WorkshopPLUS

Microsoft Azure Infrastructure as a Service (IaaS)

VNet-to-VNet Connectivity with BGP (ARM)

Student Lab Manual

V1.3, February 8, 2018

Information in this document is subject to change without notice. The example companies, organizations, products, people, and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarked, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2014 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, MS, Windows, Windows NT, MSDN, Active Directory, BizTalk, SQL Server, SharePoint, Outlook, PowerPoint, FrontPage, Visual Basic, Visual C++, Visual J++, Visual InterDev, Visual SourceSafe, Visual C#, Visual J#,  and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names herein may be the trademarks of their respective owners.

Contents

[Exercise 1 – VNet-to-VNet Connectivity 5](#_Toc510792080)

[Prerequisites 5](#_Toc510792081)

[Task 1 – Create the first virtual Network and Virtual Network gateway 5](#_Toc510792082)

[Task 2 – Create the second Virtual Network and Virtual Network gateway 12](#_Toc510792083)

[Task 3 – Confirm Virtual Network Gateway creation 15](#_Toc510792084)

[Task 4 – Create the virtual network connections 15](#_Toc510792085)

[Task 5 – Confirm the connection between the virtual networks 18](#_Toc510792086)

[Exercise 2 - Enable BGP on virtual network gateways and connections 19](#_Toc510792087)

[Task 1 - Check the BGP status on the existing virtual network gateway 19](#_Toc510792088)

[Task 2 - Enable BGP on the virtual network gateway and connections 19](#_Toc510792089)

[Task 3 – Confirm that BGP has been enabled 22](#_Toc510792090)

[Exercise 3 - Configure Virtual Network Service Endpoints and Storage Account Firewall 22](#_Toc510792091)

[Task 1 – Configure Virtual Network Service Endpoints 23](#_Toc510792092)

[Task 2 – Configure Storage Account Firewall 24](#_Toc510792093)

**Introduction to VNet-to-VNet Connectivity with BGP**

In this lab, you will create two Azure virtual networks in different regions 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 two Azure virtual networks
* How to define two Azure virtual gateways
* How to connect the virtual networks using Azure Connections
* How to confirm connectivity between the two virtual networks
* How to enable BGP and confirm its implementation

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

## Prerequisites

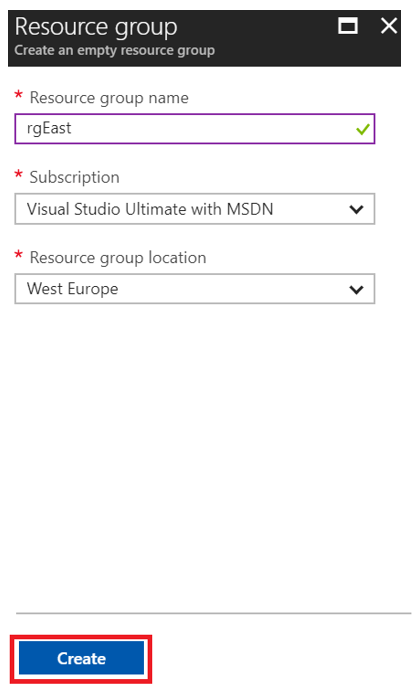
The following is required to complete this hands-on lab:

* Microsoft Azure PowerShell
* A Microsoft Azure subscription
* Windows Azure PowerShell ISE

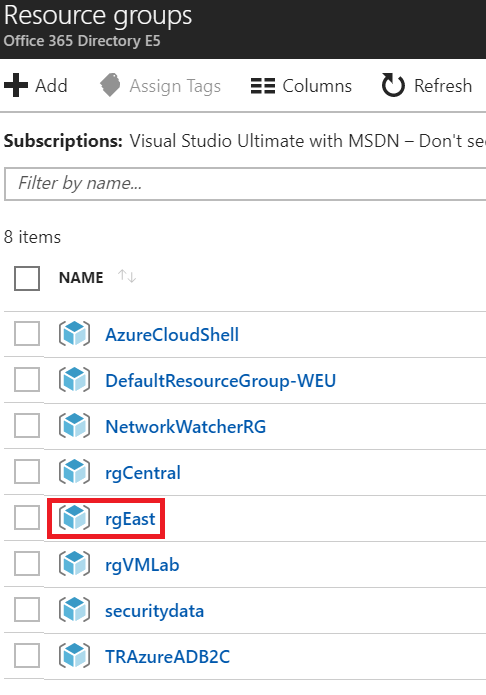
## Task 1 – Create the first virtual Network and Virtual Network gateway

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. Log in to the Azure portal at https://portal.azure.com.
2. Select the **Resource Groups** menu item (which will open the Resource Groups blade) and then select **+Add**.
3. Create a new resource group in the region of your choosing. In our example, we will name this *rgEast*. Make sure that the data center you choose represents the name of the resource group to prevent confusion. Click the **Create** button.

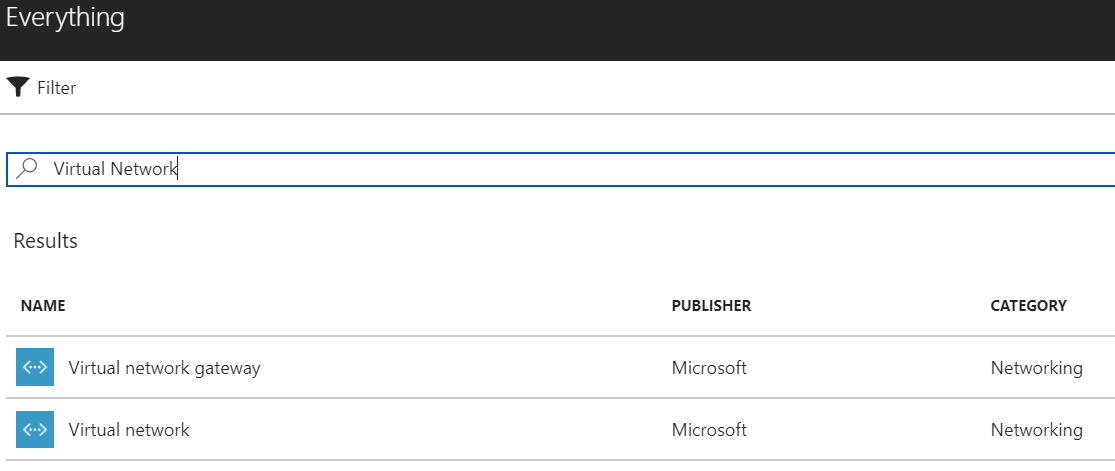


1. Repeat steps 2 and 3 but this time name the resource group *rgCentral*.
2. Go back to the Resource Groups blade and pick *rgEast*. This will open up the resource group blade.

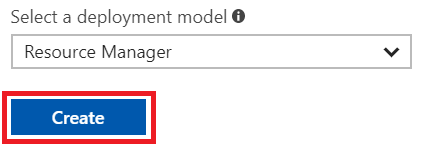


1. In the resource group blade, create a new virtual network by selecting **+Add**, entering *virtual network* into the **Search Everything** field and pressing Enter.

Select the **Virtual Network** list item; a blade will open where you can start building your virtual network.



1. Select **Resource Manager** and then the **Create** button.



1. Name the virtual network *vnetEast*.

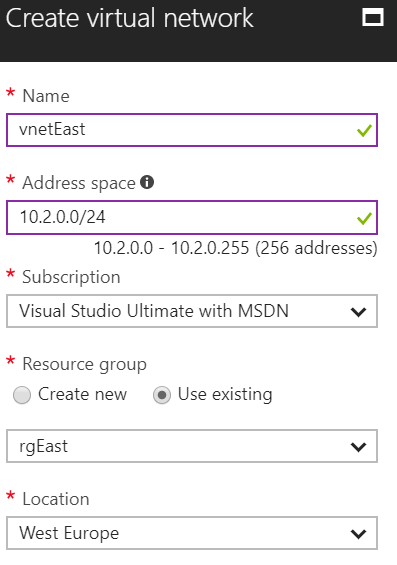
In this exercise, we could start with an internal IP address range, but, we want to make sure that whatever IP range we choose does not overlap with the IP address range we will be using in our second virtual network.

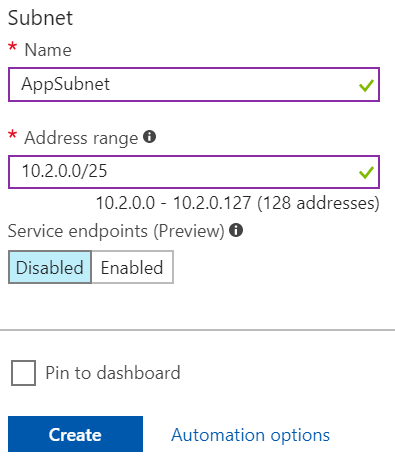
1. For the *address space*, enter the IP **10.2.0.0/24**, with a subnet name of **AppSubnet**.

The *Subnet address range* should be **10.2.0.0/25**. This will leave us with about half the addresses to use for other subnets.

Make sure you choose to put this virtual network in the **rgEast** resource group.

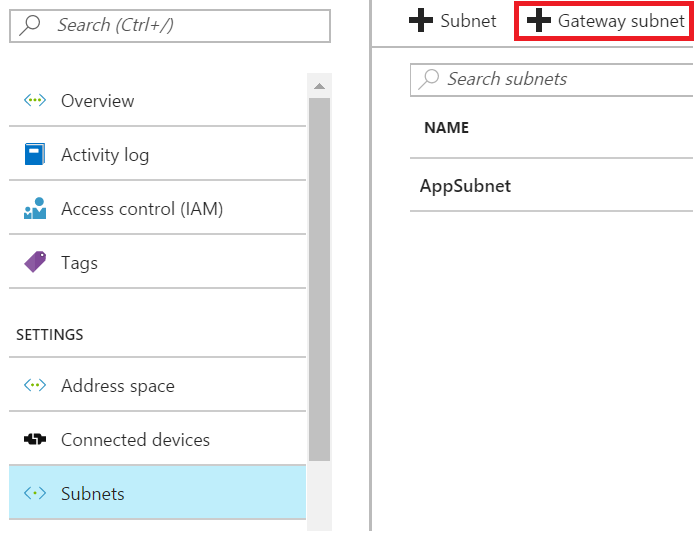
Click **Create**.





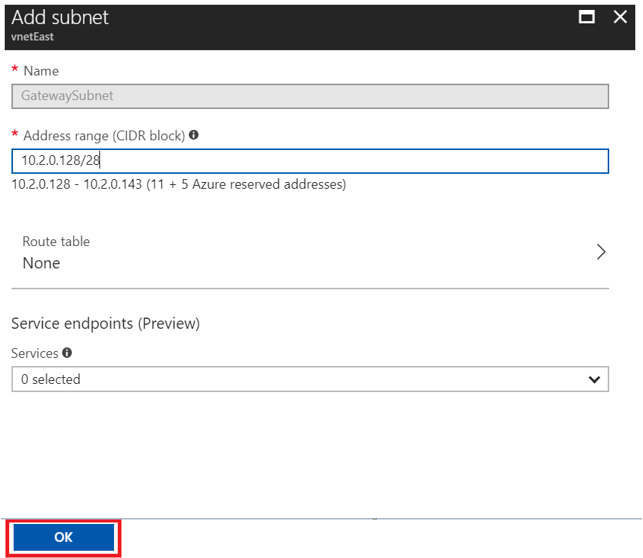
1. Go back to the **rgEast** resource group blade and click on the **vnetEast**. This will bring up the *vnetEast* blade so we can add a subnet.
2. In the *Settings* blade, click on the **Subnets** link.

You then need to click the **+Gateway** **Subnet** button in the Subnets blade to add a new gateway subnet.



1. Accept the default address range and click **OK**.

Once the gateway subnet has been created, go back to the **rgEast** resource group blade.

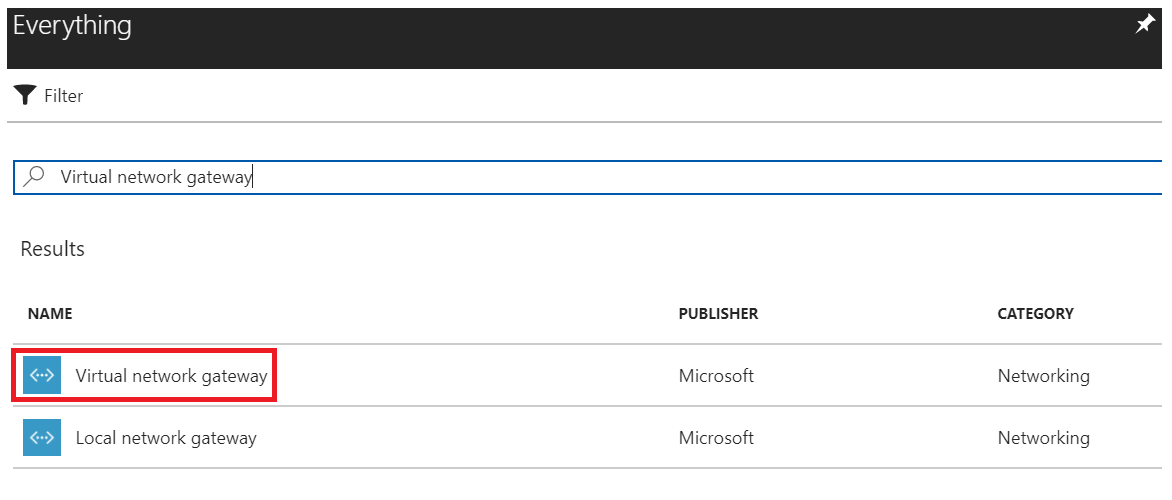


1. In order for our virtual network to connect to another network outside of its Azure region, it needs to have a *virtual network gateway*.

Click the **+Add** button in your resource group blade and then type in **virtual network gateway** into the *Everything* blade.

Then select the **Virtual Network gateway** list item.

Click the **Create** button.

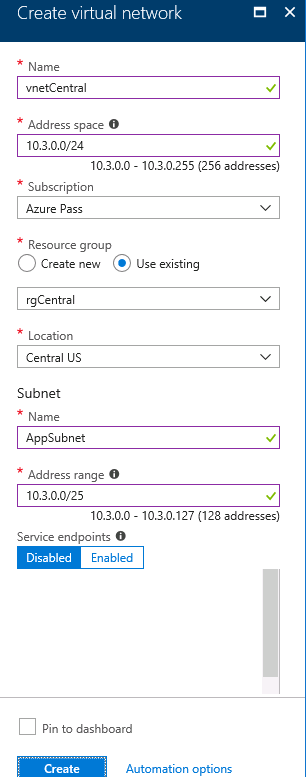


1. Configure the properties of the virtual network gateway as shown in the table below. Please note that it can take 20 minutes for the gateway creation process to complete, but you should be able to move forward with the lab while waiting for it to finish.

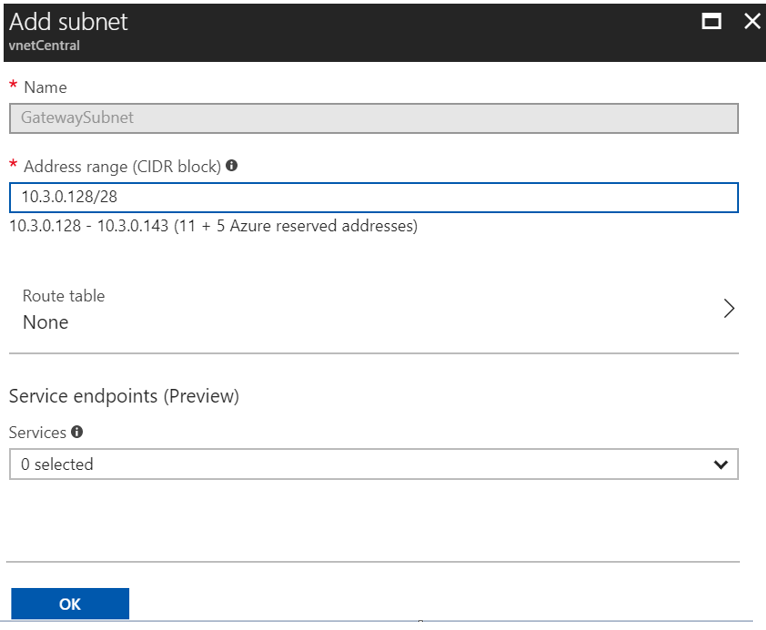
|  |  |
| --- | --- |
| * **Name**: Pick a name for the gateway. It can be anything you wish, within your subscription, but name it so you will know that it is a gateway and not a virtual network. * **Gateway Type**: Choose **VPN** * **VPN Type**: Choose **Route-based** * **SKU**: Choose **VpnGw1** * **Virtual network**: Click on the Virtual Network link and choose **vnetEast** * **First IP Configuration**: Select “Create new”. All you need to do is give the address a unique name within your subscription (for example, **vnetgwEast-pip**). Azure will then create the IP address when you select **OK** in the **Create public IP address** blade. * **Configure BGP ASN**: While it is now possible to enable BGP during creation of the gateway, leave this unchecked. We will enable this via PowerShell later in the lab. * **Location**: Make sure you choose the same data center that you put your virtual network in * Click the **Create** button |  |

## Task 2 – Create the second Virtual Network and Virtual Network gateway

1. Go back to the main **Resource Groups** blade and select the resource group **rgCentral**. You are going to go through the same steps of creating a virtual network with a virtual network gateway that you did in the previous task, except that this will be for the *rgCentral* resource group.
2. Click the **+Add** button and add a new virtual network named **vnetCentral** using the settings in the screenshot below. Pay close attention to the IP addresses that are being used.

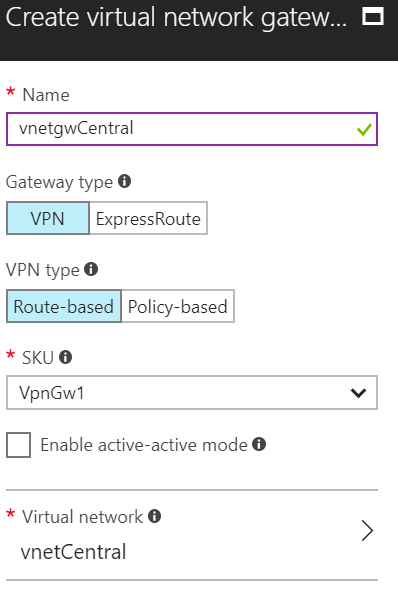


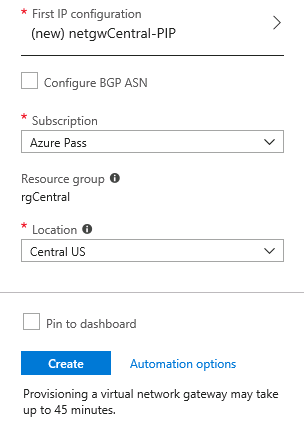
1. Once the virtual network has been created, create a new **gateway subnet**, using the settings shown in the screenshot below.



1. Create a virtual network gateway named **vnetgwCentral** as shown in the screenshot below. Note that you may have to select your region first, so that you will be able to see your *vnetCentral* virtual network.

You need to choose your new *vnetCentral* virtual network, have a different public IP address than *vnetgwEast* and make sure you choose *Route-based* VPN type.



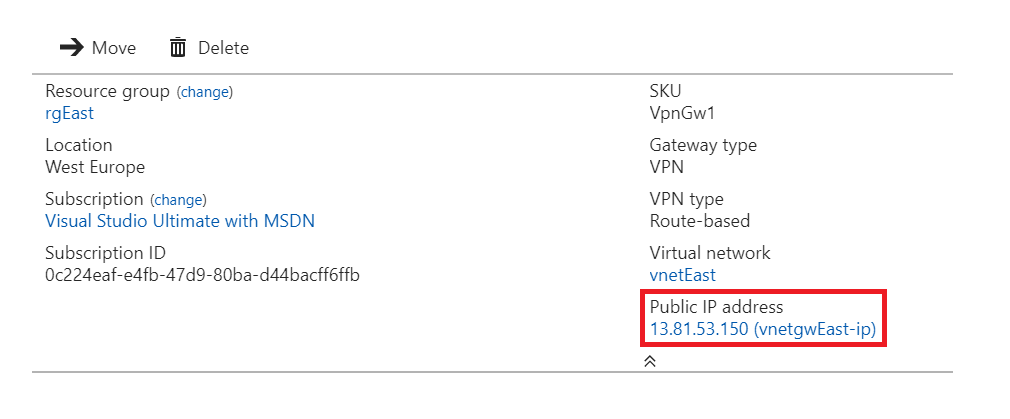


1. Remember that it can take quite a few minutes to create the gateway.

## Task 3 – Confirm Virtual Network Gateway creation

You will know that your virtual network gateway(s) are created, when Azure provides a new public IP address to the gateway. You need to check both gateways before continuing.

1. Go into the *rgEast* resource group and click on your *virtual network gateway*.
2. You will see your new public IP address in the virtual network gateway blade. Look for Public IP address.



1. Repeat the process for the **rgCentral** resource group.

## Task 4 – Create the virtual network connections

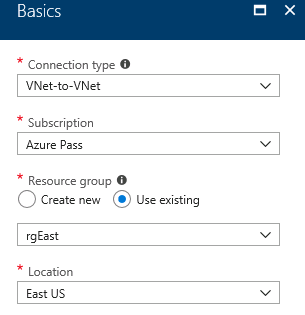
Now that you have the virtual network gateways created (this takes quite a while), you need to create an *Azure Connection* so that the gateways can connect together.

1. From within the *rgEast* resource group blade, select **+Add** and then enter *Connection.*

Select **Connection** in the Everything blade.

Click the **Create** button.

1. On the Basics blade, leave everything as is and select the **OK** button:



1. On the **Settings** blade, review the properties in the table below.

|  |  |
| --- | --- |
| * **First virtual network gateway**: Since we are already ‘in’ the rgEast resource group, we will choose the first virtual network gateway, which is **vnetgwEast** * **Second virtual network gateway**: Our other gateway created in a previous task is **vnetgwCentral** * **Establish bidirectional connectivity**: Select to use * **First** and **Second Connection Names**: Type in connection names or accept the default names * **Shared Key: Very important if bidirectional connectivity is unticked** – the Shared key(s) must be identical on both the central connection and the east connection. You can have up to 8 characters/numbers. For this lab, simply enter “abc123” * **Enable BGP**: leave unchecked |  |

1. Select the **OK** button.
2. Select the **OK** button on the **Summary** page.
3. Because you selected the bidirectional option on the **Settings** blade (above), you do not need to setup a connection in *rgCentral*.

## Task 5 – Confirm the connection between the virtual networks

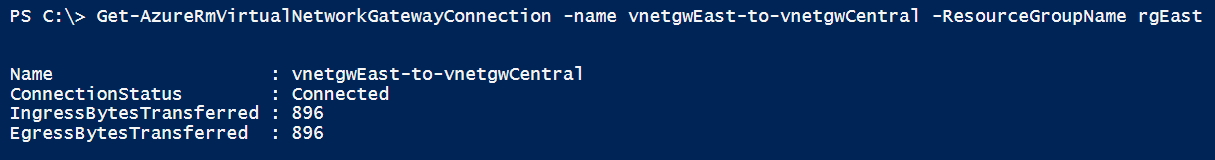
There are multiple ways to confirm connectivity between virtual networks, such as putting virtual machines in the networks and pinging machines in other networks, but the fastest way is to use PowerShell for the confirmation.

1. Open **PowerShell ISE** as an Administrator.
2. In the *PowerShell command prompt*, type in **Login-AzureRMAccount**, press Enter, and log in to your subscription.

NOTE: If you have multiple subscriptions, you will need to use **Select-AzureRMSubscription** in order to select the correct subscription for usage in the PowerShell window.

1. To confirm the *rgEast* connection to the *rgCentral*, type in the following command. If you have used different naming conventions from the suggested ones, modify the command before running it. When prompted to confirm the action, select **Yes to All**:

Get-AzureRmVirtualNetworkGatewayConnection -name vnetgwEast-to-vnetgwCentral -ResourceGroupName rgEast | fl Name, ConnectionStatus, IngressBytesTransferred, EgressBytesTransferred



You should be able to see the ConnectionStatus and the number of ingress and egress bytes transferred.

1. Perform the same PowerShell cmdlet but this time for the vnetgwCentral-to-vnetgwEast connection in the *rgEast* resource group.
2. Leave your PowerShell session open.

# Exercise 2 - Enable BGP on virtual network gateways and connections

BGP is a routing protocol that enables routers to exchange routing 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.

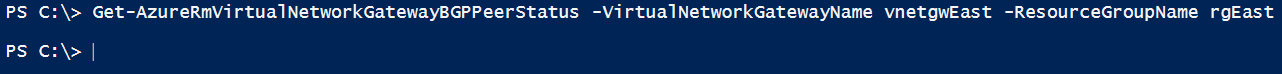
During the previous steps of this lab, you configured a VNet-to-VNet VPN connection whereby the routing paths were configured between the two gateways during the creation of your VPN connections. These routing paths were derived from each of the VNets address spaces (this is the reason why a local network 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:

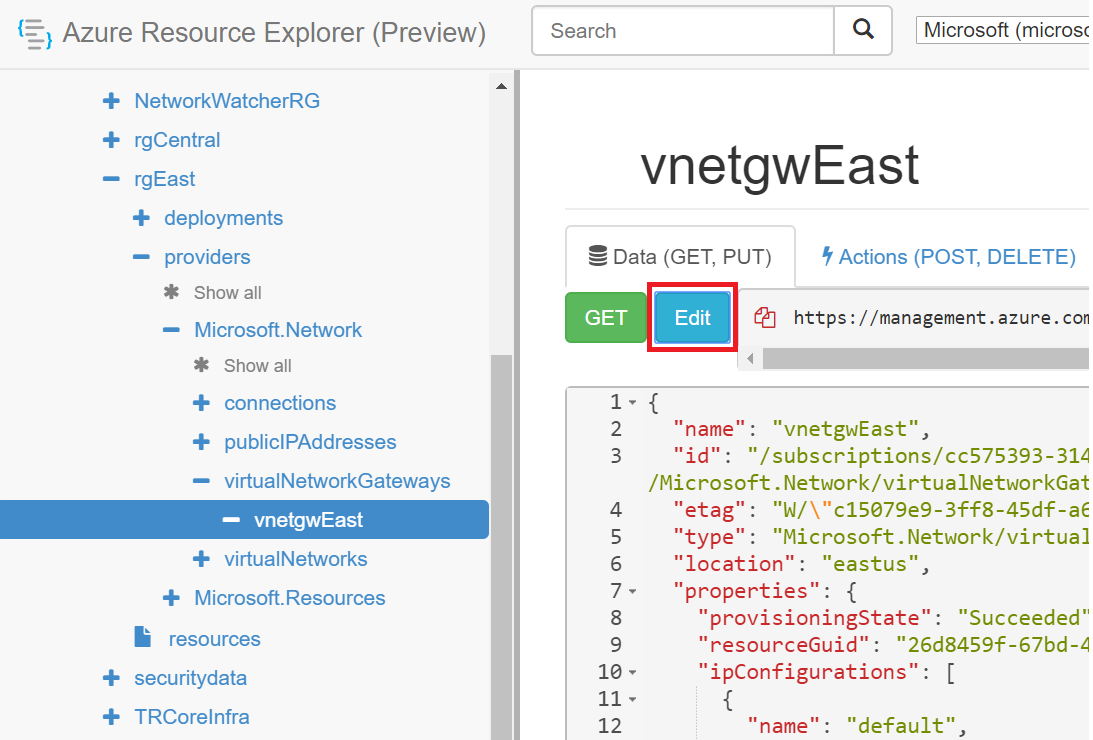
Get-AzureRmVirtualNetworkGatewayBGPPeerStatus -VirtualNetworkGatewayName vnetgwEast -ResourceGroupName rgEast



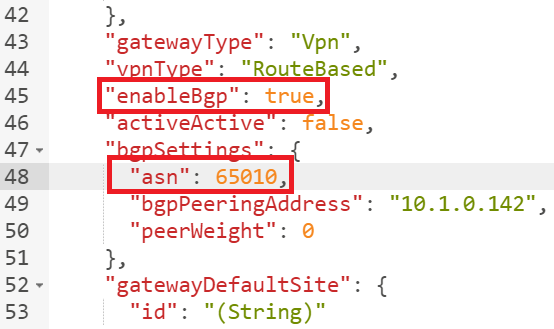
1. Repeat the above for the *vnetgwCentral* gateway.
2. Leave your PowerShell session open.

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

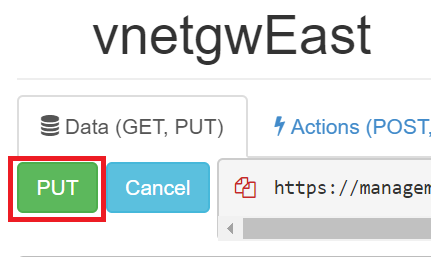
1. Navigate to https://resources.azure.com/ and login with your Azure administrator account.
2. In the left-hand pane, expand **subscriptions|*SubscriptionName*|resourceGroups|rgEast|providers|Microsoft.Network|virtualNetworkGateways|vnetgwEast** and click **Edit** in the right-hand pane.



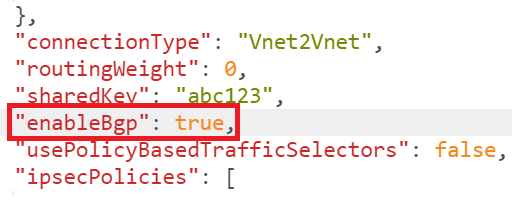
1. In the right-hand pane, scroll down to the **“enableBgp”** tag and configure it to **true** and configure its **ASN** tag value to **65010.**



1. Click the **Read/Write** button (top right of window).
2. Scroll to the top and click the **Put** button.



1. Repeat this process for the **vnetgwCentral** 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.
2. Navigate to **subscriptions*|SubscriptionName*|resourceGroups|rgEast|providers|Microsoft.Network|connections|** **vnetgwCentral-to-vnetgwEast** and click **Edit** in the right-hand pane.
3. In the right-hand pane, scroll down to the **“enableBgp”** tag and configure it to **true** and click the **Put** button.

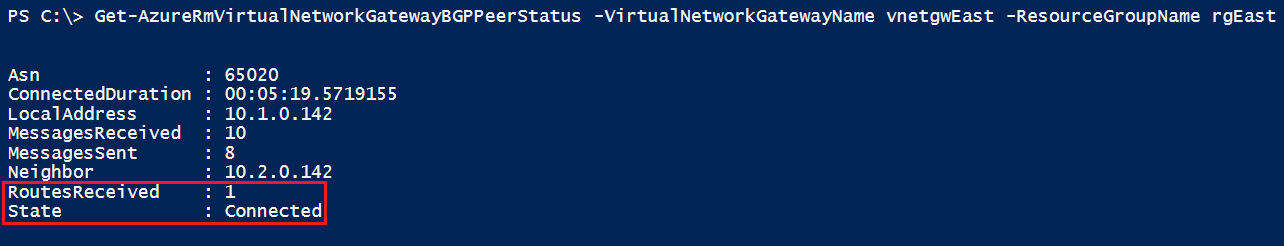


1. Repeat this process for the *vnetgwEast-to-vnetgwCentral* gateway connection.

## 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:

Get-AzureRmVirtualNetworkGatewayBGPPeerStatus -VirtualNetworkGatewayName vnetgwEast -ResourceGroupName rgEast



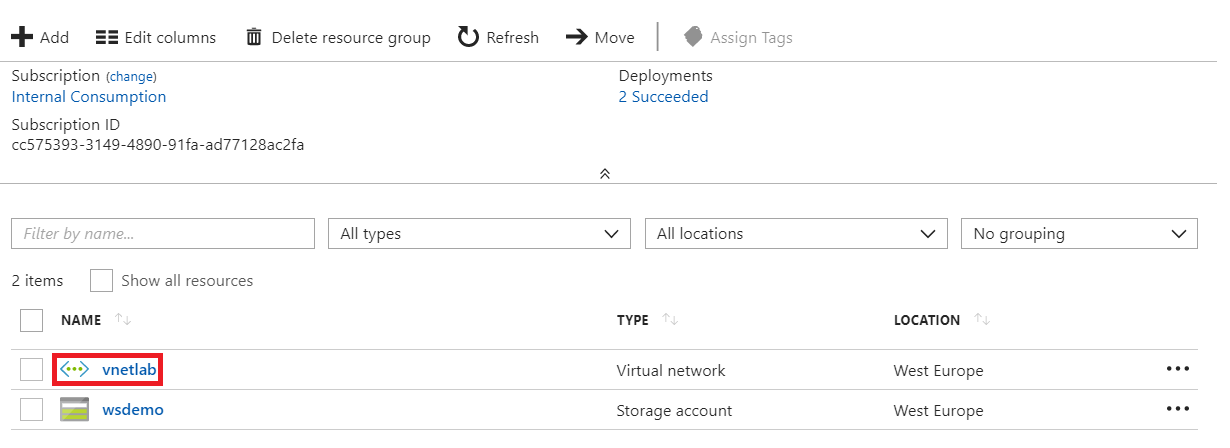
1. Confirm that there is a successful connection with your BGP peer (which is the other VNet gateway in this case) and that at least 1 route has been received or learnt.

# 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.

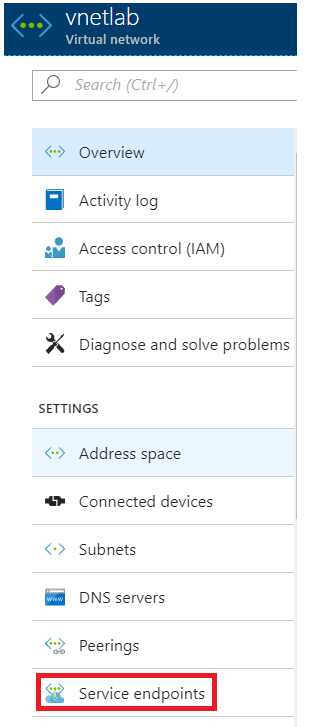
## Task 1 – Configure Virtual Network Service Endpoints

From within the Azure portal, navigate to the resource group that was used to store the IIS and SQL servers from the previous lab and click on the VNet that was created.



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

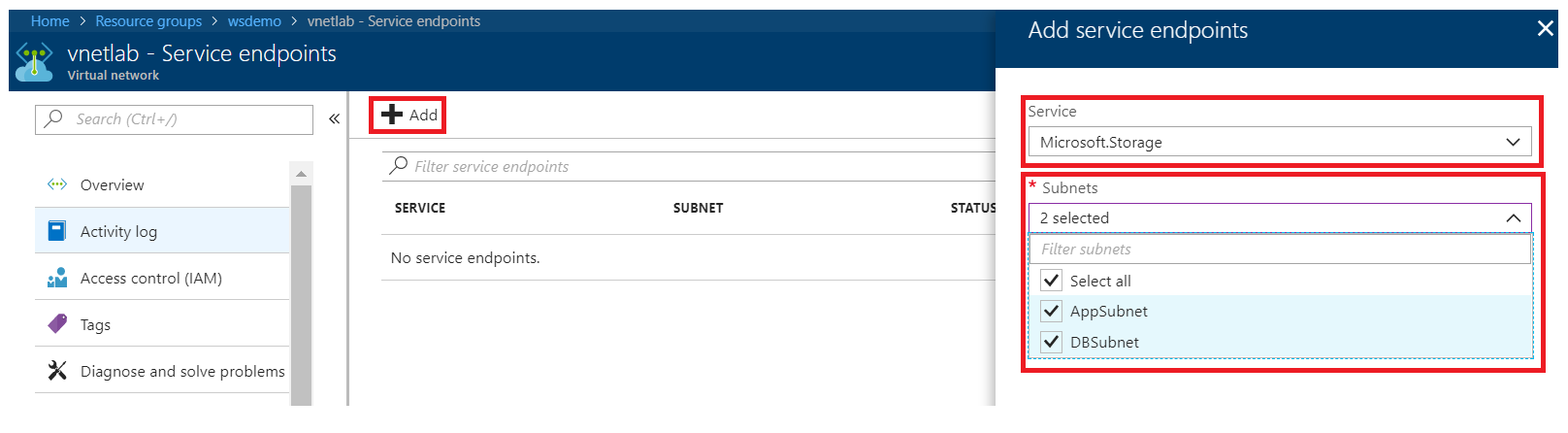
## 



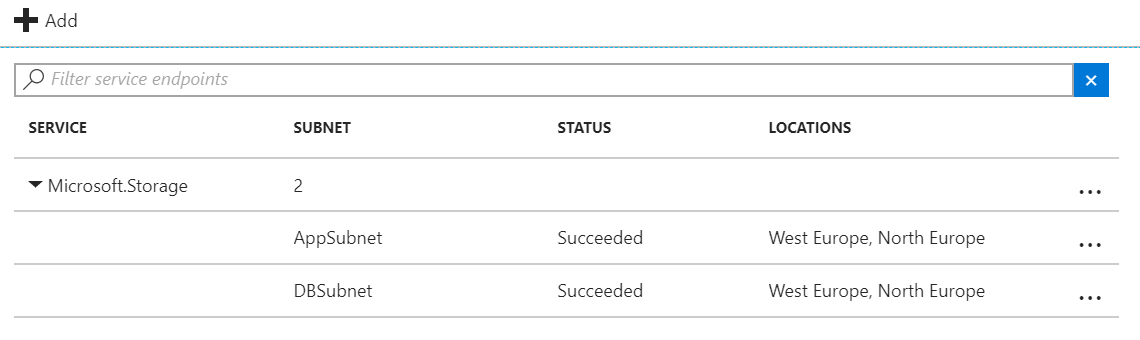
1. In the right-hand pane, click **+Add** and select **Microsoft.Storage** from the **Service** drop down menu.

From the **Subnets** drop down menu, choose **Select all**.

Click **Add**. This process can take up to 15 minutes.

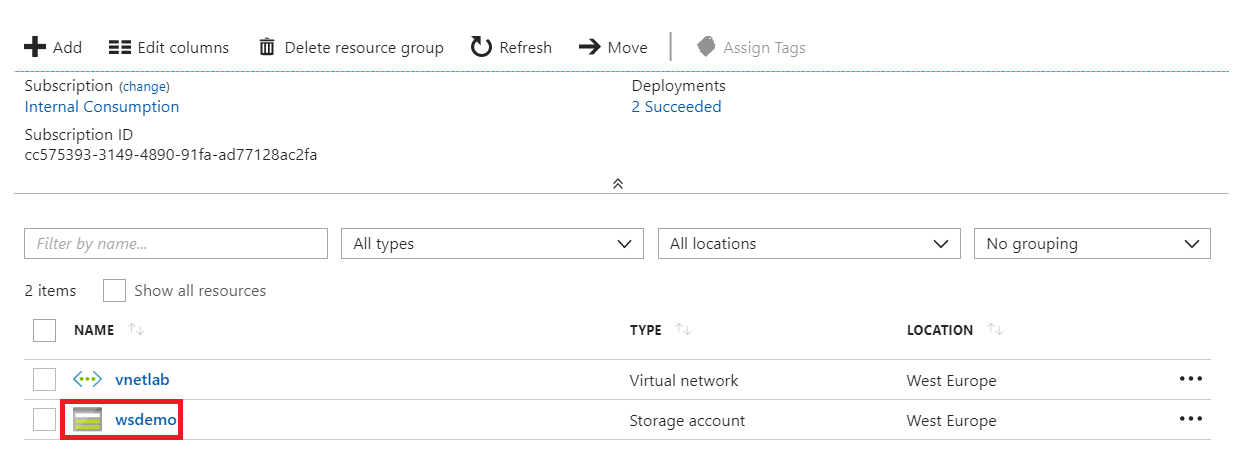


1. Confirm that the Azure Storage Service endpoints have been added whilst you are still in the Service endpoints pane. You have now configured all inbound and outbound traffic from your virtual network to your Azure storage account to go over the Microsoft Azure backbone network.

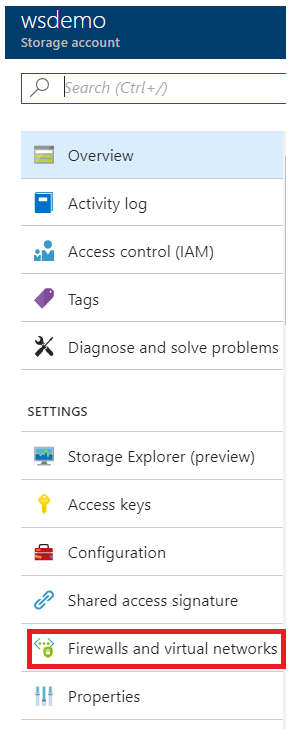


## Task 2 – Configure Storage Account Firewall

1. From within the Azure portal, navigate to the resource group that was used to store the IIS and SQL servers from the previous lab and click on the Storage account that was created.



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



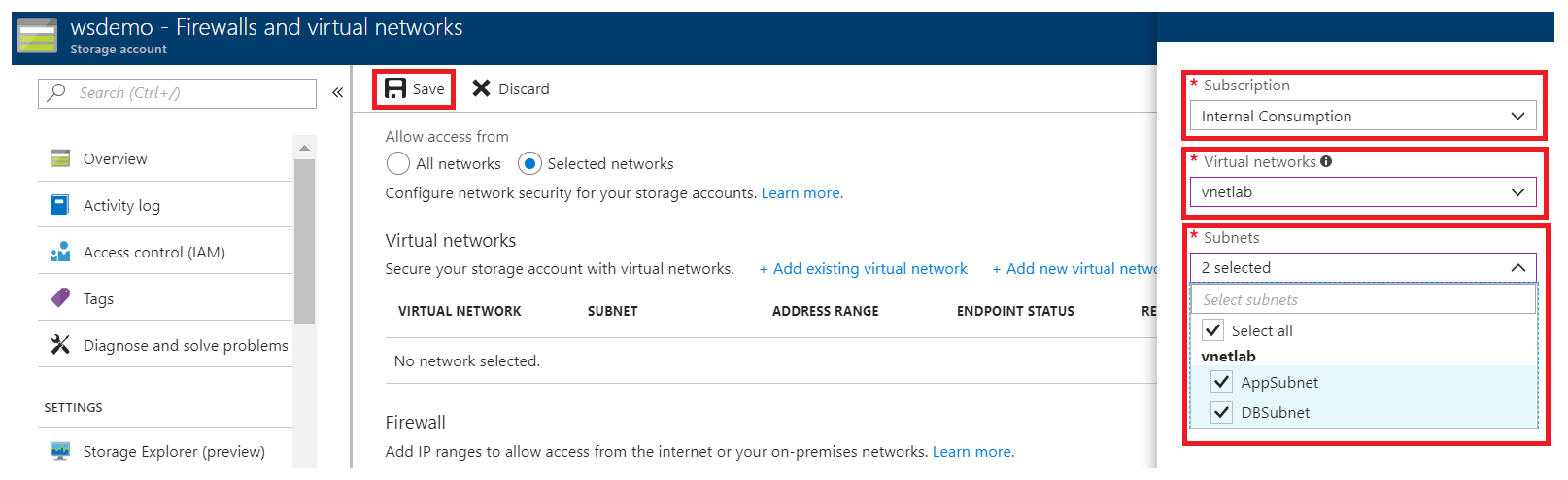
1. In the right-hand pane, click the **Selected networks** radio button.
2. Click **+Add existing virtual network**.

Select your appropriate subscription.

From the Virtual networks drop down menu, select the relevant virtual network (this would be the virtual network that you connected your IIS and SQL servers to in the previous lab).

Finally, from the **Subnets** drop down menu, choose **Select all**.

Click **Add** and then click **Save**.



1. Whilst 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 both the AppSubnet and DBSubnets in your previously created 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.

