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."

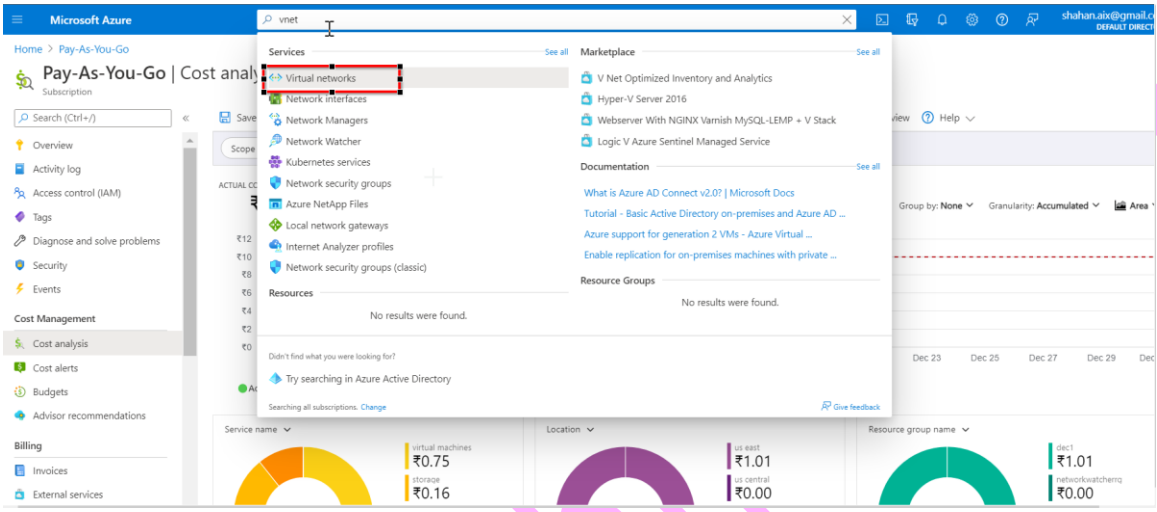
You and your suggestions are valuable to us; Help us to serve you better. In case of any suggestions, grievance, or complaints, please feel free to write us your suggestions, grievance and feedback on the following

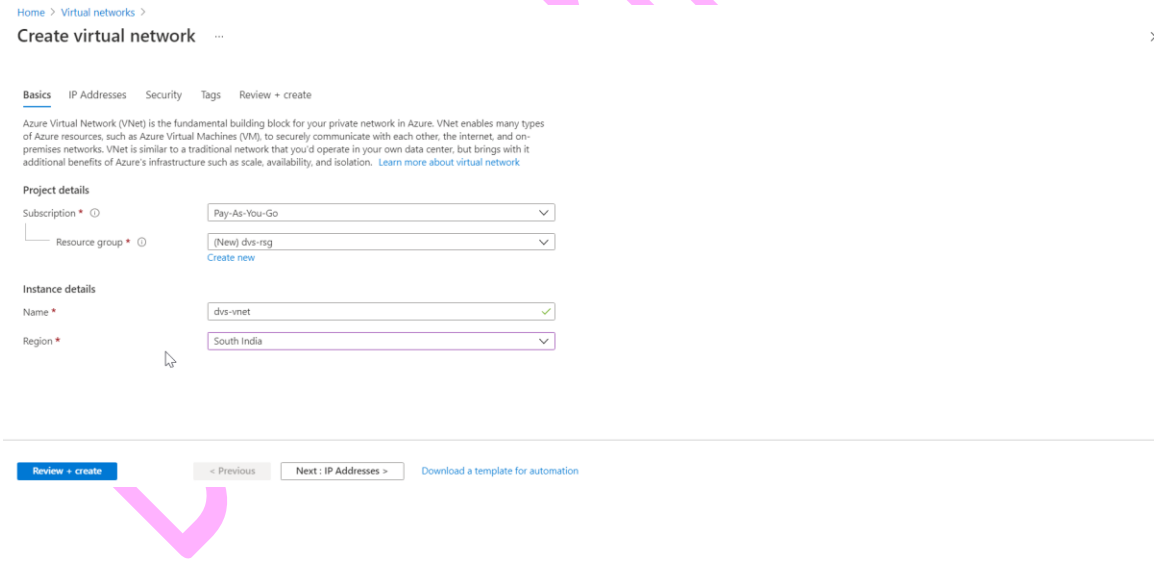
Dvs.training@gmail.com

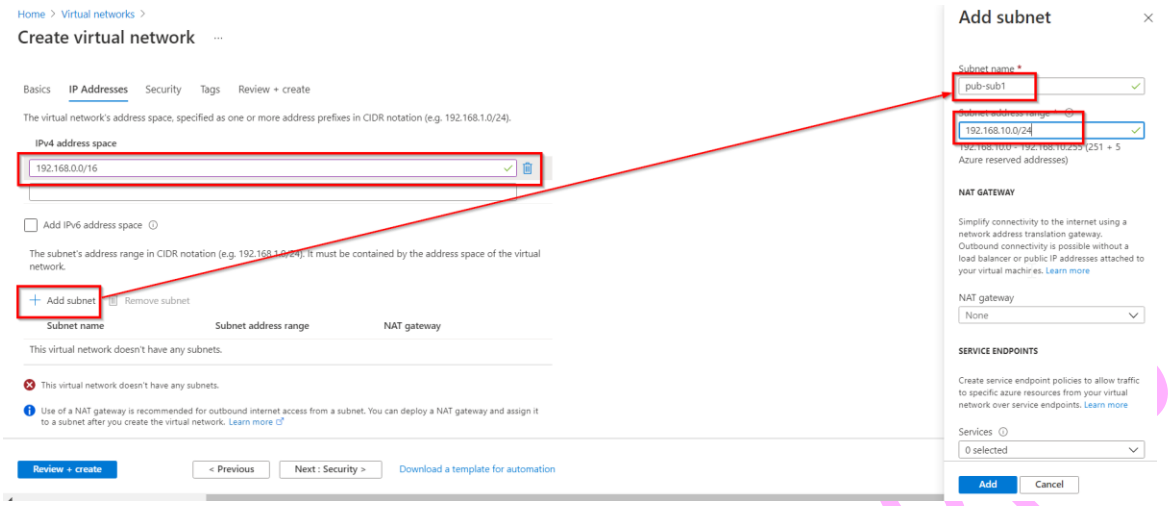
DVS Technologies

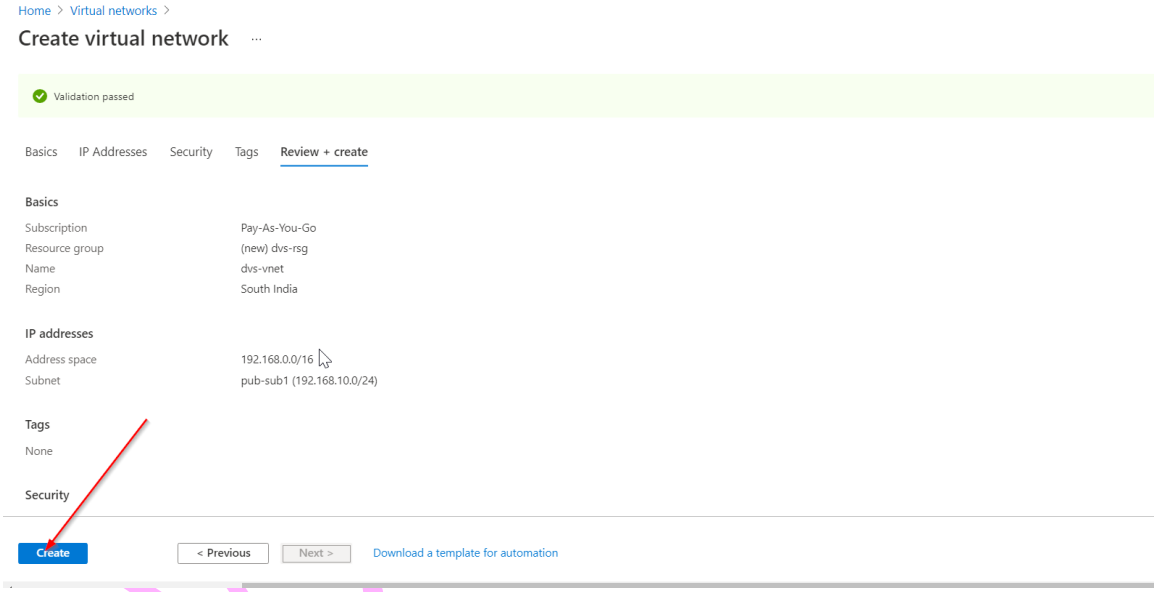
1 Create VNET with subnets

Let's create a VNET and bring up the server from the subnet.

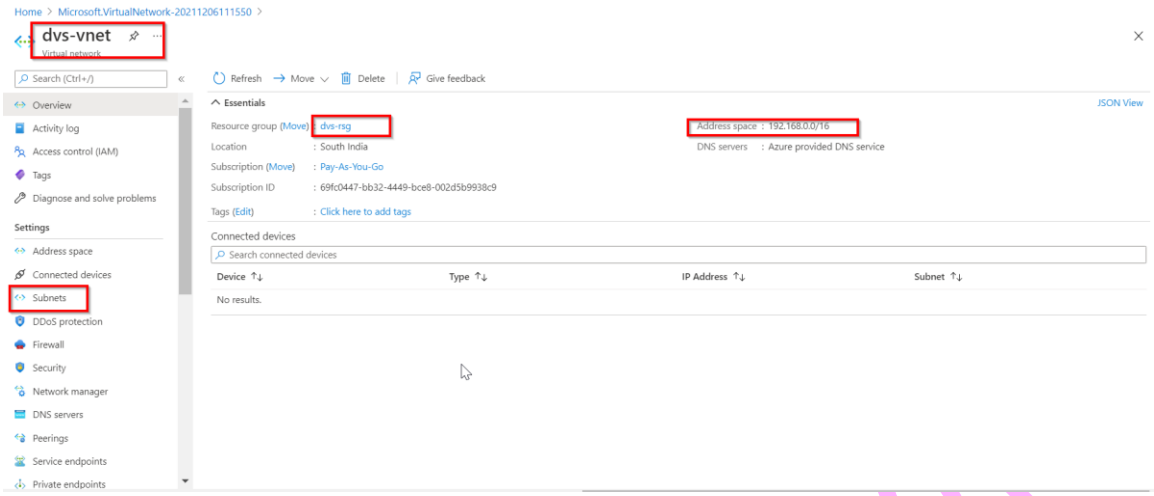


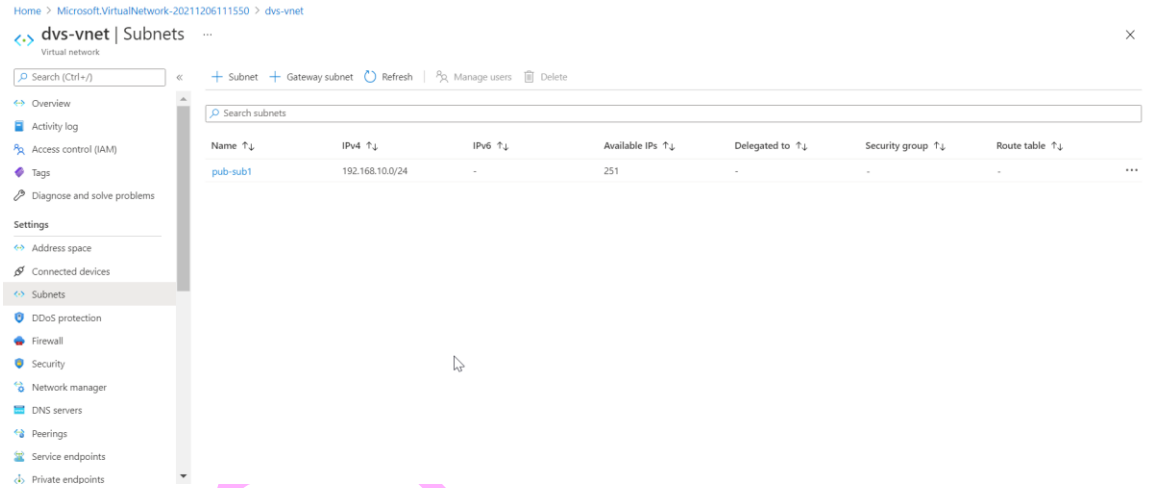






Verifying the VNET configuration:

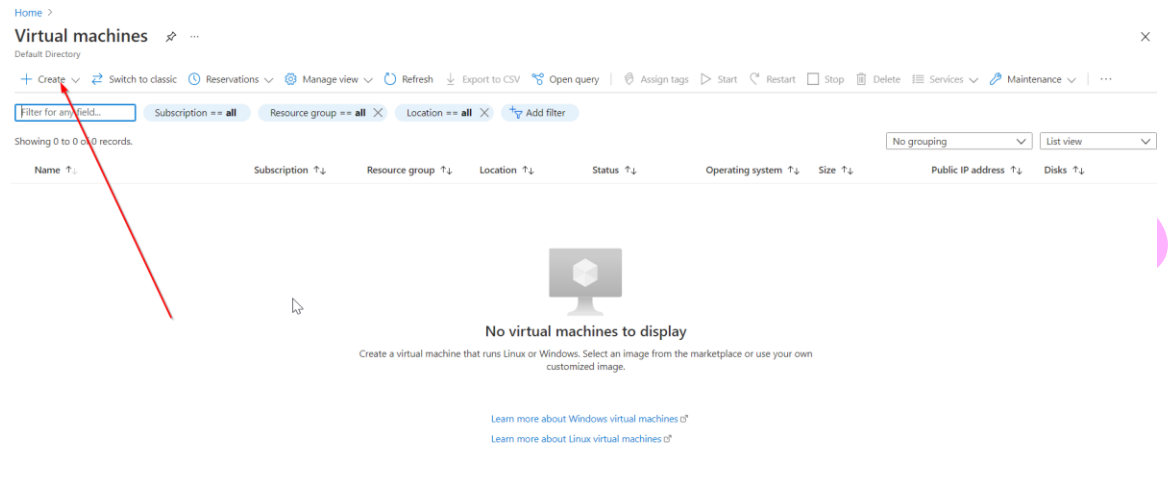


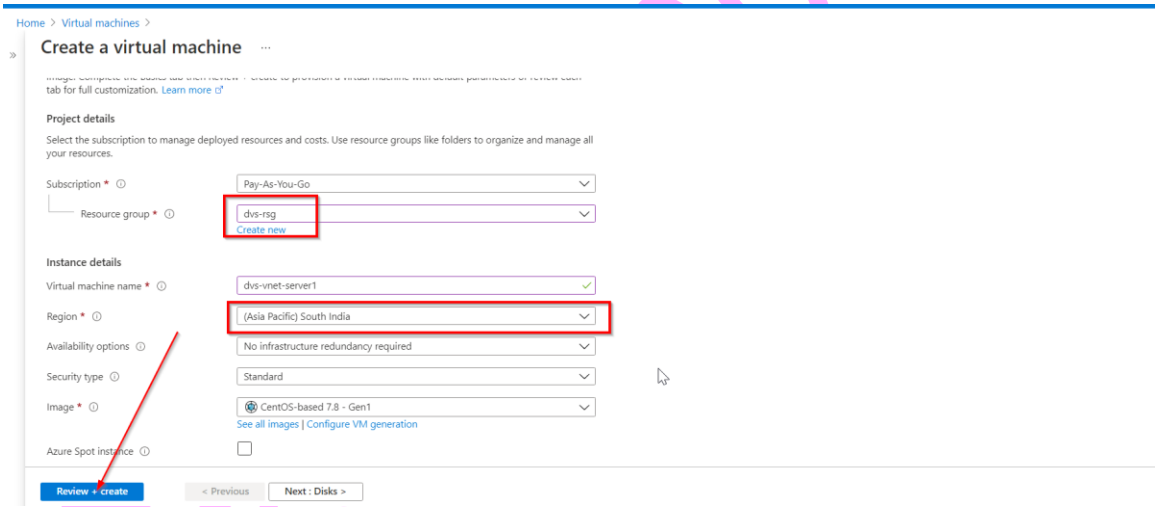


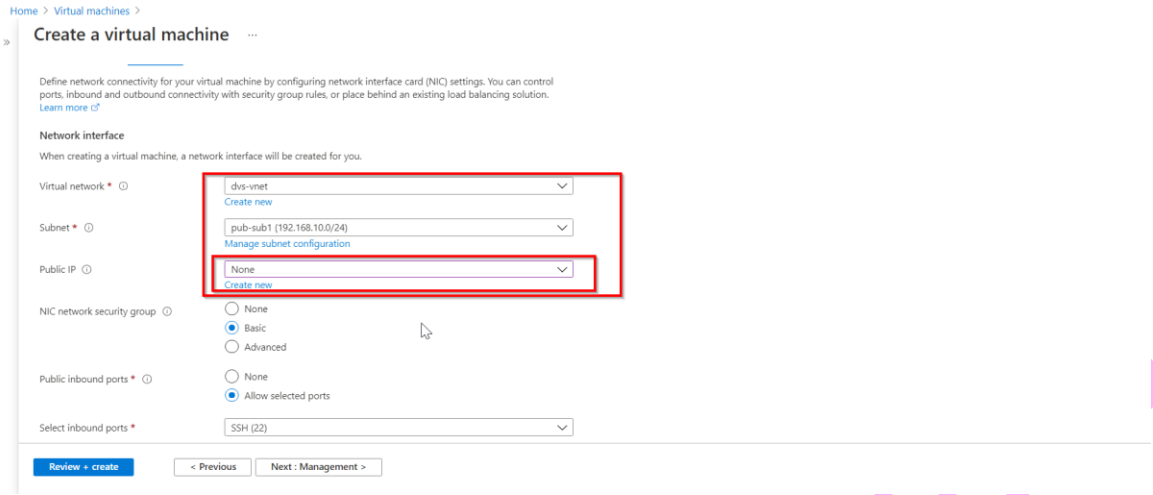
Note: At any point if you want to change the VNET ip address then you can change it before the server creations. Once server creation is done then you can't change the ipaddress allocated.

2 Create a server with subnet

Let's bring up a new server with the ip range 192.168.10.0/24.

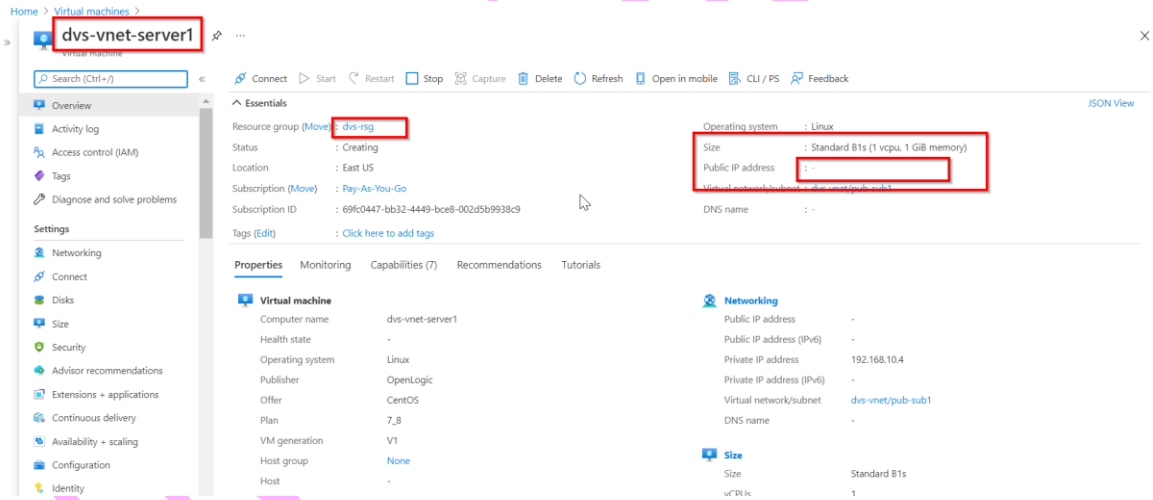






Here we are selecting the network as dvs-net with pub-sub1 and if you observe properly we are not assigning the public ipaddress for this interface.

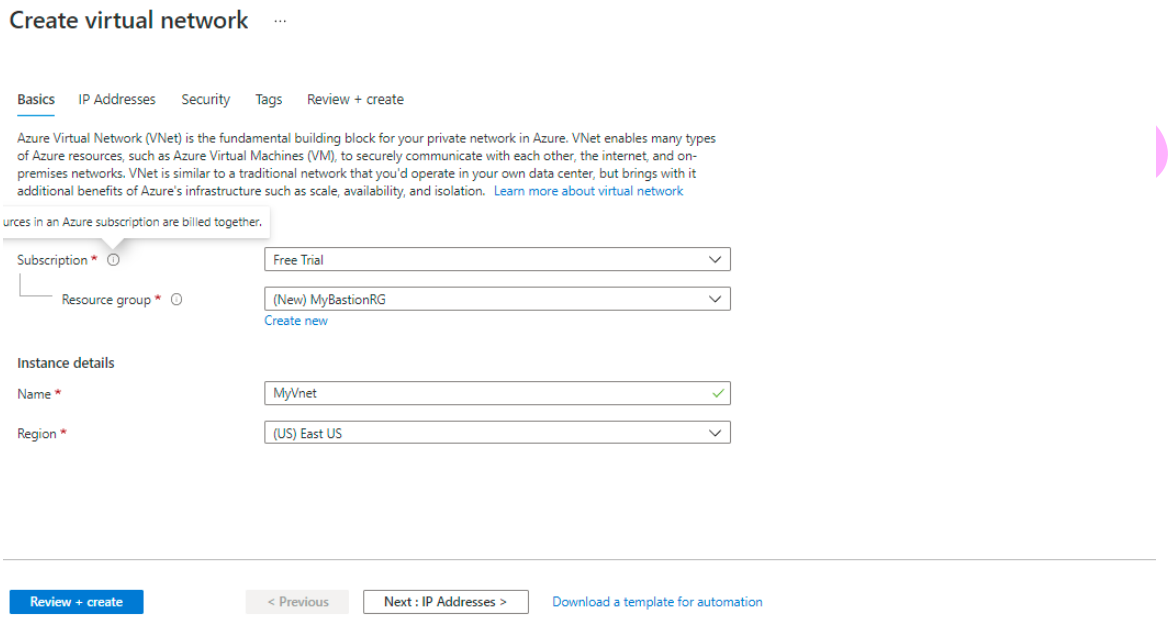
Will add the public ipaddress post server creation.

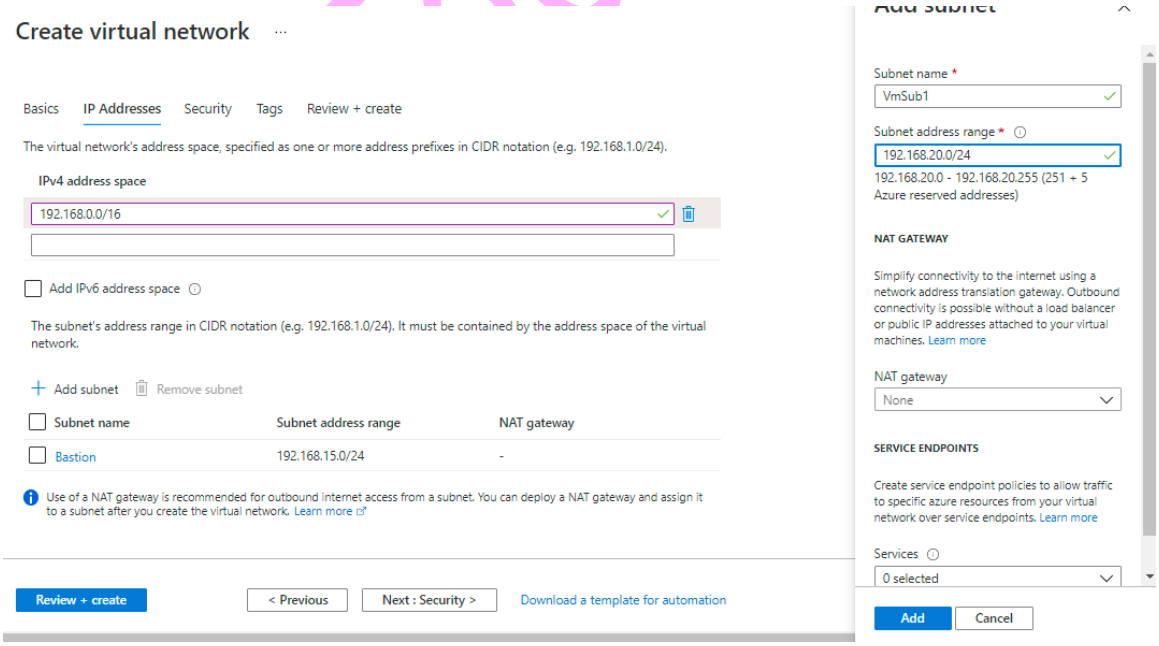


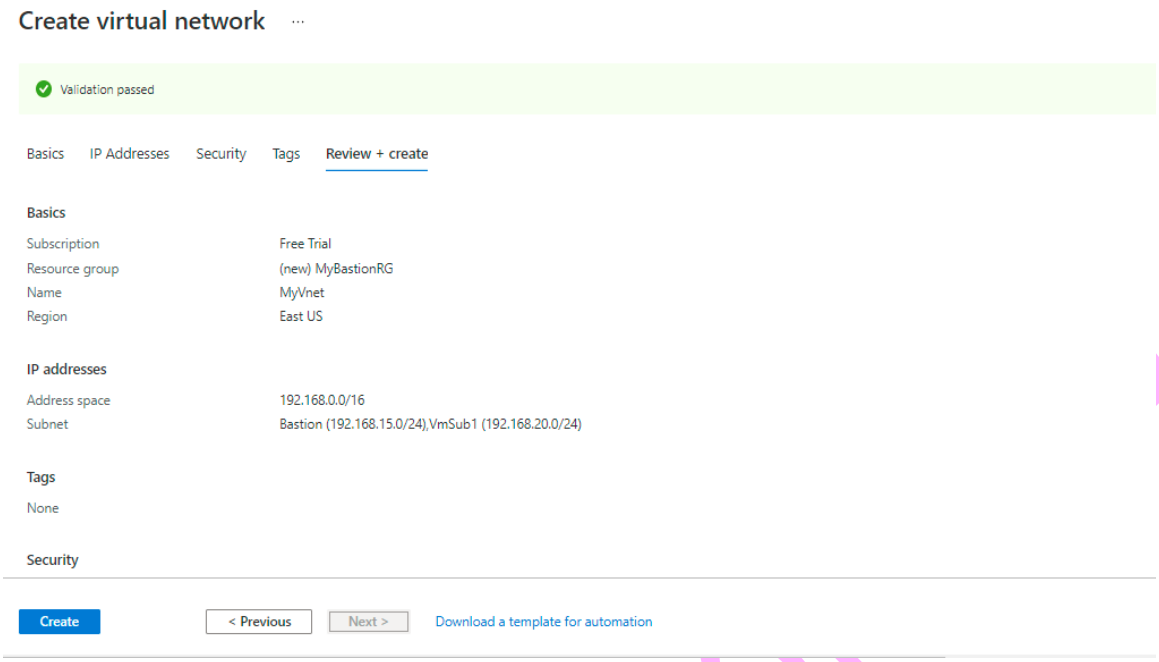
3 Creating Jump or Bastion host

Let's create our Vnet with two subnets one for server and other for Bastion

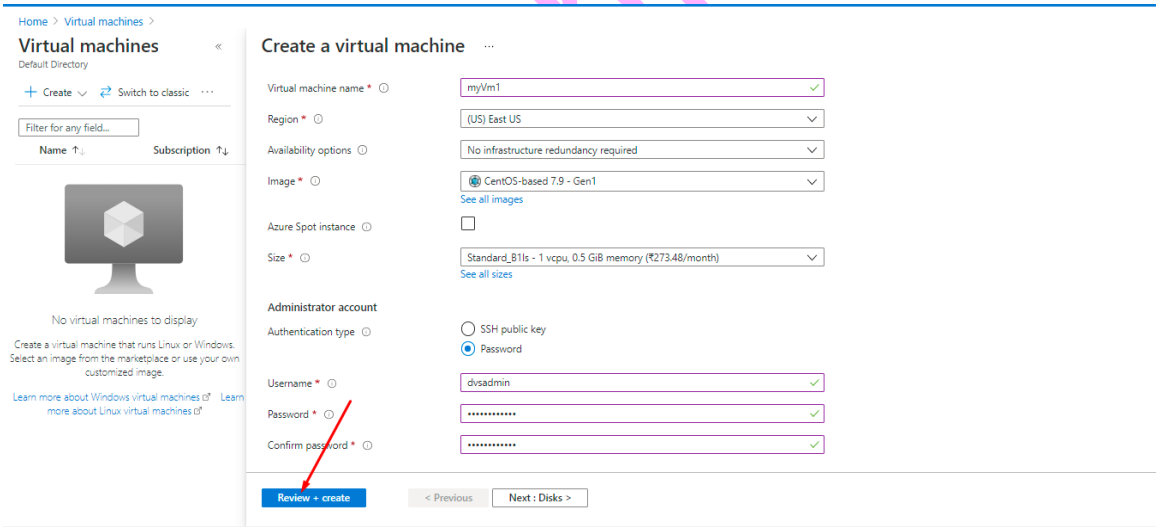
Creating Vnet:

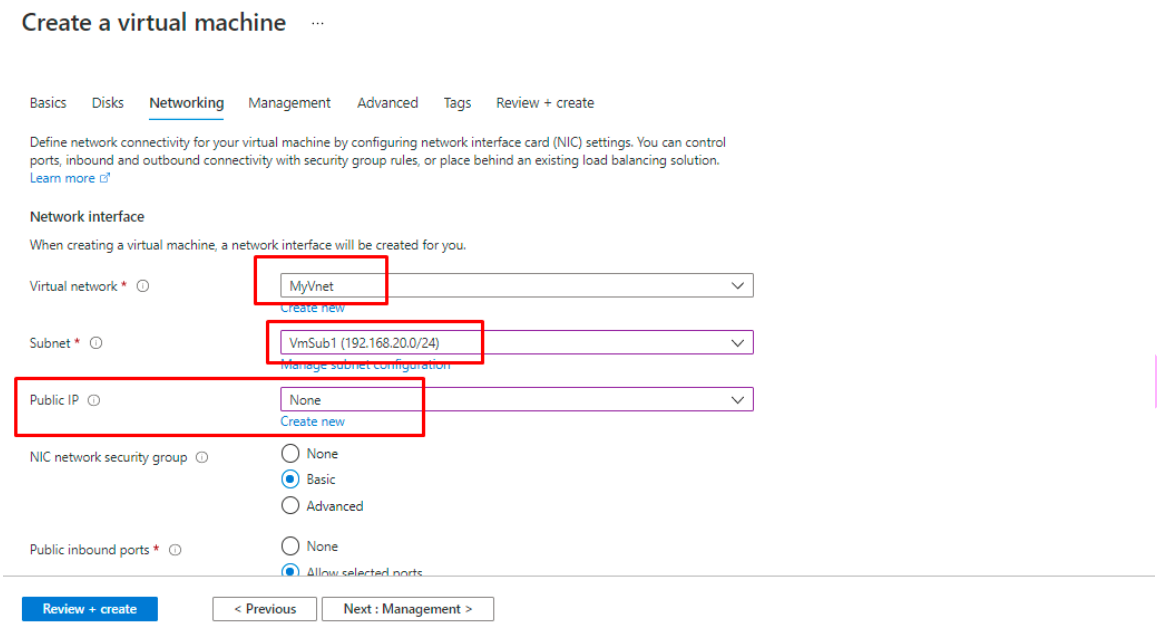




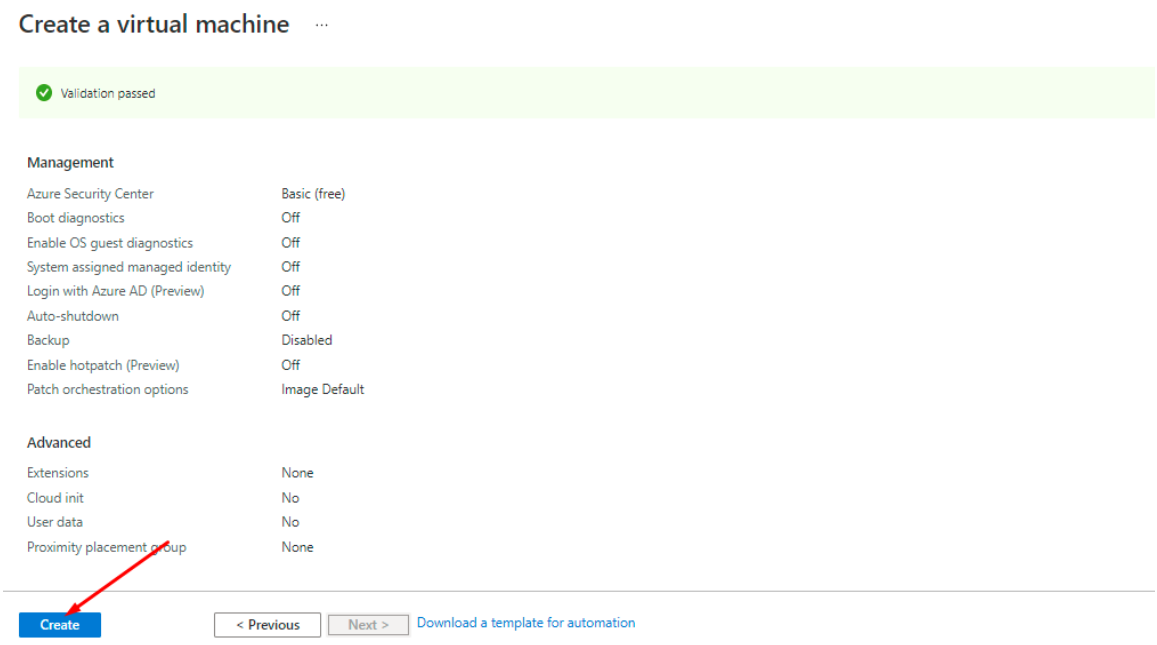


Creating a VM:





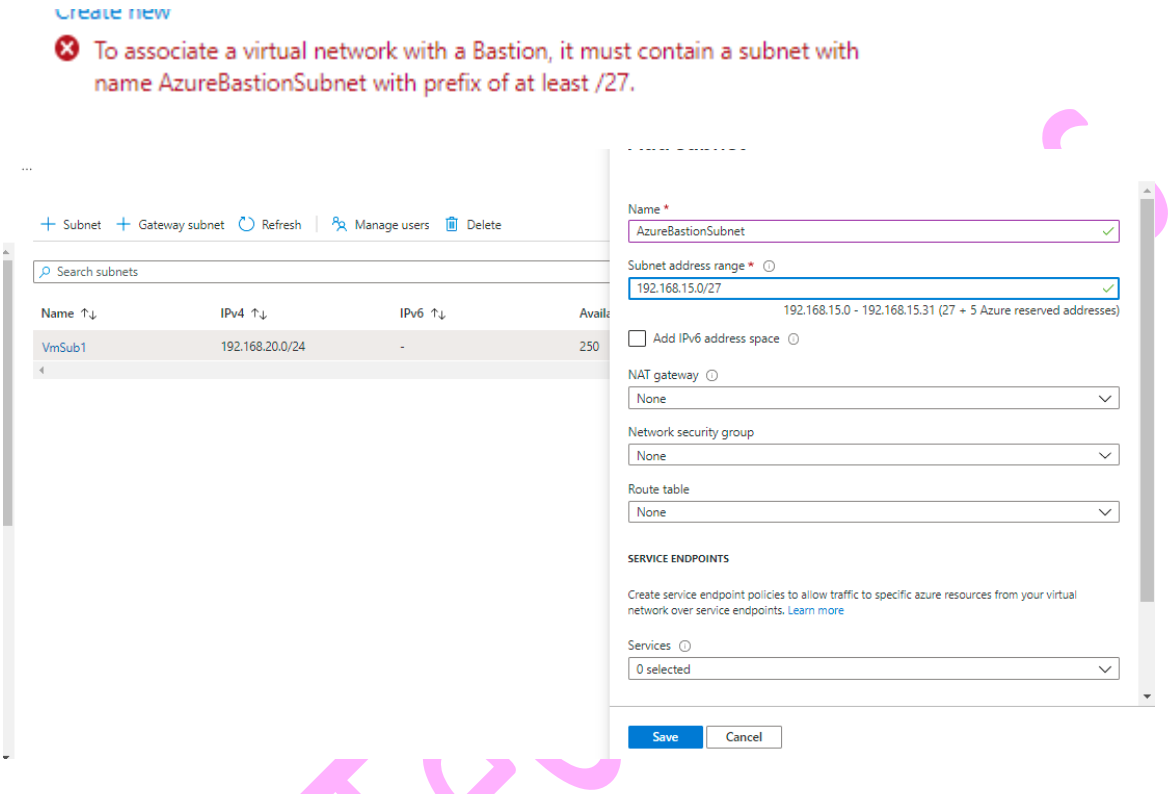
Here we are not allocating the public ipaddress for our server. We are going to connect it via Bastion

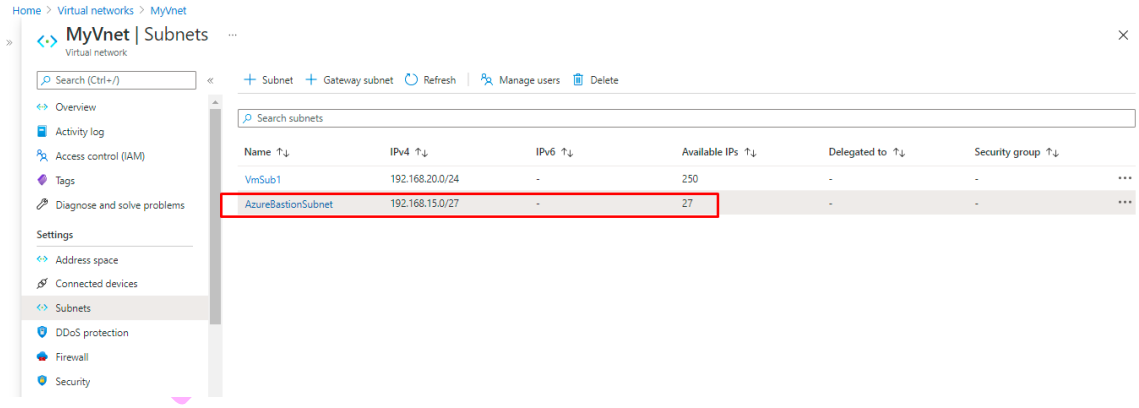


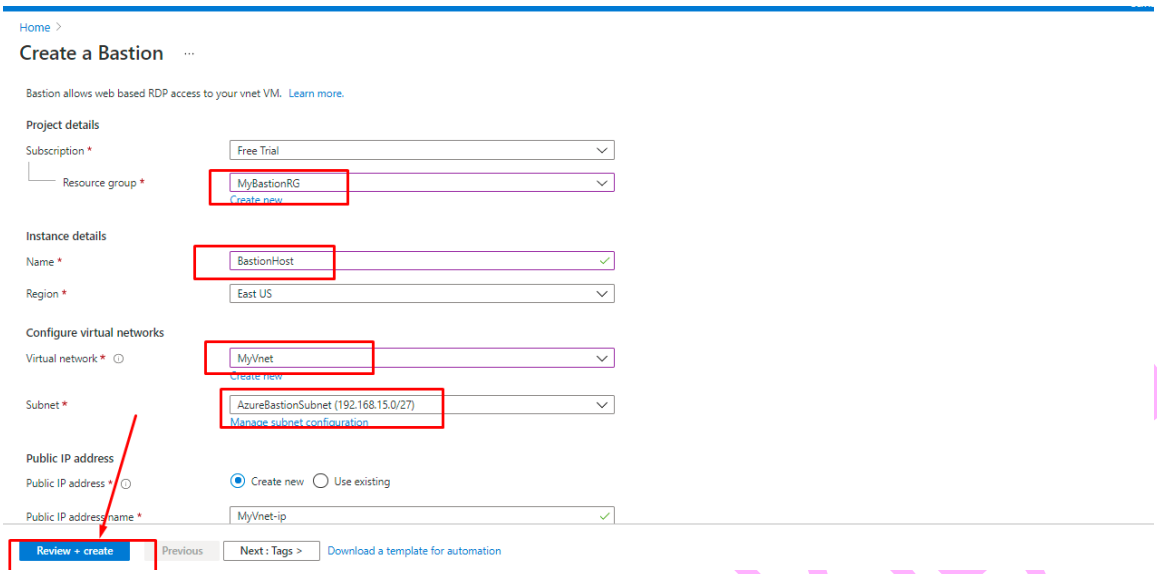
Now our VM is up & running

Let's Create our Bastion Subnet:

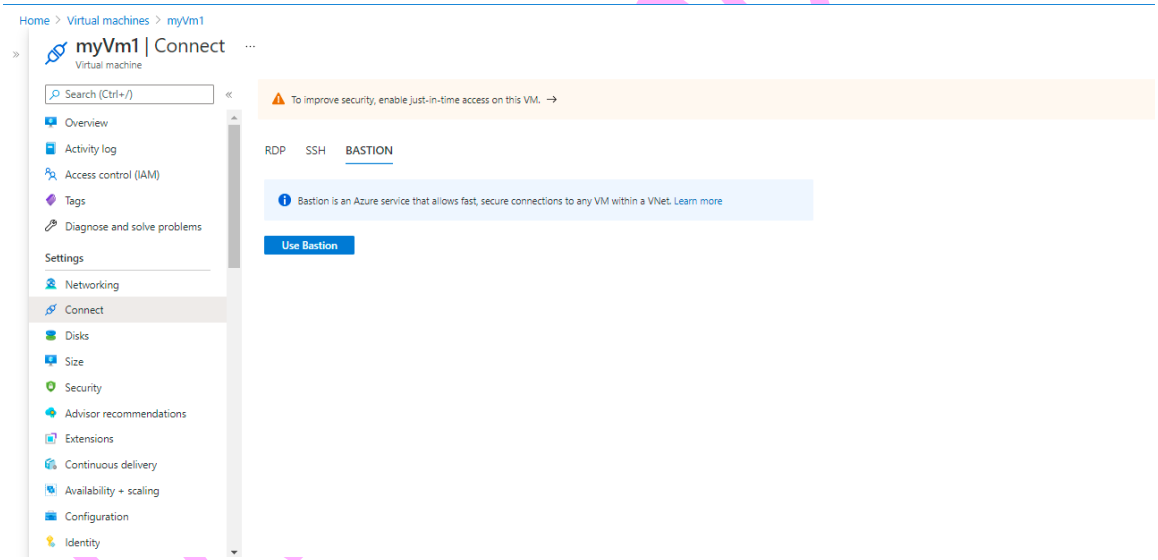
Note: Its subnet should be /26 and bastion subnet should be "AzureBastionSubnet" otherwise you will get error as below







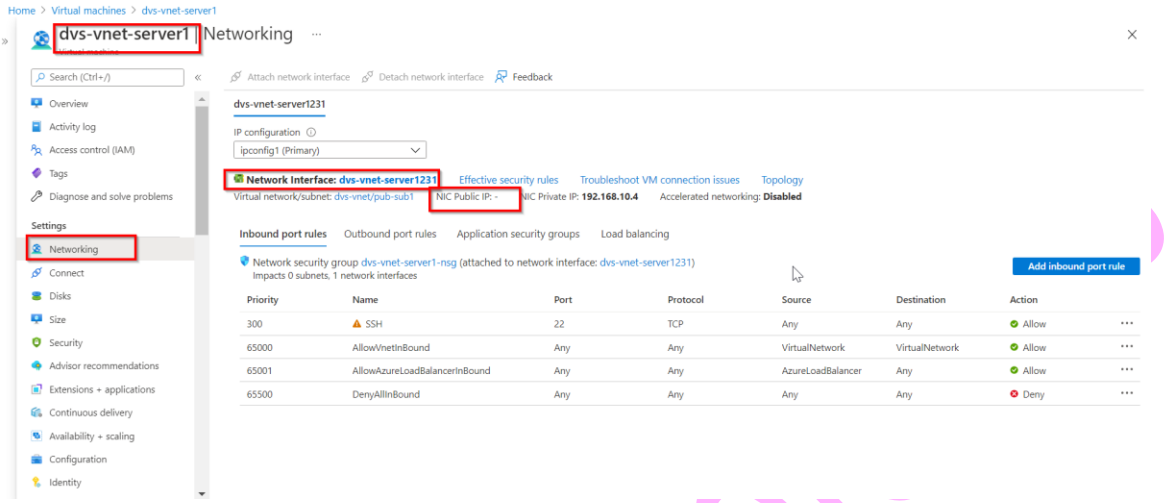
Once done with bastion let's try to login to the server



Just give your username & password & try to login

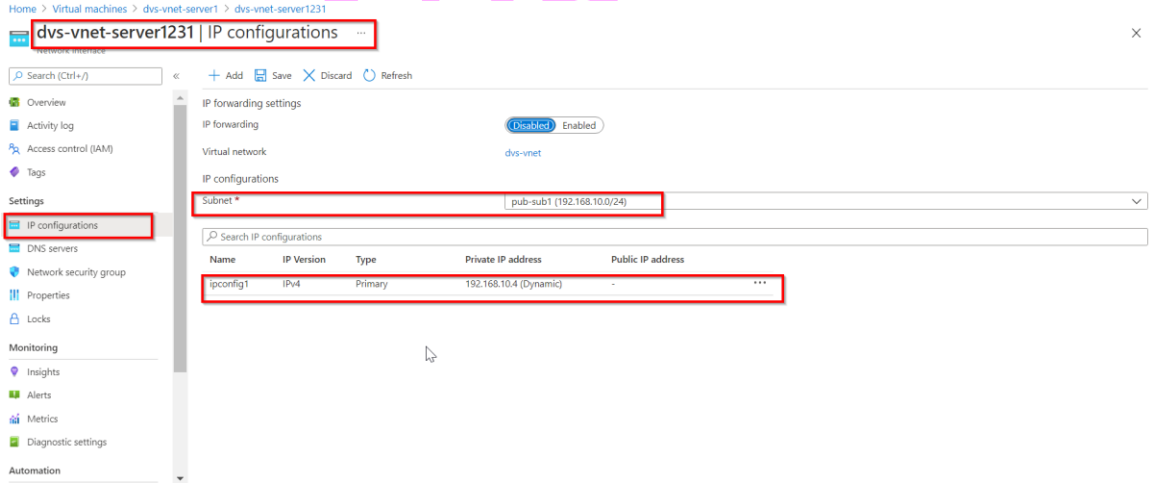
4. Working with static & dynamic public ip's

Now let's provide the public ipaddress for the instance and try to login to the server.



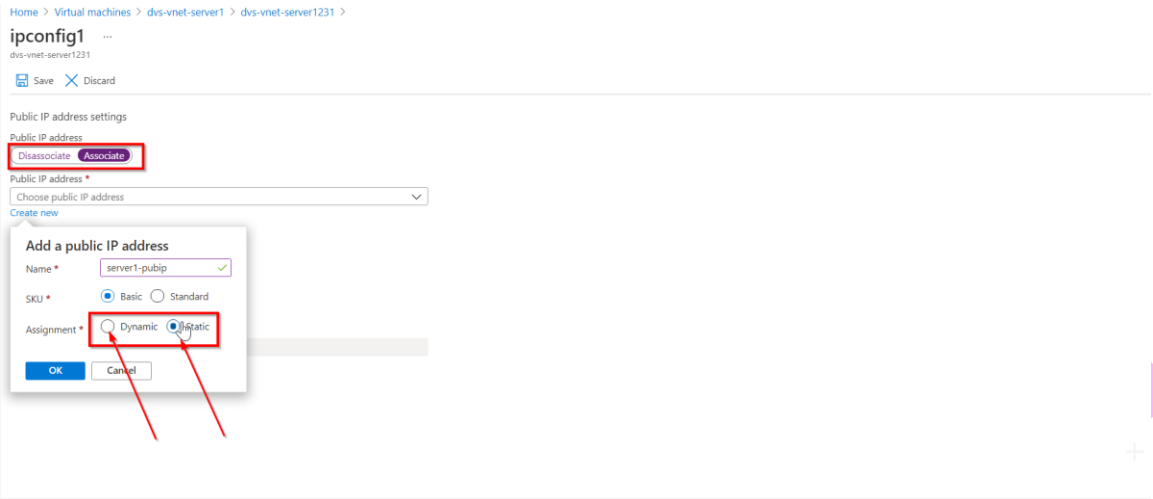
Here for the vm "dvs-vnet-server1" we have a network interface "dvs-vnet-server1231" and it don't have the public ipaddress.

Whenever you want to set the public ipaddress for the network interface then you can simply go that interface and change the allocation type.

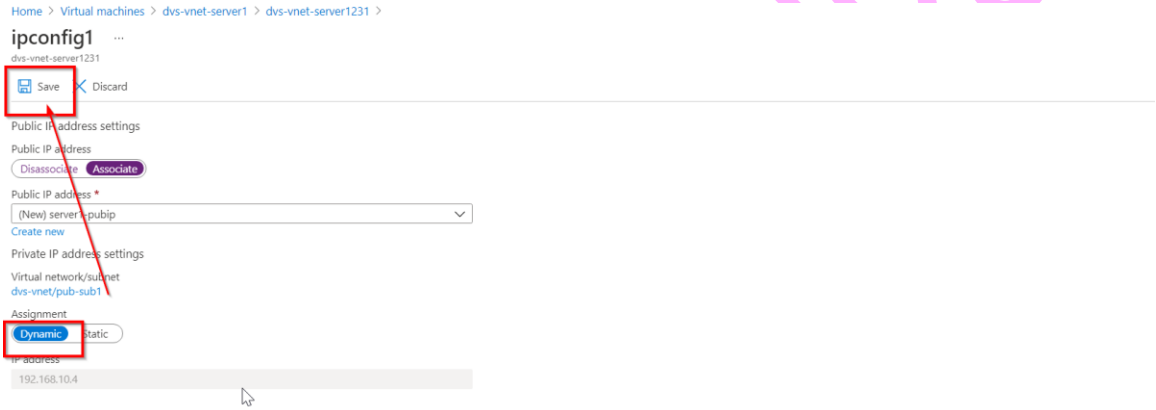


Let's provide the public ipaddress for this machine

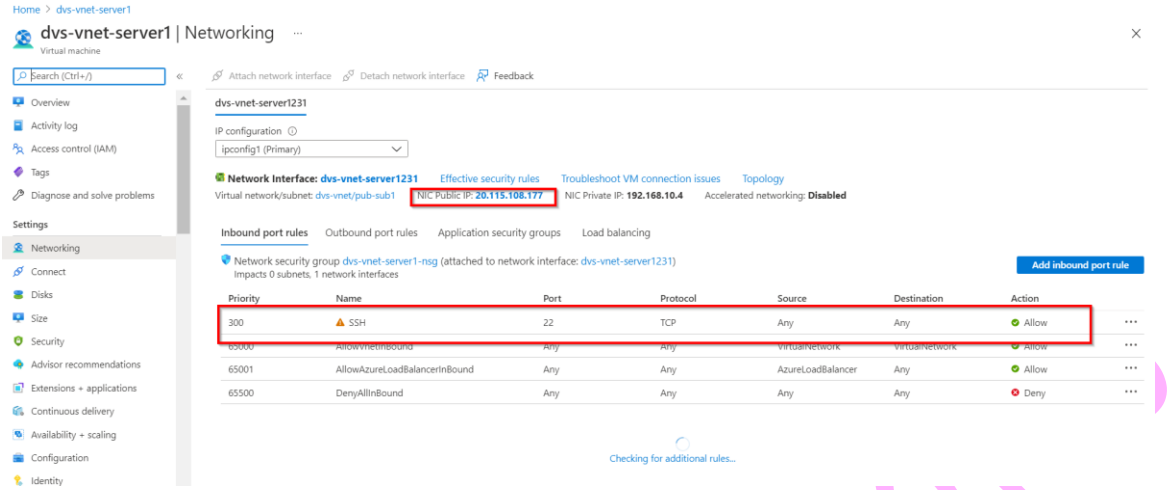
Click on ipconfig



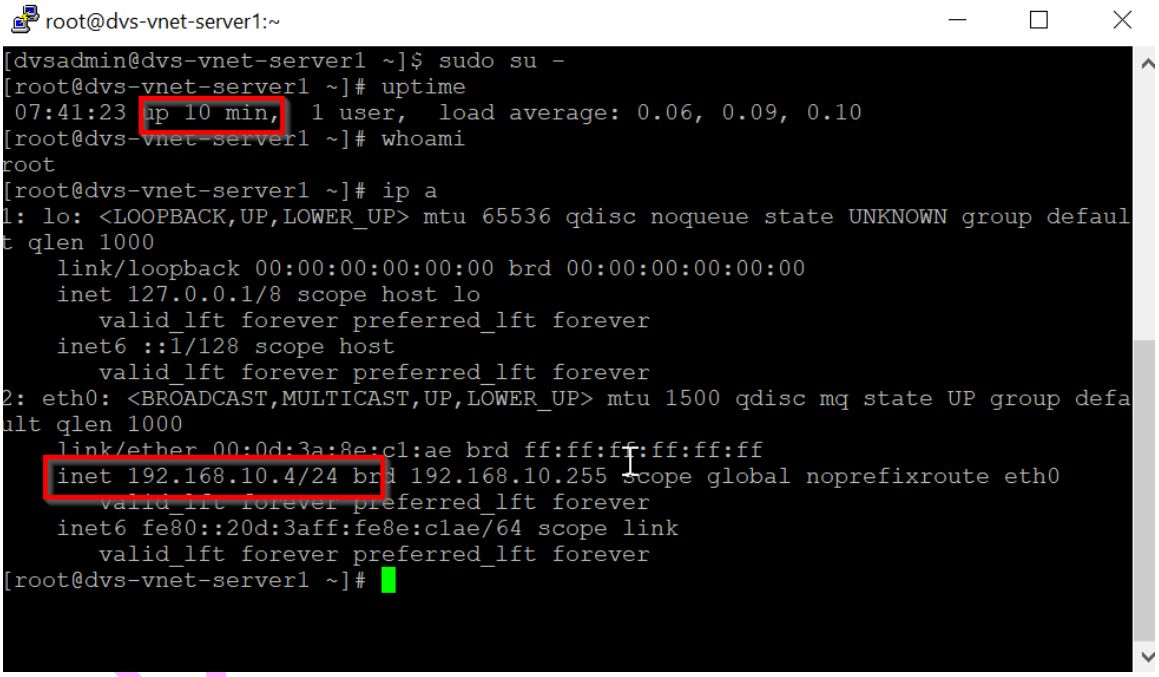
Here if you want to make the ip as static you can do it or as dynamic. It's up to your requirement.



Now let's see if we get public ipaddress for the server or not.



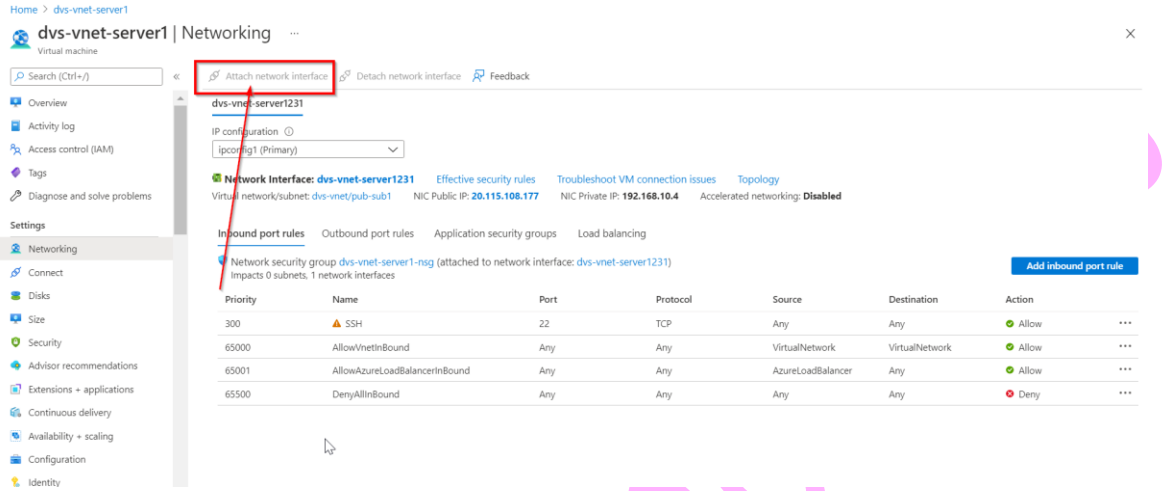
Since port 22 is allowed we should able to access the server via public ip address. Let's connect to the server and check the uptime.



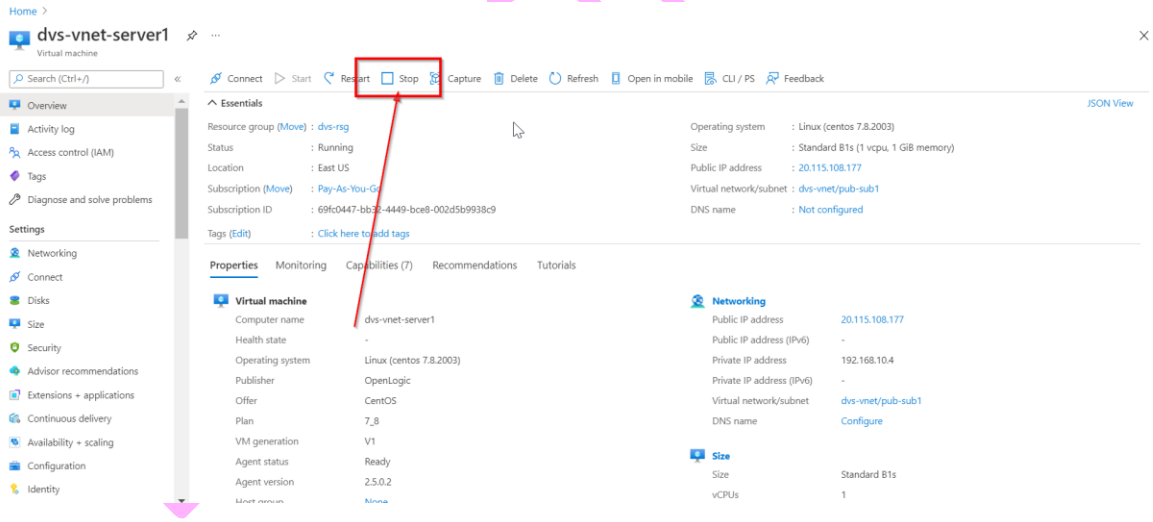
5. Adding 2nd network interface

You need downtime to add a new interface to the existing server.

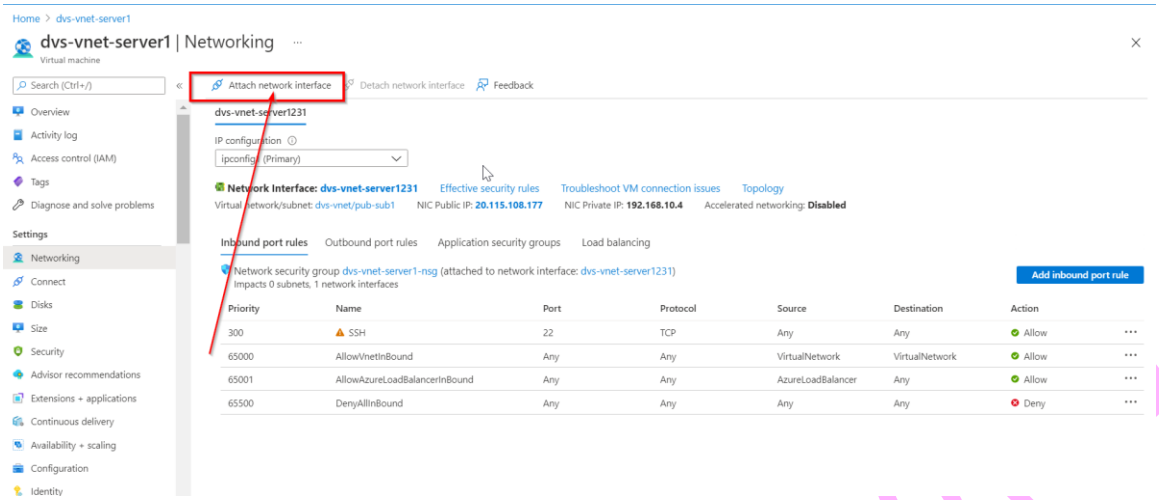
Let's try to add the second interface to the system.

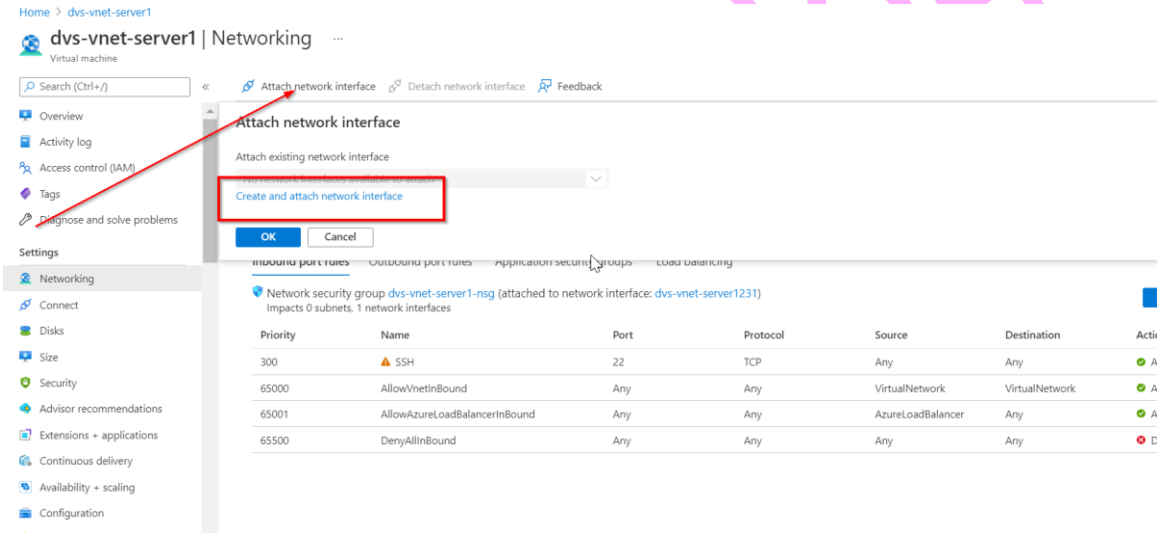


Here since the machine is up and running we see that the option is greyed out. Let's bring down the server and try to add one more interface.



Once the server is down we see the option enabled


Home > dvs-vnet-server1
dvs-vnet-server1 | Networking
Virtual machine
Search (Ctrl+/)
Attach network interface
Detach network interface
Feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Disks
Size
Security
Advisor recommendations
Extensions + applications
Continuous delivery
Availability + scaling
Configuration
Identity
dvs-vnet-server1231
IP configuration
ipconfig1 (Primary)
Network Interface: dvs-vnet-server1231
Effective security rules
Troubleshoot VM connection issues
Topology
Virtual network/subnet: dvs-vnet/pub-sub1
NIC Public IP: 20.115.108.177
NIC Private IP: 192.168.10.4
Accelerated networking: Disabled
Inbound port rules
Outbound port rules
Application security groups
Load balancing
Network security group dvs-vnet-server1-nsg (attached to network interface: dvs-vnet-server1231)
Impacts 0 subnets, 1 network interfaces
Add inbound port rule
Priority
Name
Port
Protocol
Source
Destination
Action
300
SSH
22
TCP
Any
Any
Allow
65000
AllowVnetInBound
Any
Any
VirtualNetwork
VirtualNetwork
Allow
65001
AllowAzureLoadBalancerInBound
Any
Any
AzureLoadBalancer
Any
Allow
65500
DenyAllInBound
Any
Any
Any
Any
Deny


Home > dvs-vnet-server1
dvs-vnet-server1 | Networking
Virtual machine
Search (Ctrl+/)
Attach network interface
Detach network interface
Feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Disks
Size
Security
Advisor recommendations
Extensions + applications
Continuous delivery
Availability + scaling
Configuration
Attach network interface
Attach existing network interface
Create and attach network interface
OK
Cancel
Network security group dvs-vnet-server1-nsg (attached to network interface: dvs-vnet-server1231)
Impacts 0 subnets, 1 network interfaces
Priority
Name
Port
Protocol
Source
Destination
300
SSH
22
TCP
Any
Any
65000
AllowVnetInBound
Any
Any
VirtualNetwork
VirtualNetwork
65001
AllowAzureLoadBalancerInBound
Any
Any
AzureLoadBalancer
Any
65500
DenyAllInBound
Any
Any
Any
Any

Home > dvs-vnet-server1 >

Create network interface

Project details

Subscription
Pay-As-You-Go

Resource group *
dvs-rsg
Create new

Location
(US) East US

Network interface

Name *
svr1-interface2

Virtual network
dvs-vnet

Subnet *
pub-sub1 (192.168.10.0/24)

NIC network security group
None

Create

Home > dvs-vnet-server1

dvs-vnet-server1 | Networking

Virtual machine

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings

Networking
Connect
Disks
Size
Security
Advisor recommendations
Extensions + applications
Continuous delivery
Availability + scaling
Configuration
Identity

Attach network interface | Detach network interface | Feedback

dvs-vnet-server1231 | svr1-interface2

IP configuration
ipconfig1 (Primary)

Network Interface: dvs-vnet-server1231 | Effective security rules | Troubleshoot VM connection issues | Topology

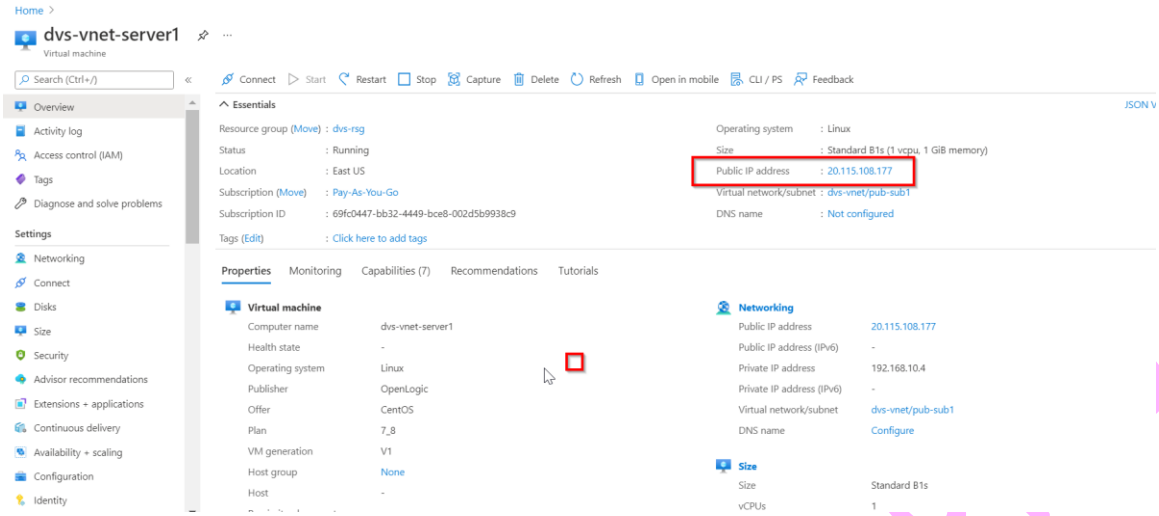
Virtual network/subnet: dvs-vnet/pub-sub1 | NIC Public IP: **20.115.108.177** | NIC Private IP: **192.168.10.4** | Accelerated networking: **Disabled**

Inbound port rules | Outbound port rules | Application security groups | Load balancing

Network security group dvs-vnet-server1-nsg (attached to network interface: dvs-vnet-server1231)
Impacts 0 subnets, 1 network interfaces

Add inbound port ru

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny



Now let's check how many ip's the system have

root@dvs-vnet-server1:~

```
[root@dvs-vnet-server1 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0d:3a:8e:c1:ae brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.4/24 brd 192.168.10.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20d:3aff:fe8e:c1ae/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:22:48:2a:cc:1a brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.5/24 brd 192.168.10.255 scope global noprefixroute eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::bcf6:4639:6f8d:d3b8/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@dvs-vnet-server1 ~]#
```

If you observe we see two interfaces to the same server.

6 Network security group at interface

NSG you can assign it a single server or to an entire subnet

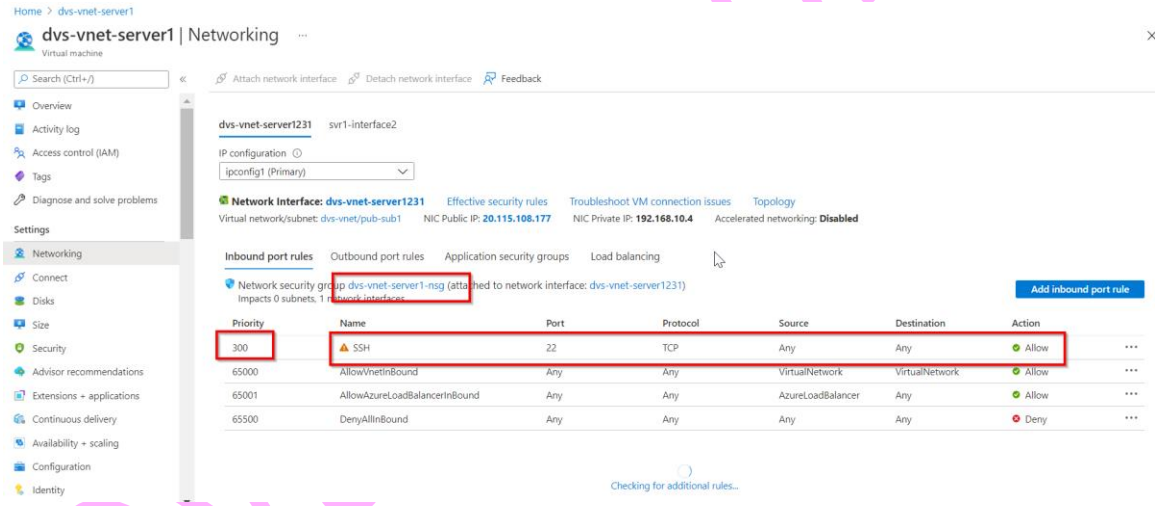
You can't change/delete the default rules

Explain about priority

Let's verify the connectivity with NSG and with out NSG rule

```
       valid_lft forever preferred_lft forever
[root@dvs-vnet-server1 ~]# uptime
 08:06:46 up 5 min,  1 user,  load average: 0.03, 0.25, 0.15
[root@dvs-vnet-server1 ~]#
```

I can connect to the server as port 22 is allowed to access the server.



Here "dvs-vnet-server1-nsg" is our network security group where we see port 22 is allowed for anyone hence we can able to access the server. Now let me delete the rule and see if the access works or not.

```
[redacted]:~$ ssh dvsadmin@20.115.108.177
```

Now it won't work. Please make a note that NSG works based on the priority value the less the value you give the more the priority it have.

7 Network security group at subnet level

NSG at subnet level have more priority than NSG at server level

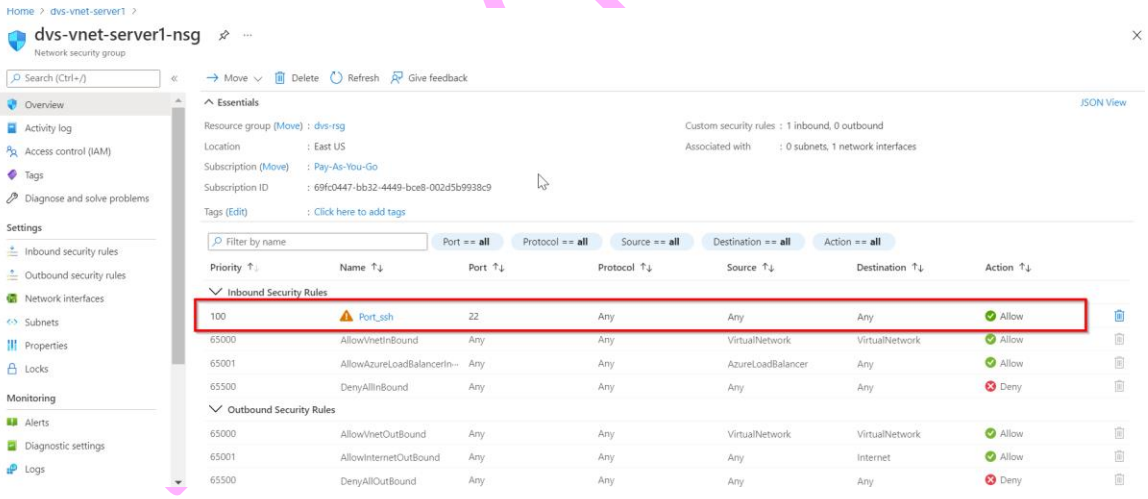
Create a server and then attach one NSG with port 80 allowed
Then add one new NSG at subnet level and don't allow port 80. Check what will happen

Note: If you don't give the NSG then you are allowing all traffic on to your server

Now let's test this connectivity by giving NSG at the server level & create NSG at the subnet level. NSG at the subnet level will have more priority than the NSG at server level.

Test1:
create NSG at subnet & server level. Then allow port 22at both levels.

Allowed port 22 at the NSG server level.

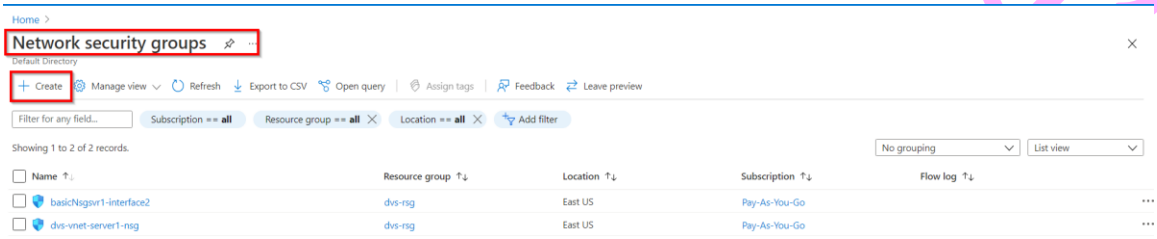


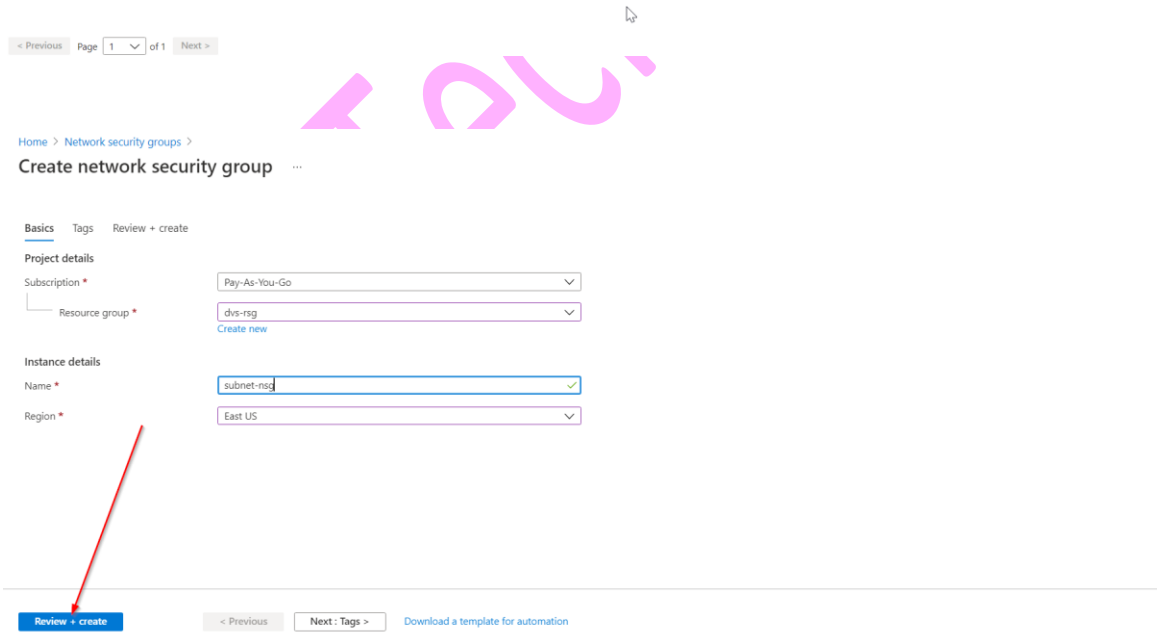
Let's try to login

```
shahan.shaik@ubuntu-tpl:~$ ssh dvsadmin@20.115.108.177
dvsadmin@20.115.108.177's password:
Last login: Mon Dec  6 08:03:58 2021 from 207.254.25.36
[dvsadmin@dvs-vnet-server1 ~]$ uptime
 08:27:03 up 25 min,  1 user,  load average: 0.00, 0.01, 0.05
[dvsadmin@dvs-vnet-server1 ~]$
```

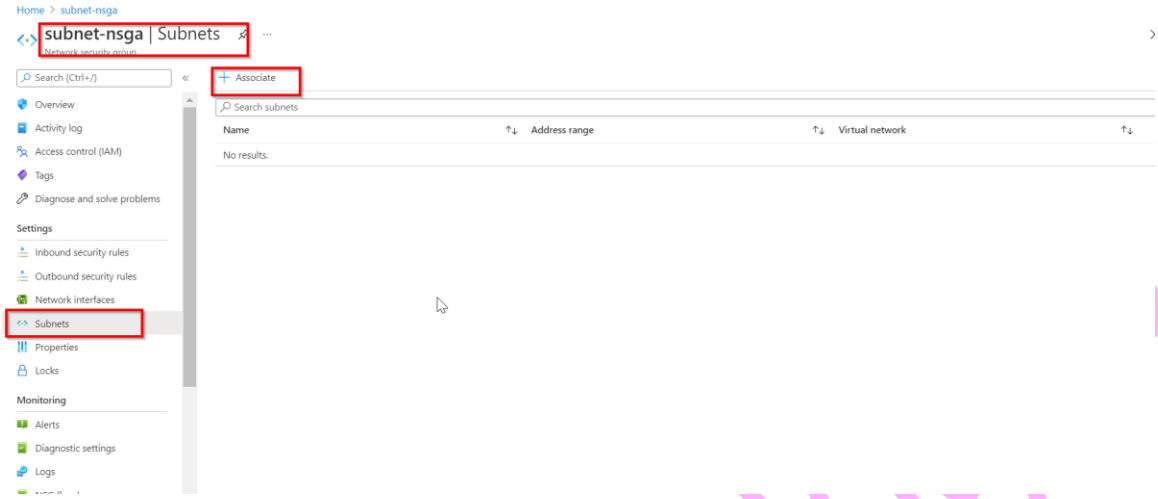
Now it works.

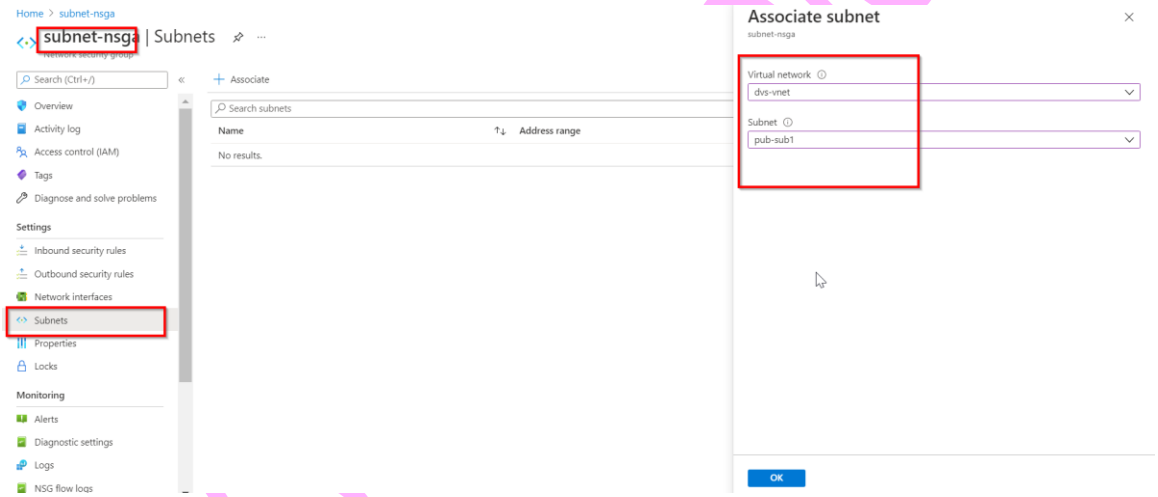
Let's create NSG at the subnet level and try to allow port 22



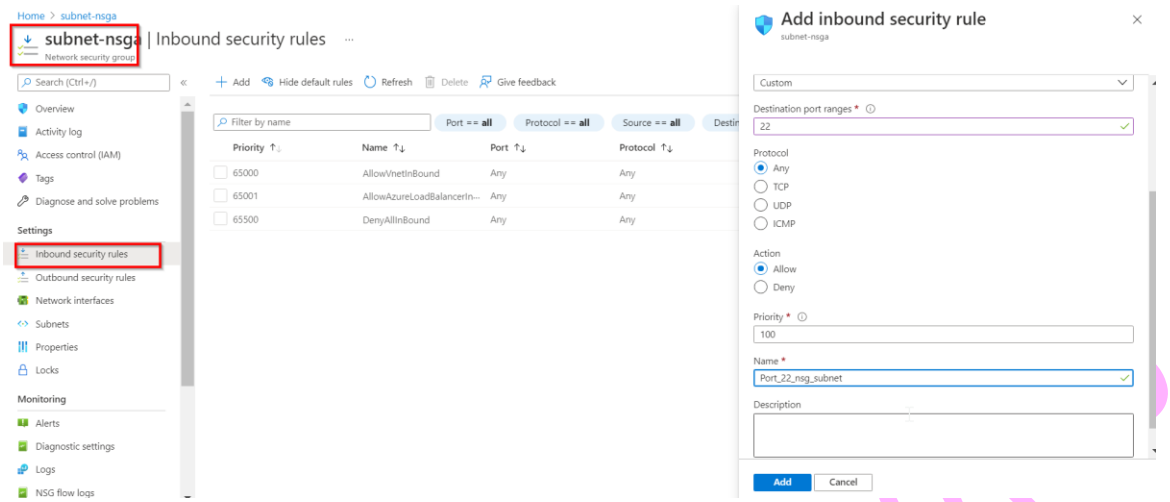


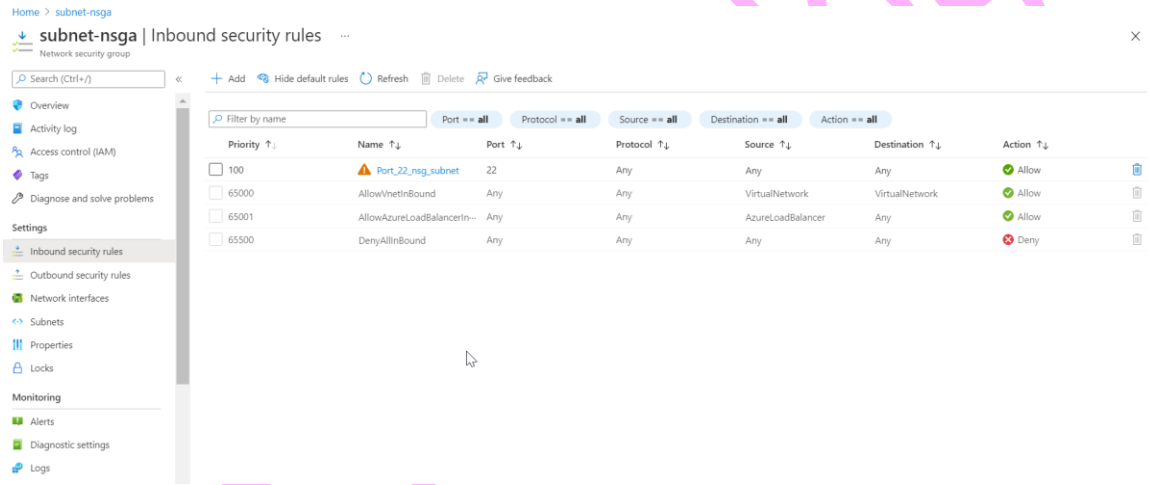
Let's attach this one to the subnet





Let's allow port 22 from NSG subnet level & try to access the server.

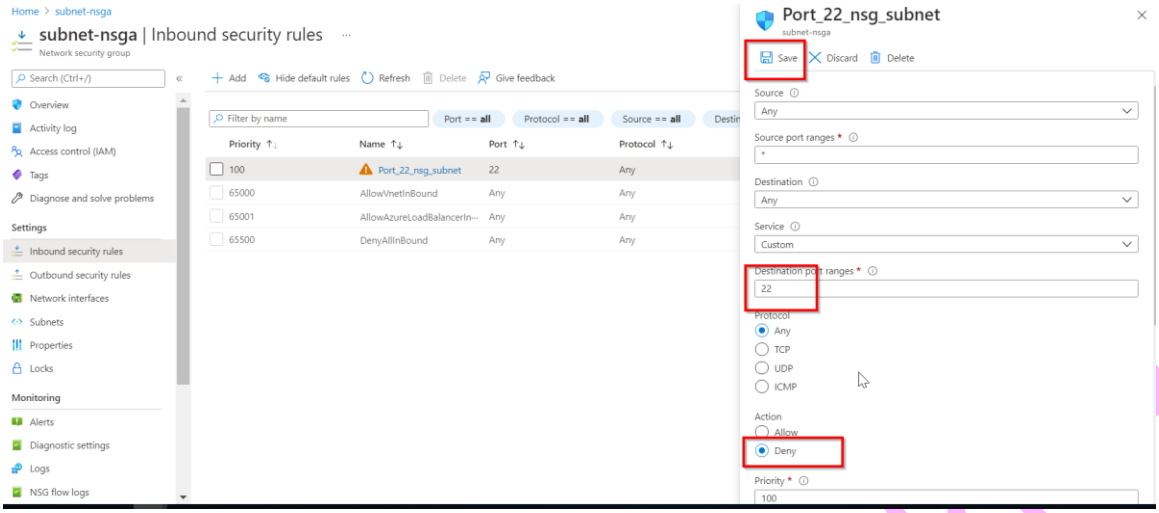


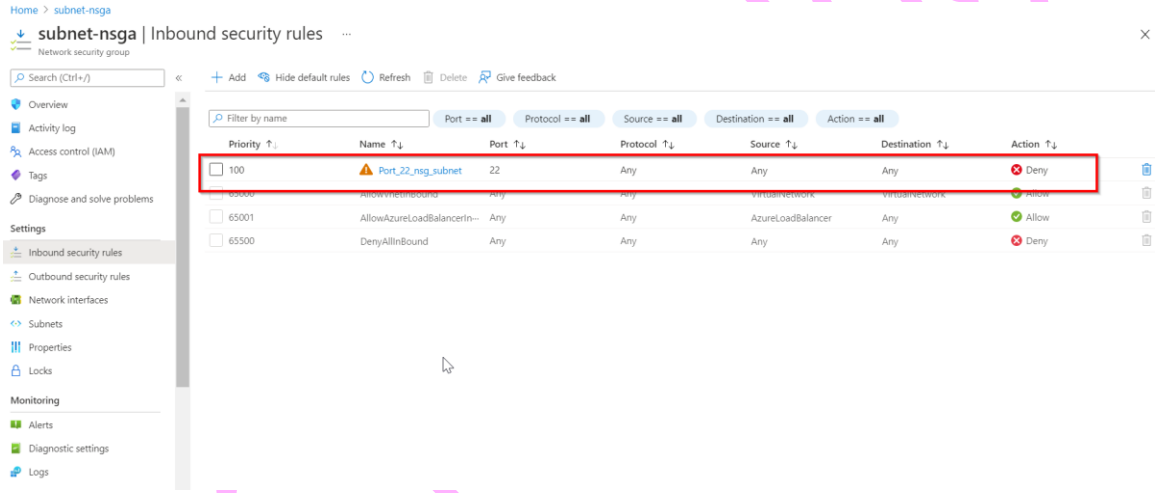


Now let's test the connectivity.

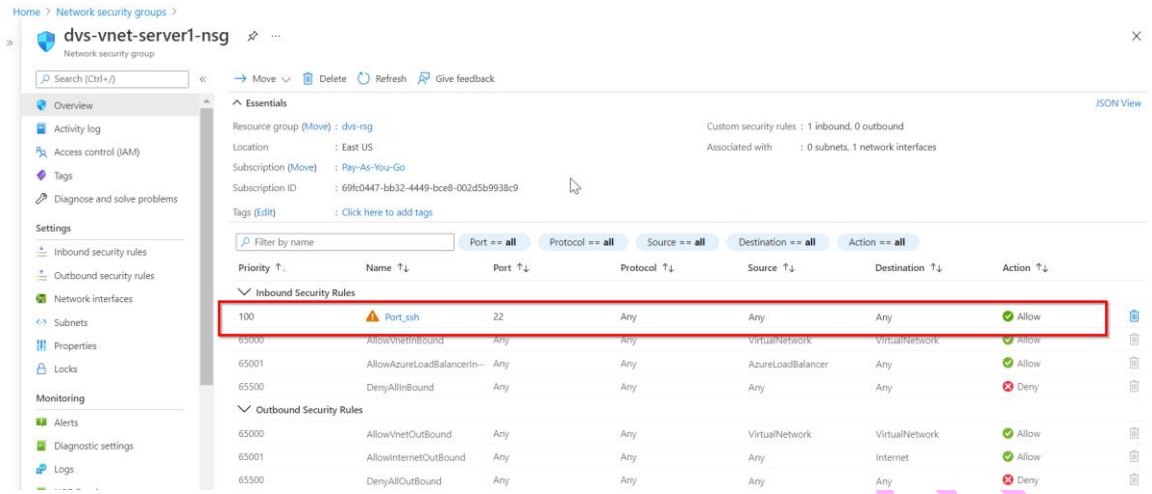
```
shahan.shaik@ubuntu-tpl:~$ ssh dvsadmin@20.115.108.177
dvsadmin@20.115.108.177's password:
Last login: Mon Dec  6 08:26:59 2021 from 207.254.25.36
[dvsadmin@dvs-vnet-server1 ~]$ uptime
 08:43:36 up 41 min,  1 user,  load average: 0.00, 0.03, 0.05
[dvsadmin@dvs-vnet-server1 ~]$
```

Now let's block the port at the subnet NSG then check the connectivity.





Here port 22 is blocked by NSG-subnet level let's test the connectivity now.



Here we allowed at NSG of server

```
shahan.shaik@ubuntu-tpl:~$ ssh dvsadmin@20.115.108.177
```

Here if you see the connectivity it's not working. Hence we can say that subnet NSG have more priority than NSG at server level.

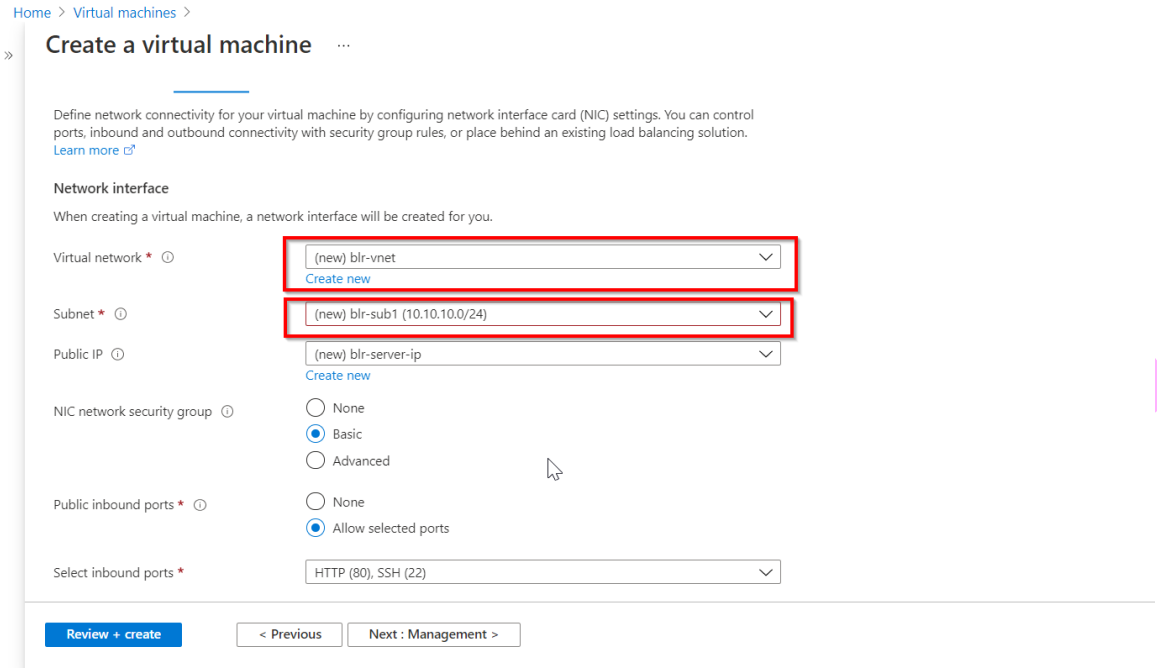
Note: NSG at the subnet level gets implemented for all the servers in that subnet.

8 Virtual network Peering

If you want to connect two diff networks then you can use the option of vpc peering.

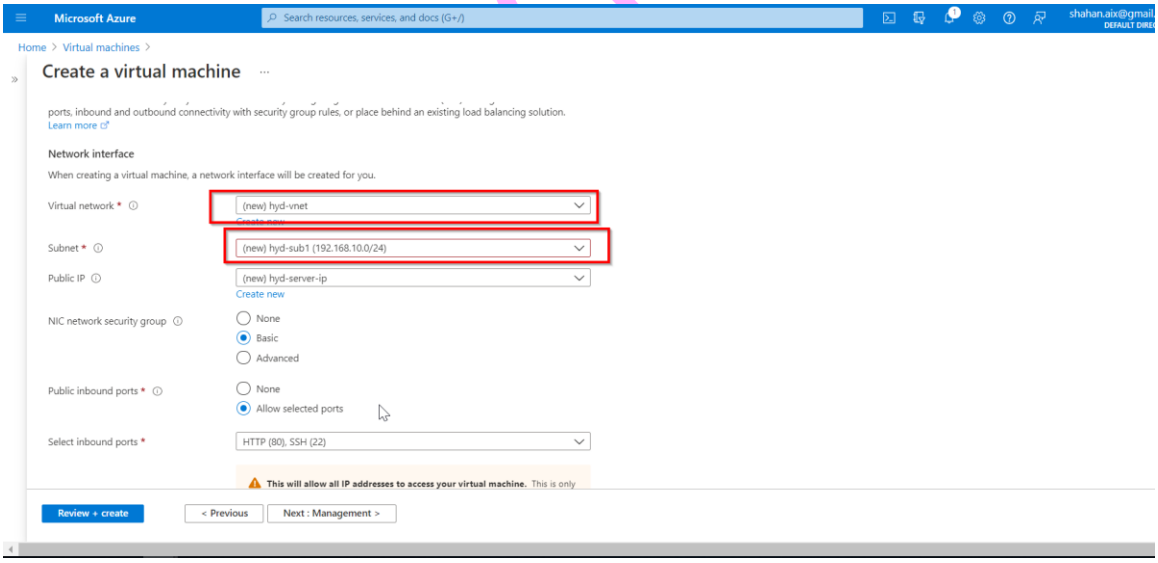
Let's create two servers with diff networks like blr-server with 10.10.0.0/16 & hyd-server with 192.168.0.0/16 network.

Create blr-server using below:

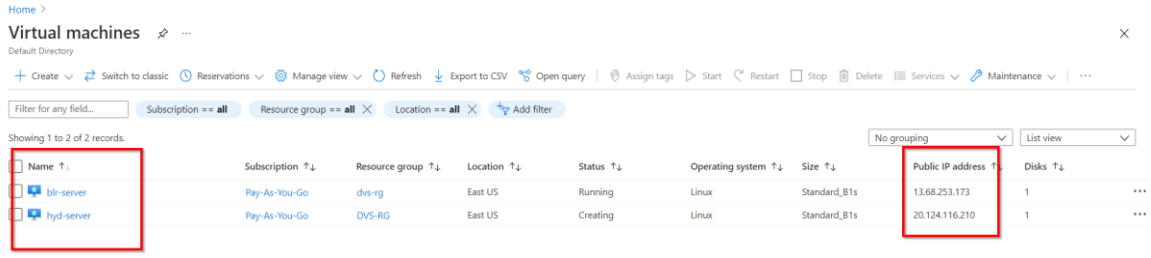


Note: Make sure you are allowing port 22,80 in the ASG

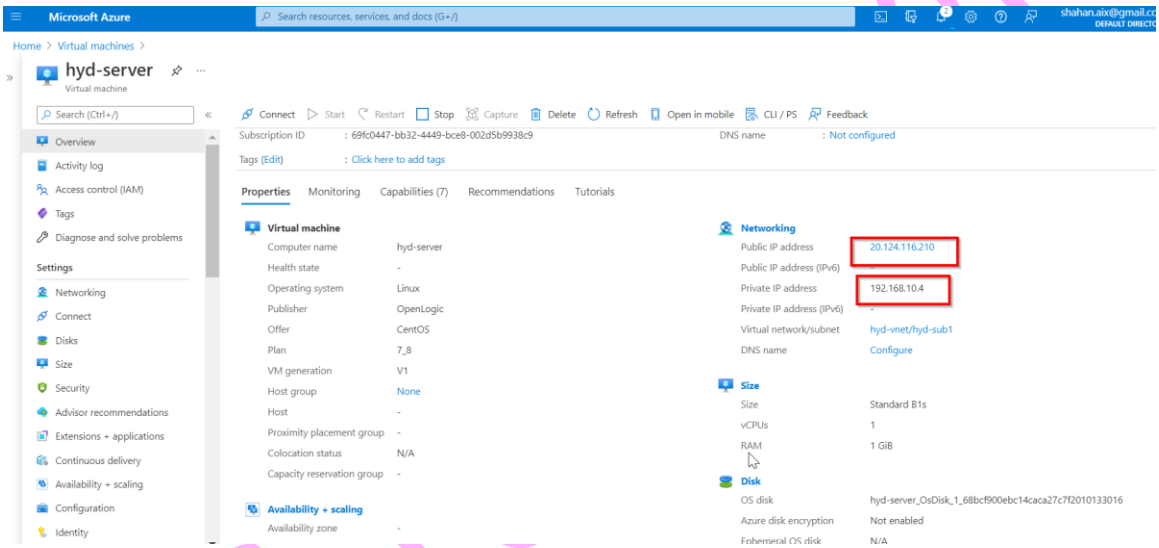
Create hyd-server using below:



Once the machines are up let's try to login to the servers



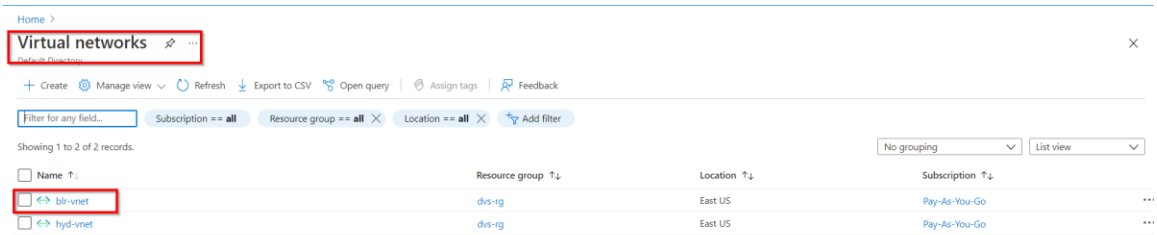
Let's try to login to BLR server & do ssh for hyd server



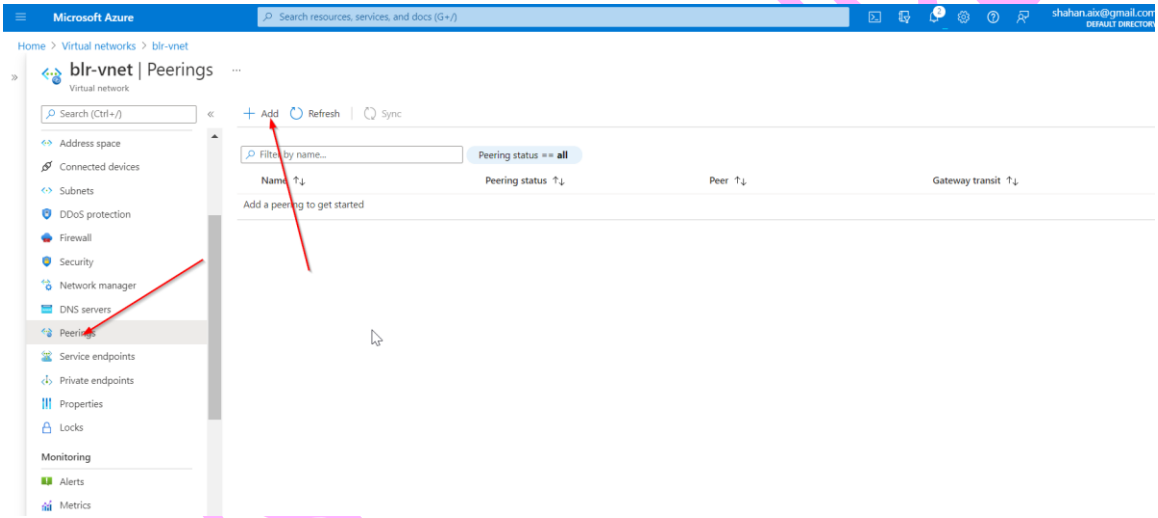
dvsadmin@blr-server:~

```
[dvsadmin@blr-server ~]$ ssh 192.168.10.4
```

If you observer above its not working now let's configure the VNET peering so that we can able to connect to hyd-server from blr-server



Let's go blr-vnet & raise a peering request
Note: you can do vice-versa



Microsoft Azure

Search resources, services, and docs (G+/)

Home > Virtual networks > blr-vnet >

Add peering

blr-vnet

This virtual network

Peering link name *

blr-to-hyd

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

Peering link name *

hyd-to-blr

Virtual network deployment model

- (•) Resource manager
- ( ) Classic

Add

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Virtual networks > blr-vnet >

Add peering

blr-vnet

- ( ) Classic

[ ] I know my resource ID

Subscription *

Pay-As-You-Go

Virtual network *

hyd-vnet

Traffic to remote virtual network

- (•) Allow (default)
- ( ) Block all traffic to the remote virtual network

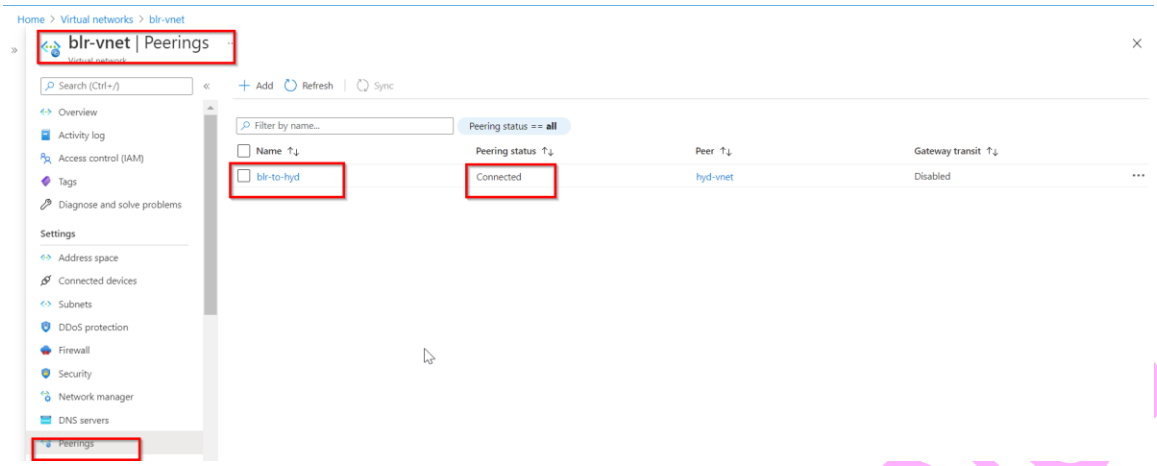
Traffic forwarded from remote virtual network

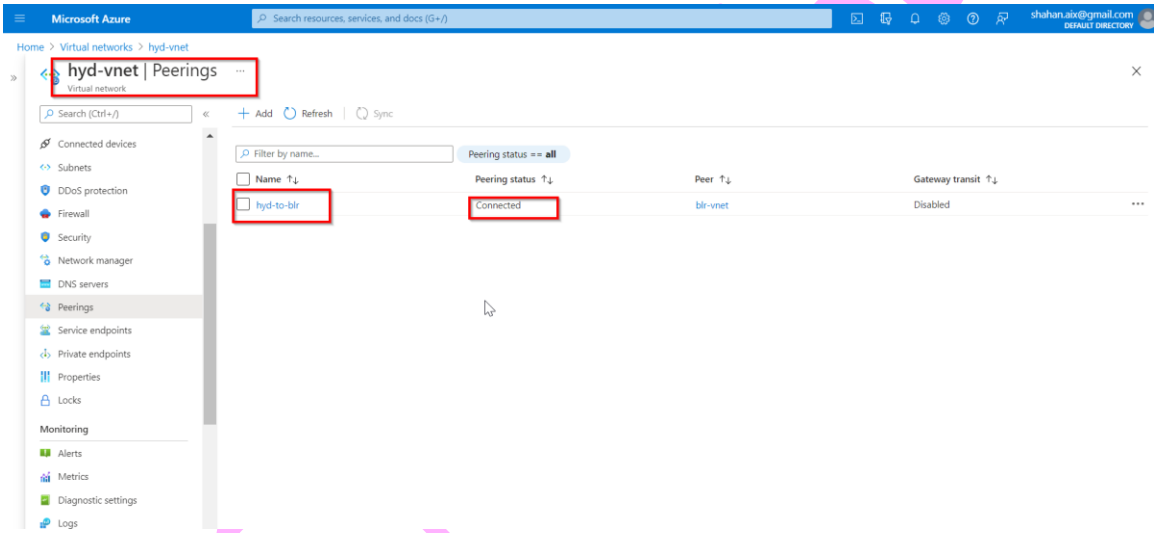
- (•) Allow (default)
- ( ) Block traffic that originates from outside this virtual network

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)

Add





If you observe above we can see that vpc peering status shows as connected.

Now let's test the connectivity from server

```
[dvsadmin@blr-server ~]$ ssh dvsadmin@192.168.10.4
The authenticity of host '192.168.10.4 (192.168.10.4)' can't be established.
ECDSA key fingerprint is SHA256:8vYt/Nmq998UF8DssJiCcqgcygBEhob8yrmWQ5Cx4sQ.
ECDSA key fingerprint is MD5:8a:fa:96:0a:3e:93:95:a1:d9:a8:6a:92:4a:b9:90:ad.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.10.4' (ECDSA) to the list of known hosts.
```

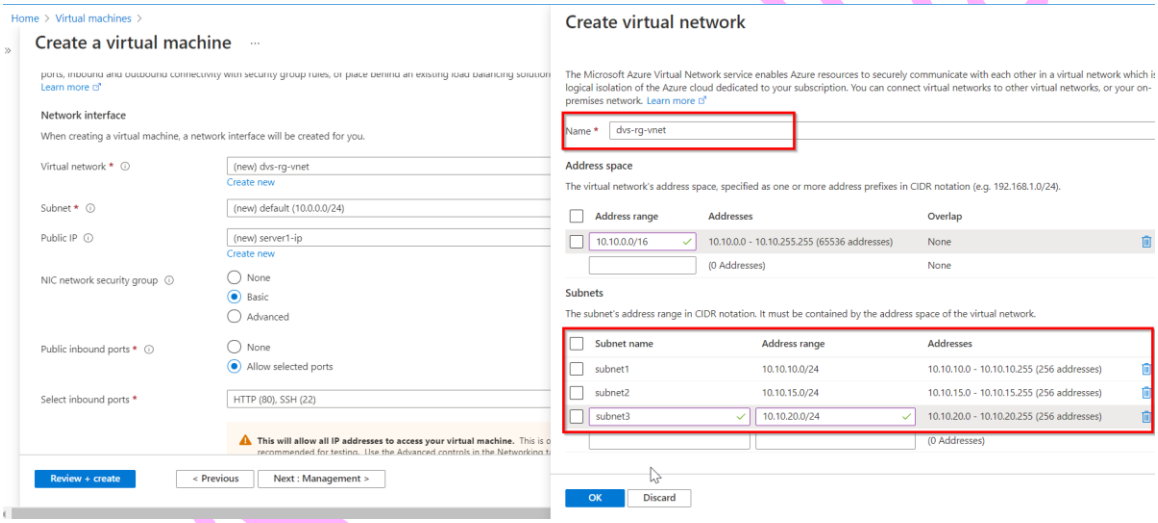
Now I can able to connect to the hyd-server from the blr-server with out public ipaddress. You can create peering connection like this.

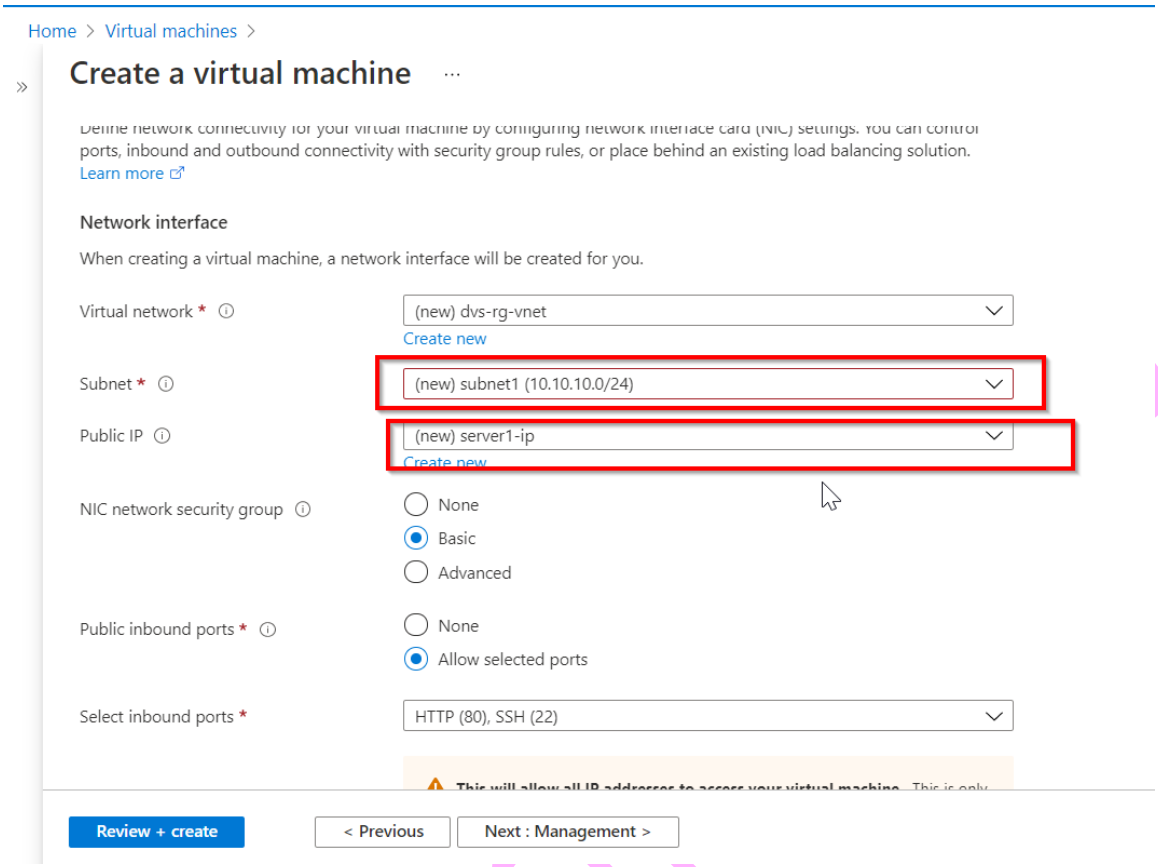
9 User defined routes

In general all the subnets in VNET can communicate each other. Imagine a situation you want to route the traffic between servers of same VNET in diff subnets & you want to control the communication to happen via some other server in the other subnet then we can define the user defined routes & can apply the same to the respective servers so that we can have the control on our in-out of the environment traffic.

In order to understand more about this let's create three servers

VNET: 10.10.0.0/16
Server1 (subnet1 - 10.10.10.0/24)
Server2 (subnet2 - 10.10.15.0/24)
Server3 (subnet3 - 10.10.20.0/24)
Our goal is to reach server3 from the server1 via server2





Please build other two servers with subnet2,subnet3

Only for server3 just make sure you are installing apache

```
#!/bin/bash
yum install httpd -y
systemctl enable httpd
echo "Hi I am from server3" > /var/www/html/index.html
systemctl restart httpd
```

Once done try to reach out to server3 from server1, since they all belongs to same network they should able to access directly via private ipaddress.

Testing before change:

```
dvsadmin@server1:~
[dvsadmin@server1 ~]$ nslookup server3
Server:         168.63.129.16
Address:        168.63.129.16#53

Non-authoritative answer:
Name:   server3.4vcvotcuzvvuxil01fk4p1lb2f.bx.internal.cloudapp.net
Address: 10.10.20.4

[dvsadmin@server1 ~]$ curl http://server3
Hi I am from server3
[dvsadmin@server1 ~]$
```

Now let's configure the route table.

Home > Route tables >

Create Route table

Basics | Tags | Review + create

Project details

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 * : dvs-rg

Create new

Instance details

Region * : East US

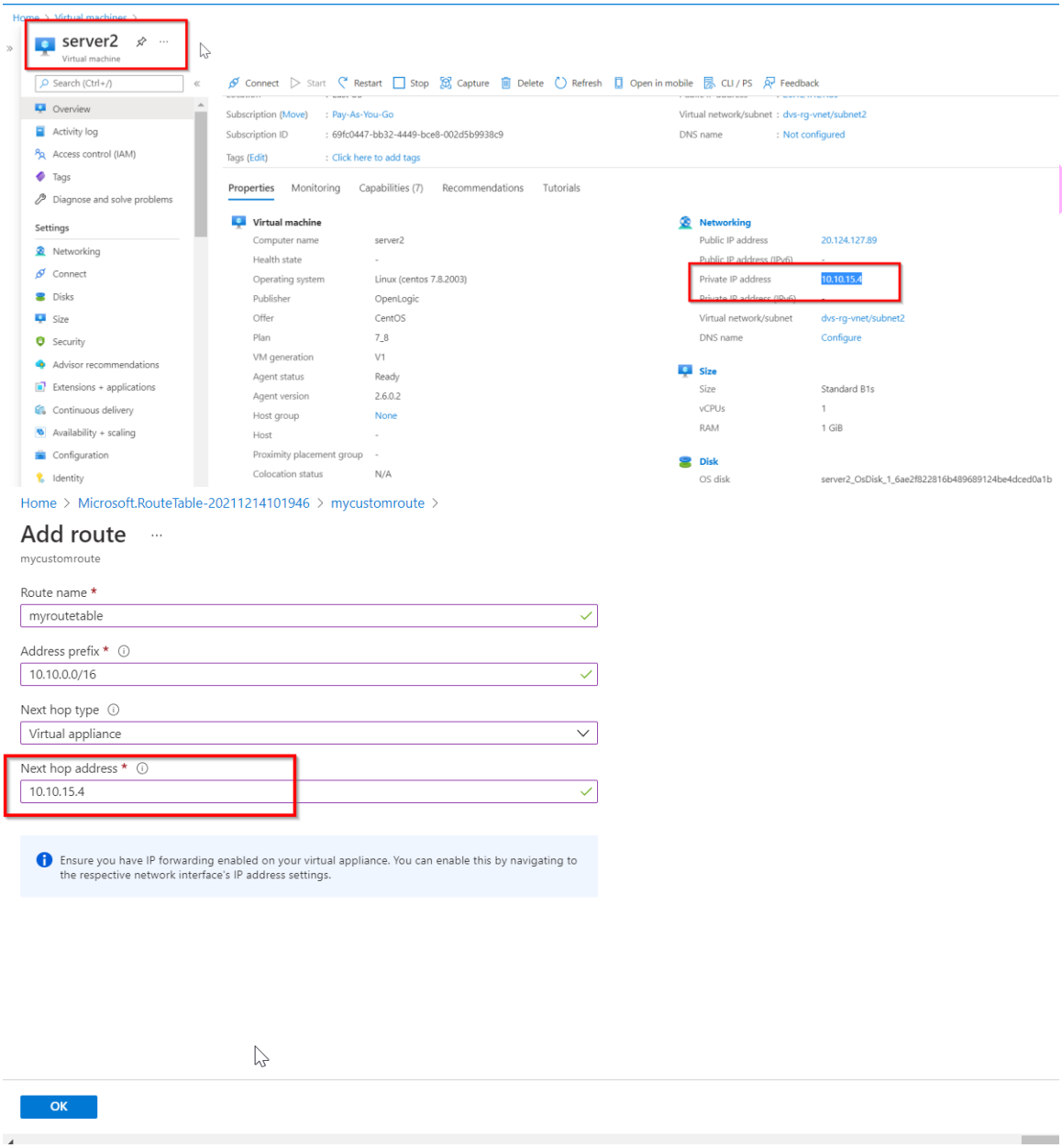
Name * : mycustomroute

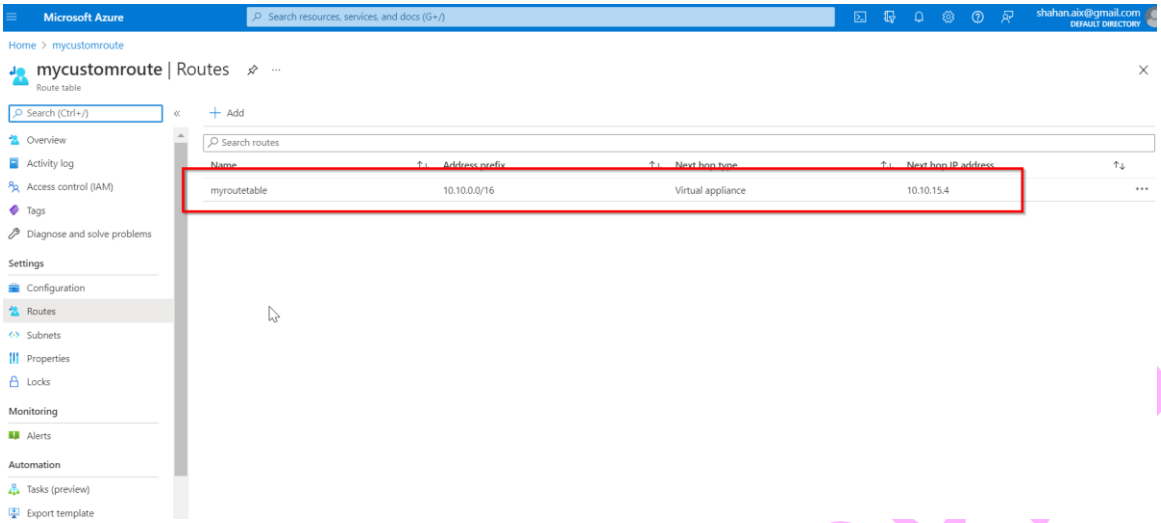
Propagate gateway routes * : Yes / No

Review + create | < Previous | Next : Tags >

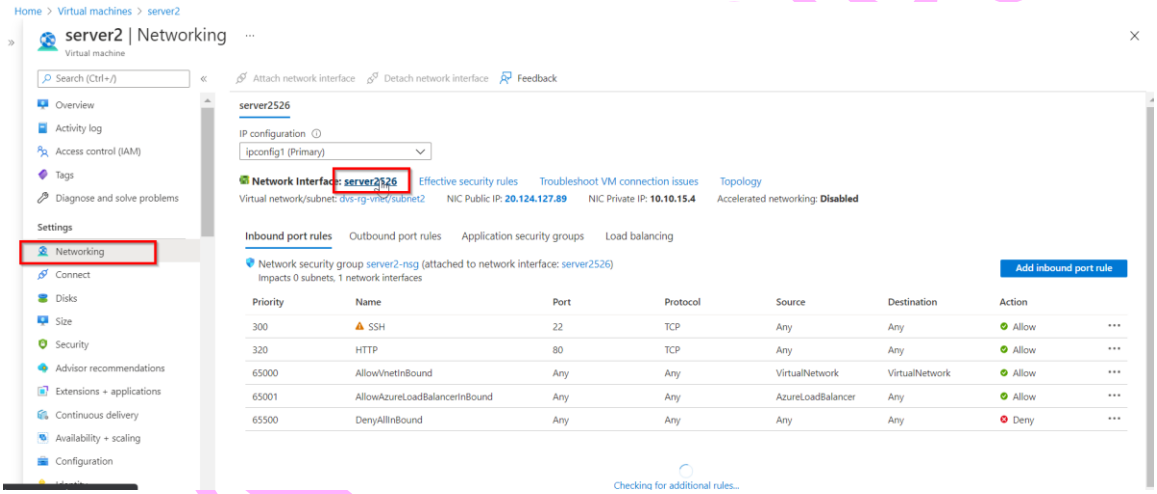
Now let's add the route

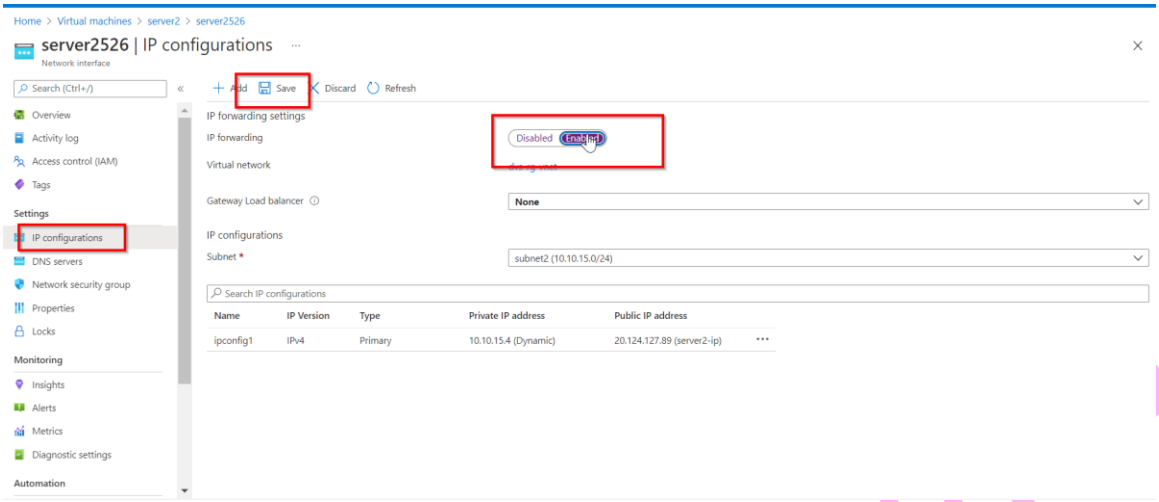
Here we are adding the server2 ipaddress as we want to make server2 as a bridge for our communication from server1 to server3



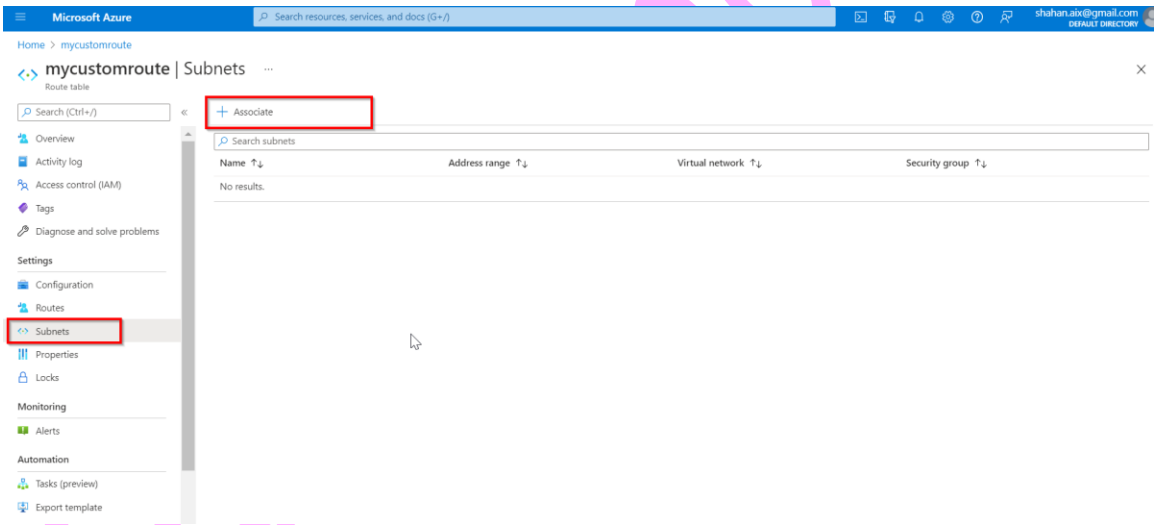


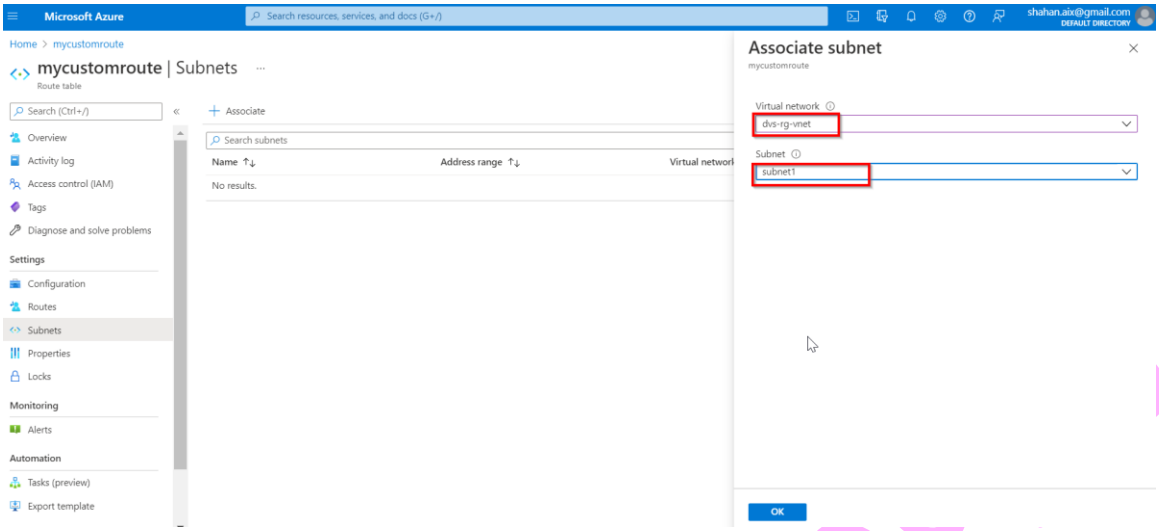
Now let's make sure that server2 is allowing the forwording

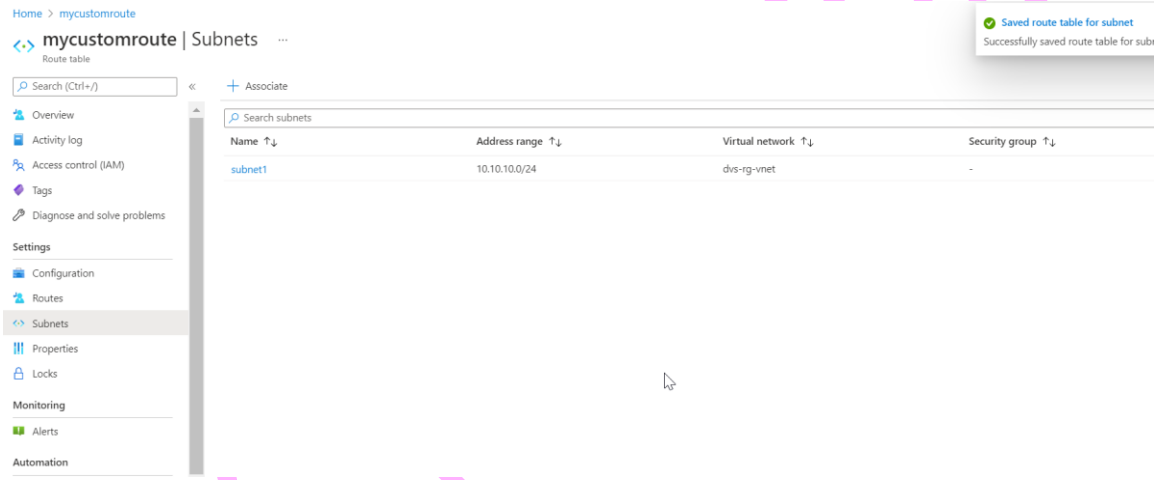




Now we configured that all the traffic should go via server2 but we didn't specified who should follow this rule. Hence we need to add the subnets to this route. In our case we need to add subnet1





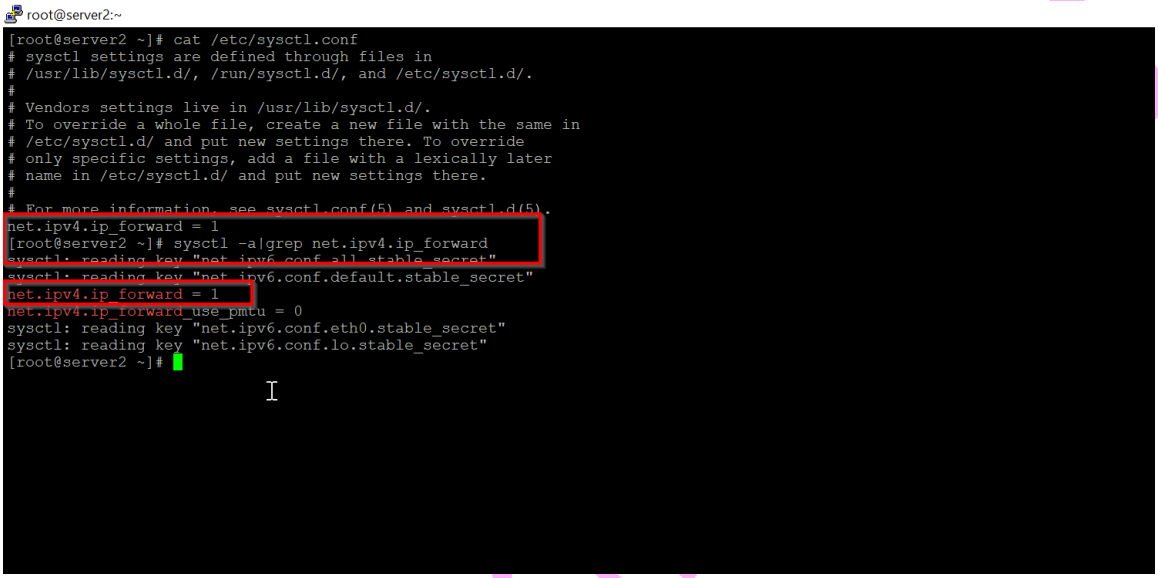


Now let's try to reach to server3 from server1

Now if you observe we can't reach to server3 as the request is going to server2 and from server2 the request is not going to server3

We need to enable ipforwarding from the server2 end. We can do it using below

vi /etc/sysctl.conf
net.ipv4.ip_forward = 1



To refersh the configuraton pls execute "sysctl -p /etc/sysctl.conf"

Once done now you can try to access the server3 from server1

DVS Tech

dvsadmin@server1:~

```
[dvsadmin@server1 ~]$ curl http://server3
Hi I am from server3
[dvsadmin@server1 ~]$
```

Now your entire traffic is hitting destination server3 from server1 via server2.

DVS Technologies