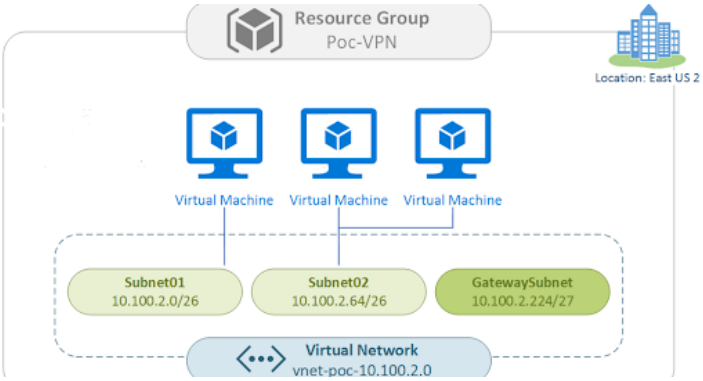
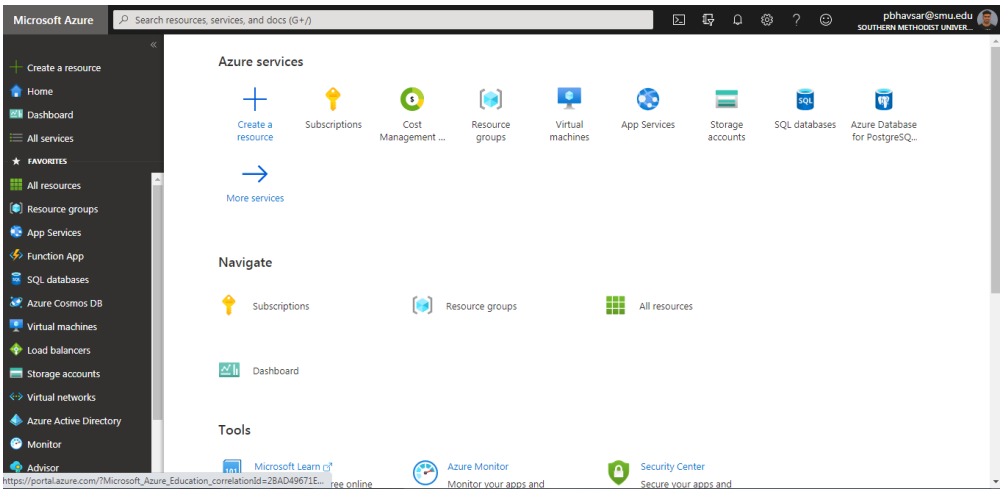
Lab: Build Your Azure Network Design and Launch a Web Server

In this Lab, we'll create custom Resource Group along with Virtual Networks, Subnets and Security Groups. We will then launch a web server on one of the Public Subnet and access the Website externally.

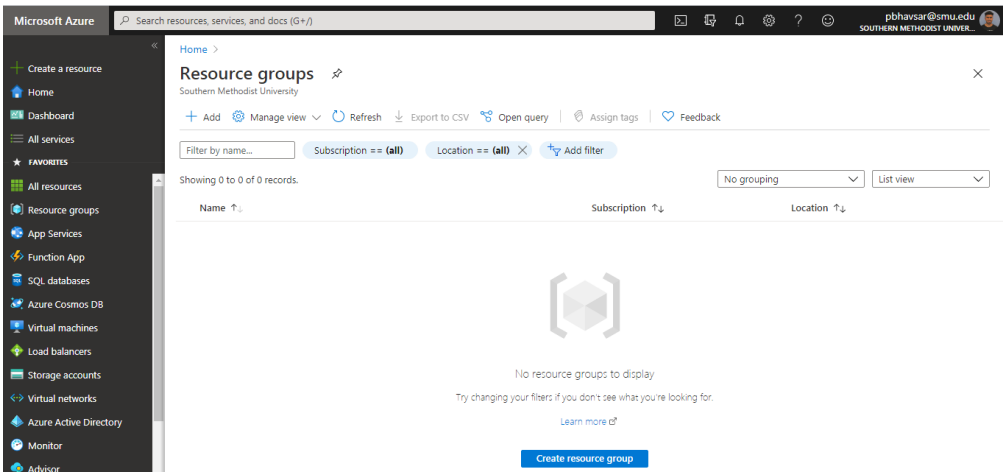


Task 1: Create your Resource Group.

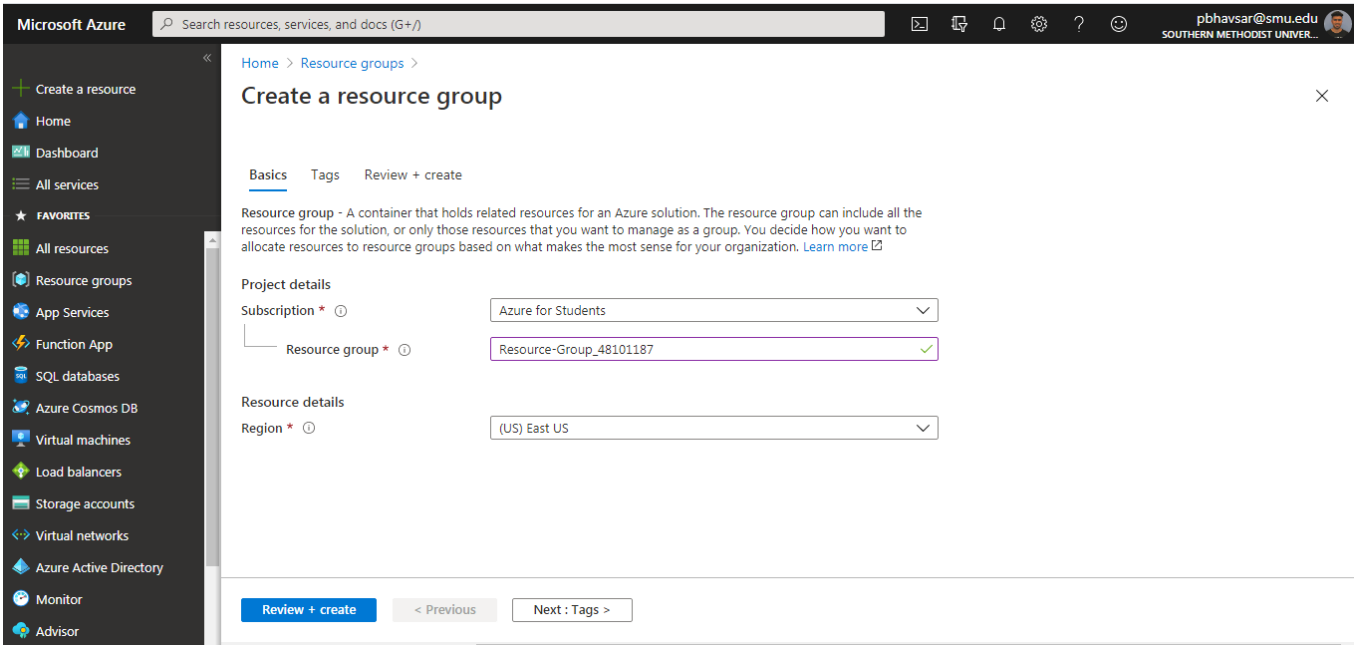
Login to your Azure Portal with your credentials.



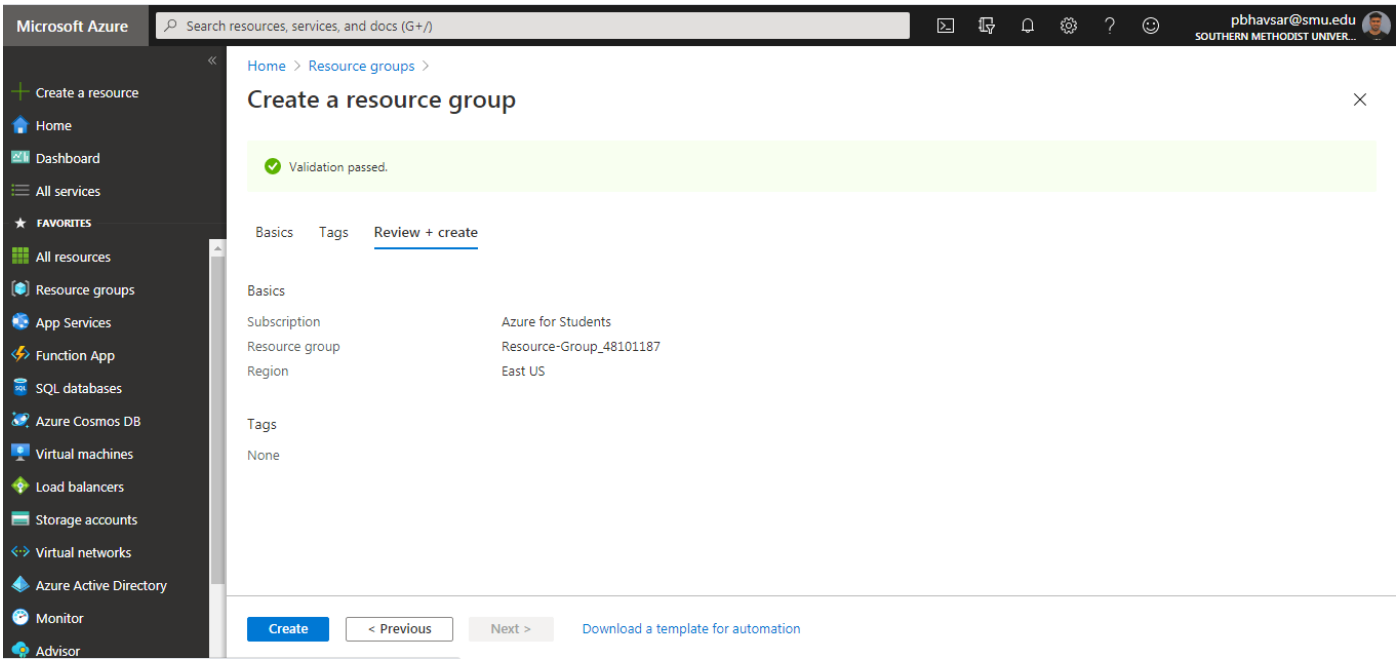
Under Search, search for **Resource Group**. Click on "+Add".



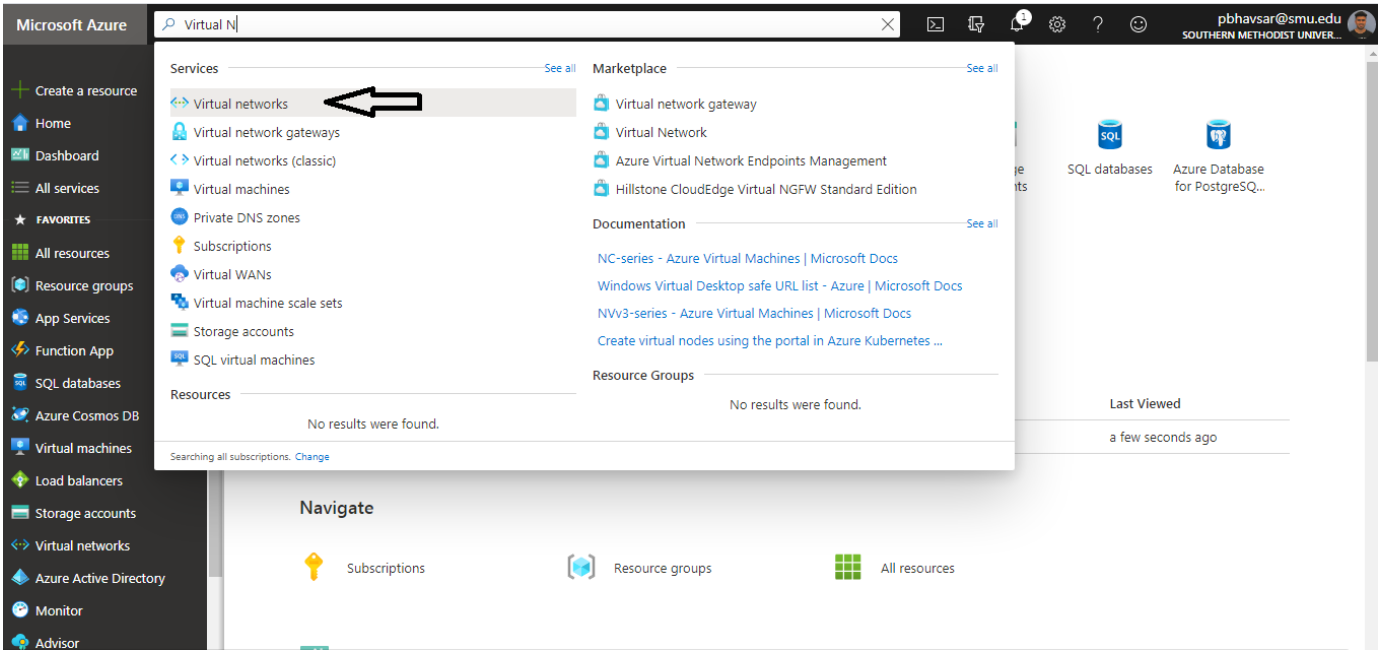
Specify Resource Group Name as “Resource-Group_SMUID” and Region as “(US)East US”.



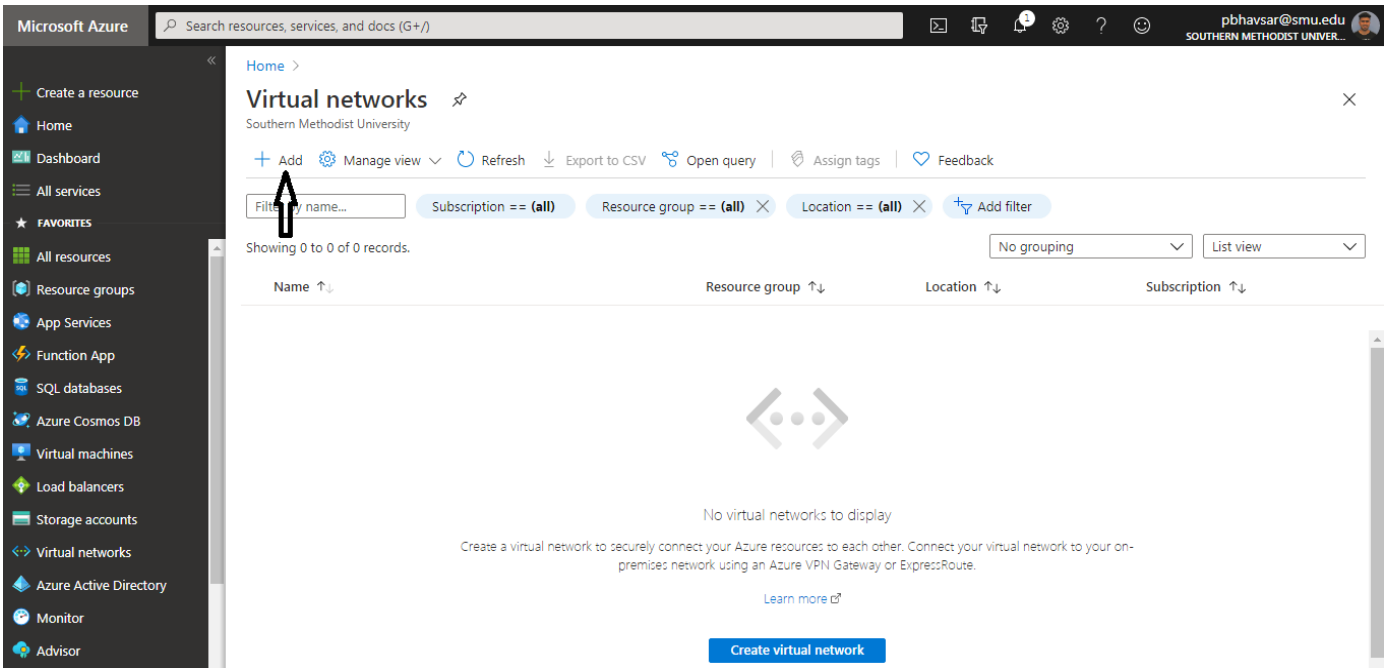
Specify the Tags if you wish and click on Next. Review the Resource Group configurations and click on Create.



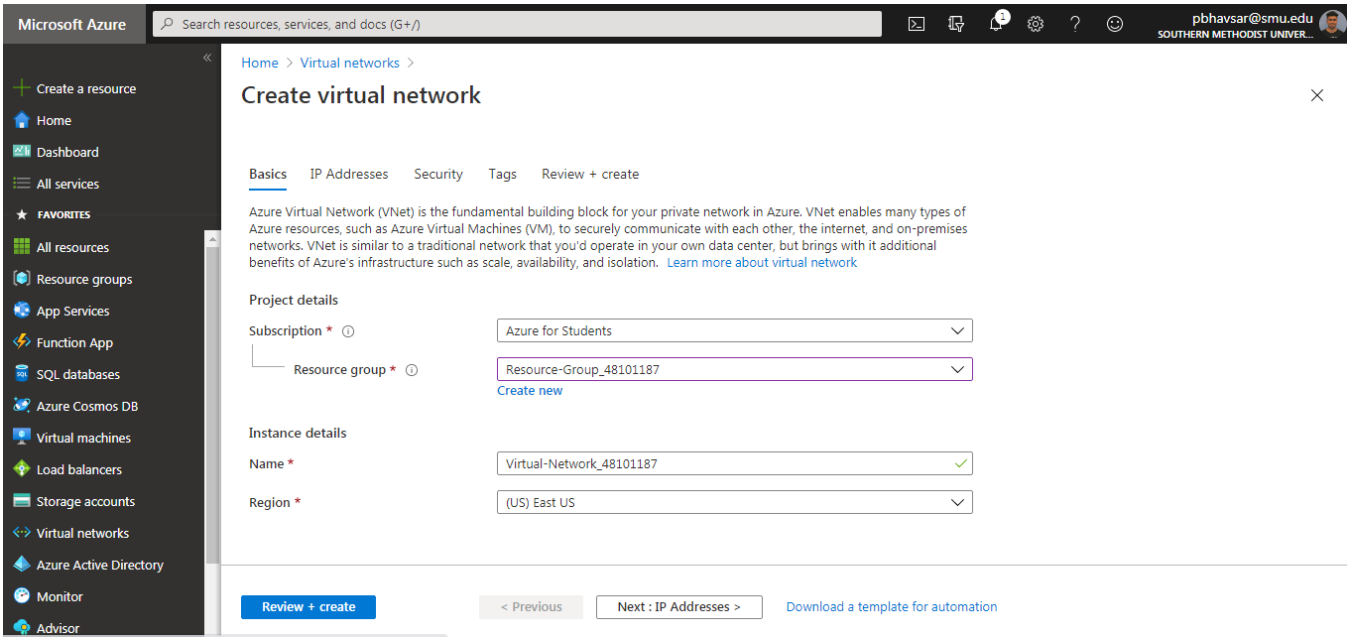
Now under Search, search for Virtual Networks.



Click on “+Add”.



Specify the Resource Group which you created earlier, Virtual Network Name and Region as “(US) East US”.

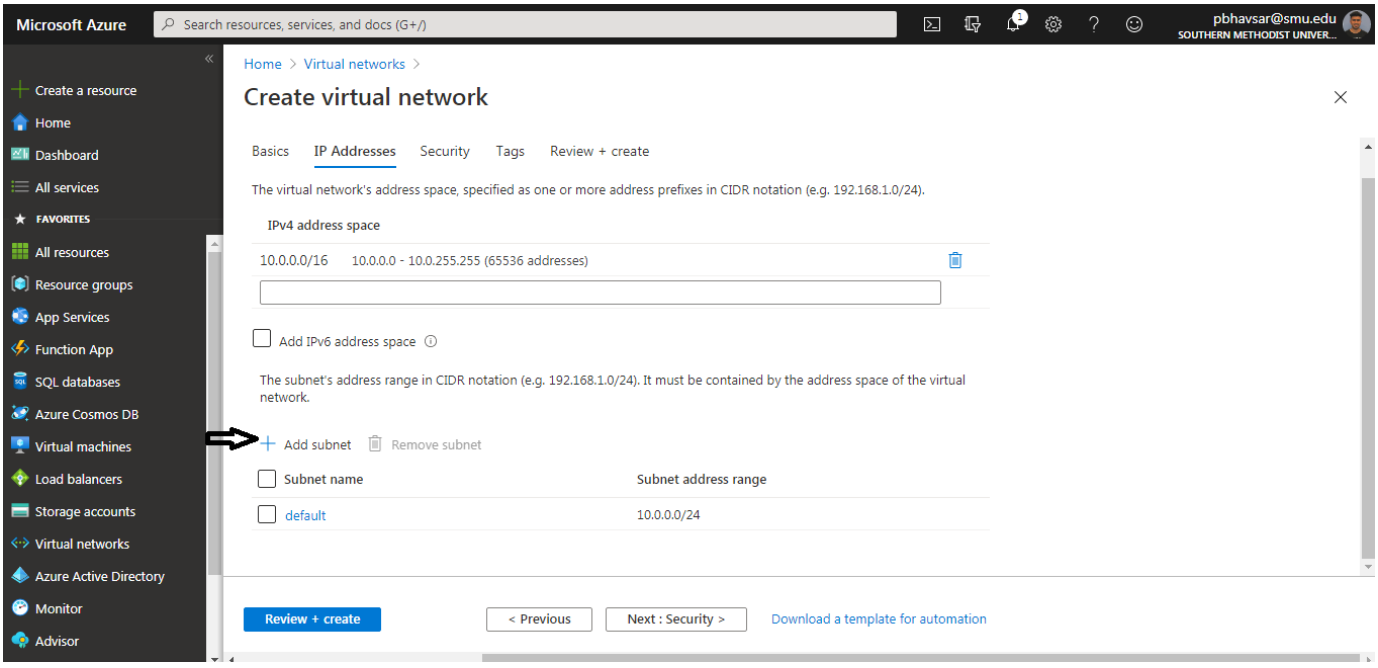


Click on Next: IP Addresses.

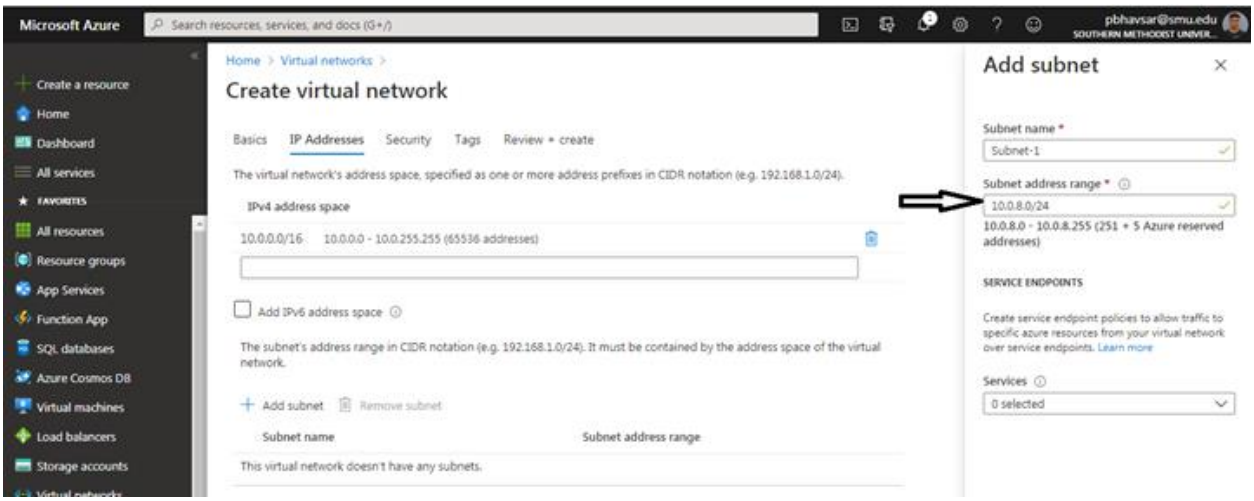
If you notice, the IPv4 Address Space for Virtual Network is “10.0.0.0/16”.

Now let’s specify the Subnets inside the Virtual Network.

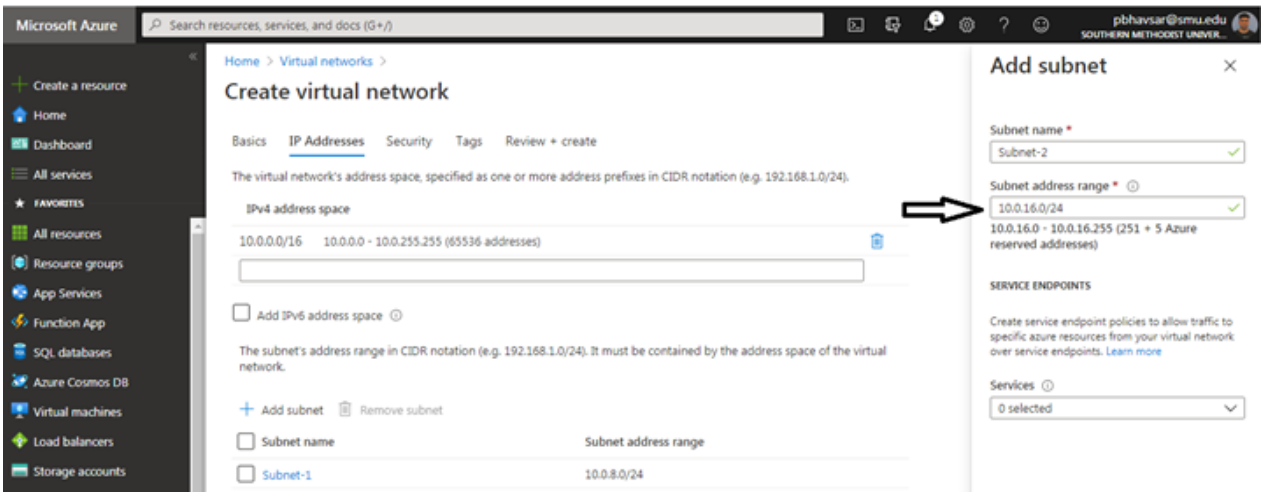
Click on “+ Add Subnet”.

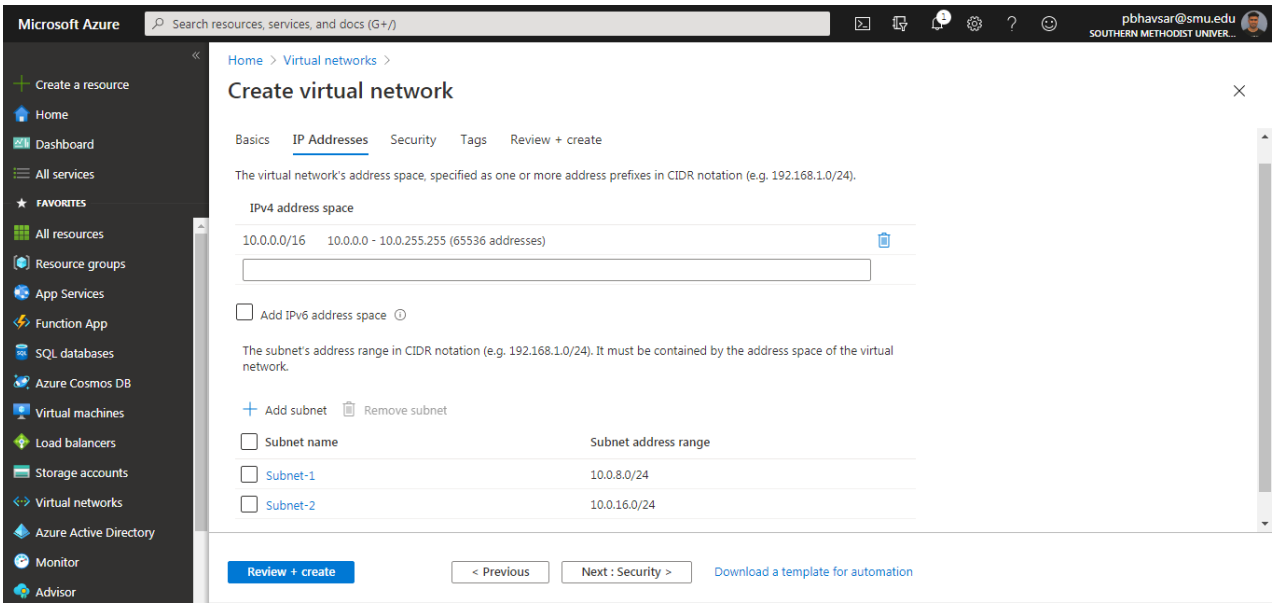


Specify the Subnet-1 as follows with the Subnet Address Range “10.0.8.0/24”.

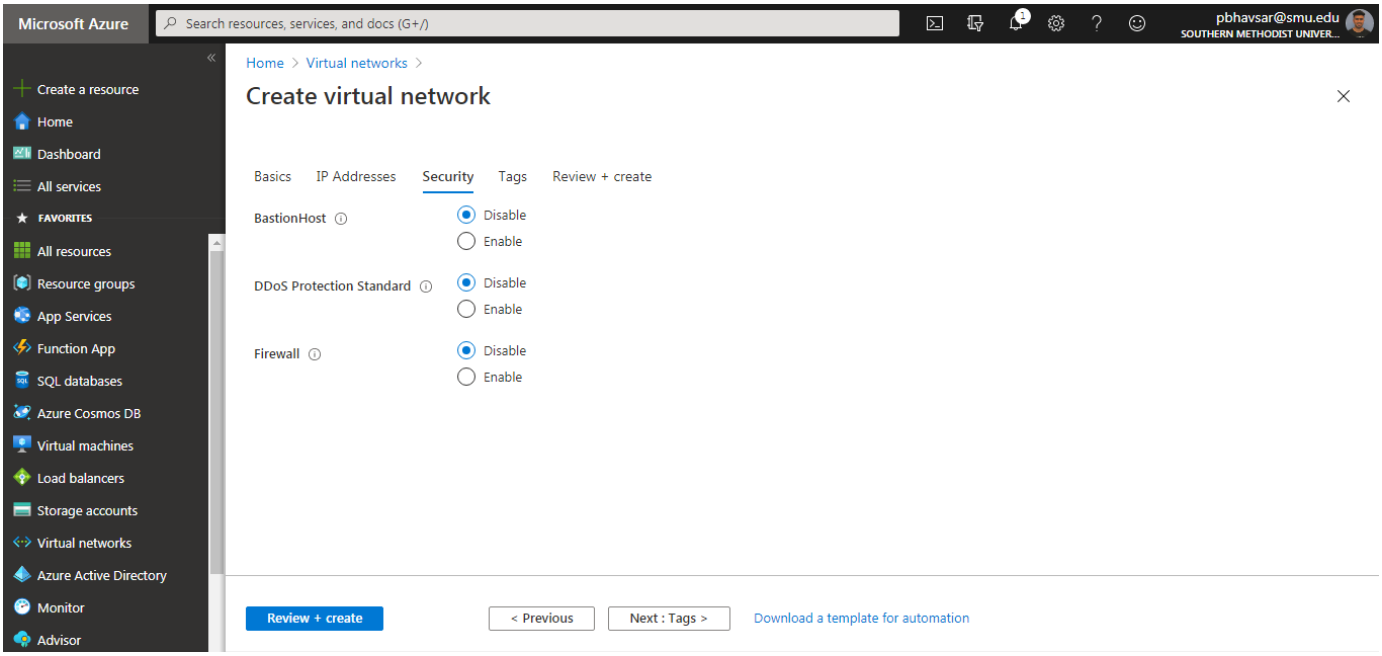


Similarly, create Subnet-2 as follows with the Subnet Address Range “10.0.16.0/24”.

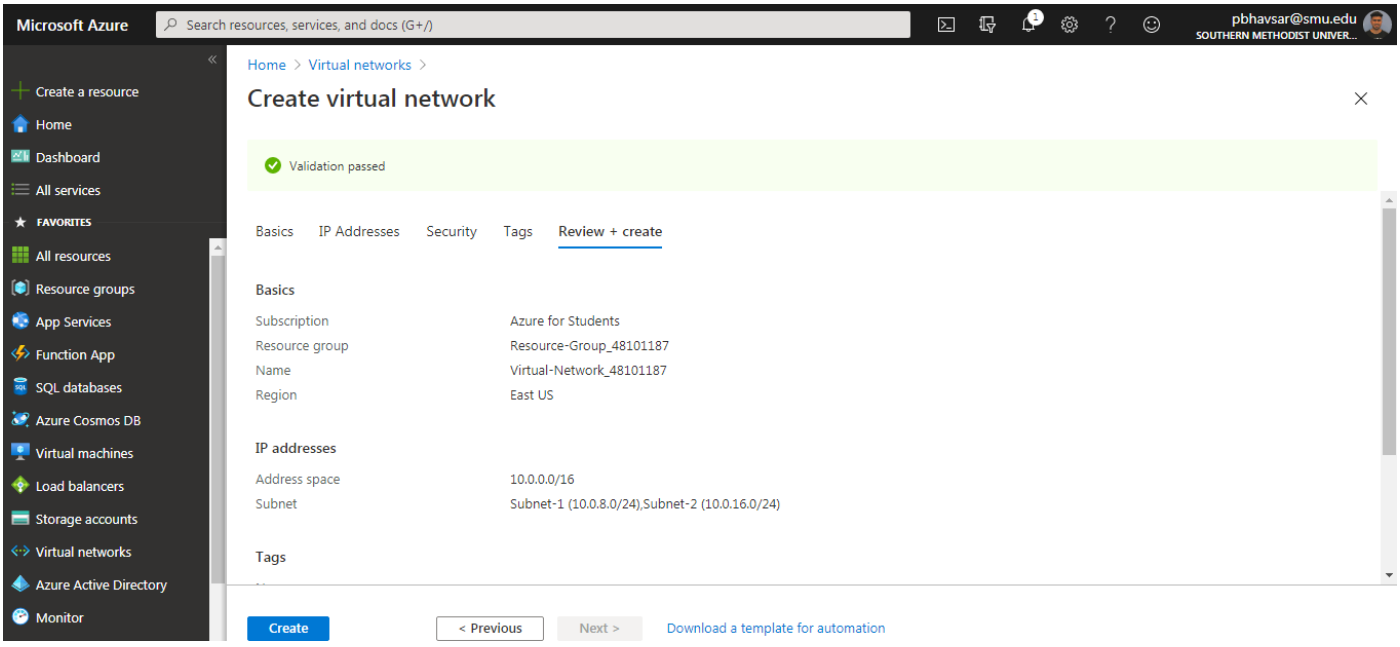




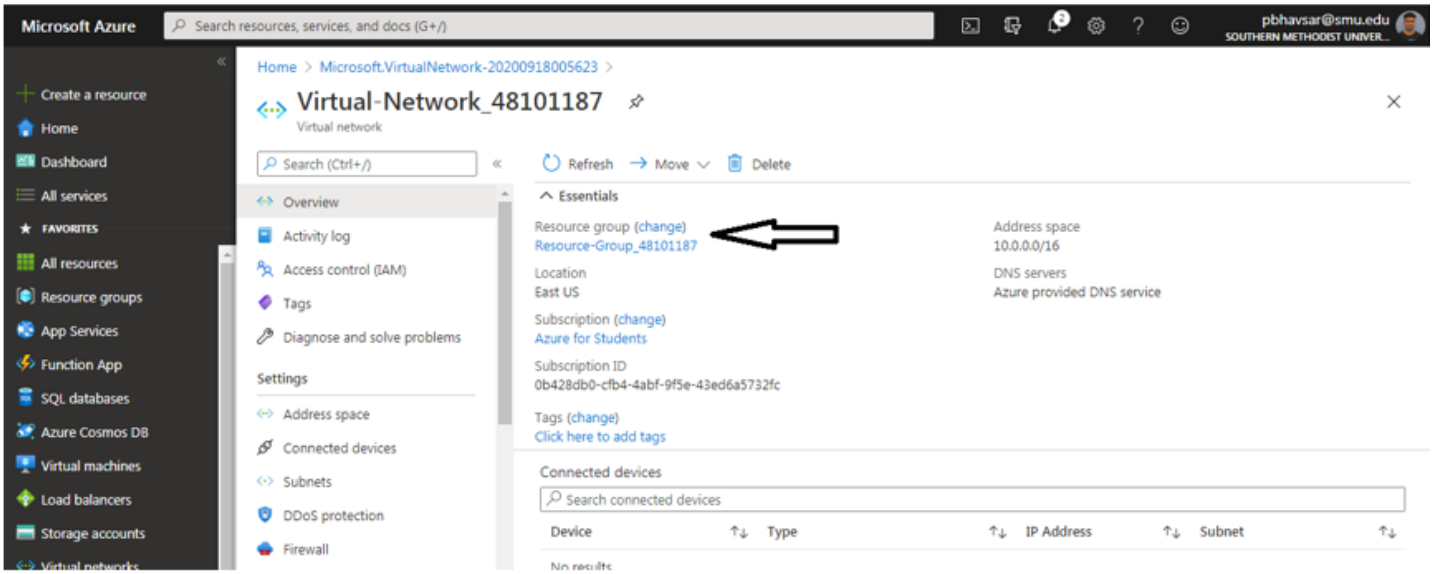
Keep the Security settings as defaults.



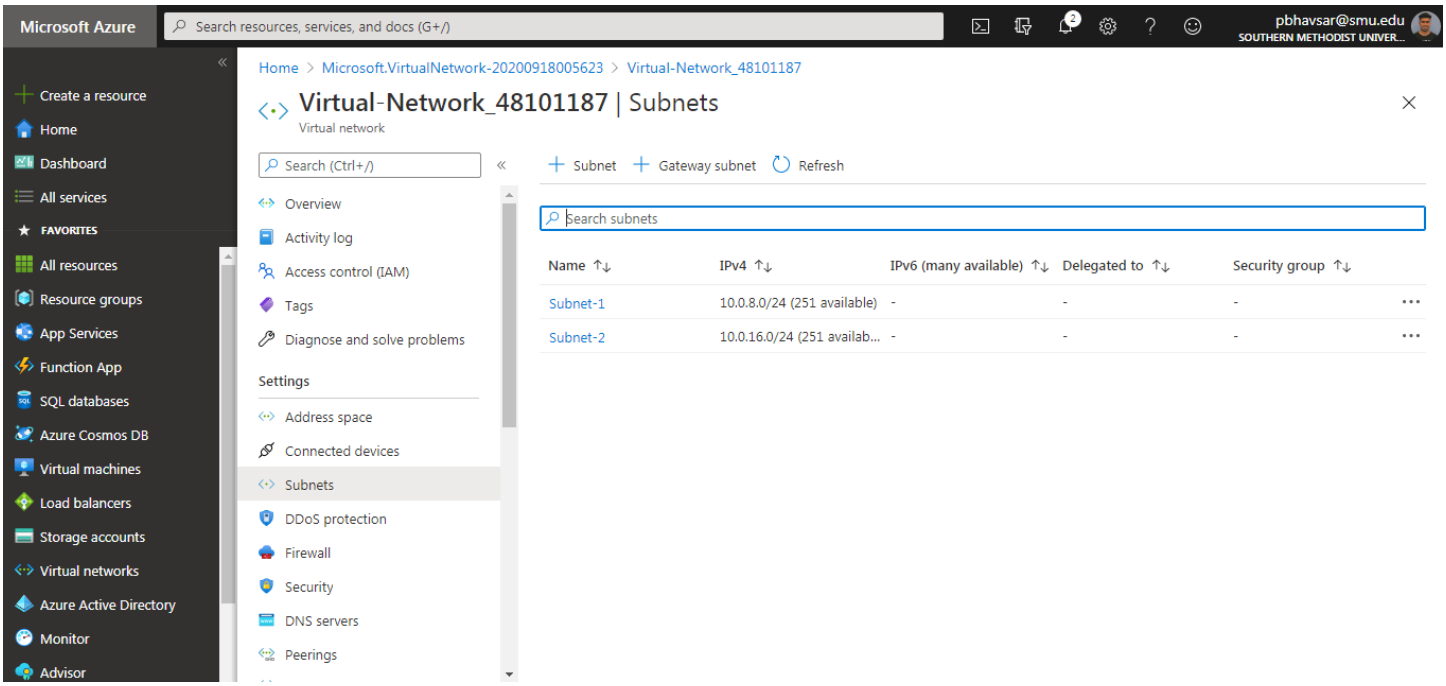
Review the Virtual Network configuration settings and click on Create.



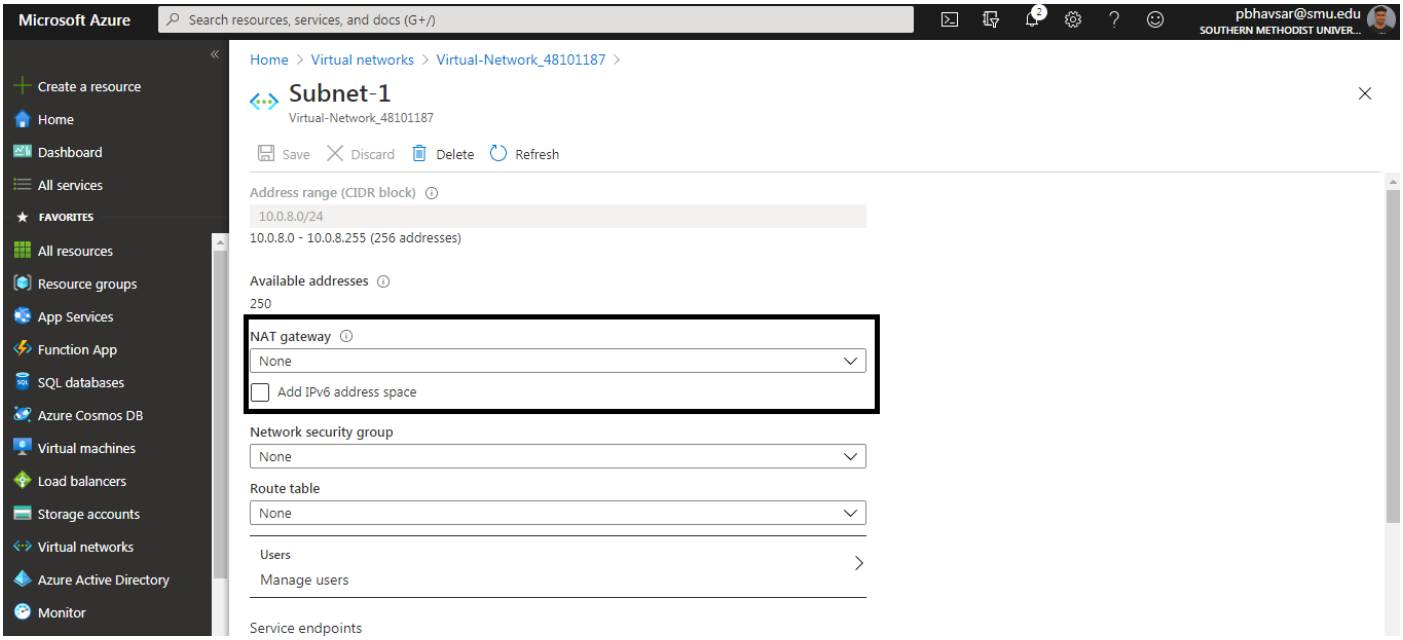
Once, the Virtual Network is created, you'll notice that it is attached to the Resource Group. Just like VPC CIDR attached to VPC in AWS.



Click on Subnets, you'll see both the Subnets which you created earlier.



Click on Subnet-1, you'll notice that it hasn't been configured with any NAT gateways. Hence, we can call it as a Public Subnet.

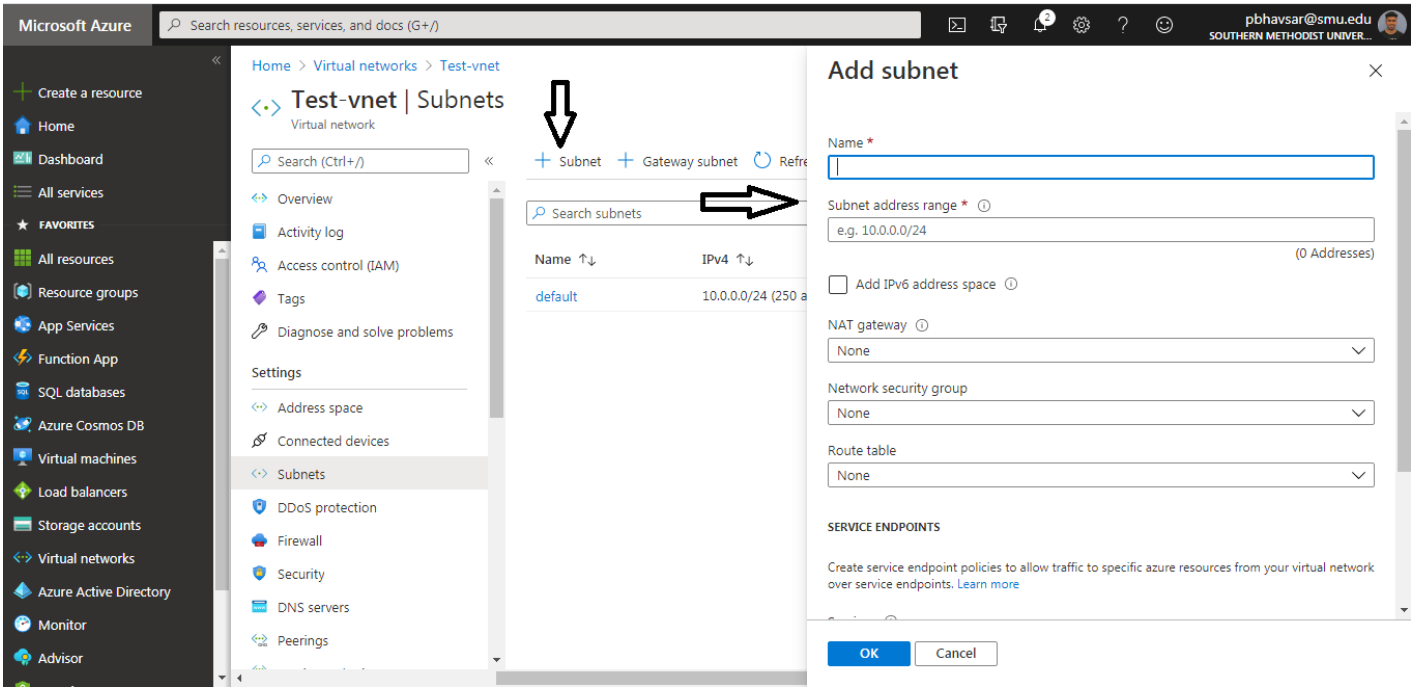


Similarly, verify the Subnet-2 which is also Public Subnet.

Task 2: Create Additional Subnets

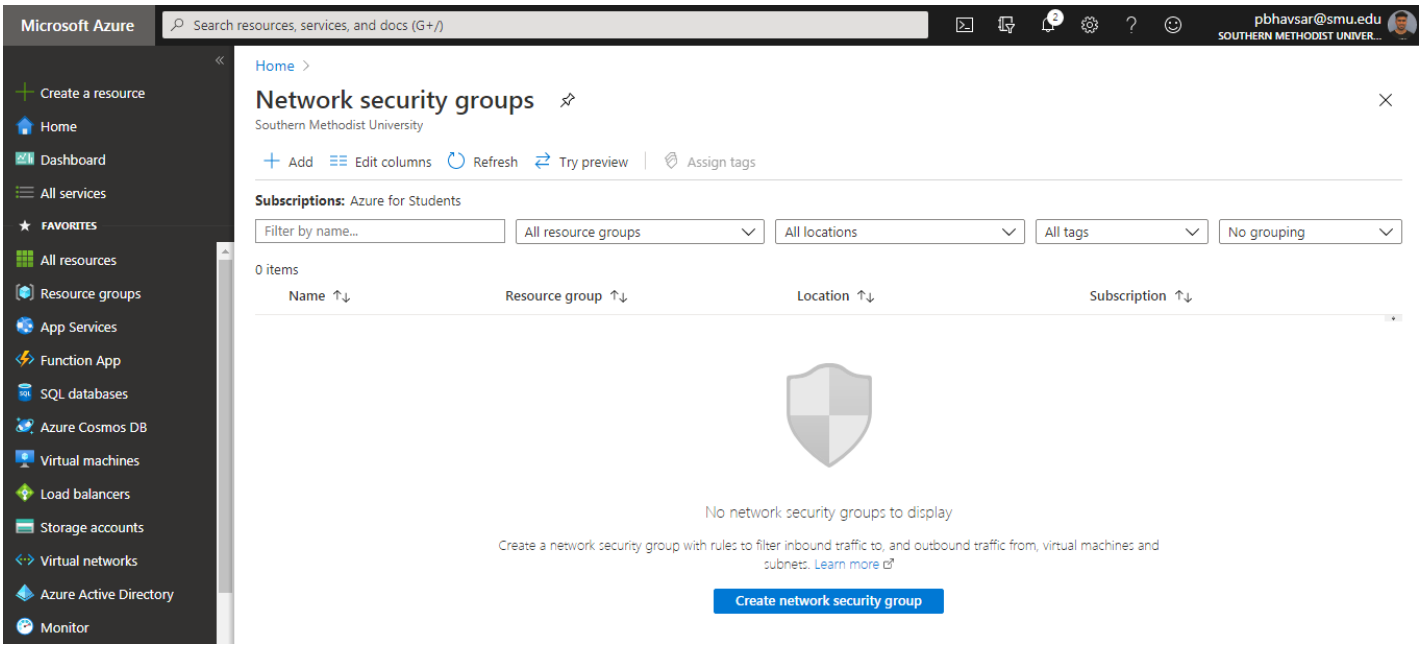
To create Additional Subnets in Virtual Networks, navigate to the Virtual Network Service and select the Virtual Network which you've configured earlier.

Click on Subnets and Click on Add to add more Subnets in Virtual Network (VNet).

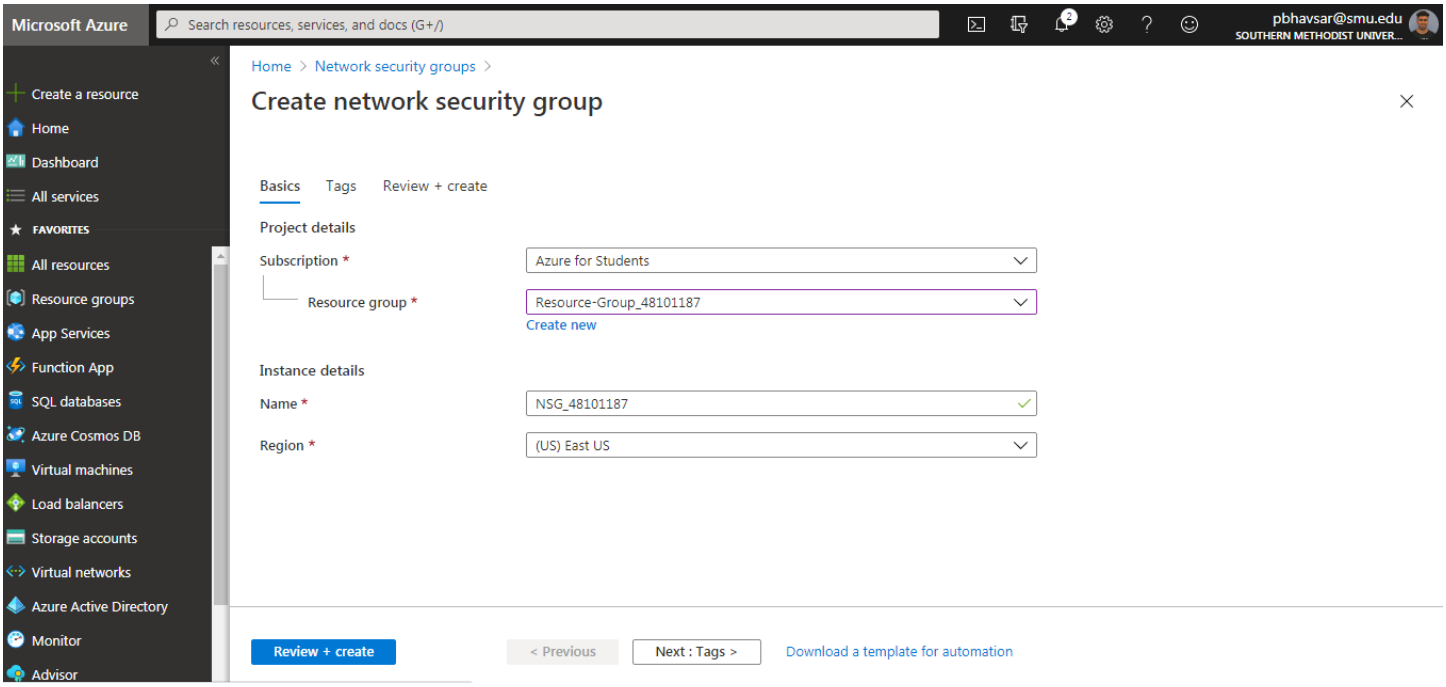


Task 3: Create a VPC Security Group

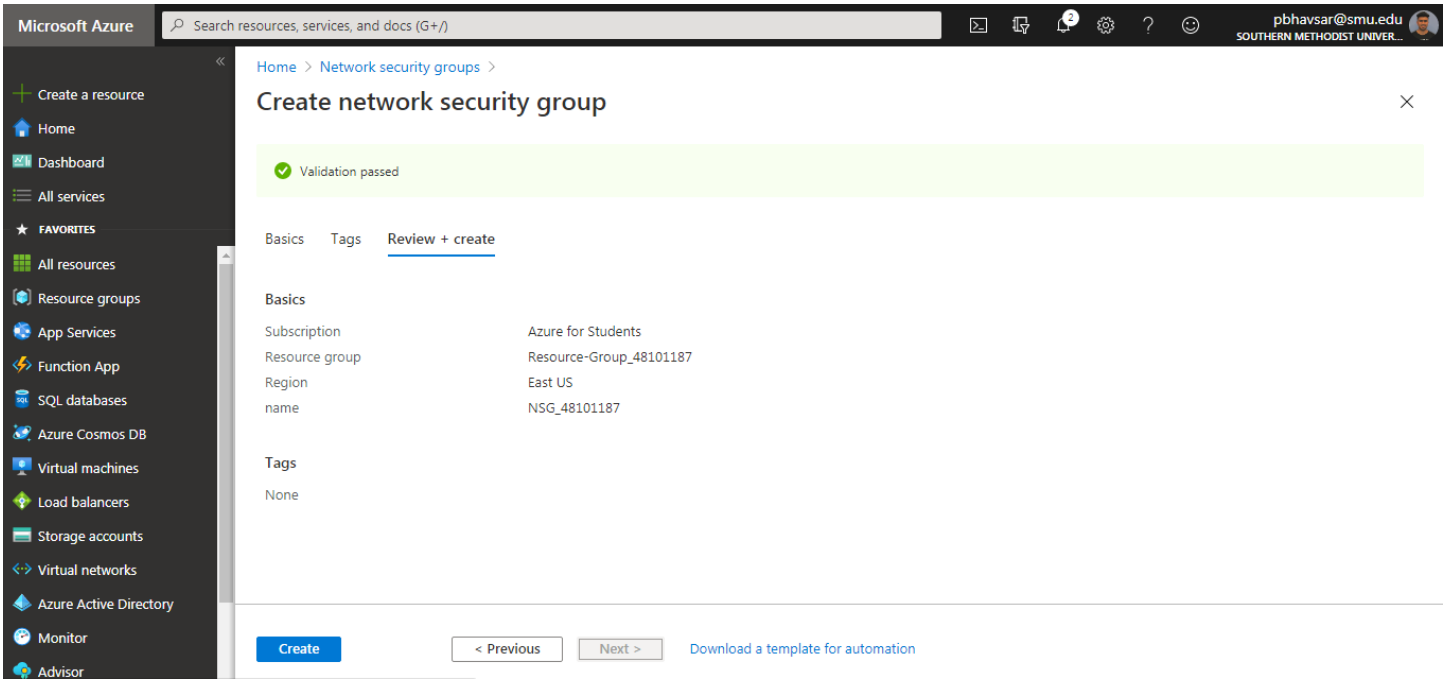
In the Search bar, search for Network Security Group Service. Click on "+Add".



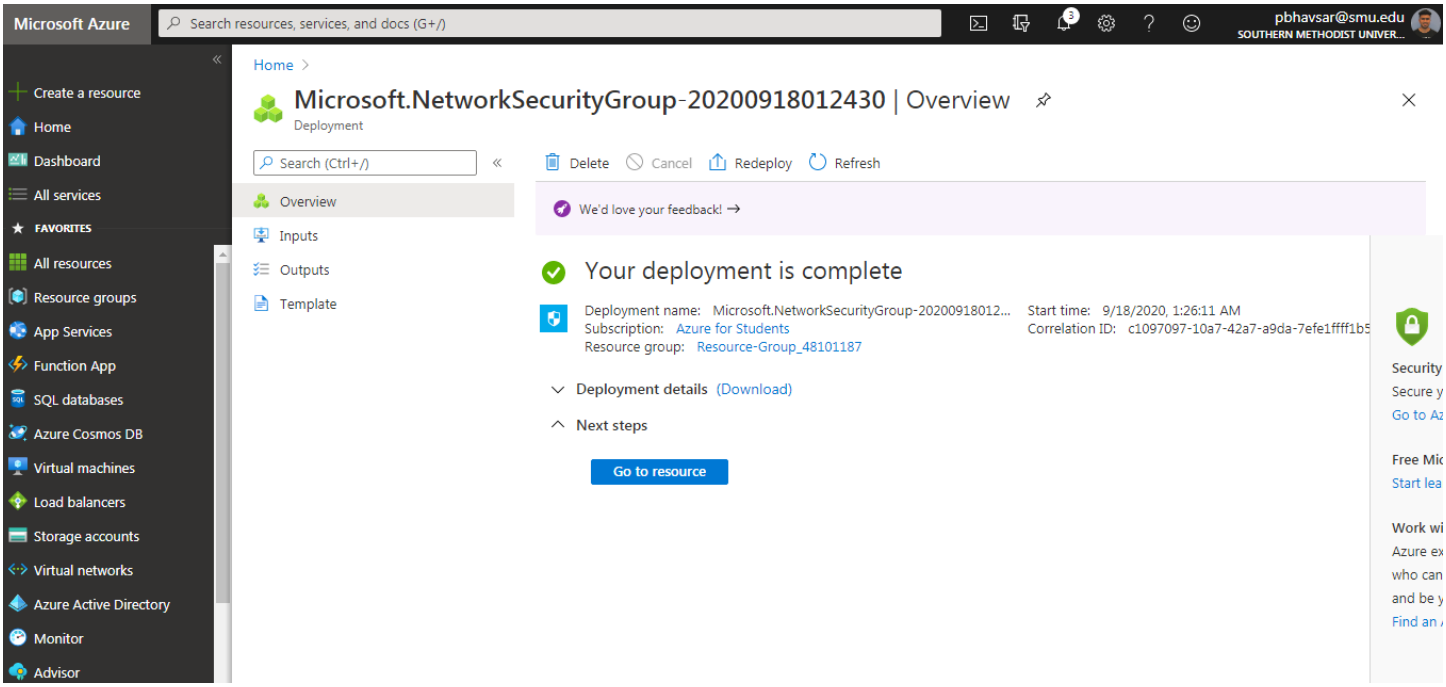
Specify the Resource Group which you've created earlier and Name of the Network Security Group (NSG), Region (US) East US.



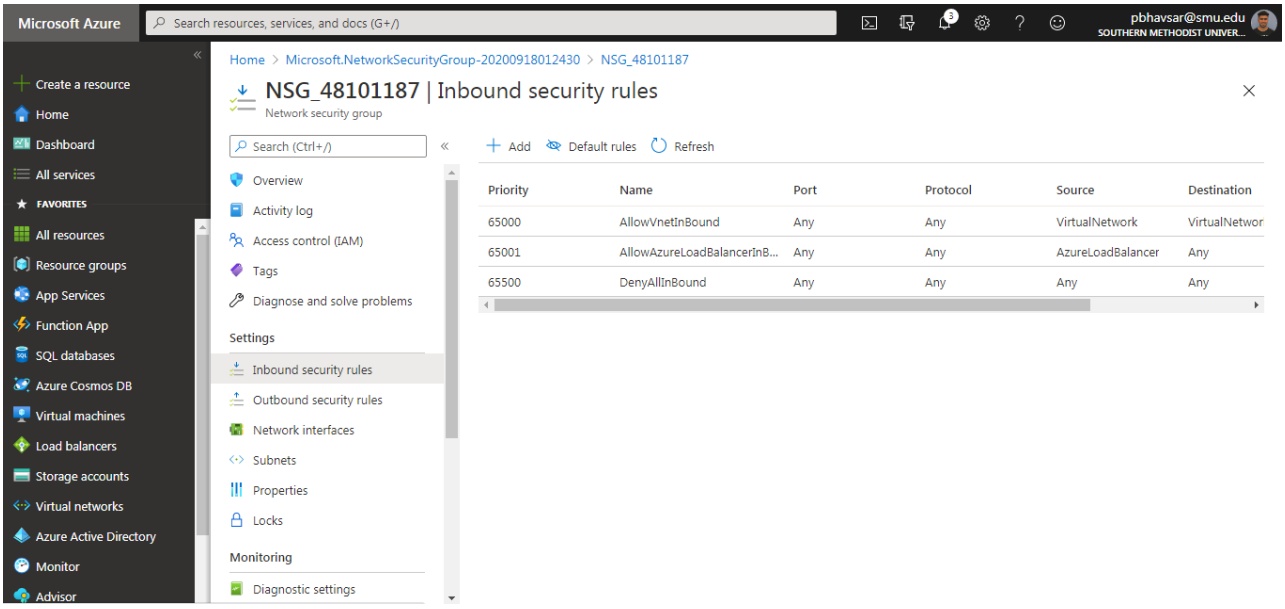
Review your Network Security Group settings and click on Create.



Wait for the Resource Deployment to get complete.

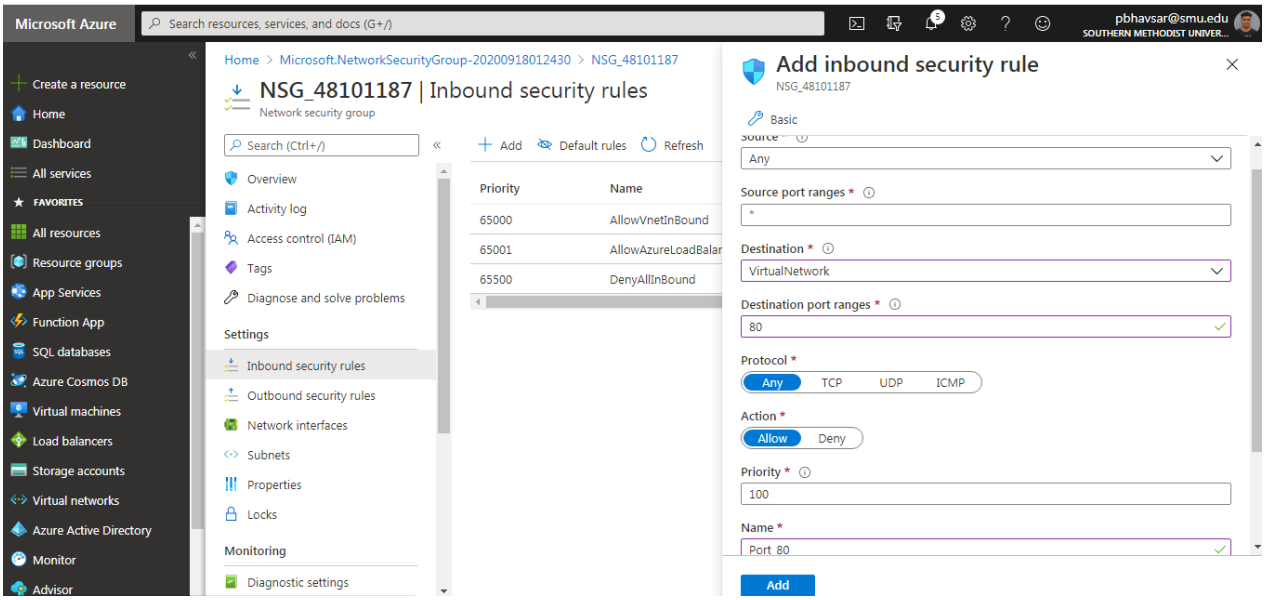


Under your Network Security Group, click on “Inbound Security Group”. You’ll observe the default Inbound rules which allows traffic from VNet, Azure Load Balancer and denies all the other traffic.



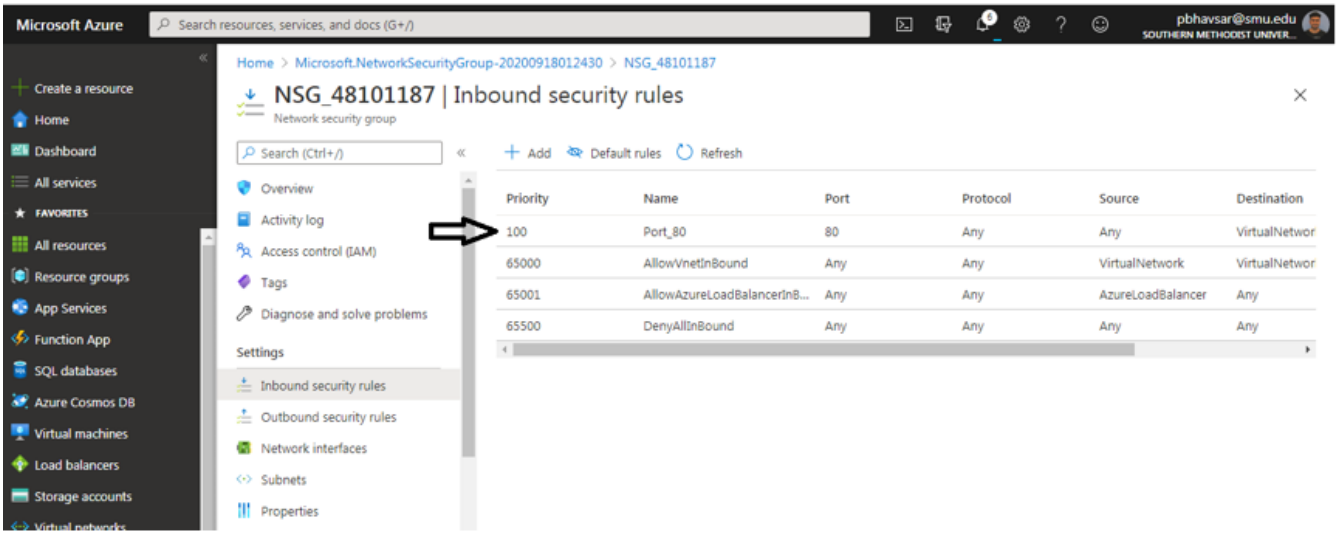
Add the Inbound Rule for the HTTP (Port 80) traffic as follows.

- Source: Any
- Source Port Ranges: *
- Destination: Virtual Network
- Destination Port Ranges: 80
- Name: Port_80



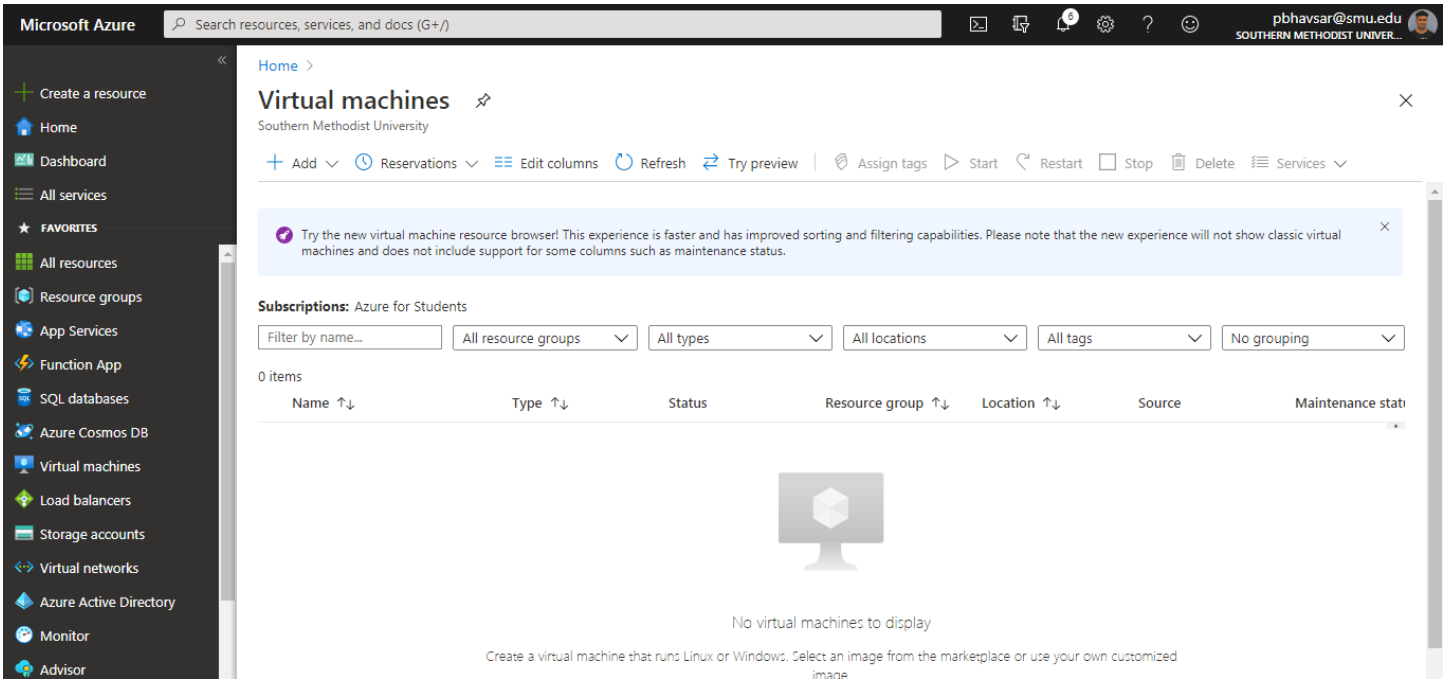
If you notice, we’ve specified Destination as VirtualNetwork. It means Network Security Group can be added at Virtual Machine level, Subnet level or entire Virtual Network (VNet) level. However, in AWS, we’ve security groups for securing EC2 Instances and NACL for security particular VPC Subnets.

Custom Inbound Rule to allow HTTP (Port 80) traffic has been enabled successfully.

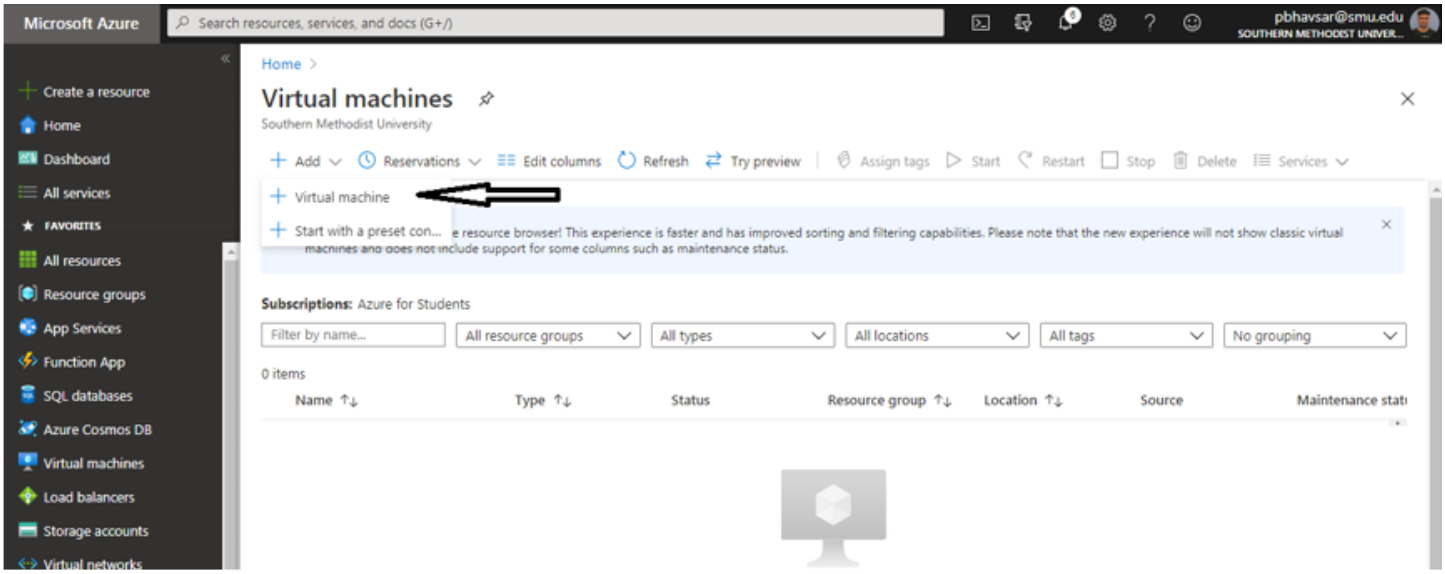


Task 4: Launch a Web Server Instance

Navigate to Microsoft Azure Portal and under the Search bar, search for the “Virtual Machines” Service.

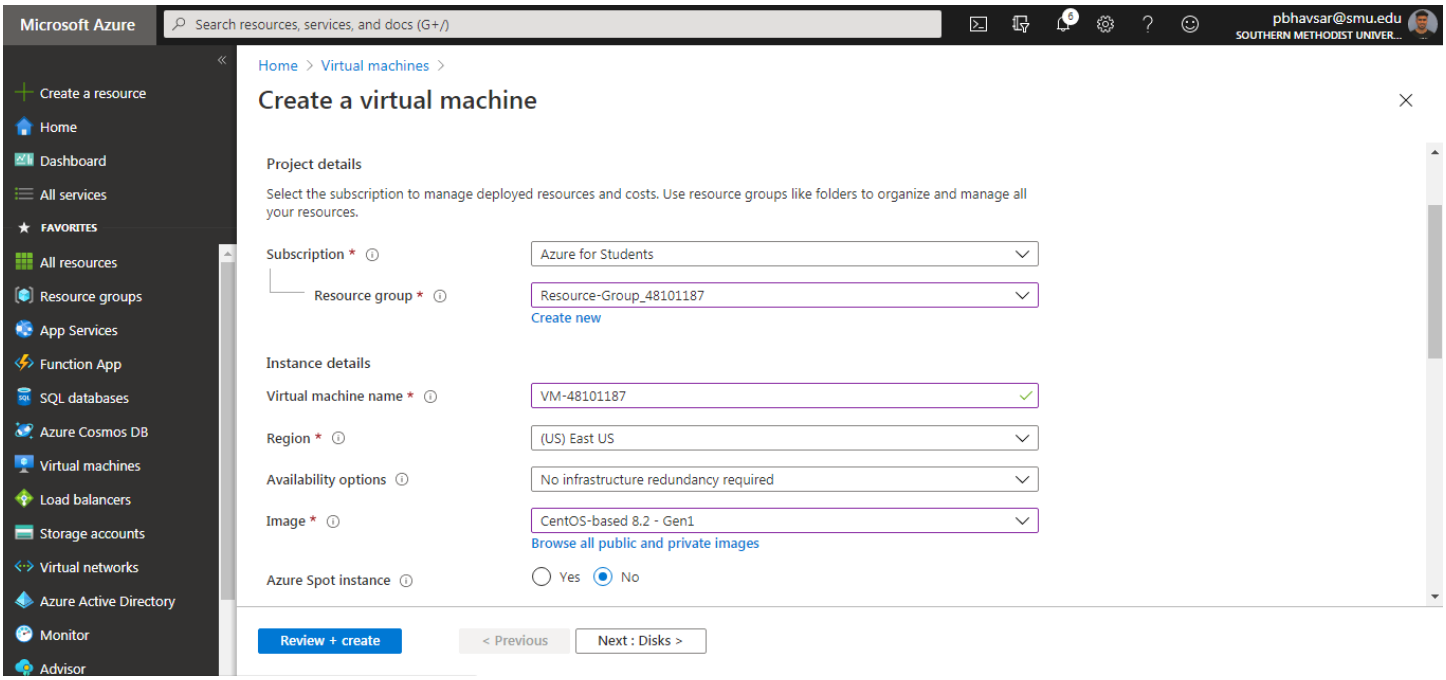


Click on "+ Add" to create a new Azure Virtual Machine (VM).

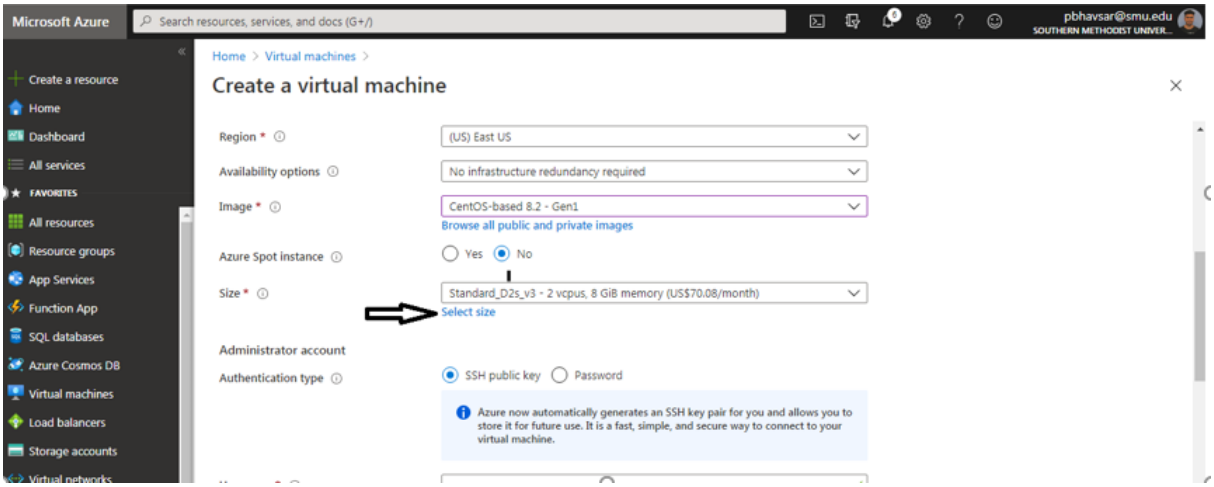


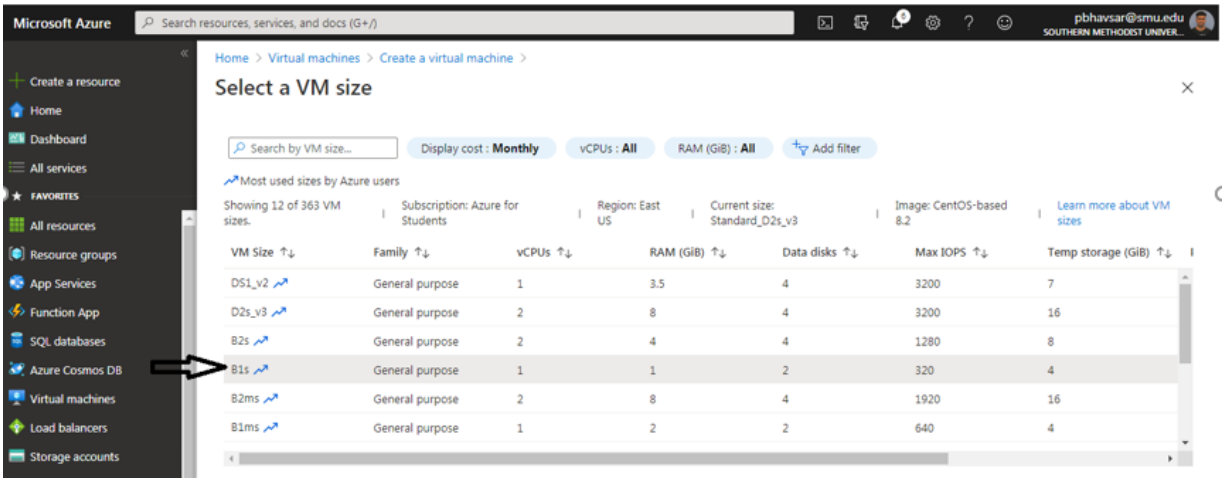
Under Resource Group, specify the Resource Group which you created earlier.

Specify the Virtual Machine Name, Region and Image as follow. We are deploying a CentOS-8 VM on Microsoft Azure.

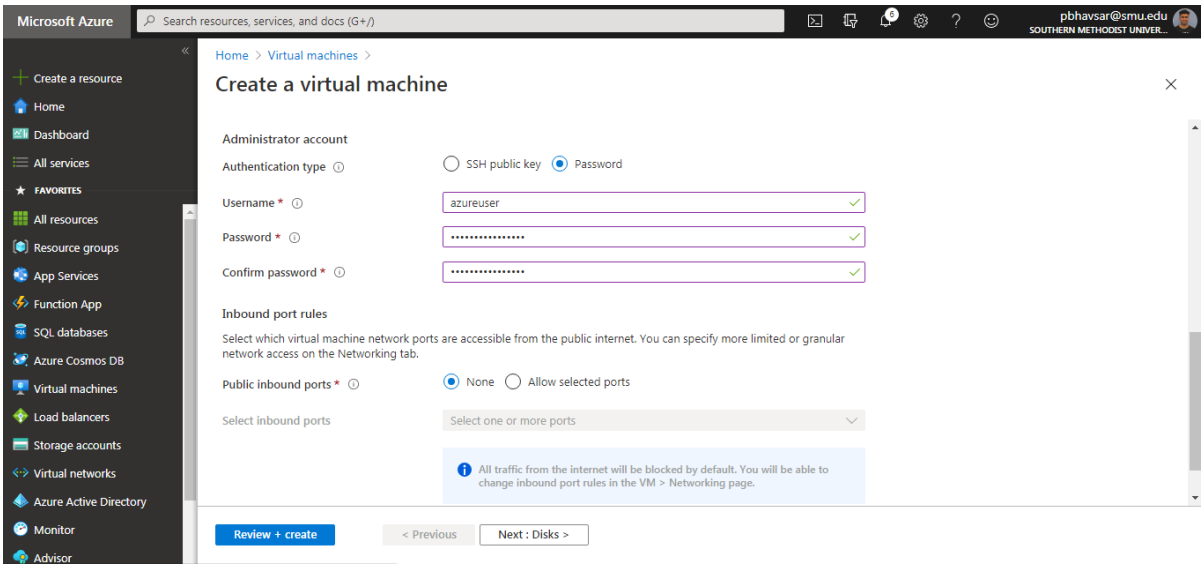


Select the Virtual Machine size as Standard_D2s_v3.

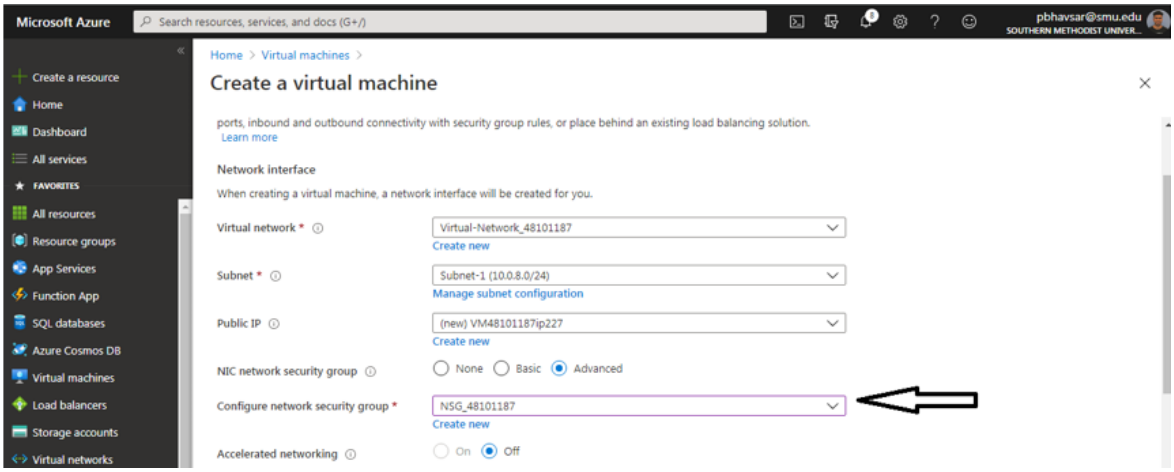




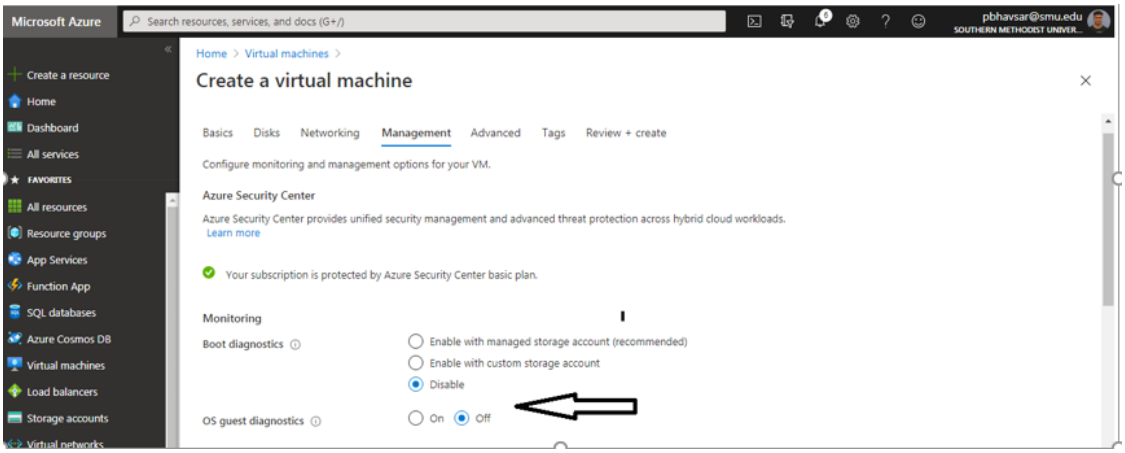
Select Authentication Type as Password, and Specify the Username as “azureuser” and Password of your choice. Do not specify any Inbound Ports, we’ll do it through Network Security Group (NSG).



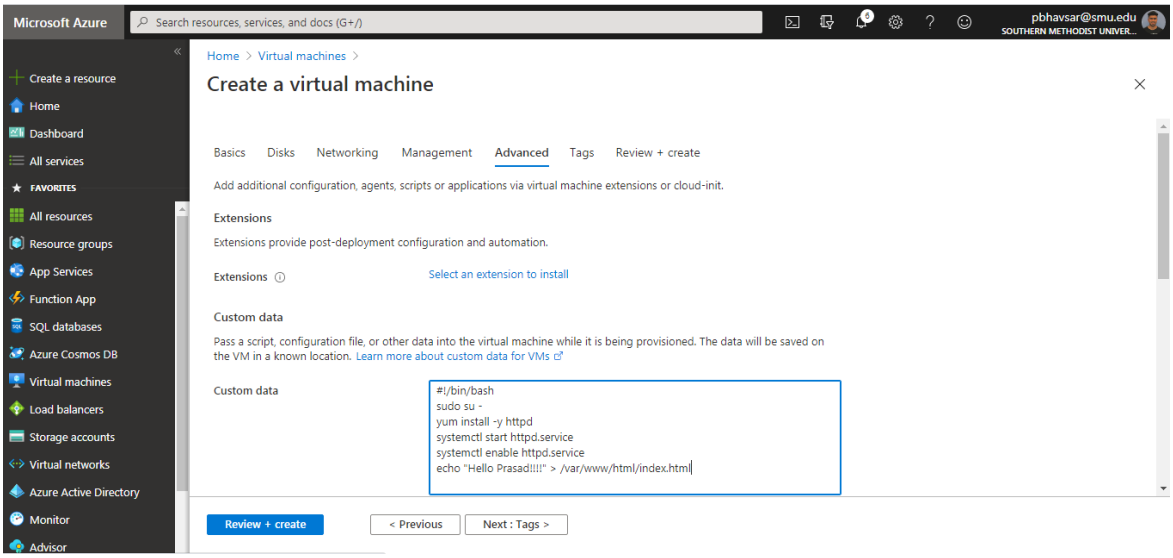
Specify the Virtual Network, Subnet, Network Security Group which we created earlier and generate a new Public IP.



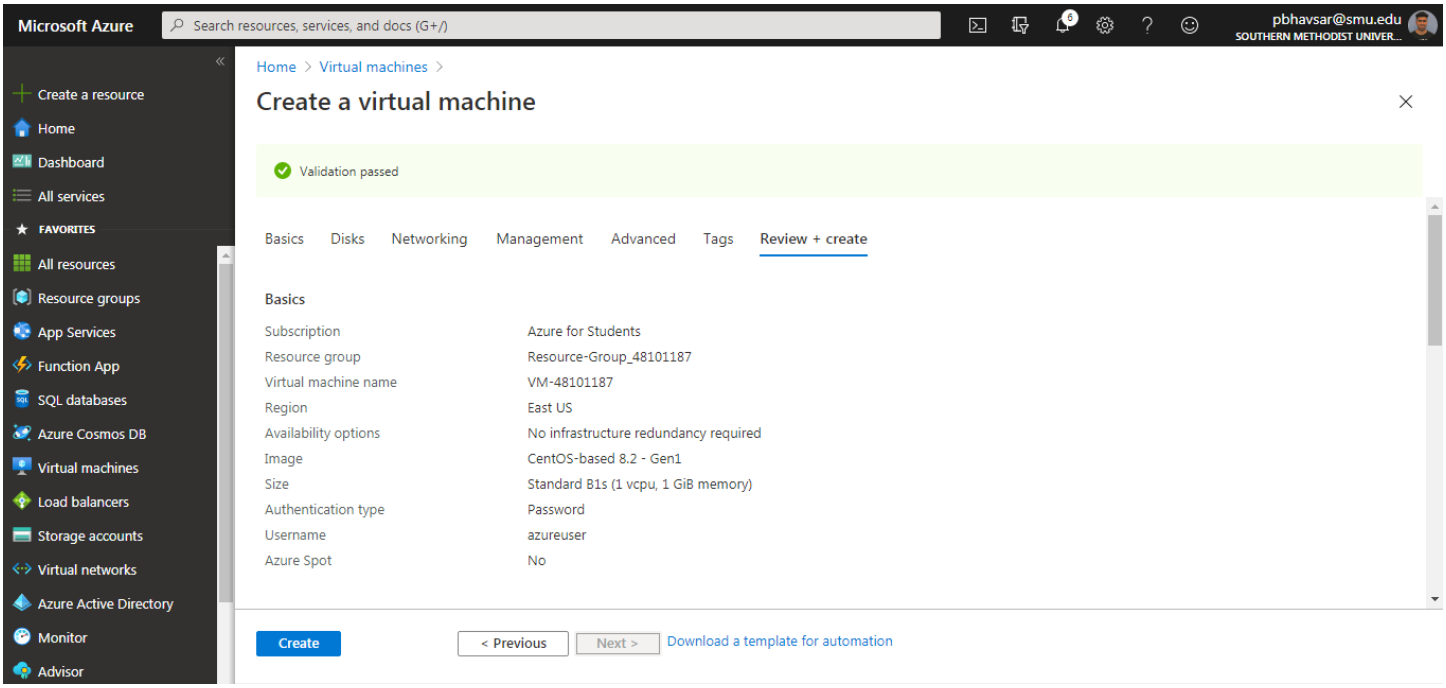
Disable Boot diagnostics and OS Guest Dianostics.



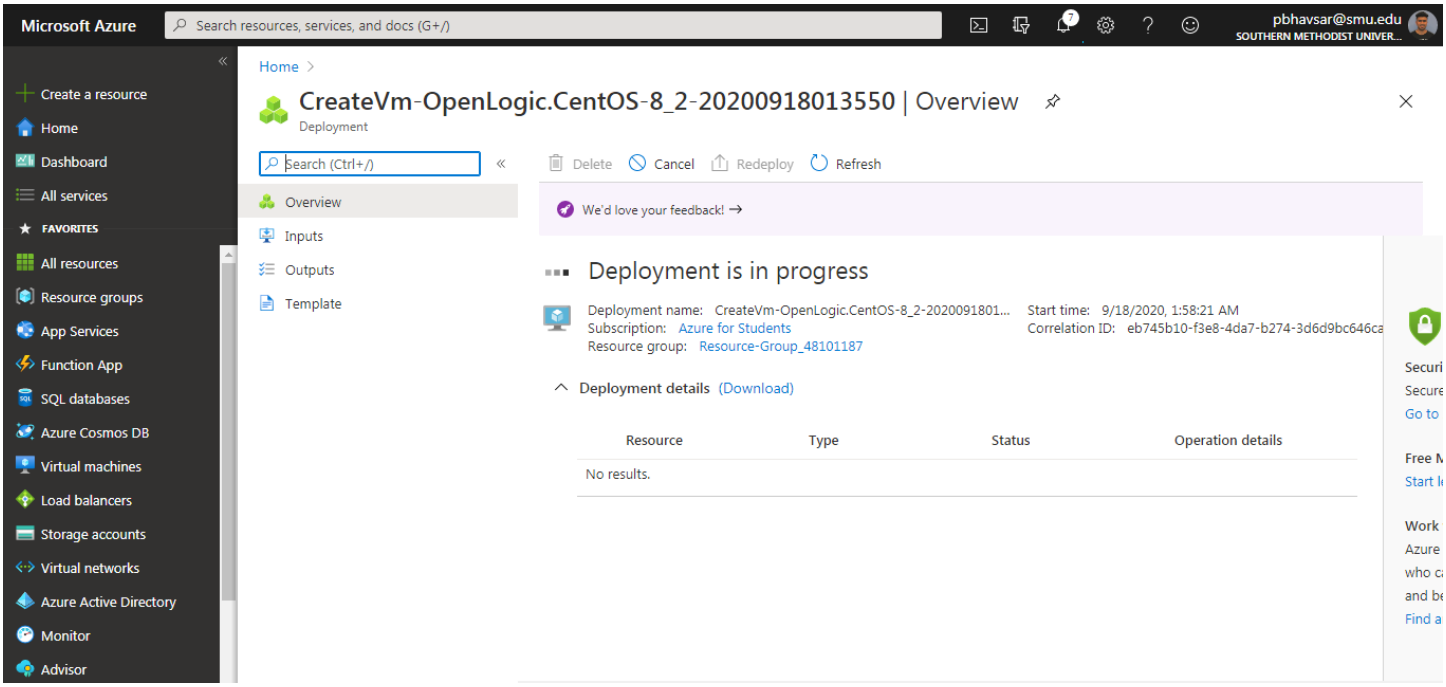
Now in the Advanced Tab, under “Custom Data”, write a bash script which would configure the Web Server for you during the Virtual Machine Boot Up process. This is exactly same as the “User Data” field in the AWS-EC2 Service.



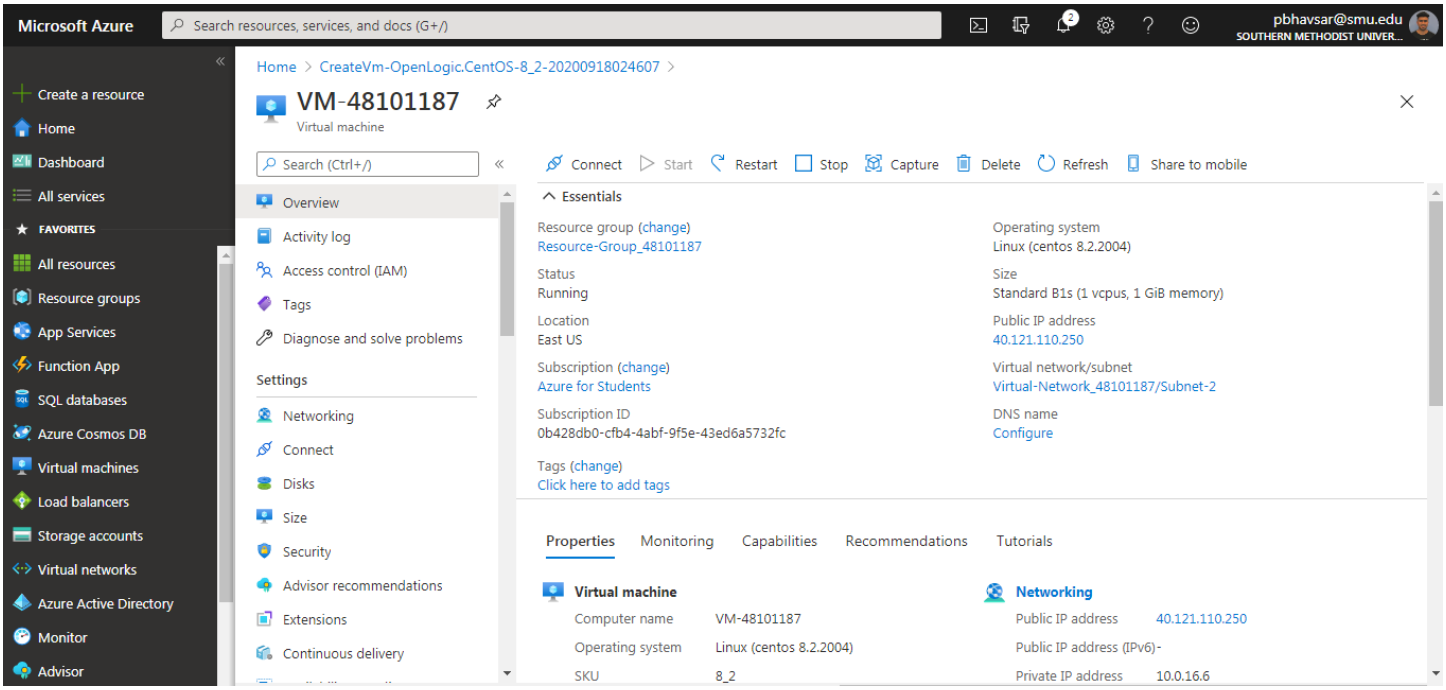
Review all the Virtual Machine's configurations and click on CREATE.



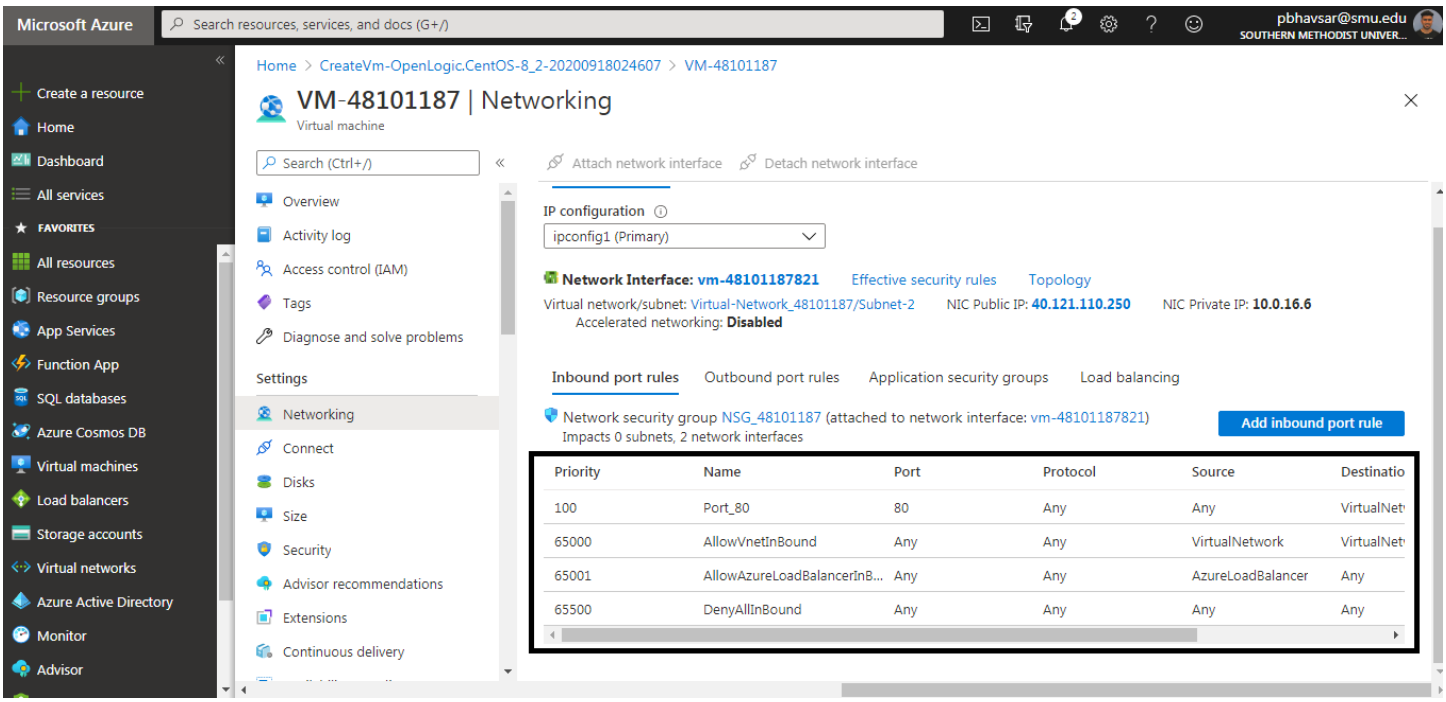
Wait for the Deployment to get complete.



Once completed, Under the Virtual Machine (VM), click on Overview.



Verify the Inbound Rules of the Network Security Group (NSG) has been applied to Virtual Machine or not?



Copy the Public IP Address of the Virtual Machine and Paste it in your Browser. It should open the Web Page.

Task 5: Update Network Security Group

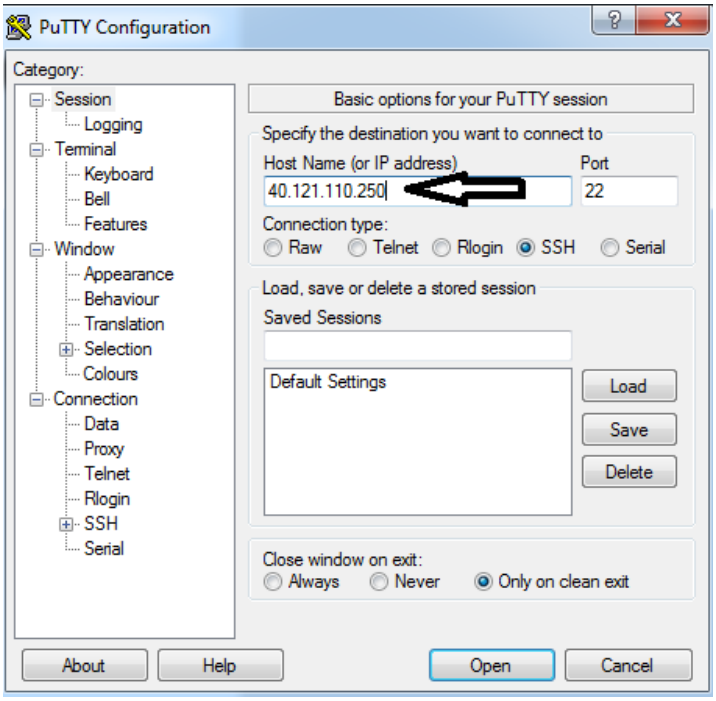
Let's download the PuTTY in our system now and access the Virtual Machine which we deployed on MS Azure.

Download and Install Putty on your local device:

https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

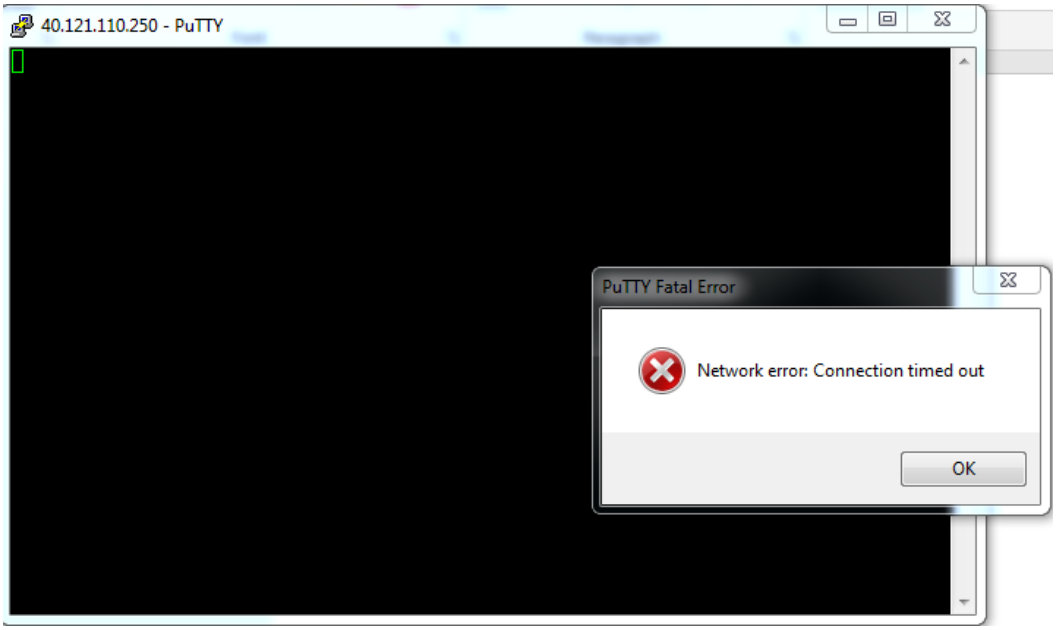
Copy the Public IP of the Virtual Machine (VM).

Open the PuTTY and Paste the Public IP of the Virtual Machine.



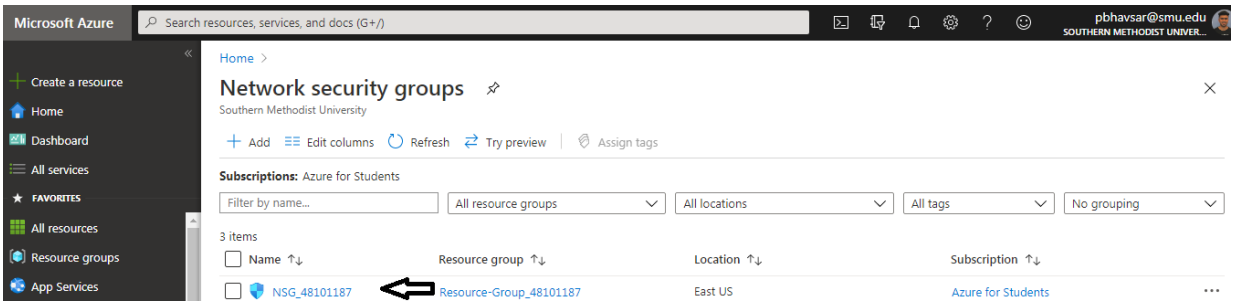
Login with your credentials.

It would fail as we haven't allowed SSH (Port: 22) traffic on the Network Security Group.

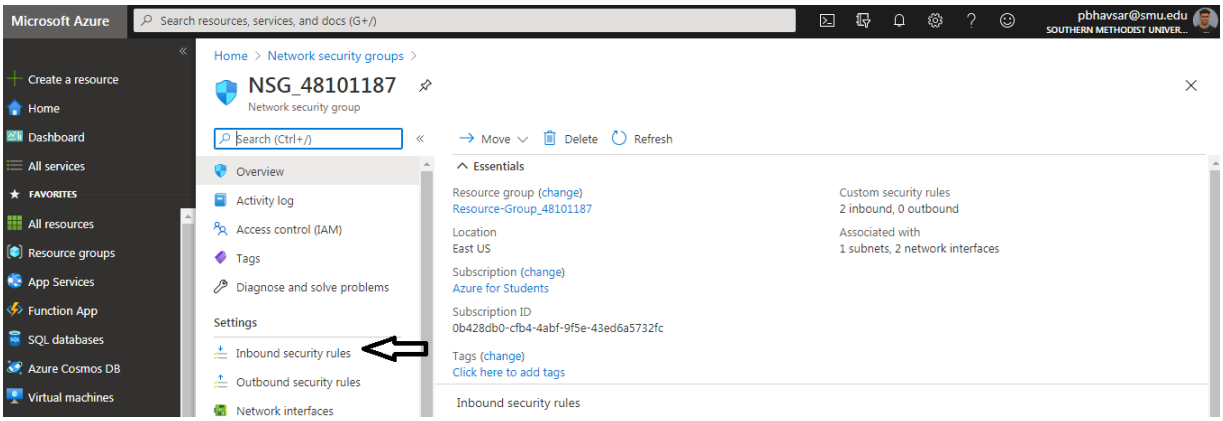


Let's first allow the SSH on the configured Network Security Group (NSG).

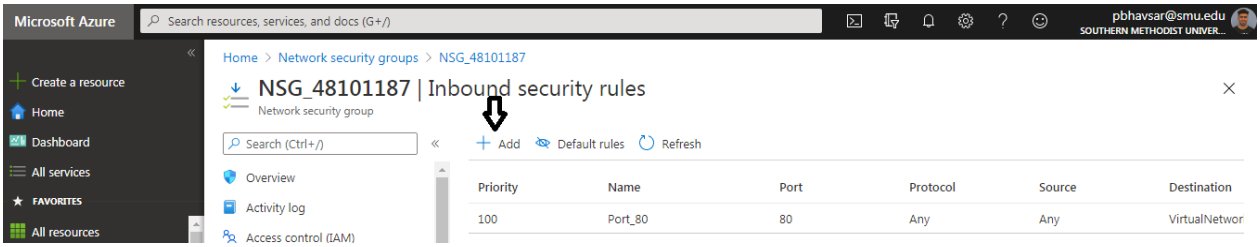
Navigate to Network Security Group (NSG) Service.



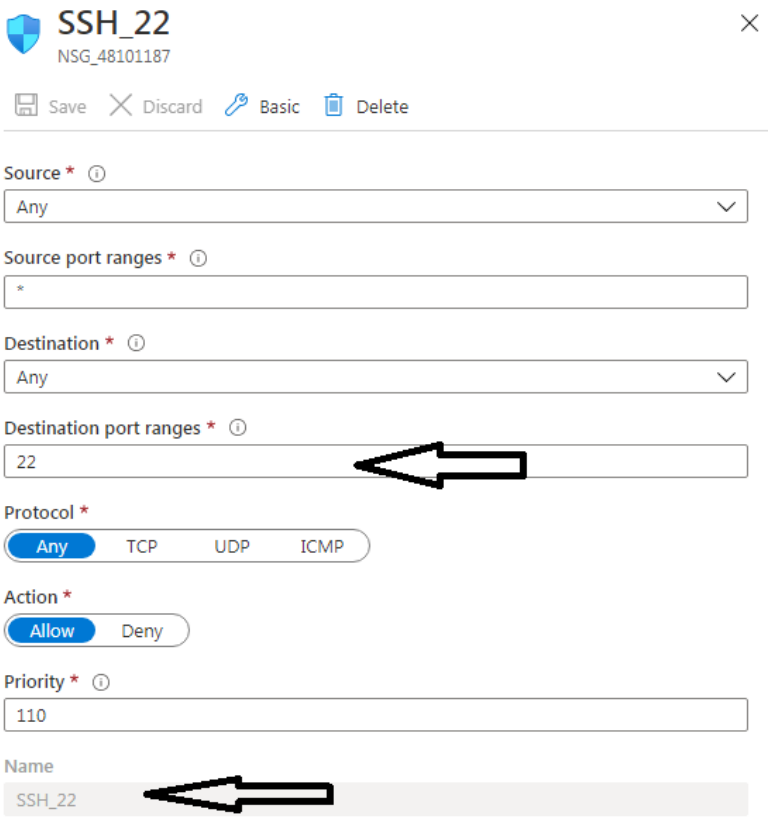
Click on Inbound Rules.



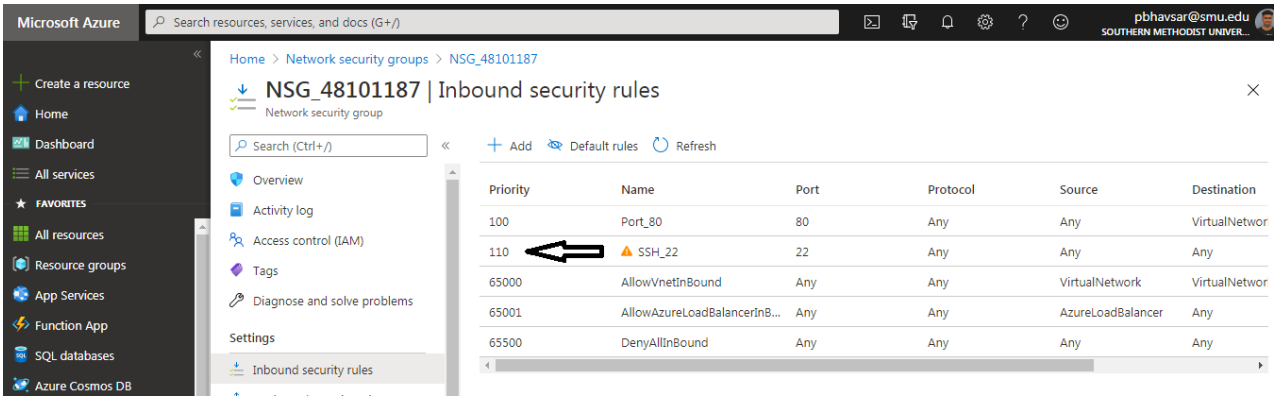
Click on Add.



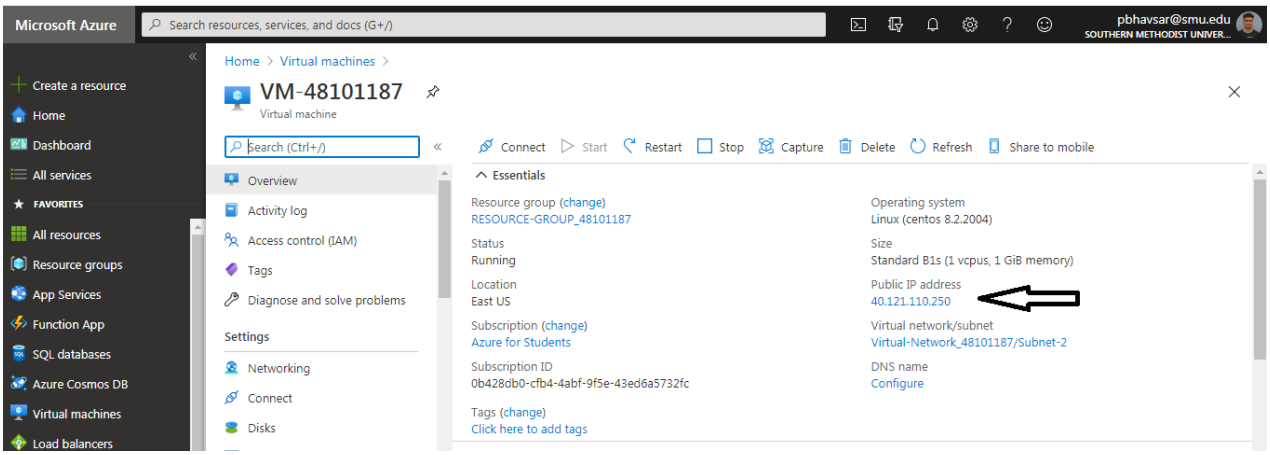
Select the Destination Port Ranges: 22 and specify the Rule Name as SSH_22 and click on Save.



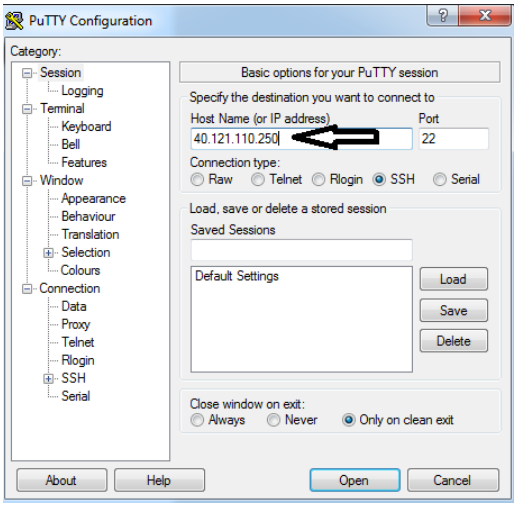
Your SSH Rule has been successfully configured on Network Security Group (NSG).



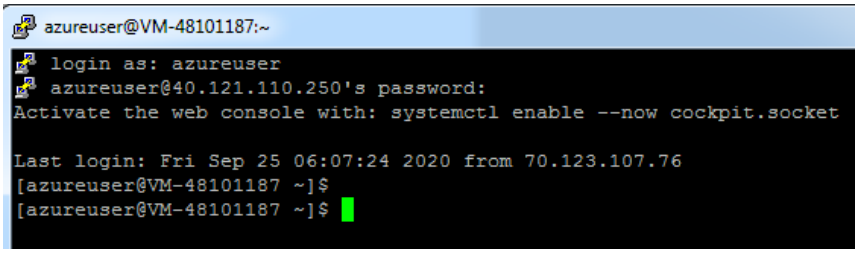
Again, copy the Public IP of the Azure Virtual Machine.



Open the PuTTY and Paste the Public IP of the Virtual Machine.



It would now be successful !!!



-----END OF LAB-----

For questions, contact on below information.
Email: pbhavsar@smu.edu