SEMANA

PROFISSÃO CLOUD

Enterprise Class Networking

Material Didático **versão 1.5**

ZECA NUNES

Sumário

Sobre o Autor

Zeca Nunes é Profissional de TI, Arquiteto de Nuvem e instrutor oficial Microsoft.

Ministra treinamentos de Cloud Computing para grandes corporações: Itaú, Bradesco, Porto Seguro, Casas Bahia, Petrobras e muito outros.

Conecte-se ao meu Linkedin

Esse material é frequentemente alterado para você ficar sempre atualizado! Você tem em mãos a **versão 1.5** dessa Apostila, sempre que passar por aqui verifique se está com a versão mais nova clicando AQUI nesse link. Qualquer dúvida ou sugestão, me envie um email para suporte@zecanunes.com

#1 Bem vindo a Semana Profissão Cloud

Esse é seu material de apoio para participar durante o Workshop de Cloud Computing, então aperte os cintos e vamos começar.

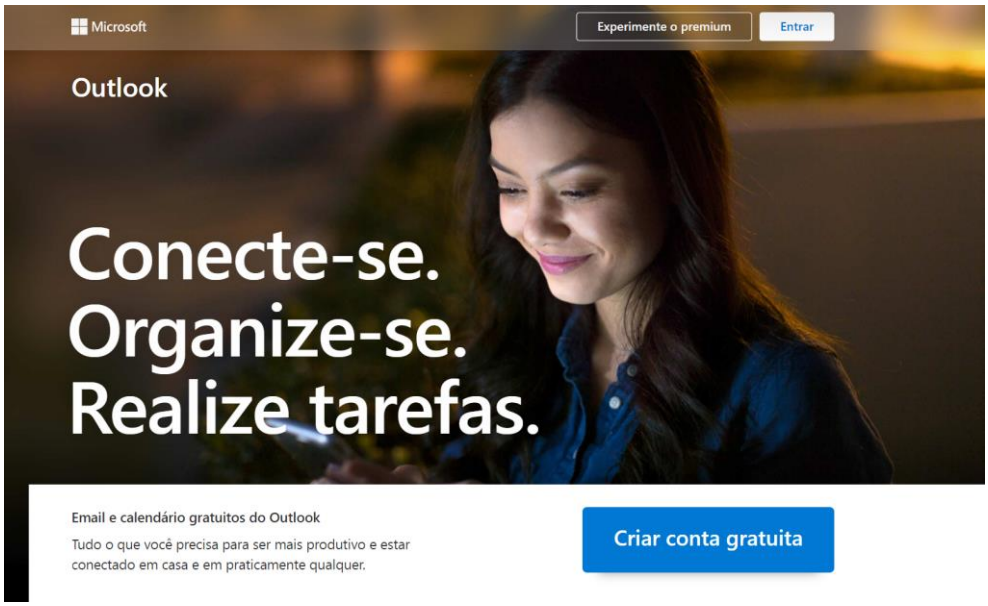
A programação das LIVE está apresentada da seguinte maneira:

- #1 – 22/03 – 20hs – Aquecimento: https://youtu.be/A1DCLjvYC4o
- #2 – 23/03 – 20hs – Cenário Inicial: https://youtu.be/Y3_X5yrdVNc
- #3 – 24/03 – 20hs – Mão na Massa: https://youtu.be/U80ICZMQ2Ec
- #4 – 25/03 – 20hs – Mão na Massa: https://youtu.be/i9LRCqnlejE
- #5 – 26/03 – 20hs – Apresentação da Solução: https://youtu.be/wn2eLZvF_nM

Criação da conta Outlook.com

O primeito passo é você criar um email exclusivo para esse evento, não use o seu email pessoal agora, faço questão de reforçar para você criar um email novo que vai usar somente aqui nessa semana e depois pode apagar ou esquecer ele que, pois não vai mais usar.

Acesse o seu navegador **em modo oculto (in-private)** digitando Outlook.com.



Aperte em “Criar conta gratuita” e você deverá seguir os passos para criar um usuário/senha de estudos exemplo “zecaprofissaocloud@outlook.com” para começar.

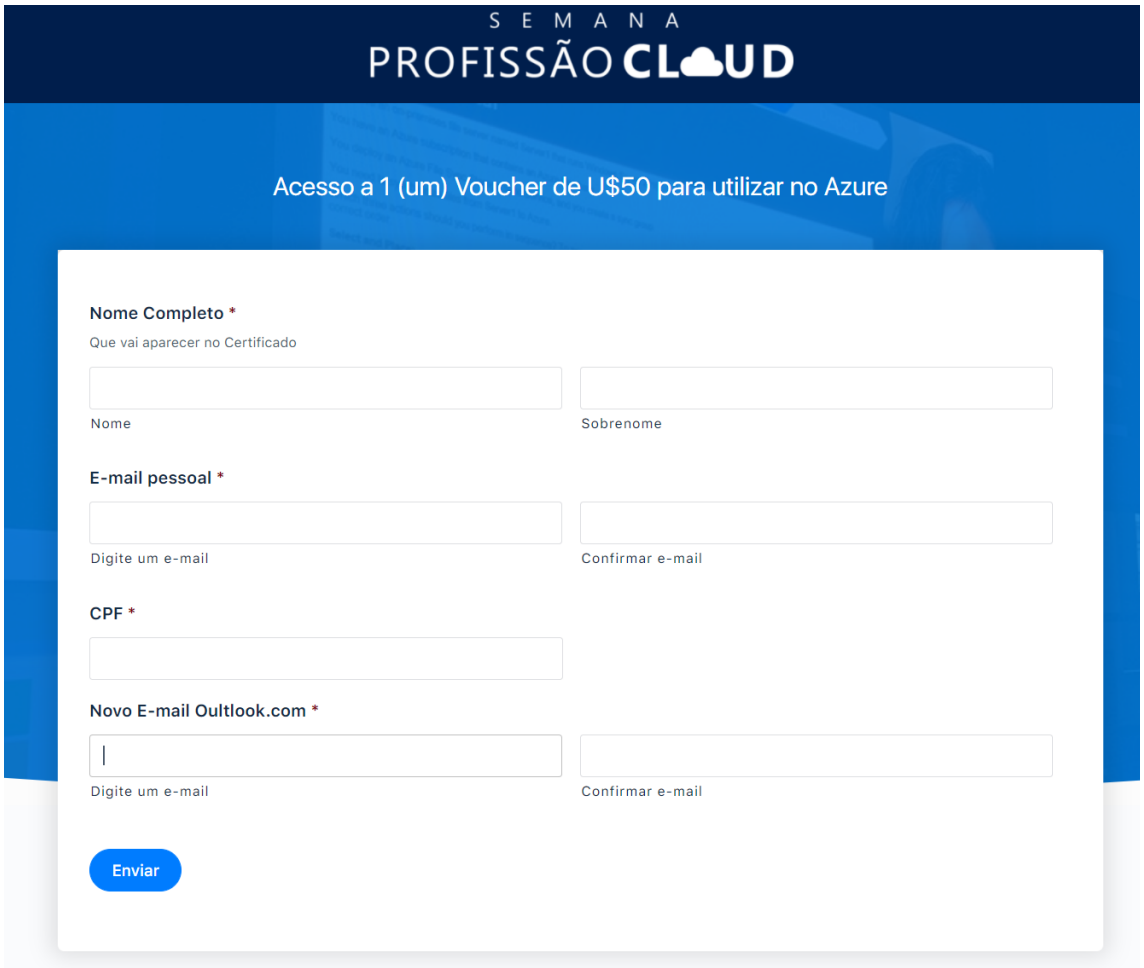
Em seguida, anote no seu caderno ou notepad o endereço e a senha que você criou pois precisará deles durante todas nossas atividades.

Solicitando seus créditos

Agora você precisa acessar o seguinte site para solicitar os seus U$50 para realizar todos os exercícios propostos em nossa semana, você vai ter acesso ao Azure de verdade, então muita atenção nessa parte!

Clique nesse link abaixo e acesse o formulário

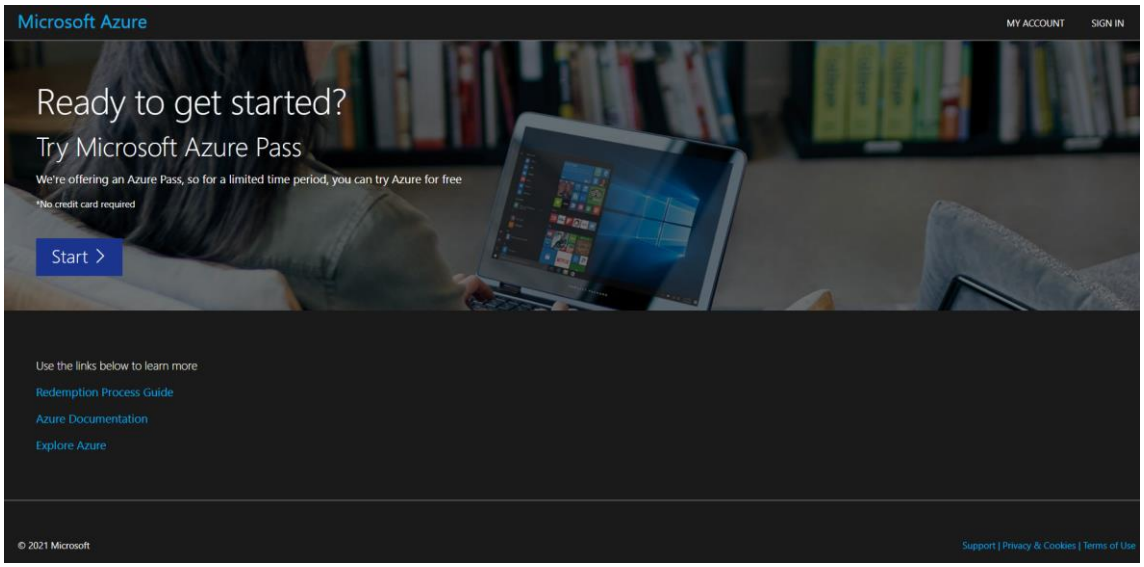
https://cursos.zecanunes.com.br/land/maratona-cloud/voucher-para-laboratorio-workshop



Preencha adequadamente dada um dos campos, conforme orientado na LIVE!

Resgatando o seu crédito

Em seguida, você deverá abrir uma nova **aba anônima** no mesmo navegador anônimo acessar o seguinte site: microsoftazurepass.com



Nessa tela você deve apertar START, em seguida confirmar o endereço de email outlook.com que você acabou de criar em um passo anterior, se tiver de digitar, faça com cuidado para não errar nenhum caractere.

Siga os próximos passos de acordo com a orientação na LIVE #1

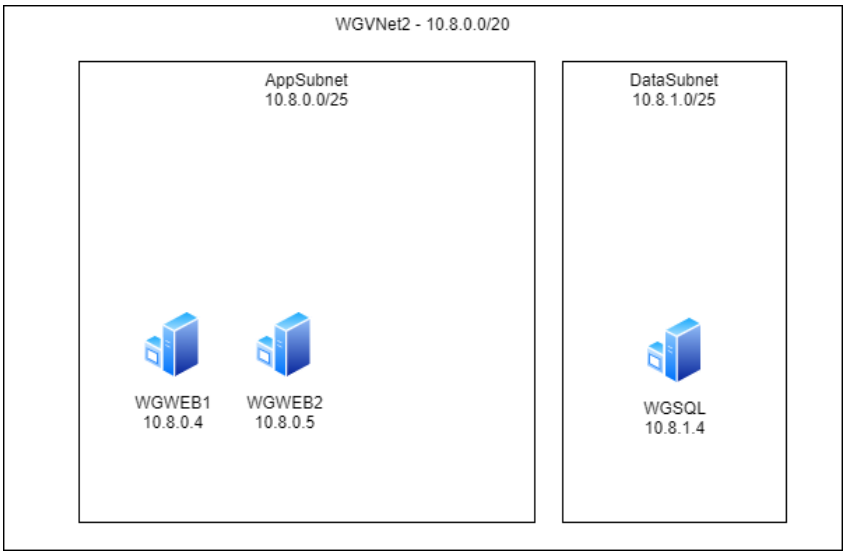
#2 Preparando o Workshop

Antes de começar a etapa mais esperada de mão na massa, nõs vamos criar um ambiente inicial utilizando uma técnica muito interessante em Cloud Computing, que é o template. Toda implementação de maquinas, redes e outros serviços pode ser previamente planejada e um modelo pode ser criado para levantar esse ambiente sempre que precisar.

Vamos aqui utilizar o seguinte arquivo de template, por favor faça o download dele na sua maquina local para utilizar no exercício.

Clique AQUI com o Botão Direito para Salvar o arquivo template no C:\Temp, por exemplo.

O Diagrama abaixo mostra o trabalho que vamos fazer nesse exercício inicial:



Exercise 0: Create a Virtual Network and provision subnets

Duration: 15 minutes

Task 1: Create a Virtual Network with Subnets

1. From your **computer**, connect to the portal.azure.com, select **+ Create a resource**, and search for **Virtual Network**, select **Create**.
2. On the **Create virtual network** blade, enter the following information:

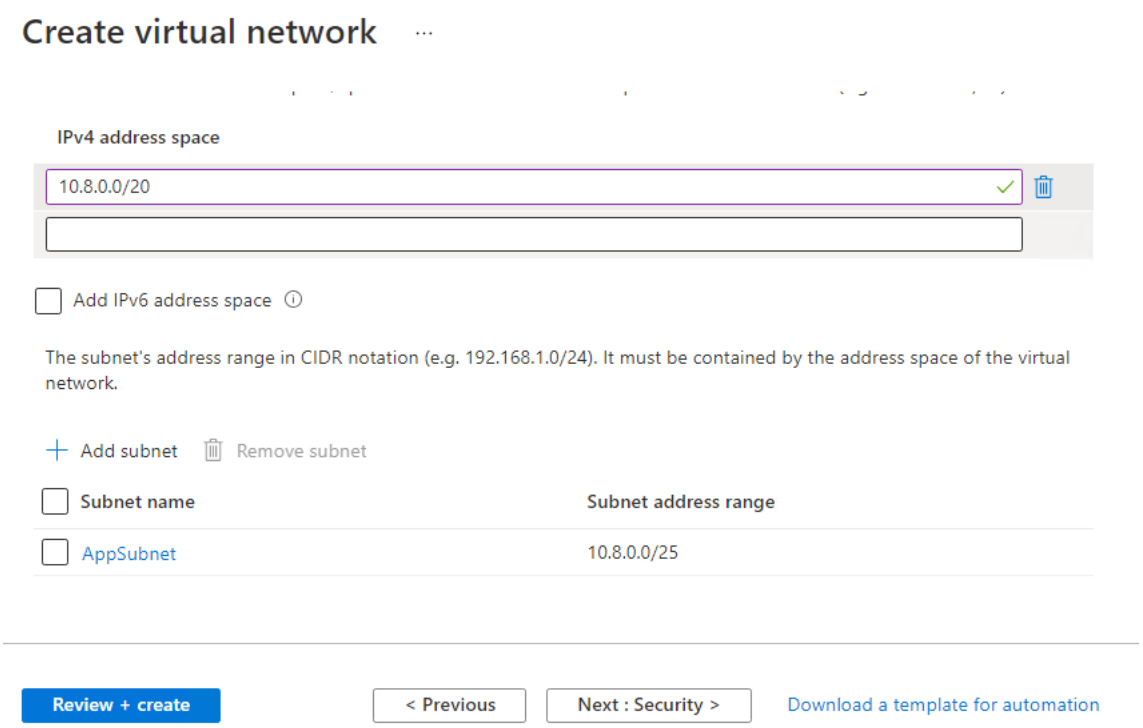
   - Subscription: **Select your subscription**.
   - Resource group: Select **Create new**, and enter the name **WGVNetRG2**

- Name: **WGVNet2**
- Location: **(US) South Central US**

Click “Next : IP Address >” button

- IPv4 address space: edit to **10.8.0.0/20**
- Click “+ Add subnet”
- Subnet name: **AppSubnet**
- IPv4 address space: **10.8.0.0/25**
- Click **“Add”**

3. Leave the other options as default for now.
4. Upon completion, it should look like the following screenshot. Validate the information is correct, and select **Review + create**.

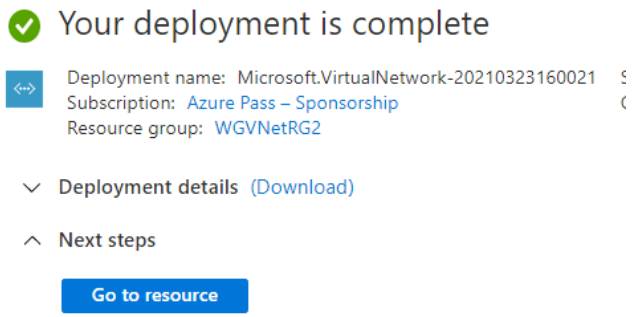


The create virtual network dialog is displayed. The configuration options specified in the previous step are showed.

>> Review + Create

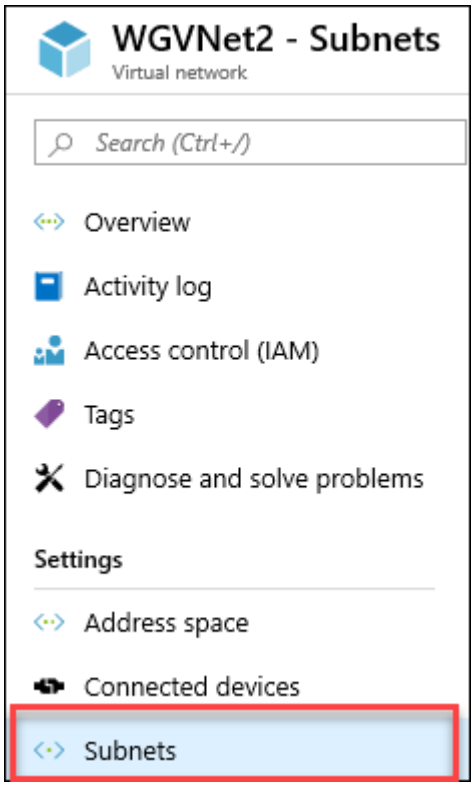
>> Create

5. Monitor the deployment status by selecting **Notifications Bell** at the top of the portal. In a minute or so, you should see a confirmation of the successful deployment. Select **Go to Resource**.



Task 2: Configure subnets

1. Go to the WGVNetRG1 Group, and select **WGVNet2 Virtual Network** blade if you're not there already, and select **Subnets** under **Settings** on the left.



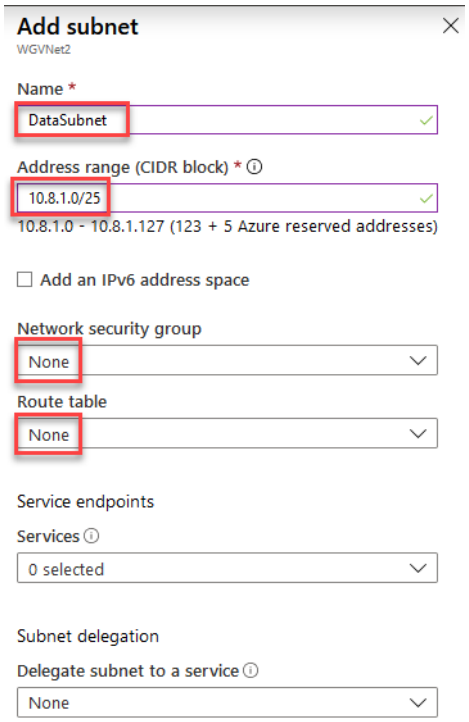
In the Virtual Network blade, under Settings, Subnets is selected.

2. In the **Subnets** blade select **+Subnet**.

In the Subnets blade, the add Subnet button is selected.

3. On the **Add subnet** blade, enter the following information:
   - Name: **DataSubnet**
   - Address range: **10.8.1.0/25**
   - Network security group: **None**
   - Route table: **None**
   - Service Endpoints: **Leave as Default**.

4. When your dialog looks like the following screenshot, select **OK** to create the subnet.



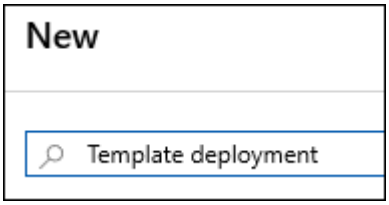
Task 3: Use the Azure portal for a template deployment

Note: If you have not downloaded the student files see this section in the before getting started section of this hands-on lab.

1. On your Computer, open the **C:\temp\CloudShop.json** student file for this lab.

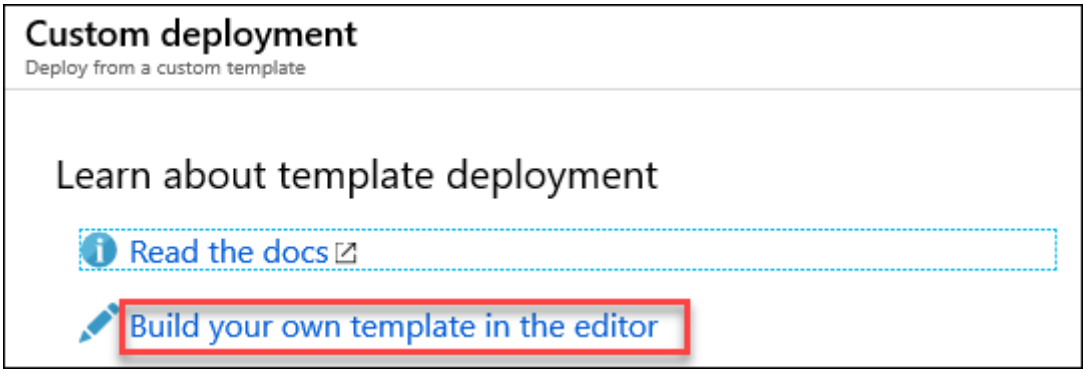
2. Make sure you are signed into home to the Azure portal at http://portal.azure.com.

3. Choose **+ Create a resource**, and search for and select **template deployment**.

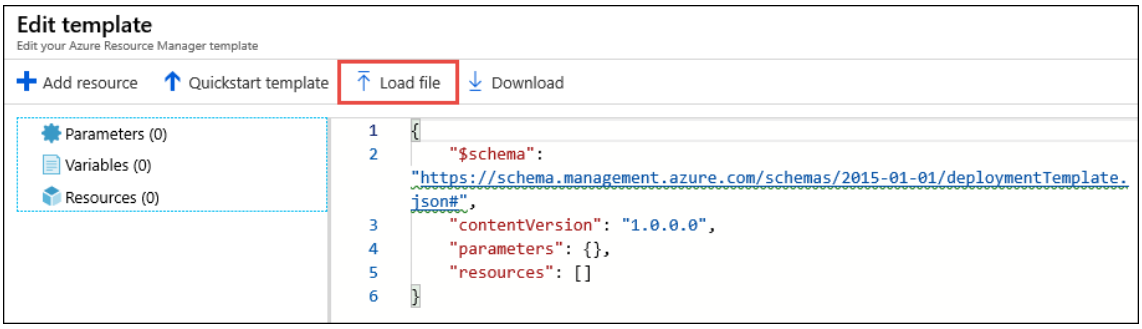


4. On the Template deployment blade, select **Create**.

5. On the Custom deployment blade, select **Build your own template in the editor**.



6. Choose **Load file** and select the **CloudShop.json** file from your **C:\temp** directory and then select **Save**.

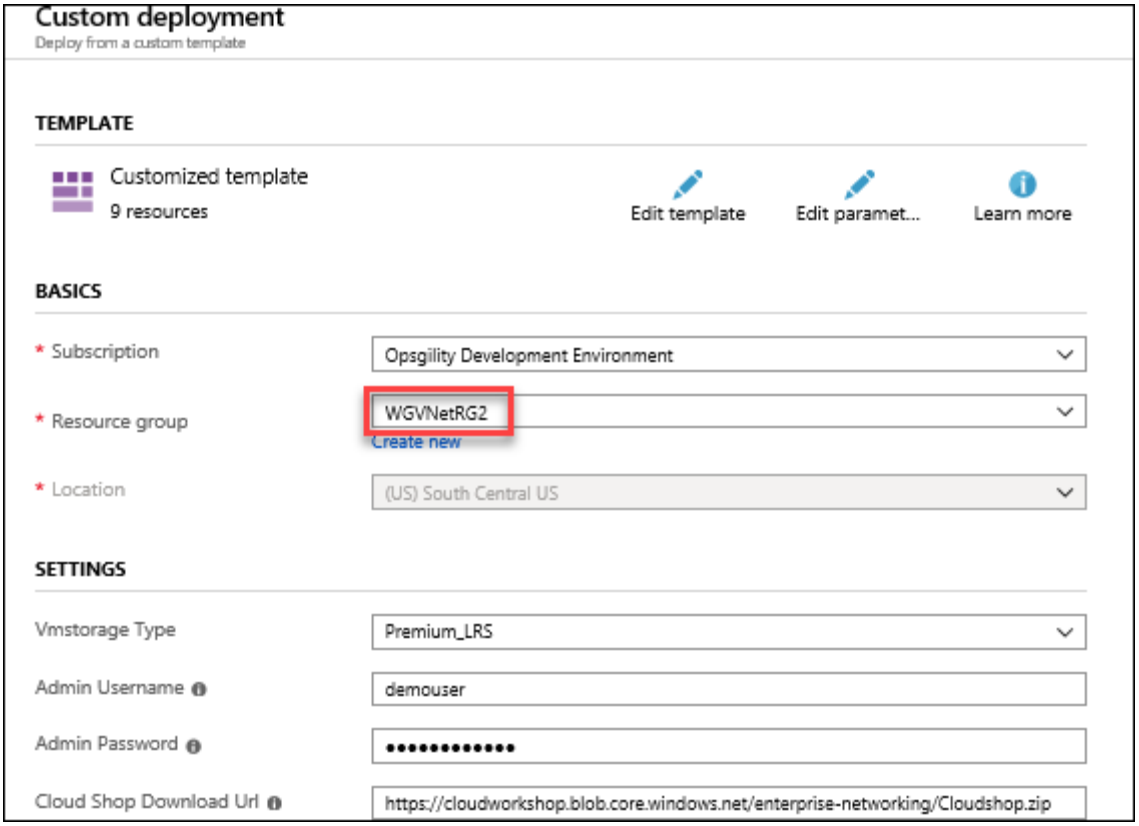


7. Validate the following parameters

   - Resource Group: Select **WGVNetRG2** you created earlier.

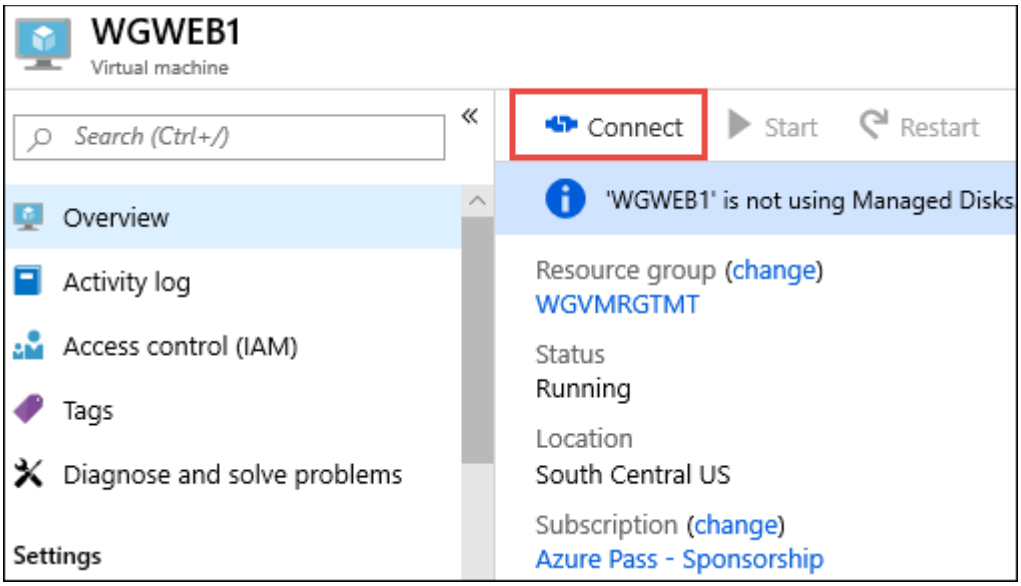
- Location: **(US) South Central US** (The same location you used to provision resources earlier in this lab.)
- Existing Virtual Network Name: **WGVNet2**
- Existing Virtual Network Resource Group: **WGVNetRG2**
- Web Subnet: **AppSubnet**
- Data Subnet: **DataSubnet**

8. Click on **Review + create** and then **Create**. This deployment will take approximately 20-40 minutes.



Task 4: Validate the CloudShop application is up after the deployment

1. Using the Azure home portal, open the **WGVNetRG2** Resource group and review the deployment.
2. Navigate to the **WGWEB1** blade.
3. On the **WGWEB1** blade, first select **Connect**, then select **RDP**, and then choose **Download RDP file** to establish a Remote Desktop session.

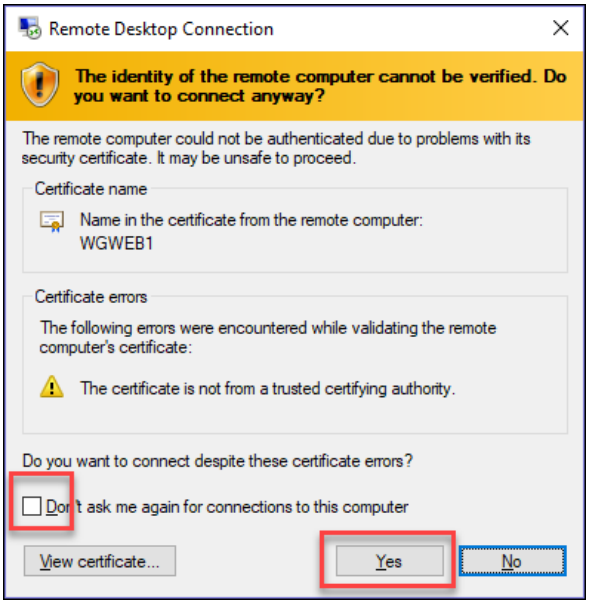


4. Depending on your Remote Desktop protocol client and browser configuration, you will either be prompted to open an RDP file, or you will need to download it and then open it separately to connect.

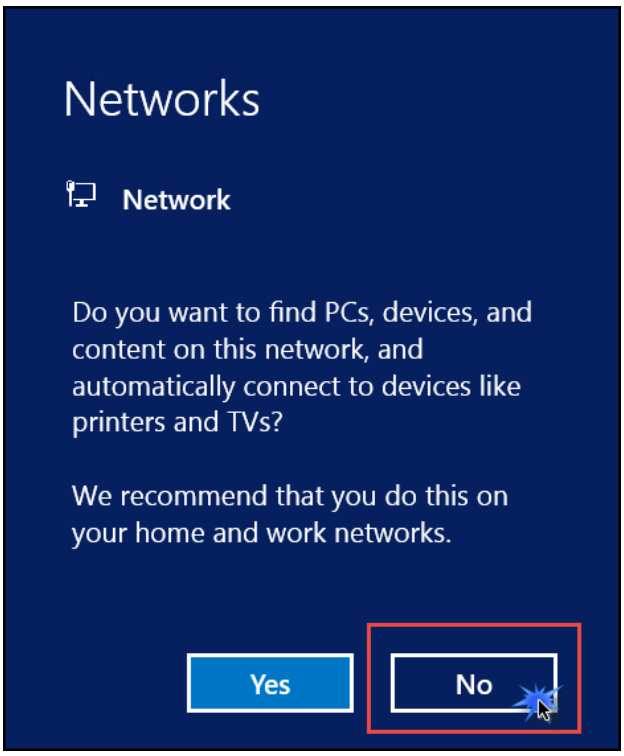
5. Log in with the credentials specified during creation:

   - User: **demouser**
   - Password: **demo@pass123**

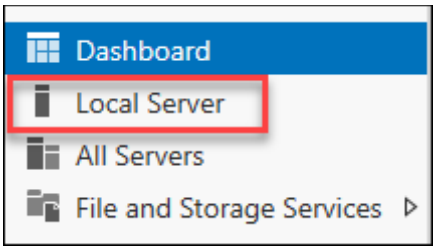
6. You will be presented with a Remote Desktop Connection warning because of a certificate trust issue. Select **Yes** to continue with the connection.



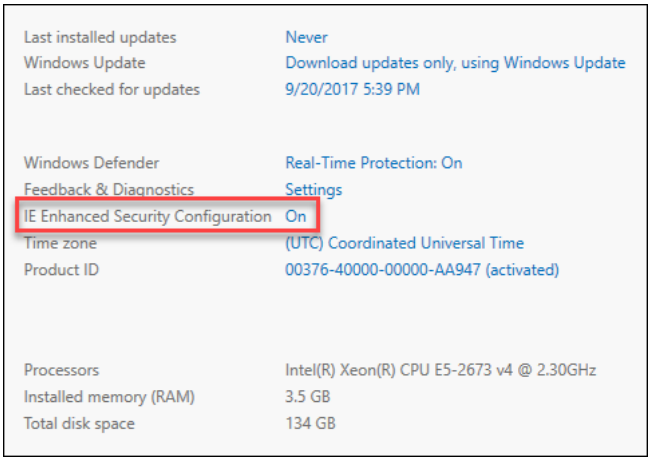
7. When logging on for the first time, you will have a prompt asking about network discovery. Select **No**.



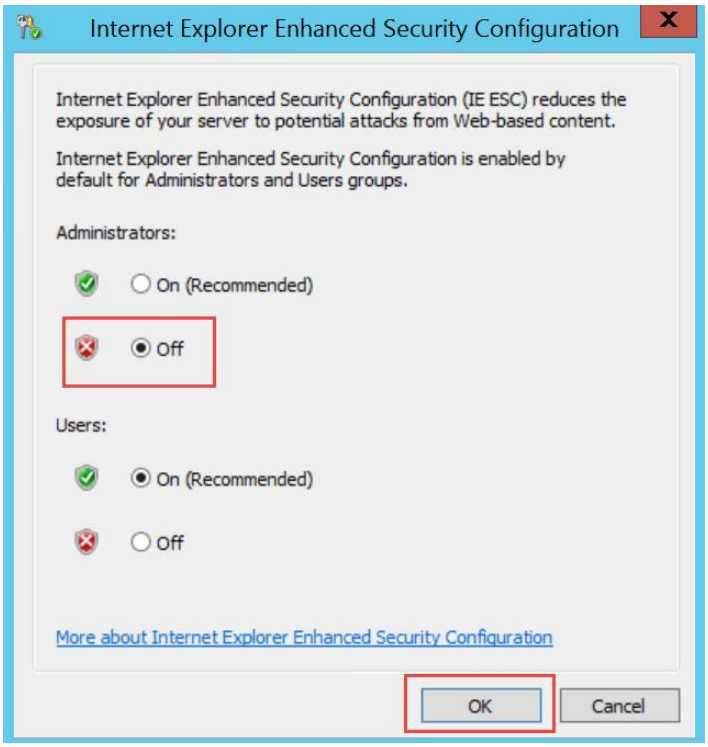
8. Notice that Server Manager opens by default. Choose **Local Server**.



9. In the Local Server pane, ensure the **IE Enhanced Security Configuration** is set to **Off**. If that is not the case, select **On**.



10. If needed, change to **Off** for Administrators, and select **OK**.



11. You will now ensure the CloudShop application is up and running. Open Internet Explorer, and browse to both the WGWEB1 and WGWEB2 servers:

```
http://wgweb1
http://wgweb2
```

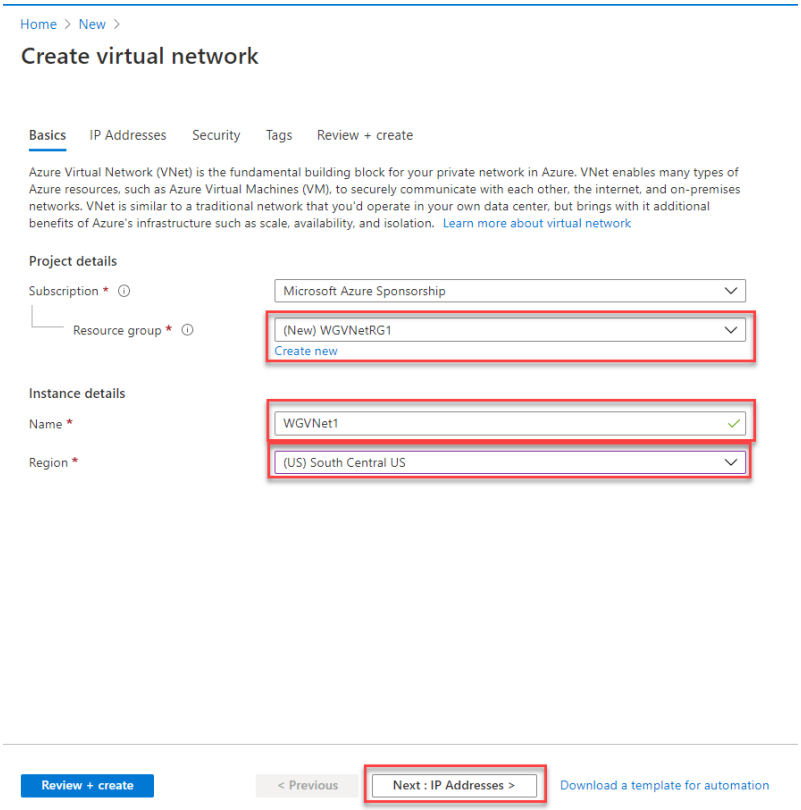
#3 HandsOn Lab (Mão-na-Massa!)

Exercise 1: Create a Virtual Network and provision subnets

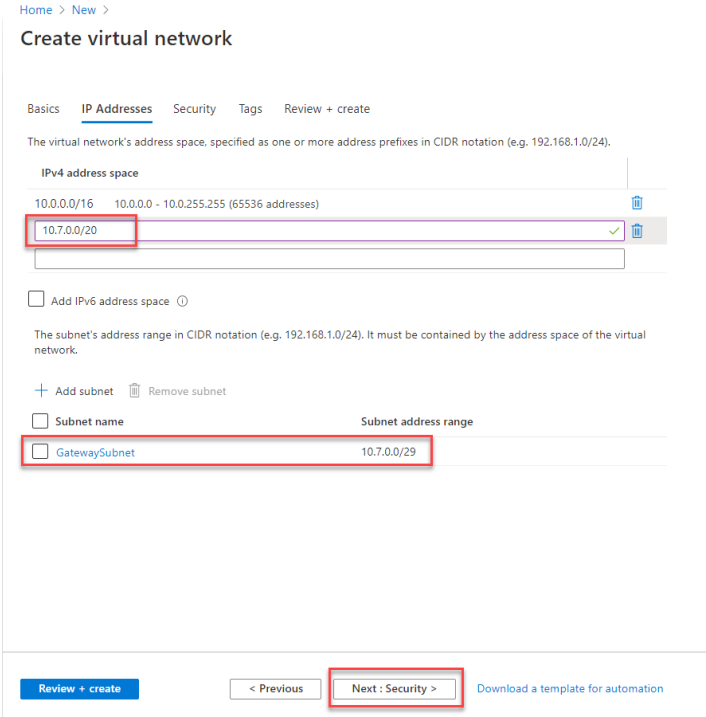
Duration: 15 minutes

Task 1: Create a Virtual Network

1. From your **computer**, connect to the Azure portal, select **+ Create a resource**, and search for **Virtual Network**, and then press **Create**
2. On the **Create virtual network** blade, on the **Basic** tab, enter the following information:
    - Subscription: **Select your subscription**.
    - Resource group: Select **Create new**, and enter the name **WGVNetRG1**.
    - Name: **WGVNet1**
    - Location: **(US) South Central US**
3. Select **Next: IP Addresses**



4. On the **Create virtual network IP Addresses** tab, enter the following information:
    - Address space: **10.7.0.0/20**
    - **+Add subnet**
    - Subnet name: **GatewaySubnet** (Select the **default** name and change to this name.)
    - Subnet address range: **10.7.0.0/29**
    - Select **Add**
5. Select **Next: Security**.

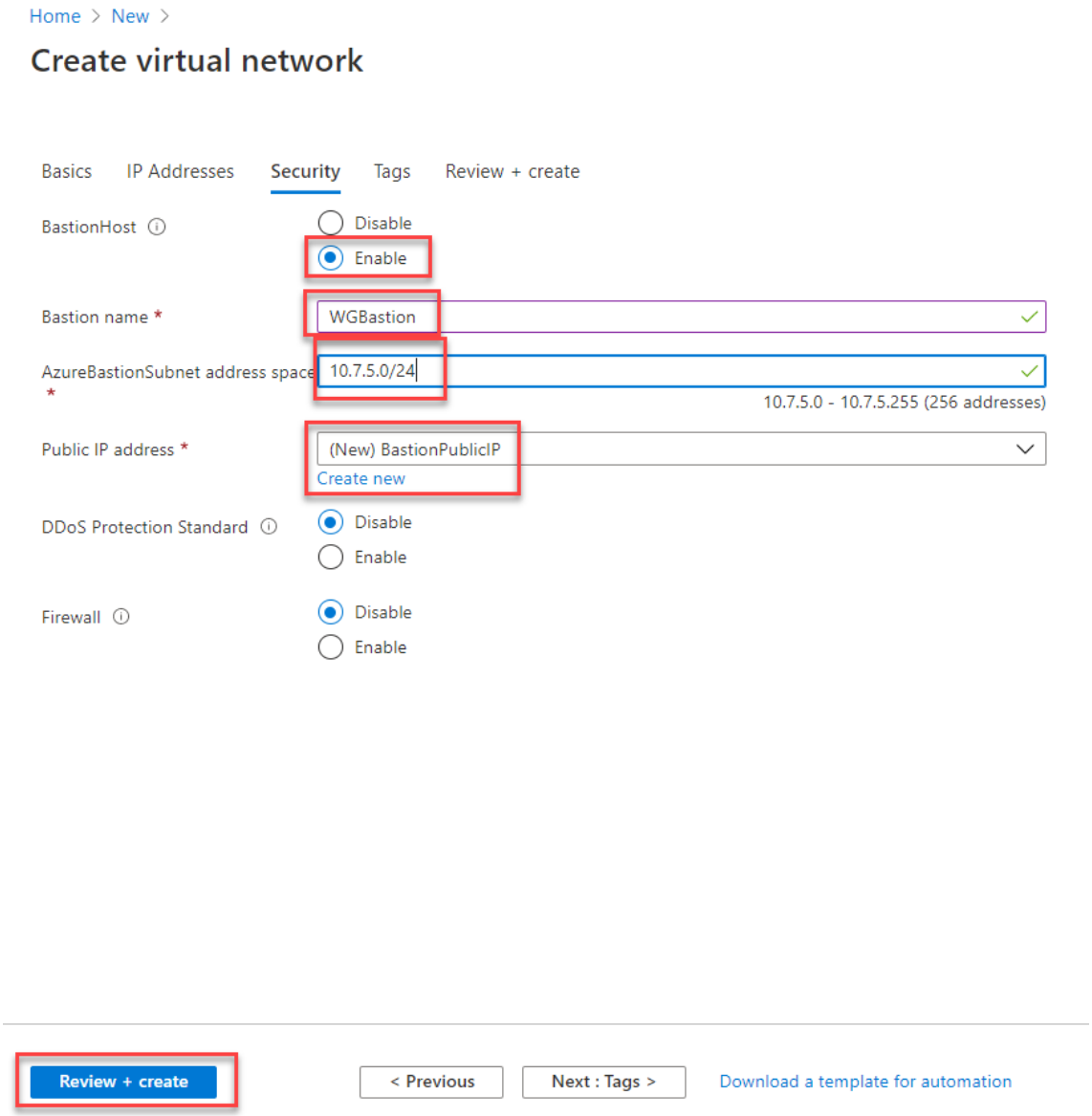


6. On the **Create virtual network Security** tab, select **Enable** for BastionHost.

7. Enter the following information:

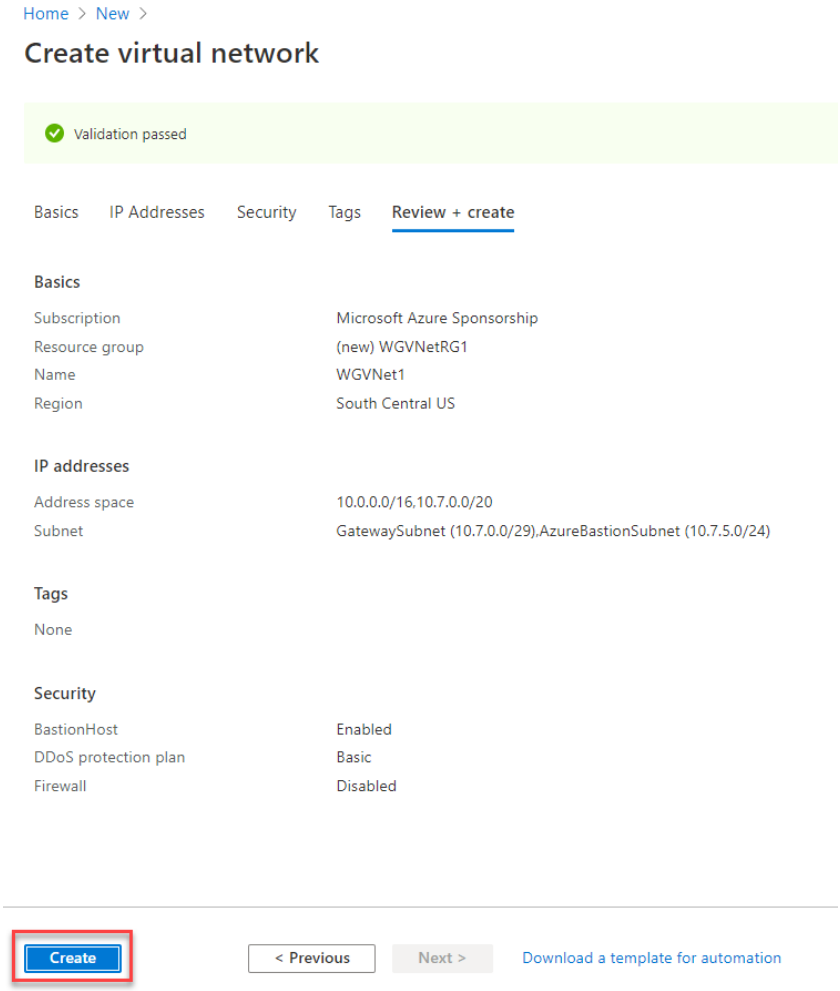
    - Bastion name: **WGBastion**
    - AzureBastionSubnet address space: **10.7.5.0/24**
    - Public IP address: **Create new**
    - Public IP address name: **BastionPublicIP**

8. Leave the other options as default for now.



9. Select **Review + Create**.

10. Review the configuration and select **Create**.

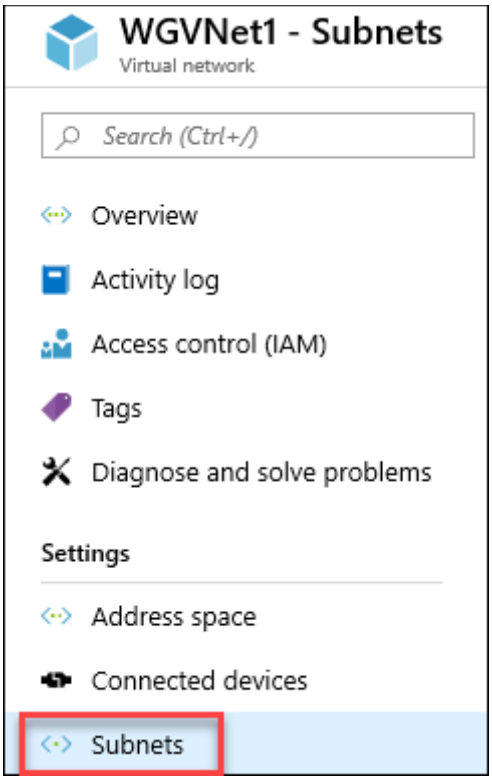


11. Upon completion, it should look like the following screenshot. Validate the information is correct, and select **Create**.

12. Monitor the deployment status by selecting **Notifications Bell** at the top of the portal. In a minute or so, you should see a confirmation of the successful deployment. Select **Go to Resource**.

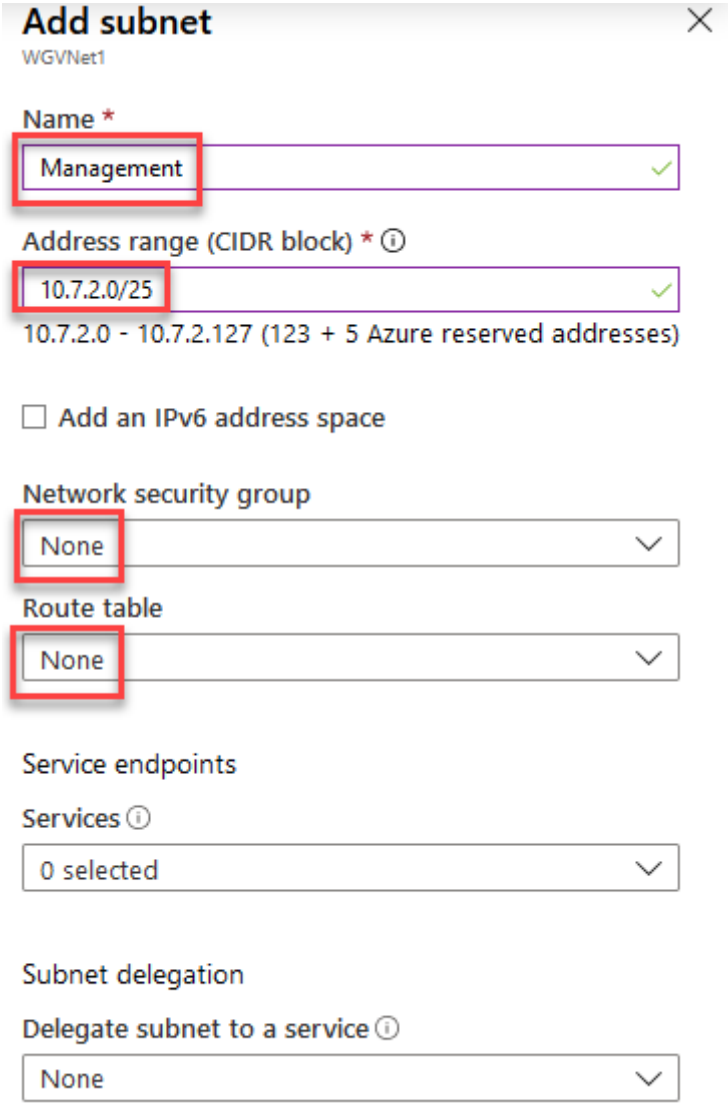
Task 2: Configure subnets

1. Go to the WGVNetRG1 Group, and select **WGVNet1 Virtual Network** blade if you're not there already, and select **Subnets** under **Settings** on the left.

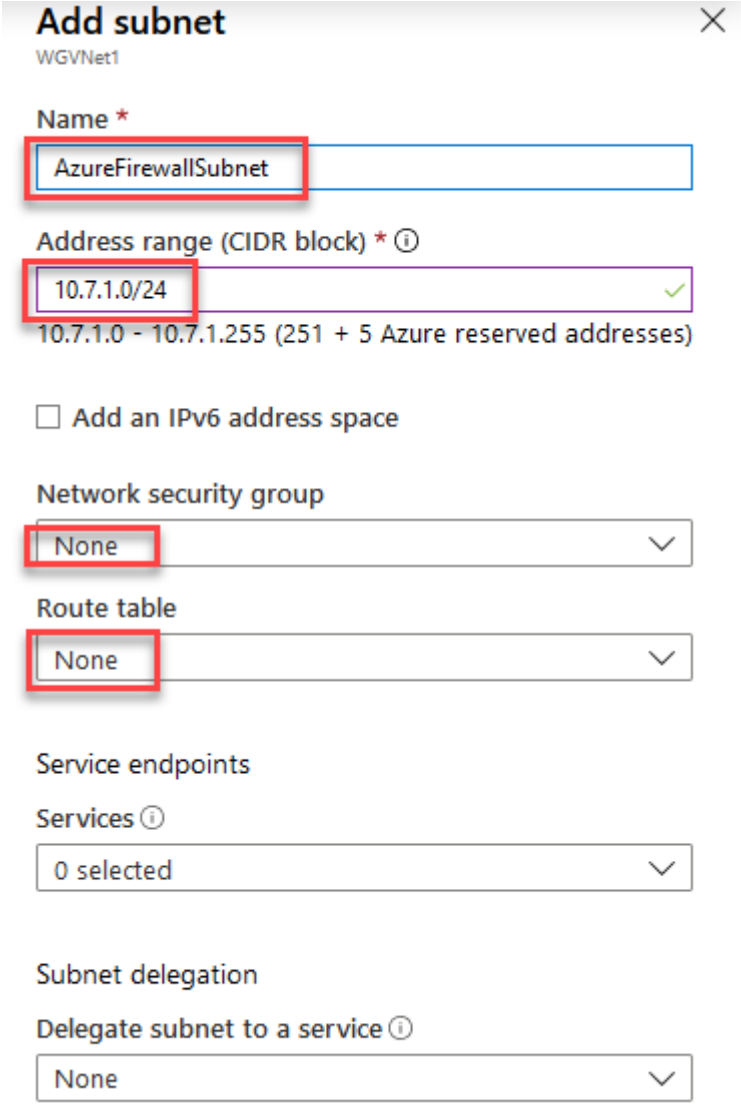


2. In the **Subnets** blade select **+Subnet**.

3. On the **Add subnet** blade, enter the following information:
   - Name: **Management**
   - Address range: **10.7.2.0/25**
   - Network security group: **None**
   - Route table: **None**
   - Service Endpoints: **Leave as Default**.
4. When your dialog looks like the following screenshot, select **OK** to create the subnet.



5. Repeat Step 3, enter the following information for the Azure Firewall which we will use to control traffic flow in and out of the Network.
    - Name: **AzureFirewallSubnet** (This name is fixed and cannot be changed.)
    - Address range: **10.7.1.0/24**
    - Network security group: **None**
    - Route table: **None**
    - Service Endpoints: **Leave as Default**



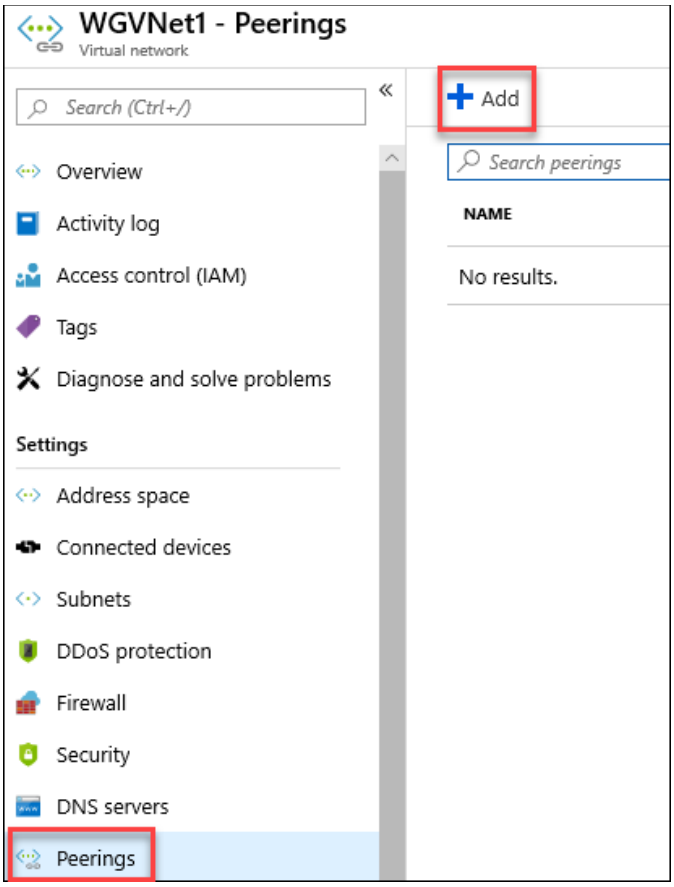
Exercise 2: Virtual Network Peering

Duration: 20 Minutes

Task 1: Configure VNet peering WGVNet1 to WGVNet2 and Vice Versa

1. Select the resource group **WGVNetRG1**, and select the configuration blade for **WGVNet1**. select **Peerings** under **Settings** on the left.

2. Select **Add**.



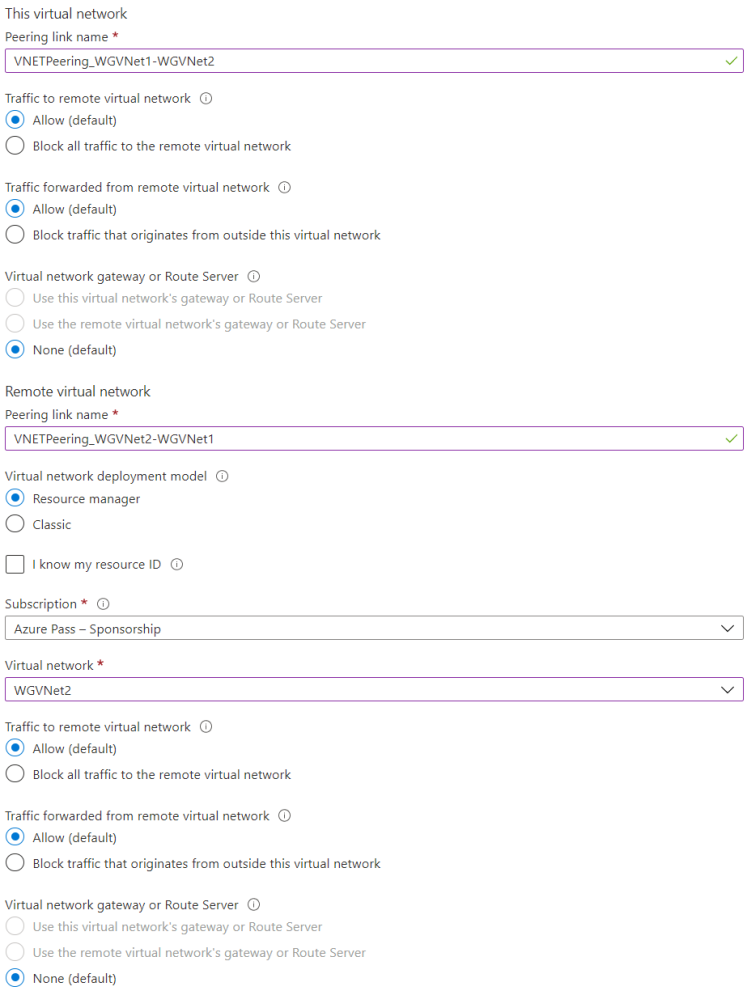
3. Set the following configuration for the new peering. Select **OK** to create the peering.

   This virtial network

   - Peering link name: **VNETPeering_WGVNet1-WGVNet2**
   - Traffic to remote virtual network: **Allow (default)**
   - Traffic forwarded from remote virtual network: **Allow (default)**

   Remote virtual network

   - Peering link name: **VNETPeering_WGVNet2-WGVNet1**
   - Virtual network deployment model: **Resource manager**
   - Subscription: **Select your Azure subscription**
   - Virtual Network: **WGVNet2**
   - Traffic to remote virtual network: **Allow (default)**
   - Traffic forwarded from remote virtual network: **Allow (default)**



Click **ADD**

Exercise 3: Configure Network Security Groups and Application Security Groups

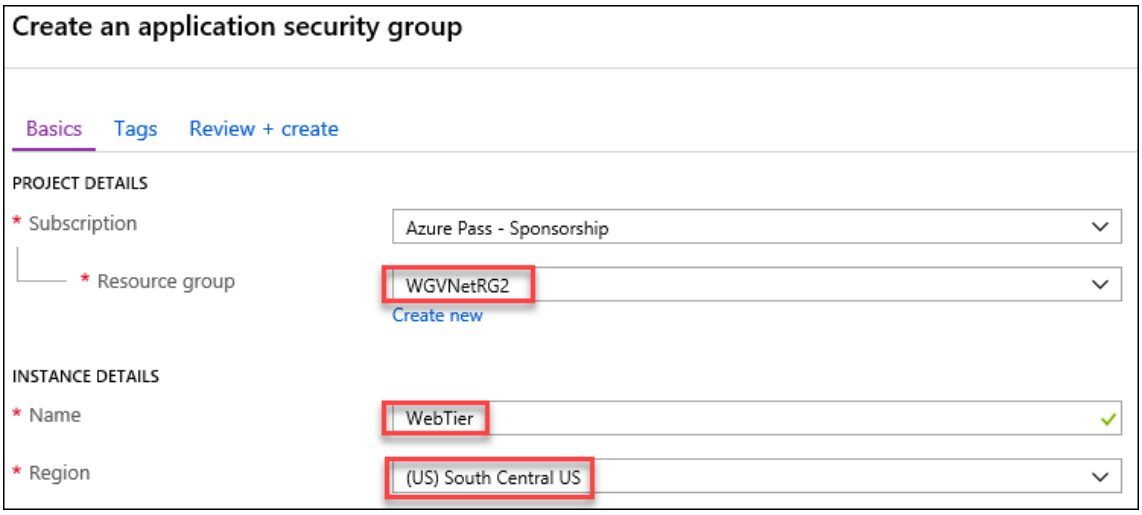
Duration: 20 minutes

In this exercise, you will restrict traffic between tiers of n-tier application by using network security groups and application security groups.

Task 1: Create application security groups

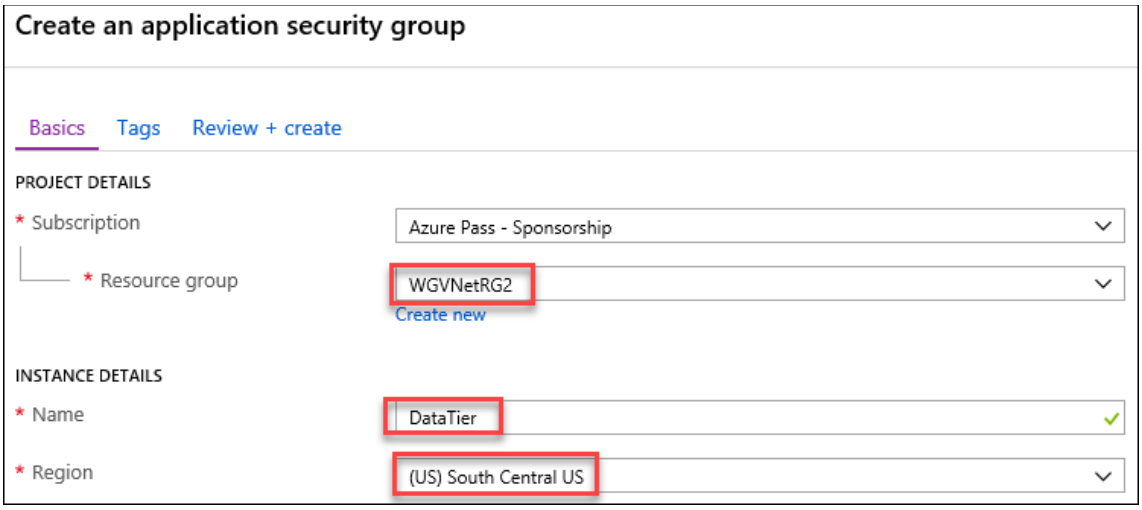
1. In the Azure portal, select **+ Create a resource**. In the **Search the Marketplace**, type **Application security group** and press Enter. Next, on the **Application security group** blade, select **Create**.

2. On the **Create an application security group** blade, on the **Basics** tab, enter the following information, and select **Review + create**:
    - Subscription: **Select your subscription**.
    - Resource group: **WGVNetRG2**
    - Name: **WebTier**
    - Region: **(US) South Central US** (This must match the location in which you created the **WGVNet2** virtual network.)



3. On the **Create an application security group** blade, on the **Review + Create** tab, ensure the validation passes, and select **Create**.

4. Repeat the previous two steps to create an application security group named **DataTier** with the settings matching those on the following screenshot.
    - Subscription: **Select your subscription**.
    - Resource group: **WGVNetRG2**
    - Name: **DataTier**
    - Region: **(US) South Central US** (This must match the location in which you created the **WGVNet2** virtual network.)



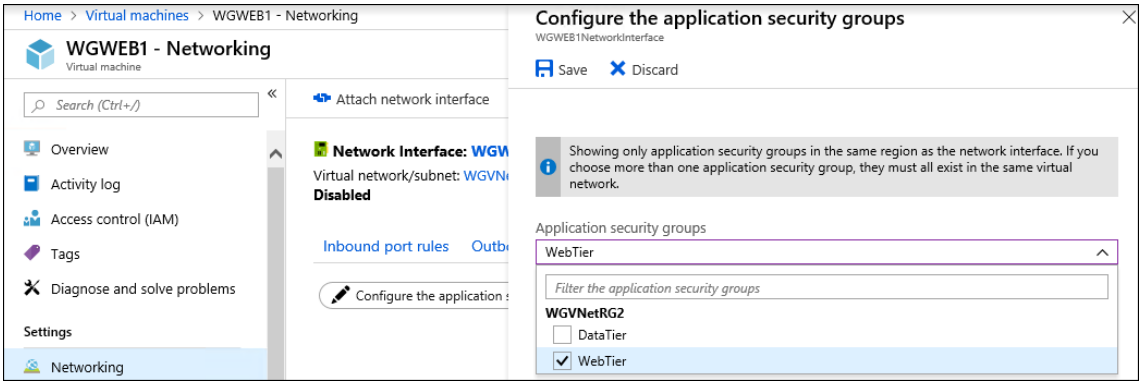
Task 2: Configure application security groups

1. In the Azure portal, navigate to the **Virtual machines** blade and select **WGWEB1**.

2. On the **WGWEB1** blade, select **Networking** under **Settings** on the left.

3. On the **WGWEB1 - Networking** blade, select **Application security groups** and then select **Configure the application security groups**.

4. On the **Configure the application security groups** blade, in the **Application security groups** drop-down list, select **WebTier**, then **Save**.



5. Repeat steps 1-4, but this time for **WGWEB2** in order to assign to its network interface the **WebTier** application security group.

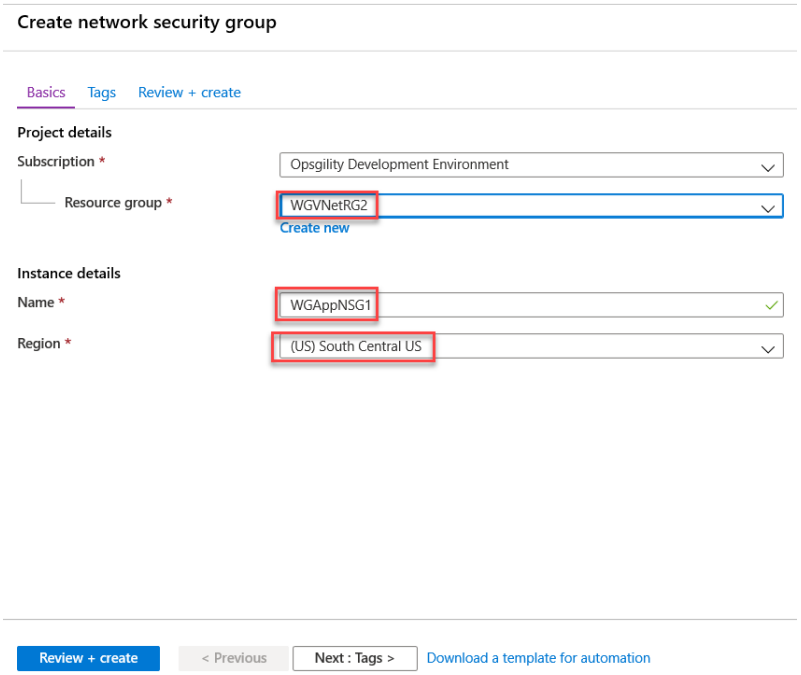
6. Repeat steps 1-4, but this time for **WGSQL1** in order to assign to its network interface the **DataTier** application security group.

Task 3: Create network security group

1. In the Azure portal, select **+ Create a resource**. In the **Search the Marketplace**, type **Network security group** and press Enter. Select it and on the **Network security group** blade, select **Create**.

2. On the **Create network security group** blade, enter the following information, and select **Review + Create** then **Create**:

    - Subscription: **Select your subscription**.
    - Resource group: **WGVNetRG2**
    - Name: **WGAppNSG1**
    - Region: **(US) South Central US** (This must match the location in which you created the **WGVNet2** virtual network.)

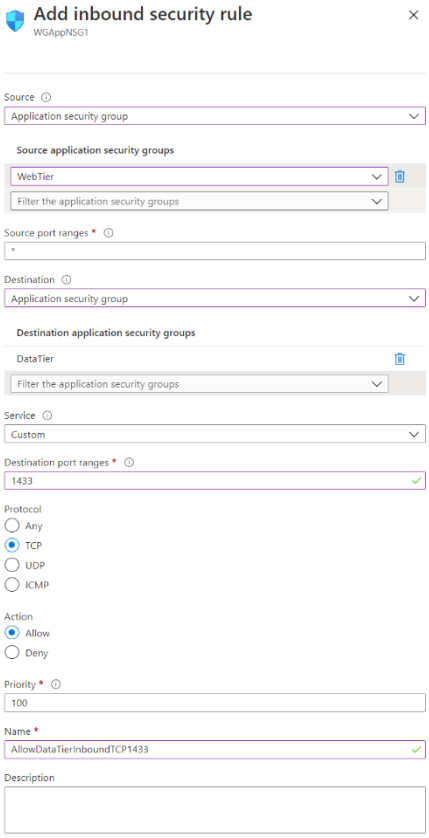


3. In the Azure Portal, navigate to **All Services**, type **Network security groups** the search box and select **Network security groups**.

4. On the **Network security groups** blade, select **WGAppNSG1**.

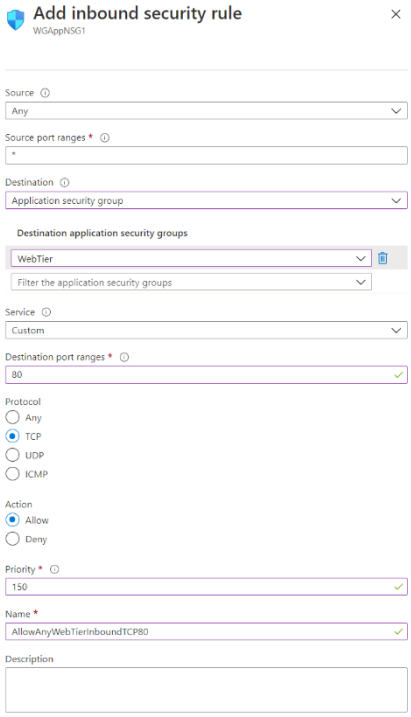
5. On the **WGAppNSG1** blade, select **Inbound security rules** under **Settings** on the left and select **Add**.

6. On the **Add inbound security rule** blade, enter the following information, and select **Add**:
    - Source: **Application security group**
    - Source application security group: **WebTier**
    - Source port ranges: *****
    - Destination: **Application security group**
    - Destination application security group: **DataTier**
    - Destination port ranges: **1433**
    - Protocol: **TCP**
    - Action: **Allow**
    - Priority: **100**
    - Name: **AllowDataTierInboundTCP1433**



7. On the **WGAppNSG1 - Inbound security rules** blade, select **Add**.

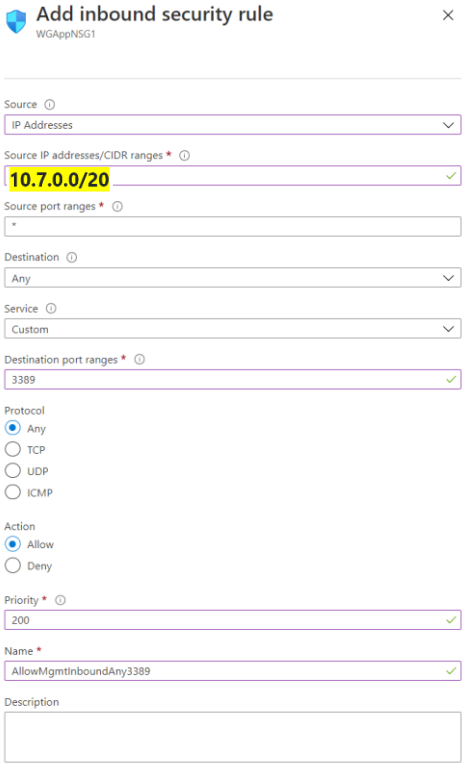
8. On the **Add inbound security rule** blade, enter the following information, and select **Add**:



   - Source: **Any**
   - Source port ranges: *****
   - Destination: **Application security group**
   - Destination application security group: **WebTier**
   - Destination port ranges: **80**
   - Protocol: **TCP**
   - Action: **Allow**
   - Priority: **150**
   - Name: **AllowAnyWebTierInboundTCP80**

9. On the **WGAppNSG1 - Inbound security rules** blade, select **Add**.

10. On the **Add inbound security rule** blade, enter the following information, and select **Add**:

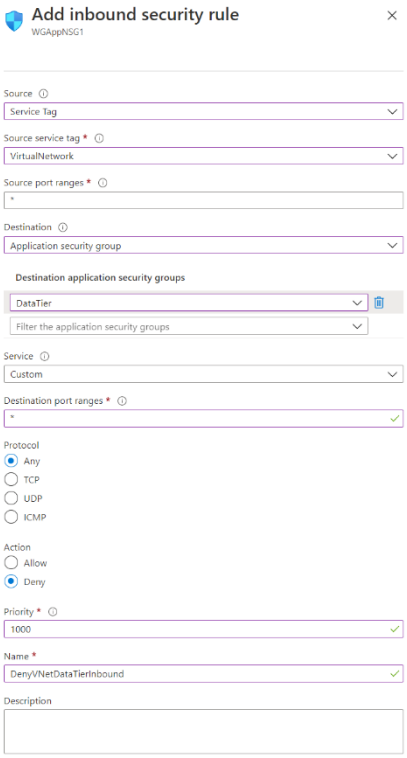


   - Source: **IP Addresses**
   - Source IP addresses/CIDR ranges: **10.7.0.0/20** (This IP address range represents WGVNet1.)
   - Source port ranges: *****
   - Destination: **Any**
   - Destination port ranges: **3389**
   - Protocol: **Any**
   - Action: **Allow**
   - Priority: **200**
   - Name: **AllowMgmtInboundAny3389**

11. On the **WGAppNSG1 - Inbound security rules** blade, select **Add**.

12. On the **Add inbound security rule** blade, enter the following information, and select **Add**:

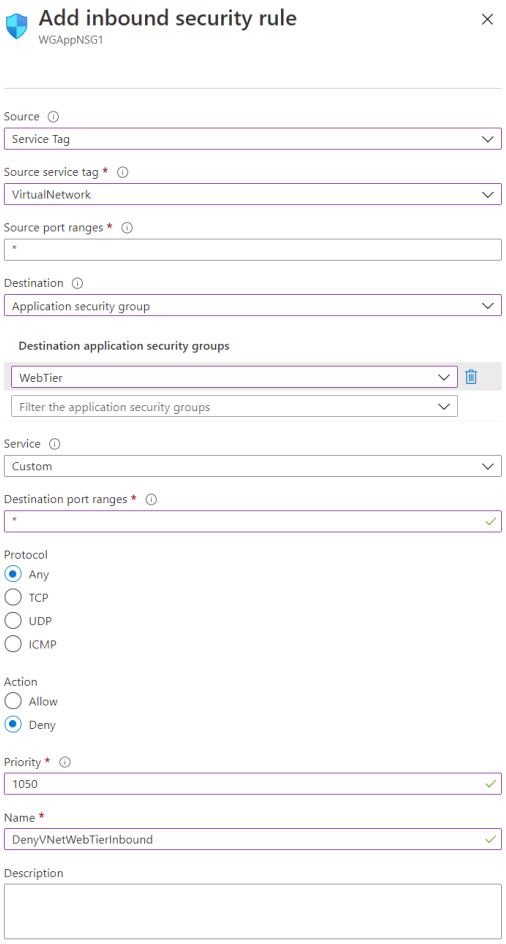
    - Source: **Service Tag**
    - Source service tag: **VirtualNetwork**
    - Source port ranges: *****
    - Destination: **Application security group**
    - Destination application security group: **DataTier**
    - Destination port ranges: *****
    - Protocol: **Any**
    - Action: **Deny**
    - Priority: **1000**
    - Name: **DenyVNetDataTierInbound**



13. On the **WGAppNSG1 - Inbound security rules** blade, select **Add**.

14. On the **Add inbound security rule** blade, enter the following information, and select **Add**:

    - Source: **Service Tag**
    - Source service tag: **VirtualNetwork**
    - Source port ranges: *****
    - Destination: **Application security group**
    - Destination application security group: **WebTier**
    - Destination port ranges: *****
    - Protocol: **Any**
    - Action: **Deny**
    - Priority: **1050**
    - Name: **DenyVNetWebTierInbound**



15. On the **WGAppNSG1 - Inbound security rules** blade, select **Subnets** under **Settings** and then select **+ Associate**.

16. On the **Associate subnet** blade, select **WGVNet2** on the **Virtual network** drop down and **AppSubnet** on the **Subnet** dropdown.

17. Select **OK** at the bottom of the **Associate subnet** blade.

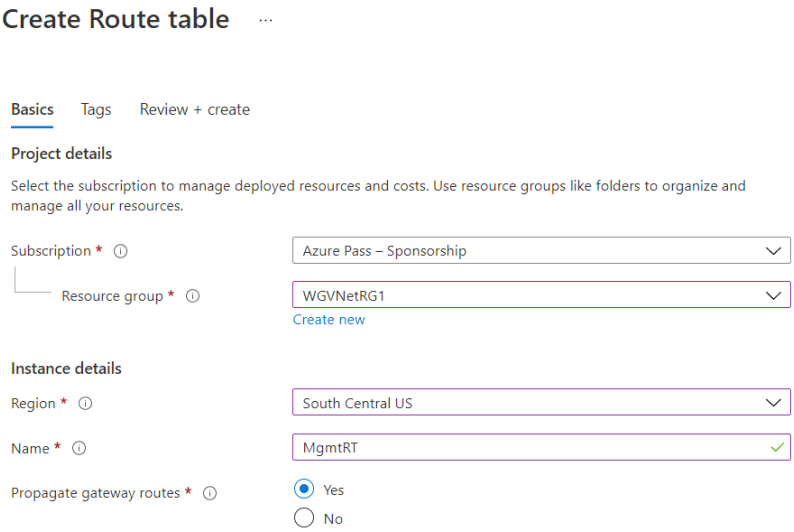
Exercise 4: Create route tables with required routes

Duration: 15 minutes

Route Tables are containers for User Defined Routes (UDRs). The route table is created and associated with a subnet. UDRs allow you to direct traffic in ways other than normal system routes would. In this case, UDRs will direct outbound traffic via the Azure firewall.

Task 1: Create route tables

1. On the main portal menu, select **+ Create a Resource**. Type **route** into the search box, and select **Route table** then select **Create**.
2. On the **Create a Route table** blade enter the following information:
   - Subscription: **Select your subscription**.
   - Resource group: Select **WGVNetRG1** from the drop down.
   - Location: **(US) South Central US**
   - Name: **MgmtRT**
   - Propagate gateway routes: **Yes**
3. When the dialog looks like the following screenshot, select **Create**.



4. Repeat steps 1 and 2 to create the **AppRT** route table:
   - Subscription: **Select your subscription**.
   - Resource group: Select **WGVNetRG2** from the drop down.
   - Location: **(US) South Central US**

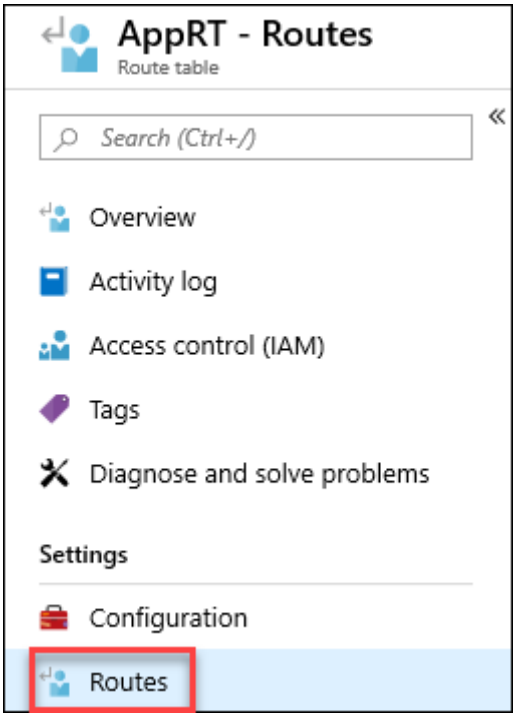
- Name: **AppRT**
- Propagate gateway routes: **Yes**

5. Once route tables are created, your **Route tables** blade should look like the following screenshot:

NAME	RESOURCE GROUP	LOCATION
AppRT	WGVNetRG2	South Central US
MgmtRT	WGVNetRG1	South Central US

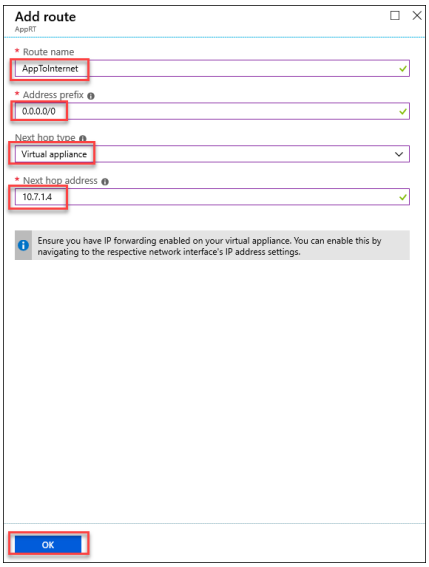
Task 2: Add routes to each route table

1. Select the **AppRT** route table, and select **Routes** under **Settings** on the left.



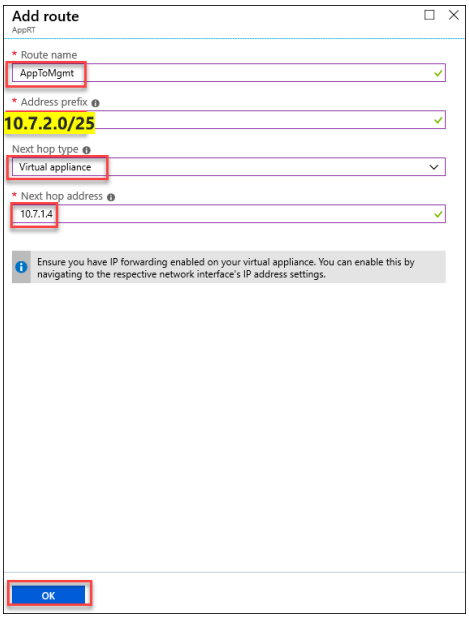
2. On the **Routes** blade, select **+ Add**. Enter the following information, and select **OK**:
   - Route name: **AppToInternet**
   - Address prefix: **0.0.0.0/0**
   - Next hop type: **Virtual appliance**

- Next hop address: **10.7.1.4**

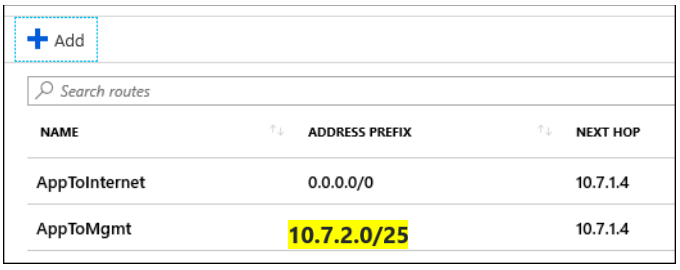


3. Repeat this procedure to add the **AppToMgmt** route using the following information:

   - Route name: **AppToMgmt**
   - Address prefix: **10.7.2.0/25**
   - Next hop type: **Virtual appliance**
   - Next hop address: **10.7.1.4**

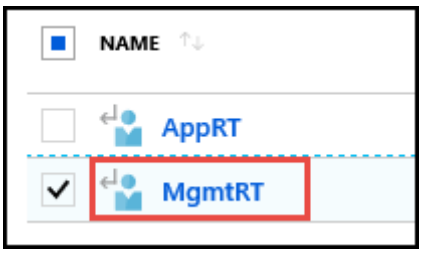


4. Upon completion, your routes in the **AppRT** route table should look like the following screenshot:



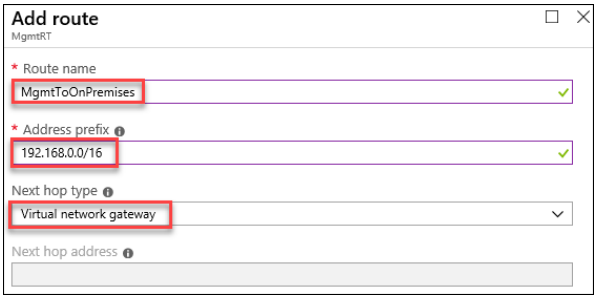
5. In the Azure Portal, go to All Services and type Route in the search box and select **Route tables**.

6. Select **MgmtRT**, and select **Routes** under **Settings** on the left.



7. On the **Routes** blade, select +**Add**. Enter the following information, and select **OK**:

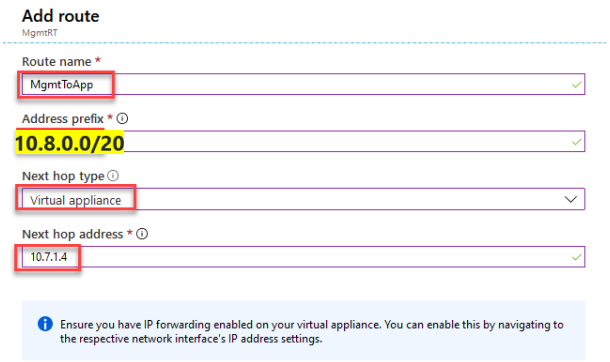
   - Route name: **MgmtToOnPremises**
   - Address prefix: **192.168.0.0/16**
   - Next hop type: **Virtual network gateway**
   - Next hop address: **Leave blank**.



8. Add the **MgmtToApp** route using the following information:

   - Route name: **MgmtToApp**
   - Address prefix: **10.8.0.0/20**
   - Next hop type: **Virtual appliance**

- Next hop address: **10.7.1.4** (This is the private IP of Azure Firewall.)



9. Upon completion, your routes in the **MgmtRT** route table should look like the following screenshot:

Name	Address prefix	Next hop
MgmtToApp	10.8.0.0/20	10.7.1.4
MgmtToOnPremises	192.168.0.0/16	Virtual network gateway

Note: The route tables and routes you have just created are not associated with any subnets yet, so they are not impacting any traffic flow yet. This will be accomplished later in the lab.

Exercise 5: Configure n-tier application and validate functionality

Duration: 20 minutes

In this exercise, you will create and configure a load balancer to distribute load between the web servers.

Task 1: Create a load balancer to distribute load between the web servers

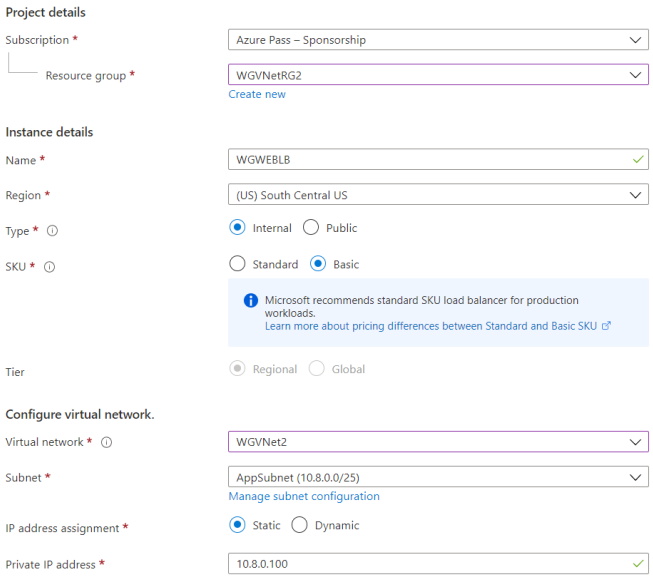
1. In the Azure portal, select **+ Create a resource**, then search for **Load Balancer**.

2. On the **Create load balancer** blade, on the **Basics** tab, enter the following values:

   - Subscription: **Select your subscription**.

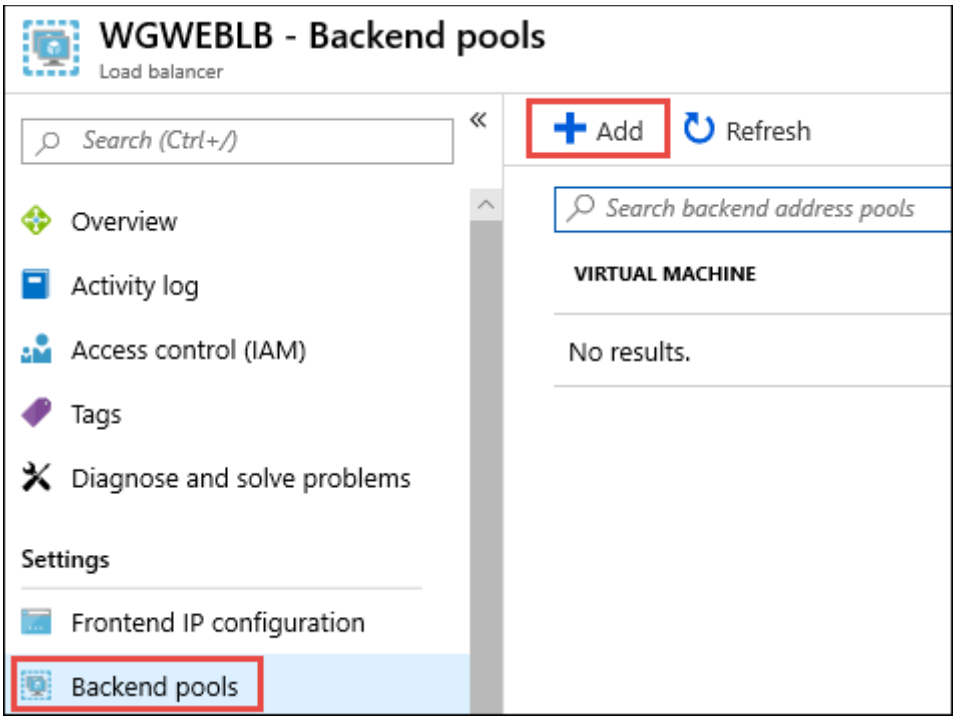
- Resource group: **WGVNetRG2**
- Name: **WGWEBLB**
- Region: **(US) South Central US**
- Type: **Internal**
- SKU: **Basic**
- Virtual network: **WGVNet2**
- Subnet: **AppSubnet (10.8.0.0/25)**
- IP address assignment: Select **Static** and enter the IP address **10.8.0.100**

Ensure your **Create load balancer** dialog looks like the following, and select **Review + create** then select **Create**.

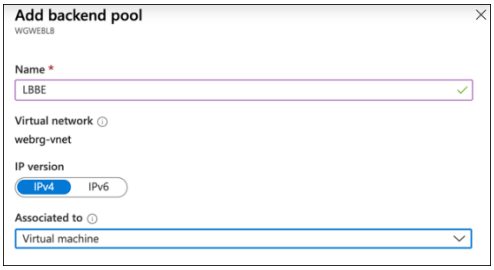


Task 2: Configure the load balancer

1. Open the **WGWEBLB** load balancer in the Azure portal.
2. Select **Backend pools**, and select **+Add** at the beginning.



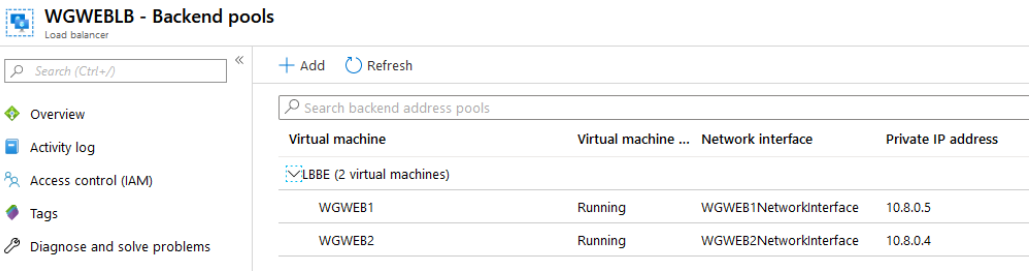
3. Enter **LBBE** for the pool name. Under **Associated to**, select **Virtual machine**.



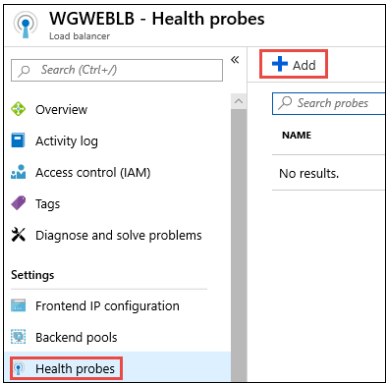
4. Under **Virtual machine**, press +Add and choose the **WGWEB1** virtual machine and **WGWEB2** virtual machine.

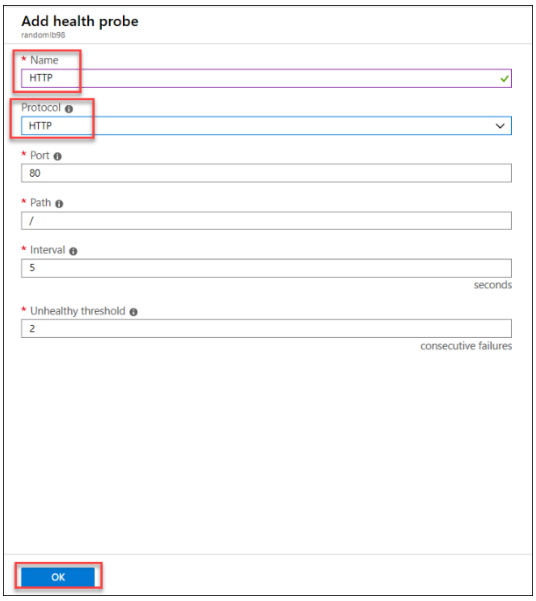
5. Select **Add** to add the backend pool.

6. Wait to proceed until the Backend pool configuration is finished updating.



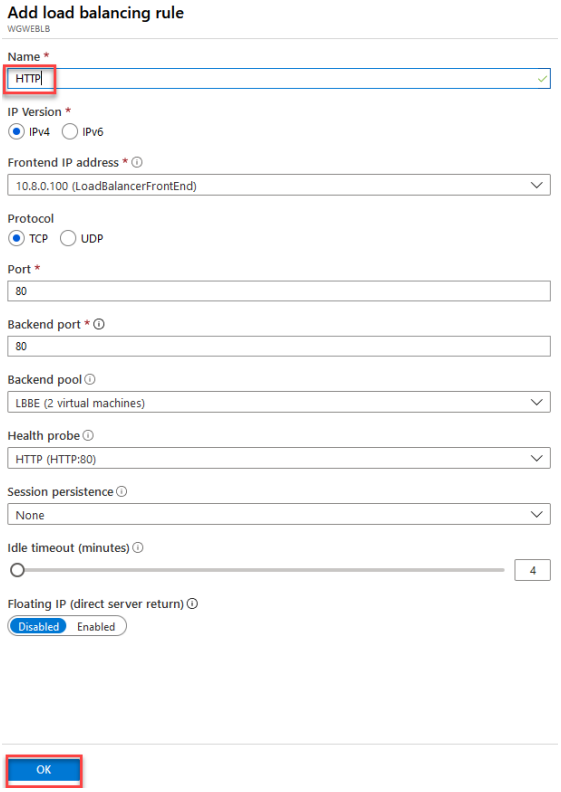
7. Next, under **Settings** on the WGWEBLB Load Balancer blade select **Health Probes**. Select **+ Add**, and use the following information to create a health probe.
    - Name: **HTTP**
    - Protocol: **HTTP**





8. Select **OK**.

9. After the Health probe has updated. Select **Load balancing rules**. Select **+Add** and complete the configuration as shown below followed by selecting **OK**.
    - Name: **HTTP**
    - Leave the rest as defaults.



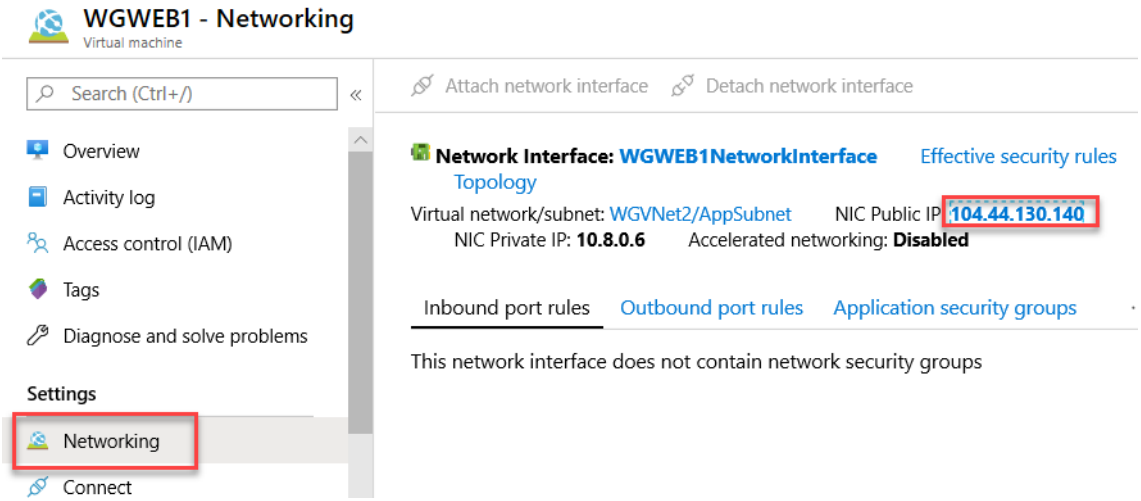
It will take 2-3 minutes for the changes to save.

10. From an RDP session to WGWEB1, open your browser and navigate to http://10.8.0.100. Ensure that you successfully connect to either one of two Web servers.

CloudShop Demo - Products - running on WEB1

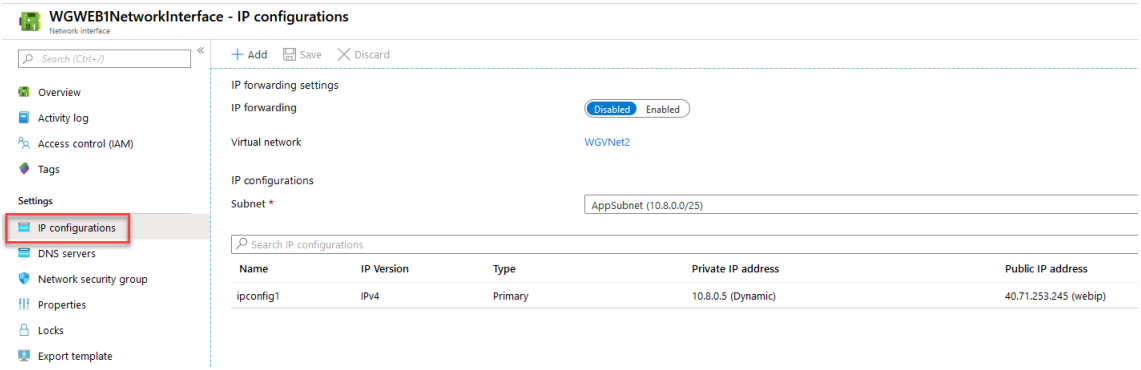
CloudShop Demo - Products - running on WEB2

11. Using the portal, disassociate the public IP from the NIC of **WGWEB1 VM**. Do this by navigating to the VM and selecting **Networking** under **Settings** on the left. Select the **NIC Public IP** then choose **Dissociate**. Select **Yes** when prompted.



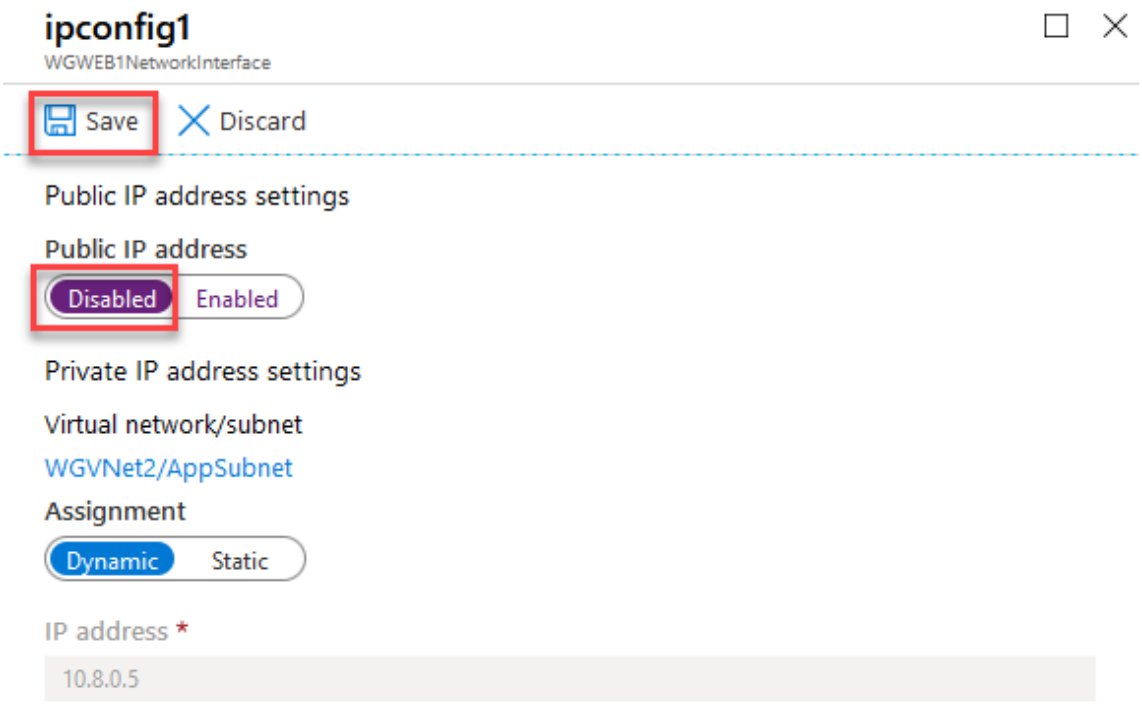
12. Next, return to the **WGWEB1 - Networking** blade and select the **Network Interface**

13. Select **IP configurations** under **Settings** on the left.



14. Next, select **ipconfig1** shown above.

15. Select and make sure that the **Public IP address settings** is shown as disabled, and select **Save** if necessary. This should remove the public IP address from the network interface of the VM.



Exercise 6: Provision and configure Azure firewall solution

Duration: 15 minutes

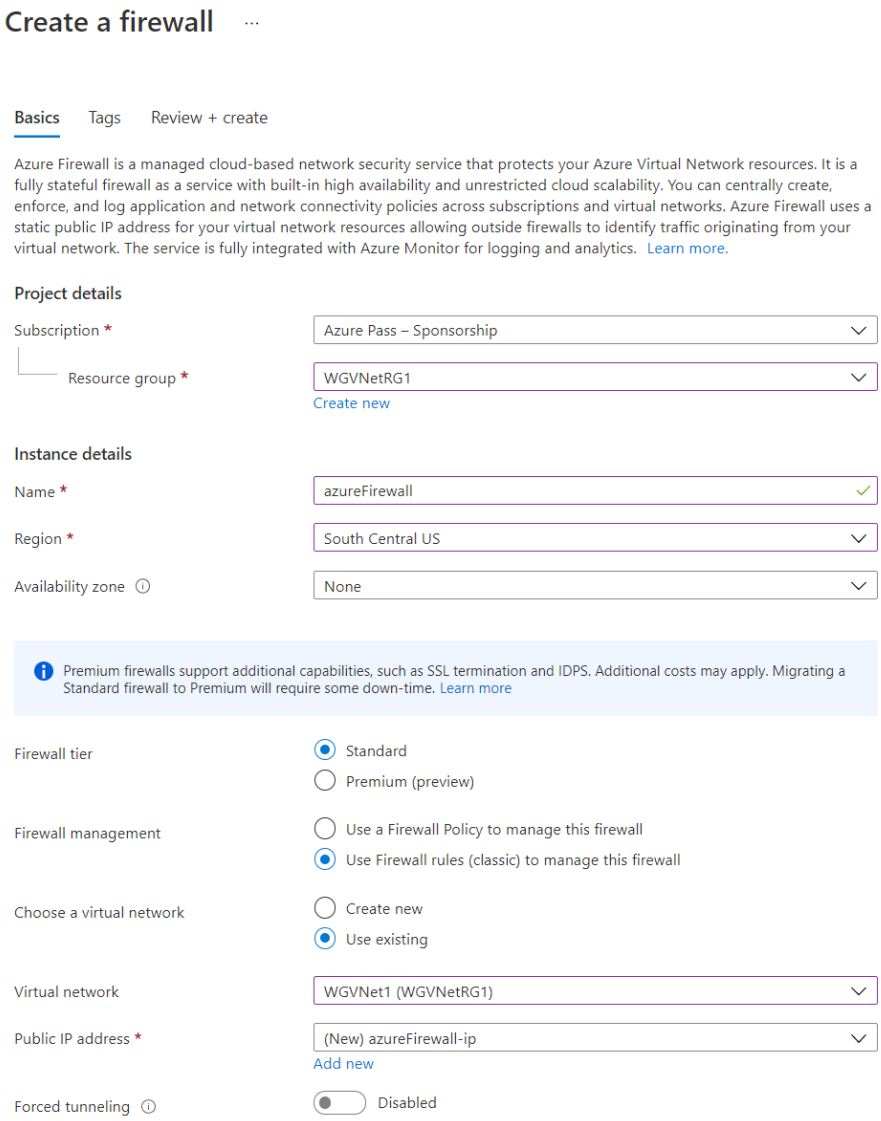
In this exercise, you will provision and configure an Azure firewall in your network.

Task 1: Provision the Azure firewall

1. In the Azure portal, select **+ Create a resource**. In the **Search the Marketplace** text box, type **Firewall**, in the list of results, select **Firewall**, and on the **Firewall** blade, select **Create**.

2. On the **Create a firewall** blade, on the **Basics** tab, enter the following information:

    - Subscription: select your subscription.
    - Resource group: **WGVNetRG1**
    - Name: **azureFirewall**
    - Region: **South Central US**
    - Availability zone: **none**
    - Firewall tier: **Standard**
    - Firewall management: **Use Firewall rules (classic) to manage this firewall**
    - Select a Virtual network: Select **Use existing** and then select **WGVNet1**.
    - Public IP address: **Add new**
    - Public IP address name: **azureFirewall-ip**
    - Forced tunneling: **Disable**



3. Select **Review + create** and then select **Create** to provision the Azure Firewall.

Task 2: Create Firewall Rules

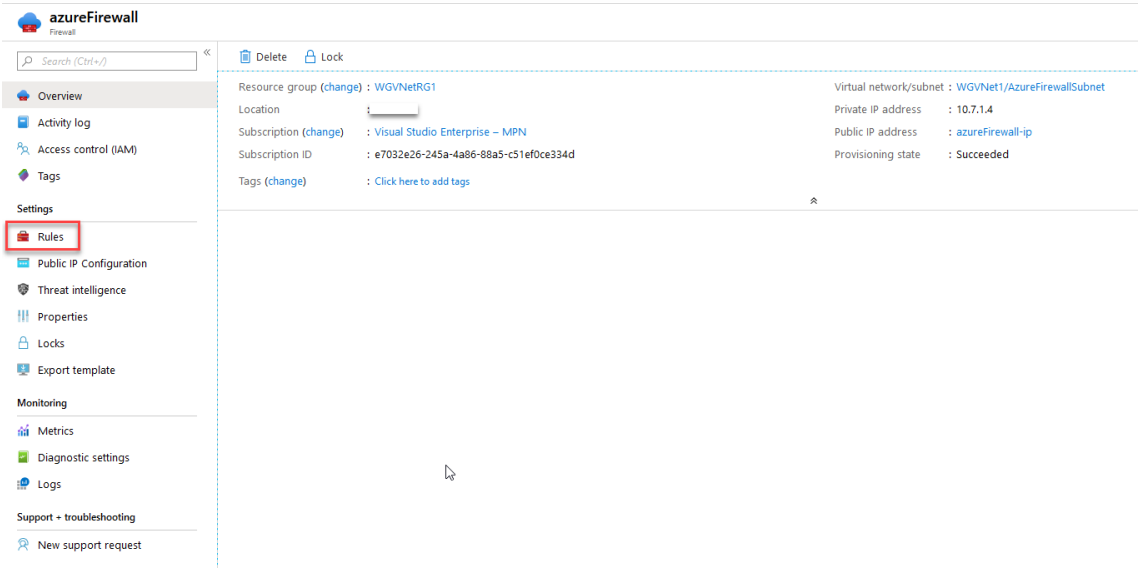
Within 1-2 minutes, the resource group **WGVNetRG1** will have the firewall created. Next, we will firewall rules to allow the inbound and outbound traffic.

1. On the main Azure menu select **Resource groups**.

2. Select the **WGVNetRG1** resource group. This resource group contains the azure firewall and its public IP address resources.

3. Navigate to the **azureFirewall-ip** blade and note the value of its public IP address. You will need it later in this task.

4. Navigate to the **azureFirewall** blade, and, on the **Overview** page, select **Rules** under **Settings** on the left.

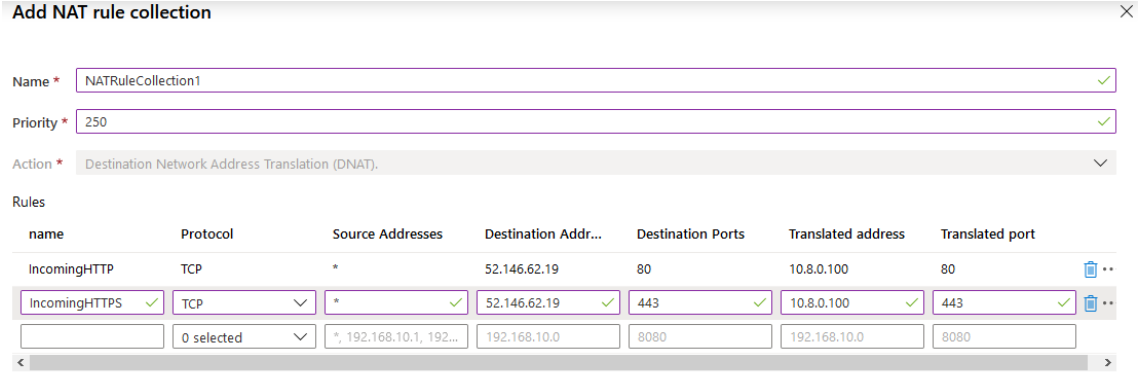


5. Select **+ Add NAT Rule collection** and enter the following information to create an inbound NAT Rule (collection is a list of rules that share the same priority and action):

   - Name: **NATRuleCollection1**
   - Priority: **250**
   - Rules Name: **IncomingHTTP**
   - Protocol: **TCP**
   - Source type: **IP address**
   - Source address: *****
   - Destination Address: Type the public IP address assigned to the firewall you identified earlier in this task.
   - Destination ports: **80** (to allow HTTP traffic)
   - Translated Address: **10.8.0.100** (Private IP of the Azure Load Balancer you deployed earlier in this lab.)
   - Translated Port: **80**

6. Create another rule for HTTPS, as illustrated on the following screenshot (alternatively you could create a single rule for both HTTP and HTTPS).

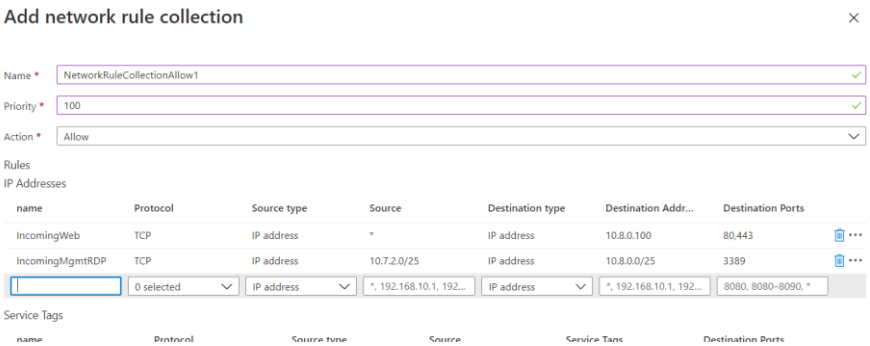
- Rule Name: **IncomingHTTPS**
- Protocol: **TCP**
- Source Addresses: *****
- Destination Address: Type the public IP address assigned to the firewall you identified earlier in this task.
- Destination ports: **443**
- Translated Address: **10.8.0.100**
- Translated Port: **443**



7. Select **Add** and wait until the update completes.
8. Back on the Azure Firewall **Rules** page, select **Network rule collection** tab. Then Select **+ Add Network Rule collection** and enter the following information to create a Network Rule for inbound traffic. This rule allows HTTP connectivity from any directly connected network targeting the frontend IP address of the load balancer.
   - Name: **NetworkRuleCollectionAllow1**
   - Priority: **100**
   - Action: **Allow**
   - Rule Name: **IncomingWeb**
   - Source type: **IP address**
   - Protocol: **TCP**
   - Source address: *****

- Destination Address: **10.8.0.100**
- Destination ports: **80,443**

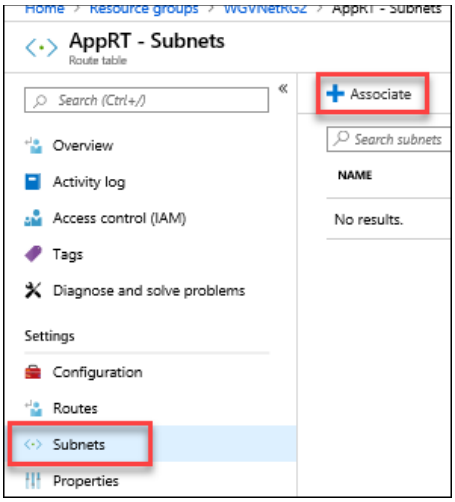
9. Crate another rule for Remote Desktop sessions from the Management subnet on WGVNet1.
    - Rule Name: **IncomingMgmtRDP**
    - Protocol: **TCP**
    - Source type: **Ip address**
    - Source address: **10.7.2.0/25**
    - Destination Address: **10.8.0.0/25**
    - Destination ports: **3389**



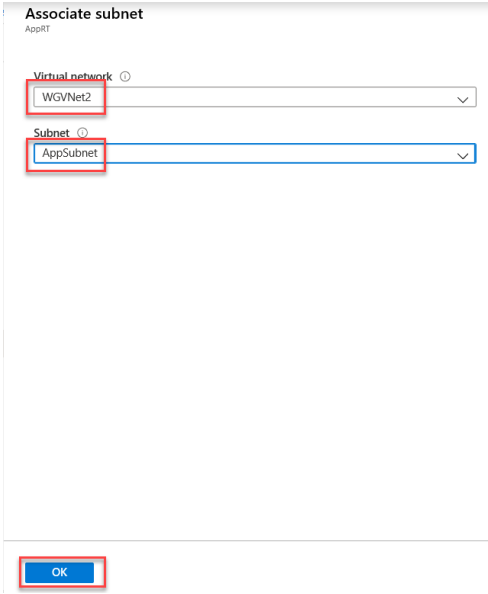
10. Select **Add** and wait until the update completes.

Task 3: Associate route tables to subnets

1. In the Azure portal, navigate to the blade displaying properties of the **WGVNetRG2** resource group.
2. Select **AppRT**, followed by **Subnets** and then select **+ Associate**.



3. On the **Associate subnet** blade, select **WGVNet2** on the **Virtual network** drop down. Select **AppSubnet** on the **Subnet** dropdown.

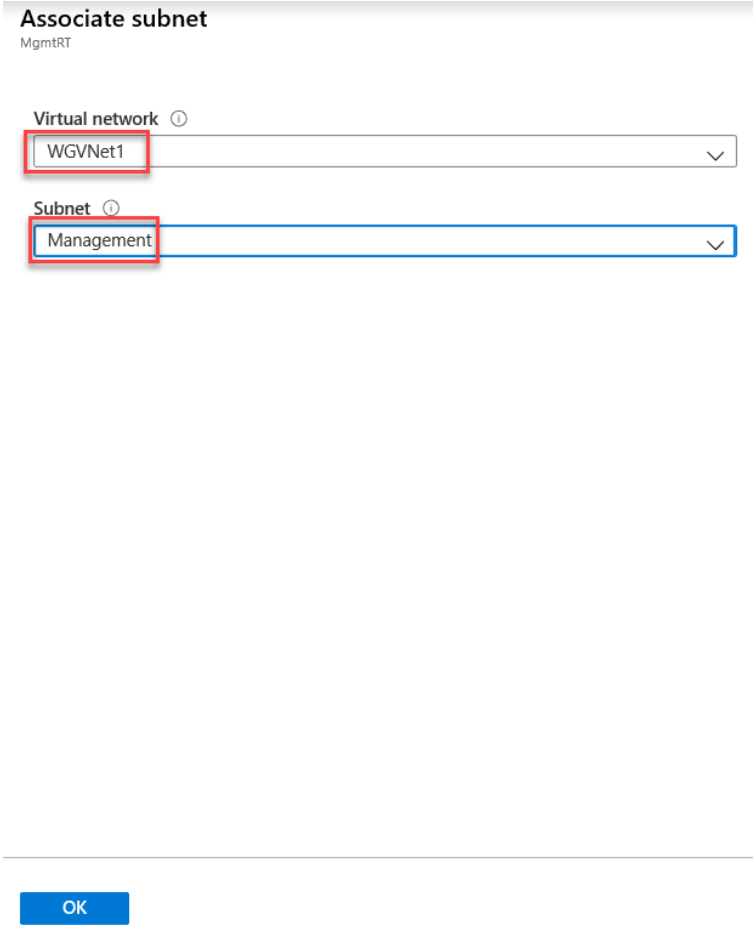


4. Select **OK** at the bottom of the **Associate subnet** blade.

5. Navigate to the blade displaying properties of the **WGVNetRG1** resource group, and select **MgmtRT**, then **Subnets**.

6. Select the **+ Associate**.

7. On the **Associate subnet** blade, select **WGVNet1** on the **Virtual network** drop down. Select **Management** on the **Subnet** dropdown.



8. Select **OK** at the bottom of the **Associate subnet** blade.

Exercise 7: Configure Site-to-Site connectivity

Duration: 60 minutes

In this exercise, we will simulate an on-premises connection to the internal web application. To do this, we will first set up another Virtual Network in a separate Azure region followed by the Site-to-Site connection of the 2 Virtual Networks Finally, we will set up a virtual machine in the new Virtual Network to simulate on-premises connectivity to the internal load-balancer.

Task 1: Create OnPrem Virtual Network

1. In the Azure portal, select **+ Create a resource**, search for **Virtual network**.

2. On the **Create virtual network** blade, enter the following information:

- Subscription: **Select your subscription**.
- Resource group: Select **Create new**, and enter the name **OnPremVNetRG**
- Name: **OnPremVNet**
- Location: **(US) East US** (Make sure this is **NOT** the same location you have specified in the previous exercises.)

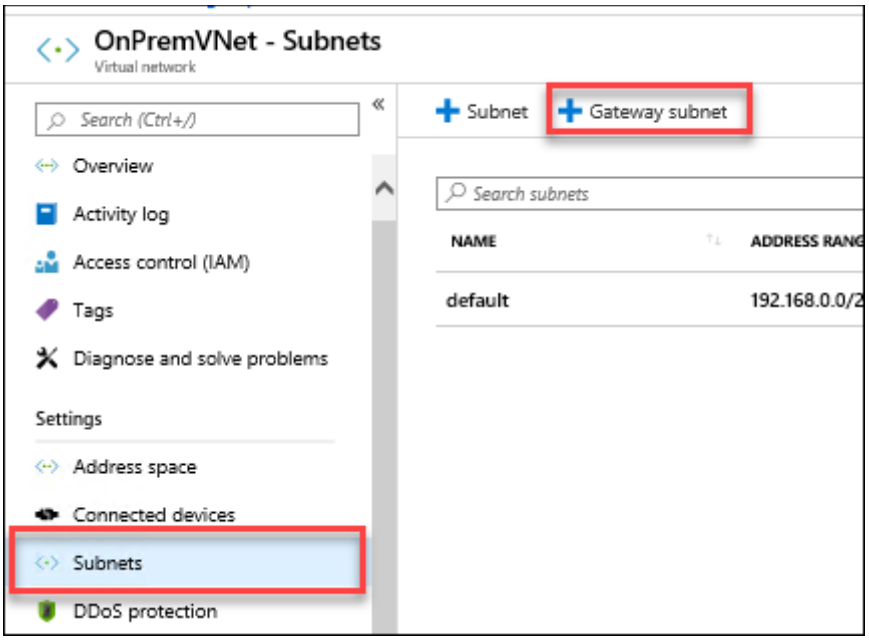
Click **Next : IP Address >**

- Address space: **192.168.0.0/16**
- **+Add subnet**
- Subnet name: **default**
- Subnet address range: **192.168.0.0/24**, click **Add**

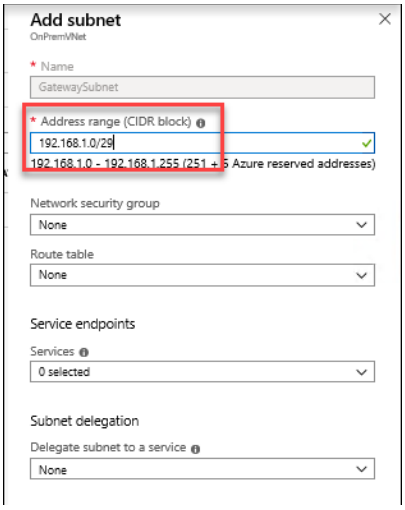
3. Leave the other options with their default values.
4. Upon completion, it should look like the following screenshot. Validate the information is correct, and select **Review + Create** and then **Create**

Task 2: Configure gateway subnets for on premise Virtual Network

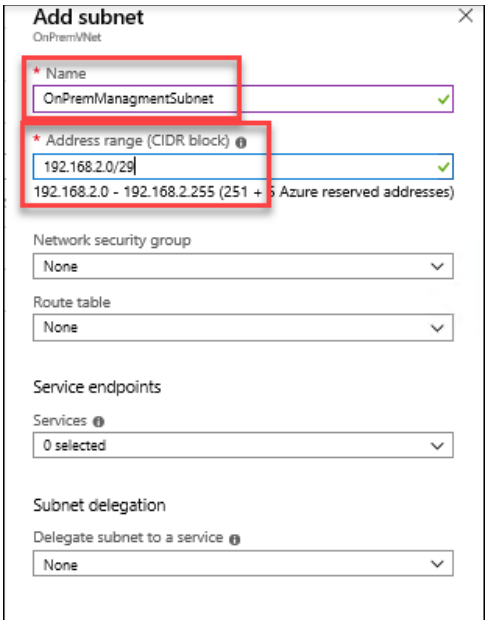
1. Select the **OnPremVnetRG** Resource Group and then open the **OnPremVNet** blade and select **Subnets**.
2. Next, select **+ Gateway subnet**.



3. Specify the following configuration for the subnet, and select **OK**:
    - Address range: **192.168.1.0/29**
    - Route table: **None** (We will add later.)



4. Next, select **+ Subnet** and add **OnPremManagementSubnet** to the **OnPremVNet**, as shown below in the screenshot:
    - Name: **OnPremManagementSubnet**
    - Address range: **192.168.2.0/29**
    - Leave the rest of the values as their defaults.



Task 3: Create the first gateway

1. Using the Azure Management portal, select **+ Create a resource**, type **Virtual Network gateway** in the **Search the Marketplace** text box, in the list of results, select **Virtual network gateway**, and then select **Create**.

2. On the **Create virtual network gateway** blade, enter the following information and select **Review + create**:

    - Subscription: **Select your subscription**.
    - Name: **OnPremWGGateway**
    - Region: **(US) East US** (This must match the location in which you created the **OnPremVNet** virtual network.)
    - Gateway type: **VPN**
    - VPN type: **Route-based**
    - SKU: **VpnGw1**
    - Generation: **Generaton1**
    - Virtual network: **OnPremVNet**
    - Public IP address: **Create new**

- Public IP address name: **onpremgatewayIP1**
- Enable active-active mode: **Enabled**
- Second Public IP address name: **onpremgatewayIP2**
- Configure BGP: **Disabled**

Create virtual network gateway ...

Basics | Tags | Review + create

Azure has provided a planning and design guide to help you configure the various VPN gateway options. Learn more.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	Azure Pass – Sponsorship
Resource group	OnPremVNetRG (derived from virtual network's resource group)

Instance details

Name *	OnPremWGGateway
Region *	East US
Gateway type *	(•) VPN ( ) ExpressRoute
VPN type *	(•) Route-based ( ) Policy-based
SKU *	VpnGw1
Generation	Generation1
Virtual network *	OnPremVNet Create virtual network
Subnet	GatewaySubnet (192.168.1.0/29)

Only virtual networks in the currently selected subscription and region are listed.

Public IP address

Public IP address *	(•) Create new ( ) Use existing
Public IP address name *	onpremgatewayIP1
Public IP address SKU	Basic
Assignment	(•) Dynamic ( ) Static
Enable active-active mode *	(•) Enabled ( ) Disabled

SECOND PUBLIC IP ADDRESS

SECOND PUBLIC IP ADDRESS *	(•) Create new ( ) Use existing
Public IP address name *	onpremgatewayIP2
Configure BGP *	( ) Enabled (•) Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's documentation regarding validated VPN devices.

3. Validate your settings and select **Review + Create** then **Create**.

   Note: The gateway will take 30-45 minutes to provision. Rather than waiting, continue to the next task.

Task 4: Create the second gateway

1. Using the Azure Management portal, select **+ Create a resource**, type **Virtual Network gateway** in the **Search the Marketplace** text box, in the list of results, select **Virtual network gateway**, and then select **Create**.

2. On the **Create virtual network gateway** blade, enter the following information and select **Review + create**:

   - Subscription: **Select your subscription**.
   - Name: **WGVNet1Gateway**
   - Region: **South Central US** (This must match the location in which you created the **WGVNet1** virtual network.)
   - Gateway type: **VPN**
   - VPN type: **Route-based**
   - SKU: **VpnGw1**
   - Generation: **Generation1**
   - Virtual network: **WGVNet1**
   - Resource group: **WGVNetRG1**
   - Public IP address: **Create new**
   - Public IP address name: **vnet1gatewayIP1**
   - Enable active-active mode: **Enabled**
   - Second Public IP address name: **vnet1gatewayIP2**
   - Configure BGP ASN: **Disabled**

Create virtual network gateway ...

Basics | Tags | Review + create

Azure has provided a planning and design guide to help you configure the various VPN gateway options. Learn more.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	Azure Pass – Sponsorship
Resource group	WGVNetRG1 (derived from virtual network's resource group)

Instance details

Name *	WGVNet1Gateway
Region *	South Central US
Gateway type *	(•) VPN ( ) ExpressRoute
VPN type *	(•) Route-based ( ) Policy-based
SKU *	VpnGw1
Generation	Generation1
Virtual network *	WGVNet1 Create virtual network
Subnet	GatewaySubnet (10.7.0.0/29)

Only virtual networks in the currently selected subscription and region are listed.

Public IP address

Public IP address *	(•) Create new ( ) Use existing
Public IP address name *	vnet1gatewayIP1
Public IP address SKU	Basic
Assignment	(•) Dynamic ( ) Static
Enable active-active mode *	(•) Enabled ( ) Disabled

SECOND PUBLIC IP ADDRESS

SECOND PUBLIC IP ADDRESS *	(•) Create new ( ) Use existing
Public IP address name *	vnet1gatewayIP2
Configure BGP *	( ) Enabled (•) Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's documentation regarding validated VPN devices.

3. Validate your settings and select **Create**.

   Note: The gateway will take 30-45 minutes to provision. You will need to wait until both gateways are provisioned before proceeding to the next section.

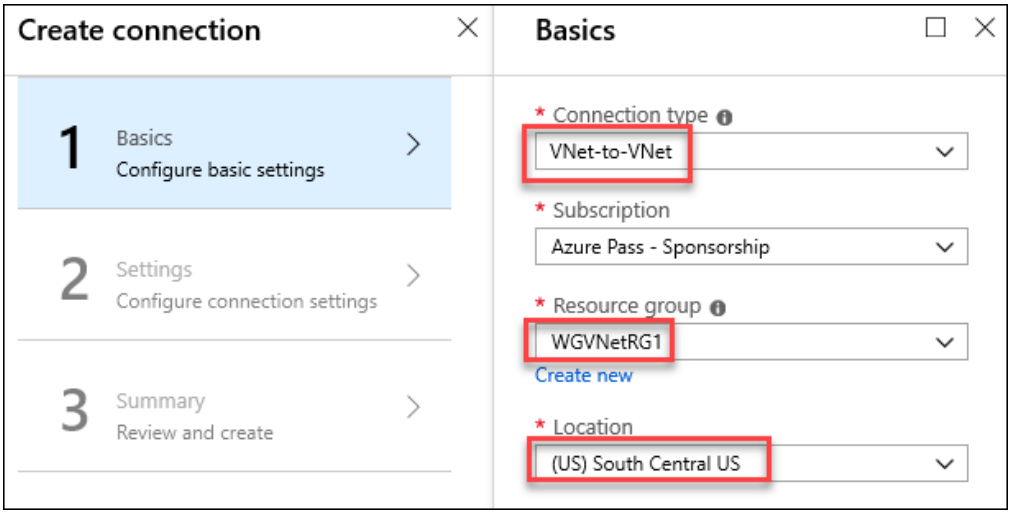
4. The Azure portal will display a notification when the deployments have completed.

#Task 5: Connect the gateways

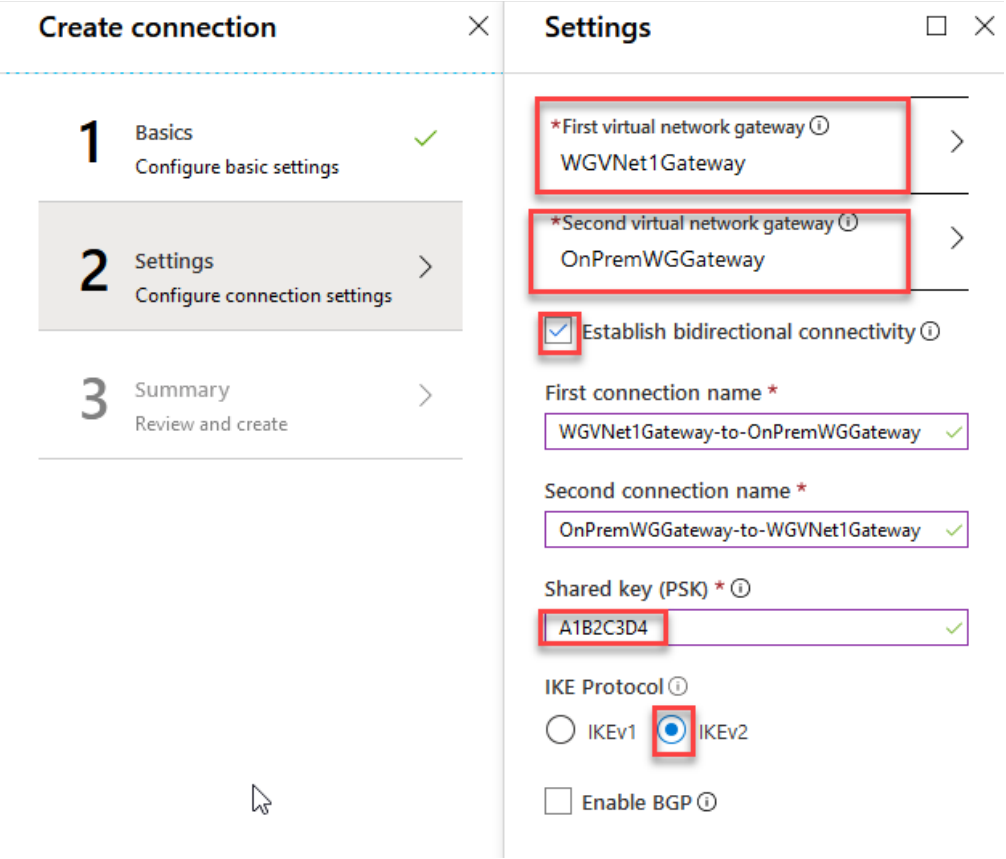
1. In the Azure portal, select **+ Create a resource**, in the **Search the Marketplace** text box, type in **Connection**, and press **Enter**.

2. On the **Connection** blade, select **Create**.

3. On the **Basics** blade, leave the **Connection type** set to **VNet-to-VNet**. Select the existing **WGVNetRG1** resource group. Then, change the location of this connection to the Azure region hosting the **WGVNet1** virtual network, **South Central US**. Select **OK**.

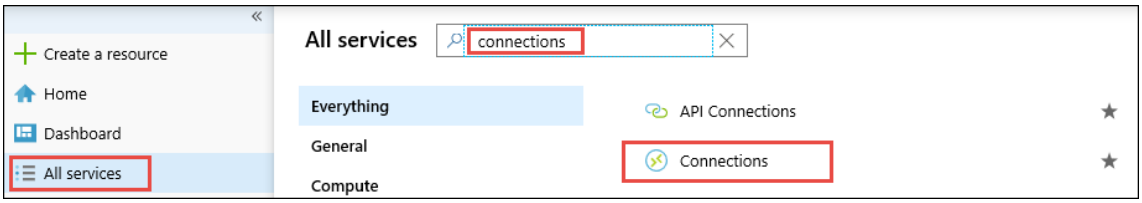


4. On the Settings tab, select **WGVNet1Gateway** as the first virtual network gateway and **OnPremWGGateway** as the second virtual network gateway. Ensure **Establish bidirectional connectivity** and **IKEv2** is selected. Enter a shared key, such as **A1B2C3D4**. Select **OK**.

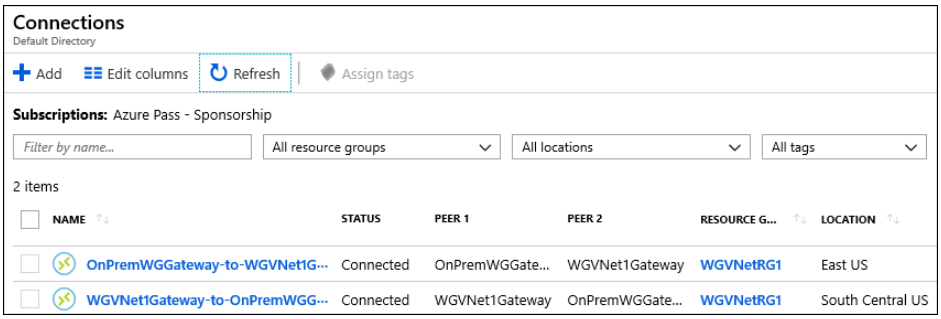


5. Select **OK** on the **Summary** page to create the connection.

6. In the Azure portal, select **All services**. Then, type **connections** in the search text box and select **Connections**.



7. Watch the progress of the connection status, and use the **Refresh** icon until the status changes for both connections from **Unknown** to **Connected**. This may take 5-10 minutes or more. You might need to refresh the page to see the change in status.



Exercise 8: Build the Bastion host service

Duration: 15 minutes

In this exercise, management of the Azure-based systems will only be available through a Bastion host. In this section, you will provision this service.

Task 1: Build the Bastion host

```
>**Note**: This step should have been completed in Exercise 1, Task 1.  If it
was not, please complete the steps below.
```

1. In the Azure portal, select **+ Create a resource** then select **Bastion**. In the search results, select the Bastion service with Microsoft as the publisher.
2. On the **Create a Bastion** blade, on the **Basics** tab, enter the following information, and select **Review + Create**:
    - Subscription: **Select your subscription**.
    - Resource group: Select **WGVnetRG1**.
    - Name: **WGBastion**
    - Region: **(US) South Central US**
    - Virtual network: **WGVNet1**
    - Subnet: **AzureBastionSubnet** Note: After creation, assign (10.7.5.0/24) as the subnet address.
    - Public IP: **Create New**
    - Public IP address name: **BastionPublicIP**
3. On the **Create a Bastion** blade, on the **Review + Create** tab, ensure the validation passes, and select **Create**. The Bastion host will take about 5 minutes to provision.

Exercise 9: Validate connectivity from 'on-premises' to Azure

Duration: 30 minutes

In this exercise, you will validate connectivity from your simulated on-premises environment to Azure.

Task 1: Create a virtual machine to validate connectivity

1. Create a new virtual machine in the OnPremVnet virtual network. In the Azure portal, select **+ Create a resource** and select **Windows Server 2016 Datacenter**.

2. On the **Create a virtual machine** blade, on the **Basics** tab, enter the following information, and select **Next : Disks >**:

    - Subscription: **Select your subscription*.
    - Resource group: Select **Create new** and enter **OnPremVMRG**.
    - Virtual machine name: **OnPremVM**
    - Region: **(US) East US** (This must much the region you created the OnPremVNet virtual network.)
    - Availability options: **No infrastructure redundancy required**
    - Image: **Windows Server 2016 Datacenter - Gen 1**
    - Size: **Standard DS1 v2**
    - User name: **demouser**
    - Password: **demo@pass123**
    - Public inbound ports: **Allow selected ports**
    - Select inbound ports: **RDP**
    - Already have a Windows license?: **No**

3. On the **Create a virtual machine** blade, on the **Disks** tab, set the following configuration and select **Next : Networking >**:

    - OS disk type: **Premium SSD**

4. On the **Create a virtual machine** blade, on the **Networking** tab, set the following configuration and select **Next : Management >**:

    - Virtual network: **OnPremVNet**
    - Subnet: **OnPremManagementSubnet (192.168.2.0/29)**
    - Public IP: **(new)OnPremVM-ip**

- NIC network security group: **Basic**
- Public inbound ports: **Allow selected ports**
- Select inbound ports: **RDP (3389)**
- Accelerated networking: **Off**
- Place this virtual machine behind an existing load balancing solution: **No**

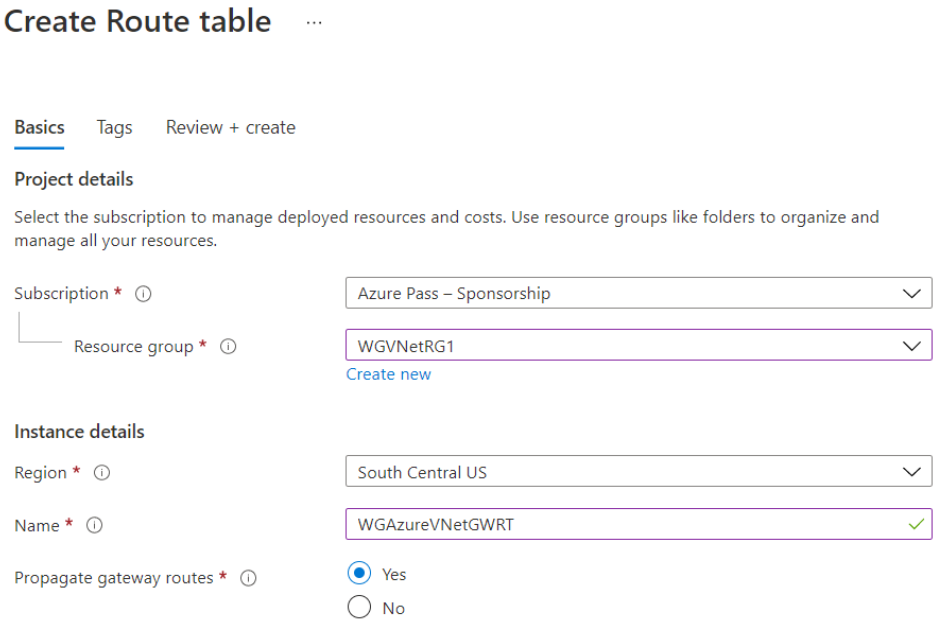
5. On the **Create a virtual machine** blade, on the **Management** tab, set the following configuration and select **Review + create**:
   - Boot diagnostics: **Disable**
   - OS guest diagnostics: **Off**
   - System assigned managed identity: **Off**
   - Enable auto-shutdown: **Off**
6. On the **Create a virtual machine** blade, on the **Review + Create** tab, ensure the validation passes, and select **Create**. The virtual machine will take about 5 minutes to provision.

Task 2: Configure routing for simulated 'on-premises' to Azure traffic

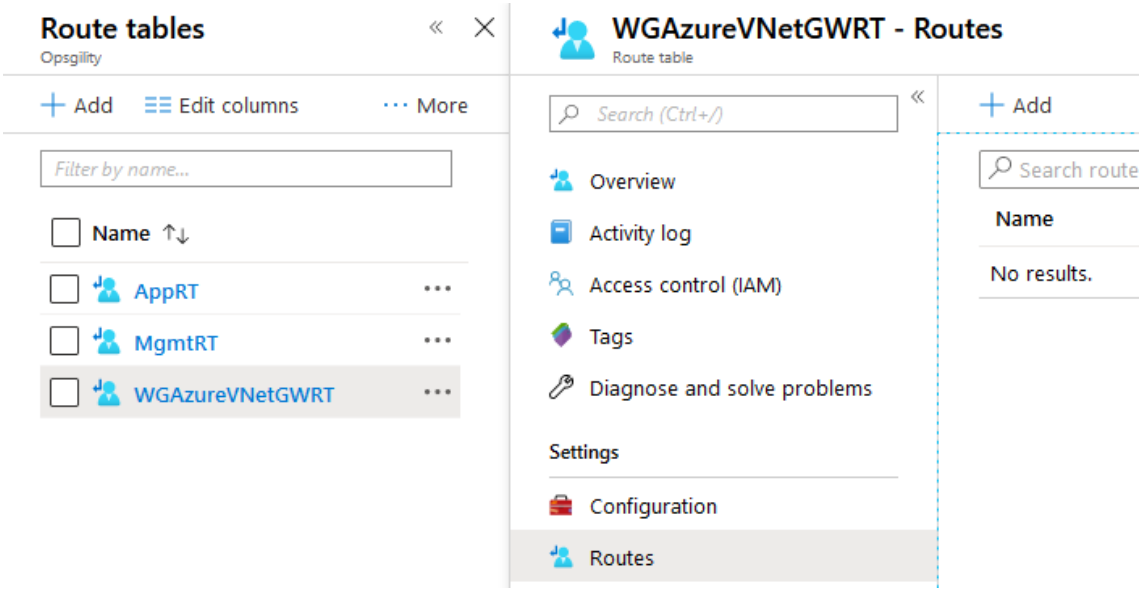
When packets arrive from the simulated 'on-premises' Virtual Network (OnPremVNet) to the 'Azure-side' (WGVNet1), they arrive at the gateway WGVNet1Gateway. This gateway is in a gateway subnet (10.7.0.0/29). For packets to be directed to the Azure firewall, we need another route table and route to be associated with the gateway subnet on the 'Azure-side'.

1. On the Azure portal select **All services** at the left navigation. Enter **Route** in the search box, and select **Route tables**.
2. On the **Route tables** blade, select **Add**.
3. On the **Create route table** blade, enter the following information:
   - Subscription: **Select your subscription**.
   - Resource group: Select the drop-down menu, and select **WGVNetRG1**.

- Location: **(US) South Central US** (This must match the location in which you created the **WGVNet1** virtual network.)
- Name: **WGAzureVNetGWRT**
- Propagate gateway routes: **Yes**

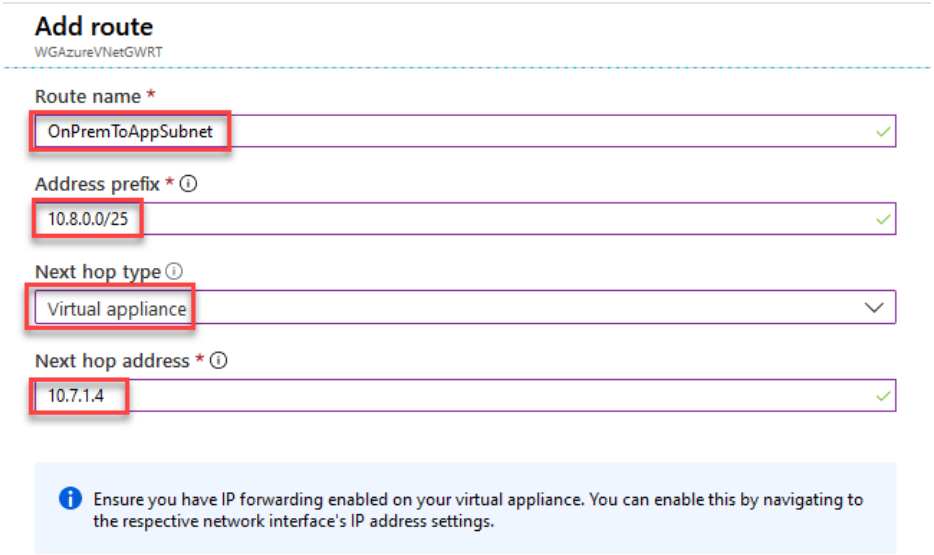


4. Select **Review + Create** and then **Create**
5. Select the **WGAzureVNetGWRT** route table.

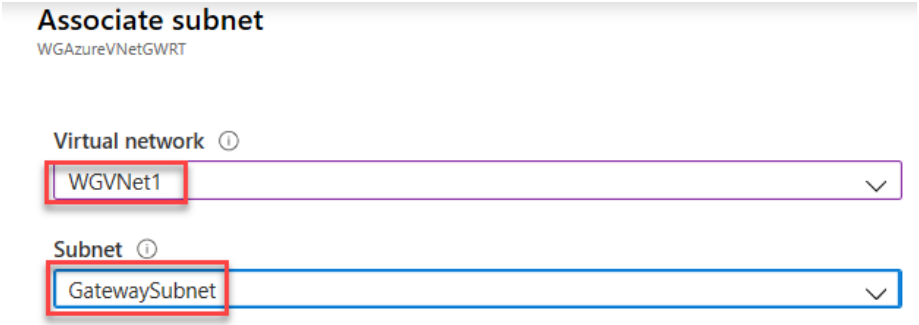


6. Select **Routes**.

7. On the **Routes** blade, select the **+Add** button. Enter the following information, and select **OK**:
    - Route name: **OnPremToAppSubnet**
    - Address prefix: **10.8.0.0/25**
    - Next hop type: **Virtual appliance**
    - Next hop address: **10.7.1.4**

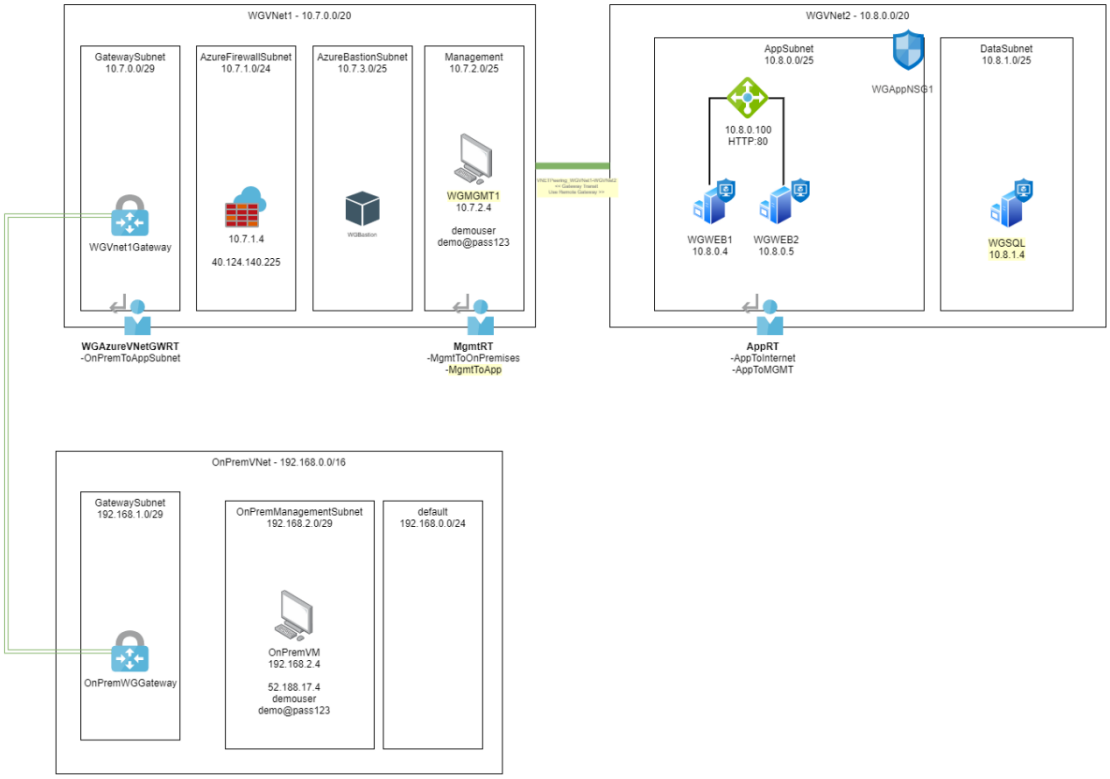


8. On the **WGAzureVNetGWRT - Routes** blade, select **Subnets** under **Settings** on the left.
9. On the **Subnets** blade, select **Associate**.
10. On the **Associate subnet** blade, select **WGVNet1** under the **Virtual Network** drop down and select **GatewaySubnet** under the **Subnet** drop down.



Task 3: Networking fix!

1. Select the resource group **WGVNetRG1**, and select the configuration blade for **WGVNet1**. Select **Peerings** under **Settings** on the left and select **VNETPeering_WGVNet1-WGVNet2** to change this item:
    - Virtual network gateway or Route Server: **Use this virtual network's gateway or Route Server**
2. Select the resource group **WGVNetRG2**, and select the configuration blade for **WGVNet2**. Select **Peerings** under **Settings** on the left and select **VNETPeering_WGVNet2-WGVNet1** to change this item:
    - Virtual network gateway or Route Server: **Use the remote virtual network's gateway or Route Server**
3. Review the Exercise 3
    - Task 3
        - Step 10
4. Review the Exercise 4
    - Task 2
        - Step 3
        - Step 8



[Download here](#) **this diagrams.net topology (draw.io)**

Task 4: Let's Test!

Note: At this point, you have configured your enterprise network. You should be able to test your Enterprise Class Network from one region to another. Your testing can include the following scenarios:

- On the 'on-premises' virtual machine (OnPremVM), attempt to initiate a Remote Desktop session to any virtual machine on the AppSubnet (10.8.0.0/25). Note that this should fail since it is blocked by Azure Firewall.
- In the Azure portal, navigate to and browse to the web application deployed to the WGVnet2 via the private IP address of the Azure Load Balancer(10.8.0.100). Note that this traffic is routed (and allowed) via Azure Firewall.
- In the Azure portal, navigate to the WGWEB1 VM and initiate a Bastion connection session to the WGWEB1 virtual machine by selecting **Connect** and **Bastion**. This should be successful since it is allowed by Azure Firewall and Azure Bastion Host.

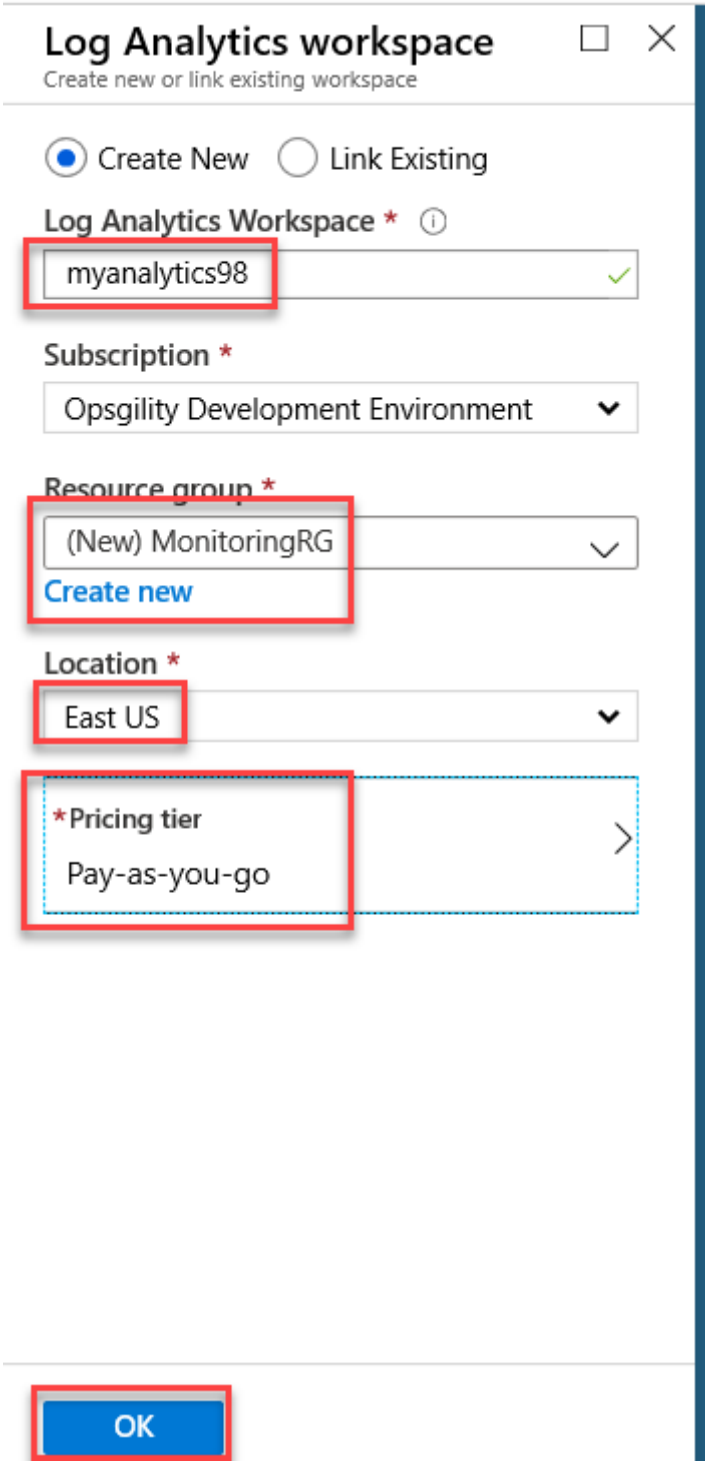
- In the Azure portal, navigate to the WGWEB1 VM and initiate a Bastion connection session to the WGWEB2 virtual machine by selecting **Connect** and **Bastion**. This should be successful since it is allowed by Azure Firewall and Azure Bastion Host.
- From within the WGWEB1 VM Bastion connection session, initiate a Remote Desktop session to the WGSQL1 via its private IP address (10.8.1.4). This should be successful since it is allowed by Azure Firewall.

Exercise 10: Create a Network Monitoring Solution (Optional)

Duration: 15 minutes

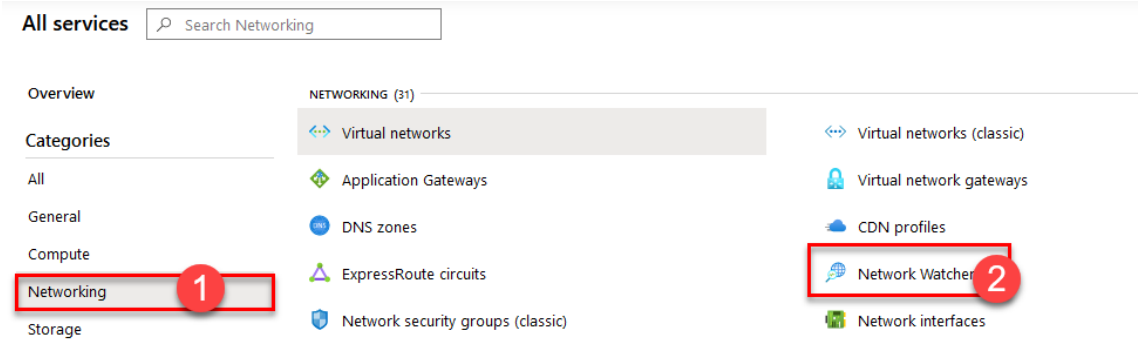
Task 1: Create a Log Analytics Workspace

1. From your **computer**, connect to the Azure portal, select **+ Create a resource**, and in the list of Marketplace categories, select **IT & Management Tools** followed by selecting **Log Analytics**.
2. On the **Create workspace** blade, enter the following information:
   - Name: **Enter Unique Name all lowercase**
   - Subscription: **Select your subscription**.
   - Resource group: Select **Create new**, and enter the name **MonitoringRG**.
   - Location: **East US**
   - Pricing Tier: **Pay-as-you-go**
3. Upon completion, it should look like the following screenshot. Validate the information is correct, and select **OK**.



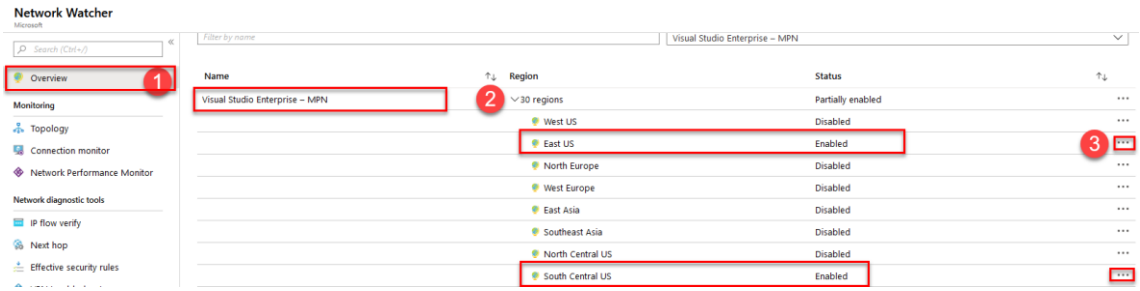
Task 2: Configure Network Watcher

1. From your **computer**, connect to the Azure portal, select **All Services**, and in the Category list, select **Networking** followed by selecting **Network Watcher**.



2. In the **Overview** blade, expand your subscription and select **SouthCentralUS** by selecting the **...** button to the right then enabling the service within the region.

3. Repeat the step above this time enabling the service within the **East US** region.



Exercise 11: Using Network Watcher to Test and Validate Connectivity (Optional)

Duration: 60 minutes

In this exercise, you will collect the flow log and perform connectivity from your simulated on-premises environment to Azure. This will be accomplished by using the Network Watcher Service in the Azure Platform.

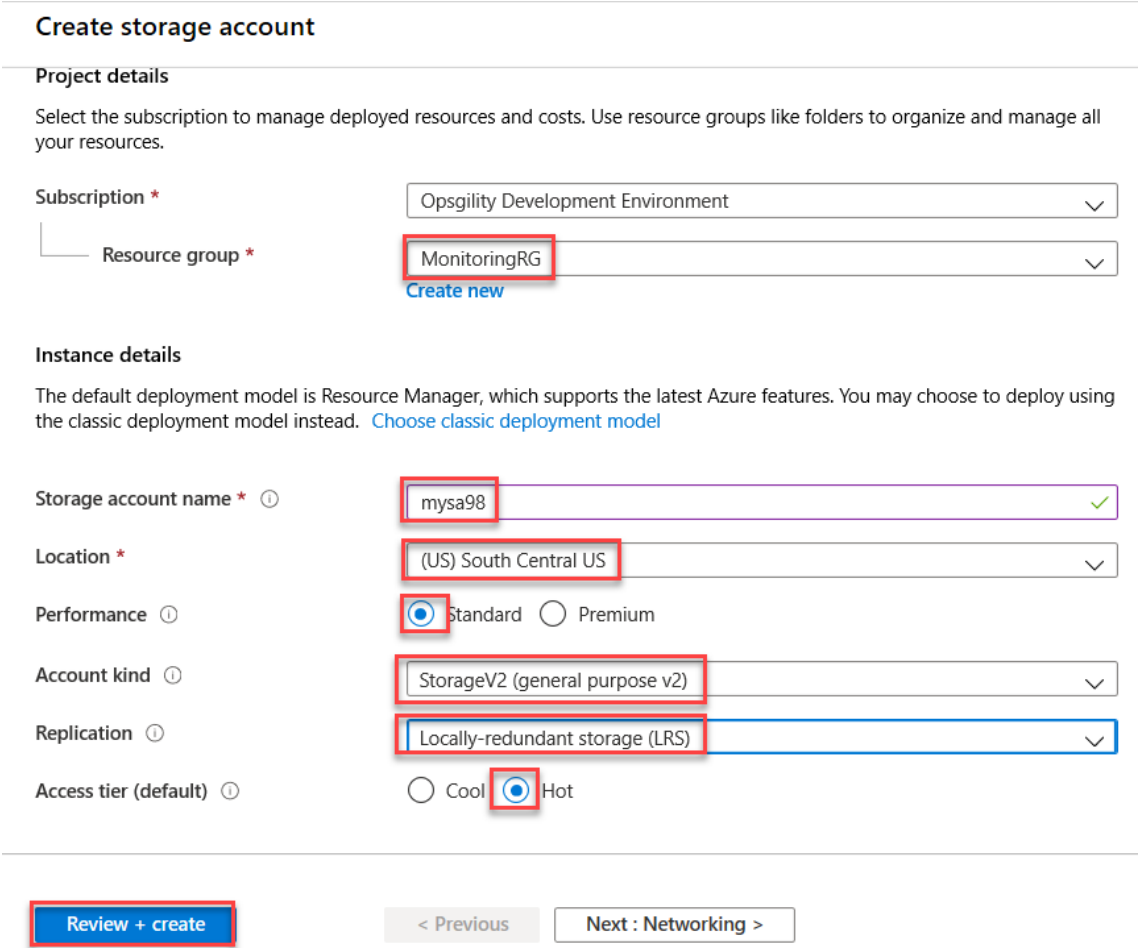
Task 1: Configuring the Storage Account for the NSG Flow Logs

1. On the Azure portal select **+ Create a resource**. From the Azure Marketplace menu select **storage** then select **Storage Account**

2. On the **Create Storage account** blade. Enter the following information, and select **Review + Create** then select the **Create** button:

    - Subscription: **Your Subscription**

- Resource Group: **MonitoringRG** (Use the existing resource group created earlier.)
- Storage Account Name: **This must be Unique and alphanumeric, lowercase and no special characters.**
- Location: **South Central US**
- Performance: **Standard**
- Account Kind: **StorageV2 (general purpose v2)**
- Replication: **Locally-redundant storage (LRS)**
- Access Tier Default: **Hot**



Note: Ensure the storage account is created before continuing.

3. Repeat step 2, but select **East US** for the region and give it a different name.

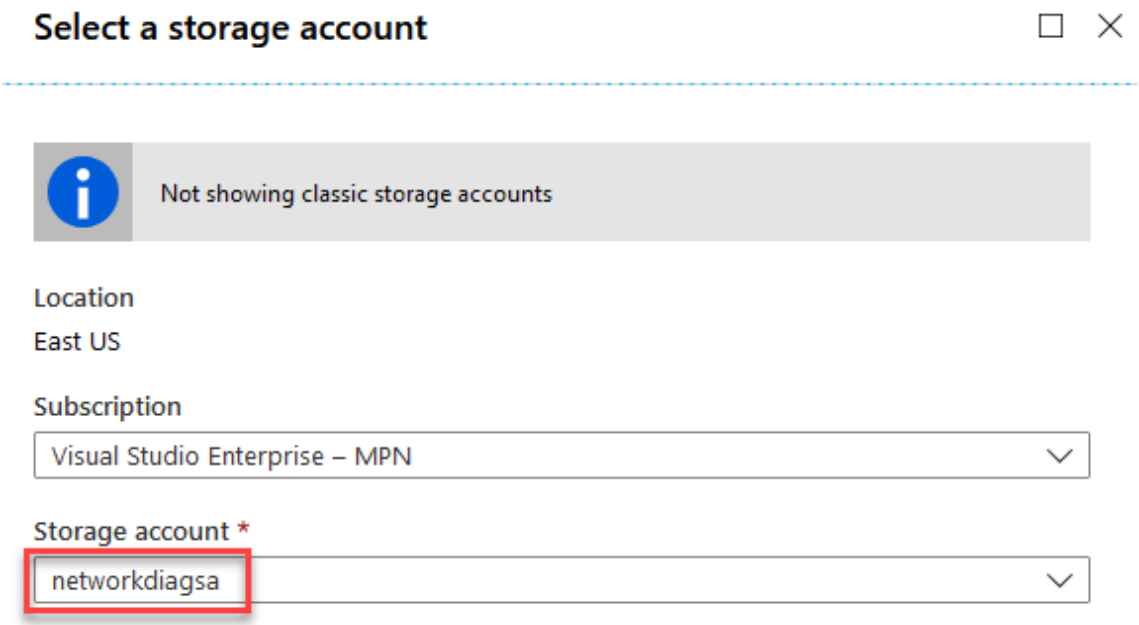
4. On the Azure portal select **All services** at the left navigation. From the Categories menu select **Networking** then select **Network Watcher**.

5. From the **Network Watcher** blade under the **Logs** menu select **NSG flow logs**. You will see both the **OnPremVM-nsg** and **WGAppNSG1** Network Security Groups.

Name	Resource type	Resource group	Status
OnPremVM-nsg	Network security group	OnPremVNetRG	Disabled
WGAppNSG1	Network security group	WGVNetRG2	Disabled

6. Select the **WGAppNSG1** network security group to open the flow log settings. Select **On** and then select **Version 2** for the Flow logs version.

7. Select **Storage Account-Configure**. From the drop down select the available storage account created earlier, then the **OK** button.



8. Select **On** to enable the traffic analytics status and set the interval to 10 minutes. Select the **Log Analytics Workspace** created earlier. Select **Save** at the top to confirm the settings.

Flow logs settings

Save Discard

Status

Off On

Flow Logs version

Version 1 Version 2

Version 1 logs ingress and egress IP traffic flows for both allowed and denied traffic. Version 2 provides additional throughput information (bytes and packets) per flow.
Learn more.

Storage account
networkdiagsa

Retention

NSG Flow logs data is stored indefinitely.
Learn more about deletion of old data

Traffic Analytics

Traffic Analytics provides rich analytics and visualization derived from NSG flow logs and other Azure resources' data. Drill through geo-map, easily figure out traffic hotspots and get insights into optimization possibilities.

Learn about all features

To use this feature, choose an Log Analytics workspace. To minimize data egress costs, we recommend that you choose a workspace in the same region your flow logs storage account is located. Network Performance Monitor solution will be installed on the workspace.
We also advise that you use the same workspace for all NSGs as much as possible. Additional meta-data is added to your flow logs data, to provide enhanced analytics.

Traffic Analytics status

Off On

Traffic Analytics processing interval

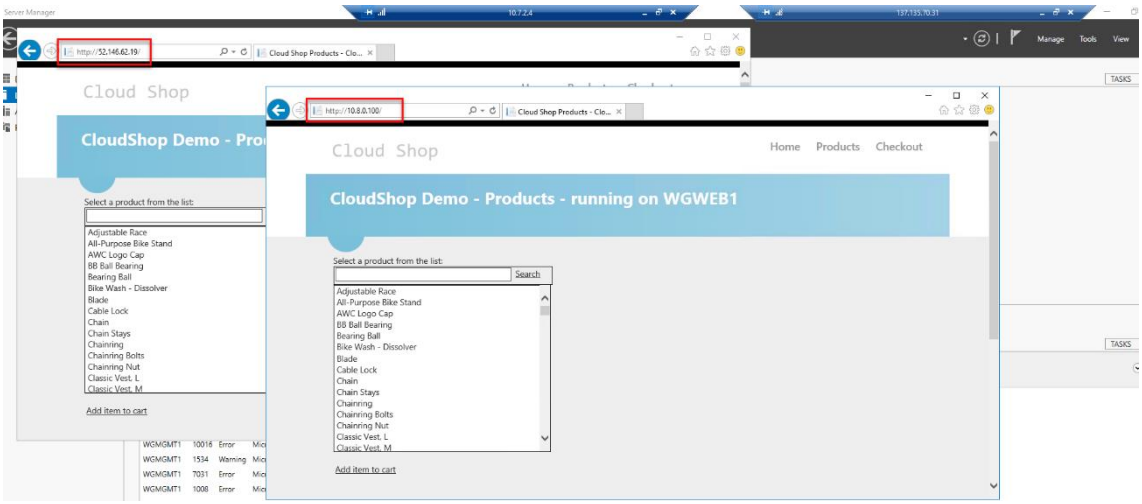
Every 10 mins

Log Analytics workspace
vnetdiagws

9. Repeat Steps 4 - 7 to enable the **OnPremVM-nsg** Network Security Group as well. When completed your configuration should show as the following image.

Name	Resource type	Resource group	Status
OnPremVM-nsg	Network security group	OnPremVNetRG	Enabled
WGAppNSG1	Network security group	WGVNetRG2	Enabled

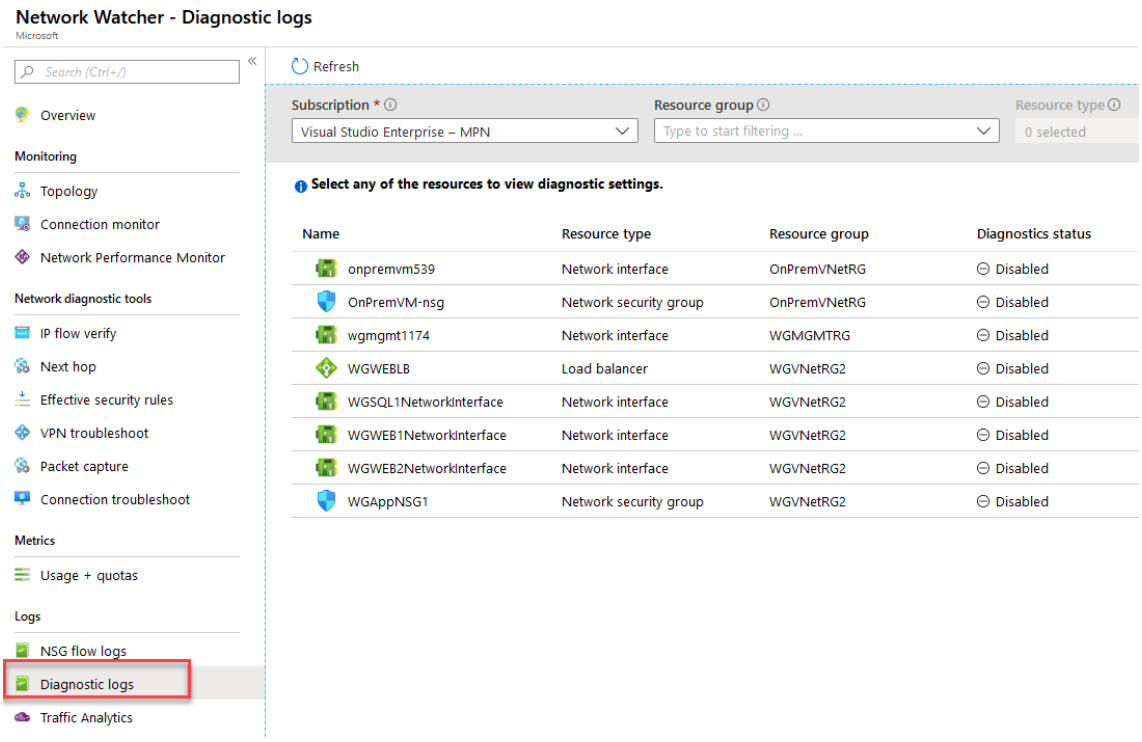
10. Navigate back to the **OnPremVM**. Connect to it by downloading and opening the RDP file. Then open another RDP connection to the **WGMGMT1** virtual machine within the connection to **OnPremVM**. In the RDP connection to **WGMGMT1**, navigate to the load balancer's private ip and generate some traffic by refreshing the browser. Allow ten minutes to pass for traffic analytics to generate.



Task 2: Configuring Diagnostic Logs

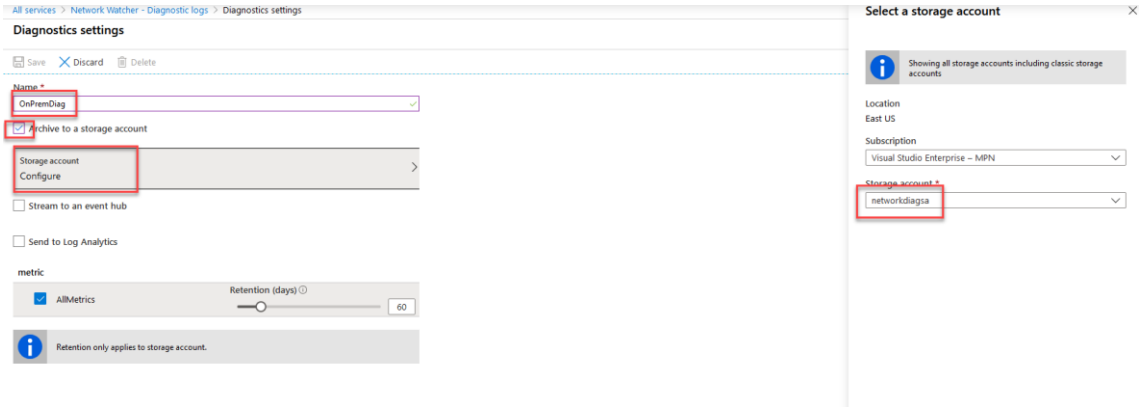
1. On the Azure portal, select **All services** at the left navigation. From the Categories menu select **Networking**, then **Network Watcher**,

2. Select **Diagnostic Logs** from the **Logs Menu** within the blade.

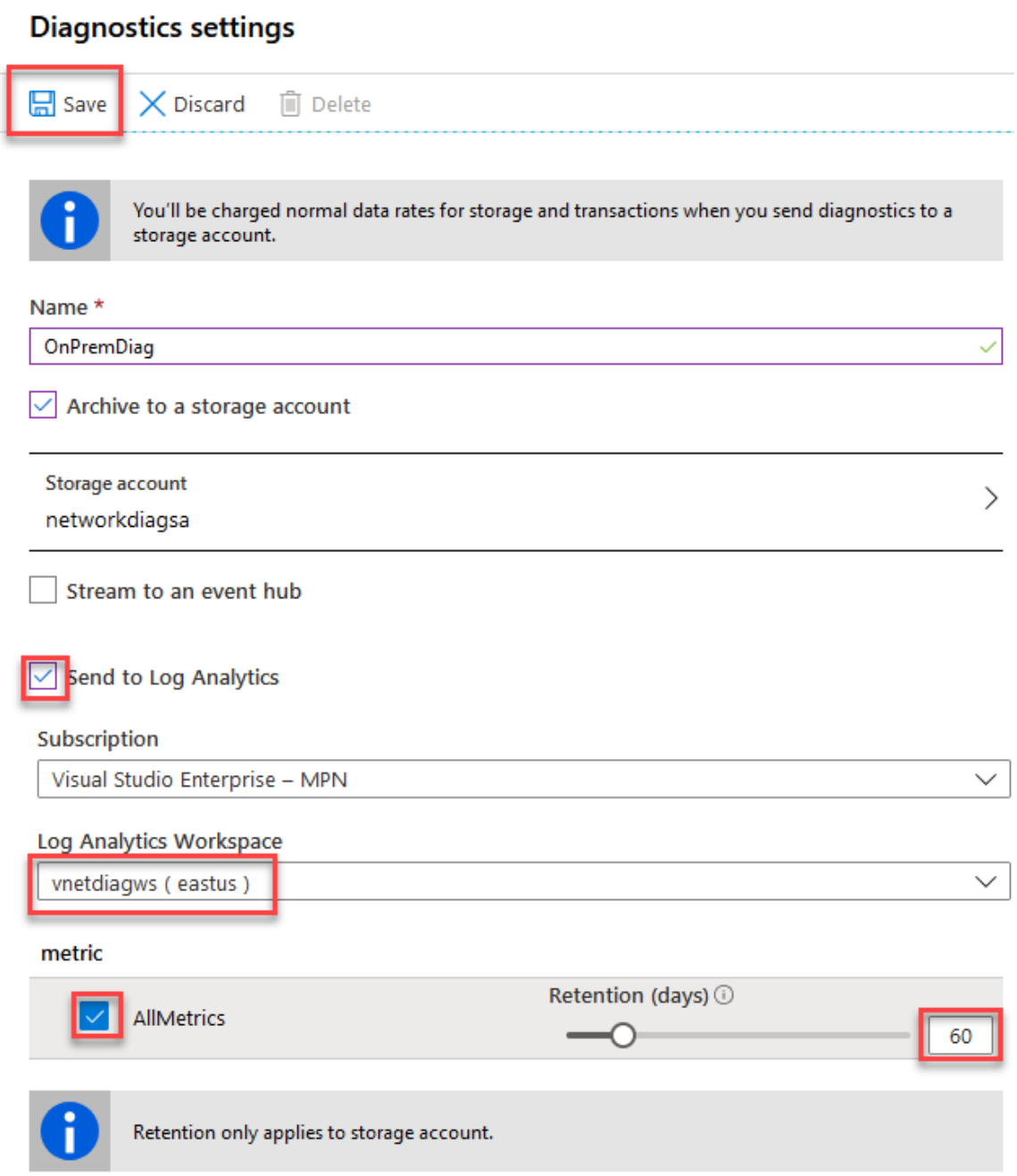


3. Select **onpremvm*NNN*** then select **+Add diagnostic setting**.

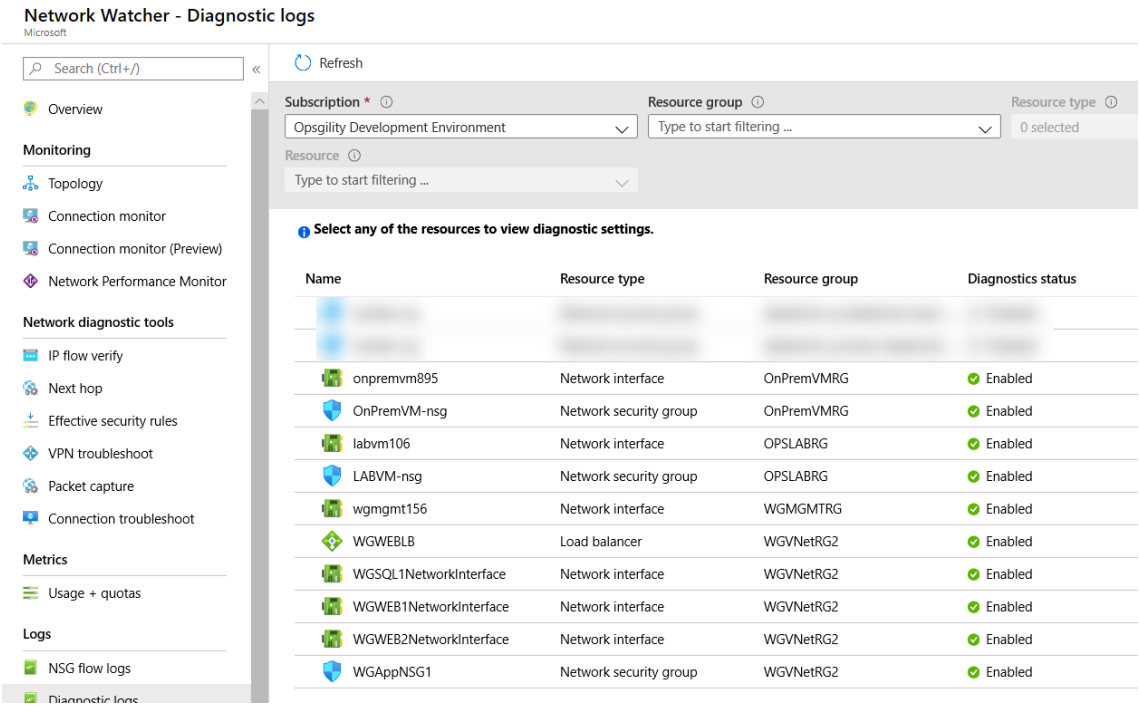
4. Enter **OnPremDiag** as the name then select the checkbox for **Archive to a storage account**. Select **Storage account** and from the drop down select the available storage account you created earlier. Select **OK**.



5. Select the **Send to Log Analytics** checkbox. Select the workspace created earlier. Select the **AllMetrics** checkbox and set the **Retention (days)** to **60**. Select the **Save** button to complete the settings.



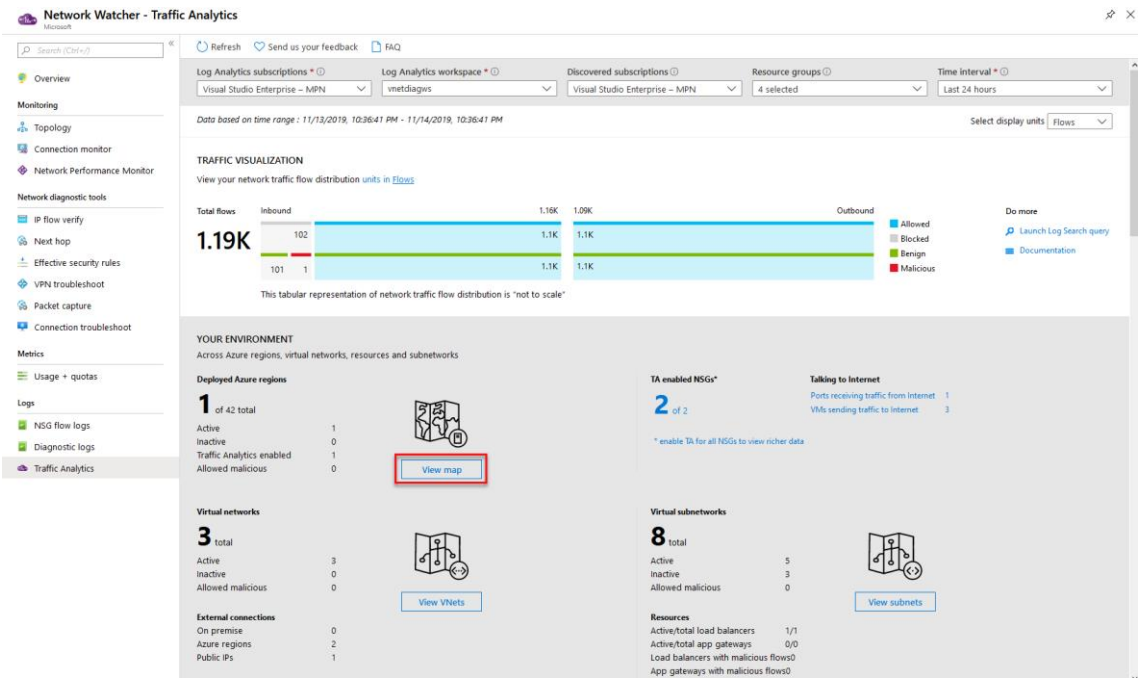
6. Repeat Steps 2 - 5 for each network resource. Once completed your settings will look like the following screenshot.



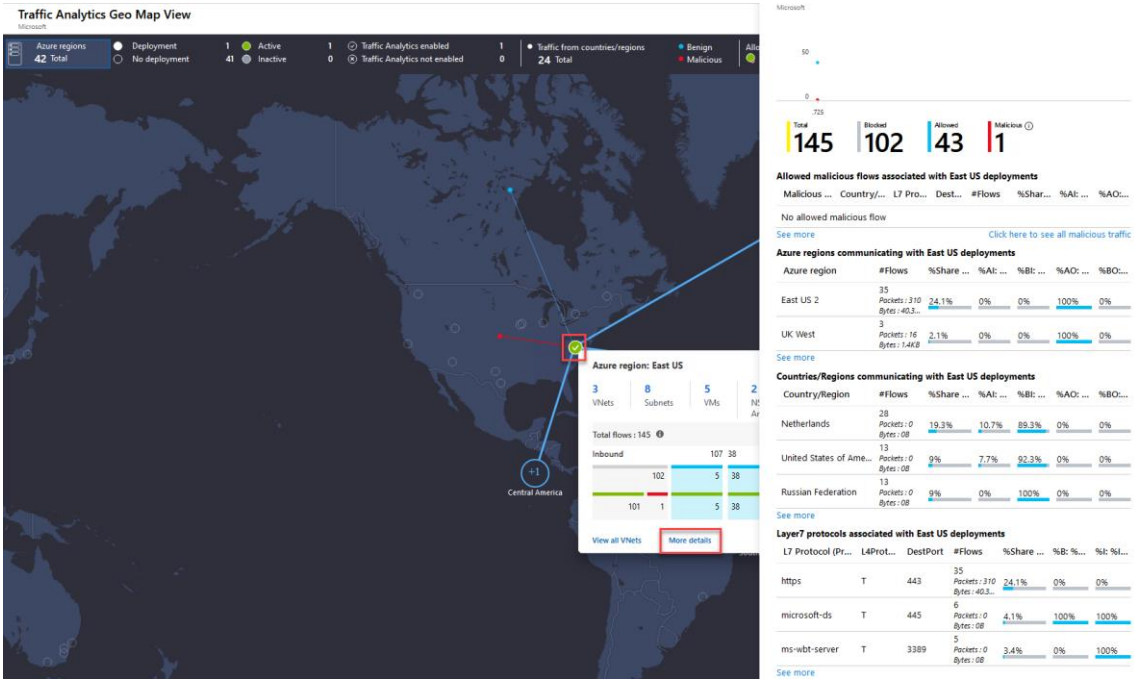
Task 3: Reviewing Network Traffic

1. On the Azure portal select **All services** at the left navigation. From the Categories menu select **Networking** then select **Network Watcher**.

2. Select **Traffic Analytics** from the **Logs** menu in the blade. At this time the diagnostic logs from the network resources have been ingested. Select **View map**.



3. Select the **green check mark** which identifies your network. Within the pop-up menu select **More Details** to propagate detailed information of the flow to and from your network.



Note: You can select the **See More** link to query the connections detail for more information.

Task 4: Network Connection Troubleshooting

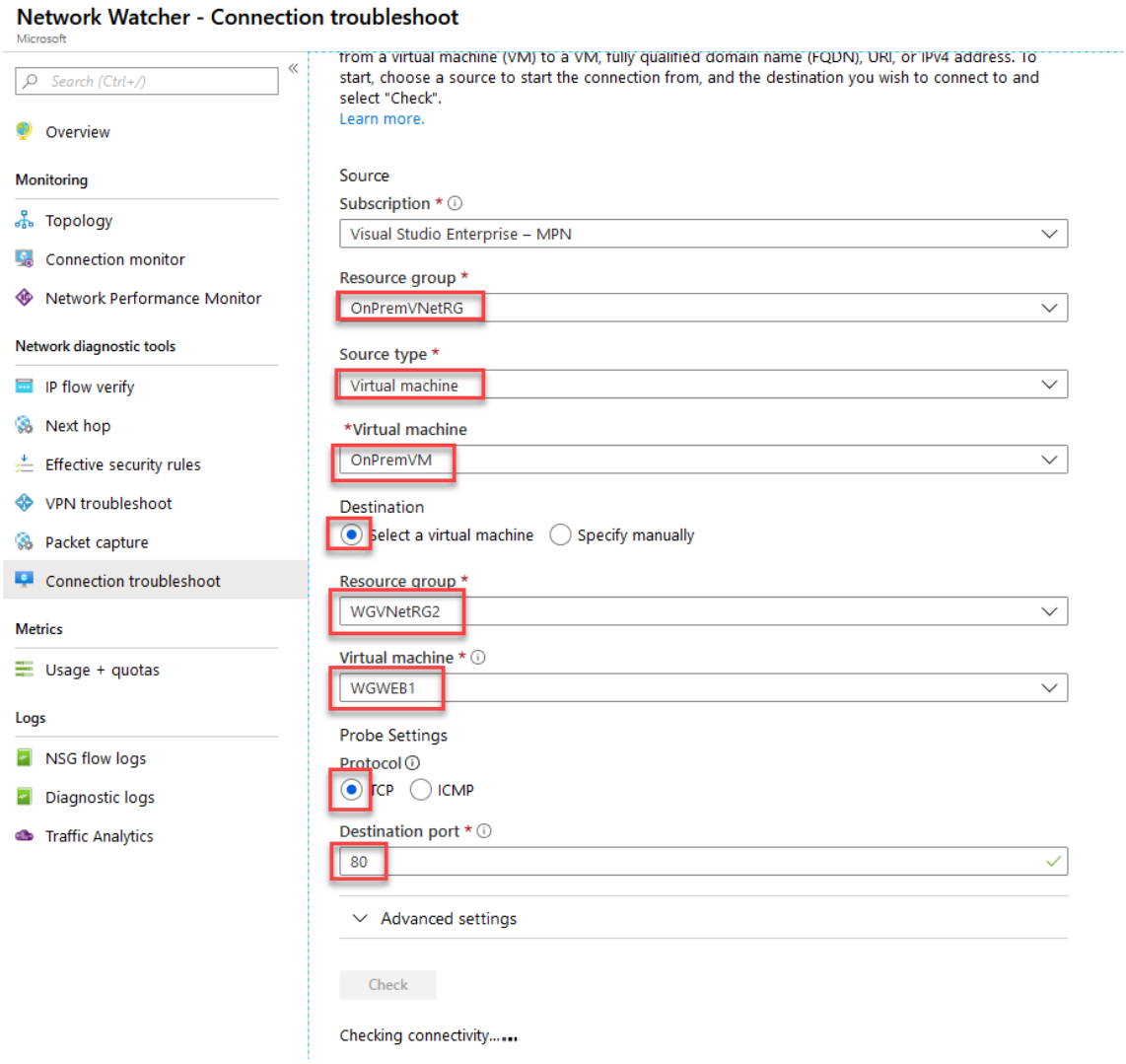
1. On the Azure portal select **All services** at the left navigation. From the Categories menu select **Networking** then select **Network Watcher**.

2. Select **Connection Troubleshoot** from the **Network Diagnostic tools** menu.

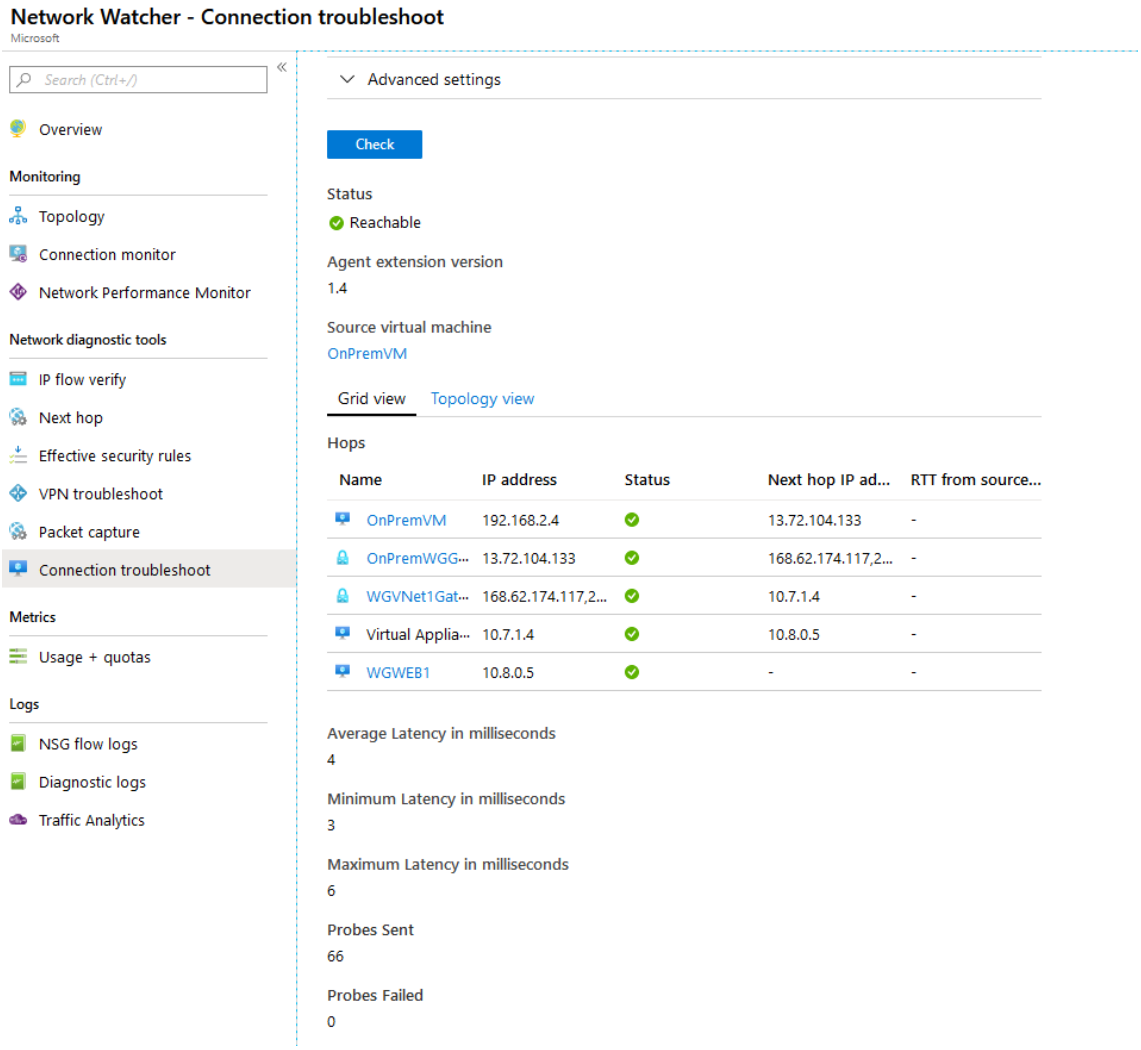
3. To troubleshoot a connection or to validate the route enter the following information and select **Check**:

    - Subscription: **Your Subscription**
    - Resource Group: **OnPremVMRG**
    - Source Type: **Virtual Machine**
    - Virtual Machine: **OnPremVM**
    - Destination: **Select a virtual machine**
    - Resource Group: **WGVNetRG2**

- Virtual Machine: **WGWEB1**
- Probe Settings: **TCP**
- Destination Port: **80**



4. Once the check is complete the connection troubleshoot feature will display a grid view on the name, IP Address Status and Next hop as seen in the following screenshot.



After the hands-on lab

Duration: 10 minutes

After you have successfully completed the Enterprise-class networking in Azure hands-on lab step-by-step, you will want to delete the Resource Groups. This will free up your subscription from future charges.

You should follow all steps provided *after* attending the Hands-on lab.