Welcome to the Microsoft Azure Infrastructure as a Service hosted lab

---

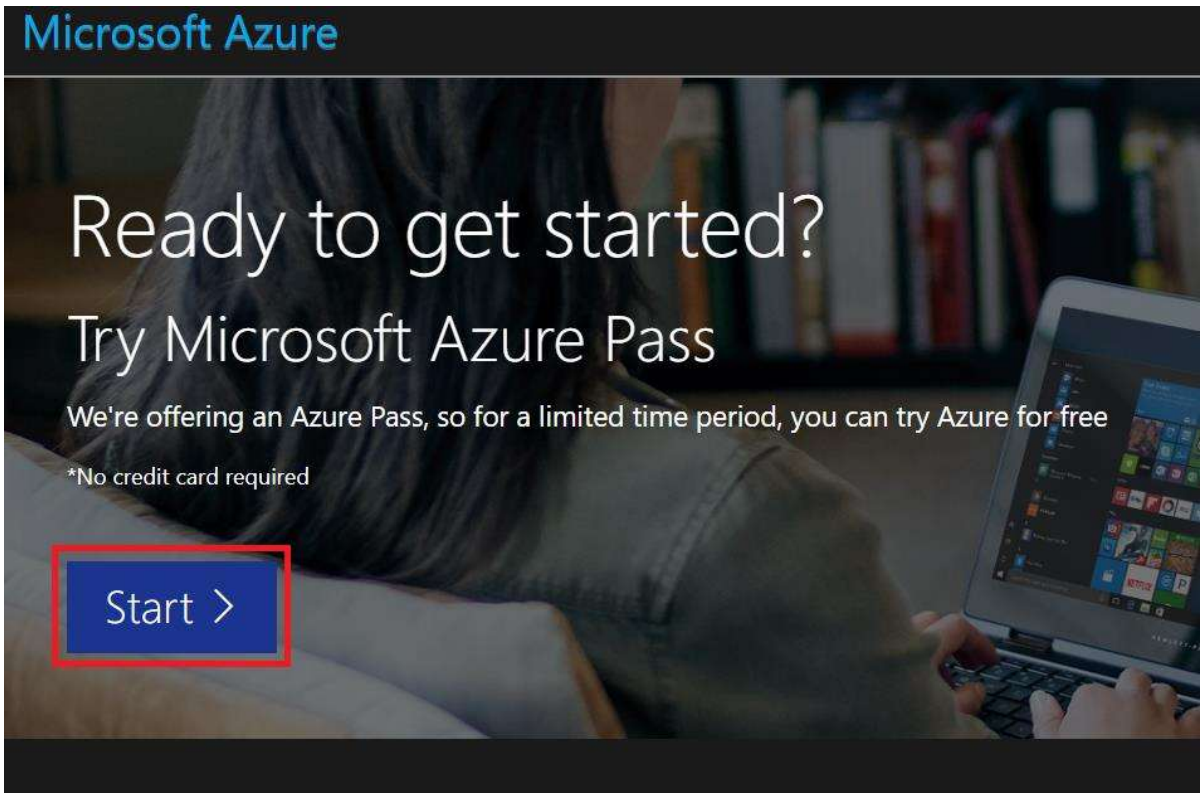
Complete the following tasks to prepare your Azure Trial Pass subscription and initialize your lab environment.

Prepare your Azure Trial Pass subscription

During the course of this lab, you will be using an **Azure Trial Pass** subscription that is valued at **$100** and activated for **7 days**. The subscription will be deactivated once the **$100** limit is reached or the **7 days** have past, whichever comes first. The following steps will be used to activate your **Azure Trial Pass** subscription.

☐ 1. A new Microsoft account is required to activate your **Azure Trial Pass** subscription, navigate to: T **https://outlook.live.com/owa/** and create a new Microsoft account. **This step must be followed in order to avoid potential activation issues with pre-existing Work, School or Microsoft accounts.**

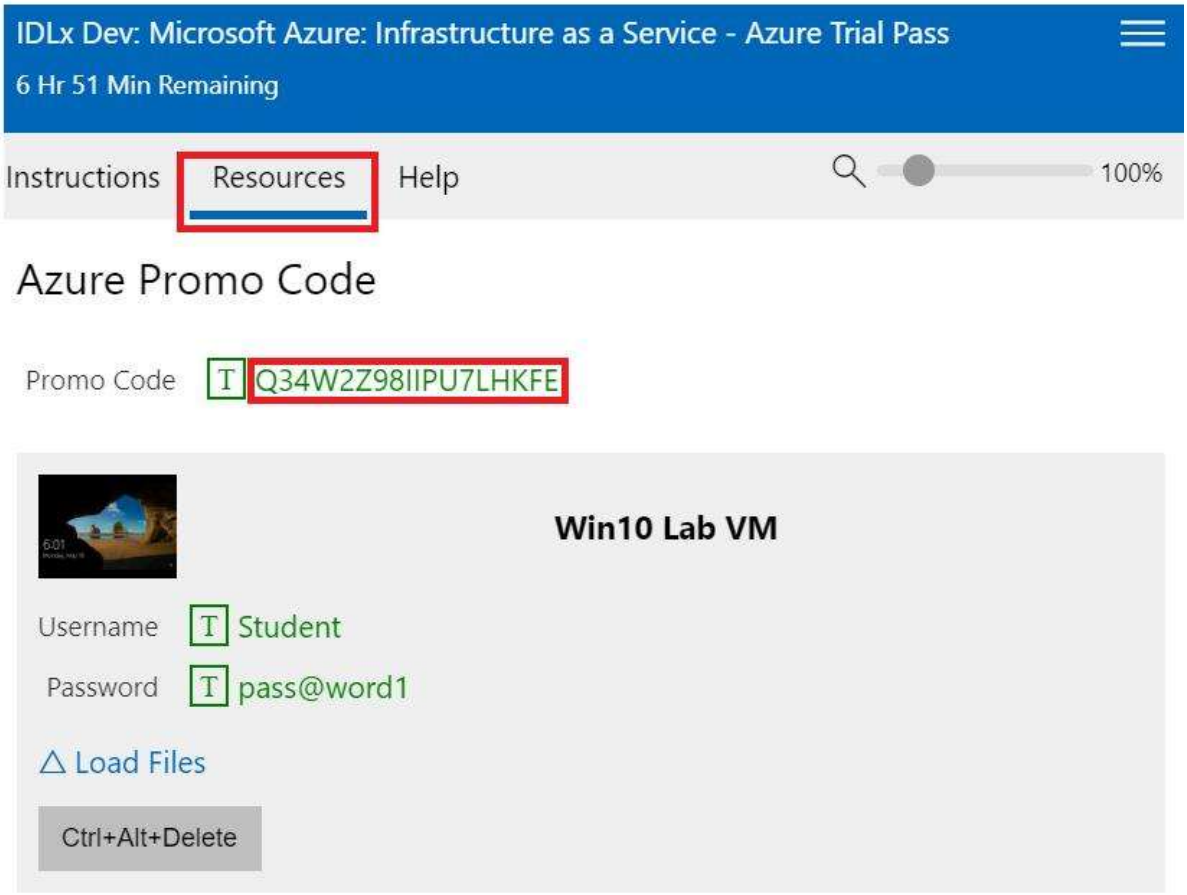
☐ 2. Open an **inPrivate** browser session and navigate to T **https://www.microsoftazurepass.com/** and click the **Start >** tile.



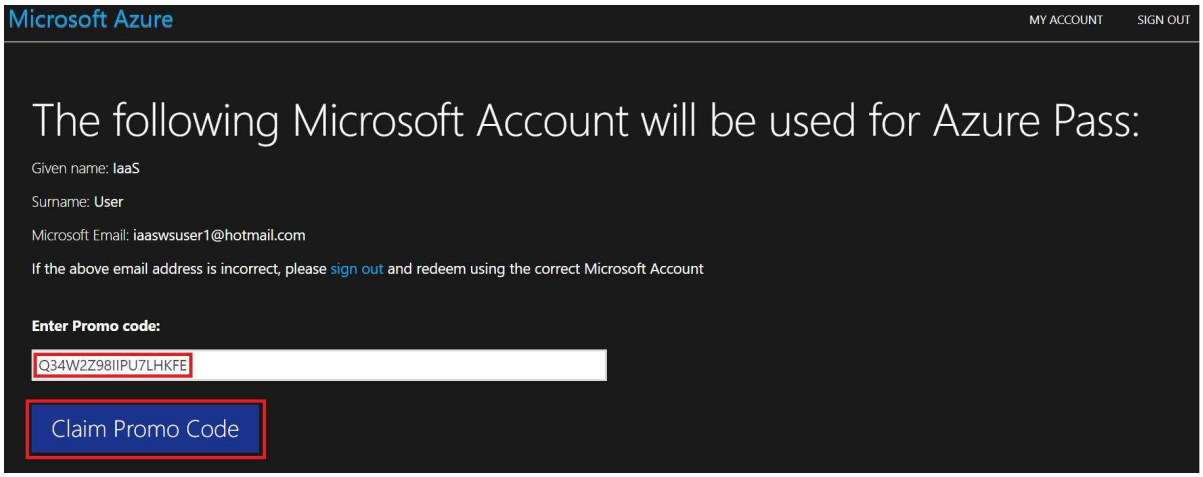
☐ 3. Sign in using the Microsoft account that was created earlier.

☐ 4. Confirm that the correct Microsoft account has been selected and click the **Confirm Microsoft Account >** tile.

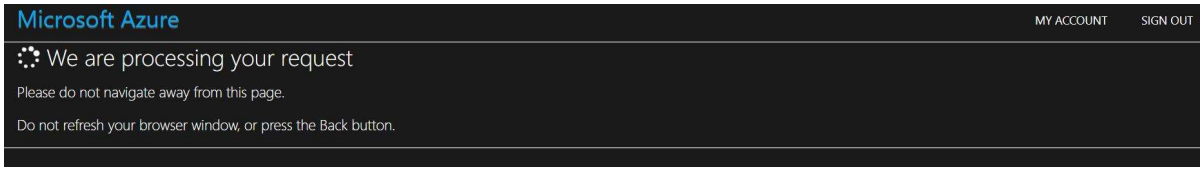
☐ 5. From within the hosted lab environment, click the **Resources** tab on the top menu bar and copy the **Azure Promo Code** value without the preceding T



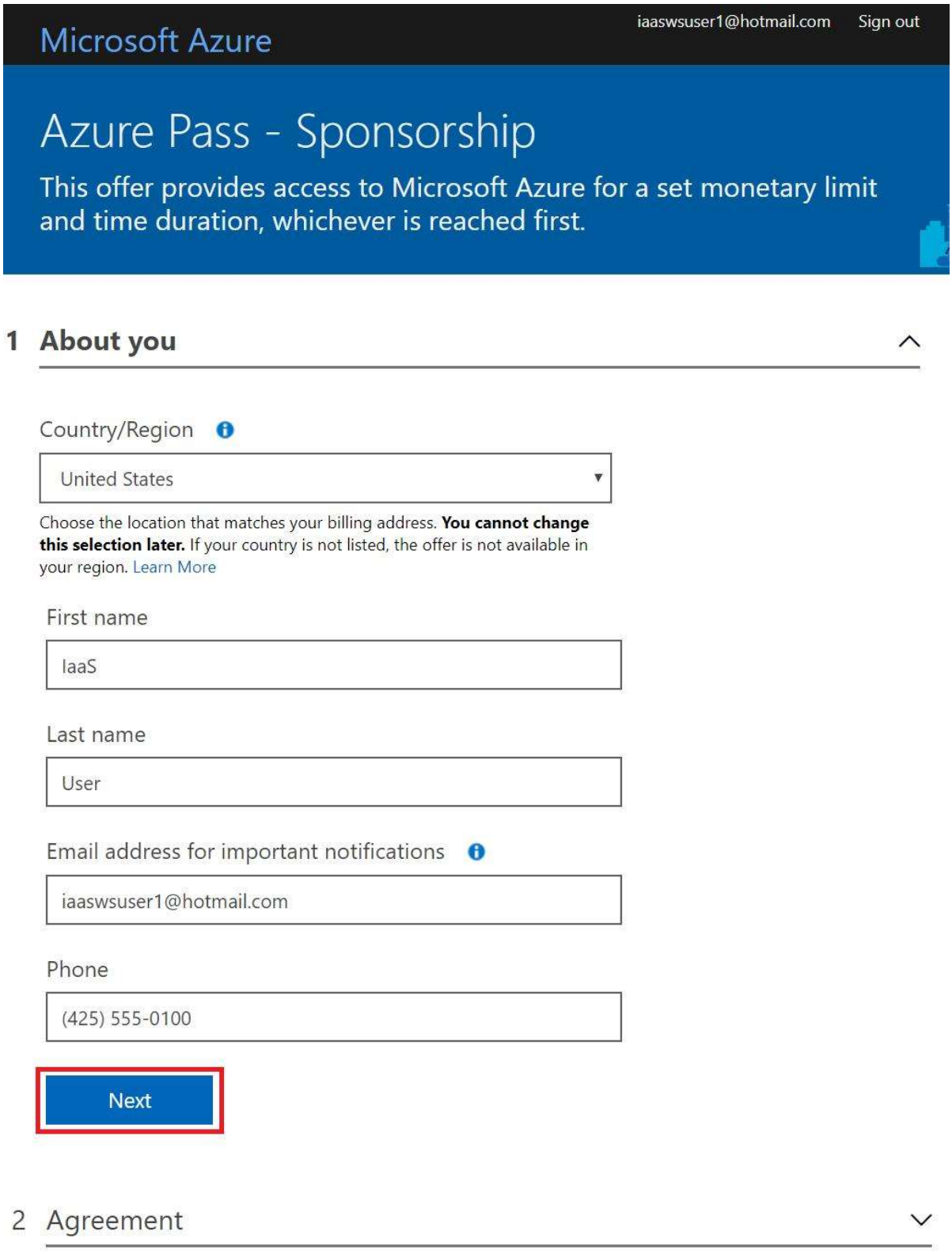
☐ 6. Paste that value into the **Enter Promo code:** box and click the **Claim Promo Code** tile.



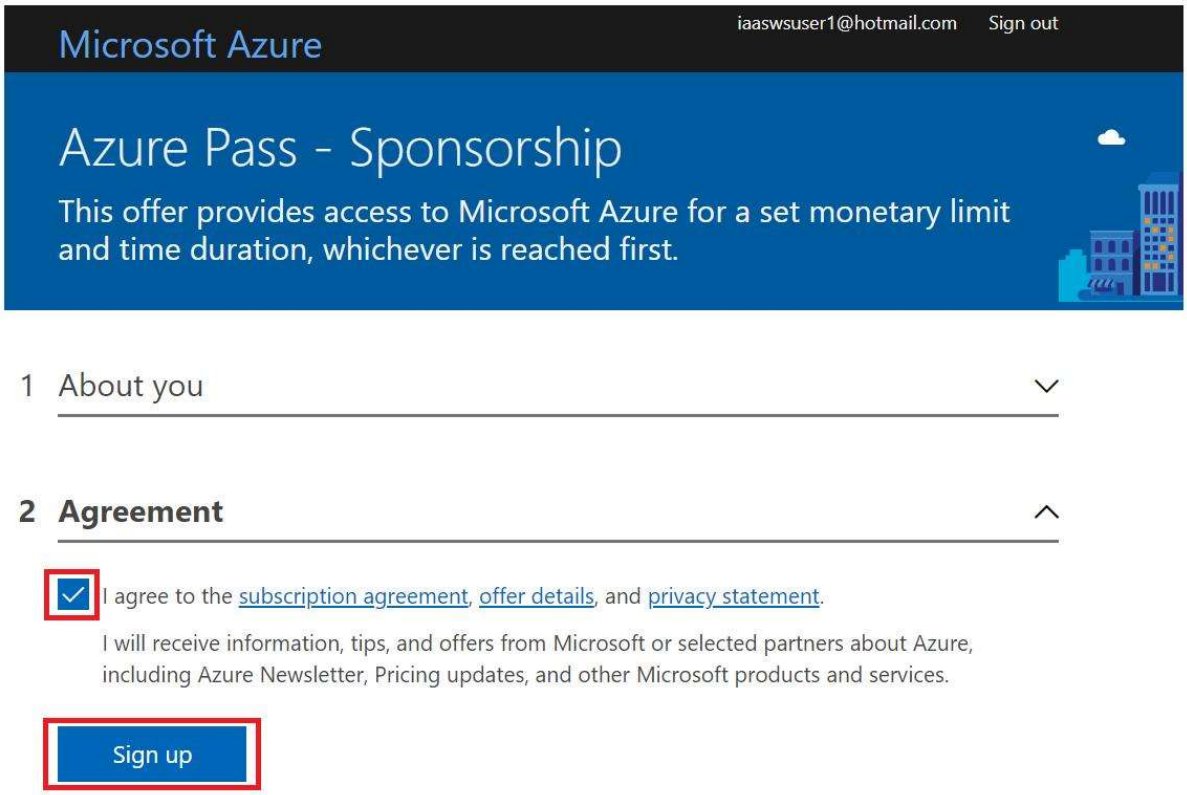
☐ 7. Confirm that your request is being processed and **do not refresh your browser or press the Back button** during this time.



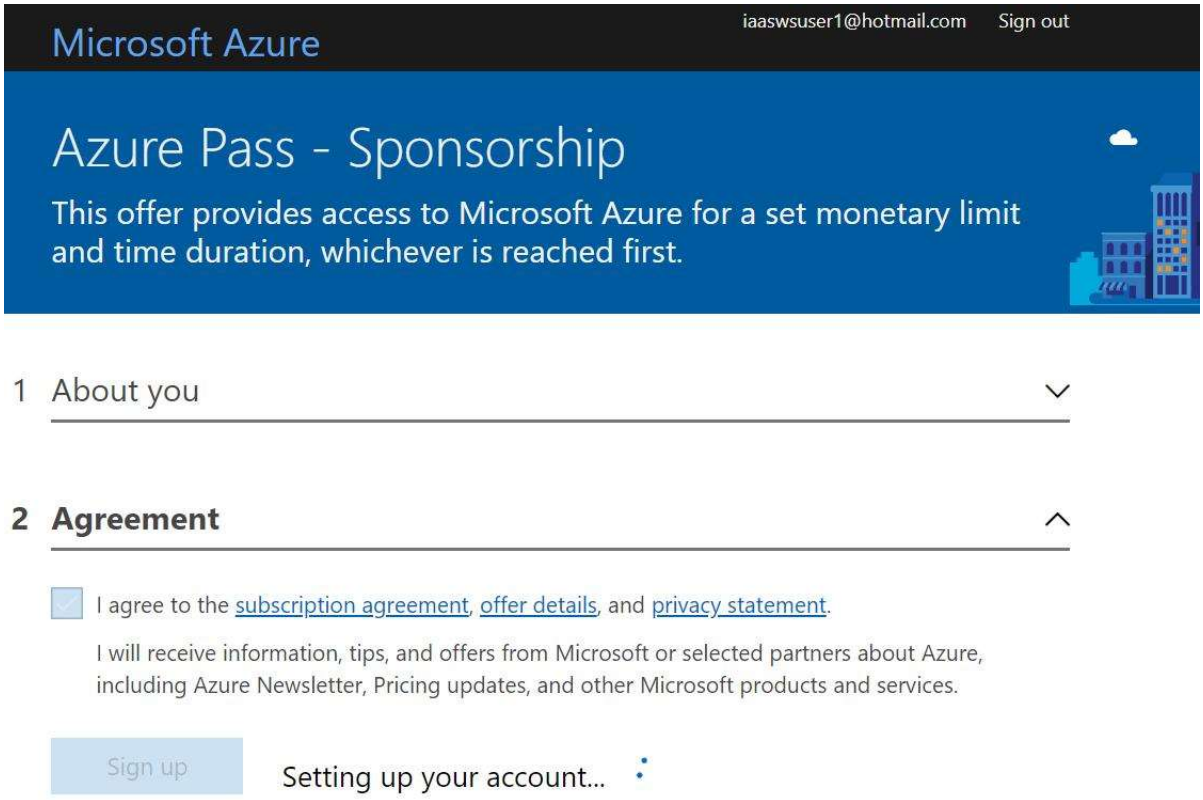
☐ 8. Complete the **Azure Pass - Sponsorship** form and click the **Next** tile.



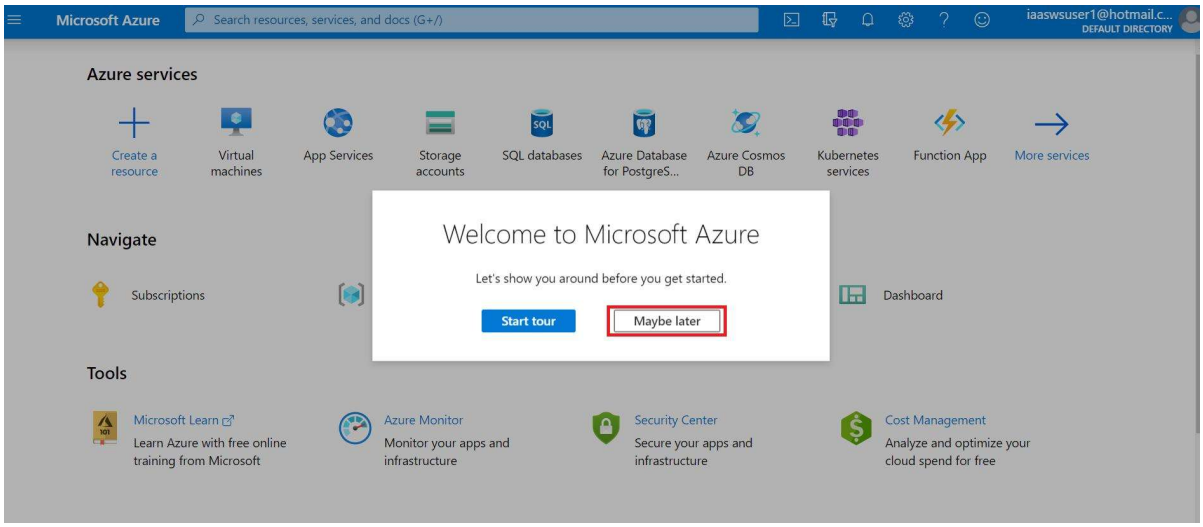
☐ 9. Tick the **subscription agreement, offer details and privacy statement** tickbox then click the **Sign up** tile.



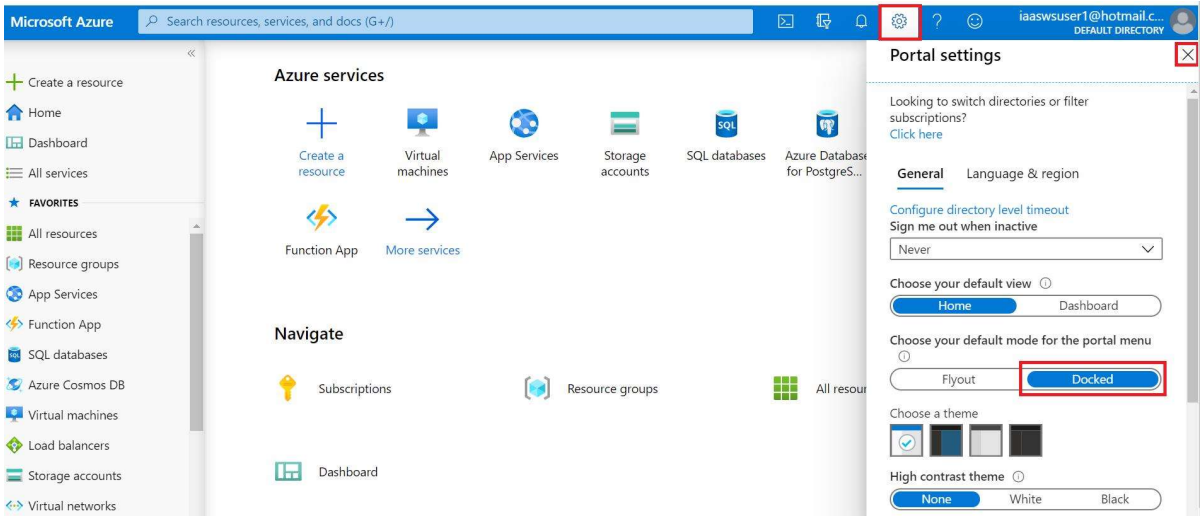
☐ 10. This should take around **two to three minutes** to process, depending on the number of activation requests received by the activation service.



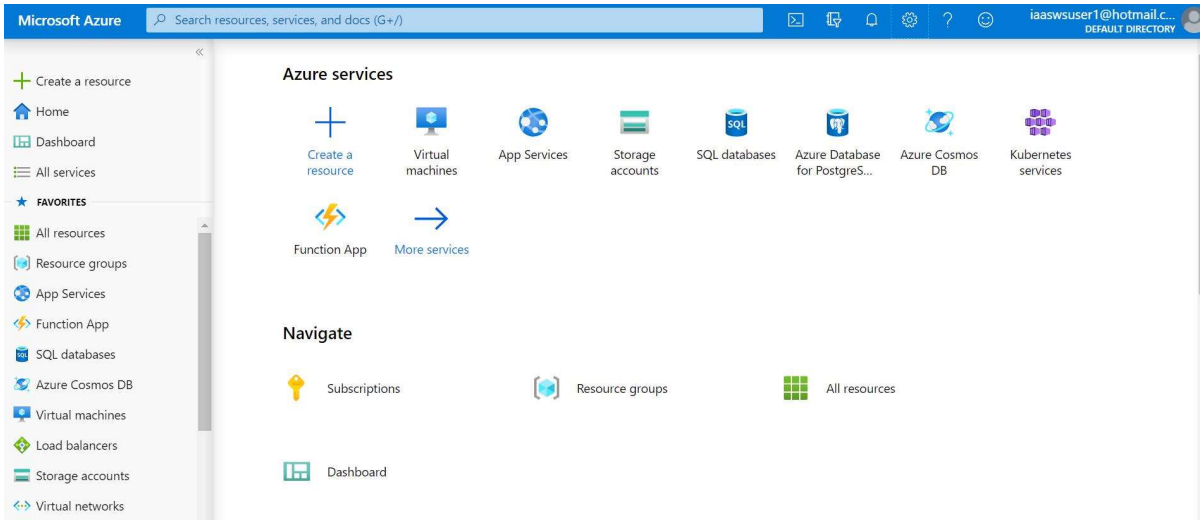
☐ 11. Click the **Maybe later** tile in the **Welcome to Microsoft Azure** pop-up pane.



☐ 12. Click the **Gear** tile, then click **Docked** in the **Choose your default mode for the portal menu** toggle bar, then close the pane.



☐ 13. Your **Azure Trial Pass** subscription is now ready for use.



Initialize your lab environment

☐ 1. Create the **Resource groups** that will be used later on in the labs. Edit the **YourLocation** placeholder value in the script below to reflect your chosen **Region**, then copy and paste the entire script into the **PowerShell scripts** pane. **Resource Groups can also be created during resource creation time, but the labs have been designed with them pre-created**.

Click the **Type Text** icon to automatically type the associated text to the active window in your hosted lab machine on the left, once you have edited the **YourLocation** placeholder value with your chosen **Region**.

```
Windows_PowerShell
New-AzResourceGroup -Name netwLabEastUS-lod{LAB_INSTANCE_ID} -Location You
New-AzResourceGroup -Name netwLabCentralUS-lod{LAB_INSTANCE_ID} -Location
```

2. Click the **Run** button or press **F5**. This will create the resource groups that will be used in your labs.

Module 1 - VNet-to-VNet Connectivity with BGP

Introduction

In this lab, you will create two Azure virtual networks and connect them together. You will then enable BGP on both networks and confirm that it has been successfully implemented.

You'll learn:

- How to create Azure virtual networks
- How to define Azure virtual gateways
- How to connect virtual networks using Azure Connections
- How to confirm connectivity between two virtual networks
- How to enable BGP and confirm its implementation
- How to enable virtual network Service Endpoints
- How to enable the storage account firewall

Prerequisites

The following are required to complete this hands-on lab:

- Microsoft Azure PowerShell v5.1.1 or later
- Microsoft Azure PowerShell Az module v2.5.0 or later
- A Microsoft Azure subscription

> Although this lab demonstrates setting up a VNet-to-VNet connection from within the Azure Portal, you can also achieve this through PowerShell. See https://azure.microsoft.com/en-us/documentation/articles/vpn-gateway-vnet-vnet-rm-ps/ for more information on using PowerShell.

Exercise 1 - VNet-to-VNet Connectivity

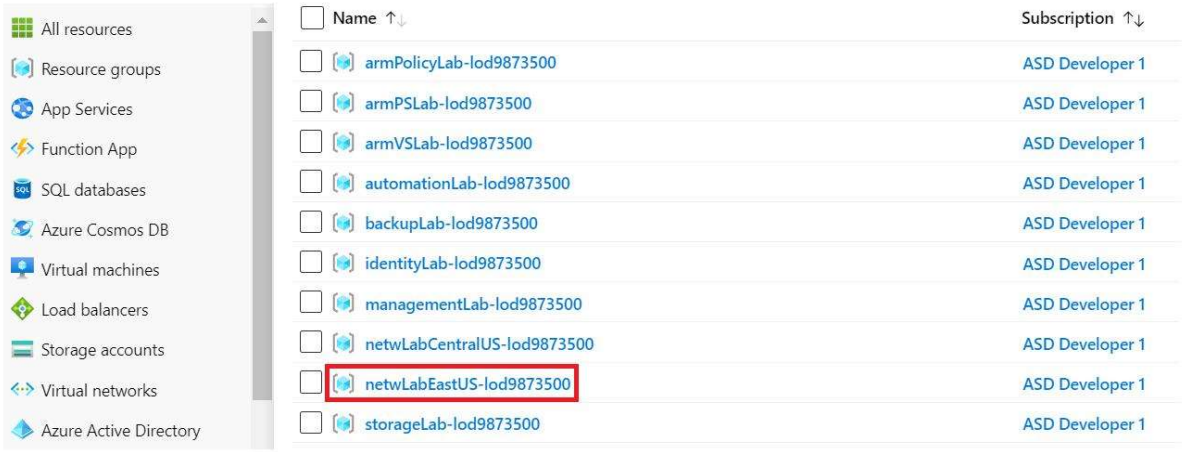
Task 1 - Create the first virtual Network and Virtual Network gateway

In this task, we will choose to create our virtual networks in two different regions, East US and Central US. You can choose whatever regions you wish to use, just remember to change your settings in the appropriate places while stepping through the exercise.

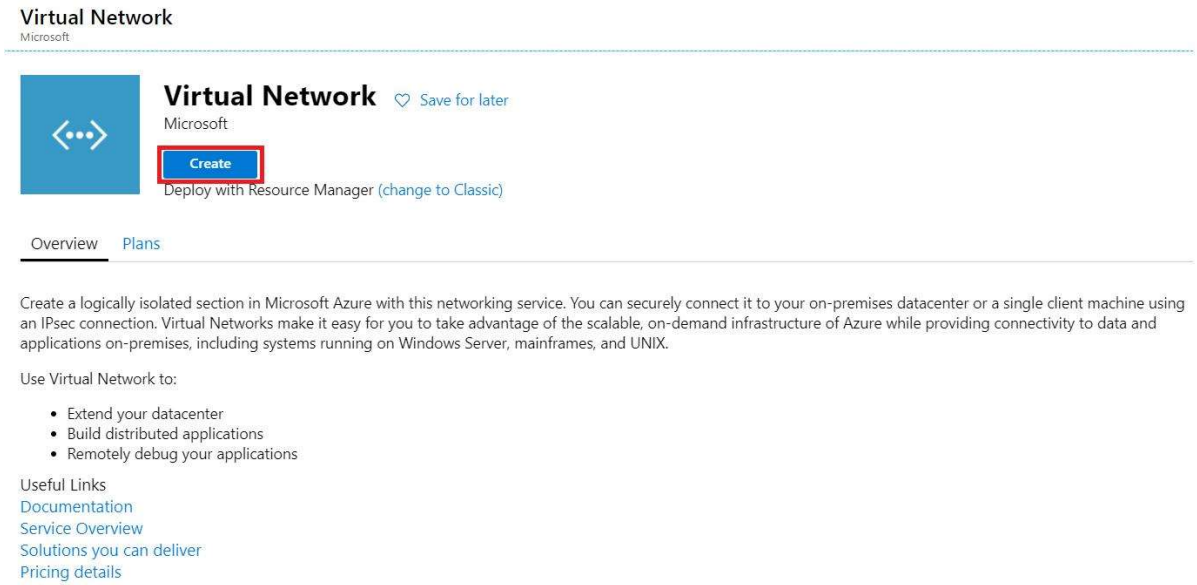
☐ 1. Connect to **Win10 Lab VM** as **Student** using **pass@word1** as the password.

☐ 2. Log in to the Azure portal at **https://portal.azure.com** using your Azure Trial Pass credentials.

☐ 3. Select the **Resource Groups** menu item (which will open the Resource Groups blade) and then select the **netwLabEastUS-lodXXXXXXX** e.g. **netwLabEastUS-lod9873500** resource group.



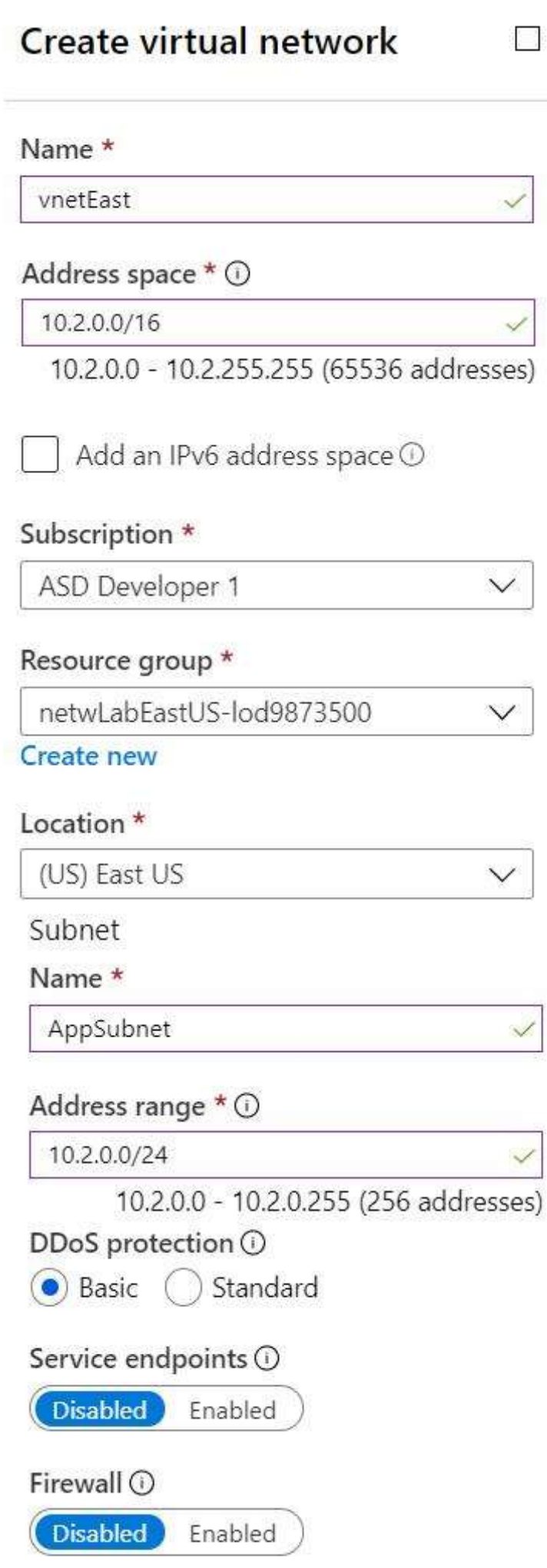
☐ 4. From within the resource group, click the **Add** button, then type in **Virtual Network** in the **Search the Marketplace** search box, then press Enter. This will list the Virtual Network resource, click **Create**.



☐ 5. When setting up the virtual network, you will need to configure:

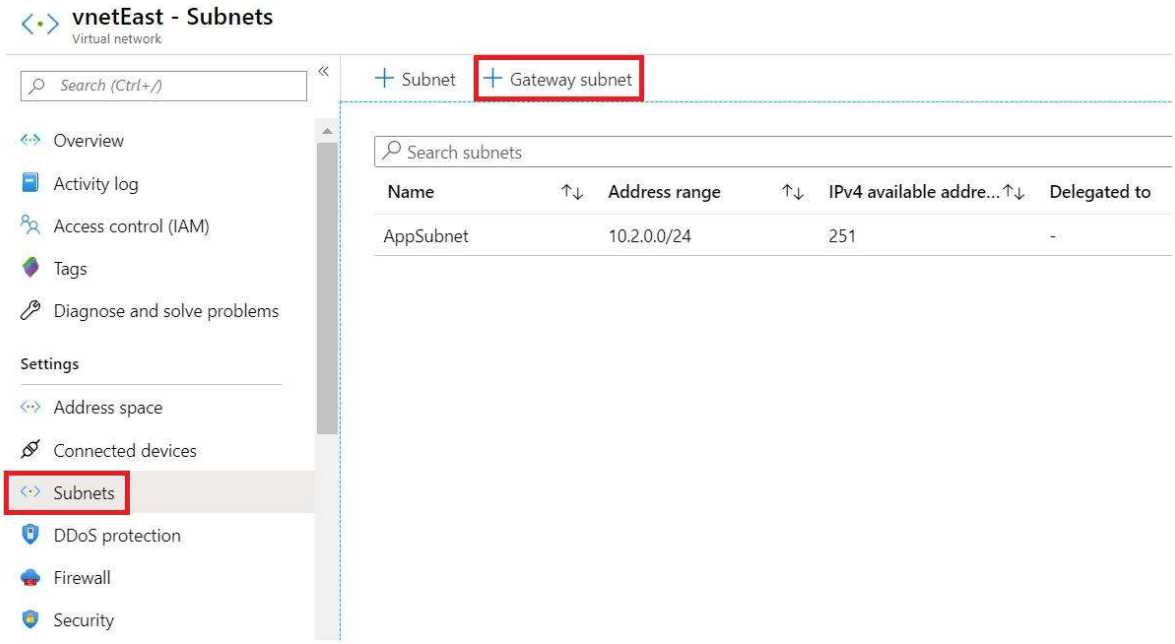
- The name of the virtual network e.g. **vnetEast**

- The address space in CIDR notation (**Use 10.2.0.0/16**) **Ignore the IP Address overlap warning, this is due to a shared Azure subscription.**
- Select your Azure subscription (Accept the default)
- Select the **netwLabEastUS-lodXXXXXXX** e.g. **netwLabEastUS-lod9873500** resource group if not already selected
- Select the Location to put the virtual network in, this should be **East US**
- The name of the subnet, for this lab exercise, name it **AppSubnet**
- Subnet address range **(Use 10.2.0.0/24)**
- DDoS protection (leave as Basic)
- Service endpoints (leave disabled)
- Firewall (leave disabled)
- Click the **Create** button

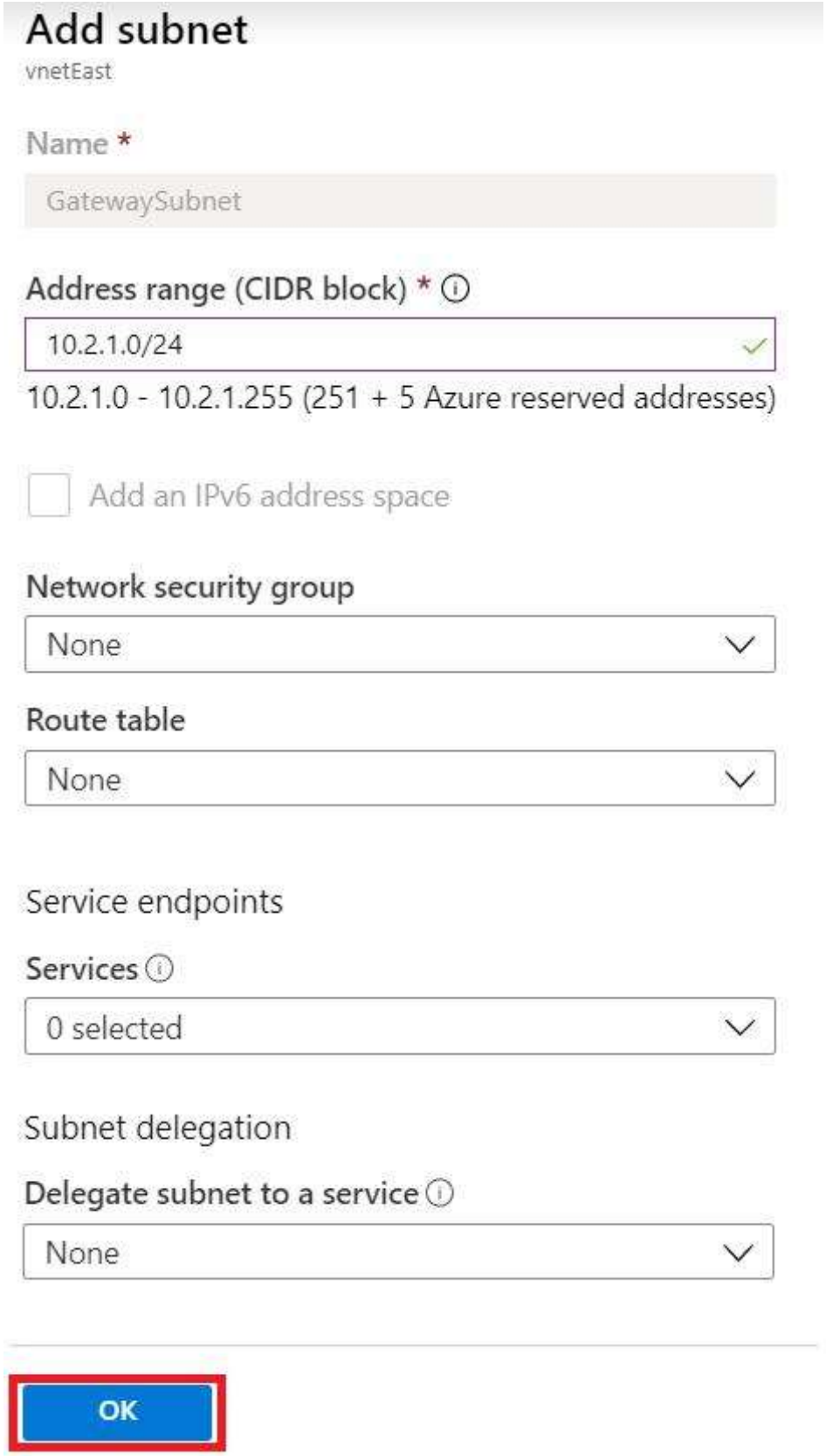

Create virtual network
Name *
vnetEast
Address space *
10.2.0.0/16
10.2.0.0 - 10.2.255.255 (65536 addresses)
Add an IPv6 address space
Subscription *
ASD Developer 1
Resource group *
netwLabEastUS-lod9873500
Create new
Location *
(US) East US
Subnet
Name *
AppSubnet
Address range *
10.2.0.0/24
10.2.0.0 - 10.2.0.255 (256 addresses)
DDoS protection
Basic
Standard
Service endpoints
Disabled
Enabled
Firewall
Disabled
Enabled

☐ 6. Go back to the **netwLabEastUS-lodXXXXXXX** e.g. **netwLabEastUS-lod9873500** resource group and click on the **vnetEast** virtual network. This will bring up the vnetEast blade.

☐ 7. In the **vnetEast** blade, click on the **Subnets** tile. Then click the **+ Gateway subnet** button in the Subnets blade to add a new gateway subnet.

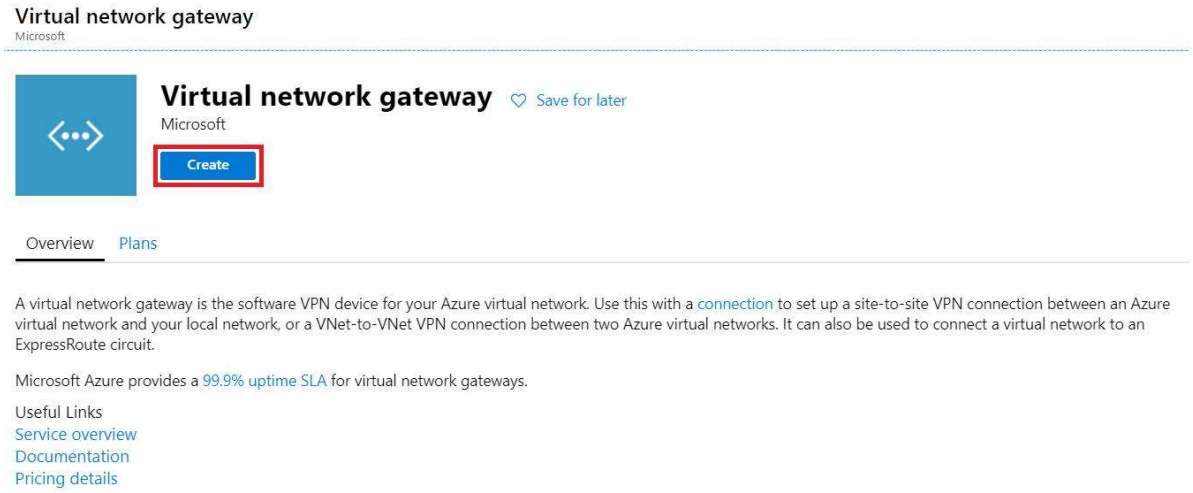


☐ 8. Accept the default address range and click OK. Once the gateway subnet has been created, go back to the **netwLabEastUS-lodXXXXXXX** e.g. **netwLabEastUS-lod9873500** resource group blade.



☐ 9. In order for our virtual network to connect to another network via an IPsec VPN, it needs to have a virtual network gateway or router implemented.

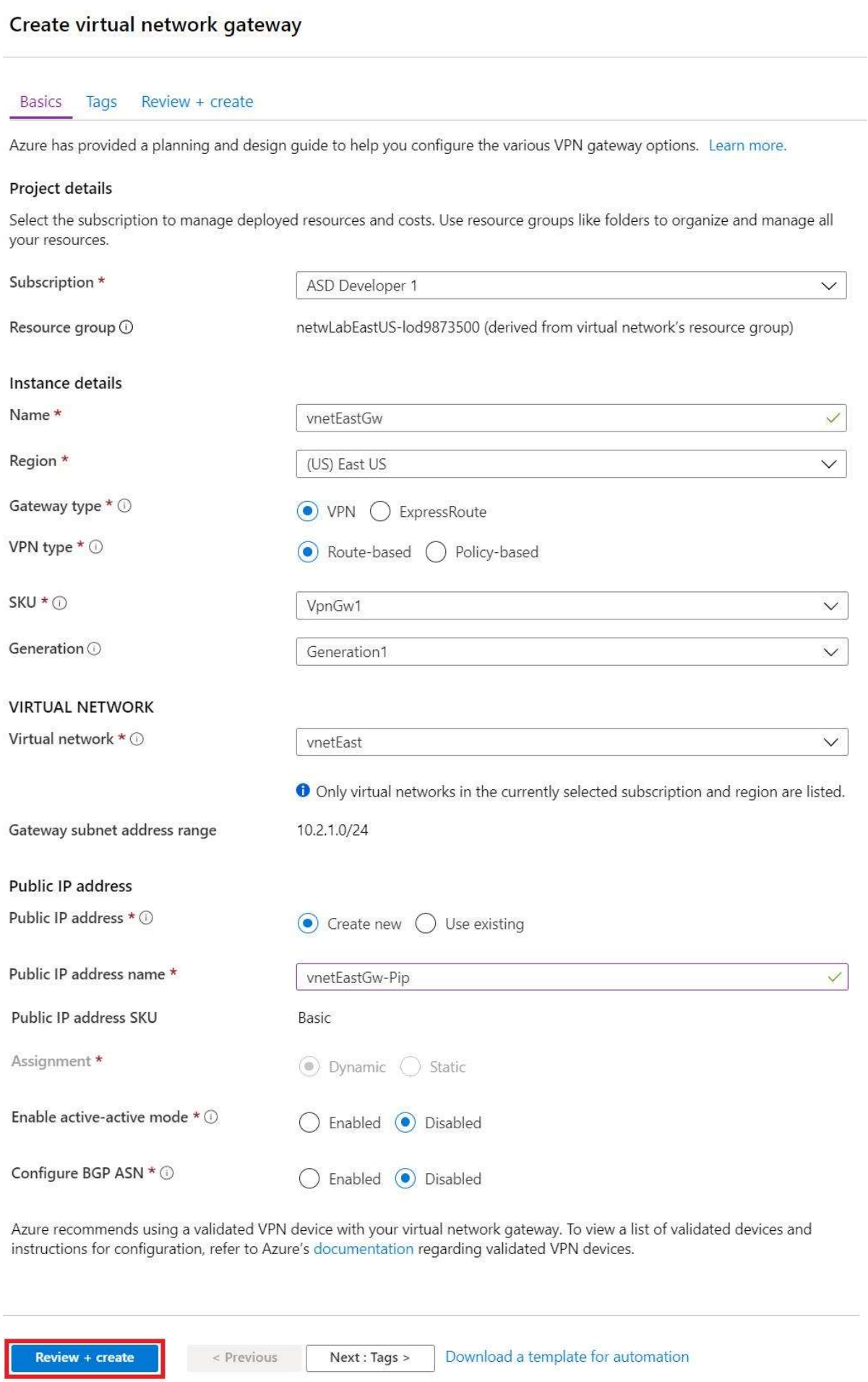
Click the **Add** button in your resource group blade and then type T **Virtual network gateway** in the **Search the Marketplace** search box, then press Enter. This will list the Virtual Network Gateway resource, click **Create**.



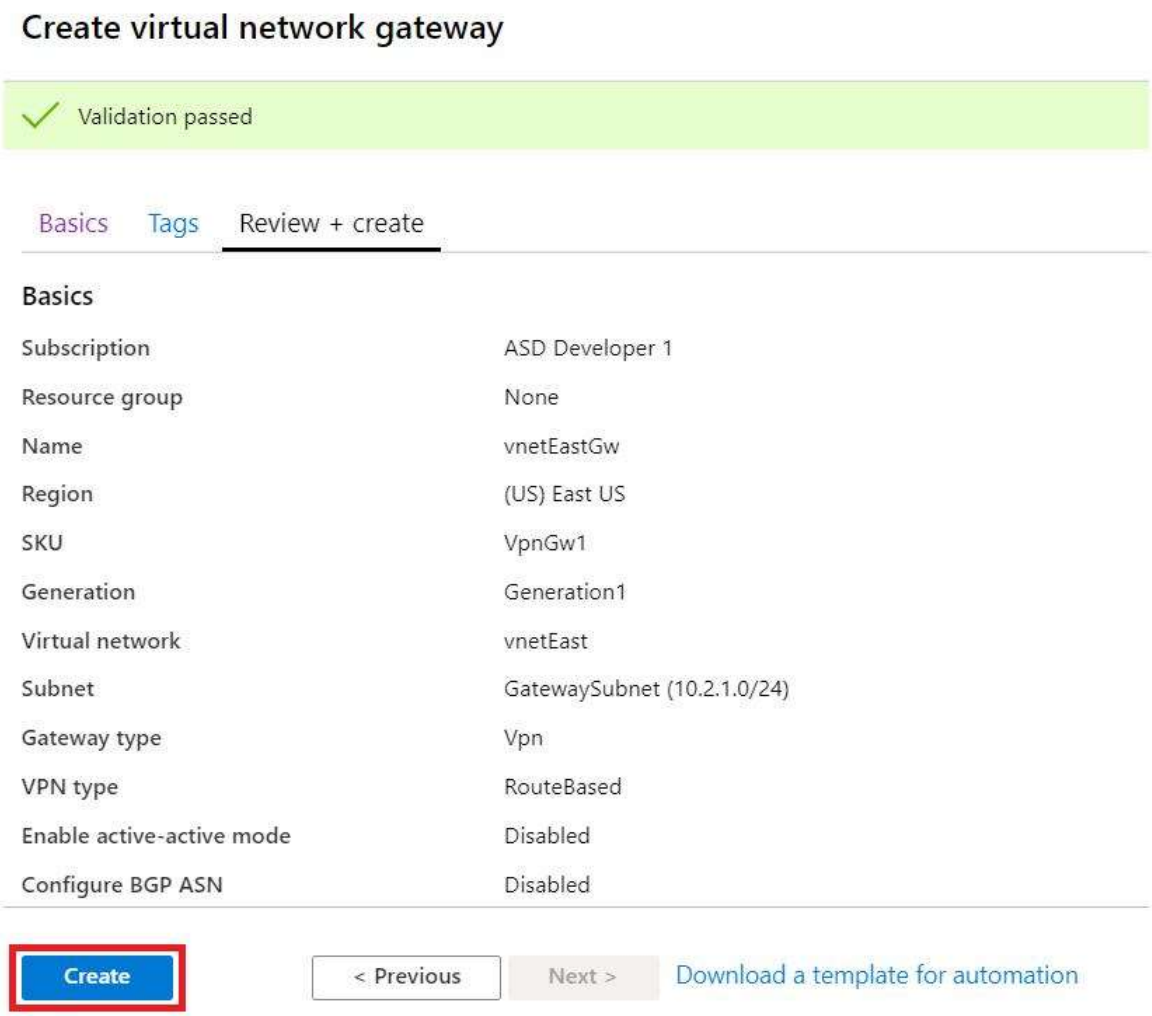
☐ 10. When setting up the virtual network gateway, you will need to configure:

- Select your Azure subscription (Accept the default)
- The name of your virtual network gateway e.g. **vnetEastGw**
- Select the Location to put the virtual network gateway in, this should be **East US**
- Gateway type, select **VPN**
- VPN type, select **Route-based**
- SKU, select **VpnGw1**
- Virtual network, select the virtual network that you recently created in this resource group e.g. **vnetEast** (this specifies which virtual network your gateway will be attached to)
- Public IP address, select **Create new**
- The name of your gateways Public IP address, e.g. **vnetEastGw-Pip**
- Enable active-active mode, select **Disabled** (this configures both gateways in an active-active configuration as opposed to an active-standby configuration)
- Configure BGP ASN, select **Disabled** (this will be configured later on using another method)

☐ 11. Click the **Review + create** button.



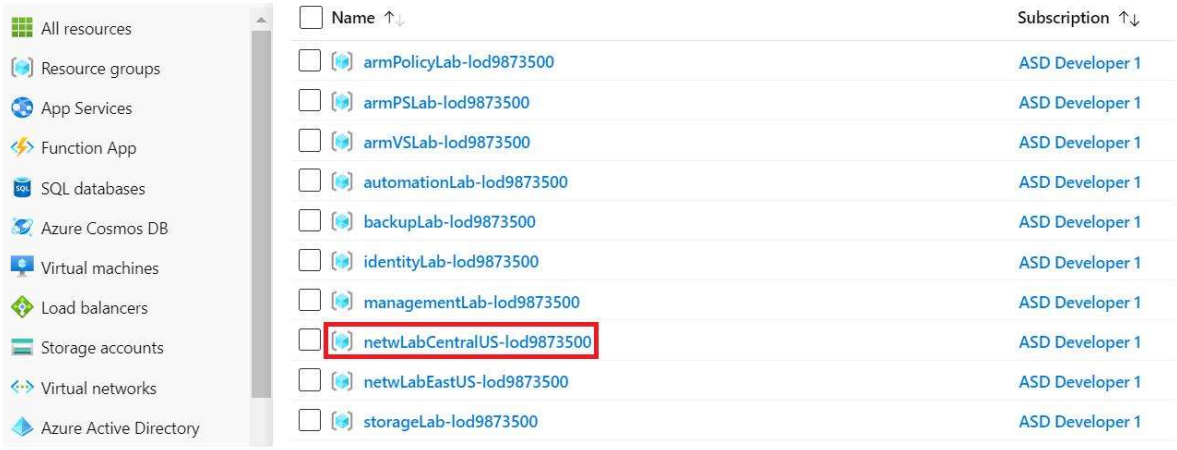
☐ 12. Click the **Create** button.



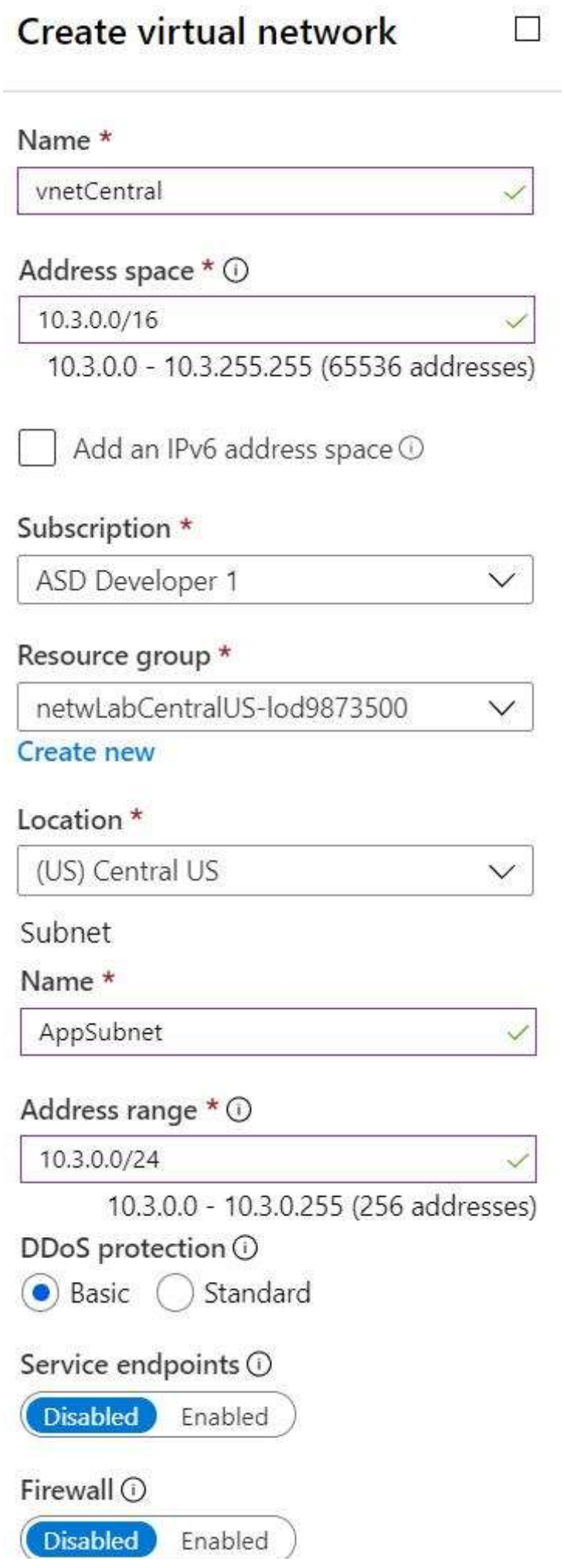
Please note that it can take up to 40 minutes for the gateway creation process to complete, you are however able to move forward with the lab whilst waiting for it to complete.

Task 2 - Create the second Virtual Network and Virtual Network gateway

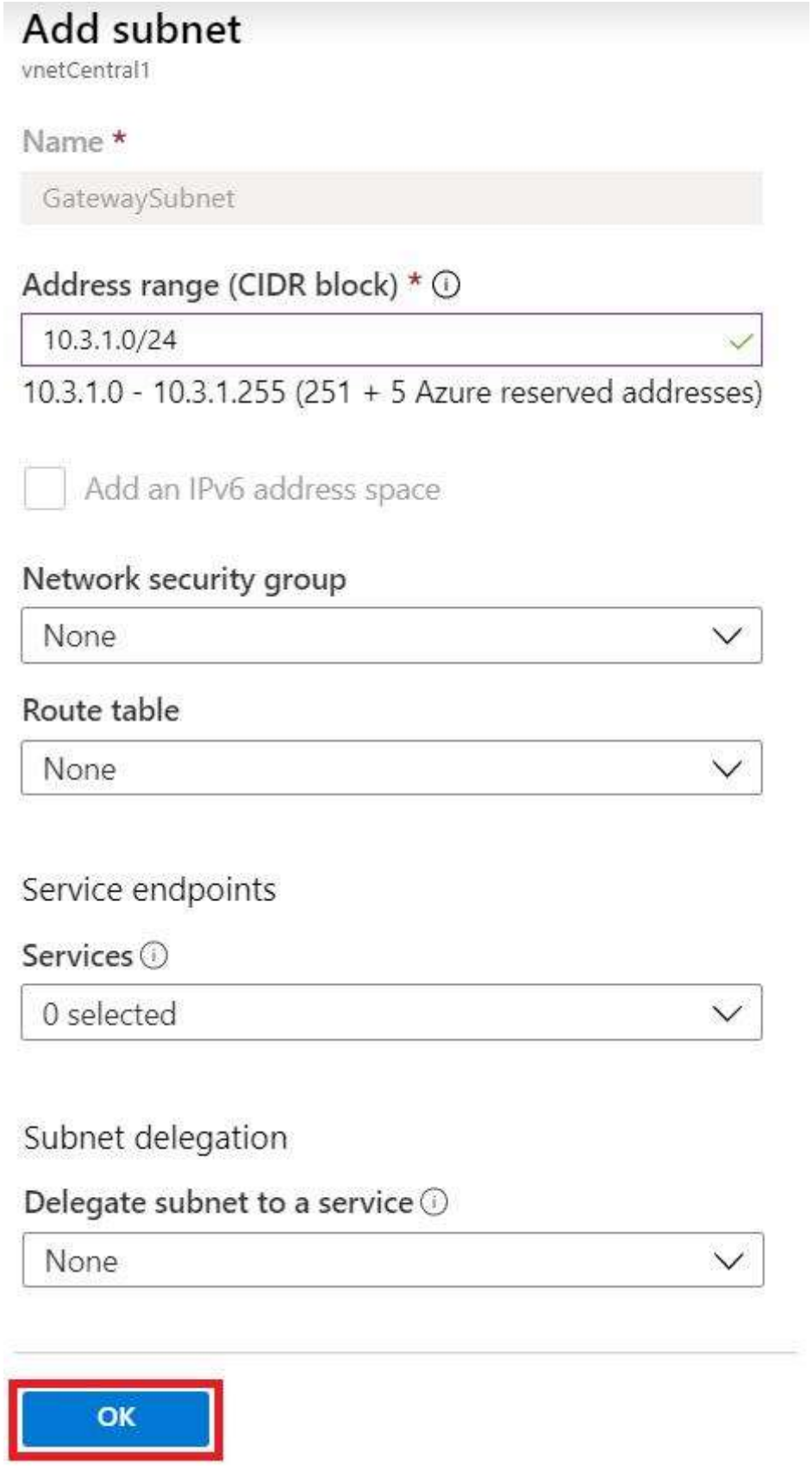
☐ 1. Go back to the **Resource Groups** blade and select the **netwLabCentralUS-lodXXXXXXX** e.g. **netwLabCentralUS-lod9873500** resource group. You are going to go through the same steps of creating a virtual network with a virtual network gateway that you carried out in the previous task, except that this will be for the **netwLabCentralUS-lodXXXXXXX** e.g. **netwLabCentralUS-lod9873500** resource group with all resources located in the **Central US** region.



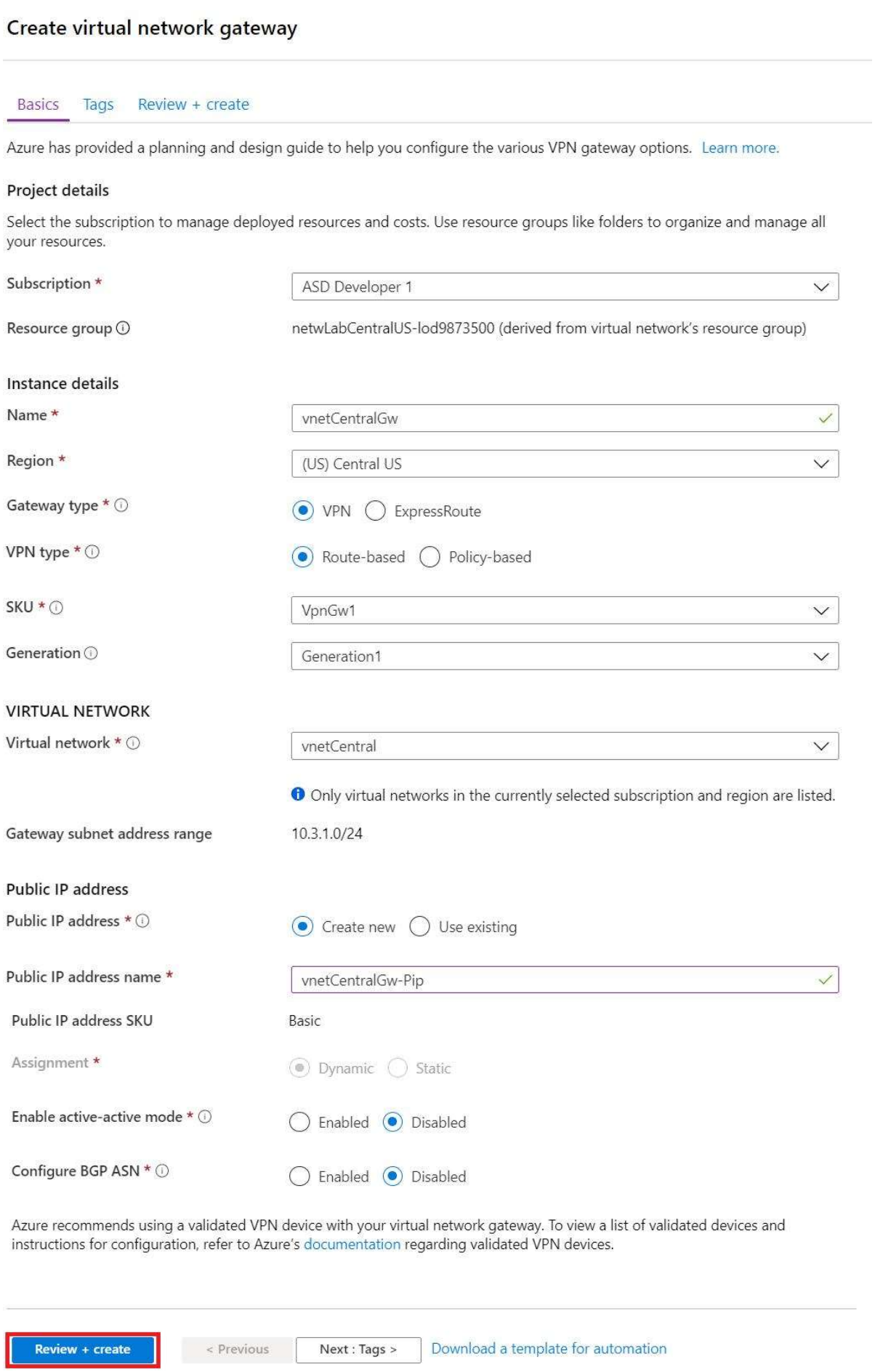
☐ 2. From within the **netwLabCentralUS-lodXXXXXXX** e.g. **netwLabCentralUS-lod9873500** resource group, click the **Add** button and add a new virtual network named **vnetCentral**. Pay close attention to the IP addresses that are being used i.e. **10.3.0.0/16** for the address space and **10.3.0.0/24** for the AppSubnet. Click the **Create** button.


Create virtual network
Name *
vnetCentral
Address space *
10.3.0.0/16
10.3.0.0 - 10.3.255.255 (65536 addresses)
Add an IPv6 address space
Subscription *
ASD Developer 1
Resource group *
netwLabCentralUS-lod9873500
Create new
Location *
(US) Central US
Subnet
Name *
AppSubnet
Address range *
10.3.0.0/24
10.3.0.0 - 10.3.0.255 (256 addresses)
DDoS protection
Basic
Standard
Service endpoints
Disabled
Enabled
Firewall
Disabled
Enabled

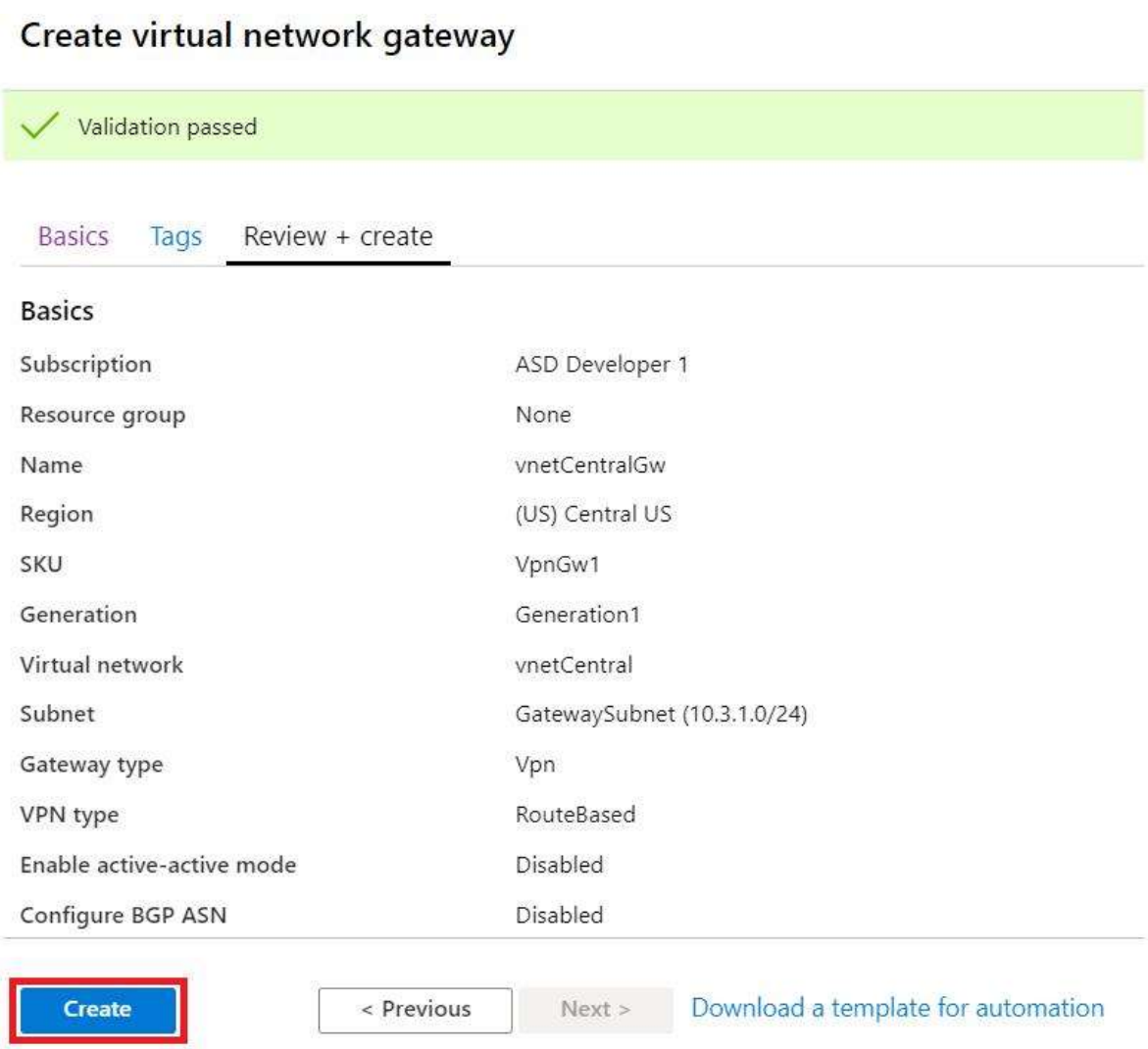
☐ 3. Once the virtual network has been created, create a new gateway subnet.



☐ 4. Create a virtual network gateway named **vnetCentralGw** and associate it with your **vnetCentral** virtual network. You also need to have a different public IP address name than **vnetEastGw** and make sure you choose the Route-based VPN type. Click the **Review + create** button.



☐ 5. On successful validation, click the **Create** button. Remember that it can take up to 40 minutes to deploy the gateway.

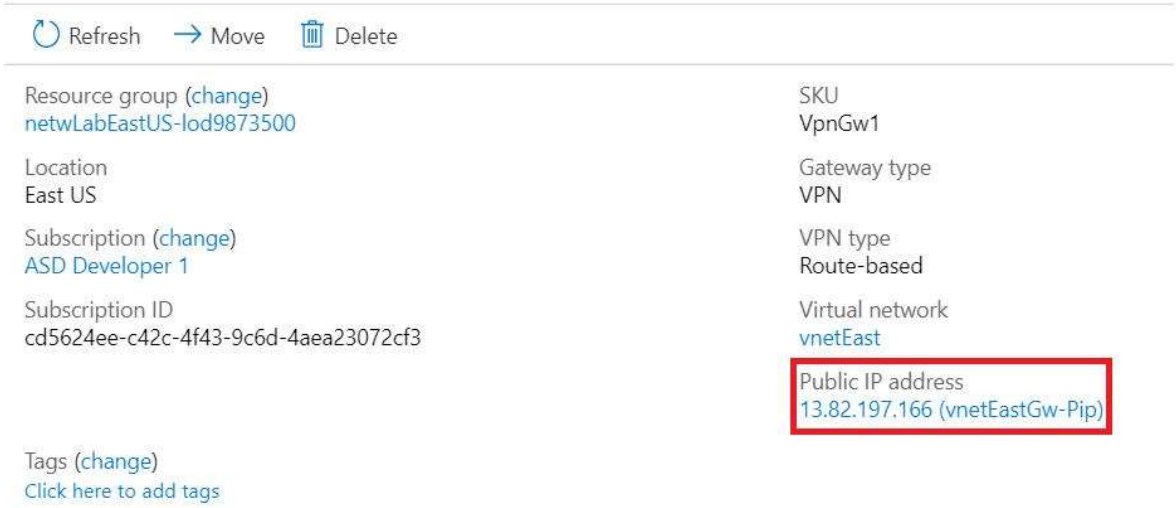

Create virtual network gateway
Validation passed
Basics
Tags
Review + create
Basics
Subscription
ASD Developer 1
Resource group
None
Name
vnetCentralGw
Region
(US) Central US
SKU
VpnGw1
Generation
Generation1
Virtual network
vnetCentral
Subnet
GatewaySubnet (10.3.1.0/24)
Gateway type
Vpn
VPN type
RouteBased
Enable active-active mode
Disabled
Configure BGP ASN
Disabled
Create
< Previous
Next >
Download a template for automation

Task 3 - Confirm Virtual Network Gateway creation

You will know that your virtual network gateways have been successfully created, when Azure provides a new public IP address to the gateway. Check both gateways.

☐ 1. Navigate to the **netwLabEastUS-lodXXXXXXX** e.g. **netwLabEastUS-lod9873500** resource group and click on your **virtual network gateway**.

☐ 2. You will notice your new public IP address in the virtual network gateway blade.



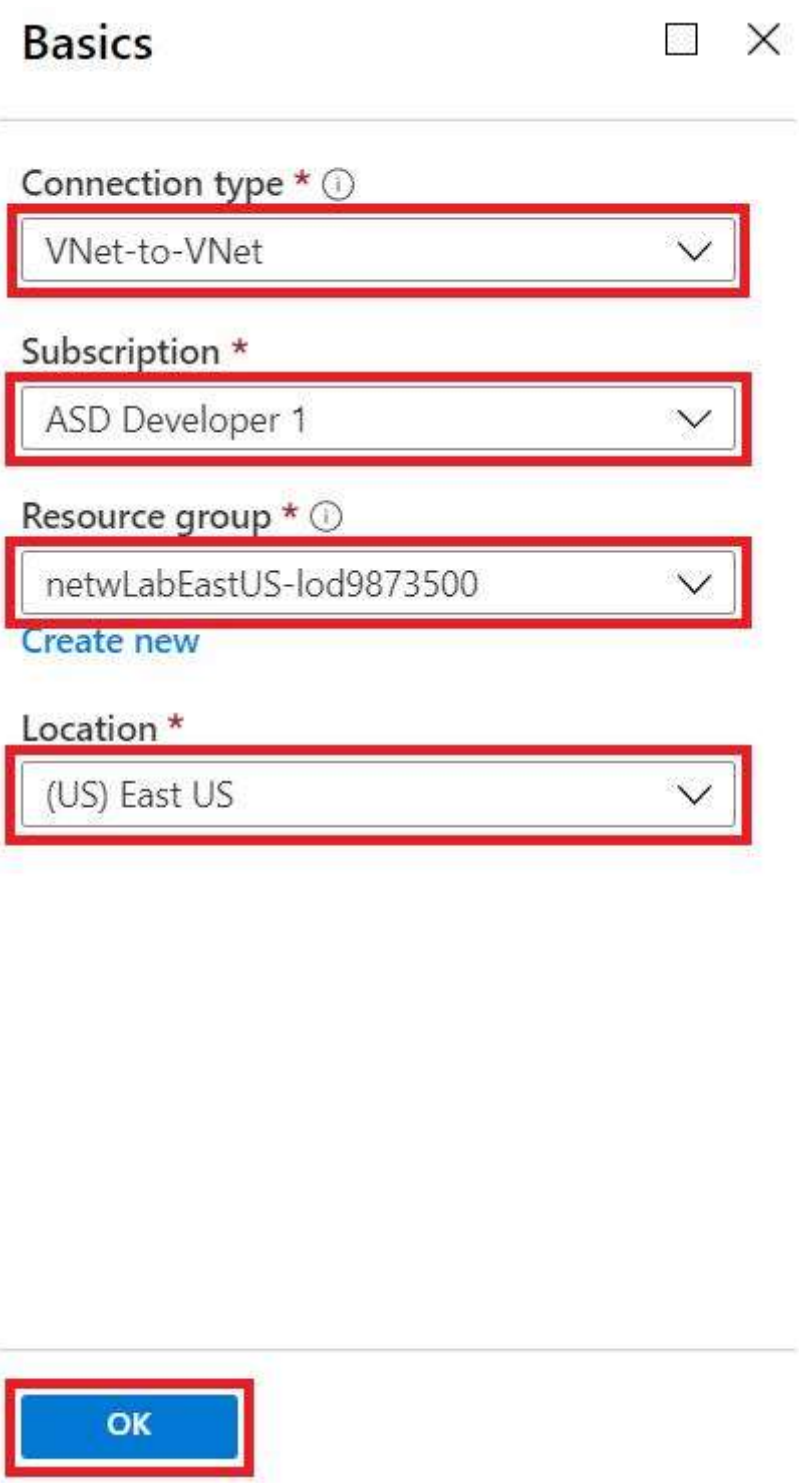
☐ 3. Repeat the process for the **netwLabCentralUS-lodXXXXXXX** e.g. **netwLabCentralUS-lod9873500** resource group and confirm that the virtual network gateway has been assigned a public IP address.

Task 4 - Create the virtual network connections

Now that you have the virtual network gateways created, you need to create a Connection to enable connectivity between the gateways.

☐ 1. From within the **netwLabEastUS-lodXXXXXXX** e.g. **netwLabEastUS-lod9873500** resource group blade, select **Add**, then type in T **Connection** in the **Search the Marketplace** search box, then press Enter. This will list the Connection resource, click **Create**.

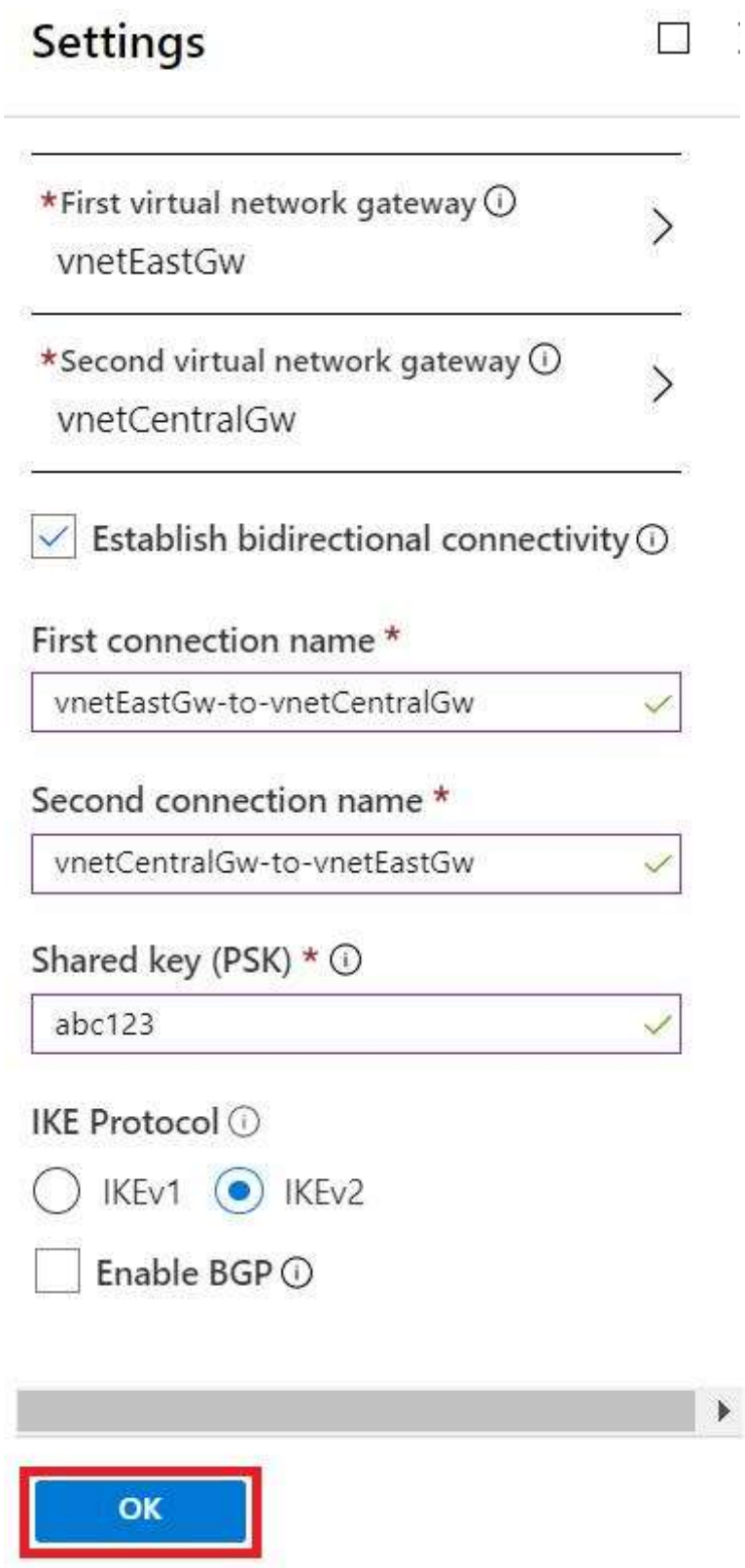
☐ 2. On the **Basics** blade, select the **VNet-to-VNet** Connection type, the default Azure subscription, the existing resource group **netwLabEastUS-lodXXXXXXX** e.g. **netwLabEastUS-lod9873500** if it has not been selected by default, also select the same location as the resource group, in this case **East US**. Click the **OK** button.



☐ 3. On the **Settings** blade, review the properties below.

- Since we are already in the **netwLabEastUS-lodXXXXXXX** e.g. **netwLabEastUS-lod9873500** resource group, we will choose the first virtual network gateway as **vnetEastGw**
- Our second gateway created in an earlier task is **vnetCentralGw**
- Select **Establish bidirectional connectivity** (to create connections in both directions, not selecting this will result in a single connection being created with traffic flow in one direction only)
- Type in connection names for the first and second connections or accept the default names

- Enter a Shared key e.g. **abc123** (this is used for the gateways to authenticate to each other, in a production environment, a more complex key should be used)
- Leave **Enable BGP** unselected, we will enable BGP at a later stage
- Click the **OK** button



☐ 4. Click the **OK** button on the summary page.

Summary

Basics

Connection type	VNet-to-VNet
Subscription	ASD Developer 1
Resource Group	netwLabEastUS-lod9873500
Location	(US) East US

Settings

First virtual network gateway	vnetEastGw
Second virtual network gateway	vnetCentralGw
Establish bidirectional connectivity	Yes
First connection name	vnetEastGw-to-vnetCentralGw
Second connection name	vnetCentralGw-to-vnetEastGw
Shared key (PSK)	abc123
IKE Protocol	IKEv2

OK

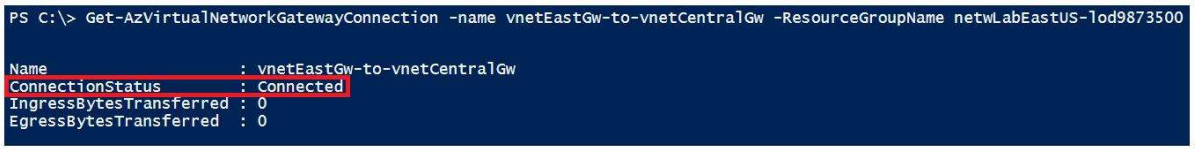
Because you selected the **Establish bidirectional connectivity** option in the Settings blade (above), you do not need to create a connection from the **vnetCentral** virtual network gateway to the **vnetEast** virtual network gateway, since this will be included during the creation of this connection.

Task 5 - Confirm the connection between the virtual networks

There are a few ways in which to verify the connectivity status between virtual networks. One of the fastest ways is to use PowerShell to do this.

- [ ] 1. Open PowerShell ISE as an Administrator.
- [ ] 2. In the PowerShell command prompt, type in **Connect-AzAccount** and press Enter, then login using your Azure Trial Pass credentials.
- [ ] 3. To confirm the **vnetEastGw** connection to **vnetCentralGw** and vice versa, type in the following and press Enter (if you are prompted to confirm the action, select Yes to All):

```
Windows_PowerShell
Get-AzVirtualNetworkGatewayConnection -name vnetEastGw-to-vnetCentralGw -
```



You should be able to see the **ConnectionStatus** with a status of **Connected**. The number of ingress and egress bytes transferred will be zero since there is no traffic flowing between the two gateways yet. If the status shows as "Unknown", "Connecting" or "Not connected" wait a few minutes and try again.

- [ ] 4. Run the same PowerShell command but this time for the vnetCentralGw-to-vnetEastGw connection in the same resource group.
- [ ] 5. Leave your PowerShell session open.

Congratulations!

You have successfully completed this exercise. Click **Next** to advance to the next exercise.

Exercise 2 - Enable BGP on virtual network gateways and connections

BGP is a routing protocol that enables routers to exchange routing table information between them. This is useful because it reduces the administrative overhead for a network administrator. Without BGP, the network administrator would have to manually configure routing paths.

During the previous steps of this lab, you configured a VNet-to-VNet VPN connection whereby the routing paths were configured between the two gateways during the creation of your VPN connections. These routing paths were derived from each of the VNets address spaces (this is the reason why a local network gateway is not required for a VNet-to-VNet connection). The routing paths were not configured by means of the gateways exchanging their routing tables.

During this exercise, we will be enabling both gateways and their respective connections to use BGP.

Task 1 - Check the BGP status on the existing virtual network gateway

☐ 1. From the previously opened PowerShell session, run the following script to confirm that BGP is not enabled on the gateways:

```
Windows_PowerShell
```

```
Get-AzVirtualNetworkGatewayBGPPeerStatus -VirtualNetworkGatewayName vnetEa
```

```
PS C:\> Get-AzVirtualNetworkGatewayBGPPeerStatus -VirtualNetworkGatewayName vnetEastGw -ResourceGroupName netwLabEastUS-lod9873500
PS C:\>
```

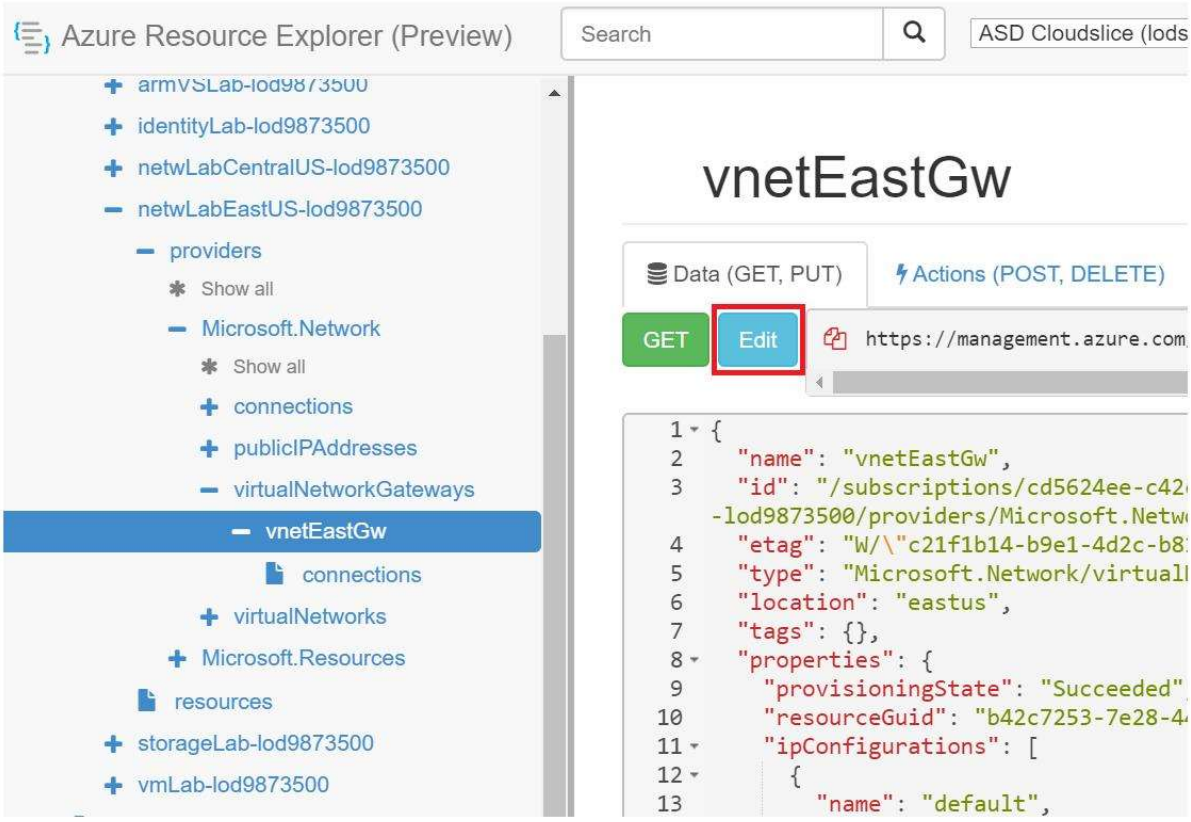
☐ 2. Repeat the above step for the vnetCentralGw gateway in the **netwLabCentralUS-lodXXXXXXX** e.g. **netwLabCentralUS-lod9873500** resource group.

☐ 3. Leave your PowerShell session open.

Task 2: - Enable BGP on the virtual network gateway and connections

- [ ] 1. Browse to https://resources.azure.com/ and login using your Azure Trial Pass credentials.
- [ ] 2. In the top right-hand corner, click the Read/Write toggle button if it has not been selected by default.

- [ ] 3. In the left-hand pane, expand **subscriptions|YourSubscriptionName|resourceGroups|netwLabEastUS-lodXXXXXXX|providers|Microsoft.Network|virtualNetworkGateways** and click the **vnetEastGw** then click **Edit** in the right-hand pane.



- [ ] 4. In the right-hand pane, scroll down to the **"enableBgp"** tag and configure it to **true** and configure its **"asn"** tag value to **65010.**

```
44      },
45      "gatewayType": "Vpn",
46      "vpnType": "RouteBased",
47      "enableBgp": true,
48      "activeActive": false,
49      "bgpSettings": {
50        "asn": 65010,
51        "bgpPeeringAddress": "10.2.1.254",
52        "peerWeight": 0
53      },
54      "gatewayDefaultSite": {
55        "id": "(String)"
```

☐ 5. Scroll to the top and click the **Put** button.

☐ 6. Repeat this process for the **vnetCentralGw** gateway and using an **asn** tag value of **65020**. This will enable both gateways for BGP. The next step is to enable BGP on the gateway connections.

☐ 7. Navigate to **subscriptions|YourSubscriptionName|resourceGroups|netwLabEastUS-lodXXXXXXX|providers|Microsoft.Network|connections** and click the **vnetCentralGw-to-vnetEastGw** connection, then click **Edit** in the right-hand pane.

☐ 8. In the right-hand pane, scroll down to the **"enableBgp"** tag (under **"connectionType": "Vnet2Vnet"**) and configure it to **true** and click the **Put** button.

☐ 9. Repeat this process for the **vnetEastGw-to-vnetCentralGw** gateway connection.

Task 3 - Confirm that BGP has been enabled

☐ 1. From the previously opened PowerShell session, run the following script to confirm that BGP has been enabled:

```
Windows_PowerShell
Get-AzVirtualNetworkGatewayBGPPeerStatus -VirtualNetworkGatewayName vnetEa
```

☐ 2. Confirm that there is a successful connection with your BGP peer (which is the other VNet gateway in this case) and that at least 1 route has been received or learnt.

☐ 3. Repeat this process for the **vnetCentralGw** gateway.

☐ 4. The exchange of routing information between the two gateways has now generated network traffic. You can confirm this by running the PowerShell command that you ran earlier.

```
Windows_PowerShell
Get-AzVirtualNetworkGatewayConnection -name vnetEastGw-to-vnetCentralGw -
```

☐ 5. Repeat this process for the **vnetCentralGw-to-vnetEastGw** gateway connection.

Congratulations!

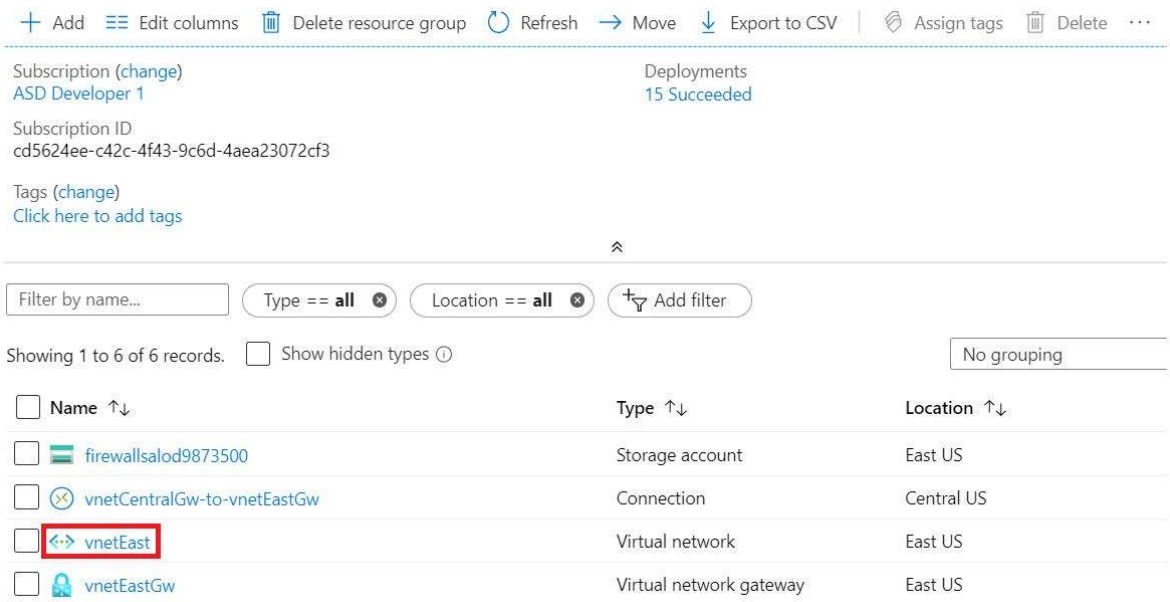
You have successfully completed this exercise. Click **Next** to advance to the next exercise.

Exercise 3 - Configure Virtual Network Service Endpoints and Storage Account Firewall

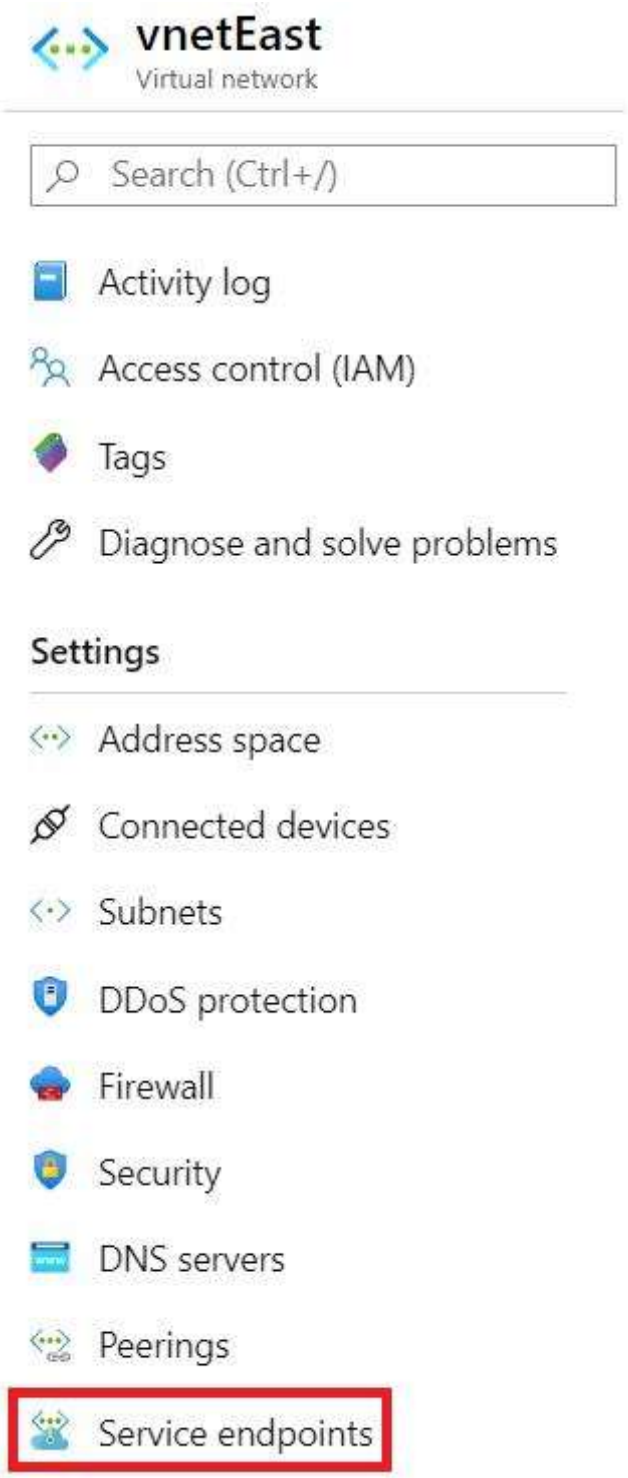
Now that we've deployed our virtual network, it's a good idea to secure communication to and from it when accessing Azure public facing services. One example of this is Azure Storage. When we access an Azure Storage account from a virtual network, we do this over the Internet albeit inside a Microsoft Azure datacenter. This does raise security concerns in most organizations. Using Virtual Network Service Endpoints, we create a connection between a virtual network and an Azure Storage account over the Microsoft Azure backbone network so traffic between a virtual network and a storage account does not go over the Internet giving you a more secure connection.

Task 1 - Configure Virtual Network Service Endpoints

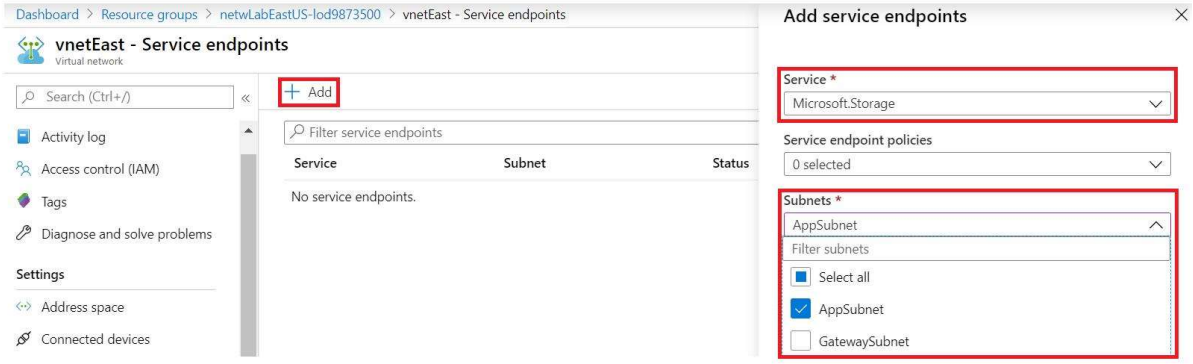
☐ 1. From within the Azure portal, navigate to the **netwLabEastUS-lodXXXXXXX** e.g. **netwLabEastUS-lod9873500** resource group and click on the vnetEast virtual network.



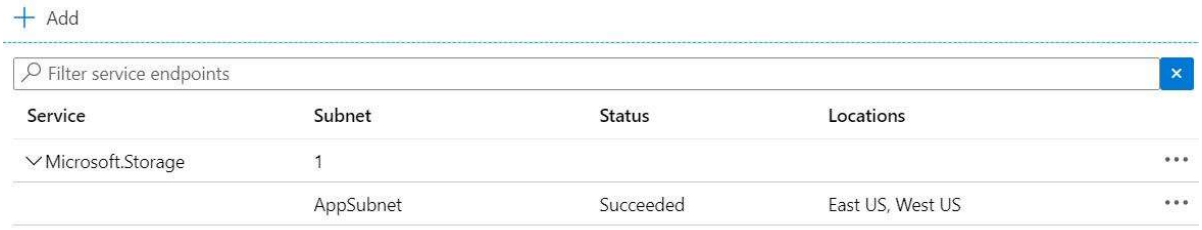
☐ 2. In the left-hand pane, click **Service endpoints**.



☐ 3. In the right-hand pane, click **Add**, then select Microsoft.Storage from the Service drop down menu, then **AppSubnet** from the Subnets drop down menu and click **Add**. This process can take up to 15 minutes.



☐ 4. Confirm that the Azure Storage Service endpoints have been added while you are still in the Service endpoints pane. You have now configured all inbound and outbound traffic from your virtual network to your Azure storage account to go over the Microsoft Azure backbone network.

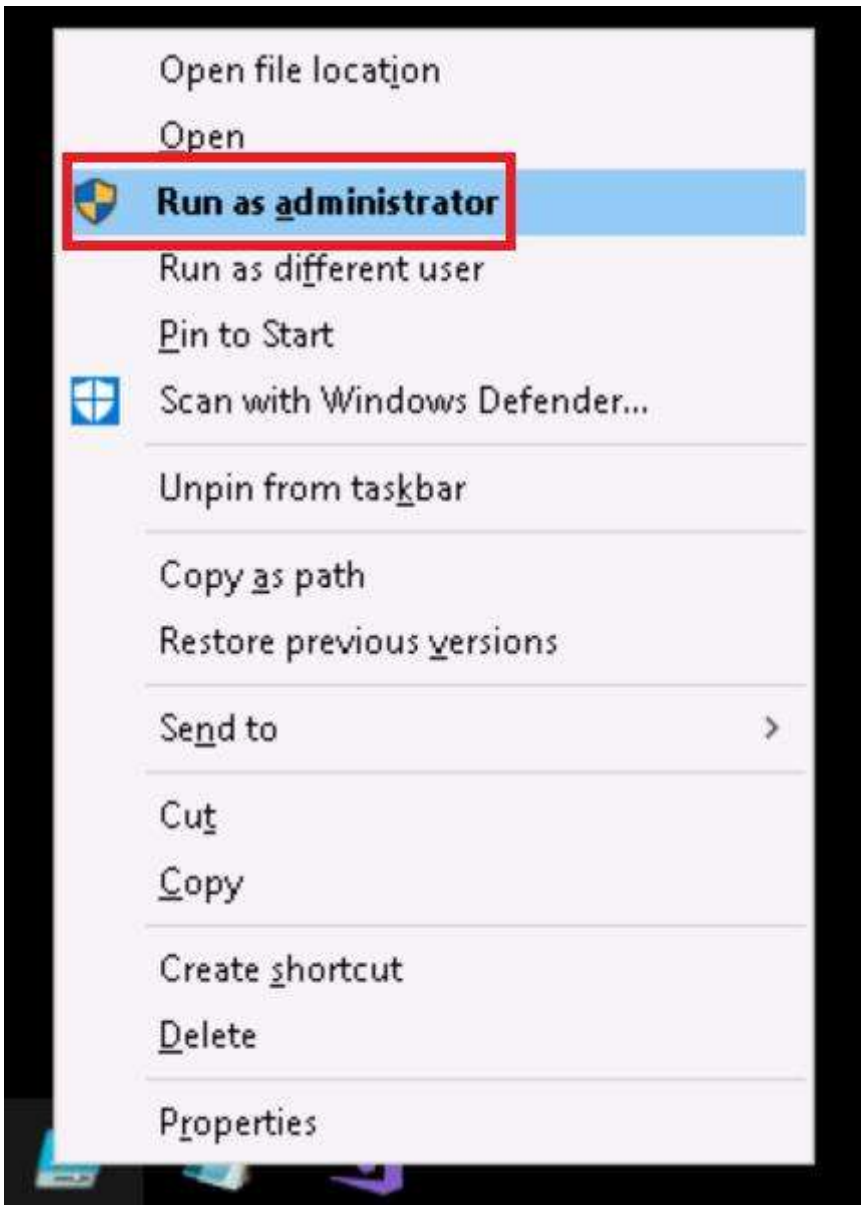


Task 2 - Configure Storage Account Firewall

Prior to configuring a storage account firewall, we need to create a storage account.

☐ 1. Login to the **Win10 Lab VM** hosted lab machine in the left hand pane with a Username of **Student** and a Password of **pass@word1** Once logged in, select your keyboard layout from the task bar.

☐ 2. Shift and right-click the PowerShell ISE shortcut on the taskbar and select **Run as administrator**



☐ 3. Click **Yes** to the User Account Control pop-up.

☐ 4. In the PowerShell ISE command prompt window, type in **Connect-AzAccount** and press **Enter**.

☐ 5. Enter the email address that was used to redeem your **Azure Trial Pass** into the Sign in dialog box and click **Next** or press **Enter**.

☐ 6. Enter your password and click **Sign in** or press **Enter**. This will log you in to your Azure Trial Pass subscription.

```
PS C:\> Connect-AzAccount

Account                 SubscriptionName         TenantId                             Environment
-------                 ----------------         --------                             -----------
iaaswslab@hotmail.com Azure Pass - Sponsorship f30ae15e-afec-42d9-aefc-3709be909663 AzureCloud
```

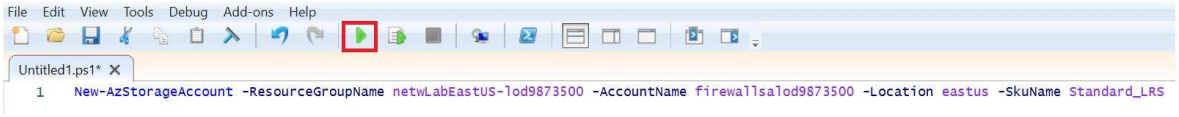
☐ 7. Copy the below PowerShell commands to your PowerShell script pane.

> Click the **Type Text** icon to automatically type the associated text to the active window in your hosted lab machine on the left.

Windows_PowerShell

```
New-AzStorageAccount -ResourceGroupName netwLabEastUS-lod{LAB_INSTANCE_ID
```

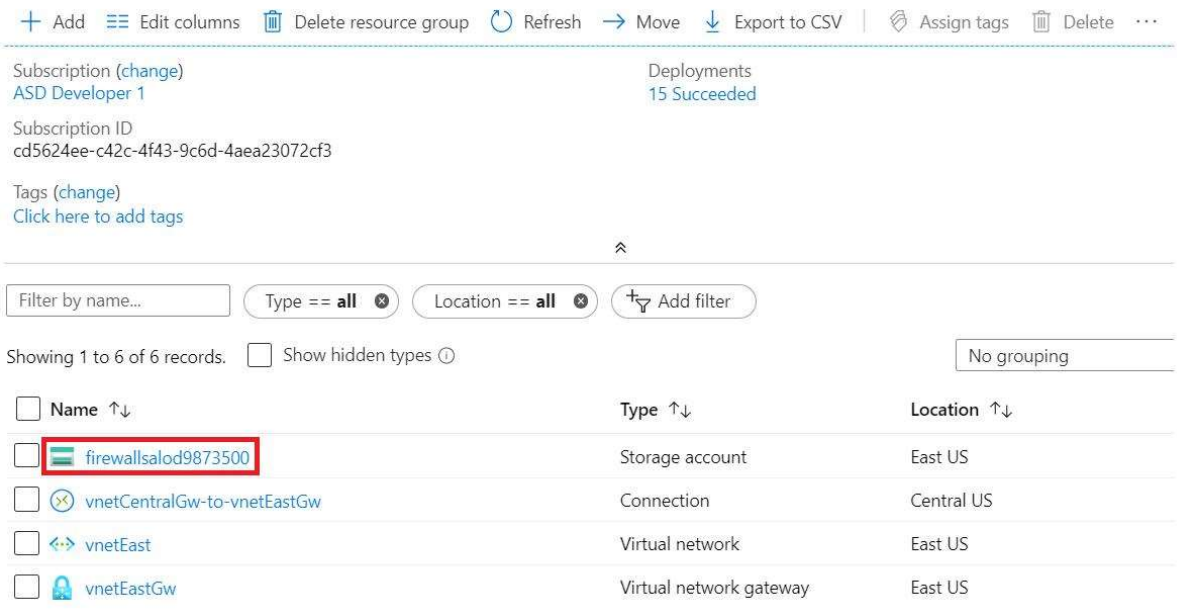
☐ 8. Click the **Run** button or press **F5**. This will create the storage account that will be used in this lab.



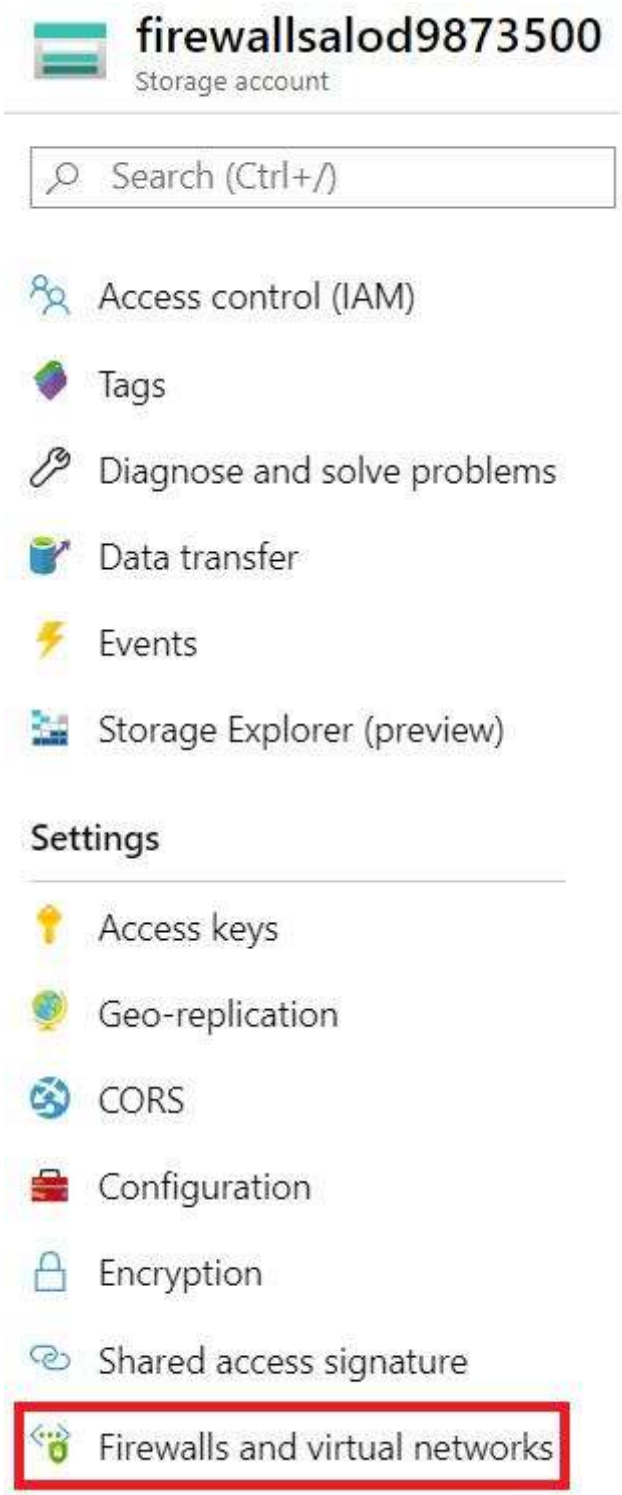
☐ 9. The storage account has been successfully created.

```
StorageAccountName   ResourceGroupName        PrimaryLocation SkuName      Kind      AccessTier CreationTime       ProvisioningState EnableHttpsTrafficOnly LargeFileSha
                                                                                                                                                  res
------------------   -----------------        --------------- -------      ----      ---------- ------------       ----------------- ---------------------- ------------
firewallsalod9873500 netwLabEastUS-lod9873500 eastus          Standard_LRS StorageV2 Hot        30-04-2020 19:54:46 Succeeded         True
```

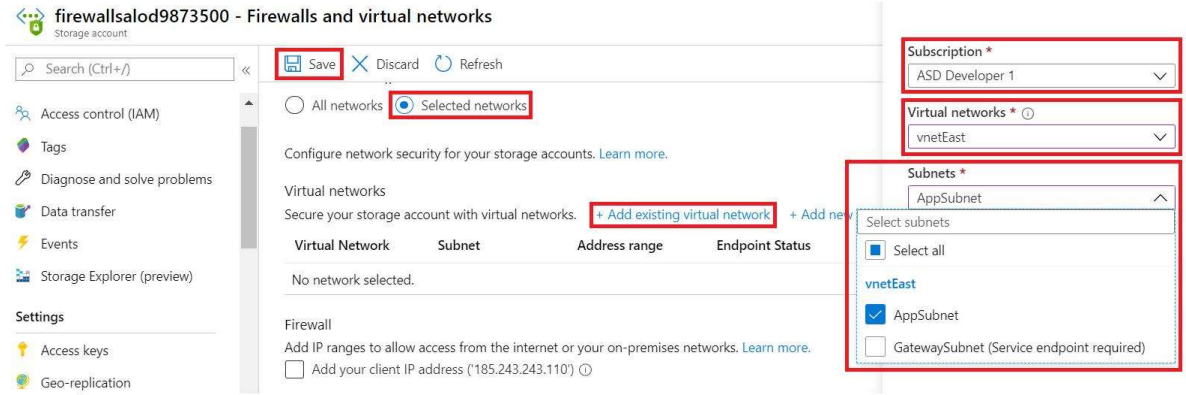
☐ 10. From within the Azure portal, navigate to the **netwLabEastUS-lodXXXXXXX** e.g. **netwLabEastUS-lod9873500** resource group and click on the **firewallsalodXXXXXXX** e.g. **firewallsalod9873500** storage account.



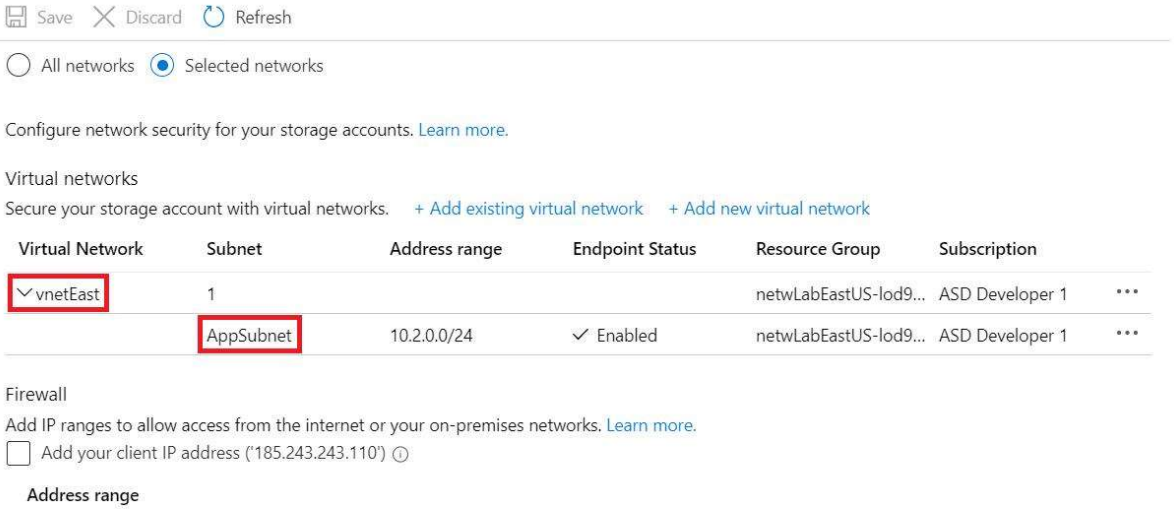
☐ 11. In the left-hand pane, click **Firewalls and virtual networks**.



☐ 12. In the right-hand pane, click the **Selected networks** radio button, then click **+ Add existing virtual network** this will automatically select your subscription, then select **vnetEast** from the Virtual networks drop down menu, and finally select **AppSubnet** from the Subnets drop down menu. Click **Add** and then click **Save**.



☐ 13. While you are still in the Firewalls and virtual networks pane, click the expand arrow under Virtual Network and confirm that the Azure Storage Account Firewall has been configured to allow network traffic from the **AppSubnet** in the **vnetEast** virtual network.



You have now successfully configured your Azure Storage Account to accept inbound and outbound network traffic from your specified virtual network only. This means that this storage account will no longer be accessible from the Internet unless additional rules are configured to allow this.

Congratulations!

You have successfully completed this module.