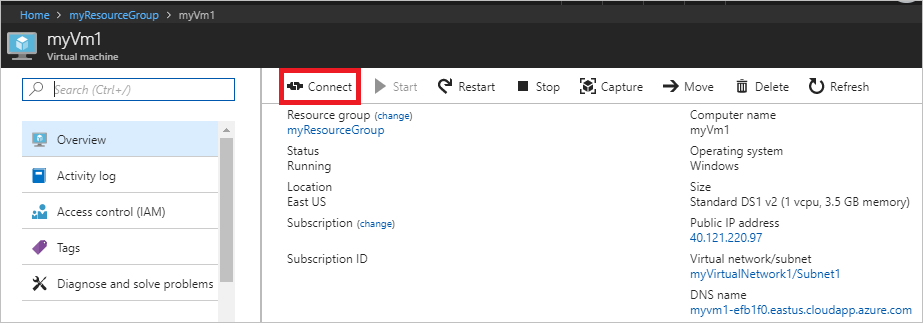
Complete steps 1-5 again, with the following changes:

| **Setting** | **Value** |
| --- | --- |
| Name | myVm2 |
| Virtual network | myVirtualNetwork2 |

The VMs take a few minutes to create. Do not continue with the remaining steps until both VMs are created.

**Task 6 Communicate between VMs**

1. In the *Search* box at the top of the portal, begin typing *myVm1*. When **myVm1** appears in the search results, select it.
2. Create a remote desktop connection to the *myVm1* VM by selecting **Connect**, as shown in the following picture:



1. To connect to the VM, open the downloaded RDP file. If prompted, select **Connect**.
2. 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**.
3. You may receive a certificate warning during the sign-in process. Select **Yes** to proceed with the connection.
4. In a later step, ping is used to communicate with the *myVm2* VM from the *myVm1* VM. Ping uses the Internet Control Message Protocol (ICMP), which is denied through the Windows Firewall, by default. On the *myVm1* VM, enable ICMP through the Windows firewall, so that you can ping this VM from *myVm2* in a later step, using PowerShell:

PowerShell

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

Though ping is used to communicate between VMs in this tutorial, allowing ICMP through the Windows Firewall for production deployments is not recommended.

1. To connect to the *myVm2* VM, enter the following command from a command prompt on the *myVm1* VM:

mstsc /v:10.1.0.4

1. Since you enabled ping on *myVm1*, you can now ping it by IP address:

ping 10.0.0.4

1. Disconnect your RDP sessions to both *myVm1* and *myVm2*.