**AWS to Azure Connectivity**

**Pre-requisites**

**On Azure**

* Virtual network gateway
* Local network gateway
* Virtual network
* Windows 2019r2 (to test the connectivity)
* Make sure you disable the firewall on the instance that we create for the test.

**On AWS**

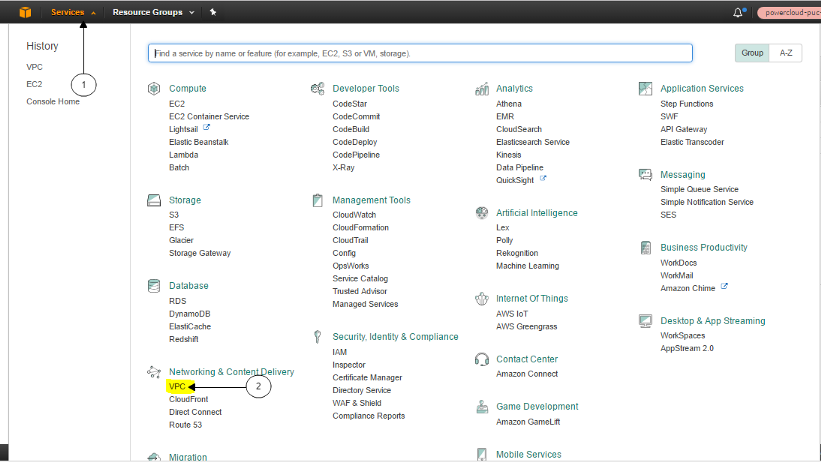
* VPC
* Windows Server 2019 R2
* Make sure to disable the firewall on the instance that we create for the test.

**Steps to configure AWS:**

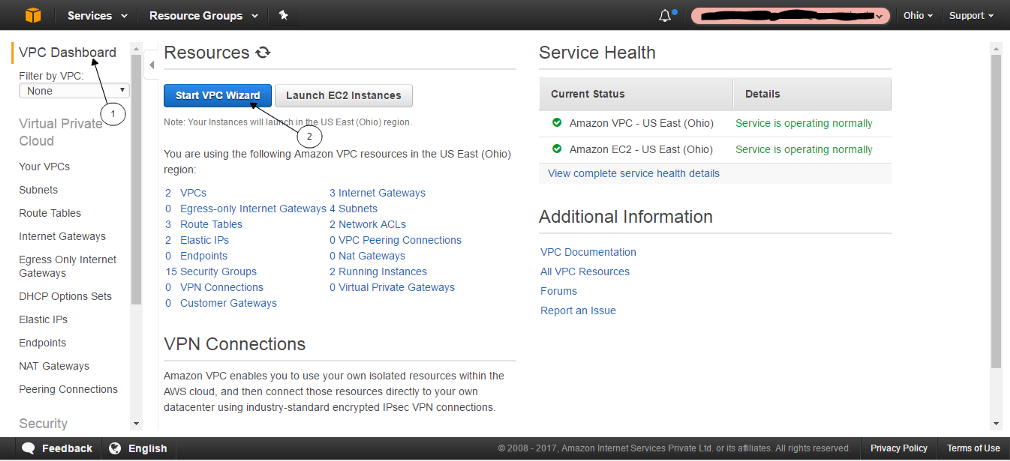
1. Let’s start with getting things configured on the AWS platform. First, let’s configure VPC with following details

* Name: AWS-Azure
* Address space: 10.0.0.0/16
* Subnet name: AWS-AZ-subnet
* CIDR: 10.0.0.0/24

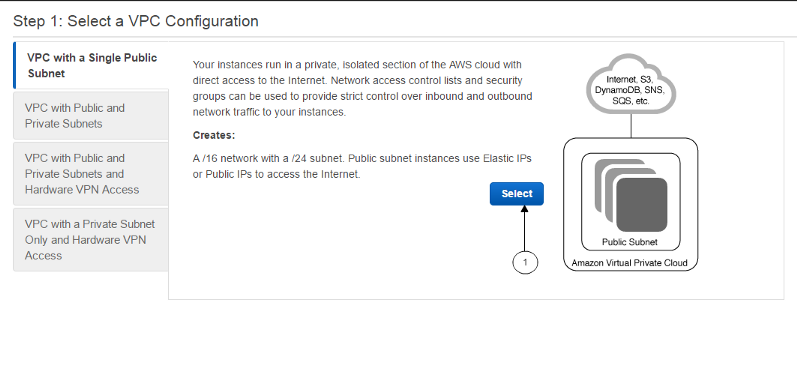
Login to AWS console and select services, under services, select VPC (marked in yellow)



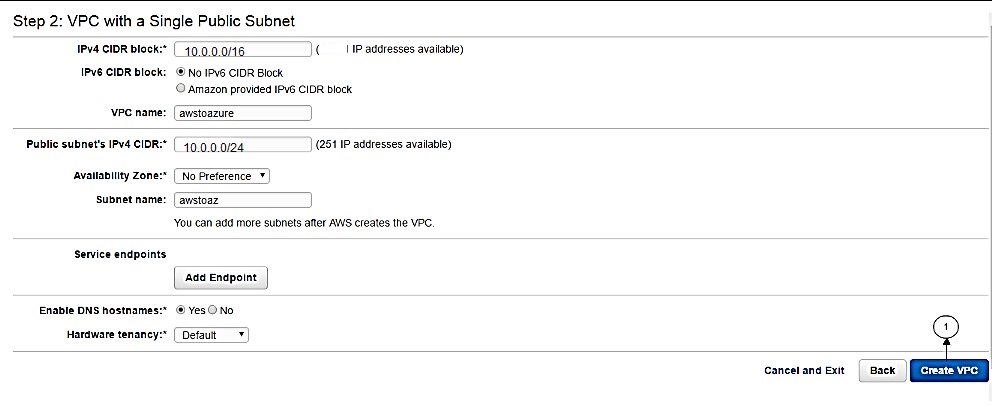
Select VPC Dashboard and then select start VPC Wizard



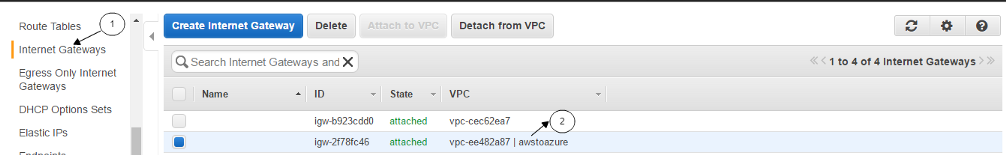
Select VPC with a Single Public Subnet



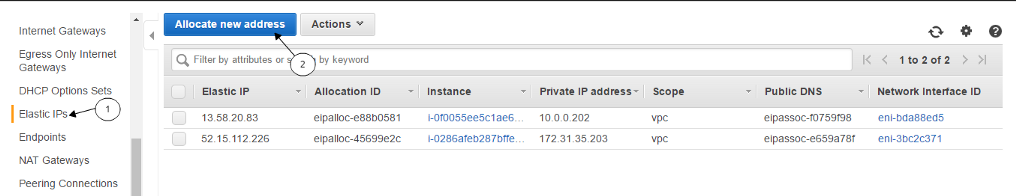
Fill in the address range and then click on Create VPC



Let’s ensure our VPC is connected to internet Gateway



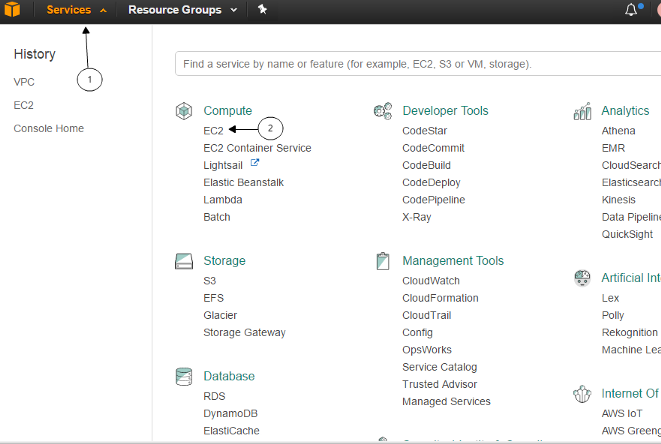
Once our VPC configured. Let’s allocate an elastic IP. In the VPC dashboard, click Elastic IPs, allocate New Address and click Yes, Allocate



Now we have a VPC configured and an Elastic IP ready. Next, we’ll deploy an EC2 instance.

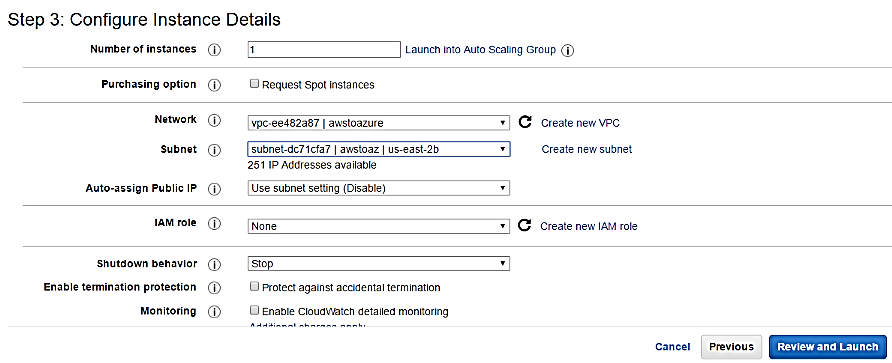
* A Windows Server 2019 R2 instance
* We have used t2.micro instance
* Ensure that Auto-assign Public IP is enabled.

To create an EC2 instance, Click on services and their select EC2 under Compute section



Select the required image, instance size as mentioned earlier

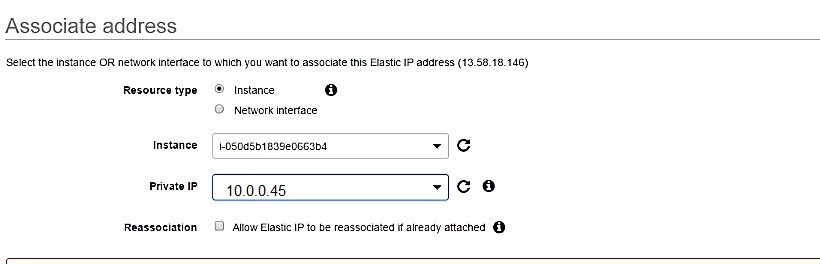
In the configuration, the section makes sure you select the correct VPC and subnet. Once done click on Review and launch.



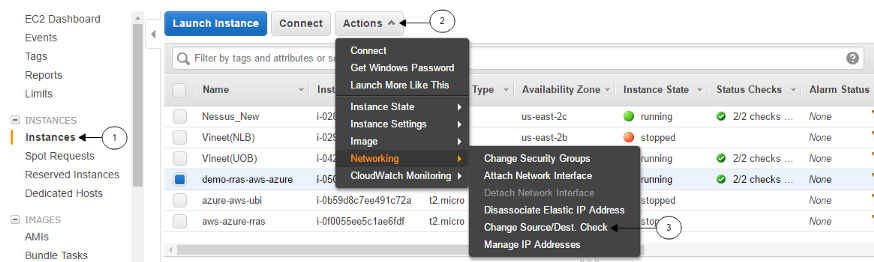
1. Once the instance is running associate the Elastic IP we created earlier to the Network interface of the instance. By clicking Elastic IPs in the VPC dashboard, selecting Associate Address in the actions menu, selecting the network interface used by the Windows Server 2019 R2 Datacentre instance we created earlier and click associate.

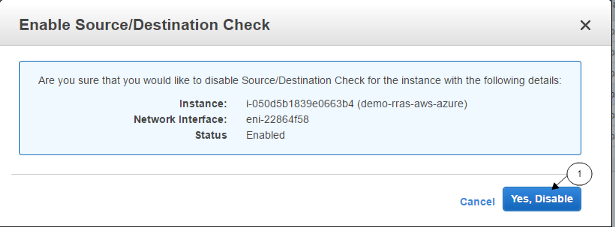


Fill in the following details and click on the associate.

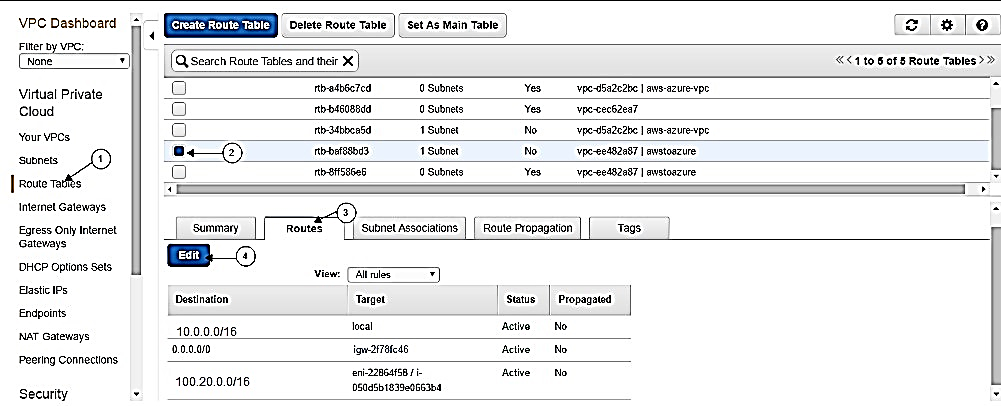


1. Next, let’s disable source/destination checking on the server. For not communication with other networks/internet which are not in the range.





1. Let’s add our Azure VNET address prefix in our RRAS server’s route table. This is to route the incoming traffic from the Azure network to AWS internal network.



Now we are good with the initial configuration on the AWS platform.

AZURE CONFIGURE:

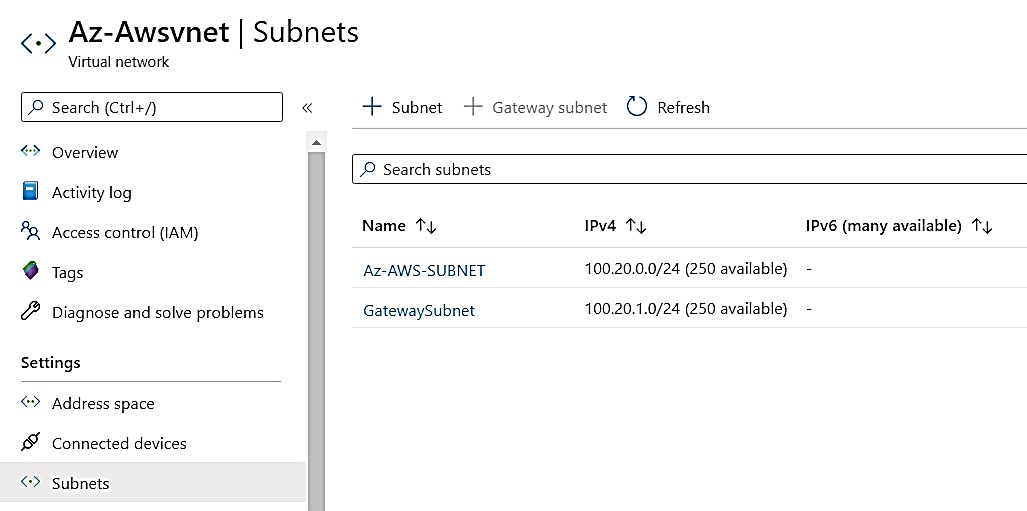
Let’s start with getting things configured on the Azure platform.

1. Let’s login to Azure subscription, let’s start with creating a resource group.

Vitual Network:

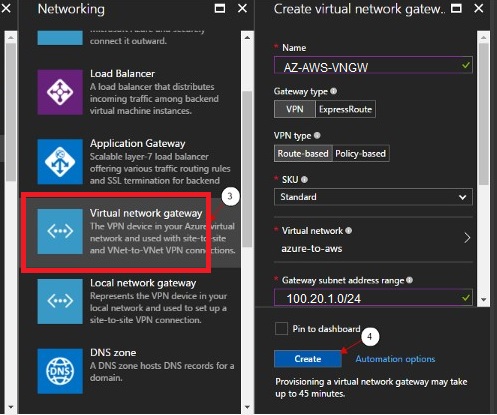
1. Next, we’ll create a virtual network with the following details

* Name: azure-to- AWS
* Address space : 100.20.0.0/16
* Subnet name: azure-AWS-sub
* CIDR: 100.20.0.0/24
* Subnet name: Gateway
* CIDR: 100.20.1.0/24
* Resource group: we created in the previous step



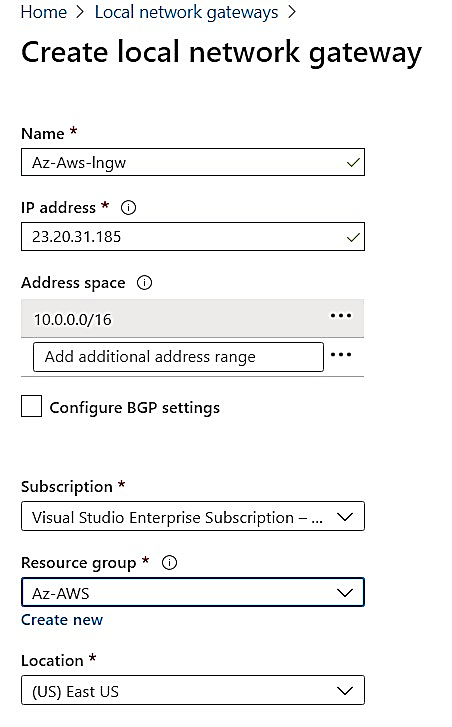
1. Now we have our virtual network ready. Let’s get started with configuring VPN on Azure. First, let’s start with configuring a virtual network gateway.

* Make sure you select the VNET that we created in the previous step.
* Make sure you select the resource group that we created at the beginning.
* For provisioning the virtual network gateway it would take approximately 30-45 minutes.



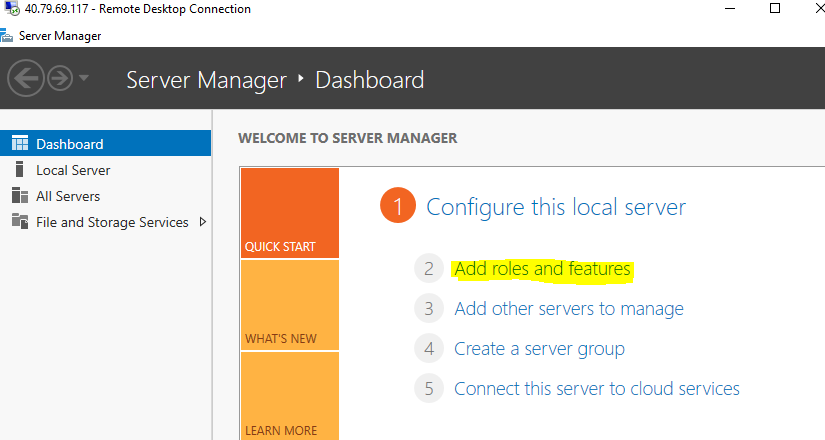
1. Since it takes time to create a virtual network gateway. Meanwhile, we can configure the local network gateway (here we define AWS address space and also the public IP of VPN server on AWS).

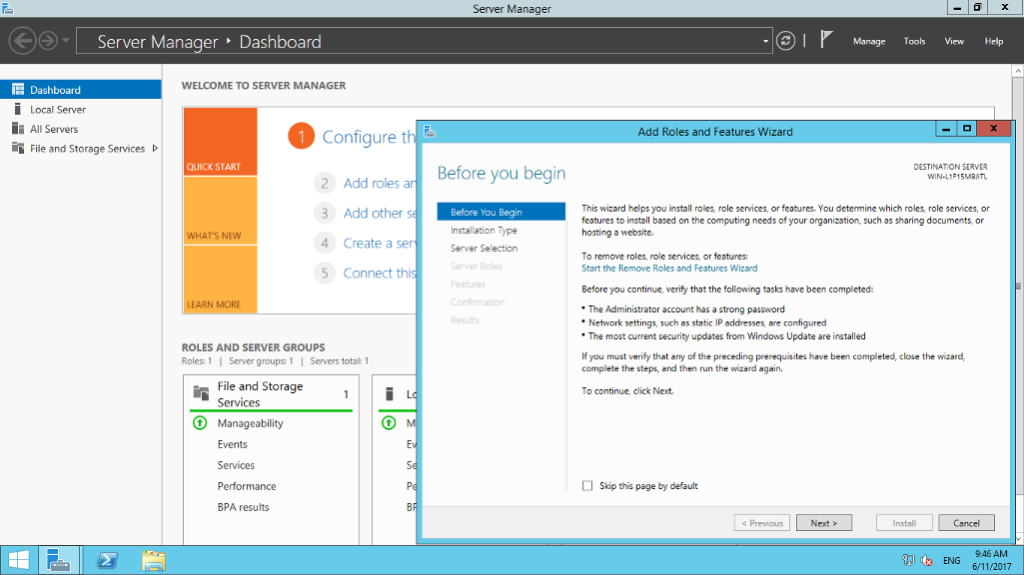
* Give the IP of the VPN server (RRAS configured server) on AWS.
* In address, space gives the VPC range of AWS.
* Use the same resource group.



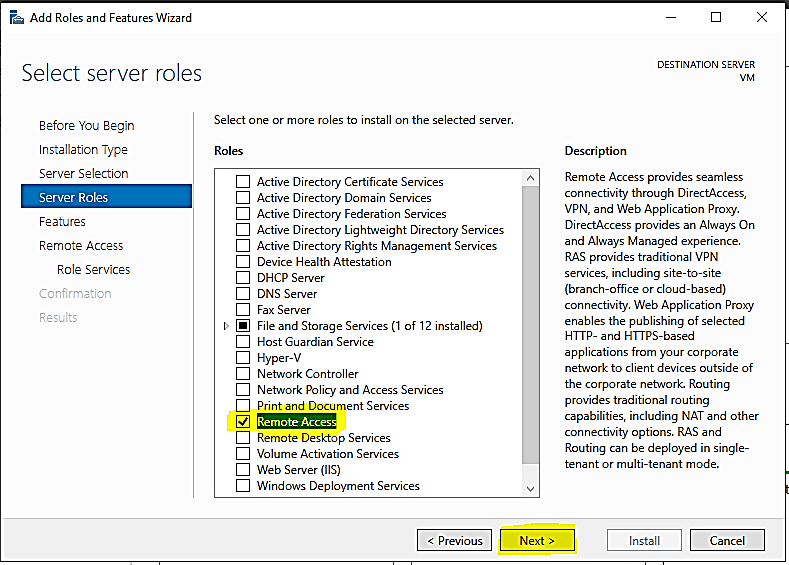
1. Let’s configure RRAS on the instance that we created in AWS (windows server 2019 R2 datacentre). Login to the server.

* Click on server manager
* Select the option Add roles and features. Add roles screen pops up click on next.

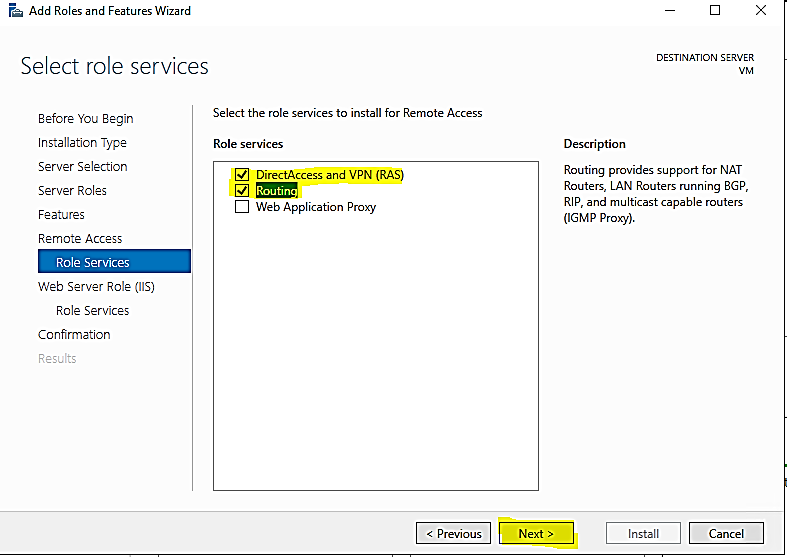


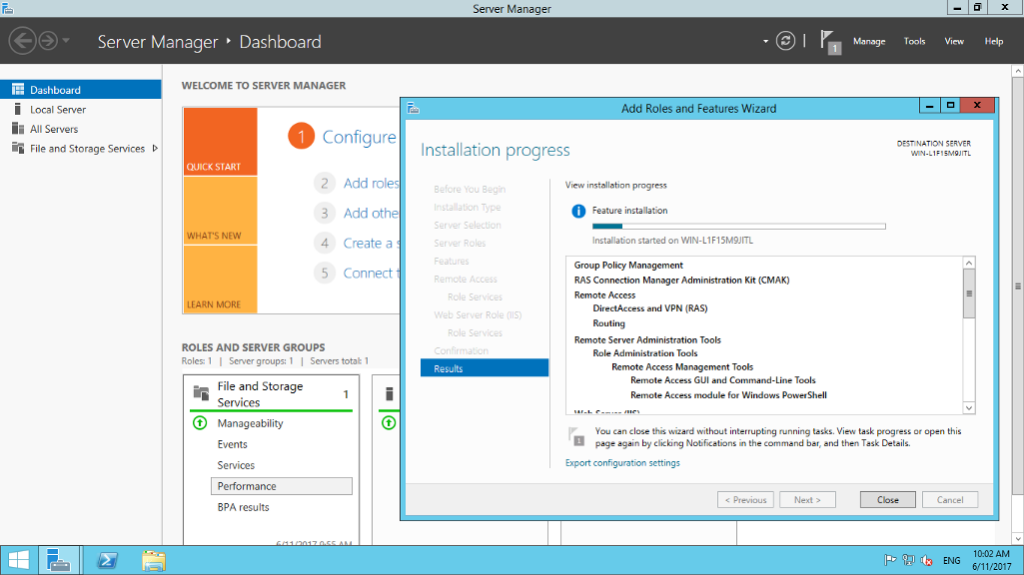


* Under Installation type and server, selection keeps the default settings and click on next. Under the server, roles select remote Access and click next.

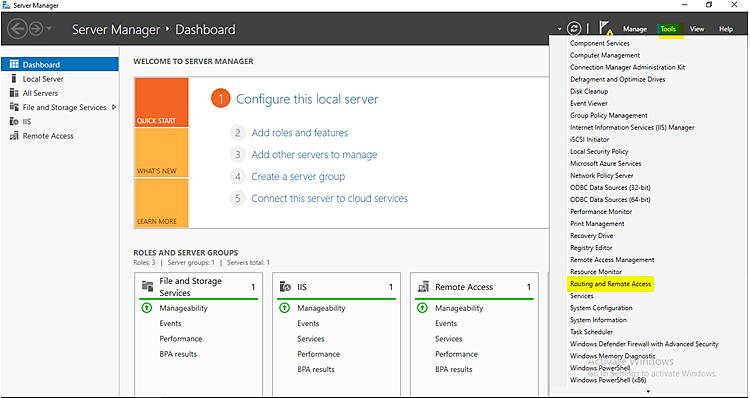


* Keep the default setting and click next until you get an option to select install. Click on install.

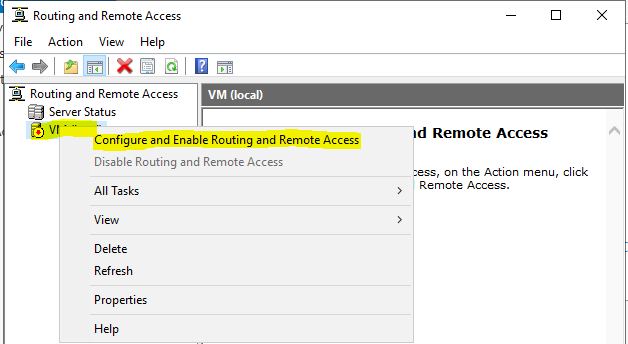




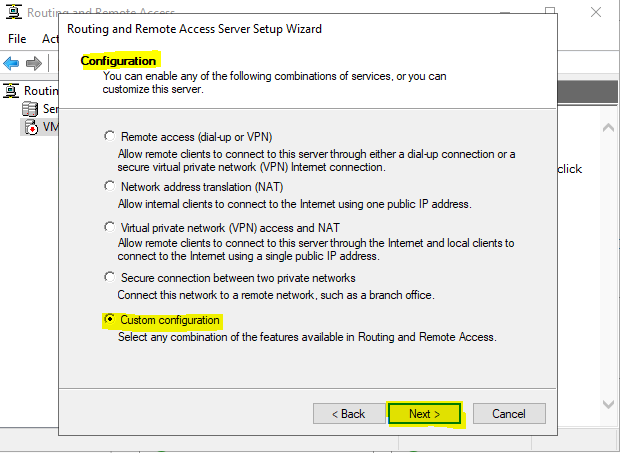
* Once the installation is completed. Open server manager and then select a remote access option on the left-hand side. Next right click on the server and then select remote access management. This redirects us to the RRAS configuration panel.



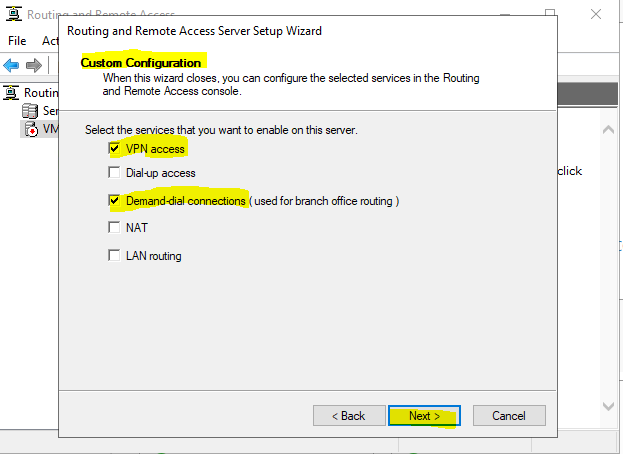
* Click on Direct Access and VPN and then click on Run the Getting Started Wizard. A wizard pops up and then select the last option Deploy VPN only.
* Routing and Remote access pane opens. Right-click on the server and then select Configure and Enable Routing and Remote access.



* Click next. Under configuration select custom configuration and click next.

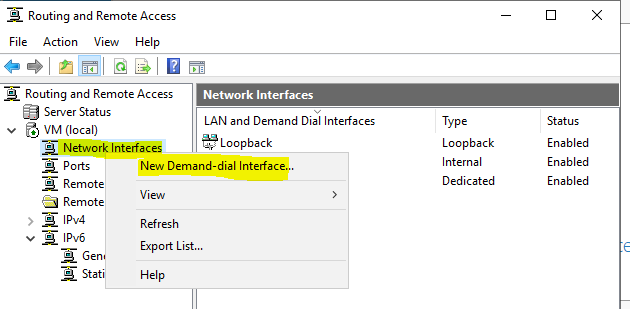


* Under custom configuration, select VPN access. And then click on finish.

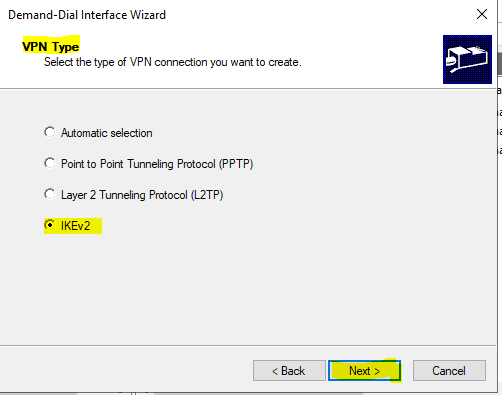


Click on Start Service.

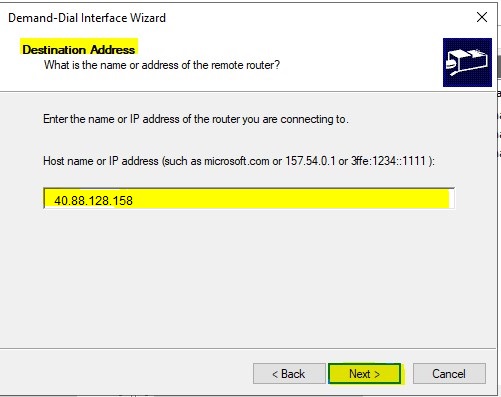
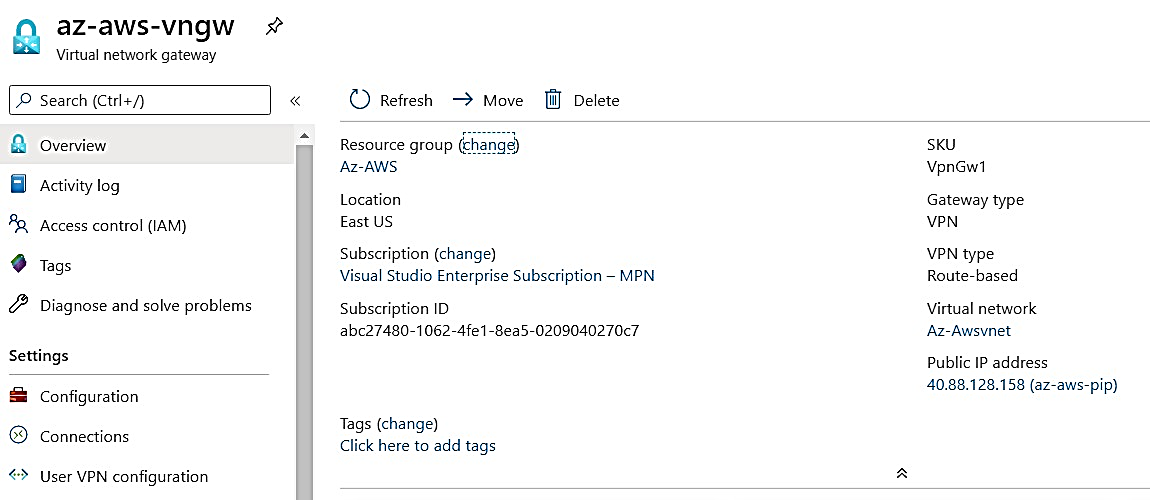
* Now we have our RRAS installed. Let’s add our azure IP to be allowed. For that right-click on Network interface and the select first option. A wizard pops up. Click on next



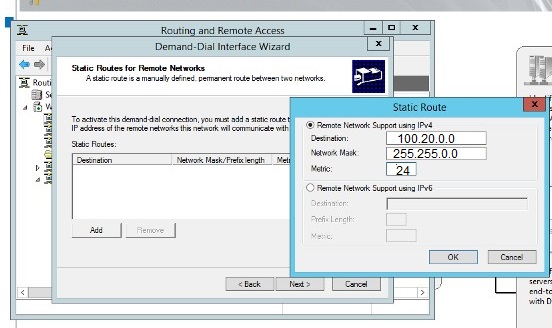
* Enter Interface Name Site-Site-interface
* Under VPN type select the IKEv2 option and click next.



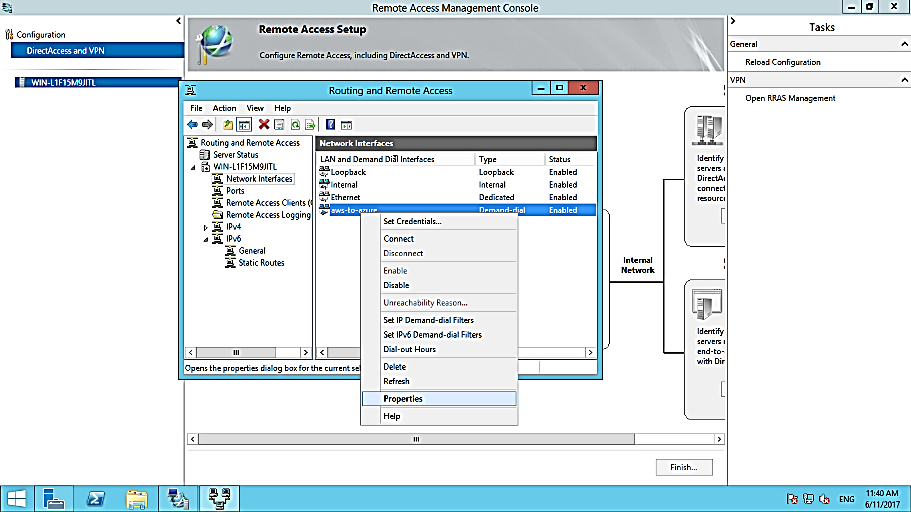
* Under destination address give the Azure gateway IP address and click next. Under protocol and security keep the default setting and click next.



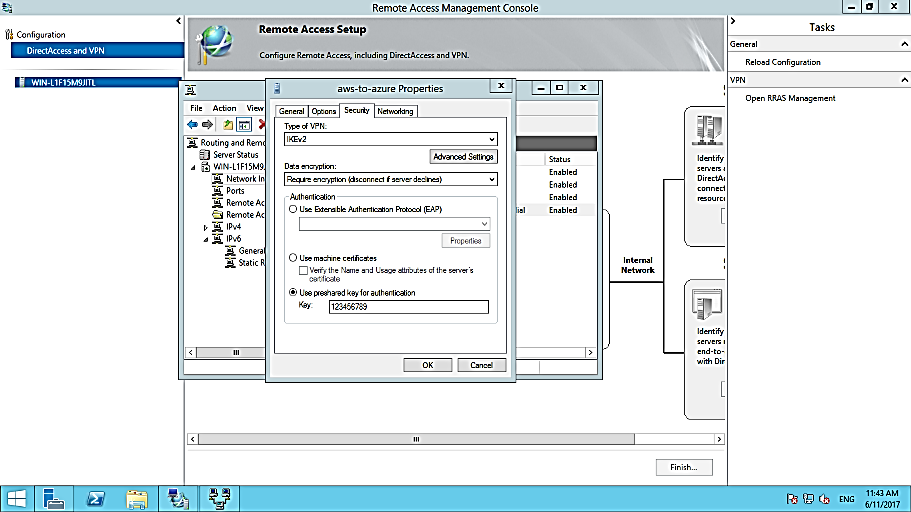
* Under static route for remote network add the Azure VNET address prefix. And then click on next. And then keep the rest of them with the default configuration.



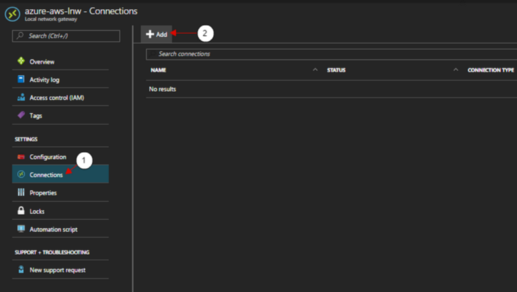
* Now right click on the created network interface and then select properties.



* Next select security option on tab, there on bottom of the screen select the option pre-shared key and give a pre-shared key and click ok.

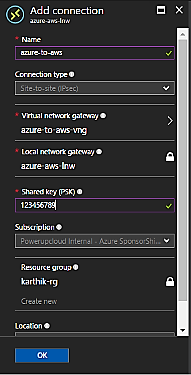


1. Now we have our RRAS server that acts as a VPN on AWS. Lest go to Azure subscription and establish the connection. Login to Azure subscription. Get into your resource group and there select Local Network Gateway that we had configured in our previous step.
2. Under the local network gateway, select Connections on the left-hand pane and there select add to add the connection.

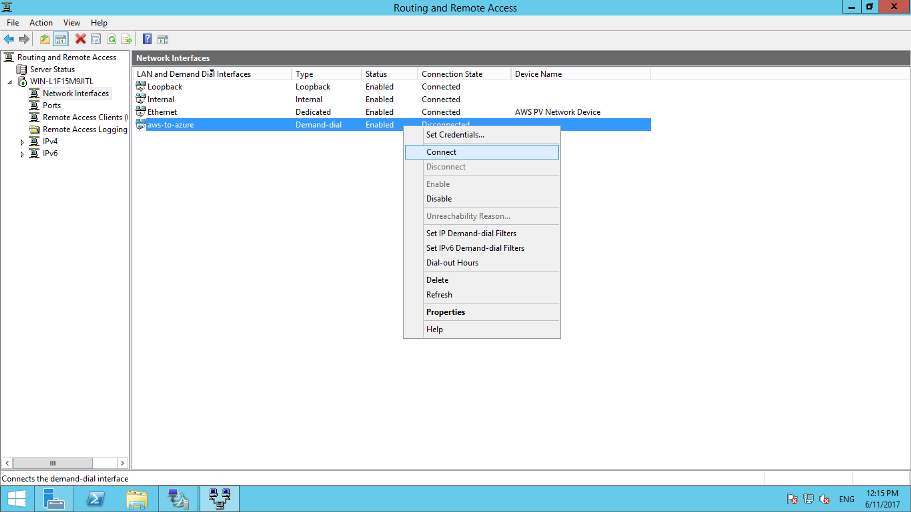


1. Now add in the following configuration

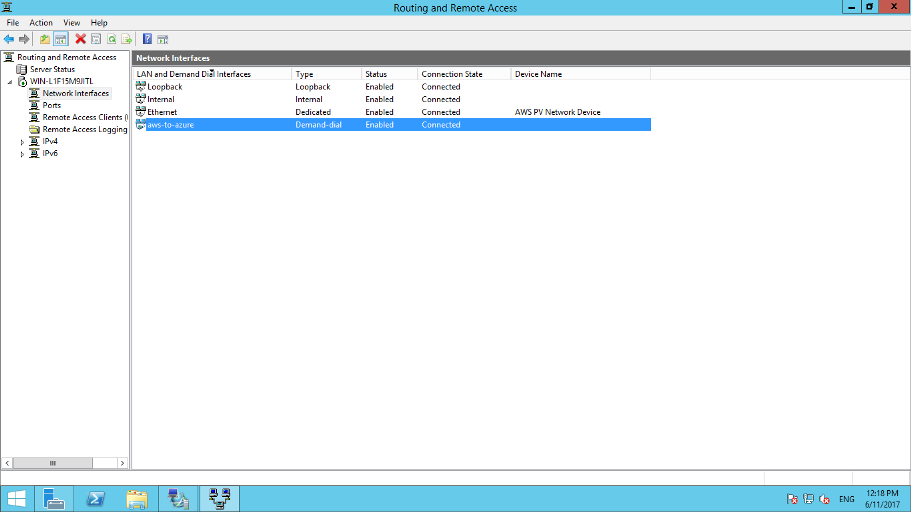
* Select the virtual network gateway that we created before.
* Make sure you give the same pre-shared key that we had given on the RRAS server present on the AWS platform.



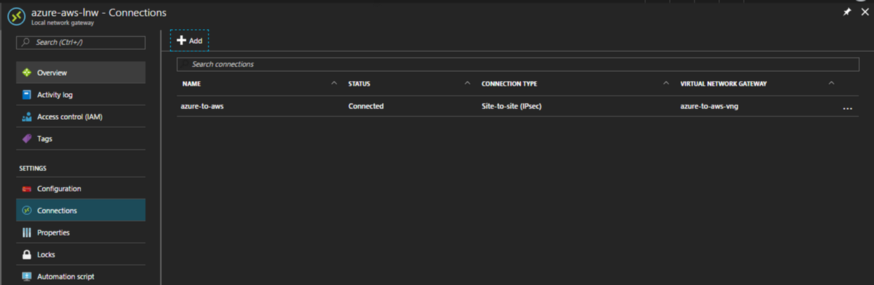
1. Now let’s Login to the RRAS server on AWS end and let’s establish a VPN. In the RRAS server right click on a network interface that we created “AWS-AZinterface” earlier and then select connect option.



Now let’s check the VPN status, we have our VPN connection status connected from AWS end.

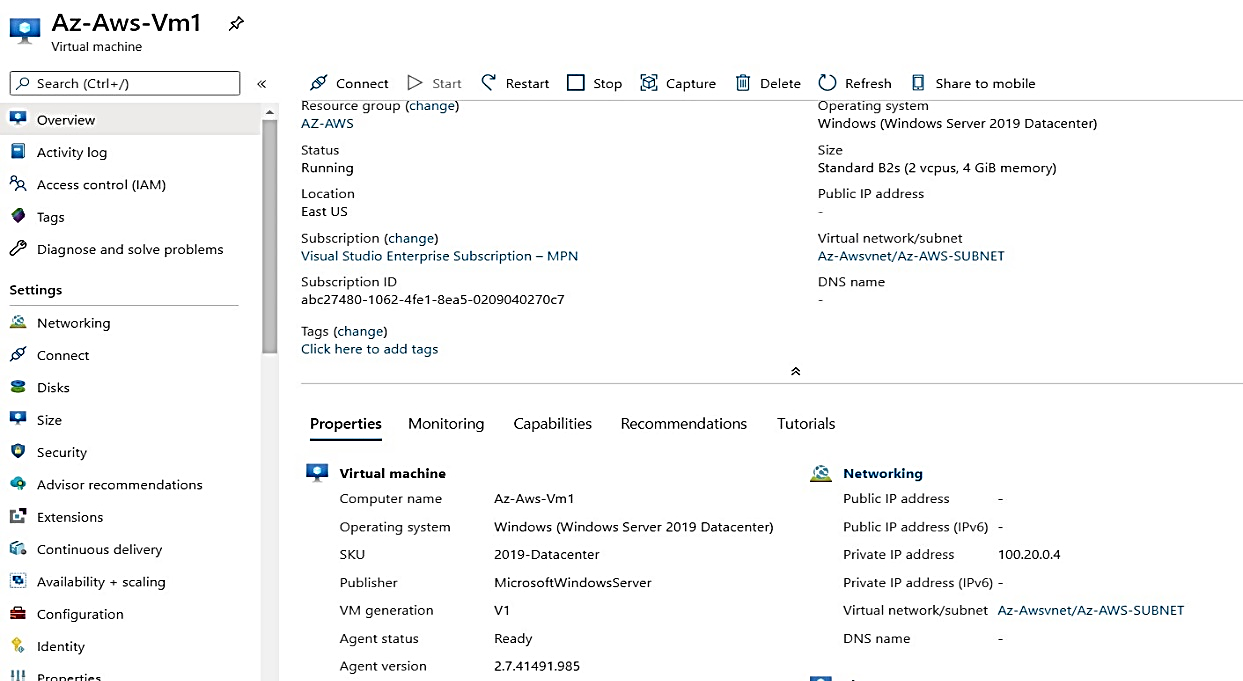


Let’s check the connection from Azure end and we have status showing From Azure end as well.

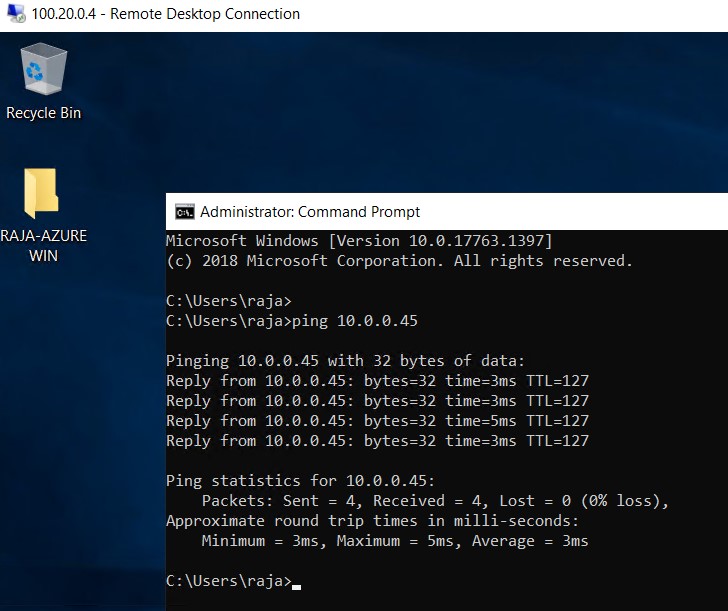


Let’s deploy the VM’s on the AWS platform and also on Azure platform and then we’ll try to ping from both the end using their private IPs.

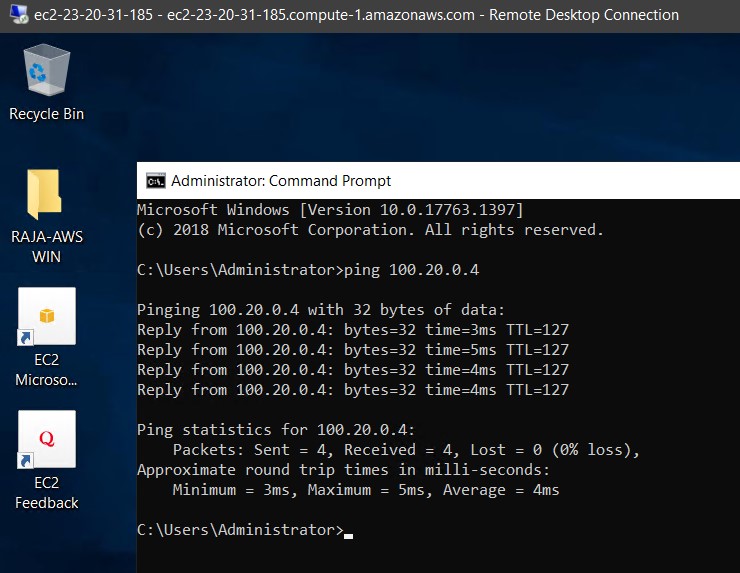
* We have an Azure Instance with IP: 100.20.0.4 (Win2019)
* We have an AWS Instance with IP: 10.0.0.45 (Win2019) Public IP: 23.20.31.185
* Turn OFF IE Enhancement Settings in Local Server in both machines
* Turn OFF Windows Firewall in Both Machines.



Now let’s try to ping AWS instance from Azure instance with private IP. We are able to ping.



Now let’s try to ping Azure instance from AWS instance with private IP. We are able to ping.

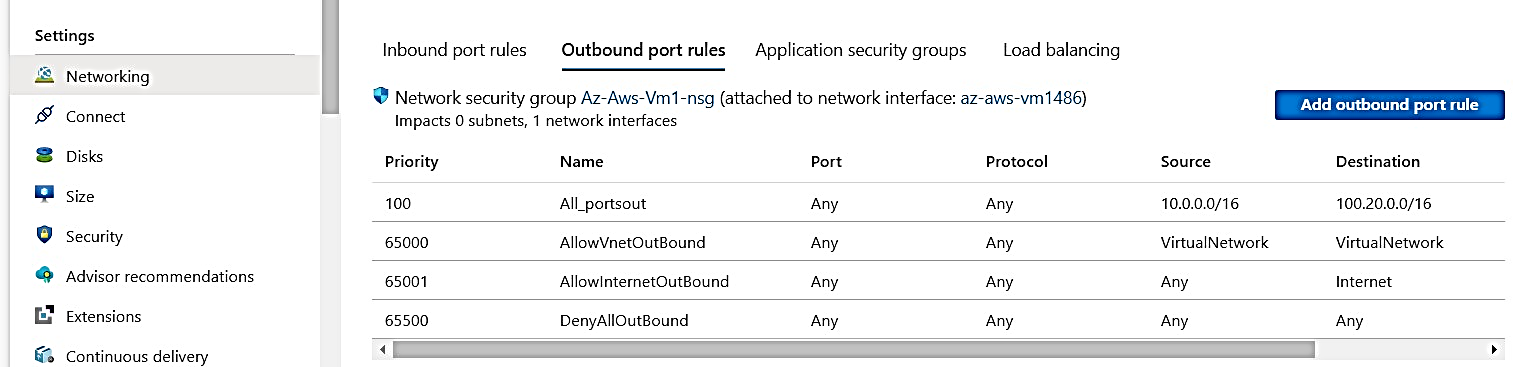
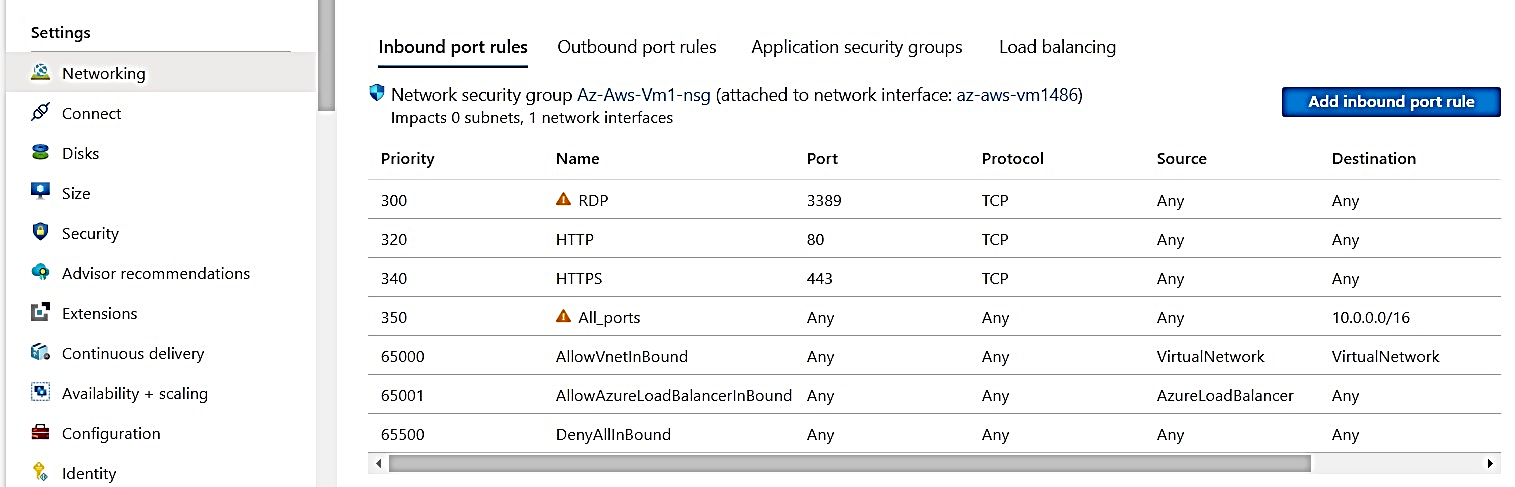


Hope you found it useful!

**Troble Shooting:**

If ping reply is not working then check with Security group of AWS and NSG Of Azure.

Add In-bound and Out-Bound rules for both.



END of the Site to site from AWS to AZURE CONNECTIVITY.

For More information

<https://www.powerupcloud.com/connecting-clouds-aws-to-azure-site-to-site-vpn-step-by-step/>

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>