Practice - Creating Virtual Networks

In this demonstration, you will create virtual networks.

Note: You can use the suggested values for the settings, or your own custom values if you prefer.

Create a virtual network in the portal

1. Sign in the to the Azure portal and search for **Virtual Networks**.
2. On the Virtual Networks page, click **Add**.

    - **Name**: *myVNet1*.
    - **Address**:*10.1.0.0/16*.
    - **Subscription**: Select your subscription.
    - **Resource group**: Select new or choose an existing resource group
    - **Location** - Select your location
    - **Subnet** - Enter *mySubnet1*.
    - **Subnet - Address range**: *10.1.0.0/24*

3. Leave the rest of the default settings and select **Create**.
4. Verify your virtual network was created.

Create a virtual network using PowerShell

1. Create a virtual network. Use values as appropriate.`$myVNet2 = New-AzVirtualNetwork -ResourceGroupName myResourceGroup -Location EastUS -Name myVNet2 -AddressPrefix 10.0.0.0/16`
2. Verify your new virtual network information.`Get-AzVirtualNetwork -Name myVNet2`
3. Create a subnet. Use values as appropriate.`$mySubnet2 = Add-AzVirtualNetworkSubnetConfig -Name mySubnet2 -AddressPrefix 10.0.0.0/24 -VirtualNetwork $myVNet2`
4. Verify your new subnet information.`Get-AzVirtualNetworkSubnetConfig -Name mySubnet2 -VirtualNetwork $myVNet2`
5. Associate the subnet to the virtual network.`$mySubnet2 | Set-AzVirtualNetwork`
6. Return to the portal and verify your new virtual network with subnet was created.

Practice - Create VMs with Multiple NICs

In this demonstration, you will learn how to create and configure multiple NICs and then attach those NICs to a VM. You can replace example parameter names with your own values if you prefer.

This demonstration uses the Azure CLI and assumes the following preparatory steps:

1. You are using the latest version of the Azure CLI and are logged in to your Azure account.
2. You have created a resource group in an appropriate location and a virtual network with a subnet, an additional backend subnet, and a network security group.For example, using **az network vnet create**, create a virtual network named *myVnet* and subnet named *mySubnetFrontEnd*:

```
az network vnet create \
    --resource-group myResourceGroup \
    --name myVnet \
    --address-prefix 10.0.0.0/16 \
    --subnet-name mySubnetFrontEnd \
    --subnet-prefix 10.0.1.0/24
```

3. Using **az network vnet subnet** create a subnet for the back-end traffic named *mySubnetBackEnd*:

```
az network vnet subnet create \
    --resource-group myResourceGroup \
    --vnet-name myVnet \
    --name mySubnetBackEnd \
    --address-prefix 10.0.2.0/24
```

4. Now using **az network nsg create**, create a network security group named *myNetworkSecurityGroup*:

```
az network nsg create \
    --resource-group myResourceGroup \
    --name myNetworkSecurityGroup
```

Create and configure multiple NICs

- Using **az network nic create**, create two NICs, named *myNic1* and *myNic2*, connect the network security group,
  with one NIC connecting to each subnet:

```
az network nic create \
    --resource-group myResourceGroup \
    --name myNic1 \
    --vnet-name myVnet \
    --subnet mySubnetFrontEnd \
    --network-security-group myNetworkSecurityGroup
```

Create a VM and attach the NICs

- When you create the VM, specify the NICs you created with the *–nics* parameter. You also need to take care when you select the VM size. There are limits for the total number of NICs that you can add to a VM. Using **az vm create**, create a Linux VM named *myVM*:

```
az vm create \
    --resource-group myResourceGroup \
    --name myVM \
    --image UbuntuLTS \
    --size Standard_DS3_v2 \
    --admin-username azureuser \
    --generate-ssh-keys \
    --nics myNic1 myNic2
```

Note: Return to the portal and verify the virtual machine now has two interfaces.

Practice - Manage IP Addresses

In this practice, you will learn how to retrieve static private IP address information for a network interface. You will run PowerShell commands to view the static private IP address information for the VM that was created in the previous demonstration. You will also remove the static private IP address that was added to the VM.

Retrieve static private IP address information

1. To view the static private IP address information for the VM created with the script above, run the following PowerShell command and note the values for PrivateIpAddress and PrivateIpAllocationMethod:

```
Get-AzNetworkInterface -Name TestNIC -ResourceGroupName TestRG
```

2. Review the information returned which includes: Name, ResourceGroupName, Location, Id, ProvisioningState, VirtualMachine, IpConfigurations, DnsSettings, EnableIPForwarding, and NetworkSecurityGroup. The information also includes whether the NIC is primary.

3. Notice in the IpConfigurations area there is a PrivateIPAddress and the PrivateIpAllocationMethod is static.

Remove a static private IP address

1. To remove the static private IP address added to the VM in the previous demonstration, run the following PowerShell commands:

```
$nic=Get-AzNetworkInterface -Name TestNIC -ResourceGroupName
TestRG
$nic.IpConfigurations[0].PrivateIpAllocationMethod = "Dynamic"
Set-AzNetworkInterface -NetworkInterface $nic
```

2. Review the output.

3. Notice in the IpConfigurations area, The PrivateIPAllocationMethod is now Dynamic.

Practice - Service Endpoints

In this demonstration, you will work with virtual network endpoints.

Note: This demonstration requires a Storage Account with an uploaded file. **Note**: You could use Storage Explorer (Preview) in the portal.

Create a storage account

1. Create a **Storage Account**.
2. Within the Storage Account, create a **file share**, and **upload** a file.
3. For the Storage Account, use the **Shared Access Signature** blade to **Generate SAS and connection string**.
4. Use Storage Explorer and the connection string to access the file share.
5. Ensure you can view your uploaded file.

Note: This part of the demonstration requires a virtual network with a subnet.

Create a subnet service endpoint

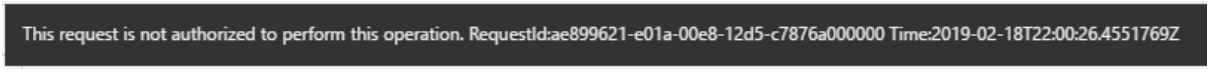
1. Select your virtual network, and then select a subnet in the virtual network.
2. Under **Service Endpoints**, view the **Services** drop-down and the different services that can be secured with an endpoint.
3. Check the **Microsoft.Storage** option.
4. **Save** your changes.

Secure the storage to the service endpoint

1. Return to your **storage account**.
2. Select **Firewalls and virtual networks**.
3. Change to **Selected networks**.
4. Add existing virtual network, verify your subnet with the new service endpoint is listed.
5. **Save** your changes.

Test the storage endpoint

1. Return to the Storage Explorer.
2. **Refresh** the storage account.
3. You should now have an access error similar to this one:



Note: If you plan to use the storage account in other scenarios be sure to return the account to **All networks** in the **Firewalls and virtual networks** blade.

Practice - Custom Routing Tables

In this demonstration, you will learn how to create a route table, define a custom route, and associate the route with a subnet.

Note: This demonstration requires a virtual network with at least one subnet.

Create a routing table

1. Access the Azure portal.
2. On the upper-left side of the screen, select **Services**, and then navigate to **Route tables**.
3. Select **+ Add**.

    - **Name**: *myRouteTablePublic*
    - **Subscription**: *select your subscription*
    - **Resource group**: *create or select a resource group*
    - **Location**: *select your location*
    - **BGP route propagation**: *Enabled*

4. Select **Create**.
5. Wait for the new routing table to be deployed.

Add a route

1. Select your new routing table, and then select **Routes**.
2. Select **+ Add**.

    - **Name**: *ToPrivateSubnet*
    - **Address prefix**: *10.0.1.0/24*
    - **Next hop type**: *Virtual appliance*
    - **Next hop address**: *10.0.2.4*

3. Read the information note: Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.
4. Select **Create**.
5. Wait for the new route to be deployed.

Associate a route table to a subnet

1. Navigate to the subnet you want to associate with the routing table.
2. Select **Route table**.
3. Select your new routing table, **myRouteTablePublic**.
4. **Save** your changes.

Use PowerShell to view your routing information

1. Open the Cloud Shell.
2. View information about your new routing table.

```
Get-AzRouteTable
```

3. Verify the **Routes** and **Subnet** information is correct.

Practice - VNet to VNet Connections

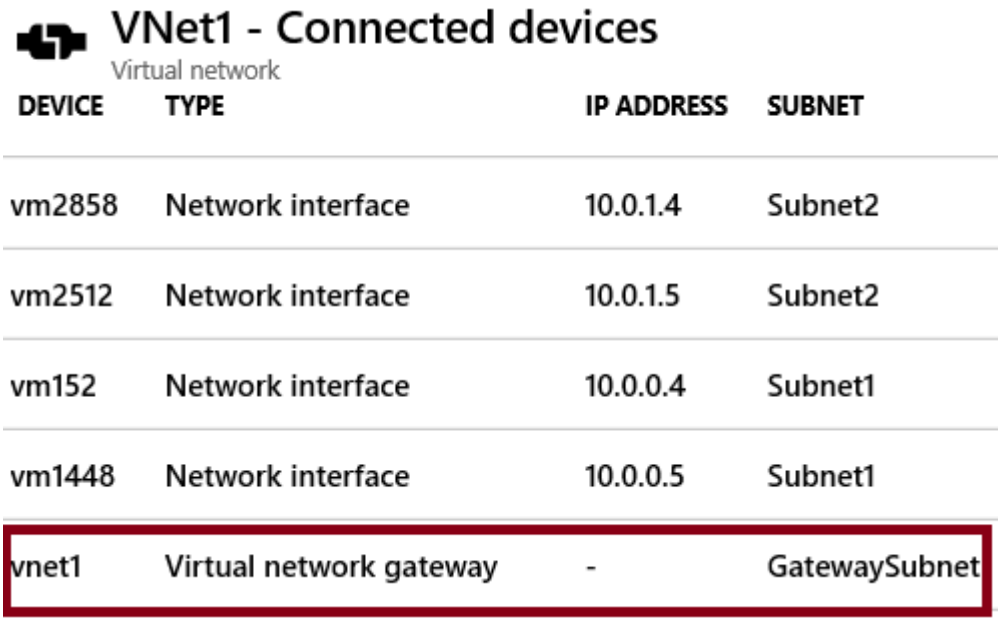
Note: This demonstration works best with two virtual networks with subnets. All the steps are in the portal.

Explore the Gateway subnet blade

1. For one of your virtual network, select the **Subnets** blade.
2. Select **+ Gateway subnet**.
   Notice the name of the subnet cannot be changed.
   Notice the **address range** of the gateway subnet. The address must be contained by the address space of the virtual network.
3. Remember each virtual network needs a gateway subnet.
4. Close the Add gateway subnet page. You do not need to save your changes.

Explore the Connected Devices blade

1. For the virtual network, select the **Connected Devices** blade.
2. After a gateway subnet is deployed it will appear on the list of connected devices.



Explore adding a virtual network gateway

1. Search for **Virtual network gateways**.
2. Click **+ Add**.

3. Review each setting for the virtual netowrk gateway.
4. Use the Information icons to learn more about the settings.
5. Notice the **Gateway type**, **VPN type**, and **SKU**.
6. Notice the need for a **Public IP address**.
7. Remember each virtual network will need a virtual network gateway.
8. Close the Add virtual network gateway. You do not need to save your changes.

Explore adding a connection between the virtual networks

1. Search for **Connections**.
2. Click **+ Add**.
3. Notice the **Connection type** can be VNet-to-VNet, Site-to-Site (IPsec), or ExpressRoute.
4. Provide enough information, so you can click the **Ok** button.
5. On the **Settings** page, notice that you will need select the two different virtual networks.
6. Read the Help information on the **Establilsh bidirectional connnectivity** checkbox.
7. Notice the **Shared key (PSK)** information.
8. Close the Add connection page. You do not need to save your changes.