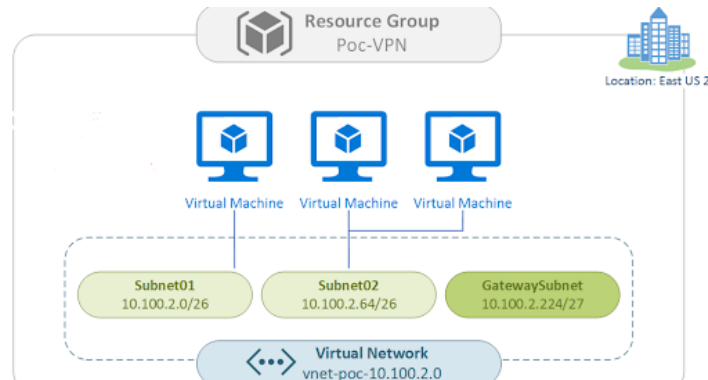
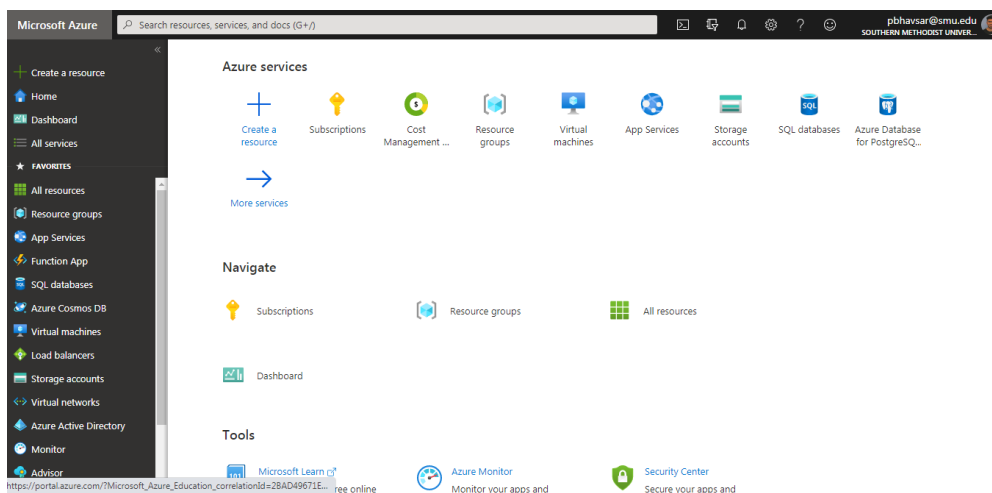


Lab: Build Your Azure Network Design and Launch a Web Server

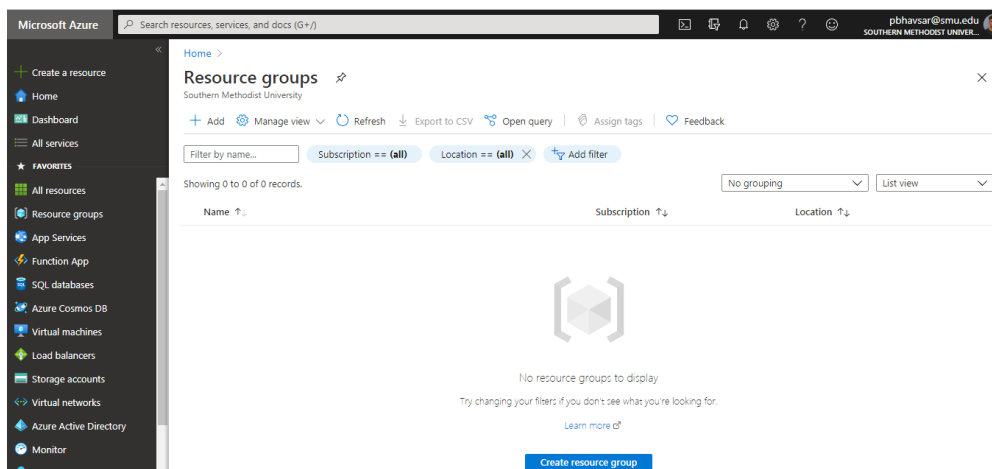
In this Lab, we'll create custom Resource Group along with Virtual Networks, Subnets and Security Groups. We will then launch a web server on one of the Public Subnet and access the Website externally.

**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”.

The screenshot shows the 'Create a resource group' page in the Microsoft Azure portal. The left sidebar contains navigation links: 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES', 'All resources', 'Resource groups', 'App Services', 'Function App', 'SQL databases', 'Azure Cosmos DB', 'Virtual machines', 'Load balancers', 'Storage accounts', 'Virtual networks', 'Azure Active Directory', 'Monitor', and 'Advisor'. The main content area is titled 'Create a resource group' and has tabs for 'Basics', 'Tags', and 'Review + create'. The 'Basics' tab is active. Below the tabs, there is a description of a resource group. The 'Project details' section contains two dropdown menus: 'Subscription *' set to 'Azure for Students' and 'Resource group *' set to 'Resource-Group_48101187'. The 'Resource details' section contains a dropdown menu: 'Region *' set to '(US) East US'. At the bottom, there are three buttons: 'Review + create' (highlighted in blue), '< Previous', and 'Next : Tags >'. The user's profile 'pbhavsar@smu.edu' is visible in the top right corner.

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

The screenshot shows the 'Create a resource group' page in the Microsoft Azure portal, now at the 'Review + create' step. The 'Basics' tab is still active. A green banner at the top of the main content area says 'Validation passed.' Below this, the 'Basics' section displays the configured values: 'Subscription' as 'Azure for Students', 'Resource group' as 'Resource-Group_48101187', and 'Region' as 'East US'. The 'Tags' section shows 'None'. At the bottom, there are four buttons: 'Create' (highlighted in blue), '< Previous', 'Next >', and a link 'Download a template for automation'. The user's profile 'pbhavsar@smu.edu' is visible in the top right corner.

Now under Search, search for Virtual Networks.

The screenshot shows the Microsoft Azure portal search results for 'Virtual Networks'. The search bar at the top contains 'Virtual N'. The results are categorized into Services, Marketplace, Documentation, and Resource Groups. Under Services, 'Virtual networks' is highlighted with a black arrow. Other services listed include Virtual network gateways, Virtual networks (classic), Virtual machines, Private DNS zones, Subscriptions, Virtual WANs, Virtual machine scale sets, Storage accounts, and SQL virtual machines. The Marketplace section lists Virtual network gateway, Virtual Network, Azure Virtual Network Endpoints Management, and Hillstone CloudEdge Virtual NGFW Standard Edition. The Documentation section includes links for NC-series, Windows Virtual Desktop, NVv3-series, and creating virtual nodes in Azure Kubernetes. The Resource Groups section shows 'No results were found.' The left sidebar shows the navigation menu with 'Virtual networks' selected. The right sidebar shows 'Last Viewed' items: SQL databases and Azure Database for PostgreSQL.

Click on "+Add".

The screenshot shows the Microsoft Azure portal 'Virtual networks' page. The page title is 'Virtual networks' with a star icon. Below the title, there are links for '+ Add', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', 'Assign tags', and 'Feedback'. A search bar is present with the text 'Filter by name...'. Below the search bar, there are filters for 'Subscription == (all)', 'Resource group == (all)', and 'Location == (all)', along with an 'Add filter' button. The page shows 'Showing 0 to 0 of 0 records.' and a table with columns for Name, Resource group, Location, and Subscription. The table is empty, and a message states 'No virtual networks to display'. Below the message, it says 'Create a virtual network to securely connect your Azure resources to each other. Connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute.' and a 'Learn more' link. At the bottom, there is a 'Create virtual network' button. The left sidebar shows the navigation menu with 'Virtual networks' selected. The right sidebar shows 'Last Viewed' items: SQL databases and Azure Database for PostgreSQL.

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

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal. The 'Basics' tab is selected. The 'Project details' section shows 'Subscription' as 'Azure for Students' and 'Resource group' as 'Resource-Group_48101187'. The 'Instance details' section shows 'Name' as 'Virtual-Network_48101187' and 'Region' as '(US) East US'. The 'Review + create' button is visible at the bottom.

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”.

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal, now on the 'IP Addresses' tab. The 'IPv4 address space' is set to '10.0.0.0/16'. The 'Add IPv6 address space' checkbox is unchecked. The 'Subnet' section shows a table with columns 'Subnet name' and 'Subnet address range'. A row is added with 'default' as the subnet name and '10.0.0.0/24' as the address range. The '+ Add subnet' button is highlighted with a red arrow.

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

Microsoft Azure

Home > Virtual networks >

Create virtual network

Basics IP Addresses Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses)

☐ Add IPv6 address space

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

+ Add subnet - Remove subnet

Subnet name	Subnet address range
This virtual network doesn't have any subnets.	

Add subnet

Subnet name * Subnet-1

Subnet address range * 10.0.8.0/24

10.0.8.0 - 10.0.8.255 (251 + 5 Azure reserved addresses)

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services 0 selected

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

Microsoft Azure

Home > Virtual networks >

Create virtual network

Basics IP Addresses Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses)

☐ Add IPv6 address space

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

+ Add subnet - Remove subnet

Subnet name	Subnet address range
Subnet-1	10.0.8.0/24

Add subnet

Subnet name * Subnet-2

Subnet address range * 10.0.16.0/24

10.0.16.0 - 10.0.16.255 (251 + 5 Azure reserved addresses)

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services 0 selected

Microsoft Azure

Home > Virtual networks >

Create virtual network

Basics IP Addresses Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses)

☐ Add IPv6 address space

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

+ Add subnet - Remove subnet

Subnet name	Subnet address range
Subnet-1	10.0.8.0/24
Subnet-2	10.0.16.0/24

Review + create < Previous Next > Security > Download a template for automation

Keep the Security settings as defaults.

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal. The 'Security' tab is selected, showing options for BastionHost, DDoS Protection Standard, and Firewall, all set to 'Disable'. The 'Review + create' button is visible at the bottom.

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

Home > Virtual networks >

Create virtual network

Basics IP Addresses **Security** Tags Review + create

BastionHost ☒ Disable ☐ Enable

DDoS Protection Standard ☒ Disable ☐ Enable

Firewall ☒ Disable ☐ Enable

[Review + create](#) [< Previous](#) [Next : Tags >](#) [Download a template for automation](#)

Review the Virtual Network configuration settings and click on Create.

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal, now in the 'Review + create' tab. A green banner indicates 'Validation passed'. The configuration details for Basics, IP addresses, and Tags are displayed.

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

Home > Virtual networks >

Create virtual network

Basics IP Addresses Security Tags **Review + create**

Validation passed

Basics

Subscription	Azure for Students
Resource group	Resource-Group_48101187
Name	Virtual-Network_48101187
Region	East US

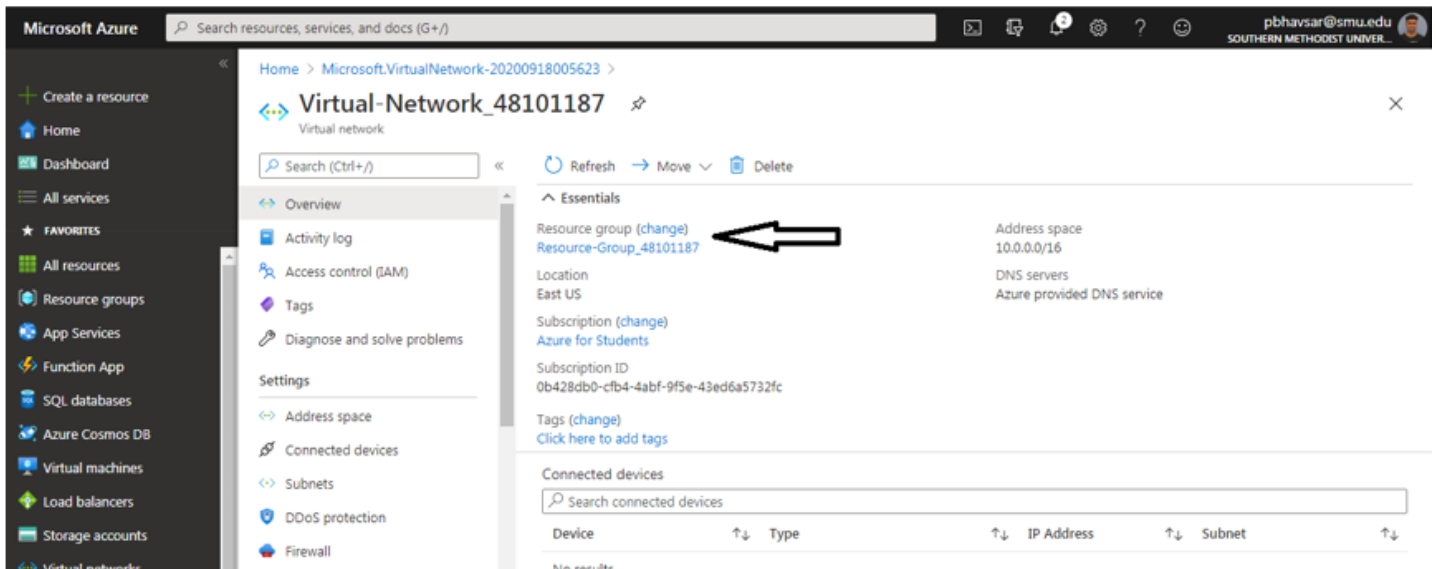
IP addresses

Address space	10.0.0.0/16
Subnet	Subnet-1 (10.0.8.0/24), Subnet-2 (10.0.16.0/24)

Tags

[Create](#) [< Previous](#) [Next >](#) [Download a template for automation](#)

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.



Microsoft Azure

Home > Microsoft.VirtualNetwork-20200918005623 > Virtual-Network_48101187

Virtual network

Search (Ctrl+/)

Refresh Move Delete

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

DDoS protection

Firewall

Essentials

Resource group (change) **Resource-Group_48101187**

Address space 10.0.0.0/16

DNS servers Azure provided DNS service

Location East US

Subscription (change) Azure for Students

Subscription ID 0b428db0-cfb4-4abf-9f5e-43ed6a5732fc

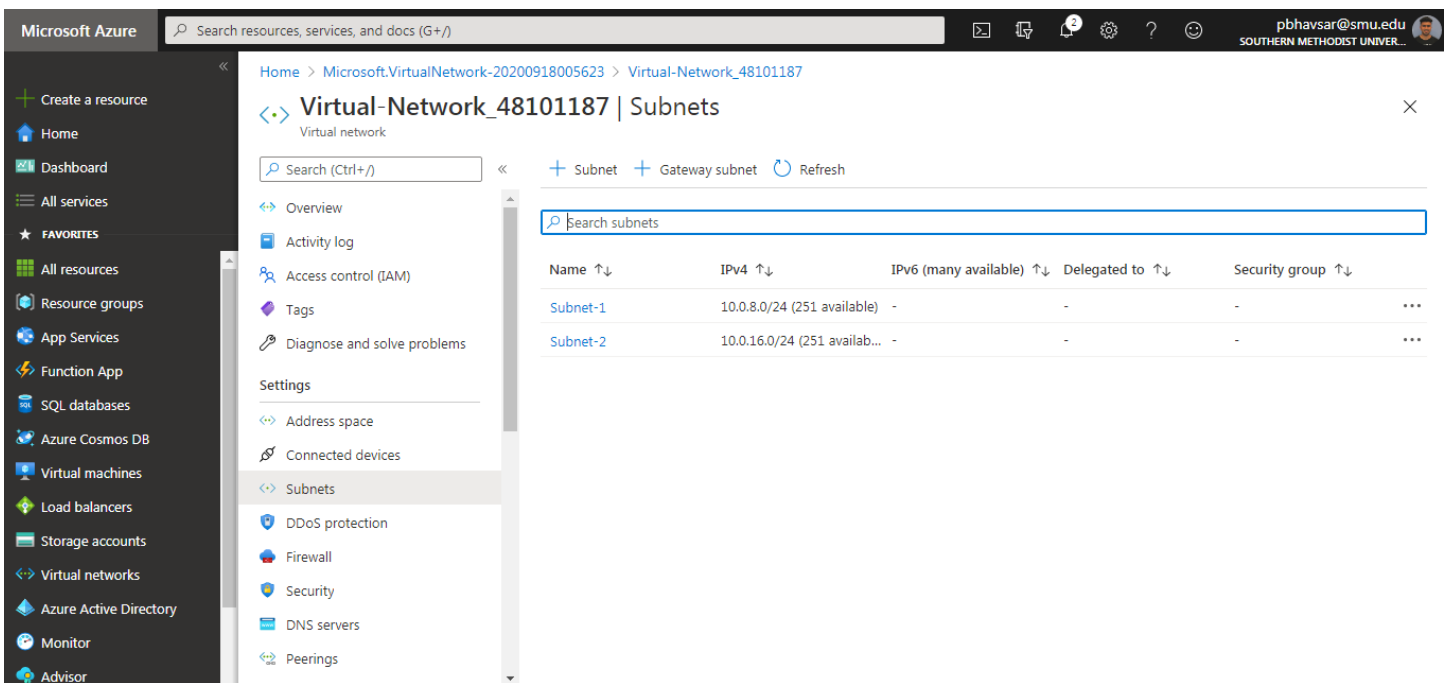
Tags (change) Click here to add tags

Connected devices

Search connected devices

Device	Type	IP Address	Subnet
No results			

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



Microsoft Azure

Home > Microsoft.VirtualNetwork-20200918005623 > Virtual-Network_48101187

Virtual network

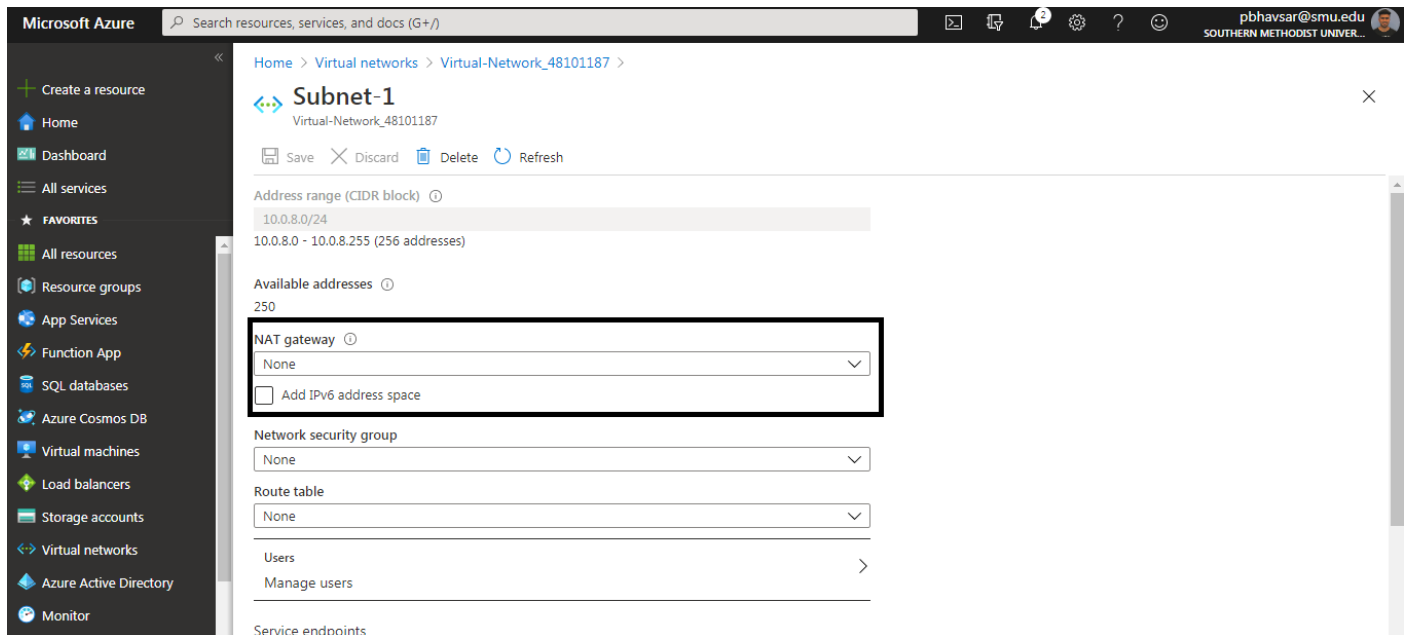
Search (Ctrl+/)

+ Subnet + Gateway subnet Refresh

Search subnets

Name	IPv4	IPv6 (many available)	Delegated to	Security group
Subnet-1	10.0.8.0/24 (251 available)	-	-	-
Subnet-2	10.0.16.0/24 (251 availab...	-	-	-

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.

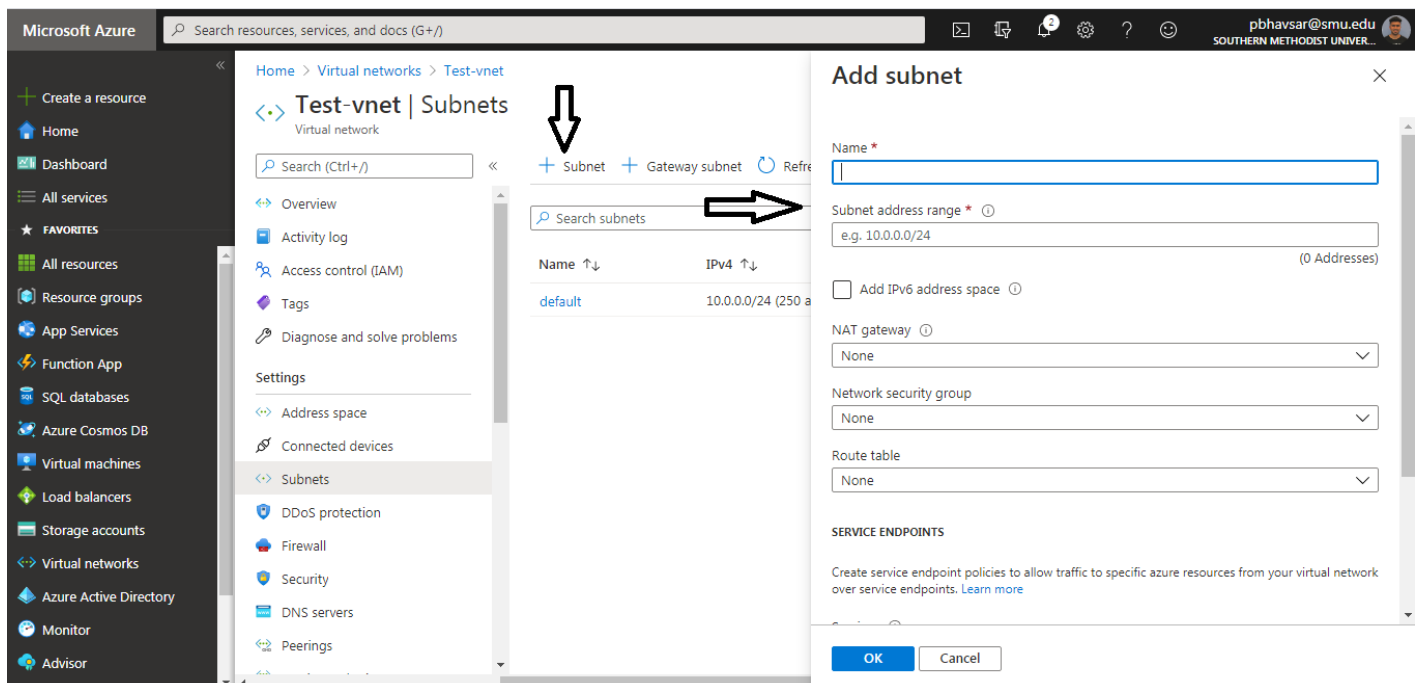


Similarly, verify the Subnet-2 which is also Public Subnet.

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”.

Microsoft Azure

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

Home >

Network security groups

Southern Methodist University

+ Add Edit columns Refresh Try preview Assign tags

Subscriptions: Azure for Students

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

0 items

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

No network security groups to display

Create a network security group with rules to filter inbound traffic to, and outbound traffic from, virtual machines and subnets. [Learn more >](#)

Create network security group

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

Microsoft Azure

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

Home > Network security groups >

Create network security group

Basics Tags Review + create

Project details

Subscription * Azure for Students

Resource group * Resource-Group_48101187

Instance details

Name * NSG_48101187

Region * (US) East US

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

Review your Network Security Group settings and click on Create.

Microsoft Azure

Search resources, services, and docs (G+)

Home > Network security groups >

Create network security group

Validation passed

Basics Tags Review + create

Basics

Subscription	Azure for Students
Resource group	Resource-Group_48101187
Region	East US
name	NSG_48101187

Tags

None

Create < Previous Next > Download a template for automation

Wait for the Resource Deployment to get complete.

Microsoft Azure

Search resources, services, and docs (G+)

Home >

Microsoft.NetworkSecurityGroup-20200918012430 | Overview

Deployment

Search (Ctrl+)

Delete Cancel Redeploy Refresh

We'd love your feedback! →

✓ Your deployment is complete

Deployment name: Microsoft.NetworkSecurityGroup-20200918012... Start time: 9/18/2020, 1:26:11 AM
Subscription: Azure for Students Correlation ID: c1097097-10a7-42a7-a9da-7efe1ffff1b5
Resource group: Resource-Group_48101187

Deployment details (Download)

Next steps

Go to resource

Security
Secure y
Go to Az
Free Mic
Start lea
Work wi
Azure ex
who can
and be y
Find an ,

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.

Priority	Name	Port	Protocol	Source	Destination
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

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

Add inbound security rule

Basic

Source: Any

Source port ranges: *

Destination: VirtualNetwork

Destination port ranges: 80

Protocol: Any

Action: Allow

Priority: 100

Name: Port_80

Add

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.

The screenshot shows the Microsoft Azure portal interface. On the left is a navigation pane with options like 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES', 'All resources', 'Resource groups', 'App Services', 'Function App', 'SQL databases', 'Azure Cosmos DB', 'Virtual machines', 'Load balancers', 'Storage accounts', and 'Virtual networks'. The main area displays the 'NSG_48101187 | Inbound security rules' page for a network security group. A table lists the inbound security rules:

Priority	Name	Port	Protocol	Source	Destination
100	Port_80	80	Any	Any	VirtualNetwork
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

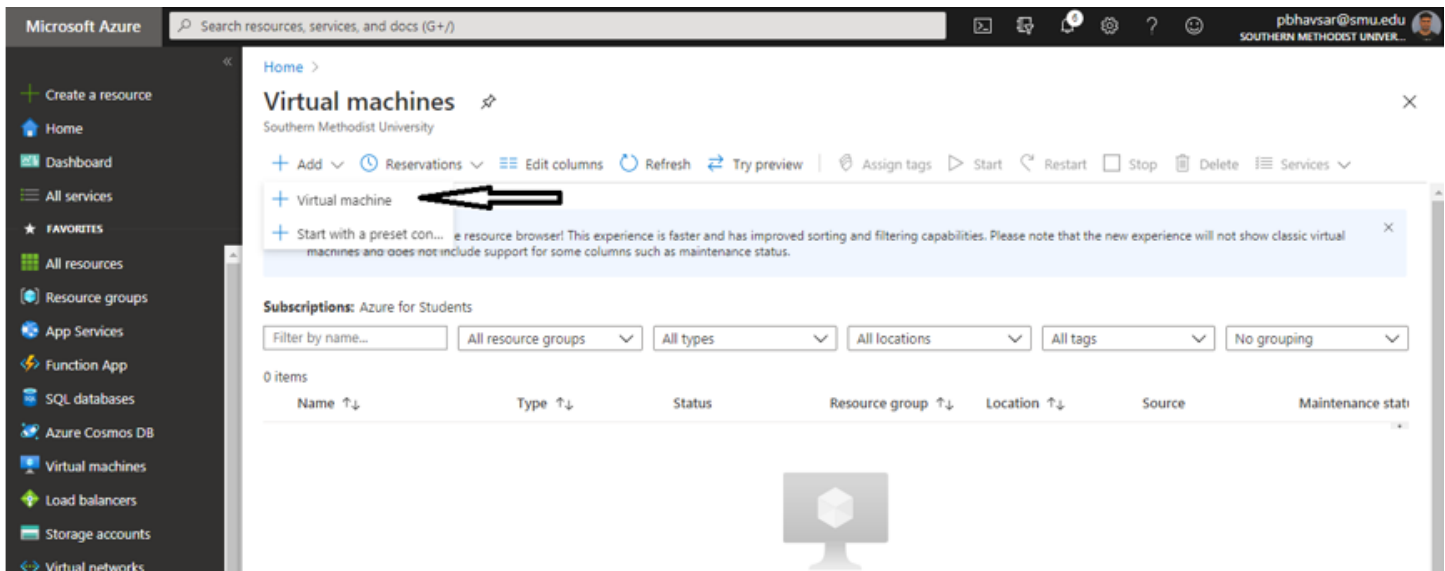
A black arrow points to the 'Port_80' rule in the table.

Task 4: Launch a Web Server Instance

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

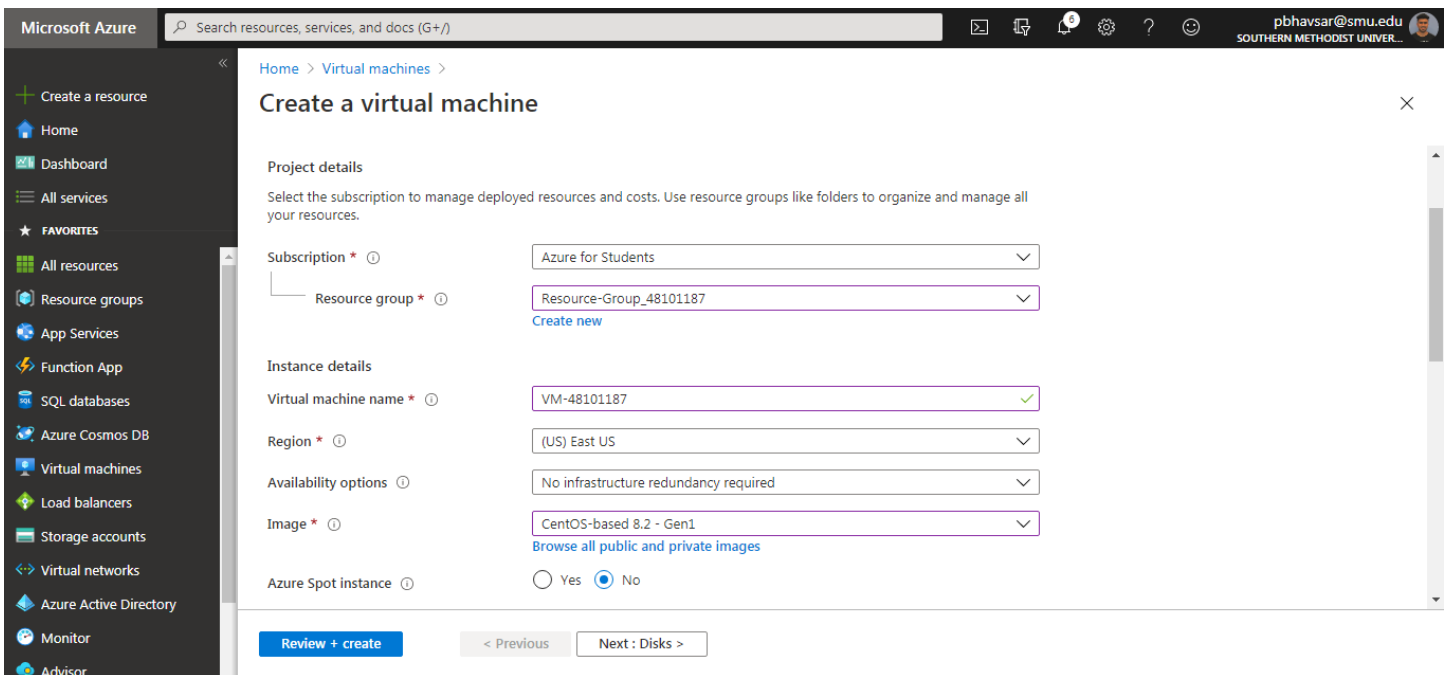
The screenshot shows the Microsoft Azure portal interface. On the left is a navigation pane with options like 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES', 'All resources', 'Resource groups', 'App Services', 'Function App', 'SQL databases', 'Azure Cosmos DB', 'Virtual machines', 'Load balancers', 'Storage accounts', 'Virtual networks', 'Azure Active Directory', 'Monitor', and 'Advisor'. The main area displays the 'Virtual machines' page for 'Southern Methodist University'. A message banner at the top says: 'Try the new virtual machine resource browser! This experience is faster and has improved sorting and filtering capabilities. Please note that the new experience will not show classic virtual machines and does not include support for some columns such as maintenance status.' Below the banner, there are filters for 'Subscriptions: Azure for Students', 'Filter by name...', 'All resource groups', 'All types', 'All locations', 'All tags', and 'No grouping'. The table below shows '0 items' with columns: Name, Type, Status, Resource group, Location, Source, and Maintenance status. A large icon of a computer monitor with a cube on it is displayed in the center of the table, with the text 'No virtual machines to display' below it. At the bottom, there is a prompt: 'Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.'

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.

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

Home > Virtual machines > Create a virtual machine

Region: (US) East US

Availability options: No infrastructure redundancy required

Image: CentOS-based 8.2 - Gen1

Azure Spot Instance: ☐ Yes ☒ No

Size: Standard_D2s_v3 - 2 vcpus, 8 GiB memory (US\$70.08/month)

Administrator account authentication type: ☒ SSH public key ☐ Password

Info: Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.

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

Home > Virtual machines > Create a virtual machine > Select a VM size

Search by VM size... | Display cost: Monthly | vCPUs: All | RAM (GiB): All | Add filter

Most used sizes by Azure users

Showing 12 of 363 VM sizes | Subscription: Azure for Students | Region: East US | Current size: Standard_D2s_v3 | Image: CentOS-based 8.2 | Learn more about VM sizes

VM Size	Family	vCPUs	RAM (GiB)	Data disks	Max IOPS	Temp storage (GiB)
D51_v2	General purpose	1	3.5	4	3200	7
D2s_v3	General purpose	2	8	4	3200	16
B2s	General purpose	2	4	4	1280	8
B1s	General purpose	1	1	2	320	4
B2ms	General purpose	2	8	4	1920	16
B1ms	General purpose	1	2	2	640	4

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).

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

Home > Virtual machines > Create a virtual machine

Administrator account authentication type: ☐ SSH public key ☒ Password

Username: azureuser

Password: [masked]

Confirm password: [masked]

Inbound port rules: Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports: ☒ None ☐ Allow selected ports

Select inbound ports: Select one or more ports

Info: All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Buttons: Review + create, < Previous, Next: Disks >

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

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

Home > Virtual machines >

Create a virtual machine

ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * [Create new](#)

Subnet * [Manage subnet configuration](#)

Public IP [Create new](#)

NIC network security group ☐ None ☐ Basic ☒ Advanced

Configure network security group * [Create new](#) ←

Accelerated networking ☐ On ☒ Off

Disable Boot diagnostics and OS Guest Diagnostics.

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

Home > Virtual machines >

Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Configure monitoring and management options for your VM.

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. [Learn more](#)

✓ Your subscription is protected by Azure Security Center basic plan.

Monitoring

Boot diagnostics ☐ Enable with managed storage account (recommended)
☐ Enable with custom storage account
☒ Disable ←

OS guest diagnostics ☐ On ☒ Off

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.

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

Home > Virtual machines >

Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions

Extensions provide post-deployment configuration and automation.

Extensions

Custom data

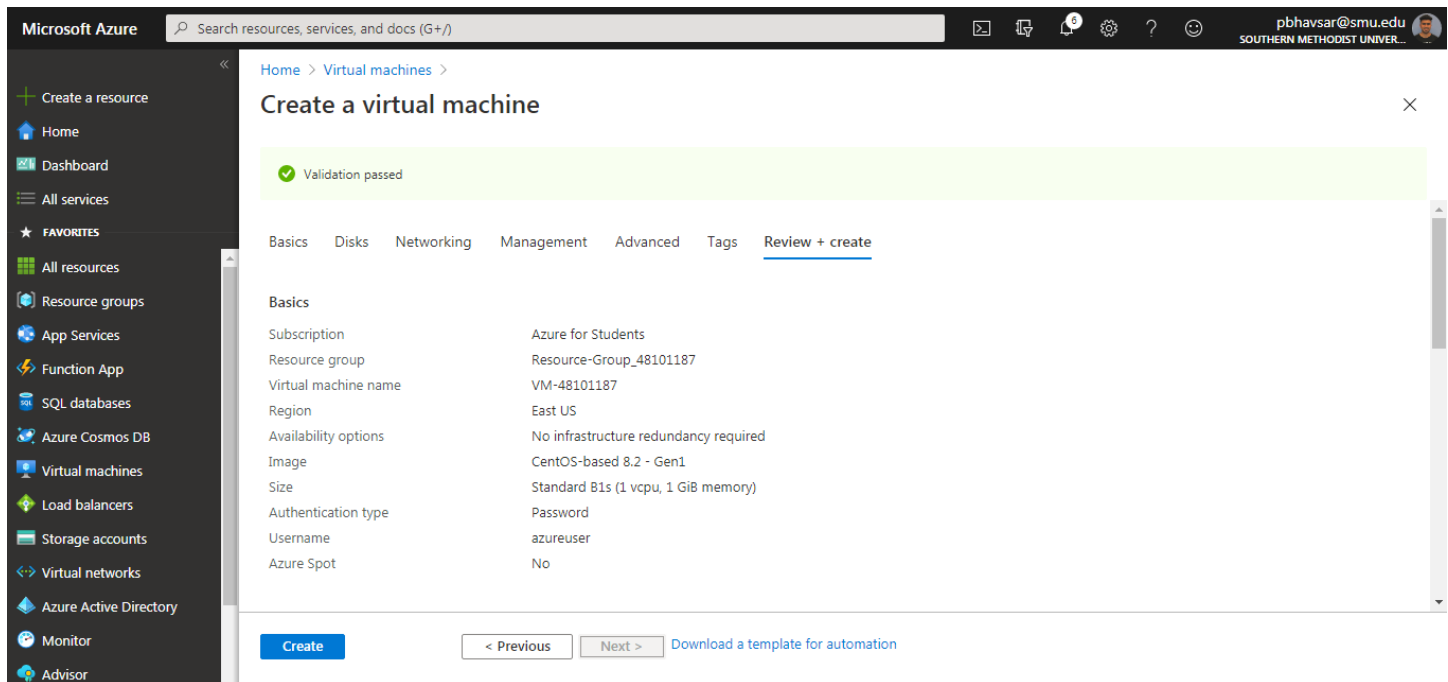
Pass a script, configuration file, or other data into the virtual machine while it is being provisioned. The data will be saved on the VM in a known location. [Learn more about custom data for VMs](#)

Custom data

```
#!/bin/bash
sudo su -
yum install -y httpd
systemctl start httpd.service
systemctl enable httpd.service
echo "Hello Prasad!!!!" > /var/www/html/index.html
```

[Review + create](#) [Previous](#) [Next: Tags](#)

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



Microsoft Azure

Home > Virtual machines >

Create a virtual machine

Validation passed

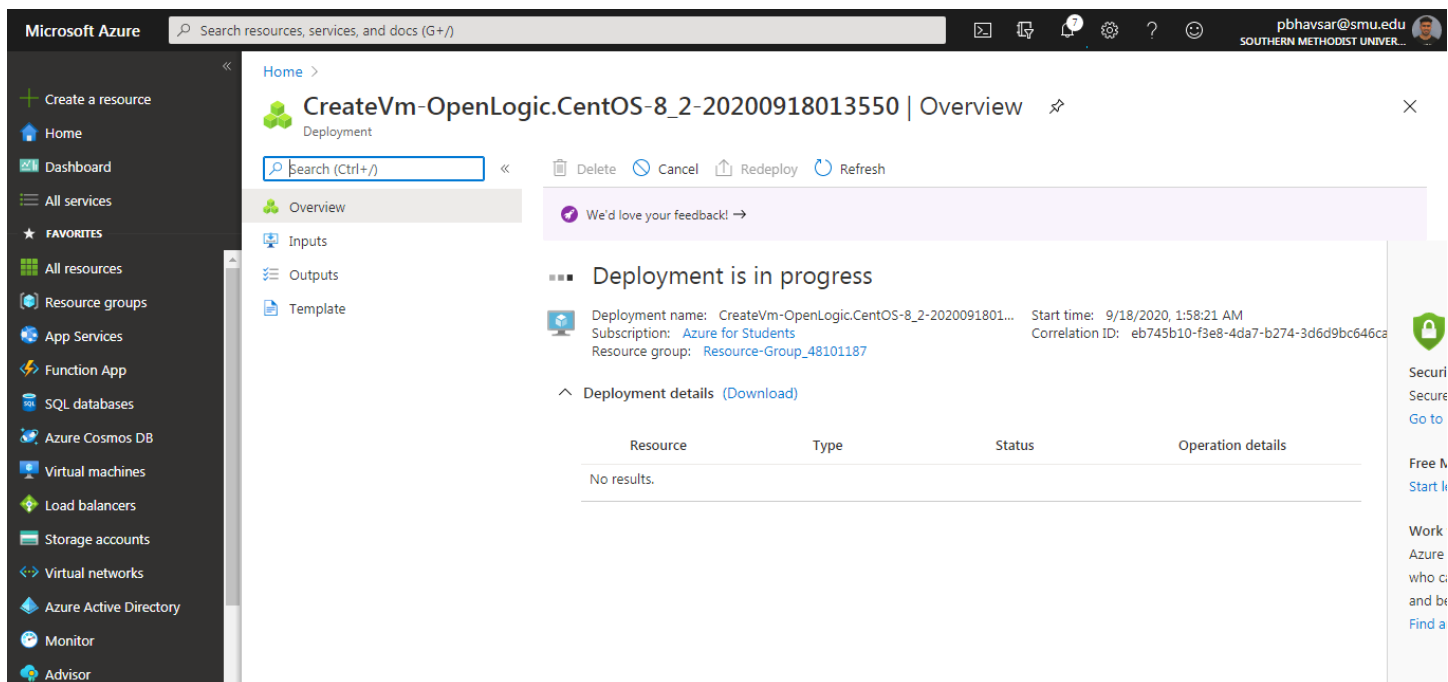
Basics Disks Networking Management Advanced Tags **Review + create**

Basics

Subscription	Azure for Students
Resource group	Resource-Group_48101187
Virtual machine name	VM-48101187
Region	East US
Availability options	No infrastructure redundancy required
Image	CentOS-based 8.2 - Gen1
Size	Standard B1s (1 vcpu, 1 GiB memory)
Authentication type	Password
Username	azureuser
Azure Spot	No

[Create](#) [< Previous](#) [Next >](#) [Download a template for automation](#)

Wait for the Deployment to get complete.



Microsoft Azure

Home >

CreateVm-OpenLogic.CentOS-8_2-20200918013550 | Overview

Deployment

Search (Ctrl+/)

Overview Inputs Outputs Template

Deployment is in progress

Deployment name: CreateVm-OpenLogic.CentOS-8_2-2020091801... Start time: 9/18/2020, 1:58:21 AM
Subscription: [Azure for Students](#) Correlation ID: eb745b10-f3e8-4da7-b274-3d6d9bc646ca
Resource group: [Resource-Group_48101187](#)

Deployment details (Download)

Resource	Type	Status	Operation details
No results.			

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

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

Home > CreateVm-OpenLogic.CentOS-8_2-20200918024607 >

VM-48101187
Virtual machine

Search (Ctrl+/)

Connect Start Restart Stop Capture Delete Refresh Share to mobile

Essentials

- Resource group (change) [Resource-Group_48101187](#)
- Operating system: Linux (centos 8.2.2004)
- Status: Running
- Location: East US
- Subscription (change) [Azure for Students](#)
- Subscription ID: 0b428db0-cfb4-4abf-9f5e-43ed6a5732fc
- Tags (change) [Click here to add tags](#)

Operating system: Linux (centos 8.2.2004)
Size: Standard B1s (1 vcpu, 1 GiB memory)
Public IP address: [40.121.110.250](#)
Virtual network/subnet: [Virtual-Network_48101187/Subnet-2](#)
DNS name: [Configure](#)

Properties Monitoring Capabilities Recommendations Tutorials

Virtual machine

Computer name	VM-48101187	Public IP address	40.121.110.250
Operating system	Linux (centos 8.2.2004)	Public IP address (IPv6)	-
SKU	8_2	Private IP address	10.0.16.6

Networking

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

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

Home > CreateVm-OpenLogic.CentOS-8_2-20200918024607 > VM-48101187

VM-48101187 | Networking
Virtual machine

Search (Ctrl+/)

Attach network interface Detach network interface

IP configuration ⓘ

ipconfig1 (Primary)

Network Interface: vm-48101187821 [Effective security rules](#) [Topology](#)

Virtual network/subnet: [Virtual-Network_48101187/Subnet-2](#) NIC Public IP: [40.121.110.250](#) NIC Private IP: [10.0.16.6](#)
Accelerated networking: **Disabled**

Inbound port rules Outbound port rules Application security groups Load balancing

Network security group [NSG_48101187](#) (attached to network interface: [vm-48101187821](#))
Impacts 0 subnets, 2 network interfaces [Add inbound port rule](#)

Priority	Name	Port	Protocol	Source	Destination
100	Port_80	80	Any	Any	VirtualNet
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNet
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

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

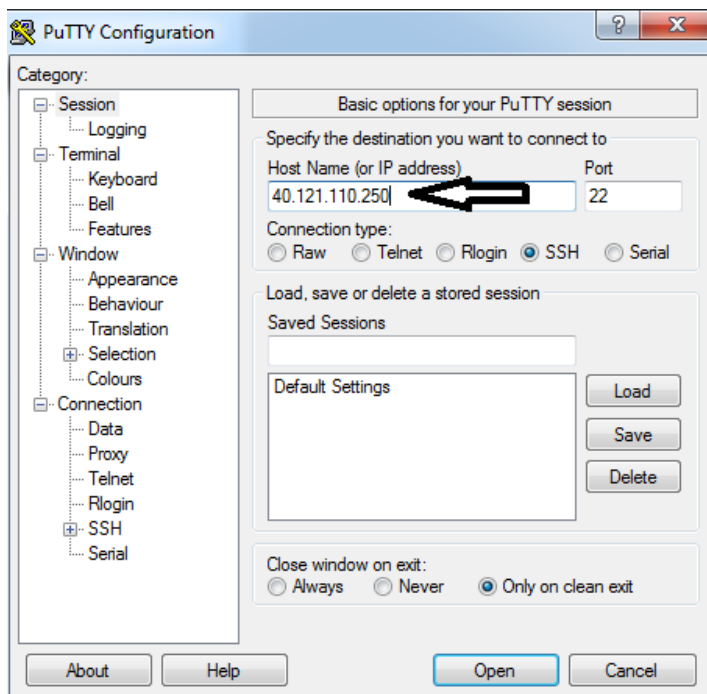
Let's download the PuTTY in our system now and access the Virtual Machine which we deployed on MS Azure.

Download and Install Putty on your local device:

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

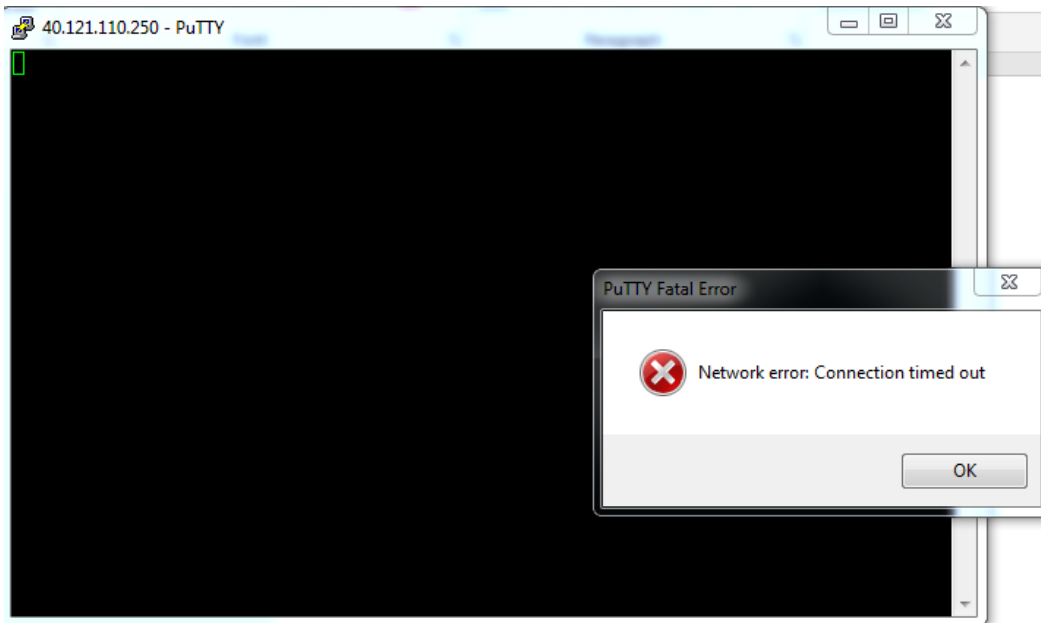
Copy the Public IP of the Virtual Machine (VM).

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



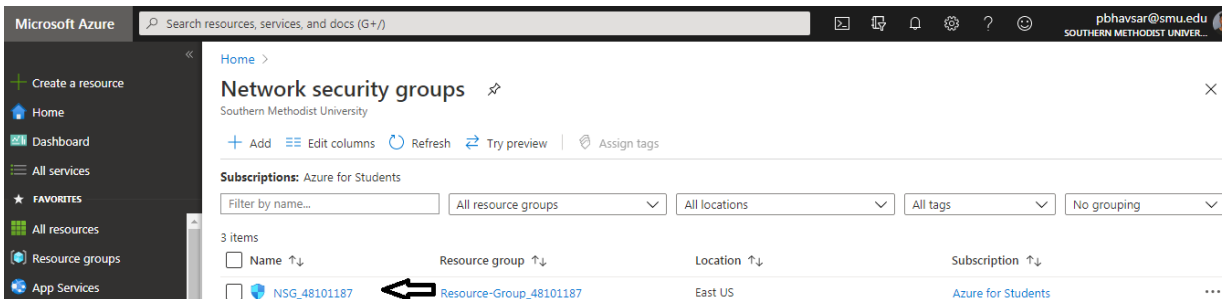
Login with your credentials.

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

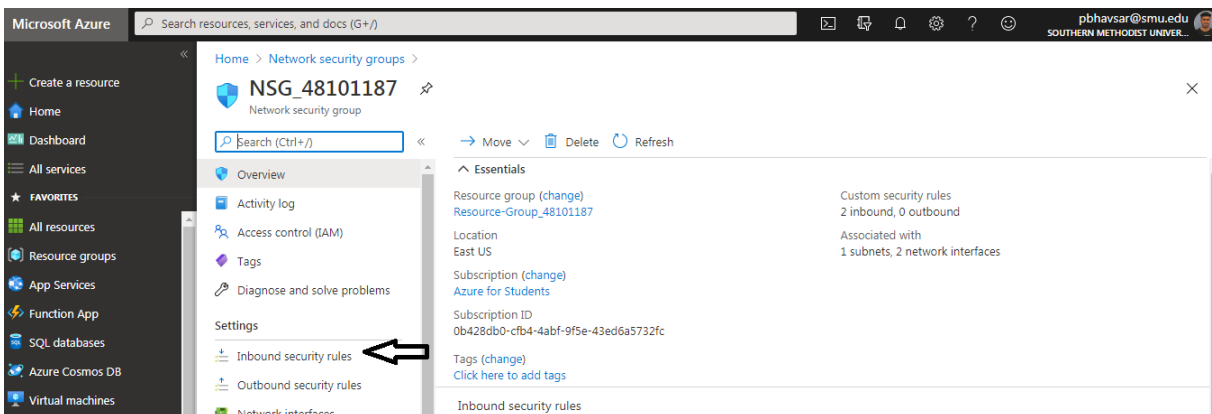


Let's first allow the SSH on the configured Network Security Group (NSG).

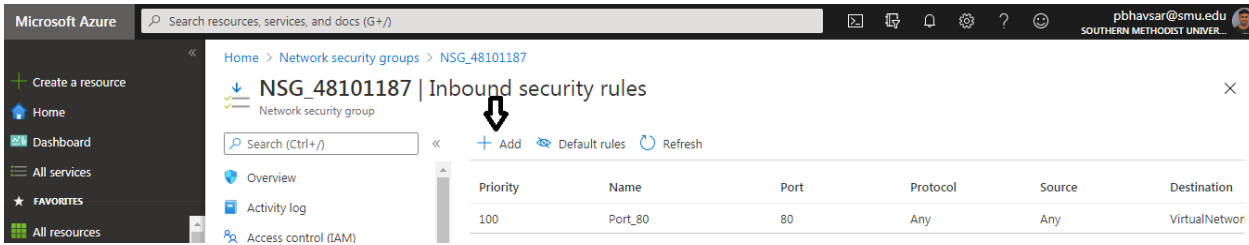
Navigate to Network Security Group (NSG) Service.



Click on Inbound Rules.



Click on Add.



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

Home > Network security groups > NSG_48101187

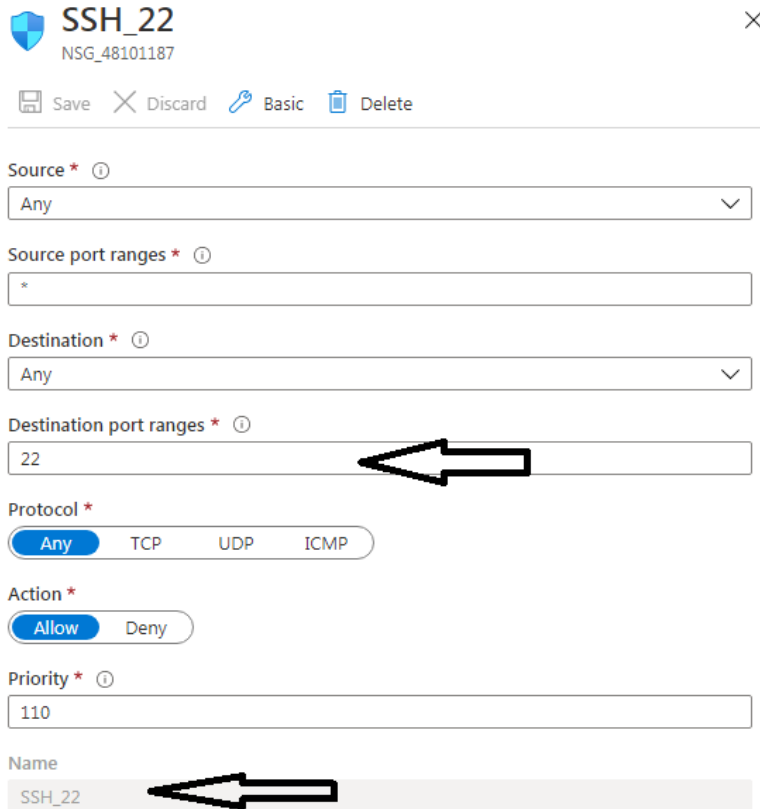
NSG_48101187 | Inbound security rules

Network security group

Search (Ctrl+/) < Add < Default rules < Refresh

Priority	Name	Port	Protocol	Source	Destination
100	Port_80	80	Any	Any	VirtualNetwork

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



SSH_22

NSG_48101187

Save Discard Basic Delete

Source * ⓘ
Any

Source port ranges * ⓘ
*

Destination * ⓘ
Any

Destination port ranges * ⓘ
22

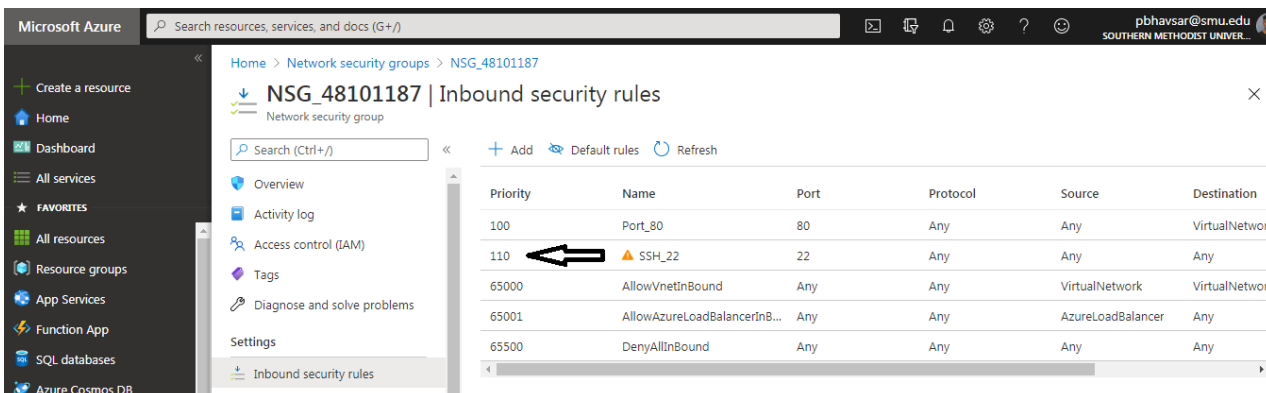
Protocol *
Any TCP UDP ICMP

Action *
Allow Deny

Priority * ⓘ
110

Name
SSH_22

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



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

Home > Network security groups > NSG_48101187

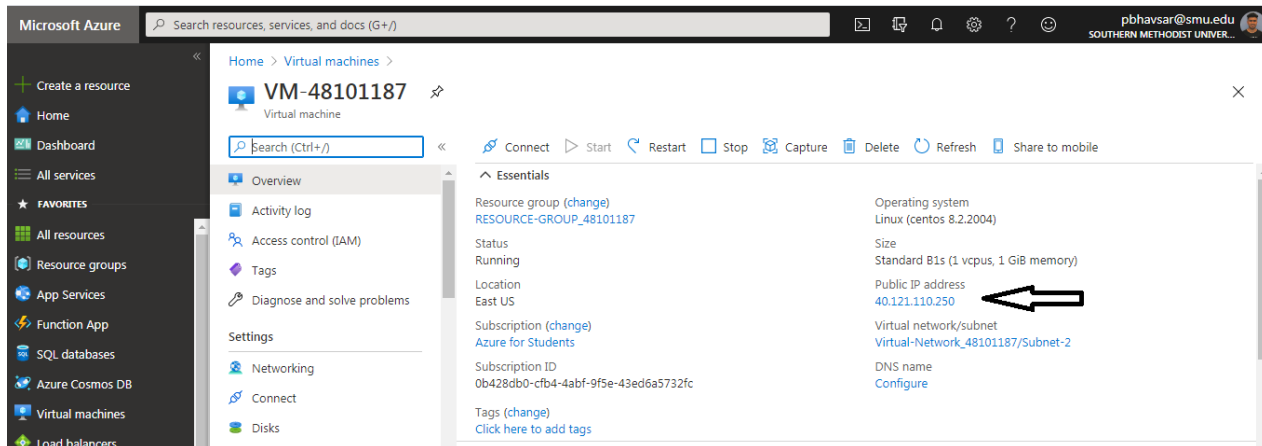
NSG_48101187 | Inbound security rules

Network security group

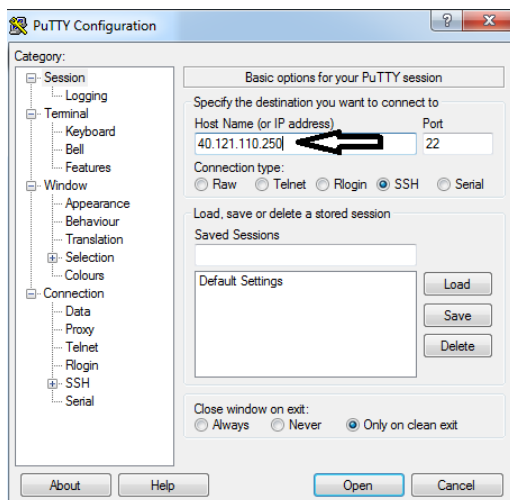
Search (Ctrl+/) < Add < Default rules < Refresh

Priority	Name	Port	Protocol	Source	Destination
100	Port_80	80	Any	Any	VirtualNetwork
110	SSH_22	22	Any	Any	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

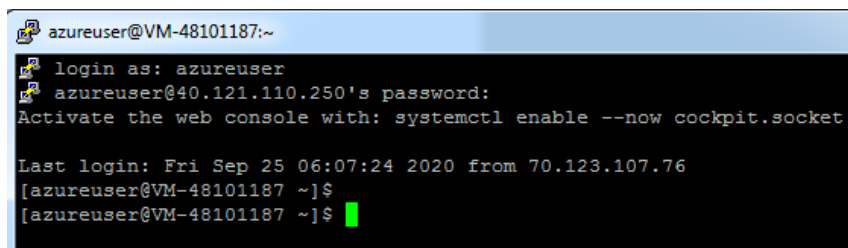
Again, copy the Public IP of the Azure Virtual Machine.



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