Microsoft Cloud Workshop

Establishing Network Connectivity in Azure

Hands-on lab step-by-step

August 2018

Establishing Network Connectivity in Azure hands-on lab step-by-step

Abstract and learning objectives

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

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

Networking References

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

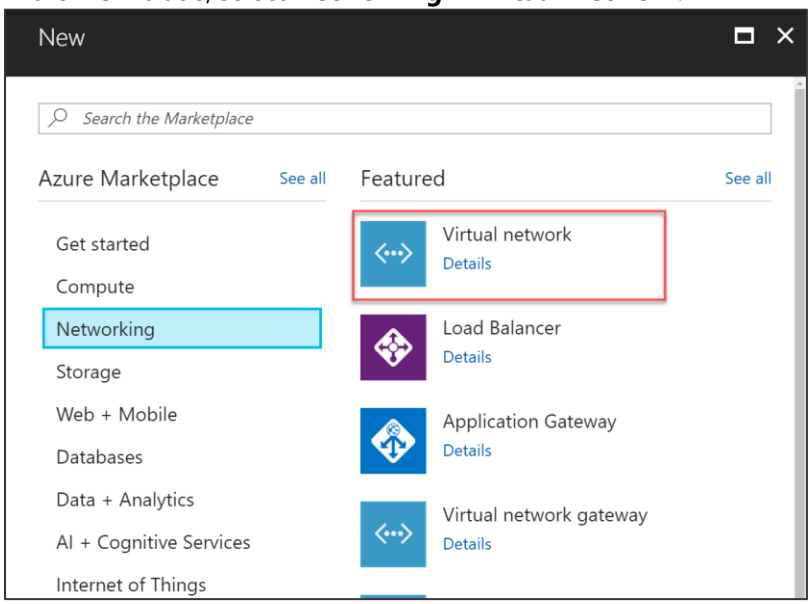
Exercise 1: Create Virtual Networks & Establish Connectivity Between Regions (VNet-to-VNet VPN Gateway)

Task 1: Create a VNET in the first region with 2 subnets

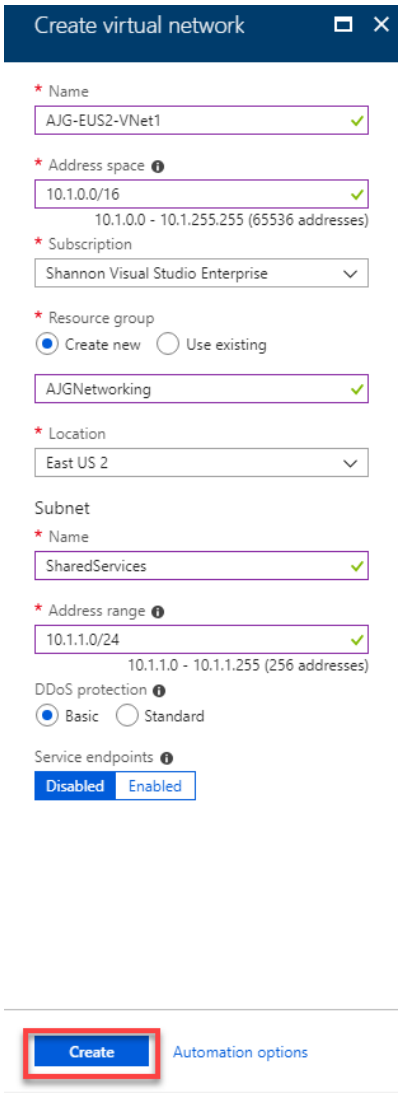
1. Browse to the Azure portal and login: https://portal.azure.com/.

2. In the left pane, click **+ Create Resource**.

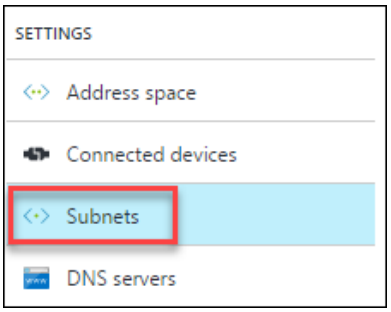
3. In the **New** blade, select **Networking > Virtual Network**.



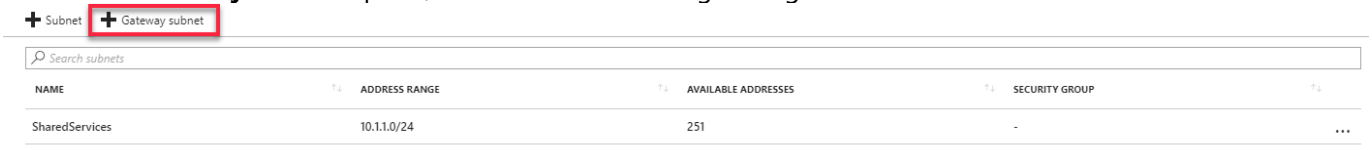
4. For the **Create virtual network** settings, enter the following information:
    a. Name: **AJG-EUS2-VNet1**
    b. Address space: **10.1.0.0/16**
    c. Subnet name: **SharedServices**
    d. Subnet address range: **10.1.1.0/24**
    e. Subscription: **Choose your subscription**
    f. Resource group: **AJGNetworking**
    g. Location: **East US 2**
    h. Leave **DDoS Protection** at **Basic** and **Service Endpoints** as **Disabled**.
    i. Click the **Create** button to continue.



5. Once the deployment is complete, add one more subnet to the VNET. To do this, select the **Subnets >** icon in the **Settings** area.



6. Click the **+ Gateway Subnet** option, and enter the following settings:

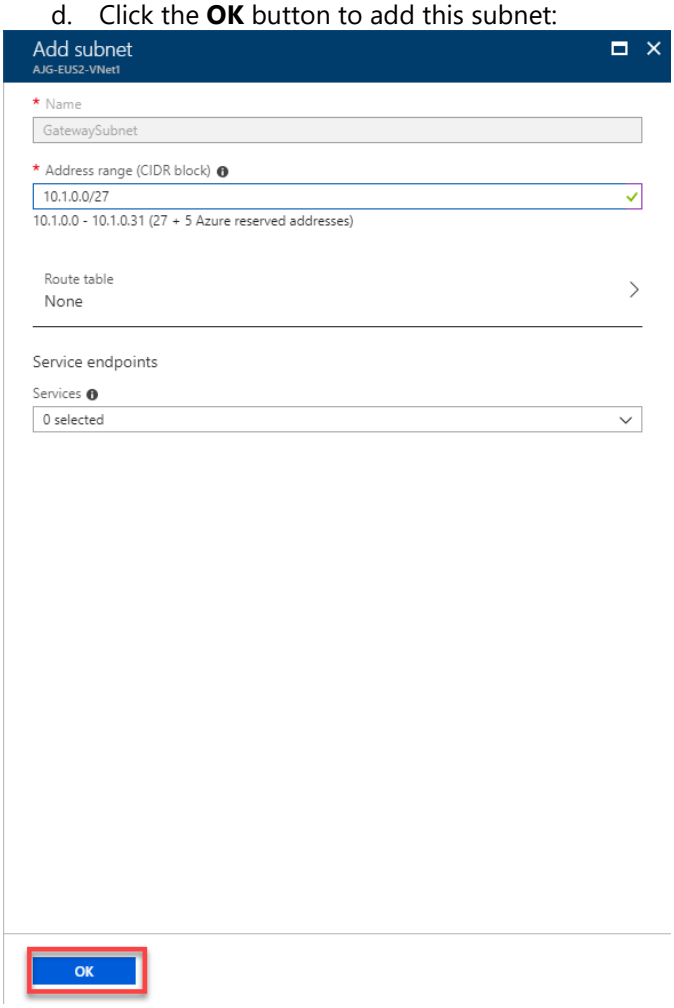


   a. The name (GatewaySubnet) cannot be changed and will be grayed out.

b. Address range (CIDR block): **10.1.0.0/27**

c. Leave the Route Table at None and do not configure Service Endpoints.

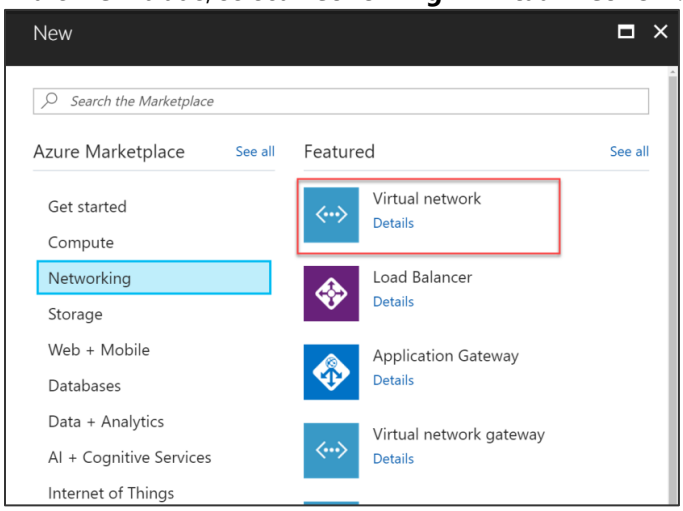
d. Click the **OK** button to add this subnet:



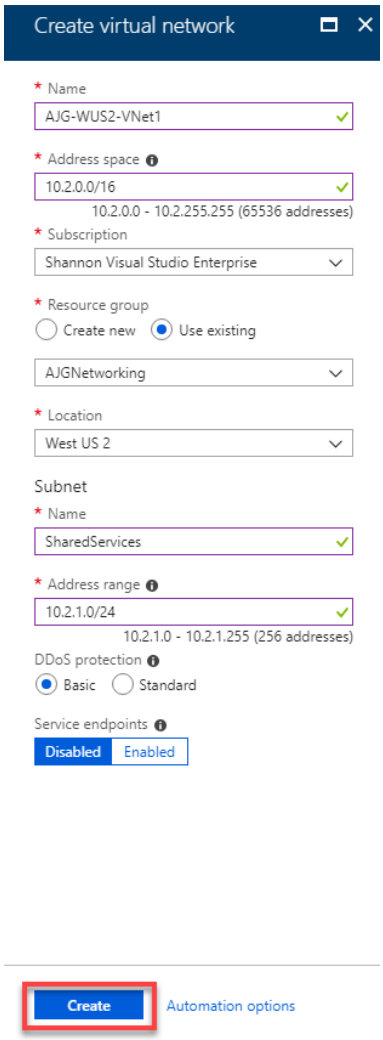
Task 2: Create a VNET in the second region with 2 subnets

1. In the left pane, click **+ Create Resource**.

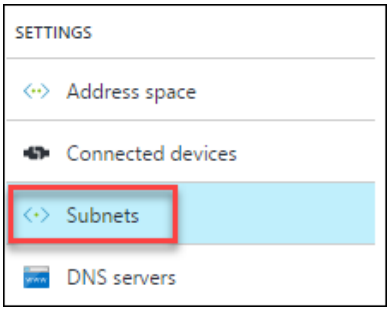
2. In the **New** blade, select **Networking > Virtual Network**.



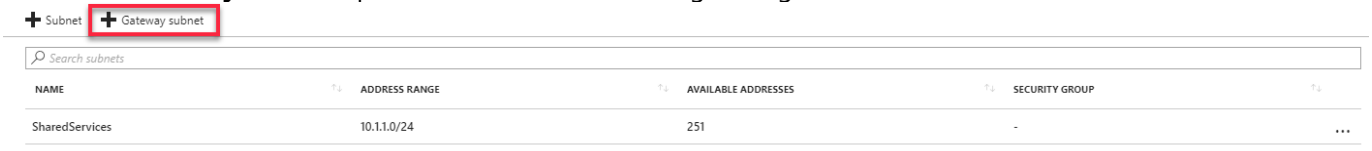
3. For the **Create virtual network** settings, enter the following information:
    a. Name: **AJG-WUS2-VNet1**
    b. Address space: **10.2.0.0/16**
    c. Subnet name: **SharedServices**
    d. Subnet address range: **10.2.1.0/24**
    e. Subscription: **Choose your subscription**
    f. Resource group: **AJGNetworking (use existing)**
    g. Location: **West US 2**
    h. Leave **DDoS Protection** at **Basic** and **Service Endpoints** as **Disabled**.
    i. Click the **Create** button to continue.



4. Once the deployment is complete, add one more subnet to the VNET. To do this, select the **Subnets >** icon in the **Settings** area.



5. Click the **+Gateway Subnet** option, and enter the following settings:

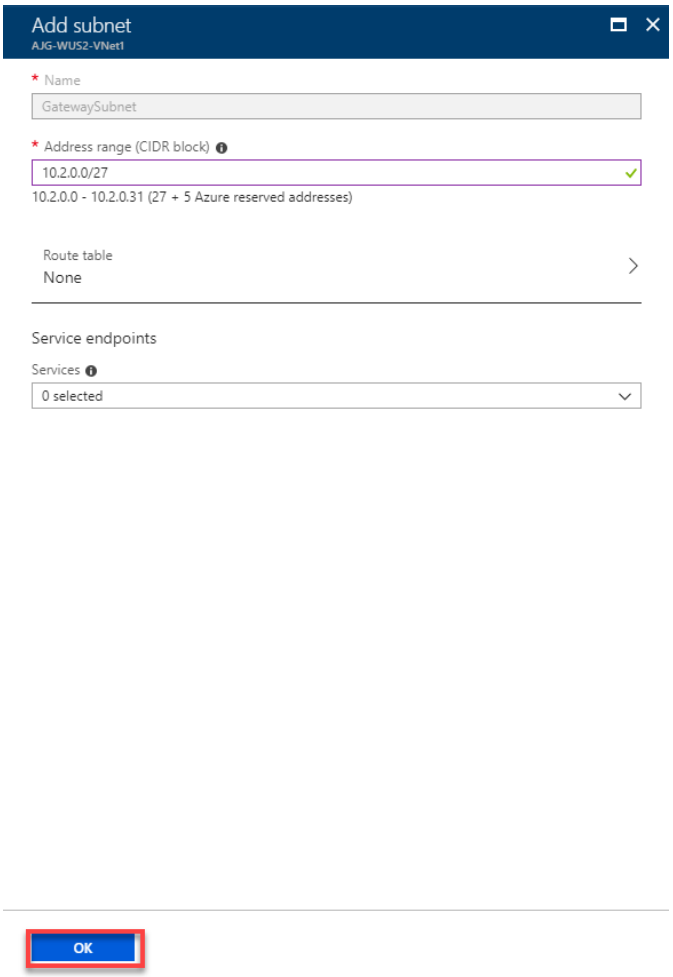


   a. The name (GatewaySubnet) cannot be changed and will be grayed out.

   b. Address range (CIDR block): **10.2.0.0/27**

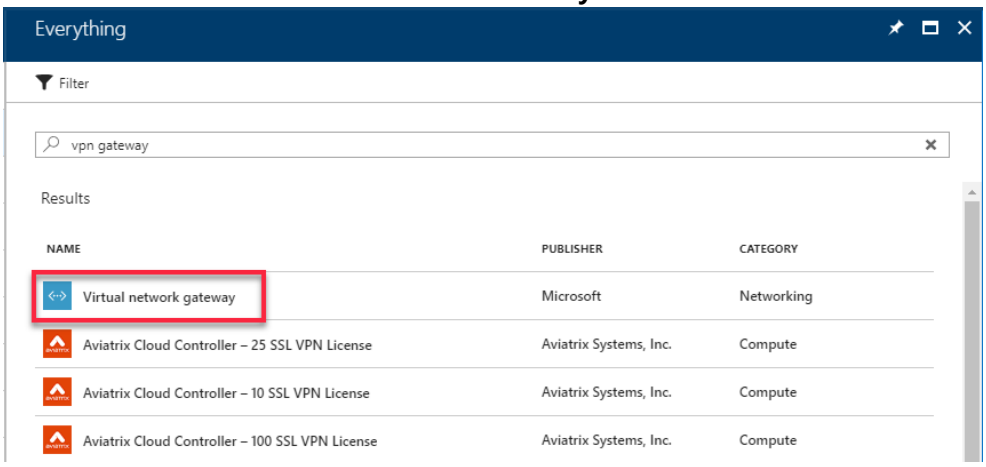
c. Leave the Route Table at None and do not configure Service Endpoints.

d. Click the **OK** button to add this subnet:



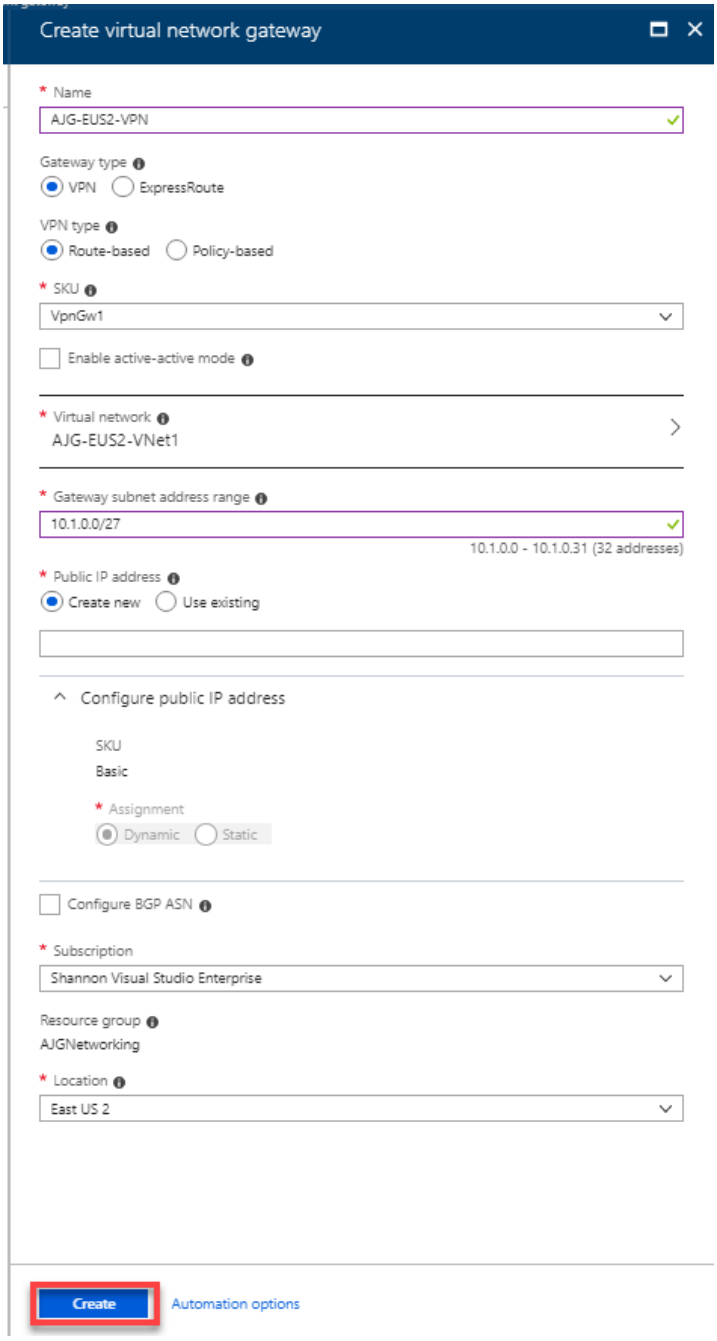
Task 3: Create a Virtual Network Gateway in first region

1. In the left pane, click **+ Create Resource**.
2. Search for and click on **Virtual Network Gateway**. Click **Create** on the next screen



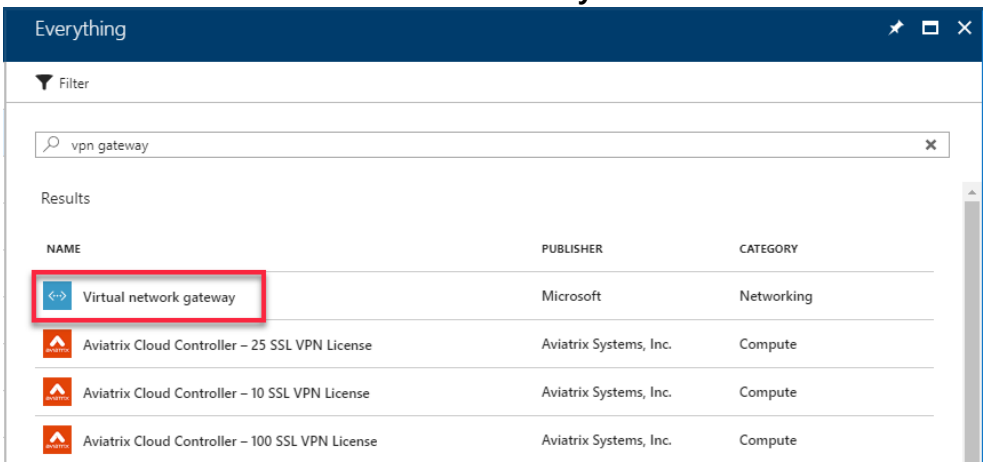
3. For the **Create virtual network gateway** settings, enter the following:

a. Name: **AJG-EUS2-VPN**
b. Gateway type: **VPN**
c. VPN Type: **Route Based**
d. SKU: **VpnGw1**
e. Leave **Enable active-active mode unchecked**
f. Virtual network: **AJG-EUS2-VNet1**
g. Create new Public IP Address: **AJG-EUS2-VPN-pip**
h. Leave Configure **BGP ASN unchecked**
i. Click **Create (this process will take approximately 40-45 minutes to create)**

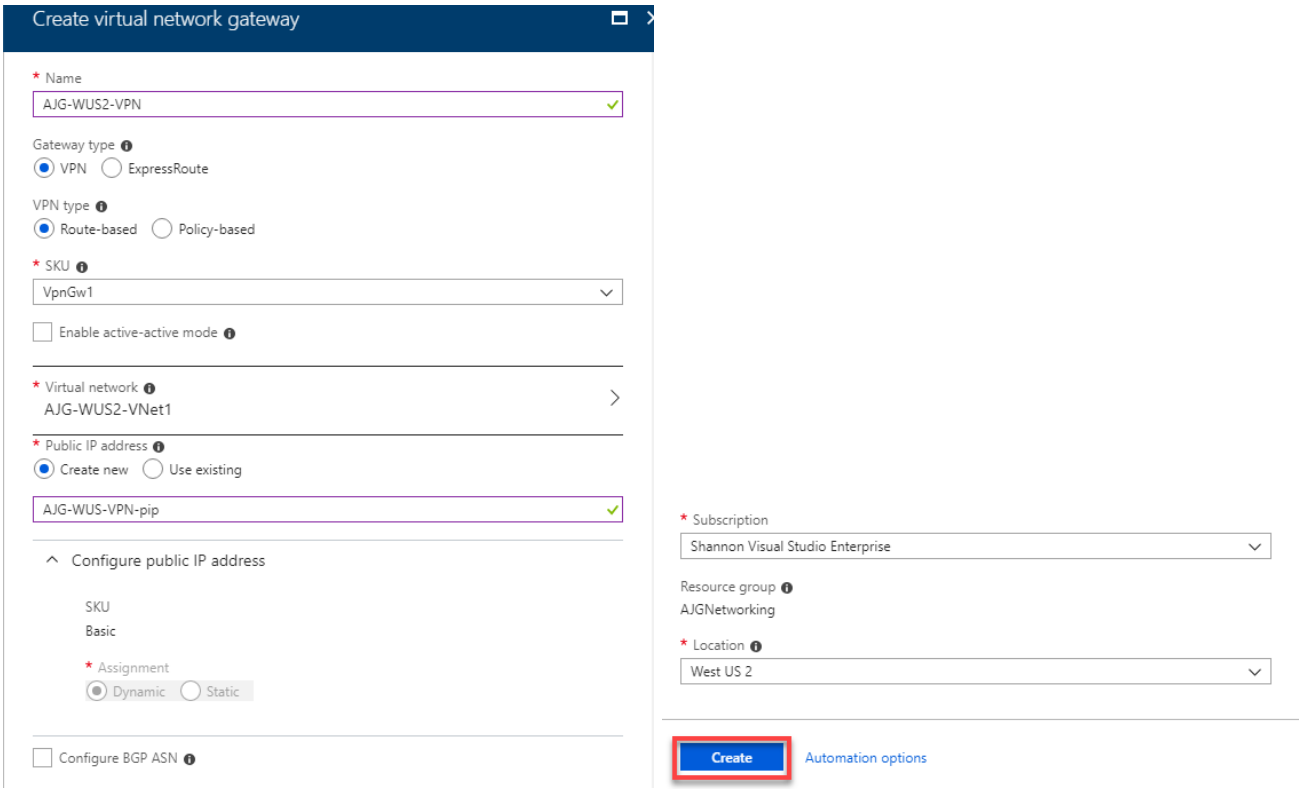


Task 4: Create a Virtual Network Gateway in second region

1. In the left pane, click **+ Create Resource**.
2. Search for and click on **Virtual Network Gateway**. Click **Create** on the next screen

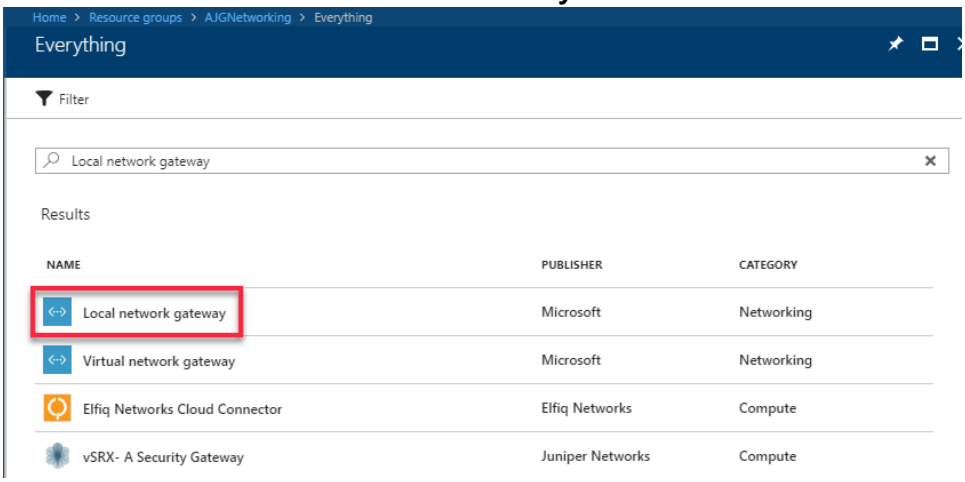


3. For the **Create virtual network gateway** settings, enter the following:
    a. Name: **AJG-WUS2-VPN**
    b. Gateway type: **VPN**
    c. VPN Type: **Route Based**
    d. SKU: **VpnGw1**
    e. Leave **Enable active-active mode unchecked**
    f. Virtual network: **AJGVNet2**
    g. Create new Public IP Address: **AJG-WUS-VPN-pip**
    h. Leave Configure **BGP ASN unchecked**
    i. Click **Create (this process will take approximately 40-45 minutes to create)**

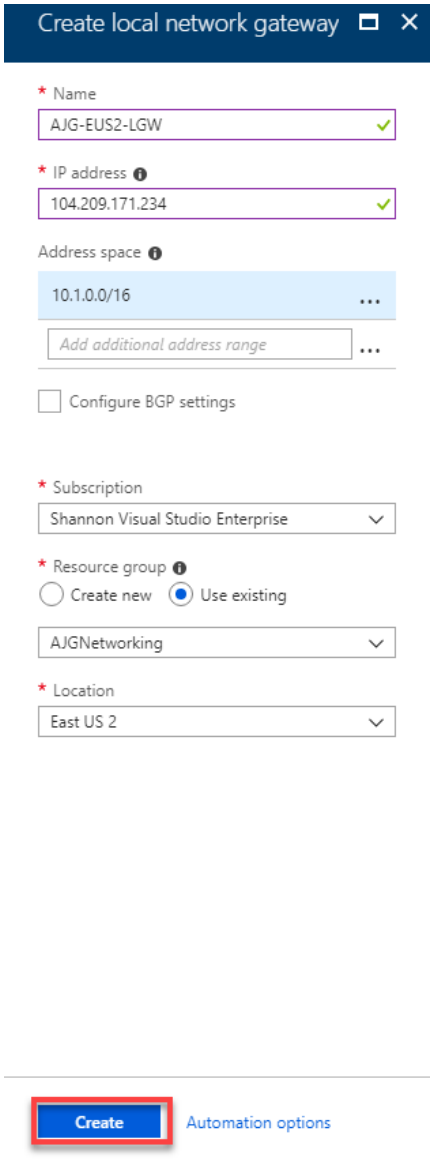


Task 5: Create Local Network Gateways, Connections, and Establish VPN

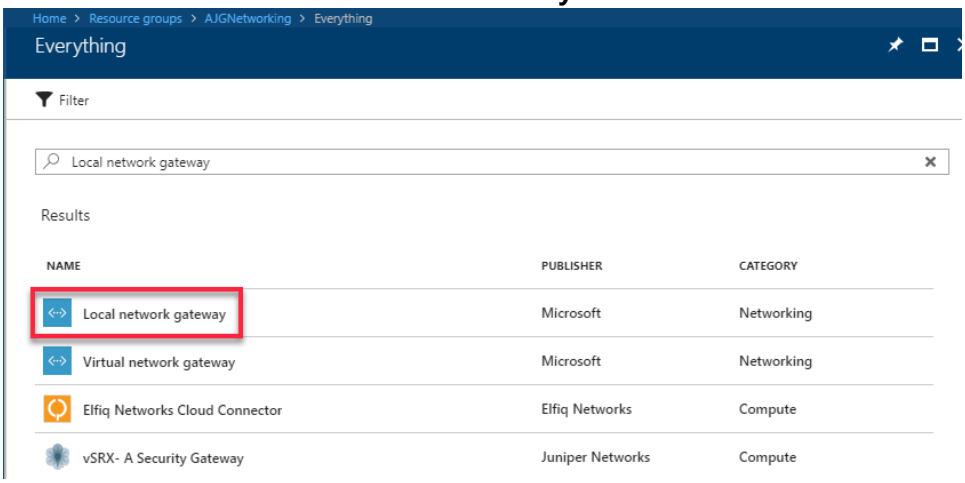
1. In the left pane, click **+ Create Resource**.
2. Search for and click on **Local Network Gateway**. Click **Create** on the next screen.



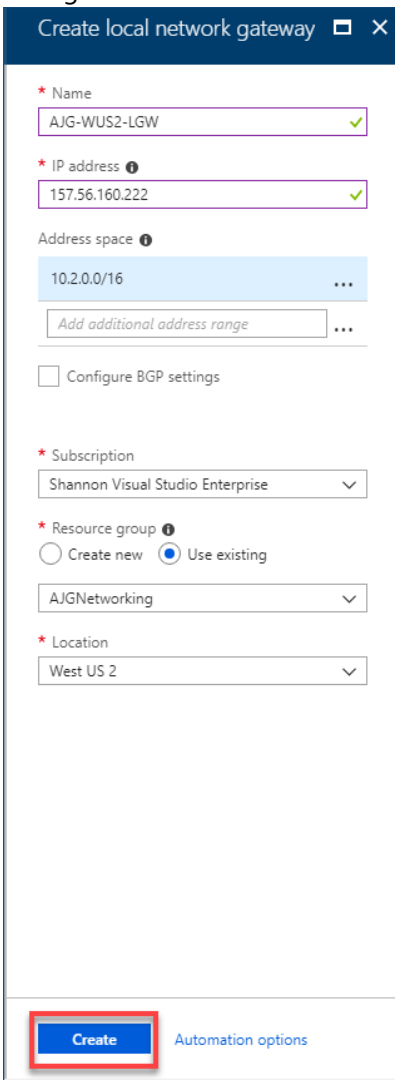
3. For the Create Local Network Gateway settings, enter the following:
   a. Name: **AJG-EUS2-LGW**
   b. IP Address: **Use public IP address assigned to VPN during creation**
   c. Address Space: **10.0.0.0/16**
   d. Leave Configure BGP settings blank
   e. Use existing Resource Group
   f. Location: **East US 2**
   g. Click Create



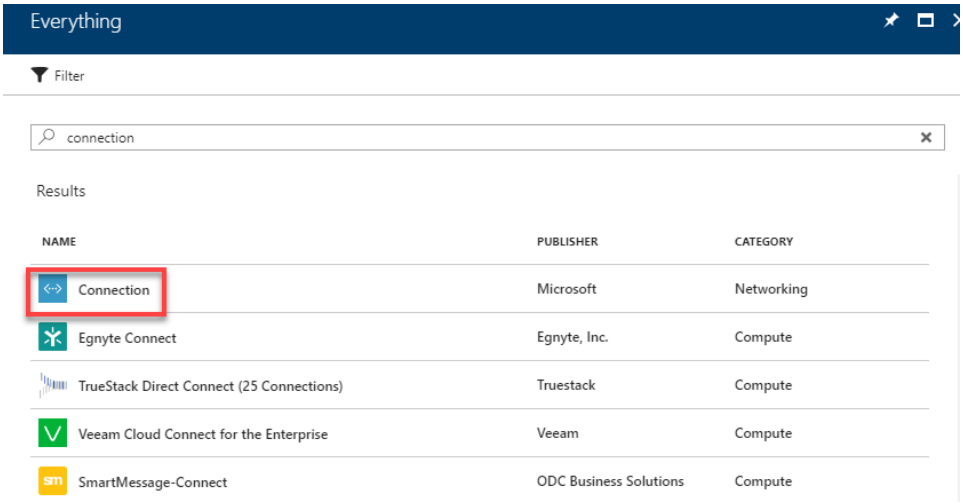
4. In the left pane, click **+ Create Resource**.
5. Search for and click on **Local Network Gateway**. Click **Create** on the next screen.



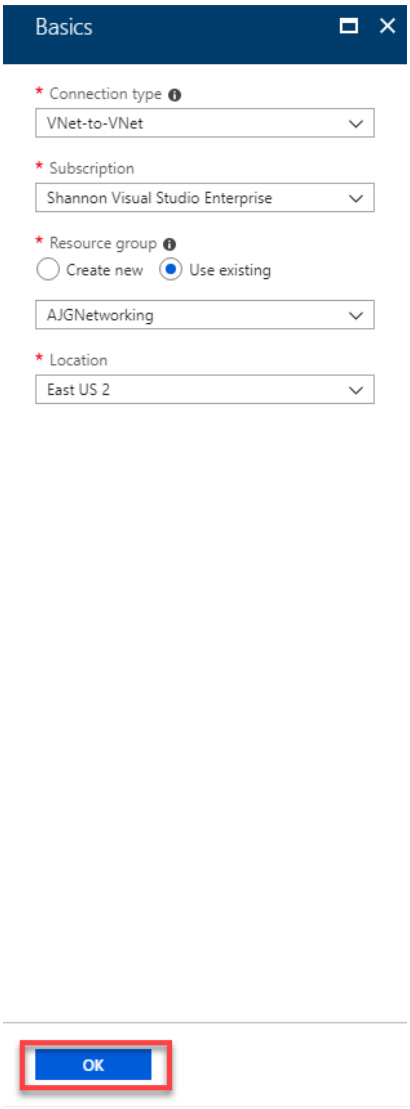
6. For the Create Local Network Gateway settings, enter the following:
   a. Name: **AJG-WUS2-LGW**
   b. IP Address: Use public IP address assigned to VPN during creation
   c. Address Space: **10.2.0.0/16**
   d. Leave Configure BGP settings blank
   e. Use existing Resource Group
   f. Location: West US 2
   g. Click Create



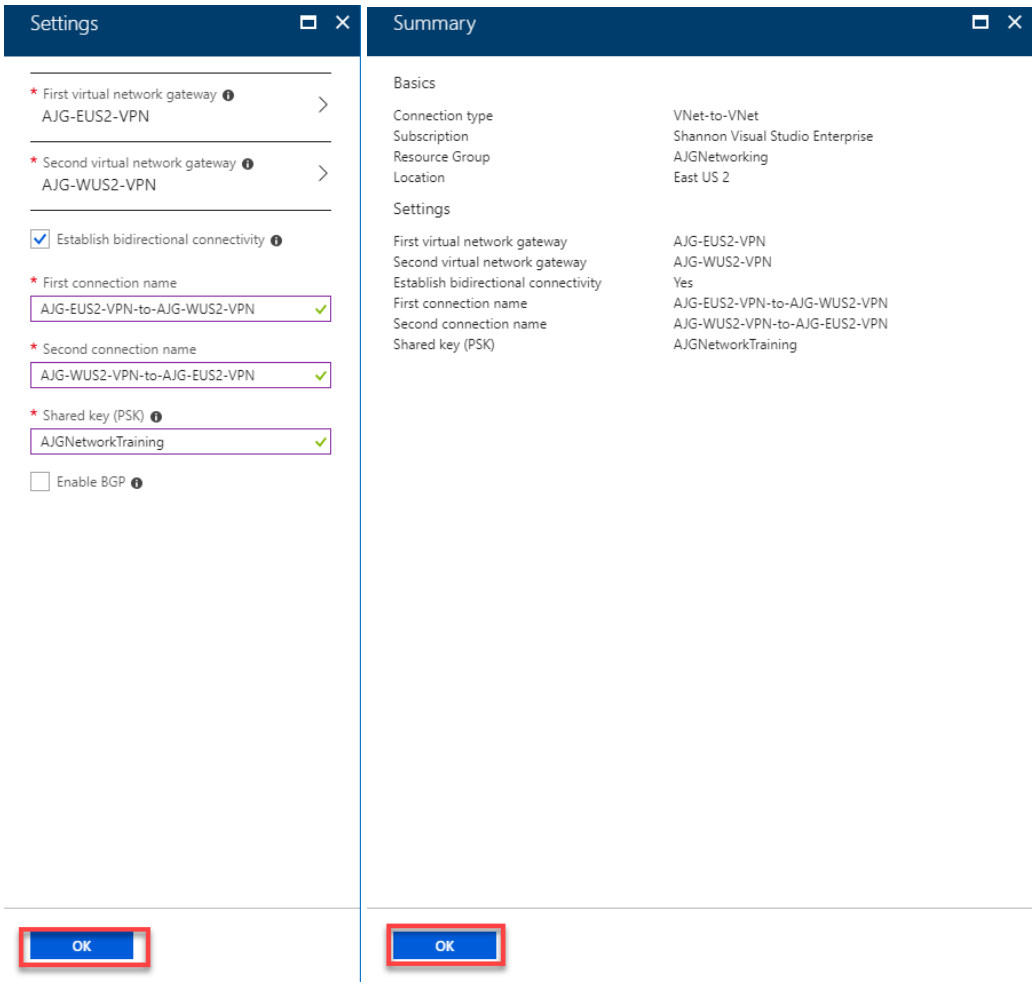
7. In the left pane, click + Create Resource.
8. Search for and click on **Connection**. Click Create on the next screen.



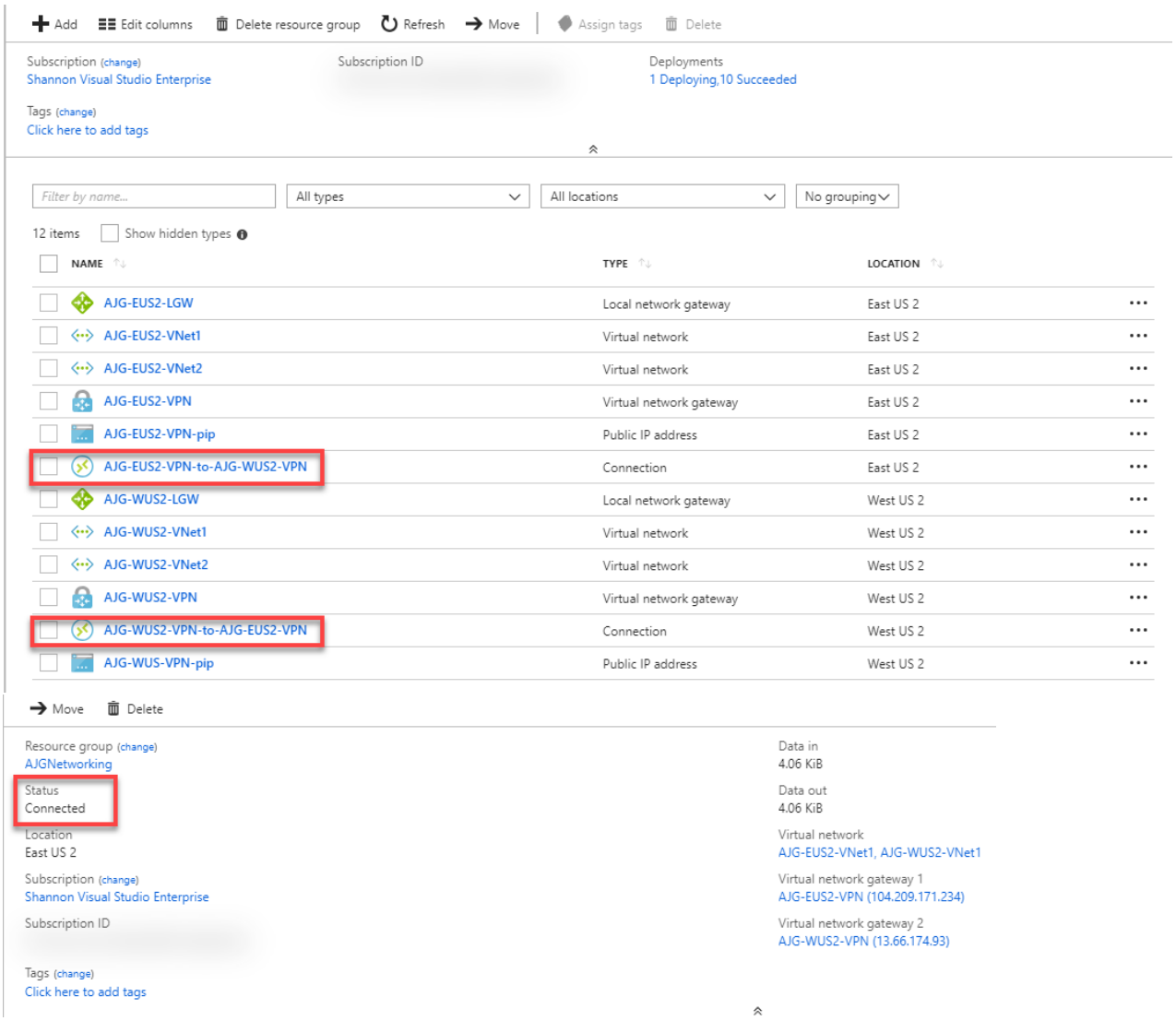
9. For the Basics blade, enter the following:
    a. Connection Type: VNet-to-VNet
    b. Select subscription
    c. Use existing Resource Group
    d. Location: East US 2
    e. Click OK



10. For the Settings blade, enter the following:
    a. Choose first virtual network gateway: AJG-EUS2-VPN
    b. Choose second virtual network gateway: AJG-WUS2-VPN
    c. Leave the check mark in Establish bidirectional connectivity
    d. Leave defaults for First connection name and second connection name
    e. Enter the Shared Key: AJGNetworkingTraining
    f. Click OK at the bottom
    g. Click OK on the summary page



11. After a minute or two, you will see 2 Connection resources show up in the resource group and both will show the VPN status as Connected:

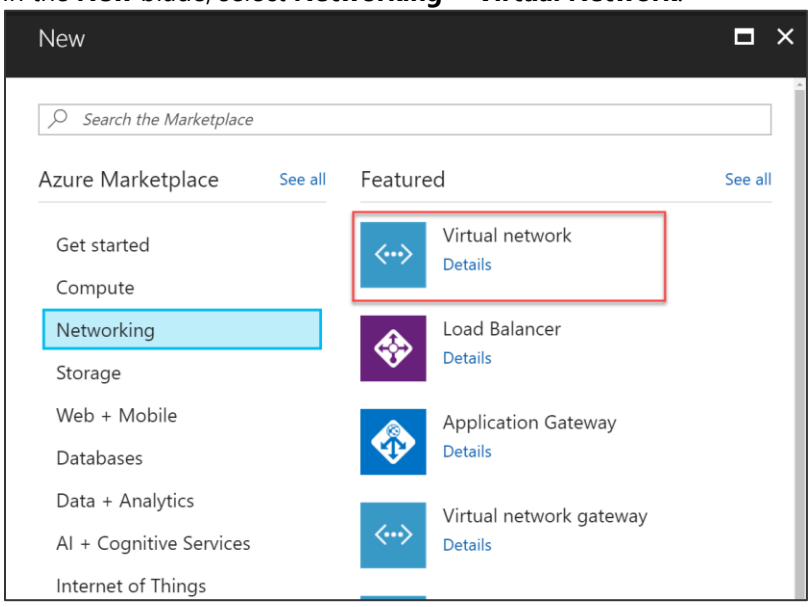


Exercise 2: Establish Connectivity with Regional and Global VNet Peering

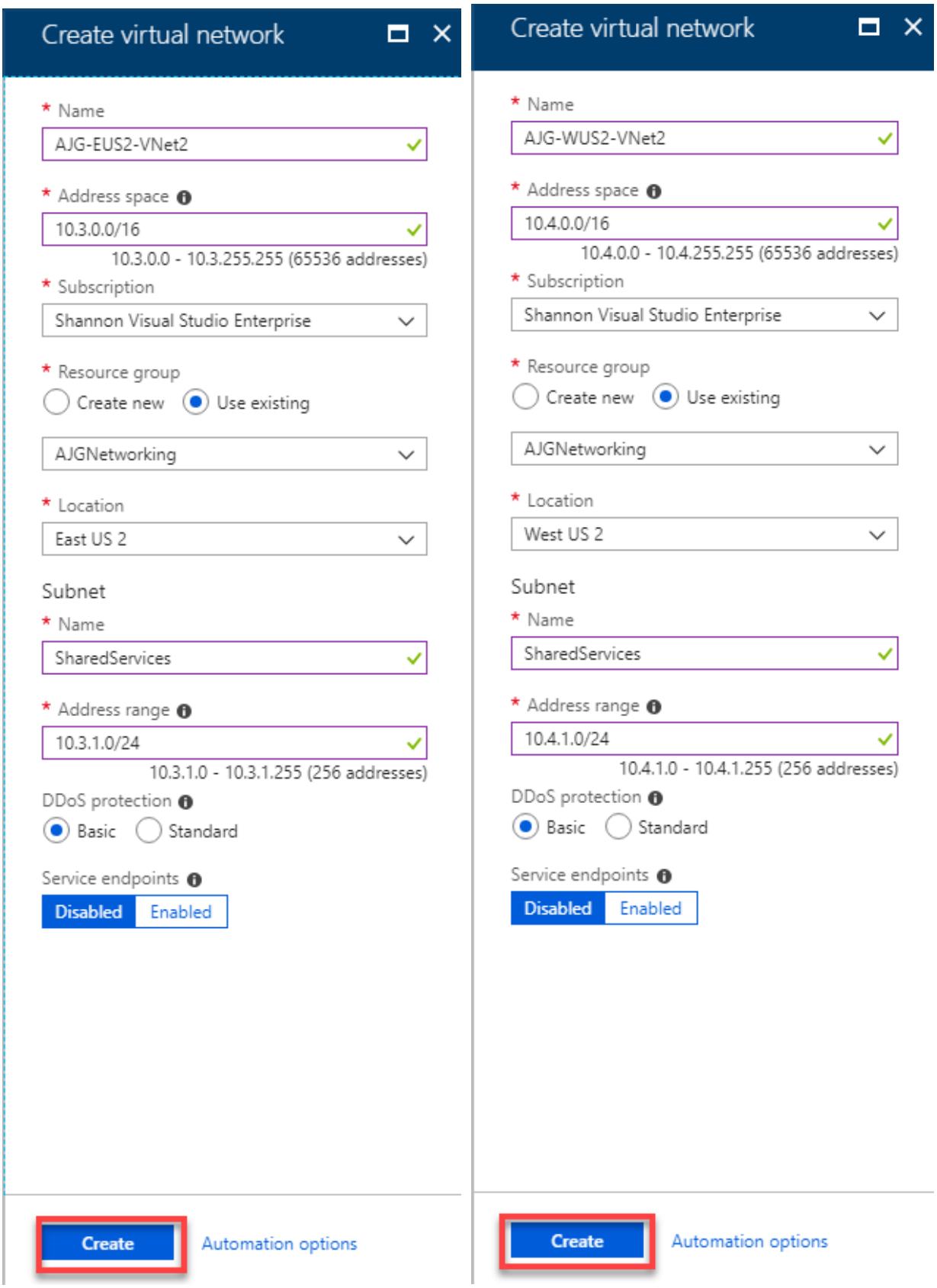
Task 1: Create 2 Additional Virtual Networks – 1 in East US and 1 in West US

1. In the left pane, click **+ Create Resource**.

2. In the **New** blade, select **Networking > Virtual Network**.

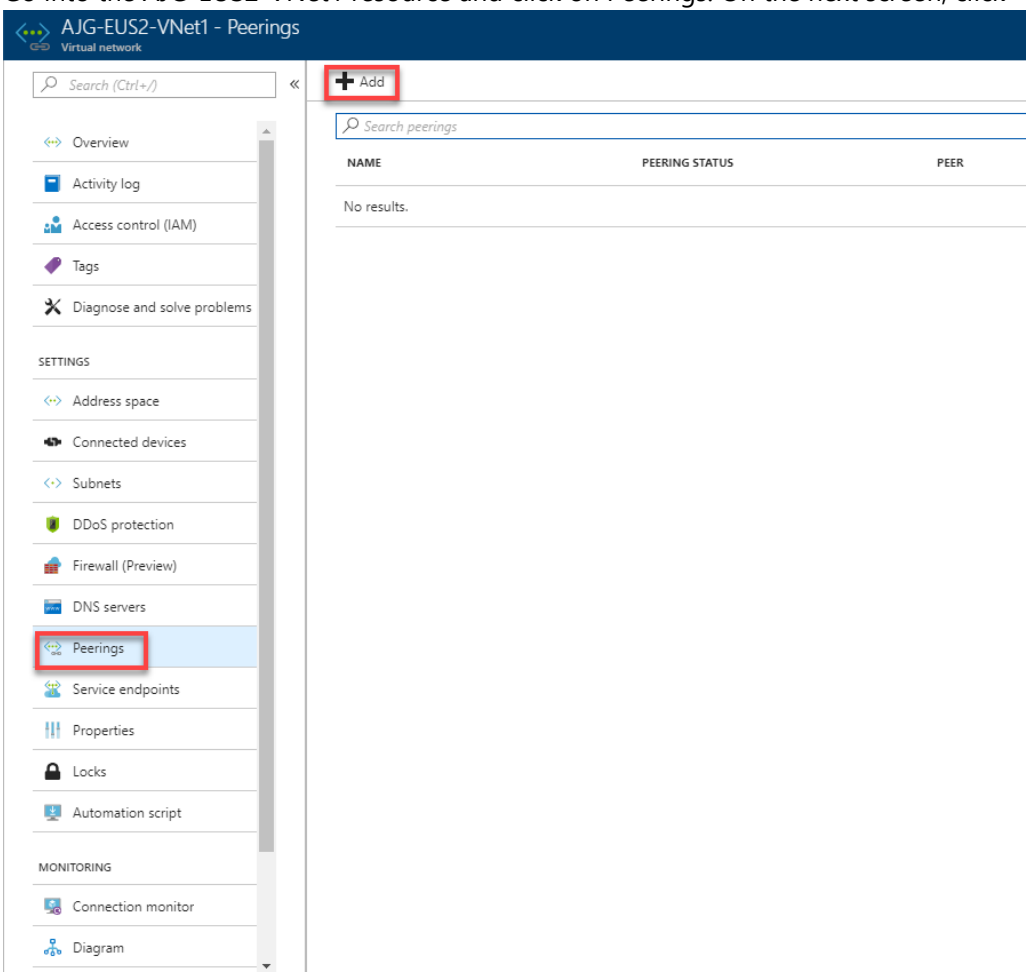


3. For the **Create virtual network** settings, enter the following information:
    a. Name: **AJG-EUS2-VNet2 (East US 2) AJG-WUS2-VNet2 (West US 2)**
    b. Address space: **10.3.0.0/16 (East US 2) 10.4.0.0/16 (West US 2)**
    c. Subnet name: **SharedServices (Both)**
    d. Subnet address range: **10.3.1.0/24 (East US 2) 10.4.1.0/24 (West US 2)**
    e. Subscription: **Choose your subscription**
    f. Resource group: **AJGNetworking**
    g. Location: **East US and West US**
    h. Leave **DDoS Protection** at **Basic** and **Service Endpoints** as **Disabled**.
    i. Click the **Create** button to continue.

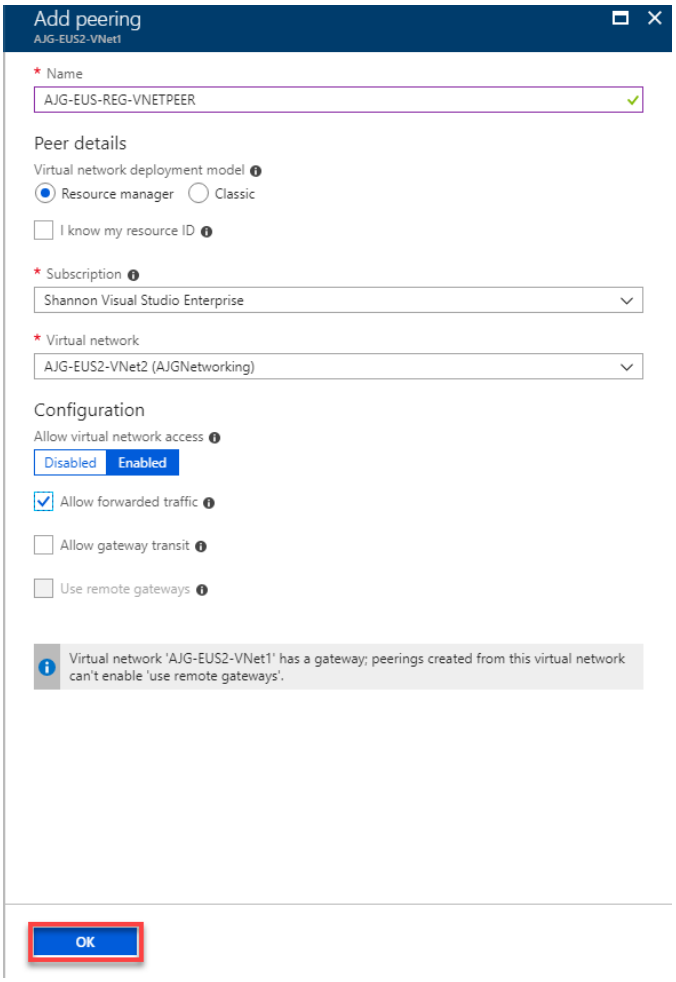


Task 2: Create Regional VNet Peer Between AJG-EUS2-VNet1 and AJG-EUS2-VNet2

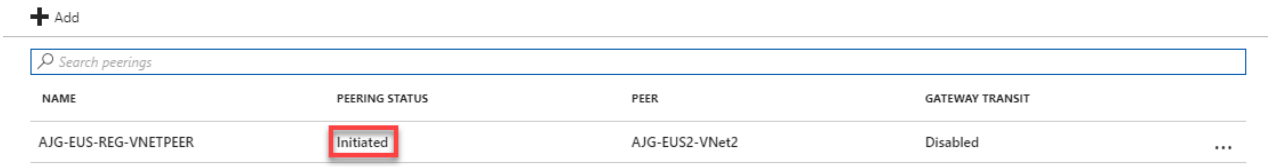
4. Go into the AJG-EUS2-VNet1 resource and click on Peerings. On the next screen, click +Add.



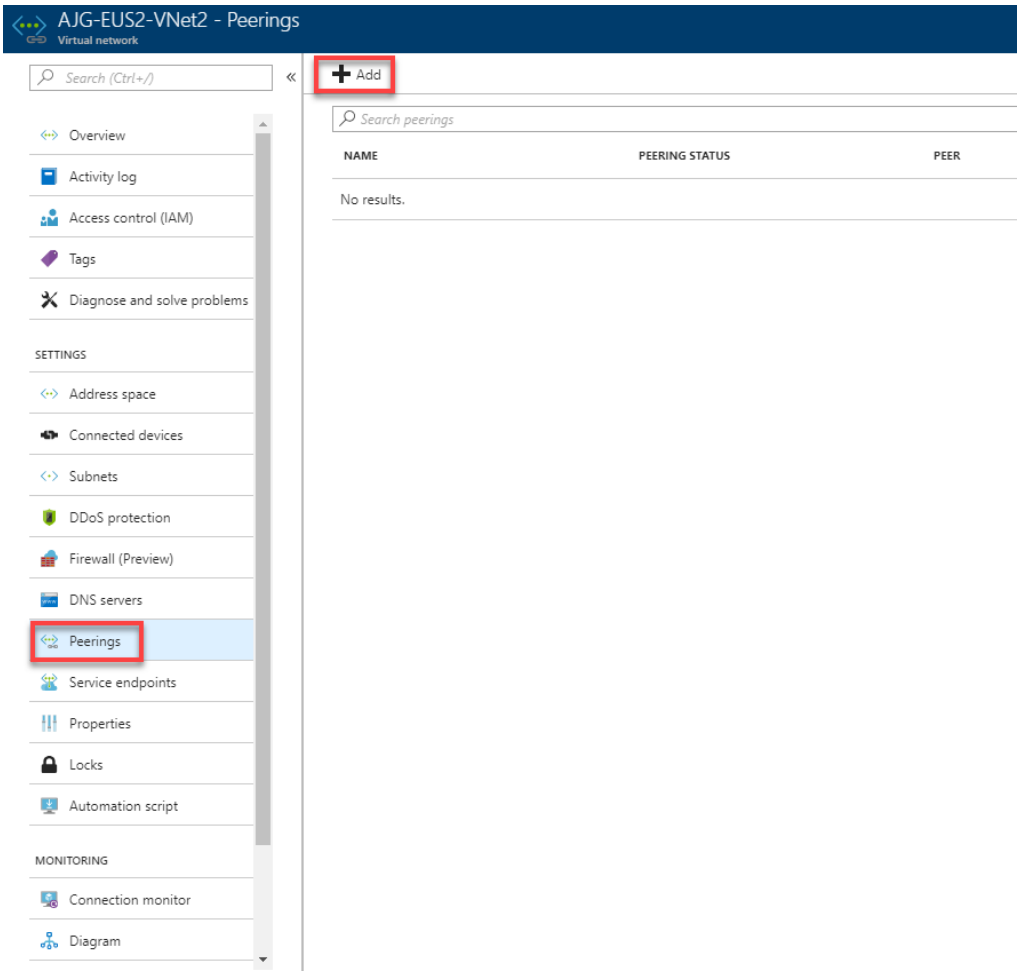
5. On the Add peering blade, enter the following information:
    a. Name: **AJG-EUS-REG-VNETPEER**
    b. **Use Resource Manager**
    c. **Select subscription**
    d. Select **AJG-EUS2-VNet2**
    e. **Leave Allow virtual network access at Enabled**
    f. Place a **check mark** next to **Allow forwarded traffic**
    g. Click OK



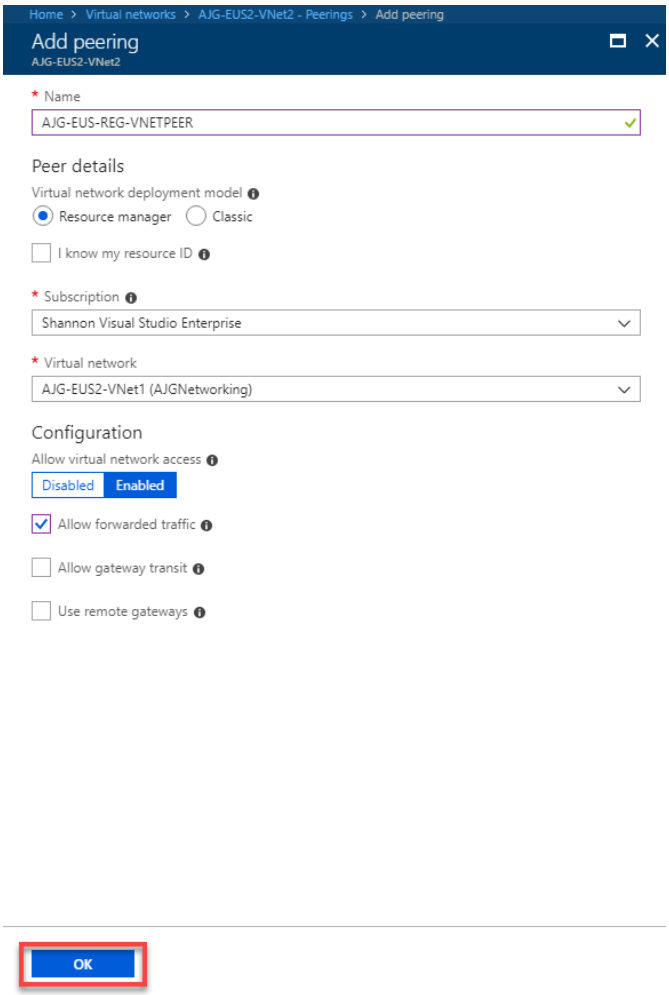
6. Move onto the next step when you see a status of **Initiated** when viewing the Peerings.



7. Go into AJG-EUS2-VNet2 and click on Peerings. On the next screen, click **+Add**.

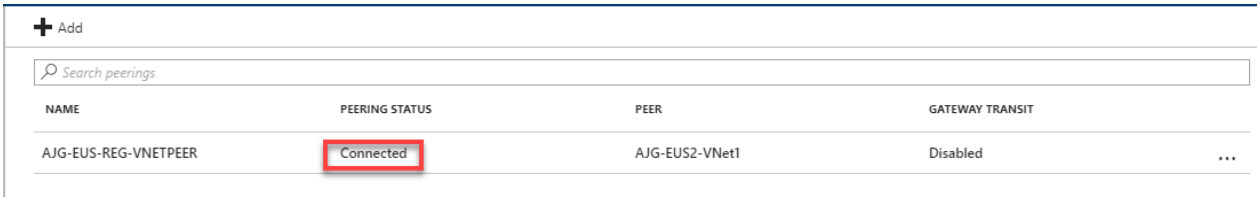


8. For the Add peering blade, enter the following information:
    a. Name: **AJG-EUS-REG-VNETPEER**
    b. Use **Resource Manager**
    c. **Select subscription**
    d. Select **AJG-EUS-VNet1**
    e. Leave Allow virtual network access at Enabled
    f. Place a check mark next to Allow forwarded traffic
    g. Click **OK**
    h. Ignore the warning about 'use remote gateways.'



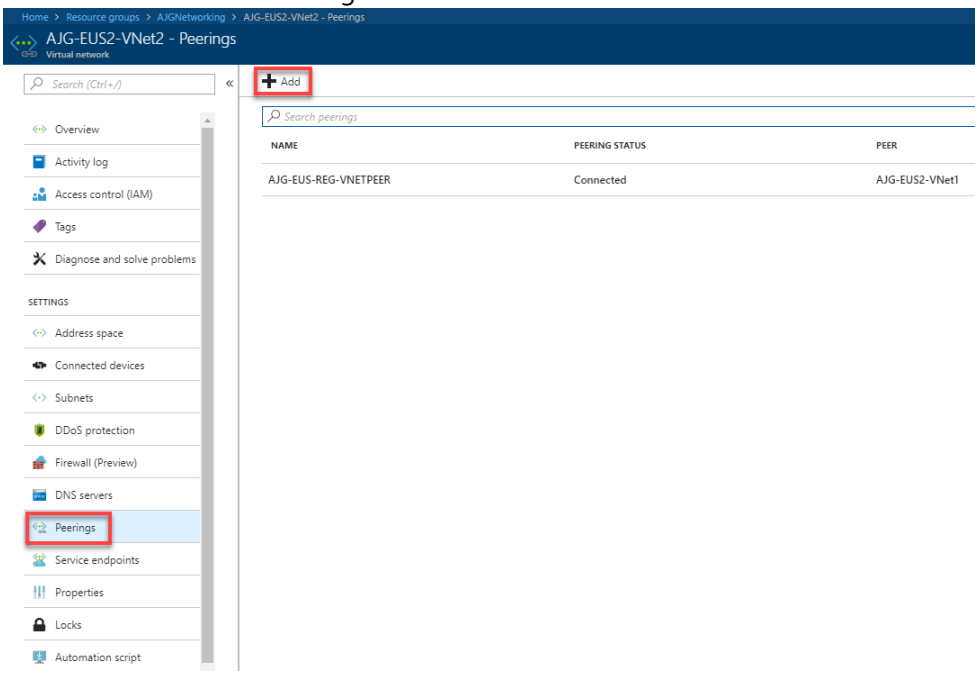
9. Both Peerings will now show **Connected**.
    a. AJG-EUS2-VNet1 to AJG-EUS2-VNet2:

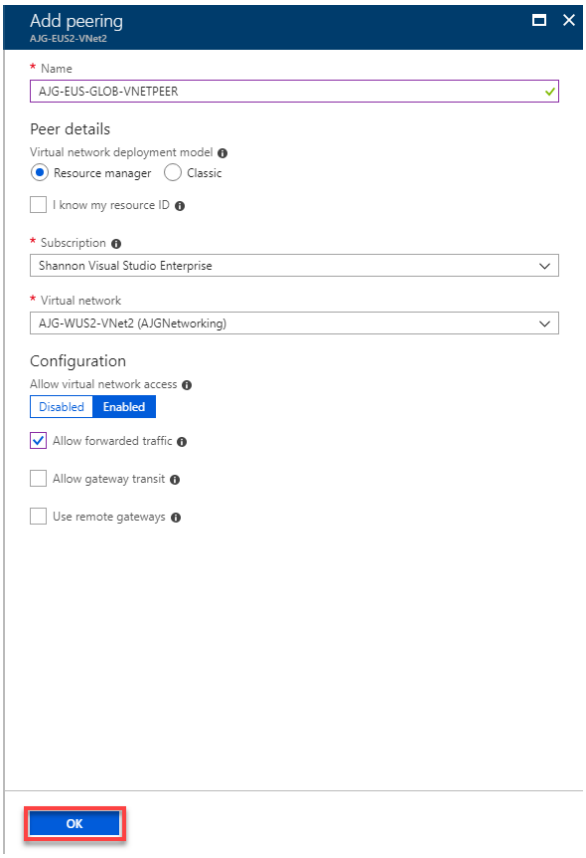
    b. AJG-EUS-VNet2 to AJG-EUS-VNet1:

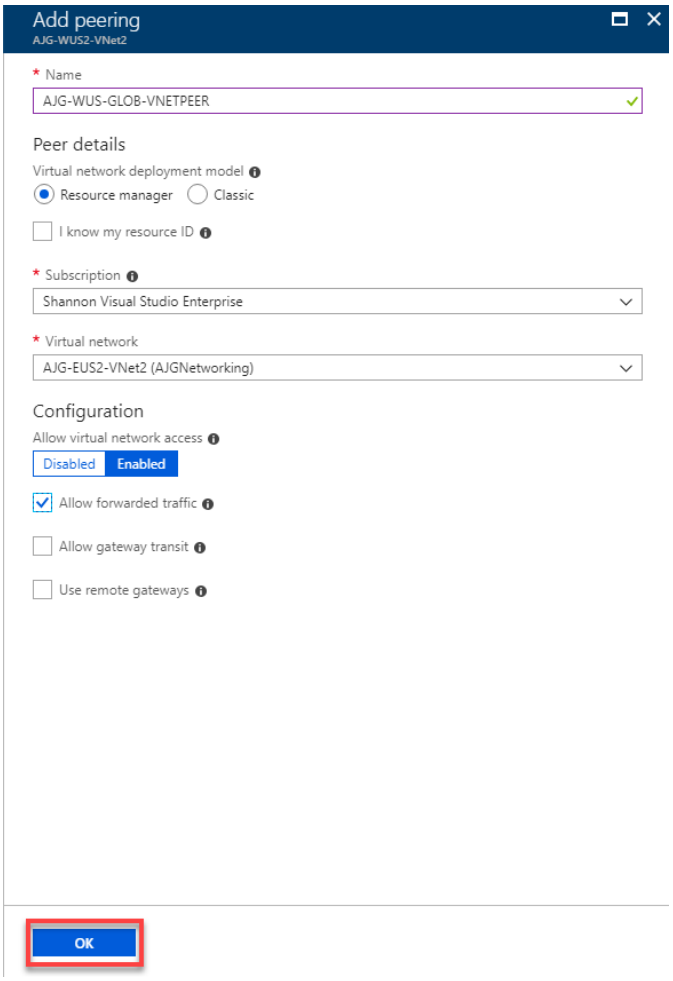


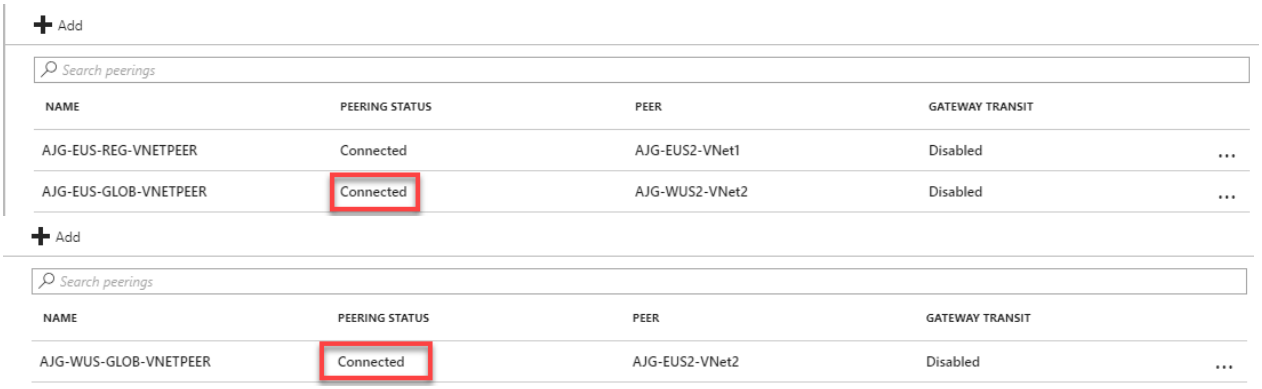
Task 3: Create Global VNet Peer Between AJGVNet4 and AJGVNet2

1. This task will follow similarly to the previous task.
2. Here are the details to enter as you walk through setting up the global VNet peer:
    a. Name: **AJG-EUS-GLOB-VNETPEER**
    b. U**se Resource Manager**
    c. **Select Subscription**
    d. Select **AJG-EUS2-VNet2** (1st configuration) Select **AJG-WUS2-VNet2** (2nd configuration)
    e. Place a checkmark next to **Allow forwarded traffic**
3. Please reference the following screen shots.






Add peering
AJG-WUS2-VNet2
* Name
AJG-WUS-GLOB-VNETPEER
Peer details
Virtual network deployment model
Resource manager
Classic
I know my resource ID
* Subscription
Shannon Visual Studio Enterprise
* Virtual network
AJG-EUS2-VNet2 (AJGNetworking)
Configuration
Allow virtual network access
Disabled
Enabled
Allow forwarded traffic
Allow gateway transit
Use remote gateways
OK

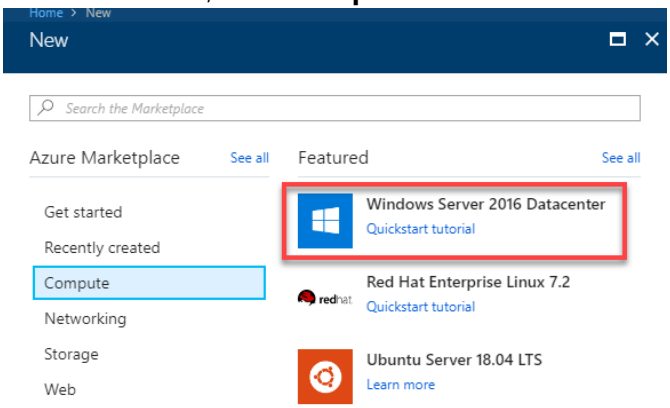

Add
Search peerings
NAME
PEERING STATUS
PEER
GATEWAY TRANSIT
AJG-EUS-REG-VNETPEER
Connected
AJG-EUS2-VNet1
Disabled
AJG-EUS-GLOB-VNETPEER
Connected
AJG-WUS2-VNet2
Disabled
Add
Search peerings
NAME
PEERING STATUS
PEER
GATEWAY TRANSIT
AJG-WUS-GLOB-VNETPEER
Connected
AJG-EUS2-VNet2
Disabled

Exercise 3: Create VMs to Test Connectivity

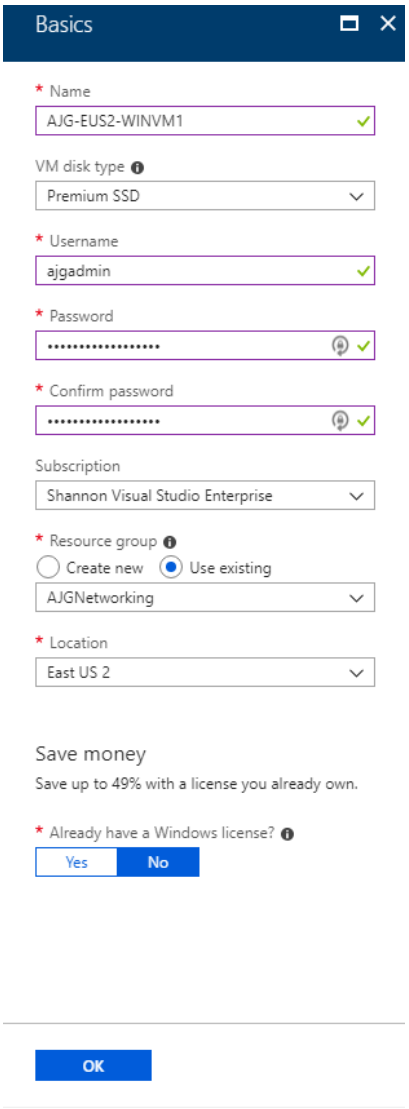
Task 1: Create Windows VM in AJG-EUS2-VNet1, AJG-EUS2-VNet2, AJG-WUS2-VNet1, and AJG-WUS2-VNet2

1. In the left pane, click **+ Create Resource**.

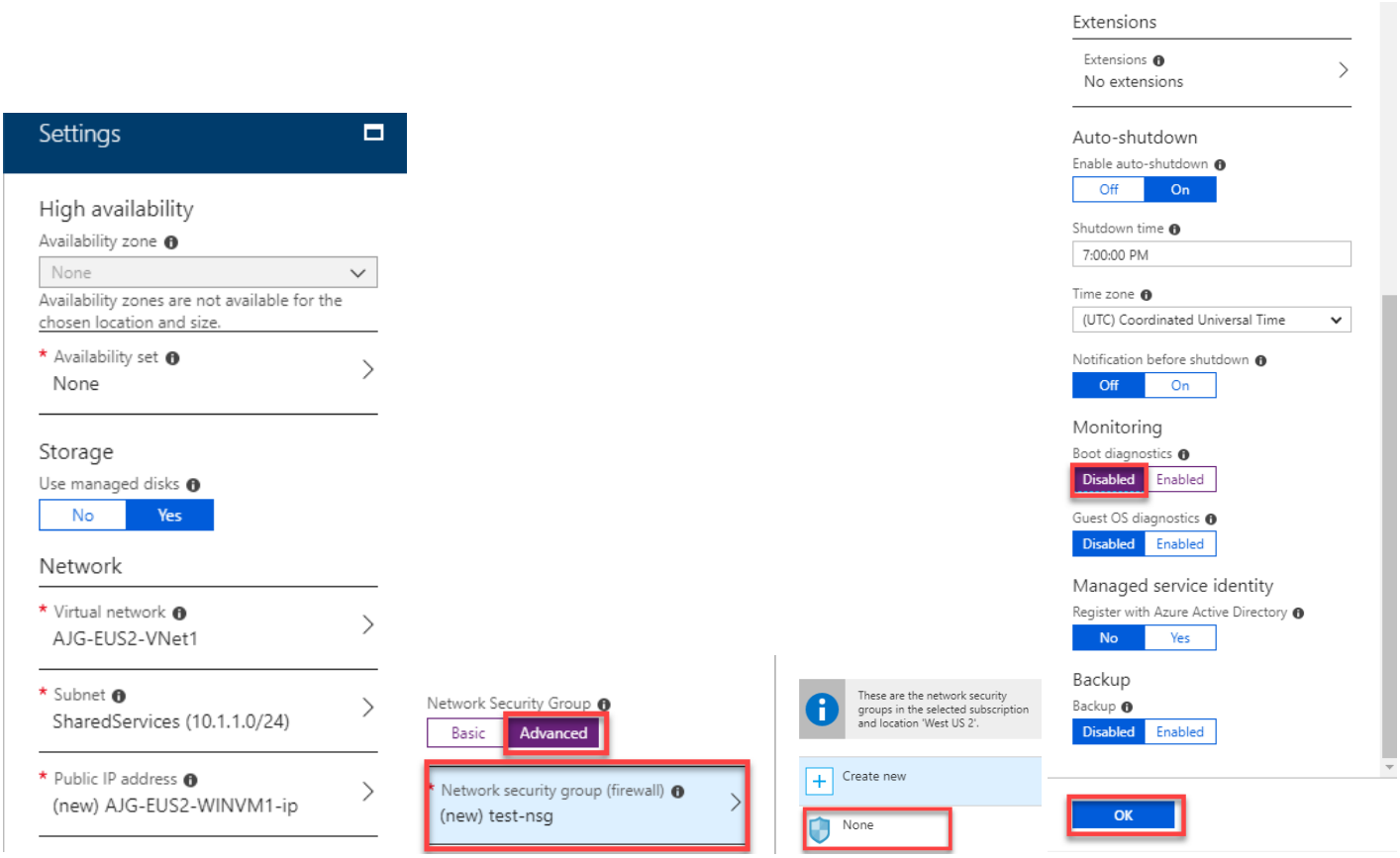
2. In the **New** blade, select **Compute >** Windows Server



3. For the Basics blade, enter the following:
   a. Name: AJG-EUS2-WINVM1
   b. Leave VM type on Premium SSD
   c. Username: ajgadmin
   d. Password: pick a complex password and input that twice
   e. Select your subscription
   f. Use the existing Resource Group
   g. Location: East US
4. Select D2_V2 (or something comparable size wise)



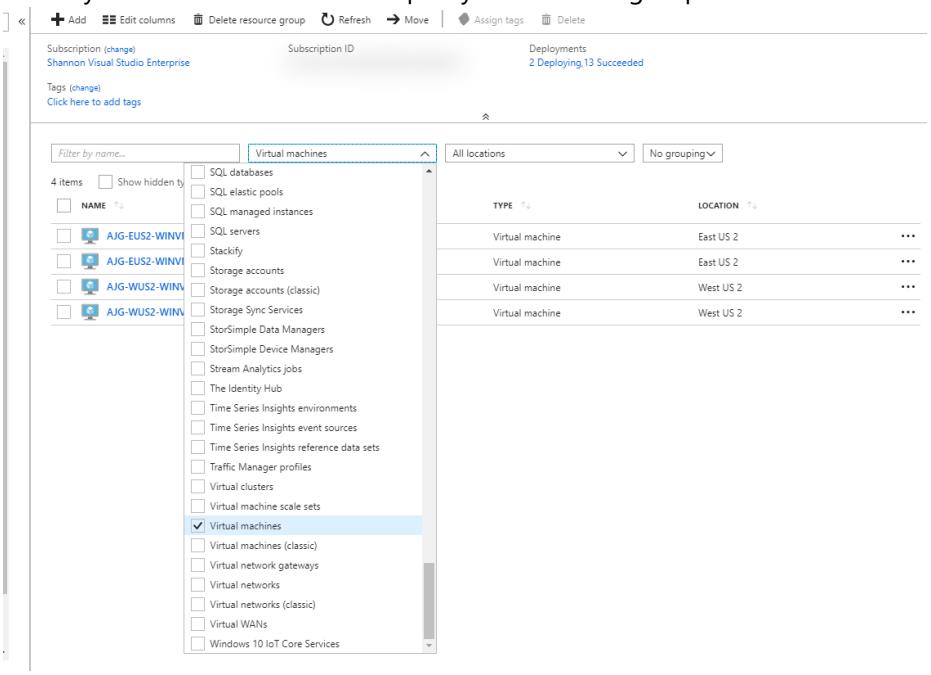
5. For the Settings blade, use the following:
    a. Leave Availability Set as 'None'
    b. Use Managed Disks
    c. Place VM in AJG-EUS2-VNet1
    d. Use the SharedServices Subnet
    e. Assign a Public IP address (leave default or change name)
    f. Click on Advanced for Network Security Group and then click on the public IP. In the new blade, select None to ensure you don't have any Network Security Groups created.
    g. Do not add extensions
    h. Turn Auto-Shutdown off
    i. Disable Boot Diagnostics
    j. Do not register a managed service identity
    k. Leave Backup as Disabled
    l. Click OK to create
    m. Once validation passes, click Create



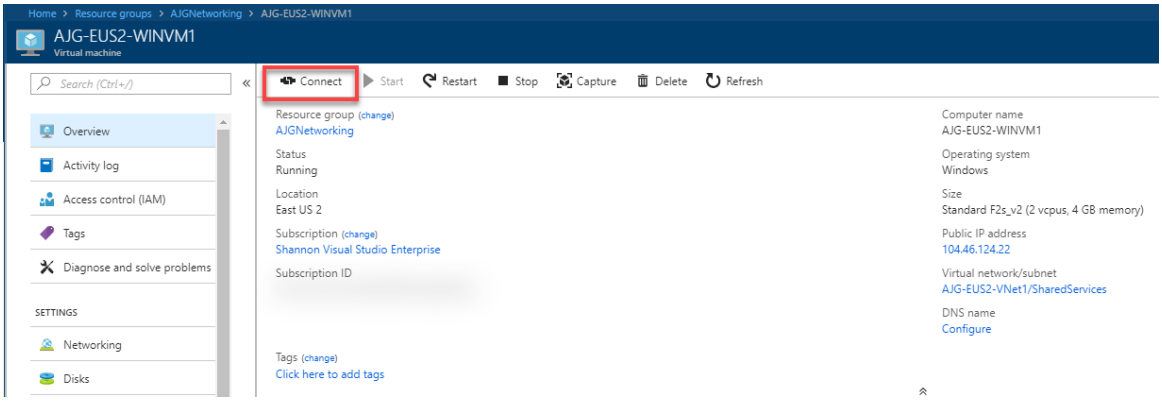
6. Follow the same steps above and create 3 more virtual machines, 1 in AJG-EUS2-VNet2, 1 in AJG-WUS2-VNet1, and 1 in AJG-WUS2-VNet2

Task 2: Log into VMs and Test Connectivity

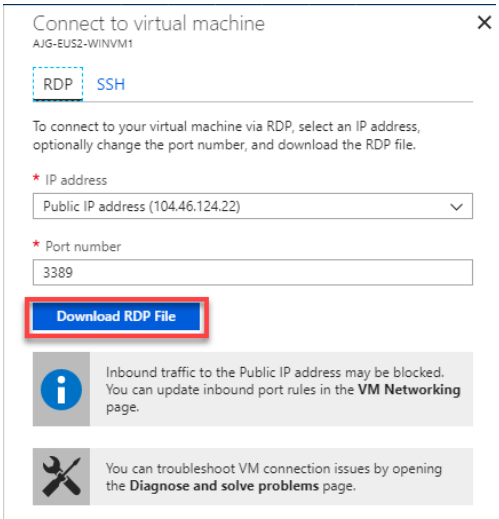
1. Go into the AJGNetworking Resource Group. By now, you will have several resources deployed to 1 Resource Group. This is by design, as after all tutorials are finished, you will easily be able to delete everything in that resource group with a simple delete Resource Group command issued from the portal.
2. Filter by Virtual Machines at the top of your resource group:



3. Click on AJG-EUS2-WINVM1. Within the Overview blade, click Connect at the top.



4. Click on Download RDP File and then double click on the Remote Desktop file that saves to your machine.



5. Once inside the computer, open up Windows PowerShell and issue out the following command:
```
New-NetFirewallRule –DisplayName “Allow ICMPv4-In” –Protocol ICMPv4
```

6. Go back to the portal and complete the same steps above for AJG-EUS2-WINVM2, AJG-WUS2-WINVM1, and AJG-WUS2-WINVM2.
7. From each PowerShell prompt, try pinging the internal IP address for the VMs you just created. Remember to ping over the S2S VPN and by each VNet Peer (regional and global). ICMP is turned off by default with Azure VMs, so creating the firewall rule above allows ICMP traffic.
8. At the end of this lab, go into AJGNetworking and delete the resource group by clicking Delete resource group at the top and entering the name of the resource group: