DVS Technologies

Dvs Technologies Azure adminstration

Compiled and Scrutinized by
Mr. Shaan Shaik
(Senior DevOps Lead)

Words To The Students

Though we have taken utmost efforts to present you this book error free, but still it may contain some errors or mistakes. Students are encouraged to bring, if there are any mistakes or errors in this document to our notice. So that it may be rectified in the next edition of this document.

"Suppressing your doubts is Hindering your growth".

We urge you to work hard and make use of the facilities we are providing to you, because there is no substitute for hard work. We wish you all the best for your future.

"The grass isn't greener on the other side; the grass is greener where you water it."

You and your suggestions are valuable to us; Help us to serve you better. In case of any suggestions, grievance, or complaints, please feel free to write us your suggestions, grievance and feedback on the following

Dvs.training@gmail.com

DVS Technologies

1 Point to Site VPN

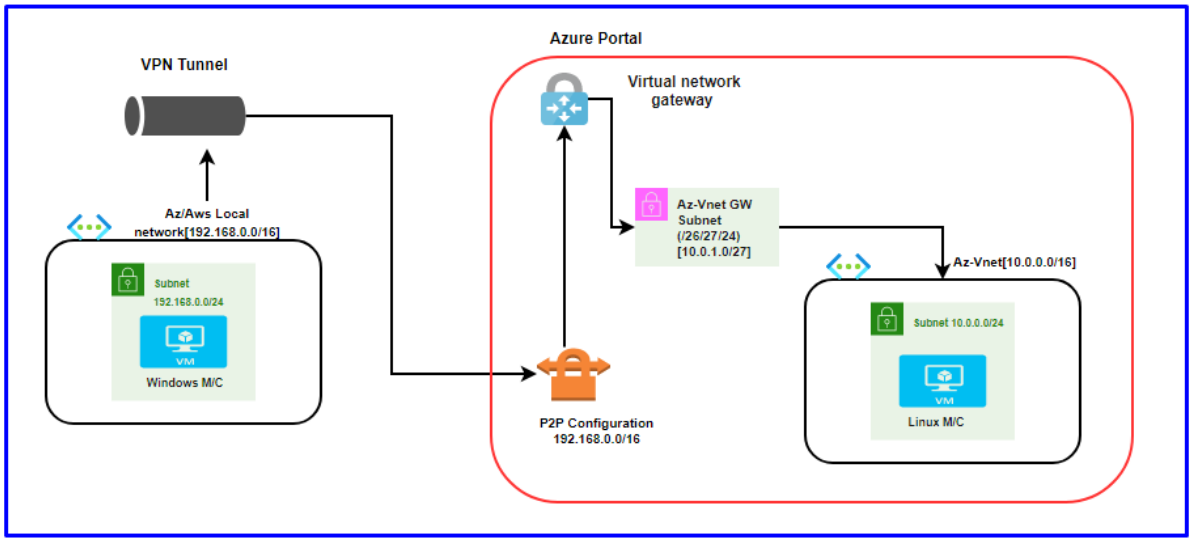
VPN help you to connect to your azure network in a secure manner without use of internet.

We have two ways of implementing this

Point to site vpn
Site to site vpn connection

Point to site we use it for small number of connections but if you feel you want to connect your entire company then you can use site to site vpn connection

1 Point to Site VPN Connection:



In this we are going to create one VNET & spin up one server with default subnet our main goal is to access this server from our laptop or our own machine

Whenever we are going to create VPN we have to make sure that we are giving separate subnet called "gateway subnet" for our VPN without which it will not work.

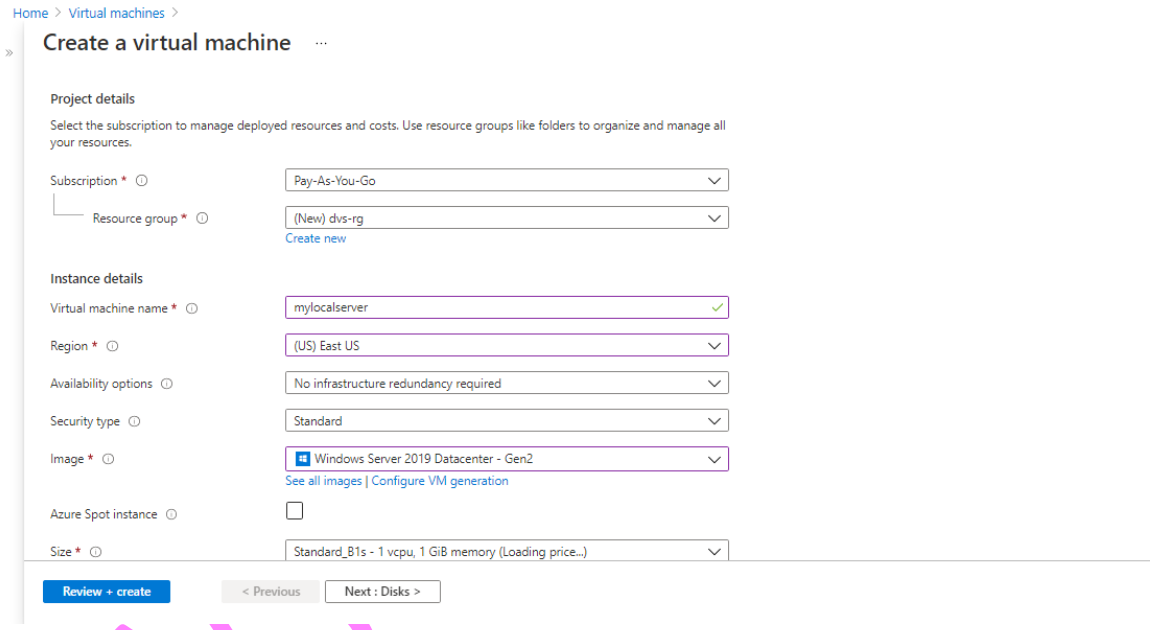
You can /26,/29, or /27 subnets for our VPN subnet (It's recommended to use not mandatory)

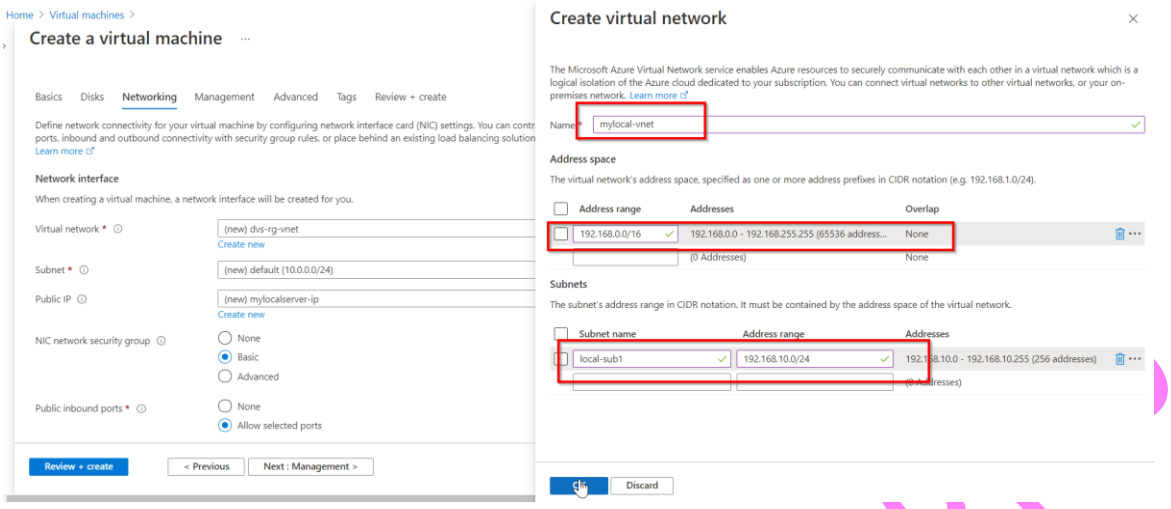
Once you are done with VPN gateway subnet creation you have to create virtual network gateway to consume the configuration

Since we don't have laptop or other windows server we are going to create two servers one from one VNET & other from other VNET.

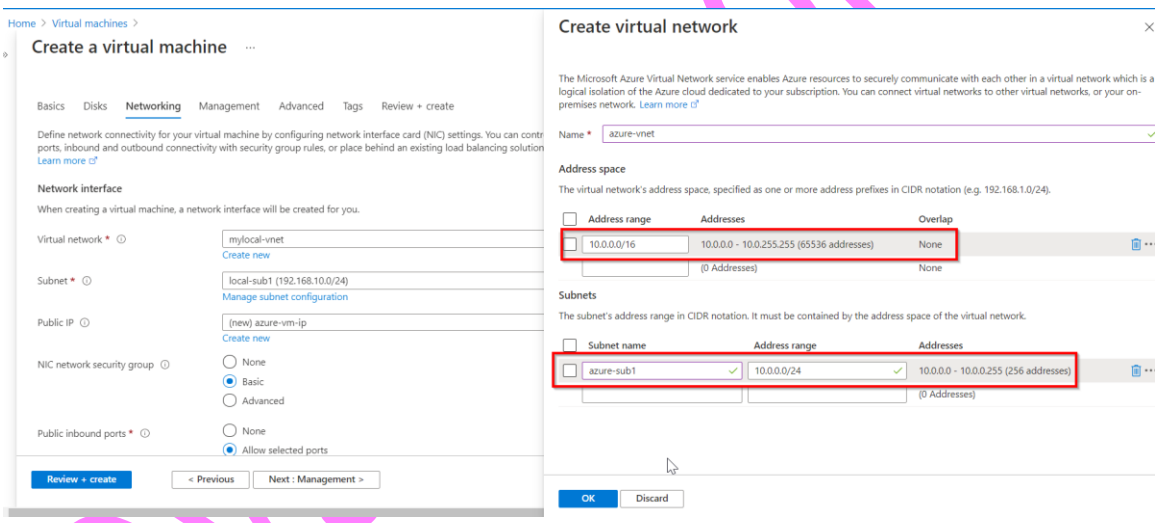
Vnet1 --> Azure network
Vnet2 --> my network

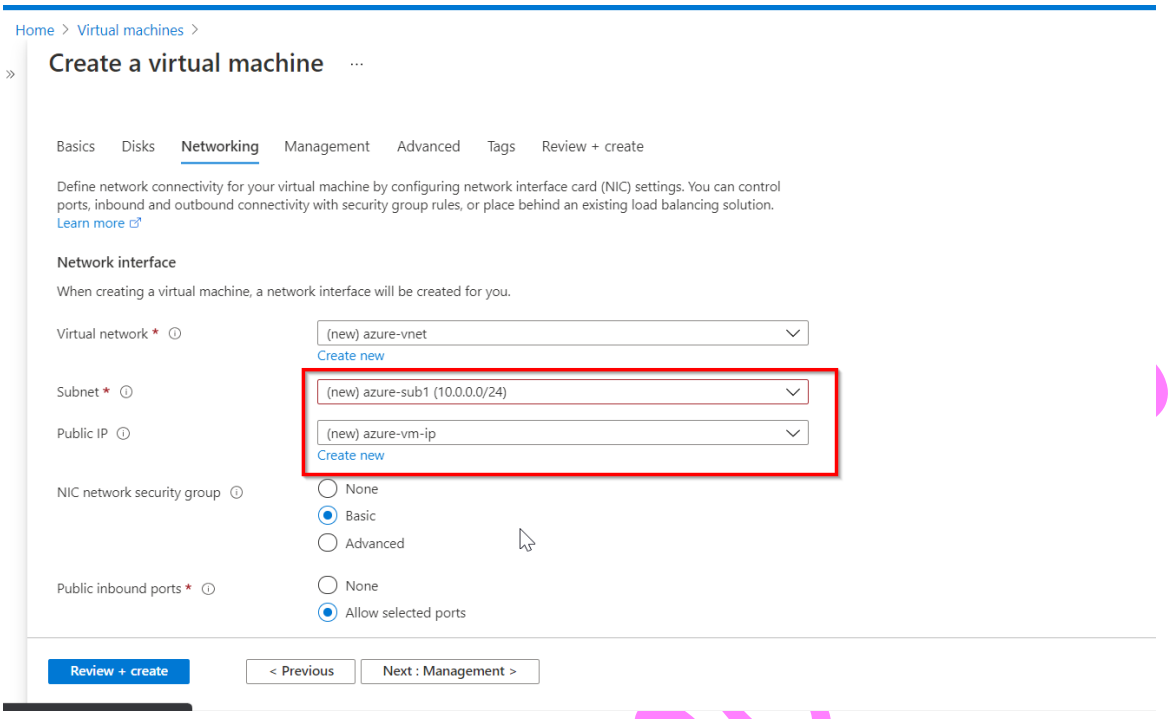
Let's build our local server:
NOTE: Let's take the windows server





Now let's create one more server with other network let's say azure-network and will install apache in that server



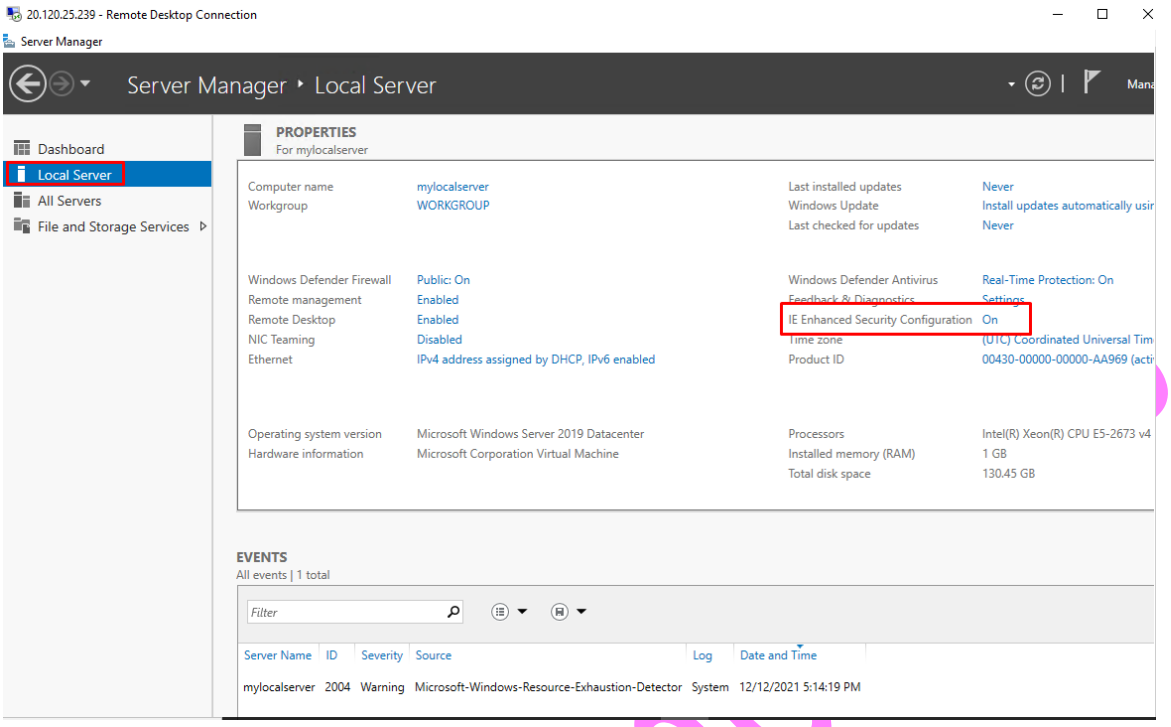


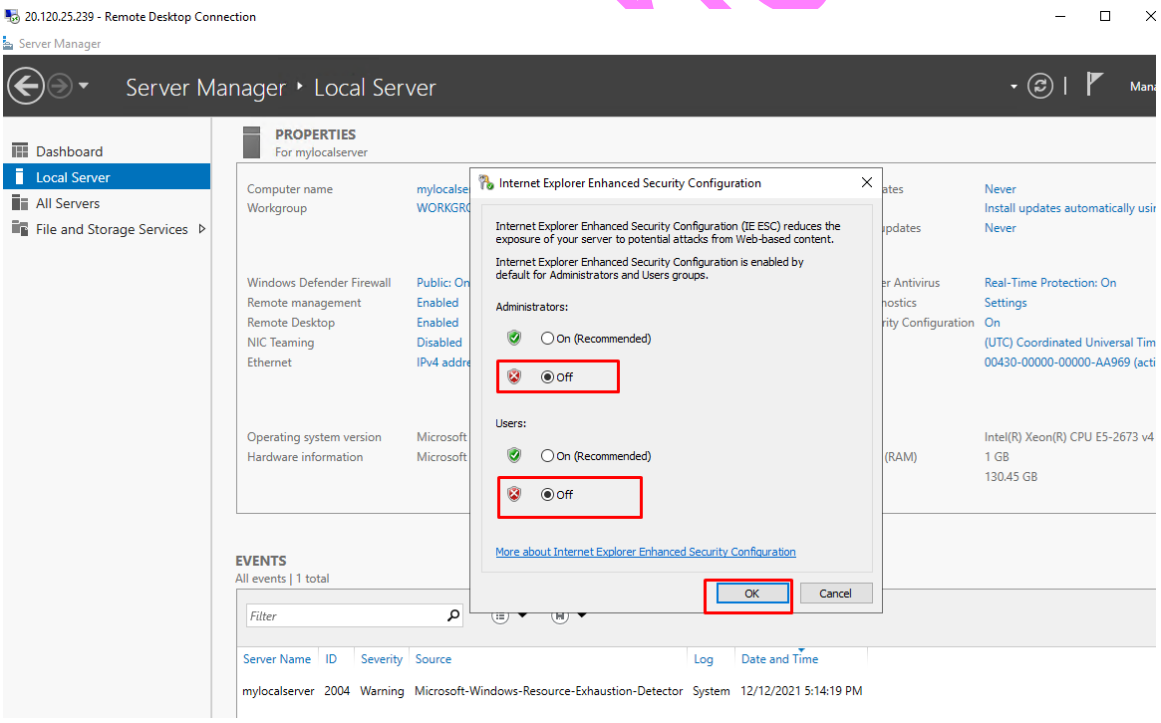
Note: use customer data for configuring the application

```
#!/bin/bash
yum install httpd -y
systemctl enable httpd
echo "Hi I am from apache server" > /var/www/html/index.html
systemctl restart httpd
```

Let's try to login to our server and try to check the application status using public ipaddress & then with private ipaddress

DVS Technologies


20.120.25.239 - Remote Desktop Connection
Server Manager
Server Manager ‣ Local Server
Dashboard
Local Server
All Servers
File and Storage Services
PROPERTIES
For mylocalserver
Computer name mylocalserver
Workgroup WORKGROUP
Last installed updates Never
Windows Update Install updates automatically usir
Last checked for updates Never
Windows Defender Firewall Public: On
Remote management Enabled
Remote Desktop Enabled
NIC Teaming Disabled
Ethernet IPv4 address assigned by DHCP, IPv6 enabled
Windows Defender Antivirus Real-Time Protection: On
Feedback & Diagnostics Settings
IE Enhanced Security Configuration On
Time zone (UTC) Coordinated Universal Tim
Product ID 00430-00000-00000-AA969 (acti
Operating system version Microsoft Windows Server 2019 Datacenter
Hardware information Microsoft Corporation Virtual Machine
Processors Intel(R) Xeon(R) CPU E5-2673 v4
Installed memory (RAM) 1 GB
Total disk space 130.45 GB
EVENTS
All events | 1 total
Filter
Server Name ID Severity Source Log Date and Time
mylocalserver 2004 Warning Microsoft-Windows-Resource-Exhaustion-Detector System 12/12/2021 5:14:19 PM

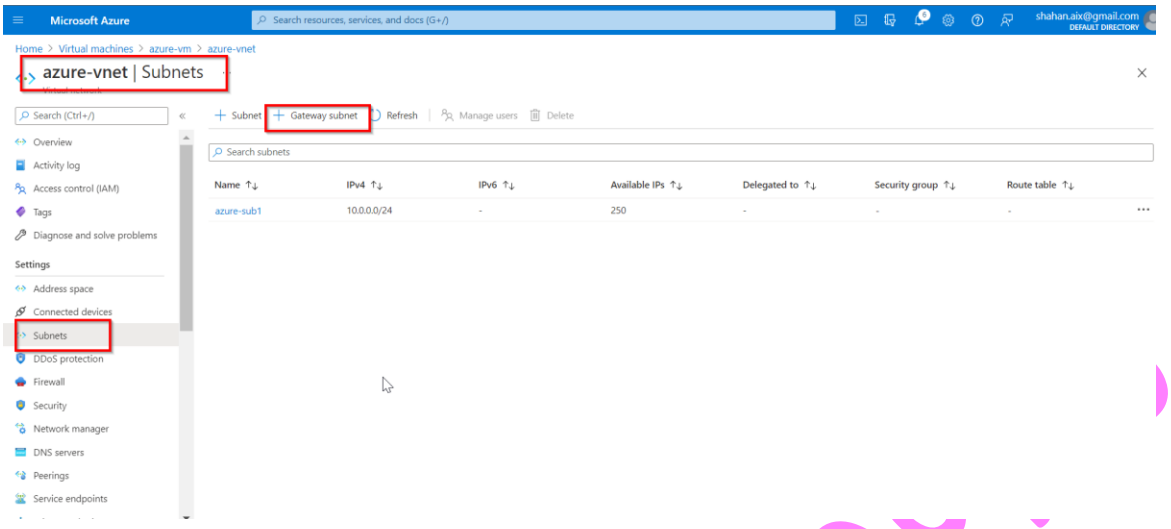

20.120.25.239 - Remote Desktop Connection
Server Manager
Server Manager ‣ Local Server
Dashboard
Local Server
All Servers
File and Storage Services
PROPERTIES
For mylocalserver
Internet Explorer Enhanced Security Configuration
Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.
Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.
Administrators:
On (Recommended)
Off
Users:
On (Recommended)
Off
More about Internet Explorer Enhanced Security Configuration
OK
Cancel
EVENTS
All events | 1 total
Filter
Server Name ID Severity Source Log Date and Time
mylocalserver 2004 Warning Microsoft-Windows-Resource-Exhaustion-Detector System 12/12/2021 5:14:19 PM

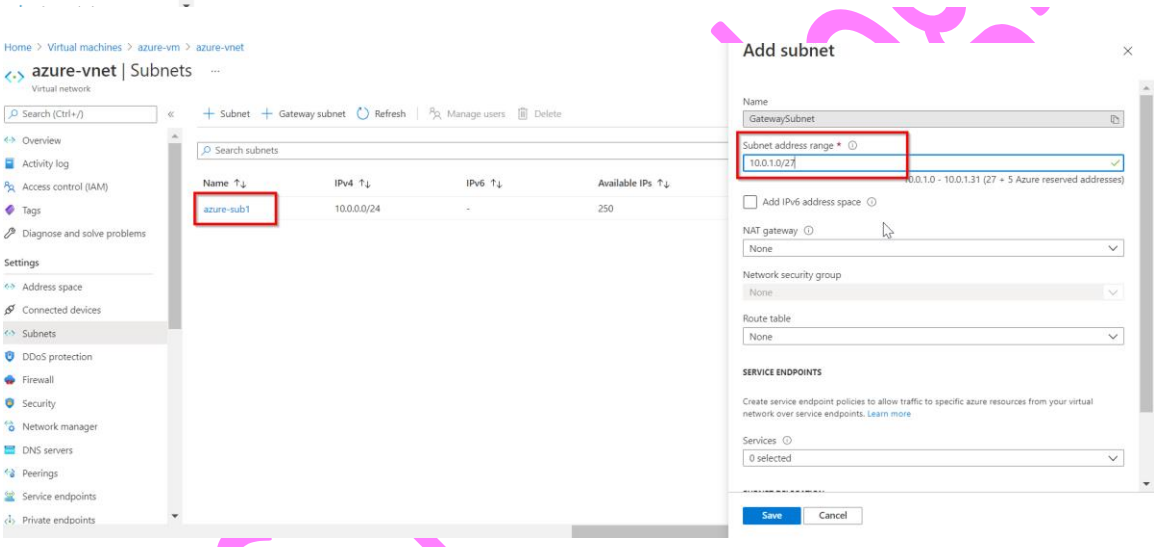
Hi I am from apache server

Can't reach this page

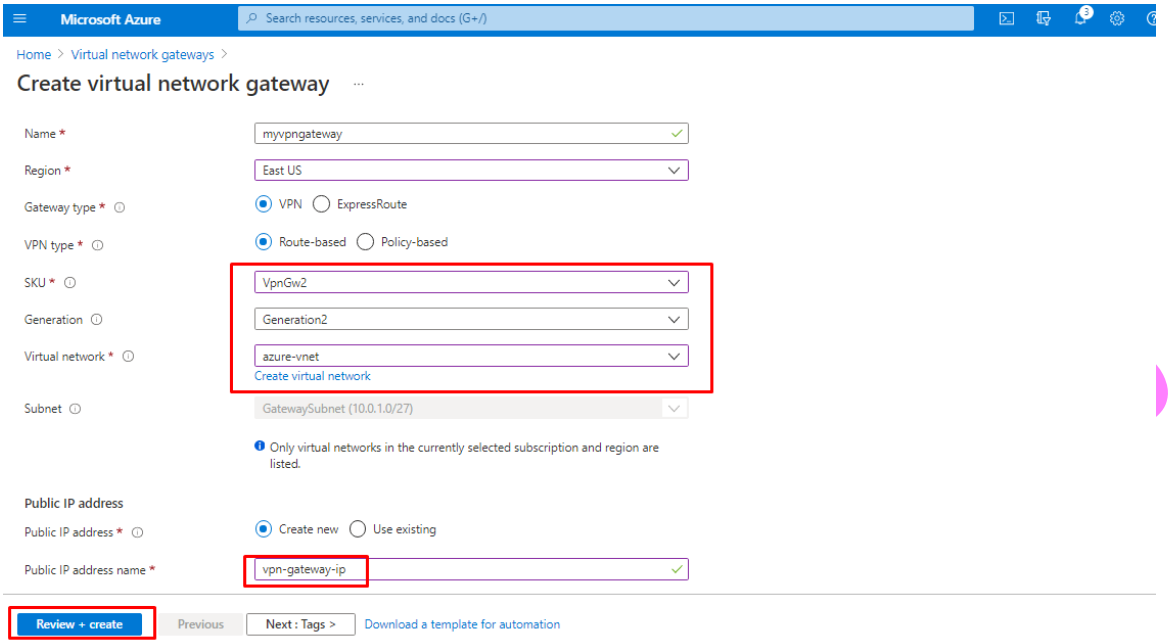
- Make sure the web address http://10.0.0.4 is correct
- Search for this site on Bing
- Refresh the page

Now let's configure the VPN to our VNET (azure-vnet)





Now let's configure the virtual network gateway for our VNET(azure-vnet)



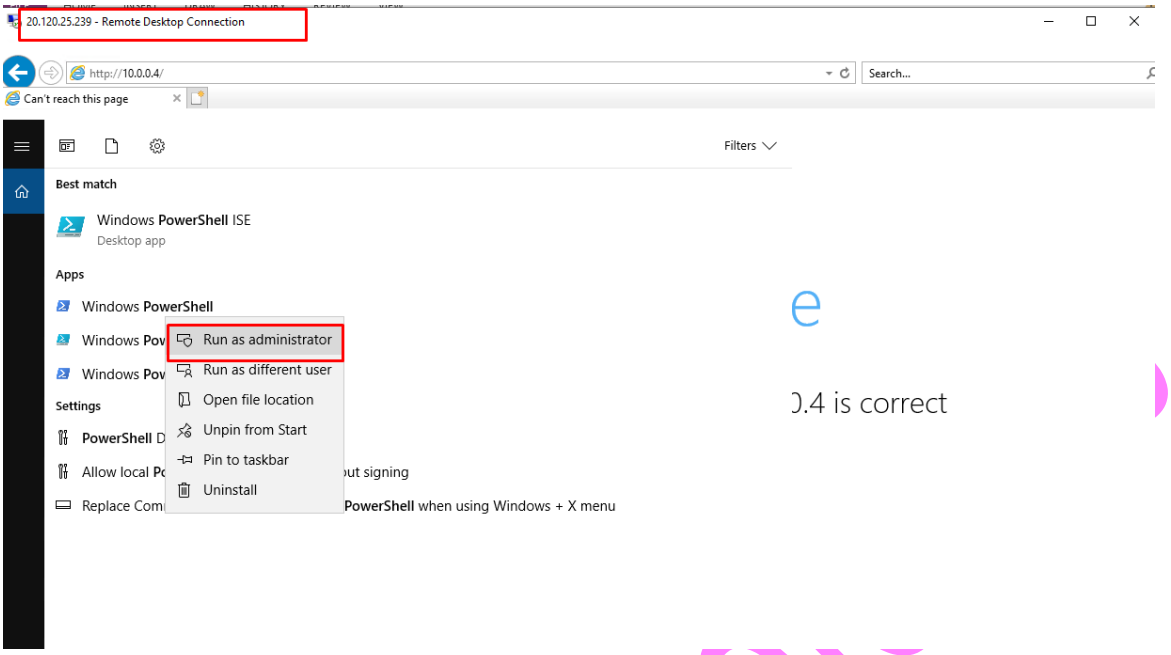
Now we are done with creating virtual network gateway
Note: VNG is costly !!! && It will take more time to create it

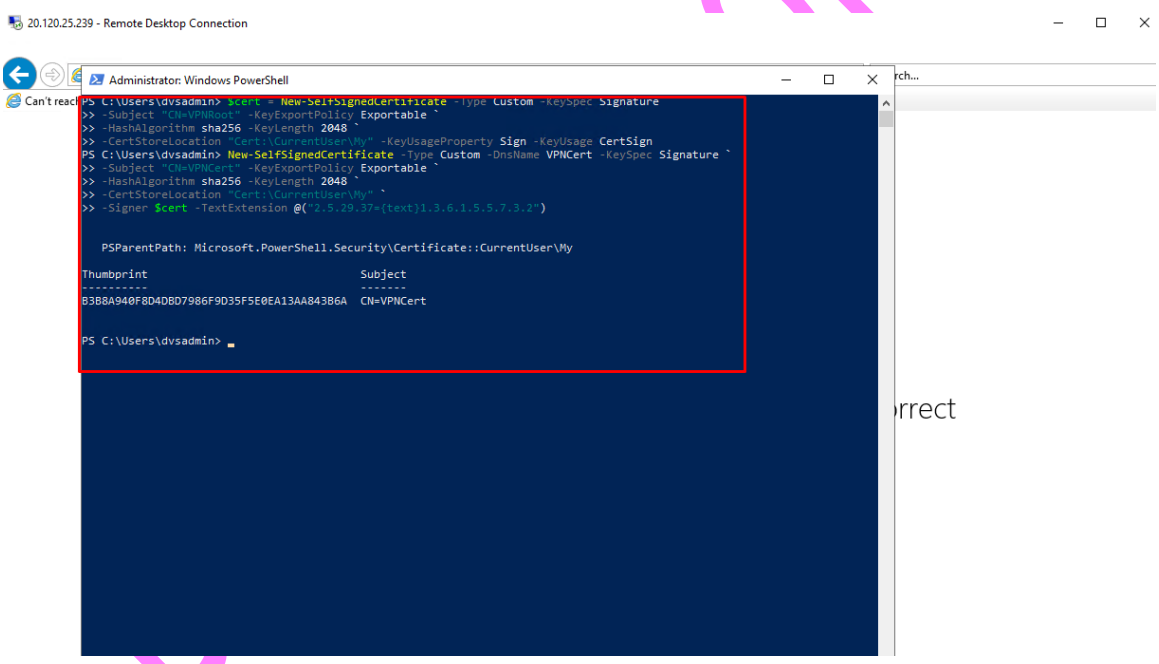
Let's generate the root & client certs in our localserver:

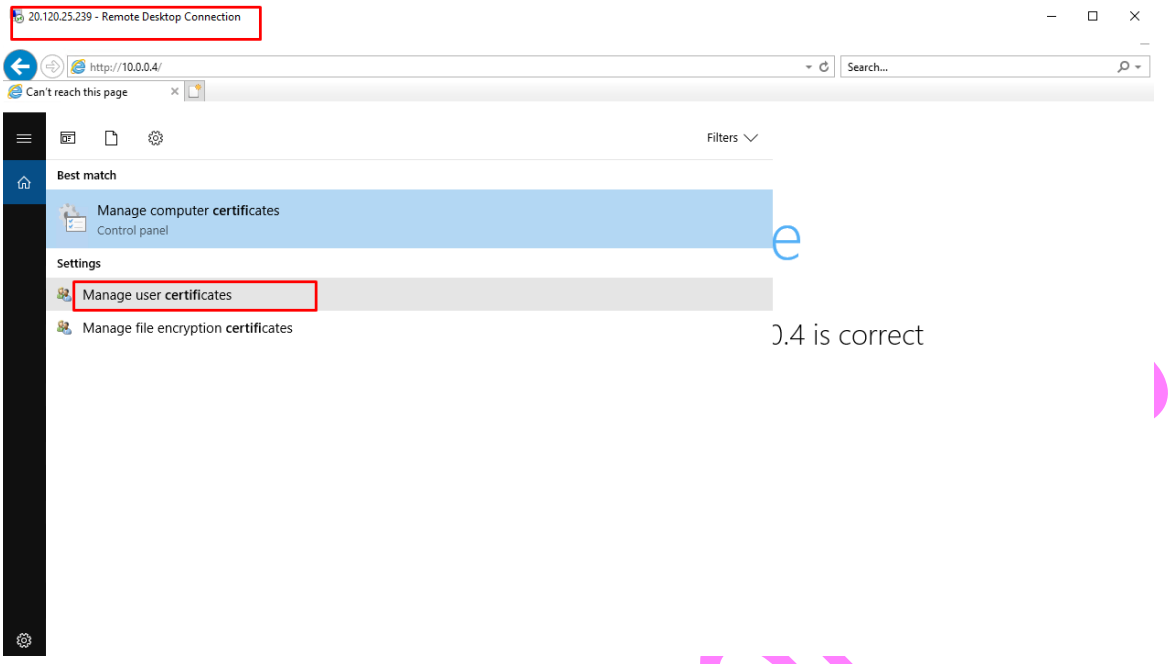
https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-vpn-client-configuration-azure-cert#linuxinstallcli

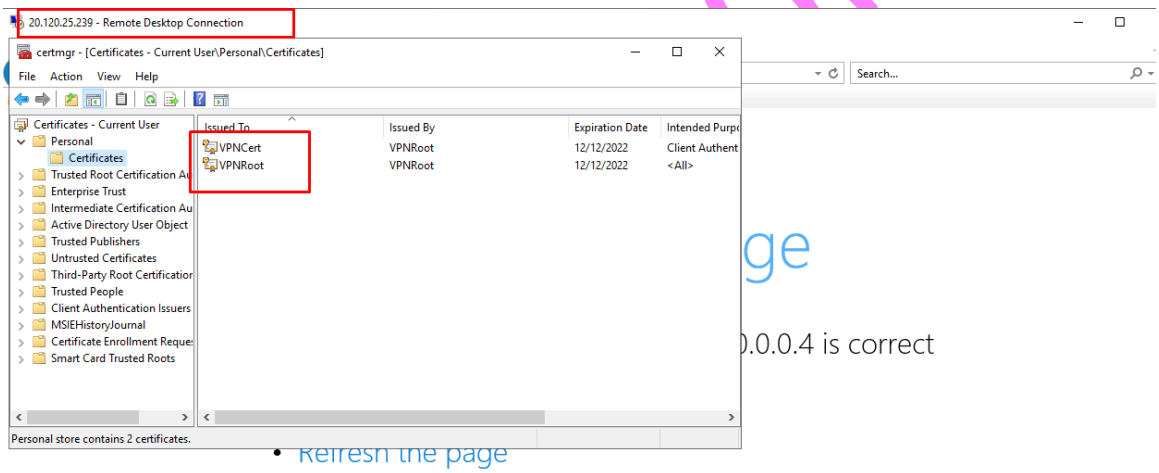
Use the above link

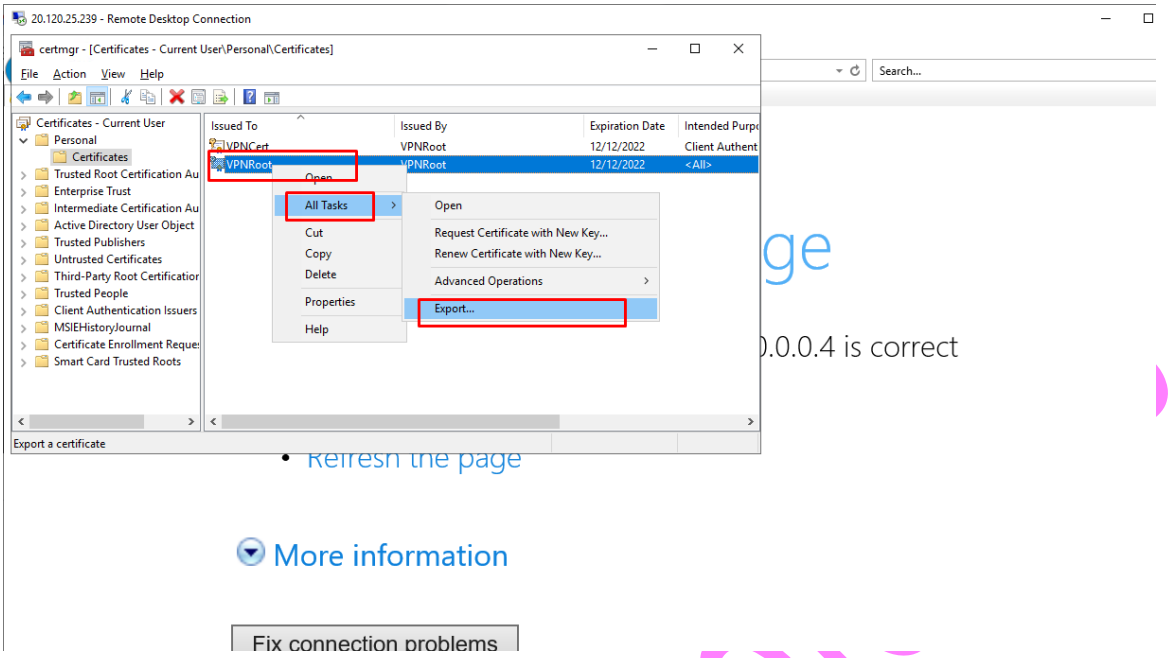
```
$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
-Subject "CN=VPNRoot" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign


New-SelfSignedCertificate -Type Custom -DnsName VPNCert -KeySpec Signature `
-Subject "CN=VPNCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" `
-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")
```

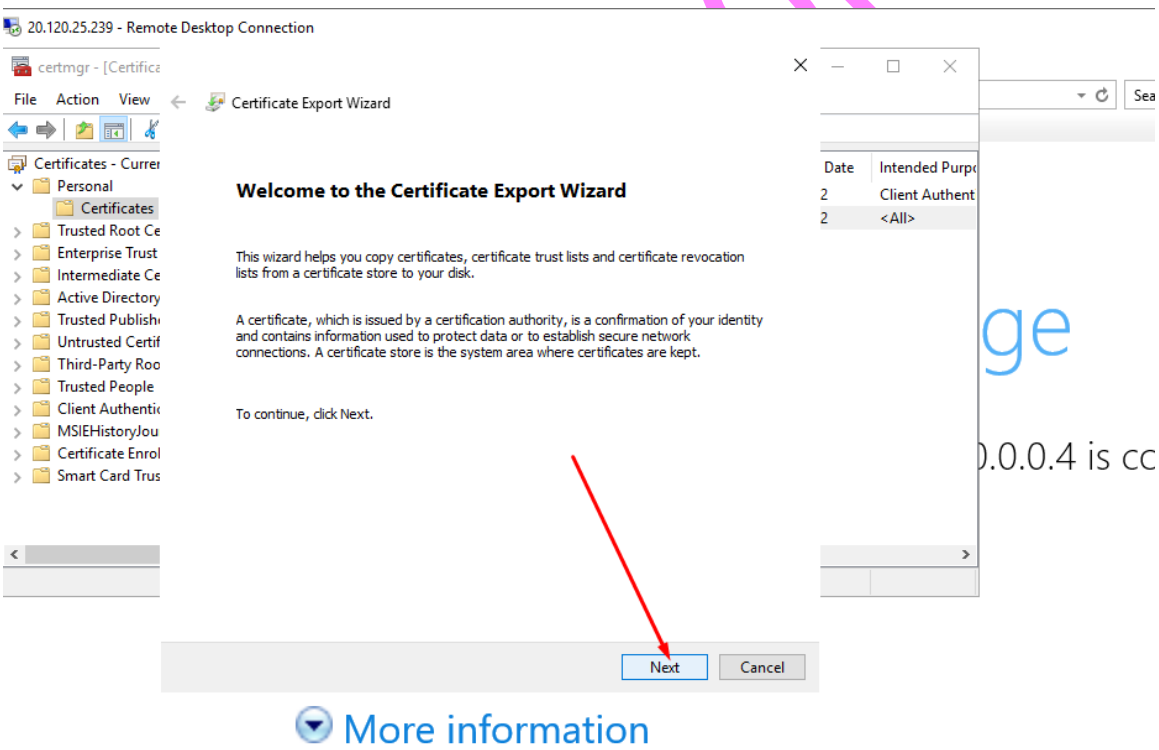

20.120.25.239 - Remote Desktop Connection
http://10.0.0.4/
Search...
Can't reach this page
Filters
Best match
Windows PowerShell ISE
Desktop app
Apps
Windows PowerShell
Windows Pov
Windows Pov
Run as administrator
Run as different user
Open file location
Unpin from Start
Pin to taskbar
Uninstall
Settings
PowerShell D
Allow local Po
Replace Com
PowerShell when using Windows + X menu

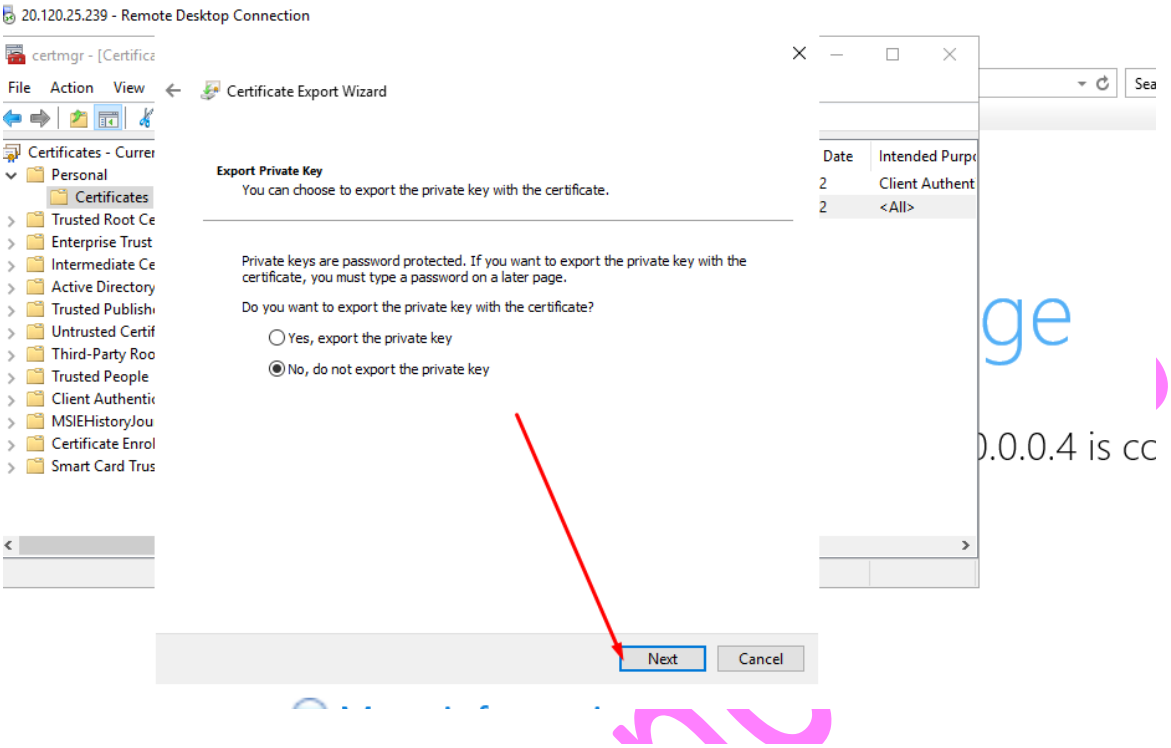

20.120.25.239 - Remote Desktop Connection
Administrator: Windows PowerShell
PS C:\Users\dvsadmin> $cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature
>> -Subject "CN=VPNRoot" -KeyExportPolicy Exportable `
>> -HashAlgorithm sha256 -KeyLength 2048 `
>> -CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign
PS C:\Users\dvsadmin> New-SelfSignedCertificate -Type Custom -DnsName VPNCert -KeySpec Signature `
>> -Subject "CN=VPNCert" -KeyExportPolicy Exportable `
>> -HashAlgorithm sha256 -KeyLength 2048 `
>> -CertStoreLocation "Cert:\CurrentUser\My" `
>> -Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")
PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My
Thumbprint Subject
B3B8A940F8D4D8D7986F9D35F5E0EA13AA843B6A CN=VPNCert
PS C:\Users\dvsadmin>

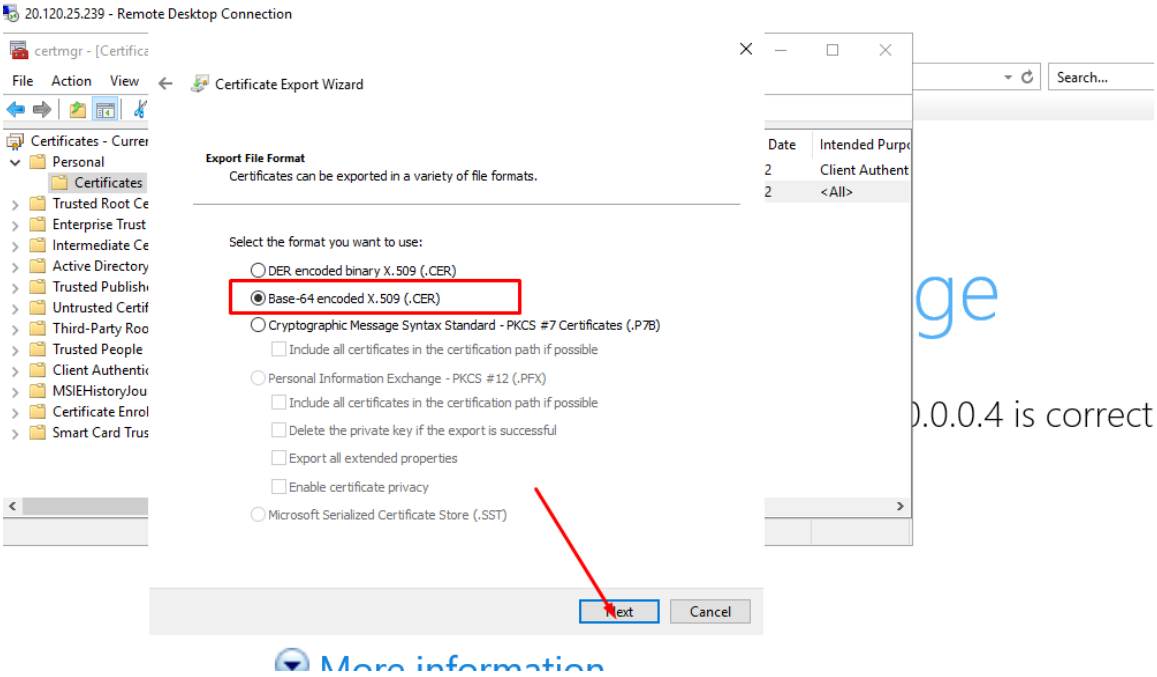

20.120.25.239 - Remote Desktop Connection
http://10.0.0.4/
Search...
Can't reach this page
Filters
Best match
Manage computer certificates
Control panel
Settings
Manage user certificates
Manage file encryption certificates

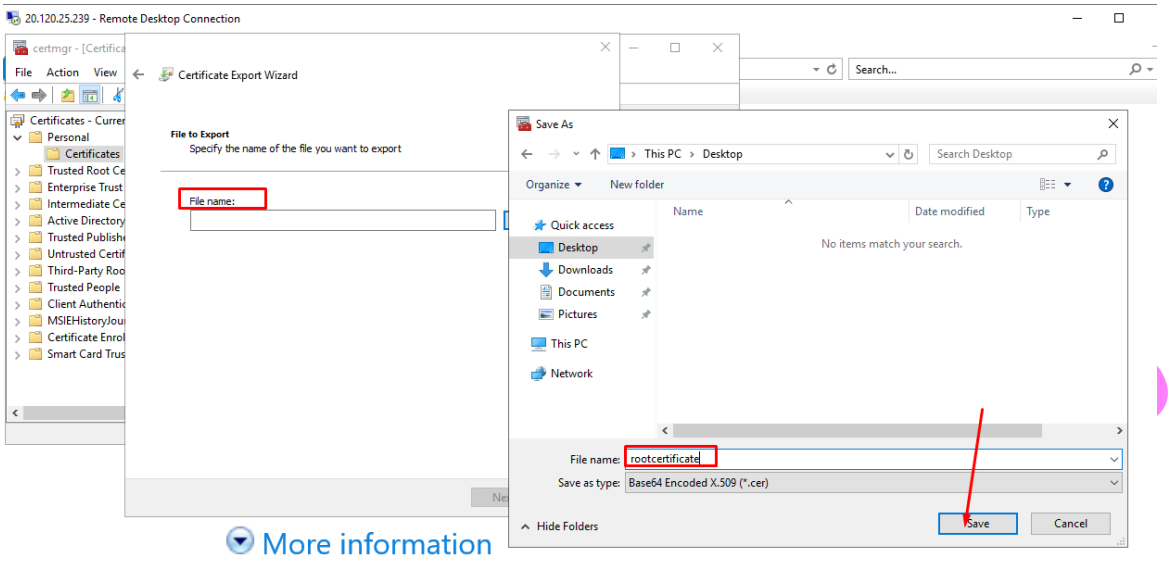

20.120.25.239 - Remote Desktop Connection
certmgr - [Certificates - Current User\Personal\Certificates]
File Action View Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Client Authentication Issuers
MSIEHistoryJournal
Certificate Enrollment Reque
Smart Card Trusted Roots
Issued To
Issued By
Expiration Date
Intended Purp
VPNCert
VPNRoot
12/12/2022
Client Authent
VPNRoot
VPNRoot
12/12/2022
<All>
Personal store contains 2 certificates.
Search...

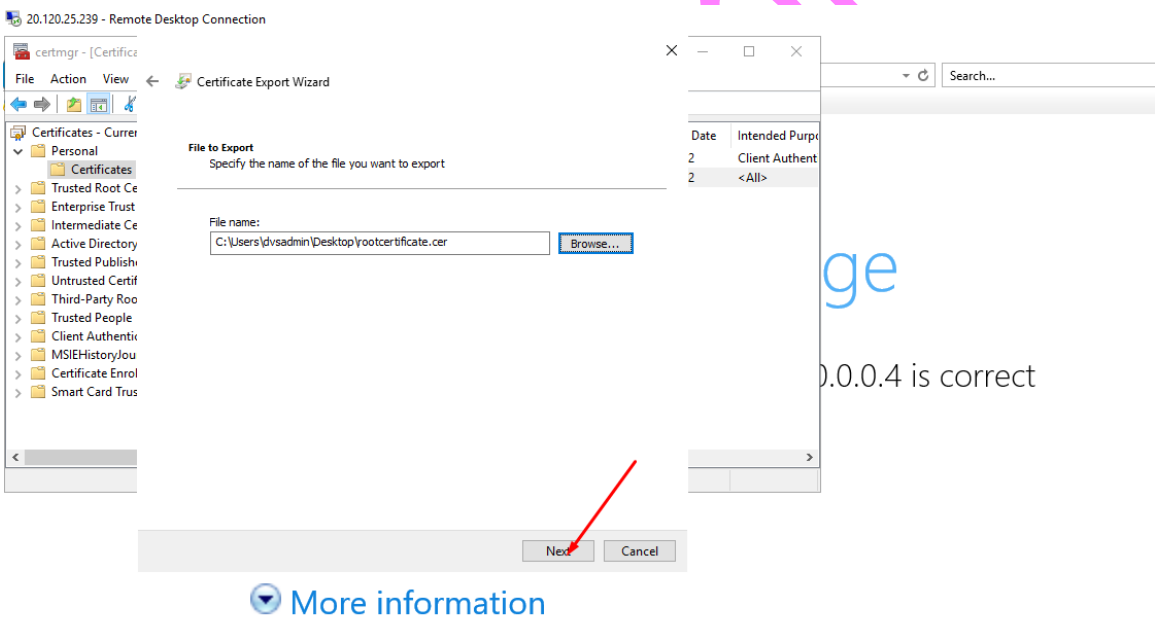

20.120.25.239 - Remote Desktop Connection
certmgr - [Certificates - Current User\Personal\Certificates]
File Action View Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Client Authentication Issuers
MSIEHistoryJournal
Certificate Enrollment Reque
Smart Card Trusted Roots
Issued To
Issued By
Expiration Date
Intended Purpo
VPNCert
VPNRoot
12/12/2022
Client Authent
<All>
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Advanced Operations
Export...
Export a certificate
Search...
ge
.0.0.4 is correct
More information
Fix connection problems

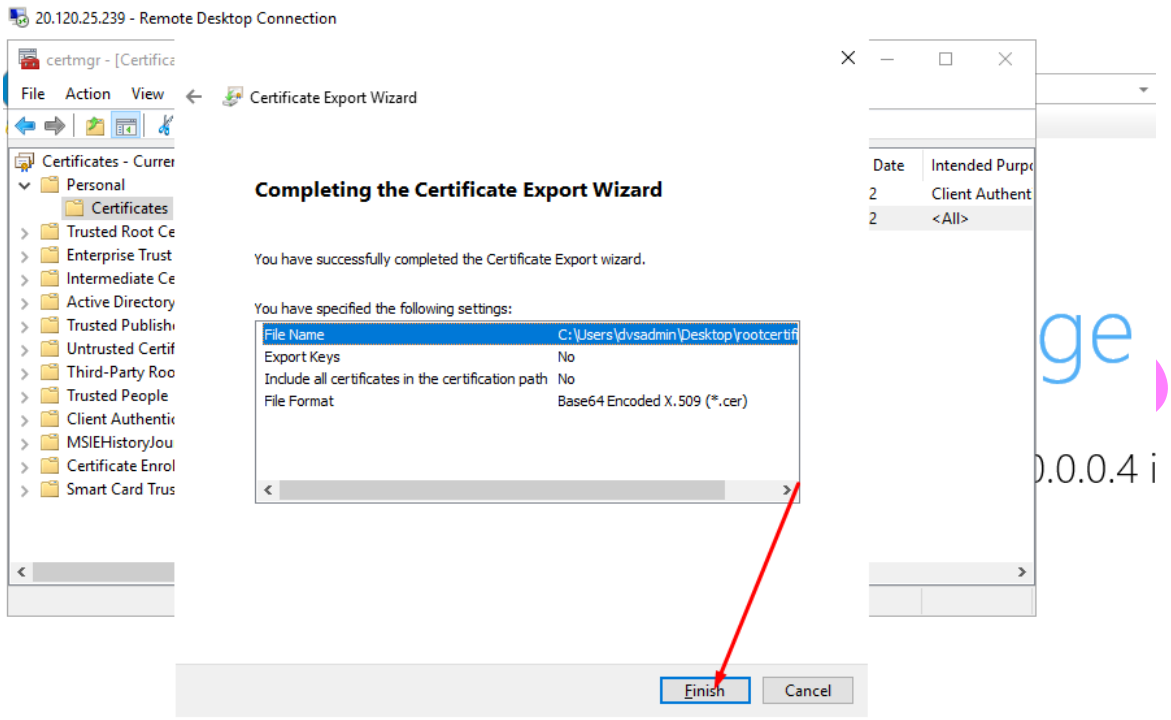

20.120.25.239 - Remote Desktop Connection
certmgr - [Certifica
File Action View
Certificates - Curre
Personal
Certificates
Trusted Root Ce
Enterprise Trust
Intermediate Ce
Active Directory
Trusted Publish
Untrusted Certif
Third-Party Roo
Trusted People
Client Authentic
MSIEHistoryJou
Certificate Enrol
Smart Card Trus
Certificate Export Wizard
Welcome to the Certificate Export Wizard
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
Next
Cancel
Date
Intended Purpo
Client Authent
<All>
ge
.0.0.4 is cc
More information

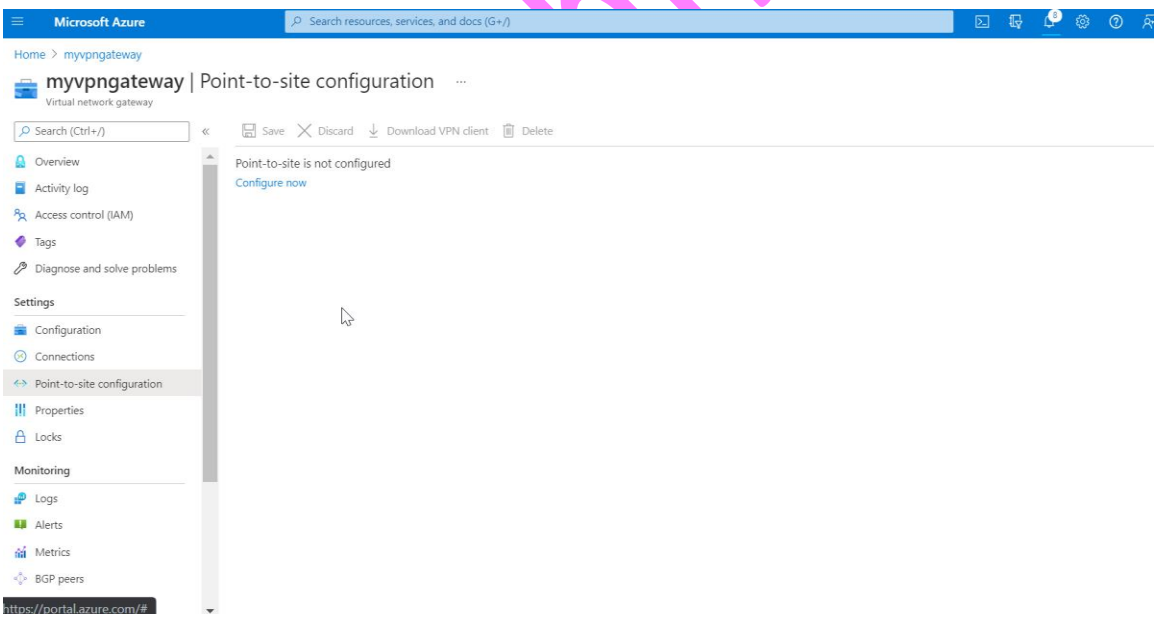

20.120.25.239 - Remote Desktop Connection
certmgr - [Certifica
File Action View
Certificate Export Wizard
Export Private Key
You can choose to export the private key with the certificate.
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.
Do you want to export the private key with the certificate?
Yes, export the private key
No, do not export the private key
Next
Cancel
Certificates - Curre
Personal
Certificates
Trusted Root Ce
Enterprise Trust
Intermediate Ce
Active Directory
Trusted Publish
Untrusted Certif
Third-Party Roo
Trusted People
Client Authentic
MSIEHistoryJou
Certificate Enrol
Smart Card Trus
Date
Intended Purpo
Client Authent
<All>

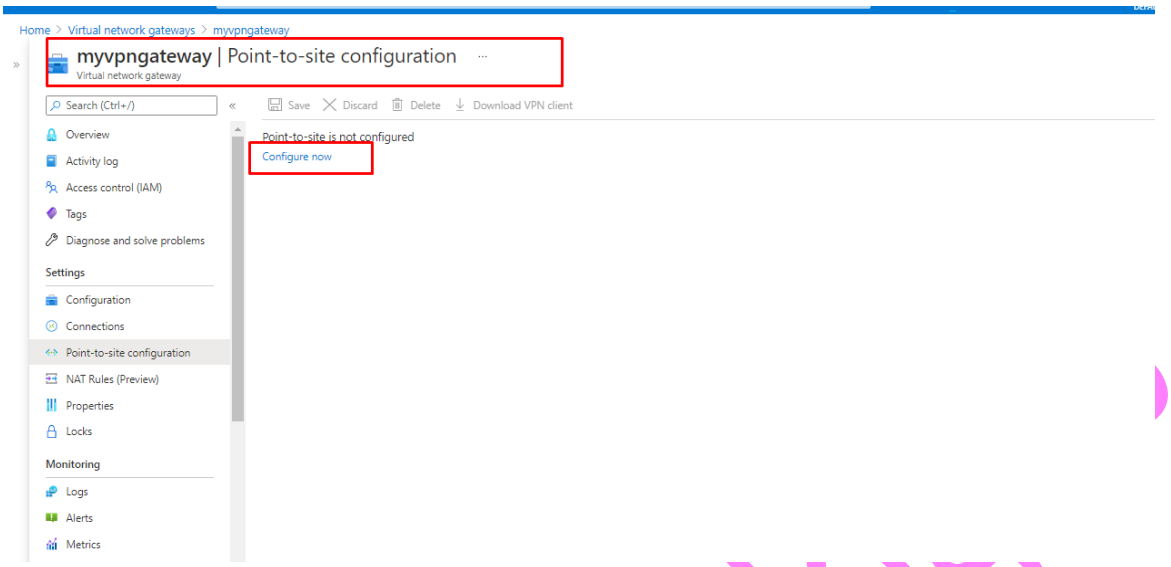

20.120.25.239 - Remote Desktop Connection
certmgr - [Certifica
File Action View
Certificate Export Wizard
Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
Personal Information Exchange - PKCS #12 (.PFX)
Include all certificates in the certification path if possible
Delete the private key if the export is successful
Export all extended properties
Enable certificate privacy
Microsoft Serialized Certificate Store (.SST)
Next
Cancel
Search...
Certificates - Curre
Personal
Certificates
Trusted Root Ce
Enterprise Trust
Intermediate Ce
Active Directory
Trusted Publish
Untrusted Certif
Third-Party Roo
Trusted People
Client Authentic
MSIEHistoryJou
Certificate Enrol
Smart Card Trus
Date
Intended Purpo
Client Authent
<All>

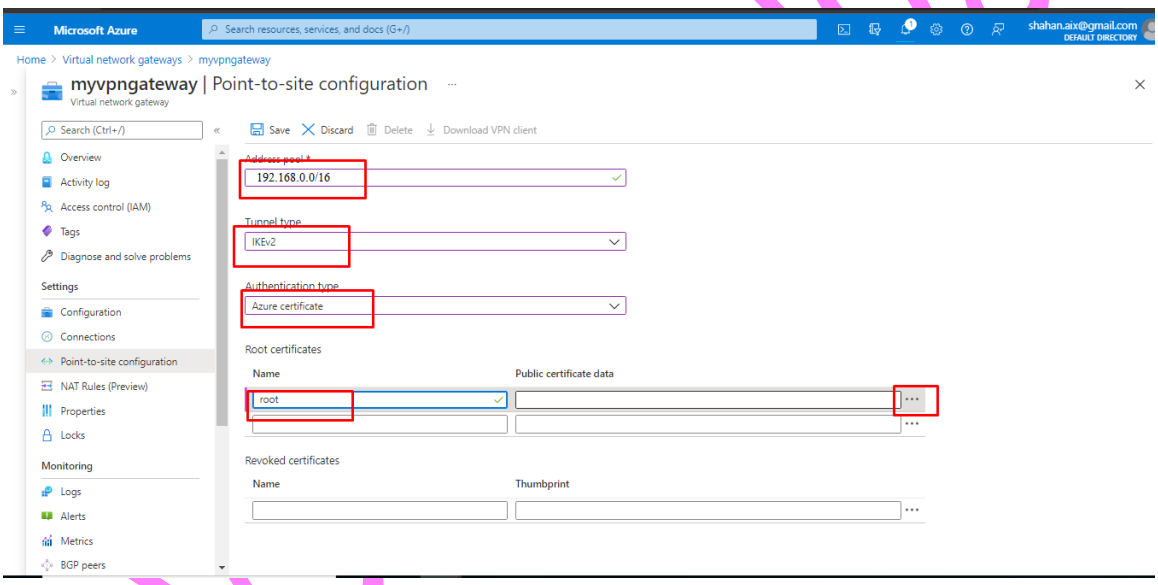

20.120.25.239 - Remote Desktop Connection
Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
Save As
This PC › Desktop
Search Desktop
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
No items match your search.
File name: rootcertificate
Save as type: Base64 Encoded X.509 (*.cer)
Hide Folders
Save
Cancel
More information

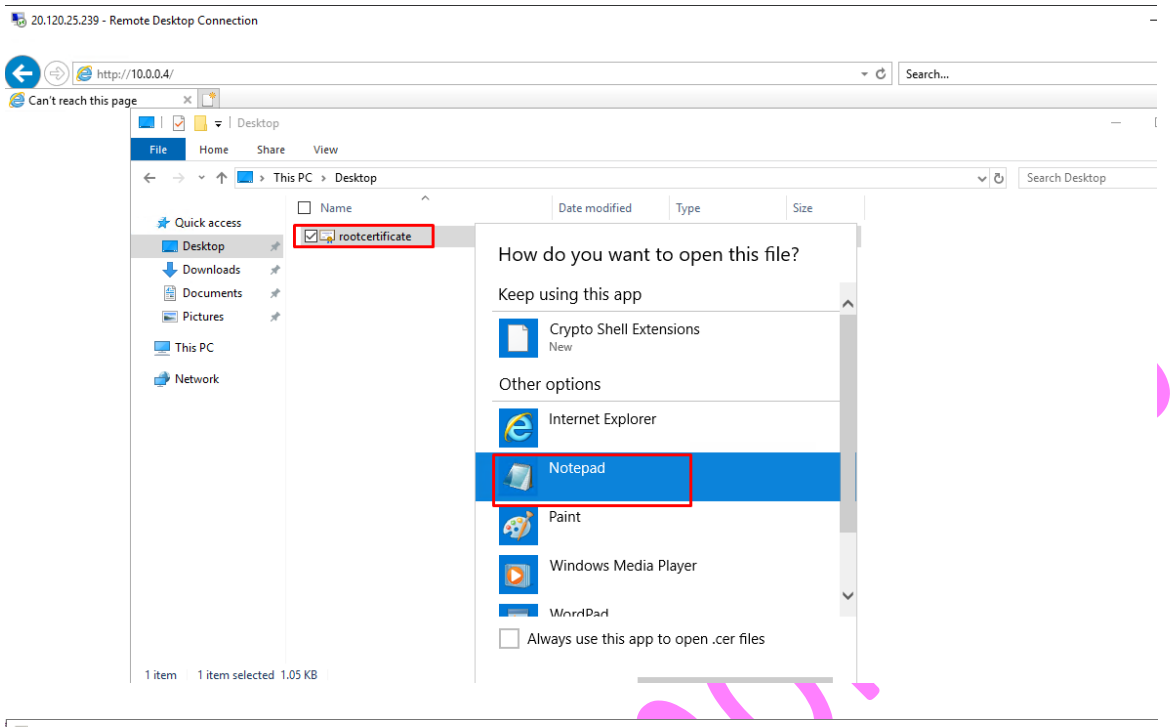

20.120.25.239 - Remote Desktop Connection
Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
C:\Users\dvsadmin\Desktop\rootcertificate.cer
Browse...
Next
Cancel
Date
Intended Purpo
Client Authent
<All>
Search...
More information

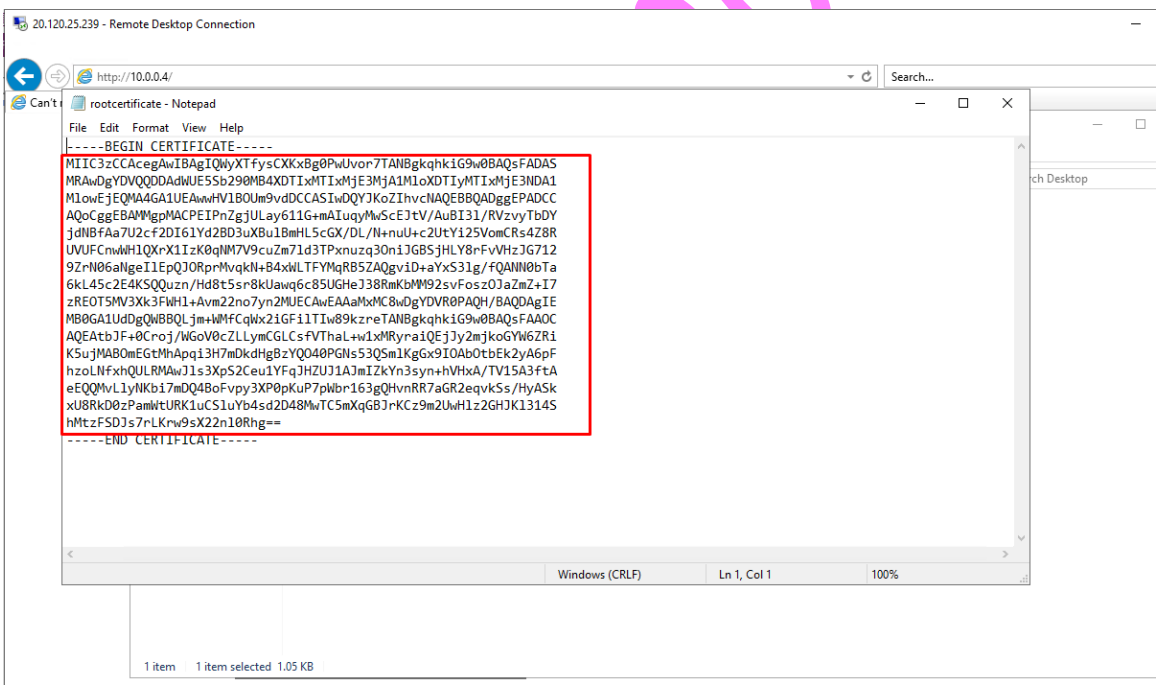

20.120.25.239 - Remote Desktop Connection
certmgr - [Certifica
File Action View
Certificate Export Wizard
Certificates - Curre
Personal
Certificates
Trusted Root Ce
Enterprise Trust
Intermediate Ce
Active Directory
Trusted Publish
Untrusted Certif
Third-Party Roo
Trusted People
Client Authentic
MSIEHistoryJou
Certificate Enrol
Smart Card Trus
Completing the Certificate Export Wizard
You have successfully completed the Certificate Export wizard.
You have specified the following settings:
File Name C:\Users\dvsadmin\Desktop\rootcertif
Export Keys No
Include all certificates in the certification path No
File Format Base64 Encoded X.509 (*.cer)
Finish
Cancel
Date
Intended Purpo
Client Authent
<All>


Microsoft Azure
Search resources, services, and docs (G+/)
Home > myvpngateway
myvpngateway | Point-to-site configuration
Virtual network gateway
Search (Ctrl+/)
Save
Discard
Download VPN client
Delete
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Connections
Point-to-site configuration
Properties
Locks
Monitoring
Logs
Alerts
Metrics
BGP peers
Point-to-site is not configured
Configure now

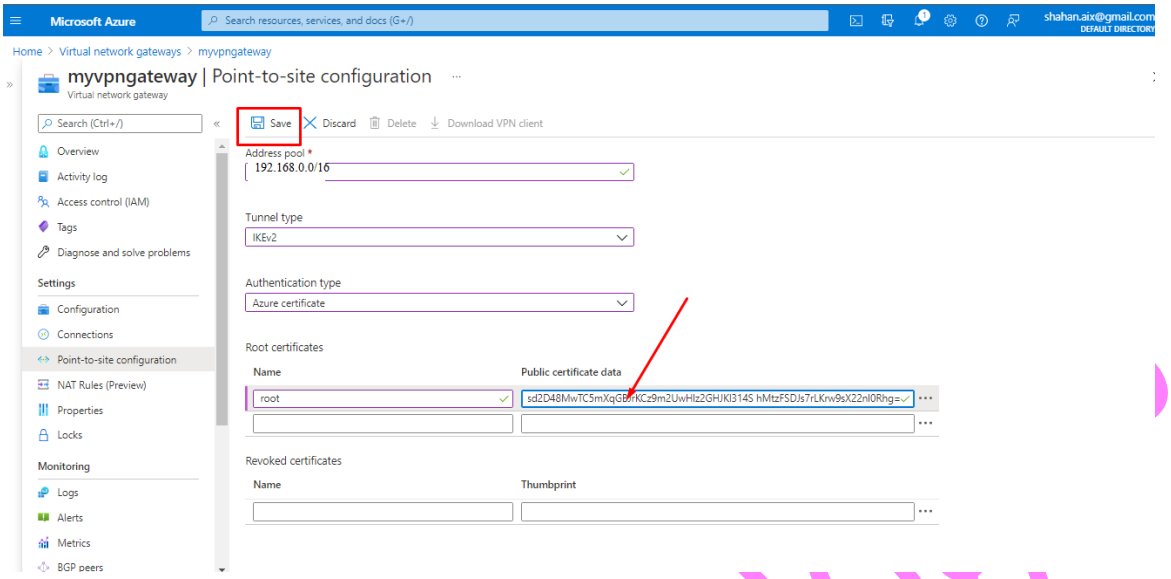

Home > Virtual network gateways > myvpngateway
myvpngateway | Point-to-site configuration
Virtual network gateway
Search (Ctrl+/)
Save
Discard
Delete
Download VPN client
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Connections
Point-to-site configuration
NAT Rules (Preview)
Properties
Locks
Monitoring
Logs
Alerts
Metrics
Point-to-site is not configured
Configure now

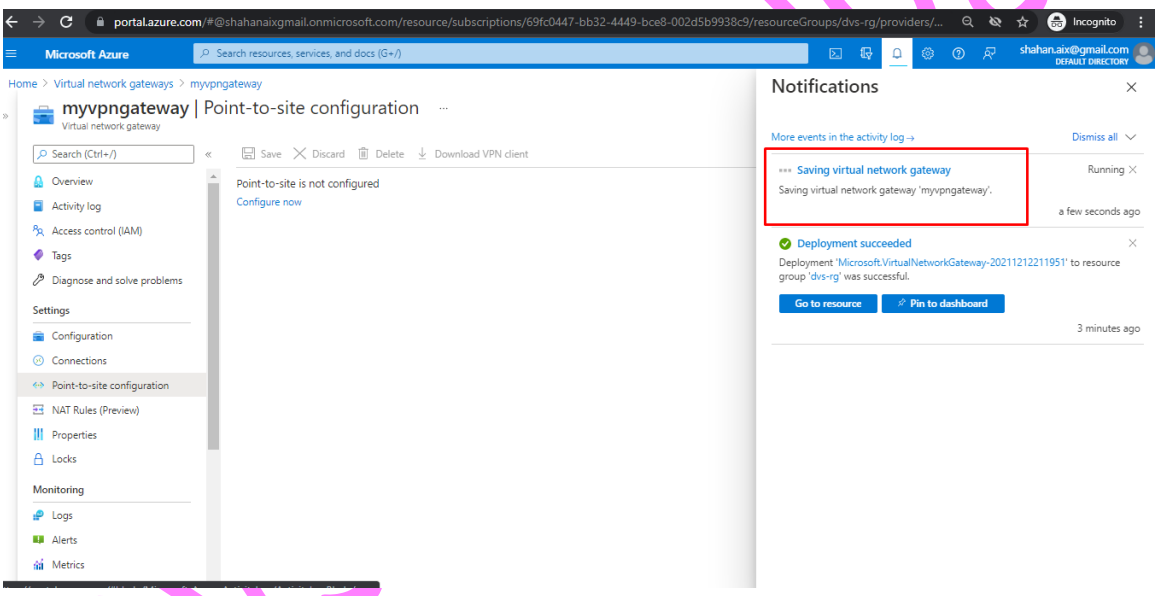

Microsoft Azure
Search resources, services, and docs (G+/)
shahan.aix@gmail.com
DEFAULT DIRECTORY
Home > Virtual network gateways > myvpngateway
myvpngateway | Point-to-site configuration
Virtual network gateway
Search (Ctrl+/)
Save
Discard
Delete
Download VPN client
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Connections
Point-to-site configuration
NAT Rules (Preview)
Properties
Locks
Monitoring
Logs
Alerts
Metrics
BGP peers
Address pool *
192.168.0.0/16
Tunnel type
IKEv2
Authentication type
Azure certificate
Root certificates
Name
Public certificate data
root
Revoked certificates
Name
Thumbprint





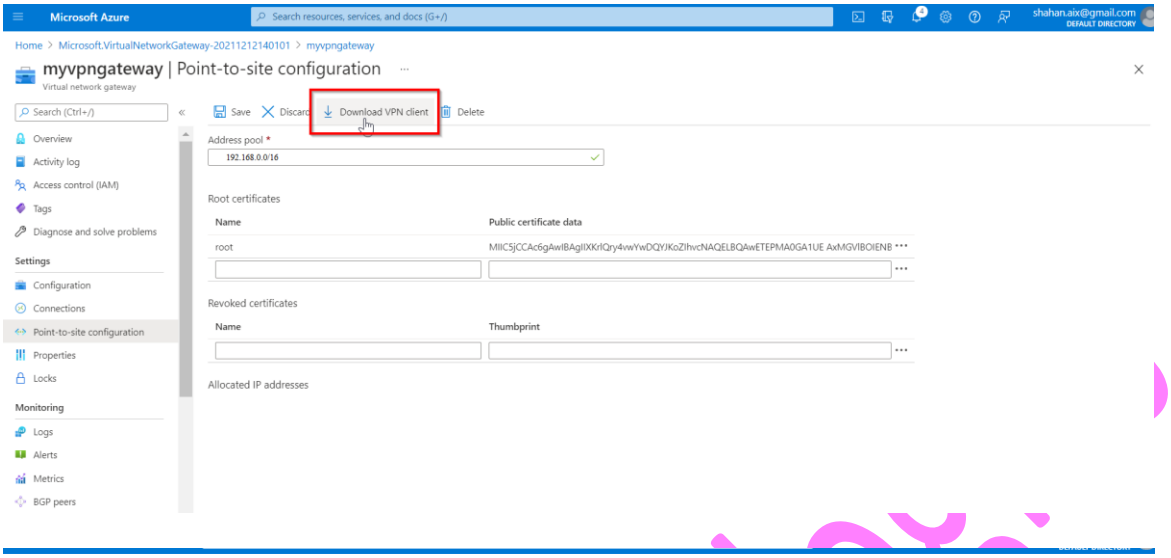
Copy the above key to the azure

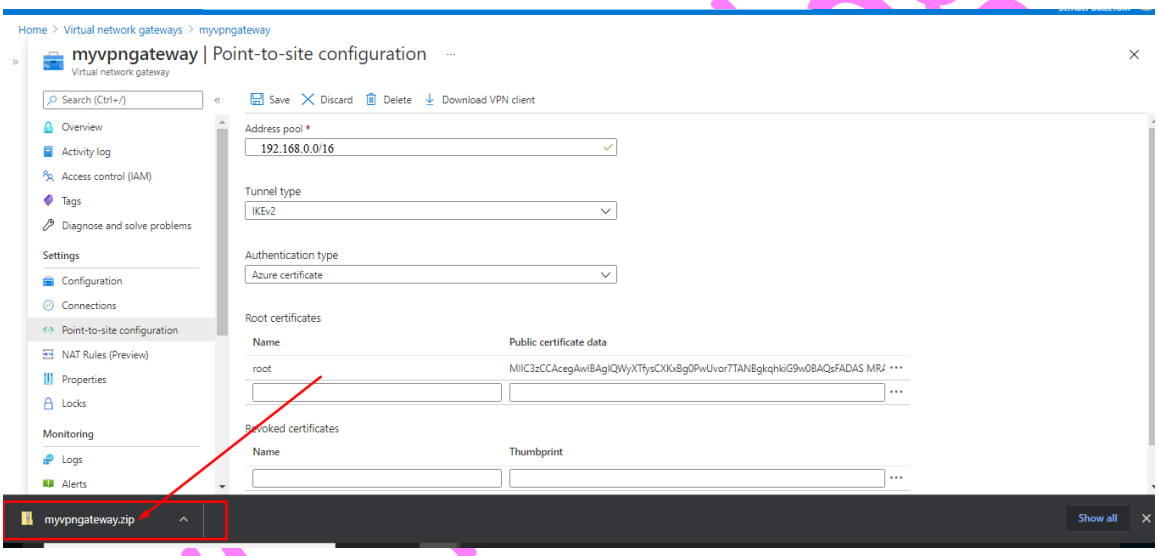




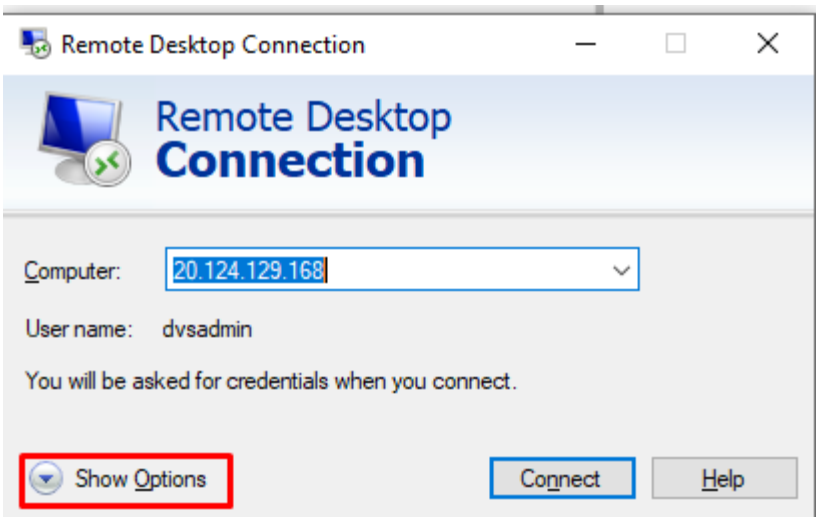
Let's wait for it to get configure as it take more time to get ready. Once done then you can download the vpn package.

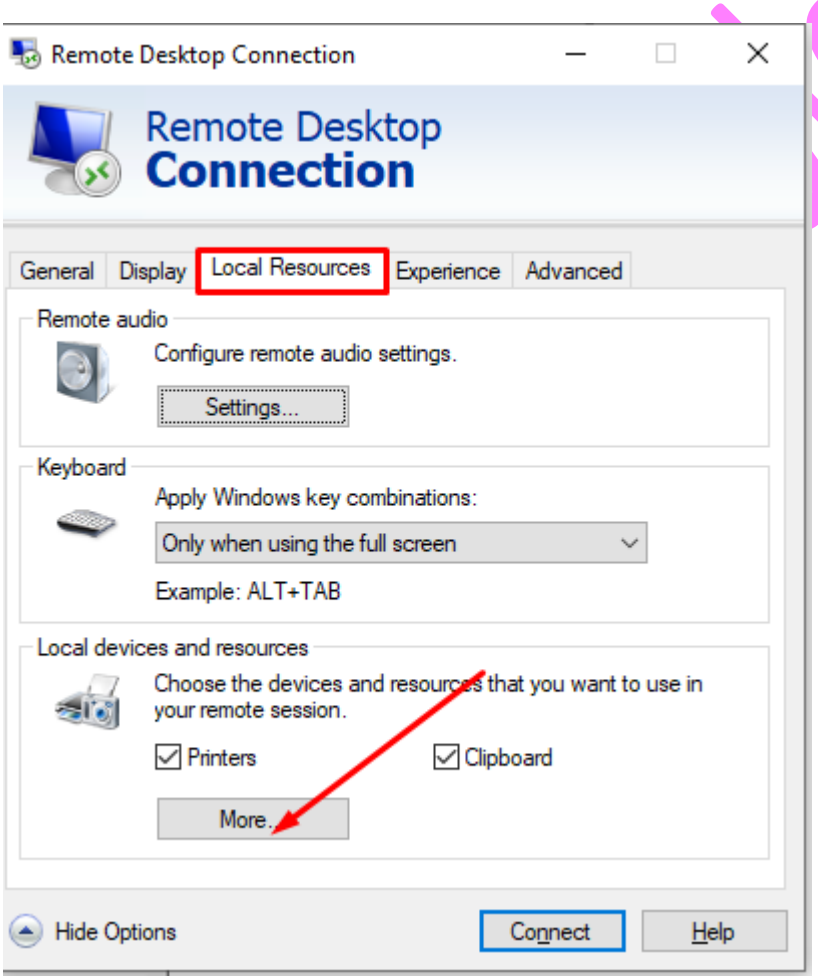
Download the vpn client package from azure portal

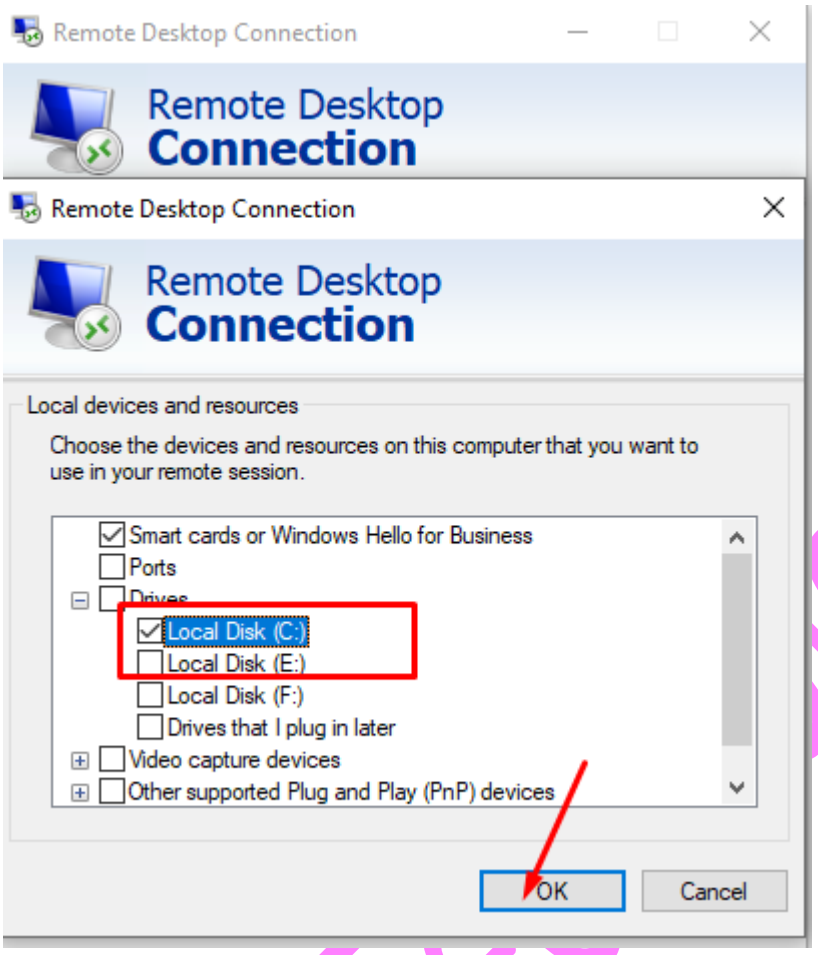




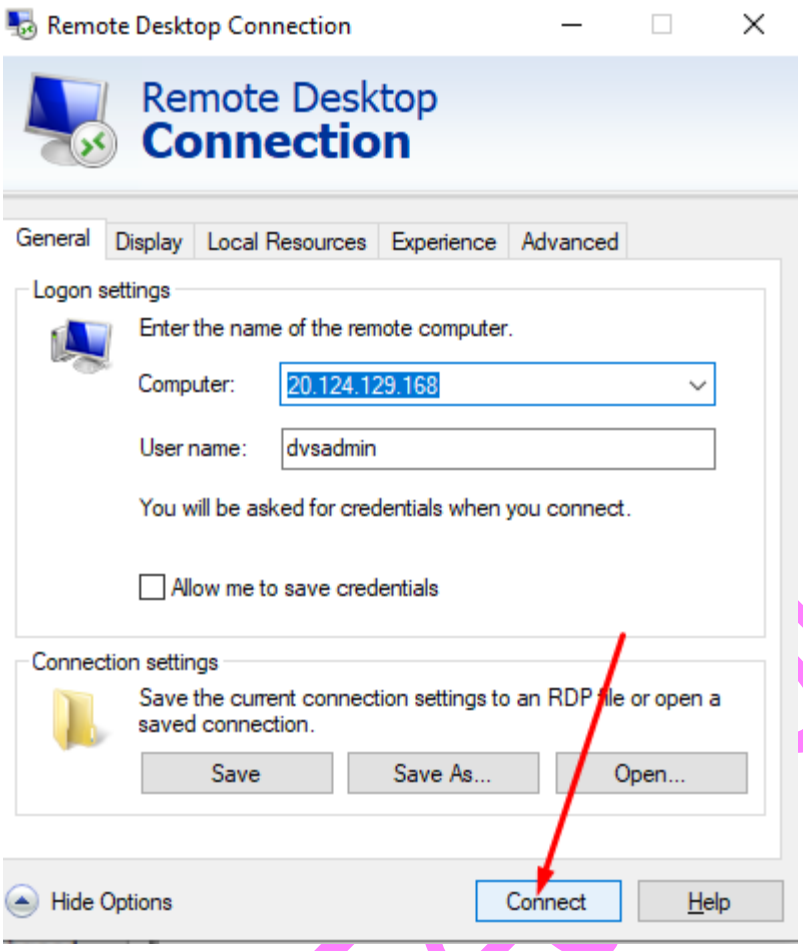
Now copy this zip file to our windows server


Remote Desktop Connection
Remote Desktop
Connection
Computer:
20.124.129.168
User name:
dvsadmin
You will be asked for credentials when you connect.
Show Options
Connect
Help

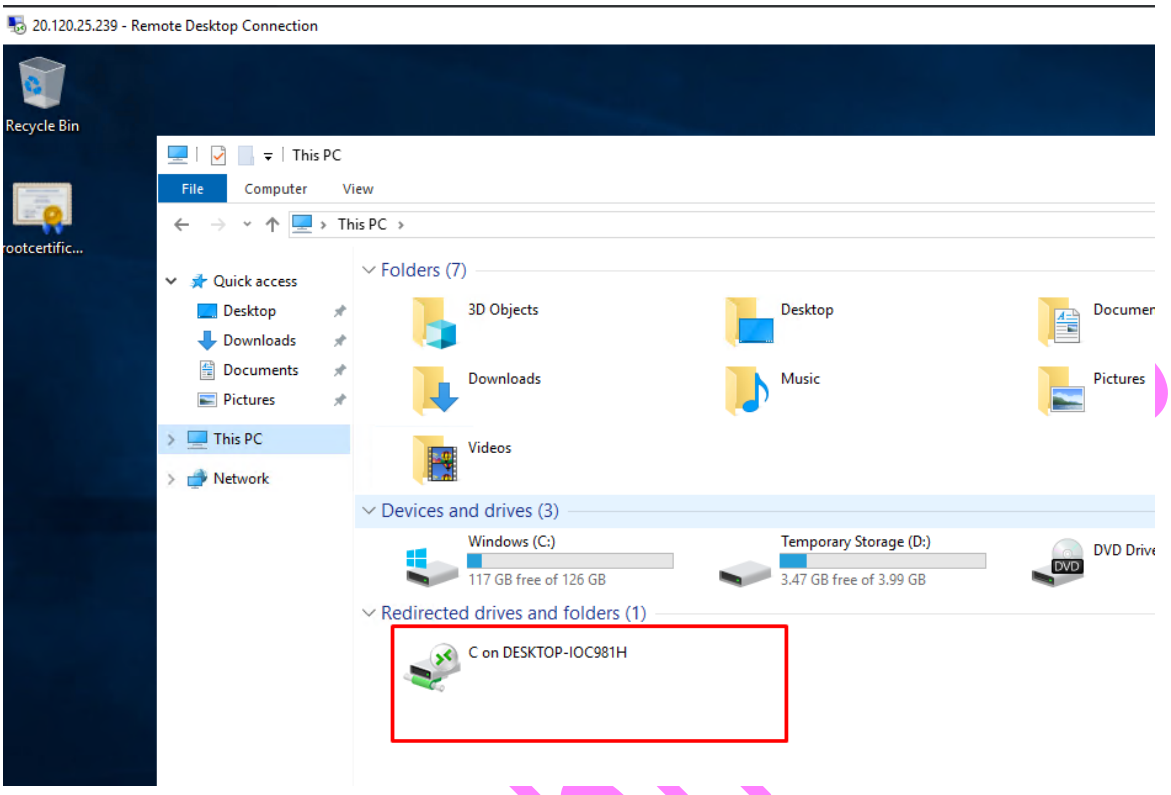

Remote Desktop Connection
Remote Desktop
Connection
General
Display
Local Resources
Experience
Advanced
Remote audio
Configure remote audio settings.
Settings...
Keyboard
Apply Windows key combinations:
Only when using the full screen
Example: ALT+TAB
Local devices and resources
Choose the devices and resources that you want to use in your remote session.
Printers
Clipboard
More...
Hide Options
Connect
Help

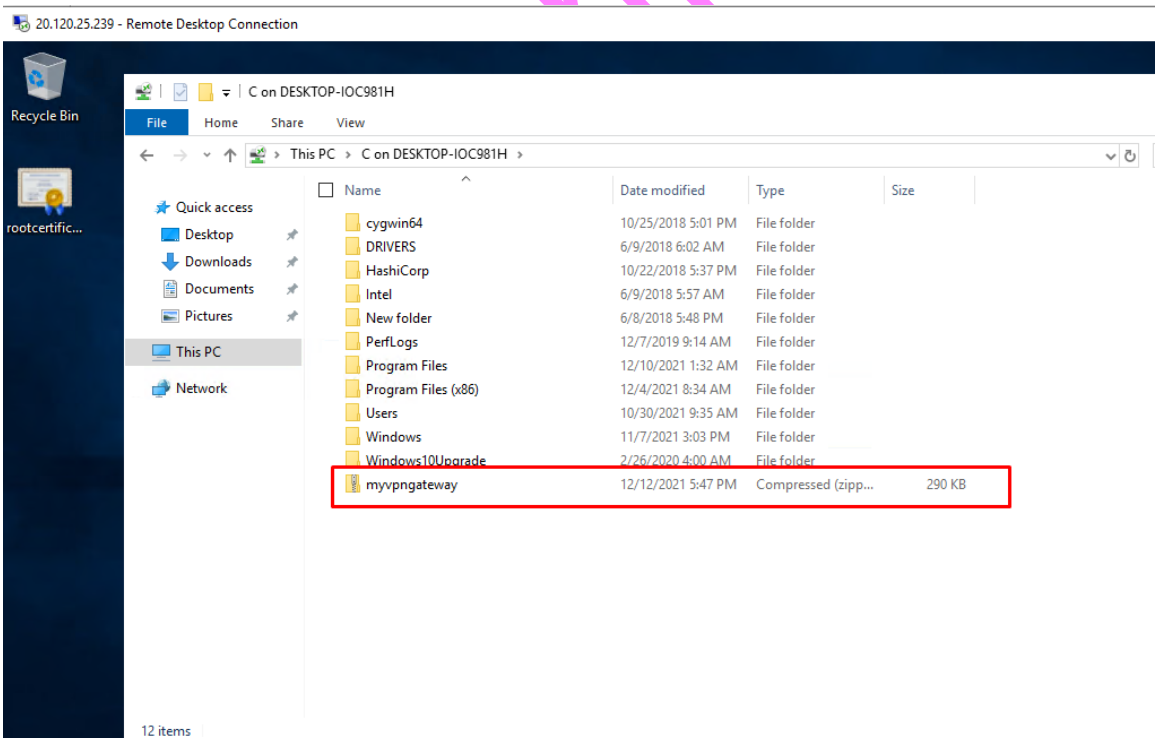


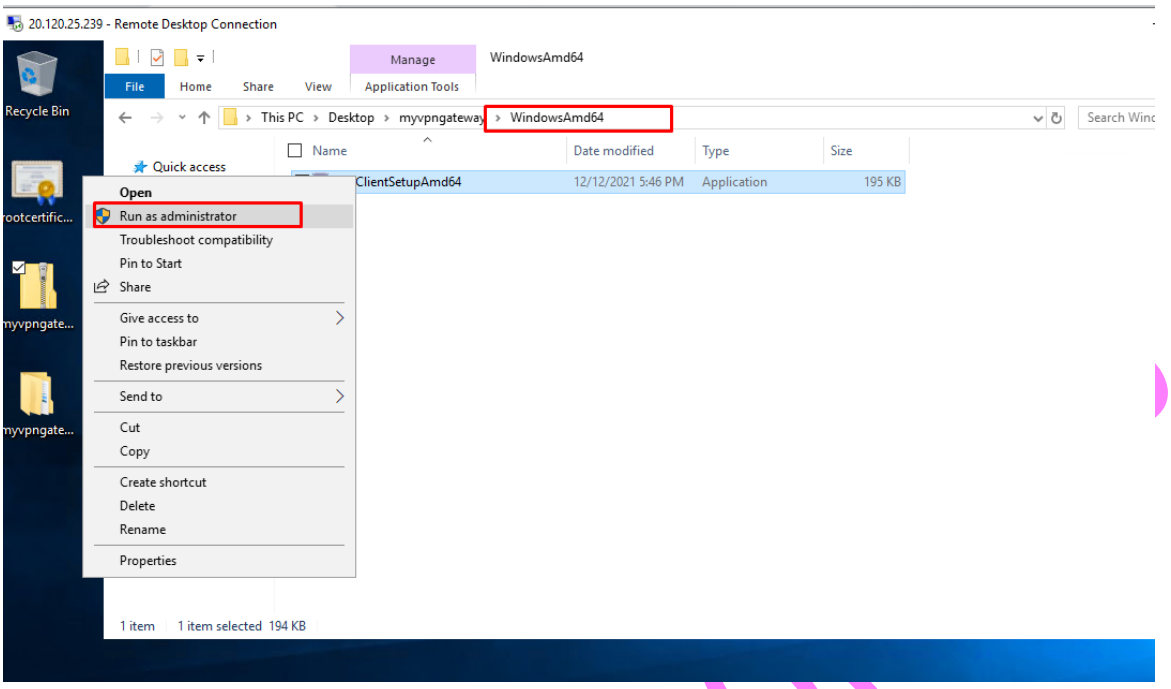
DVS Technologies

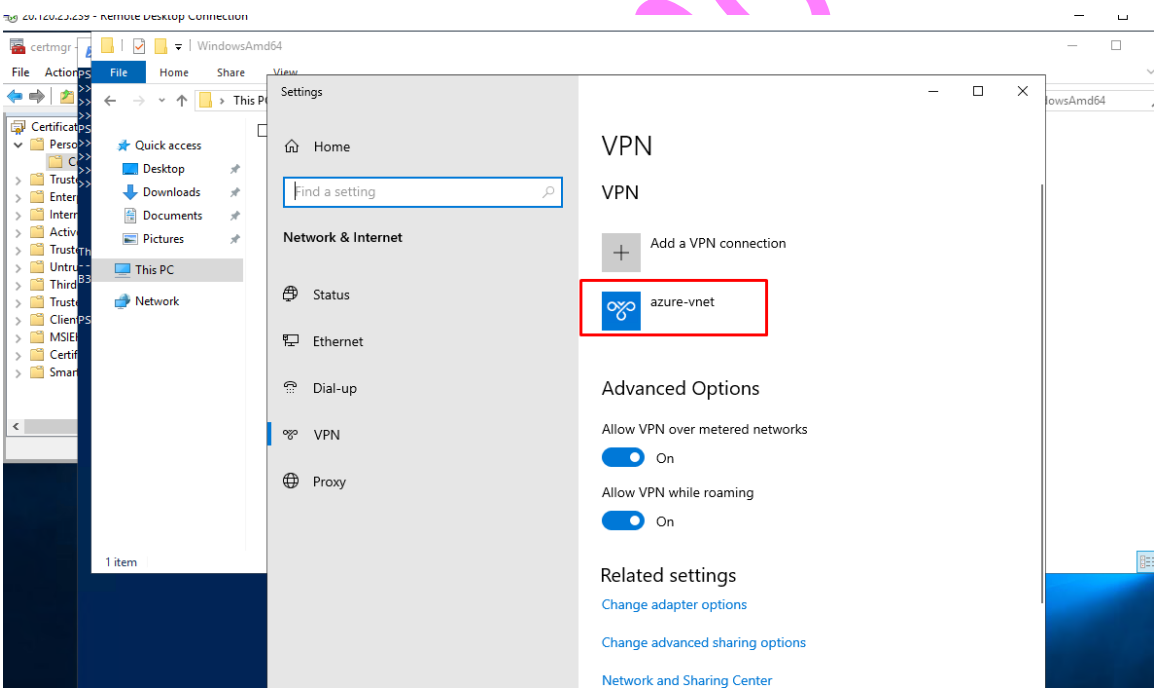


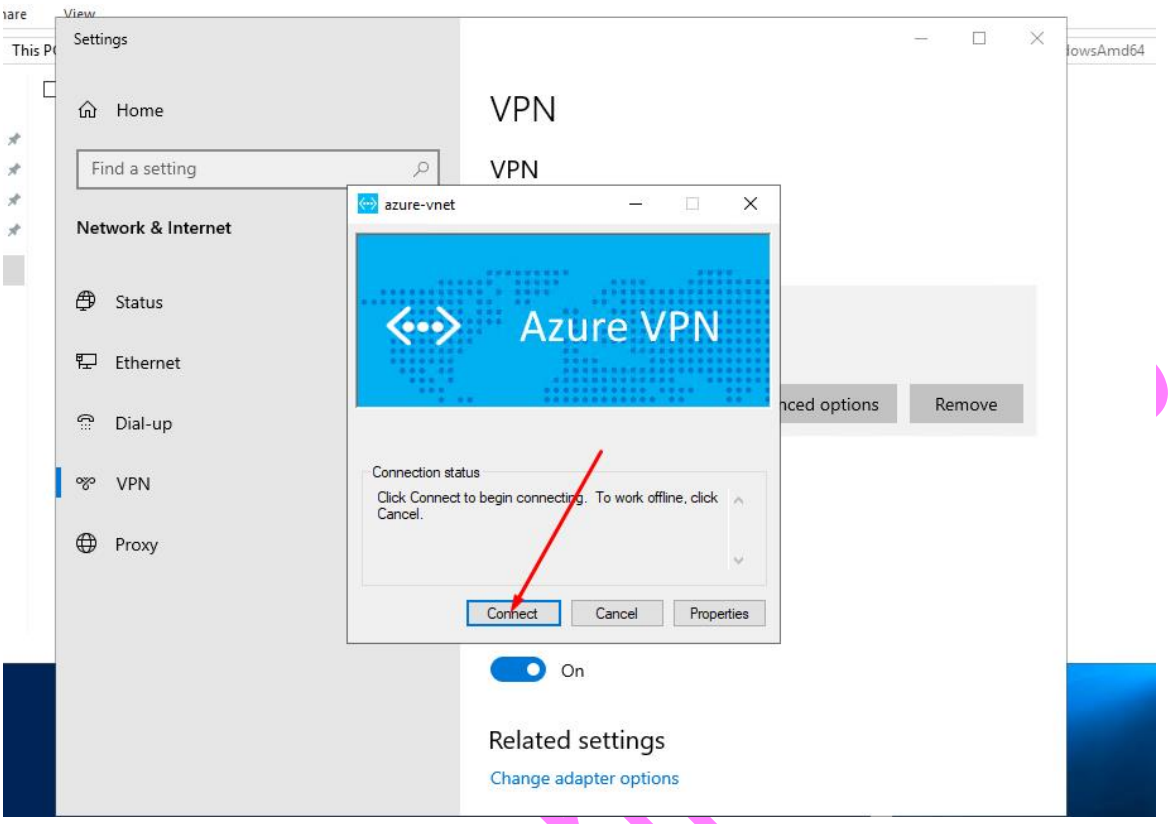
DVS Technologies

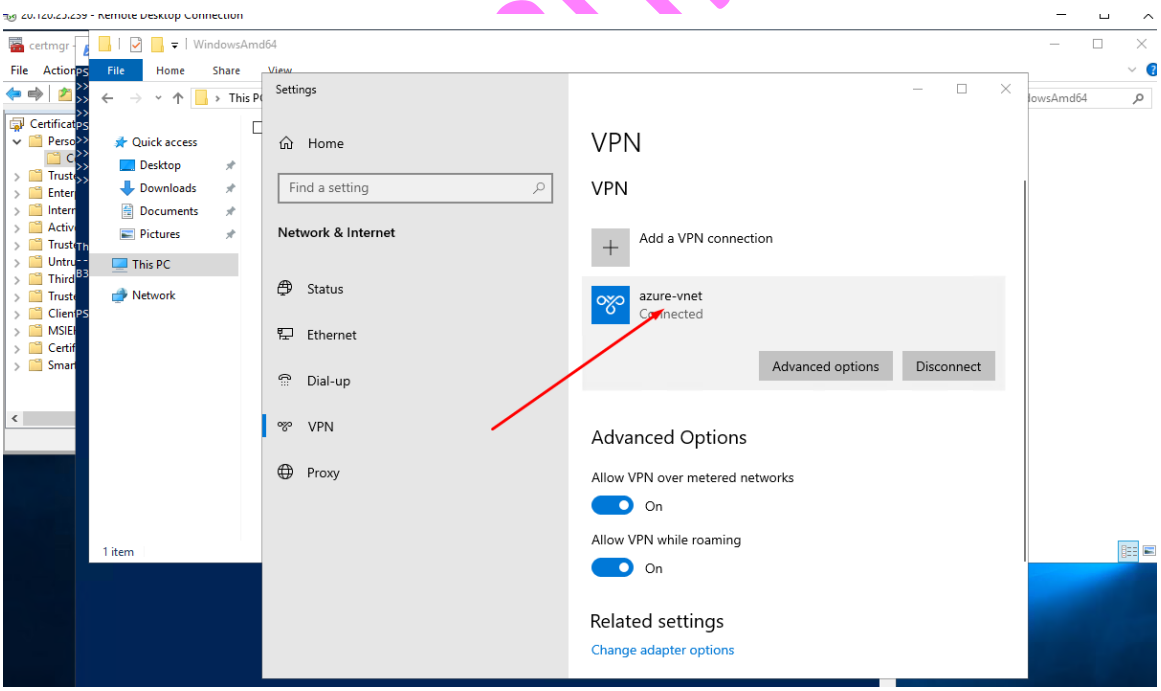

20.120.25.239 - Remote Desktop Connection
Recycle Bin
rootcertific...
This PC
File
Computer
View
This PC
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Folders (7)
3D Objects
Desktop
Documer
Downloads
Music
Pictures
Videos
Devices and drives (3)
Windows (C:)
117 GB free of 126 GB
Temporary Storage (D:)
3.47 GB free of 3.99 GB
DVD Drive
Redirected drives and folders (1)
C on DESKTOP-IOC981H


20.120.25.239 - Remote Desktop Connection
Recycle Bin
rootcertific...
C on DESKTOP-IOC981H
File
Home
Share
View
This PC
C on DESKTOP-IOC981H
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
Size
cygwin64 10/25/2018 5:01 PM File folder
DRIVERS 6/9/2018 6:02 AM File folder
HashiCorp 10/22/2018 5:37 PM File folder
Intel 6/9/2018 5:57 AM File folder
New folder 6/8/2018 5:48 PM File folder
PerfLogs 12/7/2019 9:14 AM File folder
Program Files 12/10/2021 1:32 AM File folder
Program Files (x86) 12/4/2021 8:34 AM File folder
Users 10/30/2021 9:35 AM File folder
Windows 11/7/2021 3:03 PM File folder
Windows10Upgrade 2/26/2020 4:00 AM File folder
myvpngateway 12/12/2021 5:47 PM Compressed (zipp... 290 KB
12 items

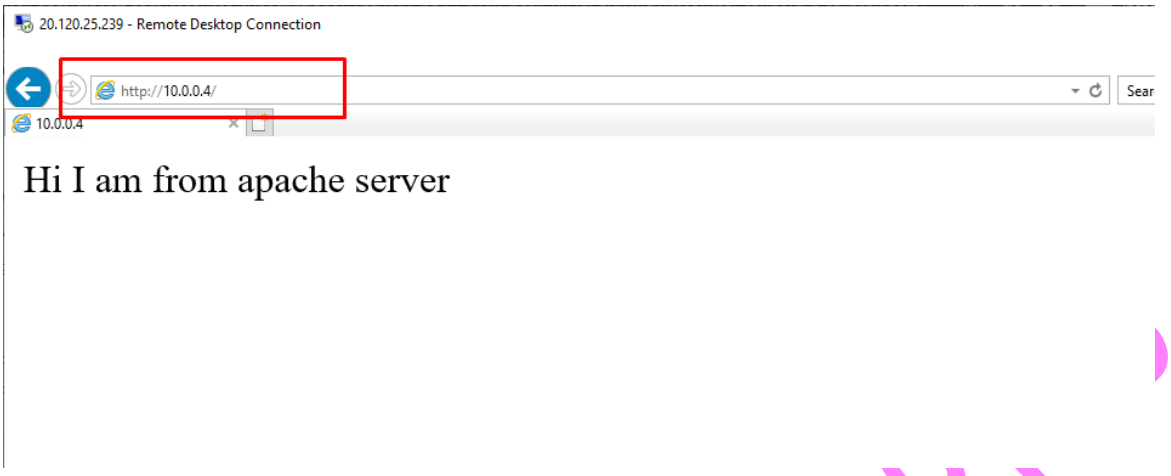

20.120.25.239 - Remote Desktop Connection
Recycle Bin
Manage
WindowsAmd64
File
Home
Share
View
Application Tools
This PC › Desktop › myvpngateway › WindowsAmd64
Search Winc
Quick access
Name
Date modified
Type
Size
ClientSetupAmd64
12/12/2021 5:46 PM
Application
195 KB
Open
Run as administrator
Troubleshoot compatibility
Pin to Start
Share
Give access to
Pin to taskbar
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
1 item
1 item selected 194 KB


Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
Proxy
VPN
VPN
Add a VPN connection
azure-vnet
Advanced Options
Allow VPN over metered networks
On
Allow VPN while roaming
On
Related settings
Change adapter options
Change advanced sharing options
Network and Sharing Center
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
1 item





Now test the connection to azure-server with private ipaddress. Since we connected to VNET we should able to access our application.



Now if you observe above we can able to reach out to the server with private public ipaddress.

DVS Technolog

2 Site to Site VPN

A Site-to-Site VPN connection is used to establish a secure connection between an on-premise network and an Azure network via the Internet.
Below is a diagram from the Microsoft documentation on a sample scenario

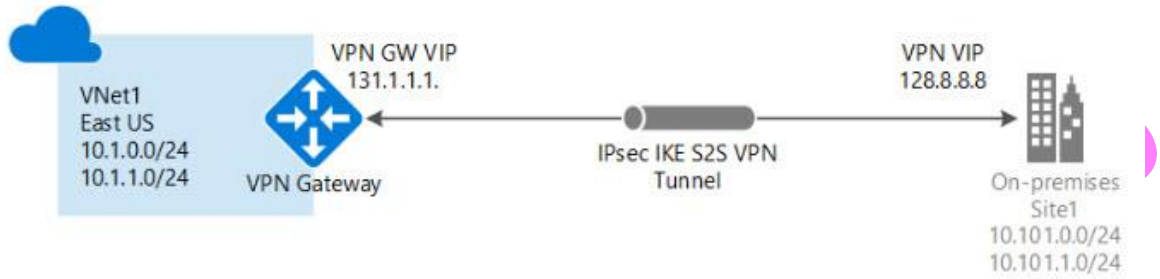
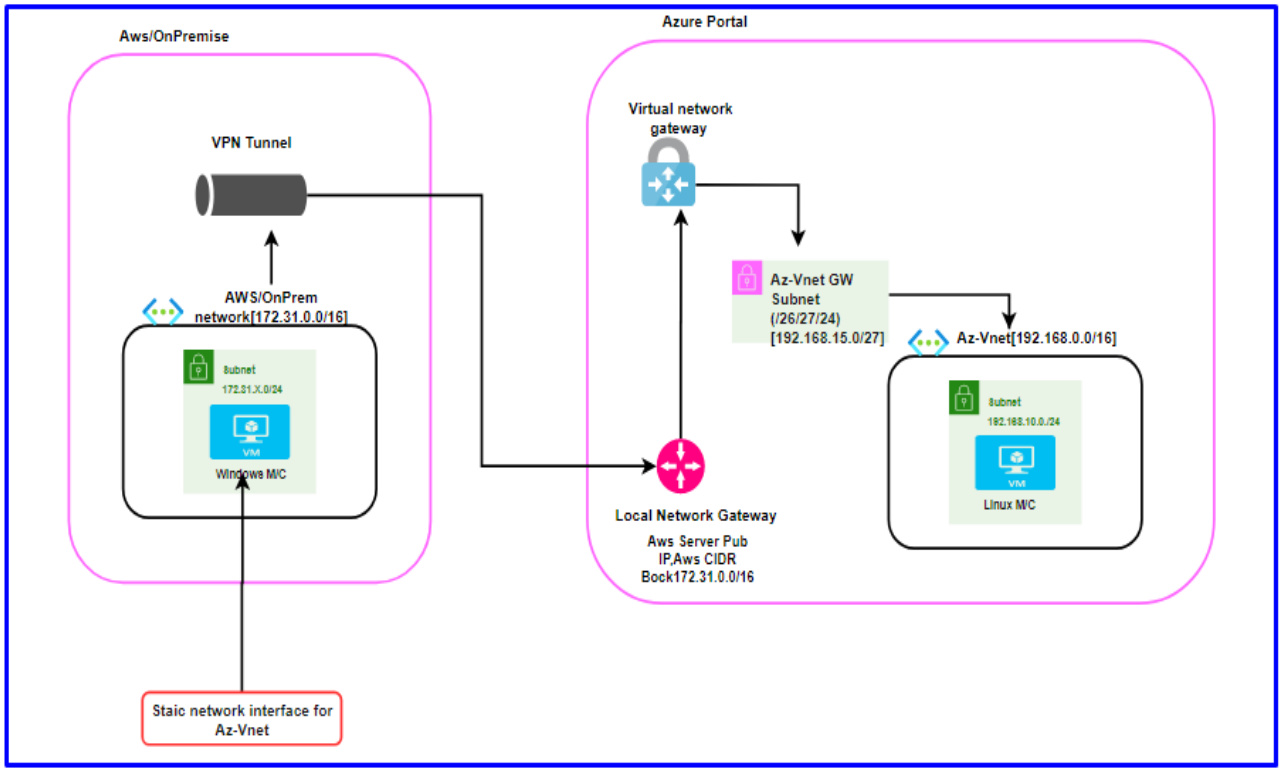


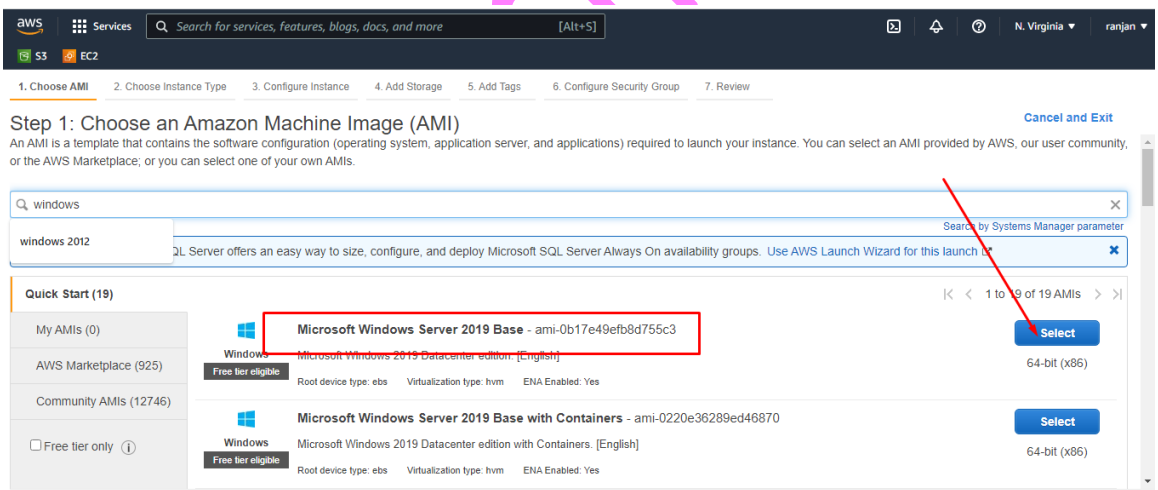
Image reference - https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

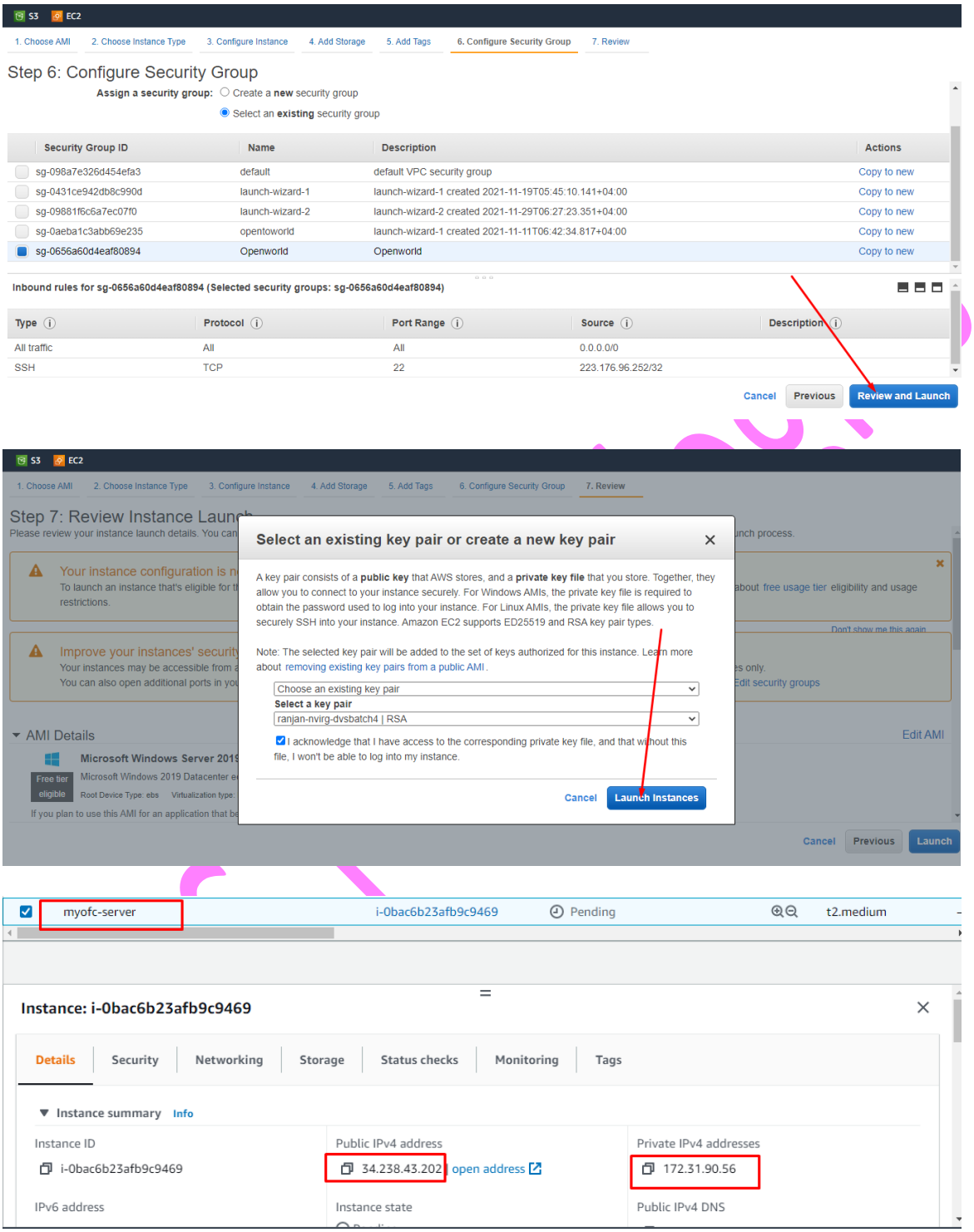
On the on-premise side, you need to have a VPN device that can route traffic via the Internet onto the VPN gateway in Azure.
The VPN device can be a hardware device like a Cisco router or a software device (e.g Windows Server 2016 running Routing and Remote services).
The VPN device needs to have a publically routable IP address.
The subnets in your on-premise network must not overlap with the subnets in your Azure virtual network
The Site-to-Site VPN connection uses an IPSec tunnel to encrypt the traffic.
The VPN gateway resource you create in Azure is used to route encrypted traffic between your on-premise data center and your Azure virtual network.
There are different SKU's for the Azure VPN gateway service. Each SKU has a different pricing and attributes associated with it - Reference - https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings

Let's do the site-to-site vpn connectivity since we don't have the on-premise hence let's do the configuration between Aws & Azure
We are going to configure the S2S connectivity between Aws & Azure so that we can connect azure servers directly from aws.
Building windows server in AWS:
We are going to build vm in the network 172.31.0.0/16

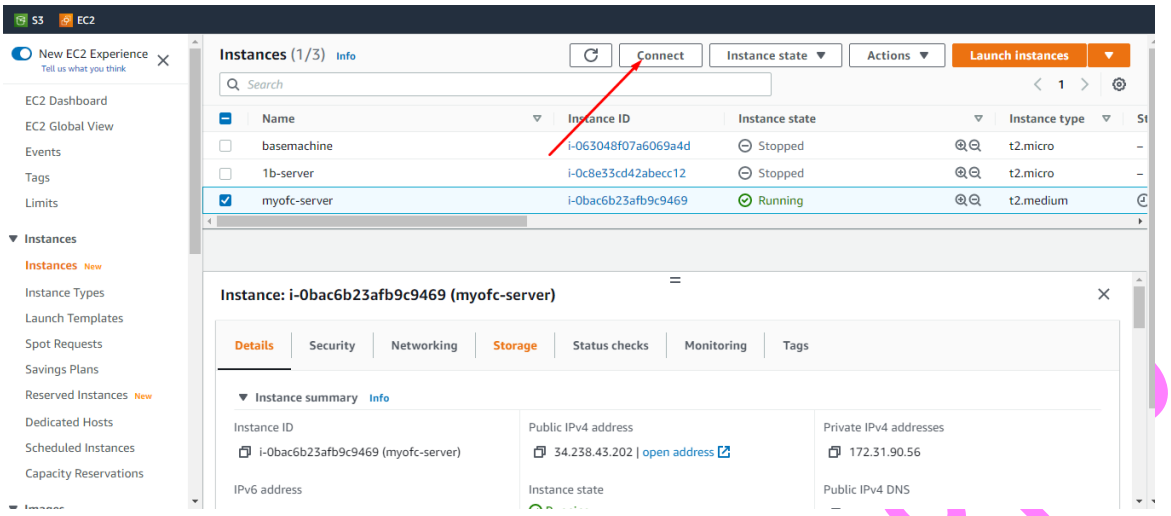
DVS Technologies

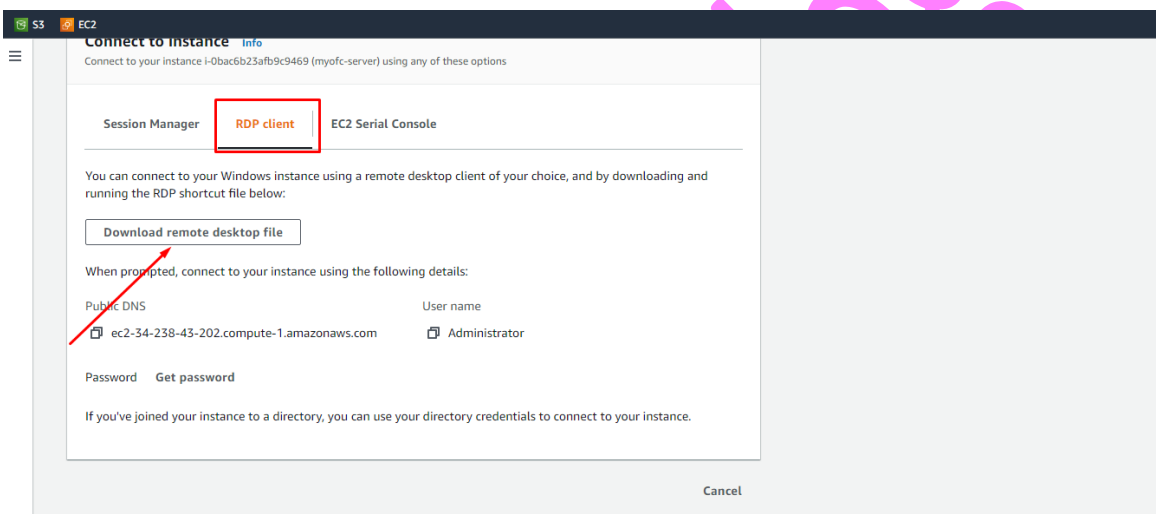

Aws/OnPremise
Azure Portal
VPN Tunnel
Virtual network gateway
AWS/OnPrem network[172.31.0.0/16]
Az-Vnet GW Subnet (/26/27/24) [192.168.15.0/27]
Az-Vnet[192.168.0.0/16]
Subnet 172.31.X.0/24
VM
Windows M/C
Subnet 192.168.10.0/24
VM
Linux M/C
Local Network Gateway
Aws Server Pub IP,Aws CIDR Bock172.31.0.0/16
Staic network interface for Az-Vnet

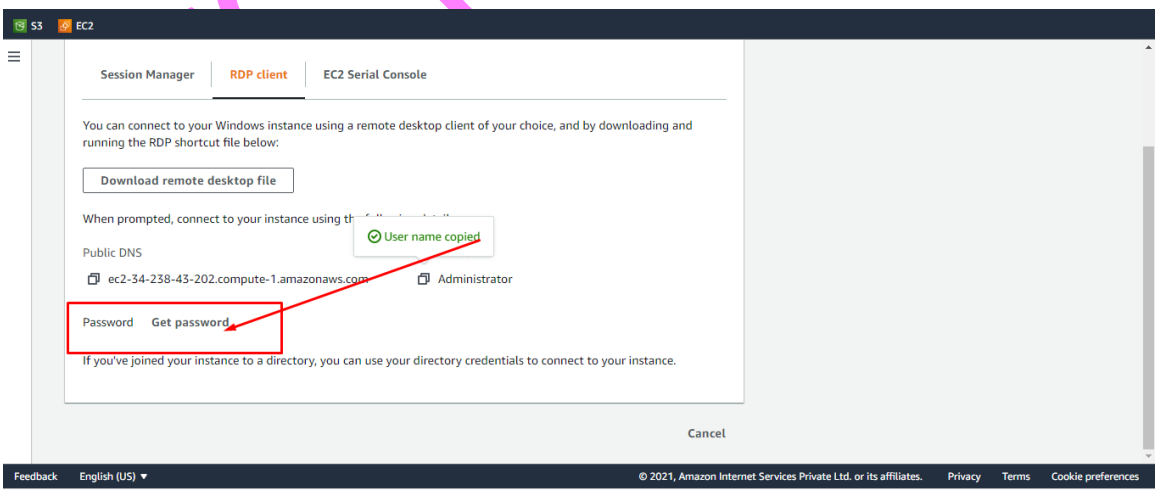

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
ranjan
S3
EC2
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 1: Choose an Amazon Machine Image (AMI)
Cancel and Exit
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.
windows
windows 2012
Search by Systems Manager parameter
Quick Start (19)
1 to 19 of 19 AMIs
My AMIs (0)
AWS Marketplace (925)
Community AMIs (12746)
Free tier only
Microsoft Windows Server 2019 Base - ami-0b17e49efb8d755c3
Microsoft Windows 2019 Datacenter edition. [English]
Windows
Free tier eligible
Root device type: ebs
Virtualization type: hvm
ENA Enabled: Yes
Select
64-bit (x86)
Microsoft Windows Server 2019 Base with Containers - ami-0220e36289ed46870
Microsoft Windows 2019 Datacenter edition with Containers. [English]
Windows
Free tier eligible
Root device type: ebs
Virtualization type: hvm
ENA Enabled: Yes
Select
64-bit (x86)

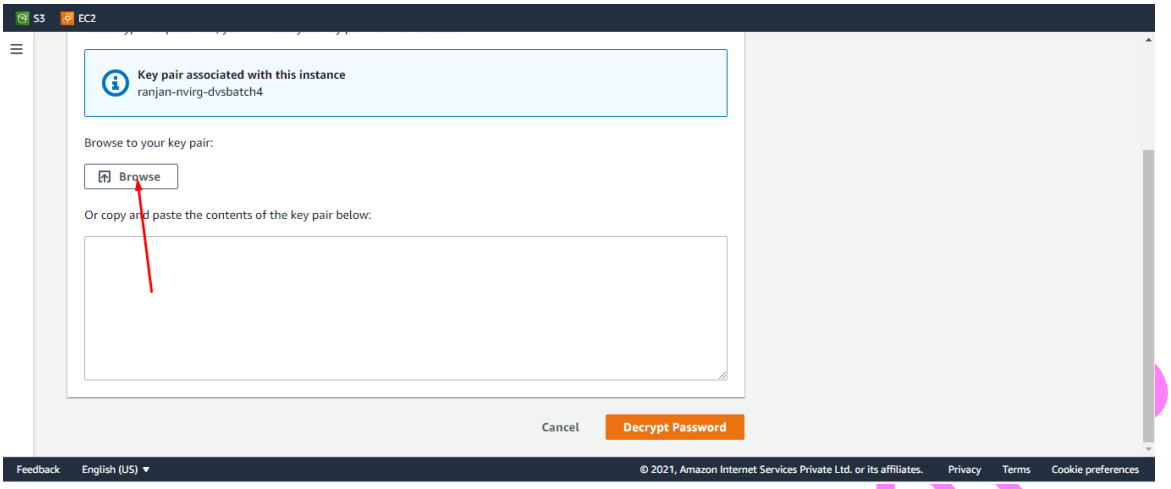


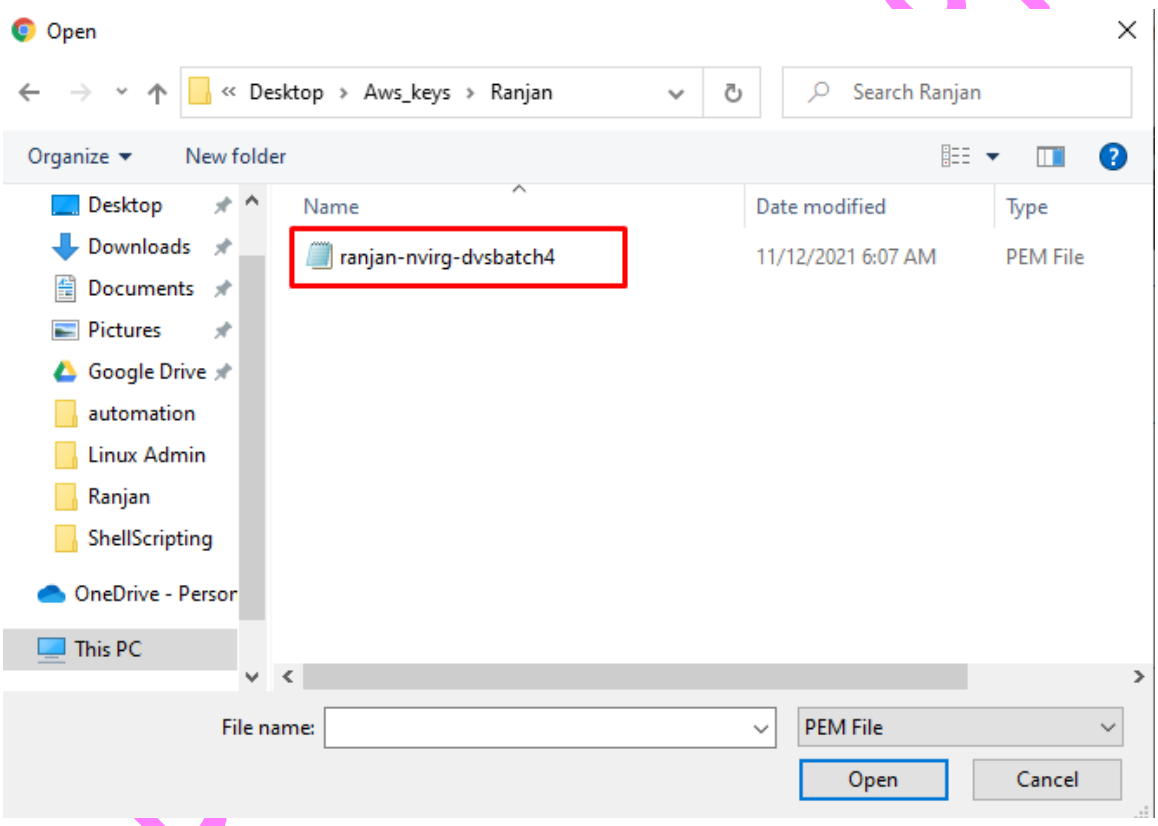
Let's login to the aws vm

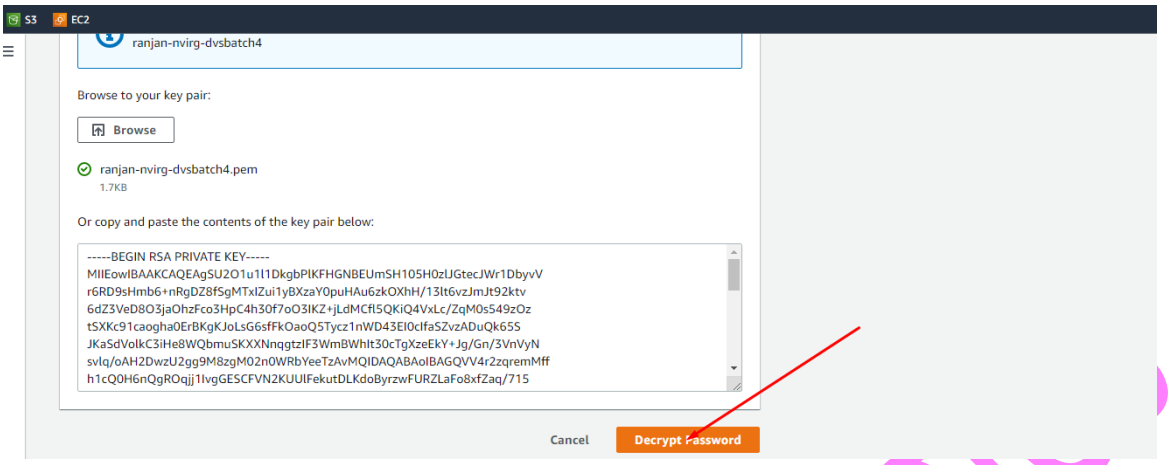

S3
EC2
New EC2 Experience
Tell us what you think
EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances
Instances New
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances New
Dedicated Hosts
Scheduled Instances
Capacity Reservations
Instances (1/3) Info
Connect
Instance state
Actions
Launch instances
Search
Name
Instance ID
Instance state
Instance type
basemachine
i-063048f07a6069a4d
Stopped
t2.micro
1b-server
i-0c8e33cd42abecc12
Stopped
t2.micro
myofc-server
i-0bac6b23afb9c9469
Running
t2.medium
Instance: i-0bac6b23afb9c9469 (myofc-server)
Details
Security
Networking
Storage
Status checks
Monitoring
Tags
Instance summary Info
Instance ID
i-0bac6b23afb9c9469 (myofc-server)
Public IPv4 address
34.238.43.202 | open address
Private IPv4 addresses
172.31.90.56
IPv6 address
Instance state
Public IPv4 DNS

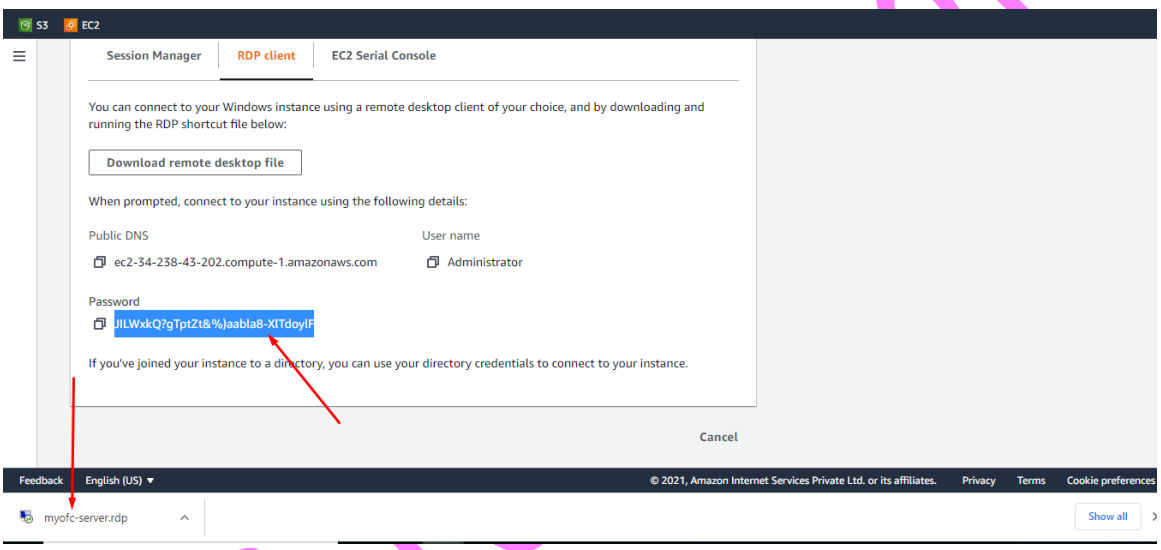

S3
EC2
Connect to instance Info
Connect to your instance i-0bac6b23afb9c9469 (myofc-server) using any of these options
Session Manager
RDP client
EC2 Serial Console
You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:
Download remote desktop file
When prompted, connect to your instance using the following details:
Public DNS
ec2-34-238-43-202.compute-1.amazonaws.com
User name
Administrator
Password
Get password
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.
Cancel

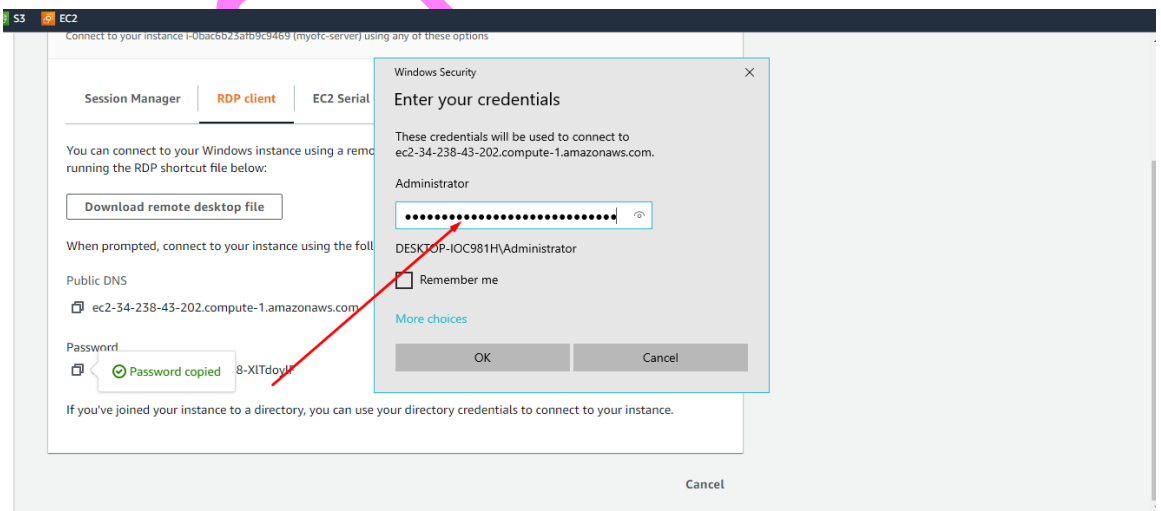

S3
EC2
Session Manager
RDP client
EC2 Serial Console
You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:
Download remote desktop file
User name copied
Public DNS
ec2-34-238-43-202.compute-1.amazonaws.com
Administrator
Password
Get password
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.
Cancel
Feedback
English (US)
© 2021, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

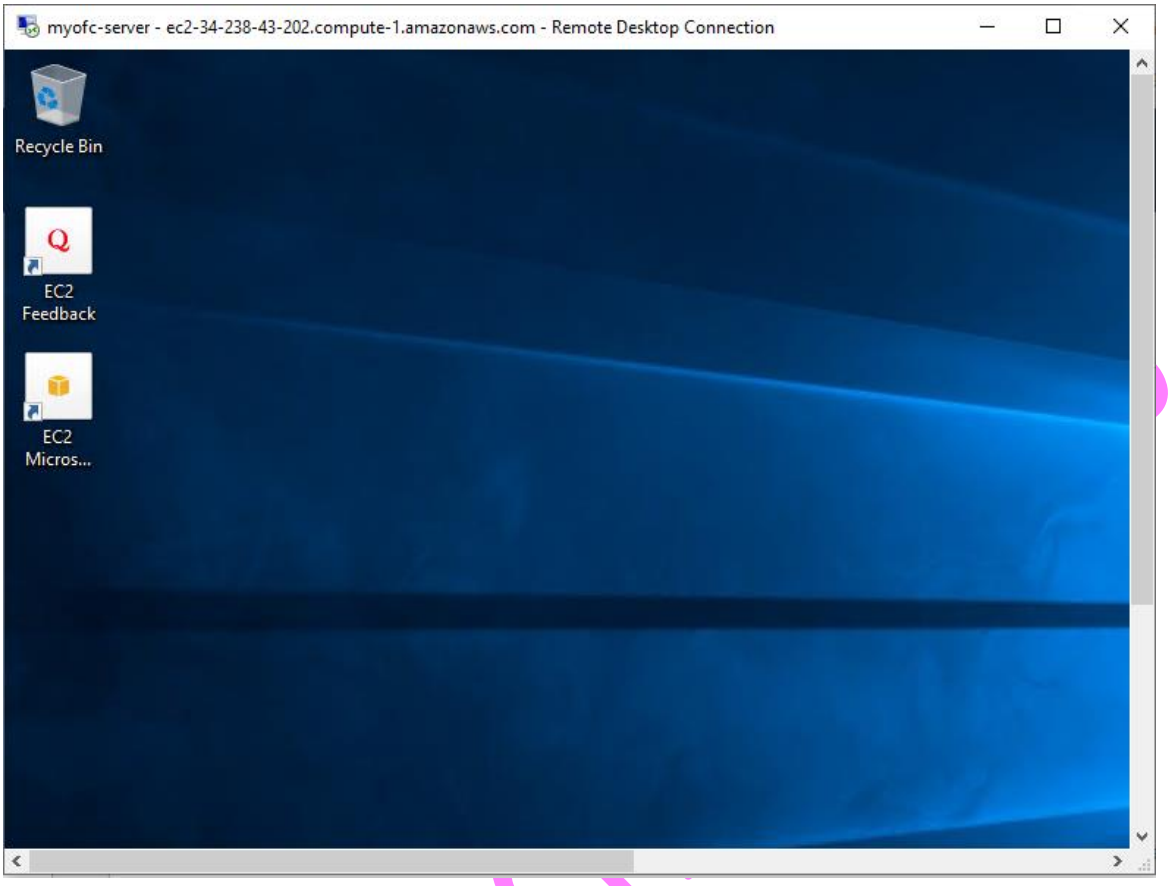

S3
EC2
Key pair associated with this instance
ranjan-nvirg-dvsbatch4
Browse to your key pair:
Browse
Or copy and paste the contents of the key pair below:
Cancel
Decrypt Password
Feedback
English (US)
© 2021, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences


Open
Desktop › Aws_keys › Ranjan
Search Ranjan
Organize
New folder
Desktop
Downloads
Documents
Pictures
Google Drive
automation
Linux Admin
Ranjan
ShellScripting
OneDrive - Persor
This PC
Name
Date modified
Type
ranjan-nvirg-dvsbatch4
11/12/2021 6:07 AM
PEM File
File name:
PEM File
Open
Cancel

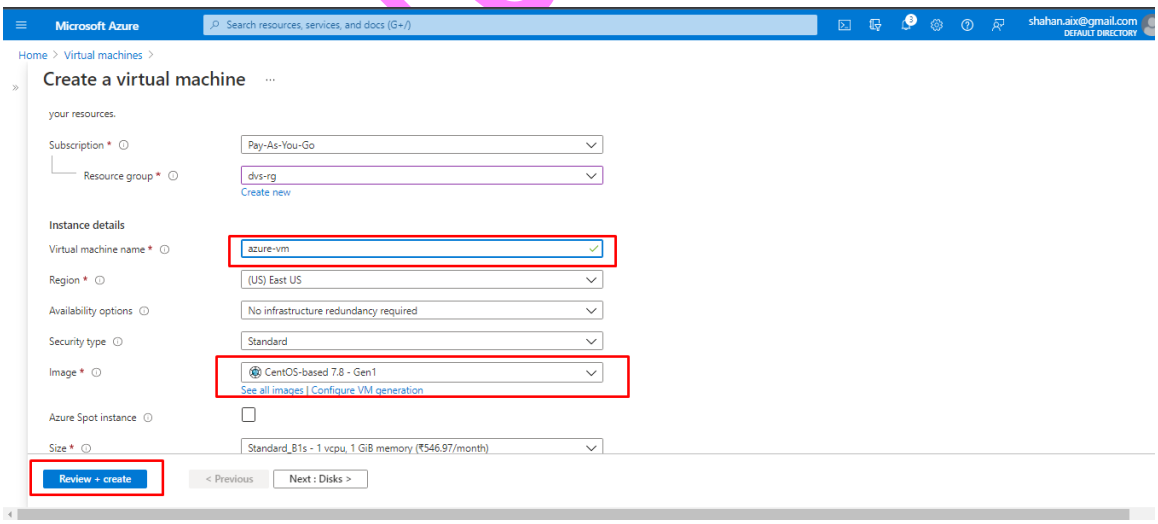

S3
EC2
ranjan-nvirg-dvsbatch4
Browse to your key pair:
Browse
ranjan-nvirg-dvsbatch4.pem
1.7KB
Or copy and paste the contents of the key pair below:
-----BEGIN RSA PRIVATE KEY-----
Cancel
Decrypt Password


S3
EC2
Session Manager
RDP client
EC2 Serial Console
You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:
Download remote desktop file
When prompted, connect to your instance using the following details:
Public DNS
ec2-34-238-43-202.compute-1.amazonaws.com
User name
Administrator
Password
JILWxkQ?gTptZt&%)aabla8-XlTdoylF
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.
Cancel
Feedback
English (US)
© 2021, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
myofc-server.rdp
Show all

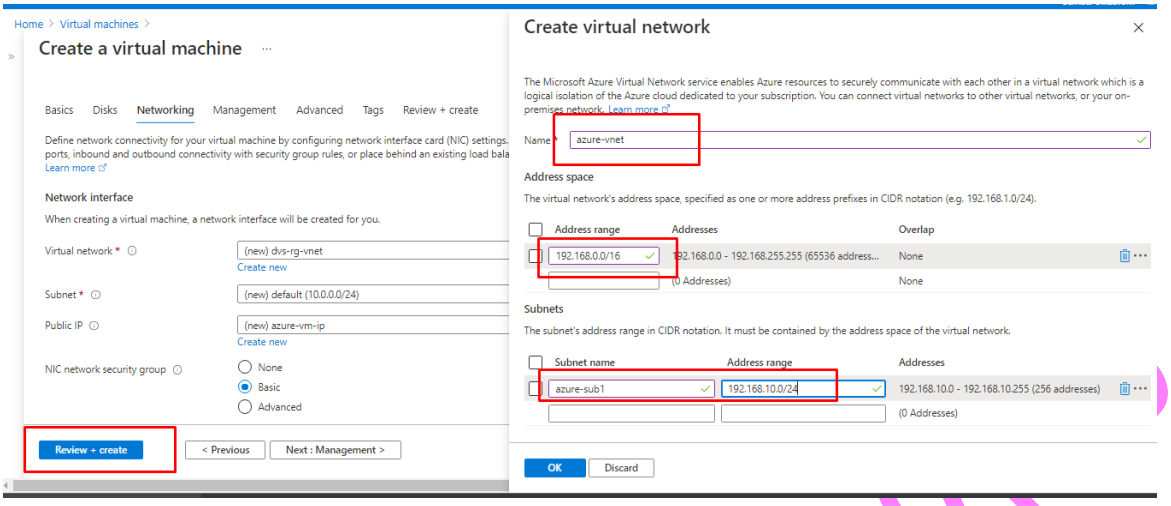

S3
EC2
Windows Security
Enter your credentials
These credentials will be used to connect to ec2-34-238-43-202.compute-1.amazonaws.com.
Administrator
DESKTOP-IOC981H\Administrator
Remember me
More choices
OK
Cancel
Session Manager
RDP client
Download remote desktop file
Public DNS
ec2-34-238-43-202.compute-1.amazonaws.com
Password
Password copied
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.
Cancel



Now let's build the azure network & servers so that we can connect to the azure from aws servers.

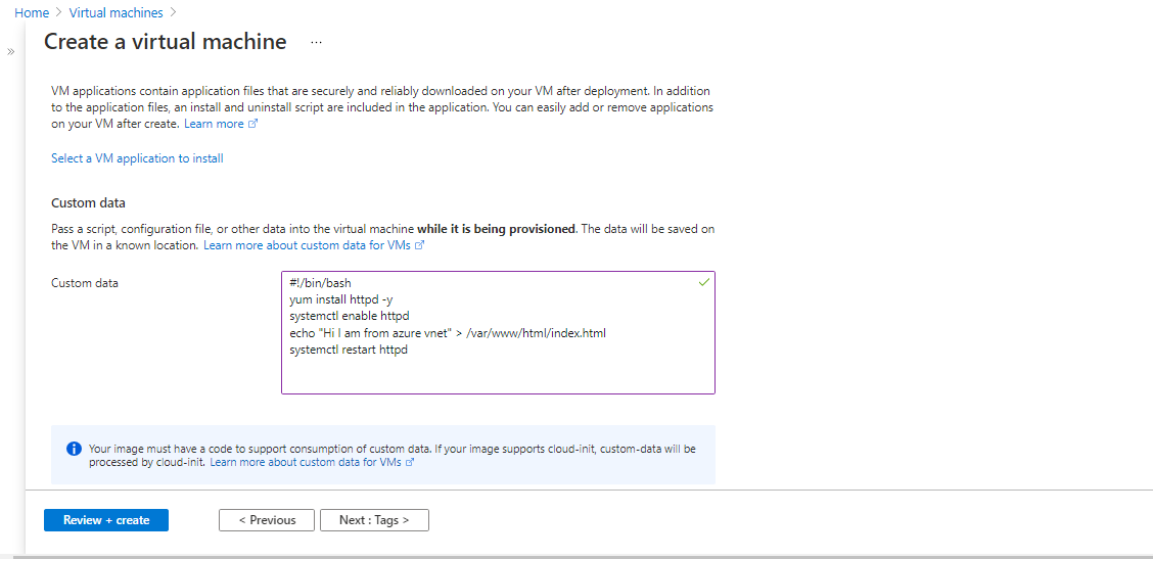


We are going to take 192.168.0.0/16 for azure network & 192.168.10.0/24 as vm subnet.

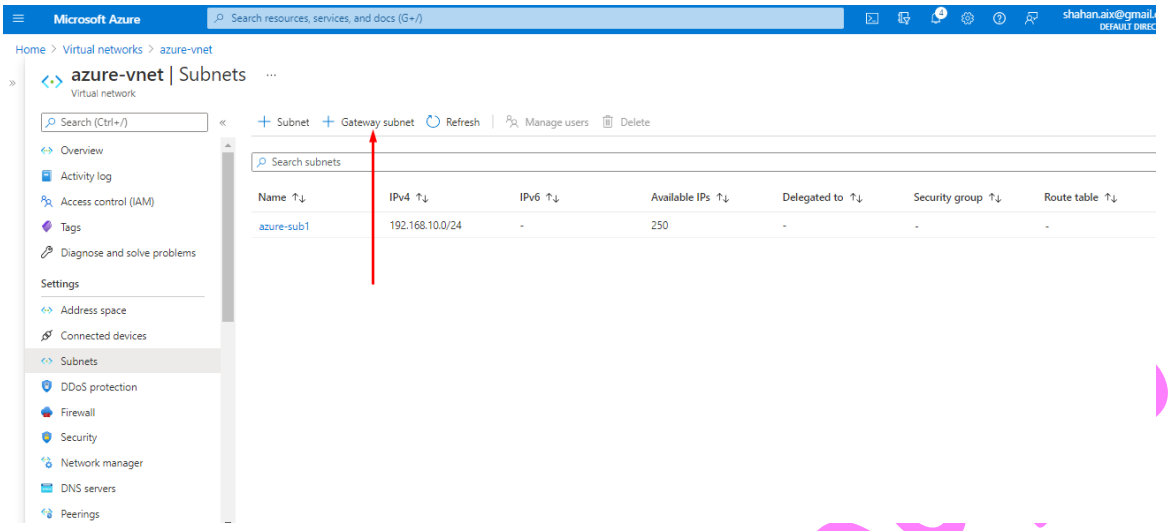


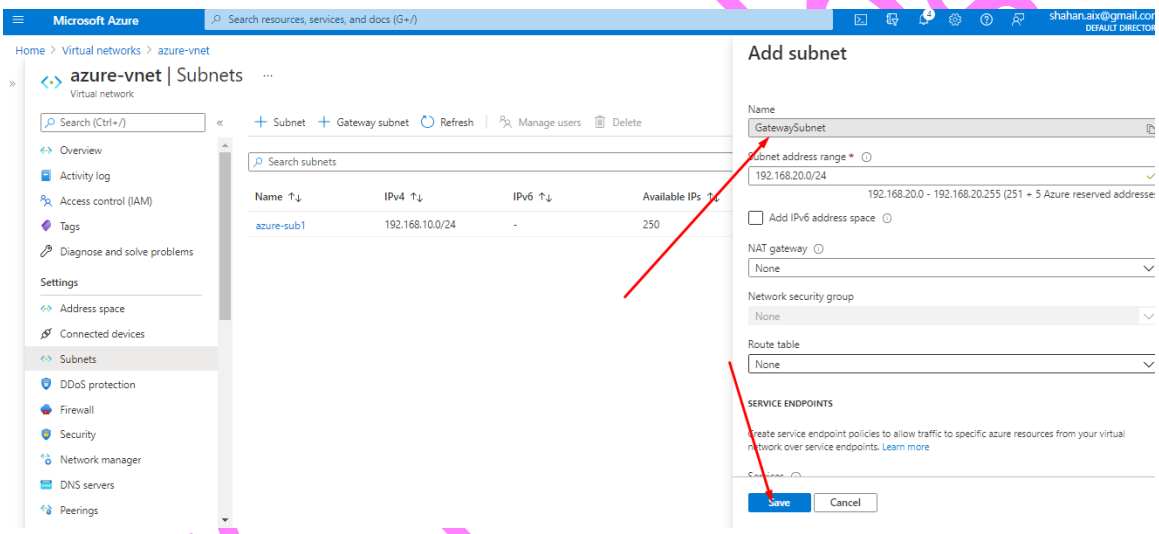
Let's configure the apache

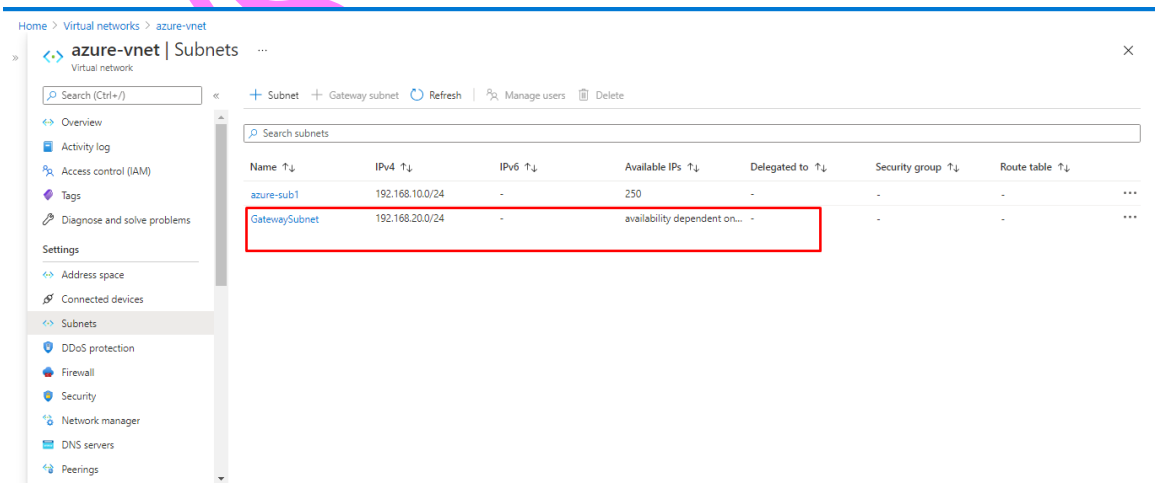
```
#!/bin/bash
yum install httpd -y
systemctl enable httpd
echo "Hi I am from azure vnet" > /var/www/html/index.html
systemctl restart httpd
```



Now let's configure the gateway subnet for our azure VNET so that we can create the virtual network gateway







Let's create virtual network gateway

Home >

Virtual network gateways

Default Directory

+ Create | Manage view | Refresh | Export to CSV | Open query | Assign tags | Feedback

Filter for any field... | Subscription == all | Resource group == all | Location == all | Add filter

Showing 0 to 0 of 0 records. | No grouping | List view

Name

No virtual network gateways to display

Azure VPN Gateway connects your on-premises networks to Azure through Site-to-Site VPNs in a similar way that you set up and connect to a remote branch office. The connectivity is secure and uses the industry-standard protocols Internet Protocol Security (IPsec) and Internet Key Exchange (IKE).

Create virtual network gateway

Learn more about Virtual network gateway

Home > Virtual network gateways >

Create virtual network gateway

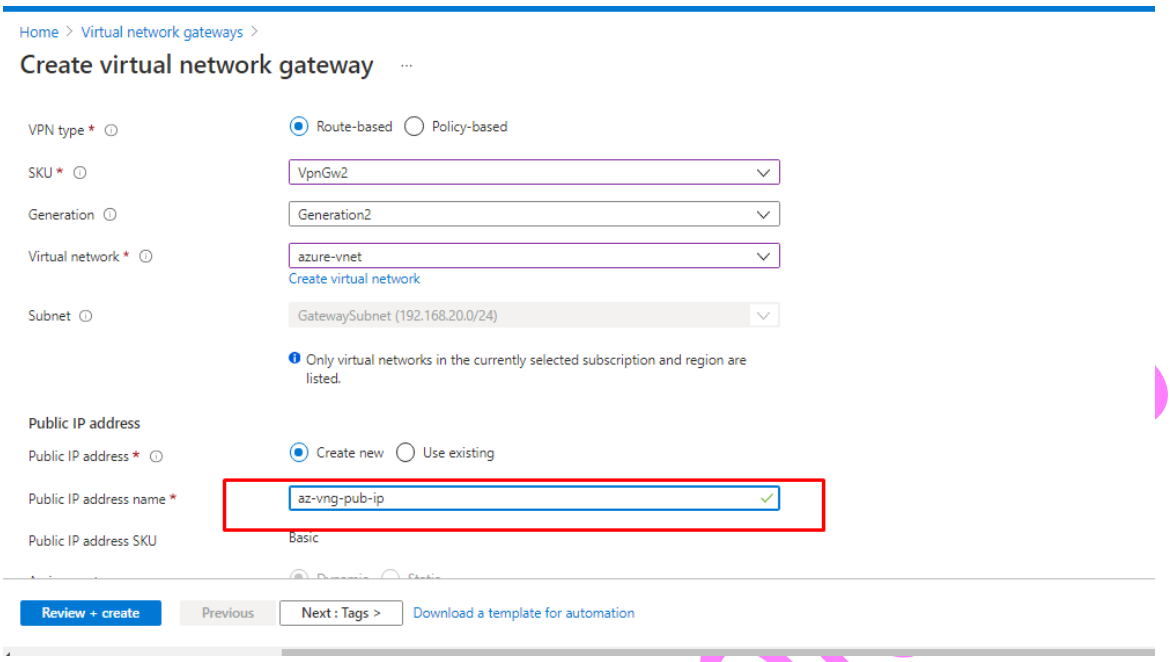
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

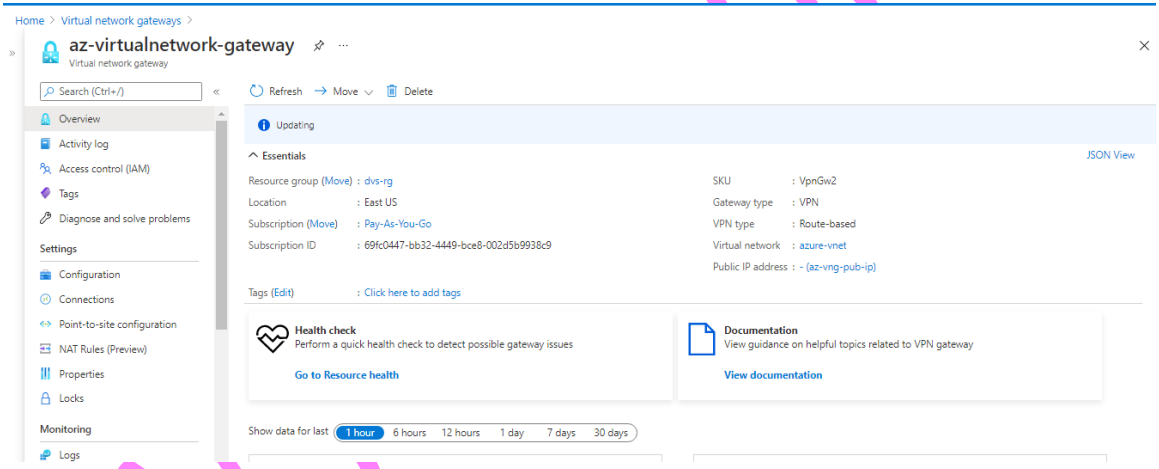
Subscription *	Pay-As-You-Go
Resource group	Select a virtual network to get resource group

Instance details

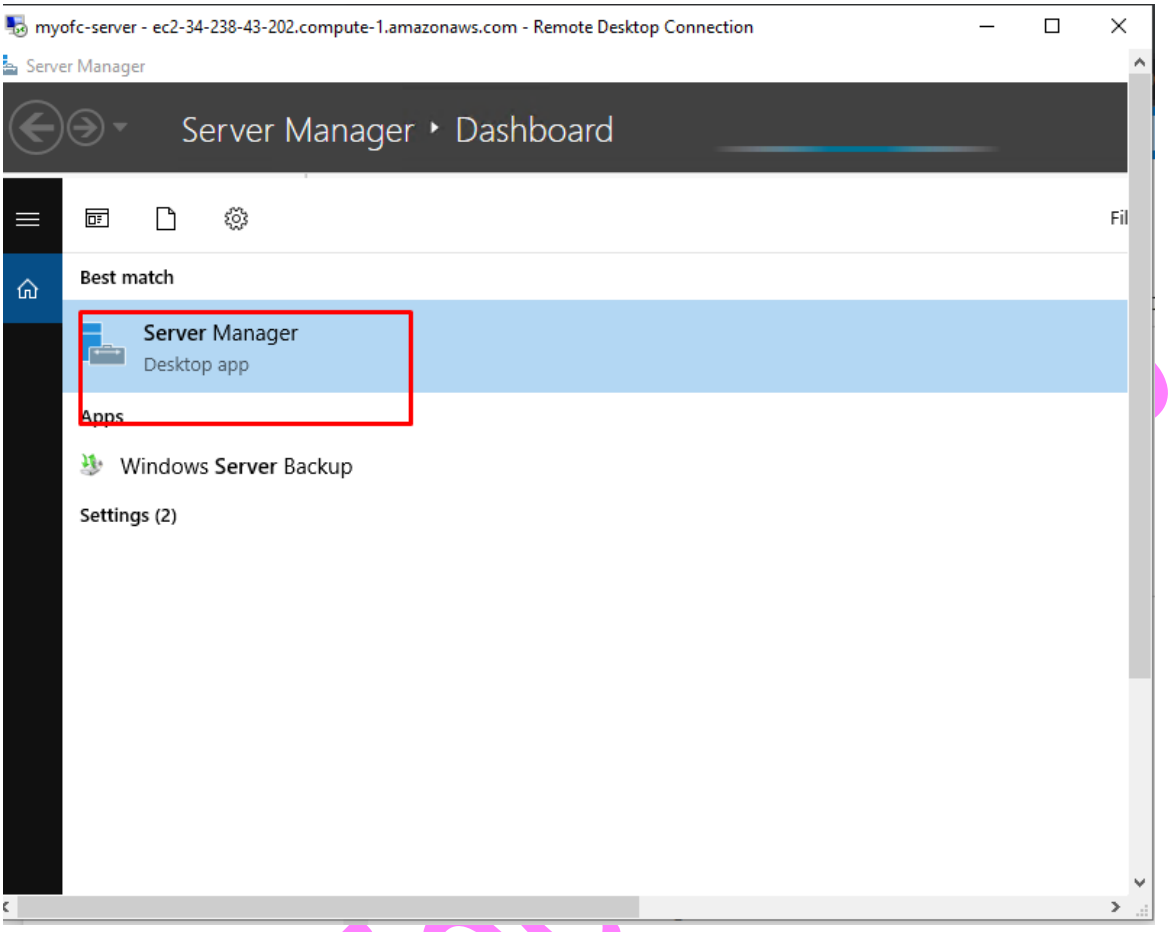
Name *	az-virtualnetwork-gateway
Region *	East US
Gateway type *	VPN / ExpressRoute
VPN type *	Route-based / Policy-based
SKU *	VpnGw2
Generation	Generation2
Virtual network *	

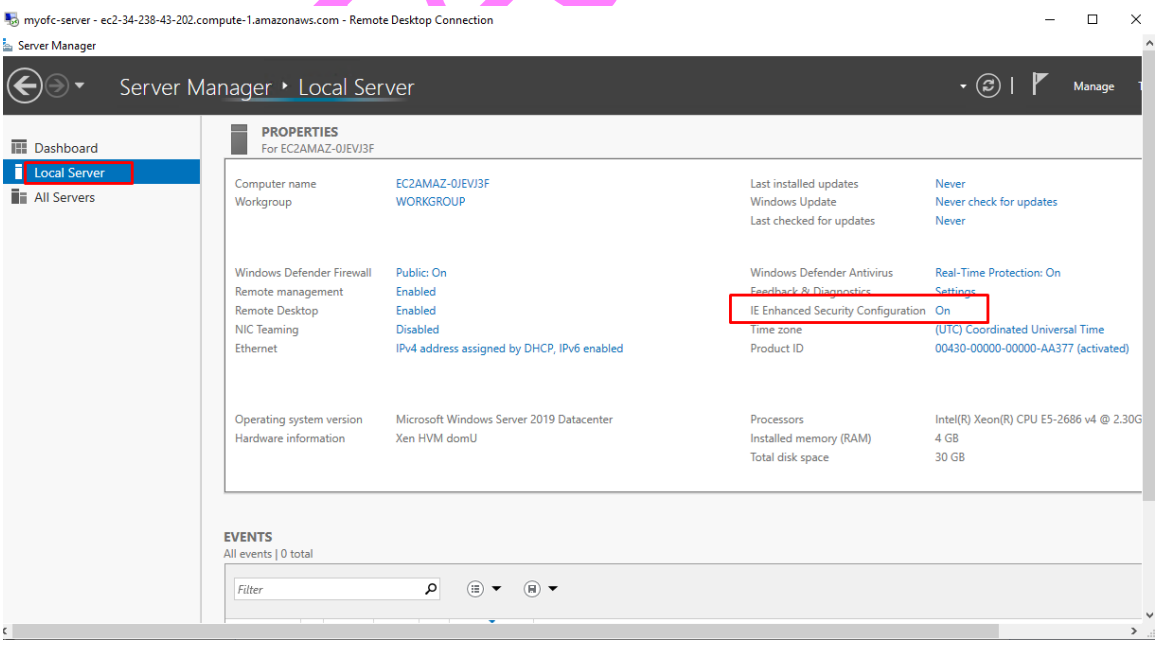
Review + create | Previous | Next : Tags > | Download a template for automation

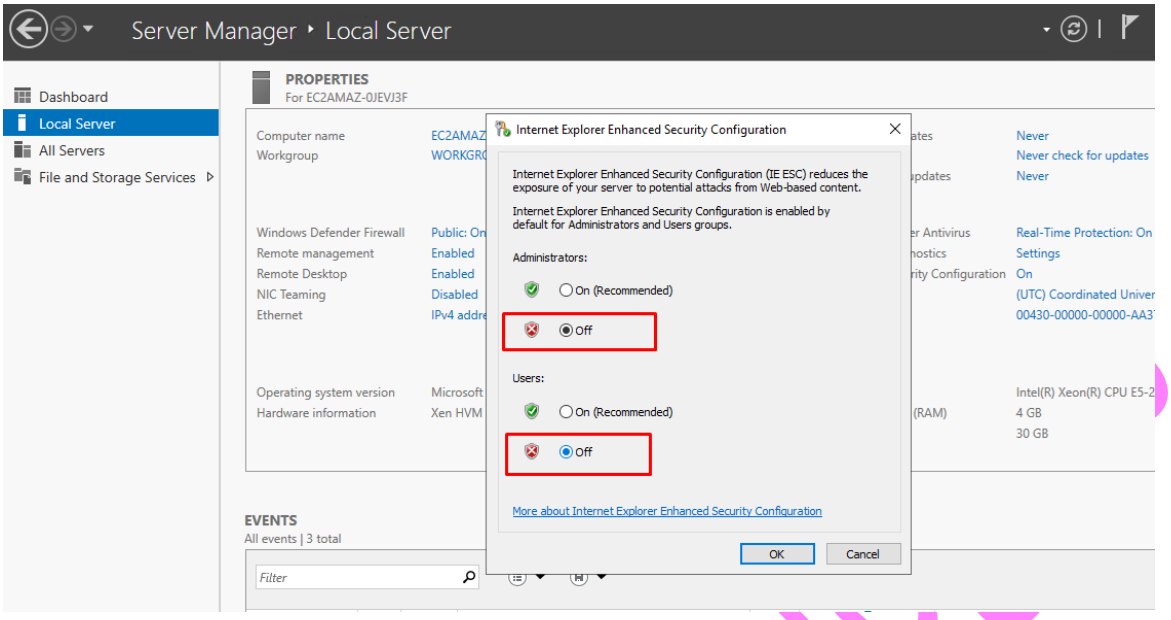


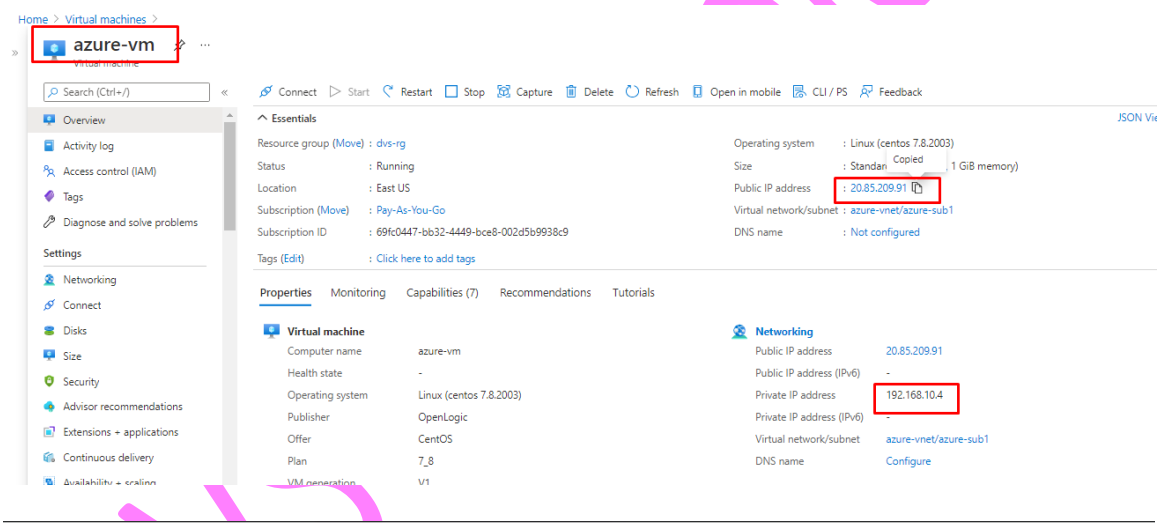


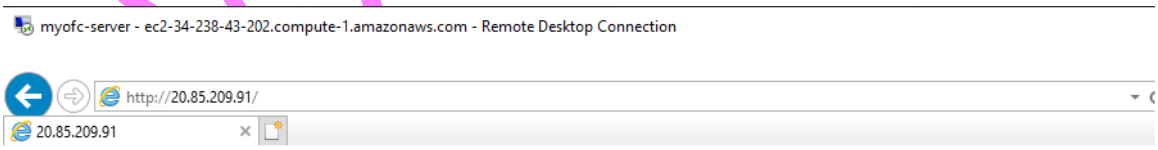
Now let's test the connectivity of azure vm from aws vm with public ip & private ip. We should connect with public & it will fail with priavate ip


myofc-server - ec2-34-238-43-202.compute-1.amazonaws.com - Remote Desktop Connection
Server Manager
Server Manager ‣ Dashboard
Best match
Server Manager
Desktop app
Apps
Windows Server Backup
Settings (2)


myofc-server - ec2-34-238-43-202.compute-1.amazonaws.com - Remote Desktop Connection
Server Manager
Server Manager ‣ Local Server
Manage
Dashboard
Local Server
All Servers
PROPERTIES
For EC2AMAZ-0JEVJ3F
Computer name EC2AMAZ-0JEVJ3F
Workgroup WORKGROUP
Last installed updates Never
Windows Update Never check for updates
Last checked for updates Never
Windows Defender Firewall Public: On
Remote management Enabled
Remote Desktop Enabled
NIC Teaming Disabled
Ethernet IPv4 address assigned by DHCP, IPv6 enabled
Windows Defender Antivirus Real-Time Protection: On
Feedback & Diagnostics Settings
IE Enhanced Security Configuration On
Time zone (UTC) Coordinated Universal Time
Product ID 00430-00000-00000-AA377 (activated)
Operating system version Microsoft Windows Server 2019 Datacenter
Hardware information Xen HVM domU
Processors Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30G
Installed memory (RAM) 4 GB
Total disk space 30 GB
EVENTS
All events | 0 total
Filter







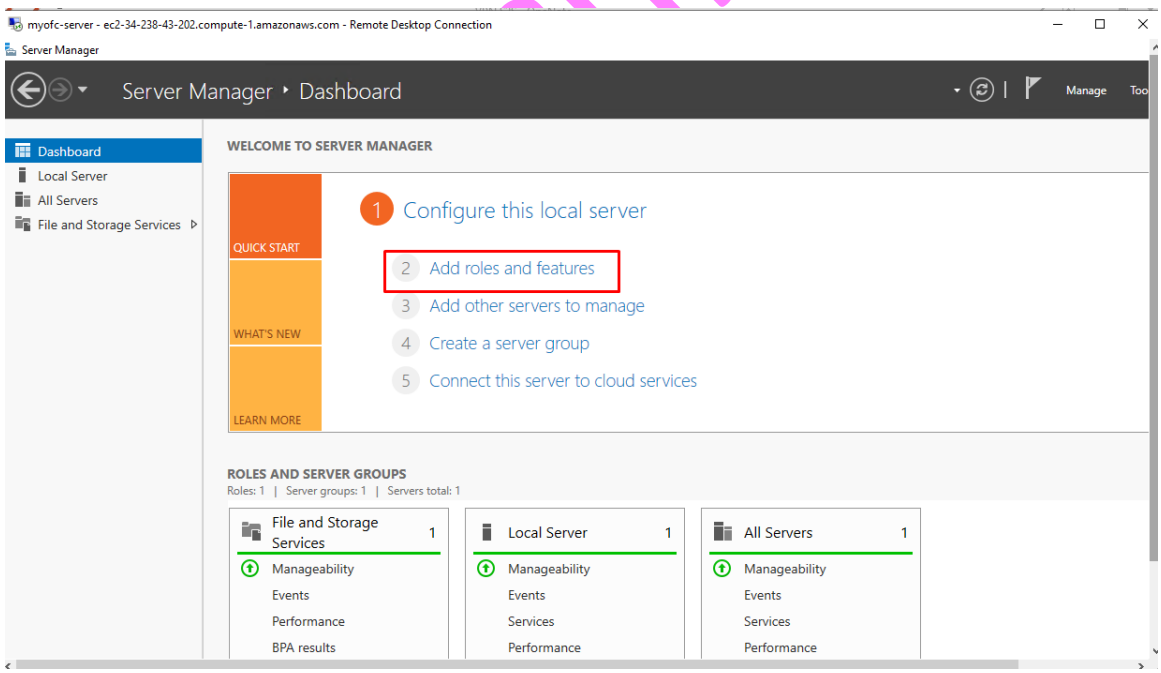
Hi I am from azure vnet

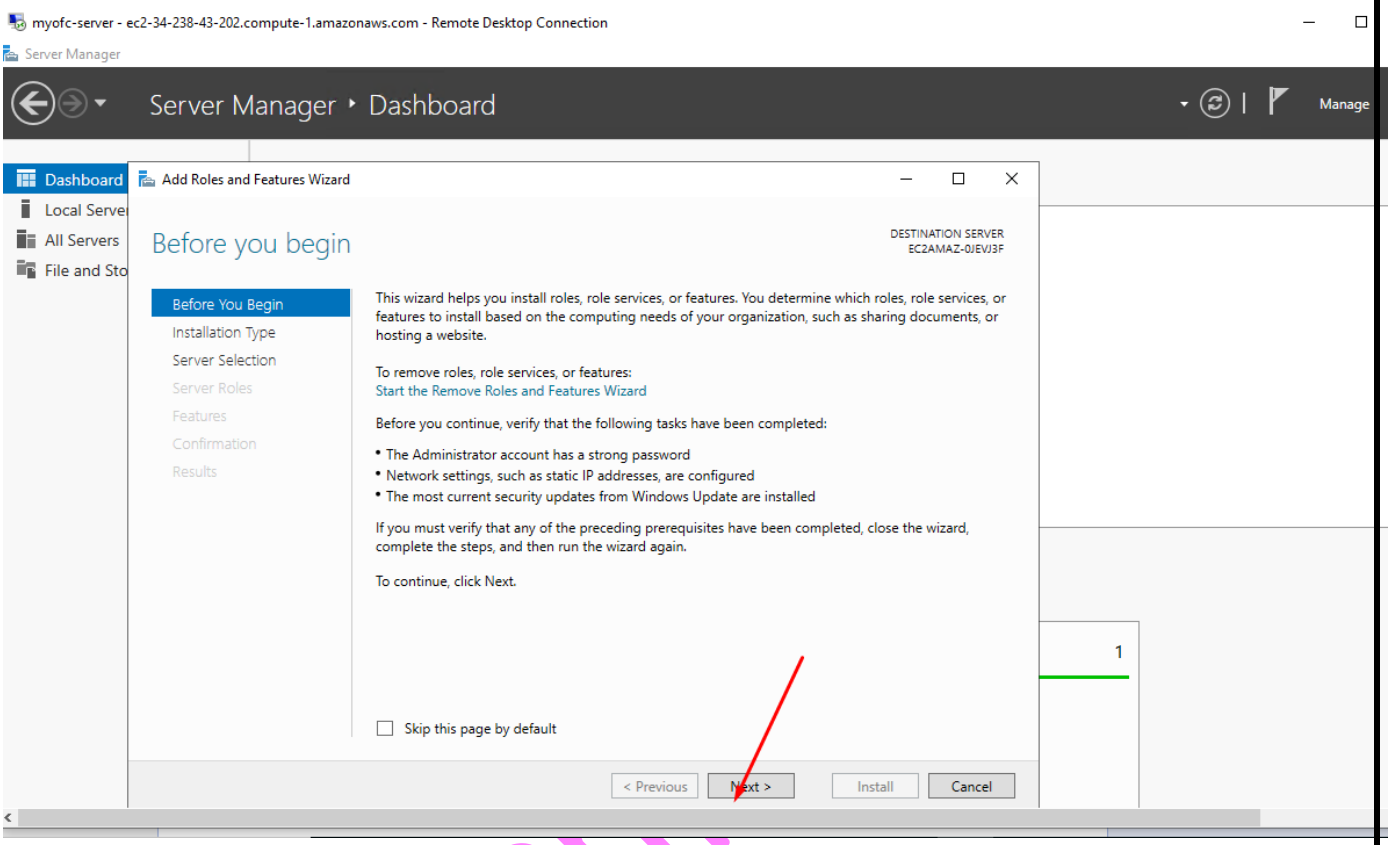
an't reach this page

- Make sure the web address http://192.168.10.4 is correct
- Search for this site on Bing
- Refresh the page

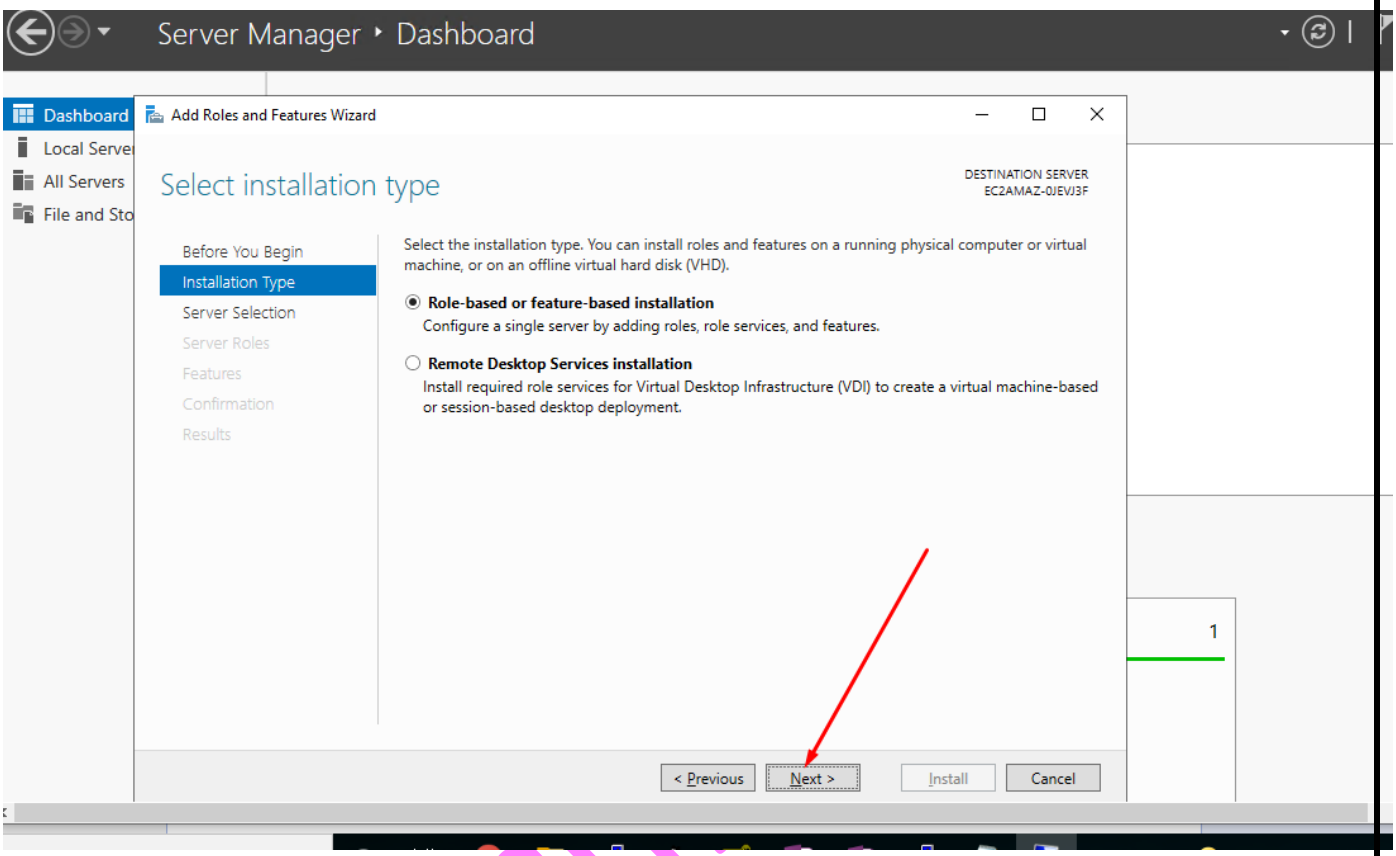
More information

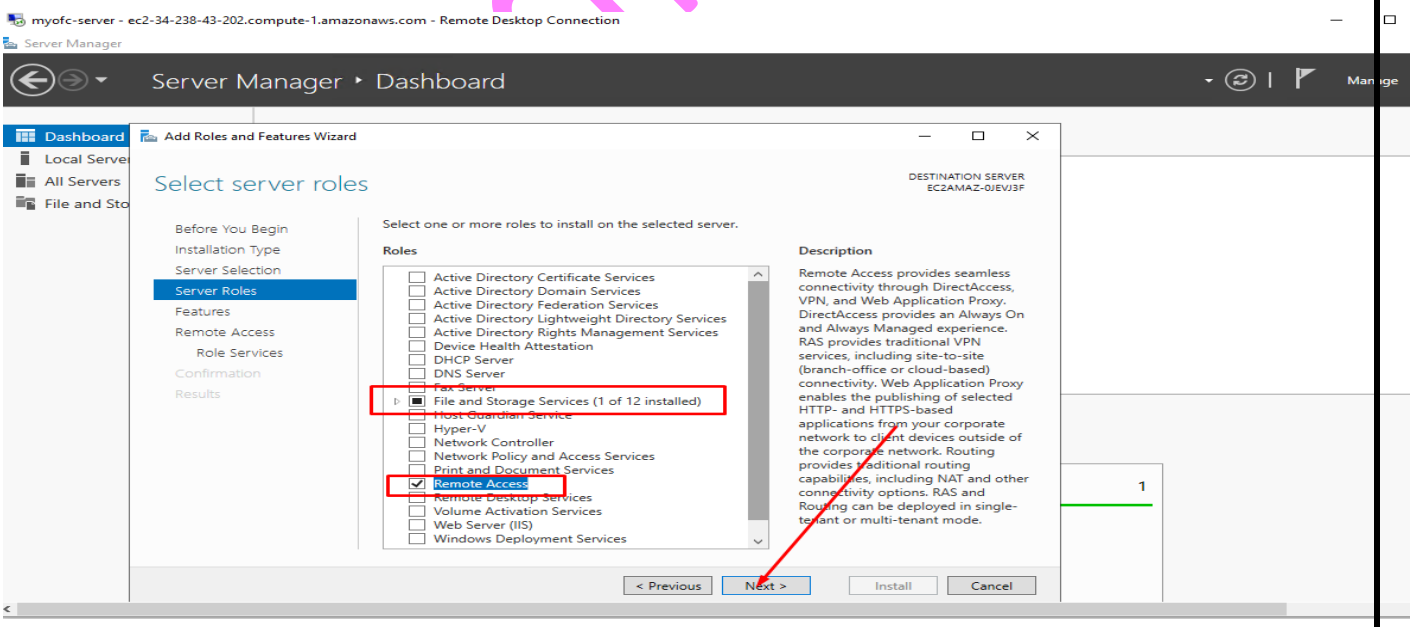
Let's configure the S2S vpn so that we can connect the azure vm from aws vm
We need to have localgateway inorder to configure this setup and need to configure roles in the windows server
Do the below in aws windows server:




myofc-server - ec2-34-238-43-202.compute-1.amazonaws.com - Remote Desktop Connection
Server Manager
Server Manager ‣ Dashboard
Manage
Dashboard
Local Serve
All Servers
File and Sto
Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
EC2AMAZ-0JEVJ3F
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.
To remove roles, role services, or features:
Start the Remove Roles and Features Wizard
Before you continue, verify that the following tasks have been completed:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The most current security updates from Windows Update are installed
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel
1

DVS Techn


Server Manager ‣ Dashboard
Dashboard
Local Serve
All Servers
File and Sto
Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
EC2AMAZ-0JEVJ3F
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel


myofc-server - ec2-34-238-43-202.compute-1.amazonaws.com - Remote Desktop Connection
Server Manager
Server Manager ‣ Dashboard
Dashboard
Local Serve
All Servers
File and Sto
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
EC2AMAZ-0JEVJ3F
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
Network Controller
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Description
Remote Access provides seamless connectivity through DirectAccess, VPN, and Web Application Proxy. DirectAccess provides an Always On and Always Managed experience. RAS provides traditional VPN services, including site-to-site (branch-office or cloud-based) connectivity. Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. Routing provides traditional routing capabilities, including NAT and other connectivity options. RAS and Routing can be deployed in single-tenant or multi-tenant mode.
< Previous
Next >
Install
Cancel

myofc-server - ec2-34-238-43-202.compute-1.amazonaws.com - Remote Desktop Connection

Server Manager

Server Manager ‣ Dashboard

Dashboard
Local Server
All Servers
File and Sto

Add Roles and Features Wizard

Select features

DESTINATION SERVER
EC2AMAZ-0JEVJ3F

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Confirmation
Results

Select one or more features to install on the selected server.

Features

- [ ] .NET Framework 3.5 Features
- [x] .NET Framework 4.7 Features (2 of 7 installed)
- [ ] Background Intelligent Transfer Service (BITS)
- [ ] BitLocker Drive Encryption
- [ ] BitLocker Network Unlock
- [ ] BranchCache
- [ ] Client for NFS
- [ ] Containers
- [ ] Data Center Bridging
- [ ] Direct Play
- [x] Enhanced Storage
- [ ] Failover Clustering
- [ ] Group Policy Management
- [ ] Host Guardian Hyper-V Support
- [ ] I/O Quality of Service
- [ ] IIS Hostable Web Core
- [ ] Internet Printing Client
- [ ] IP Address Management (IPAM) Server
- [ ] iSNS Server service

Description

Enhanced Storage enables support for accessing additional functions made available by Enhanced Storage devices. Enhanced Storage devices have built-in safety features that let you control who can access the data on the device.

< Previous | Next > | Install | Cancel

1

Server Manager

Server Manager ‣ Dashboard

Dashboard
Local Server
All Servers
File and Sto

Add Roles and Features Wizard

Remote Access

DESTINATION SERVER
EC2AMAZ-0JEVJ3F

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Confirmation
Results

Remote Access integrates DirectAccess, VPN, and Web Application Proxy in a single management console.

Deploy DirectAccess to allow managed domain-joined computers to connect to the internal corporate network as DirectAccess clients. Connectivity is seamless and transparent, and is available any time client computers are located on the Internet. DirectAccess administrators can remotely manage clients, ensuring that mobile computers are kept up-to-date with security updates and corporate compliance requirements.

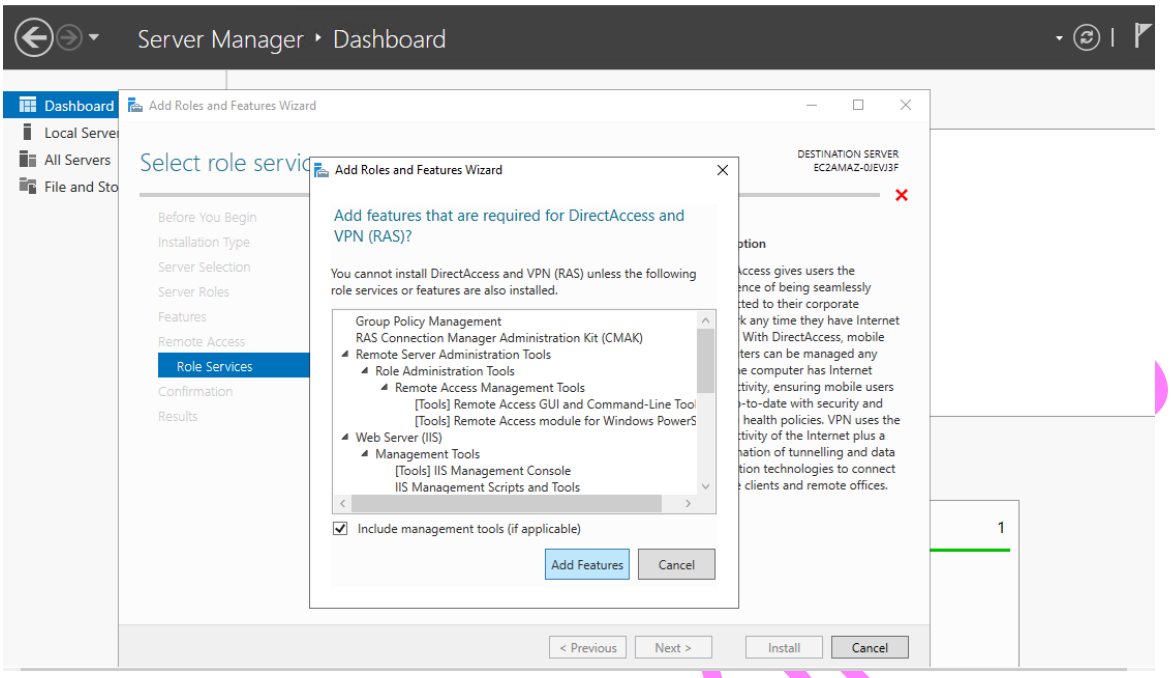
Deploy VPN to allow client computers running operating systems not supported by DirectAccess, or configured in a workgroup, to remotely access corporate networks over a VPN connection.

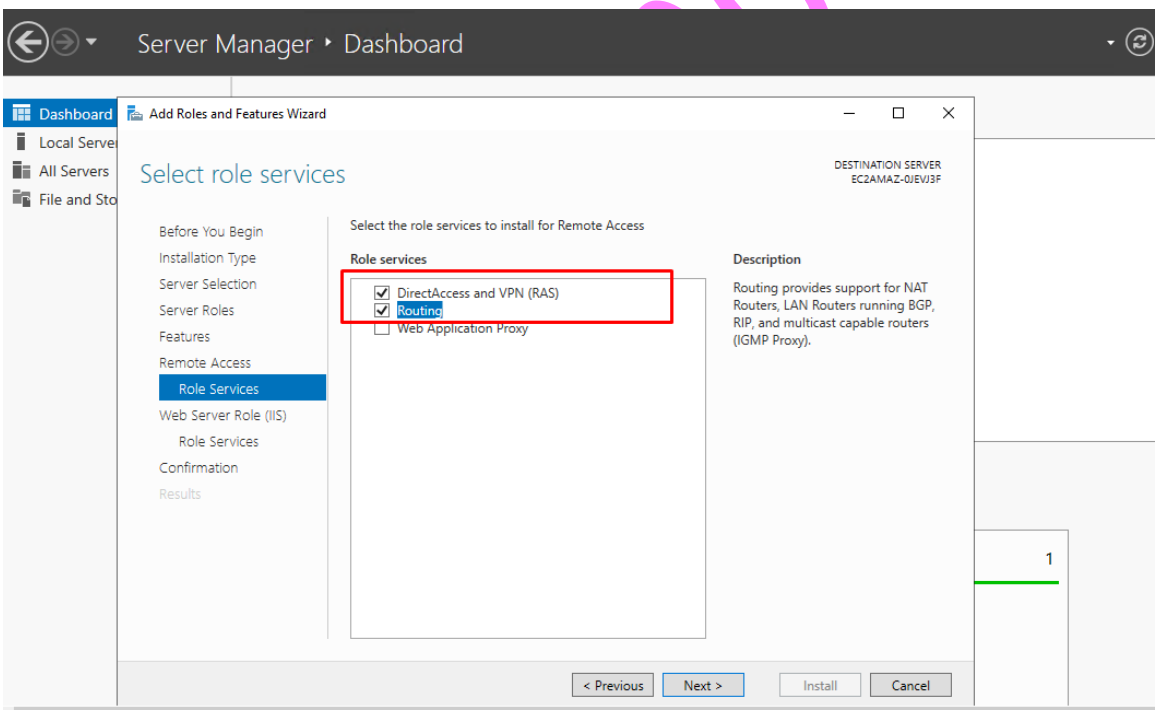
Deploy Web Application Proxy to publish selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. It can use AD FS to ensure that users are authenticated before they gain access to published applications. Web Application Proxy also provides proxy functionality for your AD FS servers.

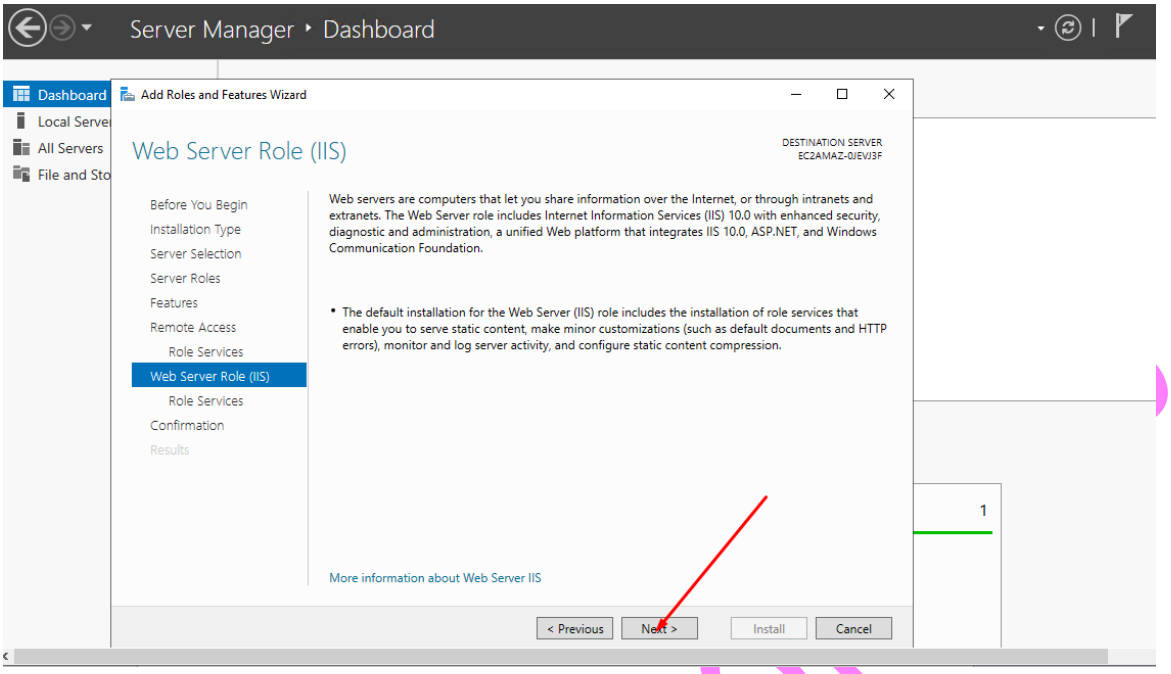
Configure RRAS routing features using the Routing and Remote Access console.

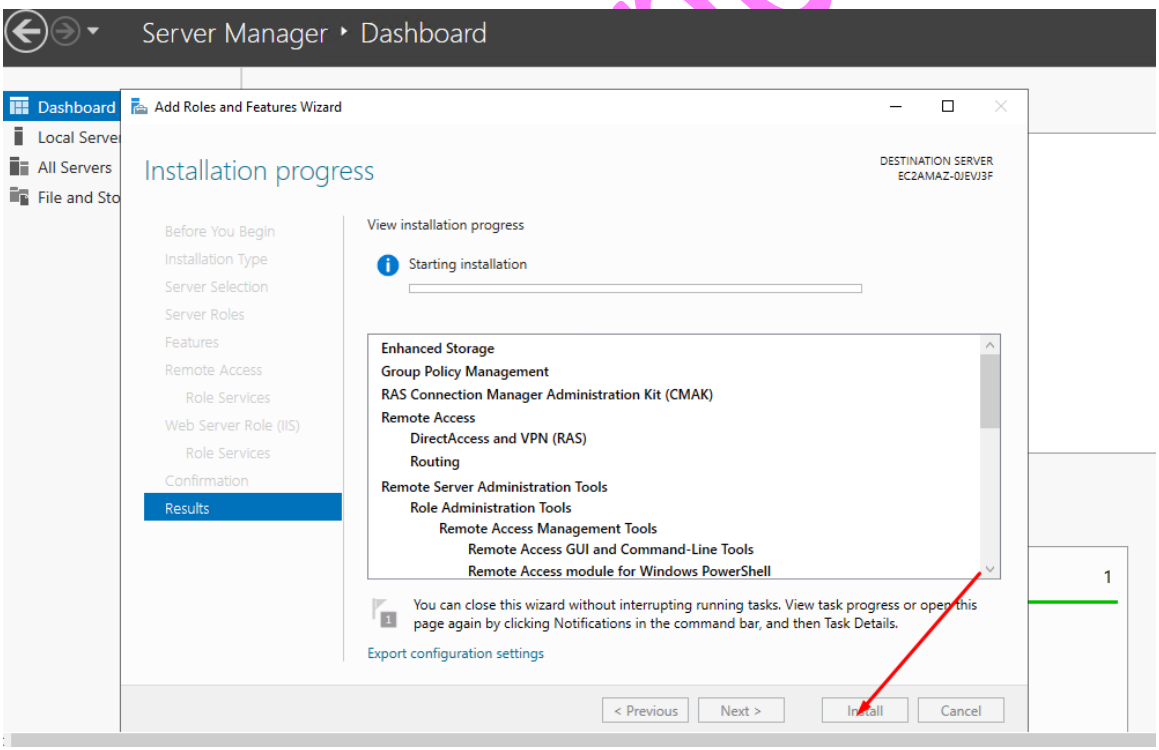
< Previous | Next > | Install | Cancel

1


Server Manager ‣ Dashboard
Dashboard
Local Server
All Servers
File and Sto
Add Roles and Features Wizard
Select role servic
DESTINATION SERVER
EC2AMAZ-0JEVJ3F
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for DirectAccess and VPN (RAS)?
You cannot install DirectAccess and VPN (RAS) unless the following role services or features are also installed.
Group Policy Management
RAS Connection Manager Administration Kit (CMAK)
Remote Server Administration Tools
Role Administration Tools
Remote Access Management Tools
[Tools] Remote Access GUI and Command-Line Tool
[Tools] Remote Access module for Windows PowerS
Web Server (IIS)
Management Tools
[Tools] IIS Management Console
IIS Management Scripts and Tools
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel


Server Manager ‣ Dashboard
Dashboard
Local Server
All Servers
File and Sto
Add Roles and Features Wizard
Select role services
DESTINATION SERVER
EC2AMAZ-0JEVJ3F
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Remote Access
Role services
DirectAccess and VPN (RAS)
Routing
Web Application Proxy
Description
Routing provides support for NAT Routers, LAN Routers running BGP, RIP, and multicast capable routers (IGMP Proxy).
< Previous
Next >
Install
Cancel





Now let's create the Local network gateway so that we can combine this to network virtual gateway

Home >

Local network gateways

Default Directory

+ Create | Edit columns | Refresh | Try preview | Feedback | Assign tags

Subscriptions: Pay-As-You-Go

Filter by name... | All resource groups | All locations | All tags | No grouping

0 items

Name ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓

No local network gateways to display

Create a local network gateway to represent the on-premises site that you want to connect to a virtual network. The local network gateway specifies the public IP address of the VPN device and IP address ranges located on the on-premises site. Later, create a VPN gateway connection between the virtual network gateway for the virtual network, and the local network gateway for the on-premises site. Learn more

Create local network gateway

---

console.aws.amazon.com/ec2/v2/home?r...

aws | Services | N. Virginia | ranjan

S3 | EC2

- Images
  - AMIs New
  - AMI Catalog
- Elastic Block Store
  - Volumes New
  - Snapshots New
  - Lifecycle Manager New
- Network & Security
  - Security Groups
  - Elastic IPs
  - Placement Groups
  - Key Pairs
  - Network Interfaces
- Load Balancing
  - Load Balancers
  - Target Groups New
- Auto Scaling
  - Launch Configurations
  - Auto Scaling Groups

EC2 > ... > i-0bac6b23afb9c9469

Instance summary for i-0bac6b23afb9c9469 (myofc-server) Info

Updated less than a minute ago

Connect | Instance state | Actions

Instance ID i-0bac6b23afb9c9469 (myofc-server)	Public IPv4 address 34.238.43.202 | open address
Private IPv4 addresses 172.31.90.56	IPv6 address –
Instance state Running	Public IPv4 DNS ec2-34-238-43-202.compute-1.amazonaws.com | open address
Hostname type IP name: ip-172-31-90-56.ec2.internal	Private IP DNS name (IPv4 only) ip-172-31-90-56.ec2.internal
Answer private resource DNS name IPv4 (A)	Instance type t2.medium
Elastic IP addresses –	VPC ID vpc-0a8d3927b2c9cb63f (DONOTDELETE)

portal.azure.com/#create/Microsoft.LocalNet...

Incognito

Microsoft Azure | Search resources, services, and docs (G+/)

Home > Local network gateways >

Create local network gateway

Learn more.

Project details

Subscription * : Pay-As-You-Go

Resource group * : dvs-rg

Create new

Instance details

Region * : East US

Name * : mylocalnetwork

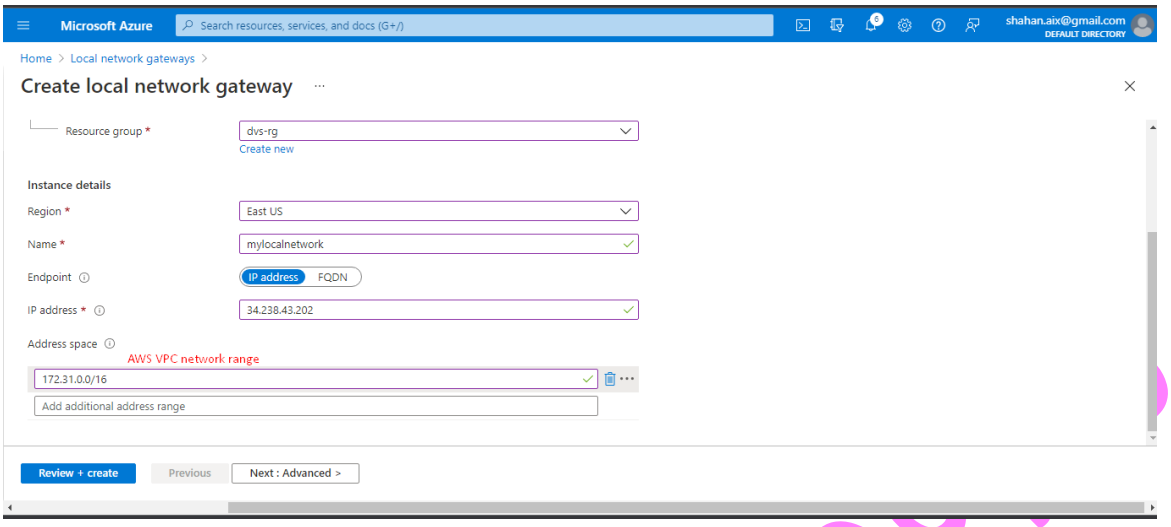
Endpoint : IP address | FQDN

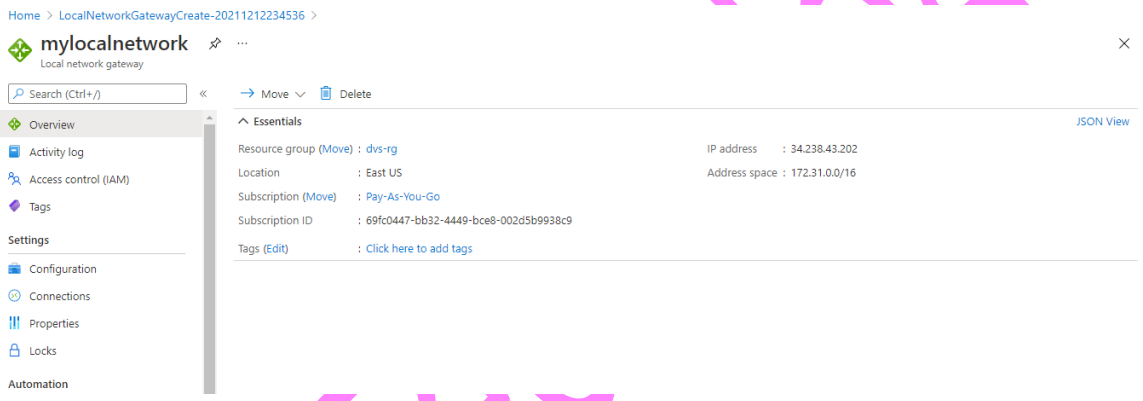
IP address * : 34.238.43.202

Address space : 172.31.0.0/16

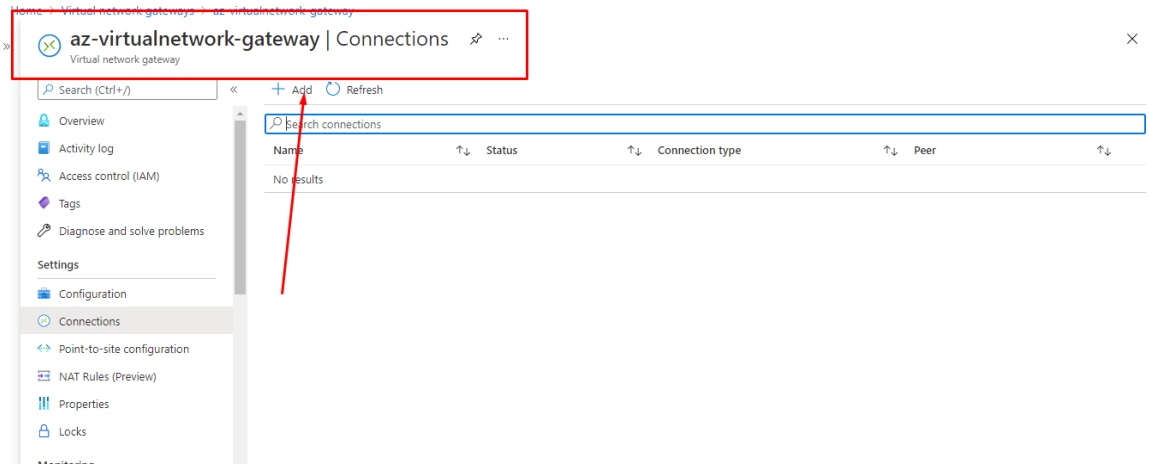
Add additional address range

Review + create | Previous | Next : Advanced >





Now let's create the Virtual network gateway with this local network gateway



Home > Virtual network gateways > az-virtualnetwork-gateway >

Add connection

az-virtualnetwork-gateway

Name *

mycompany-conn

Connection type

Site-to-site (IPsec)

*Virtual network gateway

az-virtualnetwork-gateway

*Local network gateway

mylocalnetwork

Shared key (PSK) *

Use Azure Private IP Address

Enable BGP

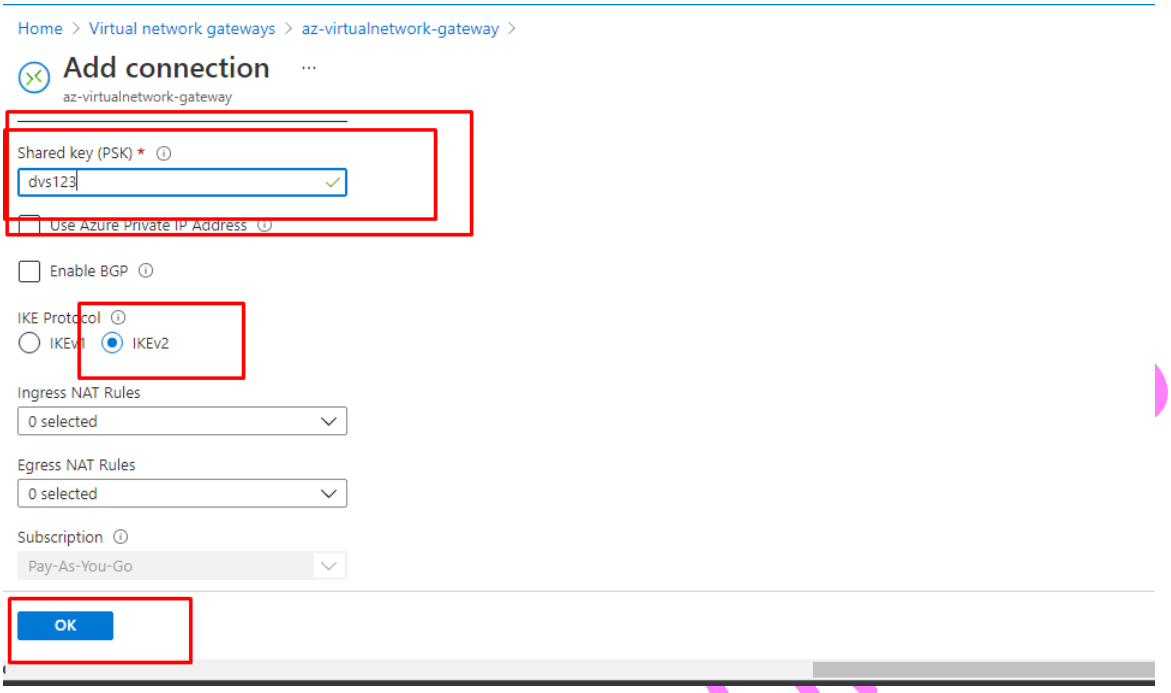
OK

Home > Virtual network gateways > az-virtualnetwork-gateway > Add connection >

Choose local network gateway

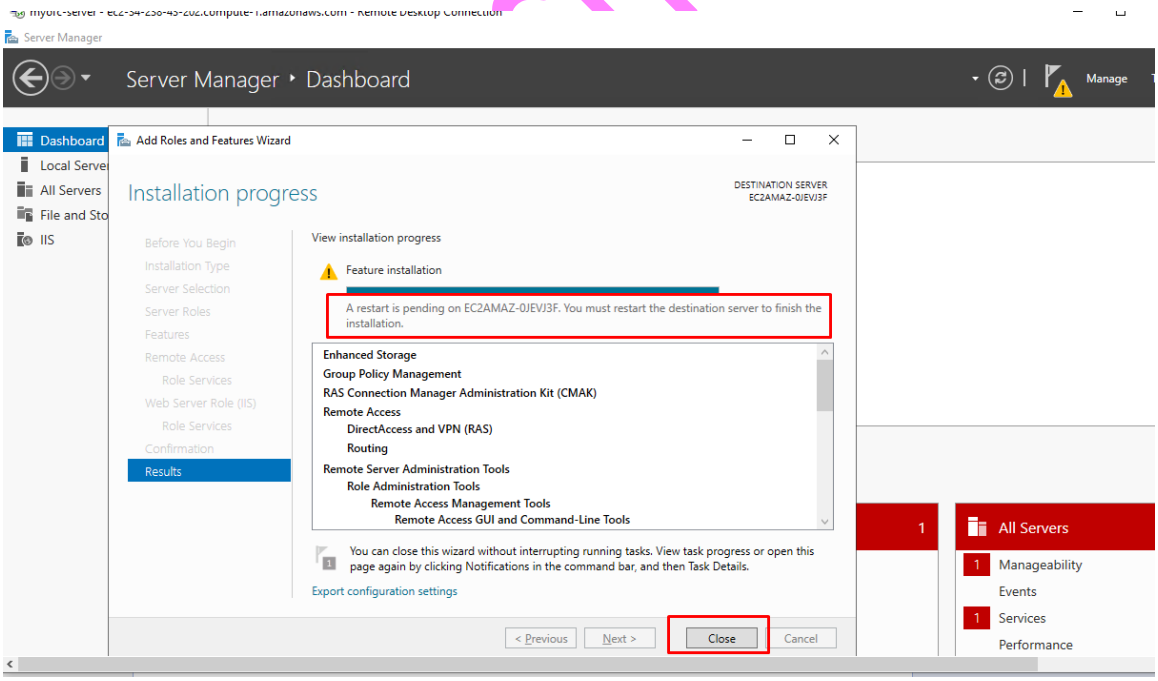
Create new

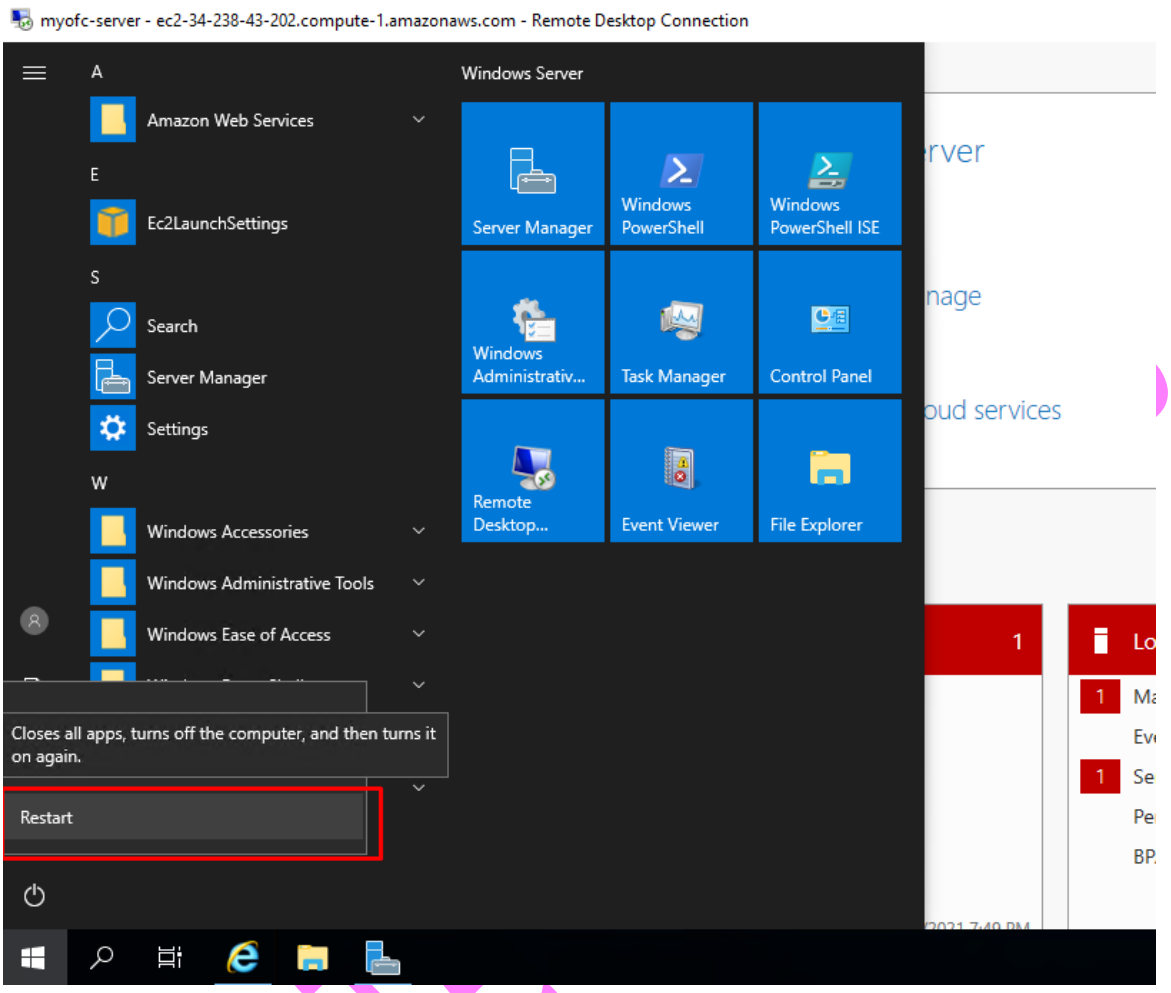
mylocalnetwork
dvs-rg



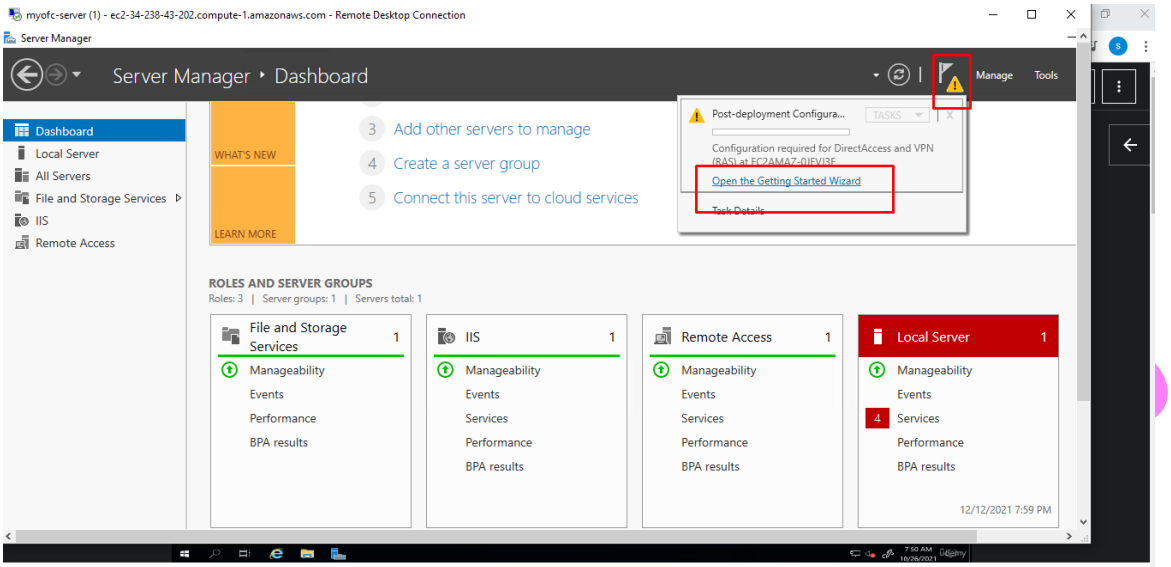
Note: Please make a note of PSK(shared key)

Now we are done with azure configuration, let's configure aws VM

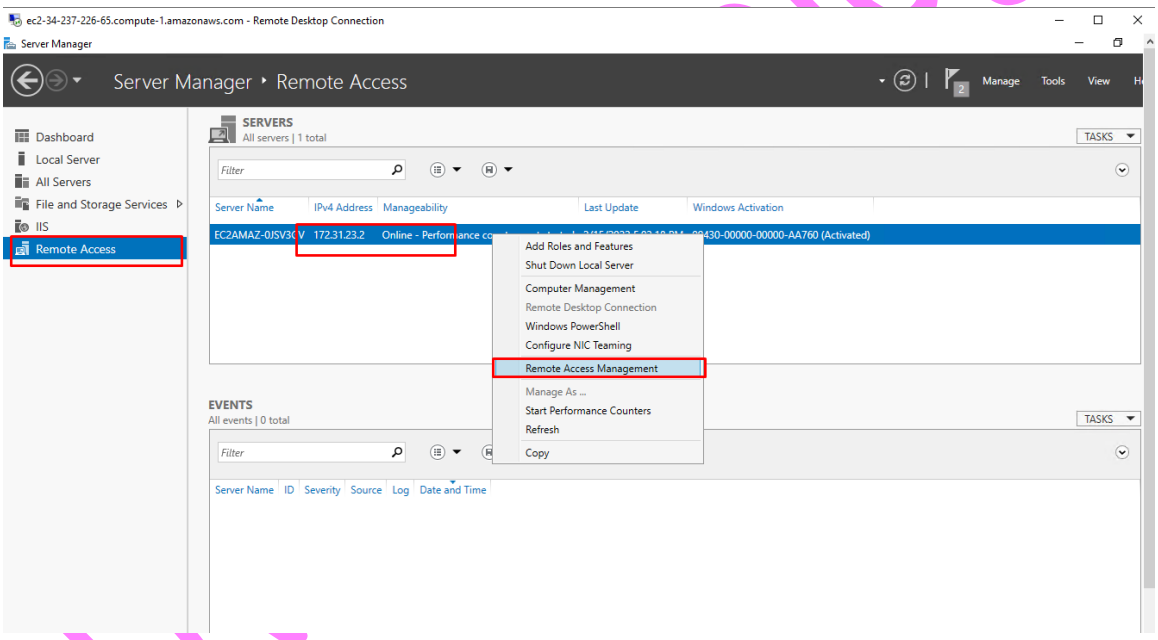


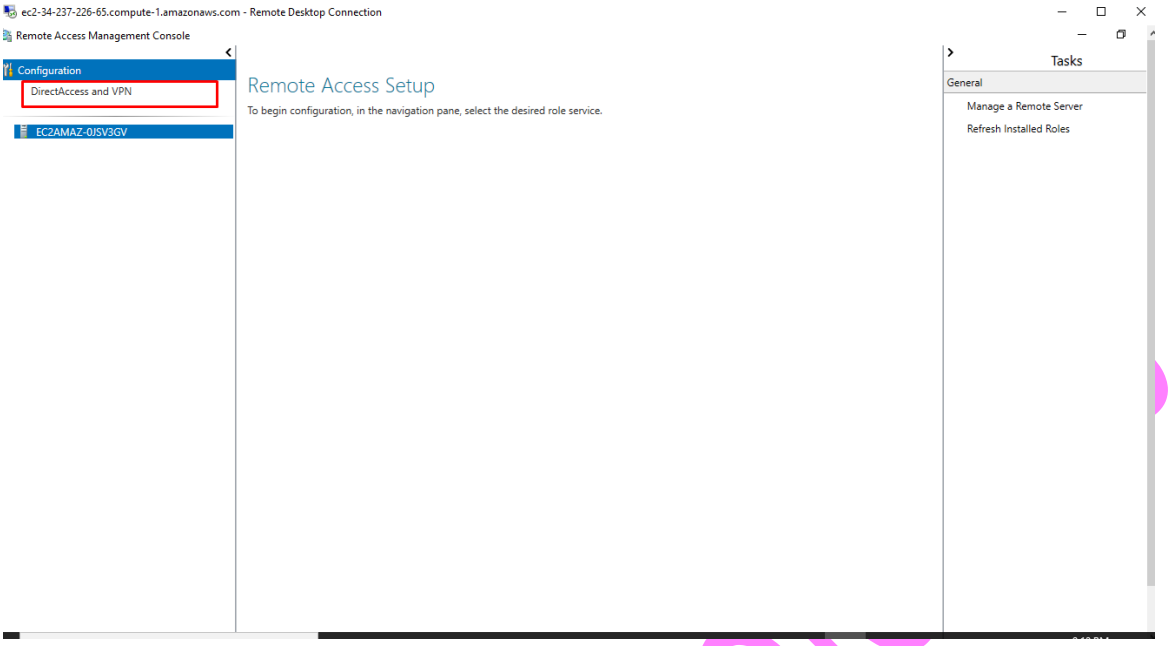


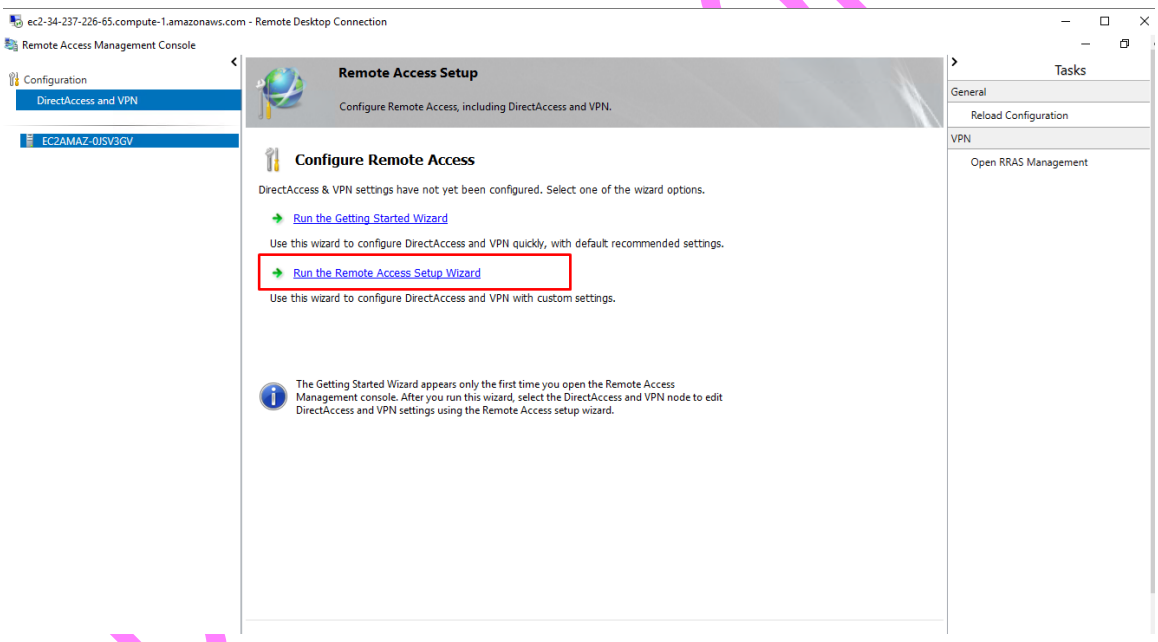
Once system is restarted try to login to the machine

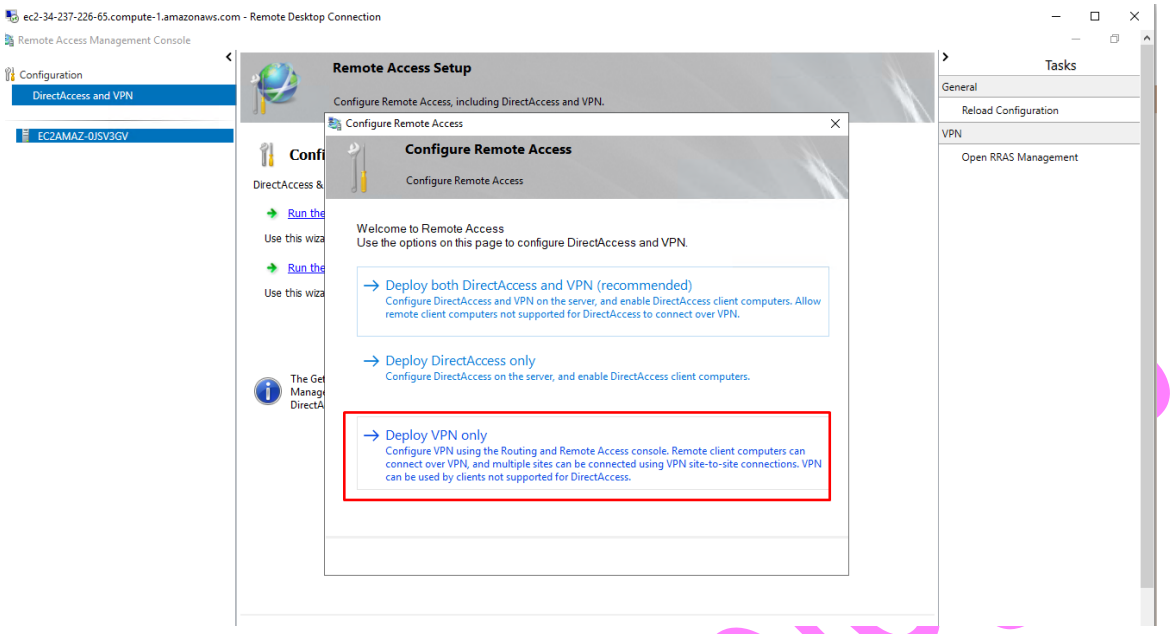


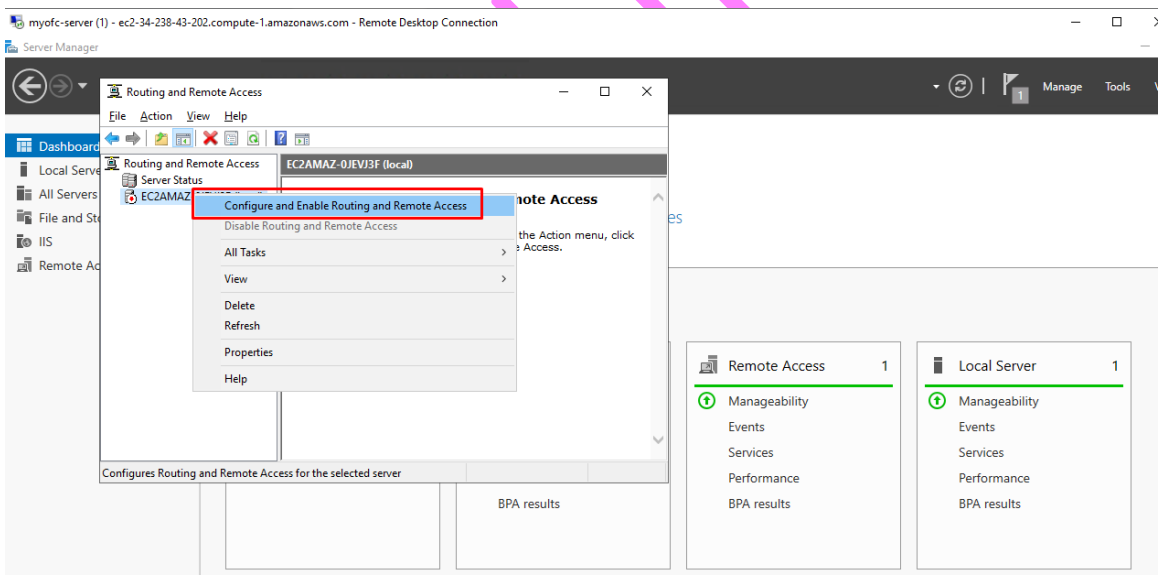
Course content Overview Q&A Notes Announcements Reviews

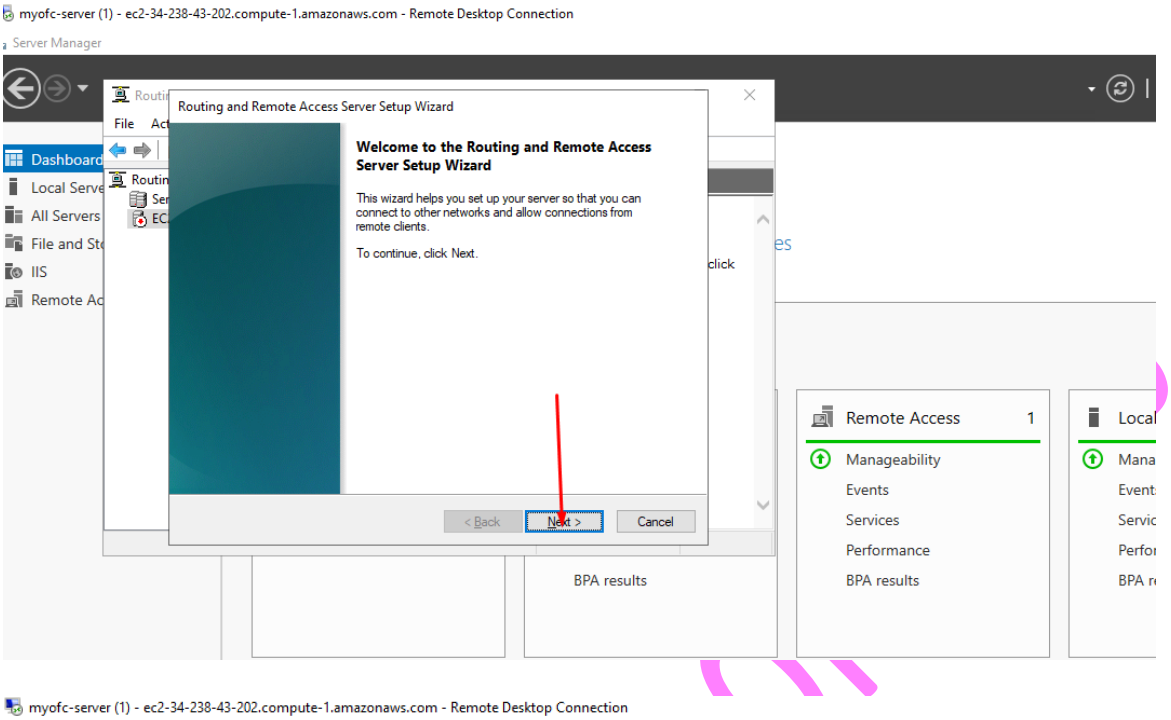


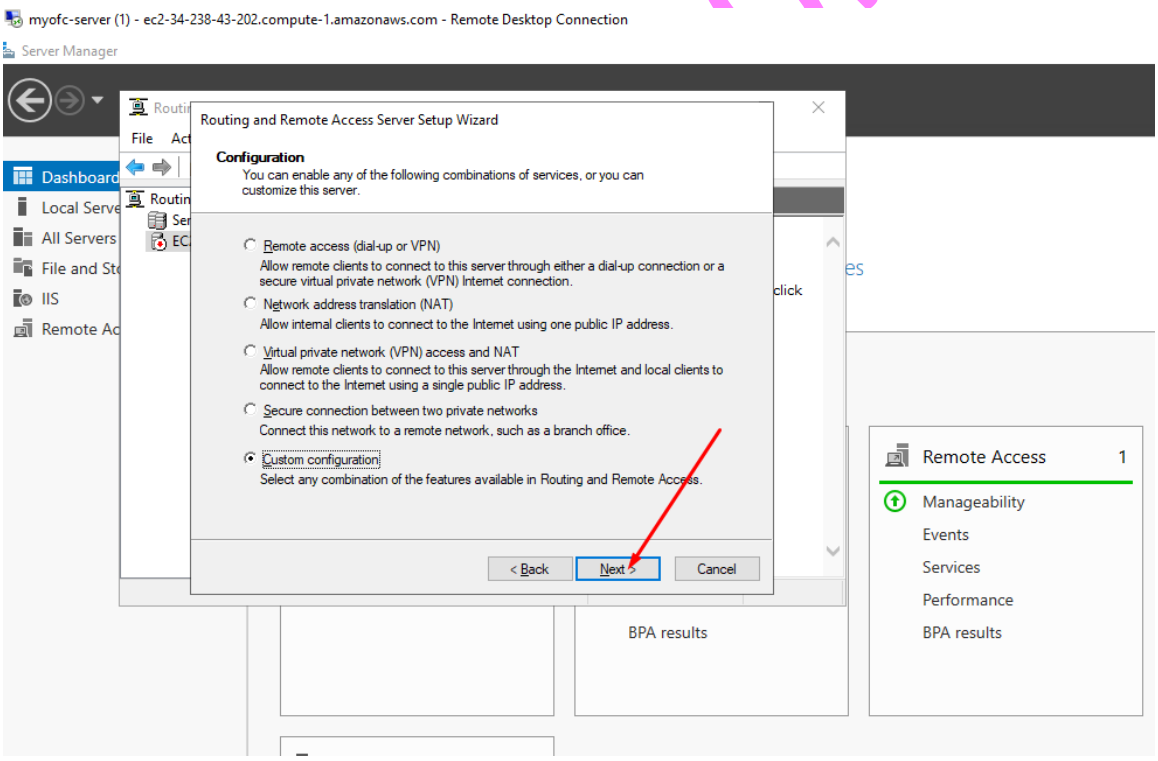

ec2-34-237-226-65.compute-1.amazonaws.com - Remote Desktop Connection
Remote Access Management Console
Configuration
DirectAccess and VPN
EC2AMAZ-0JSV3GV
Remote Access Setup
To begin configuration, in the navigation pane, select the desired role service.
Tasks
General
Manage a Remote Server
Refresh Installed Roles

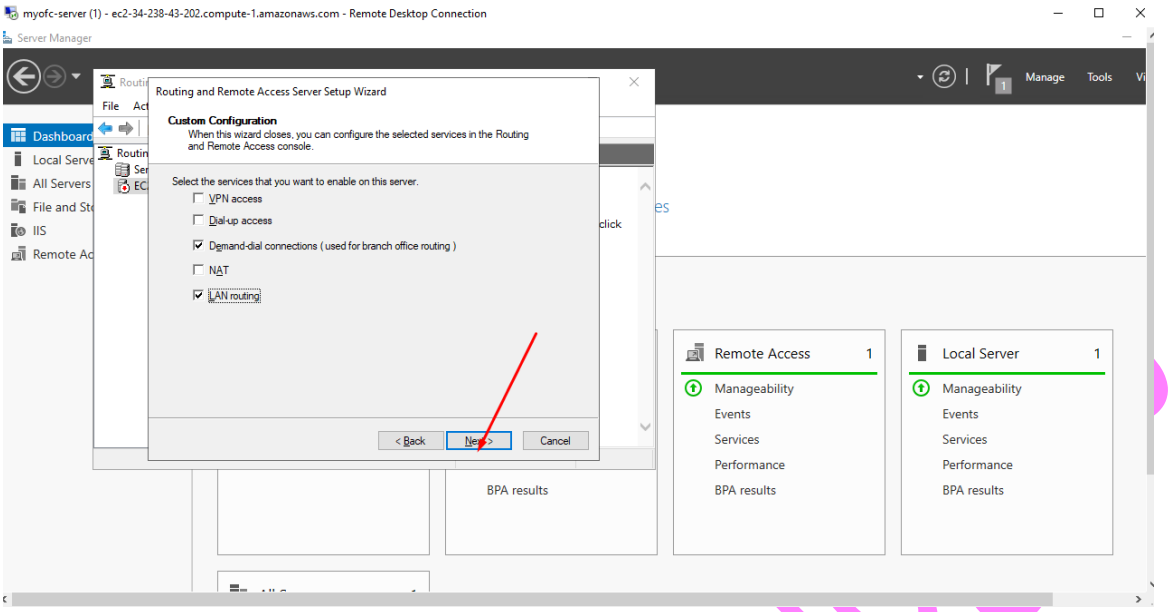

ec2-34-237-226-65.compute-1.amazonaws.com - Remote Desktop Connection
Remote Access Management Console
Configuration
DirectAccess and VPN
EC2AMAZ-0JSV3GV
Remote Access Setup
Configure Remote Access, including DirectAccess and VPN.
Configure Remote Access
DirectAccess & VPN settings have not yet been configured. Select one of the wizard options.
Run the Getting Started Wizard
Use this wizard to configure DirectAccess and VPN quickly, with default recommended settings.
Run the Remote Access Setup Wizard
Use this wizard to configure DirectAccess and VPN with custom settings.
The Getting Started Wizard appears only the first time you open the Remote Access Management console. After you run this wizard, select the DirectAccess and VPN node to edit DirectAccess and VPN settings using the Remote Access setup wizard.
Tasks
General
Reload Configuration
VPN
Open RRAS Management

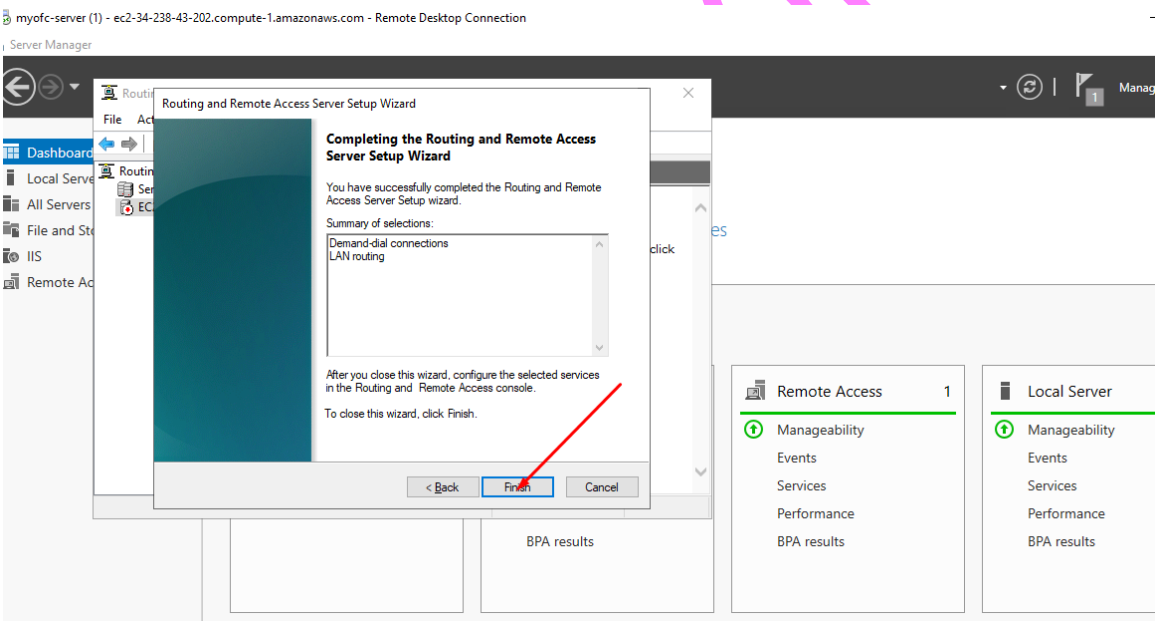

ec2-34-237-226-65.compute-1.amazonaws.com - Remote Desktop Connection
Remote Access Management Console
Configuration
DirectAccess and VPN
EC2AMAZ-0JSV3GV
Remote Access Setup
Configure Remote Access, including DirectAccess and VPN.
Configure Remote Access
Configure Remote Access
Configure Remote Access
Welcome to Remote Access
Use the options on this page to configure DirectAccess and VPN.
Deploy both DirectAccess and VPN (recommended)
Configure DirectAccess and VPN on the server, and enable DirectAccess client computers. Allow remote client computers not supported for DirectAccess to connect over VPN.
Deploy DirectAccess only
Configure DirectAccess on the server, and enable DirectAccess client computers.
Deploy VPN only
Configure VPN using the Routing and Remote Access console. Remote client computers can connect over VPN, and multiple sites can be connected using VPN site-to-site connections. VPN can be used by clients not supported for DirectAccess.
Tasks
General
Reload Configuration
VPN
Open RRAS Management

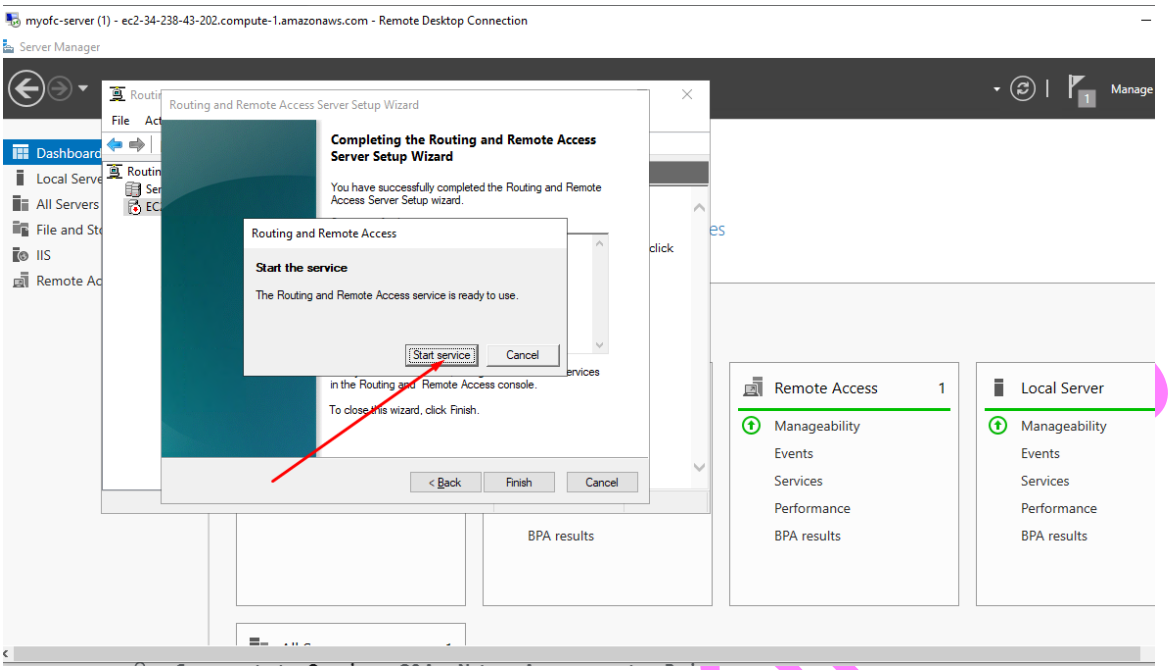

myofc-server (1) - ec2-34-238-43-202.compute-1.amazonaws.com - Remote Desktop Connection
Server Manager
Manage
Tools
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
EC2AMAZ-0JEVJ3F (local)
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
All Tasks
View
Delete
Refresh
Properties
Help
Configures Routing and Remote Access for the selected server
Dashboard
Local Serve
All Servers
File and St
IIS
Remote Ac
Remote Access 1
Manageability
Events
Services
Performance
BPA results
Local Server 1
Manageability
Events
Services
Performance
BPA results

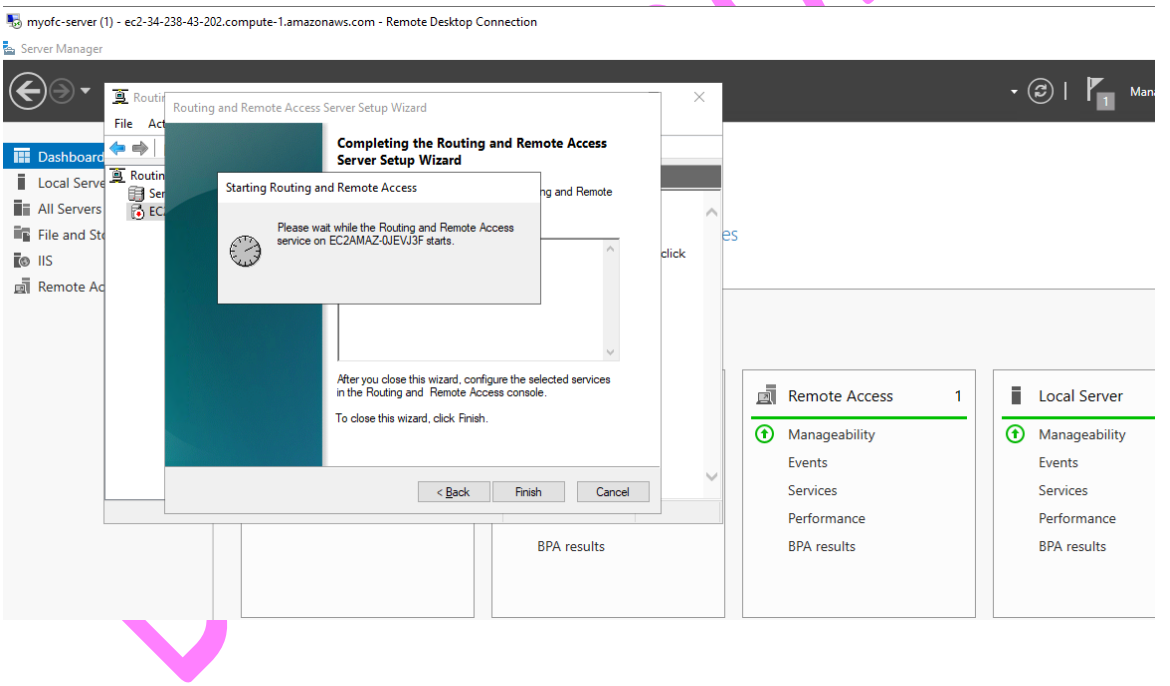

myofc-server (1) - ec2-34-238-43-202.compute-1.amazonaws.com - Remote Desktop Connection
Server Manager
Routing and Remote Access Server Setup Wizard
Welcome to the Routing and Remote Access Server Setup Wizard
This wizard helps you set up your server so that you can connect to other networks and allow connections from remote clients.
To continue, click Next.
< Back
Next >
Cancel
Dashboard
Local Serve
All Servers
File and St
IIS
Remote Ac
Remote Access 1
Manageability
Events
Services
Performance
BPA results

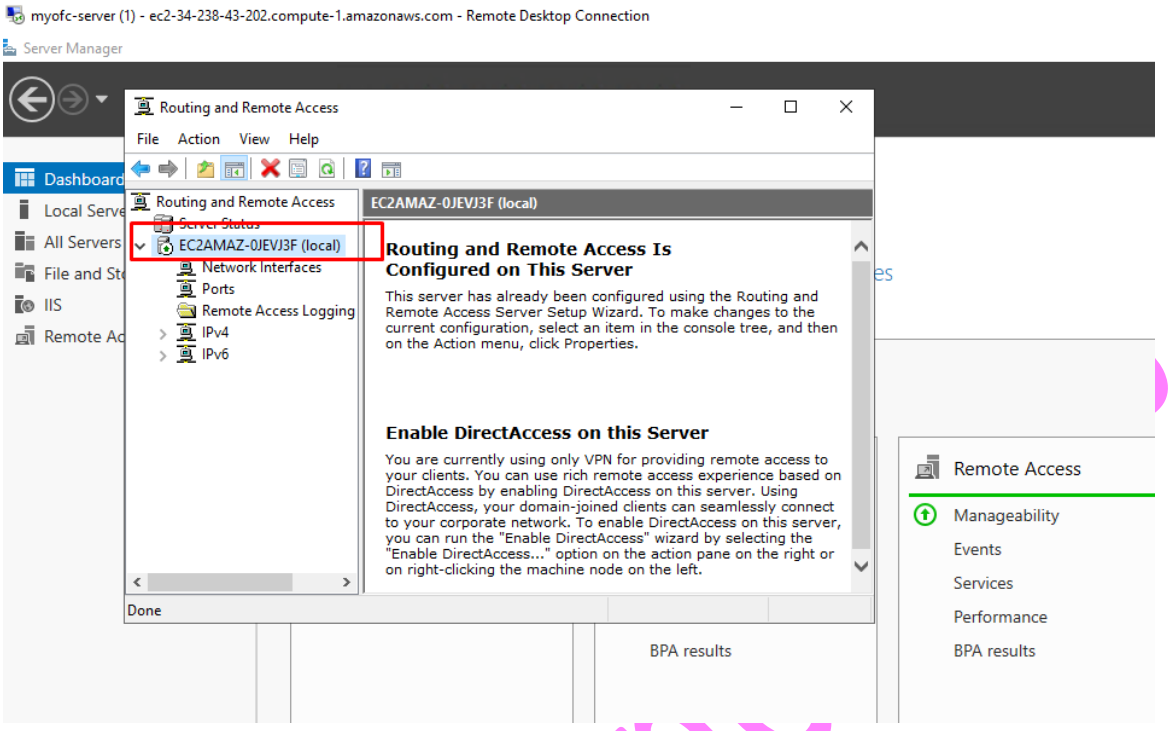

myofc-server (1) - ec2-34-238-43-202.compute-1.amazonaws.com - Remote Desktop Connection
Server Manager
Routing and Remote Access Server Setup Wizard
Configuration
You can enable any of the following combinations of services, or you can customize this server.
Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.
Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.
Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.
Secure connection between two private networks
Connect this network to a remote network, such as a branch office.
Custom configuration
Select any combination of the features available in Routing and Remote Access.
< Back
Next >
Cancel
Dashboard
Local Serve
All Servers
File and St
IIS
Remote Ac
Remote Access 1
Manageability
Events
Services
Performance
BPA results


myofc-server (1) - ec2-34-238-43-202.compute-1.amazonaws.com - Remote Desktop Connection
Server Manager
Routing and Remote Access Server Setup Wizard
Custom Configuration
When this wizard closes, you can configure the selected services in the Routing and Remote Access console.
Select the services that you want to enable on this server.
VPN access
Dial-up access
Demand-dial connections (used for branch office routing)
NAT
LAN routing
< Back
Next >
Cancel
Remote Access
Manageability
Events
Services
Performance
BPA results
Local Server
Manageability
Events
Services
Performance
BPA results

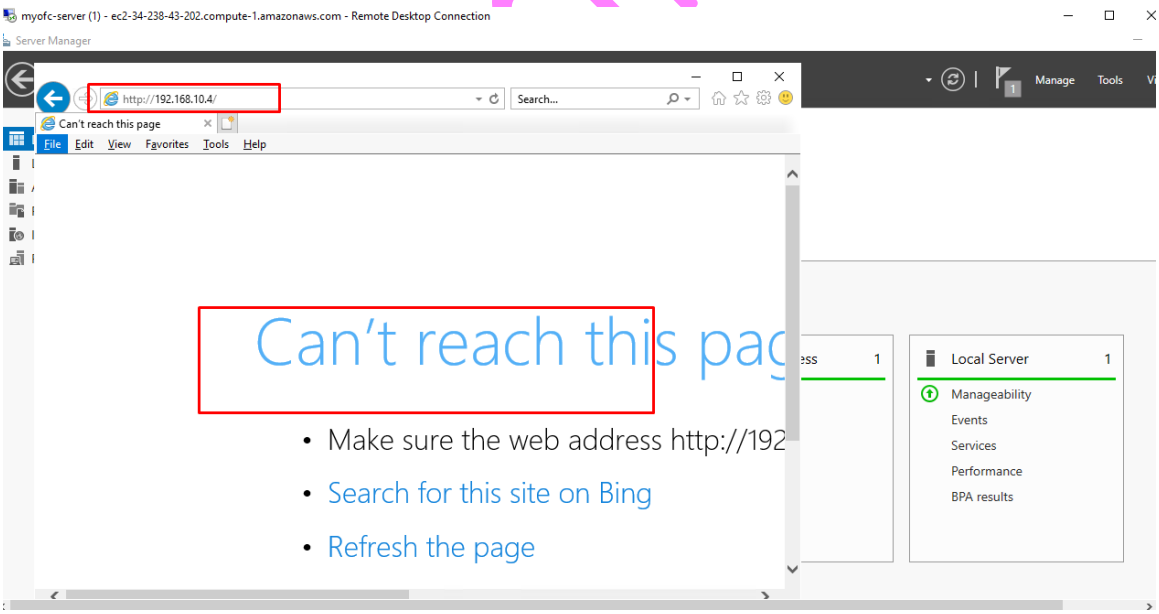

myofc-server (1) - ec2-34-238-43-202.compute-1.amazonaws.com - Remote Desktop Connection
Server Manager
Routing and Remote Access Server Setup Wizard
Completing the Routing and Remote Access Server Setup Wizard
You have successfully completed the Routing and Remote Access Server Setup wizard.
Summary of selections:
Demand-dial connections
LAN routing
After you close this wizard, configure the selected services in the Routing and Remote Access console.
To close this wizard, click Finish.
< Back
Finish
Cancel
Remote Access
Manageability
Events
Services
Performance
BPA results
Local Server
Manageability
Events
Services
Performance
BPA results


myofc-server (1) - ec2-34-238-43-202.compute-1.amazonaws.com - Remote Desktop Connection
Server Manager
Routing and Remote Access Server Setup Wizard
Completing the Routing and Remote Access Server Setup Wizard
You have successfully completed the Routing and Remote Access Server Setup wizard.
Routing and Remote Access
Start the service
The Routing and Remote Access service is ready to use.
Start service
Cancel
To close this wizard, click Finish.
< Back
Finish
Cancel
Remote Access
Local Server
Manageability
Events
Services
Performance
BPA results


myofc-server (1) - ec2-34-238-43-202.compute-1.amazonaws.com - Remote Desktop Connection
Server Manager
Routing and Remote Access Server Setup Wizard
Completing the Routing and Remote Access Server Setup Wizard
Starting Routing and Remote Access
Please wait while the Routing and Remote Access service on EC2AMAZ-0JEVJ3F starts.
After you close this wizard, configure the selected services in the Routing and Remote Access console.
To close this wizard, click Finish.
< Back
Finish
Cancel
Remote Access
Local Server
Manageability
Events
Services
Performance
BPA results

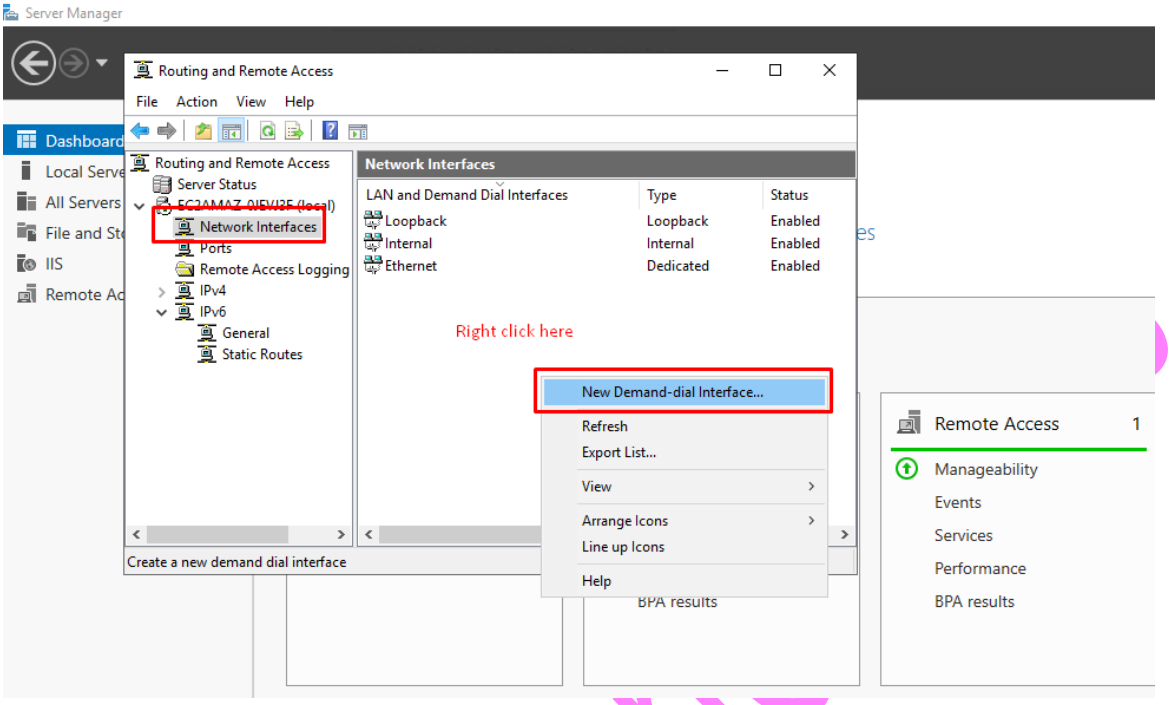


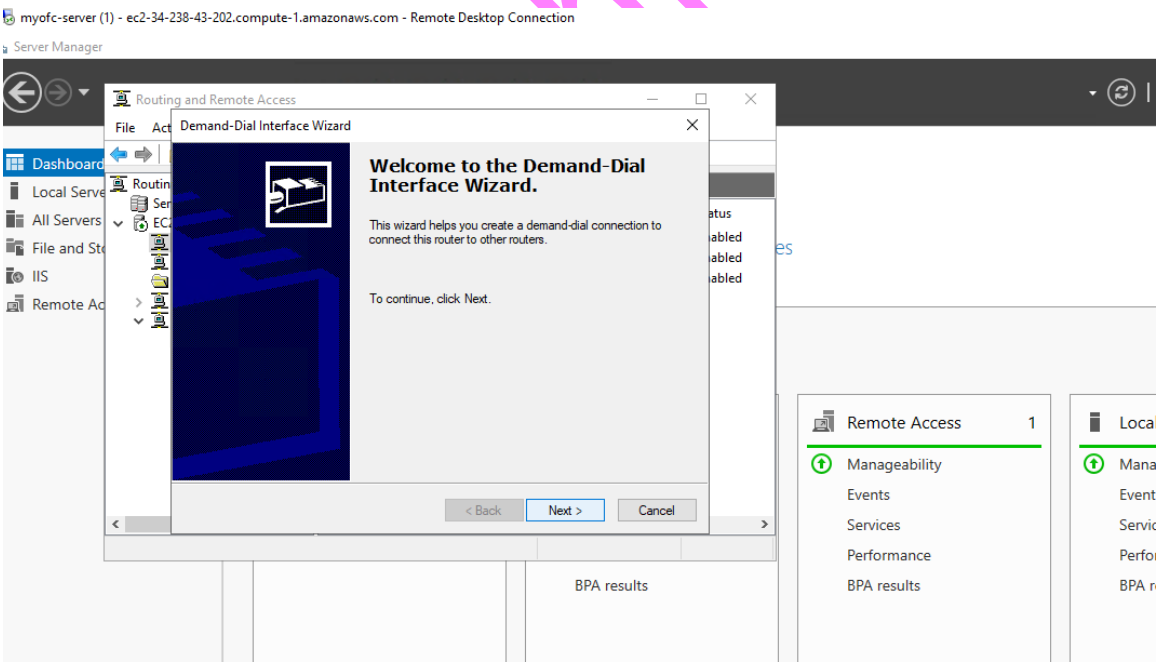
Now let's try to reach our azure vm with its private ipaddress from aws virtual machine

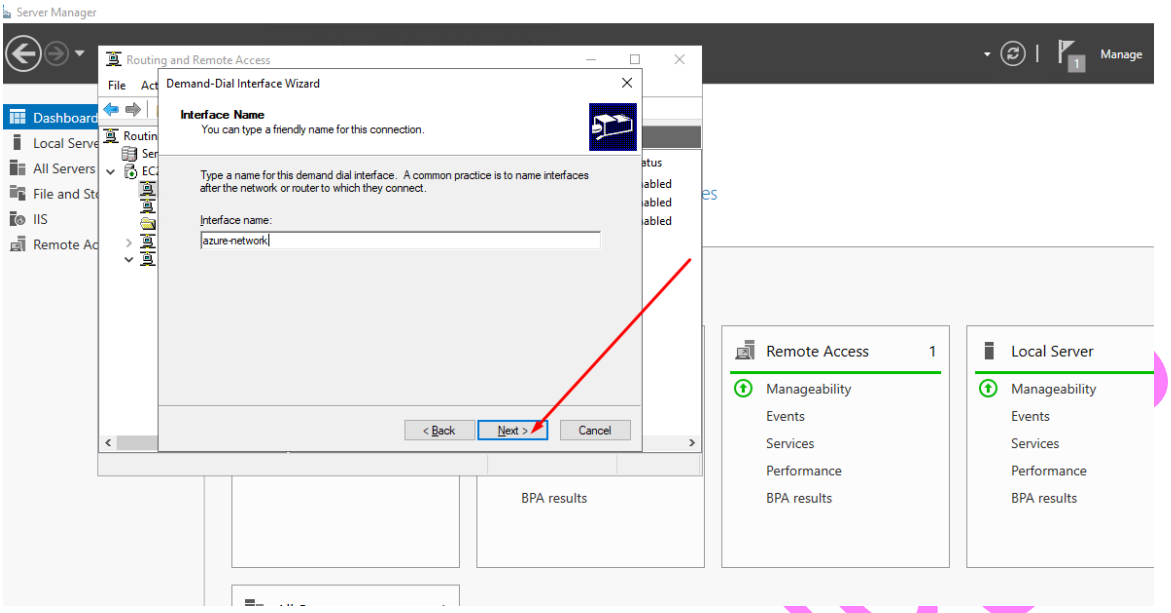


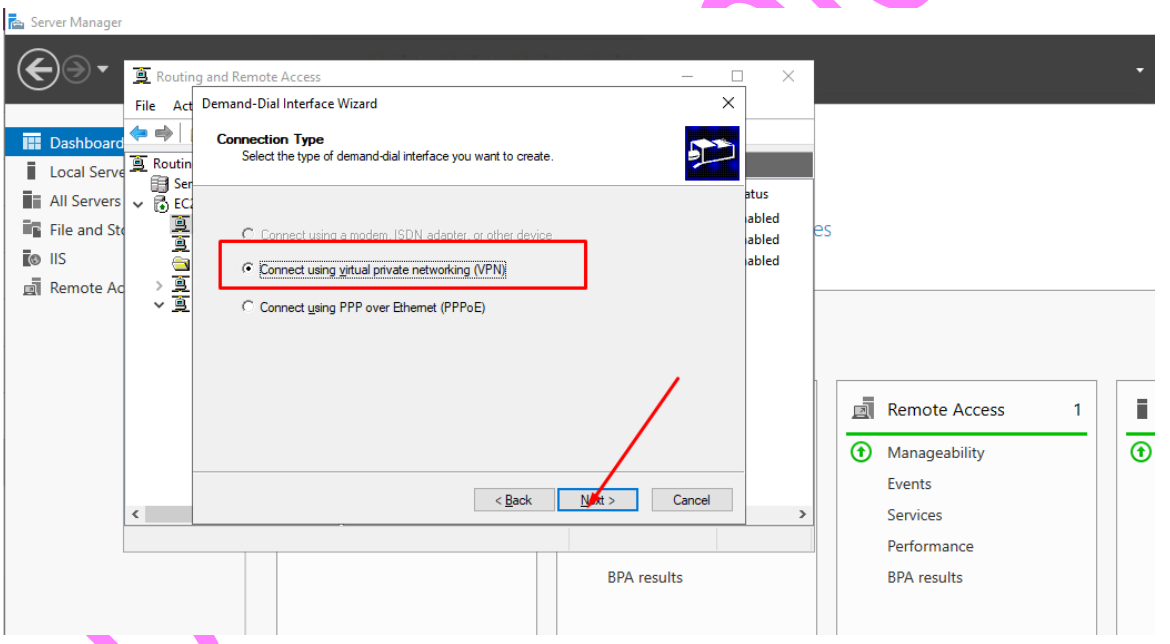
If you observe properly it's still not working

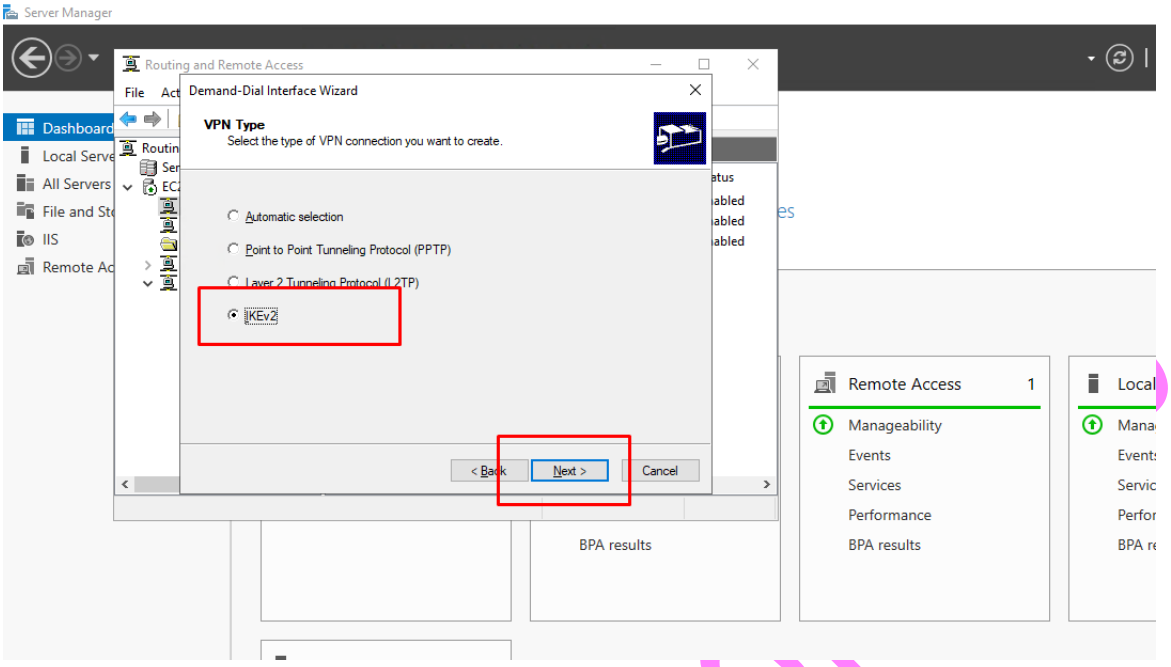
Now let's create one interface which will help in establishing the connectivity

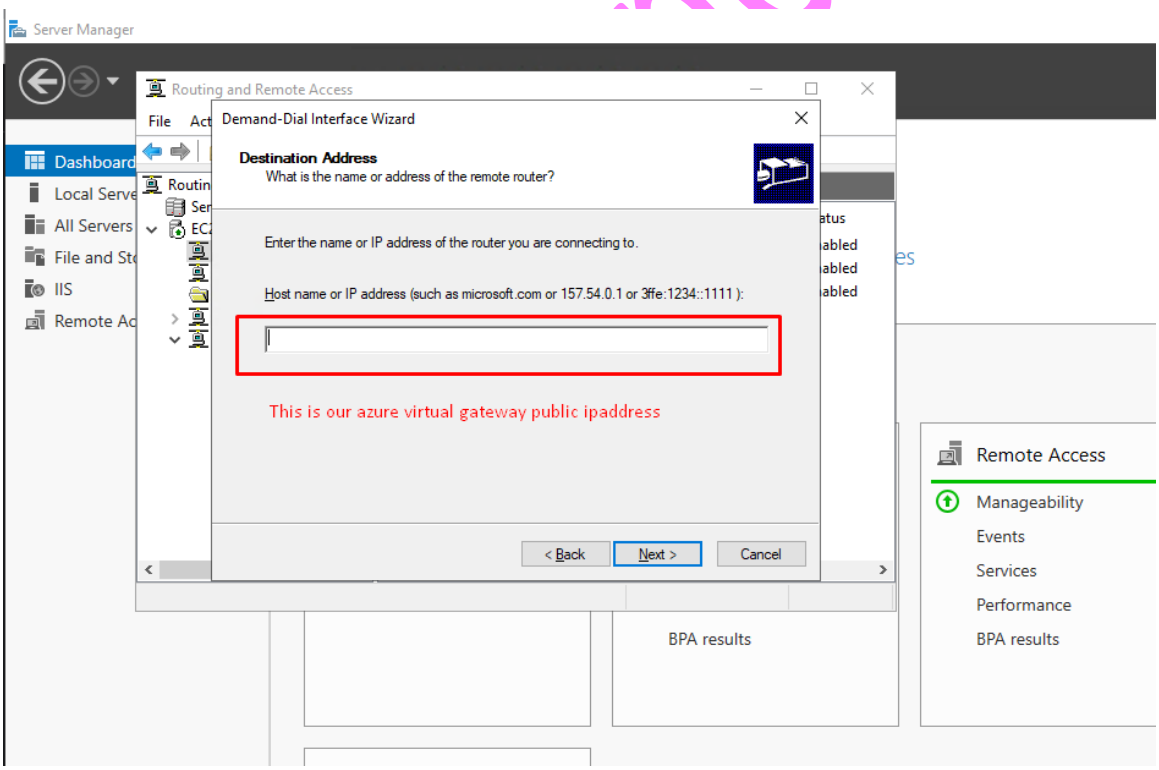

Server Manager
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
Network Interfaces
Ports
Remote Access Logging
IPv4
IPv6
General
Static Routes
Network Interfaces
LAN and Demand Dial Interfaces
Type
Status
Loopback
Loopback
Enabled
Internal
Internal
Enabled
Ethernet
Dedicated
Enabled
Right click here
New Demand-dial Interface...
Refresh
Export List...
View
Arrange Icons
Line up Icons
Help
Create a new demand dial interface
Remote Access 1
Manageability
Events
Services
Performance
BPA results

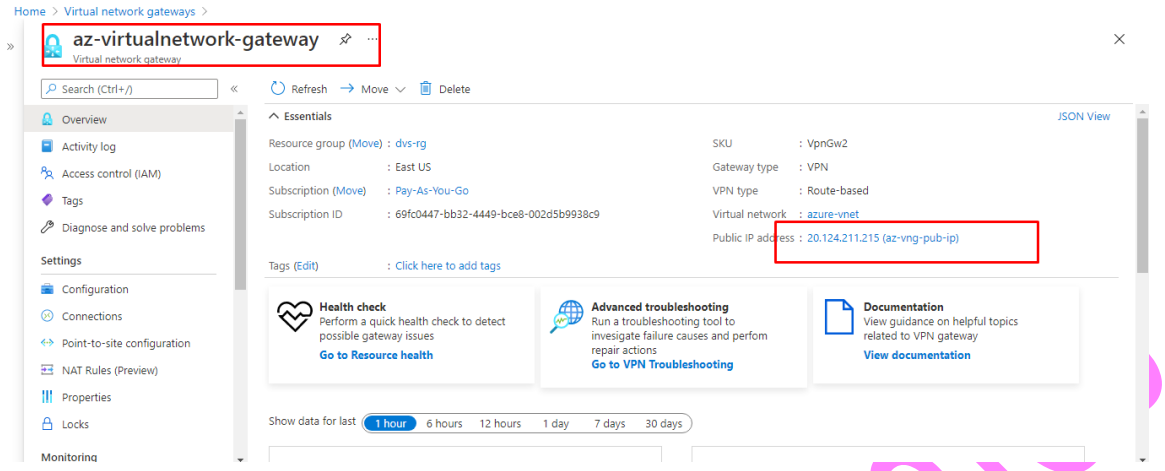

myofc-server (1) - ec2-34-238-43-202.compute-1.amazonaws.com - Remote Desktop Connection
Server Manager
Routing and Remote Access
Demand-Dial Interface Wizard
Welcome to the Demand-Dial Interface Wizard.
This wizard helps you create a demand-dial connection to connect this router to other routers.
To continue, click Next.
< Back
Next >
Cancel
Remote Access 1
Manageability
Events
Services
Performance
BPA results

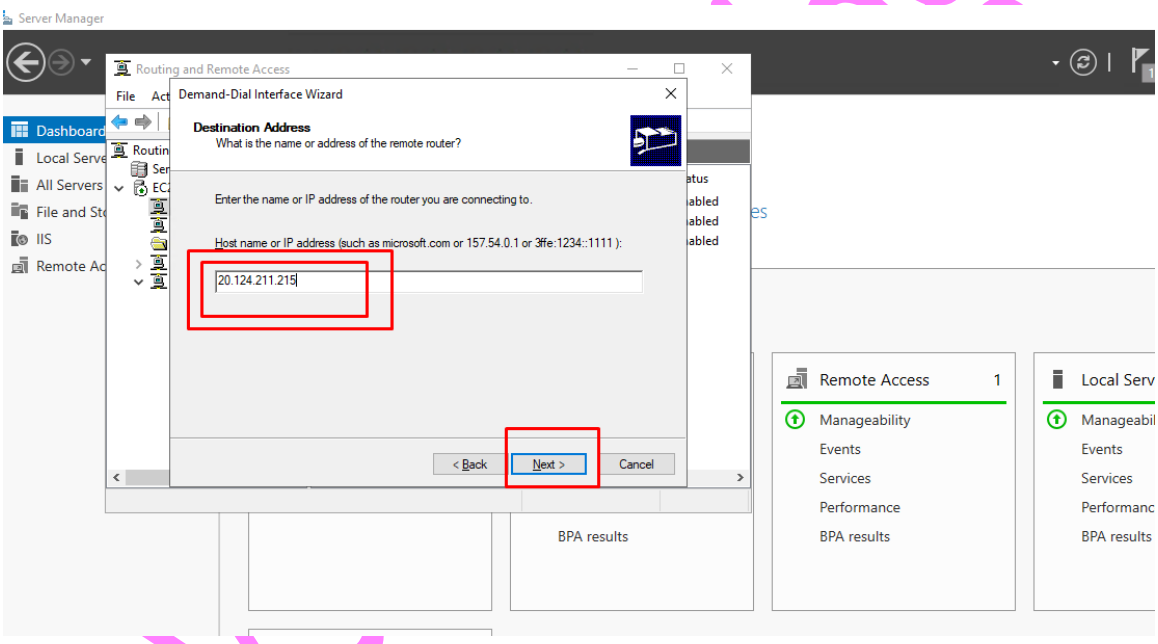

Server Manager
Routing and Remote Access
Demand-Dial Interface Wizard
Interface Name
You can type a friendly name for this connection.
Type a name for this demand dial interface. A common practice is to name interfaces after the network or router to which they connect.
Interface name:
azure-network
< Back
Next >
Cancel
Remote Access
Manageability
Events
Services
Performance
BPA results
Local Server
Manageability
Events
Services
Performance
BPA results

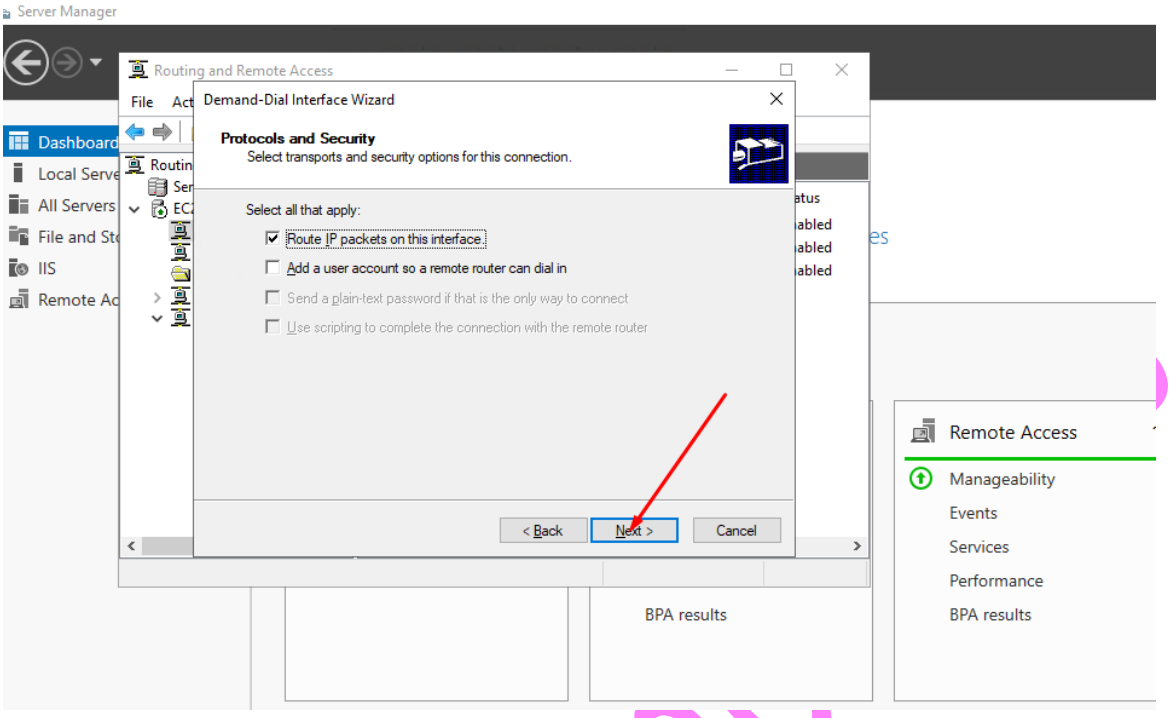

Server Manager
Routing and Remote Access
Demand-Dial Interface Wizard
Connection Type
Select the type of demand-dial interface you want to create.
Connect using a modem, ISDN adapter, or other device
Connect using virtual private networking (VPN)
Connect using PPP over Ethernet (PPPoE)
< Back
Next >
Cancel
Remote Access
Manageability
Events
Services
Performance
BPA results

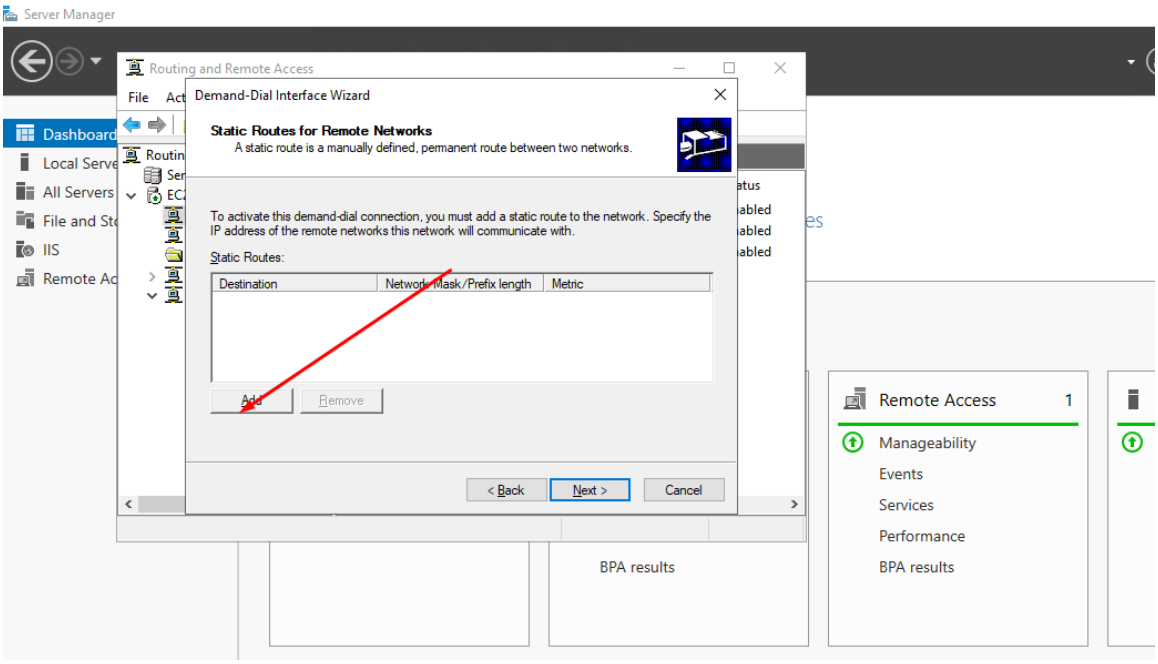

Server Manager
Routing and Remote Access
Demand-Dial Interface Wizard
VPN Type
Select the type of VPN connection you want to create.
Automatic selection
Point to Point Tunneling Protocol (PPTP)
Layer 2 Tunneling Protocol (L2TP)
IKEv2
< Back
Next >
Cancel
Remote Access
Manageability
Events
Services
Performance
BPA results

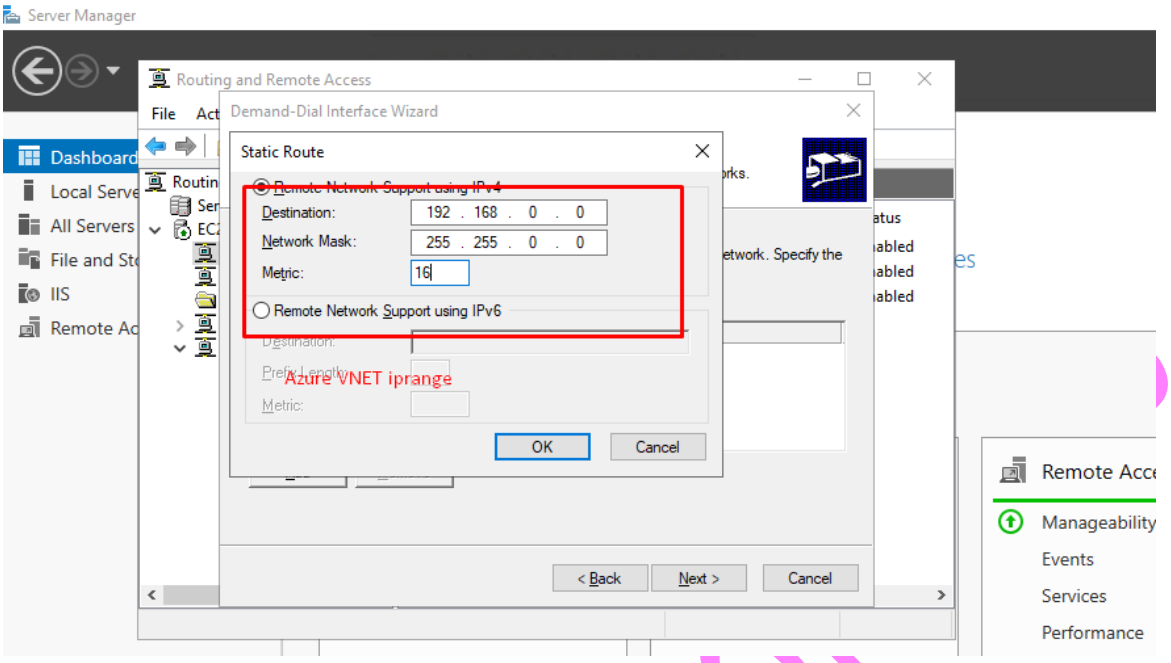

Server Manager
Routing and Remote Access
Demand-Dial Interface Wizard
Destination Address
What is the name or address of the remote router?
Enter the name or IP address of the router you are connecting to.
Host name or IP address (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111):
This is our azure virtual gateway public ipaddress
< Back
Next >
Cancel
Remote Access
Manageability
Events
Services
Performance
BPA results


Home > Virtual network gateways >
az-virtualnetwork-gateway
Virtual network gateway
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Connections
Point-to-site configuration
NAT Rules (Preview)
Properties
Locks
Monitoring
Refresh
Move
Delete
Essentials
JSON View
Resource group (Move) : dvs-rg
Location : East US
Subscription (Move) : Pay-As-You-Go
Subscription ID : 69fc0447-bb32-4449-bce8-002d5b9938c9
Tags (Edit) : Click here to add tags
SKU : VpnGw2
Gateway type : VPN
VPN type : Route-based
Virtual network : azure-vnet
Public IP address : 20.124.211.215 (az-vng-pub-ip)
Health check
Perform a quick health check to detect possible gateway issues
Go to Resource health
Advanced troubleshooting
Run a troubleshooting tool to invesigate failure causes and perfom repair actions
Go to VPN Troubleshooting
Documentation
View guidance on helpful topics related to VPN gateway
View documentation
Show data for last
1 hour
6 hours
12 hours
1 day
7 days
30 days

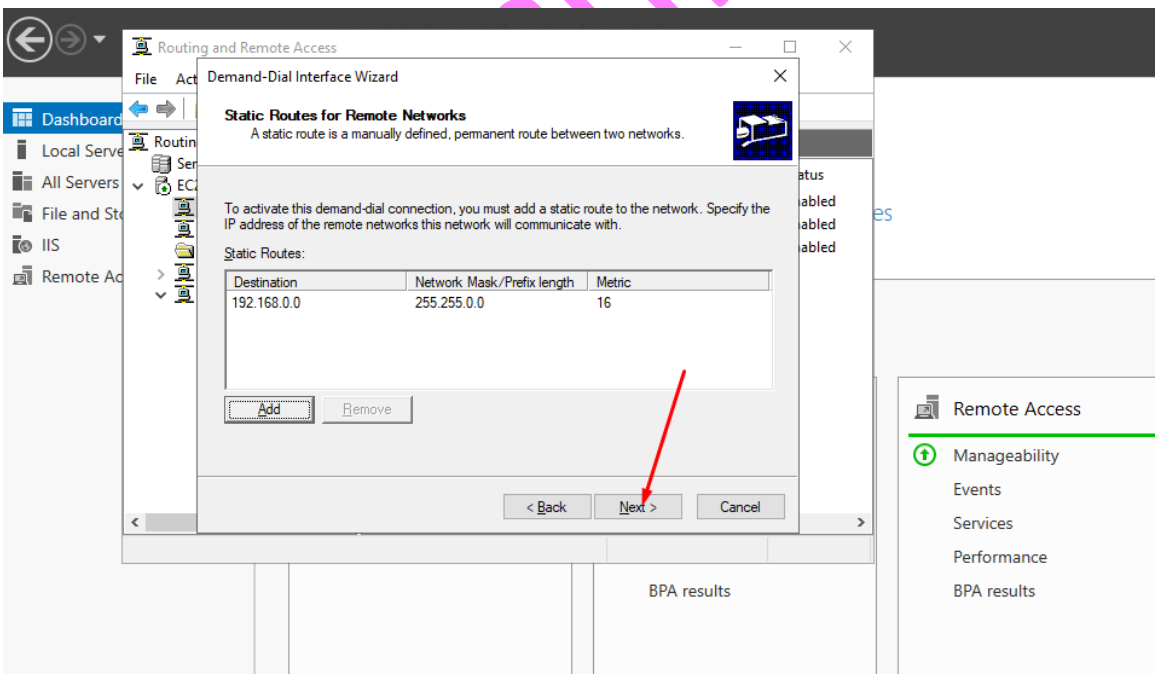

Server Manager
Routing and Remote Access
File
Demand-Dial Interface Wizard
Destination Address
What is the name or address of the remote router?
Enter the name or IP address of the router you are connecting to.
Host name or IP address (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111):
20.124.211.215
< Back
Next >
Cancel
Dashboard
Local Serve
All Servers
File and St
IIS
Remote Ac
Remote Access 1
Manageability
Events
Services
Performance
BPA results
Local Serv
Manageabil
Events
Services
Performanc
BPA results

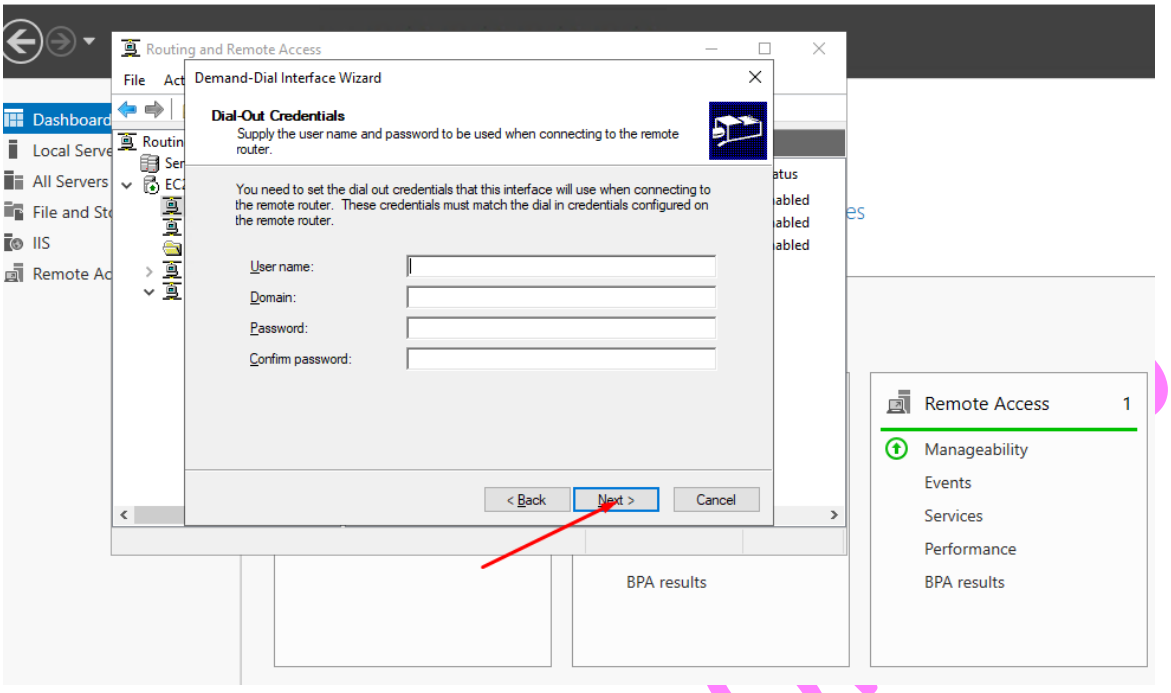

Server Manager
Routing and Remote Access
File
Demand-Dial Interface Wizard
Protocols and Security
Select transports and security options for this connection.
Select all that apply:
Route IP packets on this interface
Add a user account so a remote router can dial in
Send a plain-text password if that is the only way to connect
Use scripting to complete the connection with the remote router
< Back
Next >
Cancel
Dashboard
Local Serve
All Servers
File and St
IIS
Remote Ac
Remote Access
Manageability
Events
Services
Performance
BPA results
BPA results

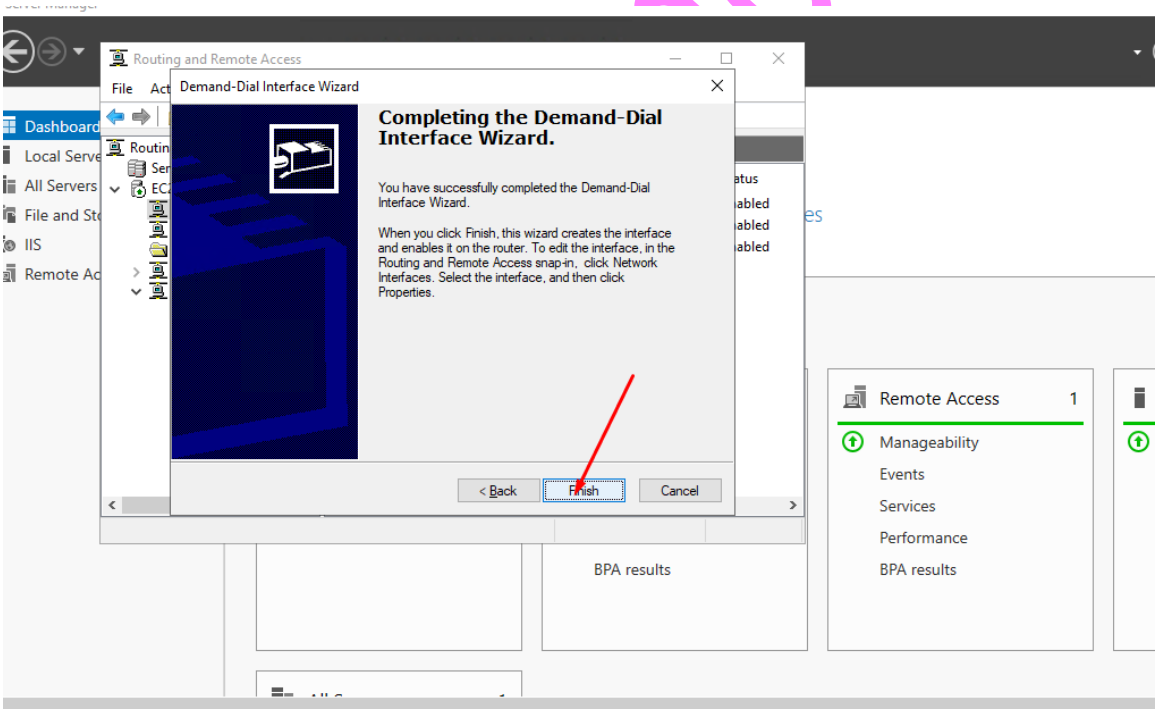

Server Manager
Routing and Remote Access
File
Demand-Dial Interface Wizard
Static Routes for Remote Networks
A static route is a manually defined, permanent route between two networks.
To activate this demand-dial connection, you must add a static route to the network. Specify the IP address of the remote networks this network will communicate with.
Static Routes:
Destination
Network Mask/Prefix length
Metric
Add
Remove
< Back
Next >
Cancel
Dashboard
Local Serve
All Servers
File and St
IIS
Remote Ac
Remote Access 1
Manageability
Events
Services
Performance
BPA results
BPA results

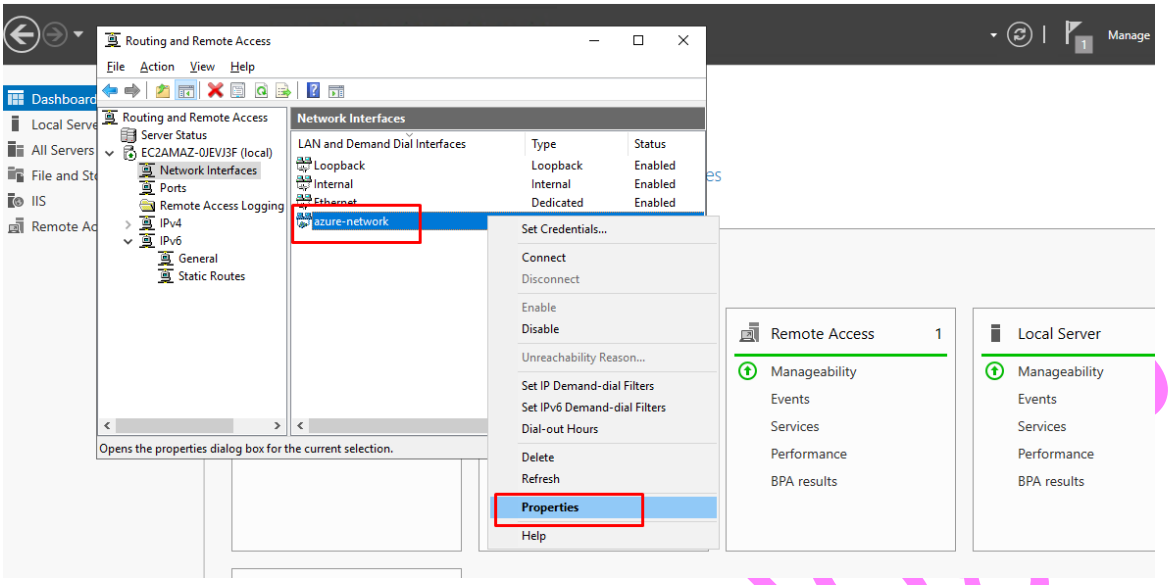


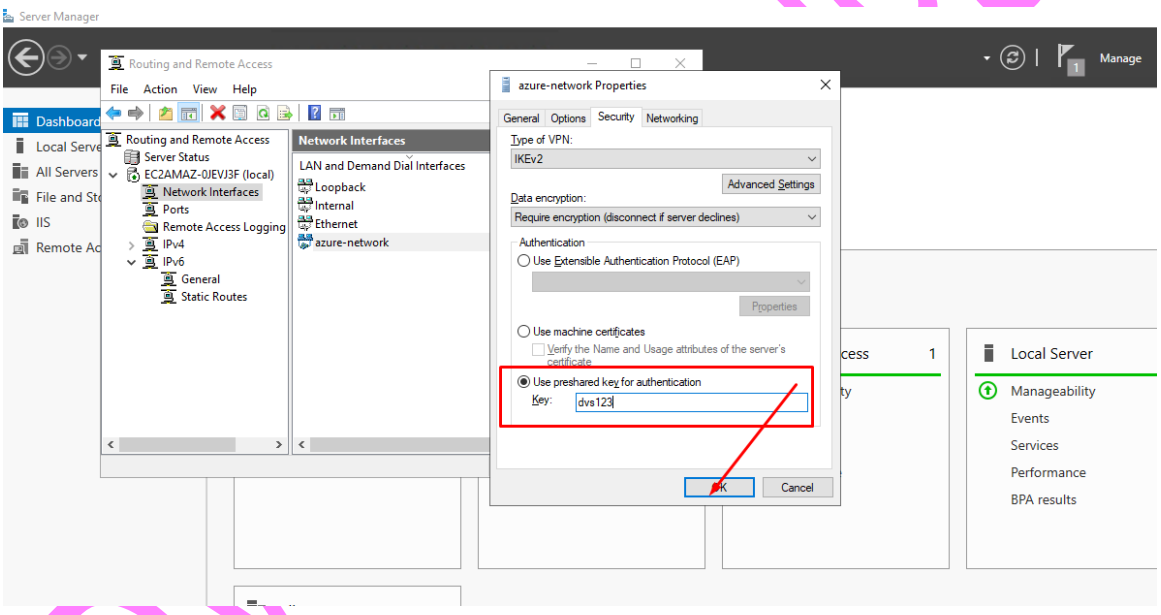
Here you have to give the azure VNET iprange in our case we took it as 192.168.0.0/16 then click on OK



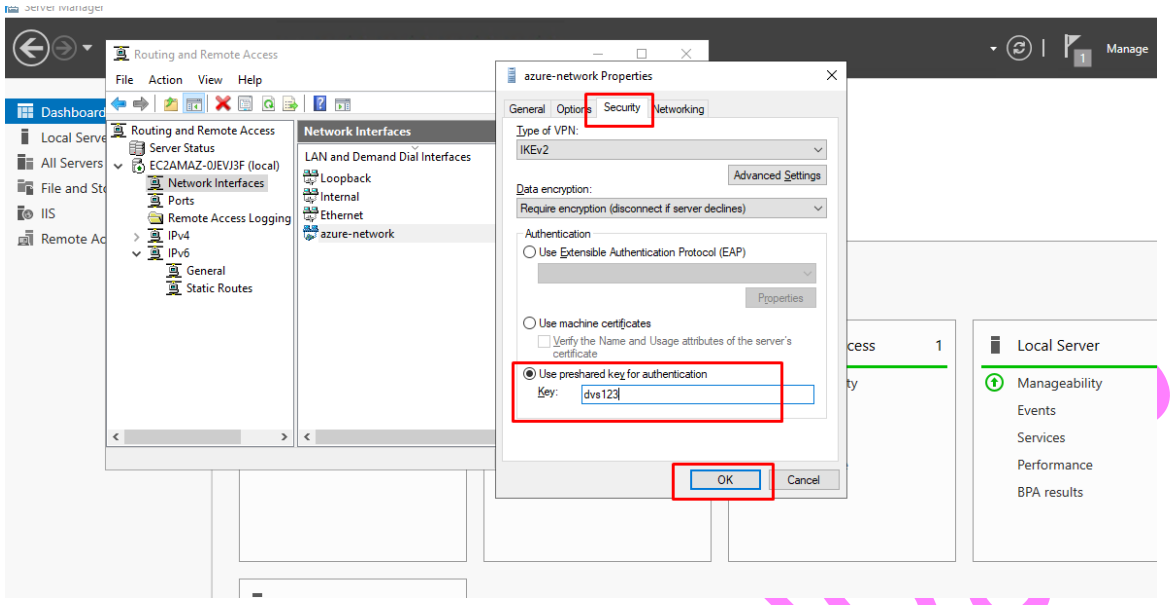

Routing and Remote Access
File
Demand-Dial Interface Wizard
Dial-Out Credentials
Supply the user name and password to be used when connecting to the remote router.
You need to set the dial out credentials that this interface will use when connecting to the remote router. These credentials must match the dial in credentials configured on the remote router.
User name:
Domain:
Password:
Confirm password:
< Back
Next >
Cancel
Dashboard
Local Serve
All Servers
File and St
IIS
Remote Ac
Remote Access 1
Manageability
Events
Services
Performance
BPA results
BPA results

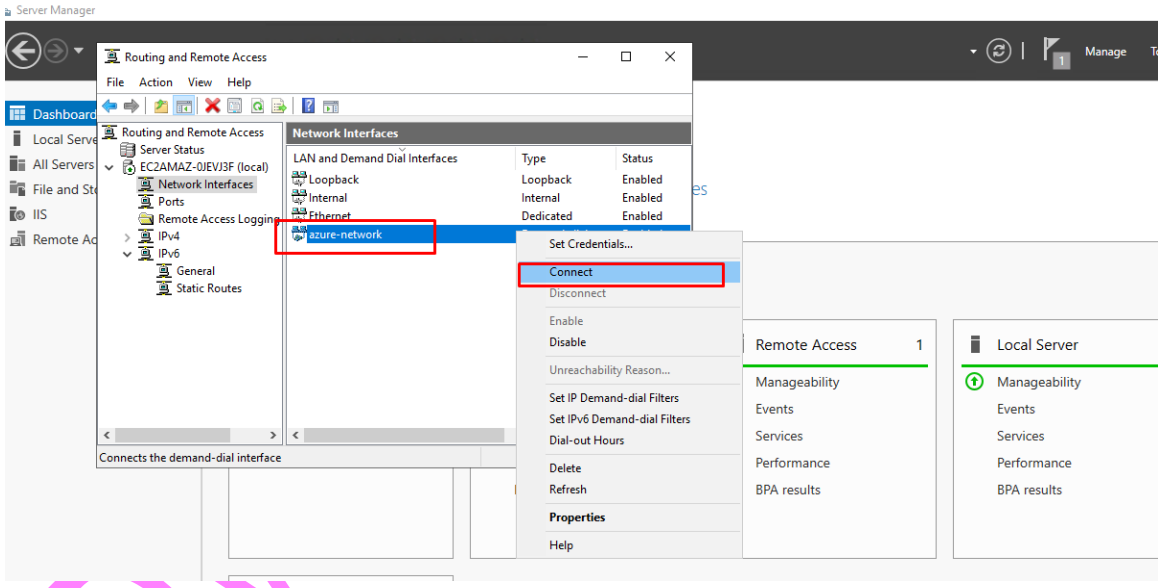

Routing and Remote Access
File
Demand-Dial Interface Wizard
Completing the Demand-Dial Interface Wizard.
You have successfully completed the Demand-Dial Interface Wizard.
When you click Finish, this wizard creates the interface and enables it on the router. To edit the interface, in the Routing and Remote Access snap-in, click Network Interfaces. Select the interface, and then click Properties.
< Back
Finish
Cancel
Dashboard
Local Serve
All Servers
File and St
IIS
Remote Ac
Remote Access 1
Manageability
Events
Services
Performance
BPA results
BPA results

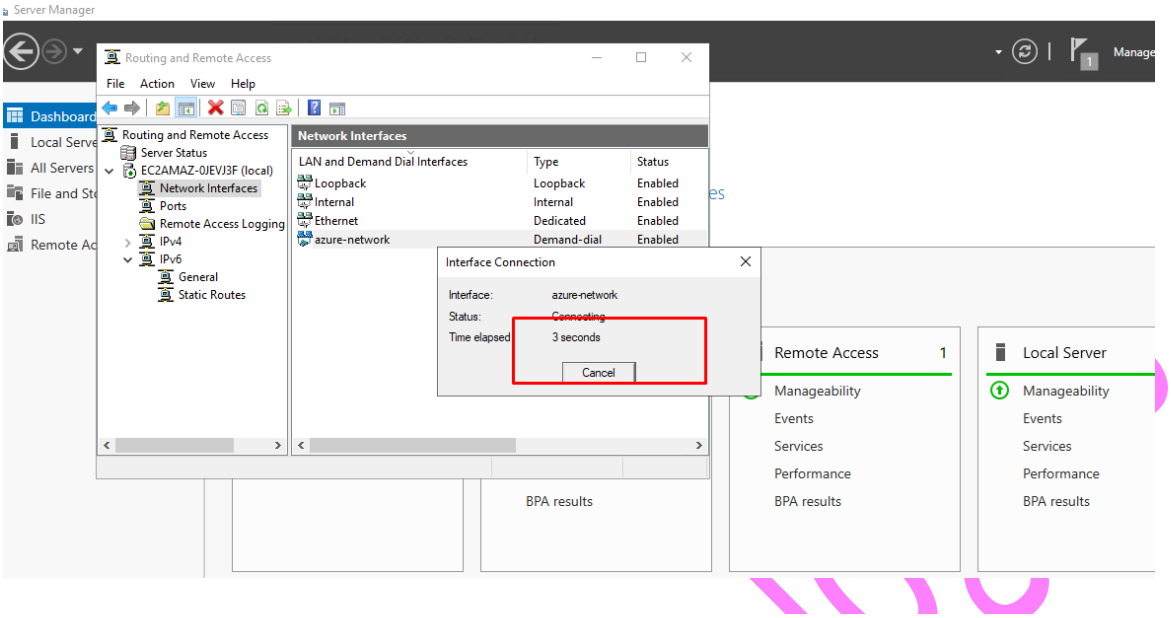


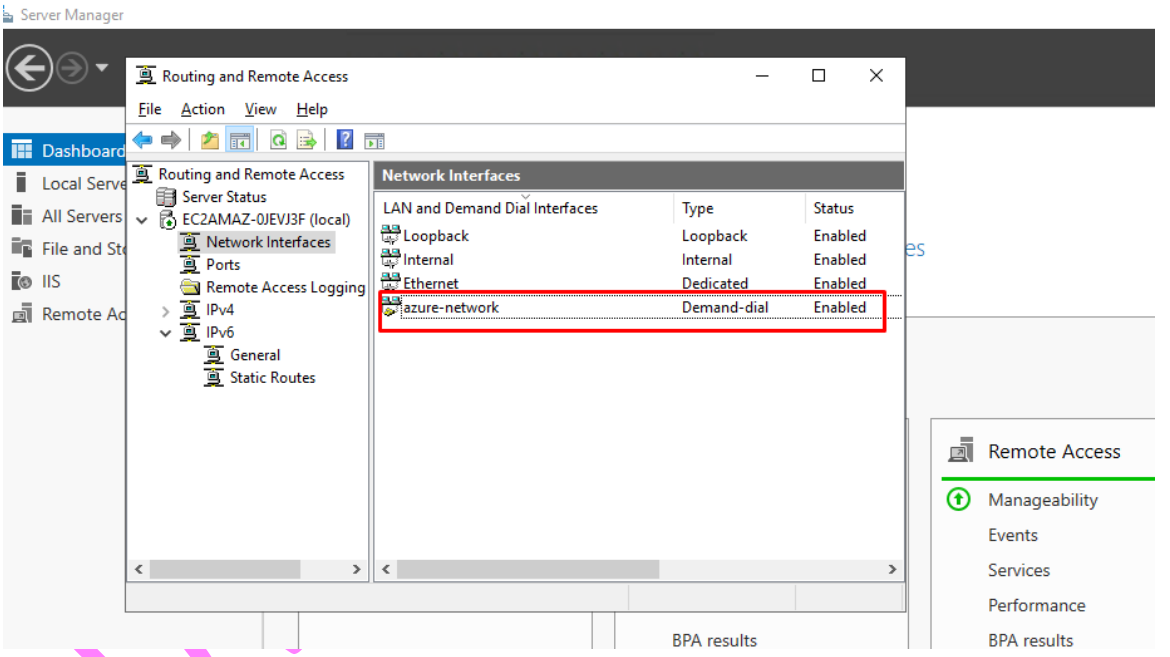


Note: remember we gave the password "dvs123"

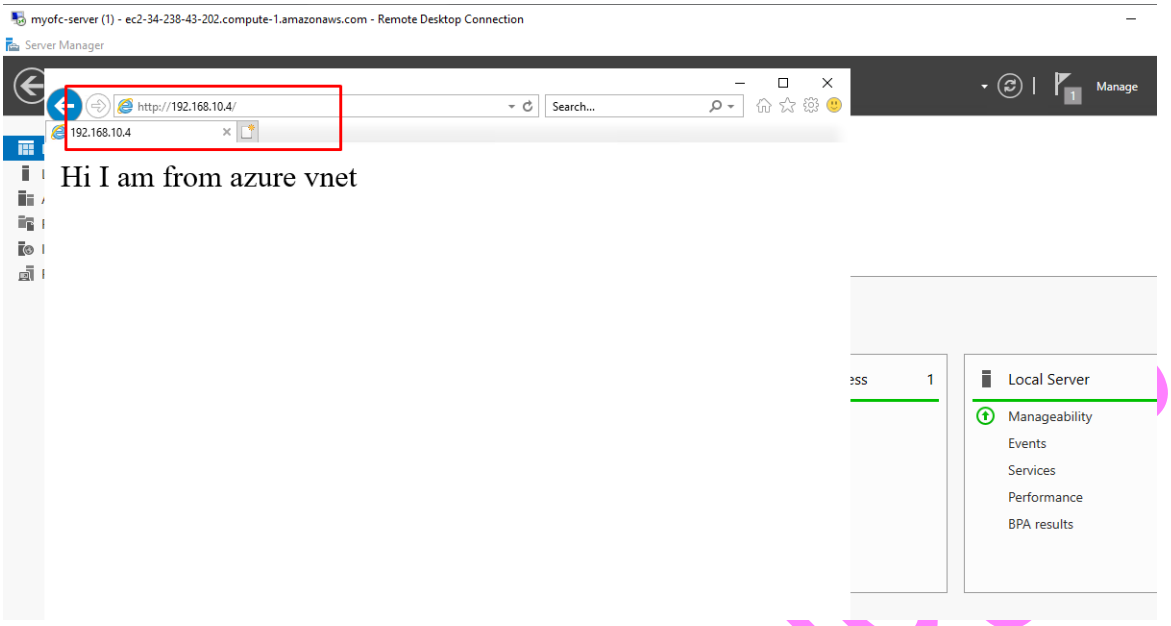

Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
EC2AMAZ-0JEVJ3F (local)
Network Interfaces
Ports
Remote Access Logging
IPv4
IPv6
General
Static Routes
Network Interfaces
LAN and Demand Dial Interfaces
Loopback
Internal
Ethernet
azure-network
azure-network Properties
General Options Security Networking
Type of VPN:
IKEv2
Advanced Settings
Data encryption:
Require encryption (disconnect if server declines)
Authentication
Use Extensible Authentication Protocol (EAP)
Properties
Use machine certificates
Verify the Name and Usage attributes of the server's certificate
Use preshared key for authentication
Key:
dvs123
OK
Cancel
Manage
Local Server
Manageability
Events
Services
Performance
BPA results


Server Manager
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
EC2AMAZ-0JEVJ3F (local)
Network Interfaces
Ports
Remote Access Logging
IPv4
IPv6
General
Static Routes
Network Interfaces
LAN and Demand Dial Interfaces
Type
Status
Loopback
Loopback
Enabled
Internal
Internal
Enabled
Ethernet
Dedicated
Enabled
azure-network
Set Credentials...
Connect
Disconnect
Enable
Disable
Unreachability Reason...
Set IP Demand-dial Filters
Set IPv6 Demand-dial Filters
Dial-out Hours
Delete
Refresh
Properties
Help
Connects the demand-dial interface
Manage
Remote Access
Manageability
Events
Services
Performance
BPA results
Local Server
Manageability
Events
Services
Performance
BPA results





Now finally test the connectivity of you azure vm page from Aws server

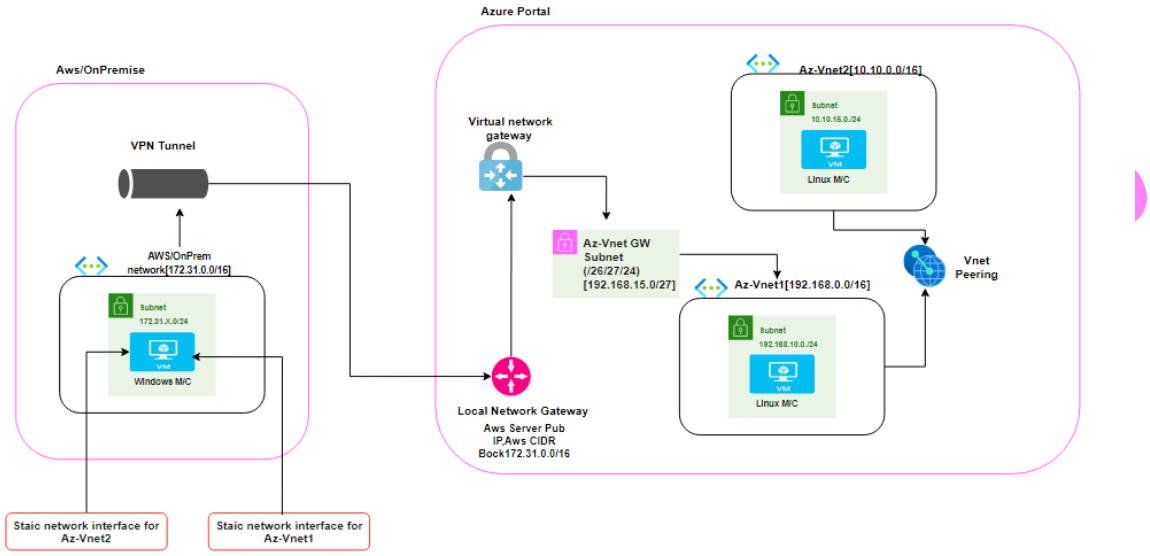


Finally we made it its working as expected …

DVS Technologies

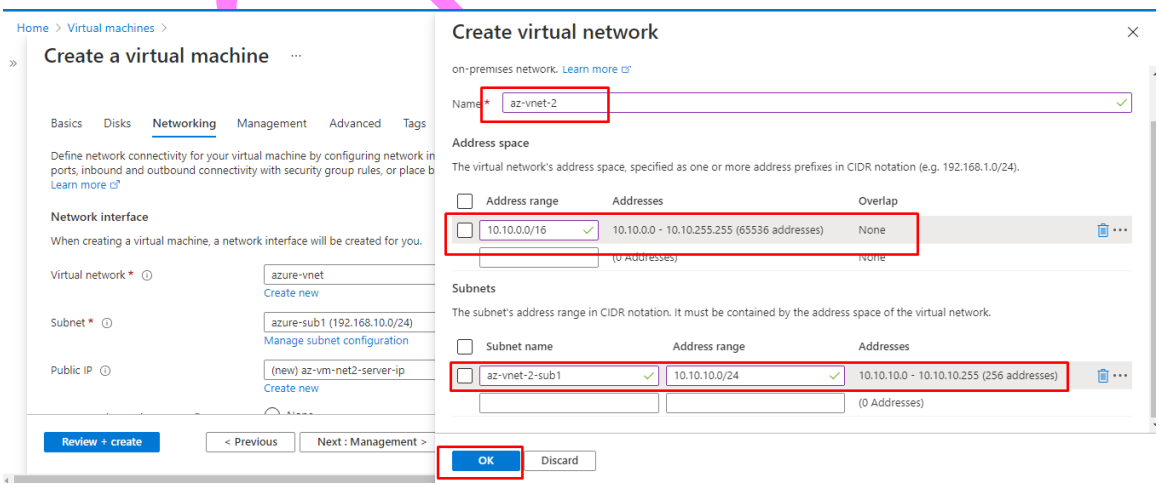
3 VPN - S2S - VNET - Peering

What if you have one more vnet available in the azure and you want to connect that VNET from aws server then ???



Let's create one more server in azure with different network let say 10.10.0.0/16 & subnet as 10.10.10.0/24 and try to install apache in that machine & then try to access that server from aws virtual machine.

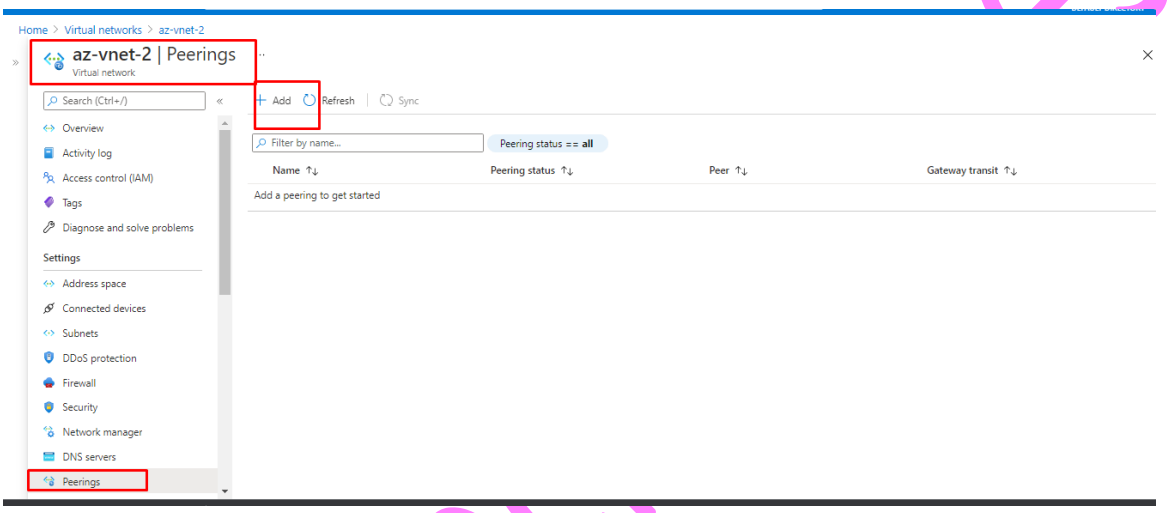
Vm creation with diff subnet:



```
#!/bin/bash
yum install httpd -y
systemctl enable httpd
echo "Hi I am from azure second network " > /var/www/html/index.html
systemctl restart httpd
```

Once VM is up since we have two VNET's 192.168.0.0/16 && 10.10.0.0/16 these two networks won't speak with each other hence configure the VNET peering connection.

DO THE PEERING FROM VNET2 TO VNET1



DVS Technologies

Home > Virtual networks > az-vnet-2 >

Add peering

az-vnet-2

This virtual network

Peering link name *

PEER2

Traffic to remote virtual network

Allow (default)

Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network

Allow (default)

Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server

Use this virtual network's gateway or Route Server

Use the remote virtual network's gateway or Route Server

None (default)

Remote virtual network

Add

Home > Virtual networks > az-vnet-2 >

Add peering

az-vnet-2

Peering link name *

PEER1

Virtual network deployment model

Resource manager

Classic

I know my resource ID

Subscription *

Pay-As-You-Go

Virtual network *

azure-vnet

Traffic to remote virtual network

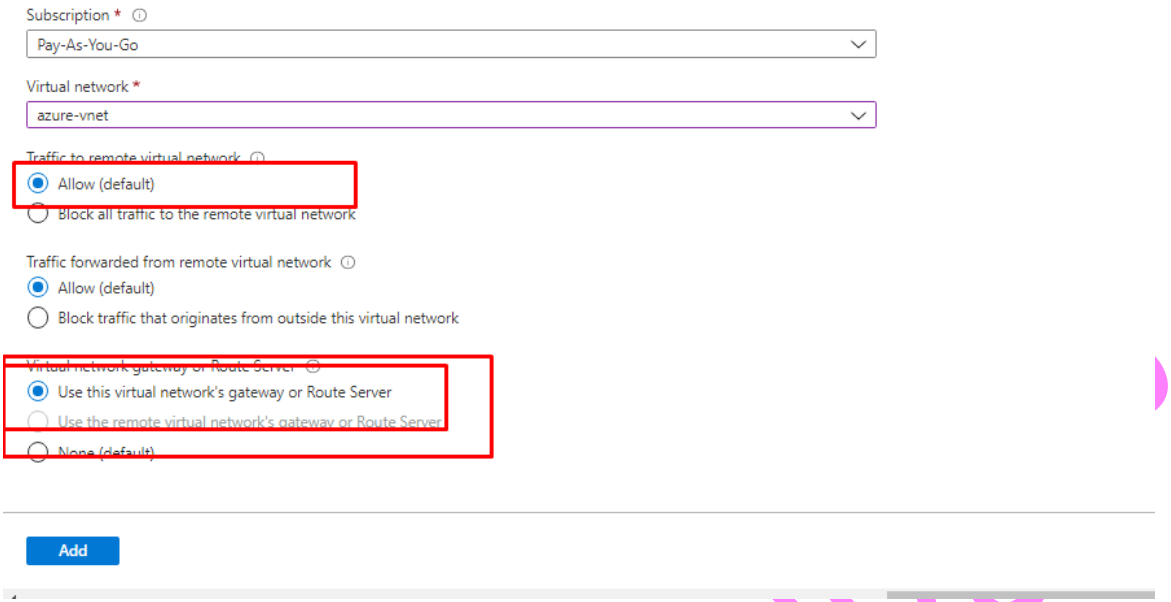
Allow (default)

Block all traffic to the remote virtual network

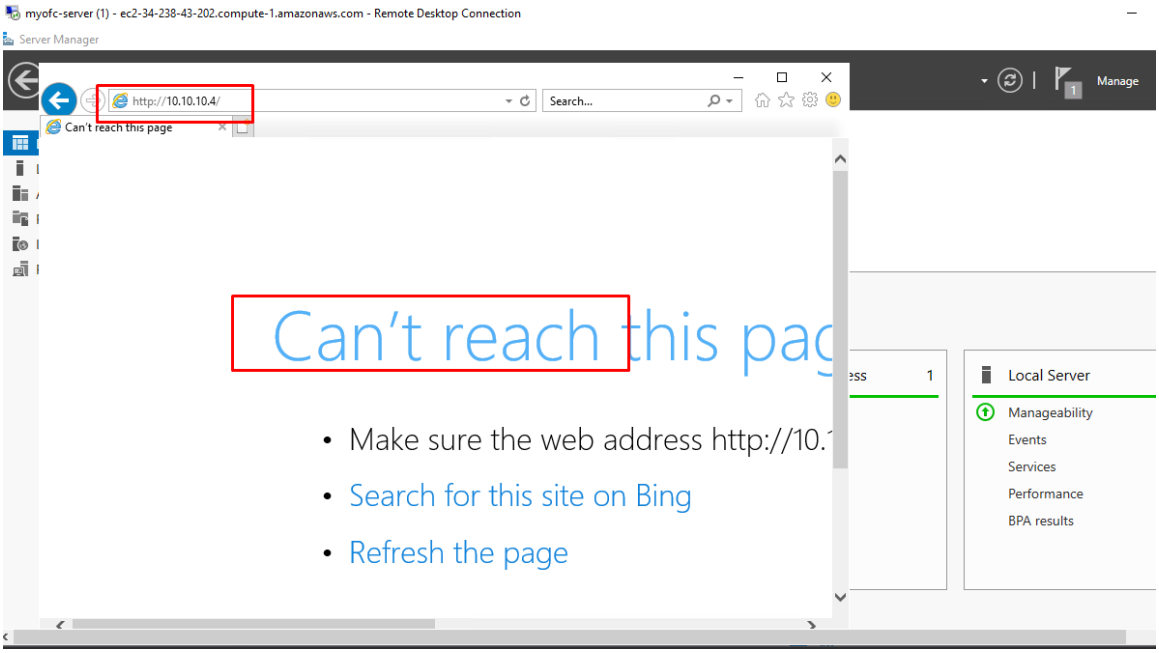
Traffic forwarded from remote virtual network

Allow (default)

Add

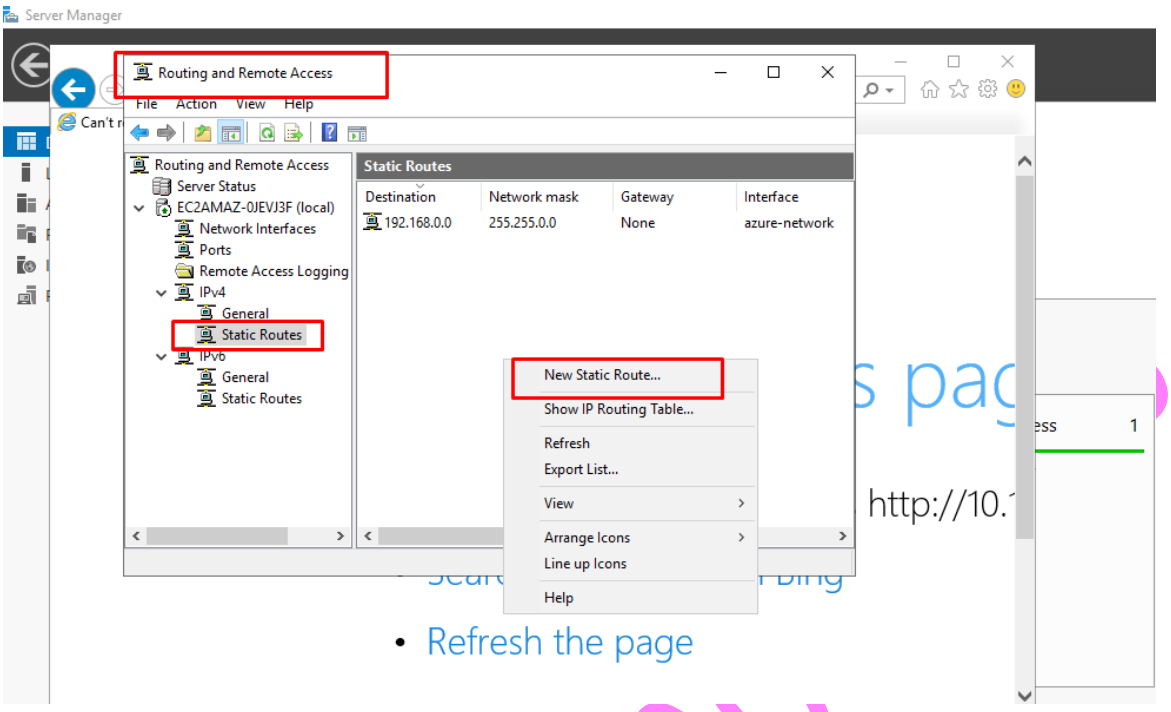


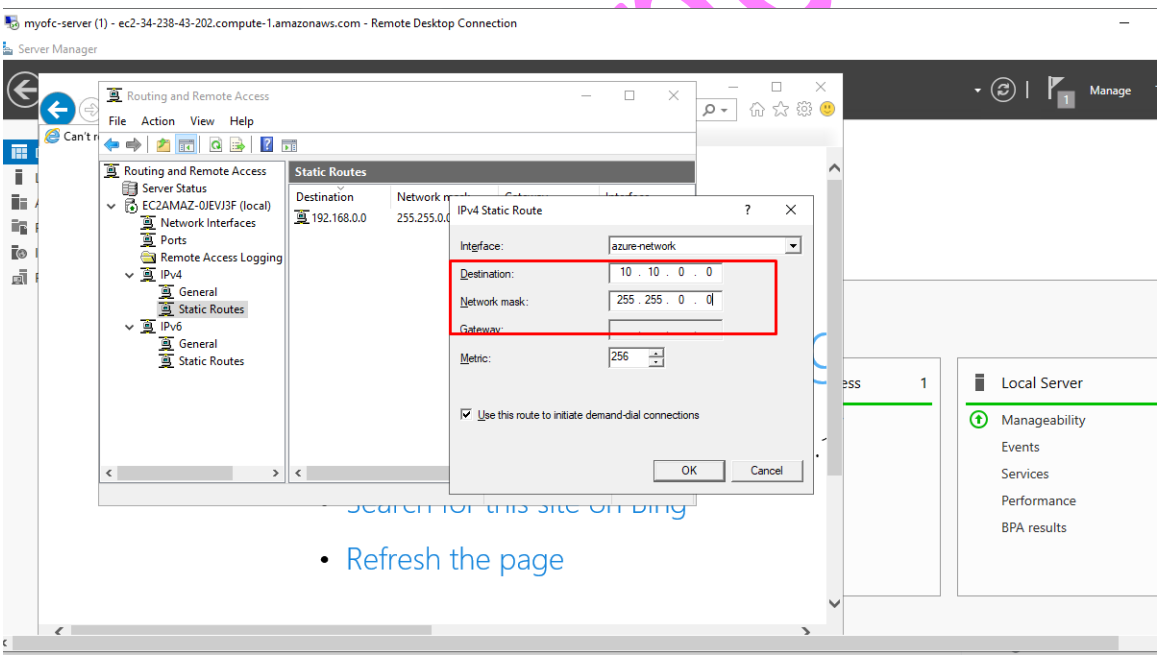
Now lets try to access our VNET-2 VM from our aws server.



Even we enable the peering connection still we can't reach the VNET2 servers from our Aws server

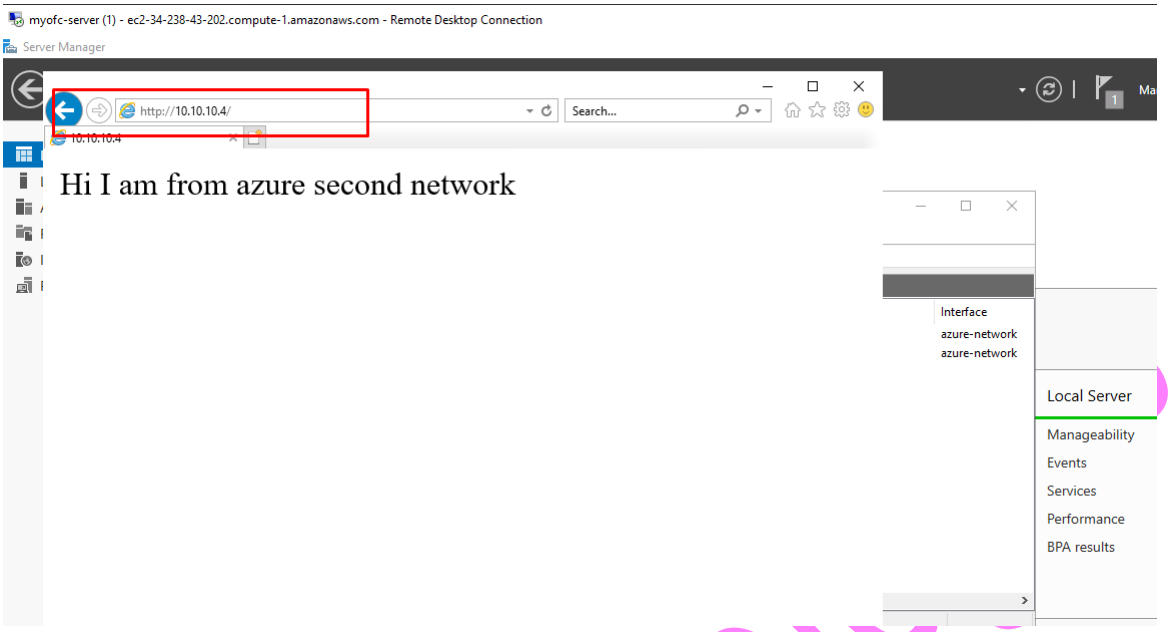
Let's try to do the modifications to our AWS server. We need to add a static route so that we can connect to VNET-2





Here we need to add our VNET2 peering ipaddress range i.e., 10.10.0.0/16

Once done you can test the new VM apache using http://10.10.10.4



DVS Technologies

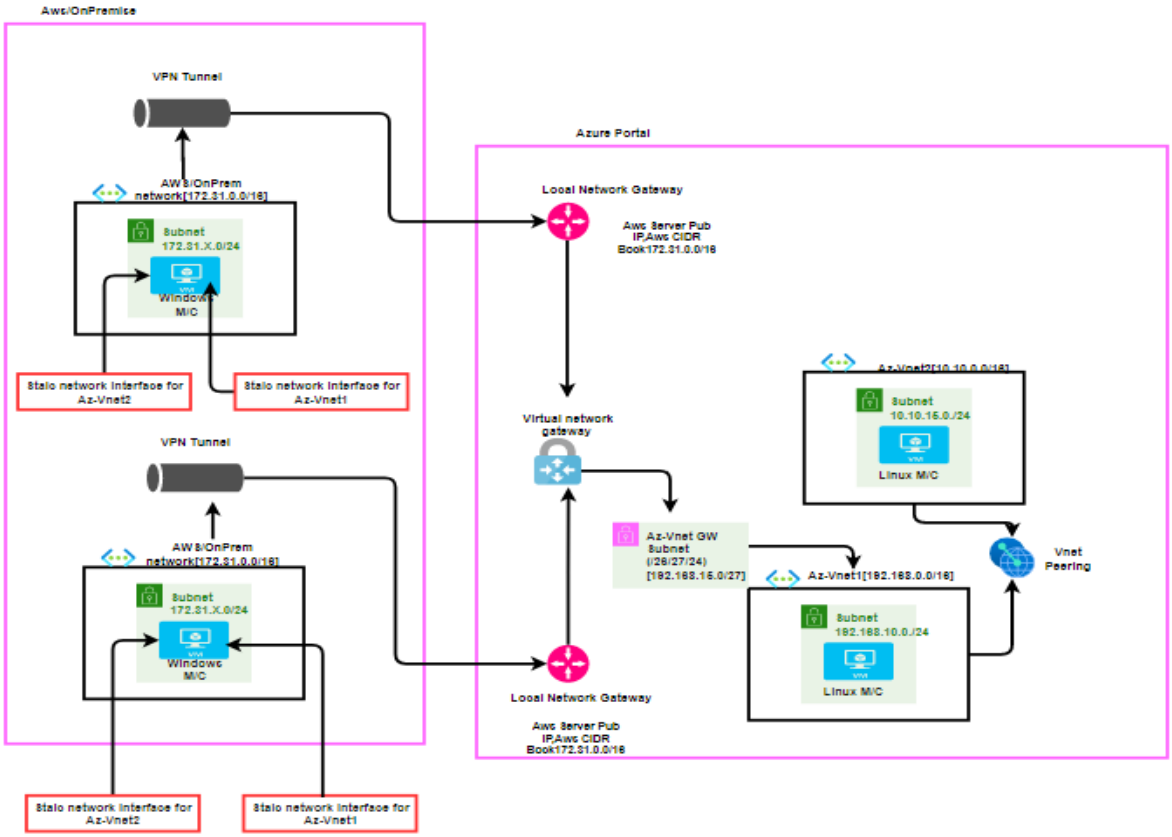
4 HA for AZ VPN gateway

You can achieve high availability for your az vpn gateway i.e., by default AZ VPN Gateway comes with HA from azure. When you are trying to connect to azure from aws then you have to have a device configured in the aws now if you want to make it HA then make sure that you are creating two devices (in our case VM's) in AWS & you have to create two Local network gateway in azure and these two networks should be added as part of the VPN gateway connections in order to make to effect.

So its going to be like below

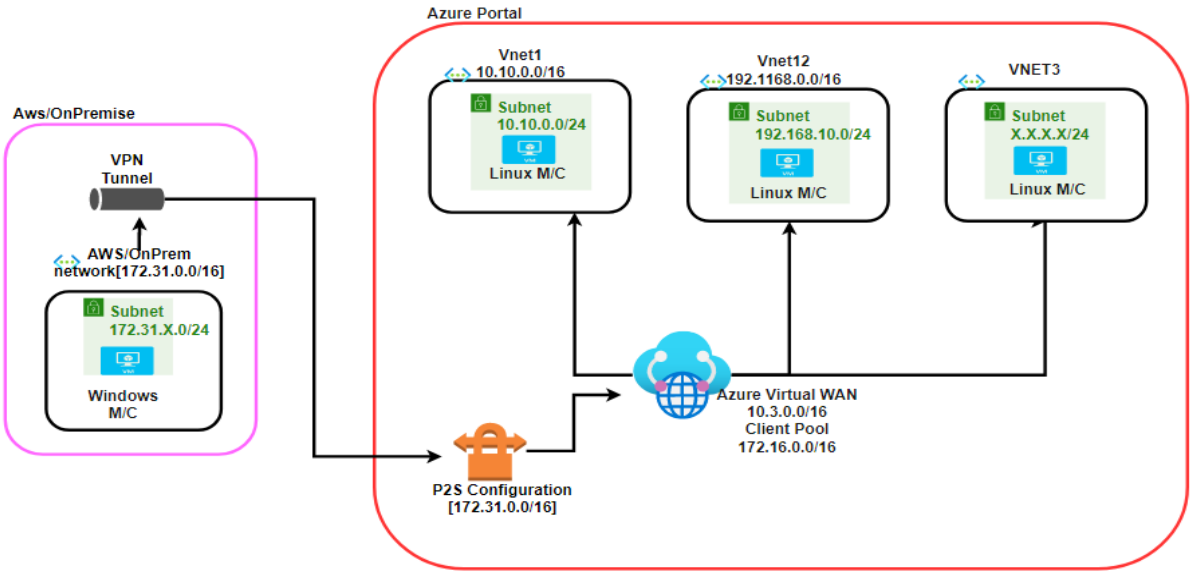
Aws (2 servers-vms) ==> connected to two Azure local gateway networks ==> these two networks connected to AZ vpn gateway connections.

By doing this if incase if one of your aws instance is down then no need to worry you will have other one in place.



5 AZ Virtual WAN Service

NOTE: It will take 30 minutes for creating the HUB



Imagine a situation that you are having 2-5 VNET's in azure and you want to connect from onpremise (vm's or switches) then as per our knowledge we have two options

Enable peering between all the VNET's
Configure the vpn gateway for individual VNETS & maintain all the configurations/connections

But Azure have come up with one more option called AZ WAN service which will help you to connect multiple VNET's of Azure from on premise without above options.

Create a virtual WAN resource with standard type

Its bit hard to implement site to site connectivity as we need entire infrastructure hence we will stick with point to site creation.
Note: here we need to generate the certs in the point server & map it to the target section with base64

Let's configure the setup:

Azure:

Create two VNET's with one servers each and configure the apache in both servers

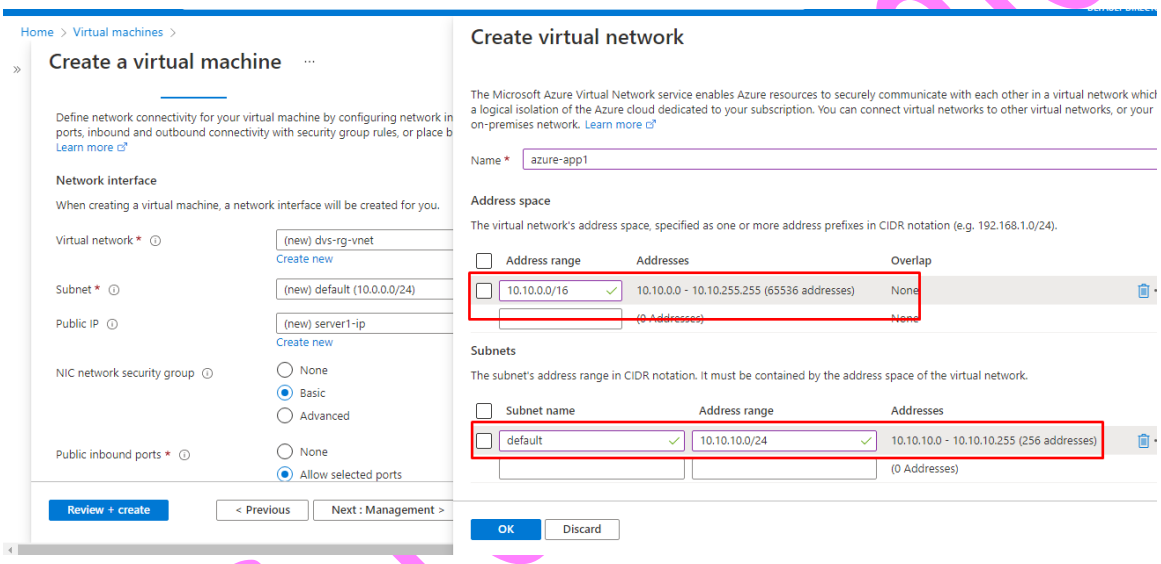
Create virtual hub

Aws:
Create one windows VM (172.31.0.0/16)
Generate the certificates in this VM so that we can use them for the P2S connectivity

Server & VNET creation:
Creating VNET's let say azure-app1 (10.10.0.0/16) & azure-app2(192.168.0.0/16):

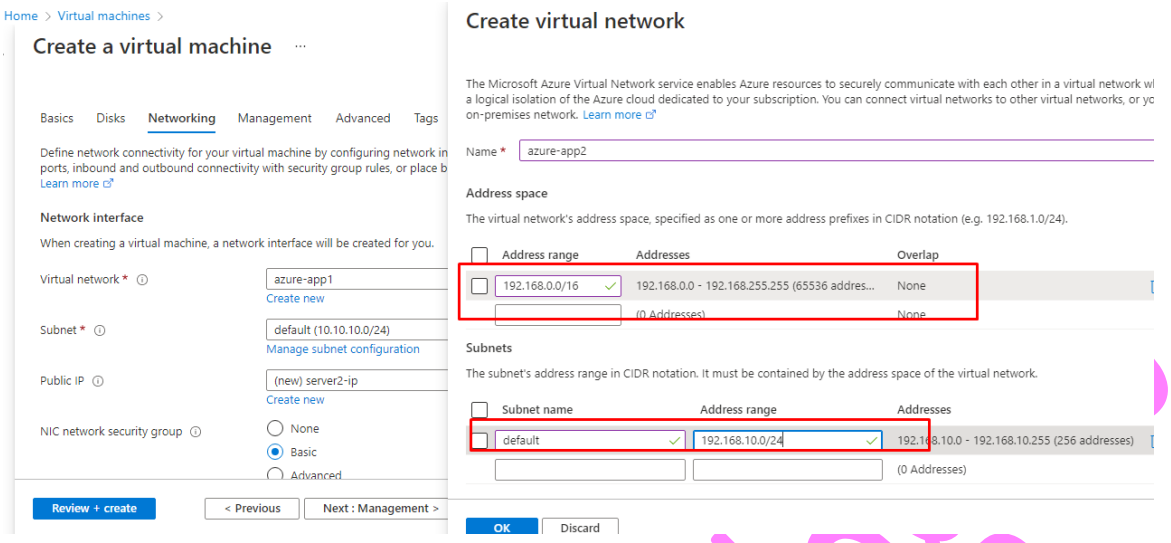
Server1:

Creating centos servers



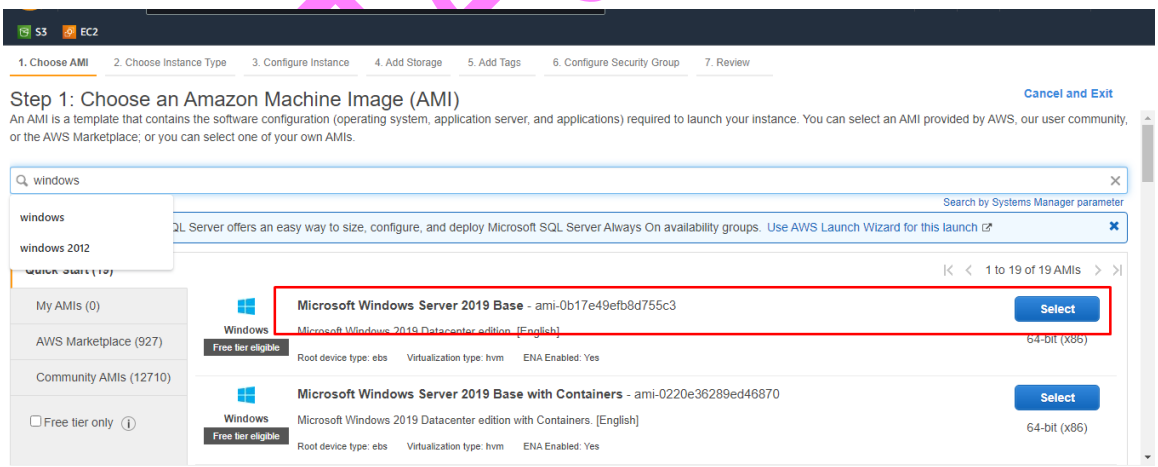
Use advanced tab & paste below
#!/bin/bash
yum install httpd -y
systemctl enable httpd
echo "Hi all I am from server1" > /var/www/html/index.html
systemctl restart httpd

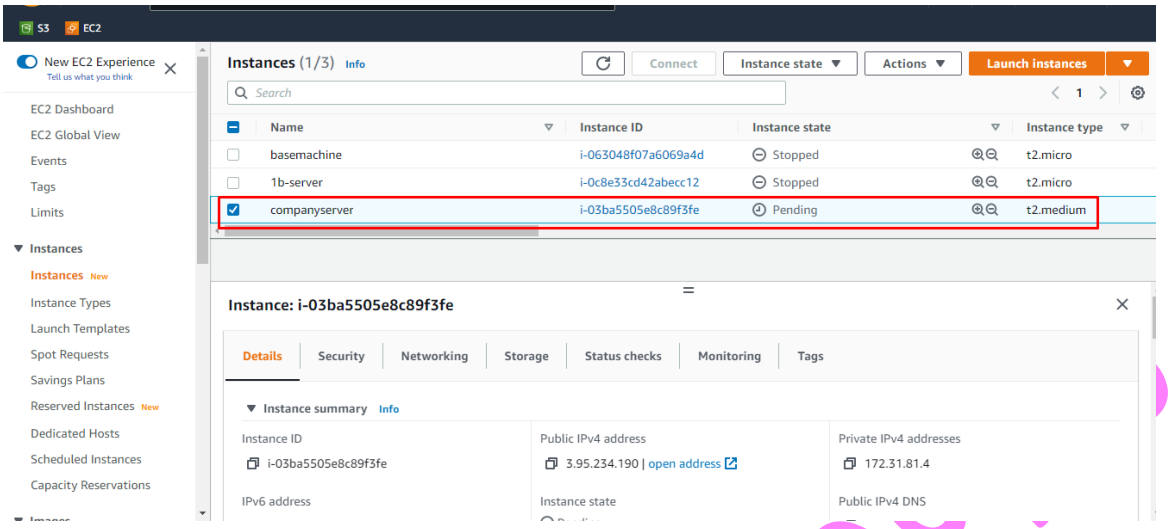
Do the same for server2



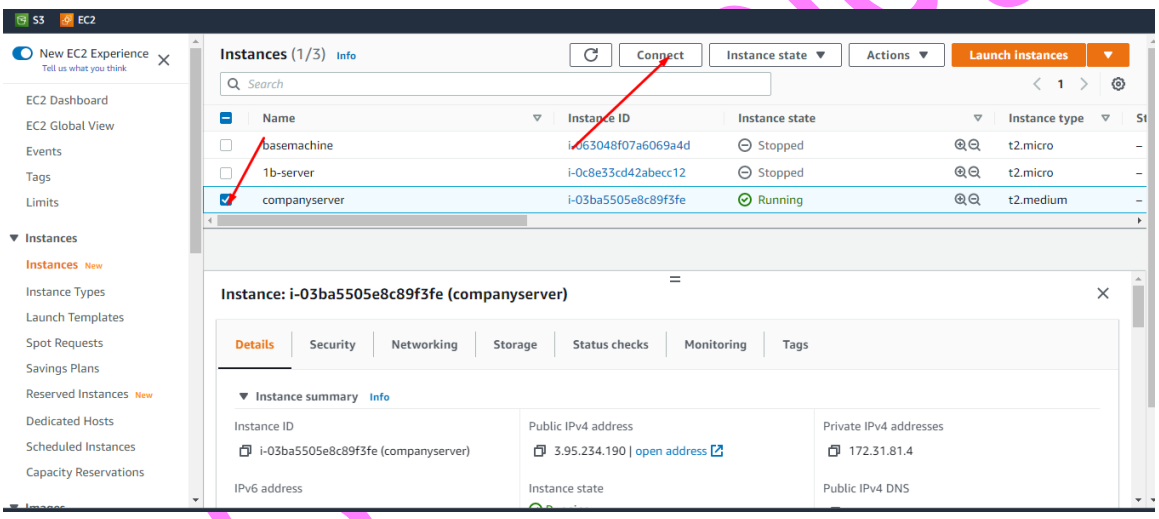
Use advanced tab & paste below
#!/bin/bash
yum install httpd -y
systemctl enable httpd
echo "Hi all I am from server2" > /var/www/html/index.html
systemctl restart httpd

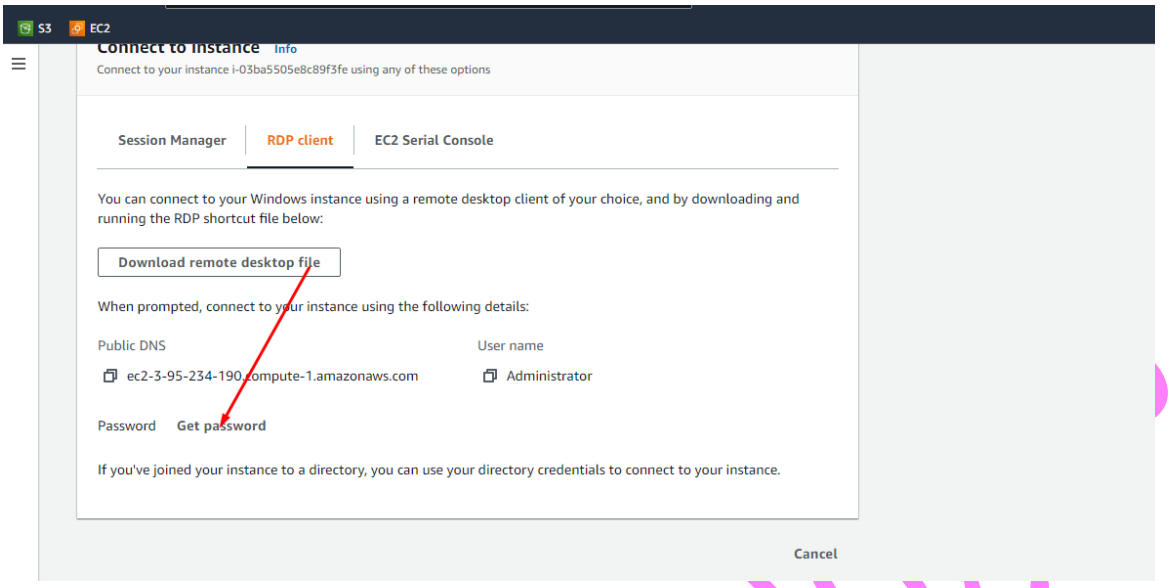
Once you are done with both servers then you can create the vm in AWS like below

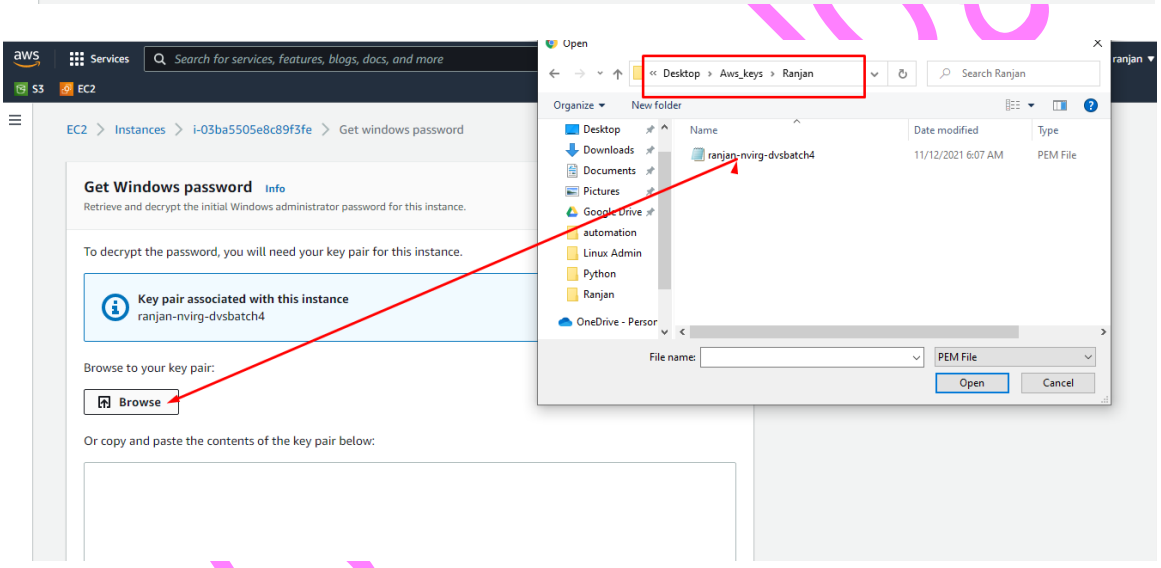


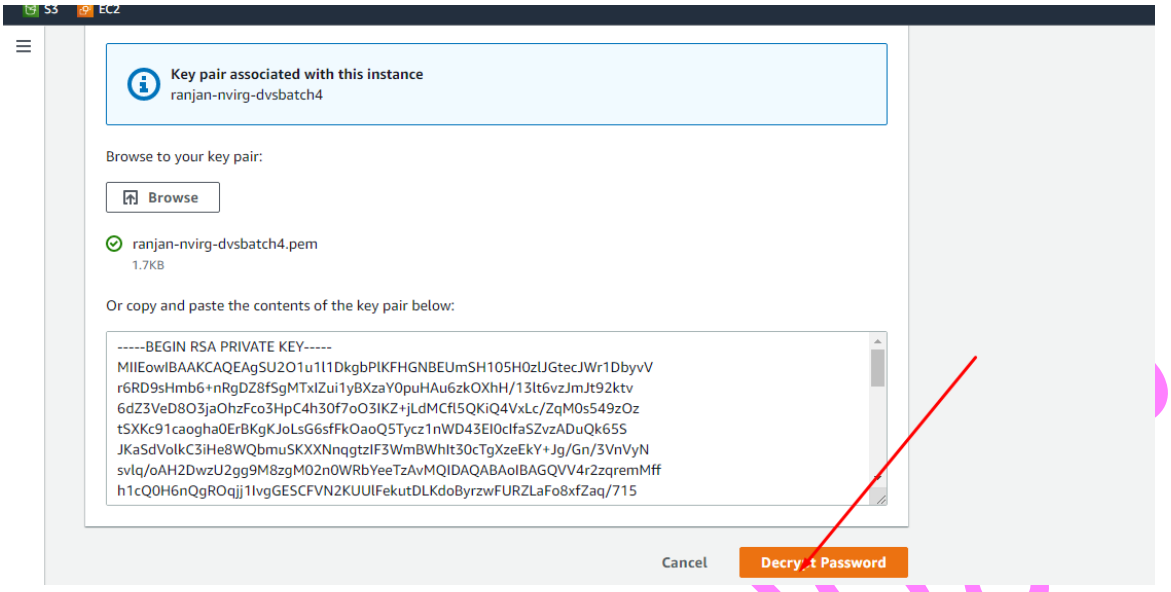


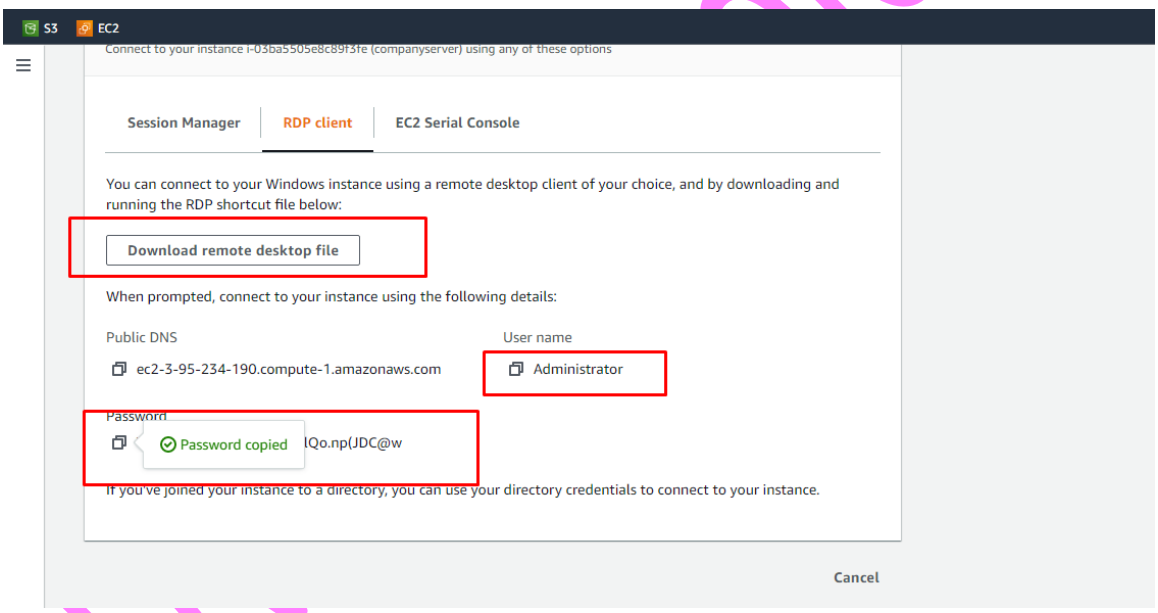
You can login to the windows server using below

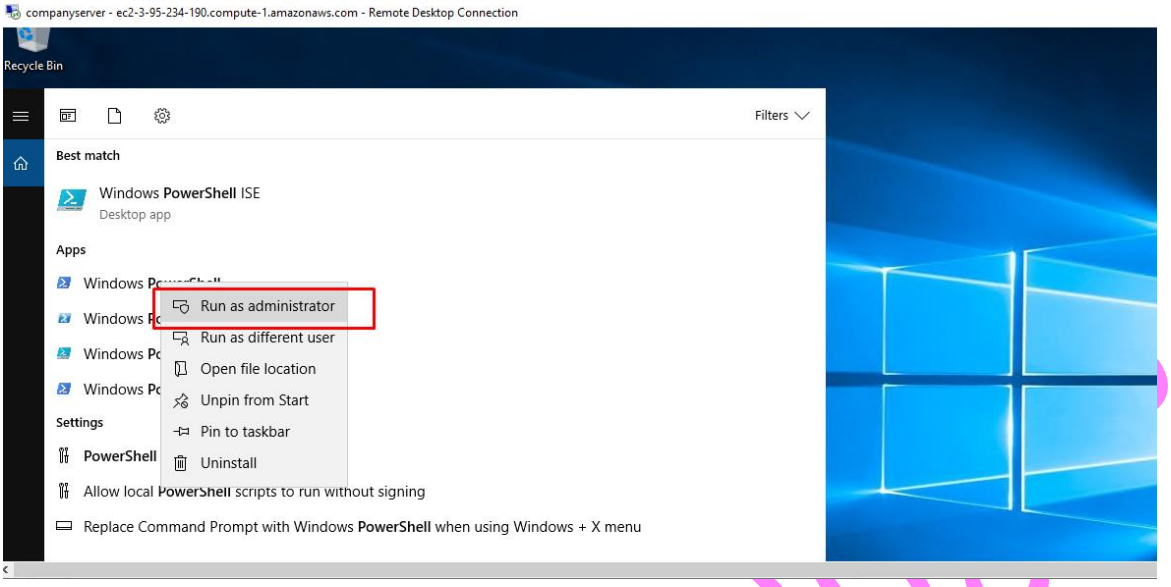



S3
EC2
Connect to instance Info
Connect to your instance i-03ba5505e8c89f3fe using any of these options
Session Manager
RDP client
EC2 Serial Console
You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:
Download remote desktop file
When prompted, connect to your instance using the following details:
Public DNS
ec2-3-95-234-190.compute-1.amazonaws.com
User name
Administrator
Password
Get password
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.
Cancel


aws
Services
Search for services, features, blogs, docs, and more
ranjan
S3
EC2
EC2 > Instances > i-03ba5505e8c89f3fe > Get windows password
Get Windows password Info
Retrieve and decrypt the initial Windows administrator password for this instance.
To decrypt the password, you will need your key pair for this instance.
Key pair associated with this instance
ranjan-nvirg-dvsbatch4
Browse to your key pair:
Browse
Or copy and paste the contents of the key pair below:
Open
Desktop > Aws_keys > Ranjan
Search Ranjan
Organize
New folder
Desktop
Downloads
Documents
Pictures
Google Drive
automation
Linux Admin
Python
Ranjan
OneDrive - Person
Name
Date modified
Type
ranjan-nvirg-dvsbatch4
11/12/2021 6:07 AM
PEM File
File name:
PEM File
Open
Cancel


S3
EC2
Key pair associated with this instance
ranjan-nvirg-dvsbatch4
Browse to your key pair:
Browse
ranjan-nvirg-dvsbatch4.pem
1.7KB
Or copy and paste the contents of the key pair below:
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAgSU2O1u1l1DkgbPlKFHGNBEUmSH105H0zlJGtecJWr1DbyvV
r6RD9sHmb6+nRgDZ8fSgMTxIZui1yBXzaY0puHAu6zkOXhH/13lt6vzJmJt92ktv
6dZ3VeD8O3jaOhzFco3HpC4h30f7oO3IKZ+jLdMCfl5QKiQ4VxLc/ZqM0s549zOz
tSXKc91caogha0ErBKgKJoLsG6sfFkOaoQ5Tycz1nWD43EI0cIfaSZvzADuQk65S
JKaSdVolkC3iHe8WQbmuSKXXNnqgtzIF3WmBWhIt30cTgXzeEkY+Jg/Gn/3VnVyN
svlq/oAH2DwzU2gg9M8zgM02n0WRbYeeTzAvMQIDAQABAoIBAGQVV4r2zqremMff
h1cQ0H6nQgROqjj1IvgGESCFVN2KUUlFekutDLKdoByrzwFURZLaFo8xfZaq/715
Cancel
Decrypt Password

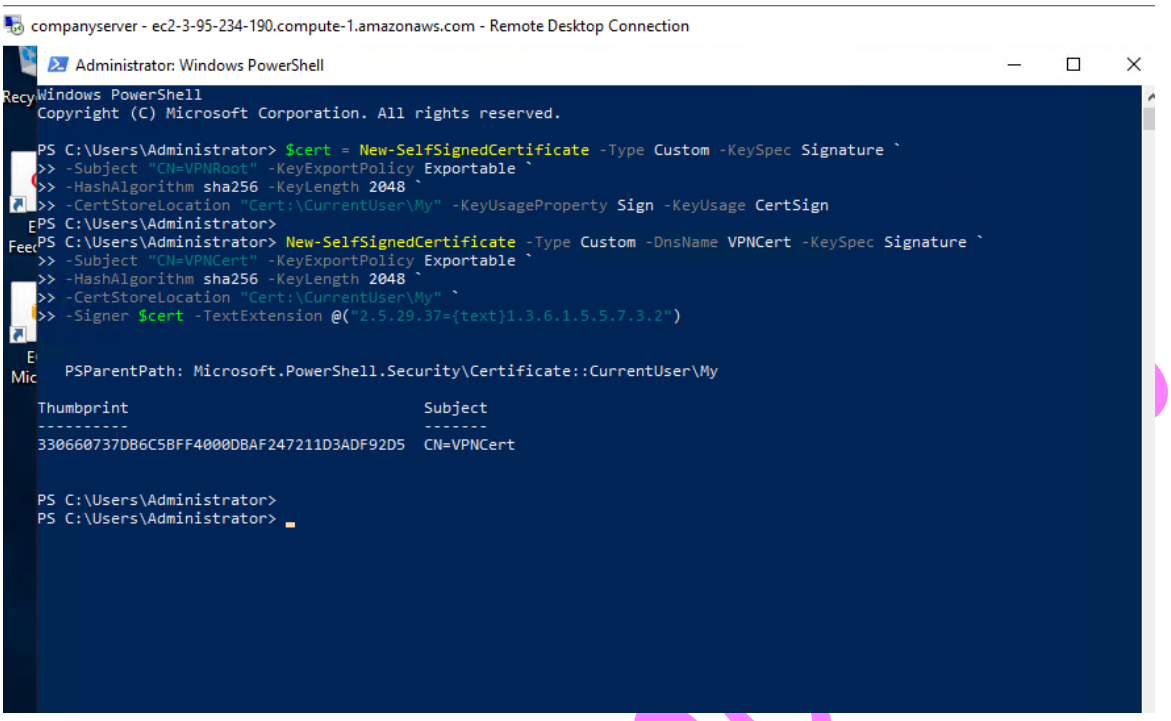

S3
EC2
Connect to your instance i-03ba5505e8c89f3fe (companyserver) using any of these options
Session Manager
RDP client
EC2 Serial Console
You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:
Download remote desktop file
When prompted, connect to your instance using the following details:
Public DNS
ec2-3-95-234-190.compute-1.amazonaws.com
User name
Administrator
Password
Password copied
lQo.np(JDC@w
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.
Cancel



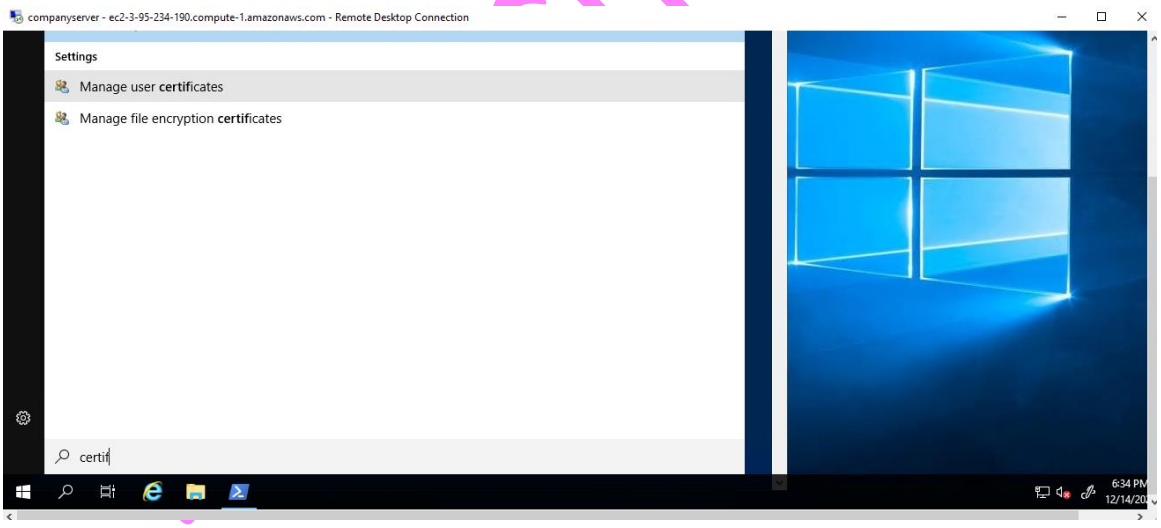

```
$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
-Subject "CN=VPNRoot" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign
```

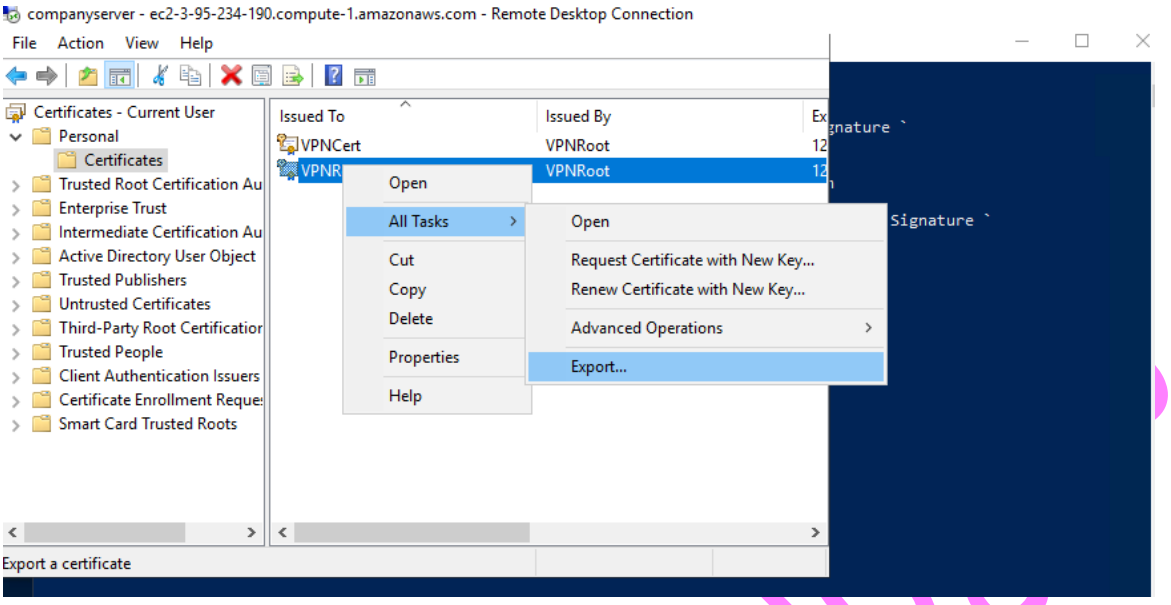
```
New-SelfSignedCertificate -Type Custom -DnsName VPNCert -KeySpec Signature `
-Subject "CN=VPNCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" `
-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")
```

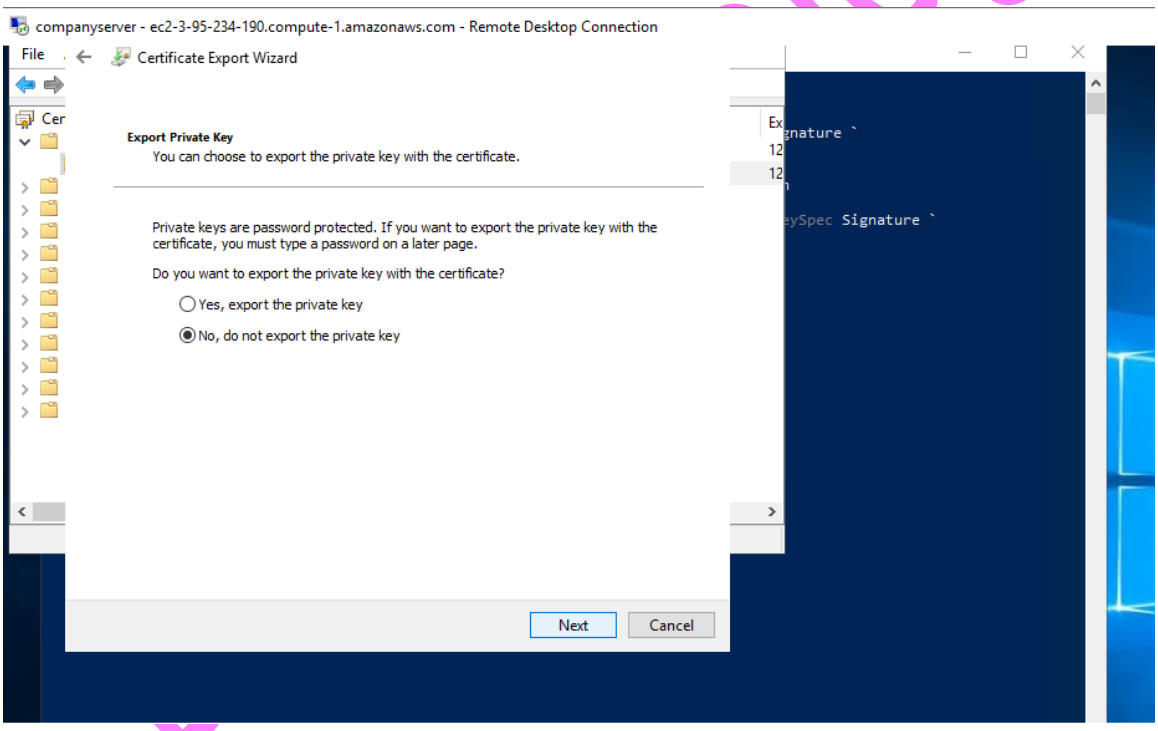
DVS Technologies

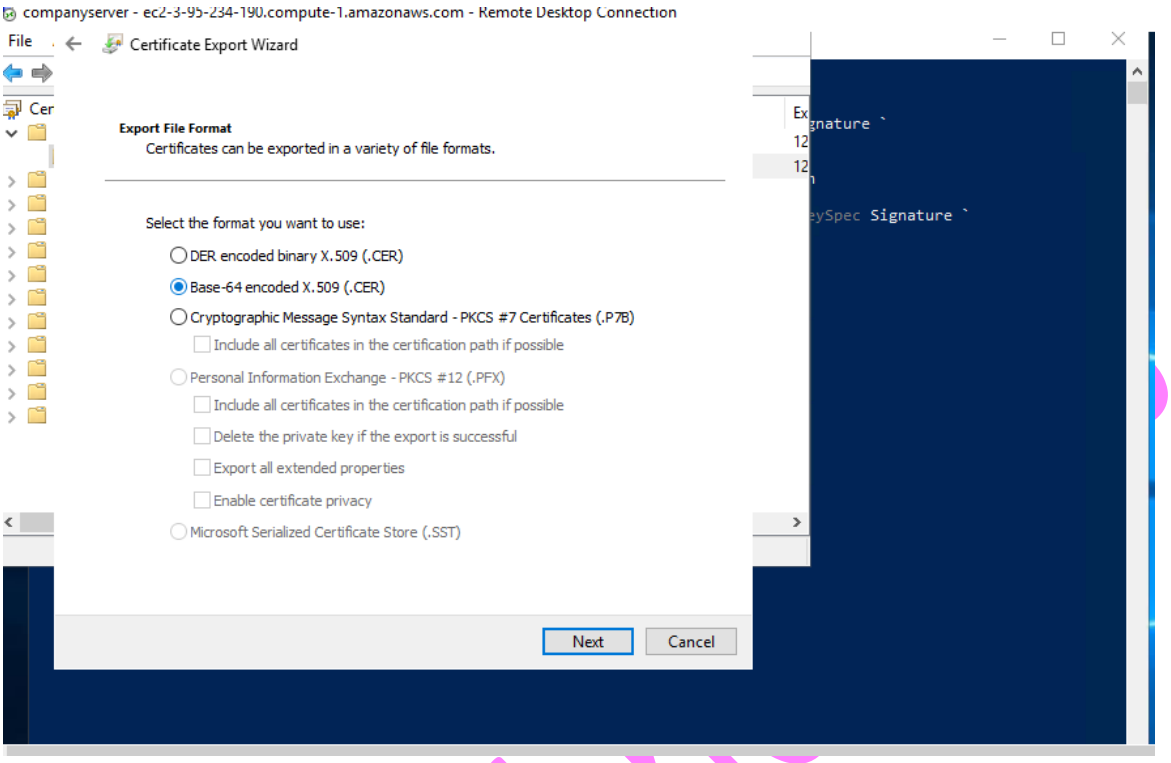


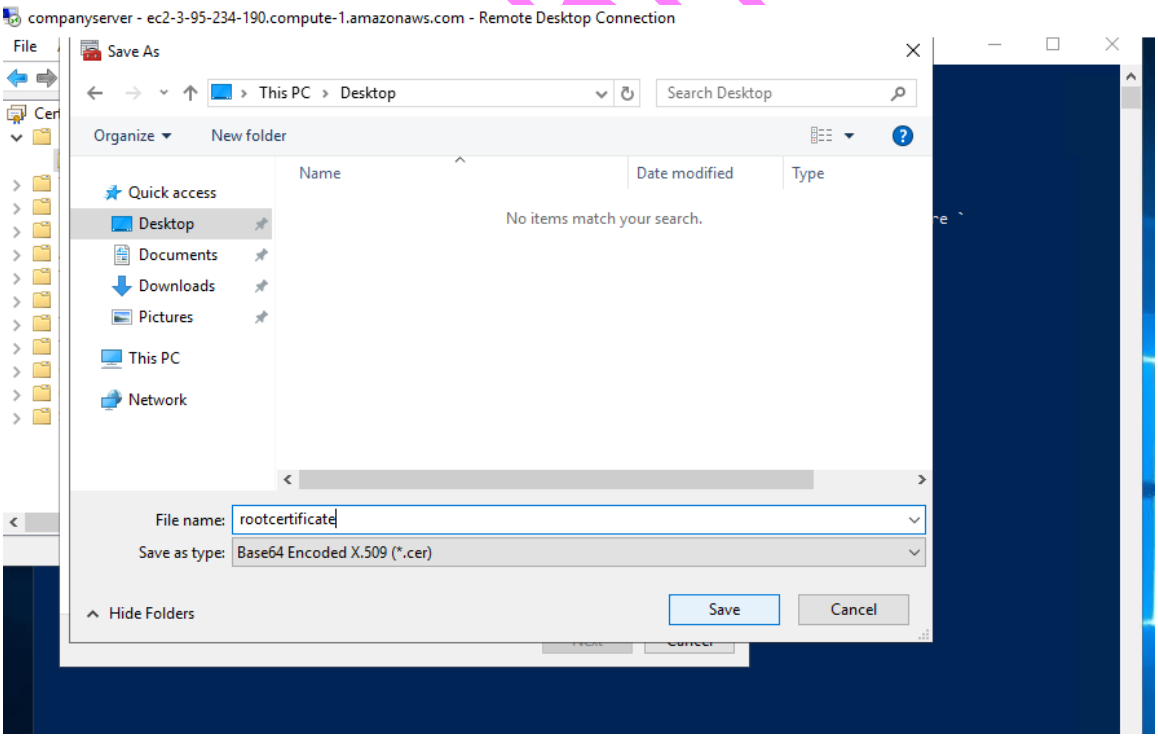
Now we are done with generating the certificates, we need to extract the cert with base64 format. Please do the below

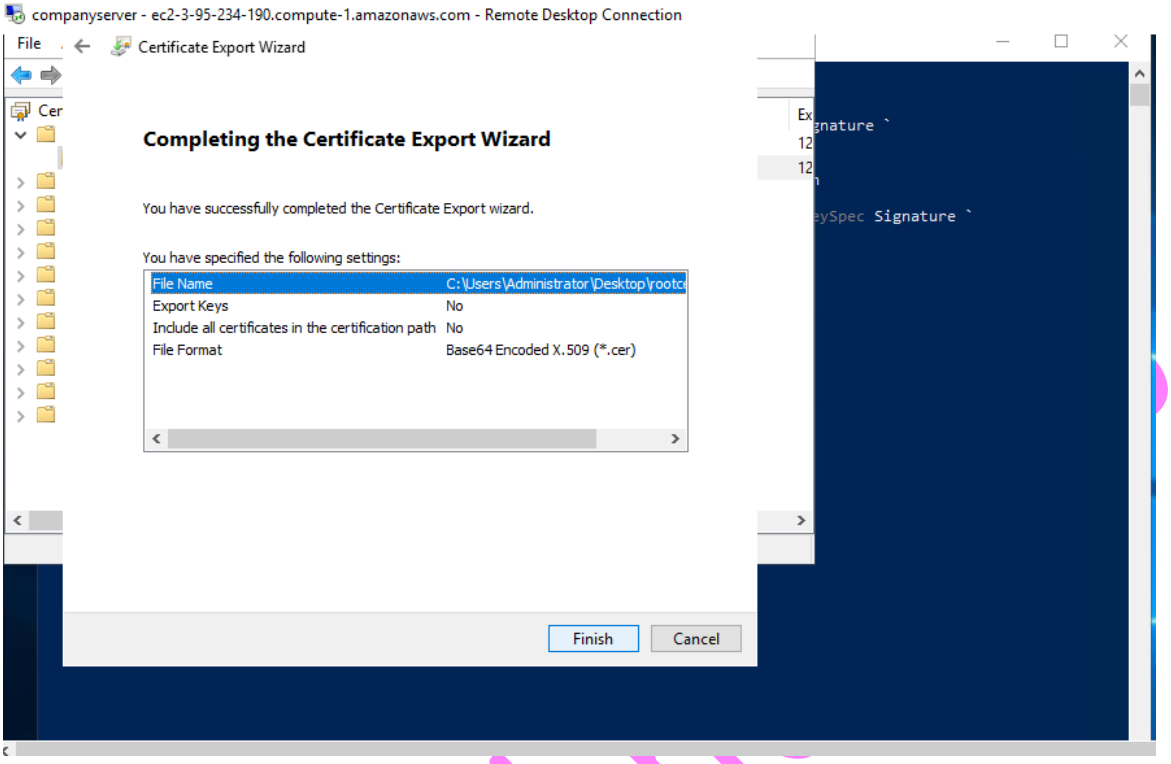


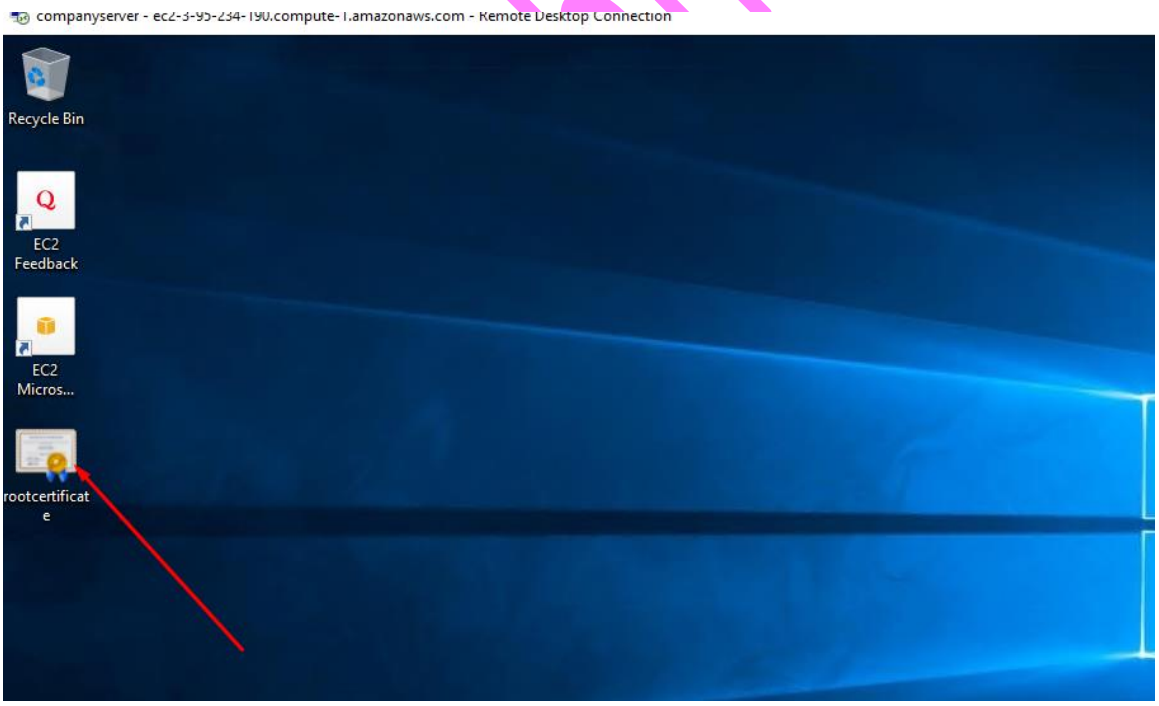

companyserver - ec2-3-95-234-190.compute-1.amazonaws.com - Remote Desktop Connection
File Action View Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Client Authentication Issuers
Certificate Enrollment Reque
Smart Card Trusted Roots
Issued To
Issued By
VPNCert
VPNRoot
VPNRoot
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Advanced Operations
Export...
Export a certificate

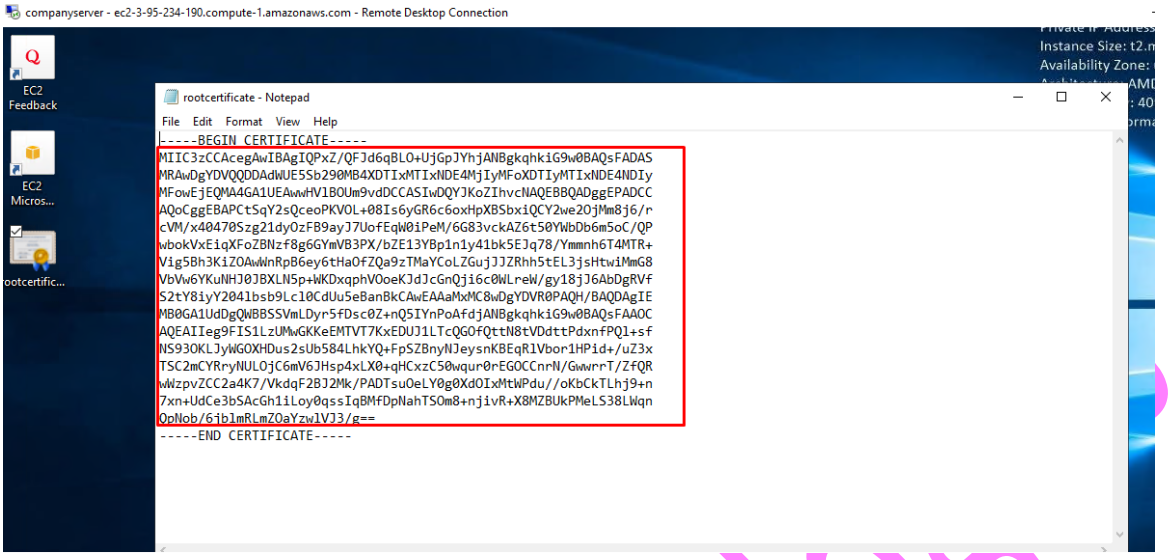

companyserver - ec2-3-95-234-190.compute-1.amazonaws.com - Remote Desktop Connection
File
Certificate Export Wizard
Export Private Key
You can choose to export the private key with the certificate.
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.
Do you want to export the private key with the certificate?
Yes, export the private key
No, do not export the private key
Next
Cancel


companyserver - ec2-3-95-234-190.compute-1.amazonaws.com - Remote Desktop Connection
File
Certificate Export Wizard
Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
Personal Information Exchange - PKCS #12 (.PFX)
Include all certificates in the certification path if possible
Delete the private key if the export is successful
Export all extended properties
Enable certificate privacy
Microsoft Serialized Certificate Store (.SST)
Next
Cancel


companyserver - ec2-3-95-234-190.compute-1.amazonaws.com - Remote Desktop Connection
File
Save As
This PC
Desktop
Search Desktop
Organize
New folder
Quick access
Desktop
Documents
Downloads
Pictures
This PC
Network
Name
Date modified
Type
No items match your search.
File name:
rootcertificate
Save as type:
Base64 Encoded X.509 (*.cer)
Hide Folders
Save
Cancel

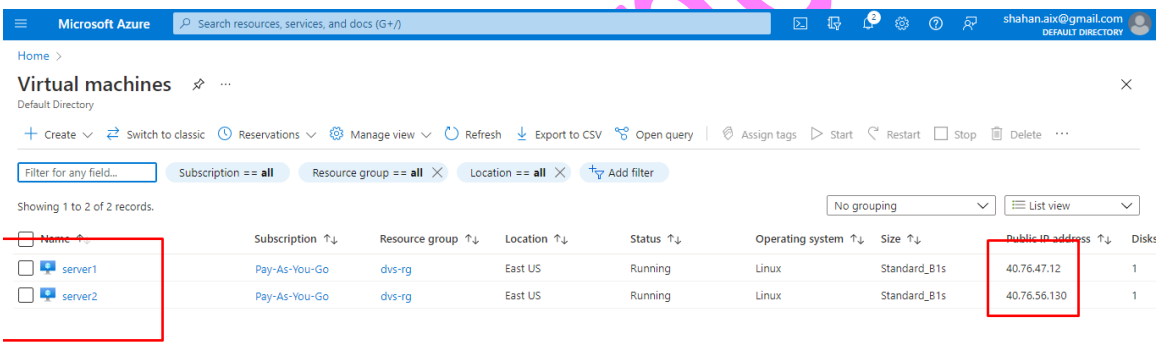

companyserver - ec2-3-95-234-190.compute-1.amazonaws.com - Remote Desktop Connection
File
Certificate Export Wizard
Completing the Certificate Export Wizard
You have successfully completed the Certificate Export wizard.
You have specified the following settings:
File Name C:\Users\Administrator\Desktop\rootc
Export Keys No
Include all certificates in the certification path No
File Format Base64 Encoded X.509 (*.cer)
Finish
Cancel

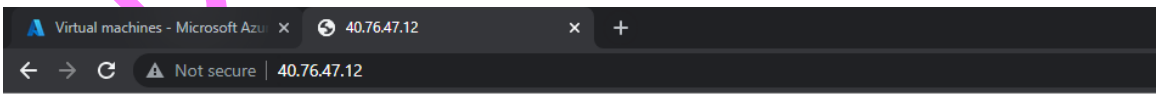

companyserver - ec2-3-95-234-190.compute-1.amazonaws.com - Remote Desktop Connection
Recycle Bin
EC2 Feedback
EC2 Micros...
rootcertificat e



Use this cert for further configuration

Testing application's in VMS:



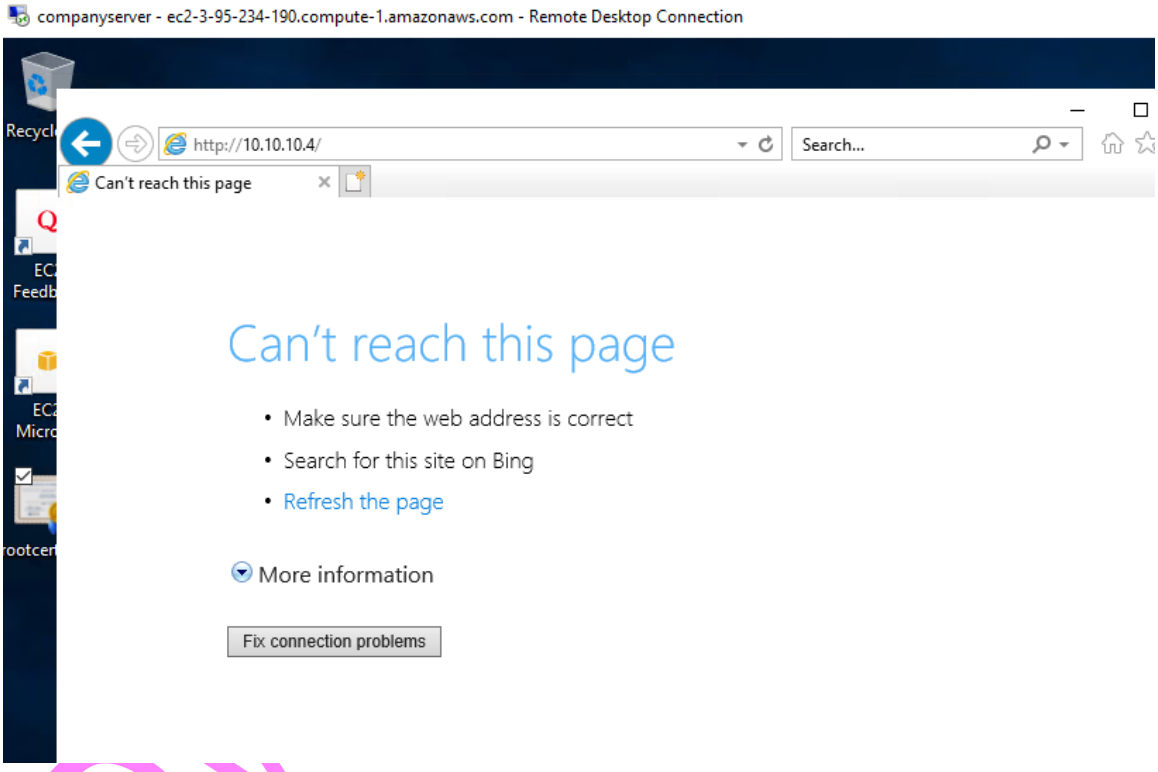


Hi all I am from server1

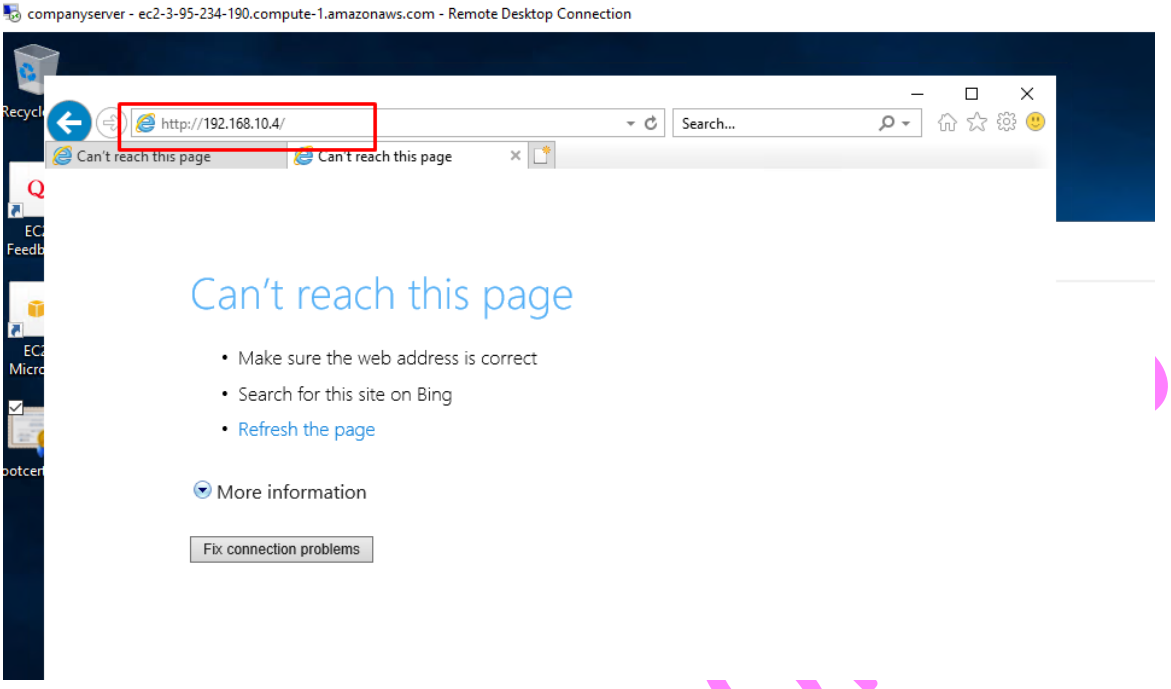
Hi all I am from server2

Now we tested from their public ipaddress now let's test the same from our AWS server with their private ipaddress. Ideally it should not work but we have to make sure that it should work.

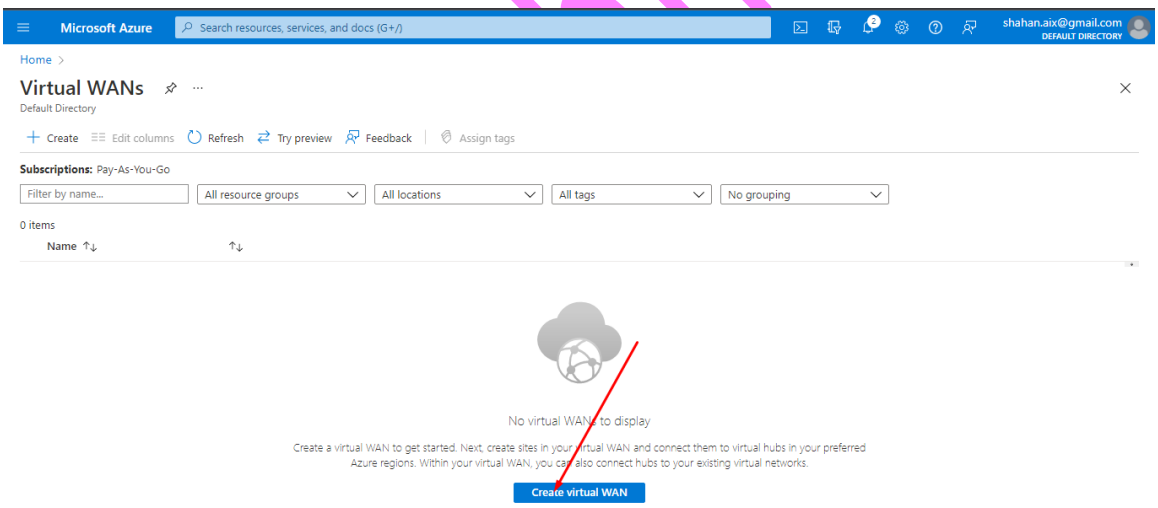
From Aws:
10.10.10.4 - server1



Server2: 192.168.10.4



Creating virtual WAN:



Microsoft Azure | Search resources, services, and docs (G+/)

Home > Virtual WANs >

Create WAN

Basics | Review + create

The virtual WAN resource represents a virtual overlay of your Azure network and is a collection of multiple resources. Learn more

Project details

Subscription * : Pay-As-You-Go

Resource group * : dvs-rg

Create new

Virtual WAN details

Resource group location * : East US

Name * : myazurehub

Type : Standard

Review + create | Previous | Next : Review + create >

Home > Virtual WANs >

Create WAN

Validation passed

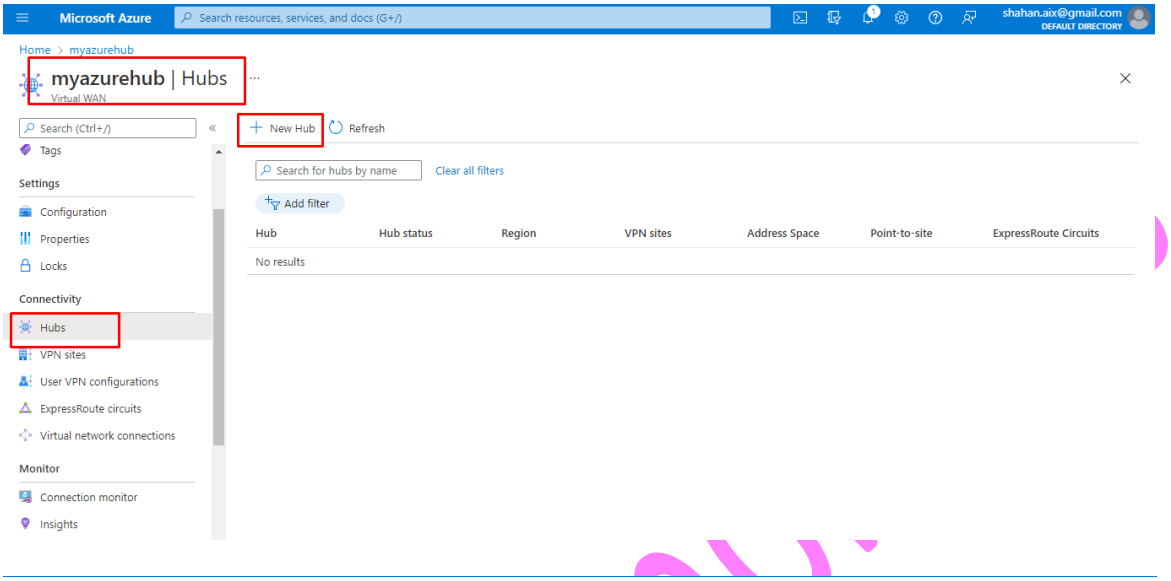
Basics | Review + create

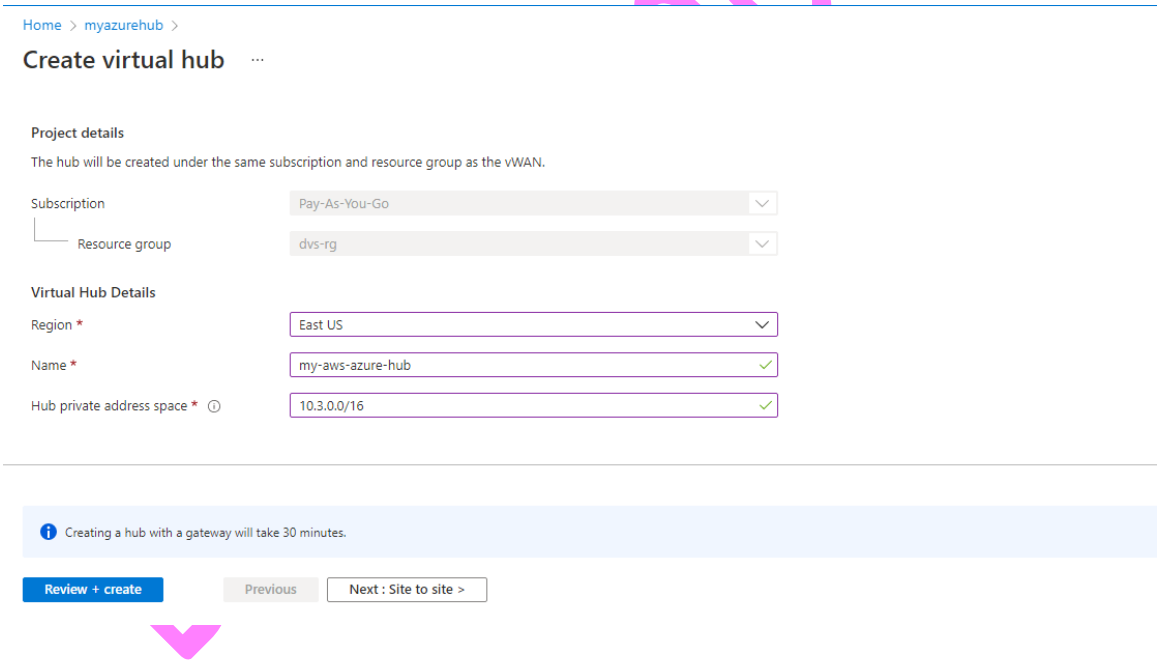
Basics

Subscription	Pay-As-You-Go
Resource group	dvs-rg
Resource group location	East US
Name	myazurehub

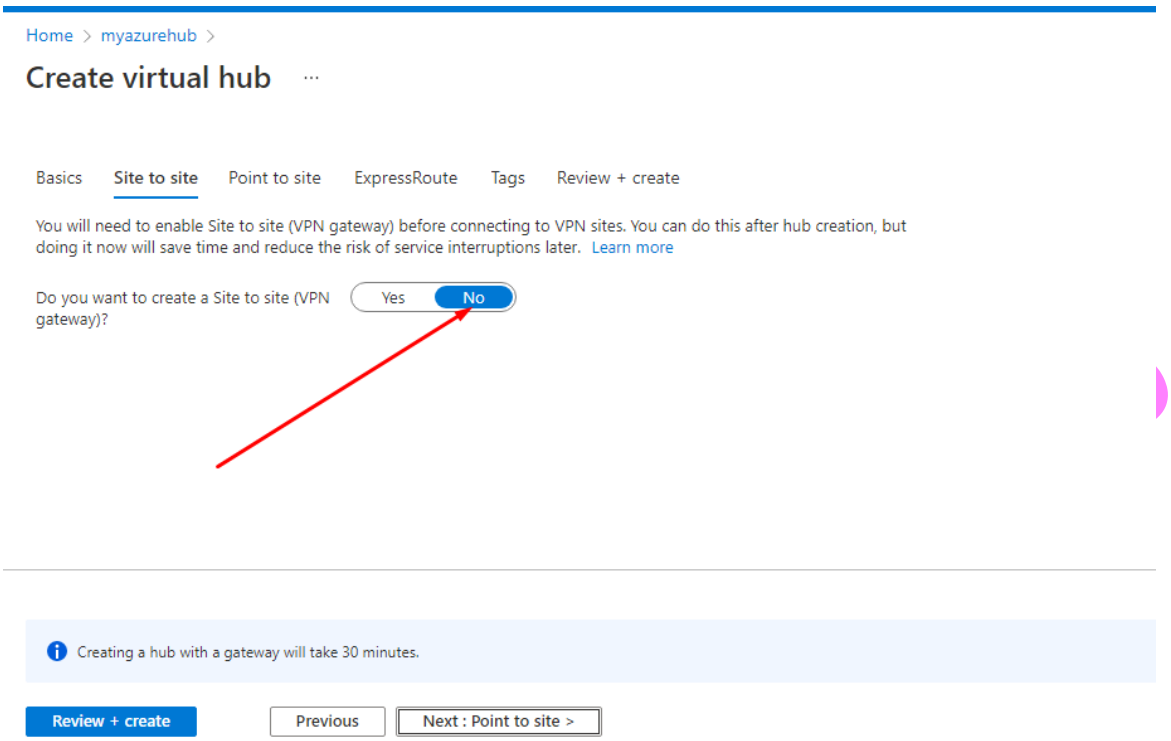
Create | Previous | Next | Download a template for automation

Let's create the hub so that we can expose the network to the users:

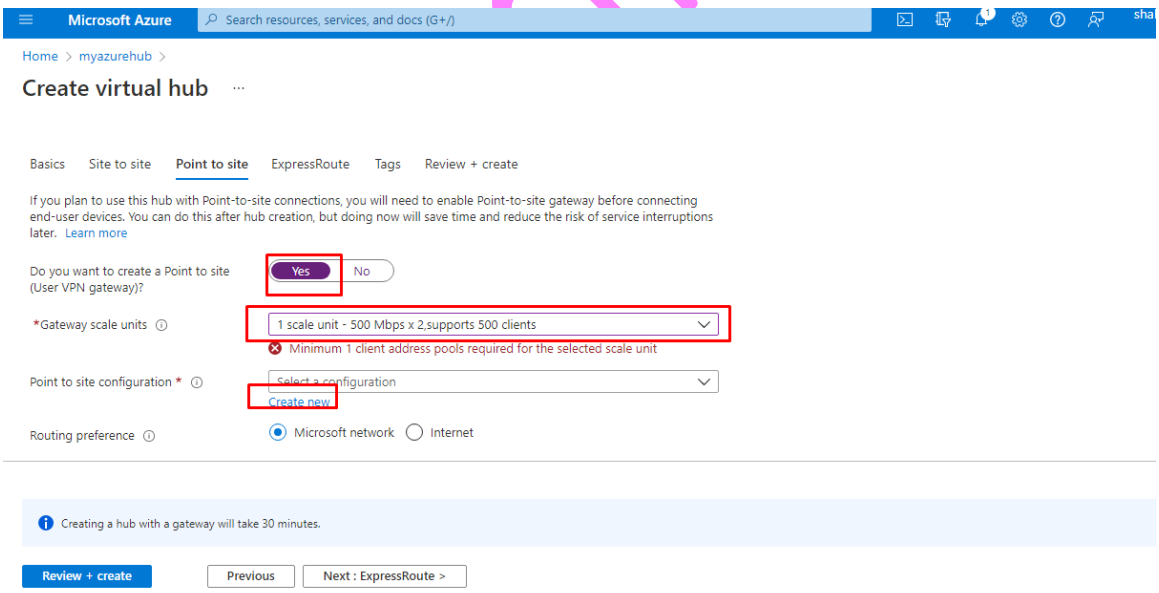


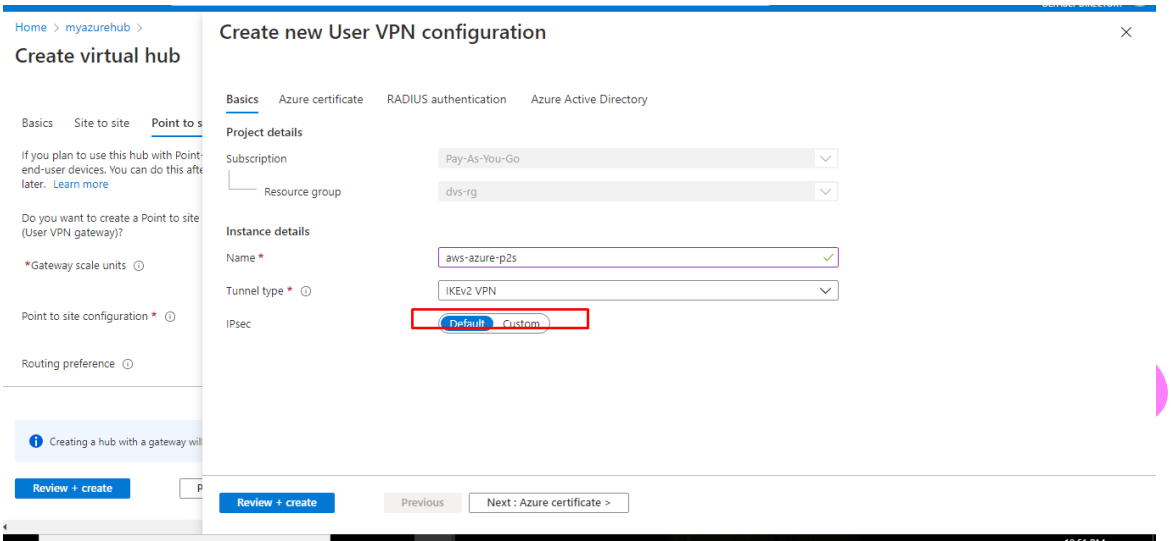


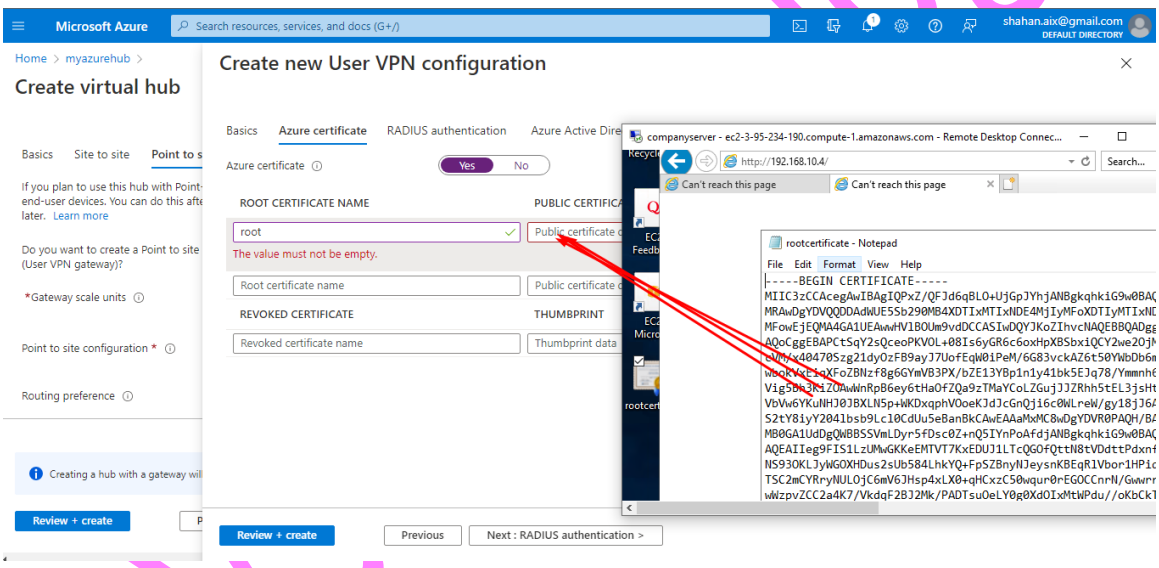
Here Hub private address space is the ip's which will be used by the hub itself during the configuration time.

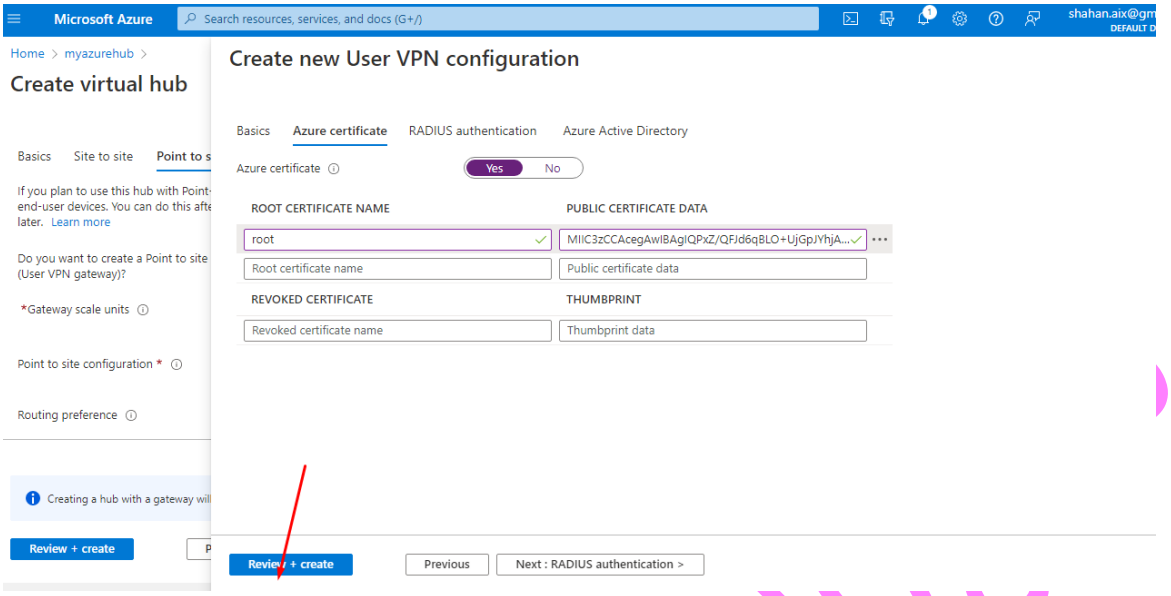


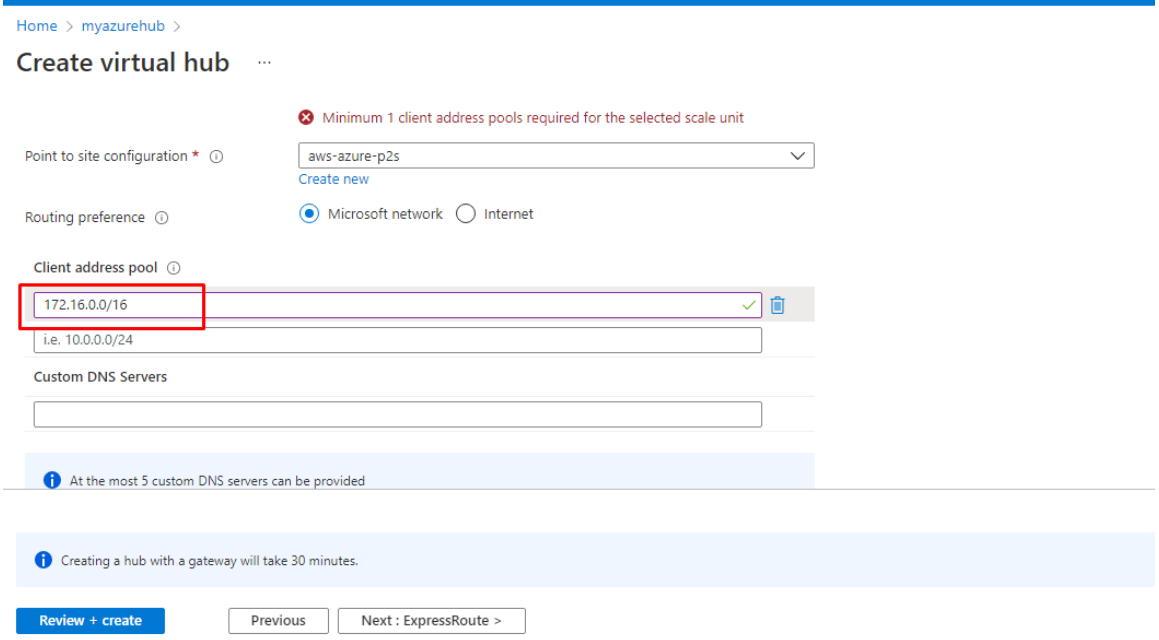
If you have the site-to-site connectivity then you can use this one other wise no



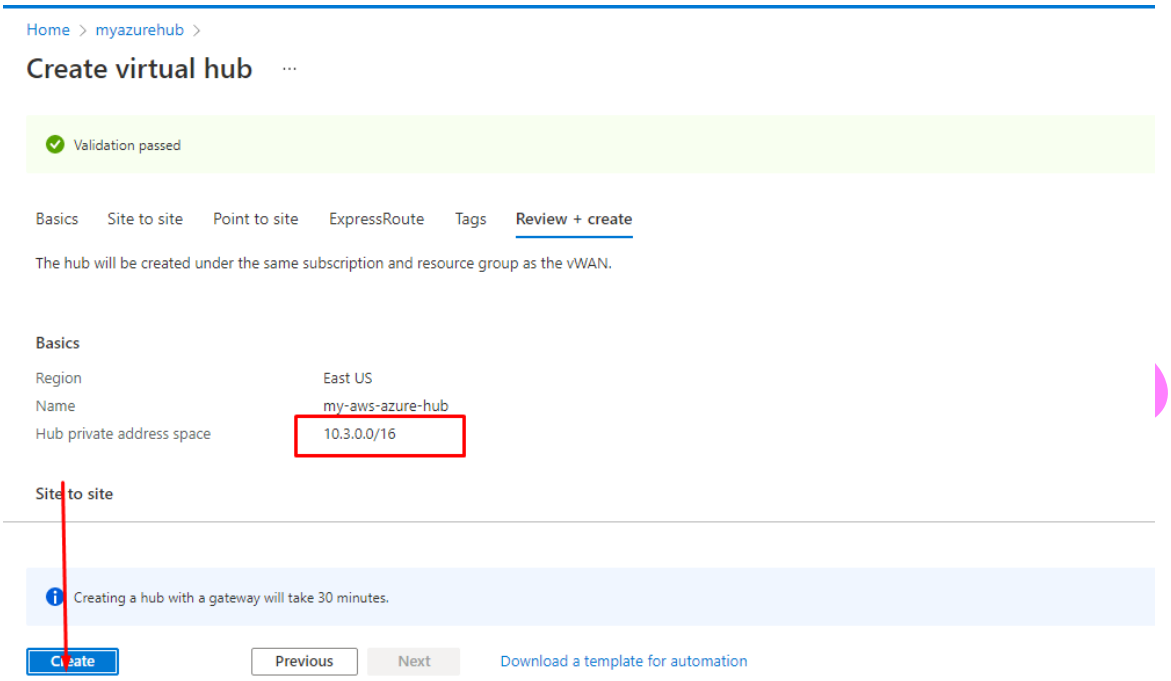

Home > myazurehub >
Create virtual hub
Basics
Site to site
Point to s
If you plan to use this hub with Point-
end-user devices. You can do this afte
later. Learn more
Do you want to create a Point to site
(User VPN gateway)?
*Gateway scale units
Point to site configuration *
Routing preference
Creating a hub with a gateway wil
Review + create
Create new User VPN configuration
Basics
Azure certificate
RADIUS authentication
Azure Active Directory
Project details
Subscription
Pay-As-You-Go
Resource group
dvs-rg
Instance details
Name *
aws-azure-p2s
Tunnel type *
IKEv2 VPN
IPsec
Default
Custom
Review + create
Previous
Next : Azure certificate >


Microsoft Azure
Search resources, services, and docs (G+/)
shahan.aix@gmail.com
DEFAULT DIRECTORY
Home > myazurehub >
Create virtual hub
Basics
Site to site
Point to s
If you plan to use this hub with Point-
end-user devices. You can do this afte
later. Learn more
Do you want to create a Point to site
(User VPN gateway)?
*Gateway scale units
Point to site configuration *
Routing preference
Creating a hub with a gateway wil
Review + create
Create new User VPN configuration
Basics
Azure certificate
RADIUS authentication
Azure Active Dire
Azure certificate
Yes
No
ROOT CERTIFICATE NAME
PUBLIC CERTIFICA
root
The value must not be empty.
Root certificate name
REVOKED CERTIFICATE
THUMBPRINT
Revoked certificate name
Thumbprint data
companyserver - ec2-3-95-234-190.compute-1.amazonaws.com - Remote Desktop Connec...
http://192.168.10.4/
Can't reach this page
Can't reach this page
rootcertificate - Notepad
File
Edit
Format
View
Help
-----BEGIN CERTIFICATE-----
Review + create
Previous
Next : RADIUS authentication >

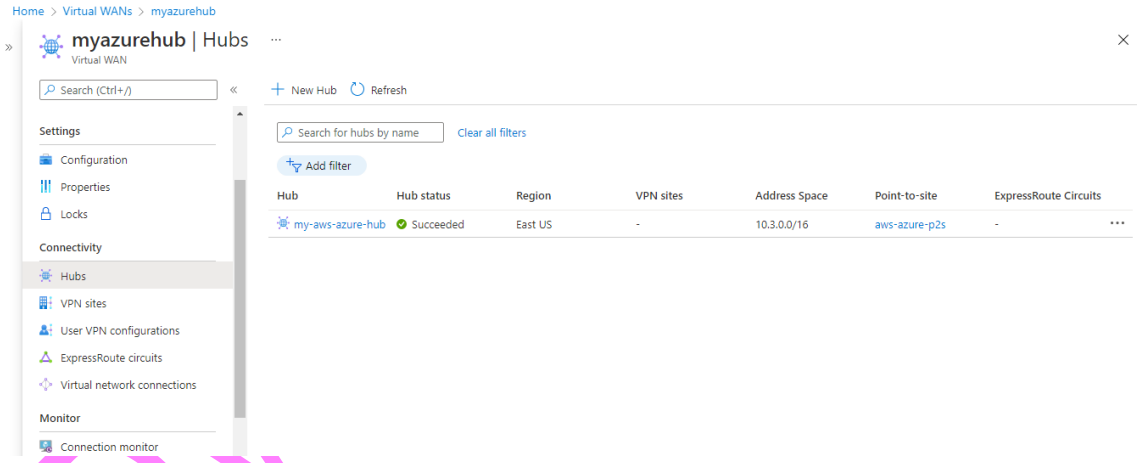




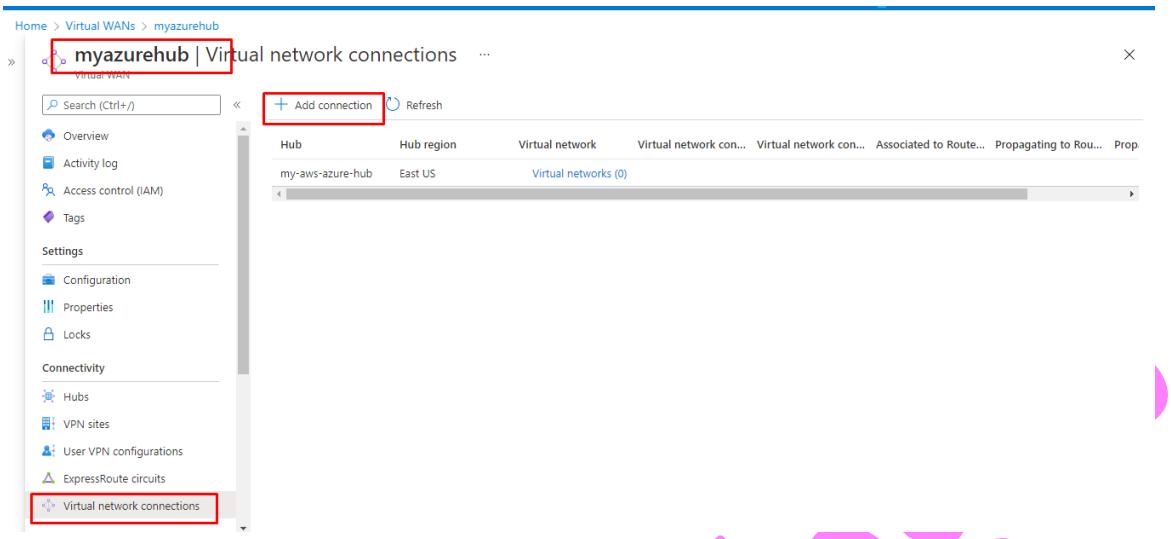
Here 172.16.0.0/16 is the client ip's which will get allocated when a client get connected

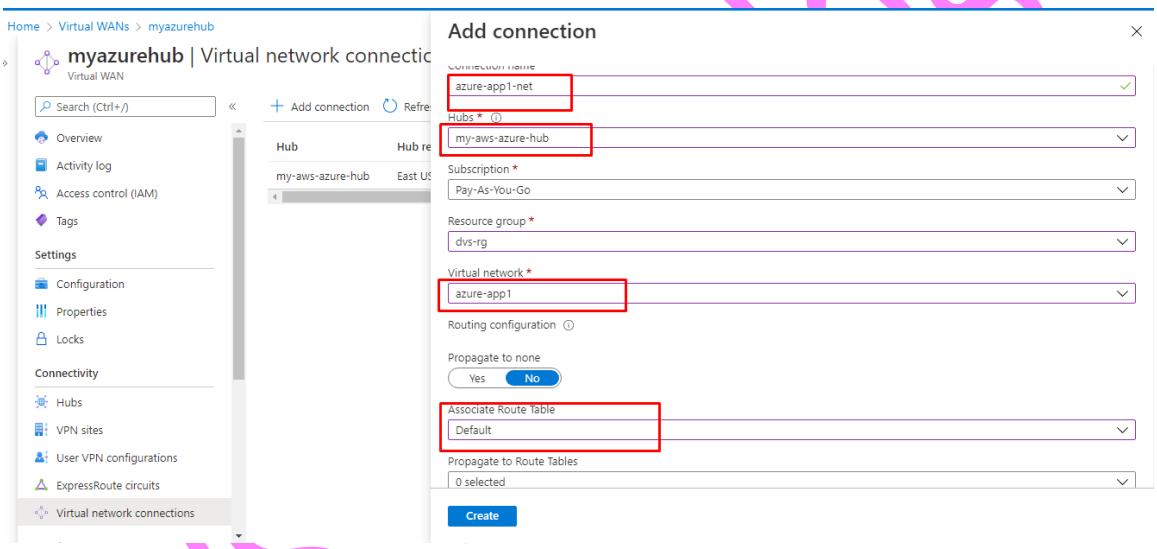


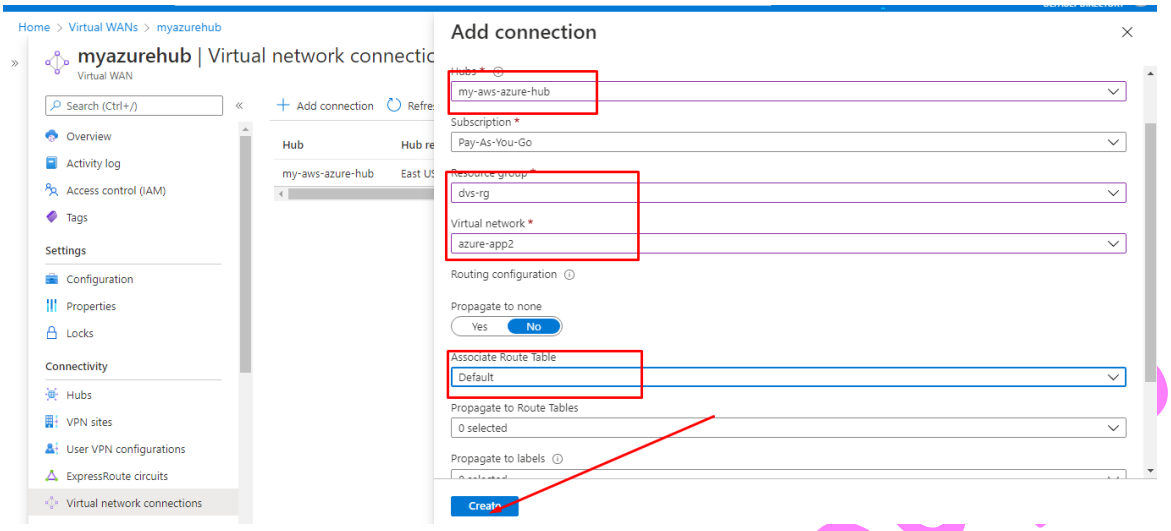
NOTE: It will take 30 minutes for creating the HUB

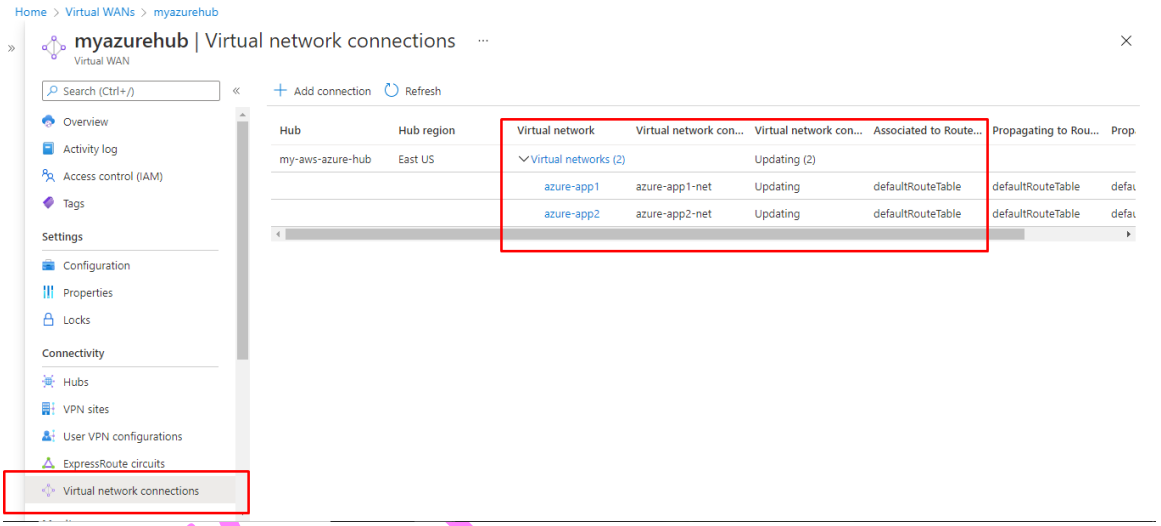


Now let's configure the VNETs to our HUB:

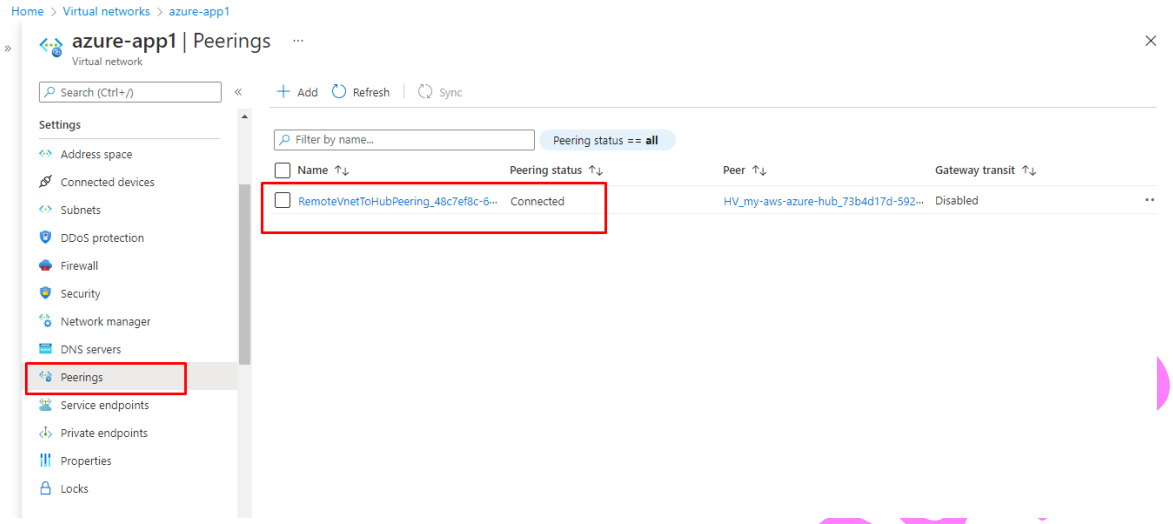

Home > Virtual WANs > myazurehub
myazurehub | Virtual network connections
Virtual WAN
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Settings
Configuration
Properties
Locks
Connectivity
Hubs
VPN sites
User VPN configurations
ExpressRoute circuits
Virtual network connections
Add connection
Refresh
Hub
Hub region
Virtual network
Virtual network con...
Virtual network con...
Associated to Route...
Propagating to Rou...
my-aws-azure-hub
East US
Virtual networks (0)

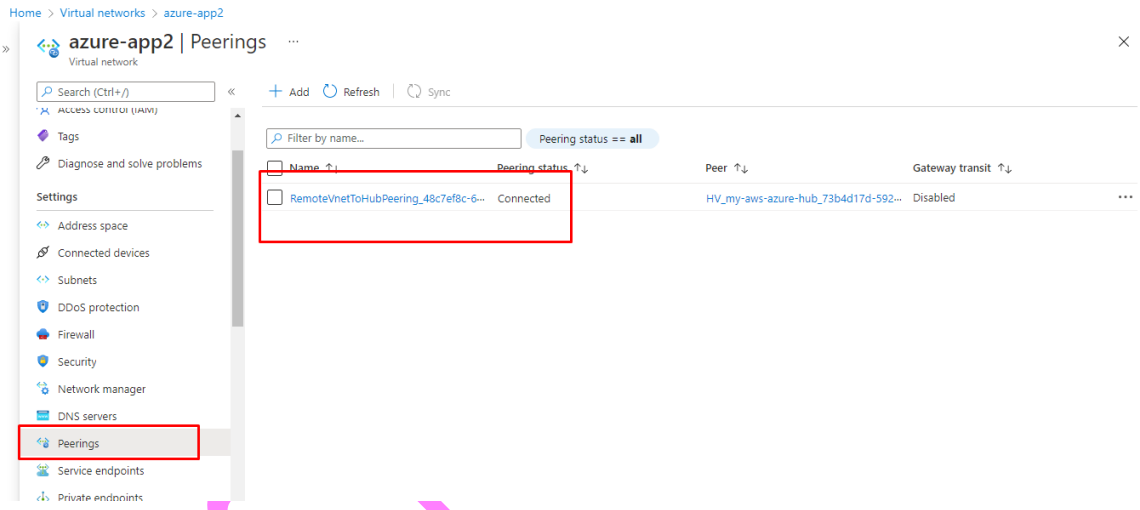

Home > Virtual WANs > myazurehub
myazurehub | Virtual network connectic
Virtual WAN
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Settings
Configuration
Properties
Locks
Connectivity
Hubs
VPN sites
User VPN configurations
ExpressRoute circuits
Virtual network connections
Add connection
Hub
my-aws-azure-hub
Add connection
azure-app1-net
Hubs *
my-aws-azure-hub
Subscription *
Pay-As-You-Go
Resource group *
dvs-rg
Virtual network *
azure-app1
Routing configuration
Propagate to none
Yes
No
Associate Route Table
Default
Propagate to Route Tables
0 selected
Create



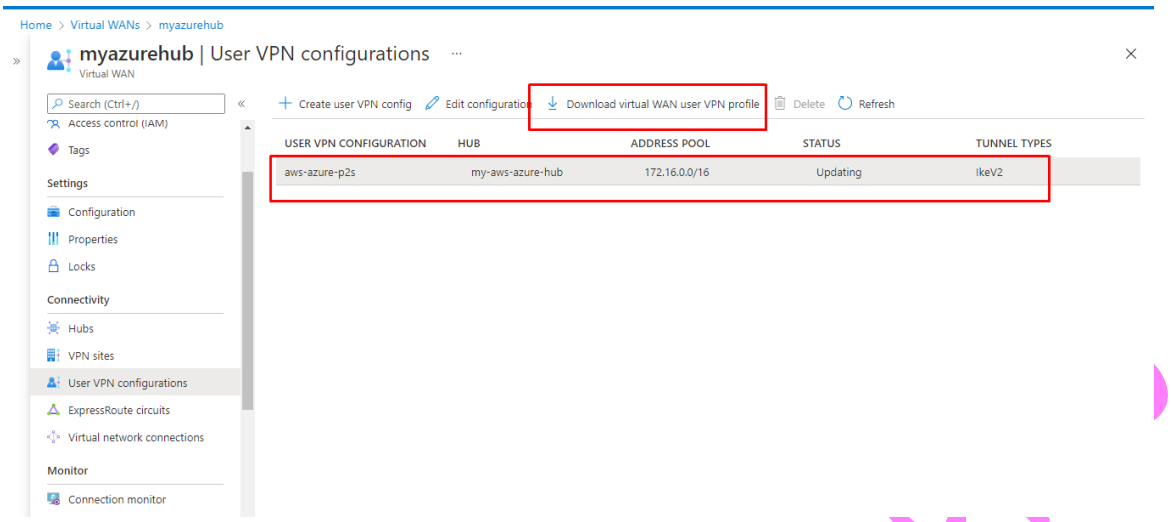


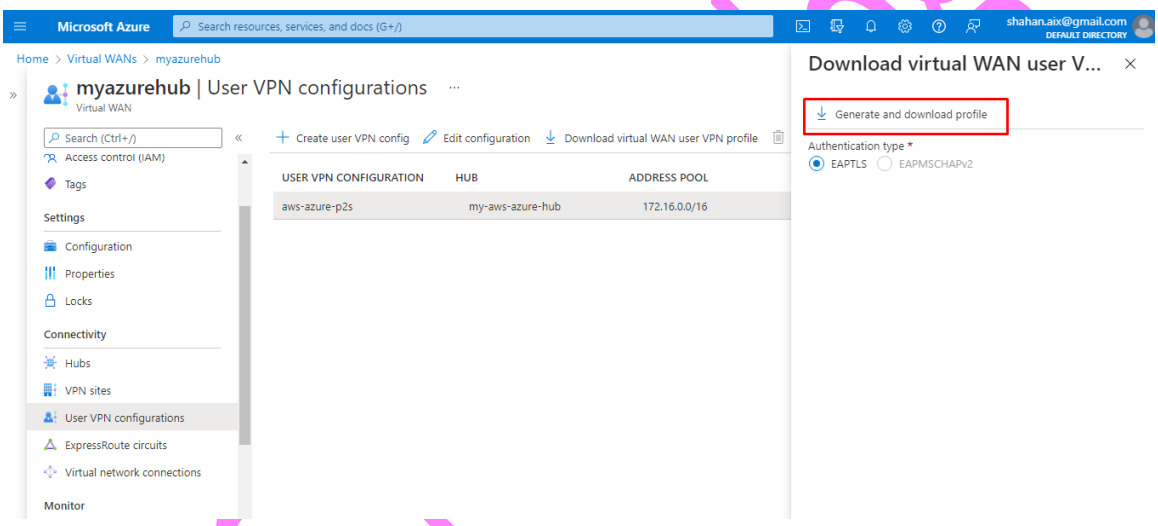
If you observe properly this virtual network connections internally it will create the peering between the VNET's



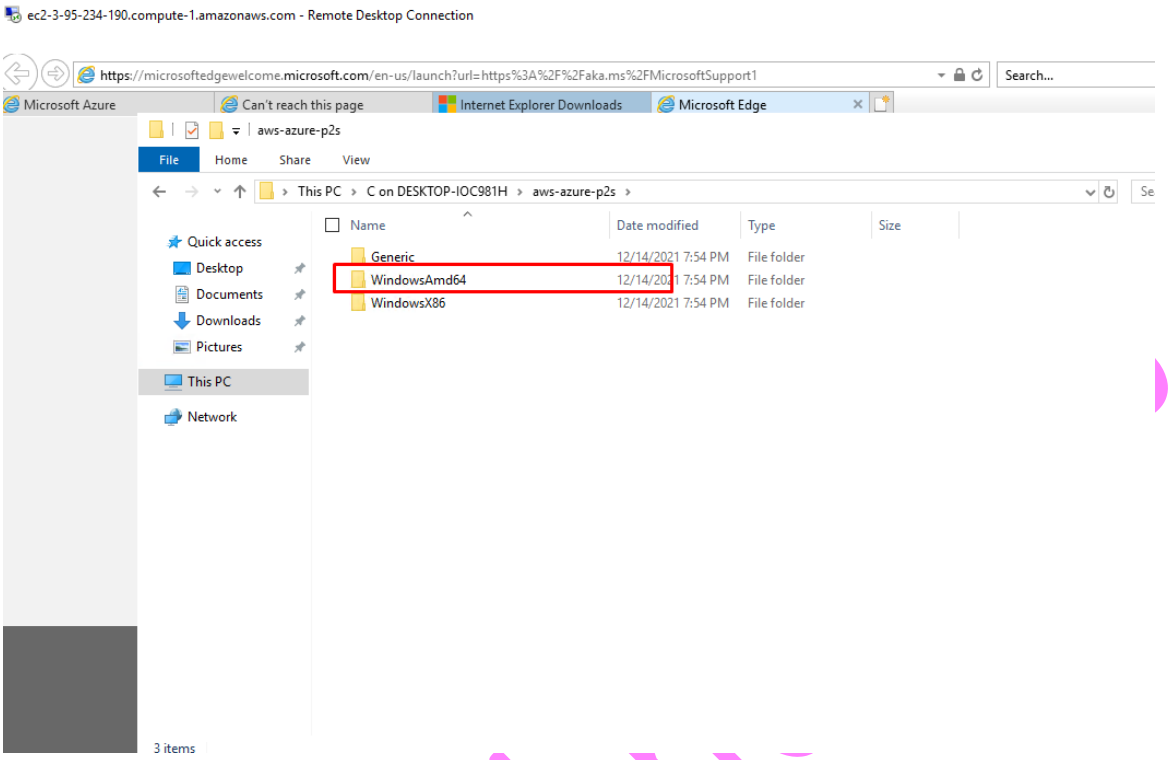


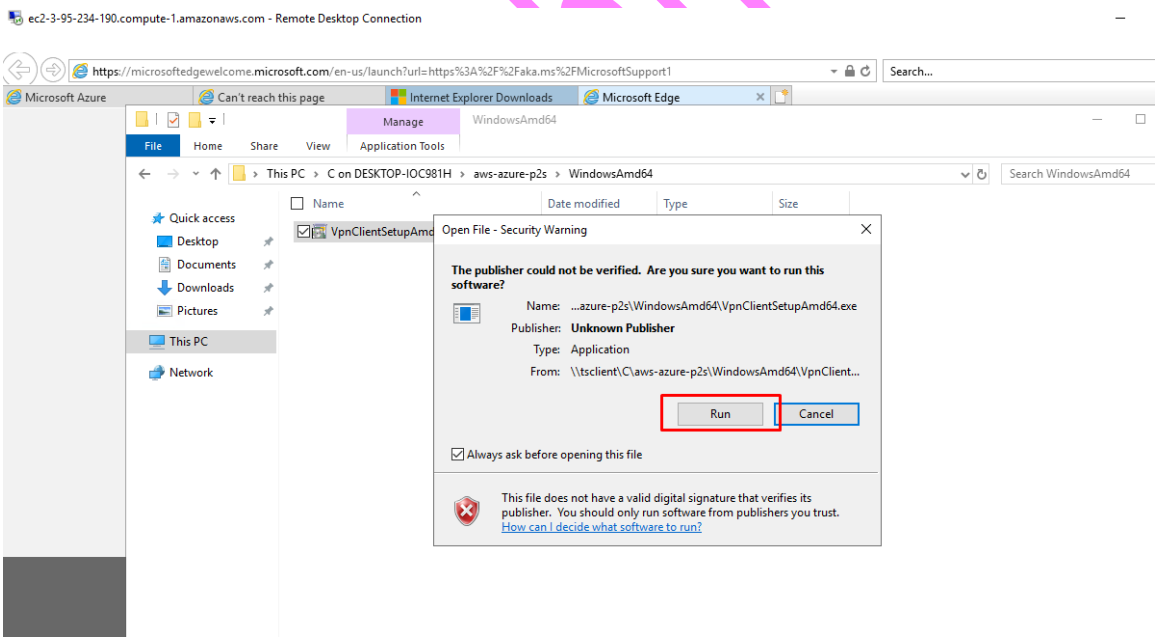
Now let's download the user's vpn file so that we can connect to the network

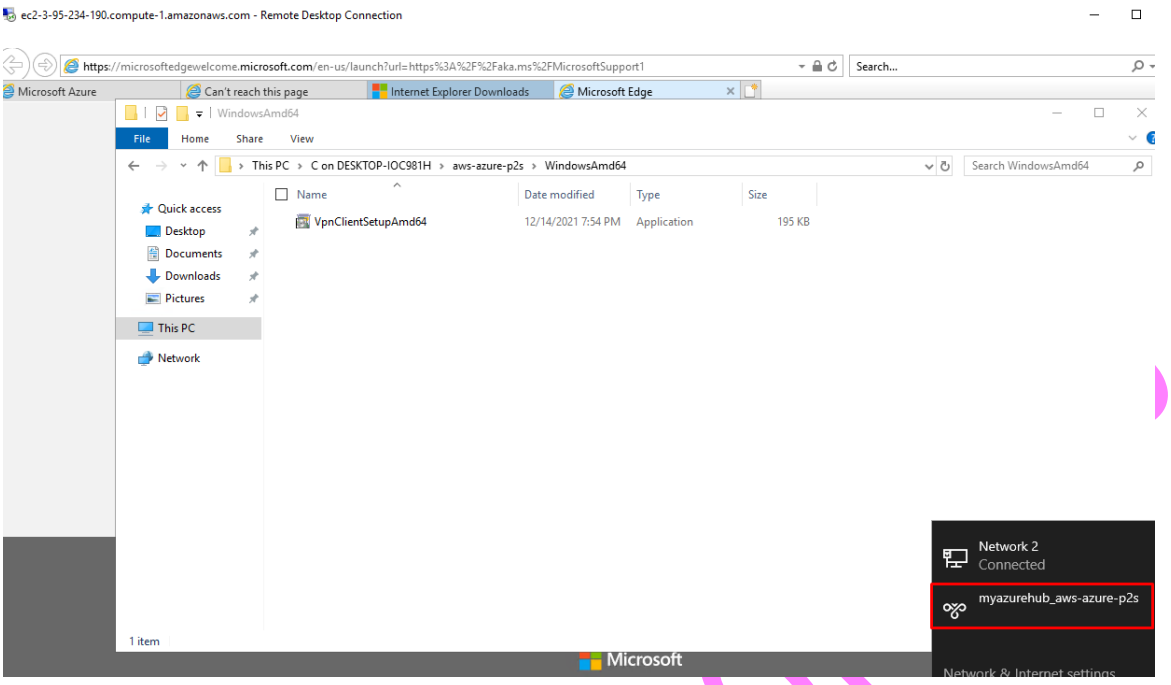

Home > Virtual WANs > myazurehub
myazurehub | User VPN configurations
Virtual WAN
Search (Ctrl+/)
Access control (IAM)
Tags
Settings
Configuration
Properties
Locks
Connectivity
Hubs
VPN sites
User VPN configurations
ExpressRoute circuits
Virtual network connections
Monitor
Connection monitor
Create user VPN config
Edit configuration
Download virtual WAN user VPN profile
Delete
Refresh
USER VPN CONFIGURATION
HUB
ADDRESS POOL
STATUS
TUNNEL TYPES
aws-azure-p2s
my-aws-azure-hub
172.16.0.0/16
Updating
IkeV2

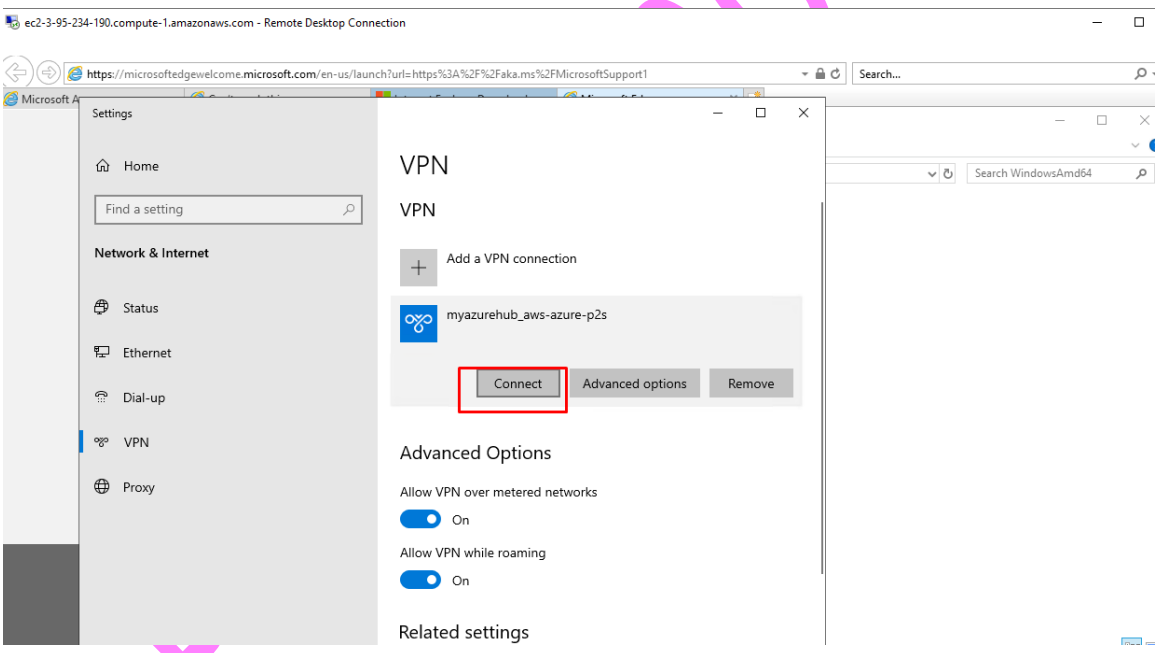

Microsoft Azure
Search resources, services, and docs (G+/)
shahan.aix@gmail.com
DEFAULT DIRECTORY
Home > Virtual WANs > myazurehub
myazurehub | User VPN configurations
Virtual WAN
Search (Ctrl+/)
Access control (IAM)
Tags
Settings
Configuration
Properties
Locks
Connectivity
Hubs
VPN sites
User VPN configurations
ExpressRoute circuits
Virtual network connections
Monitor
Create user VPN config
Edit configuration
Download virtual WAN user VPN profile
USER VPN CONFIGURATION
HUB
ADDRESS POOL
aws-azure-p2s
my-aws-azure-hub
172.16.0.0/16
Download virtual WAN user V...
Generate and download profile
Authentication type *
EAPTLS
EAPMSCHAPv2

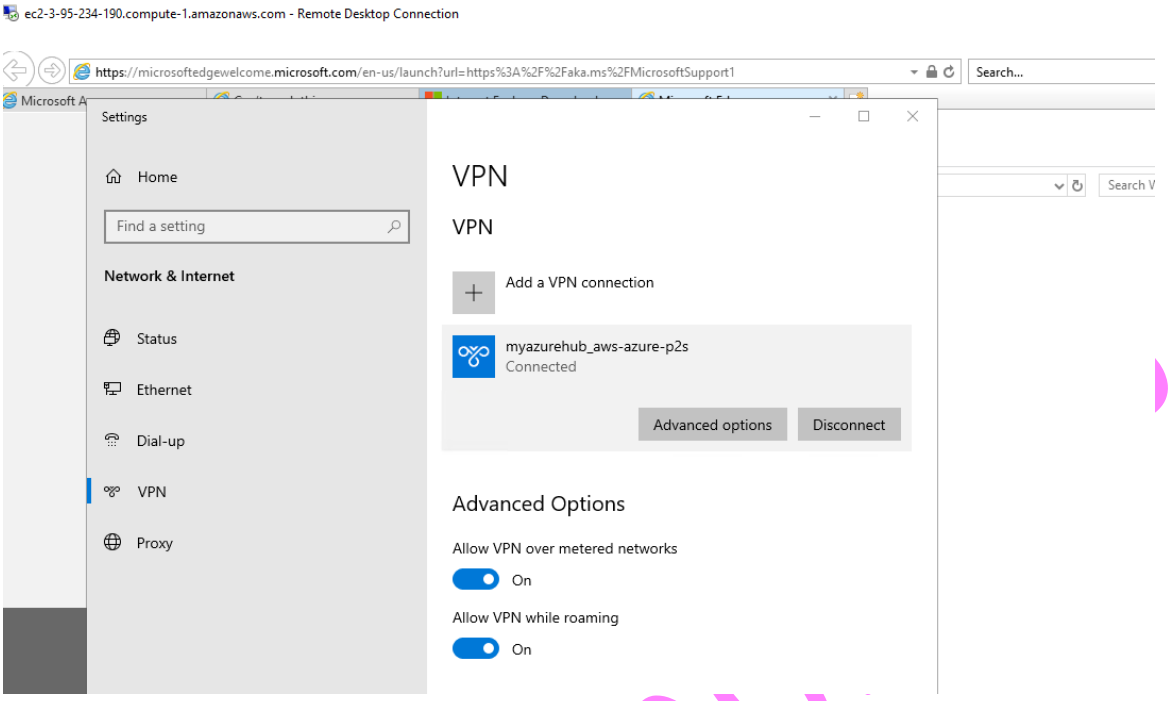
DVS


ec2-3-95-234-190.compute-1.amazonaws.com - Remote Desktop Connection
https://microsoftedgewelcome.microsoft.com/en-us/launch?url=https%3A%2F%2Faka.ms%2FMicrosoftSupport1
Search...
Microsoft Azure
Can't reach this page
Internet Explorer Downloads
Microsoft Edge
aws-azure-p2s
File
Home
Share
View
This PC › C on DESKTOP-IOC981H › aws-azure-p2s ›
Quick access
Desktop
Documents
Downloads
Pictures
This PC
Network
Name
Date modified
Type
Size
Generic
12/14/2021 7:54 PM
File folder
WindowsAmd64
12/14/2021 7:54 PM
File folder
WindowsX86
12/14/2021 7:54 PM
File folder
3 items

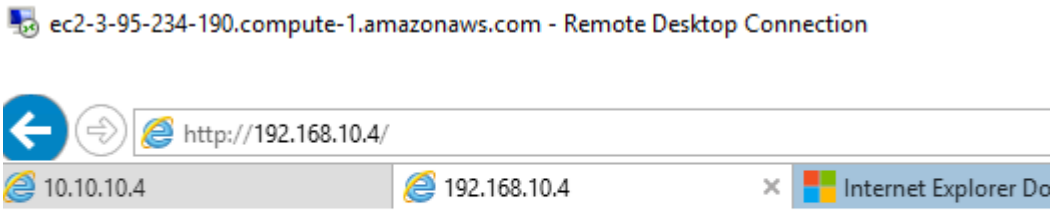

ec2-3-95-234-190.compute-1.amazonaws.com - Remote Desktop Connection
https://microsoftedgewelcome.microsoft.com/en-us/launch?url=https%3A%2F%2Faka.ms%2FMicrosoftSupport1
Search...
Microsoft Azure
Can't reach this page
Internet Explorer Downloads
Microsoft Edge
Manage
WindowsAmd64
File
Home
Share
View
Application Tools
This PC › C on DESKTOP-IOC981H › aws-azure-p2s › WindowsAmd64
Search WindowsAmd64
Quick access
Desktop
Documents
Downloads
Pictures
This PC
Network
Name
Date modified
Type
Size
VpnClientSetupAmd
Open File - Security Warning
The publisher could not be verified. Are you sure you want to run this software?
Name: ...azure-p2s\WindowsAmd64\VpnClientSetupAmd64.exe
Publisher: Unknown Publisher
Type: Application
From: \\tsclient\C\aws-azure-p2s\WindowsAmd64\VpnClient...
Run
Cancel
Always ask before opening this file
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?


ec2-3-95-234-190.compute-1.amazonaws.com - Remote Desktop Connection
https://microsoftedgewelcome.microsoft.com/en-us/launch?url=https%3A%2F%2Faka.ms%2FMicrosoftSupport1
Search...
Microsoft Azure
Can't reach this page
Internet Explorer Downloads
Microsoft Edge
WindowsAmd64
File
Home
Share
View
This PC › C on DESKTOP-IOC981H › aws-azure-p2s › WindowsAmd64
Search WindowsAmd64
Quick access
Desktop
Documents
Downloads
Pictures
This PC
Network
Name
Date modified
Type
Size
VpnClientSetupAmd64
12/14/2021 7:54 PM
Application
195 KB
1 item
Network 2
Connected
myazurehub_aws-azure-p2s
Microsoft

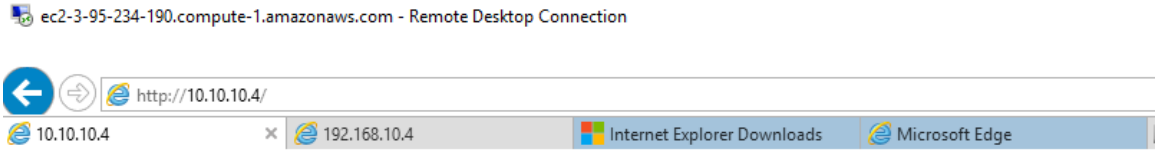

ec2-3-95-234-190.compute-1.amazonaws.com - Remote Desktop Connection
https://microsoftedgewelcome.microsoft.com/en-us/launch?url=https%3A%2F%2Faka.ms%2FMicrosoftSupport1
Search...
Search WindowsAmd64
Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
Proxy
VPN
VPN
Add a VPN connection
myazurehub_aws-azure-p2s
Connect
Advanced options
Remove
Advanced Options
Allow VPN over metered networks
On
Allow VPN while roaming
On
Related settings



Now check the applications of VM1 & VM2 with their private ip's



Hi all I am from server2



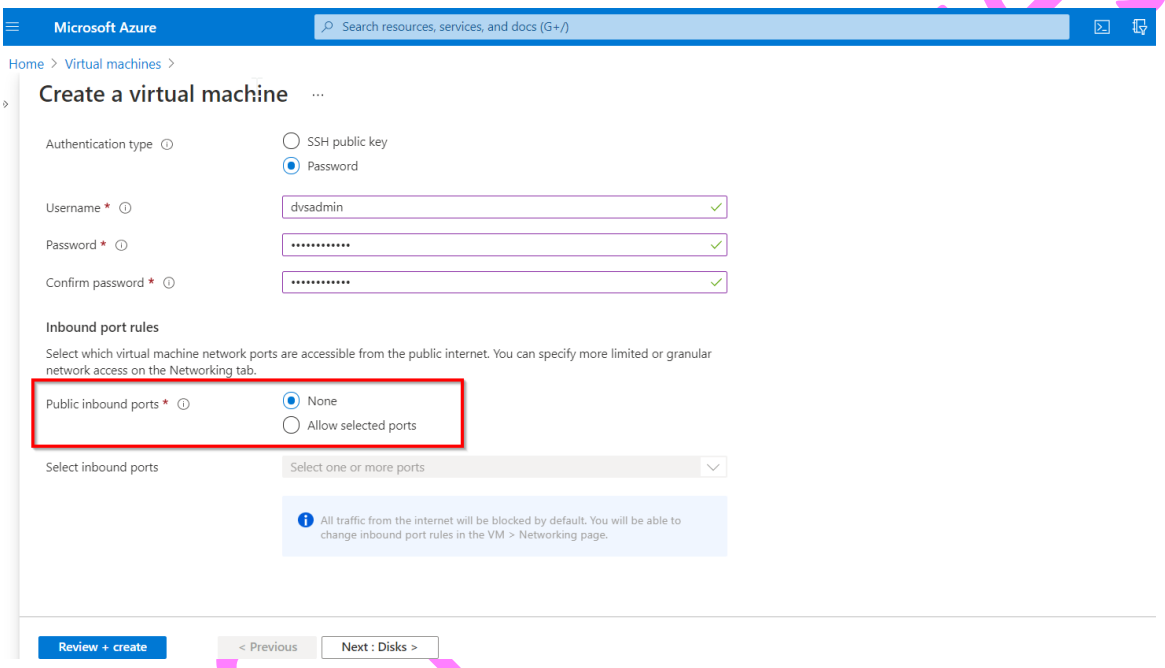
Hi all I am from server1

6 AZ N/W watcher

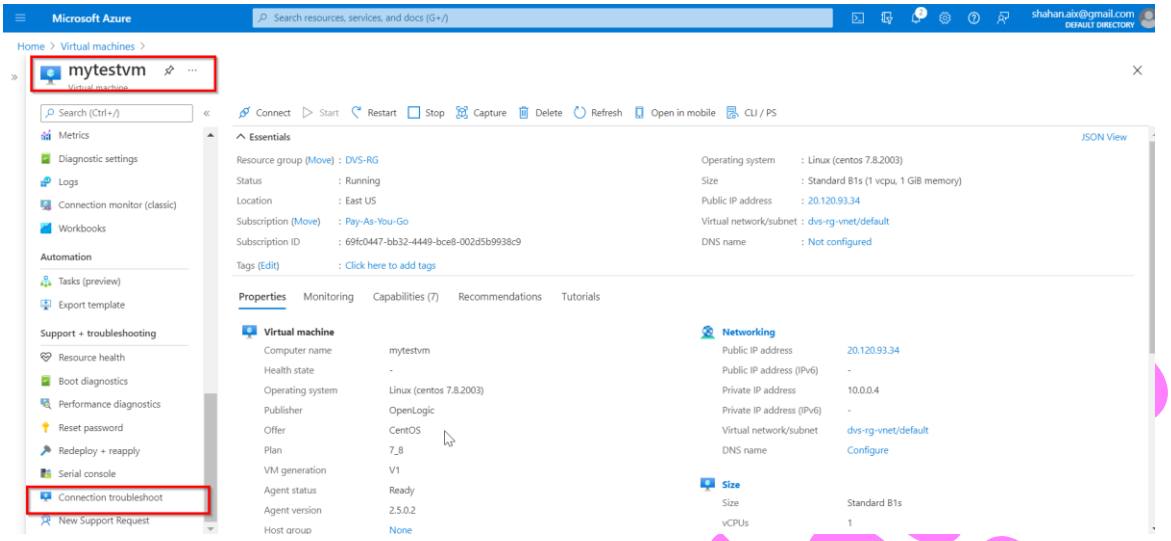
AZ N/W watcher connection troubleshoot

This feature help us to track the connectivity for the servers.
Let's say we have one VM and I want to check if port 22 is allowed or not then I can use this option.

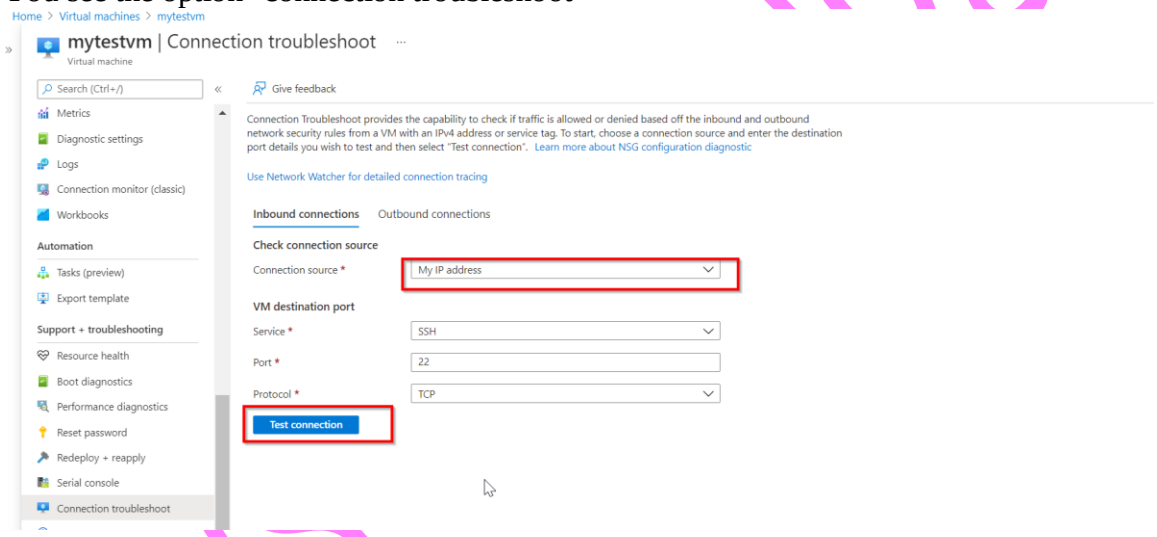
Let's build one VM



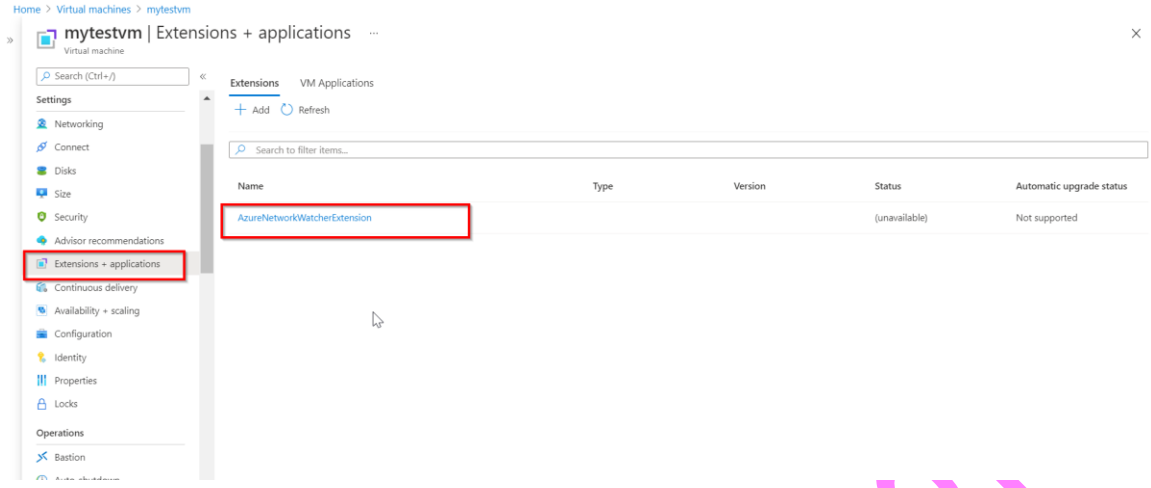
Note: I am not allowing ports for ASG



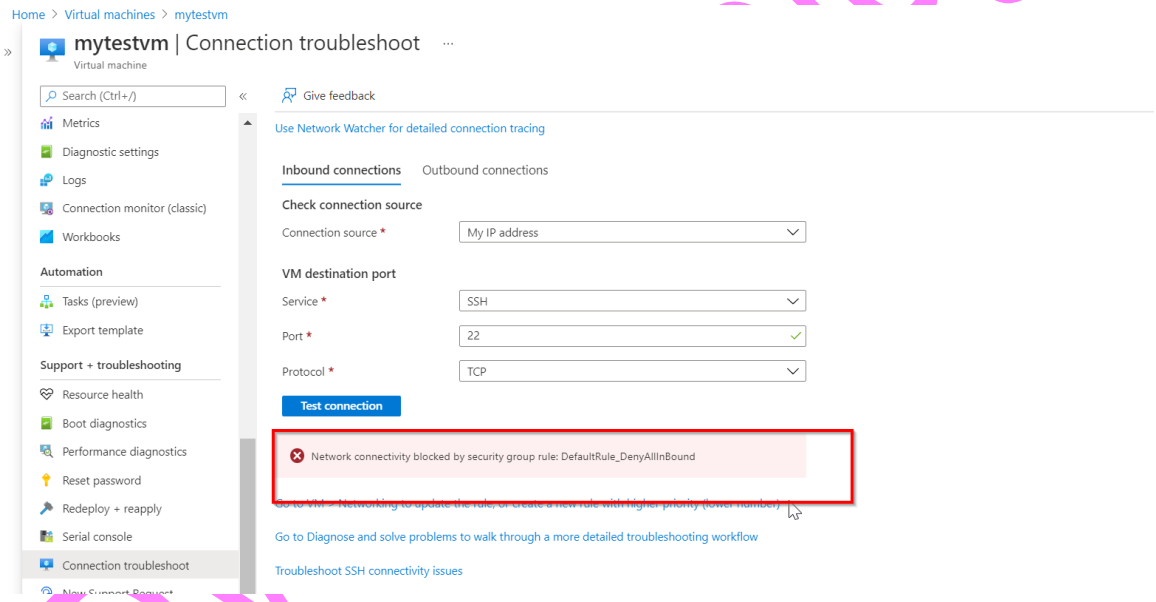
You see the option "connection troubleshoot"



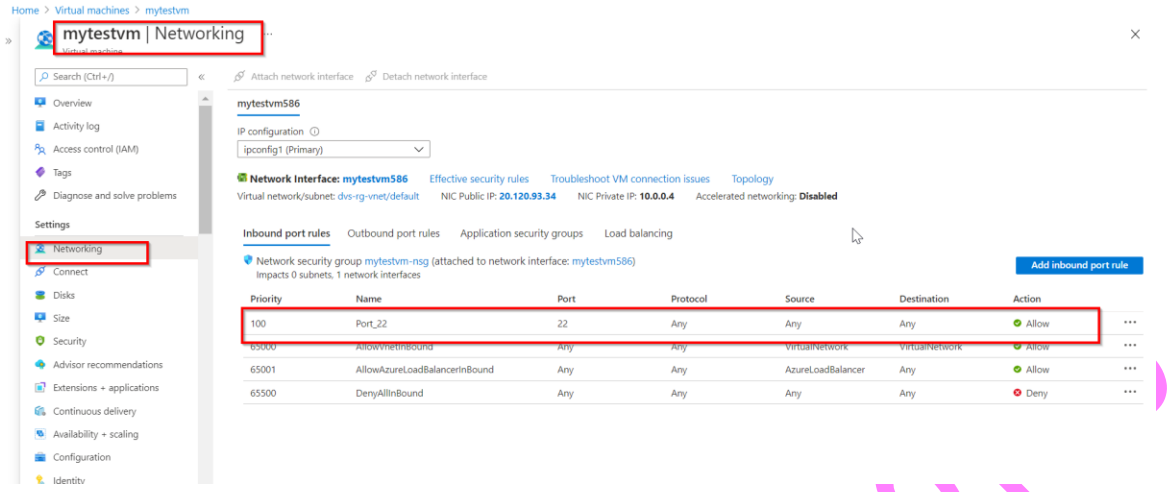
Note: first time when you click on the test connection then it will install the azure agent in the server which collect the connectivity status from the server. Let's say that you are clicking on "Test Connection" then we will see what will happen.



Let's see if we get result or not.

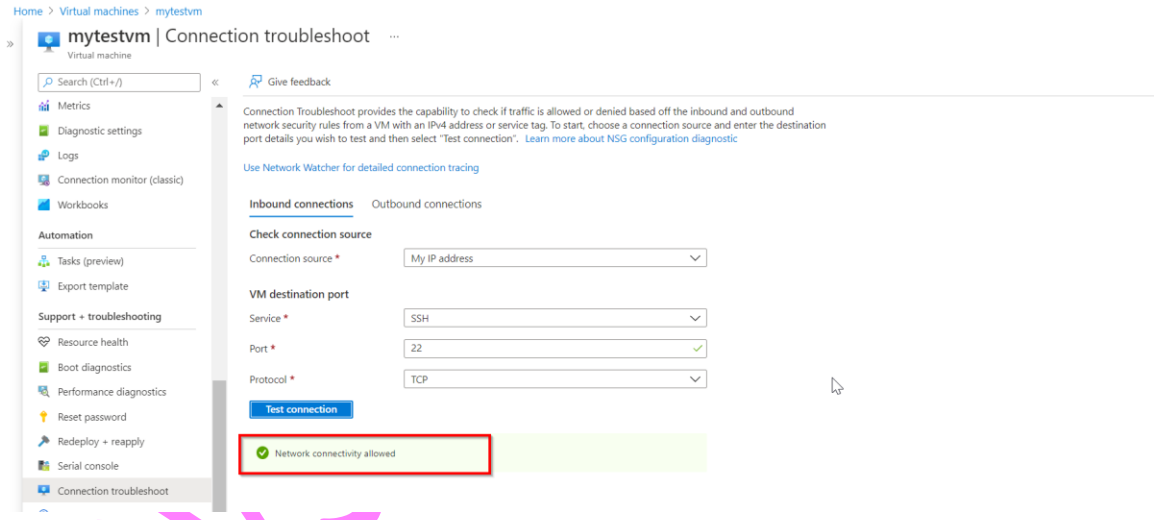


Now let's allow the port 22 and check the connectivity



Let's check the connectivity

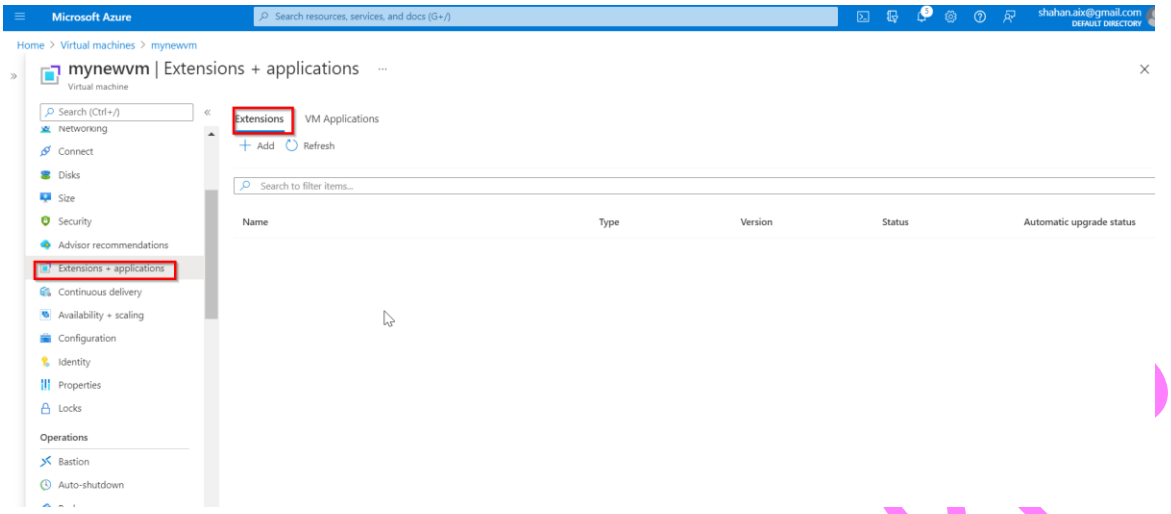
Note: when you try for the second time it will not install the package in the server

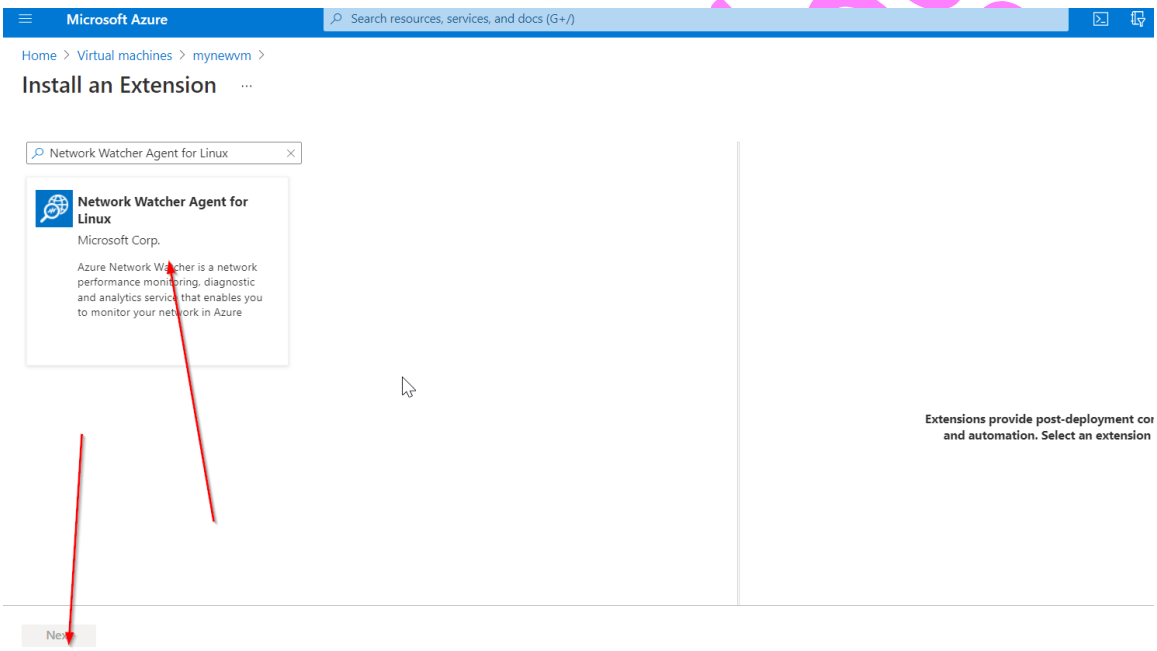


N/W watcher connection monitor:

For understanding this one let's build one more server and try to establish the monitoring from "mytestvm" to "newvm"

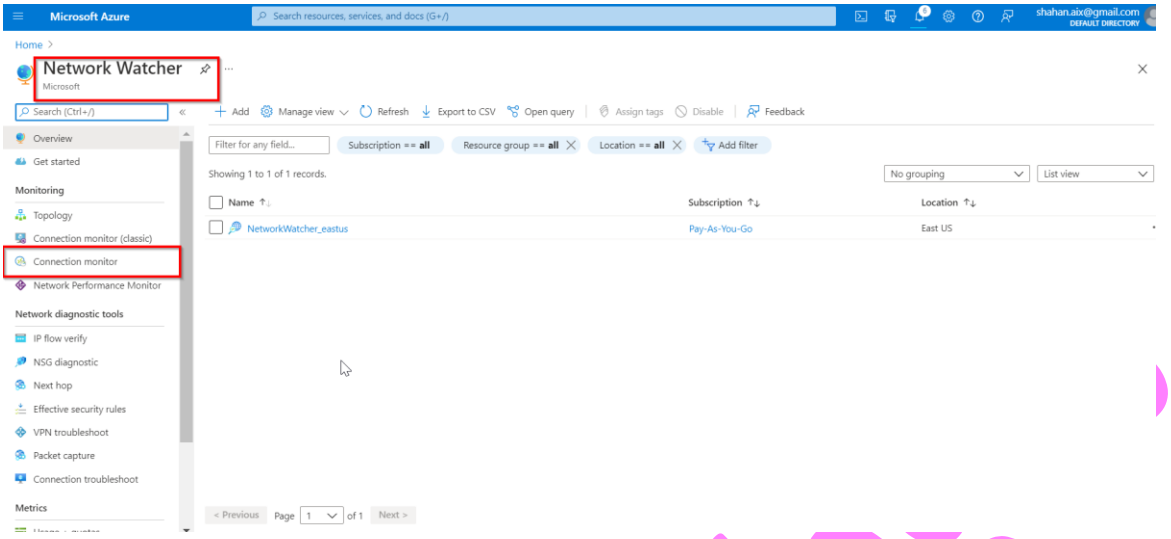
Note: Let's make sure that we are installing the network watcher extension to the "newvm" server.

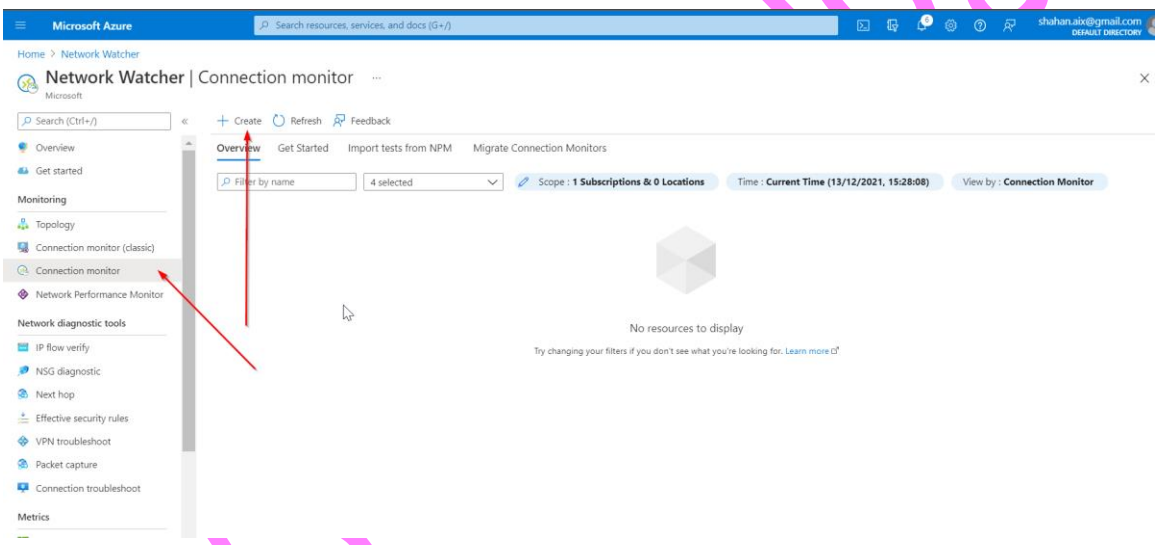




Click on create

Now move to network watcher and create the connection monitoring


Microsoft Azure
Search resources, services, and docs (G+/)
shahan.aix@gmail.com
DEFAULT DIRECTORY
Home >
Network Watcher
Microsoft
Search (Ctrl+/)
Overview
Get started
Monitoring
Topology
Connection monitor (classic)
Connection monitor
Network Performance Monitor
Network diagnostic tools
IP flow verify
NSG diagnostic
Next hop
Effective security rules
VPN troubleshoot
Packet capture
Connection troubleshoot
Metrics
Add
Manage view
Refresh
Export to CSV
Open query
Assign tags
Disable
Feedback
Filter for any field...
Subscription == all
Resource group == all
Location == all
Add filter
Showing 1 to 1 of 1 records.
No grouping
List view
Name
Subscription
Location
NetworkWatcher_eastus
Pay-As-You-Go
East US
< Previous
Page 1 of 1
Next >


Microsoft Azure
Search resources, services, and docs (G+/)
shahan.aix@gmail.com
DEFAULT DIRECTORY
Home > Network Watcher
Network Watcher | Connection monitor
Microsoft
Search (Ctrl+/)
Overview
Get started
Monitoring
Topology
Connection monitor (classic)
Connection monitor
Network Performance Monitor
Network diagnostic tools
IP flow verify
NSG diagnostic
Next hop
Effective security rules
VPN troubleshoot
Packet capture
Connection troubleshoot
Metrics
Create
Refresh
Feedback
Overview
Get Started
Import tests from NPM
Migrate Connection Monitors
Filter by name
4 selected
Scope : 1 Subscriptions & 0 Locations
Time : Current Time (13/12/2021, 15:28:08)
View by : Connection Monitor
No resources to display
Try changing your filters if you don't see what you're looking for. Learn more

Home > Network Watcher >

Create Connection Monitor

Microsoft

Basics | Test groups | Create alert | Review + create

Connection Monitor enables you to monitor connectivity in your Azure and hybrid network. Select your preferred subscription and region from which monitoring will be performed. Use workspace configuration to store monitoring data generated by Connection Monitor tests in Log Analytics workspace. Complete the Basics tab then proceed to Test Groups tab. Learn more

Connection Monitor Name * myappmonitoring

Subscription * Pay-As-You-Go

Don't see a subscription? Open Directory + Subscription settings

Region * East US

Workspace configuration

Use workspace created by connection monitor (default)

Workspace DefaultWorkspace-69fc0447-bb32-4449-bce8-002d5b9938c...
Pay-As-You-Go in eastus (system generated)

Next : Test groups >> | Review + create | Cancel

Home > Network Watcher > Create Connection Monitor >

Add test group details

A Test group lets you define a logical group that will let you validate a set of tests between a source and destination pair using a defined test configuration. start by naming your test group and selecting sources and destination based on which you would like to define test for monitoring your network. Learn more about test groups

Test group name * Enter test group name

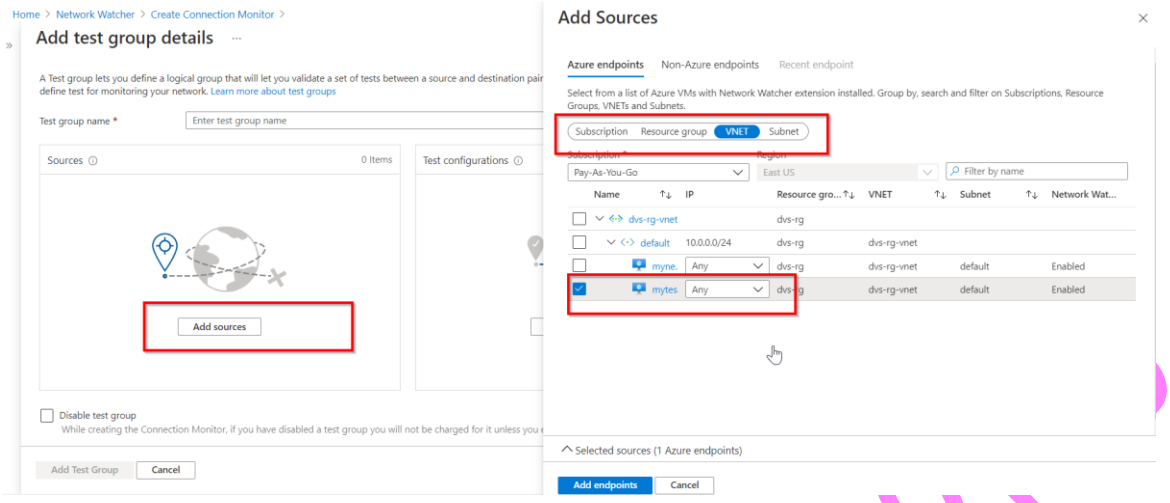
Sources 0 Items — Add sources

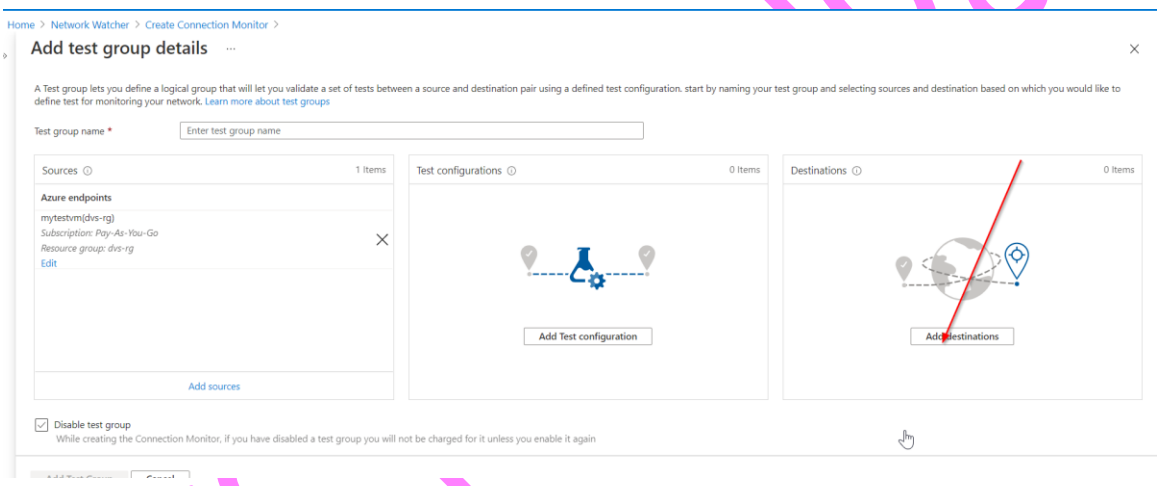
Test configurations 0 Items — Add Test configuration

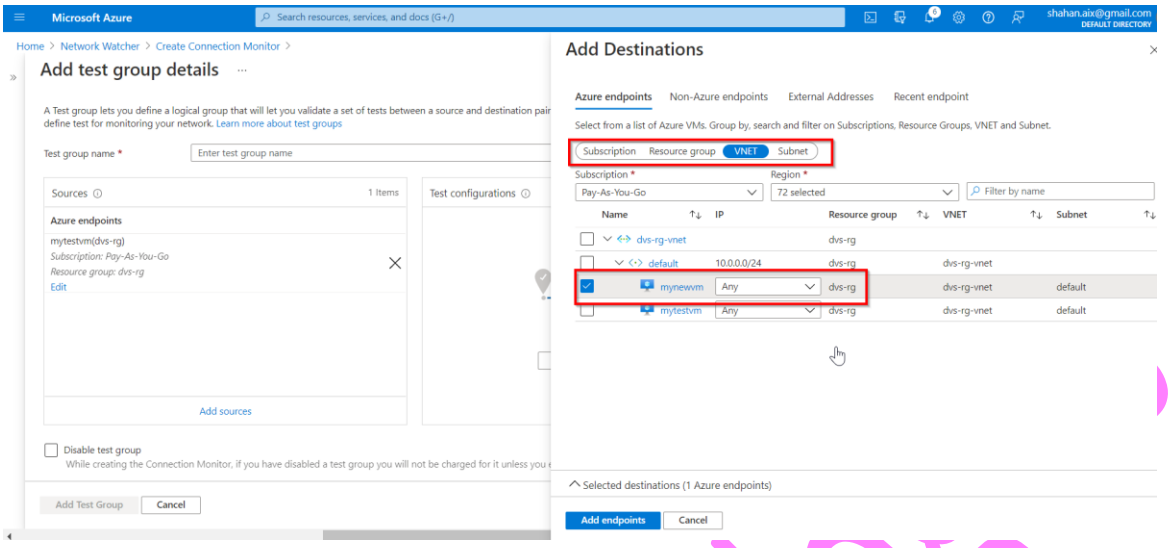
Destinations 0 Items — Add destinations

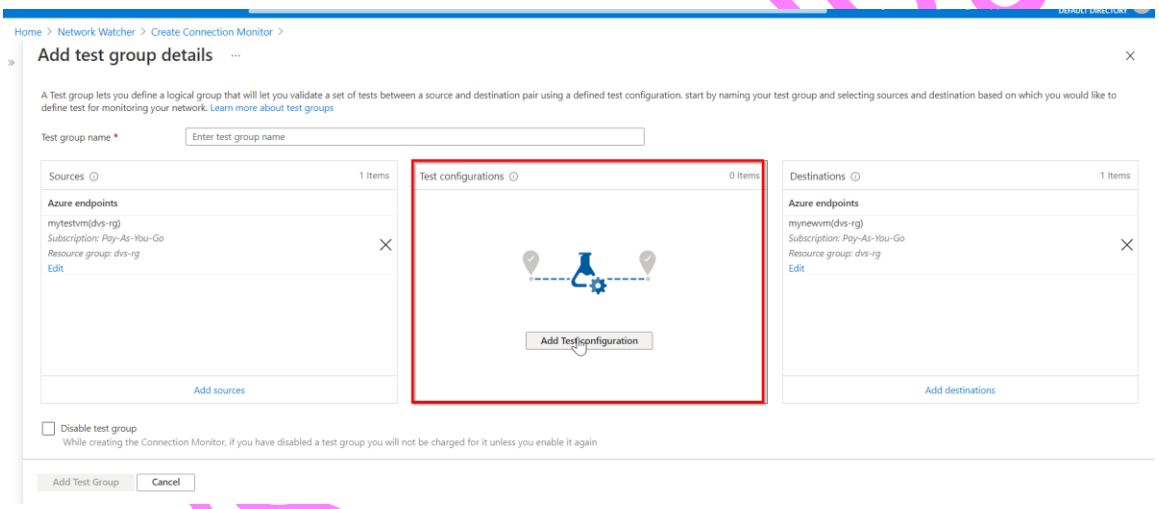
Disable test group
While creating the Connection Monitor, if you have disabled a test group you will not be charged for it unless you enable it again

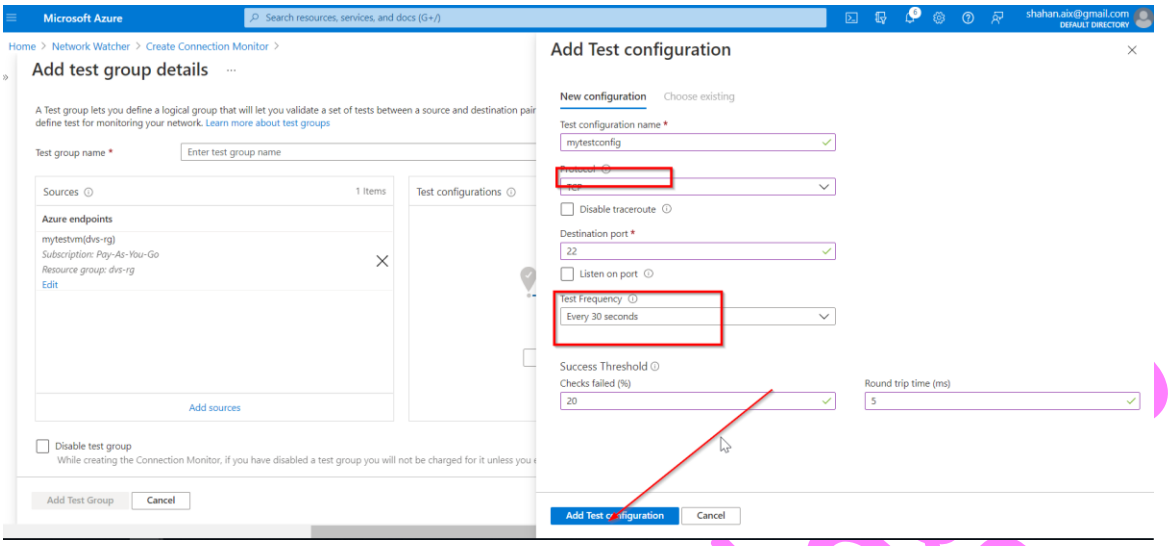
Add Test Group | Cancel

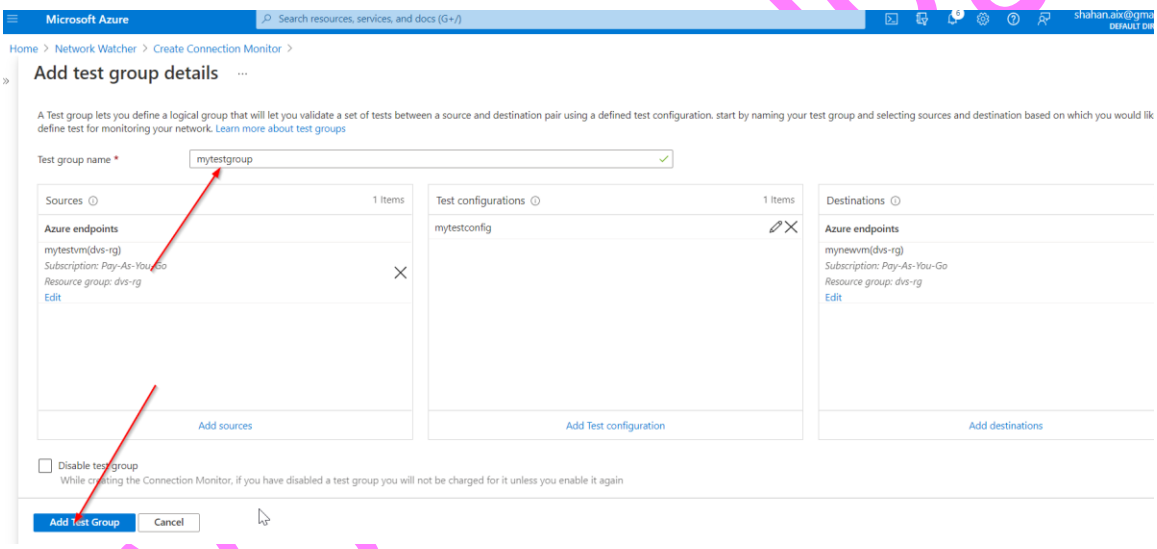

Home > Network Watcher > Create Connection Monitor >
Add test group details
A Test group lets you define a logical group that will let you validate a set of tests between a source and destination pair
define test for monitoring your network. Learn more about test groups
Test group name *
Enter test group name
Sources
0 Items
Test configurations
Add sources
Disable test group
While creating the Connection Monitor, if you have disabled a test group you will not be charged for it unless you
Add Test Group
Cancel
Add Sources
Azure endpoints
Non-Azure endpoints
Recent endpoint
Select from a list of Azure VMs with Network Watcher extension installed. Group by, search and filter on Subscriptions, Resource Groups, VNETs and Subnets.
Subscription
Resource group
VNET
Subnet
Pay-As-You-Go
East US
Filter by name
Name
IP
Resource gro...
VNET
Subnet
Network Wat...
dvs-rg-vnet
dvs-rg
default
10.0.0.0/24
dvs-rg
dvs-rg-vnet
myne.
Any
dvs-rg
dvs-rg-vnet
default
Enabled
mytes
Any
dvs-rg
dvs-rg-vnet
default
Enabled
Selected sources (1 Azure endpoints)
Add endpoints
Cancel


Home > Network Watcher > Create Connection Monitor >
Add test group details
A Test group lets you define a logical group that will let you validate a set of tests between a source and destination pair using a defined test configuration. start by naming your test group and selecting sources and destination based on which you would like to define test for monitoring your network. Learn more about test groups
Test group name *
Enter test group name
Sources
1 Items
Azure endpoints
mytestvm(dvs-rg)
Subscription: Pay-As-You-Go
Resource group: dvs-rg
Edit
Add sources
Test configurations
0 Items
Add Test configuration
Destinations
0 Items
Add destinations
Disable test group
While creating the Connection Monitor, if you have disabled a test group you will not be charged for it unless you enable it again


Microsoft Azure
Search resources, services, and docs (G+/)
shahan.aix@gmail.com
DEFAULT DIRECTORY
Home > Network Watcher > Create Connection Monitor >
Add test group details
A Test group lets you define a logical group that will let you validate a set of tests between a source and destination pair
define test for monitoring your network. Learn more about test groups
Test group name *
Enter test group name
Sources
1 Items
Azure endpoints
mytestvm(dvs-rg)
Subscription: Pay-As-You-Go
Resource group: dvs-rg
Edit
Add sources
Test configurations
Disable test group
While creating the Connection Monitor, if you have disabled a test group you will not be charged for it unless you
Add Test Group
Cancel
Add Destinations
Azure endpoints
Non-Azure endpoints
External Addresses
Recent endpoint
Select from a list of Azure VMs. Group by, search and filter on Subscriptions, Resource Groups, VNET and Subnet.
Subscription
Resource group
VNET
Subnet
Subscription *
Pay-As-You-Go
Region *
72 selected
Filter by name
Name
IP
Resource group
VNET
Subnet
dvs-rg-vnet
dvs-rg
default
10.0.0.0/24
dvs-rg
dvs-rg-vnet
mynewvm
Any
dvs-rg
dvs-rg-vnet
default
mytestvm
Any
dvs-rg
dvs-rg-vnet
default
Selected destinations (1 Azure endpoints)
Add endpoints
Cancel


Home > Network Watcher > Create Connection Monitor >
Add test group details
A Test group lets you define a logical group that will let you validate a set of tests between a source and destination pair using a defined test configuration. start by naming your test group and selecting sources and destination based on which you would like to define test for monitoring your network. Learn more about test groups
Test group name *
Enter test group name
Sources
1 Items
Azure endpoints
mytestvm(dvs-rg)
Subscription: Pay-As-You-Go
Resource group: dvs-rg
Edit
Add sources
Test configurations
0 Items
Add Test configuration
Destinations
1 Items
Azure endpoints
mynewvm(dvs-rg)
Subscription: Pay-As-You-Go
Resource group: dvs-rg
Edit
Add destinations
Disable test group
While creating the Connection Monitor, if you have disabled a test group you will not be charged for it unless you enable it again
Add Test Group
Cancel


Microsoft Azure
Search resources, services, and docs (G+/)
shahan.aix@gmail.com
DEFAULT DIRECTORY
Home > Network Watcher > Create Connection Monitor >
Add test group details
A Test group lets you define a logical group that will let you validate a set of tests between a source and destination pair
define test for monitoring your network. Learn more about test groups
Test group name *
Enter test group name
Sources
1 Items
Azure endpoints
mytestvm(dvs-rg)
Subscription: Pay-As-You-Go
Resource group: dvs-rg
Edit
Add sources
Test configurations
Disable test group
While creating the Connection Monitor, if you have disabled a test group you will not be charged for it unless you
Add Test Group
Cancel
Add Test configuration
New configuration
Choose existing
Test configuration name *
mytestconfig
Protocol
TCP
Disable traceroute
Destination port *
22
Listen on port
Test Frequency
Every 30 seconds
Success Threshold
Checks failed (%)
20
Round trip time (ms)
5
Add Test configuration
Cancel


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Network Watcher > Create Connection Monitor >
Add test group details
A Test group lets you define a logical group that will let you validate a set of tests between a source and destination pair using a defined test configuration. start by naming your test group and selecting sources and destination based on which you would lik
define test for monitoring your network. Learn more about test groups
Test group name *
mytestgroup
Sources
1 Items
Azure endpoints
mytestvm(dvs-rg)
Subscription: Pay-As-You-Go
Resource group: dvs-rg
Edit
Add sources
Test configurations
1 Items
mytestconfig
Add Test configuration
Destinations
Azure endpoints
mynewvm(dvs-rg)
Subscription: Pay-As-You-Go
Resource group: dvs-rg
Edit
Add destinations
Disable test group
While creating the Connection Monitor, if you have disabled a test group you will not be charged for it unless you enable it again
Add Test Group
Cancel

Home > Network Watcher >

Create Connection Monitor

Microsoft

Basics | Test groups | Create alert | Review + create

Each test group in Connection Monitor defines a number of sources, destinations and test configurations. All sources and destinations added to a test group with test configuration specified get broken down to individual tests. Tests
Connection Monitor. Individual tests will produce their own results, including checks failure rate and round-trip time.

Add Test Group

Name	Sources	Destination	Test Configurations	Status
mytestgroup	mytestvm(dvs-rg)	mynewvm(dvs-rg)	mytestconfig	Enabled

<< Previous | Next : Create alert >> | Review + create | Cancel

Microsoft Azure | Search resources, services, and docs (G+/) | shahan.aix@gmai DEFAULT DIR

Home > Network Watcher >

Create Connection Monitor

Microsoft

Basics | Test groups | Create alert | Review + create

This Connection Monitor's estimated monthly cost is $0 Learn more

This is not your bill. This is an estimated monthly rate for the currently configured criteria. The estimated rate does not take into account any of the discounts you may be eligible for. Currently, you will not be charged for creating Connection Monitors. Hence cur
cost/month will show $0. Once pricing is in effect, you will be charged based on published pricing Learn more. Test group wise cost is shown in the estimated cost/month column, which may not include free tests. Connection Monitor cost is shown at the end anc
includes free tests if applicable.

Primary details

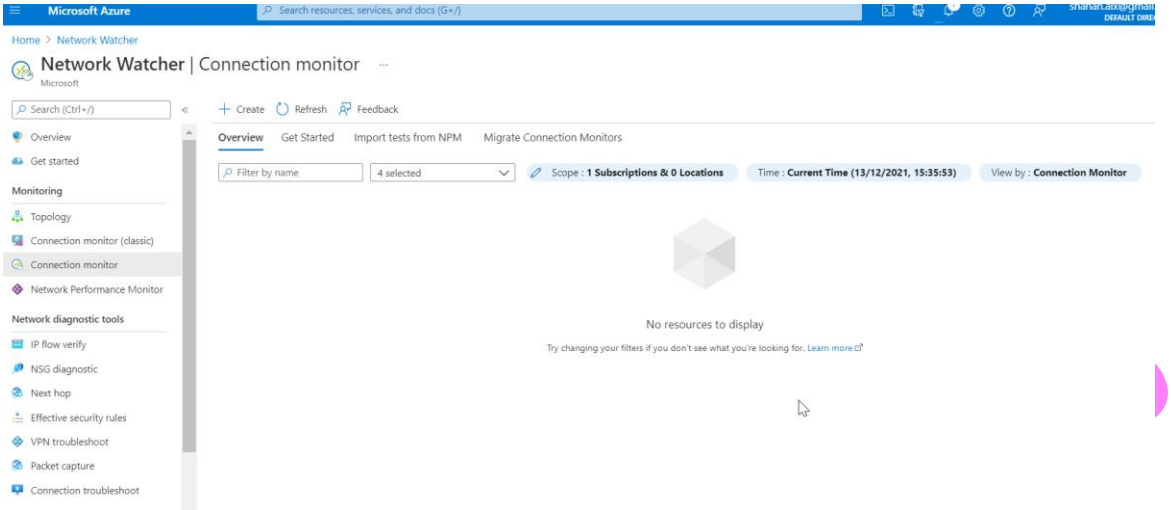
Essentials

Connection Monitor Name : myappmonitoring
Subscription : Pay-As-You-Go
Region : East US
Status : Enabled
Workspace : DefaultWorkspace-69fc0447-bb32-4449-bce8-002d5b9938c9-EUS

Test groups (1)

Name	Sources	Destination	Test Configurations	Current Cost/Month	Estimated Cost/Month	Status
mytestgroup	mytestvm(dvs-rg)	mynewvm(dvs-rg)	mytestconfig	$0.00	$0.30	Enabled

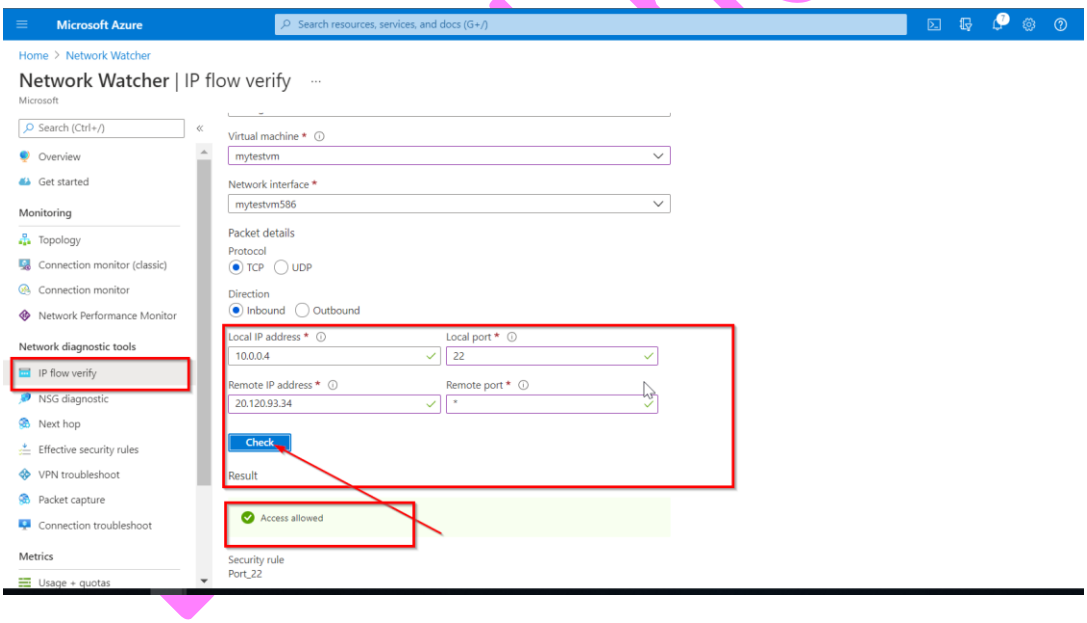
<< Previous | Create | Cancel | Download template

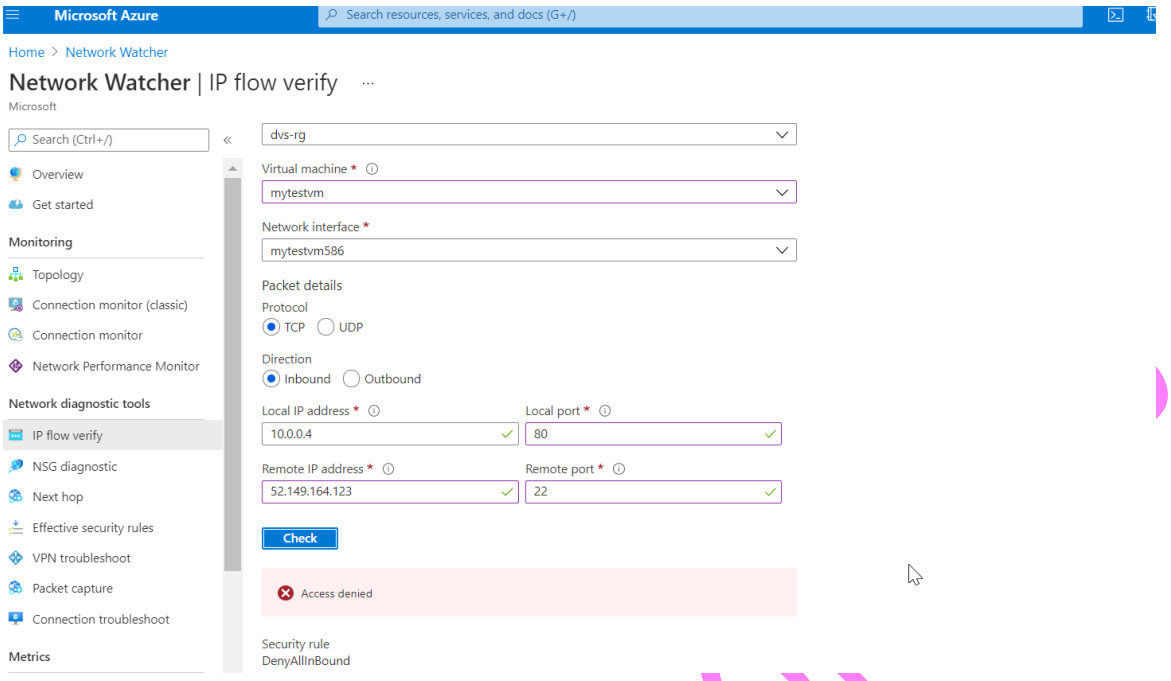


As of now no data, just wait for some more time to see some logs for the ssh login between servers.

N/W watcher - IP Flow verify:

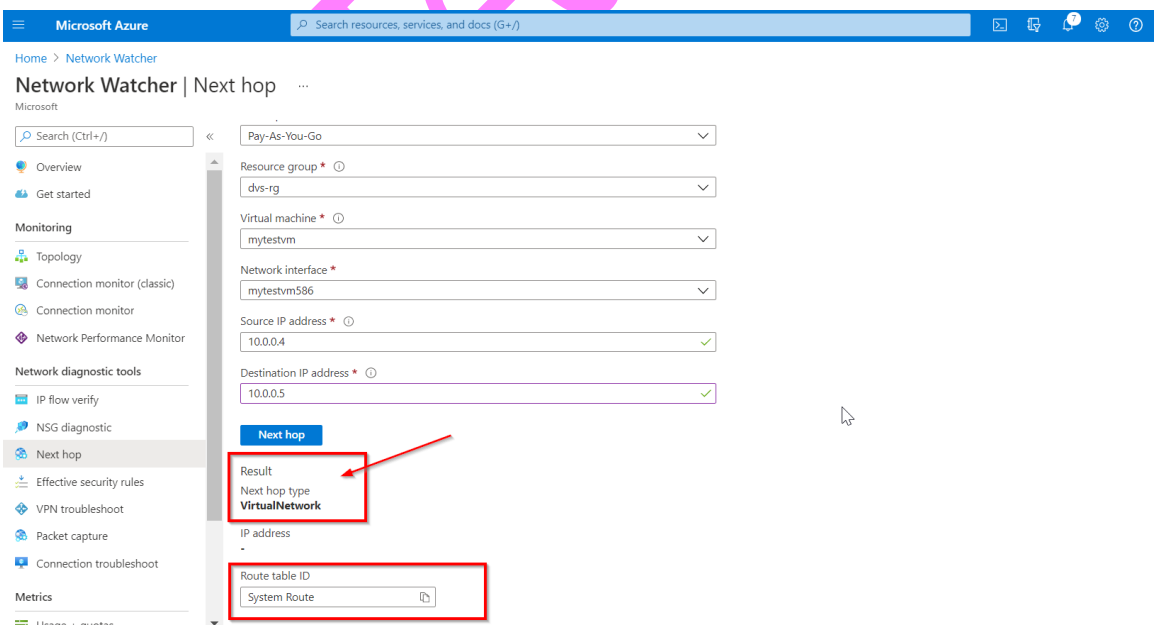
This will help you to check if any ports are opened or not from your server





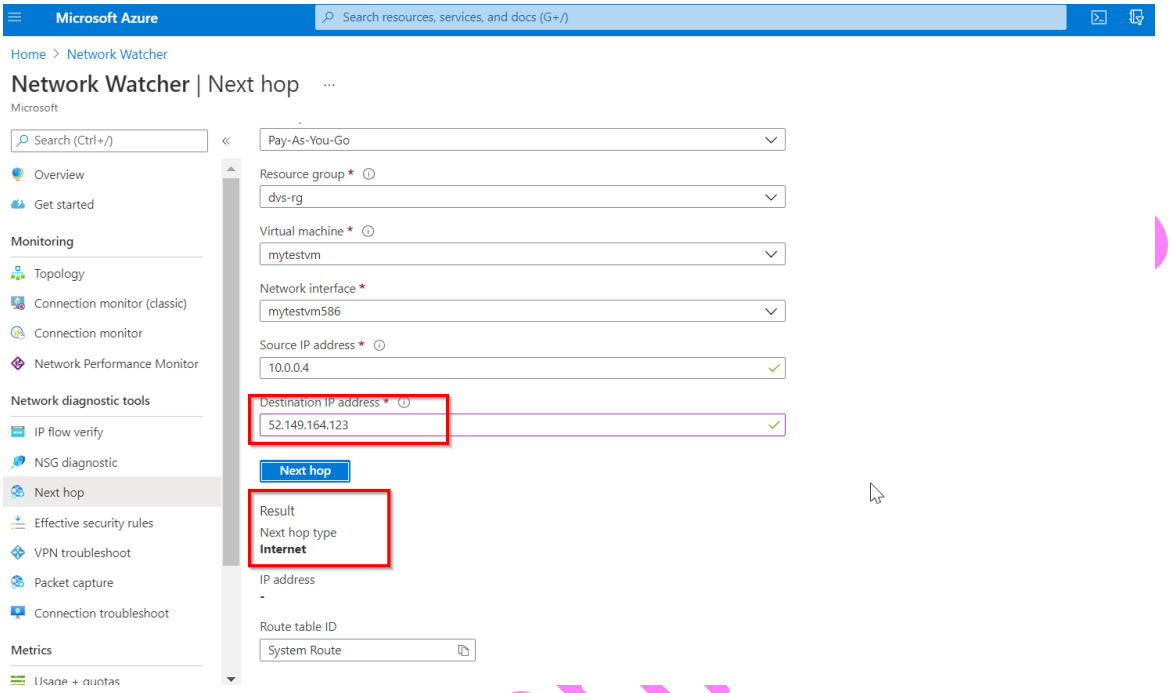
N/W watcher - next hop:
This will help us to understand where the next packet is going to land.

Let's say we have two VM's "mytestvm" & "newvm". Try to reach out to newvm from "mytestvm"



Here if you see we have the result as Virtual network

Let's try to hit our "newvm" on public ipaddress



Network Watcher - NSG Diagnostic
This help you to watch the Network security groups

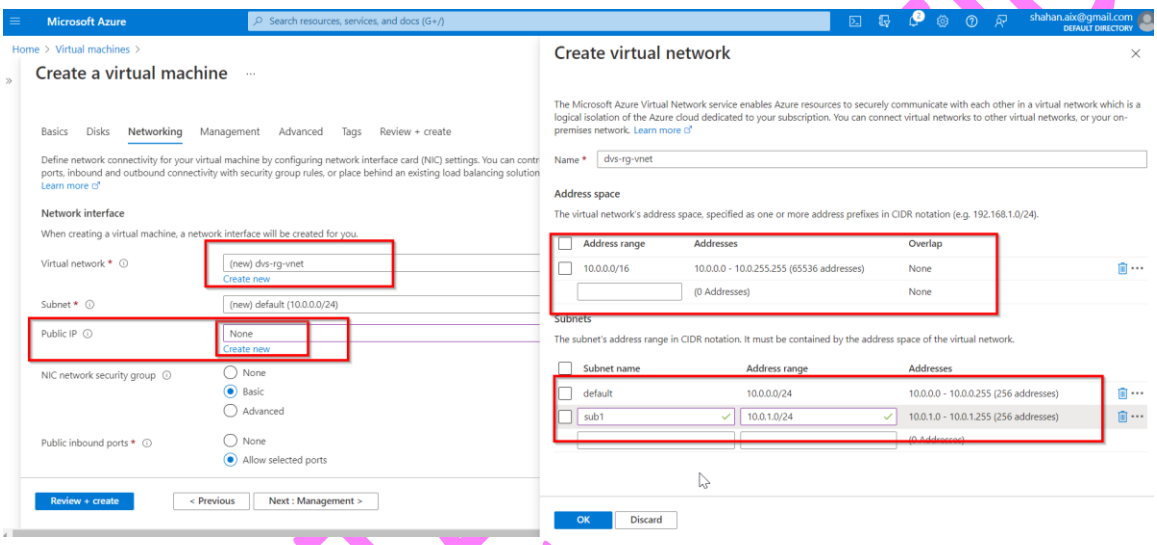
DVS Tech

7 Firewall - DNAT

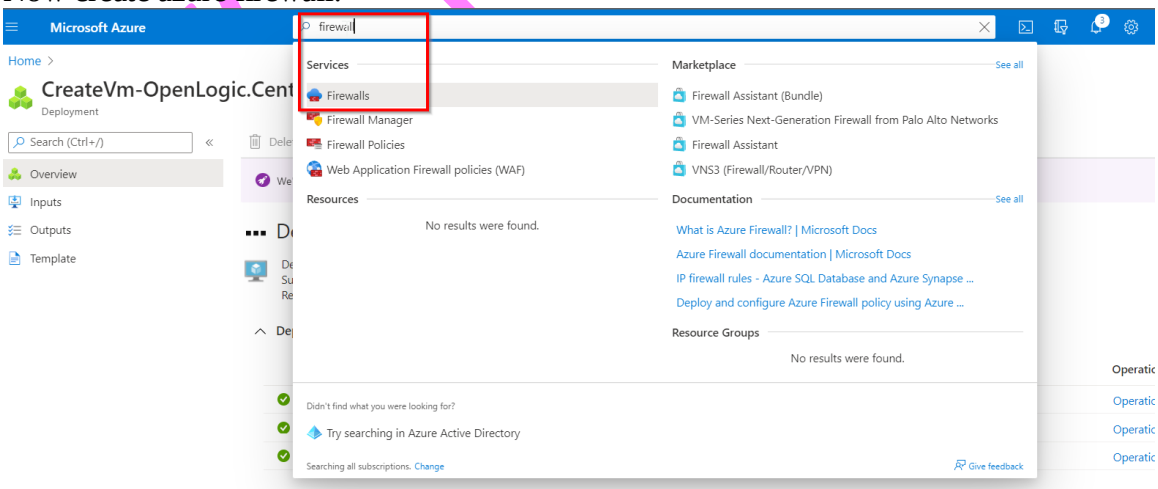
Companies in general wants to block the network to the internal infrastructure to avoid issue with attach. Now just imagine if you want to allow your internal infrastructure in azure want to align with restrictions then we can use azure firewall service.

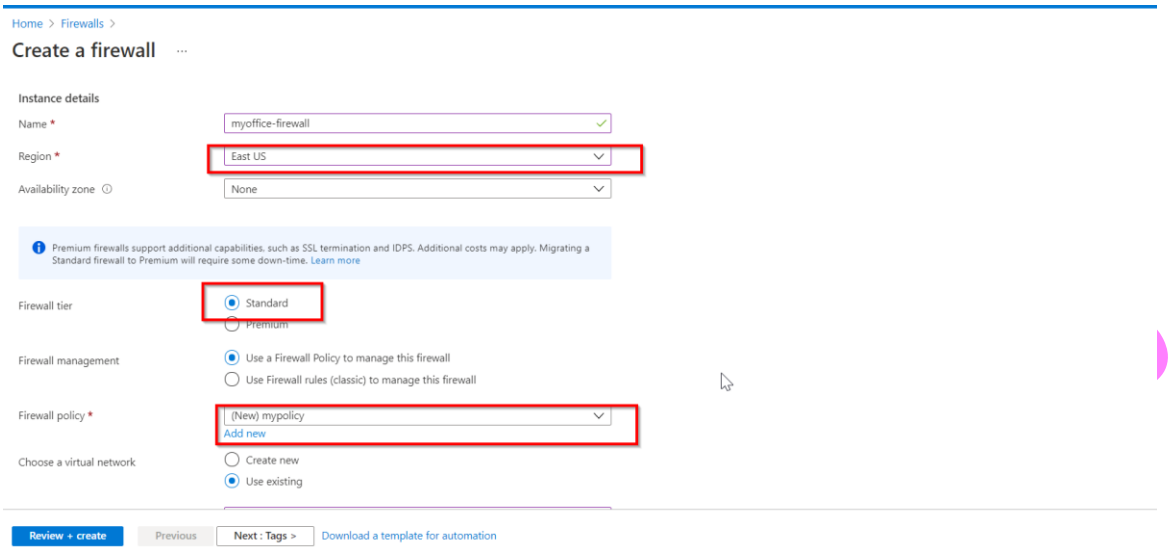
In order to understand this requirement let's try to build one VM & access it from outside world without public ipaddress. In simple we are going to use our firewall public ipaddress to access our private server from outside.

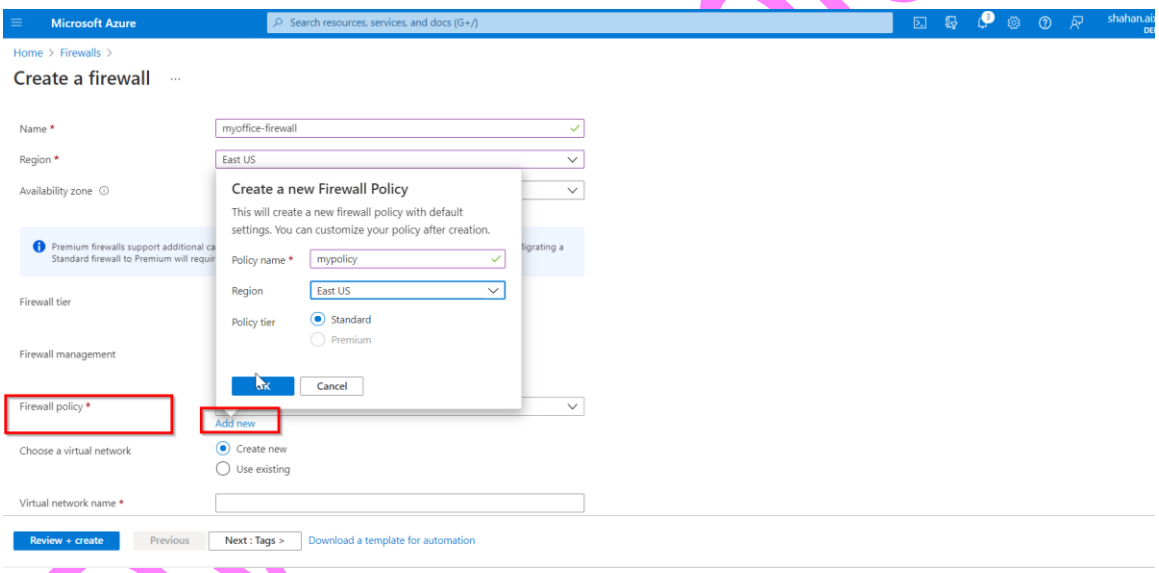
Create one VM:



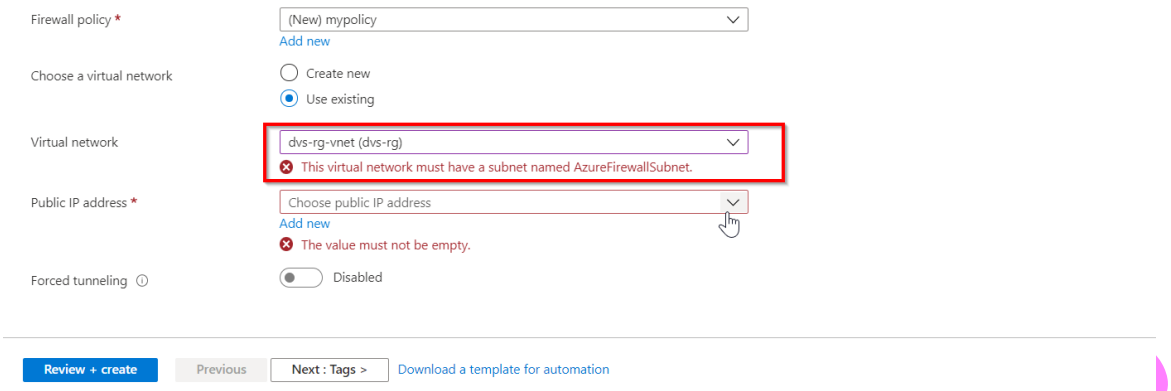
Now create azure firewall:



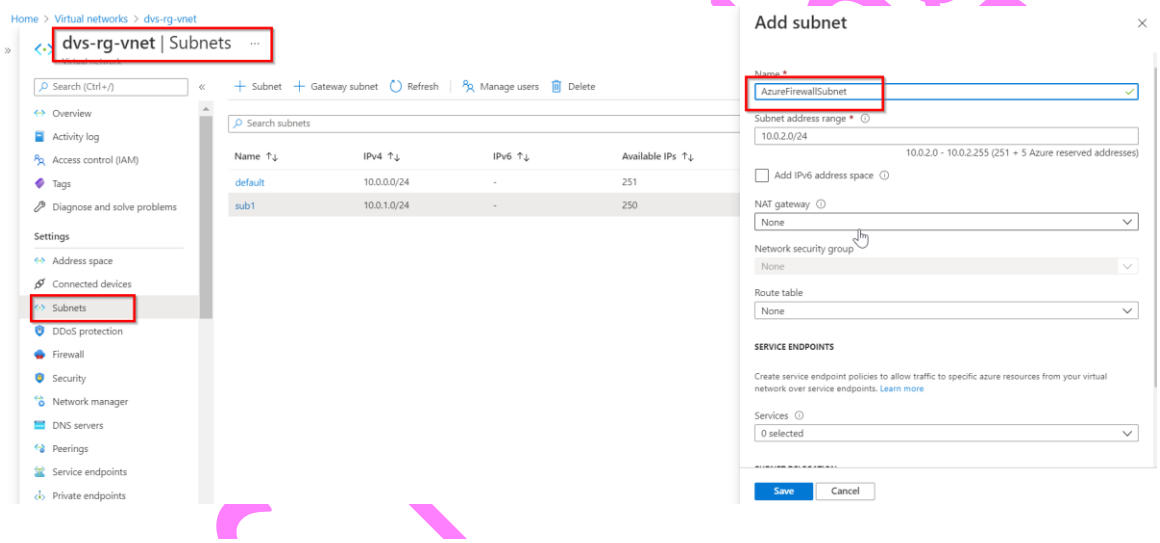


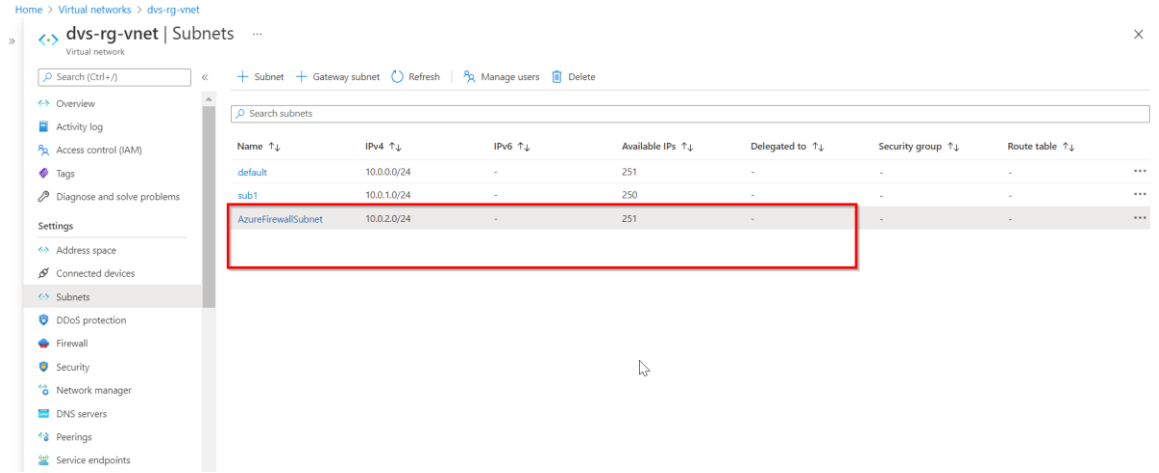


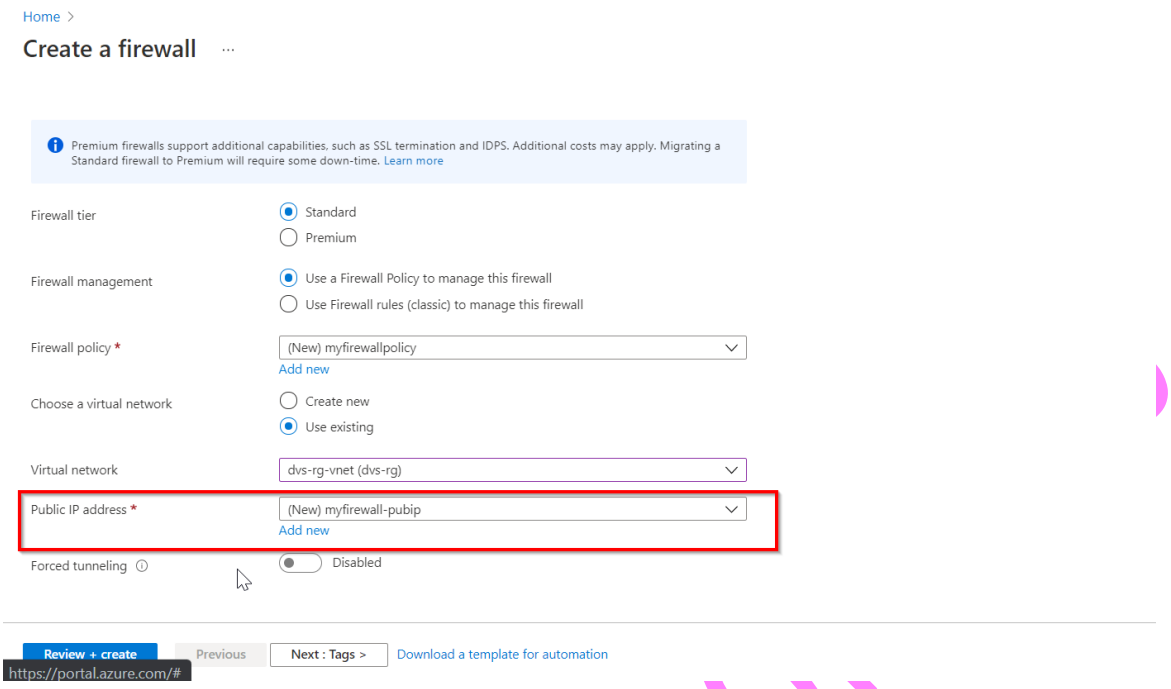
You have to make sure that you should create one subnet in the VNET with name as "AzureFirewallSubnet" & ITS VERY MANDATORY otherwise you will get below error

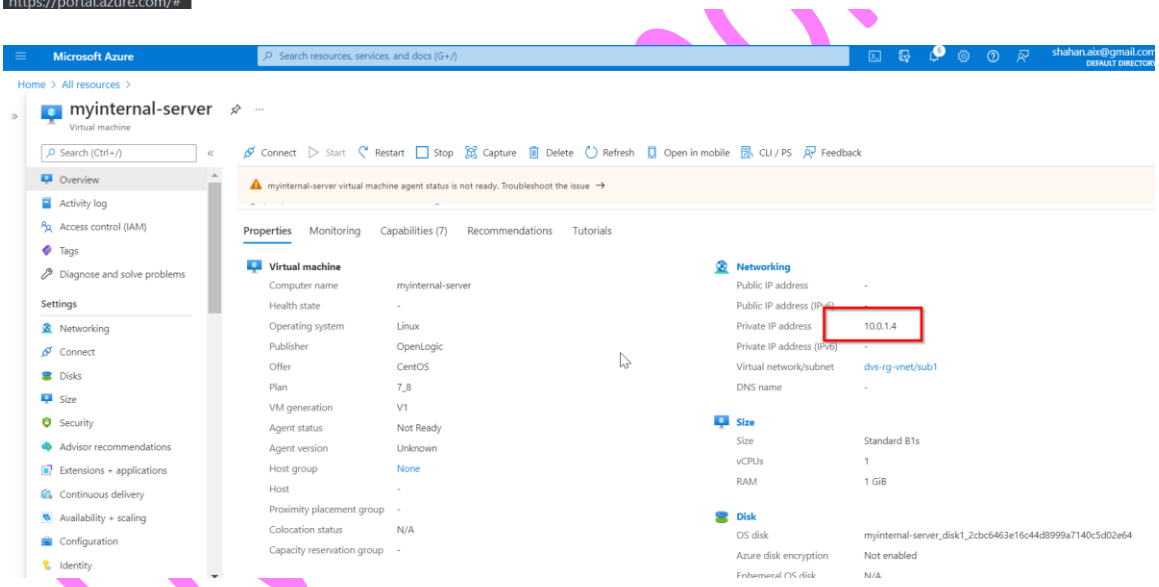


Now let's create the firewall subnet first.

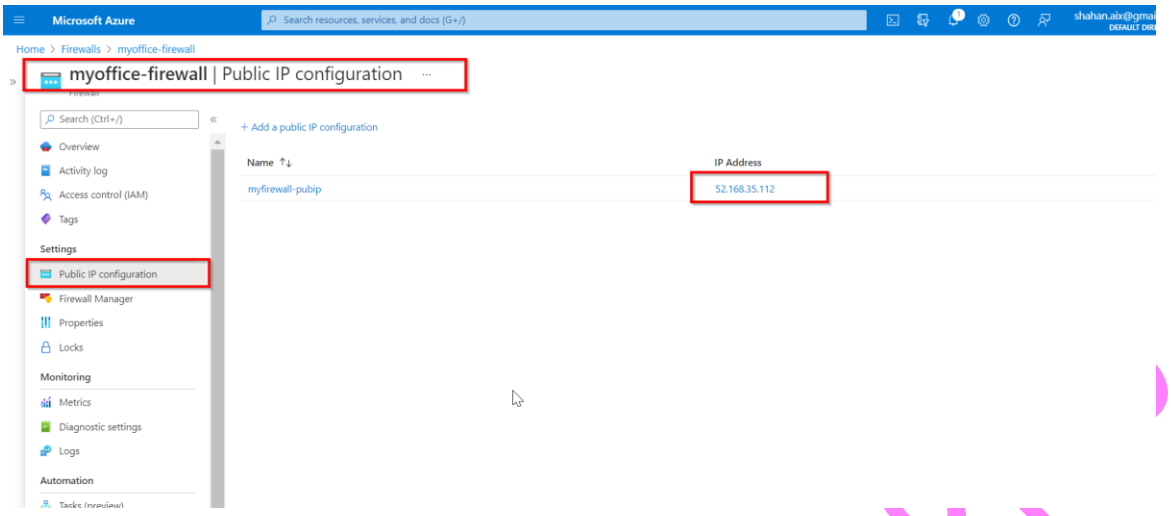






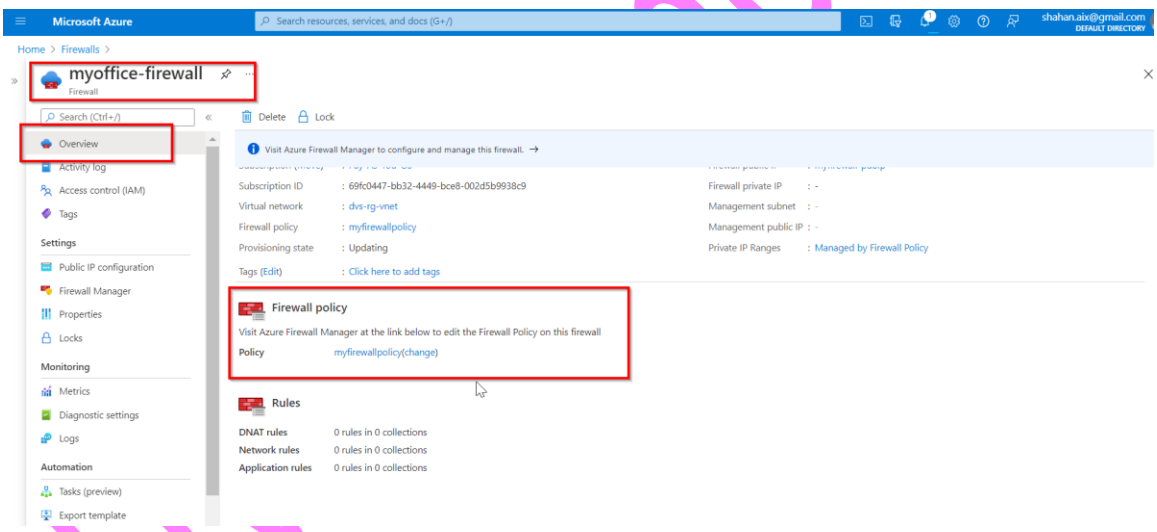


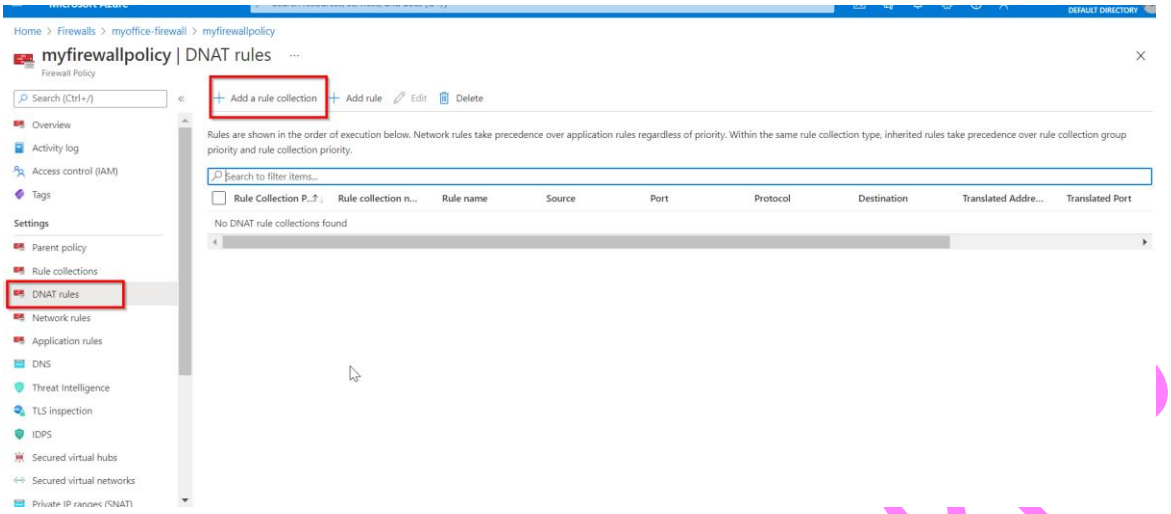
Now if you observe we have only private ip for our server, let's try to login to this server from our firewall.



This is the public ipaddress for our firewall

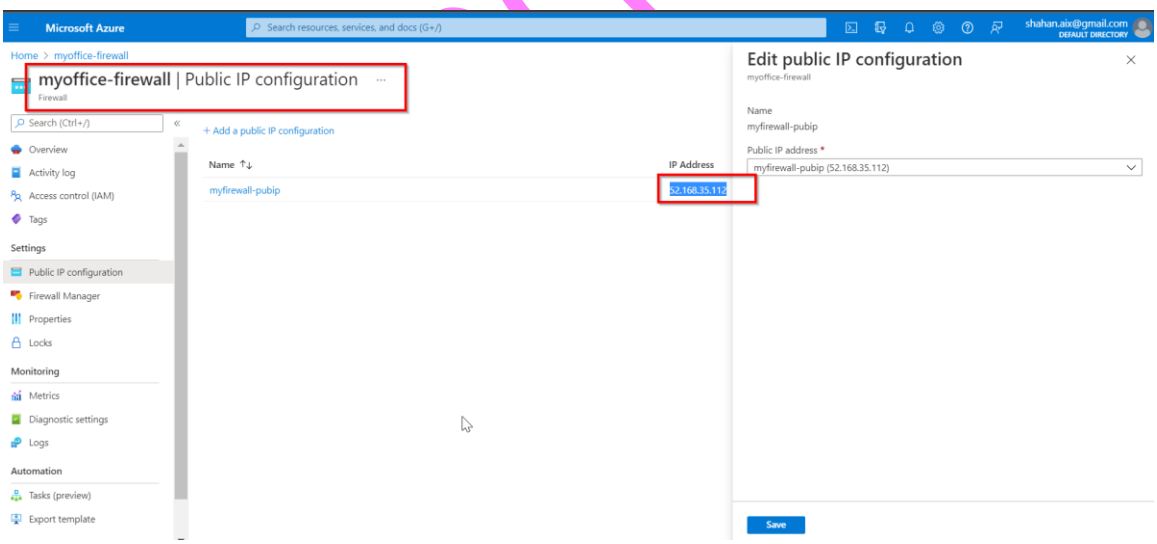
Let's configure the firewall rule as below



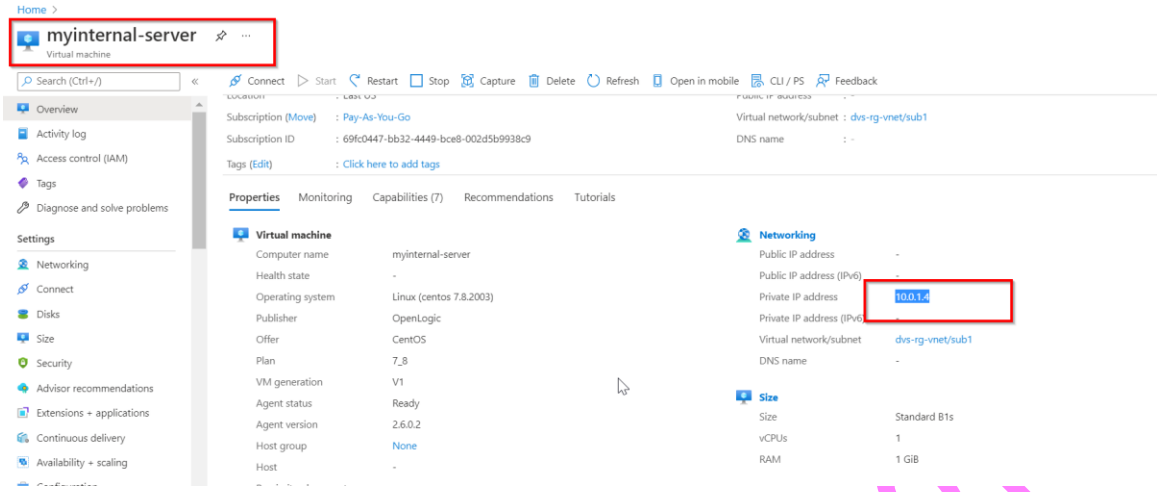


Source --> from where you want to access the server
Dest Ports --> on which port you want to hit the firewall
Dest type --> ipaddress
Destination --> firewall private ipaddress
Translate ipaddress --> Internal VM ipaddress
Translate port --> which port you want to access

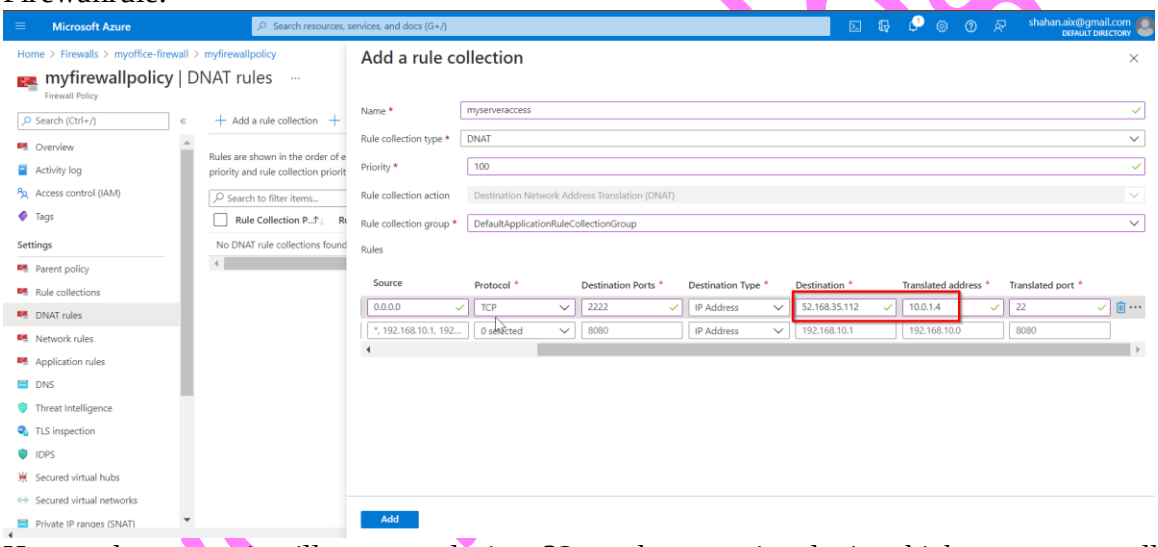
FirewallIP:



ServerIP:



Firewallrule:



Here under source it will accept only 1 or 32 you have to give the ip which you want to allow.

It takes time to create the entry pls wait

```
shahan.shaik@ubuntu-tpl:~$ ssh dvsadmin@52.168.35.112 -p 2222
The authenticity of host '[52.168.35.112]:2222 ([52.168.35.112]:2222)' can't be established.
ECDSA key fingerprint is SHA256:DIgUiP6T8YGx+WuvCPRCMQmfLVJJa+sj+A74RofQiQI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[52.168.35.112]:2222' (ECDSA) to the list of known hosts.
dvsadmin@52.168.35.112's password:
[dvsadmin@myinternal-server ~]$ hostname -I
10.0.1.4
[dvsadmin@myinternal-server ~]$
```

Now if you observe we can access server from the outside world via our firewall on custom port. But if you observe in the server

```
[dvsadmin@myinternal-server ~]$ wget http://google.com
--2021-12-14 09:27:34--  http://google.com/
Resolving google.com (google.com)... 142.251.45.14, 2607:f8b0:4004:83e::200e
Connecting to google.com (google.com)|142.251.45.14|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.google.com/ [following]
--2021-12-14 09:27:34--  http://www.google.com/
Resolving www.google.com (www.google.com)... 172.217.164.132, 2607:f8b0:4004:c0b::69, 2607:f8b0:4004:c0b::68, ...
Connecting to www.google.com (www.google.com)|172.217.164.132|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

    [ <=>                                                                                                   ] 15,128      --.-K/s   in 0s

2021-12-14 09:27:34 (119 MB/s) - 'index.html' saved [15128]

[dvsadmin@myinternal-server ~]$
```

We have access to the internet for the server.

DVS Technologies

8 Firewall - Restrict the internet

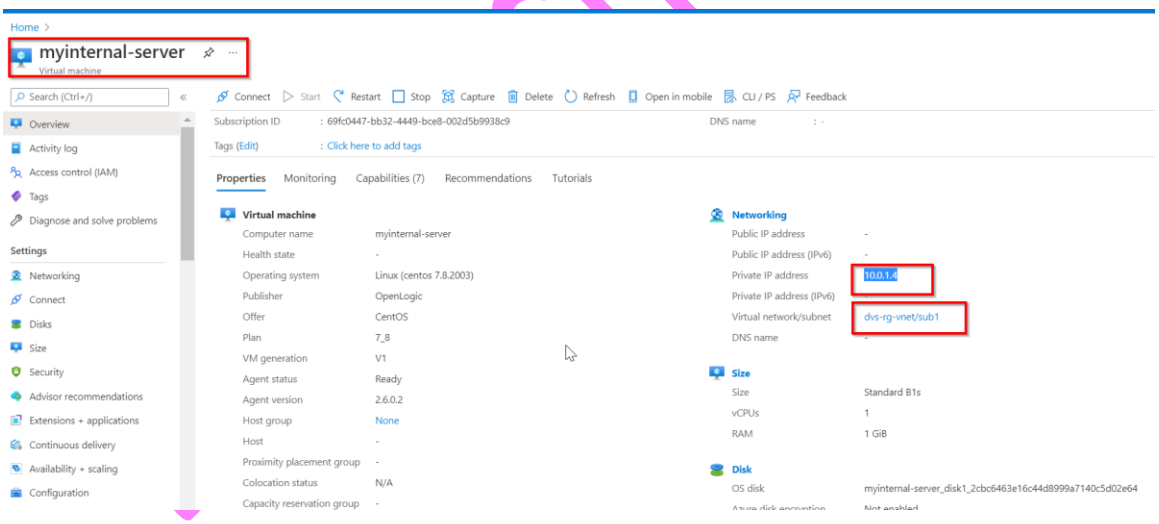
When we implement the firewall for our server access from outside world we are unable to restrict the internet for the machines hence we need to restrict the servers which websites they can use.

```
[dvsadmin@myinternal-server ~]$ wget http://google.com
--2021-12-14 09:27:34--  http://google.com/
Resolving google.com (google.com)... 142.251.45.14, 2607:f8b0:4004:83e::200e
Connecting to google.com (google.com)|142.251.45.14|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.google.com/ [following]
--2021-12-14 09:27:34--  http://www.google.com/
Resolving www.google.com (www.google.com)... 172.217.164.132, 2607:f8b0:4004:c0b::69, 2607:f8b0:4004:c0b::68, ...
Connecting to www.google.com (www.google.com)|172.217.164.132|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

    [ <=>                                                                                                   ] 15,128      --.-K/s   in 0s

2021-12-14 09:27:34 (119 MB/s) - 'index.html' saved [15128]

[dvsadmin@myinternal-server ~]$
```

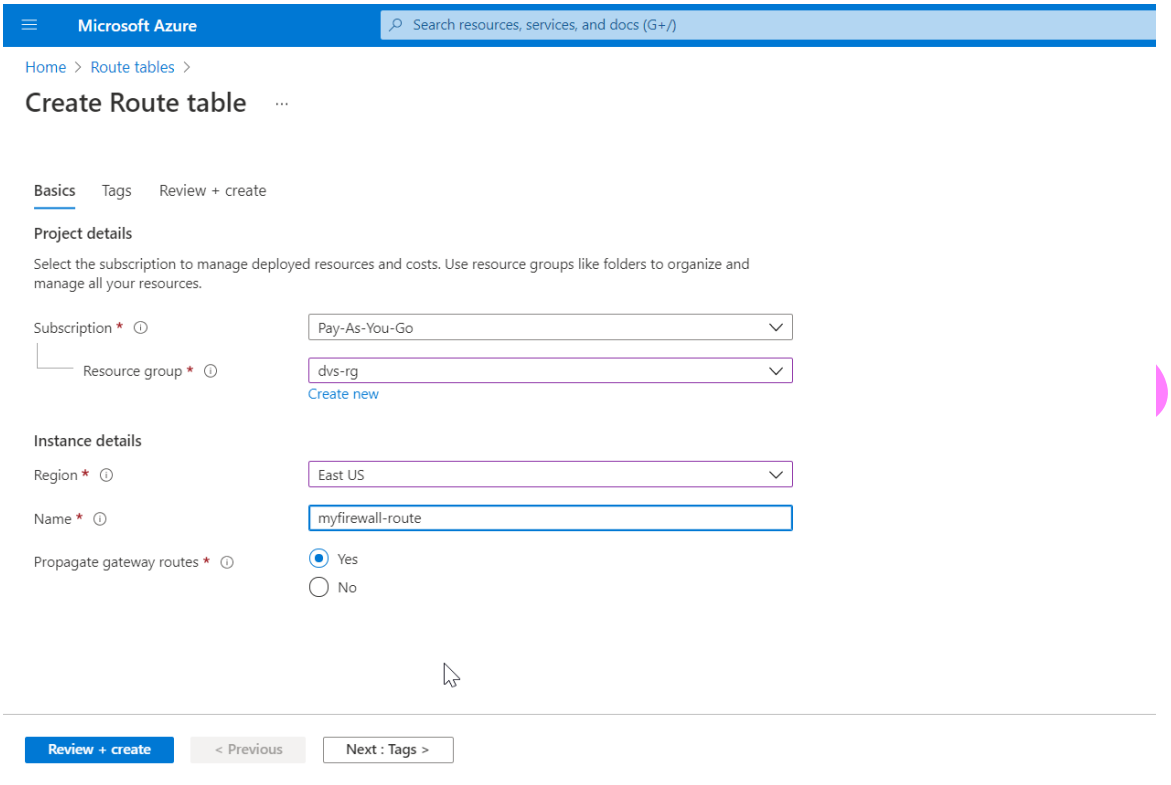
Let's do the below.

We need to create the routetable & route the traffic for the VM subnet via firewall ipaddress.

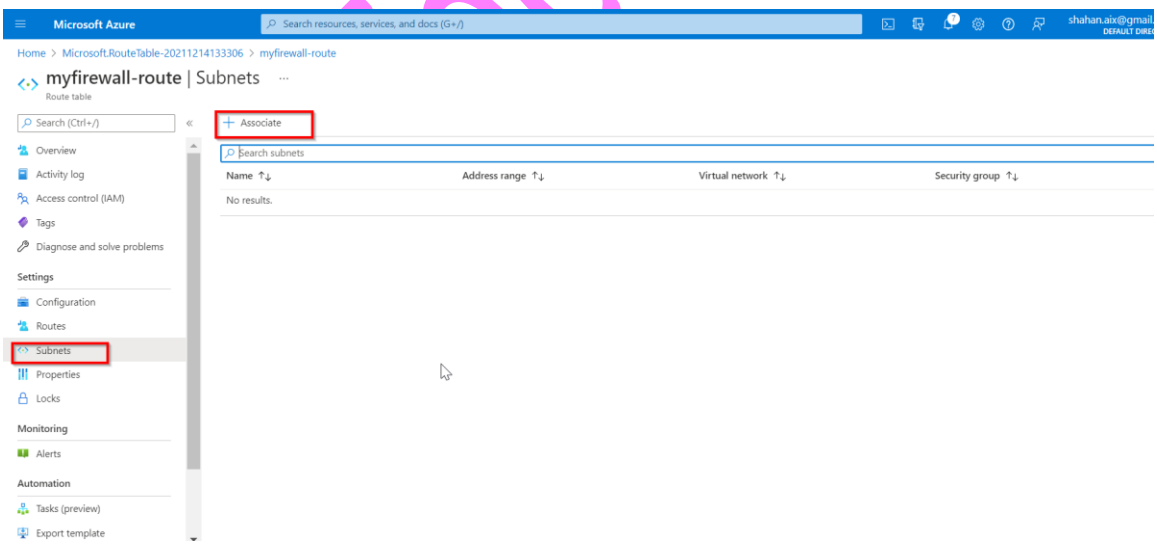
Our VM ip is in subnet

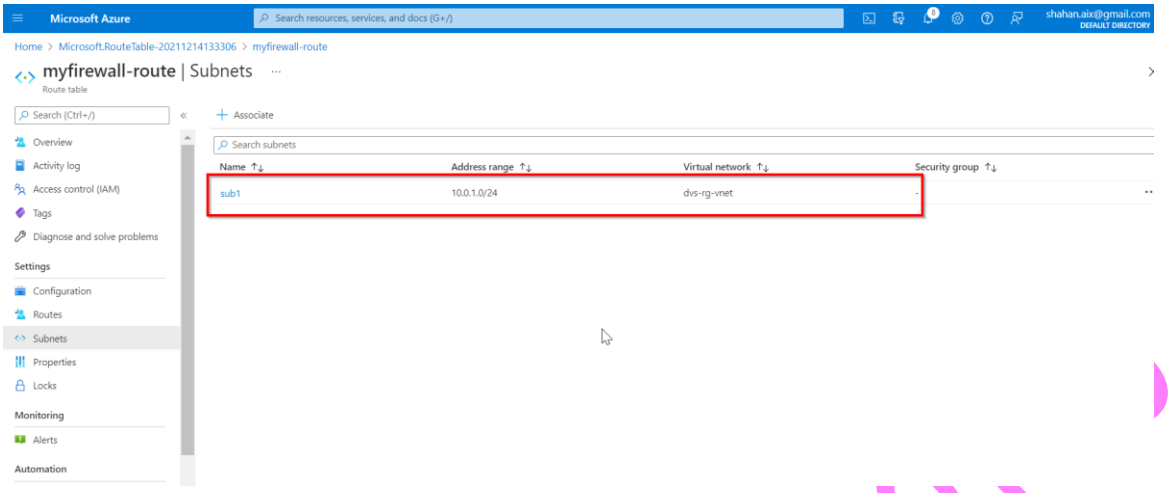


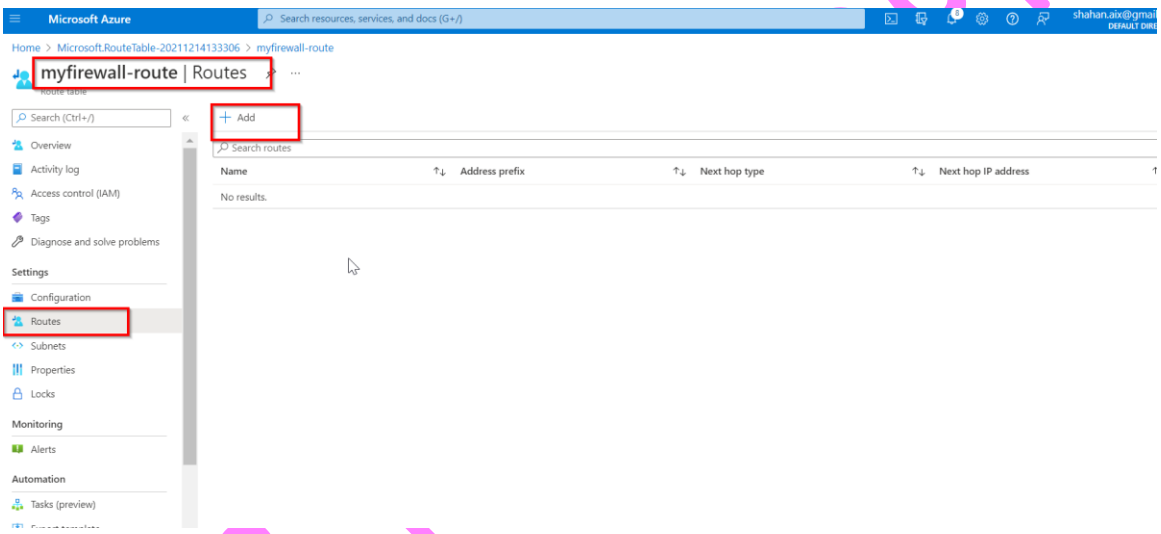
Create route table



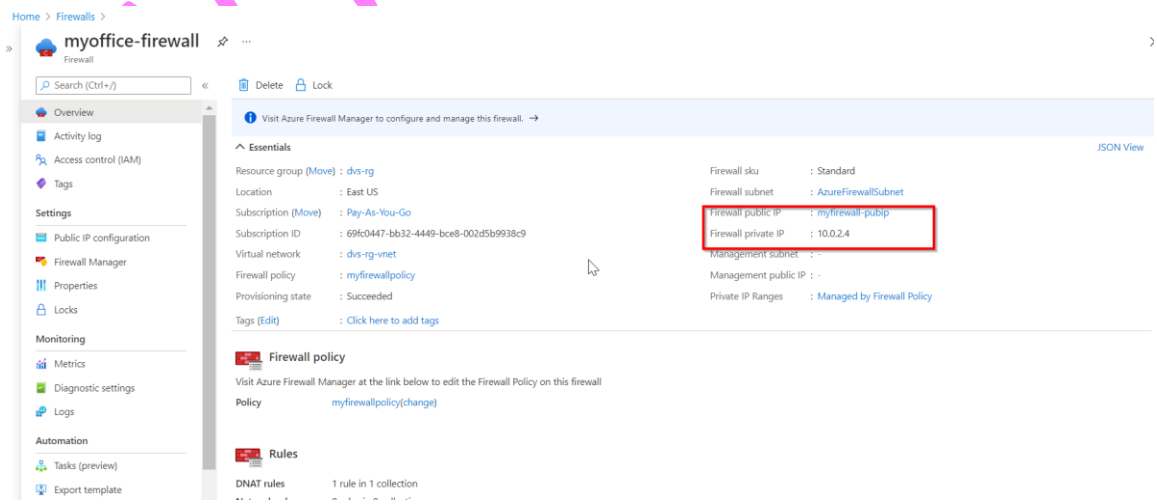
Let's add our servers subnet

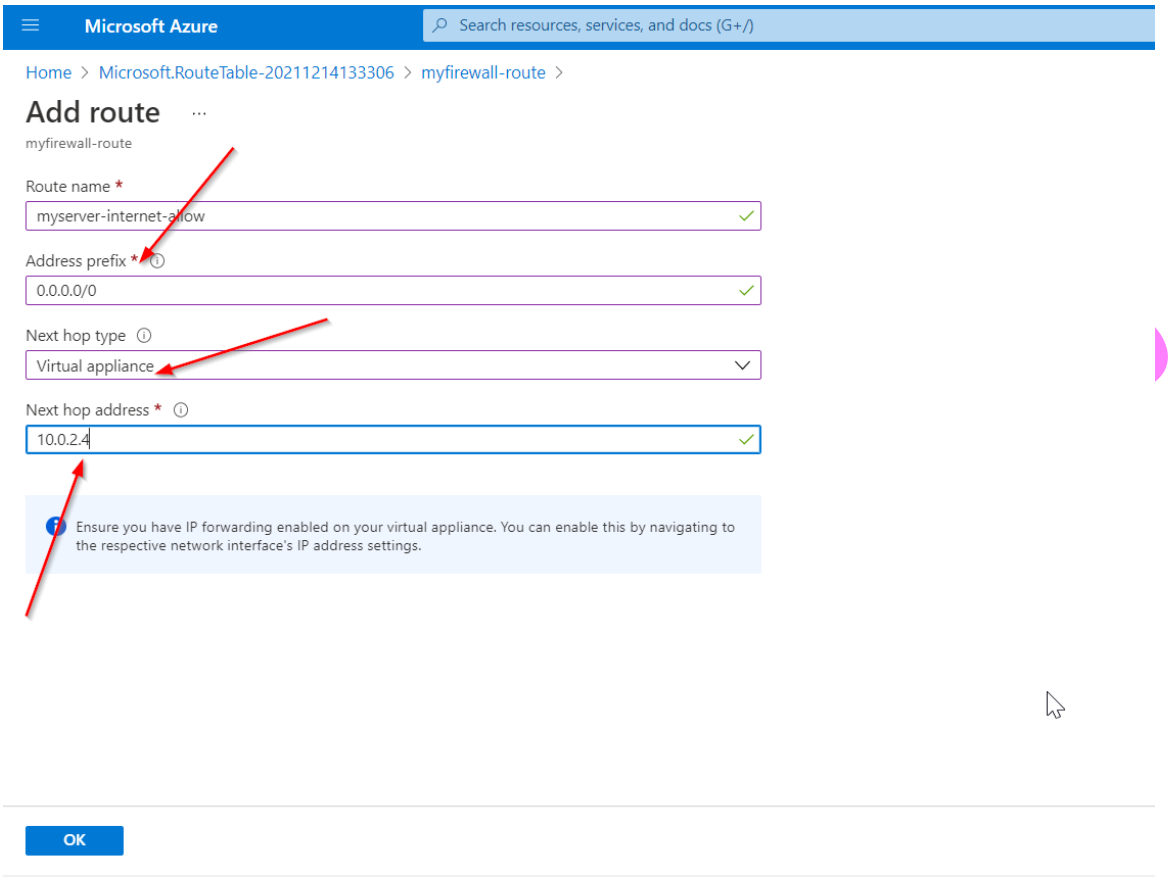



Microsoft Azure
Search resources, services, and docs (G+/)
shahan.aix@gmail.com
DEFAULT DIRECTORY
Home > Microsoft.RouteTable-20211214133306 > myfirewall-route
myfirewall-route | Subnets
Route table
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Routes
Subnets
Properties
Locks
Monitoring
Alerts
Automation
Associate
Search subnets
Name
Address range
Virtual network
Security group
sub1
10.0.1.0/24
dvs-rg-vnet

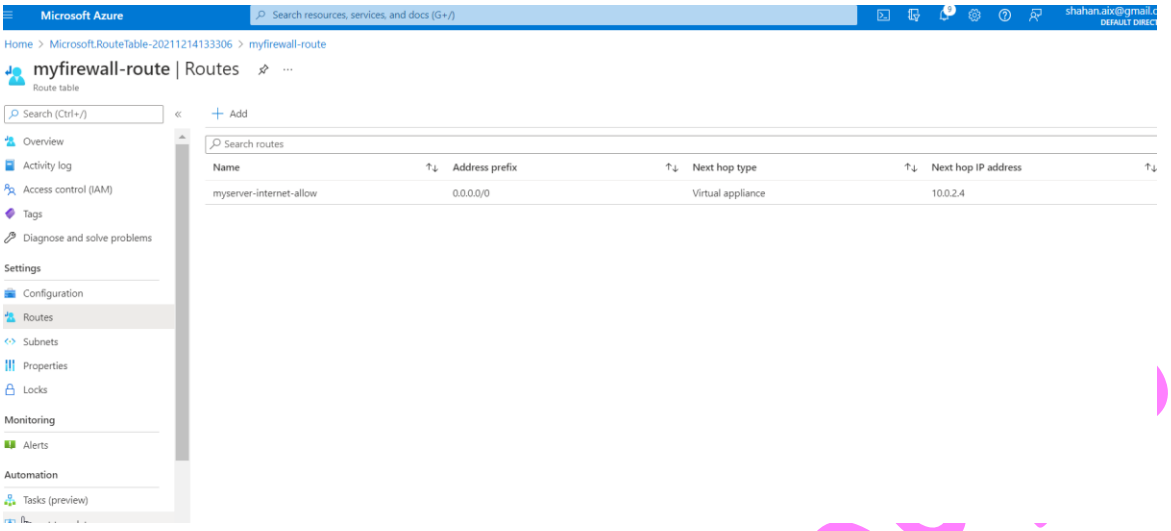

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft.RouteTable-20211214133306 > myfirewall-route
myfirewall-route | Routes
Route table
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Routes
Subnets
Properties
Locks
Monitoring
Alerts
Automation
Tasks (preview)
Add
Search routes
Name
Address prefix
Next hop type
Next hop IP address
No results.

Firewall ip:


Home > Firewalls >
myoffice-firewall
Firewall
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Settings
Public IP configuration
Firewall Manager
Properties
Locks
Monitoring
Metrics
Diagnostic settings
Logs
Automation
Tasks (preview)
Export template
Delete
Lock
Visit Azure Firewall Manager to configure and manage this firewall.
Essentials
JSON View
Resource group (Move) : dvs-rg
Location : East US
Subscription (Move) : Pay-As-You-Go
Subscription ID : 69fc0447-bb32-4449-bce8-002d5b9938c9
Virtual network : dvs-rg-vnet
Firewall policy : myfirewallpolicy
Provisioning state : Succeeded
Tags (Edit) : Click here to add tags
Firewall sku : Standard
Firewall subnet : AzureFirewallSubnet
Firewall public IP : myfirewall-pubip
Firewall private IP : 10.0.2.4
Management subnet : -
Management public IP : -
Private IP Ranges : Managed by Firewall Policy
Firewall policy
Visit Azure Firewall Manager at the link below to edit the Firewall Policy on this firewall
Policy myfirewallpolicy(change)
Rules
DNAT rules 1 rule in 1 collection

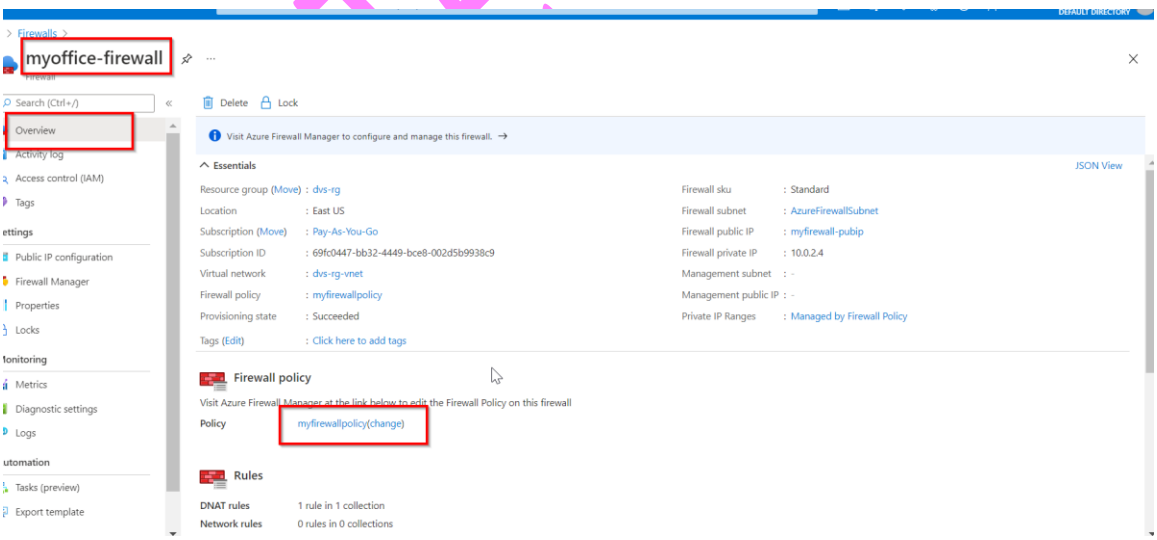


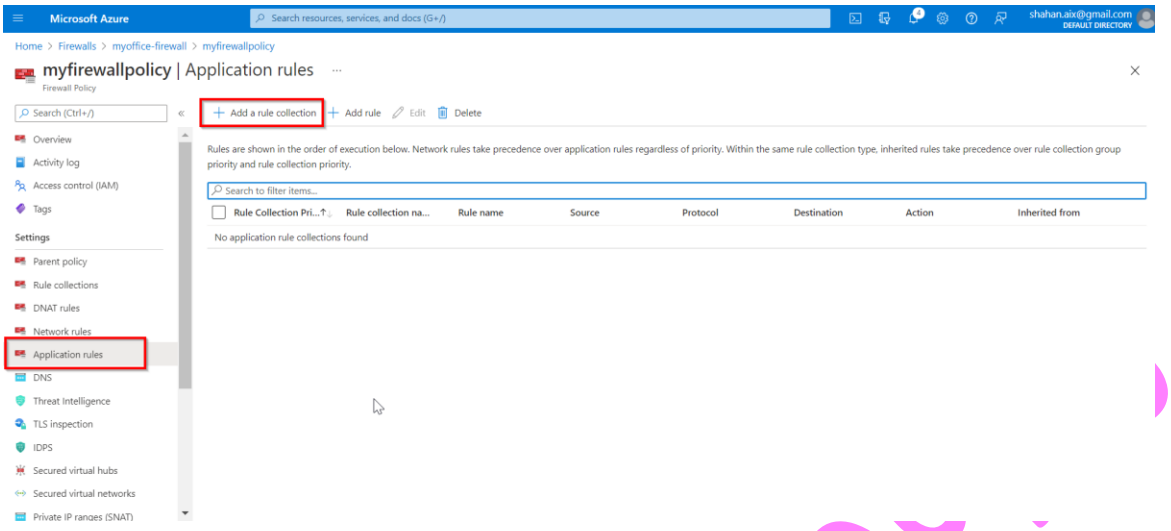
Address prefix: here we gave 0.0.0.0/0 why ? Because we want to connect to internet
Next hop address: this is our azure firewall ip via which you can connect to internet

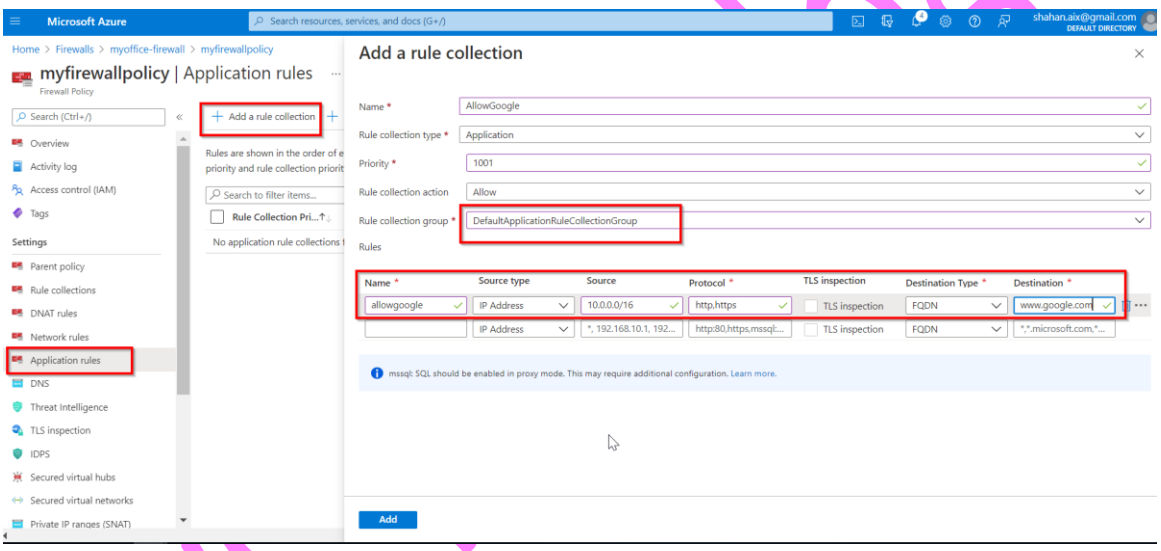


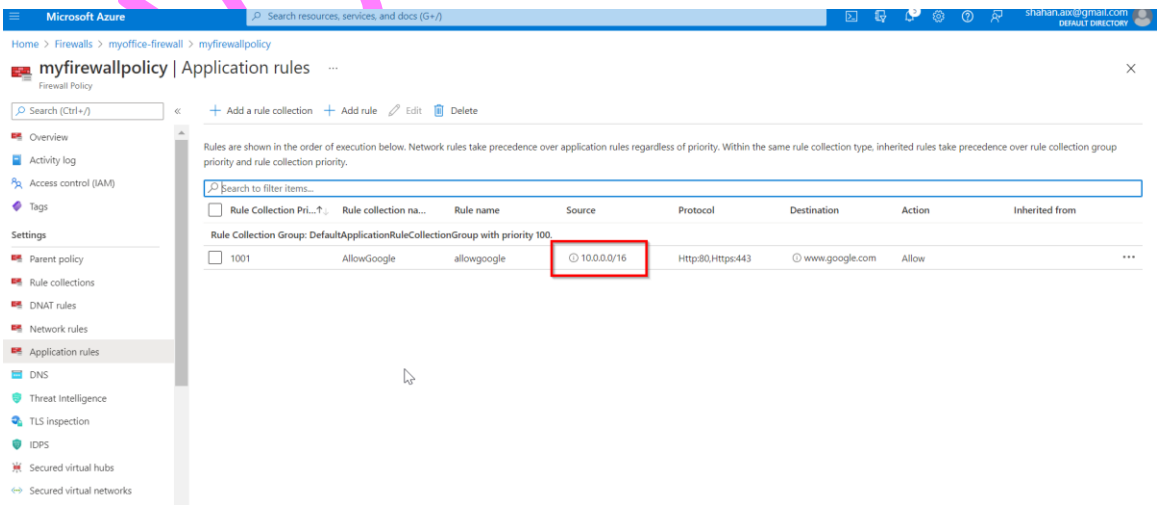
Now we have configure our subnet to go via firewall for the internet access. Let's try to reach internet now from our VM

Now its blocked you cannot access internet. If you want to allow the internet then you can do the below




Microsoft Azure
Search resources, services, and docs (G+/)
shahan.aix@gmail.com
DEFAULT DIRECTORY
Home > Firewalls > myoffice-firewall > myfirewallpolicy
myfirewallpolicy | Application rules
Firewall Policy
Search (Ctrl+/)
Add a rule collection
Add rule
Edit
Delete
Overview
Activity log
Access control (IAM)
Tags
Settings
Parent policy
Rule collections
DNAT rules
Network rules
Application rules
DNS
Threat Intelligence
TLS inspection
IDPS
Secured virtual hubs
Secured virtual networks
Private IP ranges (SNAT)
Rules are shown in the order of execution below. Network rules take precedence over application rules regardless of priority. Within the same rule collection type, inherited rules take precedence over rule collection group priority and rule collection priority.
Search to filter items...
Rule Collection Pri...
Rule collection na...
Rule name
Source
Protocol
Destination
Action
Inherited from
No application rule collections found


Microsoft Azure
Search resources, services, and docs (G+/)
shahan.aix@gmail.com
DEFAULT DIRECTORY
Home > Firewalls > myoffice-firewall > myfirewallpolicy
myfirewallpolicy | Application rules
Firewall Policy
Add a rule collection
Add a rule collection
Name *
AllowGoogle
Rule collection type *
Application
Priority *
1001
Rule collection action
Allow
Rule collection group *
DefaultApplicationRuleCollectionGroup
Rules
Name *
Source type
Source
Protocol *
TLS inspection
Destination Type *
Destination *
allowgoogle
IP Address
10.0.0.0/16
http,https
TLS inspection
FQDN
www.google.com
IP Address
*, 192.168.10.1, 192...
http:80,https,mssql:...
TLS inspection
FQDN
,.microsoft.com,*...
mssql: SQL should be enabled in proxy mode. This may require additional configuration. Learn more.
Add


Microsoft Azure
Search resources, services, and docs (G+/)
shahan.aix@gmail.com
DEFAULT DIRECTORY
Home > Firewalls > myoffice-firewall > myfirewallpolicy
myfirewallpolicy | Application rules
Firewall Policy
Add a rule collection
Add rule
Edit
Delete
Rules are shown in the order of execution below. Network rules take precedence over application rules regardless of priority. Within the same rule collection type, inherited rules take precedence over rule collection group priority and rule collection priority.
Search to filter items...
Rule Collection Pri...
Rule collection na...
Rule name
Source
Protocol
Destination
Action
Inherited from
Rule Collection Group: DefaultApplicationRuleCollectionGroup with priority 100.
1001
AllowGoogle
allowgoogle
10.0.0.0/16
Http:80,Https:443
www.google.com
Allow

Here we gave cidr 10.0.0.0/16 but you can give the specific ip as well in our case 10.0.1.4/32

```
[dvsadmin@myinternal-server ~]$ wget https://www.google.com
--2021-12-14 09:50:54--  https://www.google.com/
Resolving www.google.com (www.google.com)... 142.250.31.105, 142.250.31.147, 142.250.31.99, ...
Connecting to www.google.com (www.google.com)|142.250.31.105|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html.1'

    [ <=>                                                                                   ] 15,120      --.-K/s   in 0s

2021-12-14 09:50:54 (32.8 MB/s) - 'index.html.1' saved [15120]

[dvsadmin@myinternal-server ~]$
```

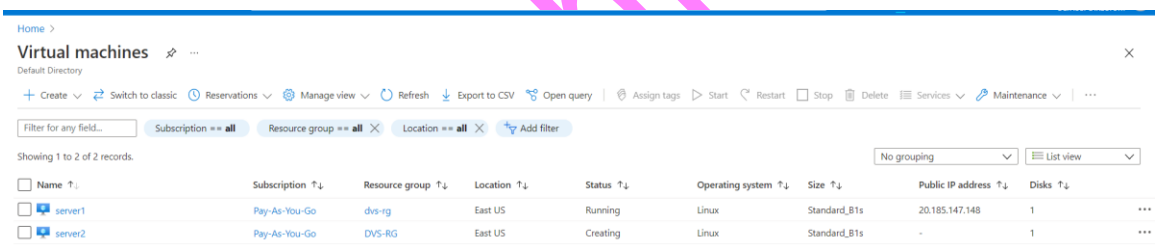
Now I can able to access google.com

9 Private DNS zone

At any point if you feel like you want to have your own DNS names for your servers then you can make use of private DNS zone.

Note: Private DNS zone is used for INTERNAL resolution only not for external purpose

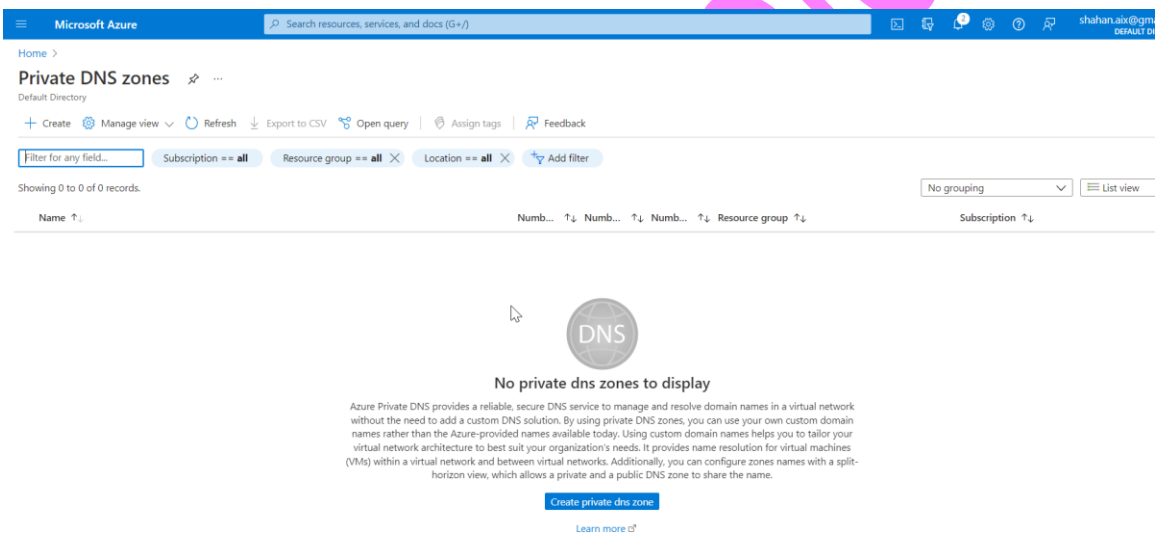
Let's create two servers and try to reach them with the dns names

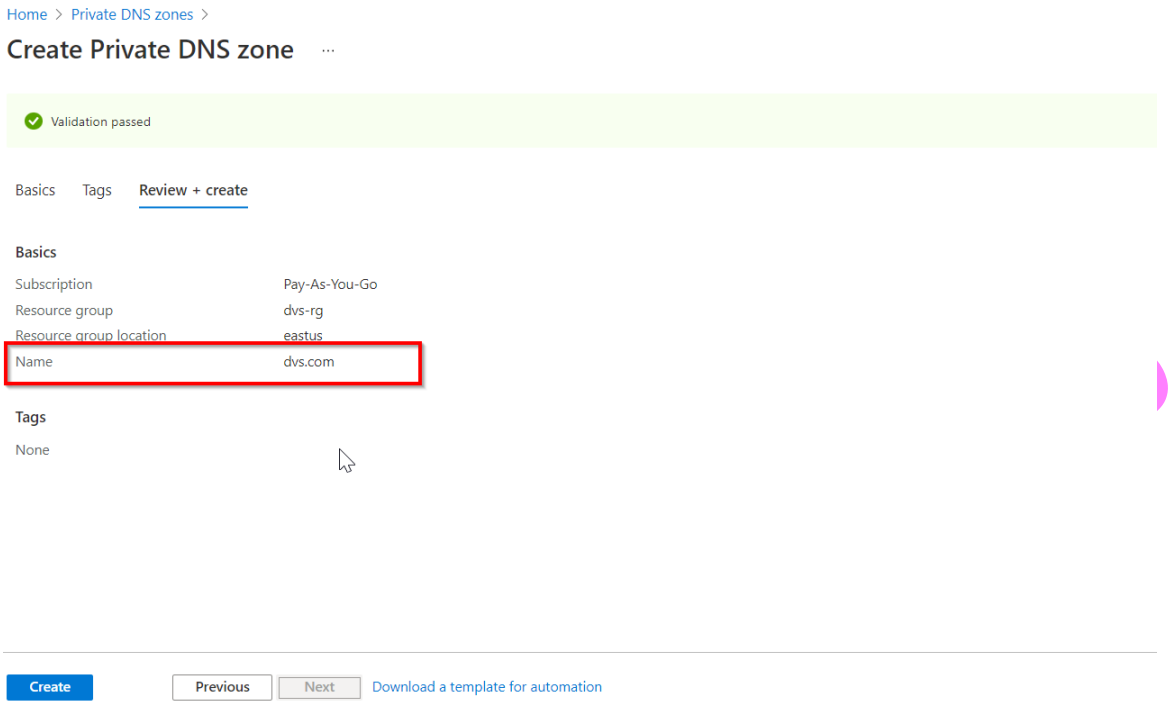


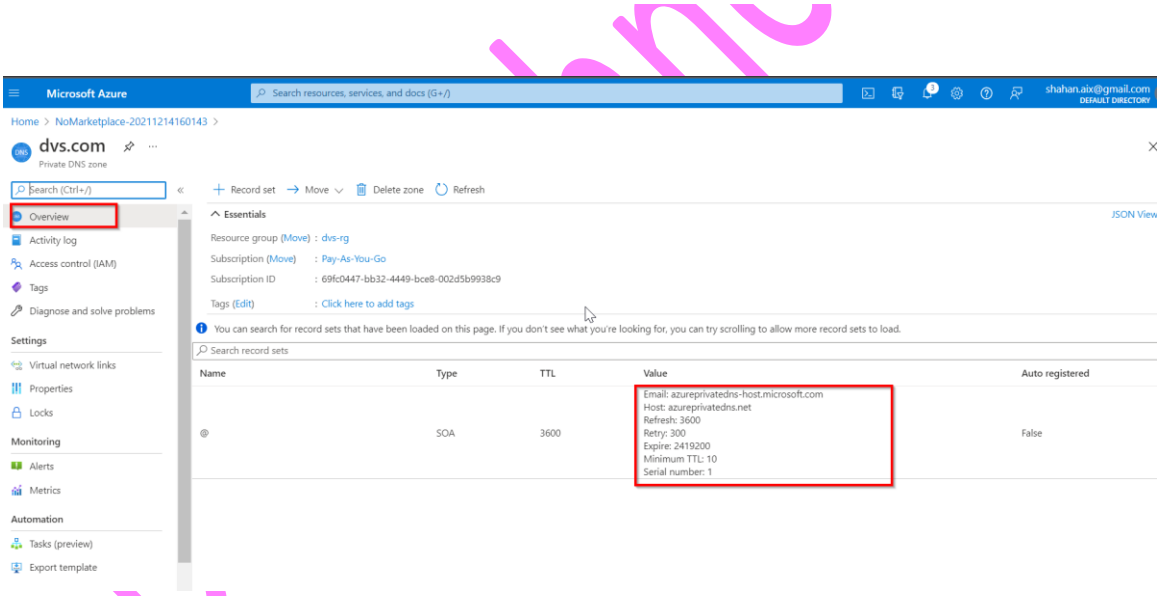
Our requirement is quite simple just login to server1 and try to resolve server2.dvs.com

```
[dvsadmin@server1 ~]$ ssh server2.dvs.com


^C
[dvsadmin@server1 ~]$
[dvsadmin@server1 ~]$ nslookup server2
Server:         168.63.129.16
Address:        168.63.129.16#53

Non-authoritative answer:
Name:   server2.qjz53nlzuynejj2izzebptdmle.bx.internal.cloudapp.net
Address: 10.0.0.5

[dvsadmin@server1 ~]$ nslookup server2.dvs.com
Server:         168.63.129.16
Address:        168.63.129.16#53

Non-authoritative answer:
Name:   server2.dvs.com
Address: 162.159.134.42

[dvsadmin@server1 ~]$
```

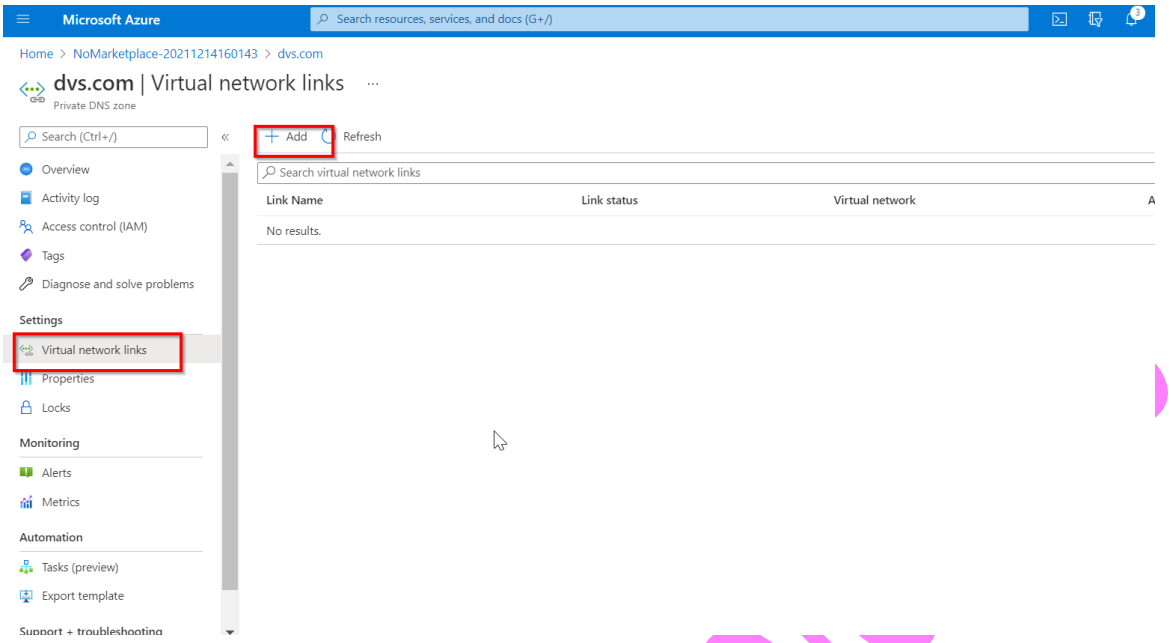
If you observe above we see that server2.dvs.com is not resolving. Let's configure our own domain.

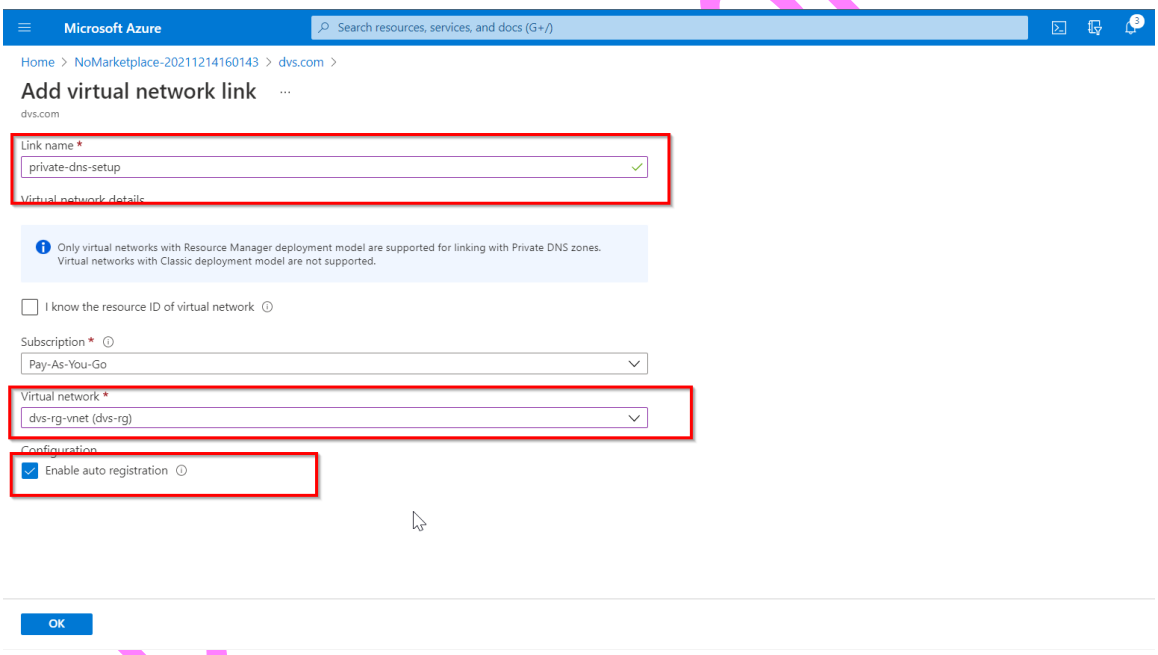


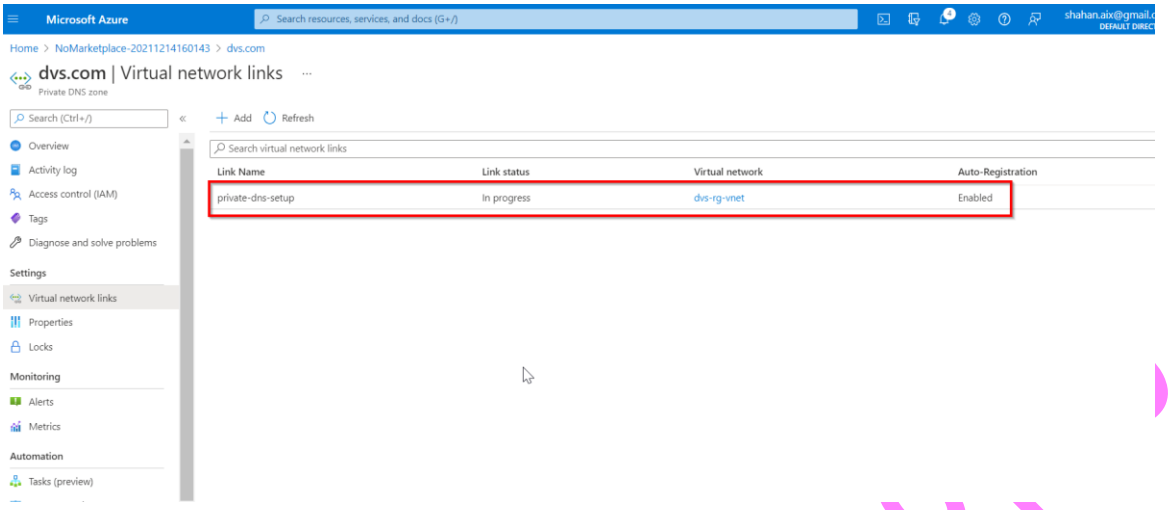




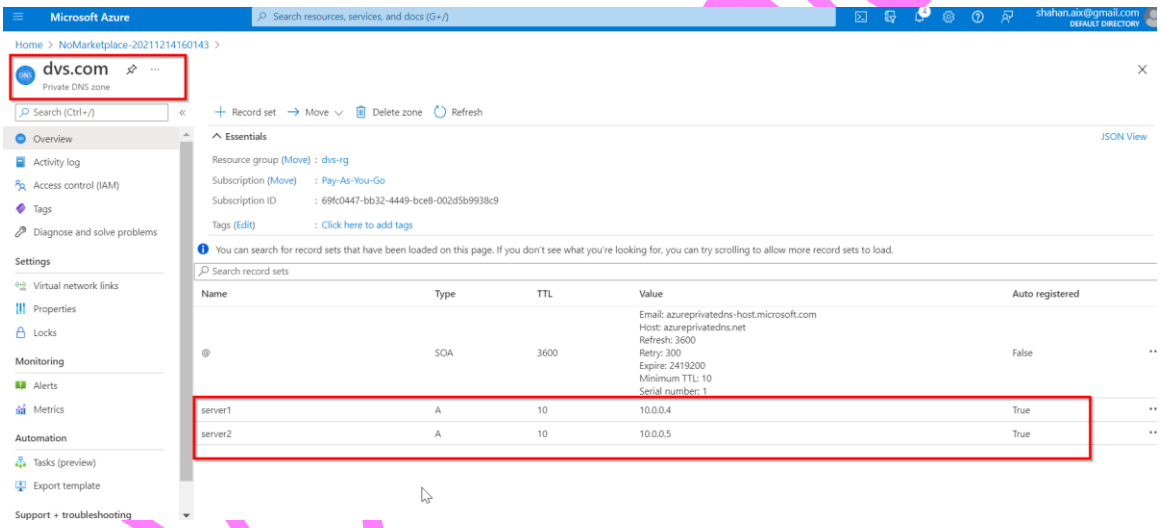
Let's link the VNET to this


Microsoft Azure
Search resources, services, and docs (G+/)
Home > NoMarketplace-20211214160143 > dvs.com
dvs.com | Virtual network links
Private DNS zone
Search (Ctrl+/)
Add
Refresh
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Virtual network links
Properties
Locks
Monitoring
Alerts
Metrics
Automation
Tasks (preview)
Export template
Search virtual network links
Link Name
Link status
Virtual network
No results.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > NoMarketplace-20211214160143 > dvs.com >
Add virtual network link
dvs.com
Link name *
private-dns-setup
Virtual network details
Only virtual networks with Resource Manager deployment model are supported for linking with Private DNS zones.
Virtual networks with Classic deployment model are not supported.
I know the resource ID of virtual network
Subscription *
Pay-As-You-Go
Virtual network *
dvs-rg-vnet (dvs-rg)
Configuration
Enable auto registration
OK



Once link status changed to connected then we should see our servers server1 & server2 as part of our DNS



Now if you observe our servers got auto registered

Let's see if we can resolve the names or not

```
[dvsadmin@server1 ~]$ nslookup server2.dvs.com
Server:         168.63.129.16
Address:        168.63.129.16#53

Non-authoritative answer:
Name:   server2.dvs.com
Address: 10.0.0.5

[dvsadmin@server1 ~]$ ssh server2.dvs.com
The authenticity of host 'server2.dvs.com (10.0.0.5)' can't be established.
ECDSA key fingerprint is SHA256:MroXndNoDMjh3peRKszwsVeGF67zuiP++Vfui3yhFUo.
ECDSA key fingerprint is MD5:36:43:6e:3e:63:45:cc:42:1a:d9:22:8e:04:06:b1:cd.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server2.dvs.com' (ECDSA) to the list of known hosts.
dvsadmin@server2.dvs.com's password:
[dvsadmin@server2 ~]$ hostname -I
10.0.0.5
[dvsadmin@server2 ~]$
```

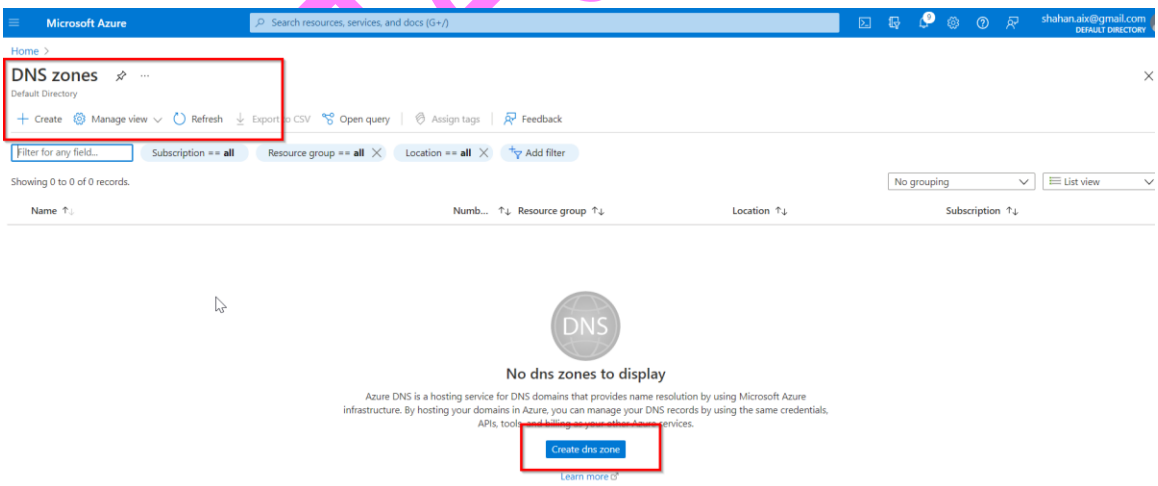
In this way we can configure our own DNS for the systems as we keep on create the servers and it auto configured we no need to add them manually.

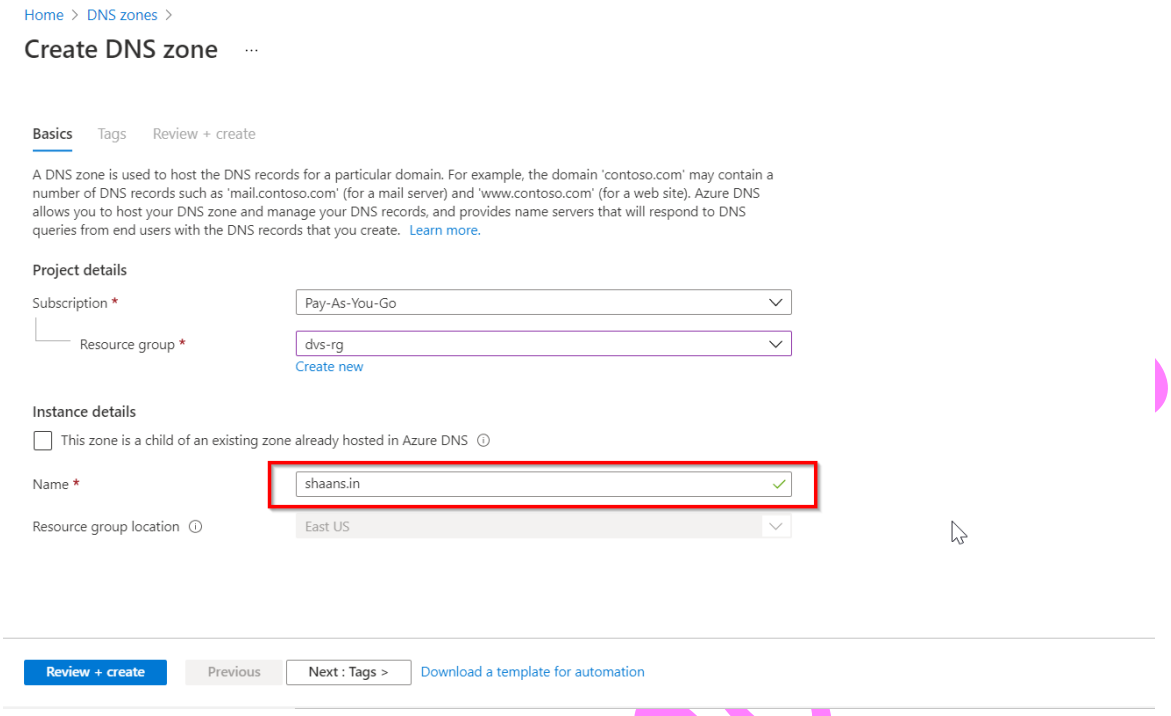
10 Public DNS

If we feel we have the public faced servers/application we can host public zone in azure and remember that you can't purchase domain in azure as of now but you can buy from 3rd party.

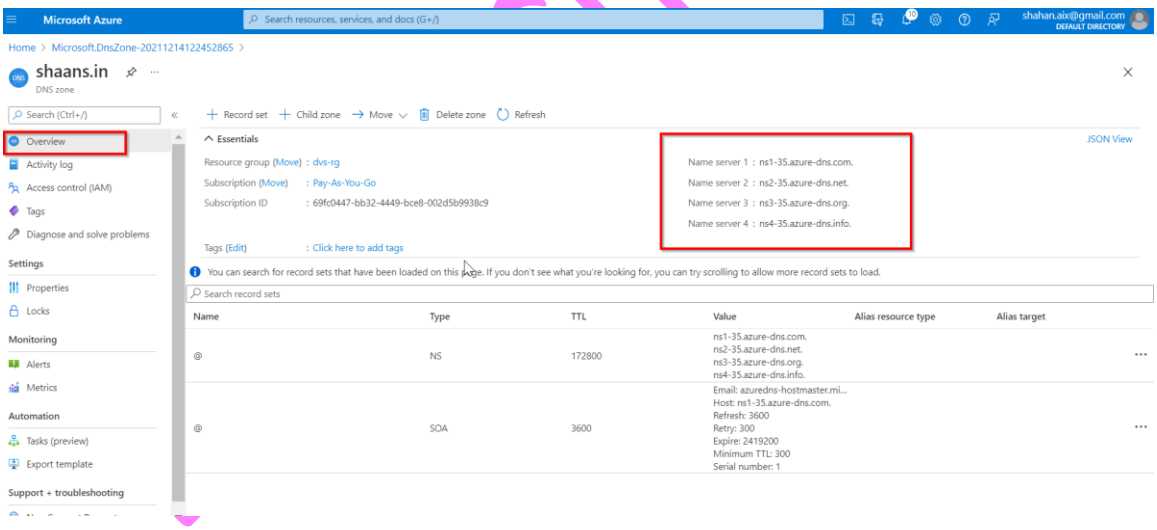
We have a domain "shaans.in" we can configure our domain with azure and try to create few record sets so that we can create and consume the applications from outside world

Creating public dns zone:



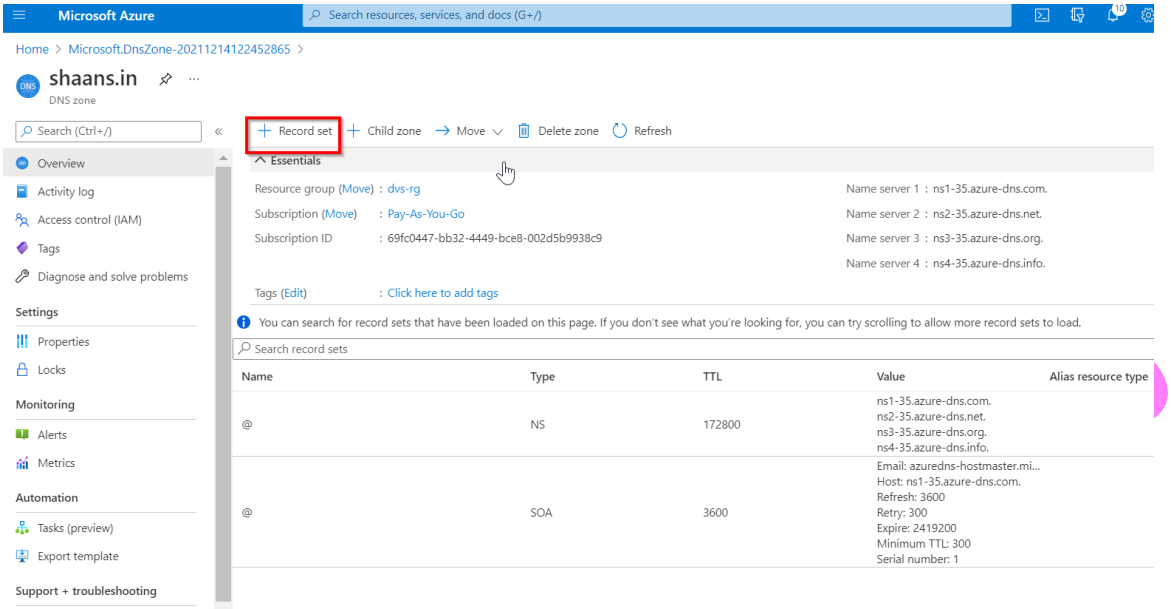


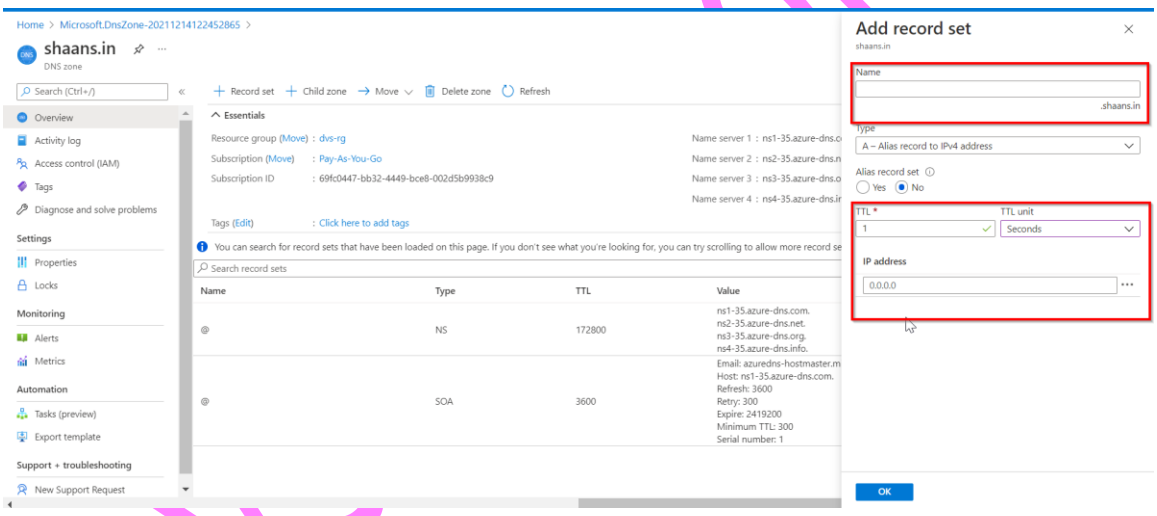
Note: you should have domain shaans.in this will not purchase the domain for you it will just create the space for you to create your records.



Now it generates NS records, just copy these records and go to godaddy & update these nameservers.

Once done you can start creating the record sets in this zone.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft.DnsZone-20211214122452865 >
shaans.in
DNS zone
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Properties
Locks
Monitoring
Alerts
Metrics
Automation
Tasks (preview)
Export template
Support + troubleshooting
Record set
Child zone
Move
Delete zone
Refresh
Essentials
Resource group (Move) : dvs-rg
Subscription (Move) : Pay-As-You-Go
Subscription ID : 69fc0447-bb32-4449-bce8-002d5b9938c9
Tags (Edit) : Click here to add tags
Name server 1 : ns1-35.azure-dns.com.
Name server 2 : ns2-35.azure-dns.net.
Name server 3 : ns3-35.azure-dns.org.
Name server 4 : ns4-35.azure-dns.info.
You can search for record sets that have been loaded on this page. If you don't see what you're looking for, you can try scrolling to allow more record sets to load.
Search record sets
Name
Type
TTL
Value
Alias resource type
@
NS
172800
ns1-35.azure-dns.com.
ns2-35.azure-dns.net.
ns3-35.azure-dns.org.
ns4-35.azure-dns.info.
@
SOA
3600
Email: azuredns-hostmaster.mi...
Host: ns1-35.azure-dns.com.
Refresh: 3600
Retry: 300
Expire: 2419200
Minimum TTL: 300
Serial number: 1


Add record set
shaans.in
Name
.shaans.in
Type
A – Alias record to IPv4 address
Alias record set
Yes
No
TTL *
1
TTL unit
Seconds
IP address
0.0.0.0
OK