Lab11– Understanding FrontEnd and BackEnd Subnets - Azure

Virtual networks

A virtual network is a virtual, isolated portion of the Azure public network. Each virtual network is dedicated to your subscription. Things to consider when deciding whether to create one virtual network, or multiple virtual networks in a subscription:

- Do any organizational security requirements exist for isolating traffic into separate virtual networks? You can choose to connect virtual networks or not. If you connect virtual networks, you can implement a network virtual appliance, such as a firewall, to control the flow of traffic between the virtual networks. For more information, see security and connectivity.
- Do any organizational requirements exist for isolating virtual networks into separate subscriptions or regions?
- A network interface enables a VM to communicate with other resources. Each network interface has one or more private IP addresses assigned to it. How many network interfaces and private IP addresses do you require in a virtual network? There are limitsto the number of network interfaces and private IP addresses that you can have within a virtual network.
- Do you want to connect the virtual network to another virtual network or on-premises network? You may choose to connect some virtual networks to each other or on-premises networks, but not others. For more information, see connectivity. Each virtual network that you connect to another virtual network, or on-premises network, must have a unique address space. Each virtual network has one or more public or private address ranges assigned to its address space. An address range is specified in classless internet domain routing (CIDR) format, such as 10.0.0.0/16. Learn more about address ranges for virtual networks.
- Do you have any organizational administration requirements for resources in different virtual networks? If so, you might separate resources into separate virtual network to simplify permission assignment to individuals in your organization or to assign different policies to different virtual networks.

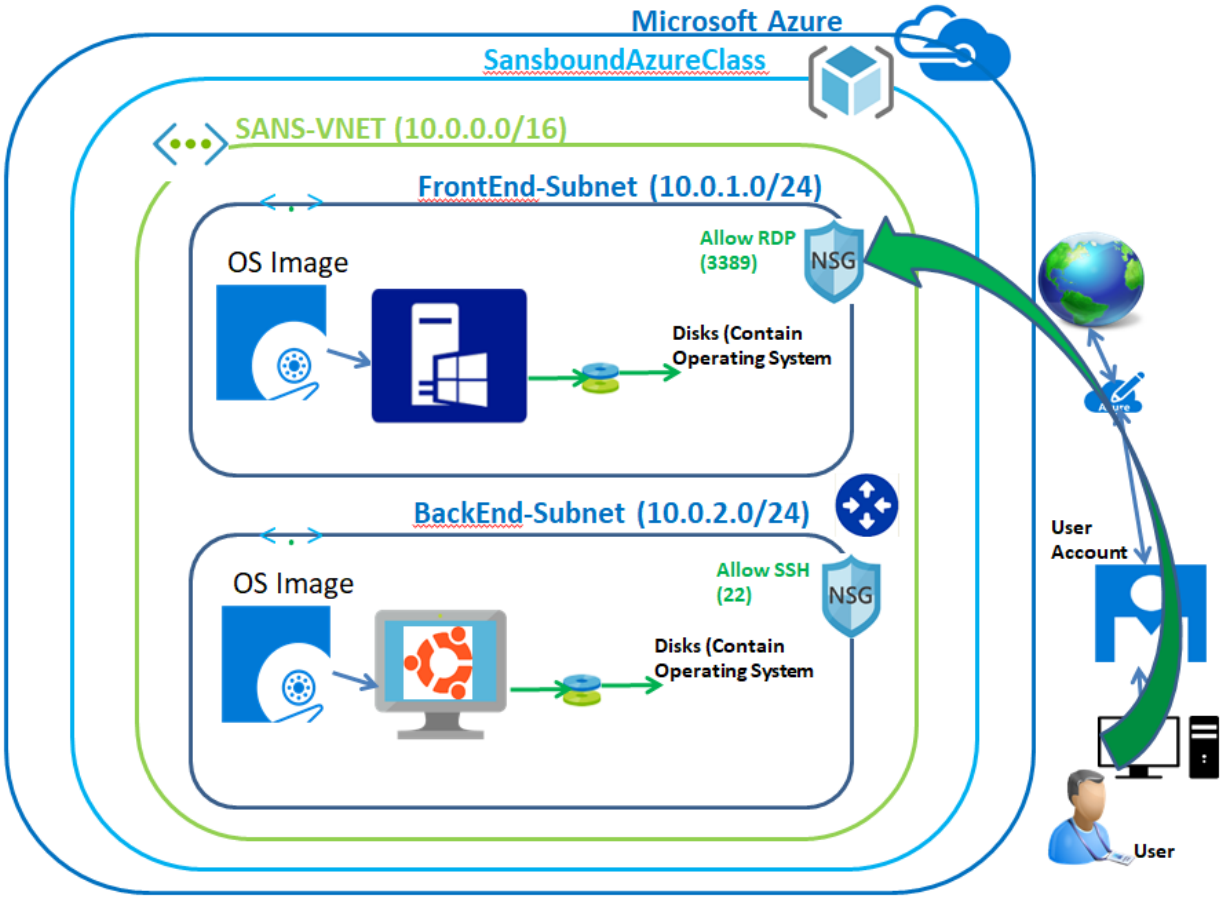
- When you deploy some Azure service resources into a virtual network, they create their own virtual network. To determine whether an Azure service creates its own virtual network, see information for each Azure service that can be deployed into a virtual network.

Subnets

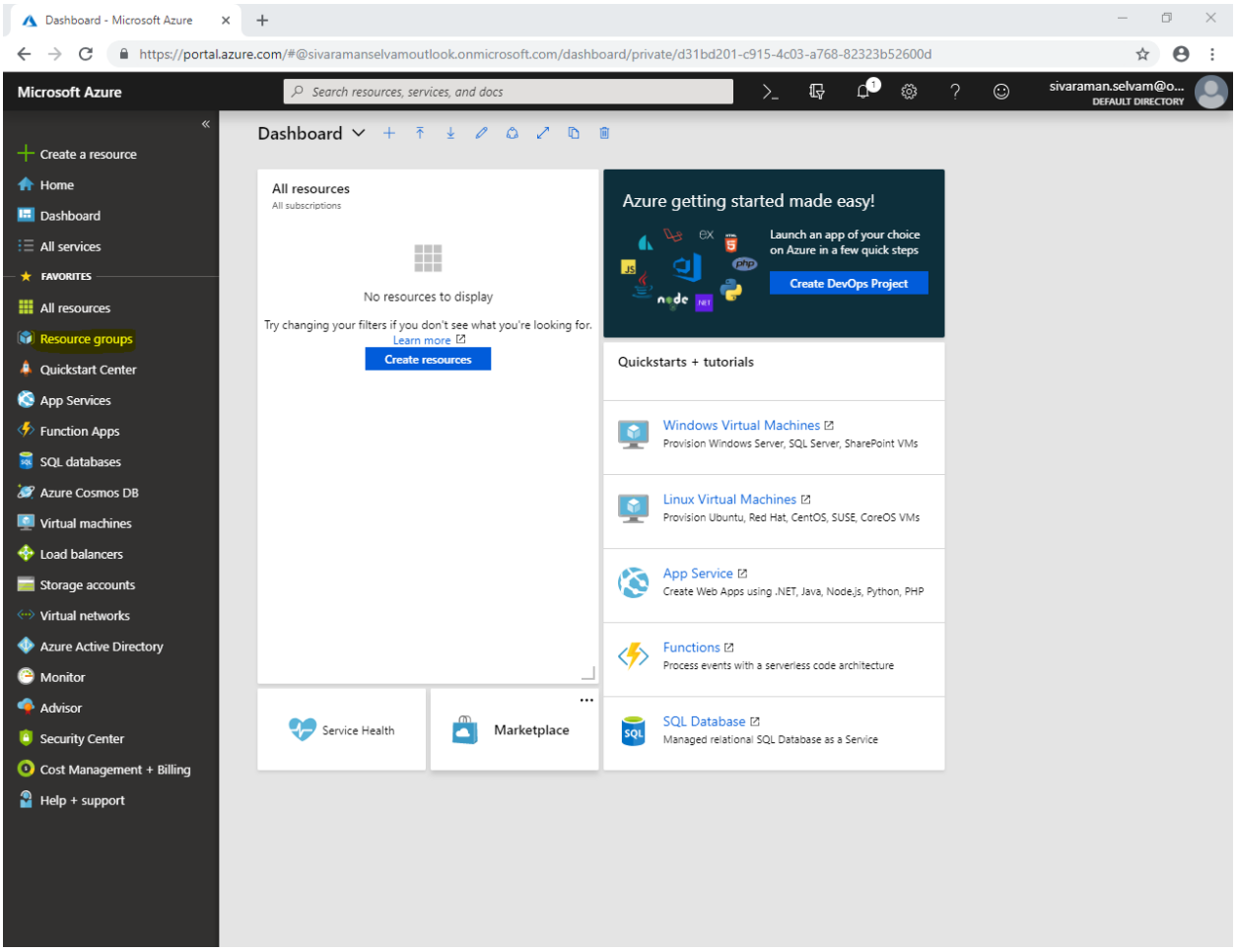
A virtual network can be segmented into one or more subnets up to the limits. Things to consider when deciding whether to create one subnet, or multiple virtual networks in a subscription:

- Each subnet must have a unique address range, specified in CIDR format, within the address space of the virtual network. The address range cannot overlap with other subnets in the virtual network.
- If you plan to deploy some Azure service resources into a virtual network, they may require, or create, their own subnet, so there must be enough unallocated space for them to do so. To determine whether an Azure service creates its own subnet, see information for each Azure service that can be deployed into a virtual network. For example, if you connect a virtual network to an on-premises network using an Azure VPN Gateway, the virtual network must have a dedicated subnet for the gateway. Learn more about gateway subnets.
- Azure routes network traffic between all subnets in a virtual network, by default. You can override Azure's default routing to prevent Azure routing between subnets, or to route traffic between subnets through a network virtual appliance, for example. If you require that traffic between resources in the same virtual network flow through a network virtual appliance (NVA), deploy the resources to different subnets. Learn more in security.
- You can limit access to Azure resources such as an Azure storage account or Azure SQL database, to specific subnets with a virtual network service endpoint. Further, you can deny access to the resources from the internet. You may create multiple subnets, and enable a service endpoint for some subnets, but not others. Learn more about service endpoints, and the Azure resources you can enable them for.
- You can associate zero or one network security group to each subnet in a virtual network. You can associate the same, or a different, network security group to each subnet. Each network security group contains rules, which allow or deny traffic to and from sources and destinations. Learn more about network security groups.

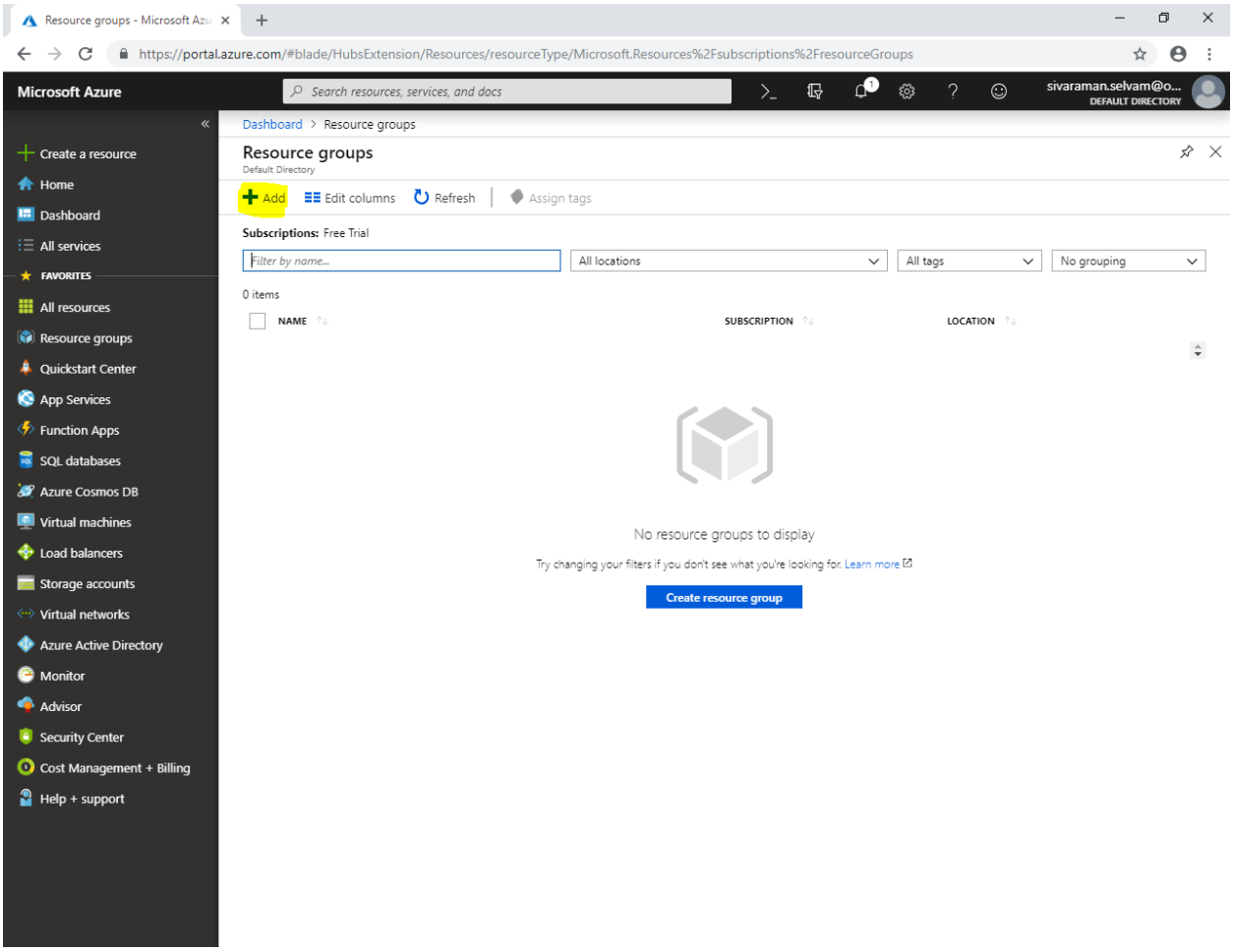
Topology


Microsoft Azure
SansboundAzureClass
SANS-VNET (10.0.0.0/16)
FrontEnd-Subnet (10.0.1.0/24)
OS Image
Allow RDP
(3389)
NSG
Disks (Contain
Operating System
BackEnd-Subnet (10.0.2.0/24)
OS Image
Allow SSH
(22)
NSG
Disks (Contain
Operating System
User
Account
User

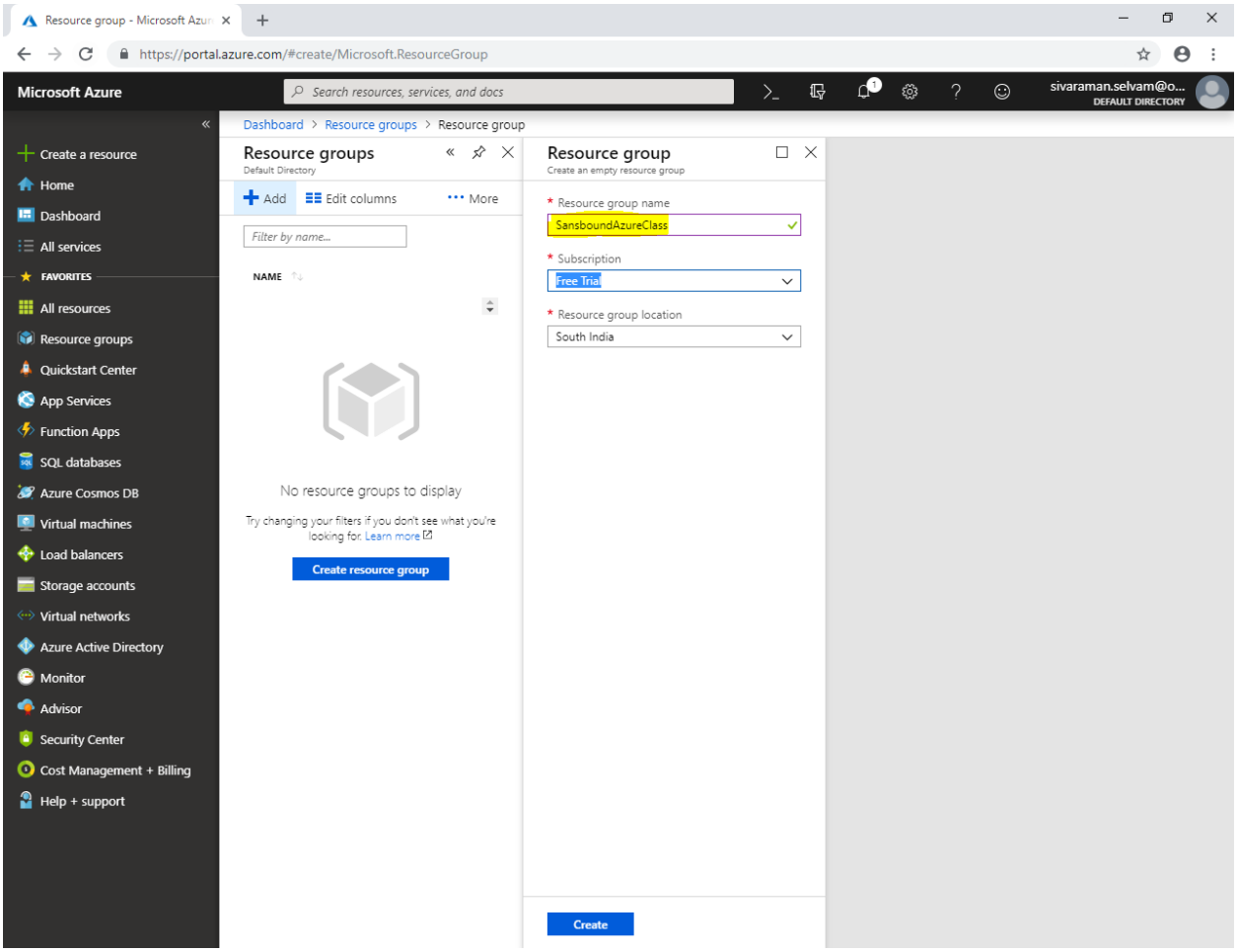
In Azure portal, click **“Resource groups”**.



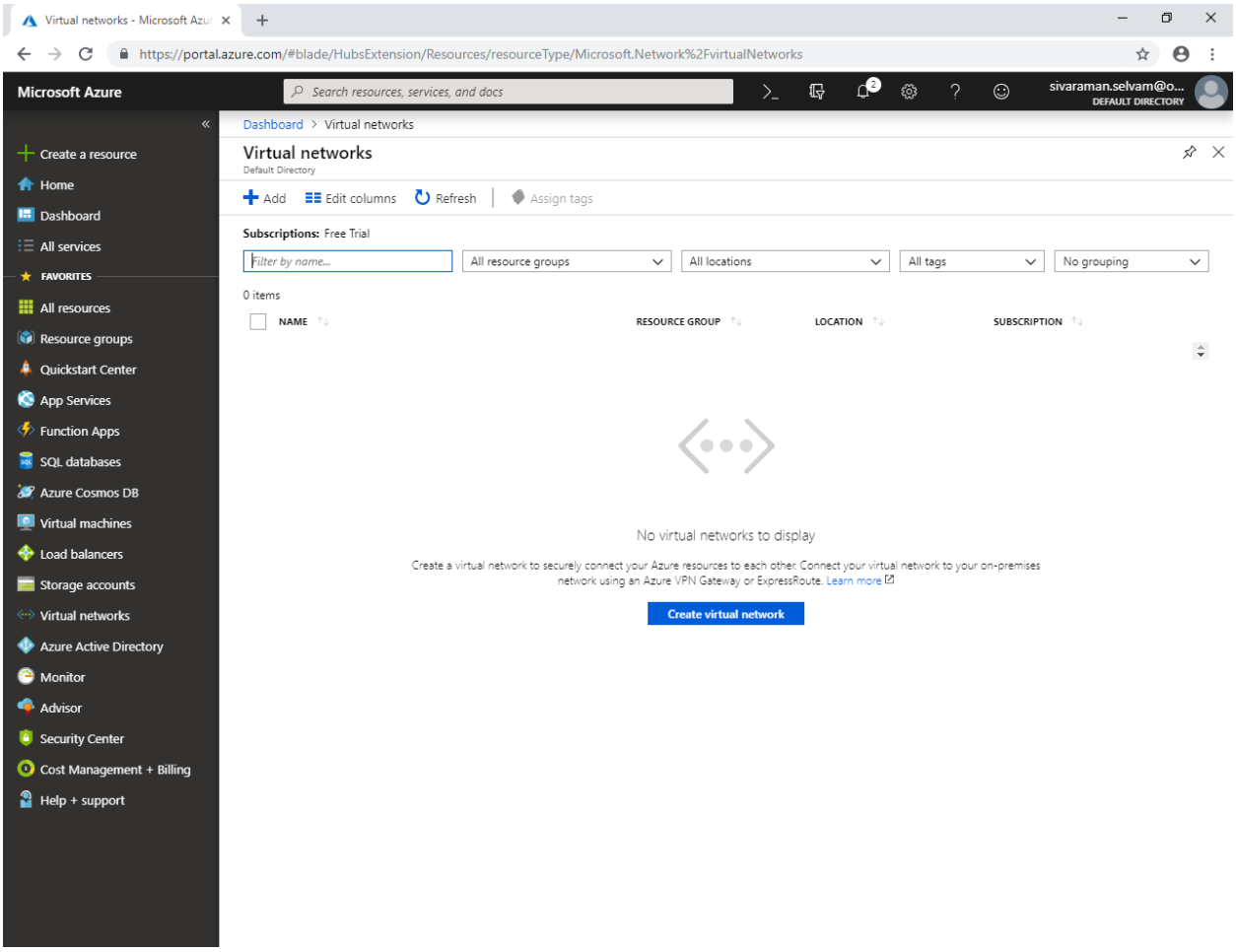
In **“Resource groups”** click **“Add”**.



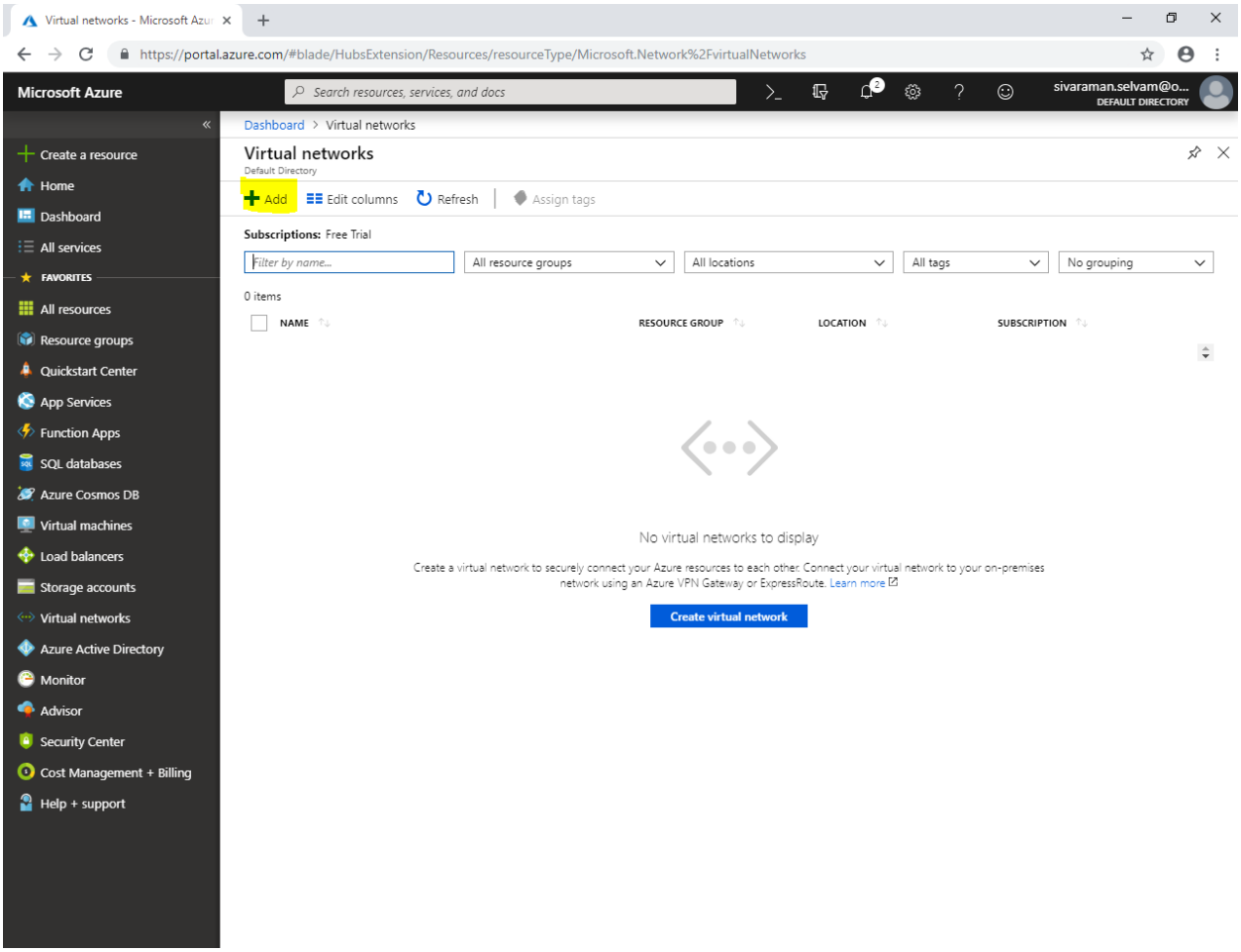
While create **“Resource group”** as type **“Resource group name”** as **“SansboundAzureClass”**.



Click on **“Virtual networks”** in left side panel.



Click **"Add".**


Virtual networks - Microsoft Azu
https://portal.azure.com/#blade/HubsExtension/Resources/resourceType/Microsoft.Network%2FvirtualNetworks
Microsoft Azure
Search resources, services, and docs
sivaraman.selvam@o...
DEFAULT DIRECTORY
Dashboard > Virtual networks
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
Quickstart Center
App Services
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
Virtual networks
Default Directory
Add
Edit columns
Refresh
Assign tags
Subscriptions: Free Trial
Filter by name...
All resource groups
All locations
All tags
No grouping
0 items
NAME
RESOURCE GROUP
LOCATION
SUBSCRIPTION
No virtual networks to display
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. Learn more
Create virtual network

While creating virtual network,

Type **“Virtual network name”** as **“SANS-VNET”**.

Type **“Address space”** as **10.0.0.0/16**

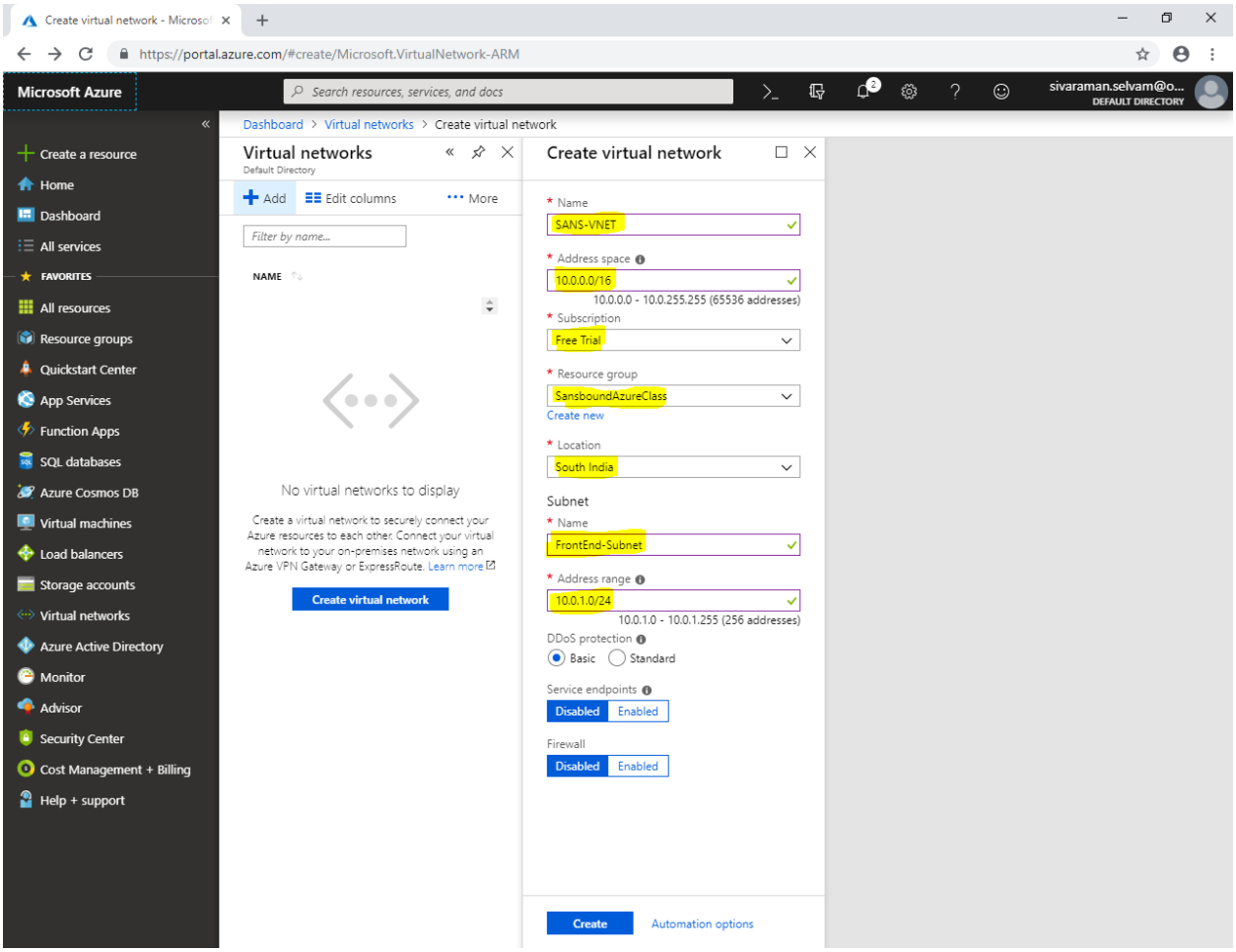
Select **“Subscription”** as **“Free Trial”**.

In **“Resource group”**, select **“SansboundAzureClass”**.

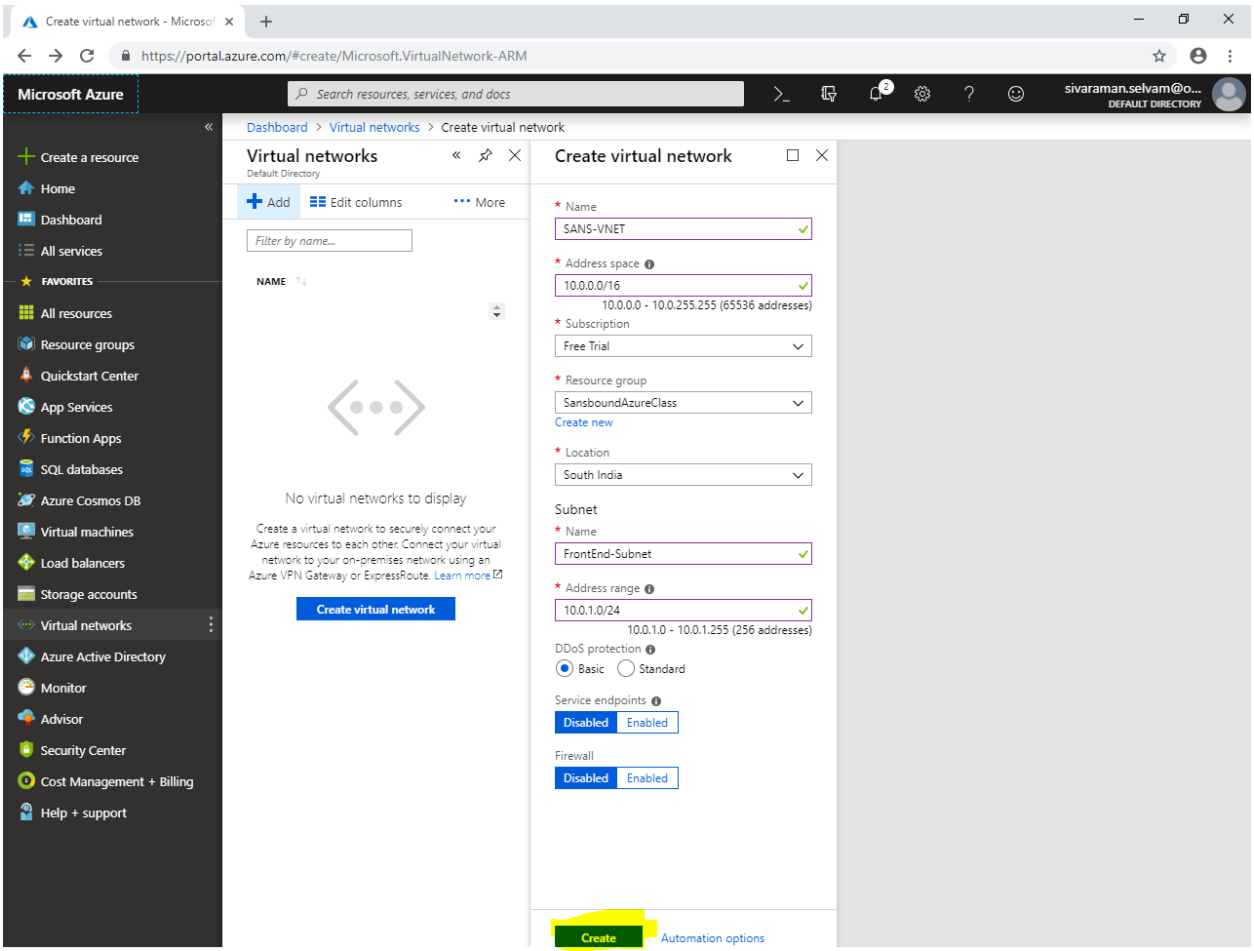
Select **“Location”** as **“South India”**.

In **“Subnet”** type Subnet name as **“FrontEnd-Subnet”**.

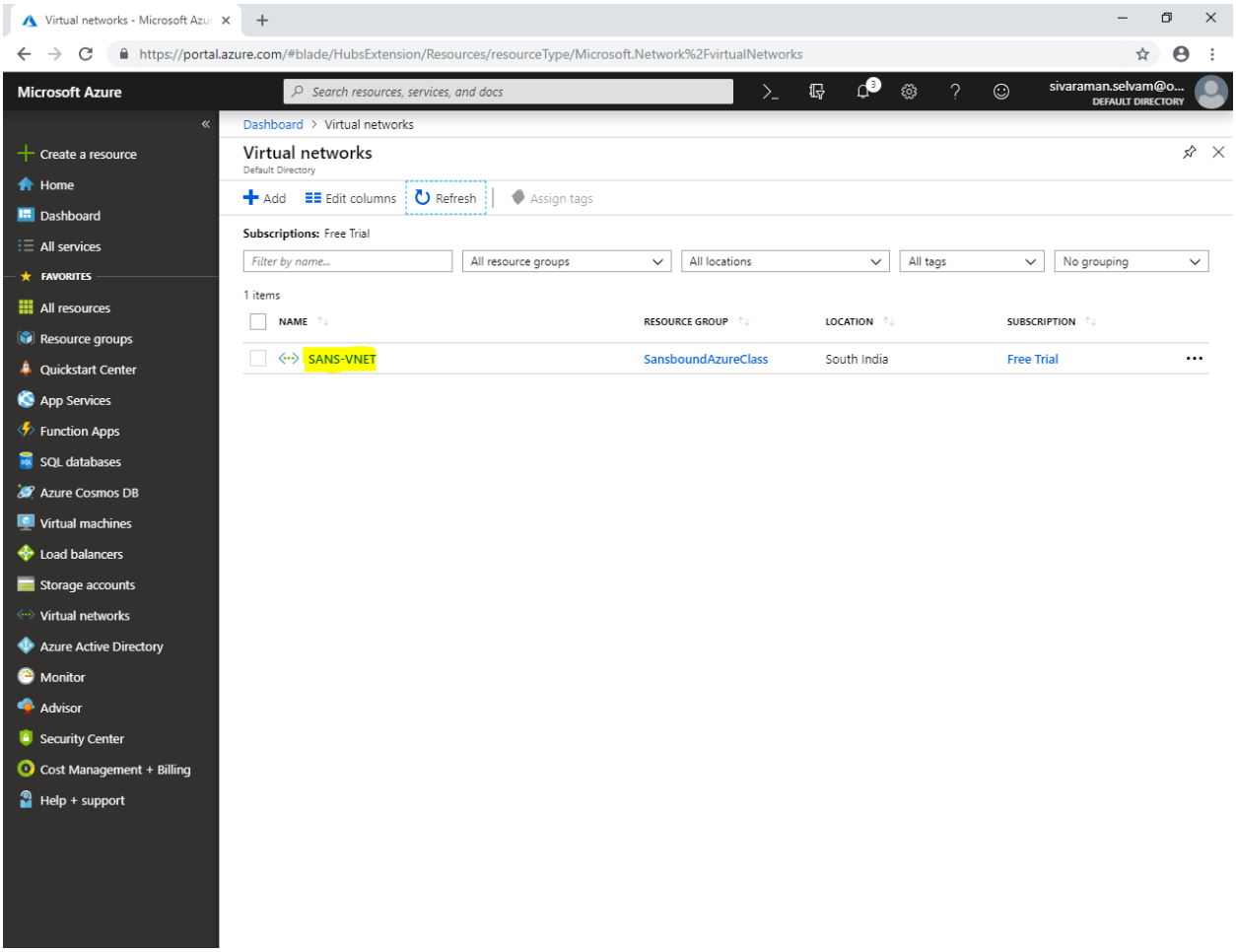
In “**Address range**” type **“10.0.1.0/24”**.



Click **"Create"**.

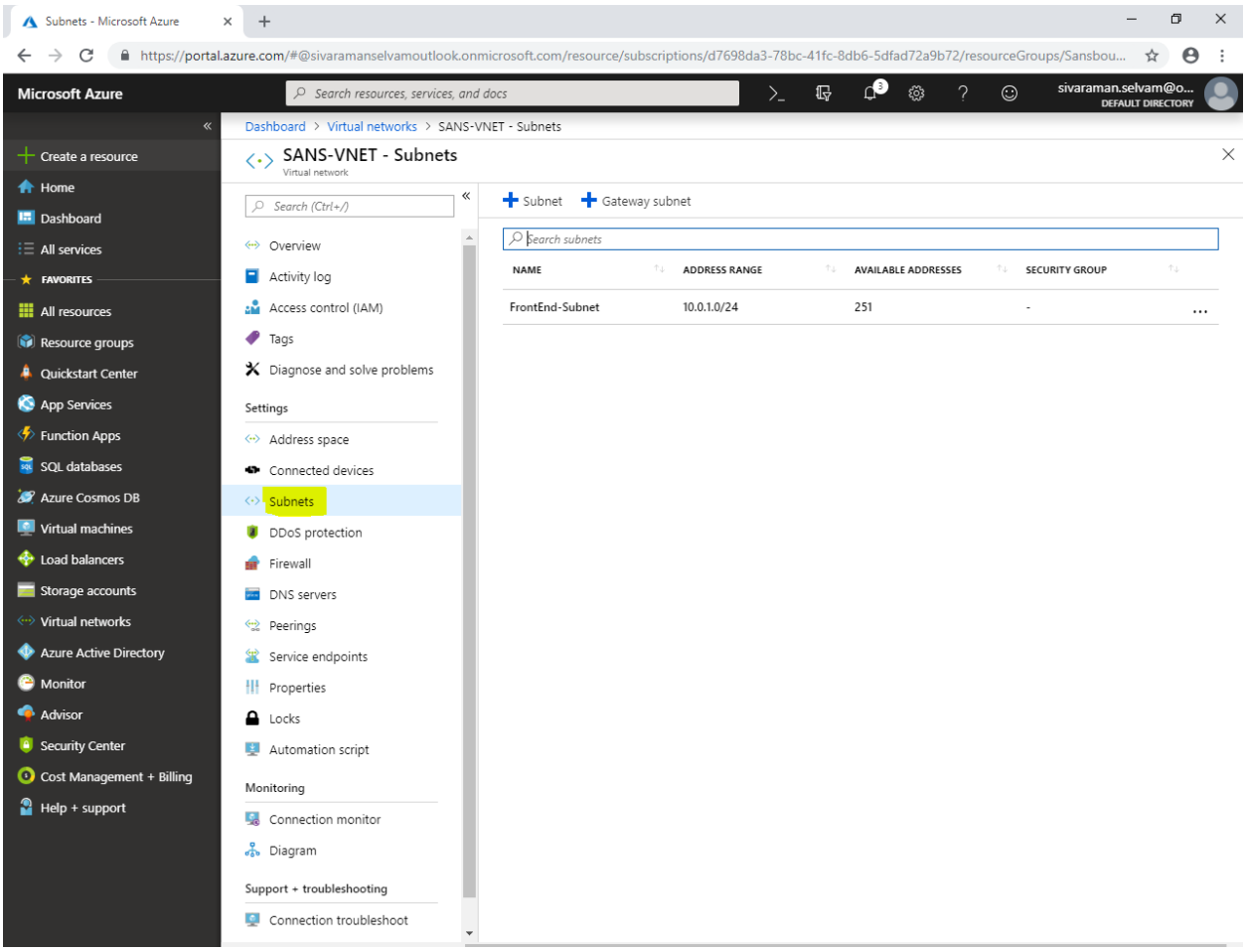


In **“Virtual networks”**, click on **“SANS-VNET”**.



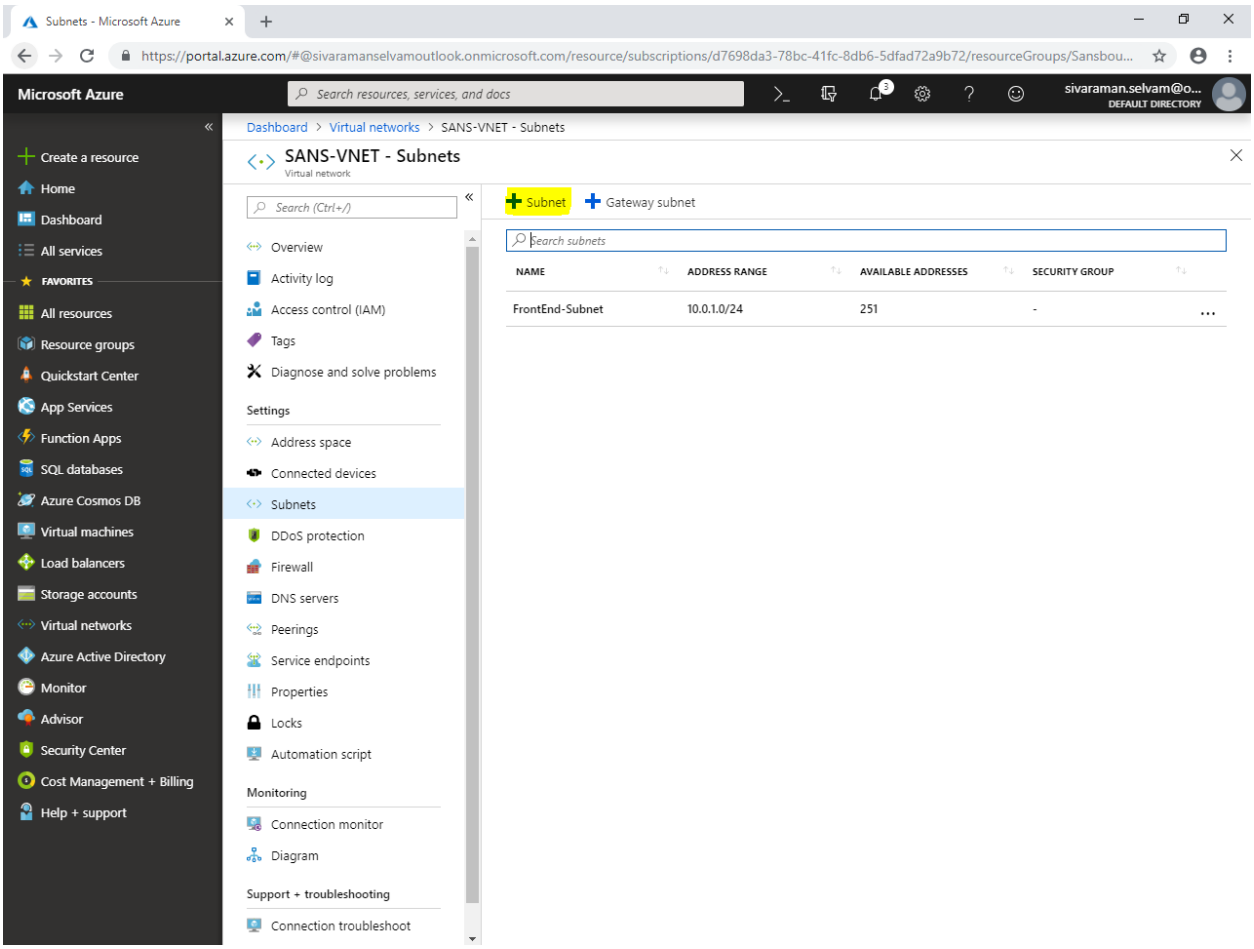
In **“SANS-VNET”** click on **“Subnets”**.

In **“FrontEnd-Subnet”** we are able to see address range as **10.0.1.0/24**.



In **“Subnets”**

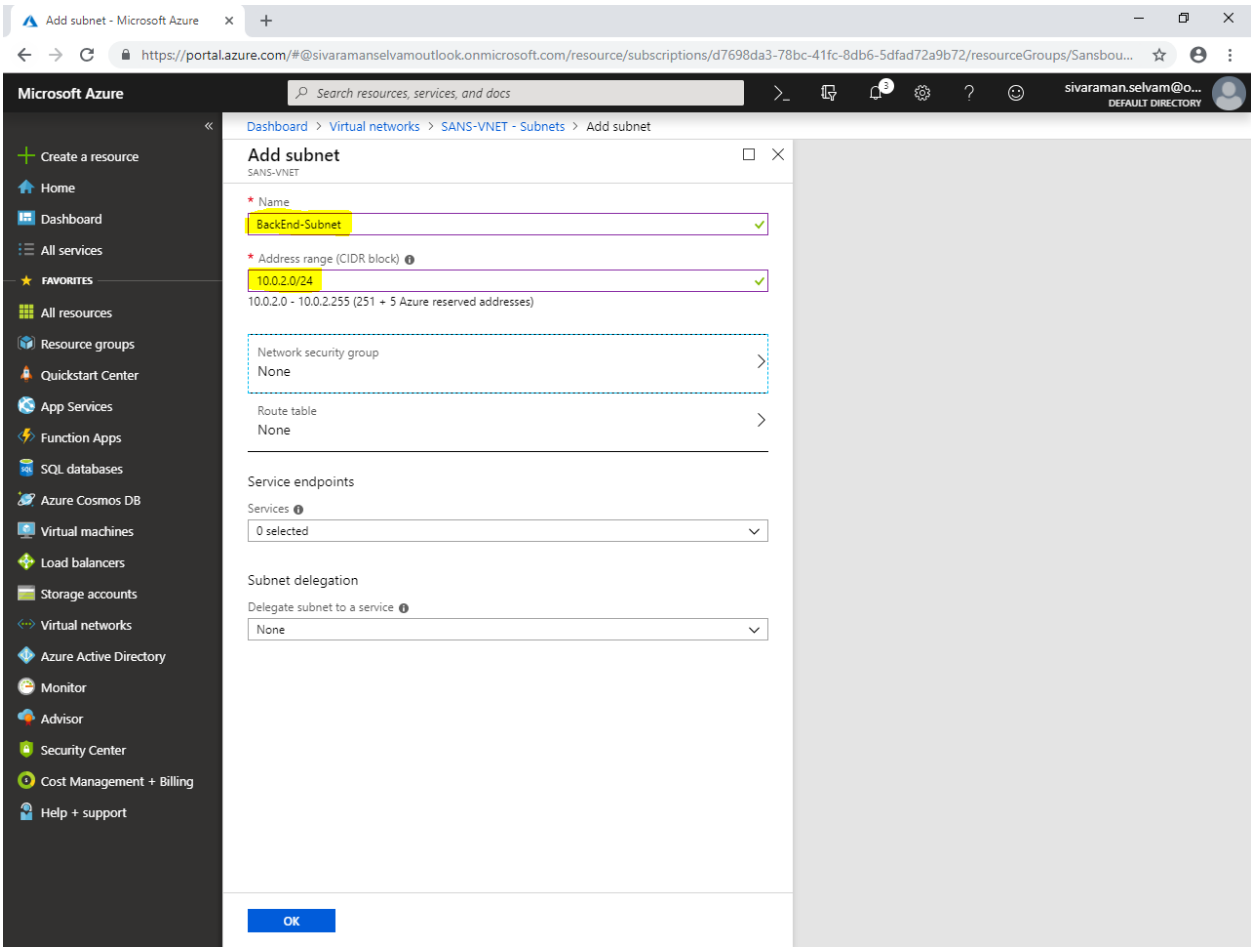
Click **“Subnet”** to add additional subnet.



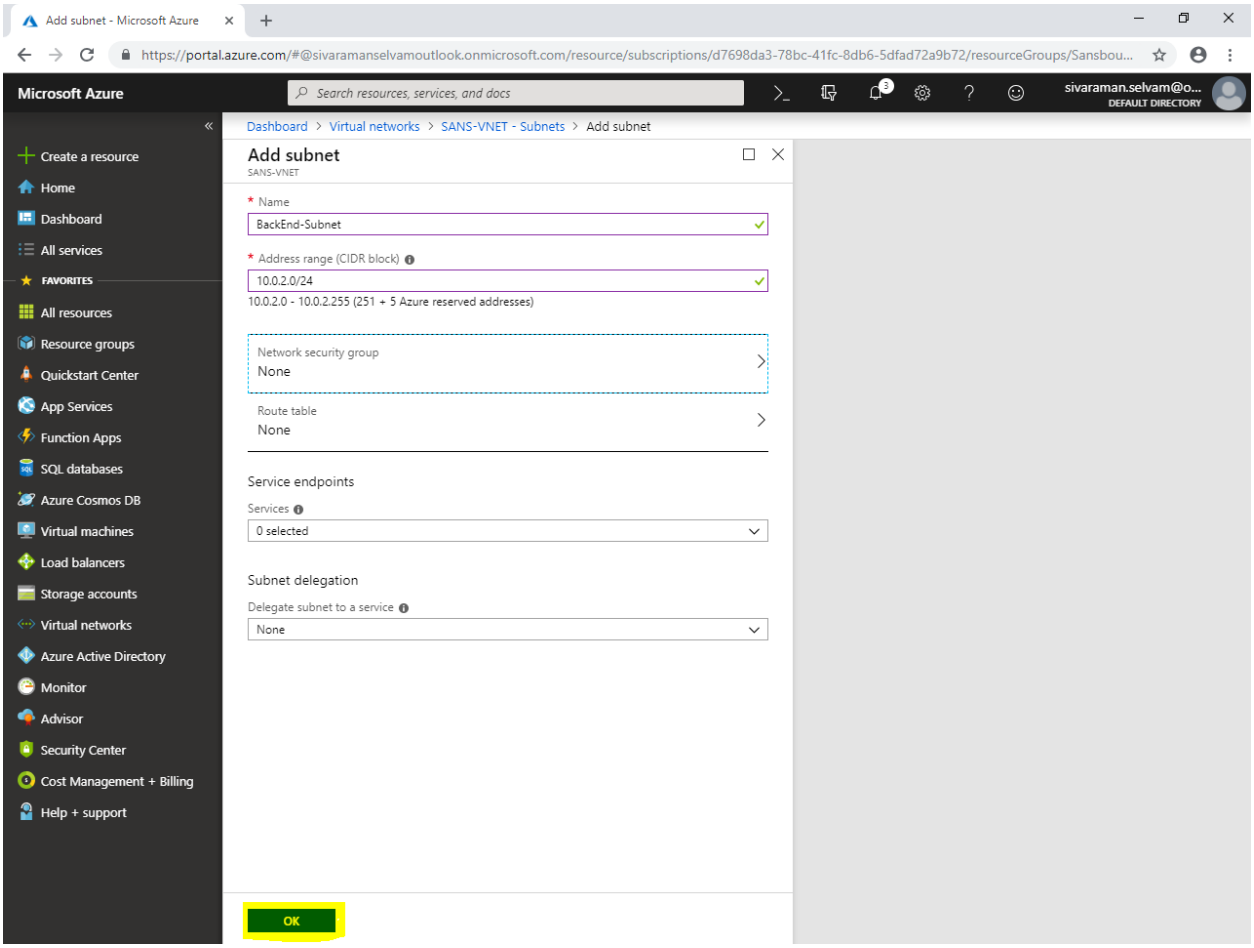
While **“Add subnet”**.

Type **“Subnet name”** as **“BackEnd-Subnet”**.

Type **“Address range”** as **“10.0.2.0/24”**.

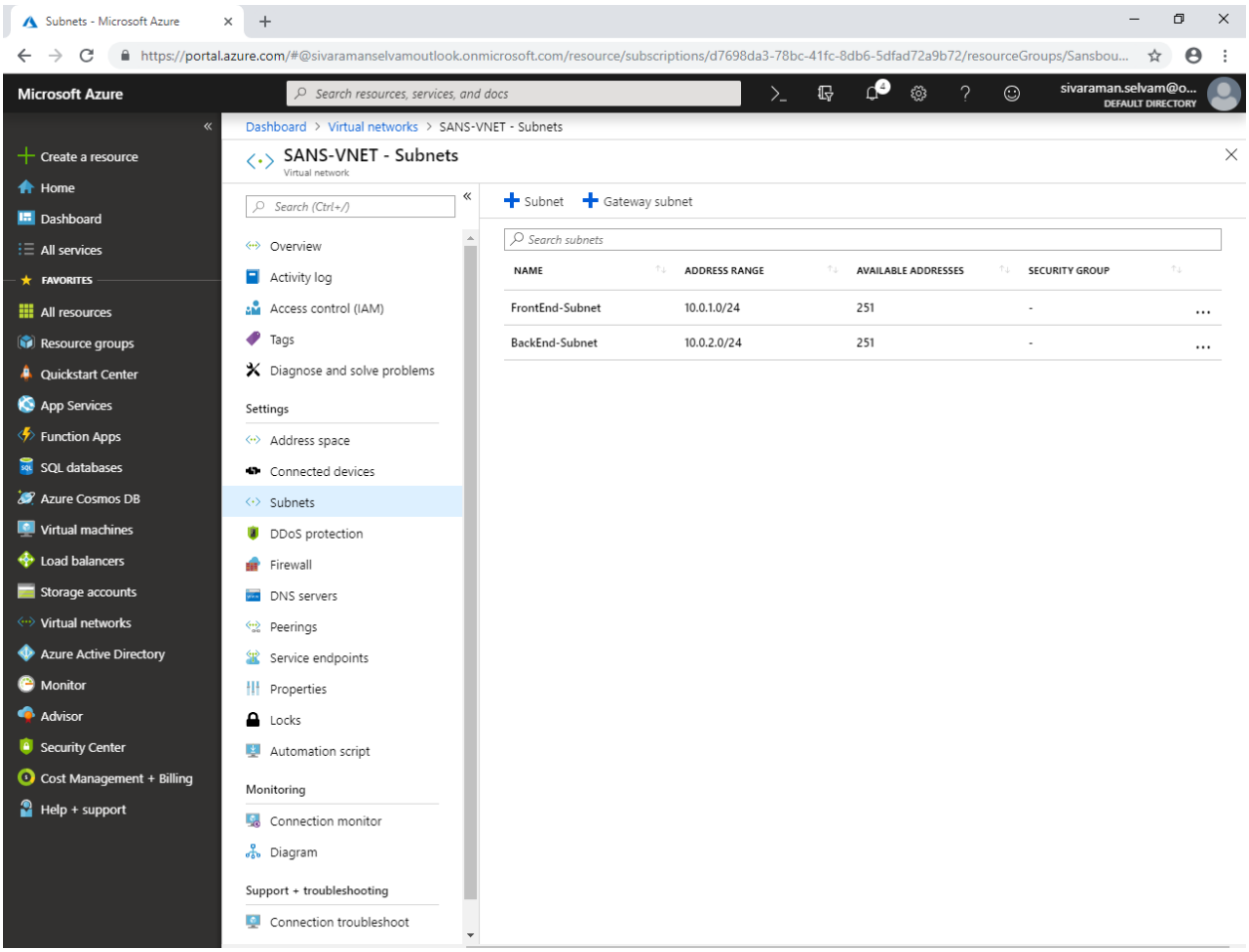


Click **“Ok”**.

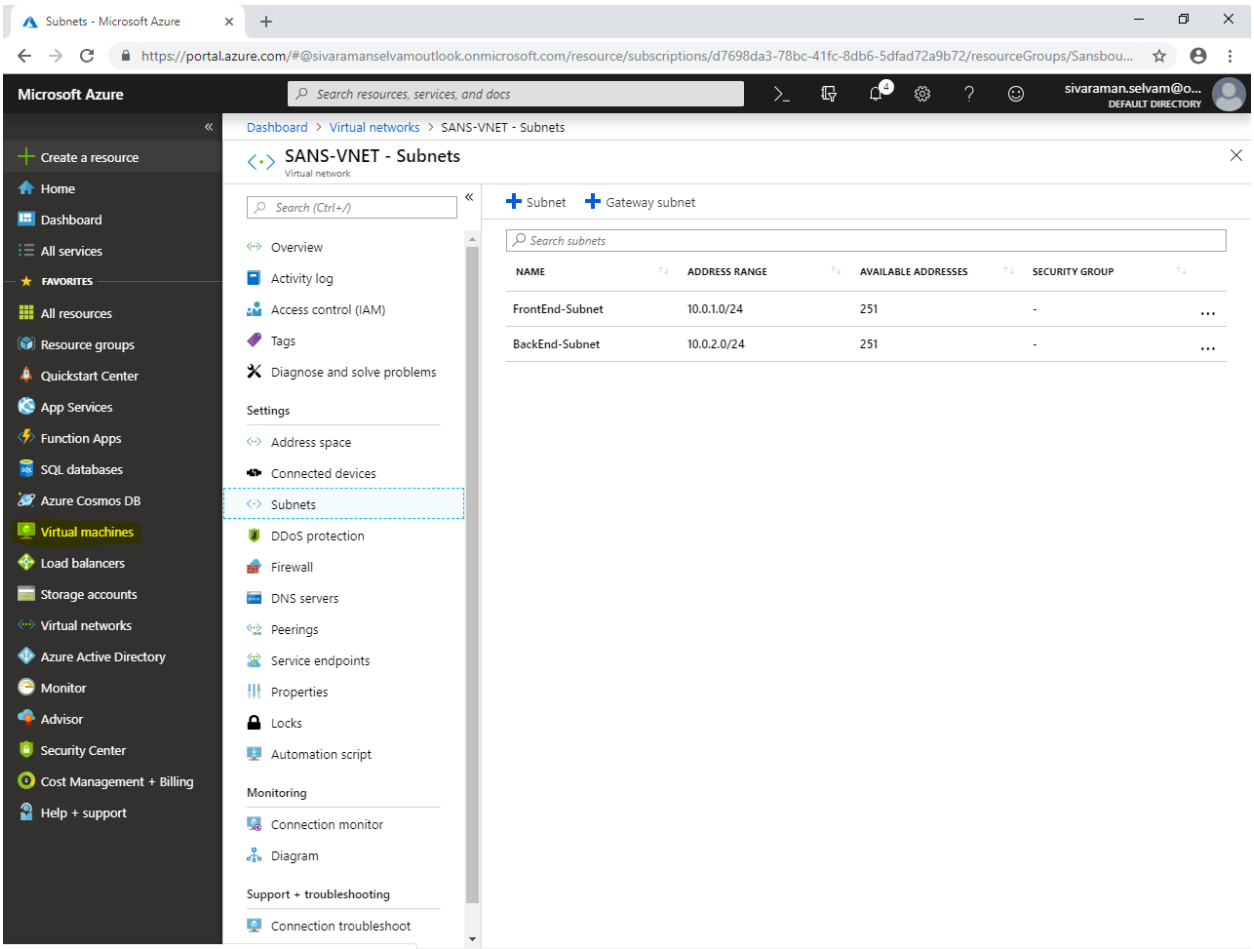

Add subnet - Microsoft Azure
https://portal.azure.com/#@sivaramanselvamoutlook.onmicrosoft.com/resource/subscriptions/d7698da3-78bc-41fc-8db6-5dfad72a9b72/resourceGroups/Sansbou...
Microsoft Azure
Search resources, services, and docs
sivaraman.selvam@o...
DEFAULT DIRECTORY
Dashboard > Virtual networks > SANS-VNET - Subnets > Add subnet
Add subnet
SANS-VNET
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
Quickstart Center
App Services
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
* Name
BackEnd-Subnet
* Address range (CIDR block)
10.0.2.0/24
10.0.2.0 - 10.0.2.255 (251 + 5 Azure reserved addresses)
Network security group
None
Route table
None
Service endpoints
Services
0 selected
Subnet delegation
Delegate subnet to a service
None
OK

In **“Subnets”**.

You have created **“FrontEnd-Subnet”** and **“BackEndSubnet”.**

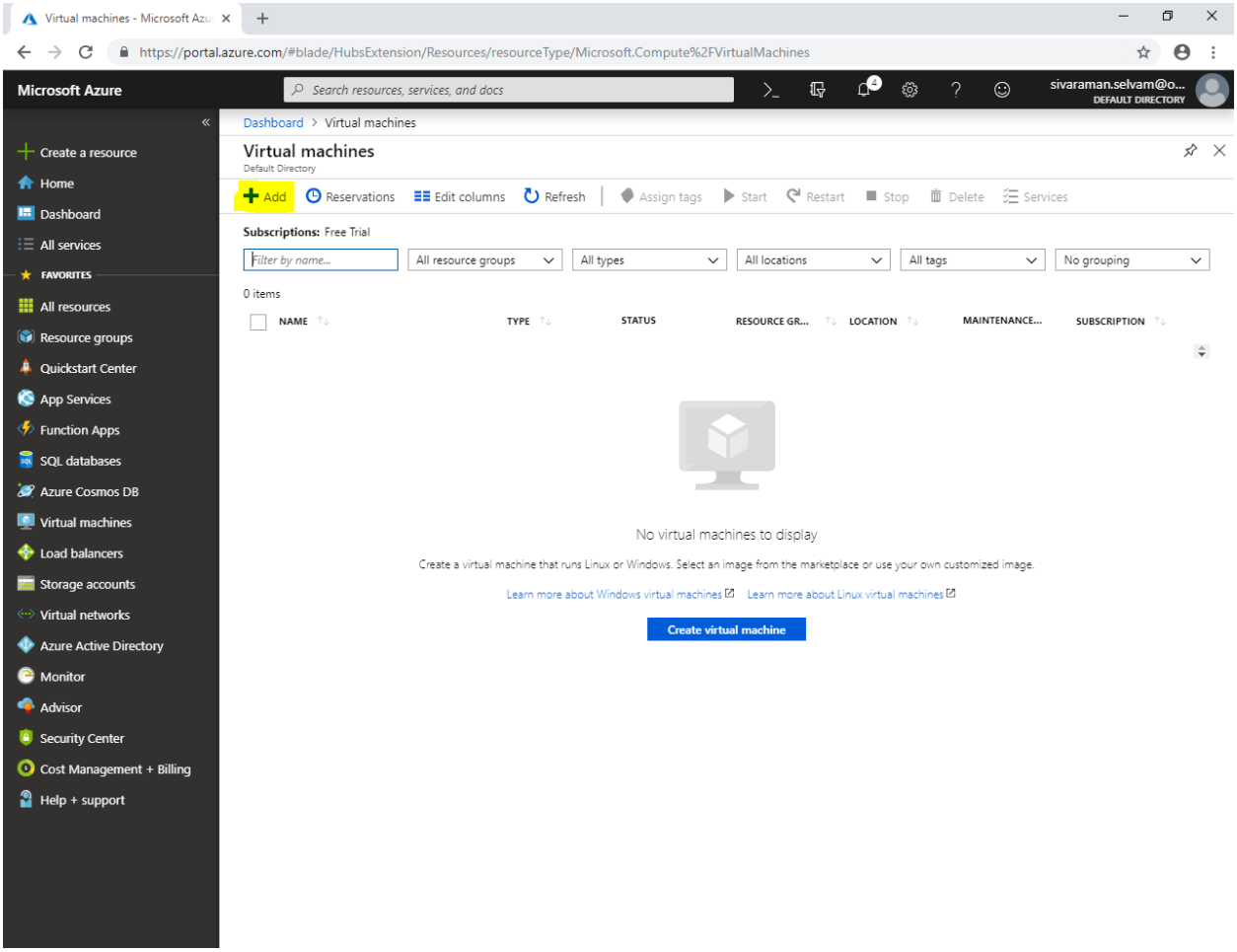


Click in **“Virtual machines”** left side of the panel.



In **“Virtual machines”**,

Click **“Add”**.



While creating **“Virtual machine”** select **“Subscription”** as **“Free Trial”**.

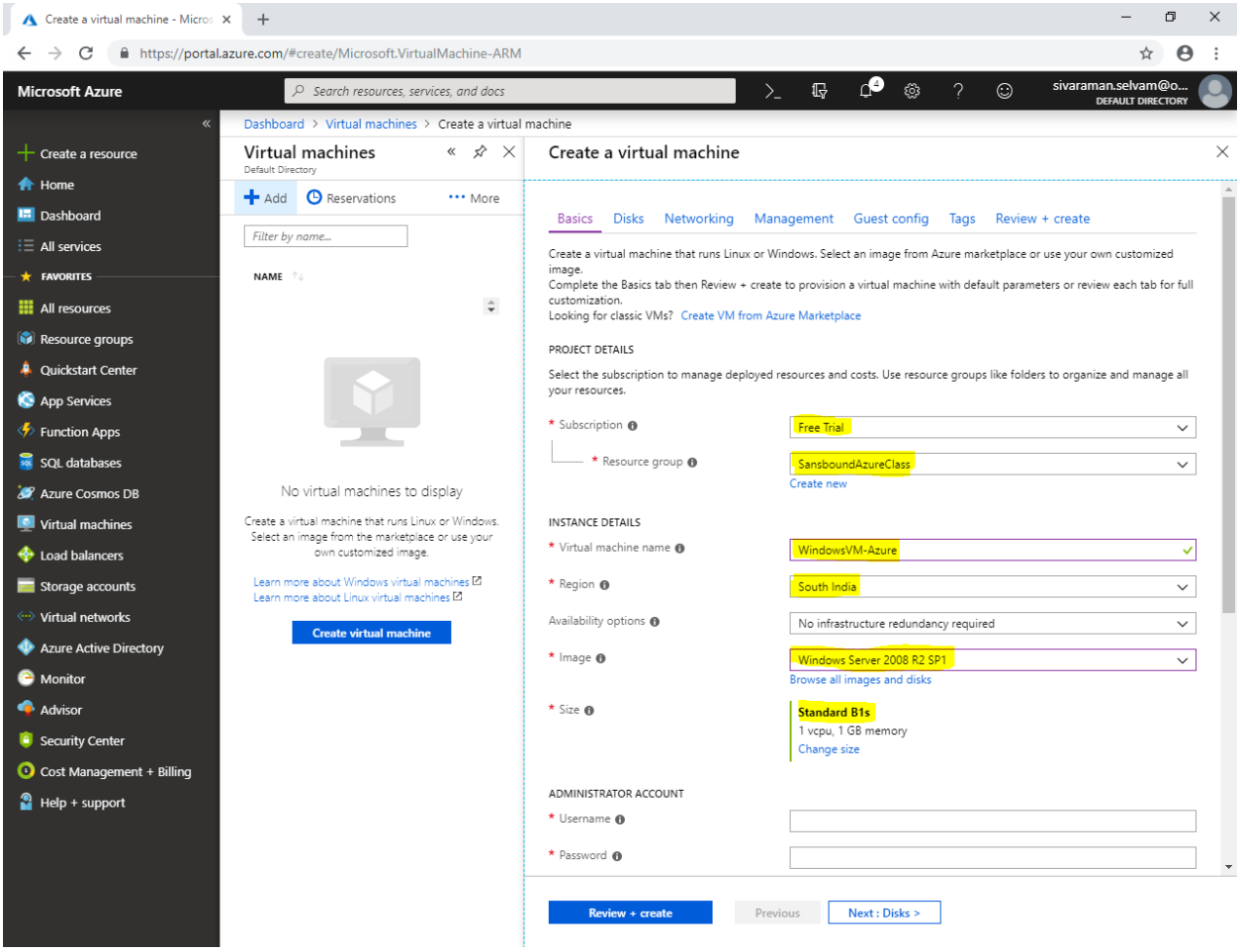
Select **“Resource group”** as **“SansboundAzureClass”**.

In **“Virtual machine name”** as **“WindowsVM-Azure”**.

Select **“Region”** as **“South India”**.

Select **“Image”** as **“Windows Server 2008 R2 SP1”**.

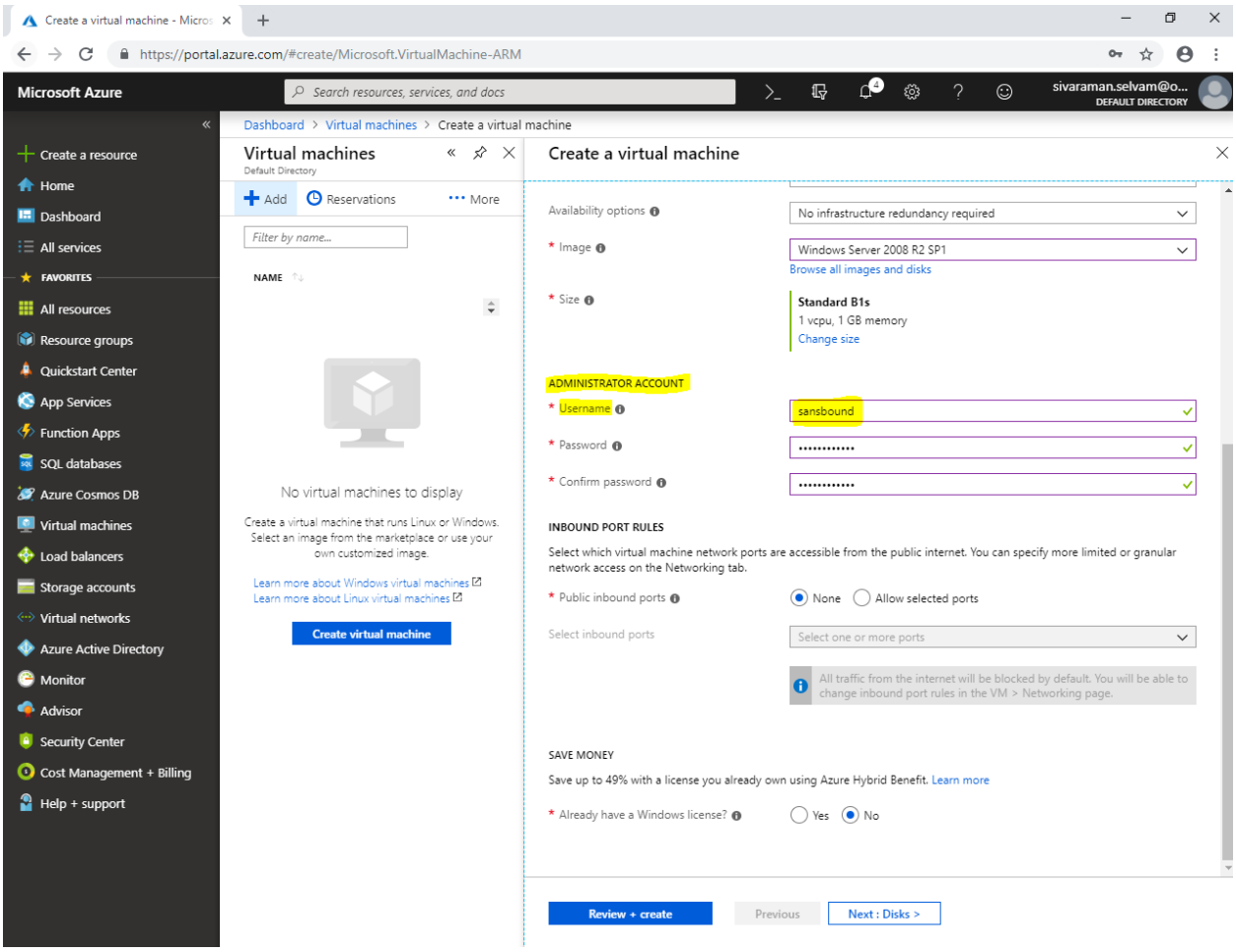
Change **“VM Size”** as **“Standard B1s”**.



In **“Administrator Account”**

Type **“username”** as **“sansbound”**.

Type **“password”** for Windows Server 2008 R2.

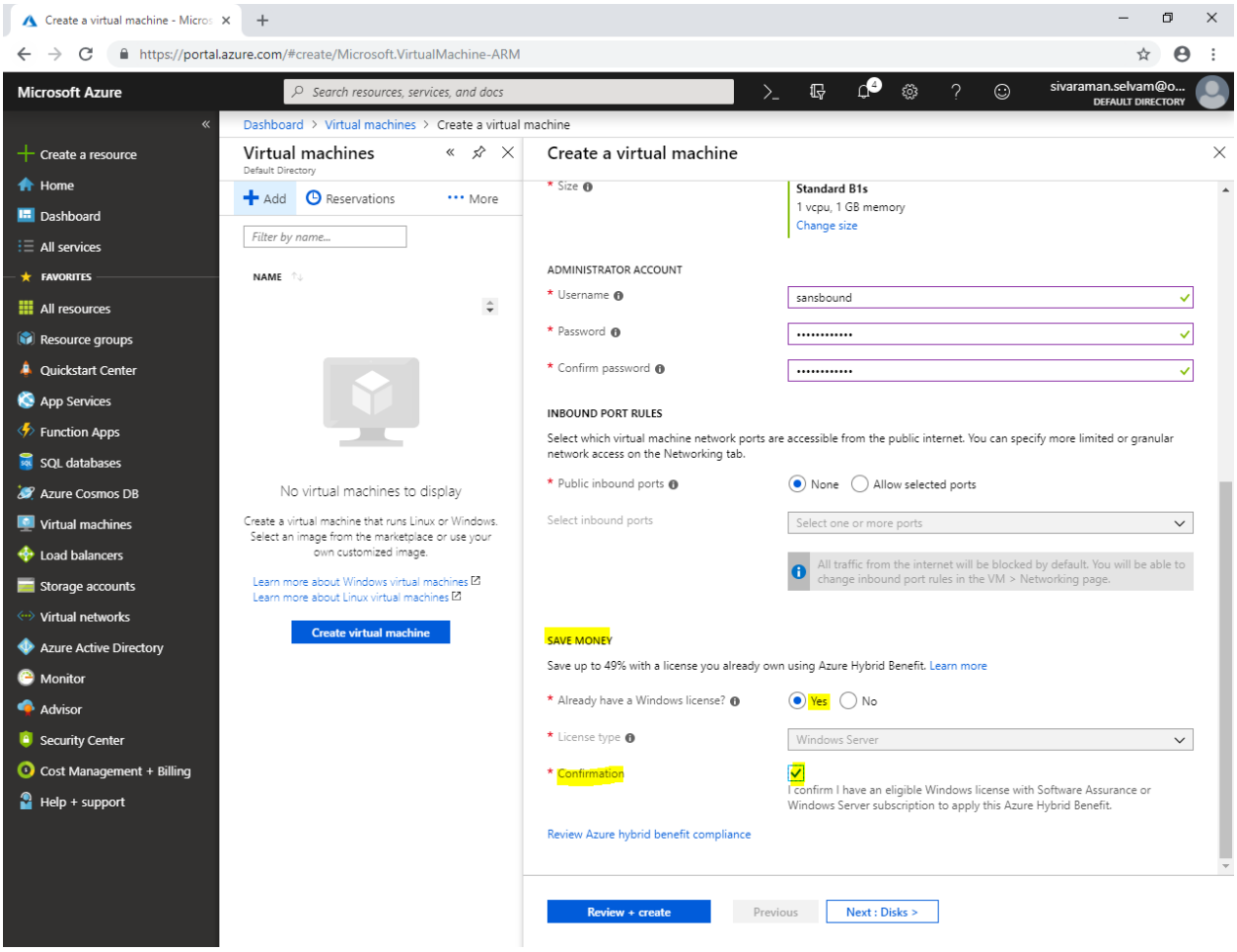


In **“Save Money”**.

Click **“Yes”** for already have a windows license.

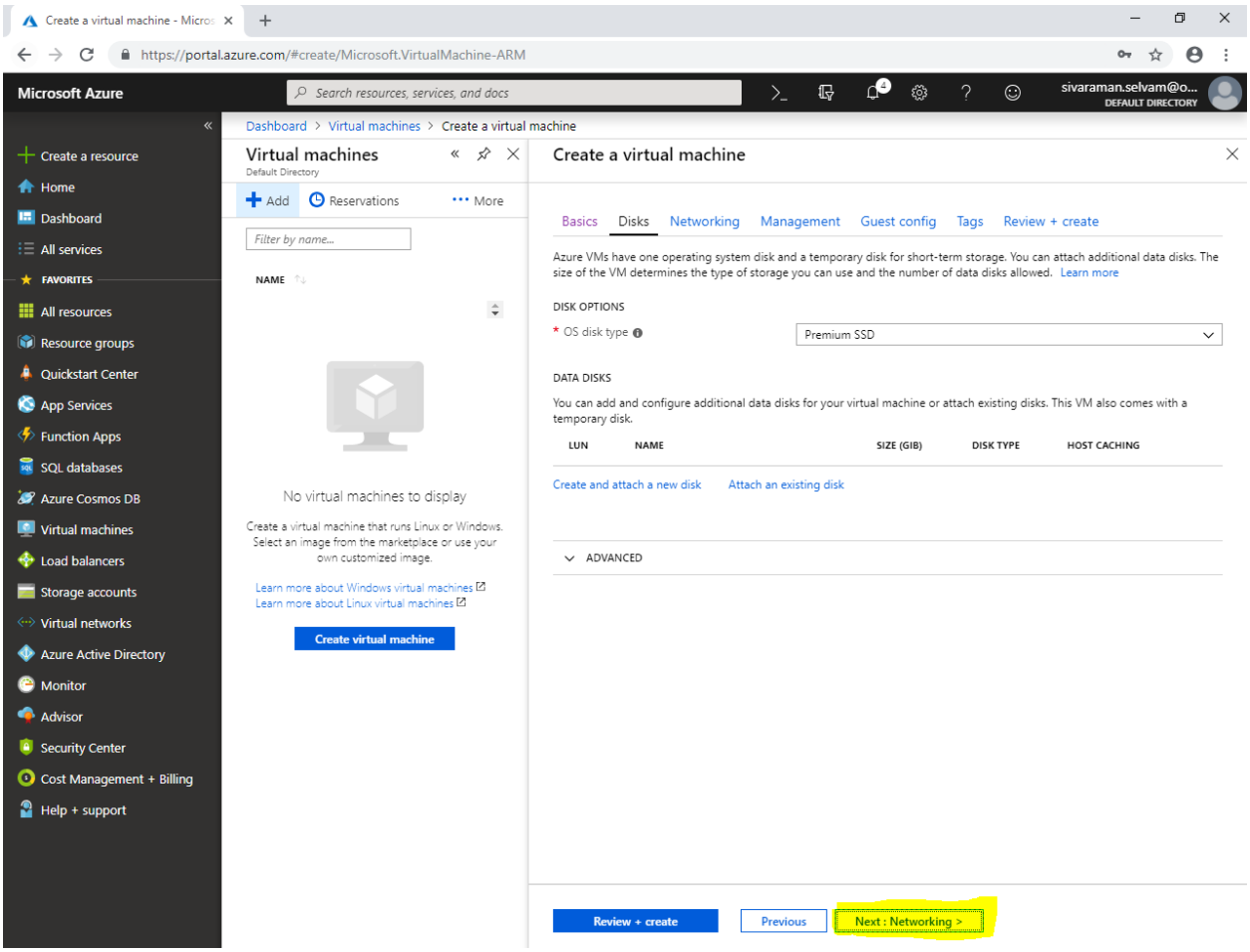
In **“Confirmation”** need to check.

Click **“Next : Disks >”**.



In **“Disks”,**

Click **“Next : Networking >”**.

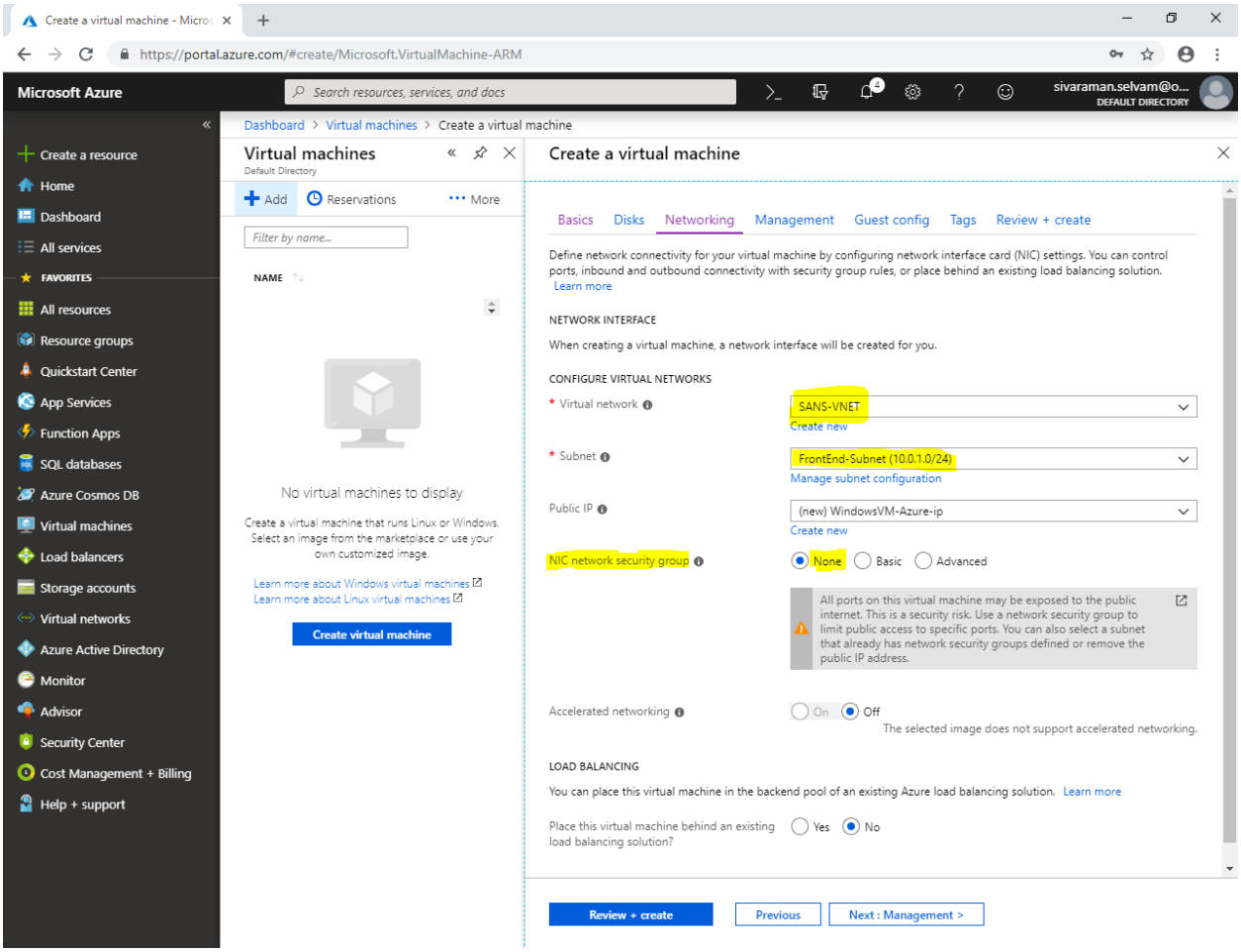


In **“Networking”**

Ensure that **“Virtual network”** as **“SANS-VNET”**.

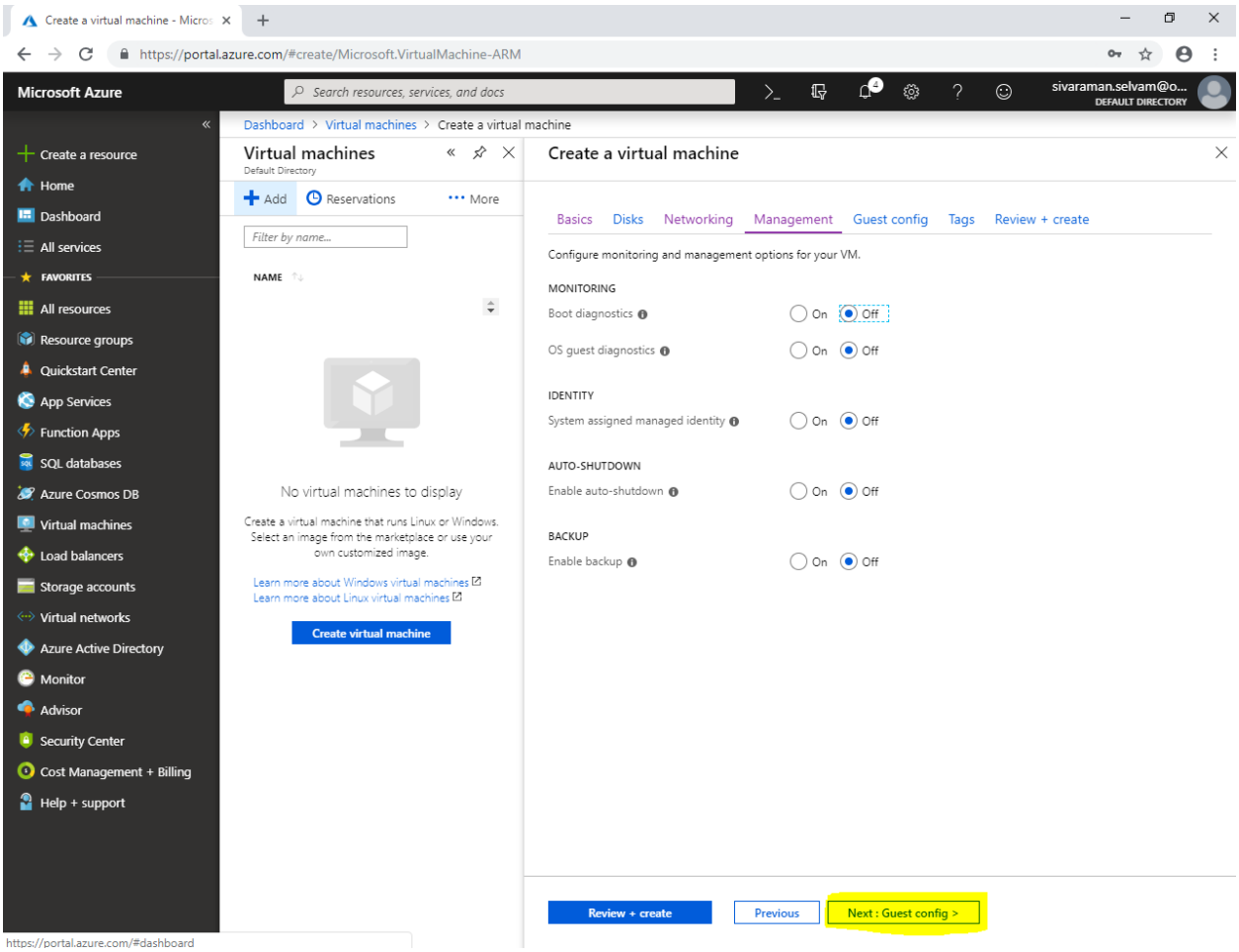
Ensure that **“FrontEnd-Subnet”** subnet is selected, because this subnet only will be accessible from public network.

In **“NIC network security group”** as **“None”**.



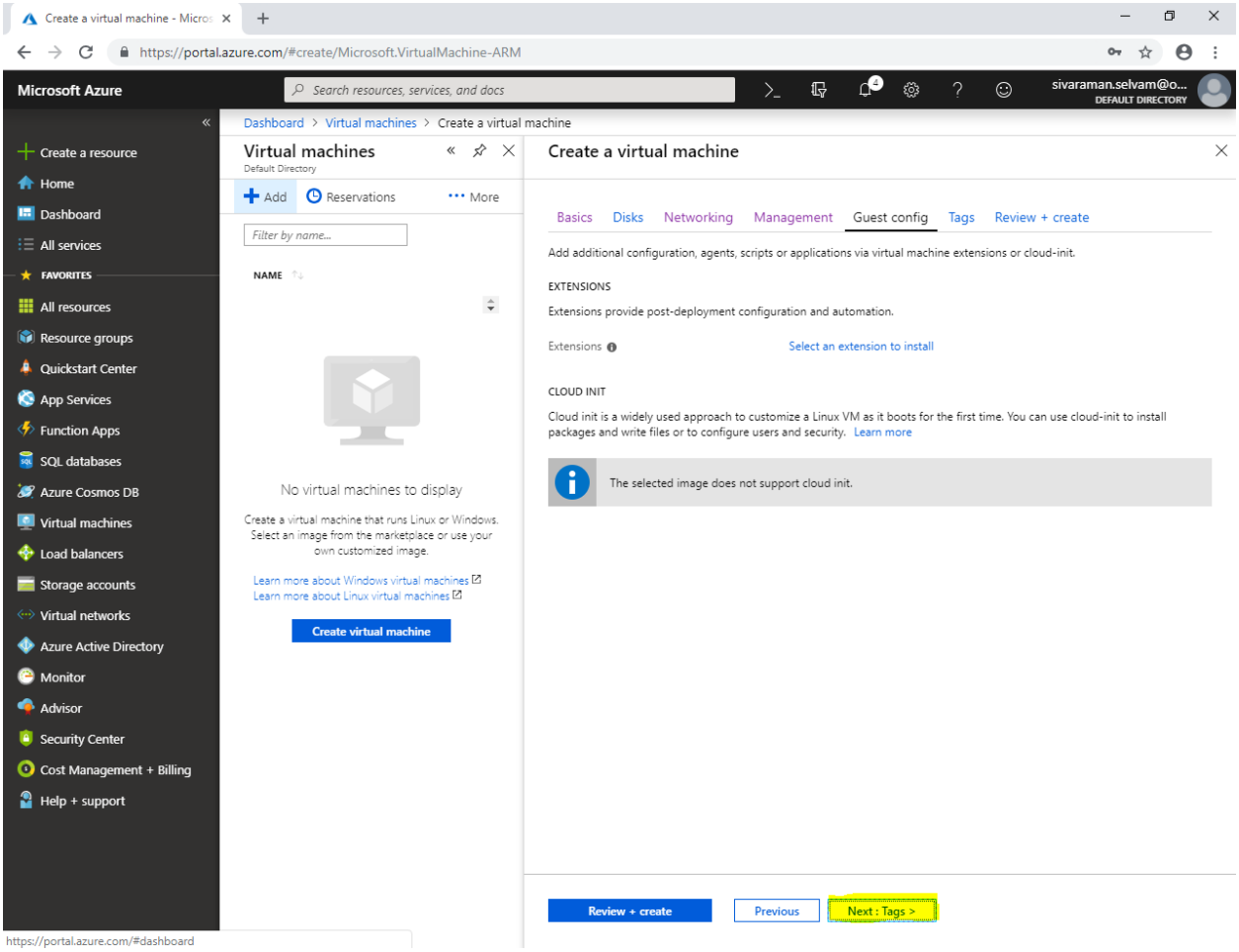
In **“Management”**

Click **“Next : Guest config >”**.



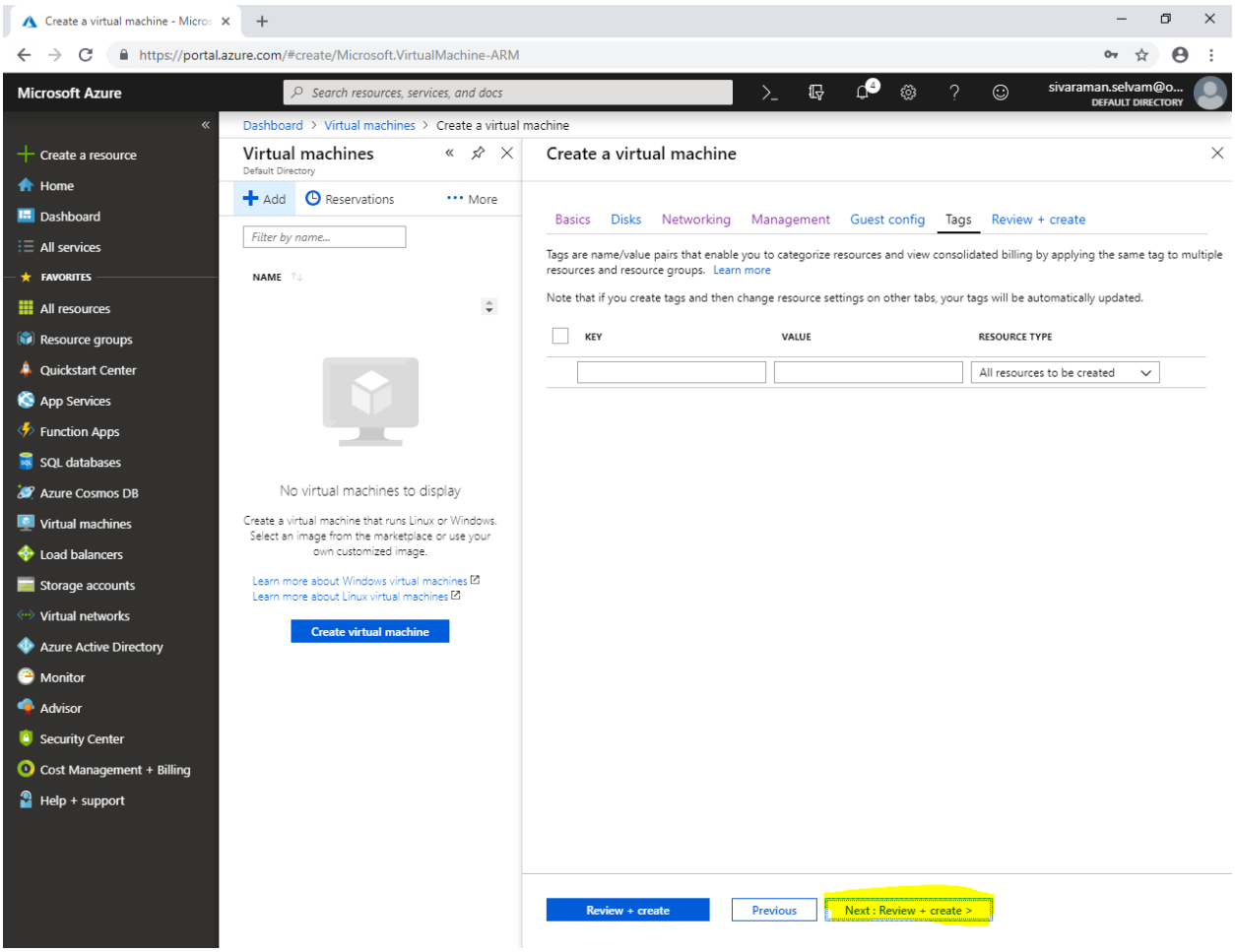
In **“Guest config”**.

Click **“Next : Tags >”**.

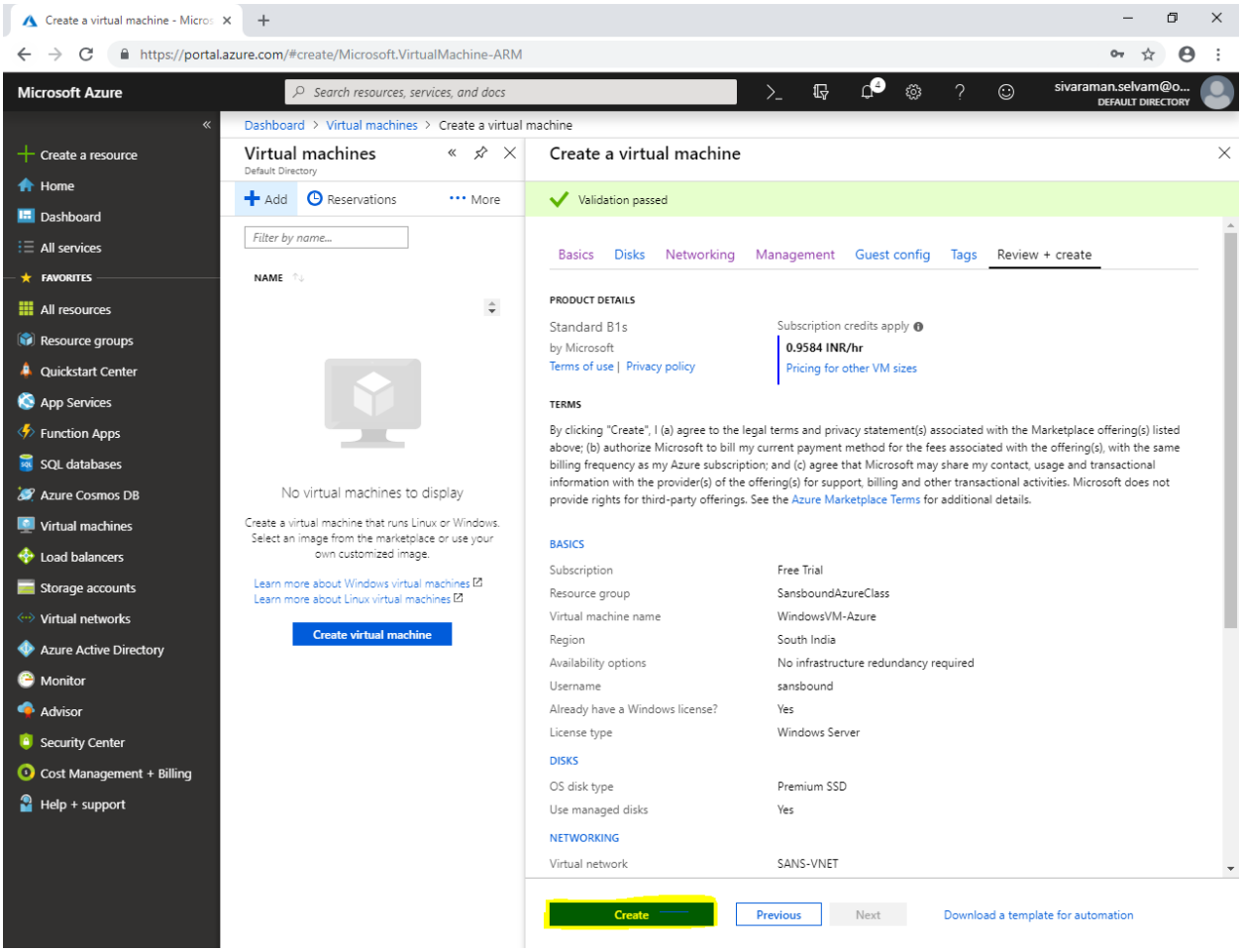


In **“Tags”**.

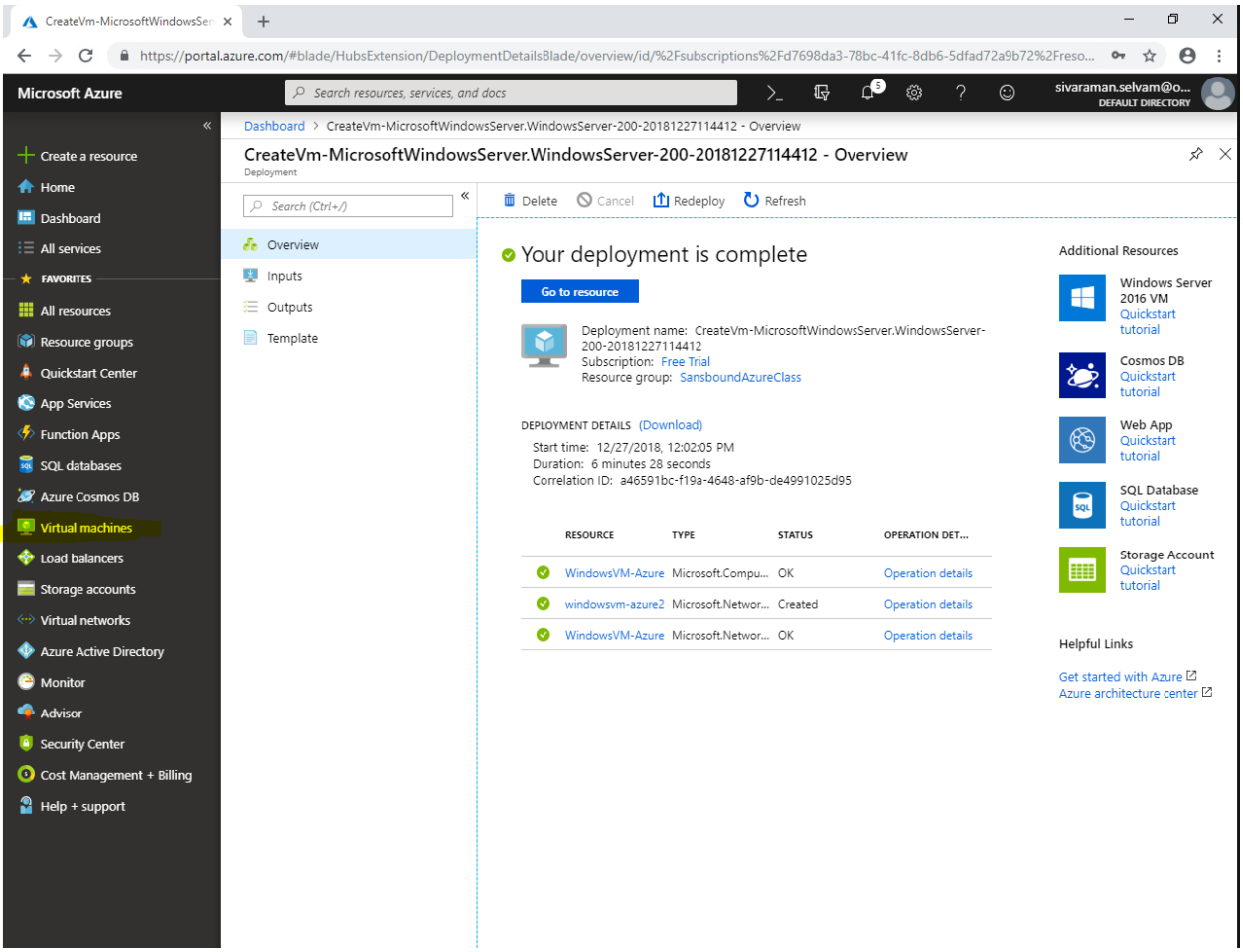
Click **“Review + create”**.



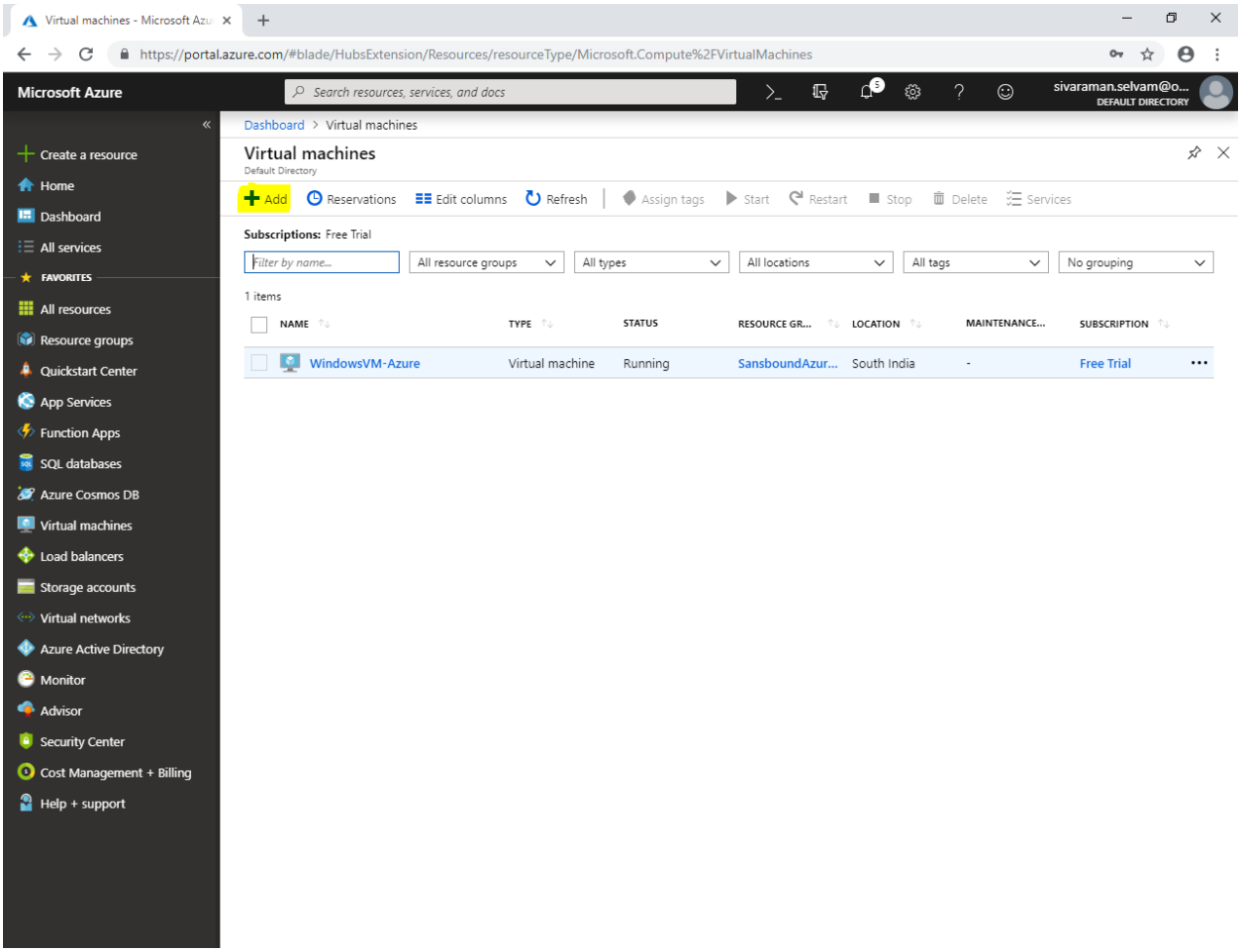
Click **"Create"**.



Click **“Virutal machine”**.



Click **“Add”** to create new virtual machine in BackEnd-Subnet which is not publicly available.



While create Virtual machine,

Select **“Subscription”** as **“Free Trial”**.

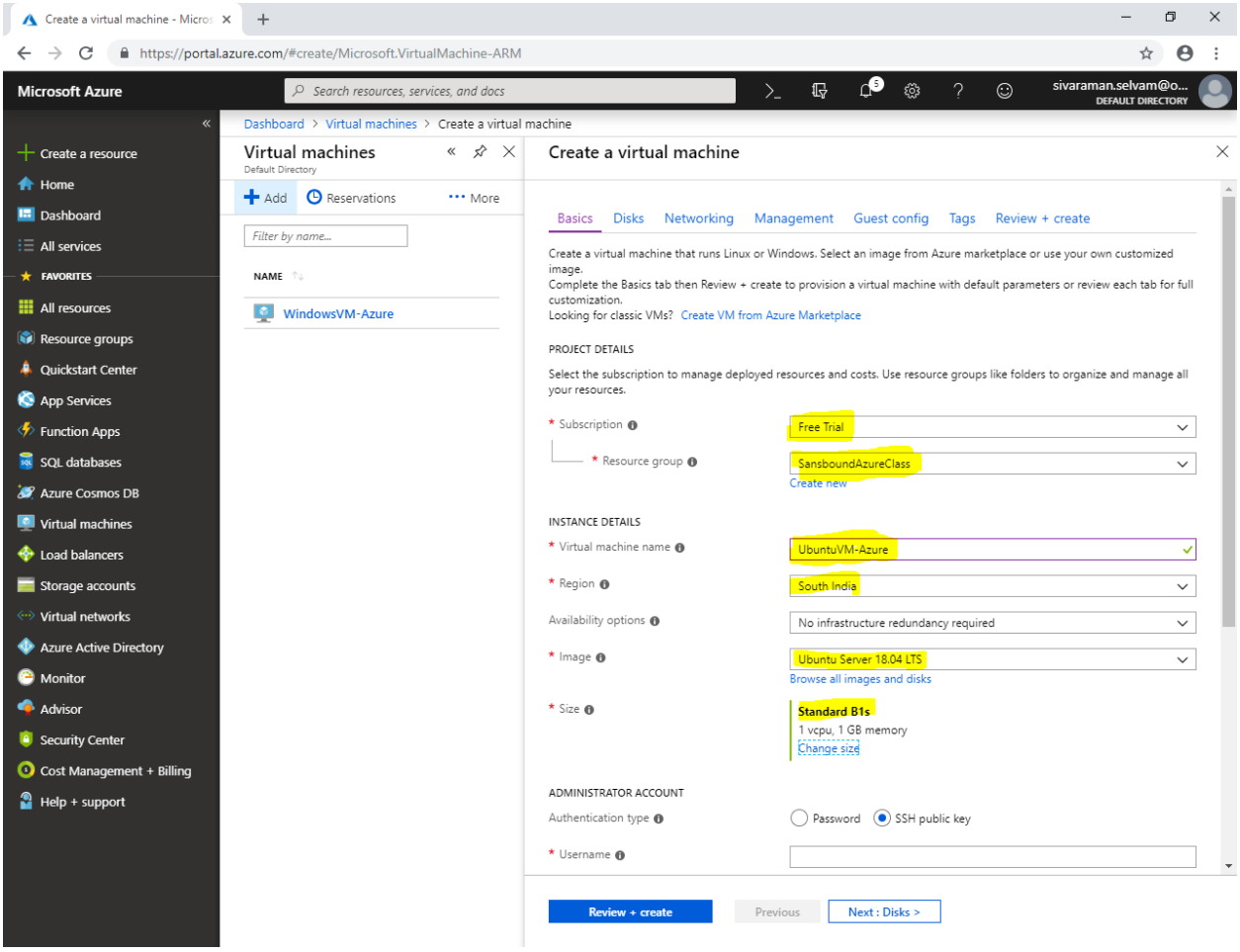
Select **“Resource group”** as **“SansboundAzureClass”**.

Type **“Virtual machine name”** as **“UbuntuVM-Azure”.**

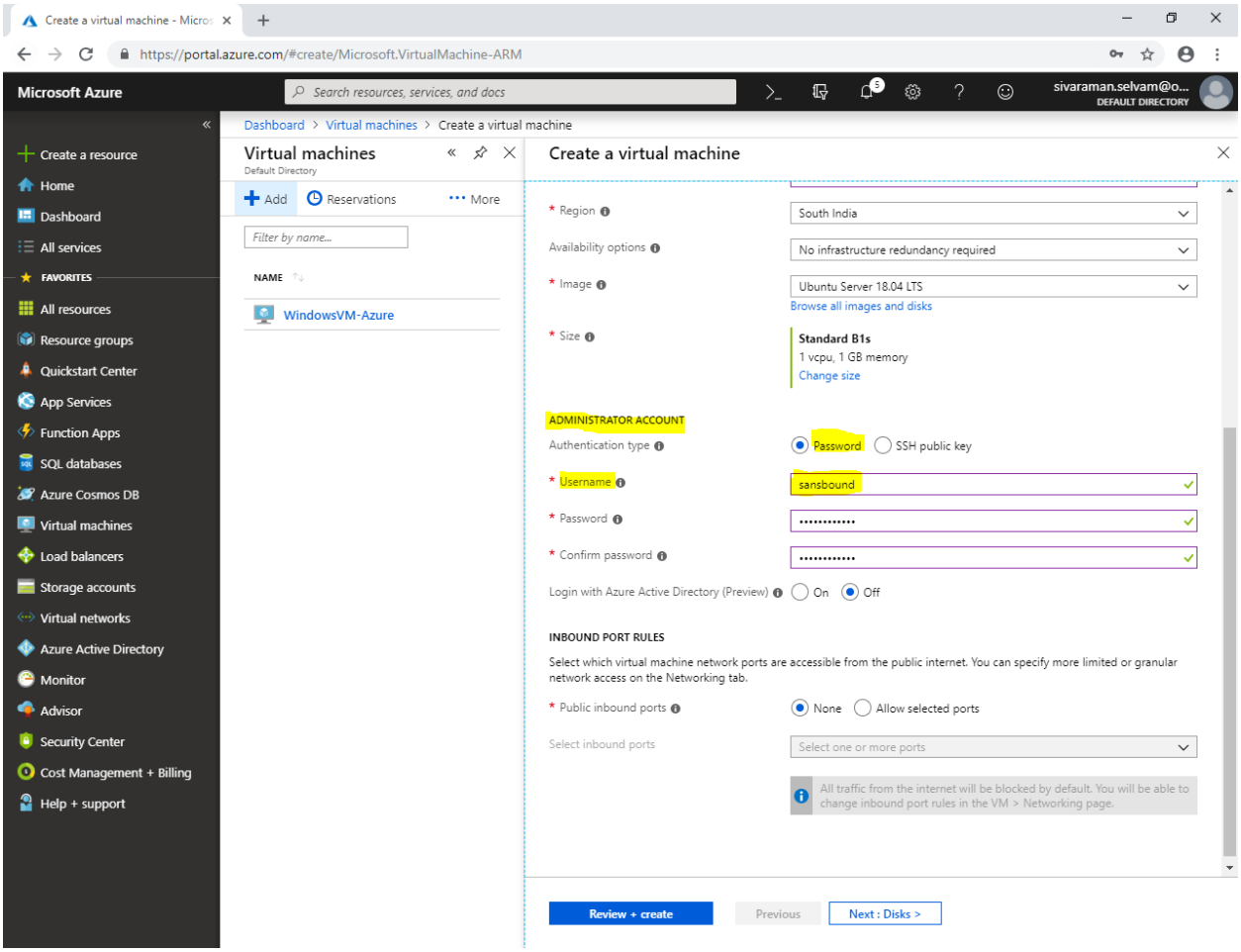
Select **“Region”** as **“South India”**.

Select **“Image”** as **“Ubuntu Server 18.04 LTS”**.

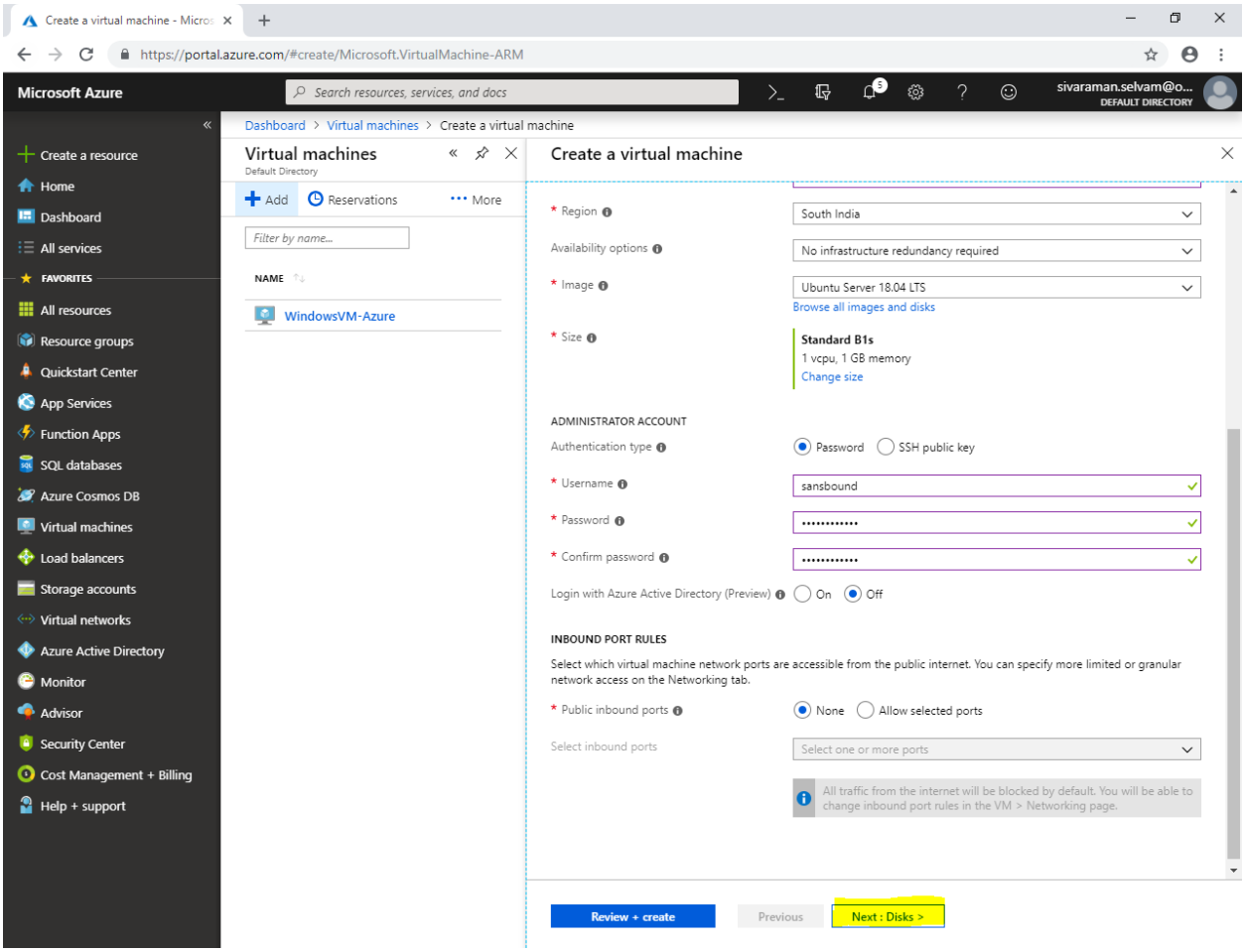
Change **“VM Size”** as **“Standard B1s”**.



In **“Administrator Account”** click **“Authentication type”** as **“Password”.**



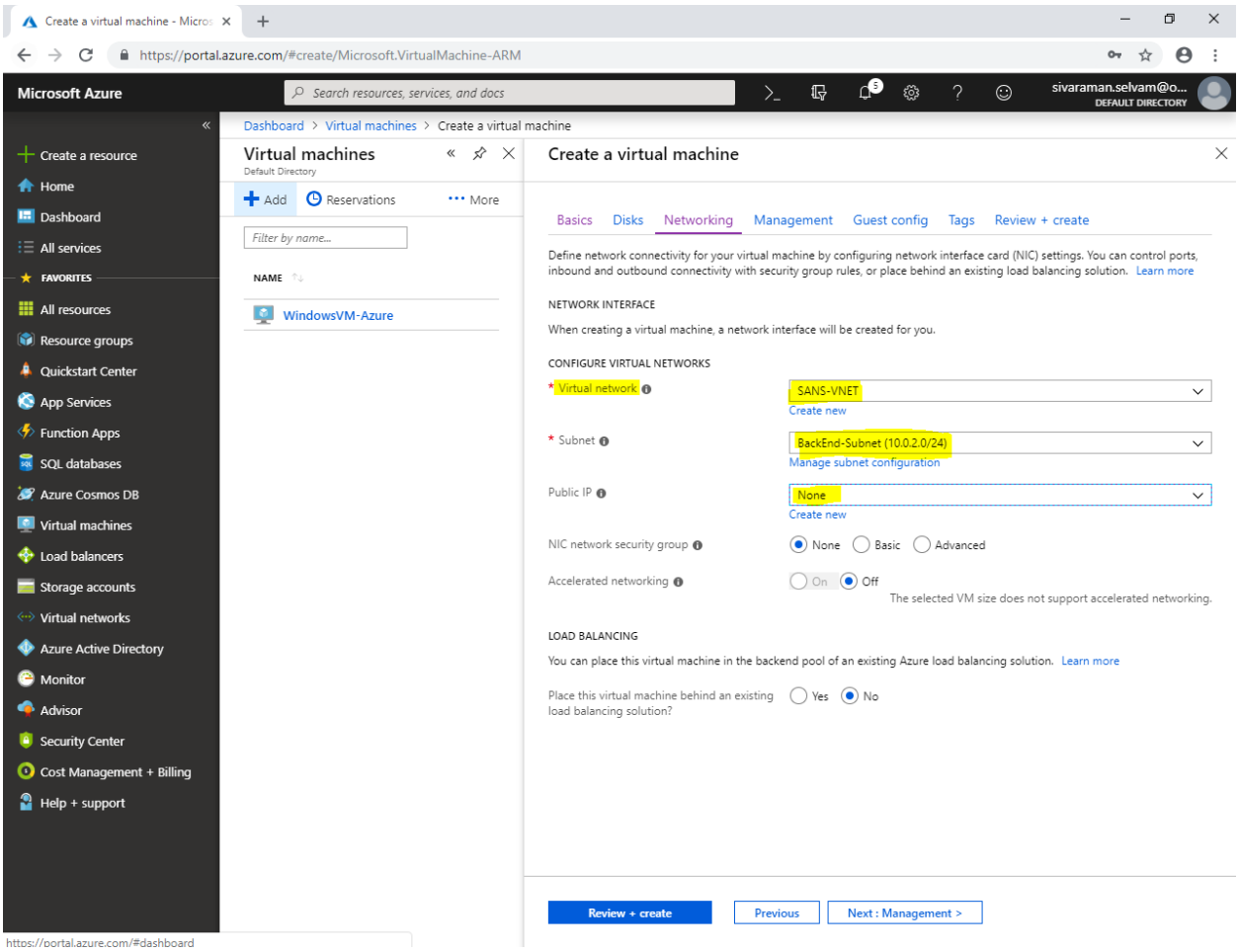
Click **“Next : Disks >”**.



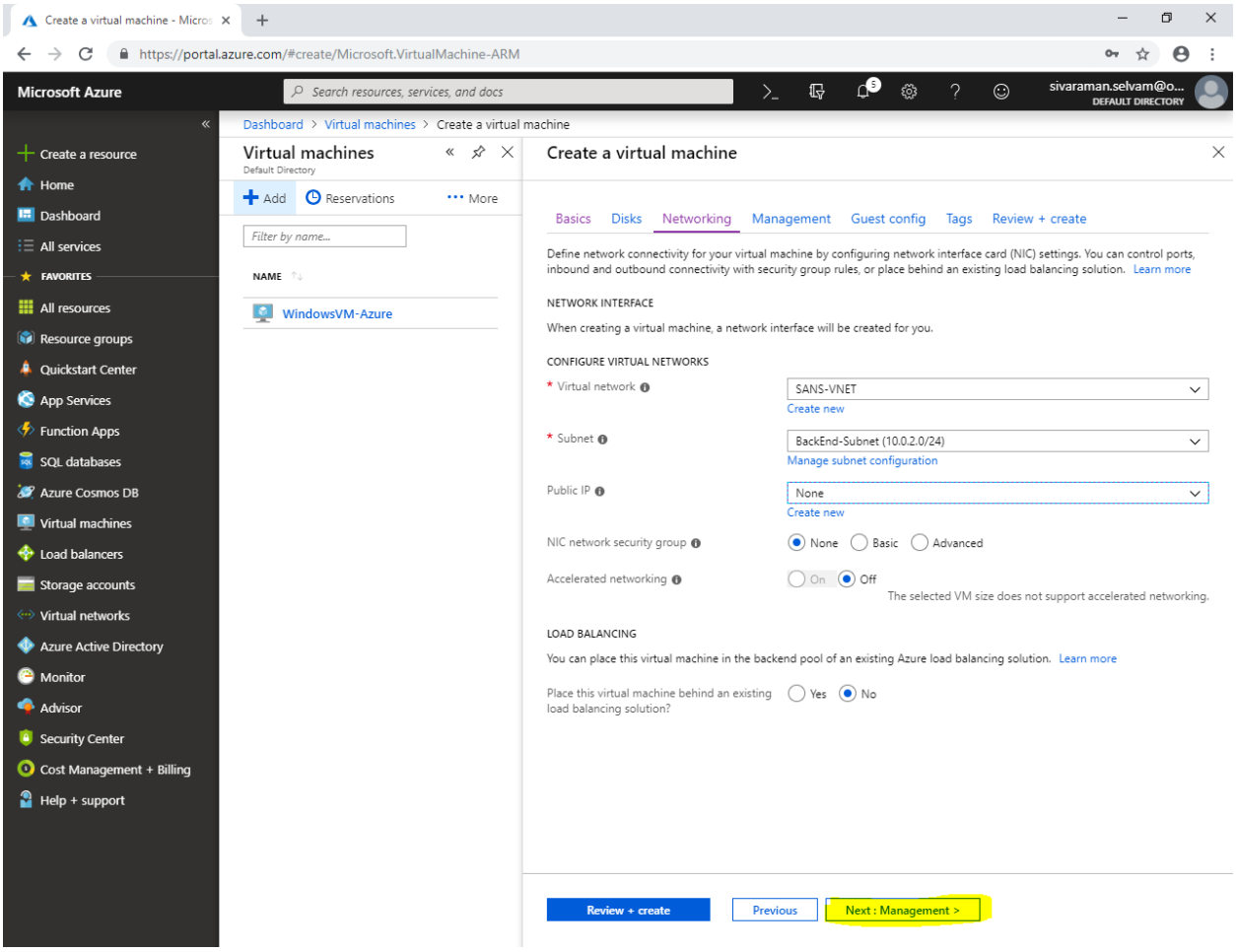
In **"Networking"**,

In **"Virtual network"** select as **"SANS-VNET"**.

In **"Subnet"** as **"BackEnd-Subnet"** because this subnet would not be accessible from public network.

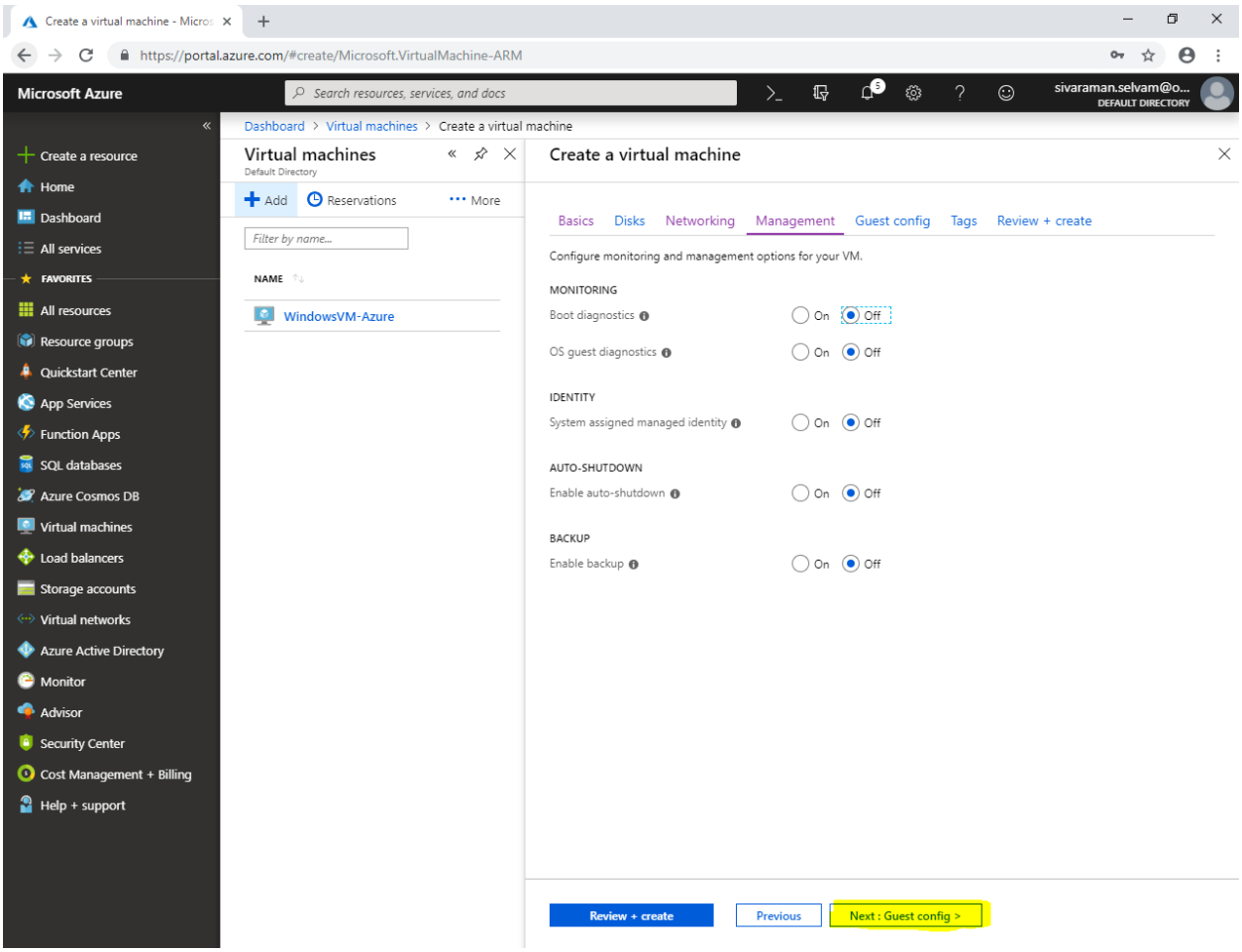


Click **“Next : Management >”**.



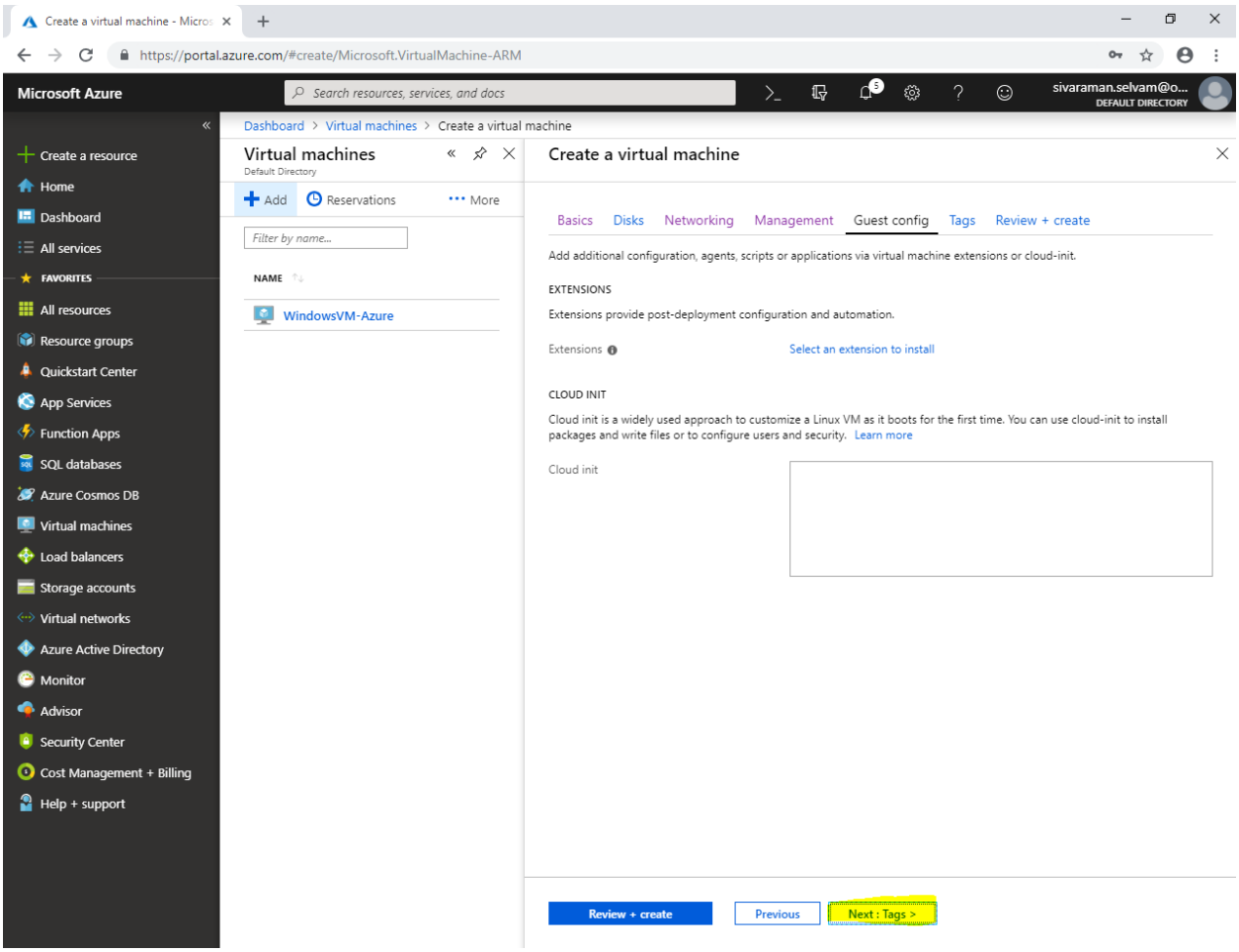
In **“Management”.**

Click **“Next : Guest config >”**.



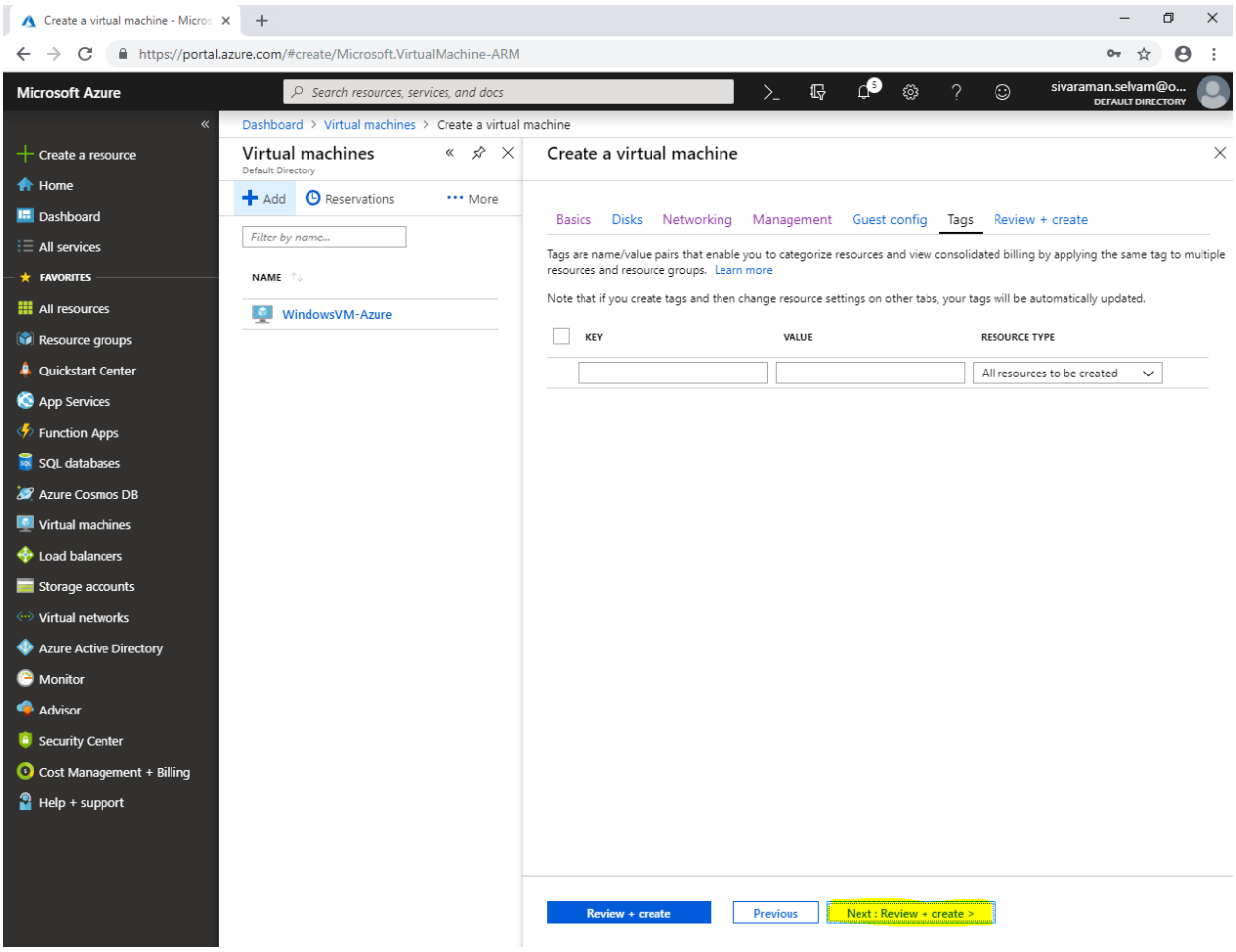
In **“Guest config”**

Click **“Next : Tags >”**.

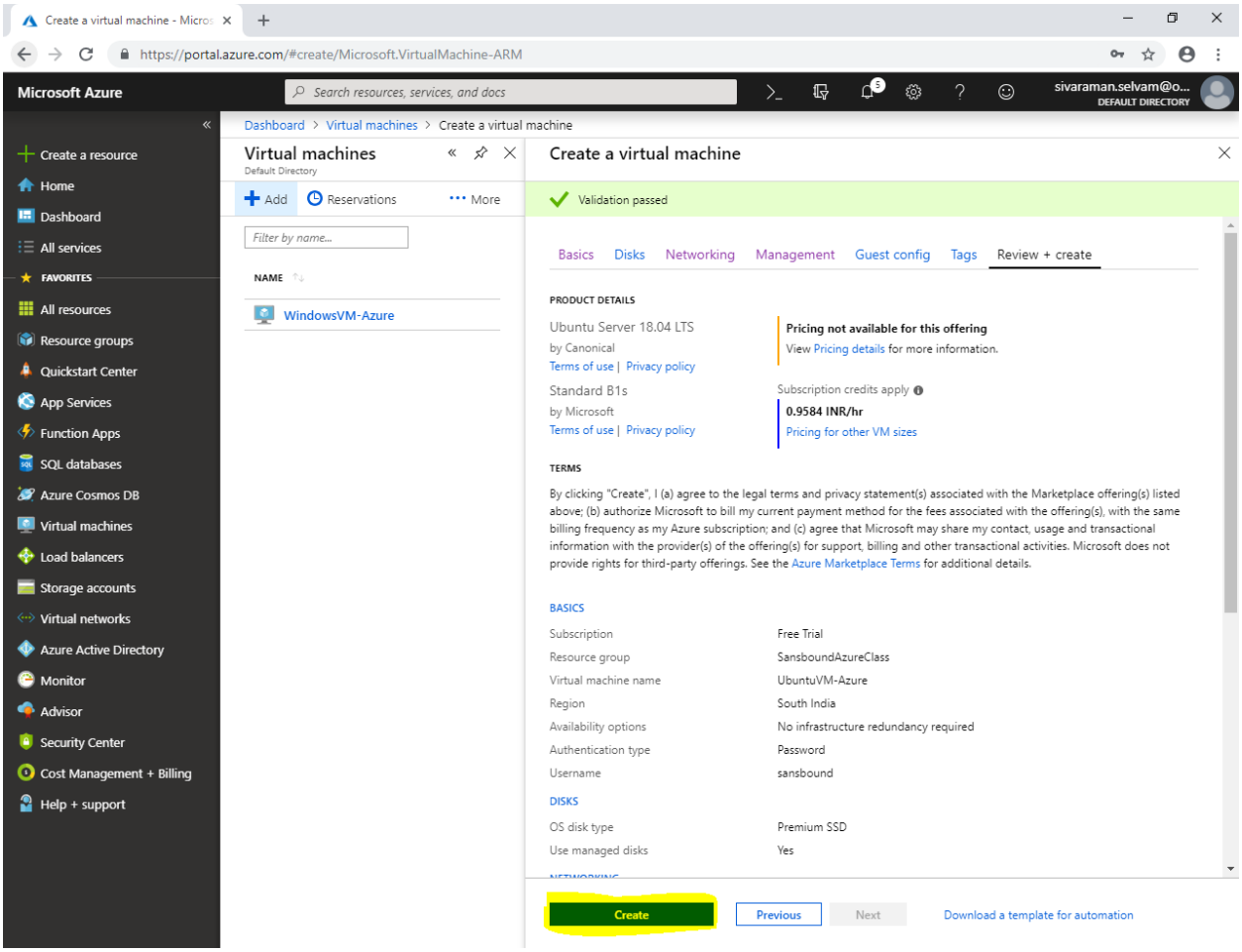


In **“Tags”.**

Click **“Review + create”**.



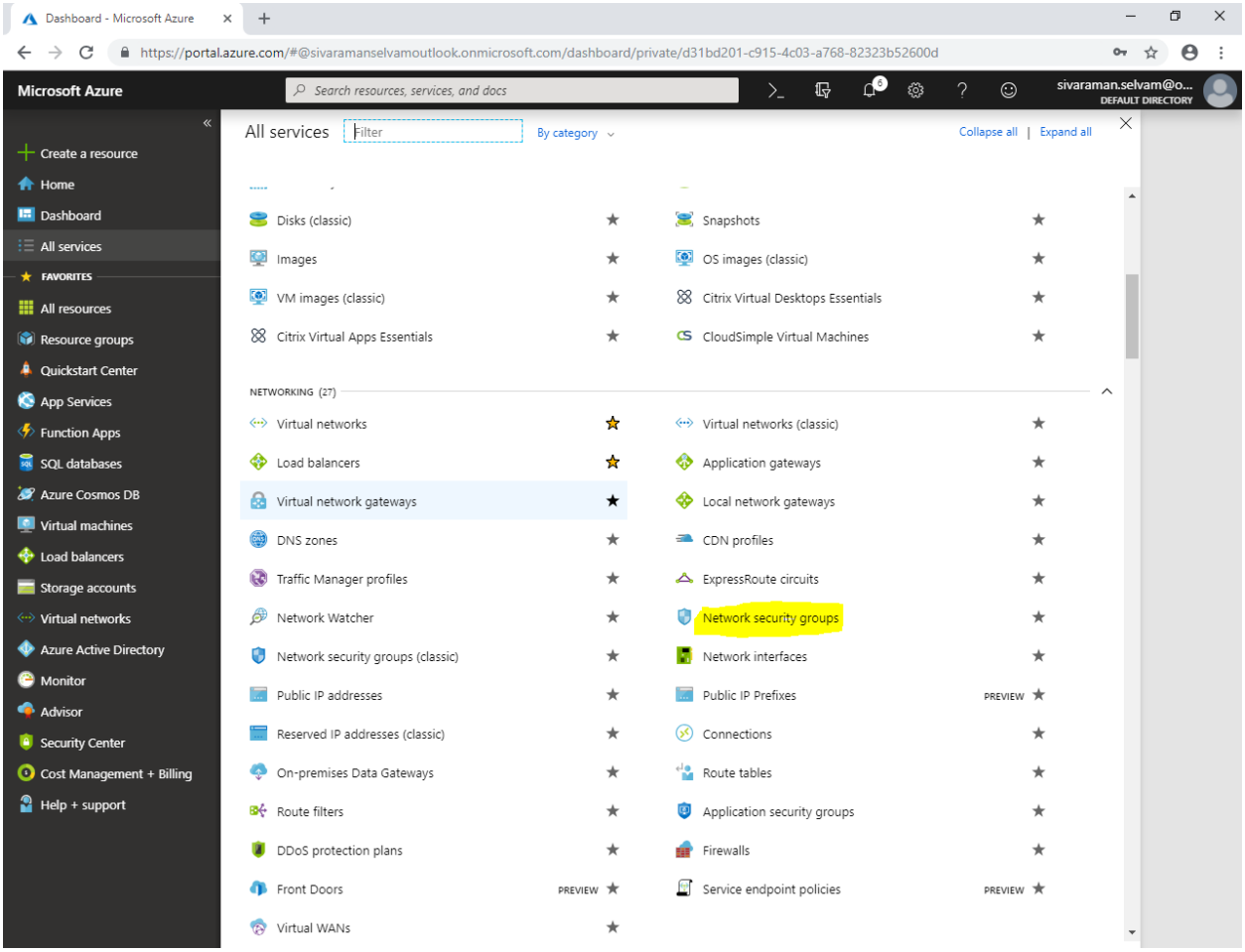
Click **“Create”**.



Click **"All services"** in dashboard (left side panel).

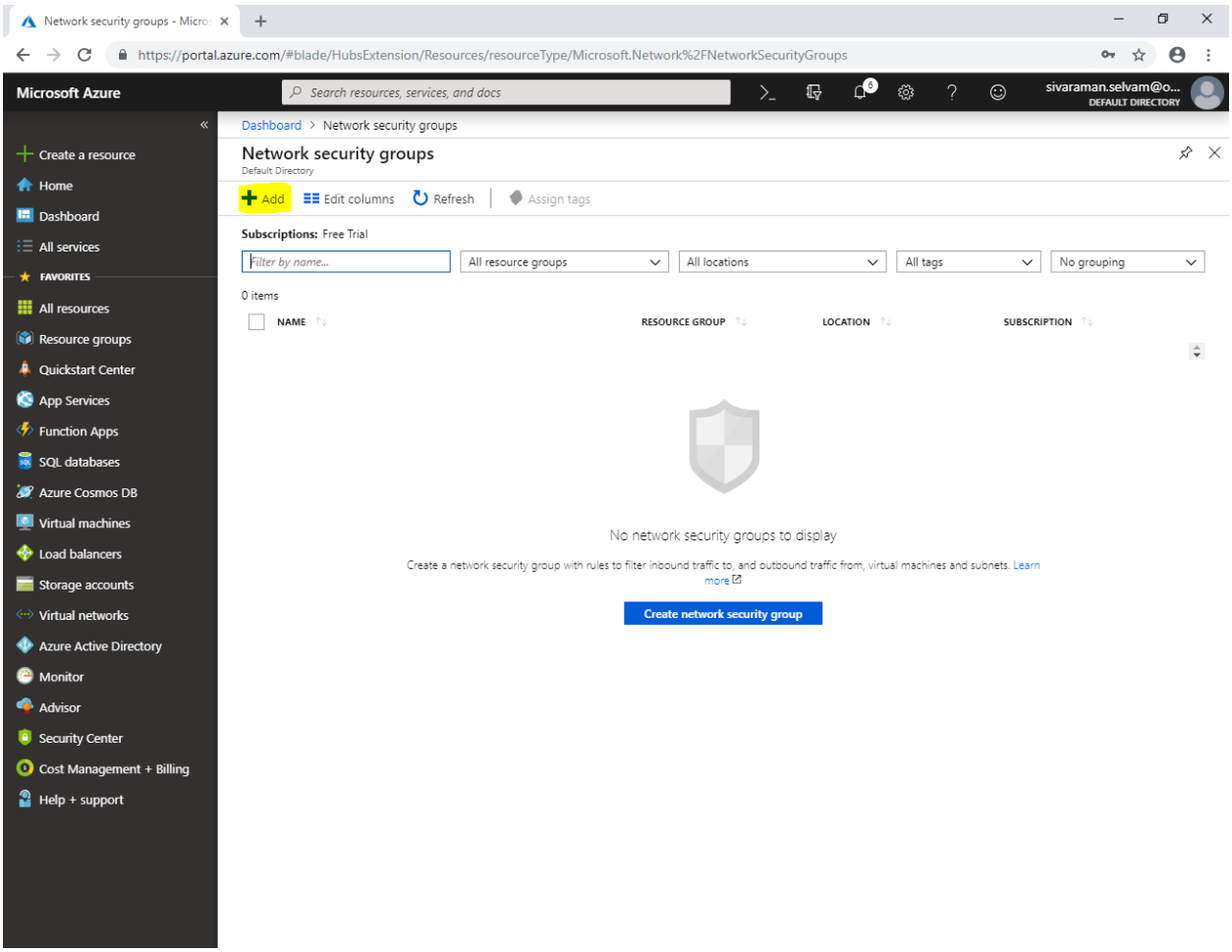
In **"Networking"**.

Click **"Network security groups"**.



In **“Network security groups”**.

Click **“Add”.**



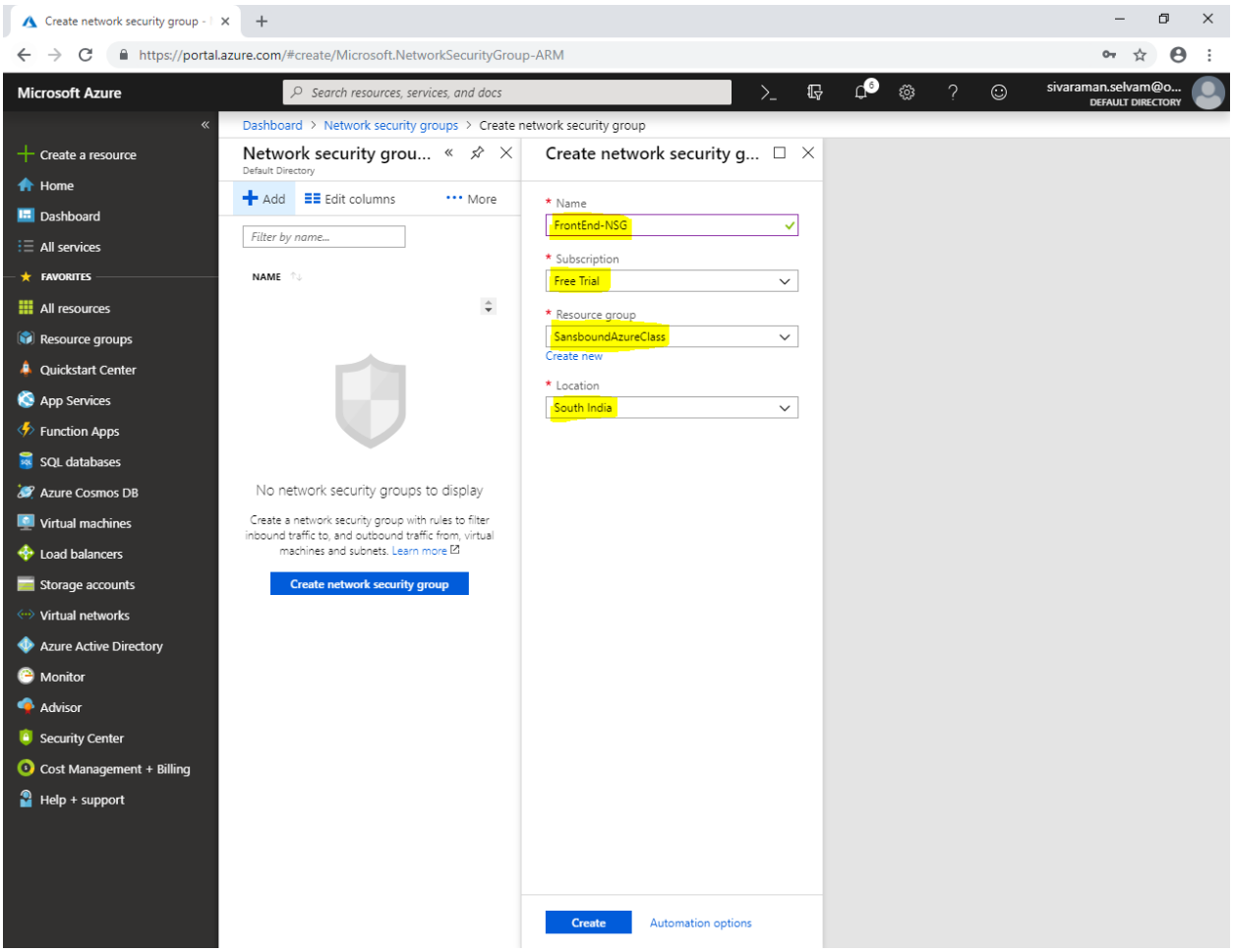
While creating **“Network Security Group”** it requires,

Name **“FrontEnd-NSG”**.

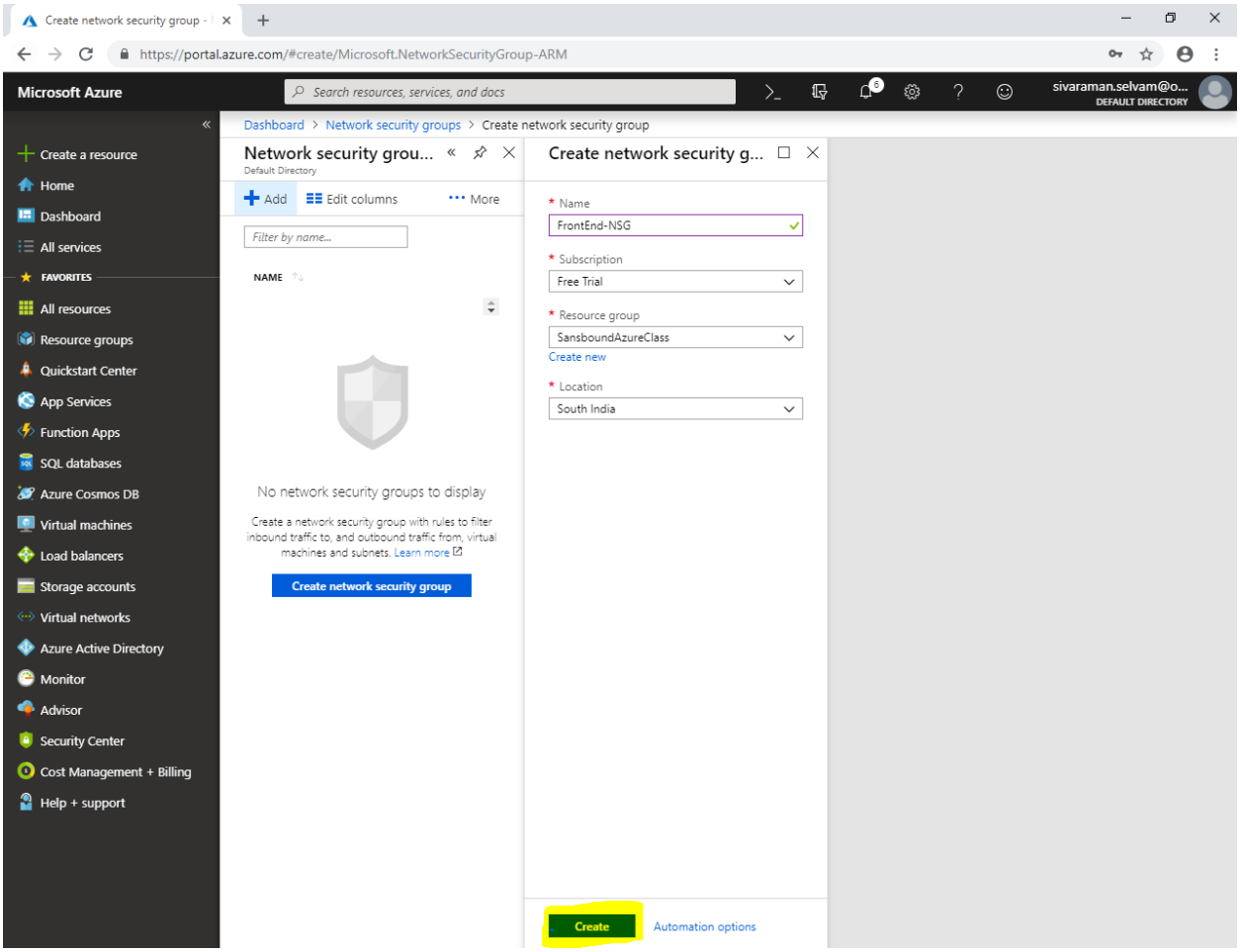
Select **“Subscription”** as **“Free Trial”**.

Select **“Resource group”** as **“SansboundAzureClass”**.

Select **“Location”** as **“South India”**.

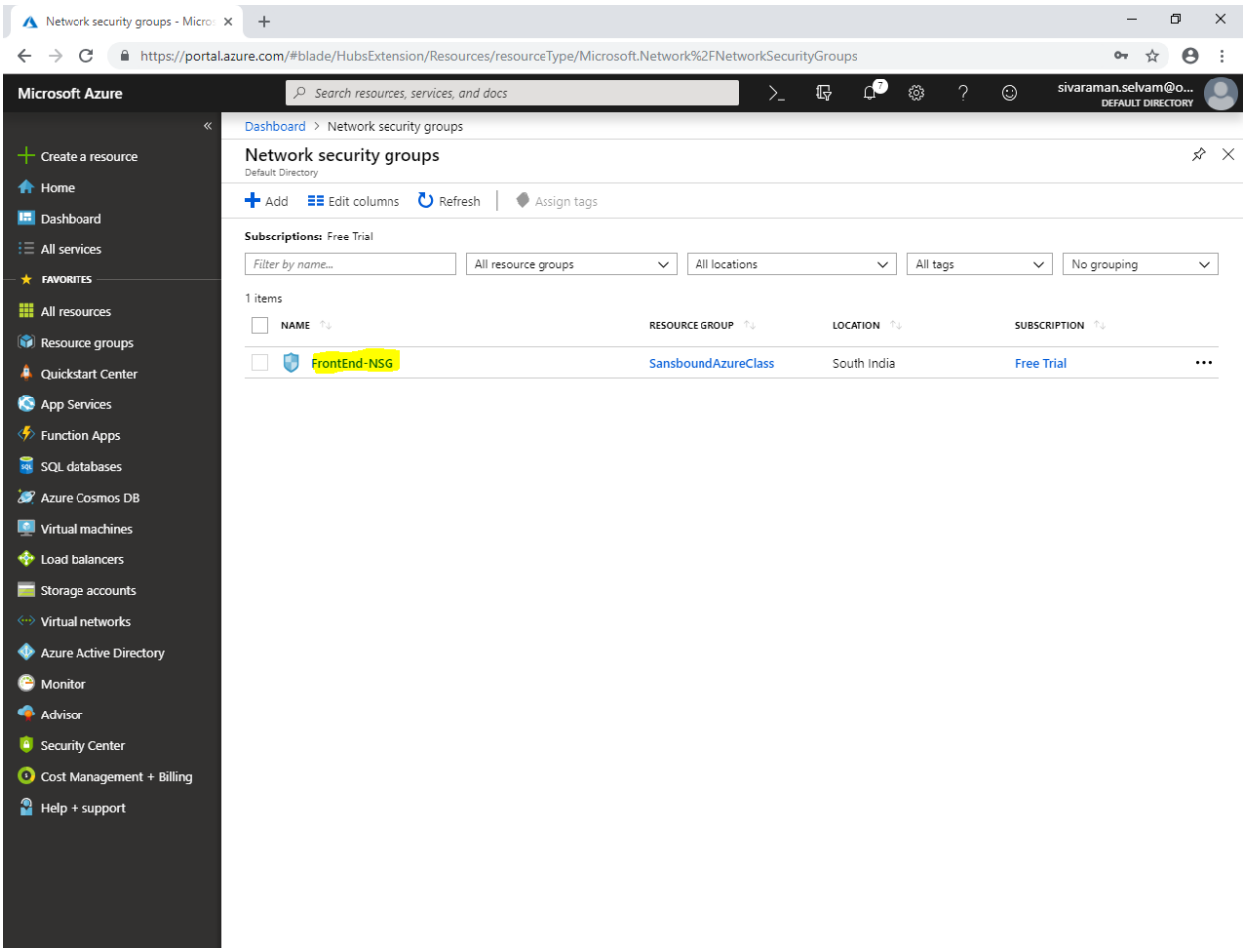


Click **“Create”**.



In **“Network security groups”** click **“Refresh”** to view the newly created **“Network Security Group”**

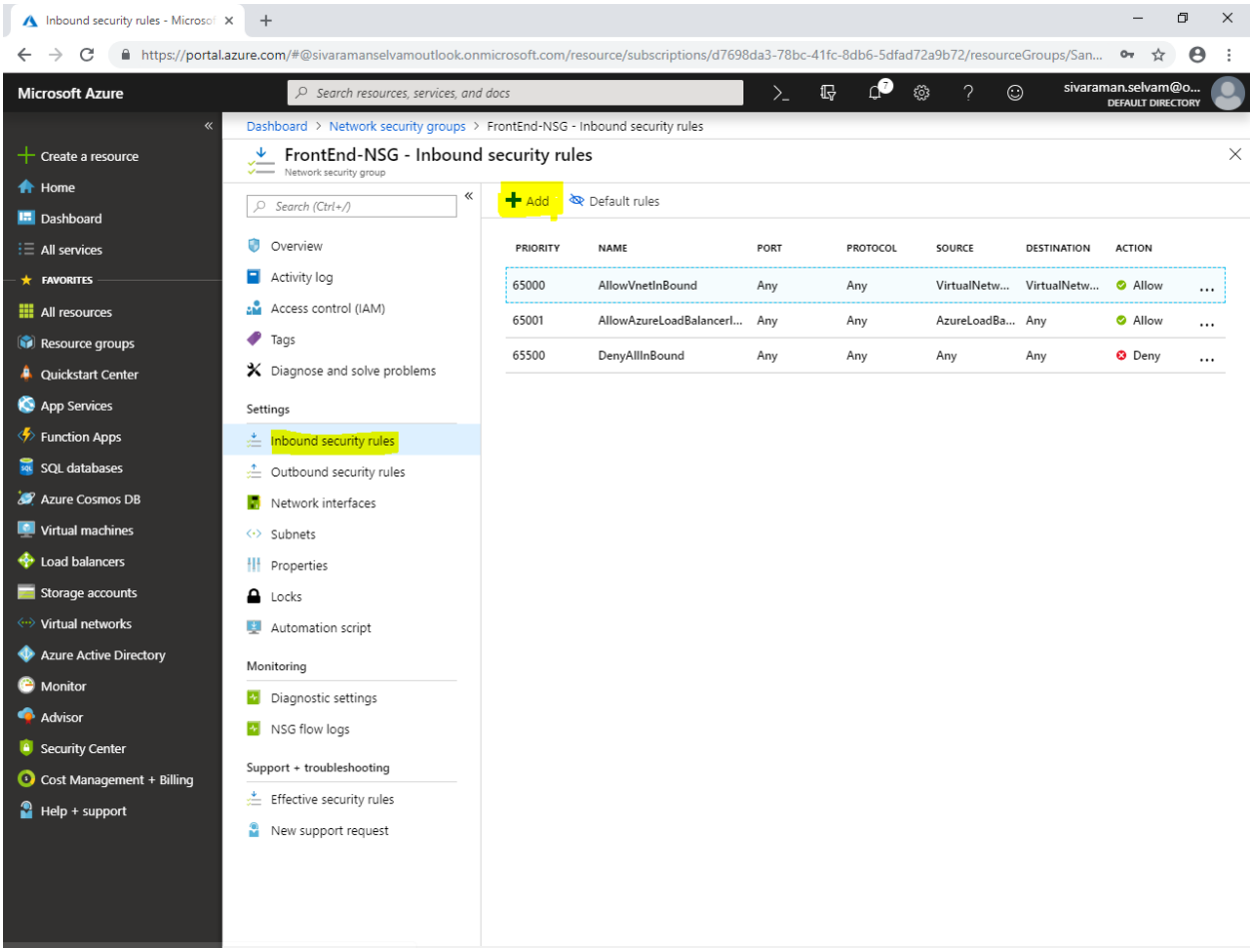
Click **“Network Security groups”** named as **“FrontEnd-NSG”**.



In **“Inbound security rules”**

You are able to see three rules created by default. In “Inbound security rules” all inbound rule has been denied due to **“DenyAllInbound”** from outside.

Click **“Add”.**



While **“Add inbound security rule”**,

In **“Source”** as **“Any”**.

In **“Source port ranges”** as **“*”** to allow from All sources.

In **“Destination”** as **“Any”**.

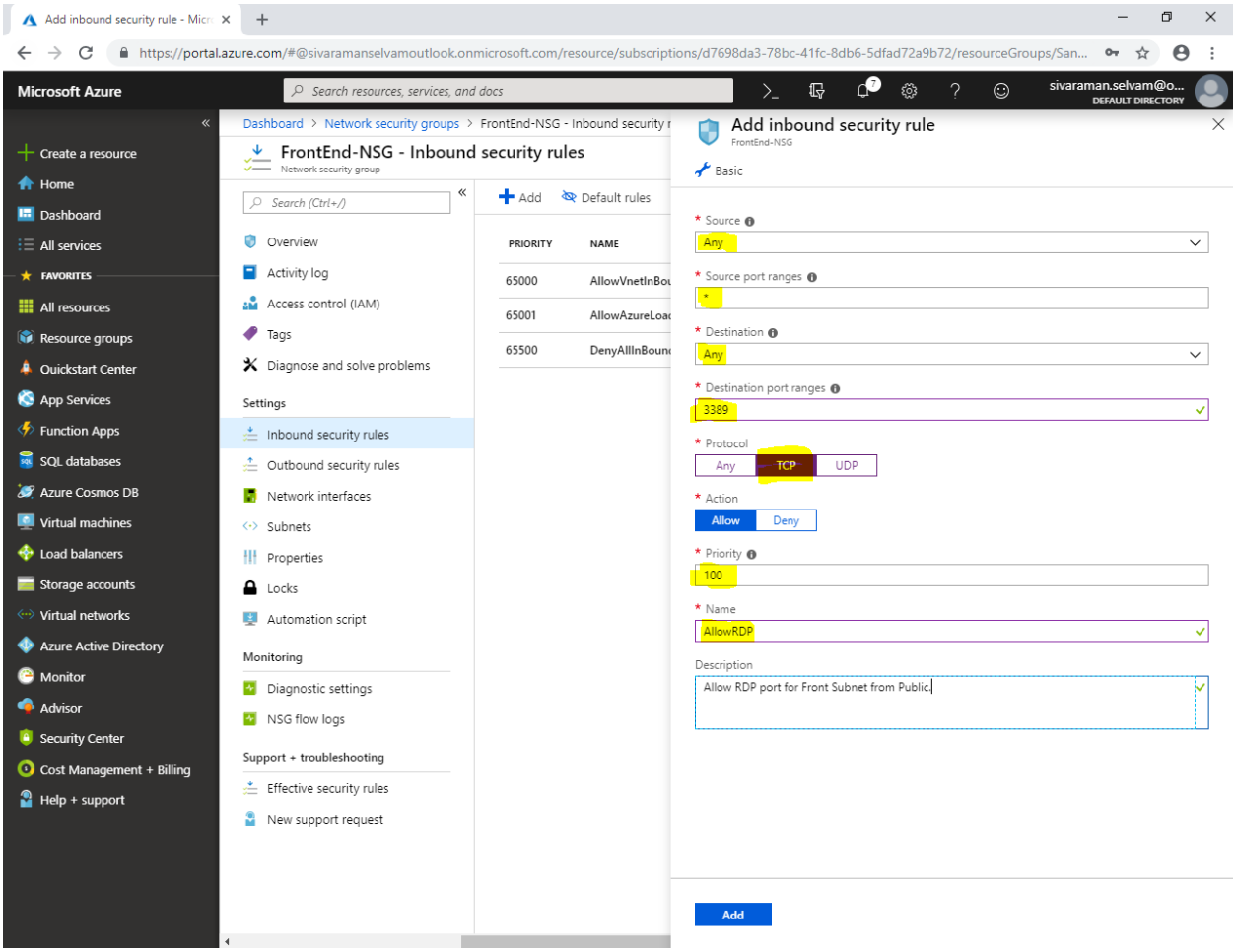
In **“Destination port ranges”** as **“3389”** (To Allow RDP port to access the server through remotely).

“Protocol” click on **“TCP”**.

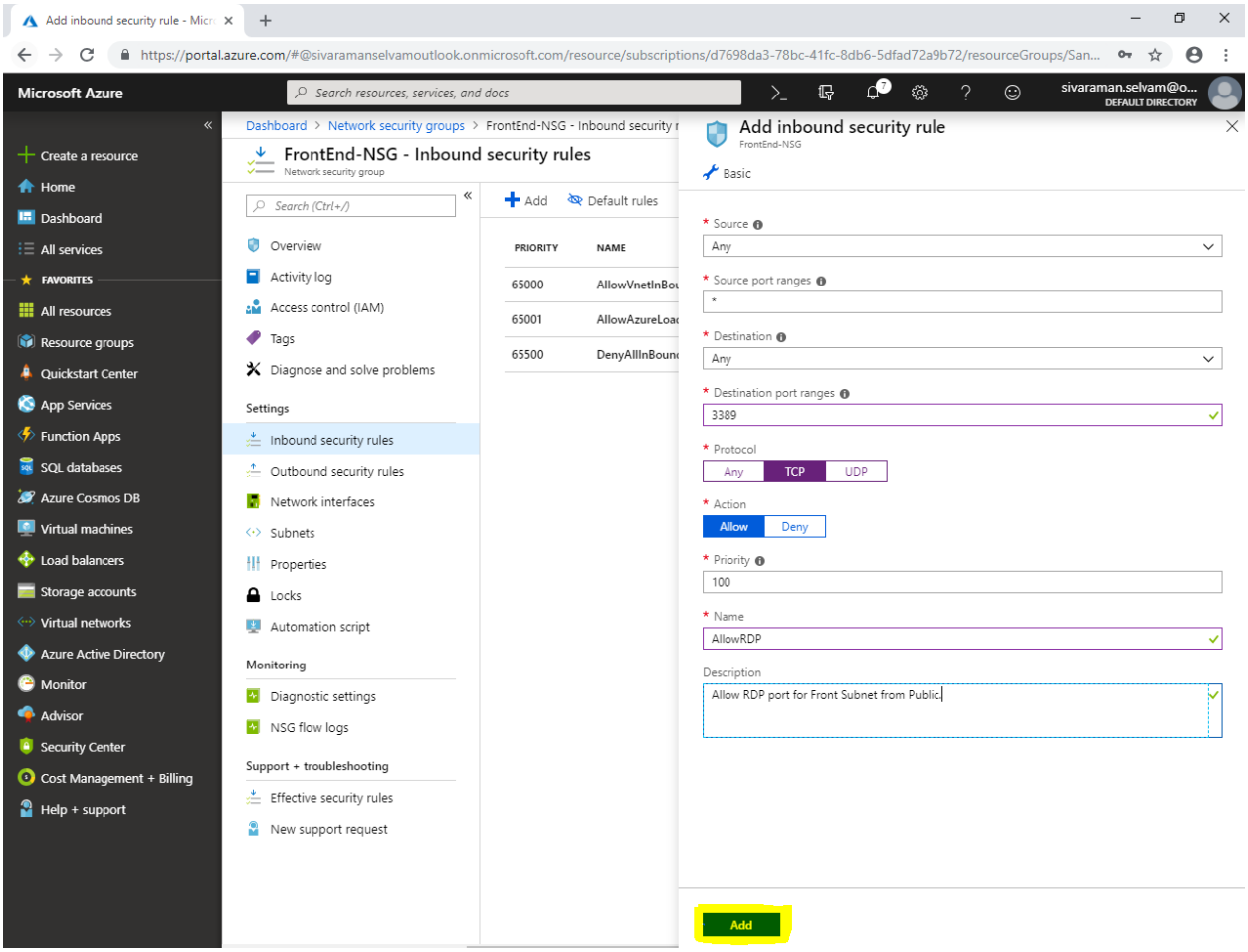
“Action” as **“Allow”**.

“Priority” as **“100”**. **(Lowest priority rule will be applied first)**”.

Type Rule **“Name”** as **“AllowRDP”.**

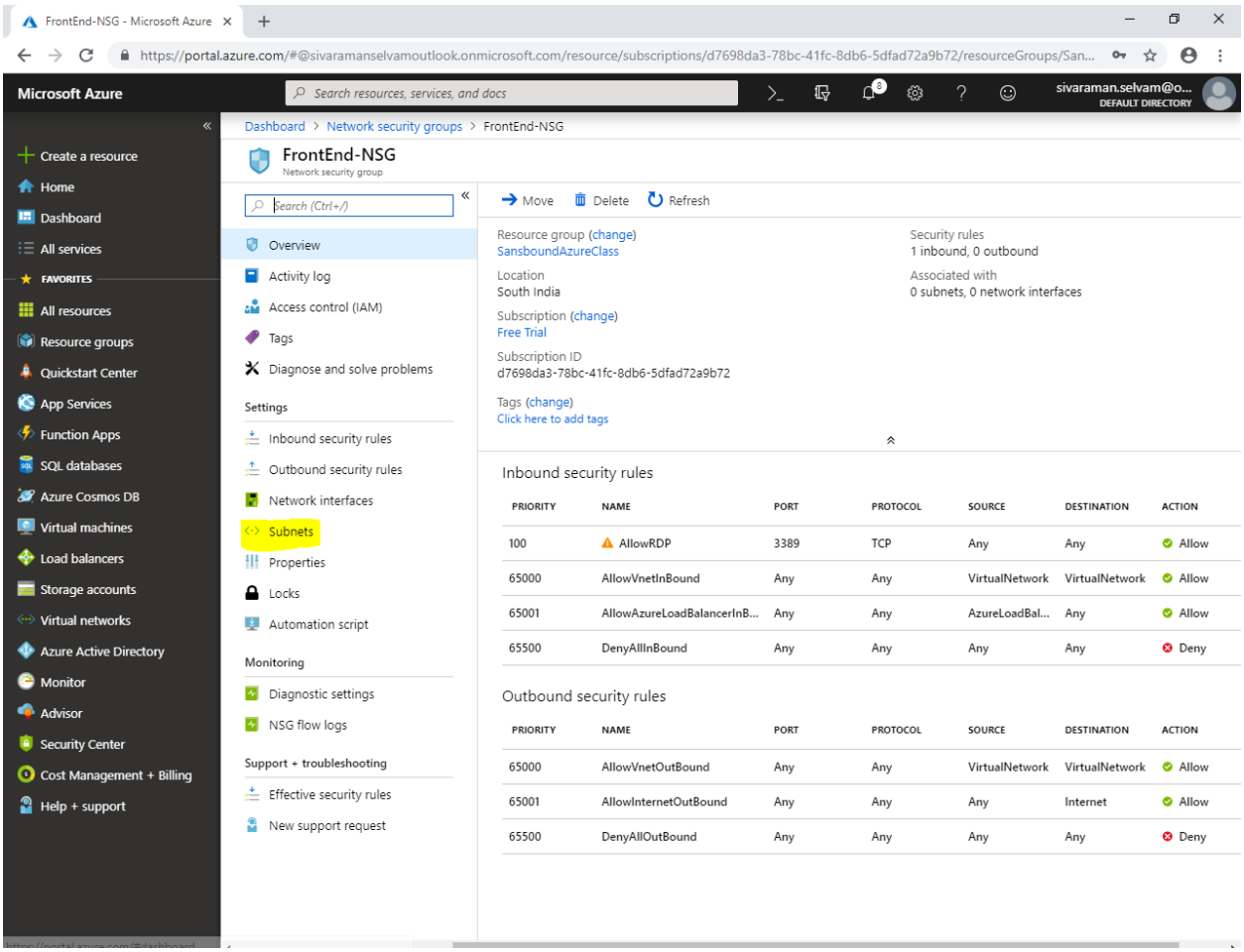


Click **"Add".**


Add inbound security rule - Micr
https://portal.azure.com/#@sivaramanselvamoutlook.onmicrosoft.com/resource/subscriptions/d7698da3-78bc-41fc-8db6-5dfad72a9b72/resourceGroups/San...
Microsoft Azure
Search resources, services, and docs
sivaraman.selvam@o...
DEFAULT DIRECTORY
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
Quickstart Center
App Services
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
Dashboard > Network security groups > FrontEnd-NSG - Inbound security r
FrontEnd-NSG - Inbound security rules
Network security group
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Automation script
Monitoring
Diagnostic settings
NSG flow logs
Support + troubleshooting
Effective security rules
New support request
Add
Default rules
PRIORITY
NAME
65000
AllowVnetInBou
65001
AllowAzureLoad
65500
DenyAllInBound
Add inbound security rule
FrontEnd-NSG
Basic
* Source
Any
* Source port ranges
*
* Destination
Any
* Destination port ranges
3389
* Protocol
Any
TCP
UDP
* Action
Allow
Deny
* Priority
100
* Name
AllowRDP
Description
Allow RDP port for Front Subnet from Public
Add

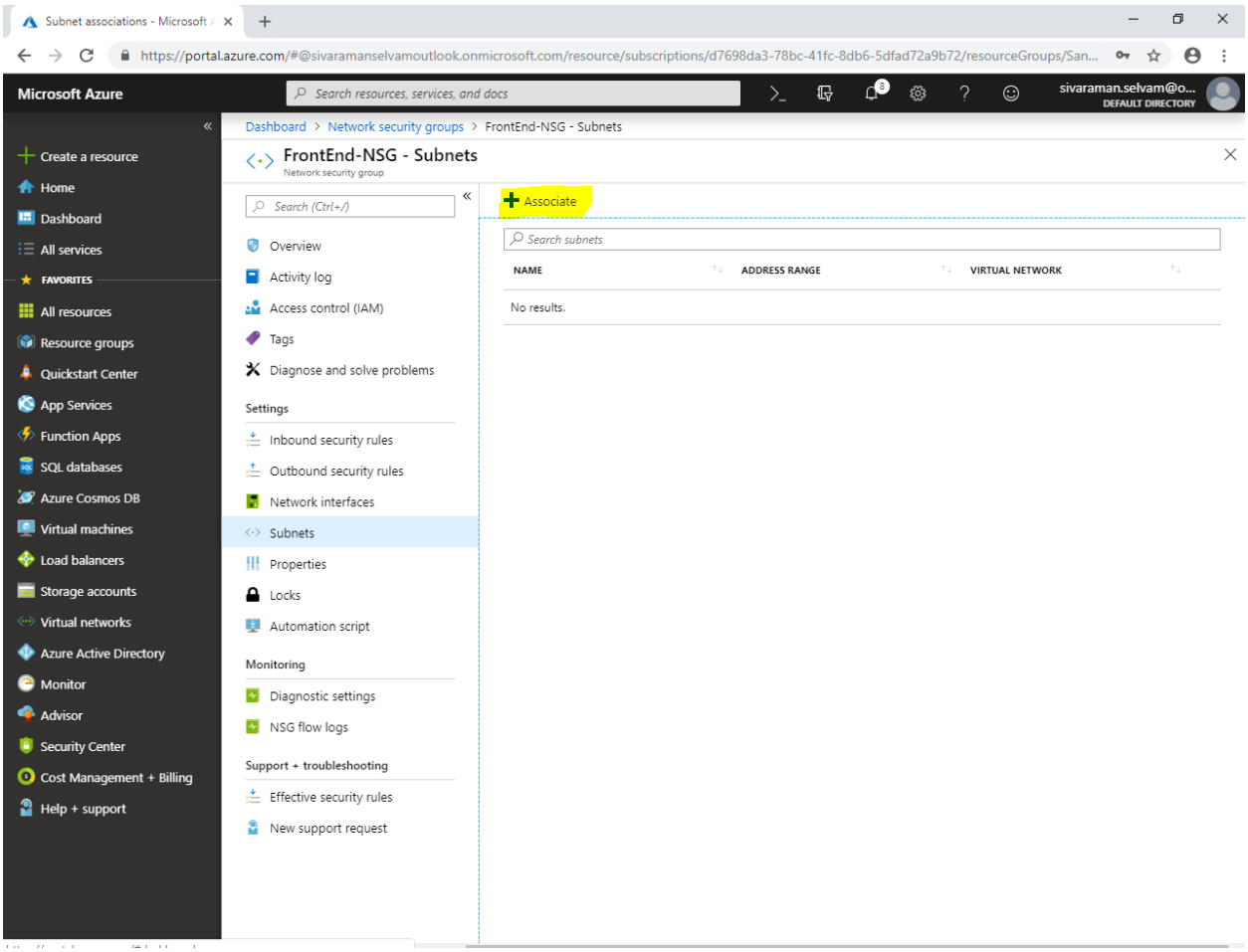
In **"FrontEnd-NSG"**,

Click **"Subnets"**.



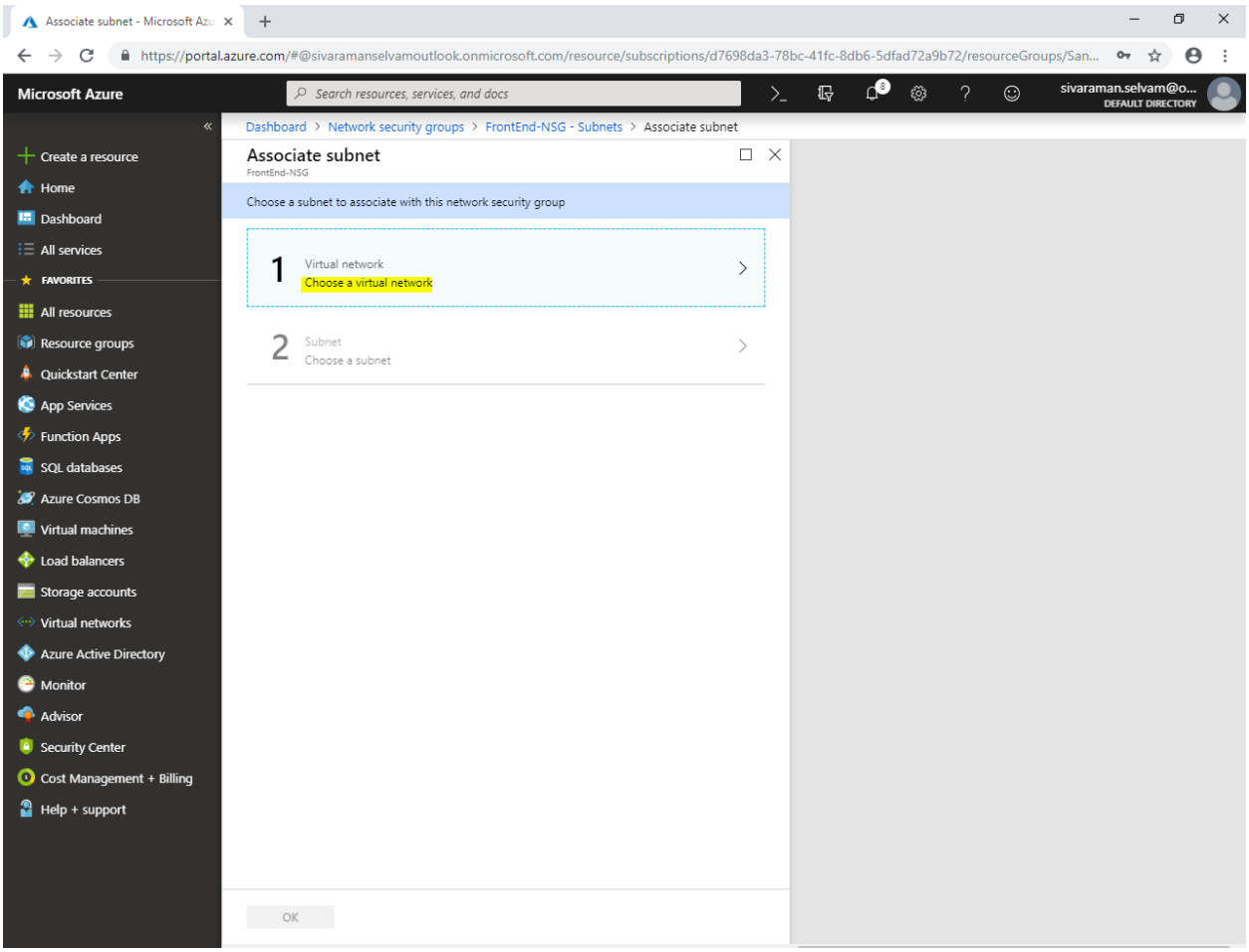
In “FrontEnd-NSG – Subnets”.

Click **“Associate”**.

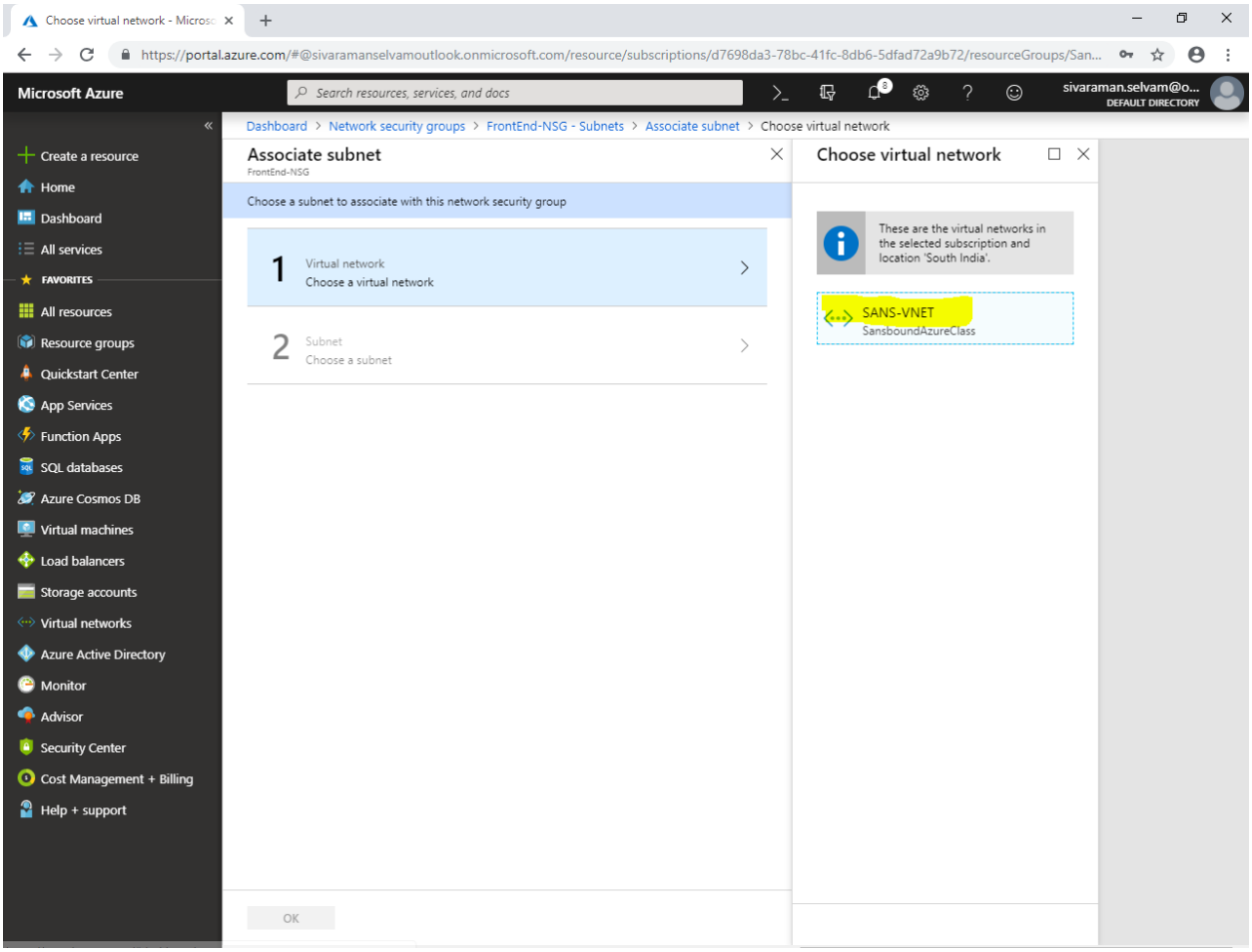


While **“Associate subnet”**

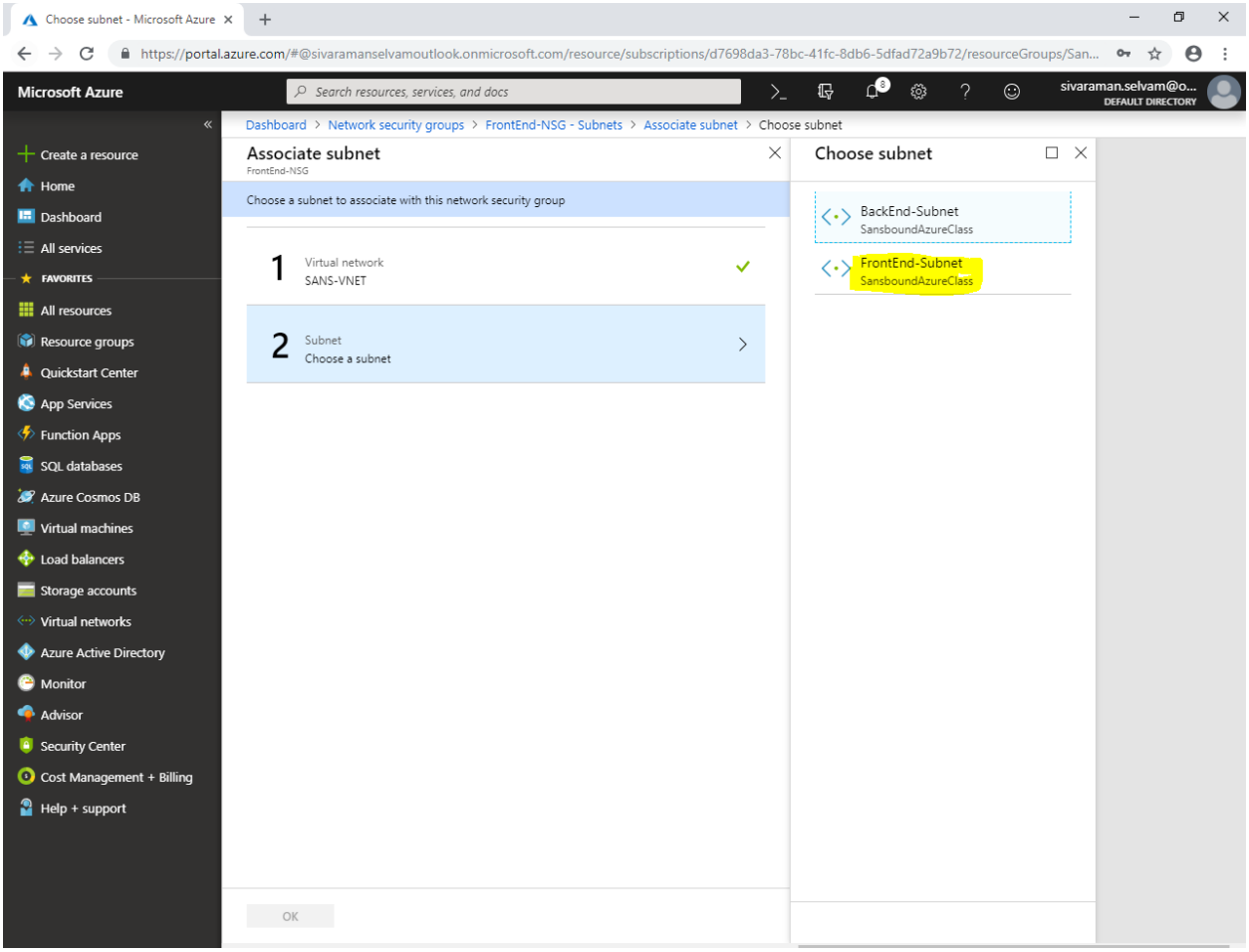
Click on **“Choose a virtual network”**.



Click on **"SANS-VNET"** to select the Virtual network for the Network Security Group.



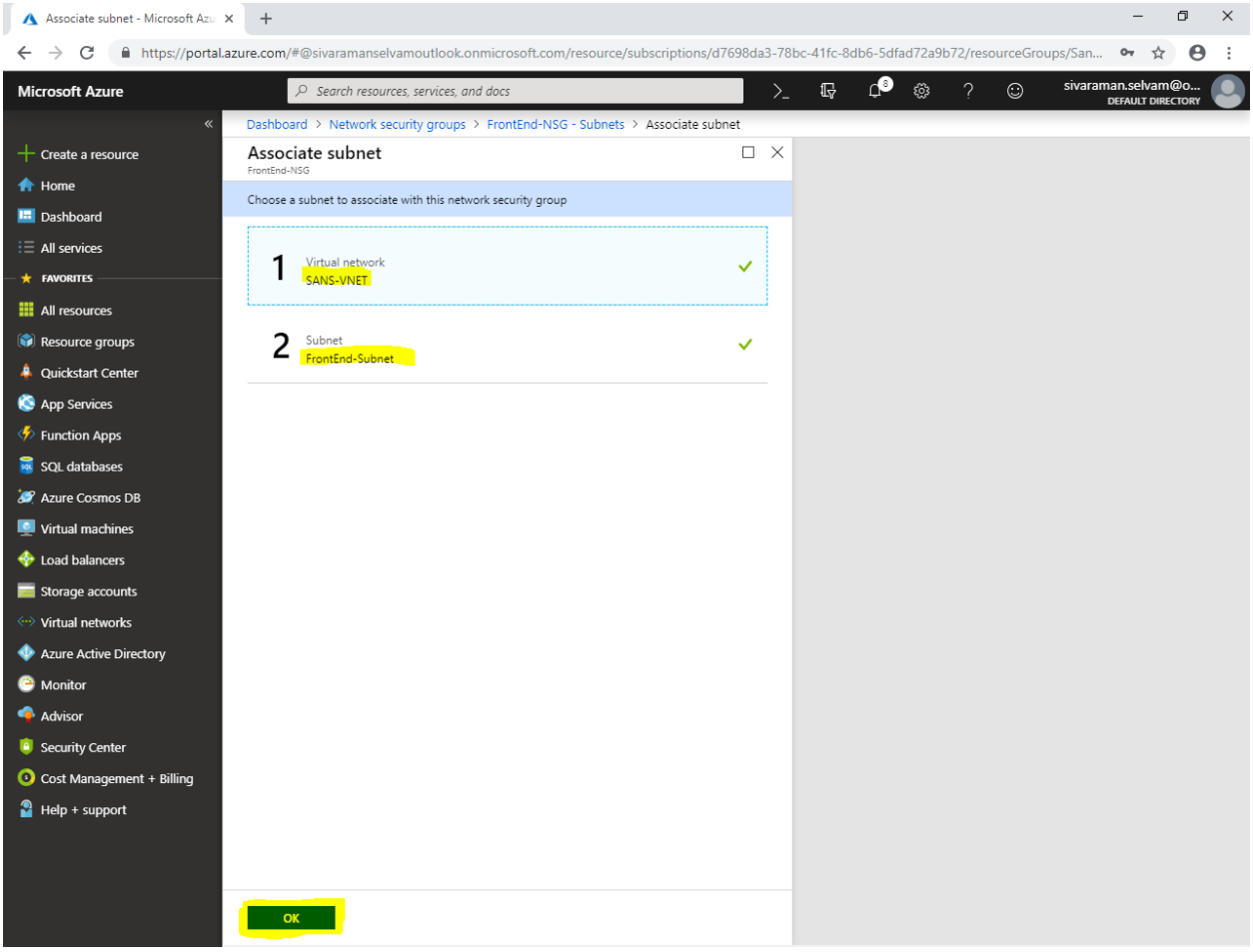
You have required to click on **"FrontEnd-Subnet"**, because we have required to access the Virtual machines through public from this subnet **10.0.1.0/24**.



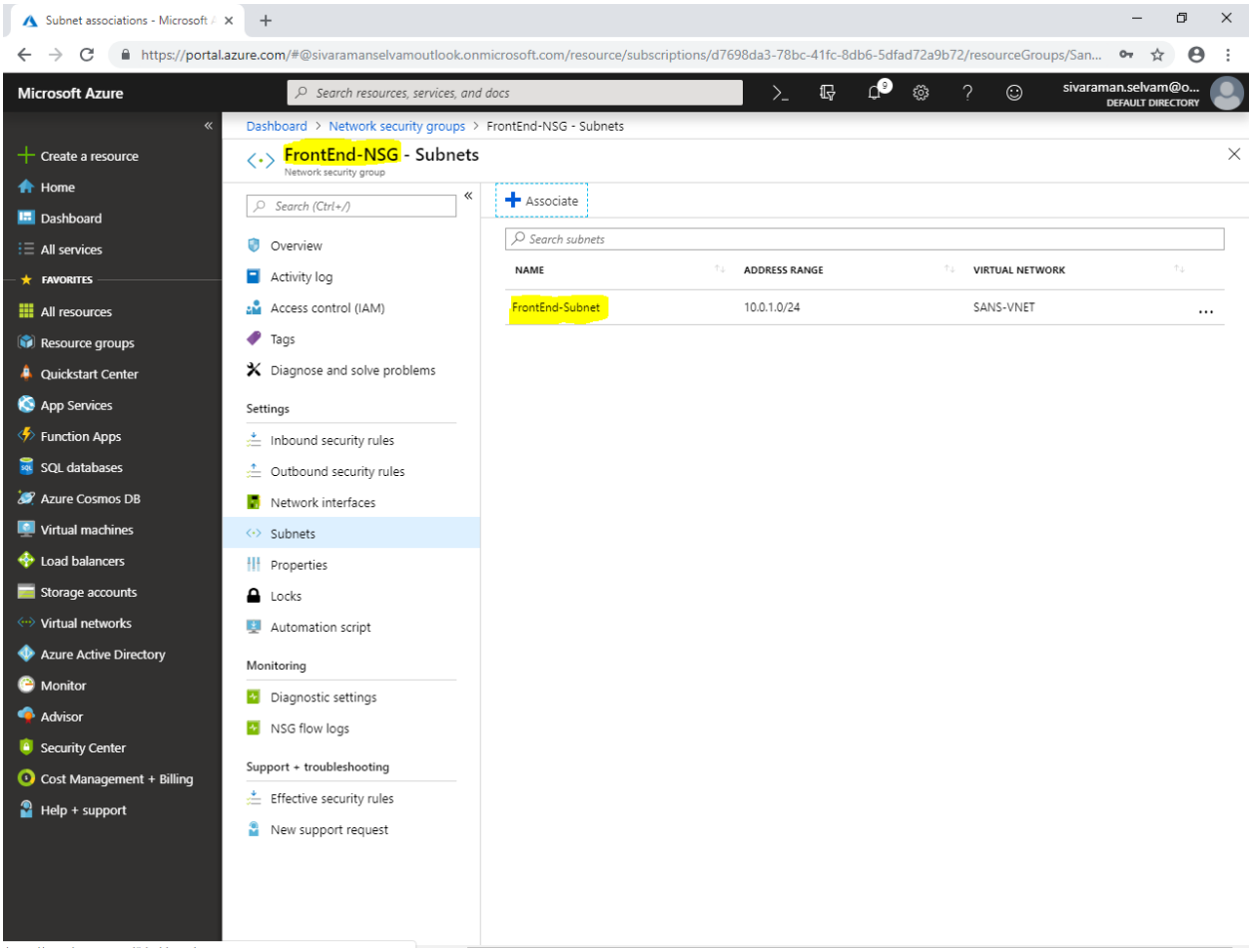
Ensure that **"Virtual network"** as **"SANS-VNET"**.

Ensure that **"Subnet"** as **"FrontEnd-Subnet"**.

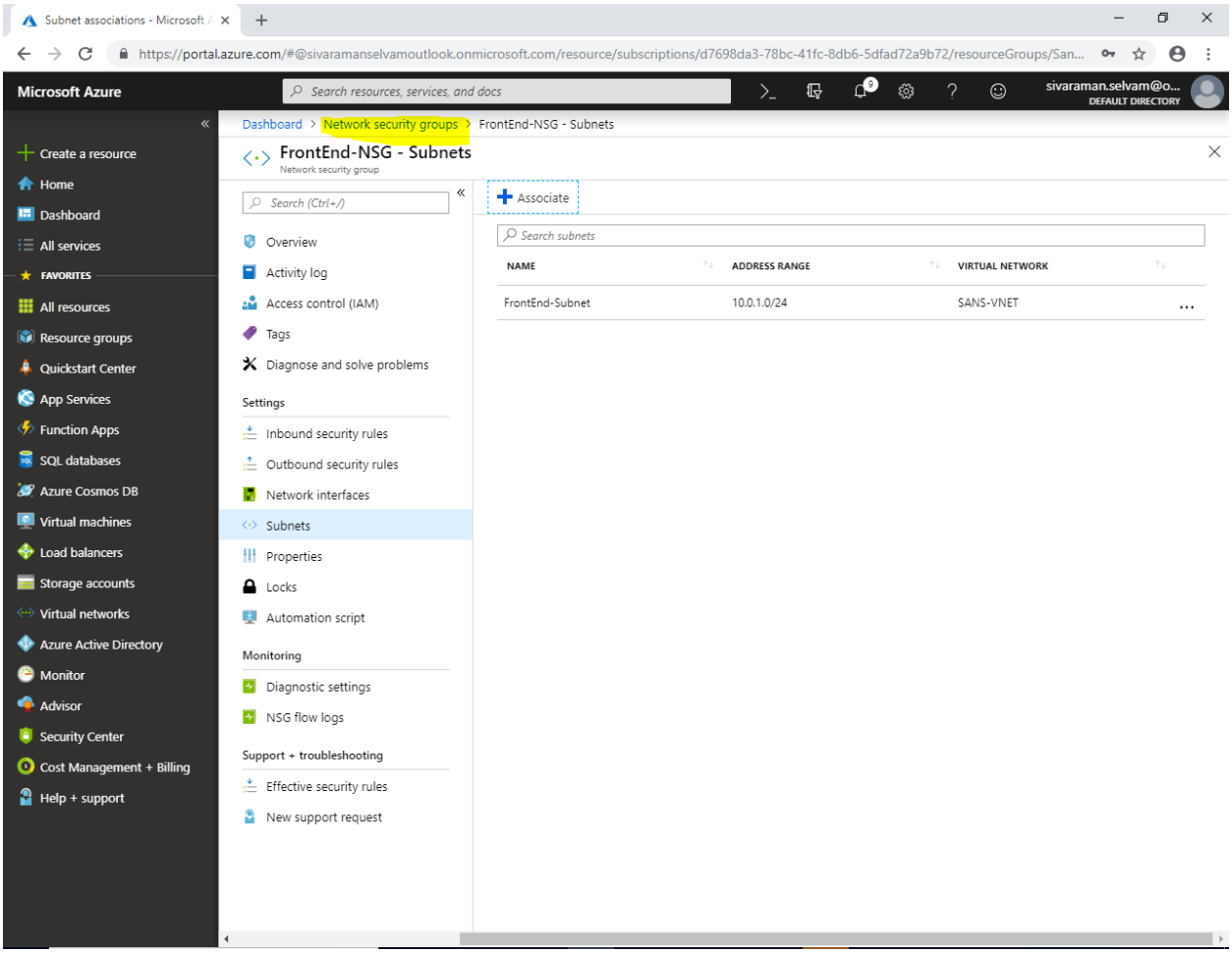
Click **"Ok"**.



In **"FrontEnd-NSG"** we have associated FrontEnd-Subnet.

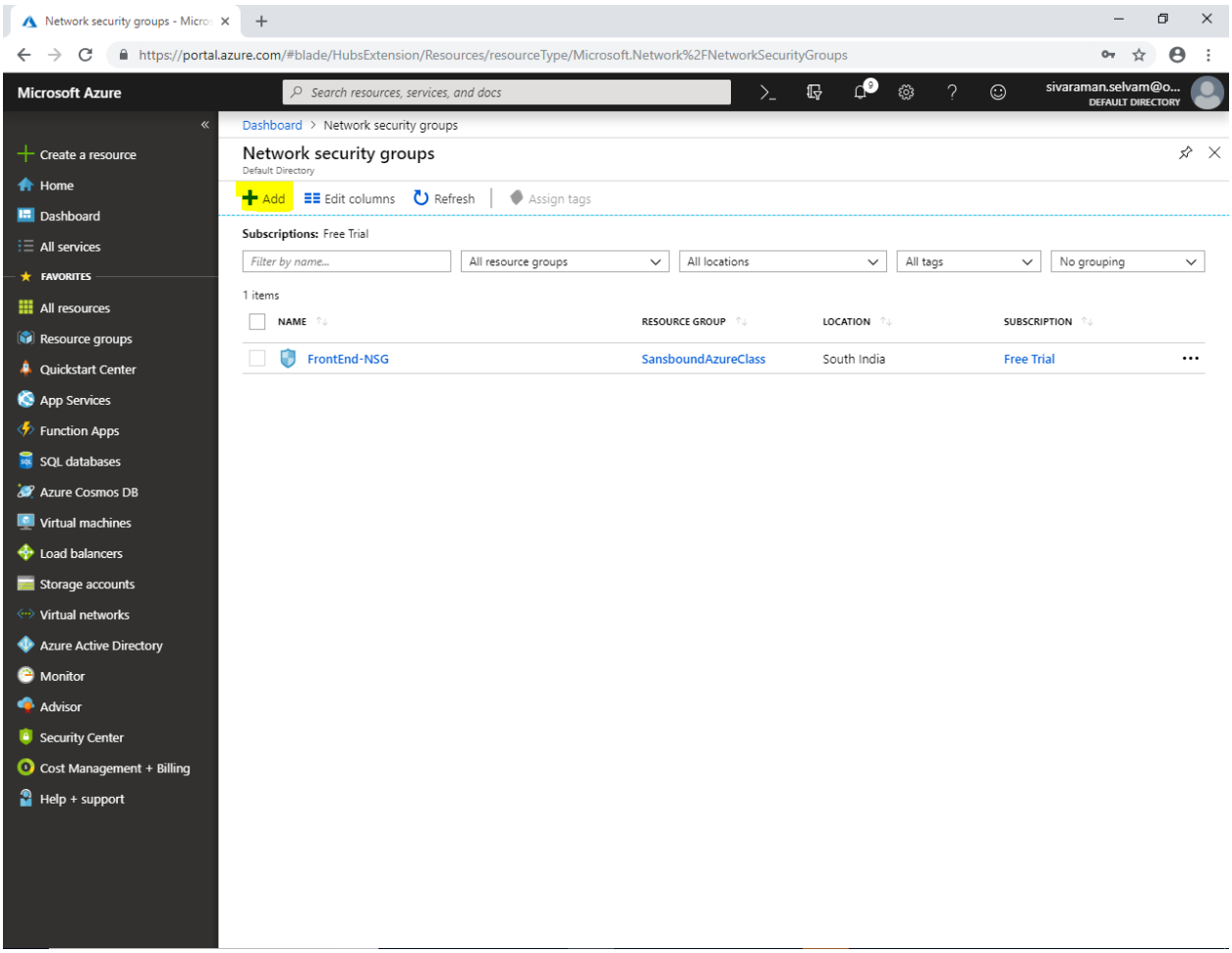


Click on **“Network security groups”**.



In **“Network Security groups”**.

Click “Add”.



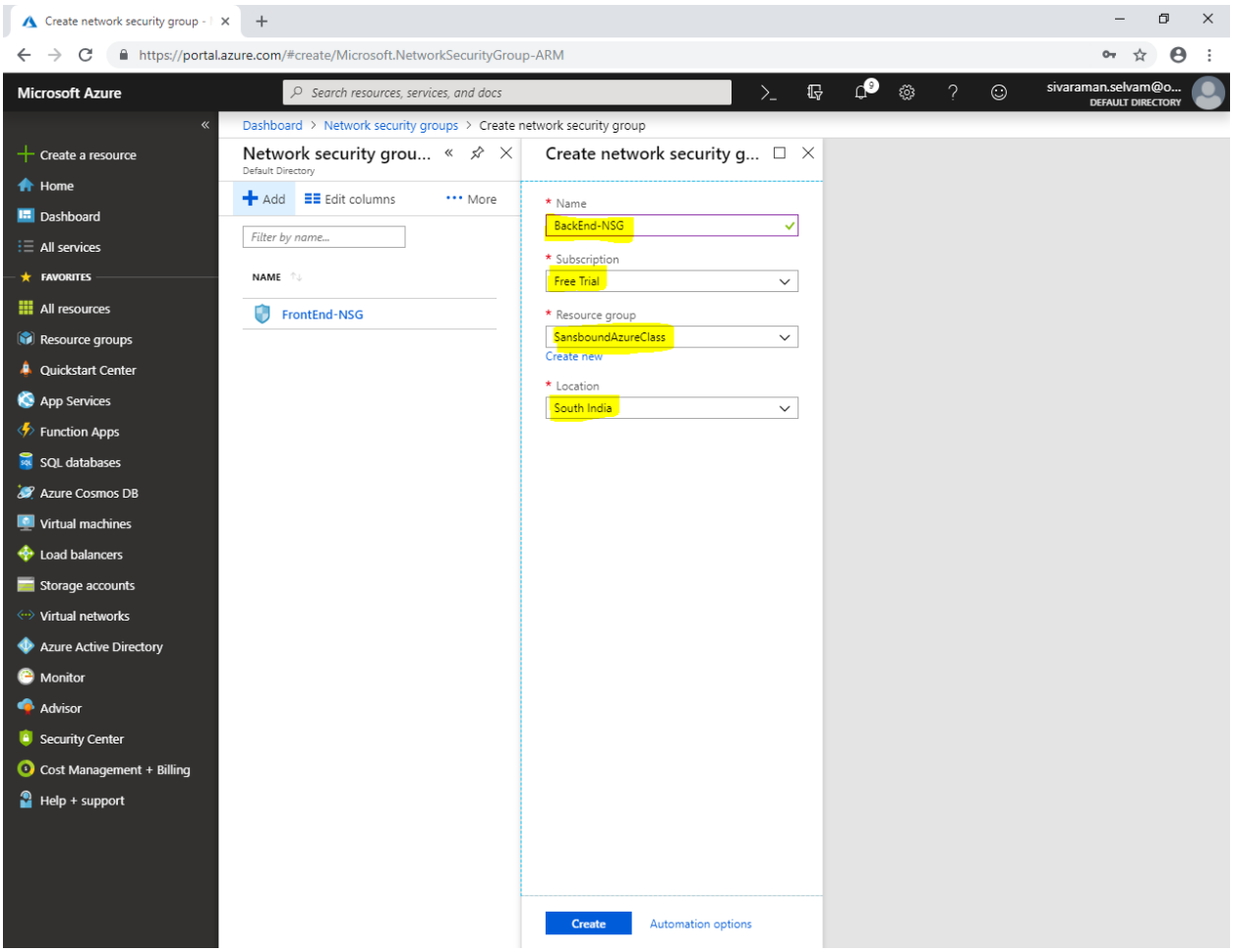
While creating **“Network security group”**

It requires **“Name”** type as **“BackEnd-NSG”**.

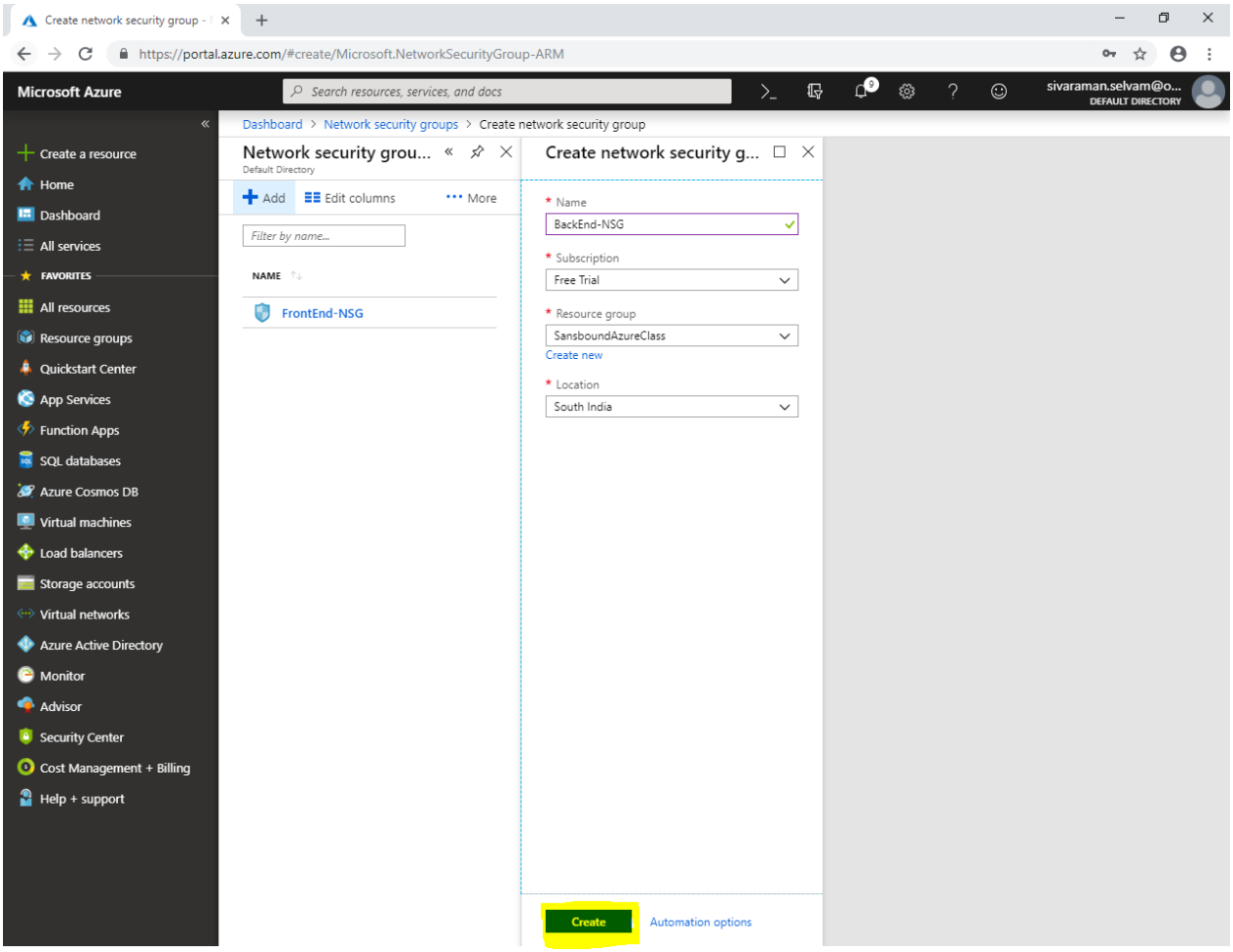
Select **“Subscription”** as **“Free Trial”**.

Select **“Resource group”** as **“SansboundAzureClass”**.

Select **“Region”** as **“South India”**.

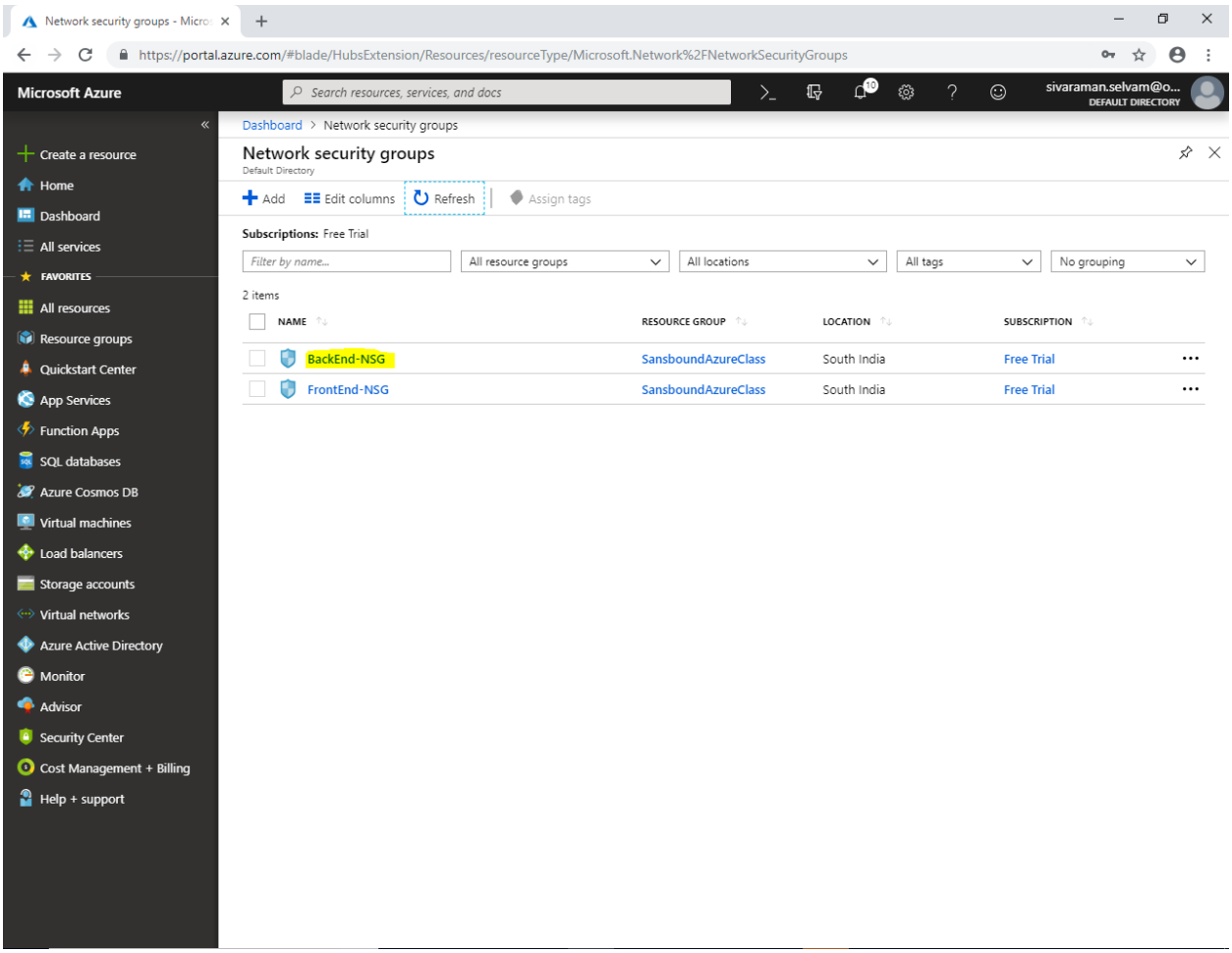


Click **”Create”.**



In **“Network security groups”** click **“Refresh”** to view newly created network security groups.

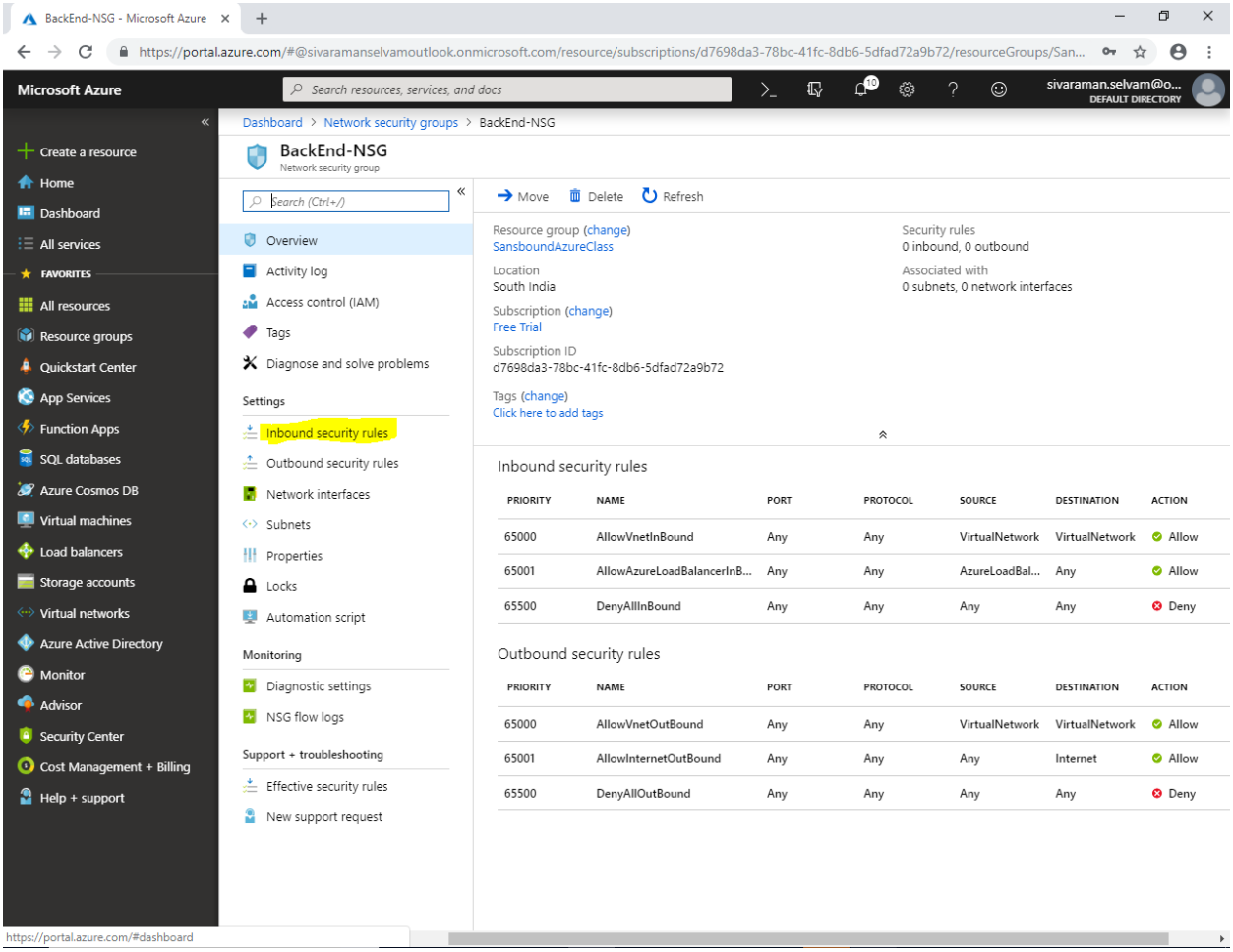
Click on **“BackEnd-NSG”**.



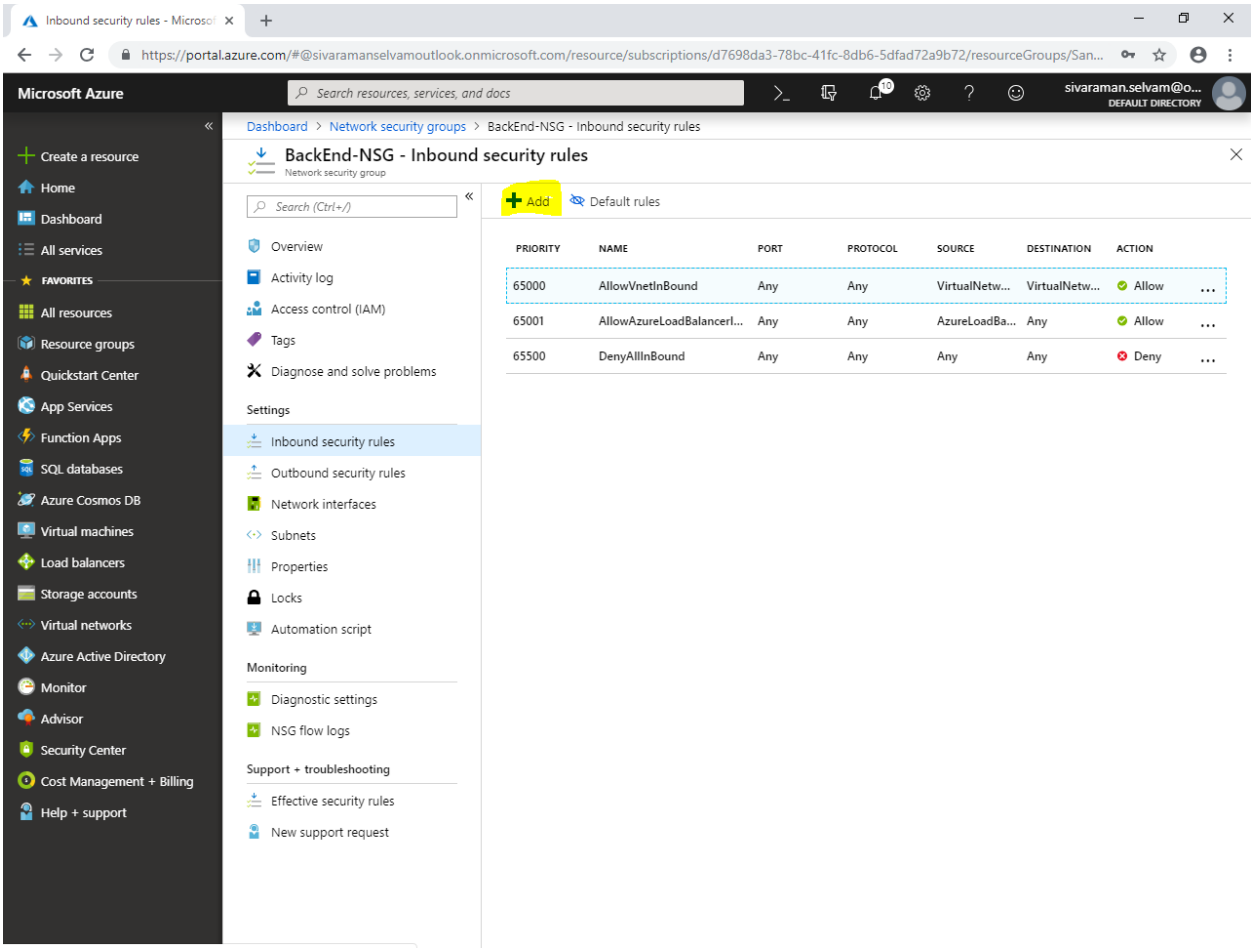
In **“Network Security groups”.**

In **“BackEnd-NSG”**.

Click **“Inbound security rules”**.



Click **"Add".**


Inbound security rules - Microsoft
https://portal.azure.com/#@sivaramanselvamoutlook.onmicrosoft.com/resource/subscriptions/d7698da3-78bc-41fc-8db6-5dfad72a9b72/resourceGroups/San...
Microsoft Azure
Search resources, services, and docs
sivaraman.selvam@o...
DEFAULT DIRECTORY
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
Quickstart Center
App Services
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
Dashboard > Network security groups > BackEnd-NSG - Inbound security rules
BackEnd-NSG - Inbound security rules
Network security group
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Automation script
Monitoring
Diagnostic settings
NSG flow logs
Support + troubleshooting
Effective security rules
New support request
Add
Default rules
PRIORITY
NAME
PORT
PROTOCOL
SOURCE
DESTINATION
ACTION
65000
AllowVnetInBound
Any
Any
VirtualNetw...
VirtualNetw...
Allow
65001
AllowAzureLoadBalancerI...
Any
Any
AzureLoadBa...
Any
Allow
65500
DenyAllInBound
Any
Any
Any
Any
Deny

While add **“Inbound security rule”**.

Select the **“Source”** as **“IP address”** and type the Subnet / IP address (**10.0.1.0/24**) as Source IP address where you are going to connect SSH.

Select **“Destination”** as “**IP address”** and type the Subnet / IP address (**10.0.2.0/24**) as Destination IP address which you have required to access.

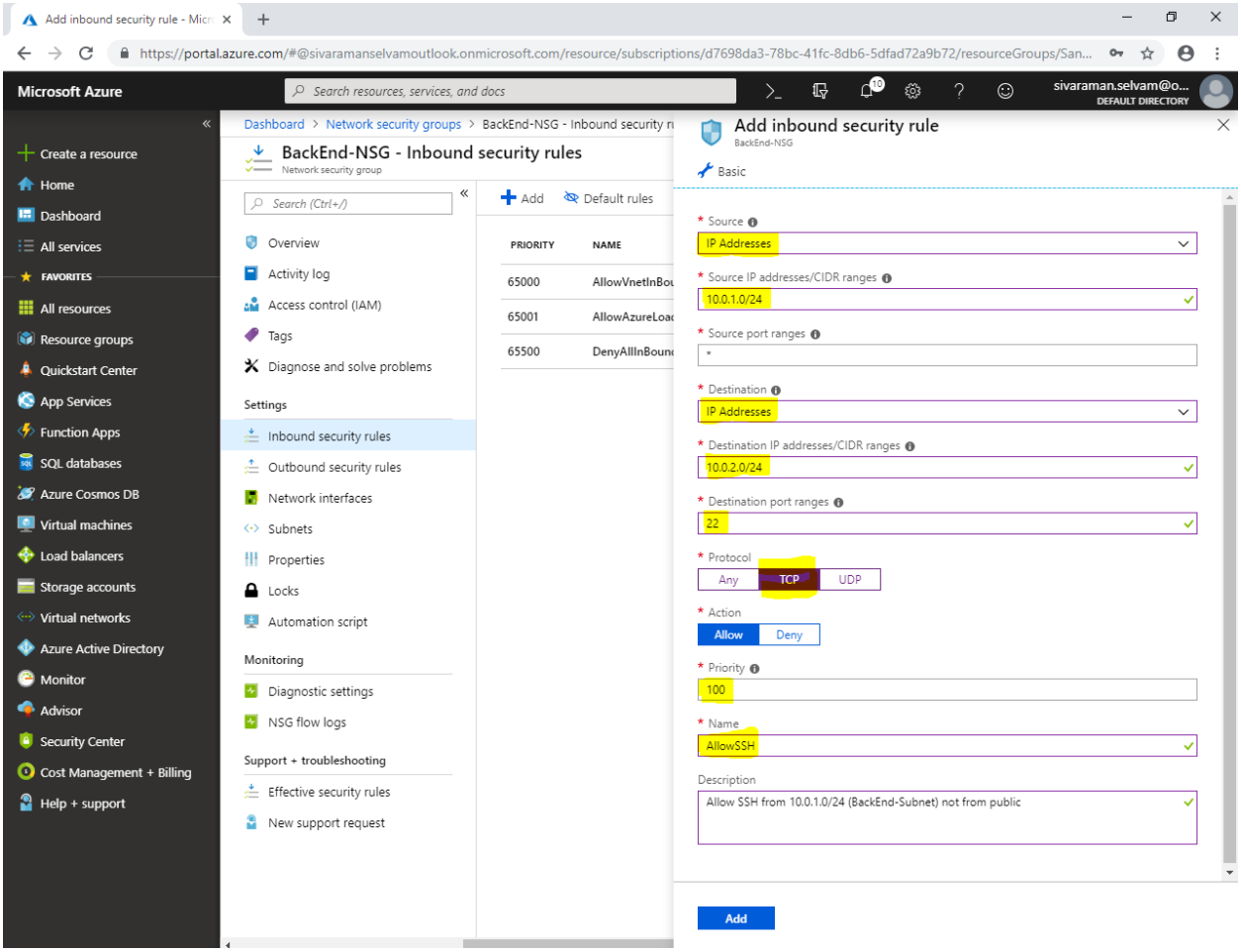
Type **“Destination port ranges”** as **“22”**.

Protocol **“TCP”**.

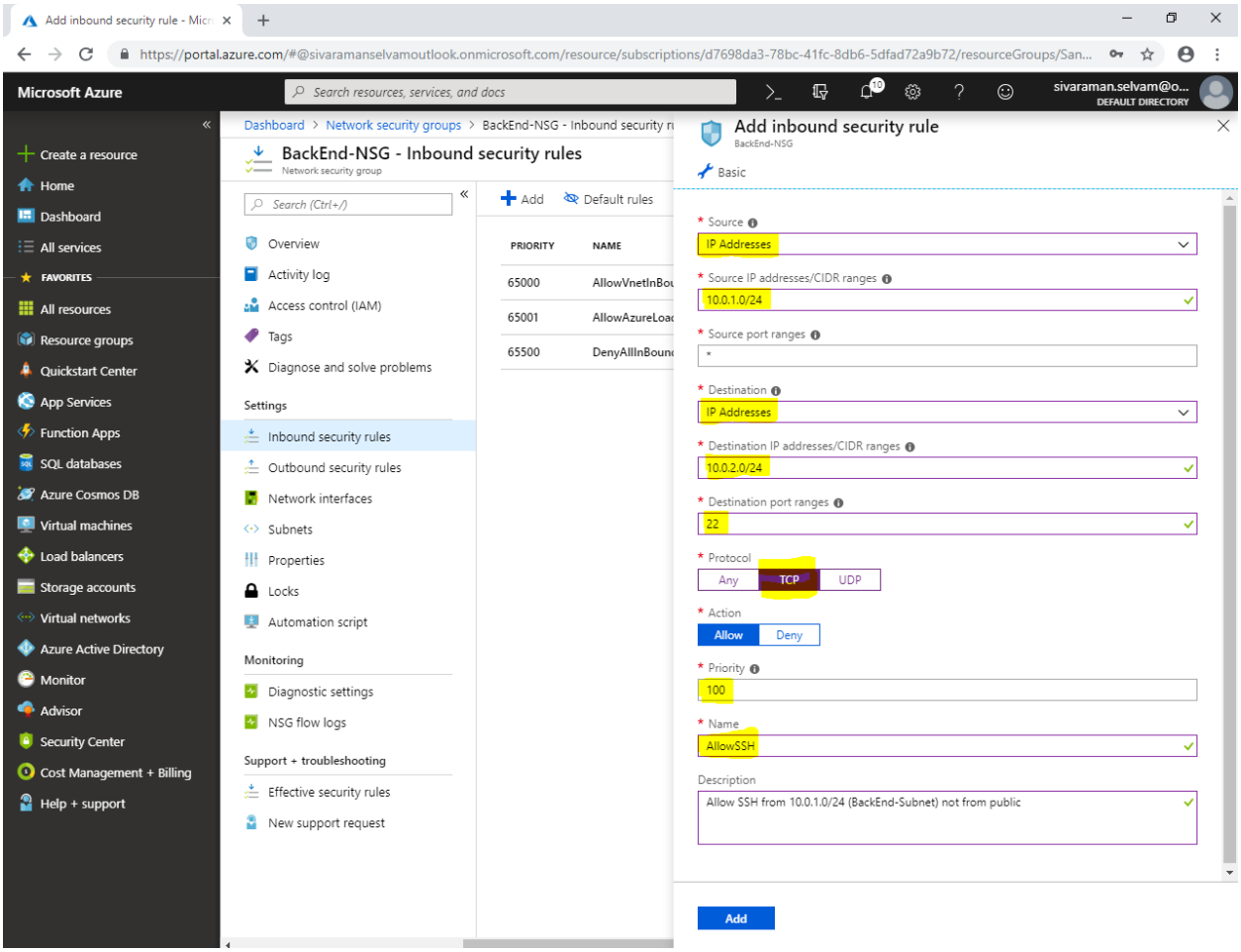
Click **“Allow”.**

In **“Priority”**, type as **100** (lowest priority rule apply first).

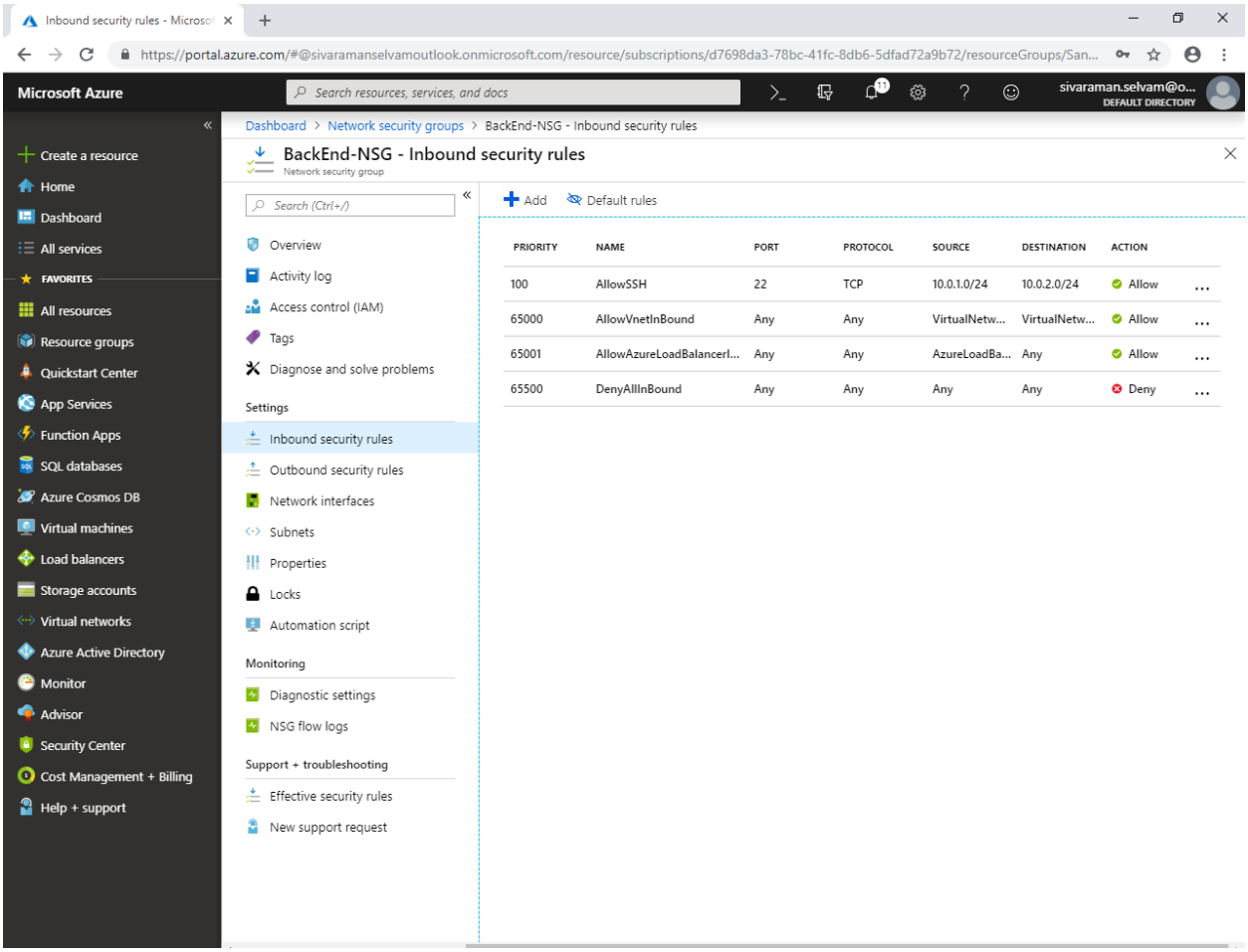
Name as **“AllowSSH”**.



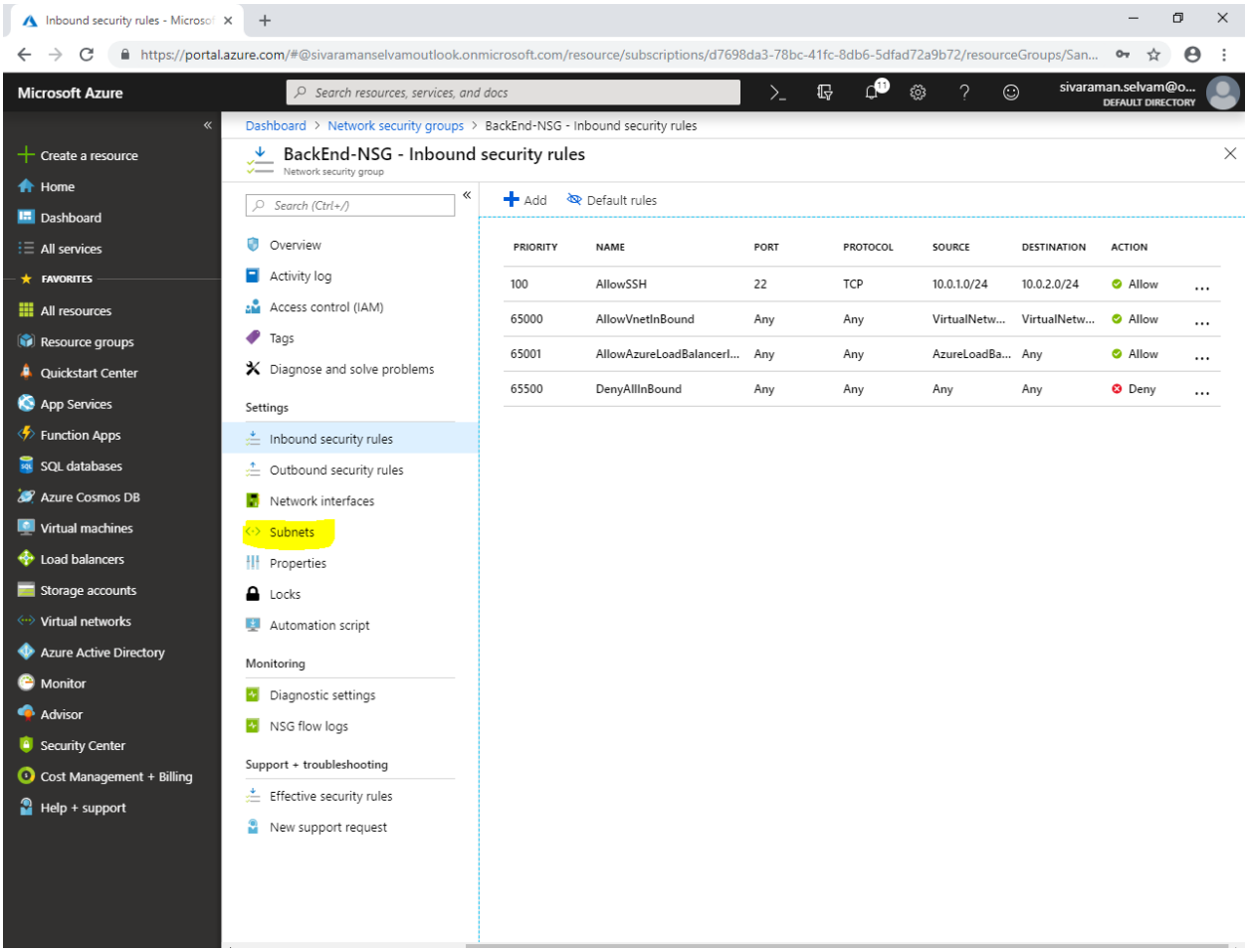
Click **"Add"** to create the Network Security Group for BackEnd-Subnet.



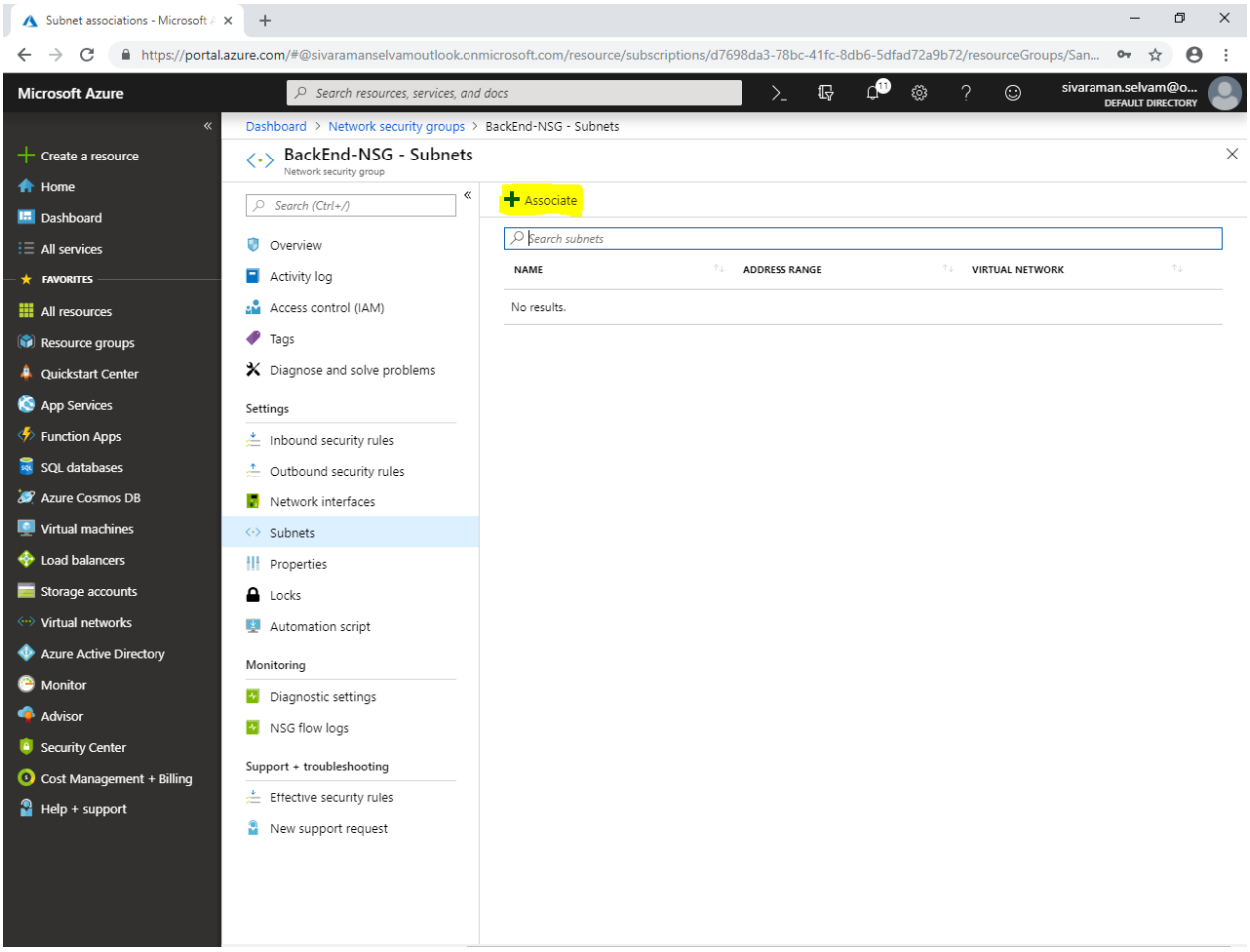
You are able to see that inbound rule with priority **"100"** has been created for **"BackEnd-Subnet".**



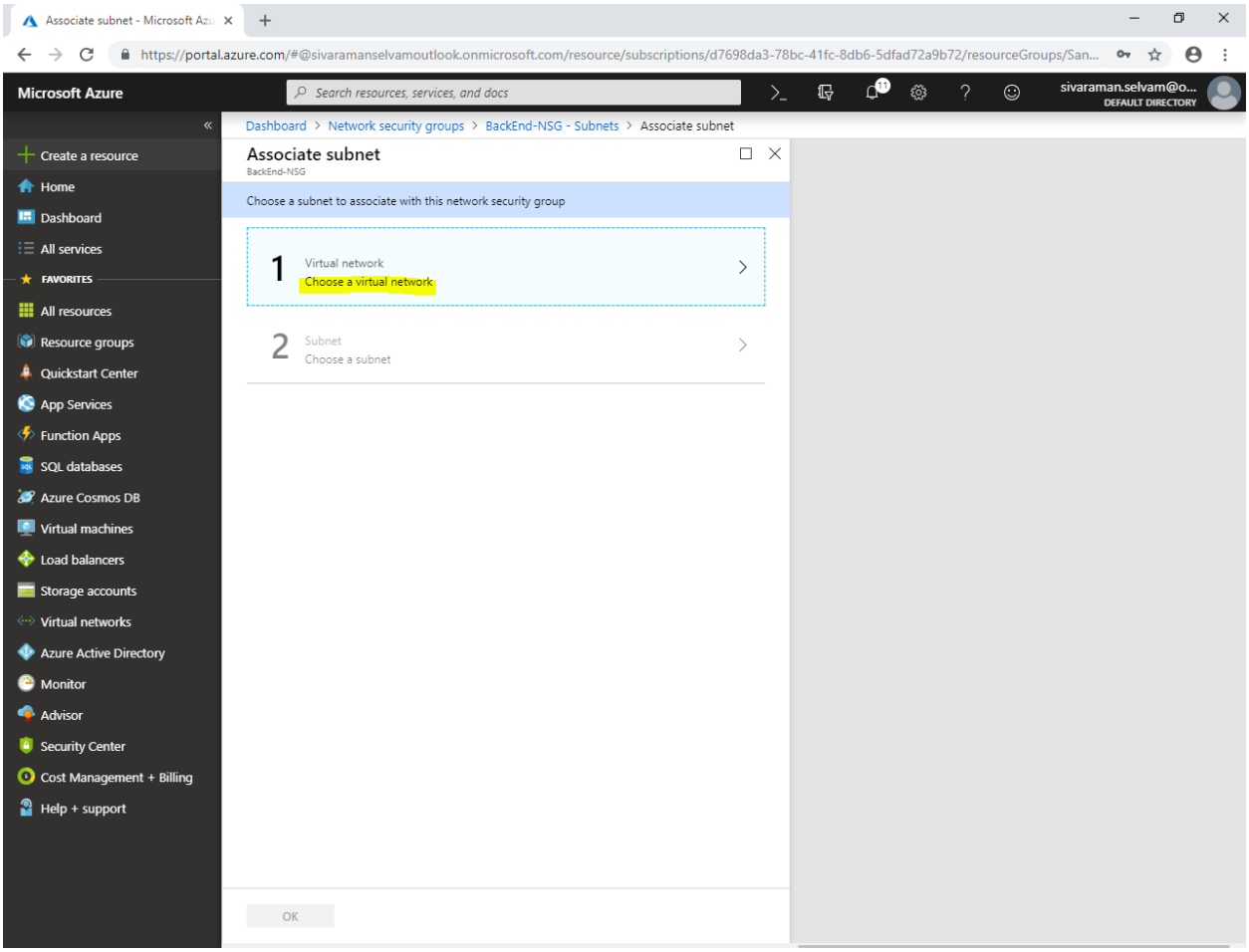
Click **“Subnets”.**



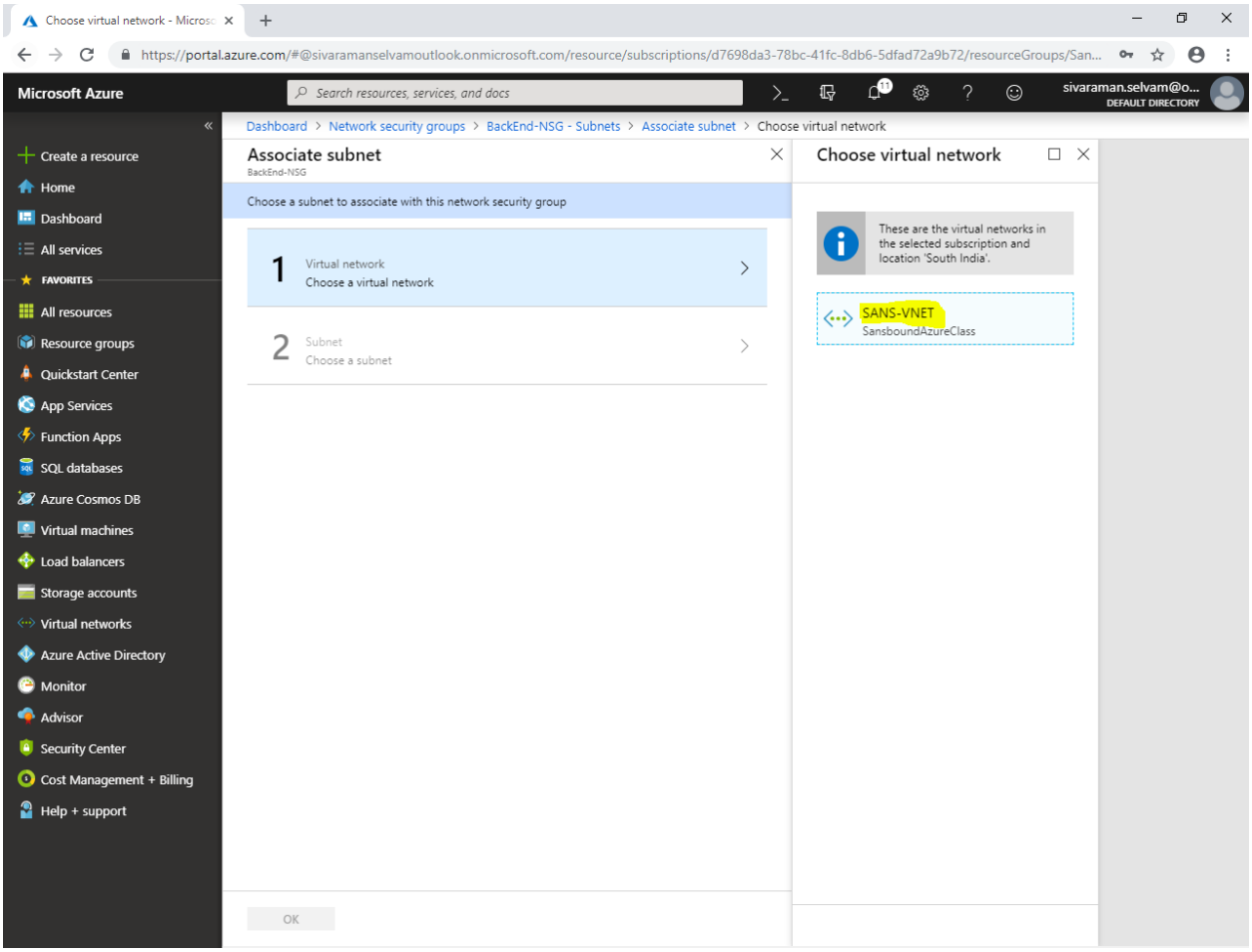
Click **"Associate"** to associate the subnet to **"Network Security Group"**.



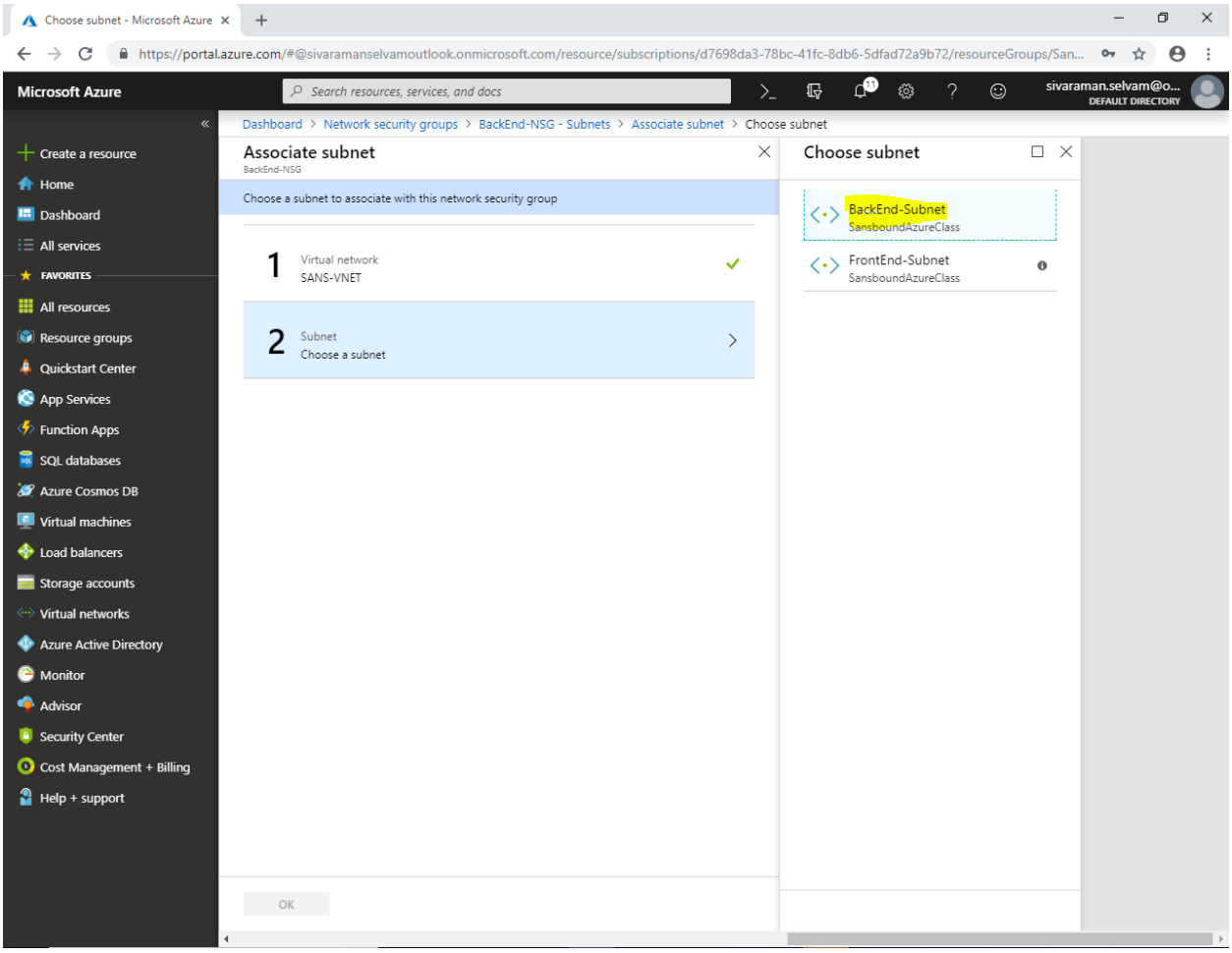
While **"Associate subnet"** click on **"Choose a virtual network"** to select **"Virtual Network"**.



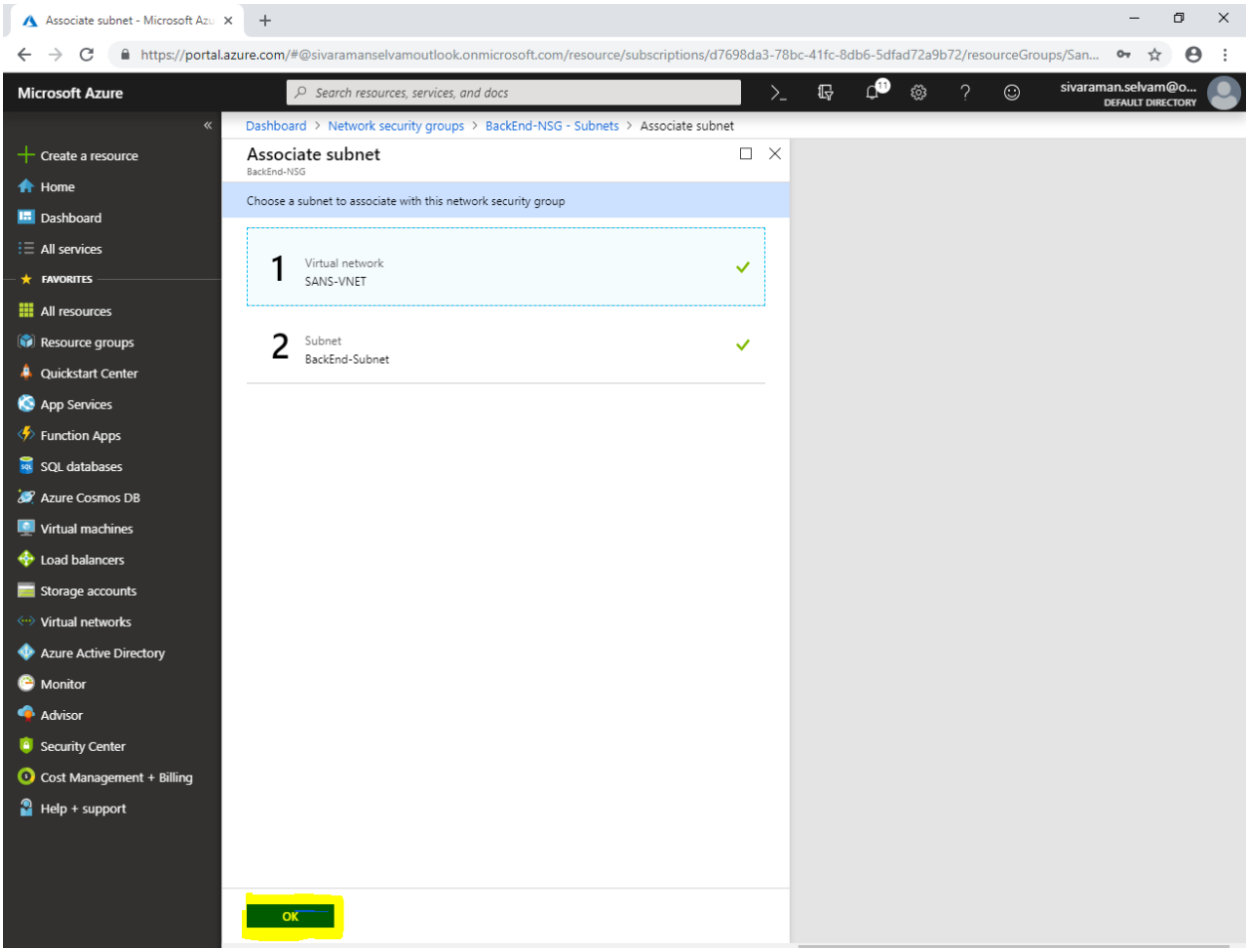
Click on **"SANS-VNET"**.



We have required to click on **“BackEnd-Subnet”**.

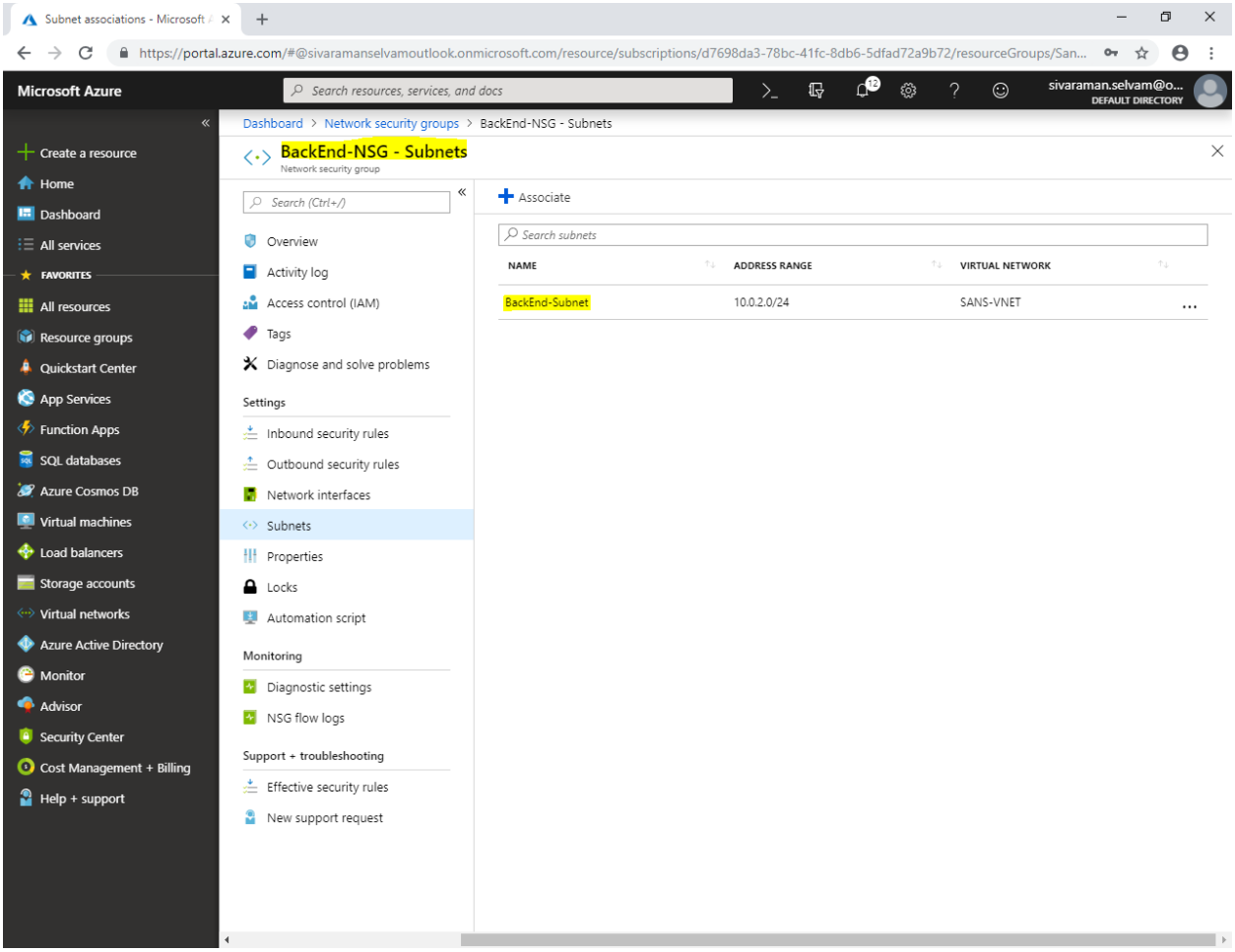


Click **“Ok”**.

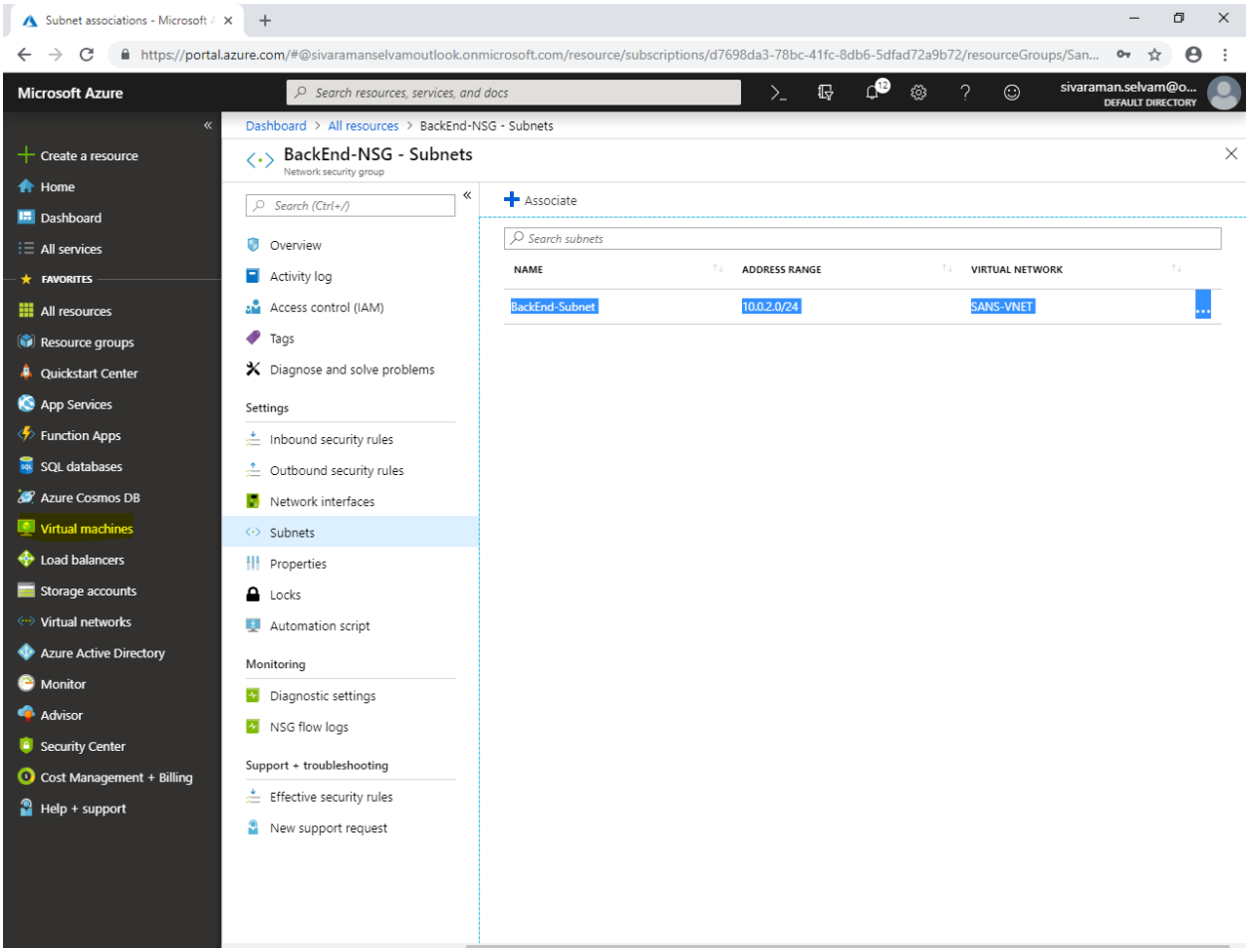

Associate subnet - Microsoft Azu
https://portal.azure.com/#@sivaramanselvamoutlook.onmicrosoft.com/resource/subscriptions/d7698da3-78bc-41fc-8db6-5dfad72a9b72/resourceGroups/San...
Microsoft Azure
Search resources, services, and docs
sivaraman.selvam@o...
DEFAULT DIRECTORY
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
Quickstart Center
App Services
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
Dashboard > Network security groups > BackEnd-NSG - Subnets > Associate subnet
Associate subnet
BackEnd-NSG
Choose a subnet to associate with this network security group
1
Virtual network
SANS-VNET
2
Subnet
BackEnd-Subnet
OK

In **"BackEnd-NSG – Subnets"**.

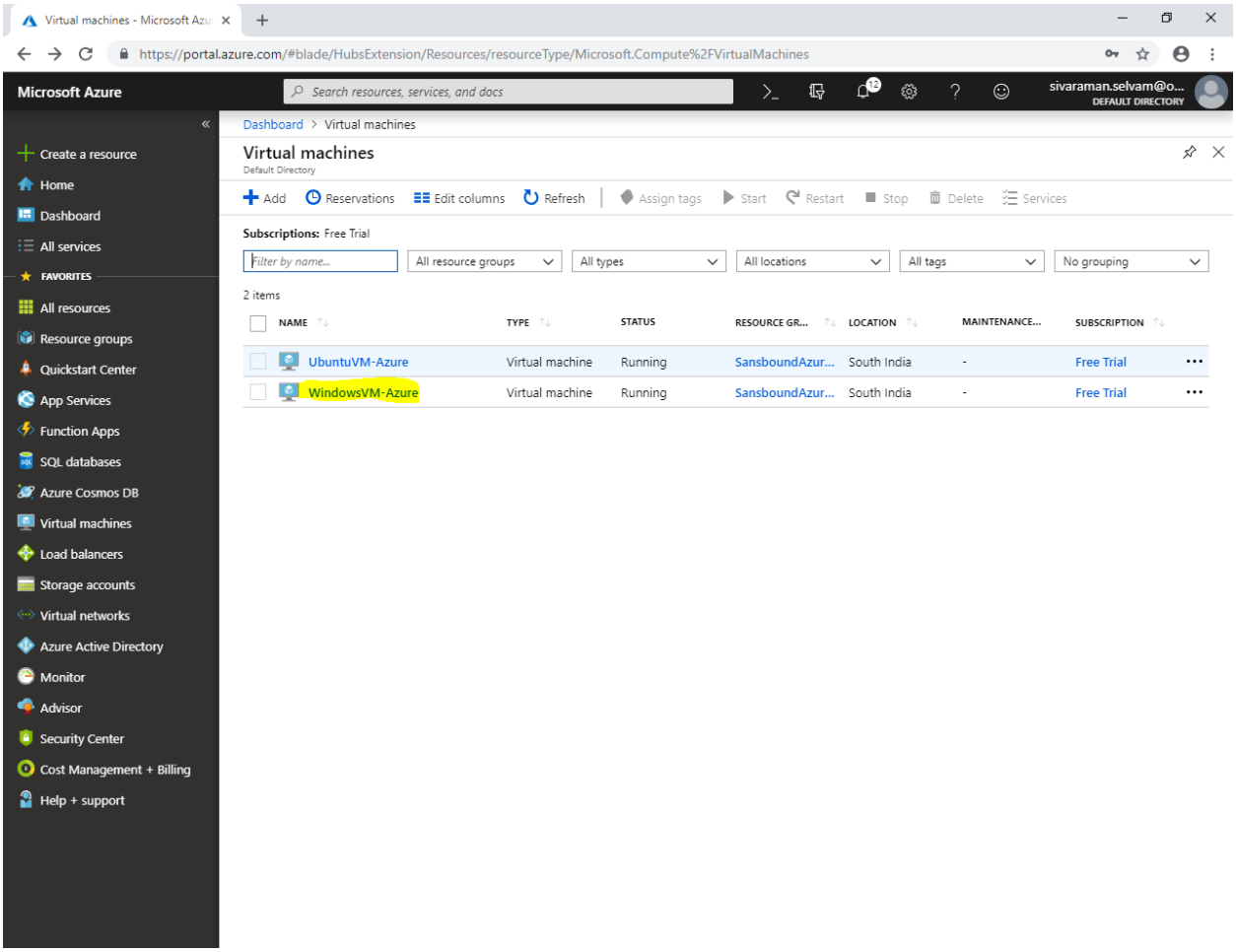
You are able to see that **"BackEnd-Subnet"** has been associated with **"BackEnd-NSG"** network security group.



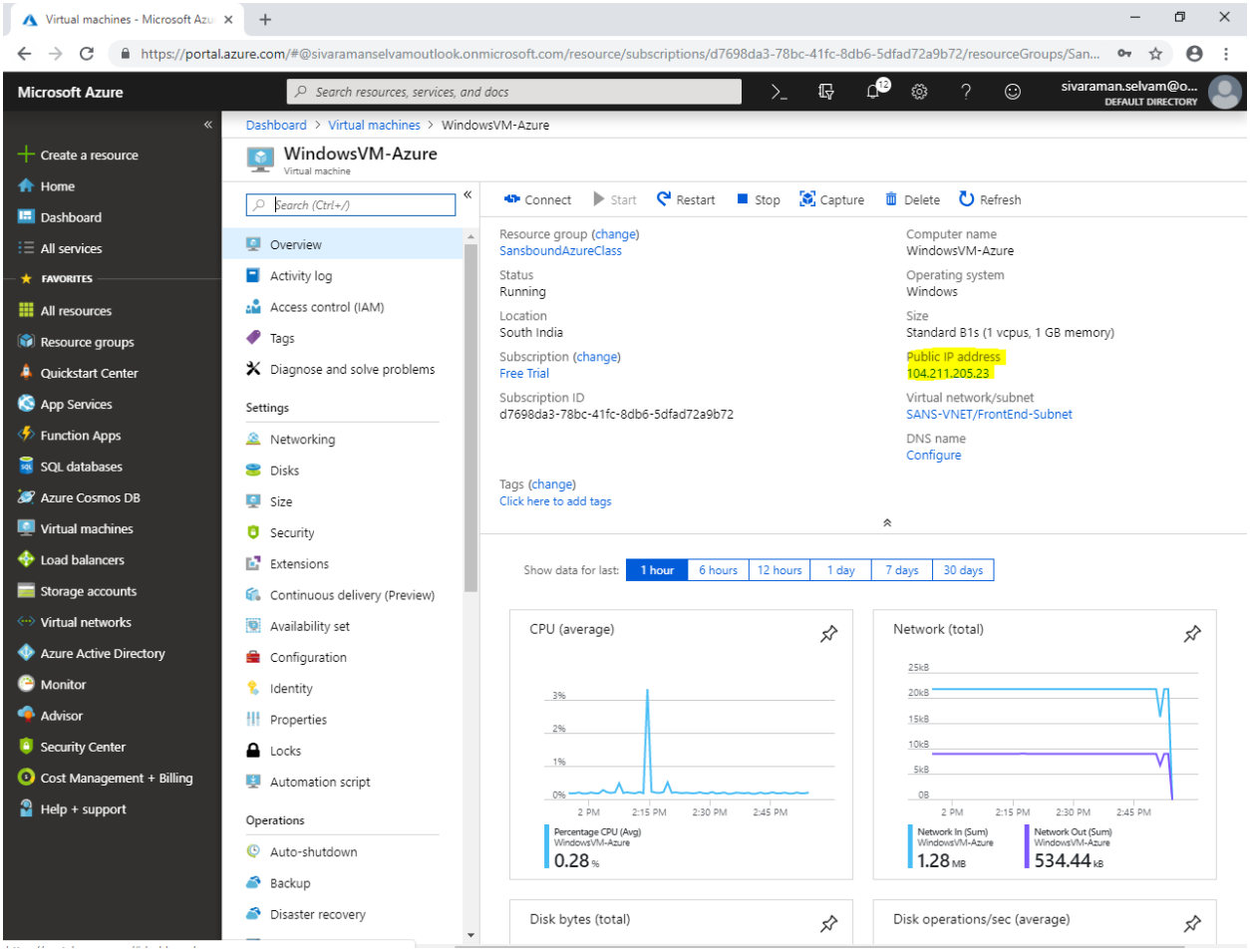
Click on **“Virtual machines”** in left side panel.



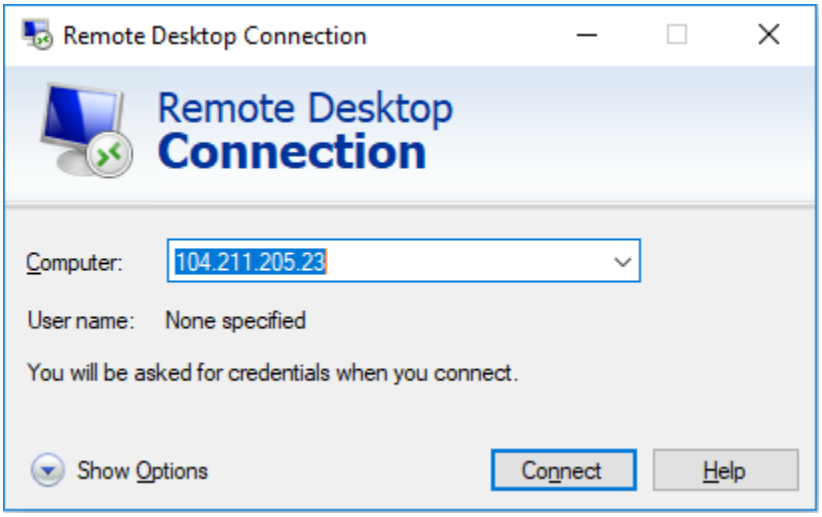
Click on **"WindowsVM-Azure"**.



Kindly note the public IP address of Windows Virtual machine which belongs to Front End network (Publicly accessible).



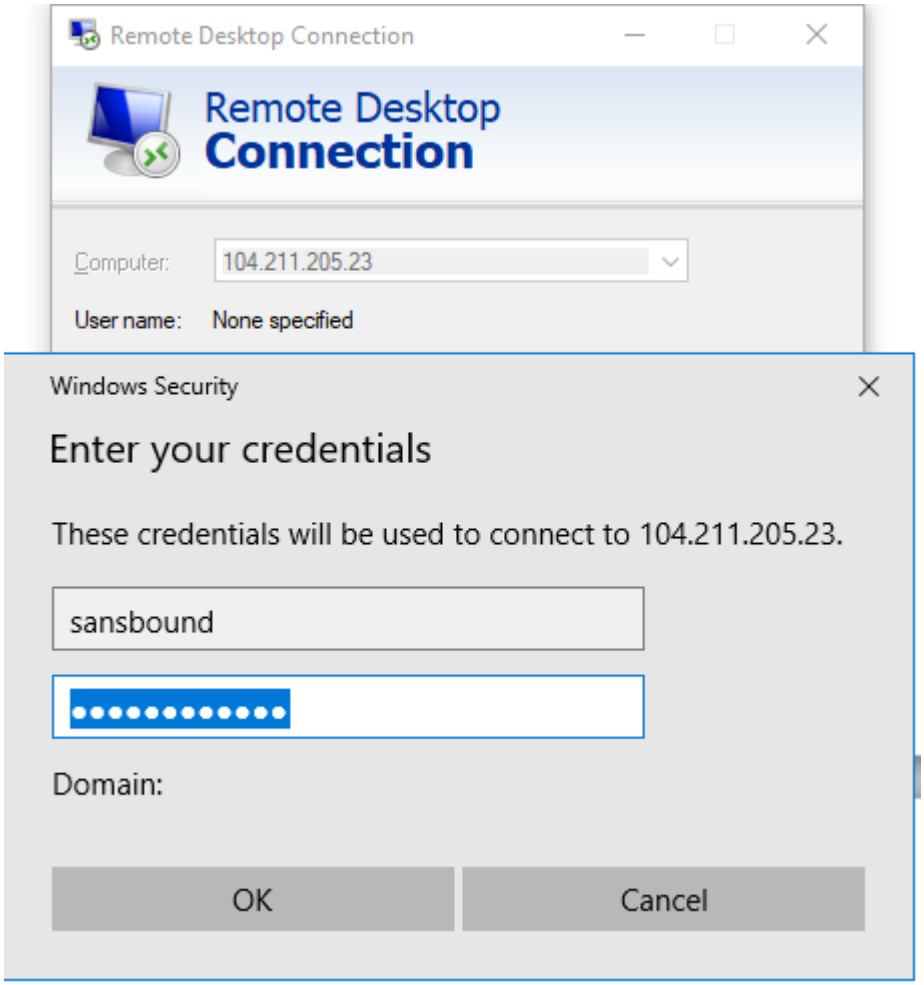
Type **“mstsc”** in your local machine, and type the Public IP address of the Windows Server 2008 R2.



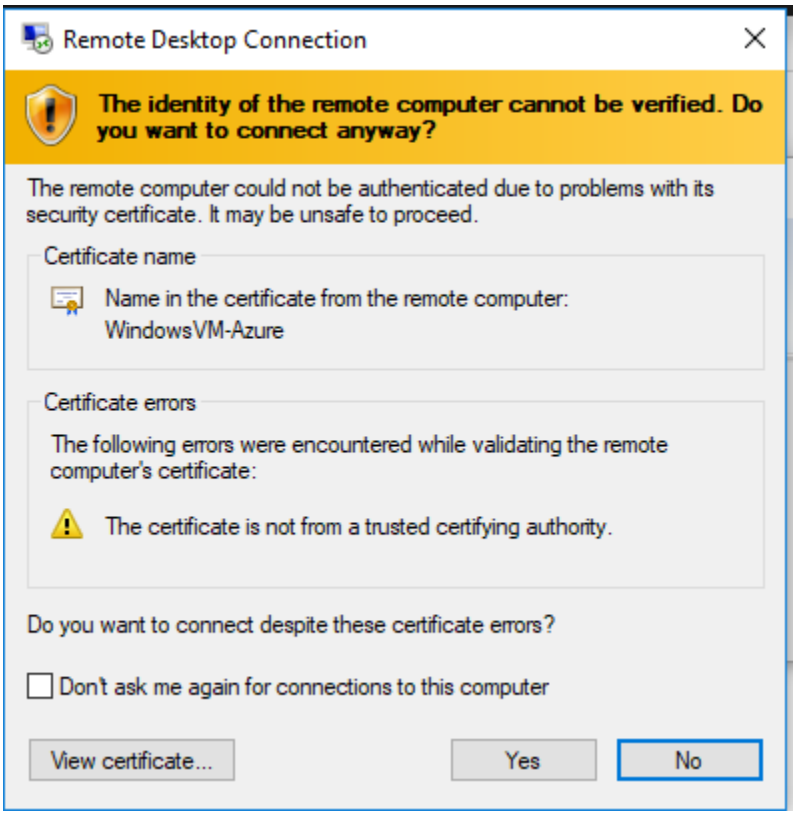
Click **“Connect”.**

Type username as “sansbound” and password which you have provided in Azure portal while create Windows virtual machine.

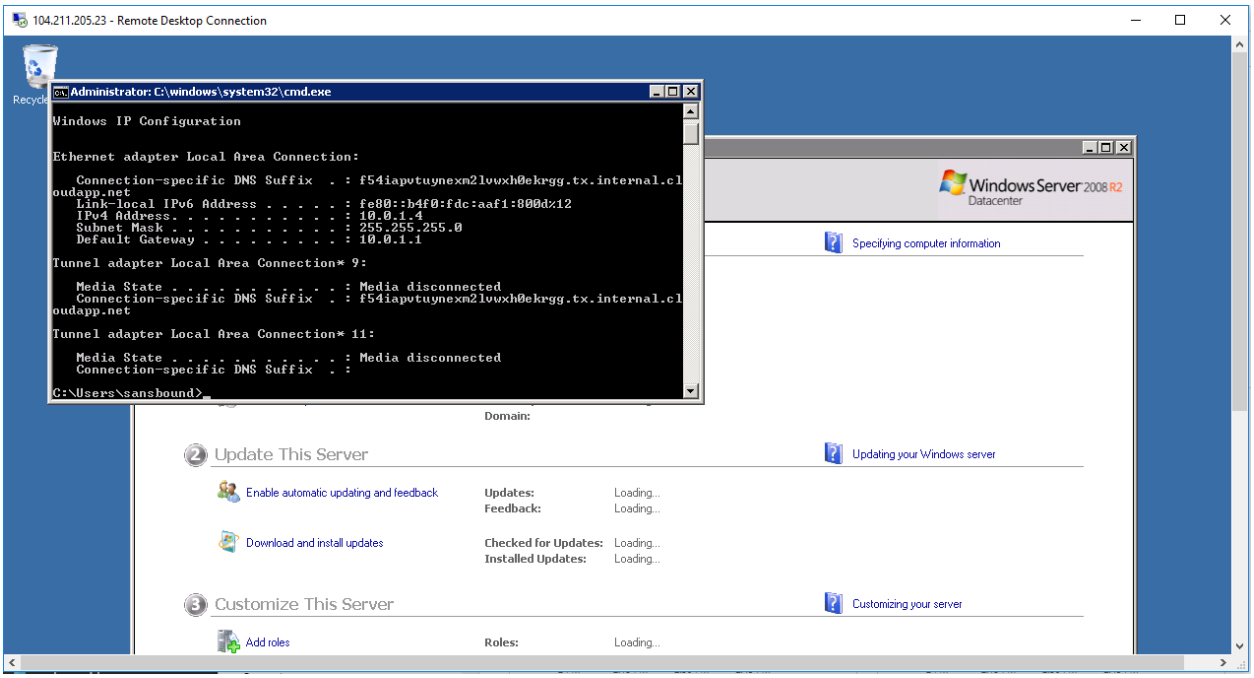
Click **“Ok”**.



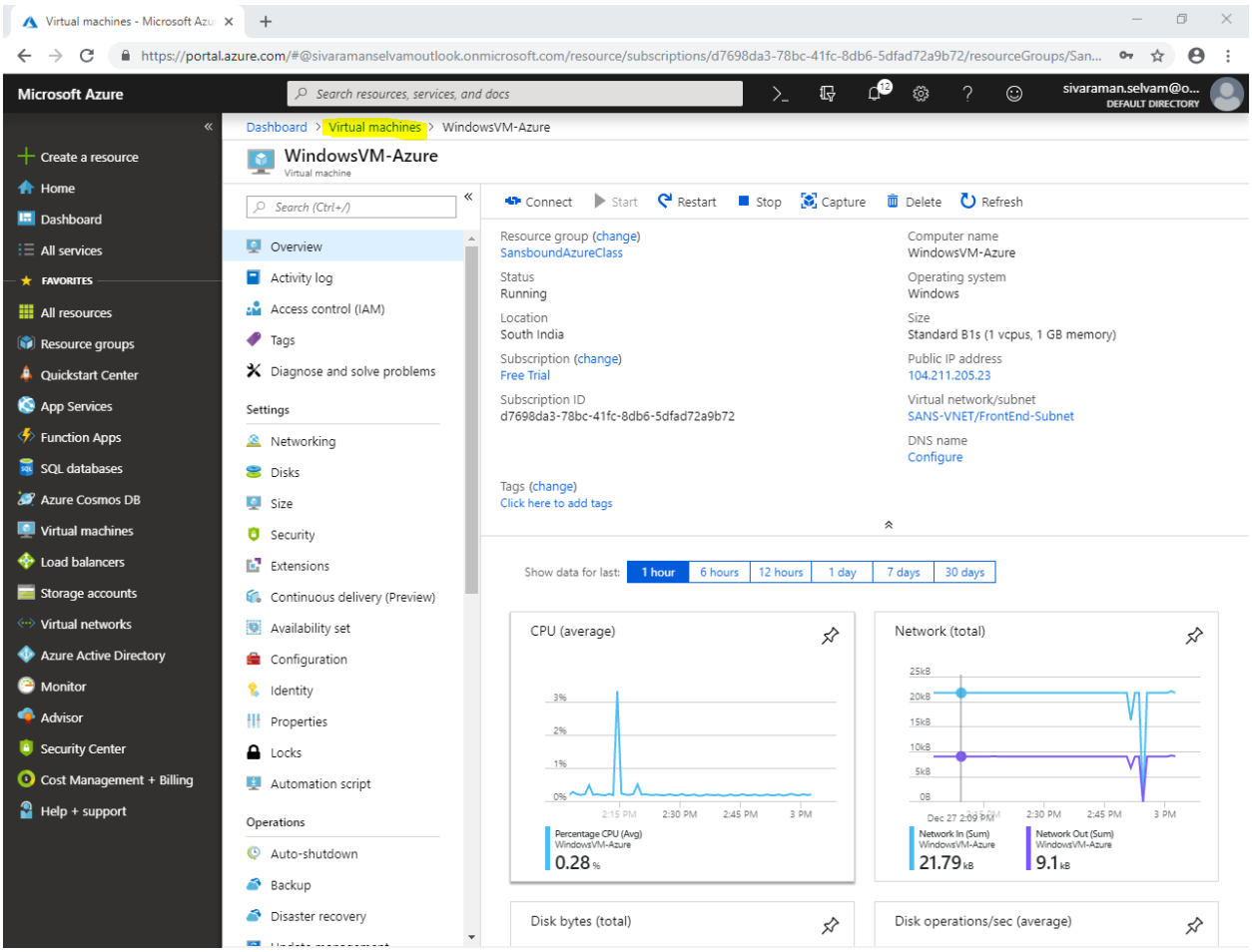
Click **“Yes”.**


Remote Desktop Connection
The identity of the remote computer cannot be verified. Do you want to connect anyway?
The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.
Certificate name
Name in the certificate from the remote computer:
WindowsVM-Azure
Certificate errors
The following errors were encountered while validating the remote computer's certificate:
The certificate is not from a trusted certifying authority.
Do you want to connect despite these certificate errors?
Don't ask me again for connections to this computer
View certificate...
Yes
No

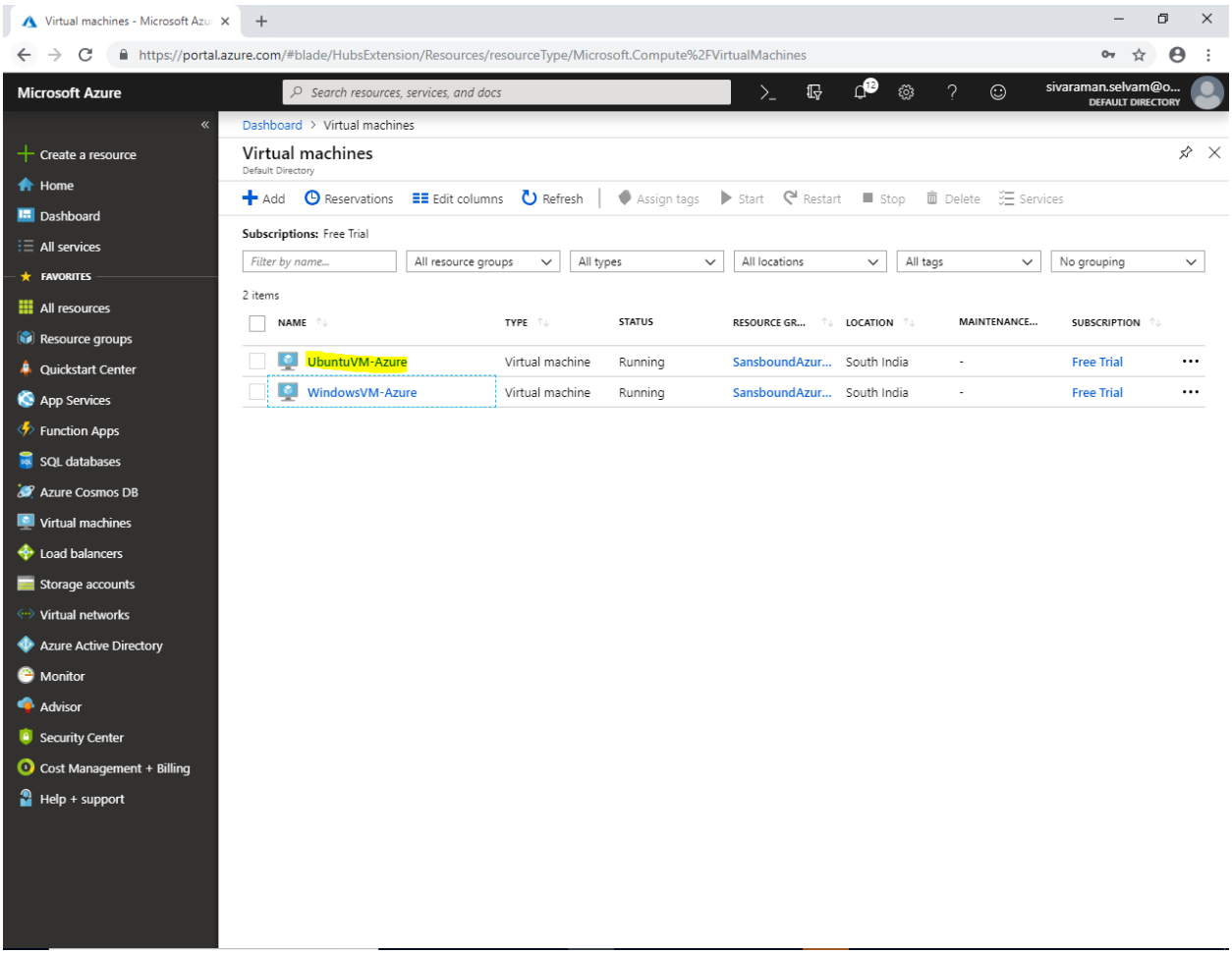
You have successfully logged on to “Windows 2008 R2 Server”, in command prompt type **“ipconfig”** and press **“Enter”**.



Click on **“Virtual machines”** in top.

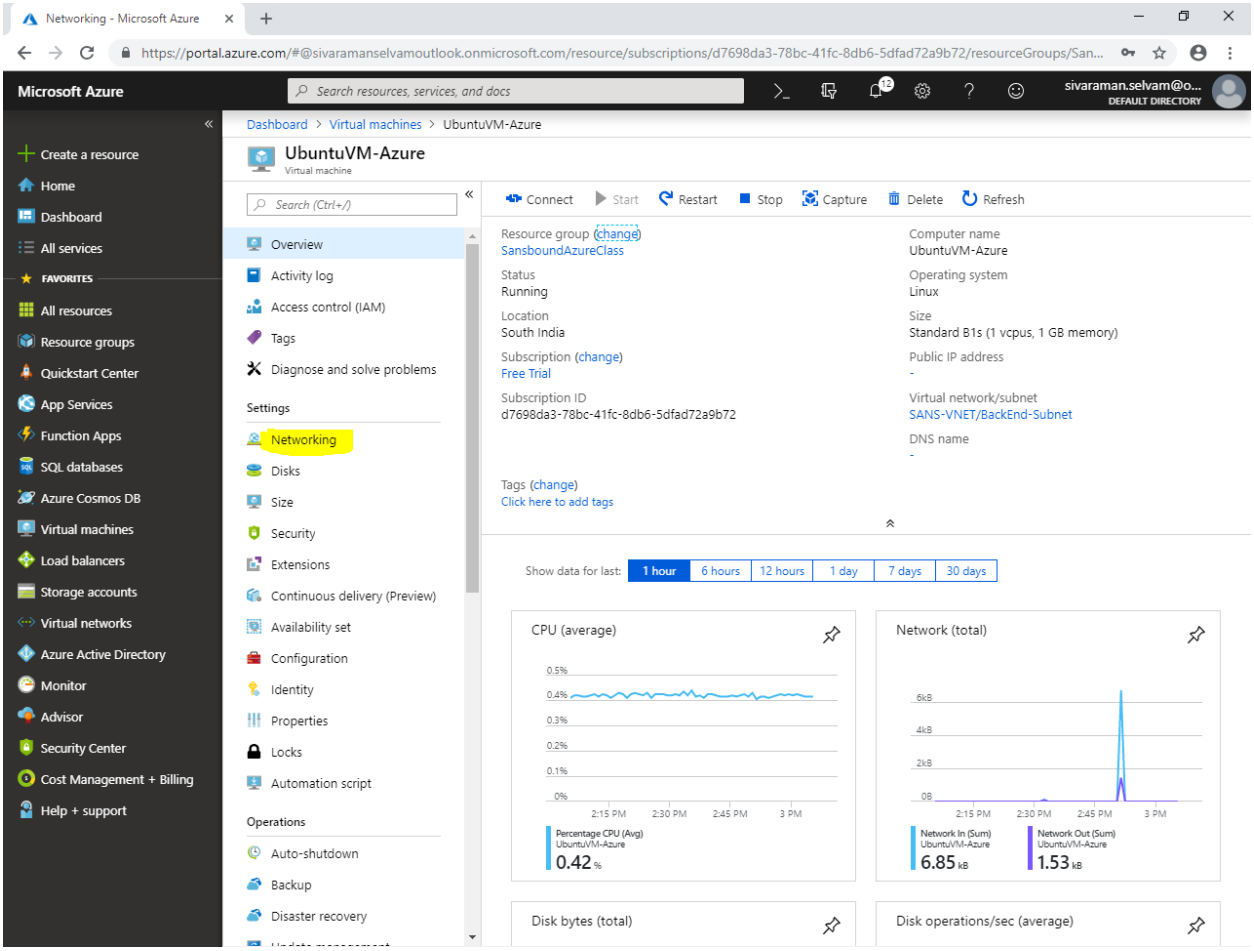


Click on **“UbuntuVM-Azure”** virtual machine.

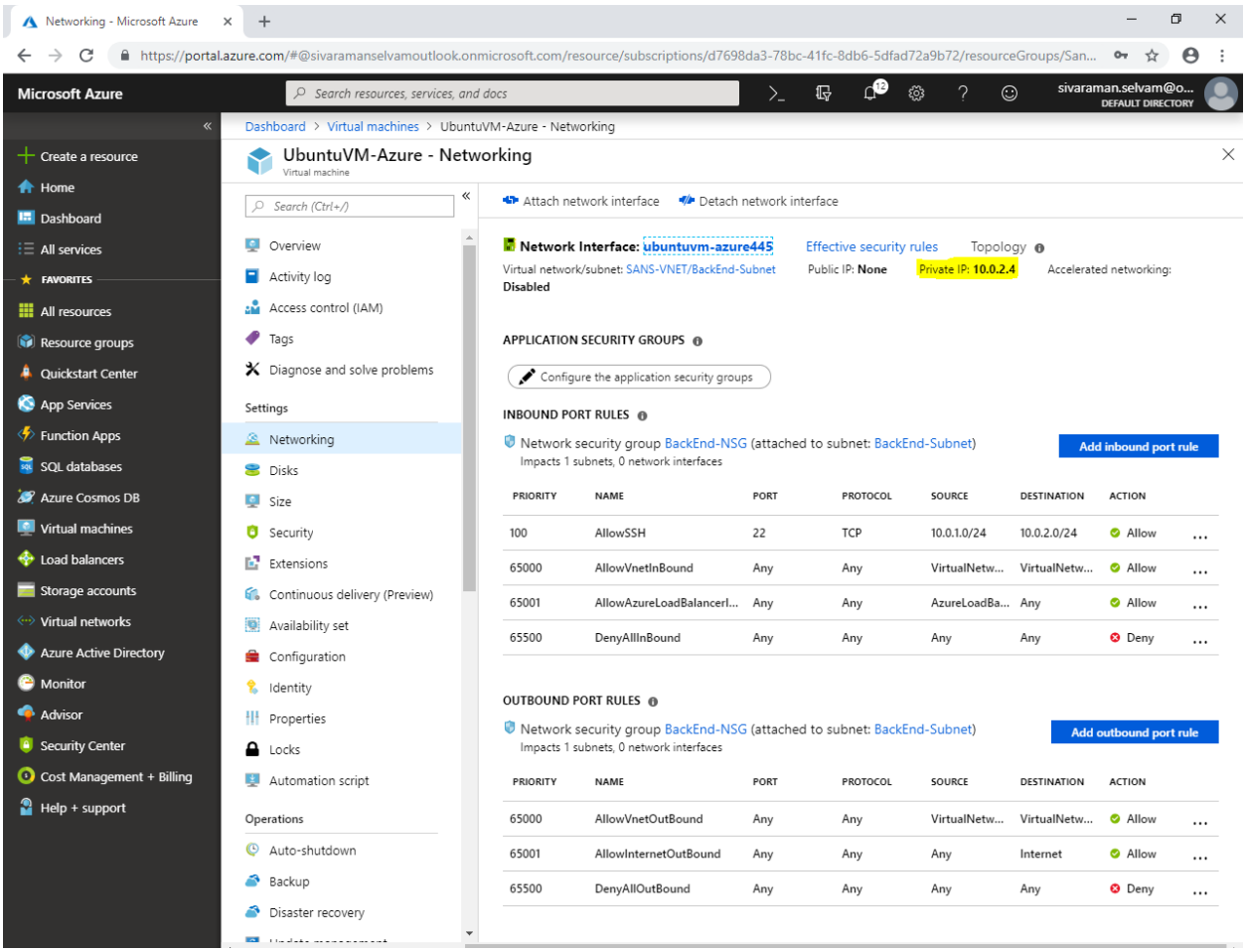


In **“UbuntuVM-Azure”**.

Click on **“Networking”**.

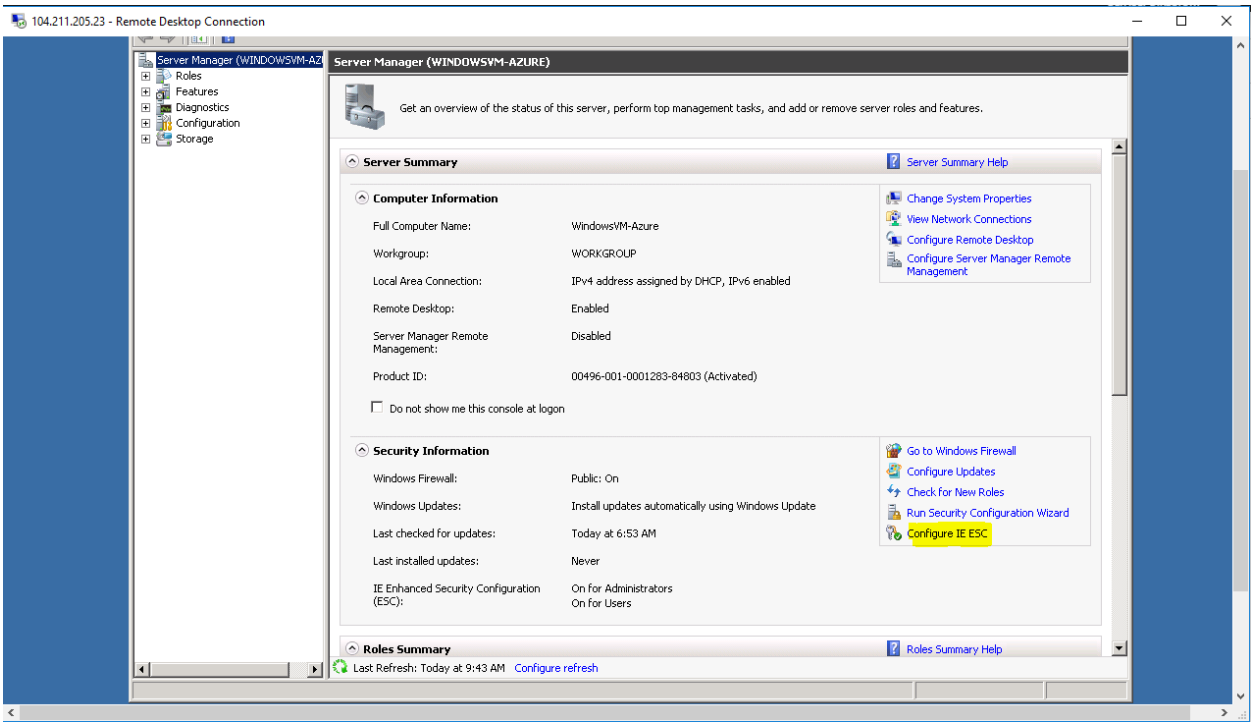


In **“Networking”** you are able to view the Private IP address of Ubuntu as **10.0.2.4**



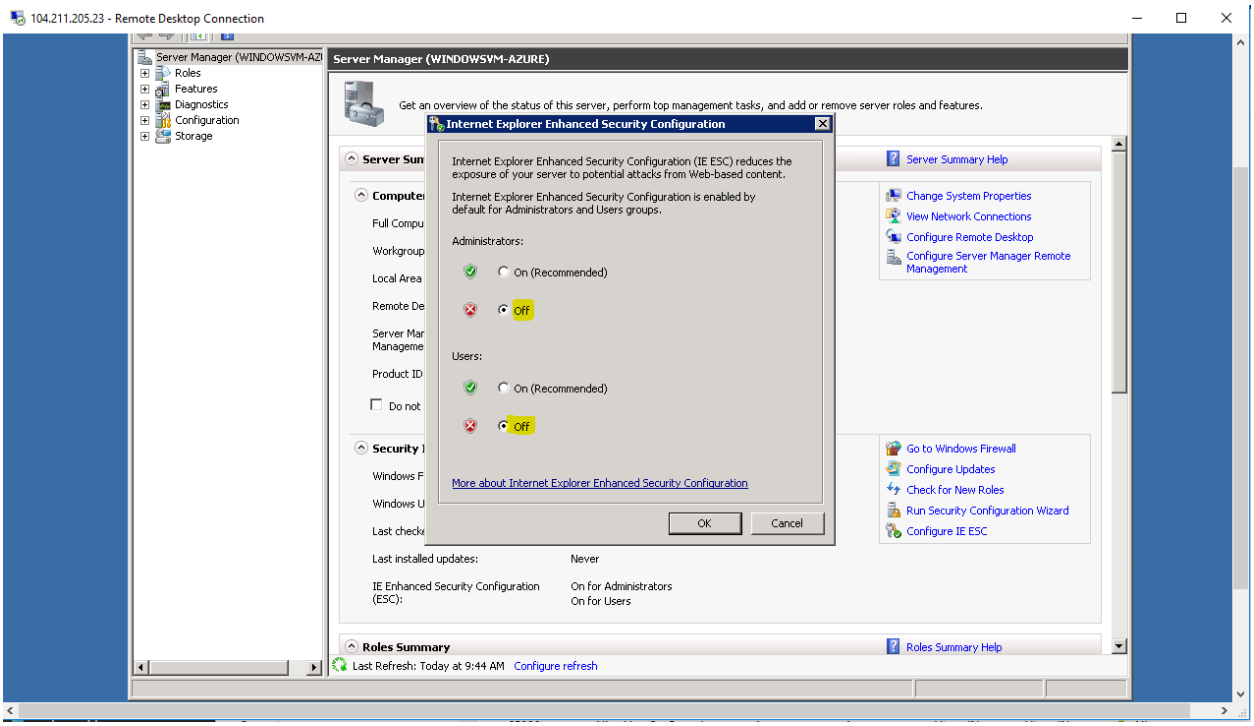
Click **“Server manager”** icon in task bar.

In **“Server manager”**, click **“Configure IE ESC”**.



You have required to set the configuration as **"Off"** to Administrators and Users.

Click **"Ok"**.

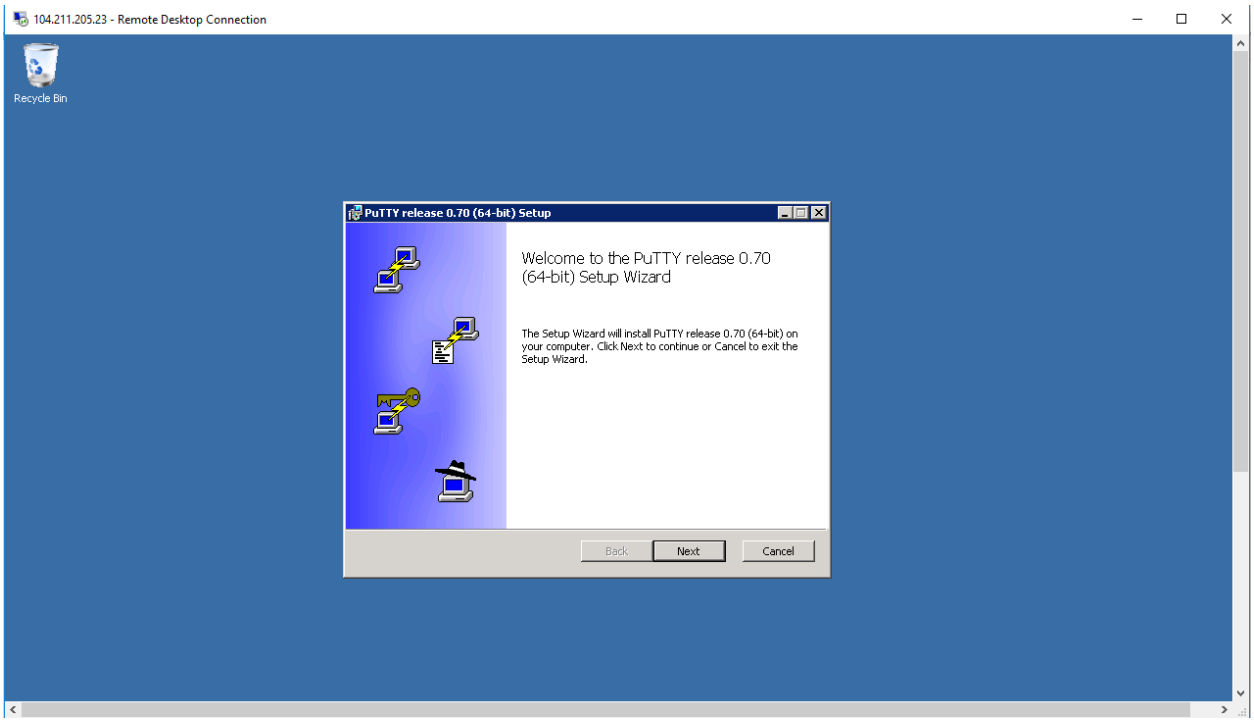


In **“Windows Server 2008 R2”**,

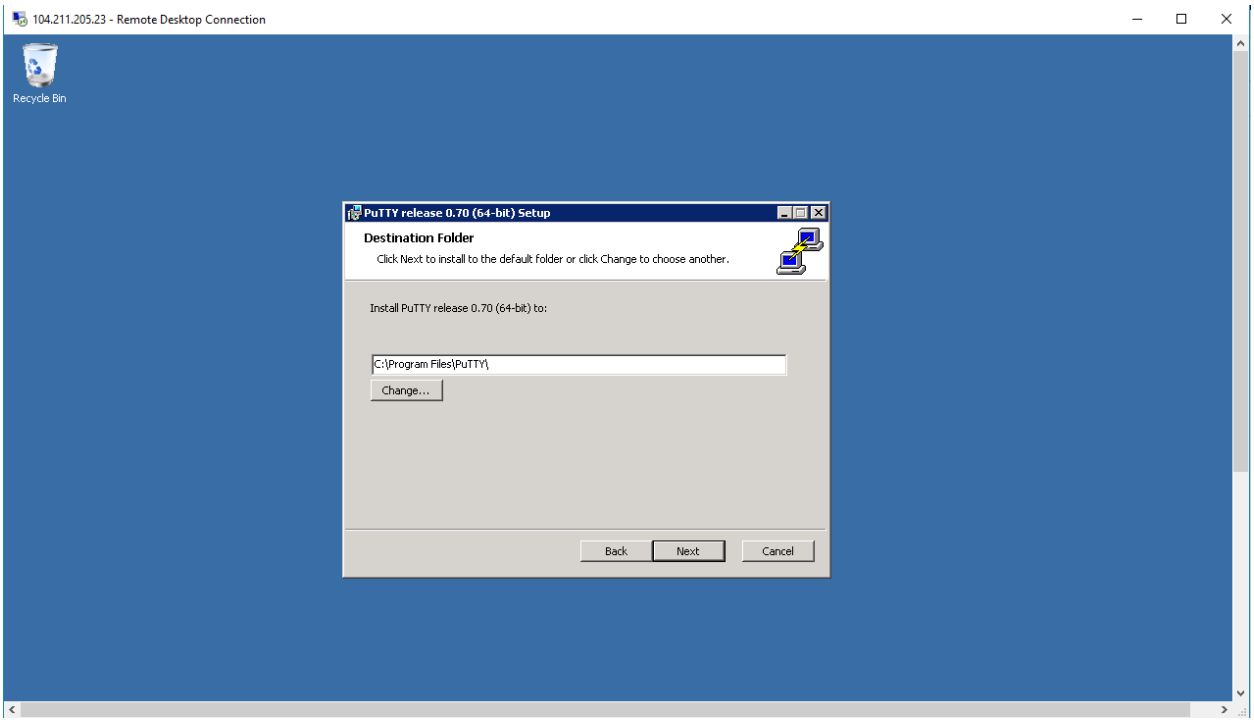
You have required to download **“Putty.exe”** for access the Ubuntu through SSH.

Run the putty setup.

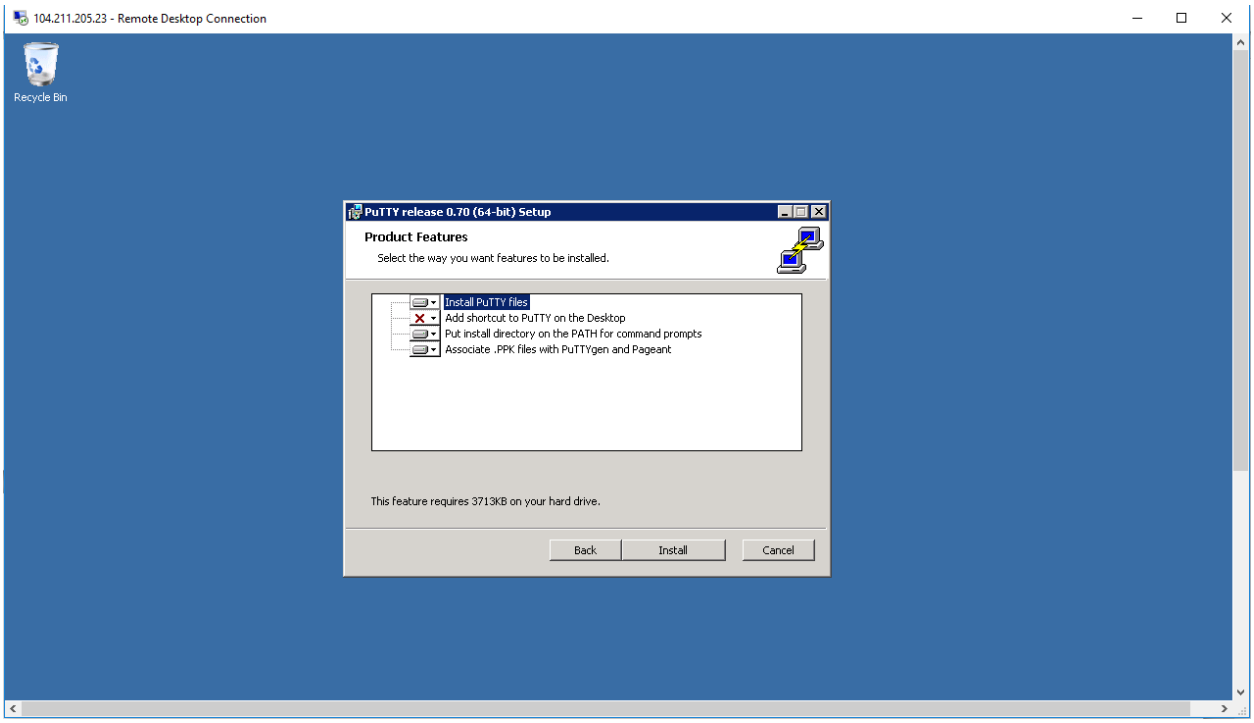
Click **“Next”** to continue.



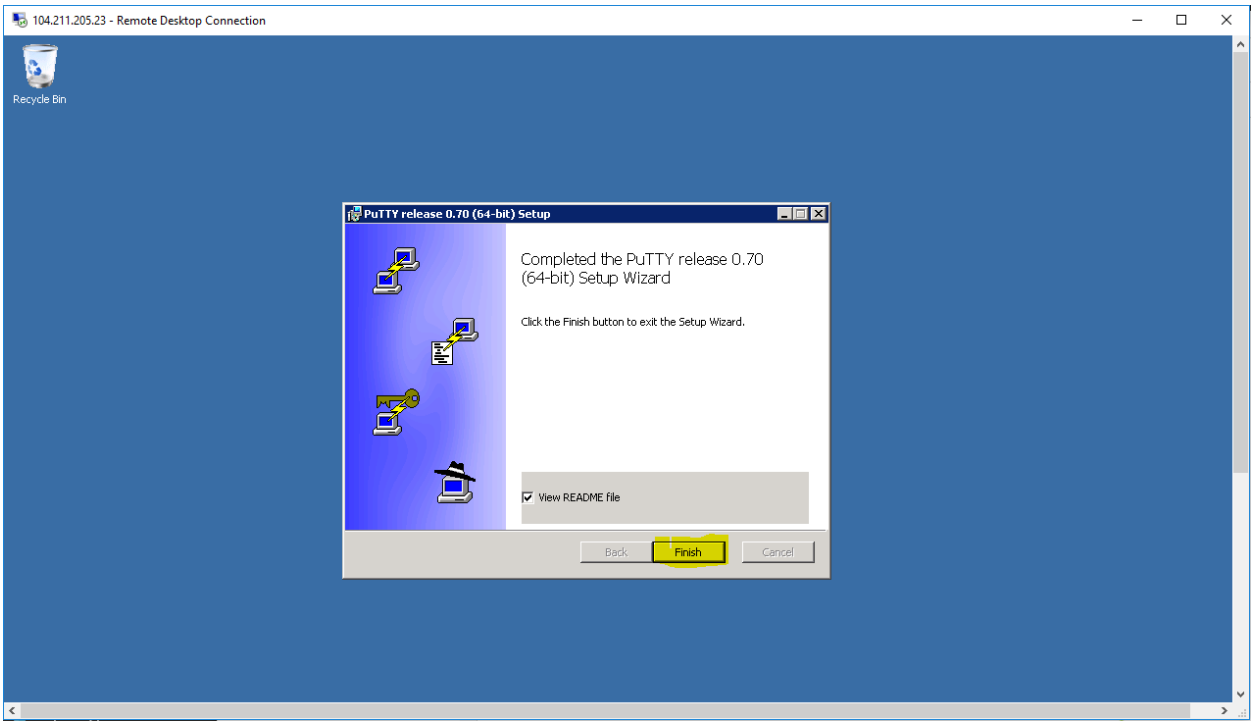
Click “**Next”**.


104.211.205.23 - Remote Desktop Connection
Recycle Bin
PuTTY release 0.70 (64-bit) Setup
Destination Folder
Click Next to install to the default folder or click Change to choose another.
Install PuTTY release 0.70 (64-bit) to:
C:\Program Files\PuTTY\
Change...
Back
Next
Cancel

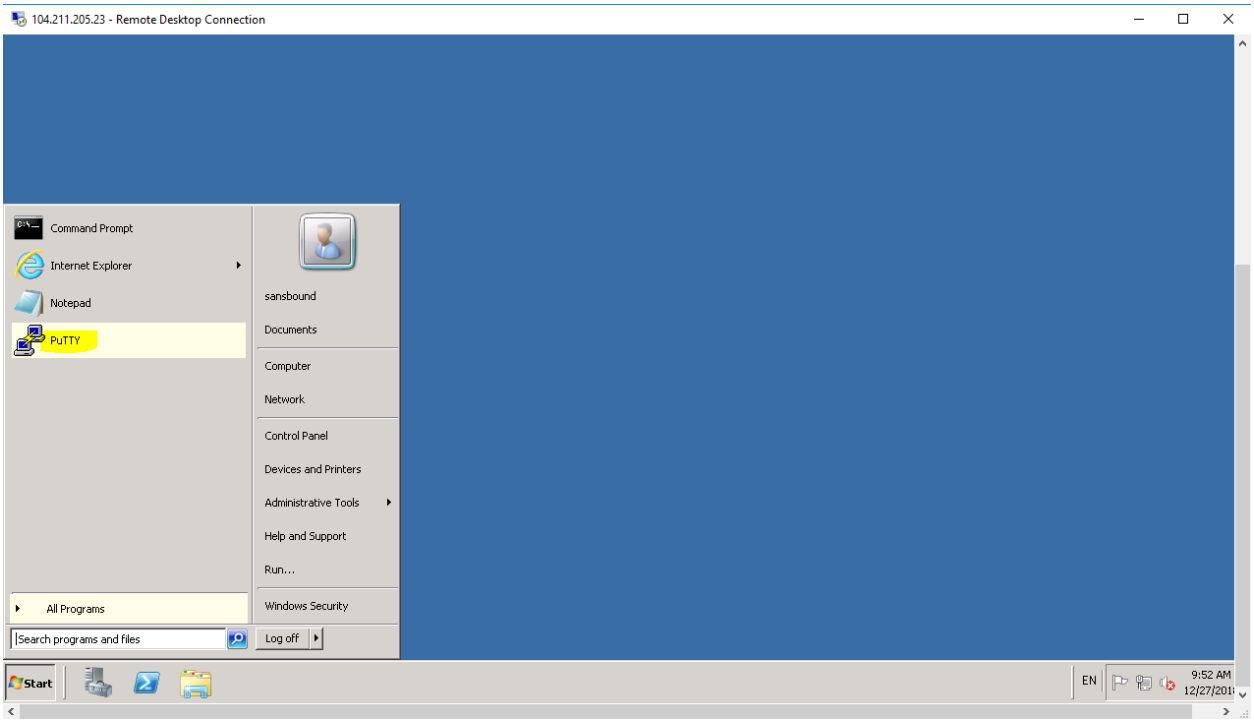
Click **“Install”.**



Click **“Finish”.**

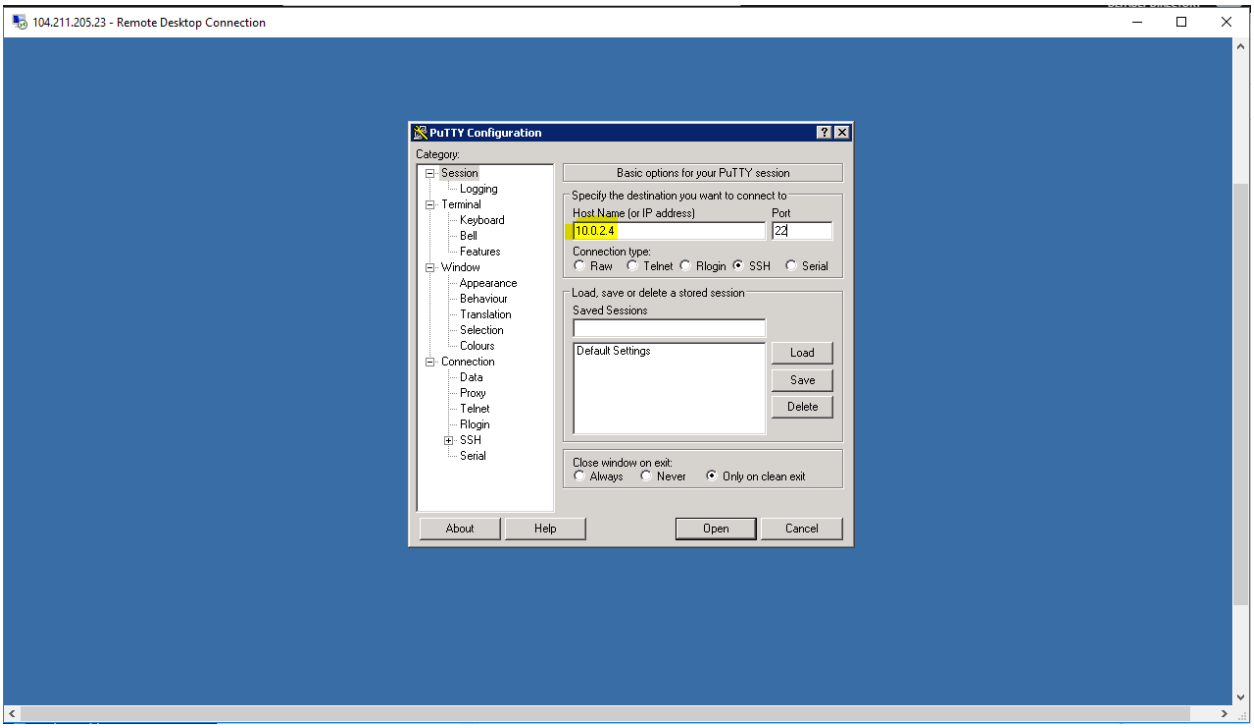


In **“Start”** you are able to see the **“putty.exe”** click it.

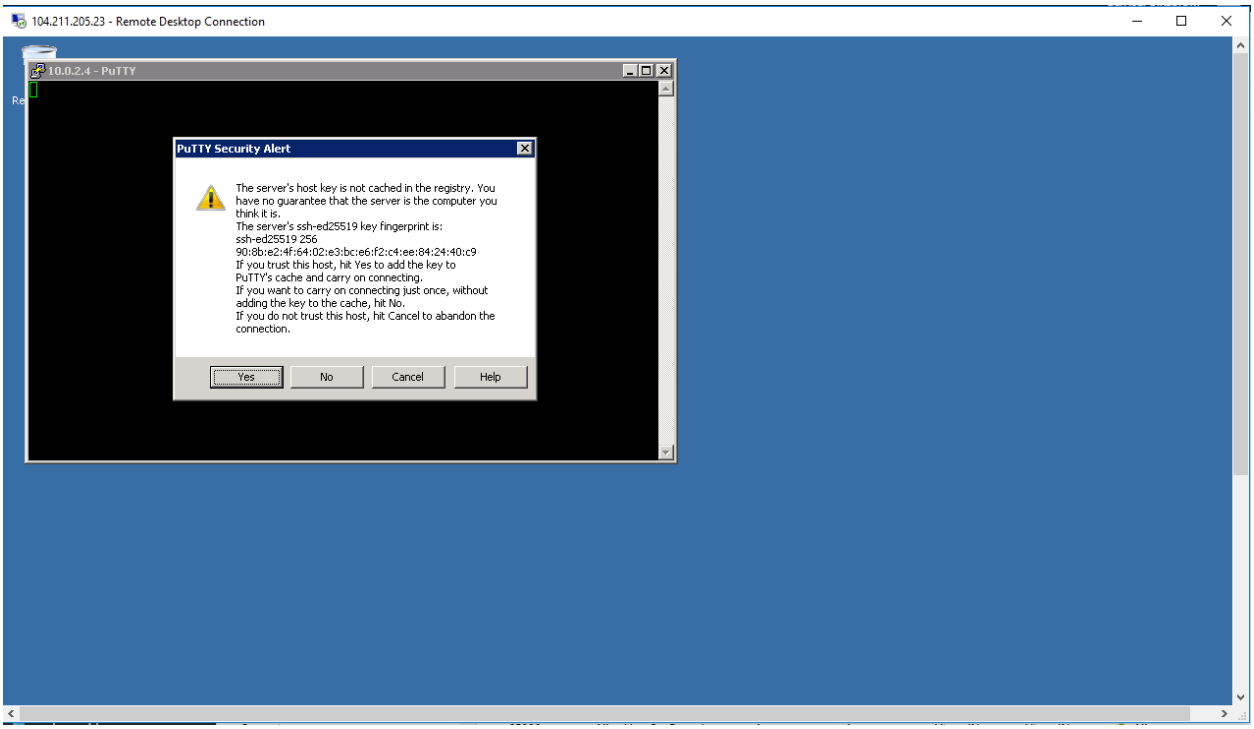


In Putty, Private IP address of as **“10.0.2.4”** Ubuntu Server which belongs to BackEnd-Subnet (10.0.2.0/24).

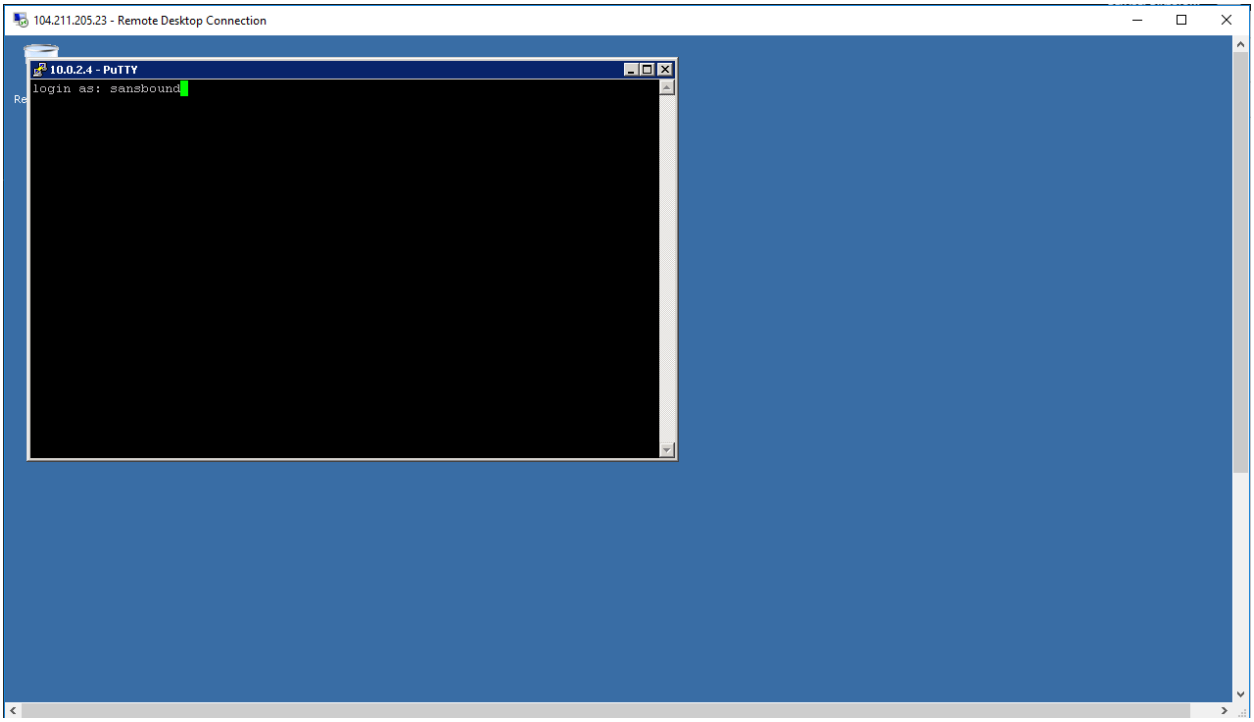
Click **“Open”** to connect to Ubuntu.



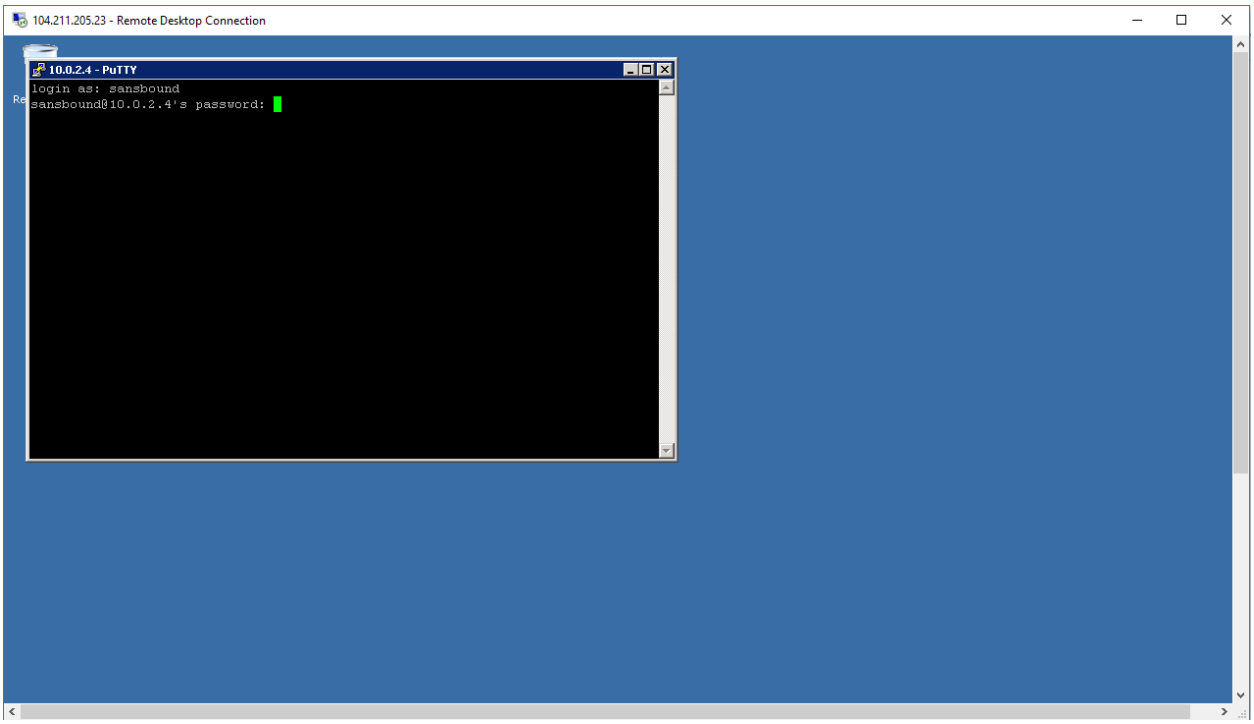
Click **“Yes”**.


104.211.205.23 - Remote Desktop Connection
10.0.2.4 - PuTTY
PuTTY Security Alert
The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 256
90:8b:e2:4f:64:02:e3:bc:e6:f2:c4:ee:84:24:40:c9
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.
Yes
No
Cancel
Help

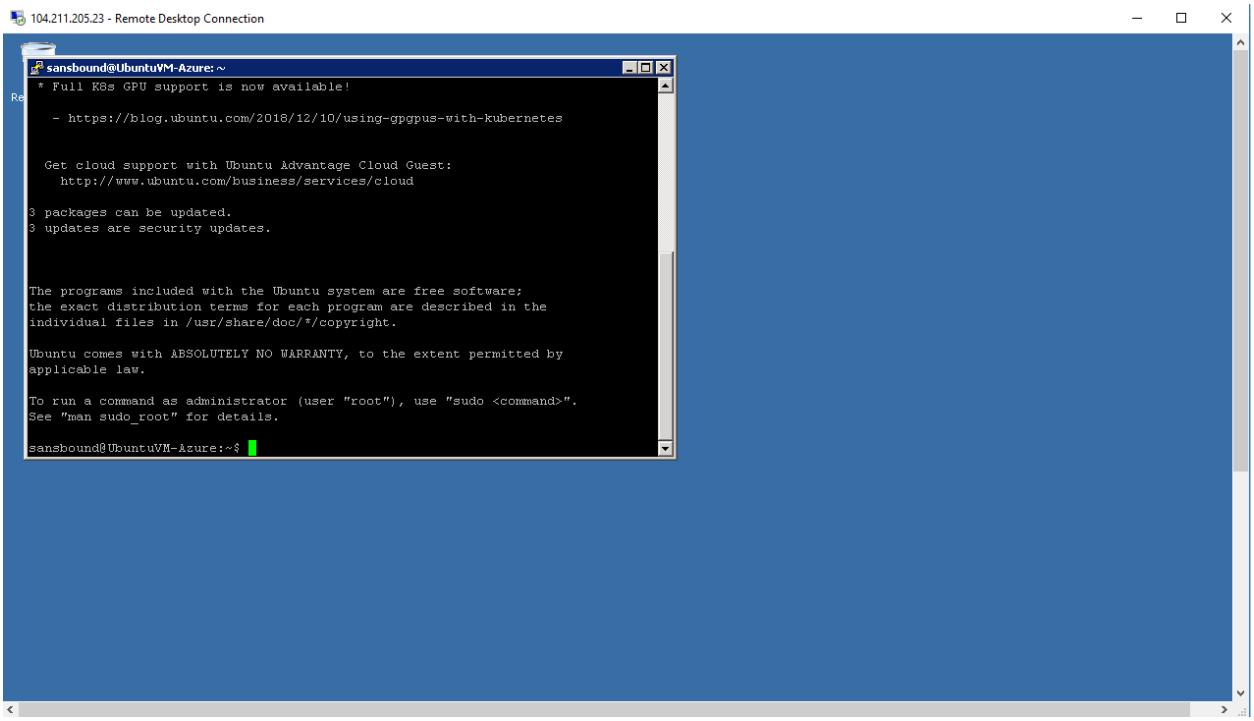
Type username of Ubuntu server as **“sansbound”**and press **“Enter”**.



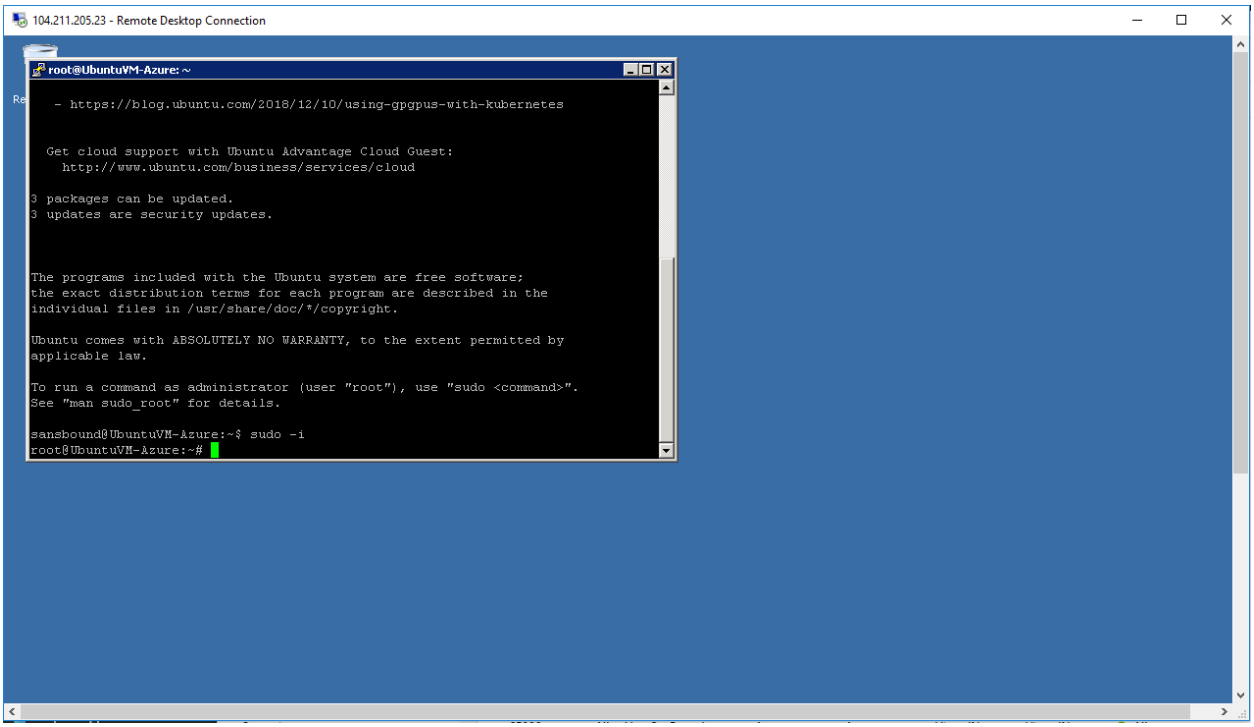
And type password for Ubuntu server and press **“Enter”.**



You have logged on successfully to Ubuntu VM by using BackEnd-Subnet (10.0.2.0/24) from “WindowsVM-Azure” virtual machine which belongs to FrontEnd-Subnet (10.0.1.0/24).



In “Ubuntu VM” SSH, type “sudo –i” to login as root user.



Now, we have understood the FrontEnd & BackEnd subnets briefly.