Lab7 – Understanding Features of Network Security Group - Azure

Network Security Group (NSG)

You can filter network traffic to and from Azure resources in an Azure virtual network with a network security group. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. To learn about which Azure resources can be deployed into a virtual network and have network security groups associated to them, see Virtual network integration for Azure services. For each rule, you can specify source and destination, port, and protocol.

This article explains network security group concepts, to help you use them effectively. If you've never created a network security group, you can complete a quick tutorial to get some experience creating one. If you're familiar with network security groups and need to manage them, see Manage a network security group. If you're having communication problems and need to troubleshoot network security groups, see Diagnose a virtual machine network traffic filter problem. You can enable network security group flow logs to analyze network traffic to and from resources that have an associated network security group.

Security rules

A network security group contains zero, or as many rules as desired, within Azure subscription limits. Each rule specifies the following properties:

Property

Explanation

Name

A unique name within the network security group.

Priority

A number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. As a result, any rules that exist with lower priorities (higher numbers) that have the same attributes as rules with higher priorities are not processed.

Source or destination

Any, or an individual IP address, classless inter-domain routing (CIDR) block (10.0.0.0/24, for example), service tag, or application security group. If you specify an address for an Azure resource, specify the private IP address assigned to the resource. Network security groups are processed after Azure translates a public IP address to a private IP address for inbound traffic, and before Azure translates a private IP address to a public IP address for outbound traffic. Learn more about Azure IP addresses. Specifying a range, a service tag, or application security group, enables you to create fewer security rules. The ability to specify multiple individual IP addresses and ranges (you cannot specify multiple service tags or application groups) in a rule is referred to as augmented security rules. Augmented security rules can only be created in network security groups created through the Resource Manager deployment model. You cannot specify multiple IP addresses and IP address ranges in network security groups created through the classic deployment model. Learn more about Azure deployment models.

Protocol

TCP, UDP, or Any, which includes TCP, UDP, and ICMP. You cannot specify ICMP alone, so if you require ICMP, use Any.

Direction

Whether the rule applies to inbound, or outbound traffic.

Port range

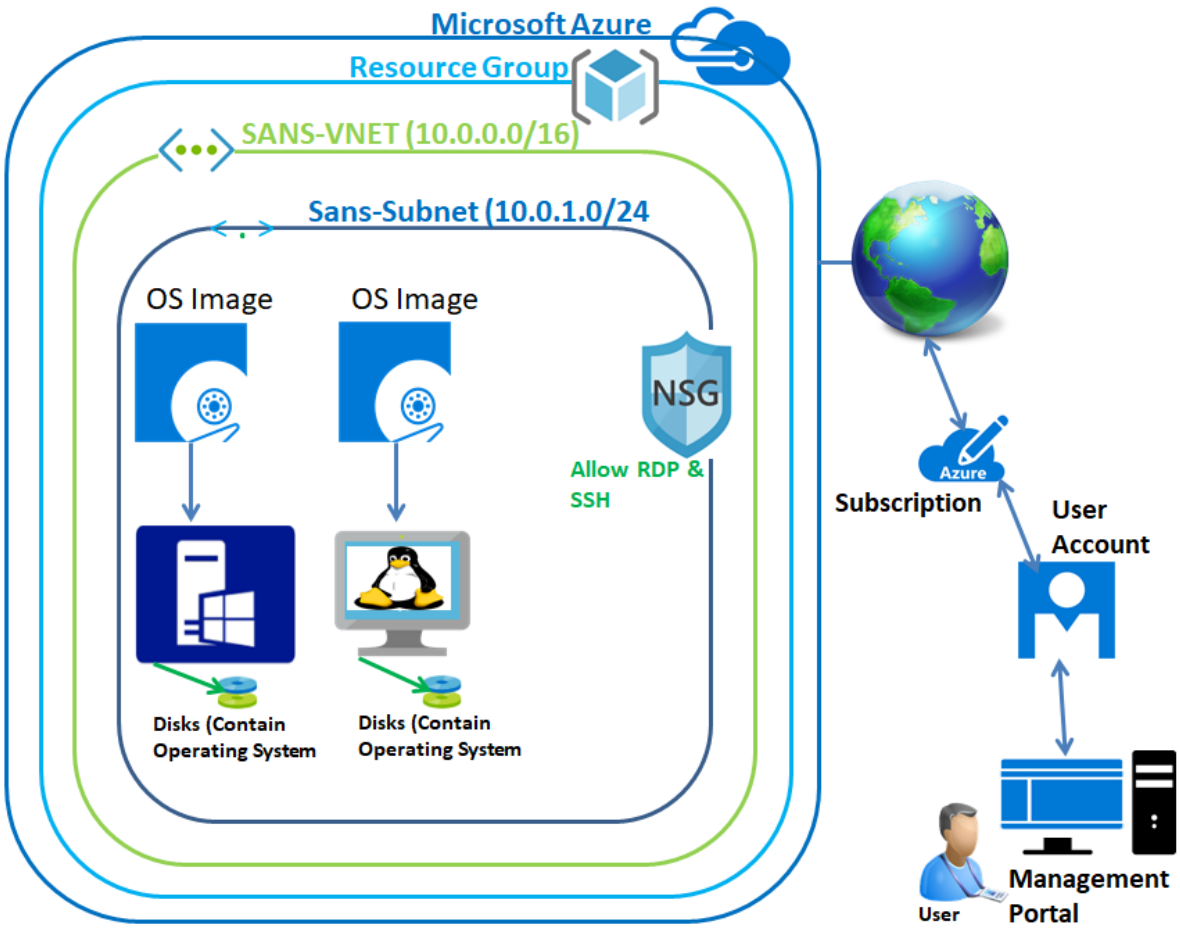
You can specify an individual or range of ports. For example, you could specify 80 or 10000-10005. Specifying ranges enables you to create fewer security rules. Augmented security rules can only be created in network security groups created through the Resource Manager deployment model. You cannot specify multiple ports or port ranges in the same security rule in network security groups created through the classic deployment model.

Action

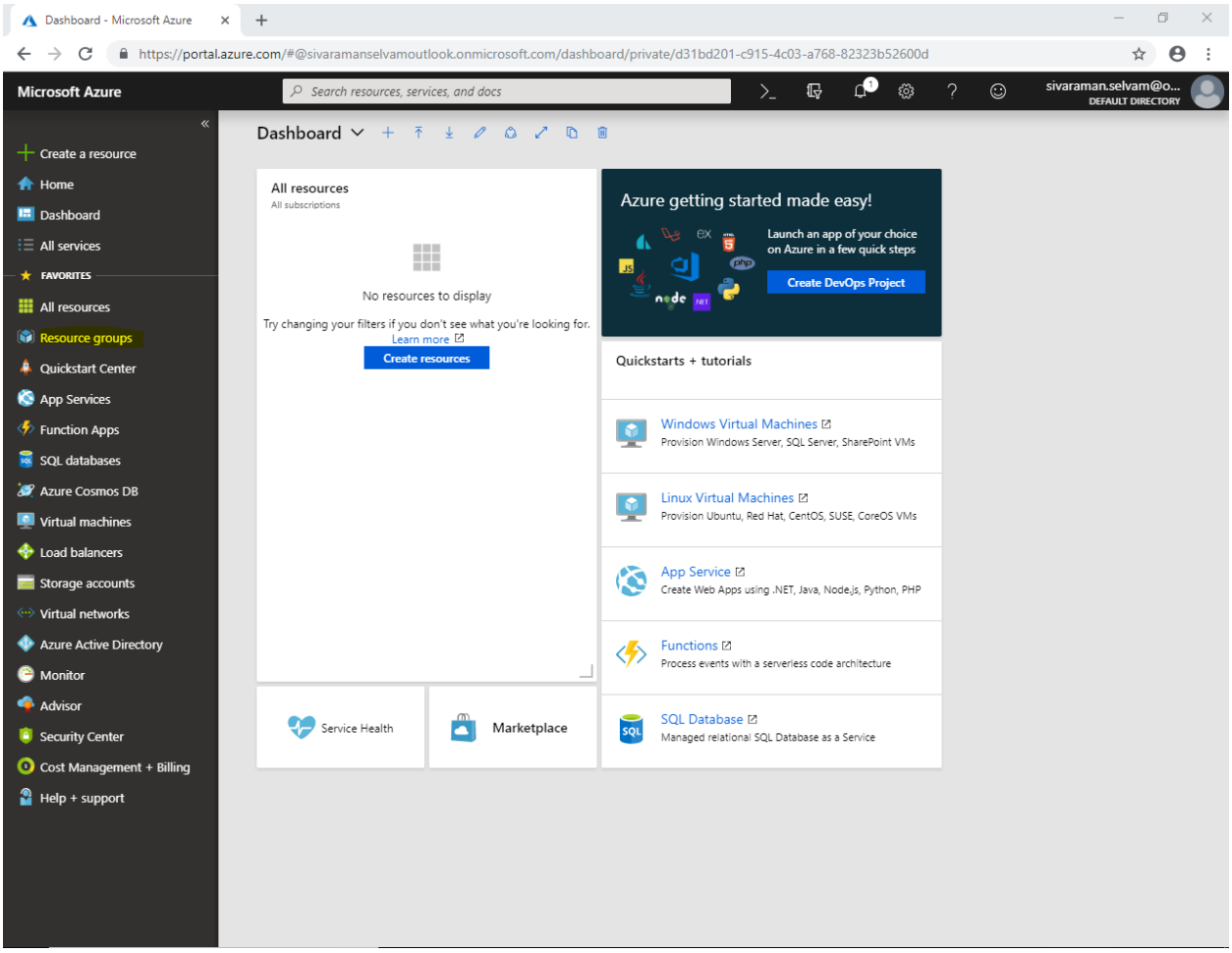
Allow or deny

Network security group security rules are evaluated by priority using the 5-tuple information (source, source port, destination, destination port, and protocol) to allow or deny the traffic. A flow record is created for existing connections. Communication is allowed or denied based on the connection state of the flow record. The flow record allows a network security group to be stateful. If you specify an outbound security rule to any address over port 80, for example, it's not necessary to specify an inbound security rule for the response to the outbound traffic. You only need to specify an inbound security rule if communication is initiated externally. The opposite is also true. If inbound traffic is allowed over a port, it's not necessary to specify an outbound security rule to respond to traffic over the port. Existing connections may not be interrupted when you remove a security rule that enabled the flow. Traffic flows are interrupted when connections are stopped and no traffic is flowing in either direction, for at least a few minutes.

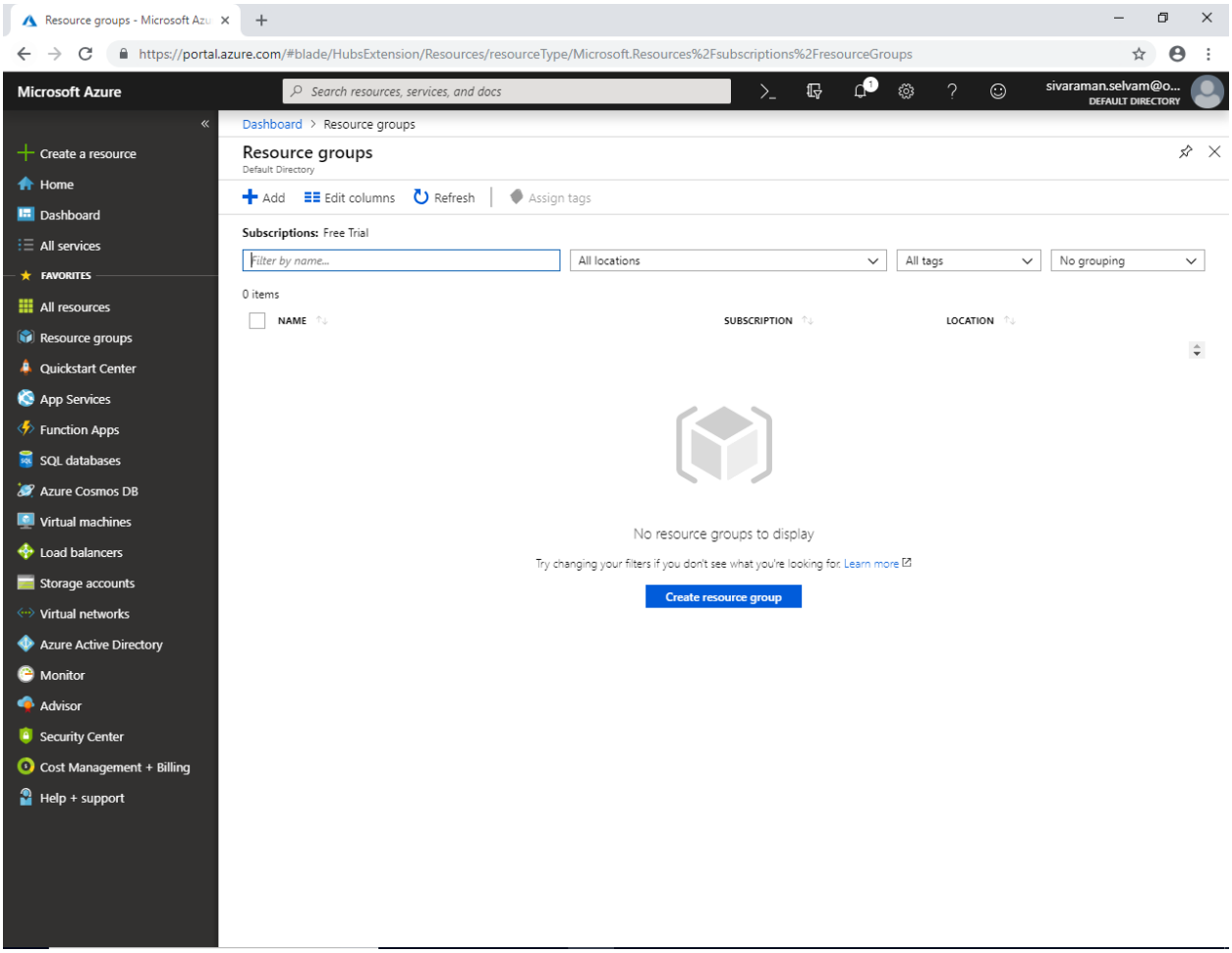
Topology:


Microsoft Azure
Resource Group
SANS-VNET (10.0.0.0/16)
Sans-Subnet (10.0.1.0/24
OS Image
OS Image
NSG
Allow RDP & SSH
Disks (Contain Operating System
Disks (Contain Operating System
Azure
Subscription
User Account
User
Management Portal

In Azure portal, click **“Resource Groups”**



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

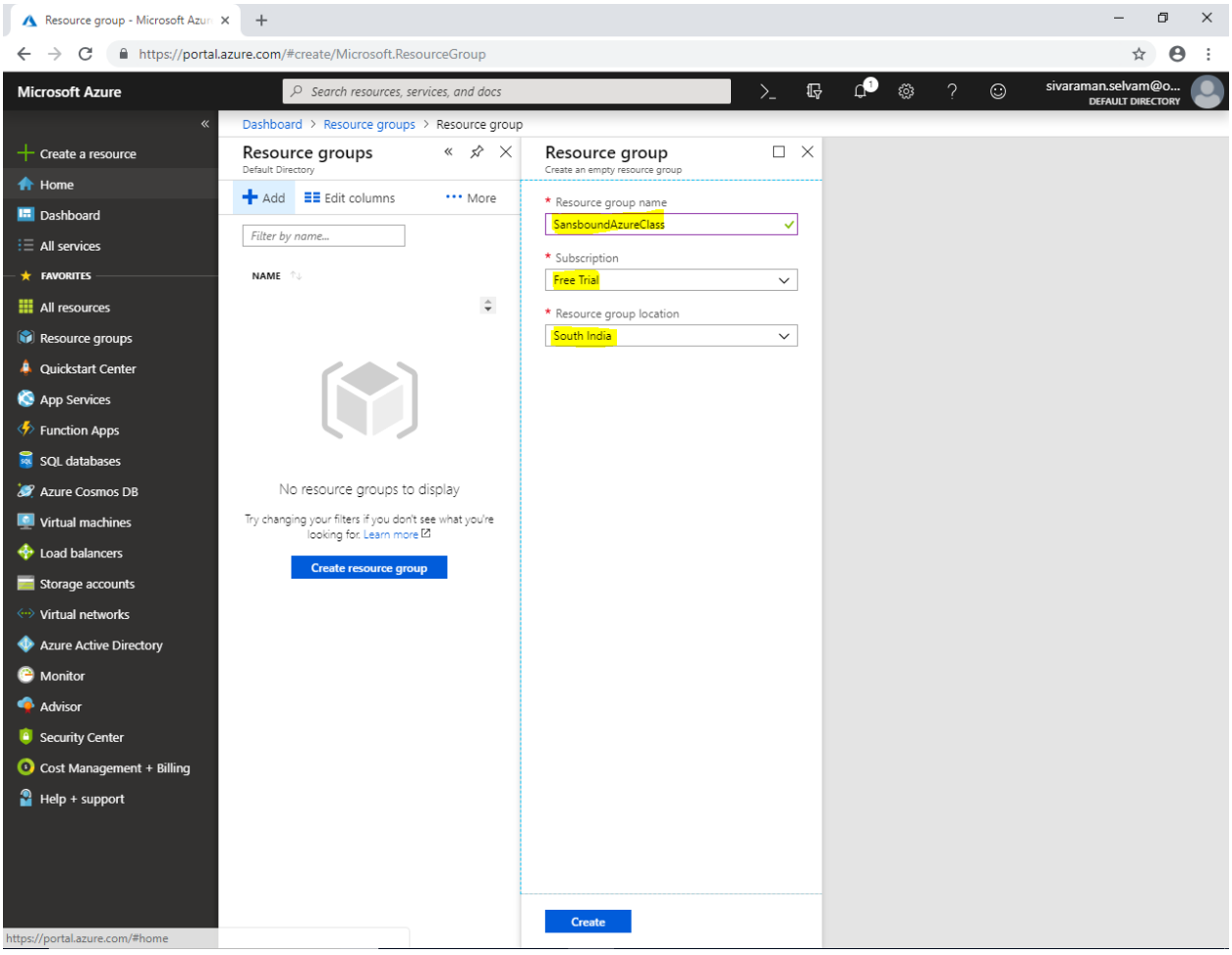


While creating **“Resource Group”**

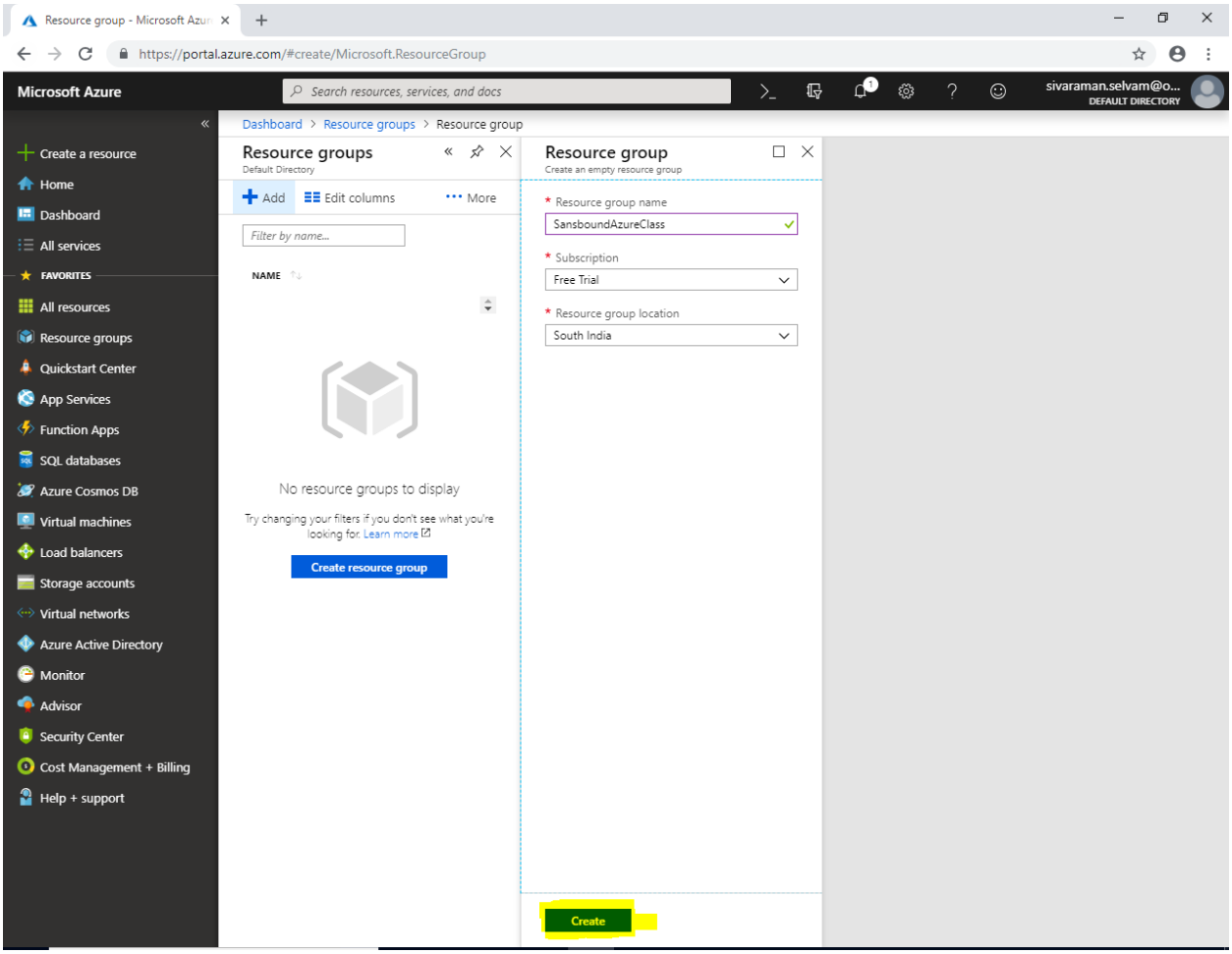
Type **“Resource Group name”** as **“SansboundAzureClass”**.

“Subscription” as **“Free Trial”**.

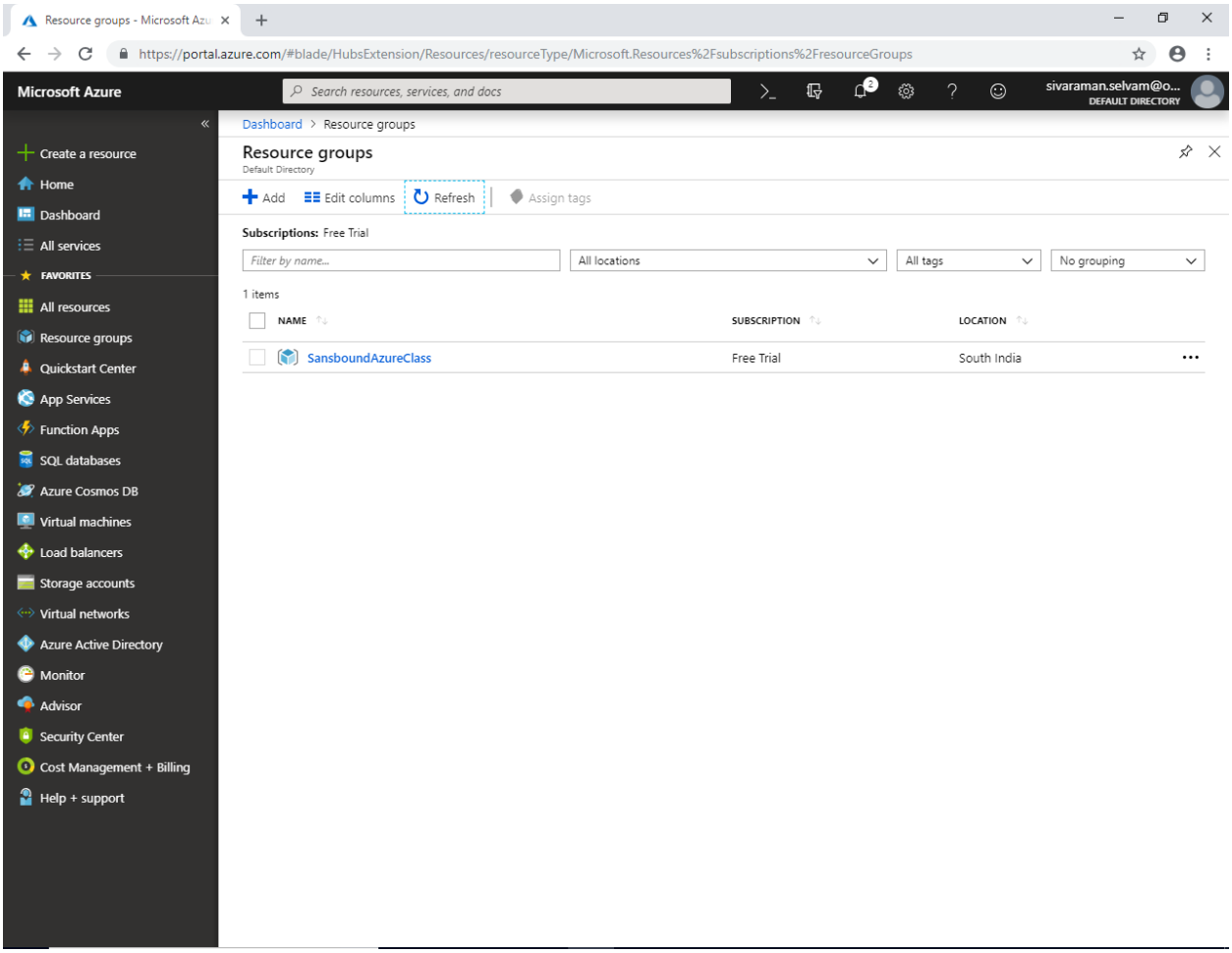
Select **“Resource Group Location”** as **“South India”**.



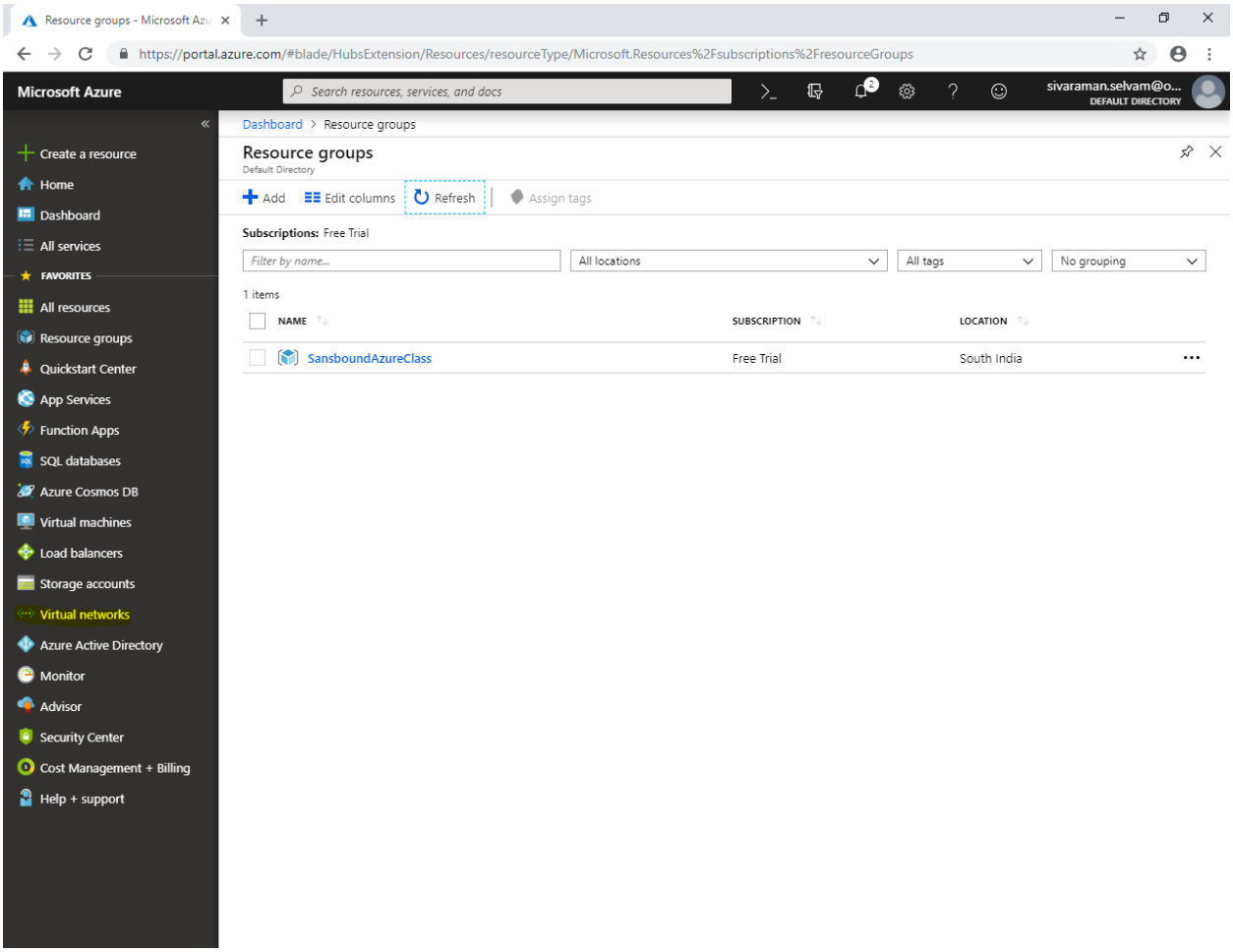
Click **"Create"** to create a new **"Resource Group"**



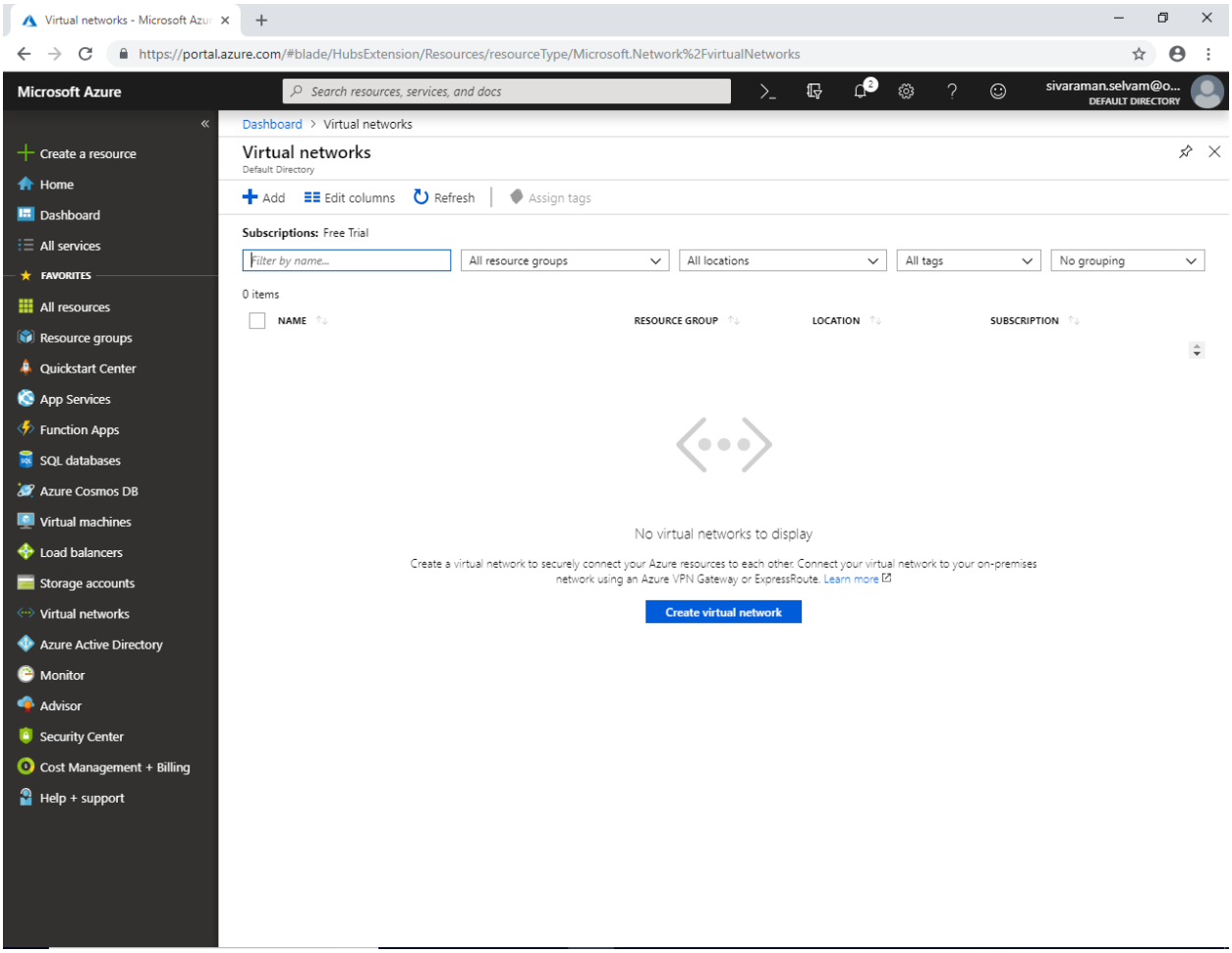
Click **“Refresh”** to view the newly created **“Resource Groups”**.



In Azure portal, click **“Virtual networks”** in left side panel.



In **“Virtual networks”** click **“Add”**.

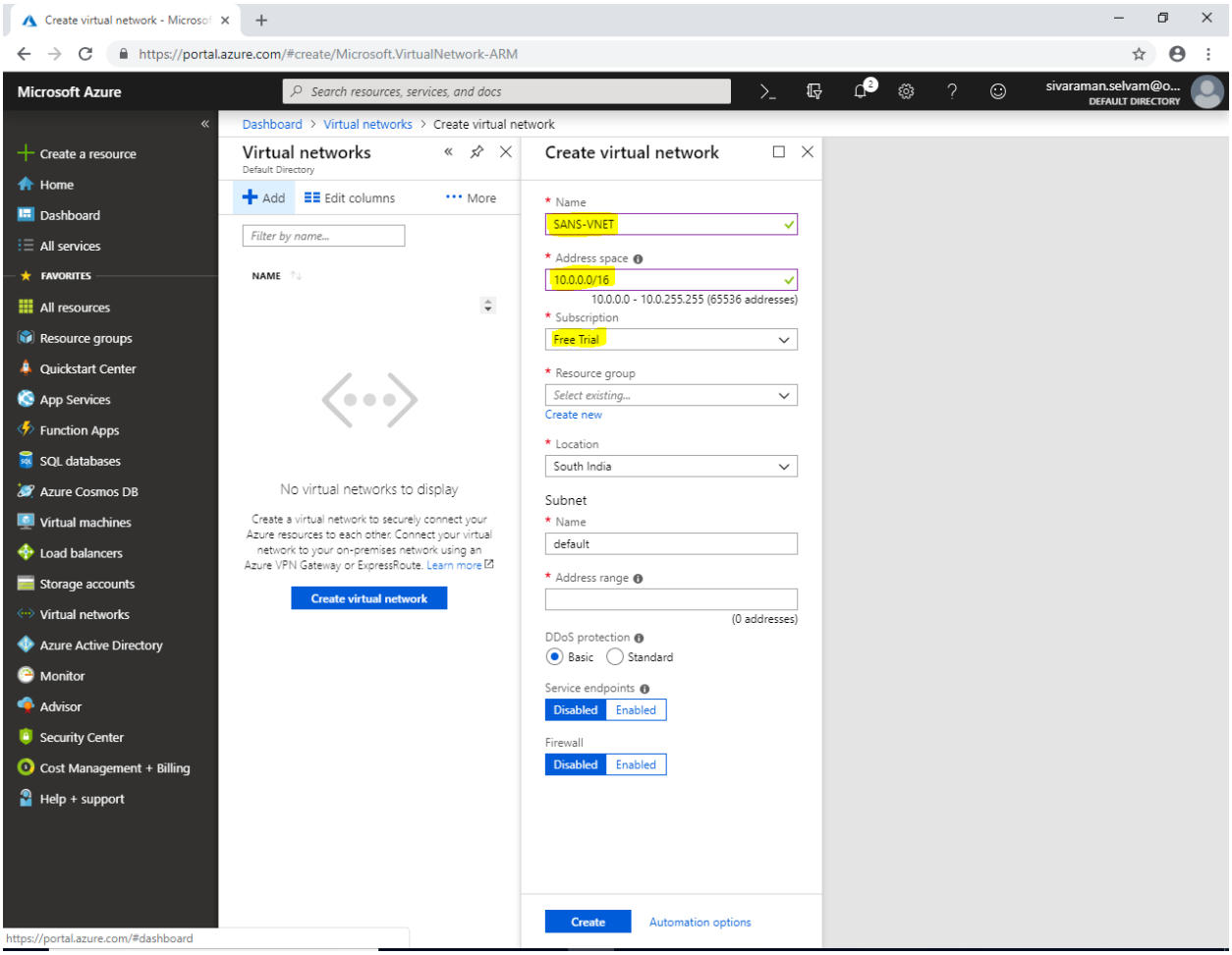


While **“Create virtual network”**

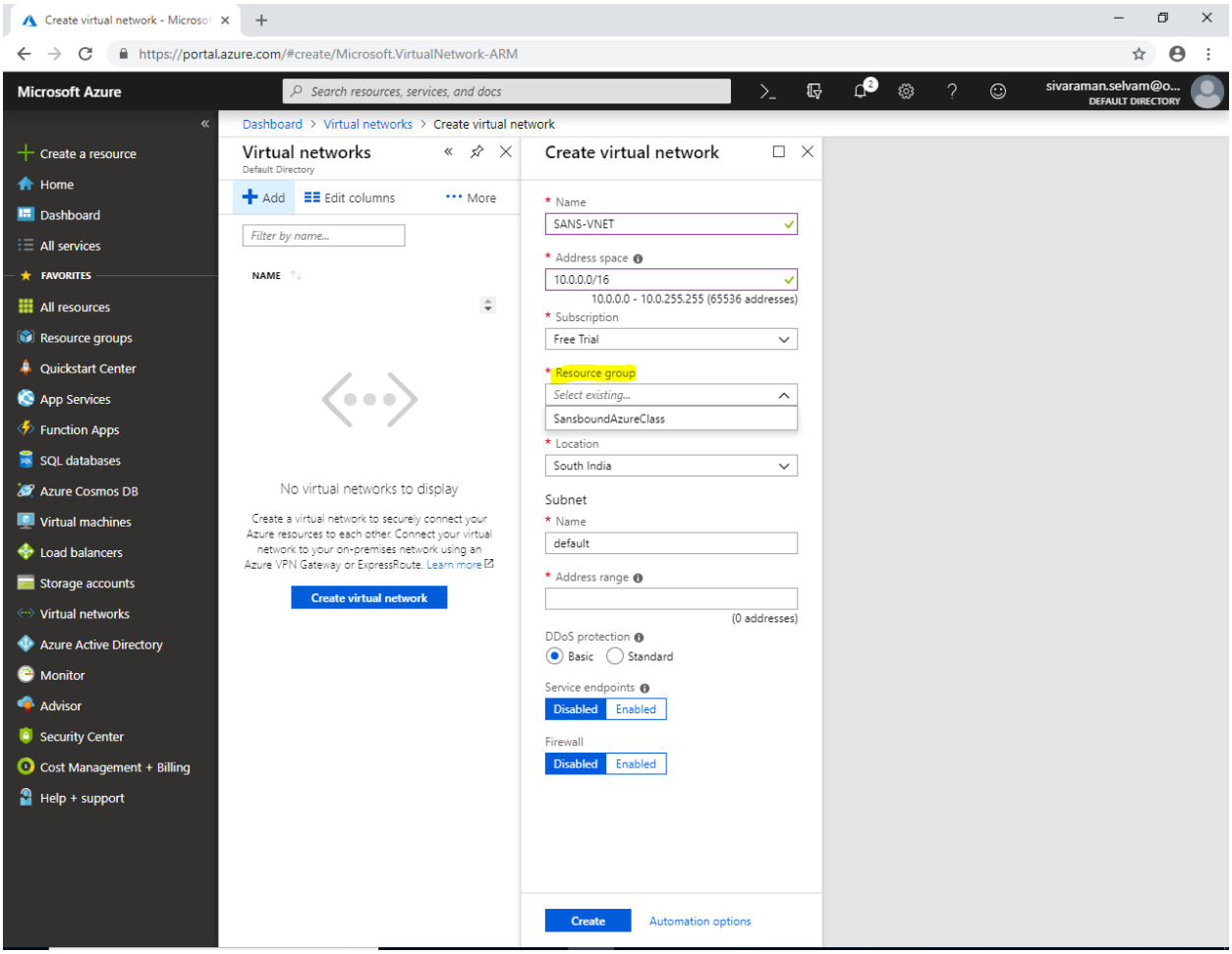
Specify **“Name”** as **“SANS-VNET”**.

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

“Subscription” as **“Free Trial”**.

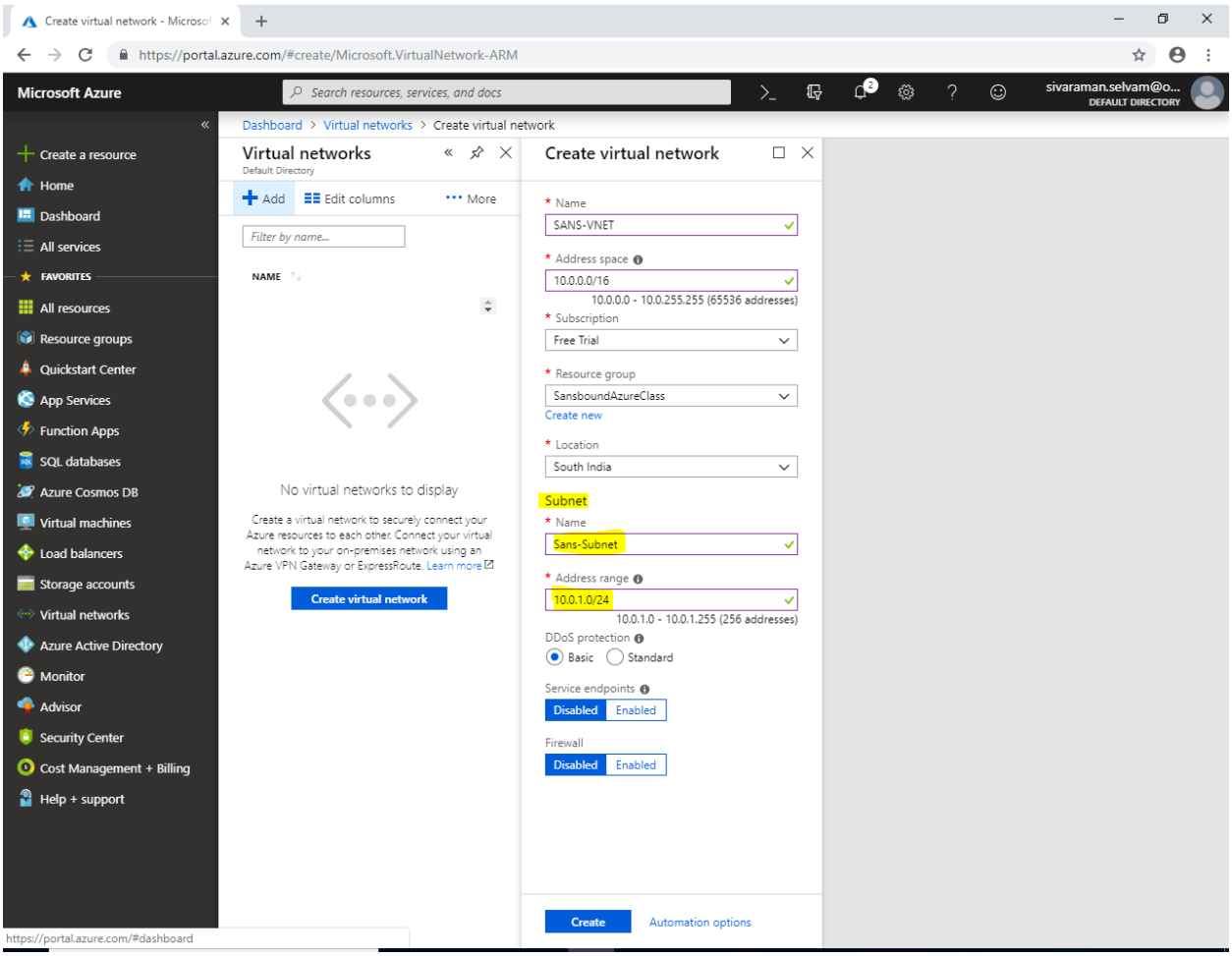


In **“Resource group”** click drop down list to select **“SansboundAzureClass”**.

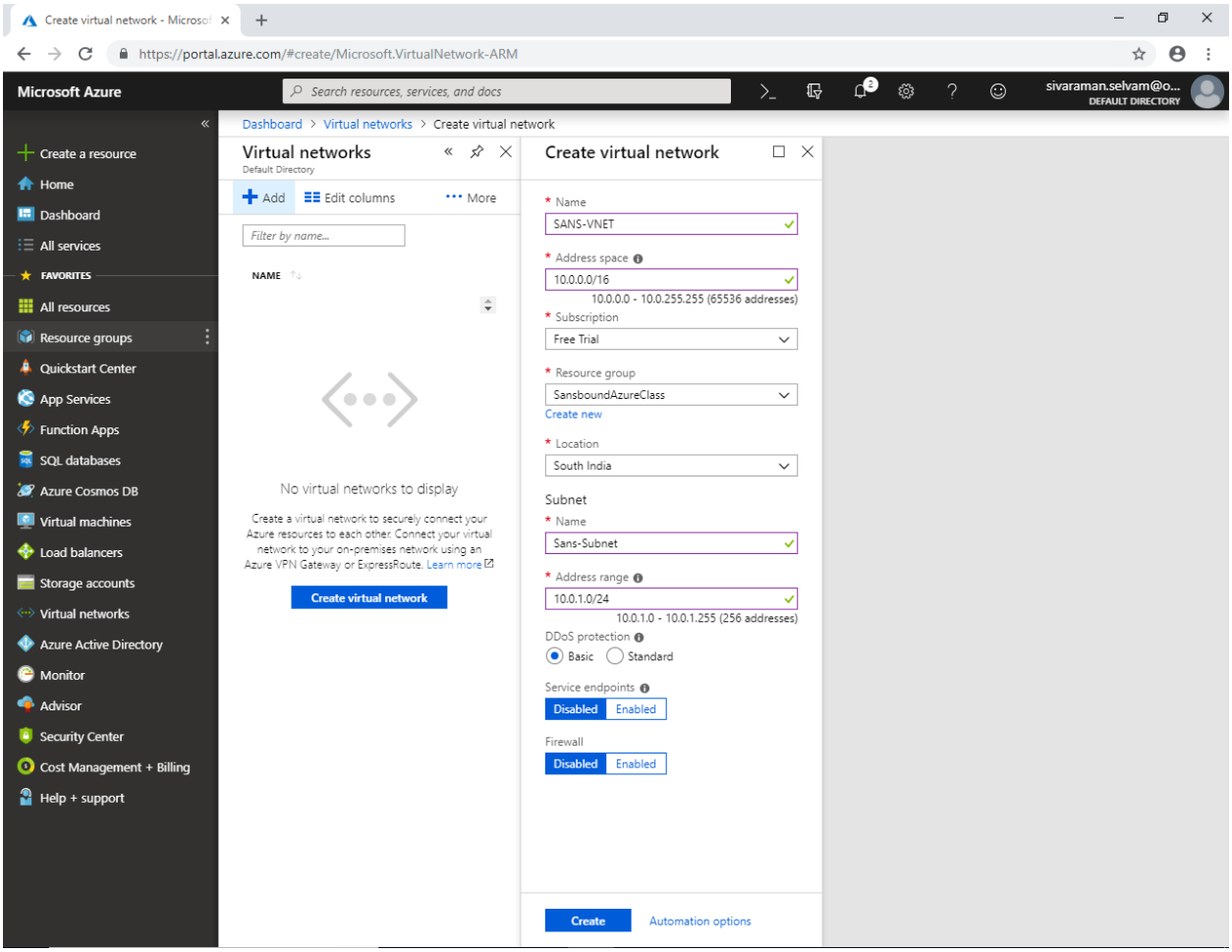


In **“Subnet”**, specify the Subnet name as **“Sans-Subnet”**.

Specify **“Address range”** as **10.0.1.0/24**

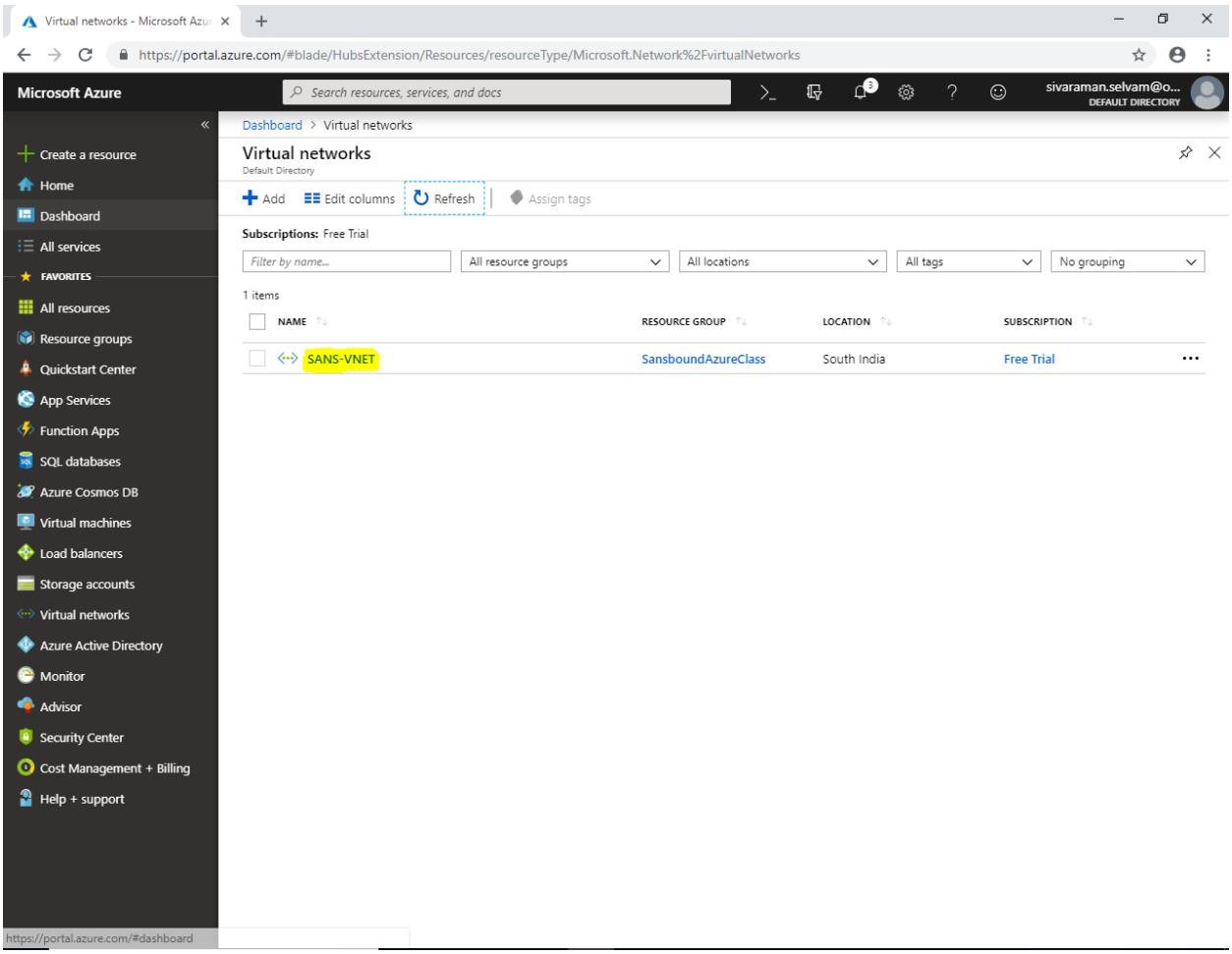


Click **“Create”**.

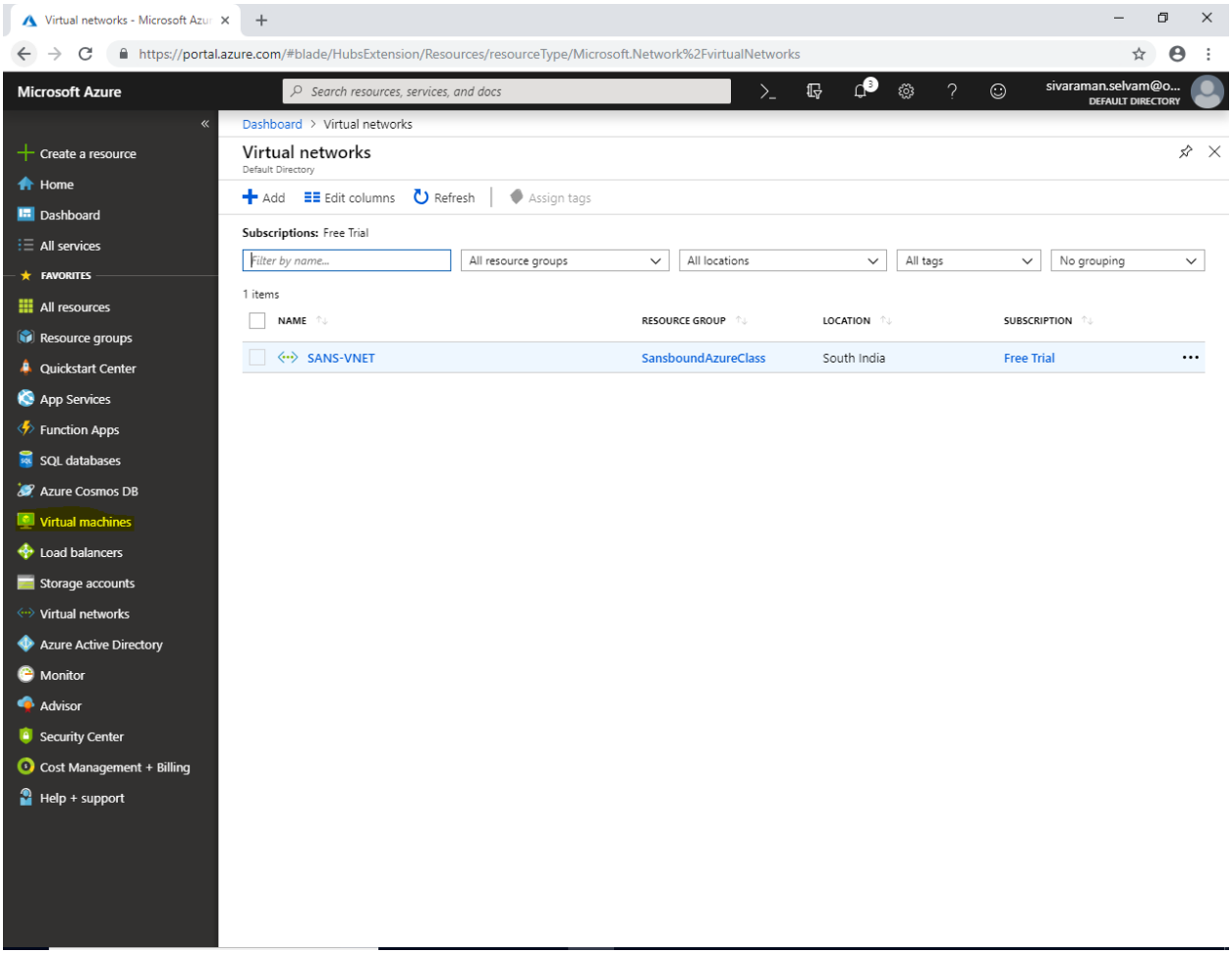


In **"Virtual networks"**, click **"Refresh"**.

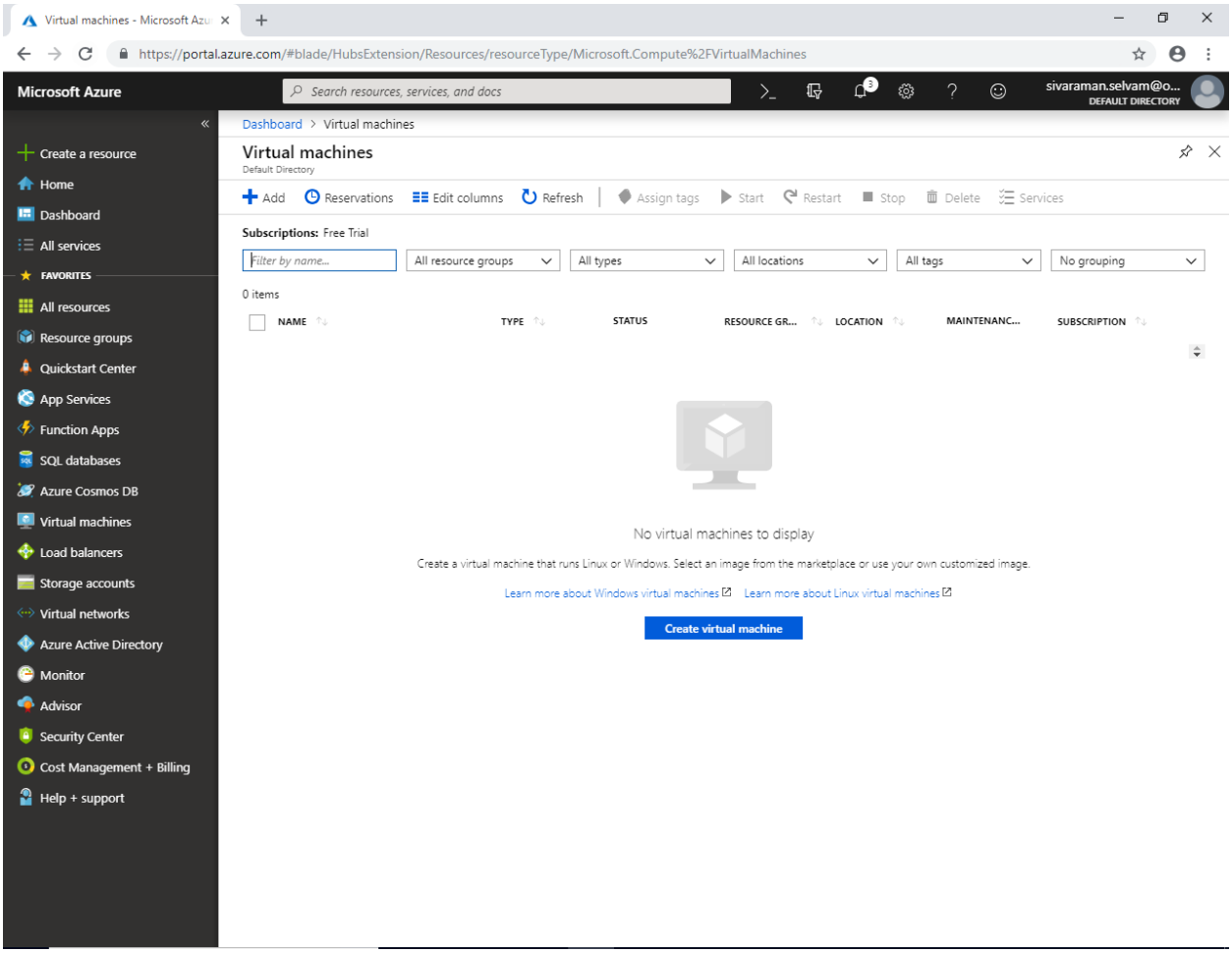
To view Virtual Network **"SANS-VNET"**



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



In **“Virtual machines”** click **“Add”**.



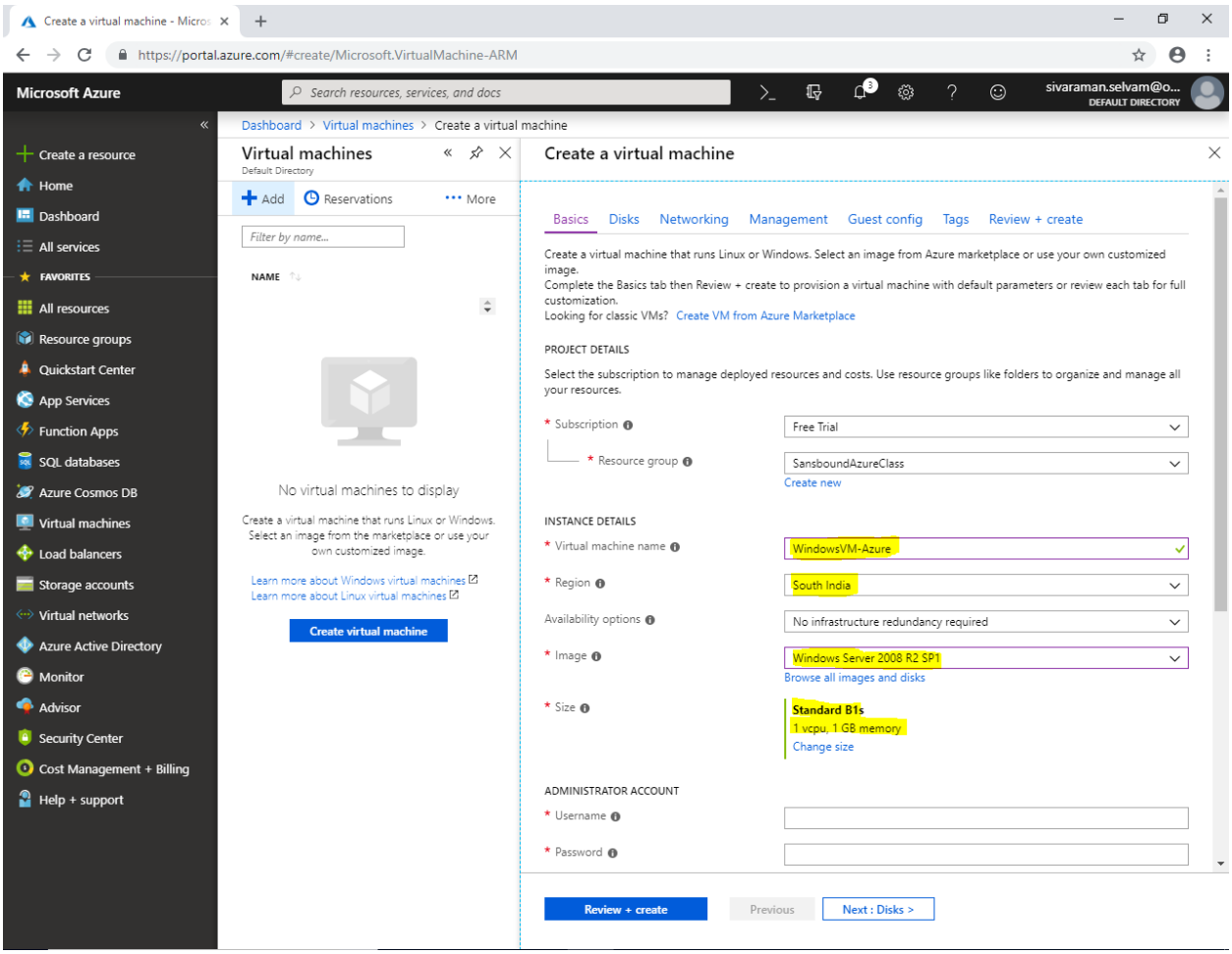
In **“Instance details”**

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

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

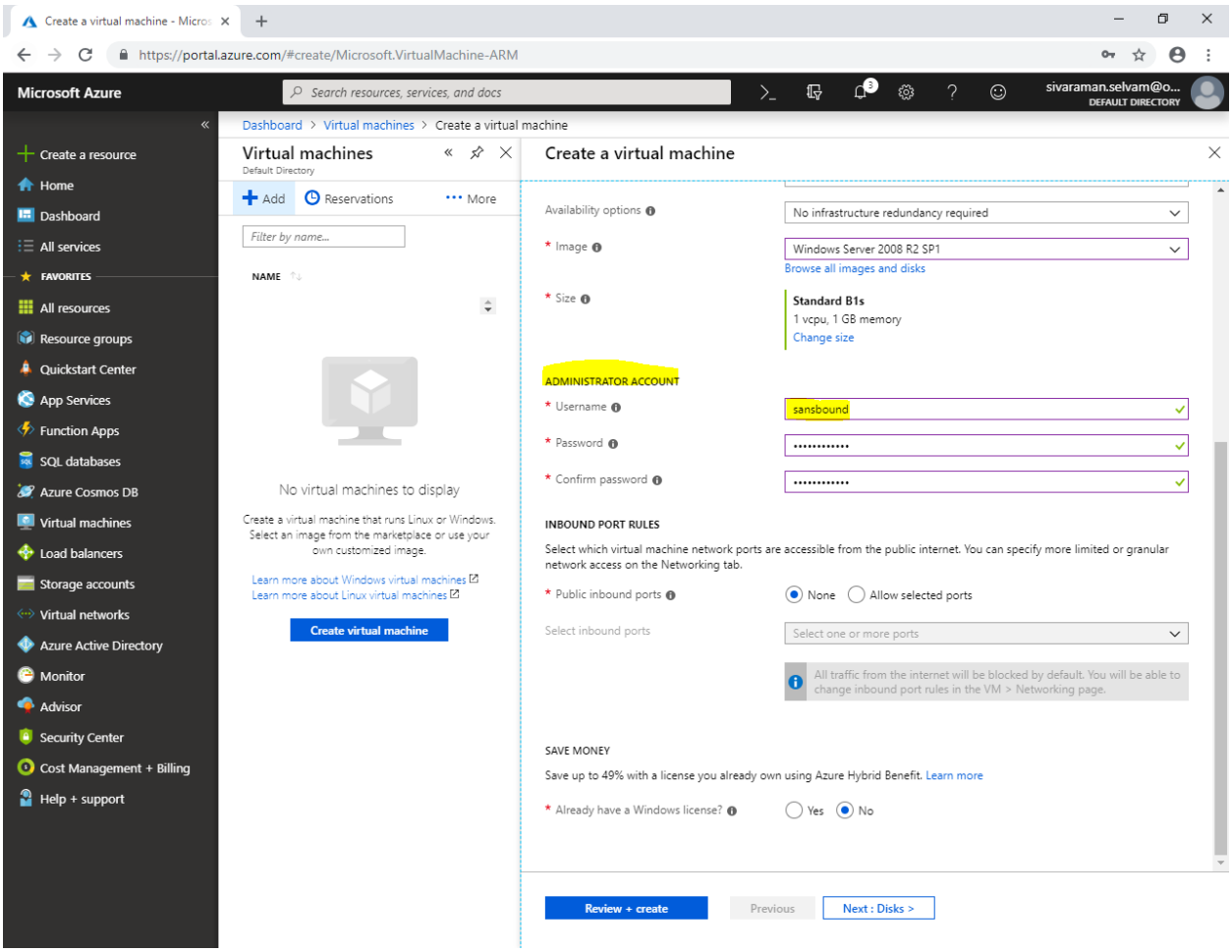
Select OS **“Image”** as **“Windows Server 2008 R2 SP1”**.

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



In **“Administrator Account”**.

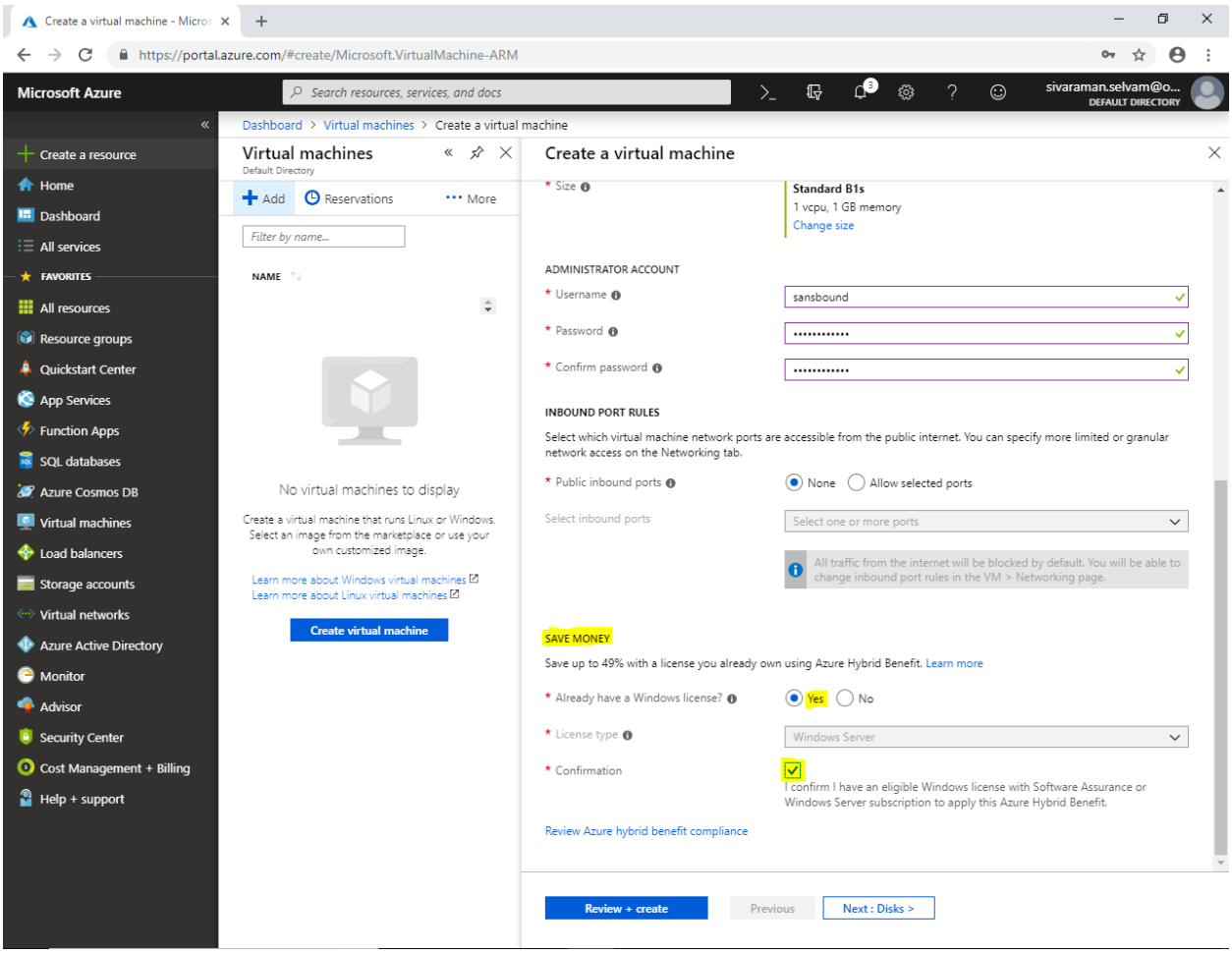
Type **“Username”** as **“sansbound”**.



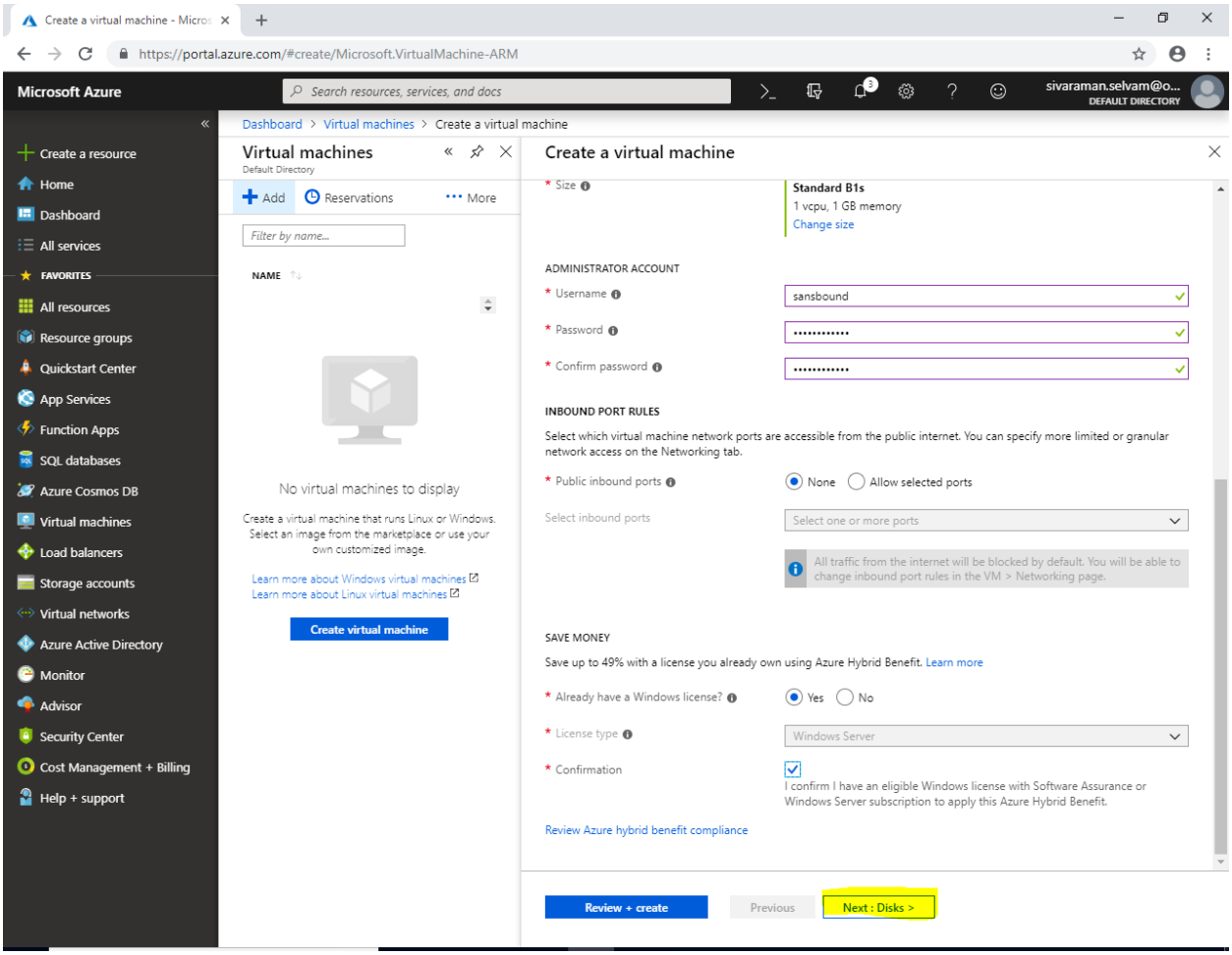
In **“Save Money”**

Click **“Yes”.**

Need to check **“Confirmation”** box.

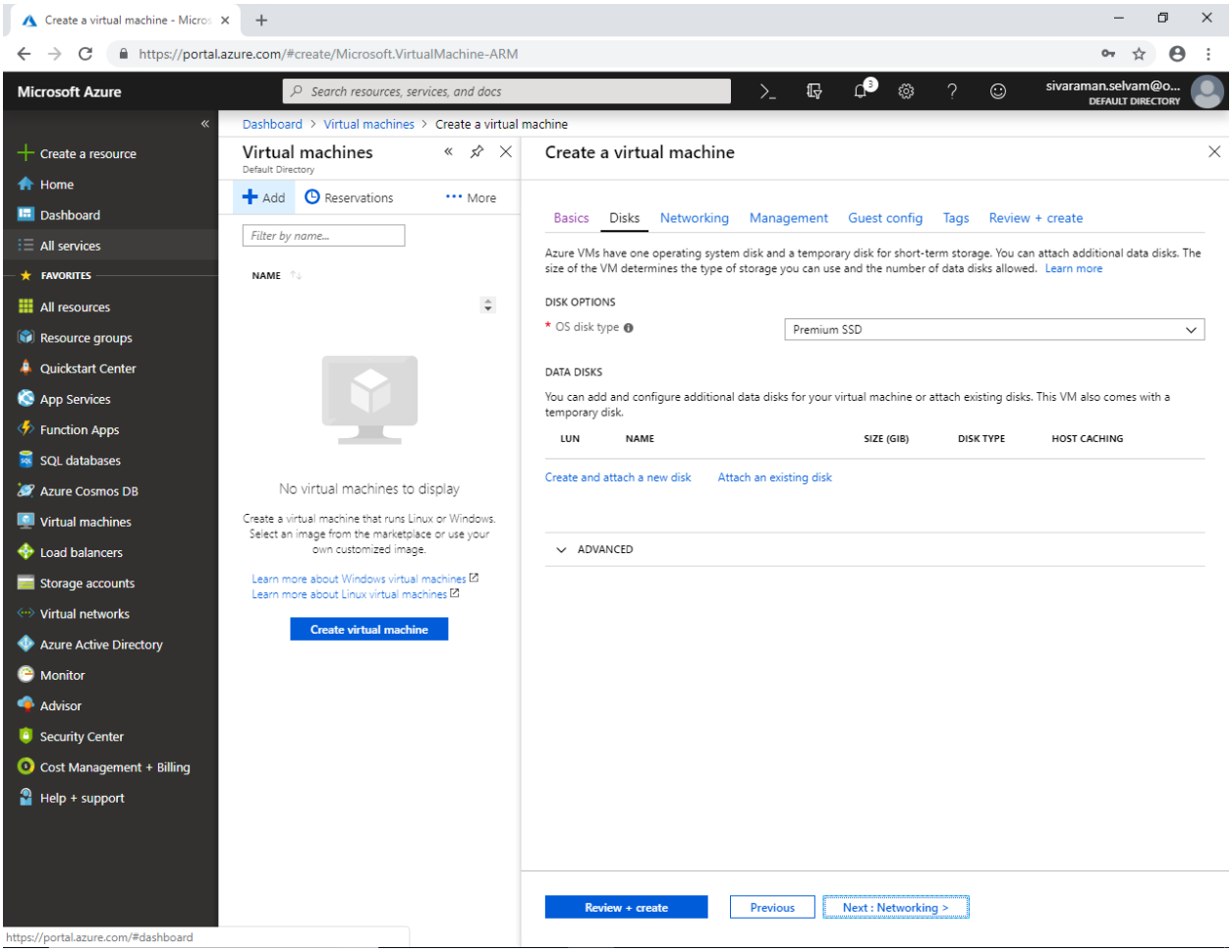


Click **“Next : Disks >”**.



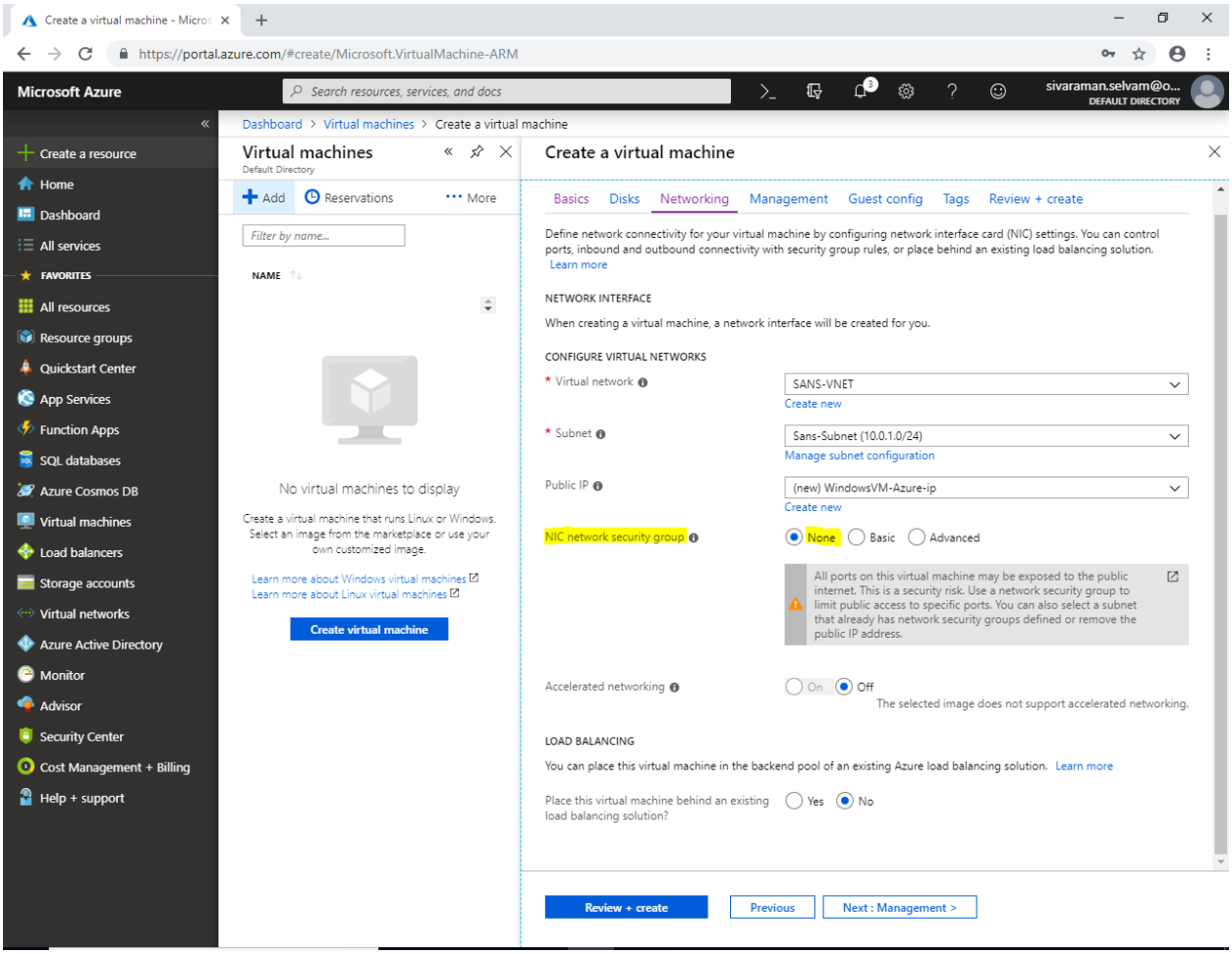
In “Disks”,

Leave default and click **“Next : Networking>”**.

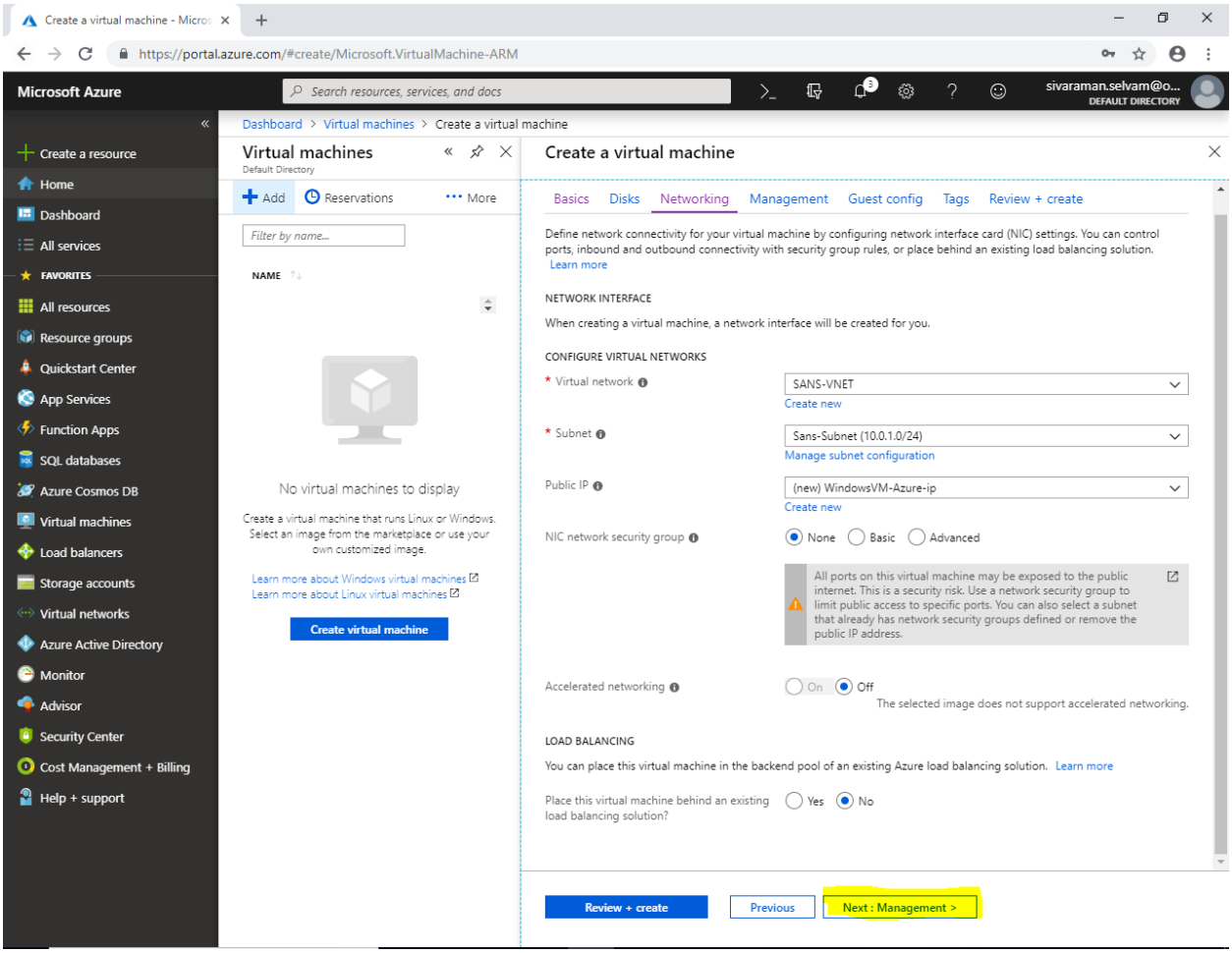


In **“Networking”**

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

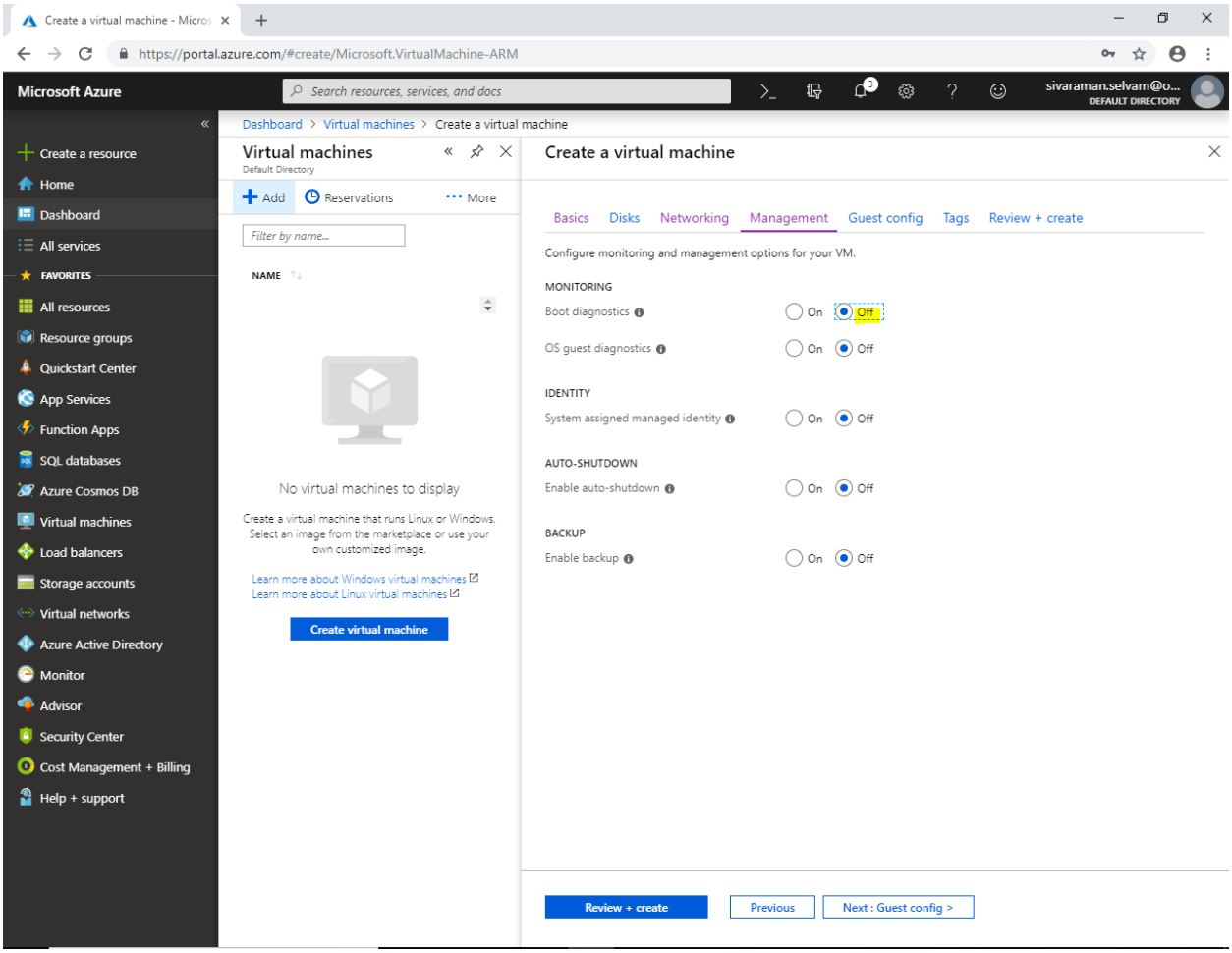


Click **“Next : Management>”**.

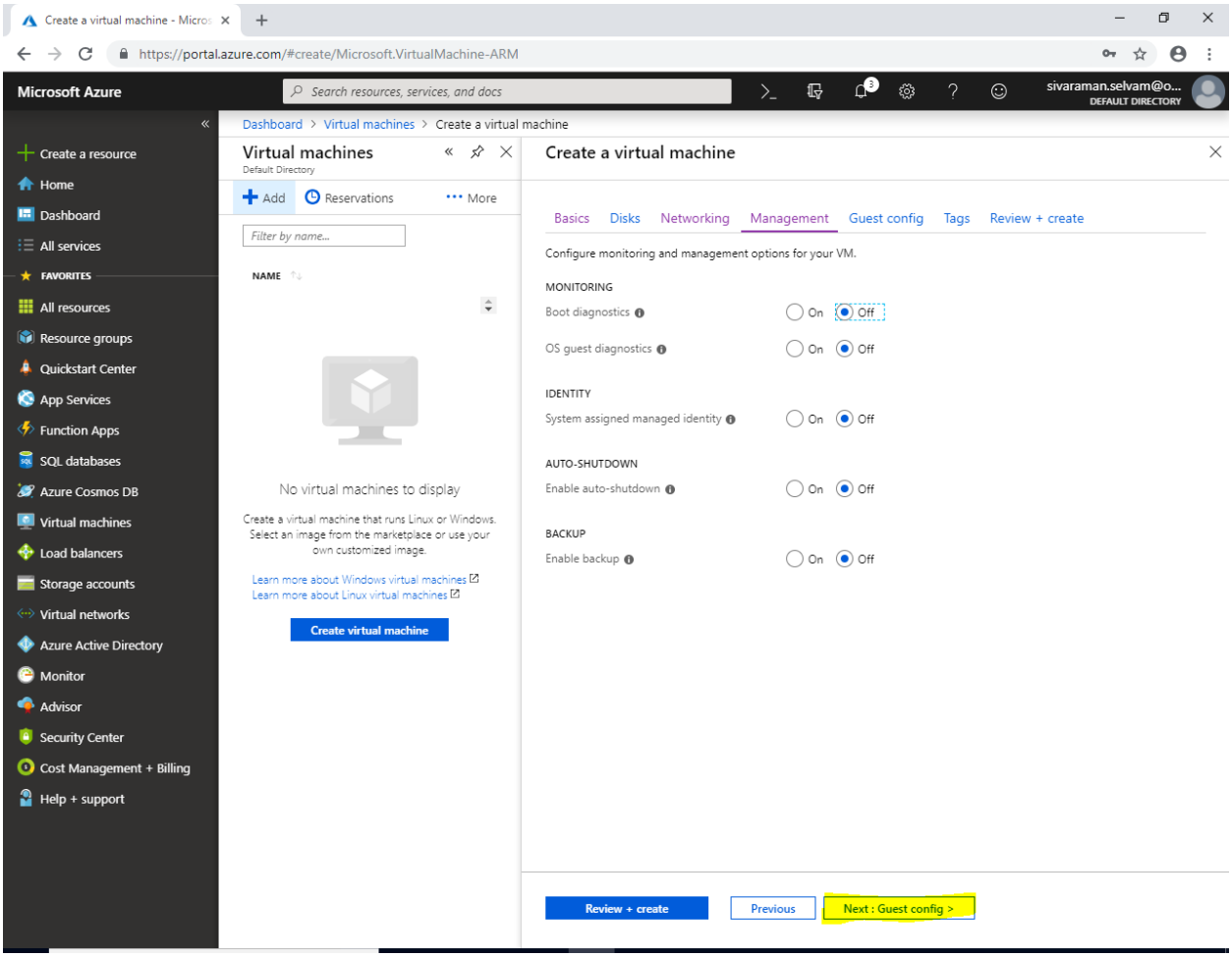


In “Management”.

Set **“Boot Diagnostics”** as **“Off”**.

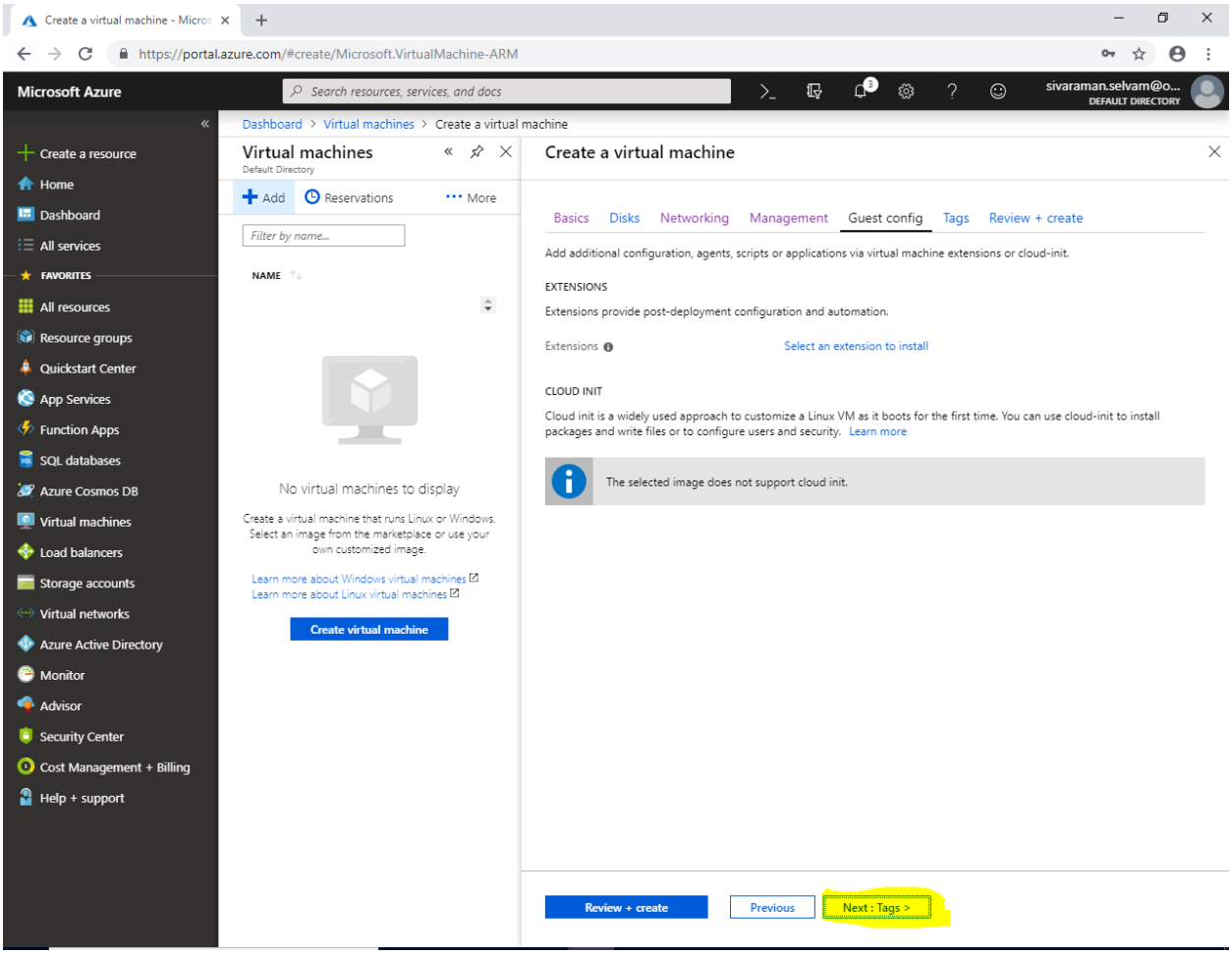


Click **“Next : Guest config>”**.



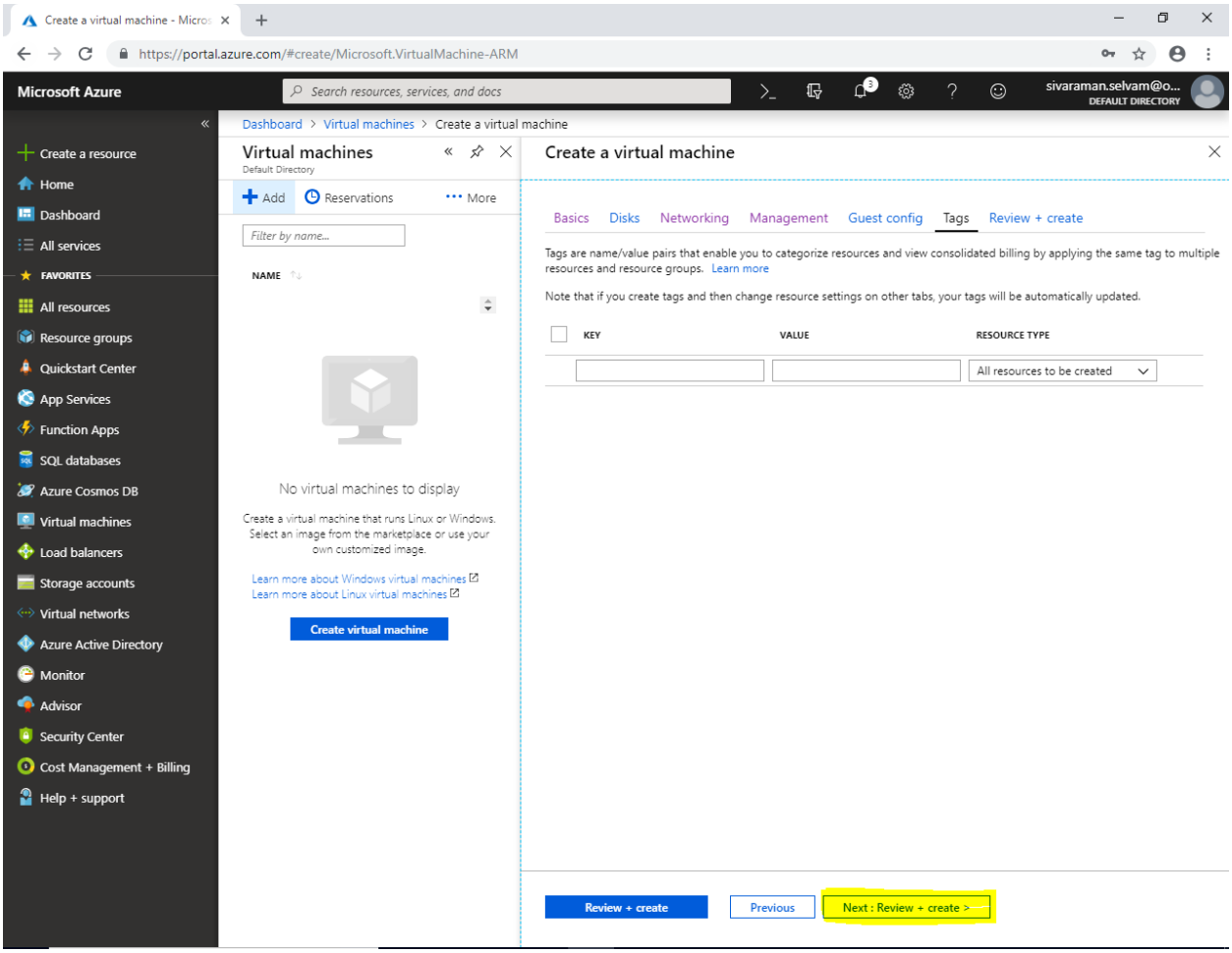
In **“Guest config”**

Click **“Next : Tags >”**.

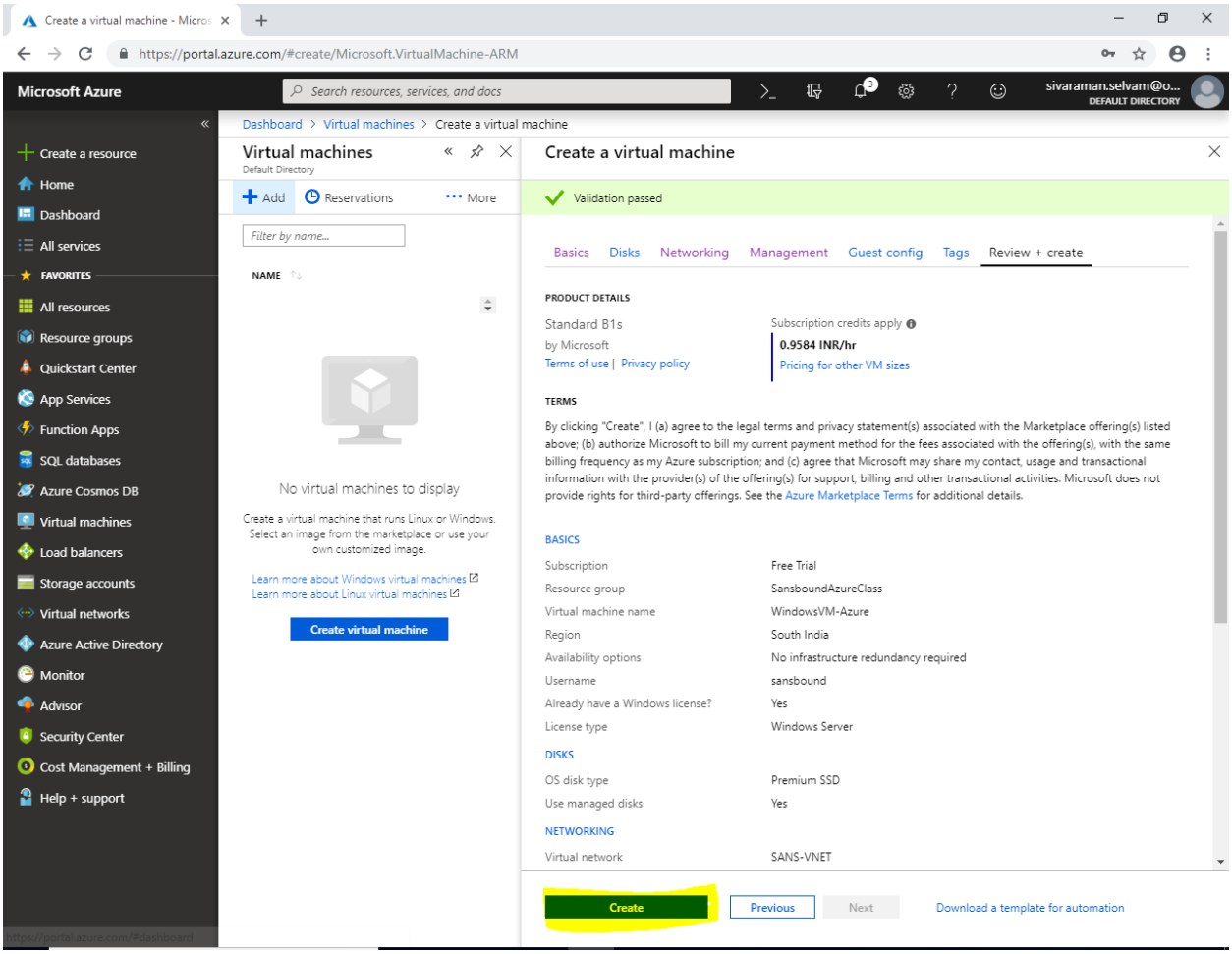


In **“Tags”**.

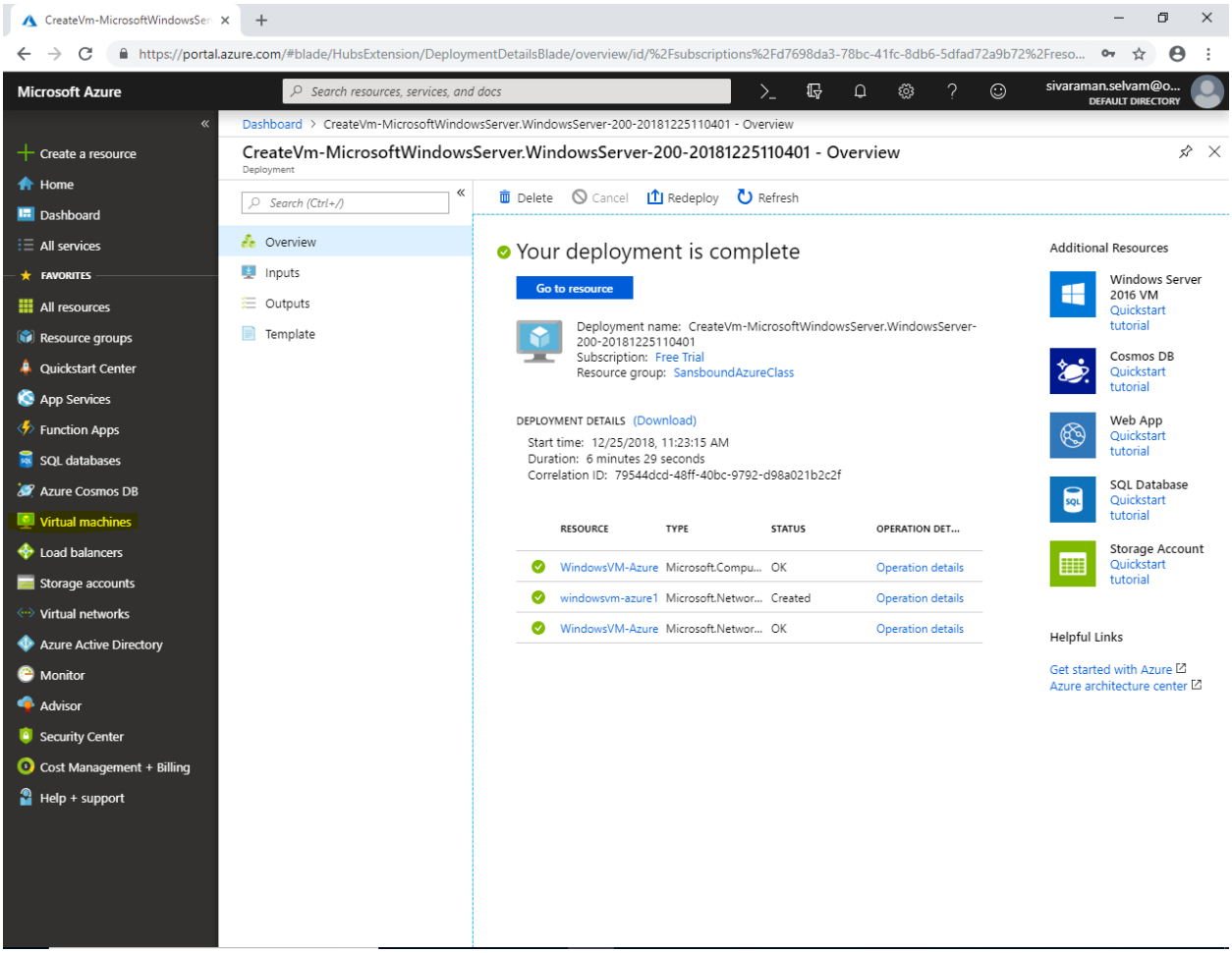
Click **“Next : Review + Create”**.



Click **"Create"**.

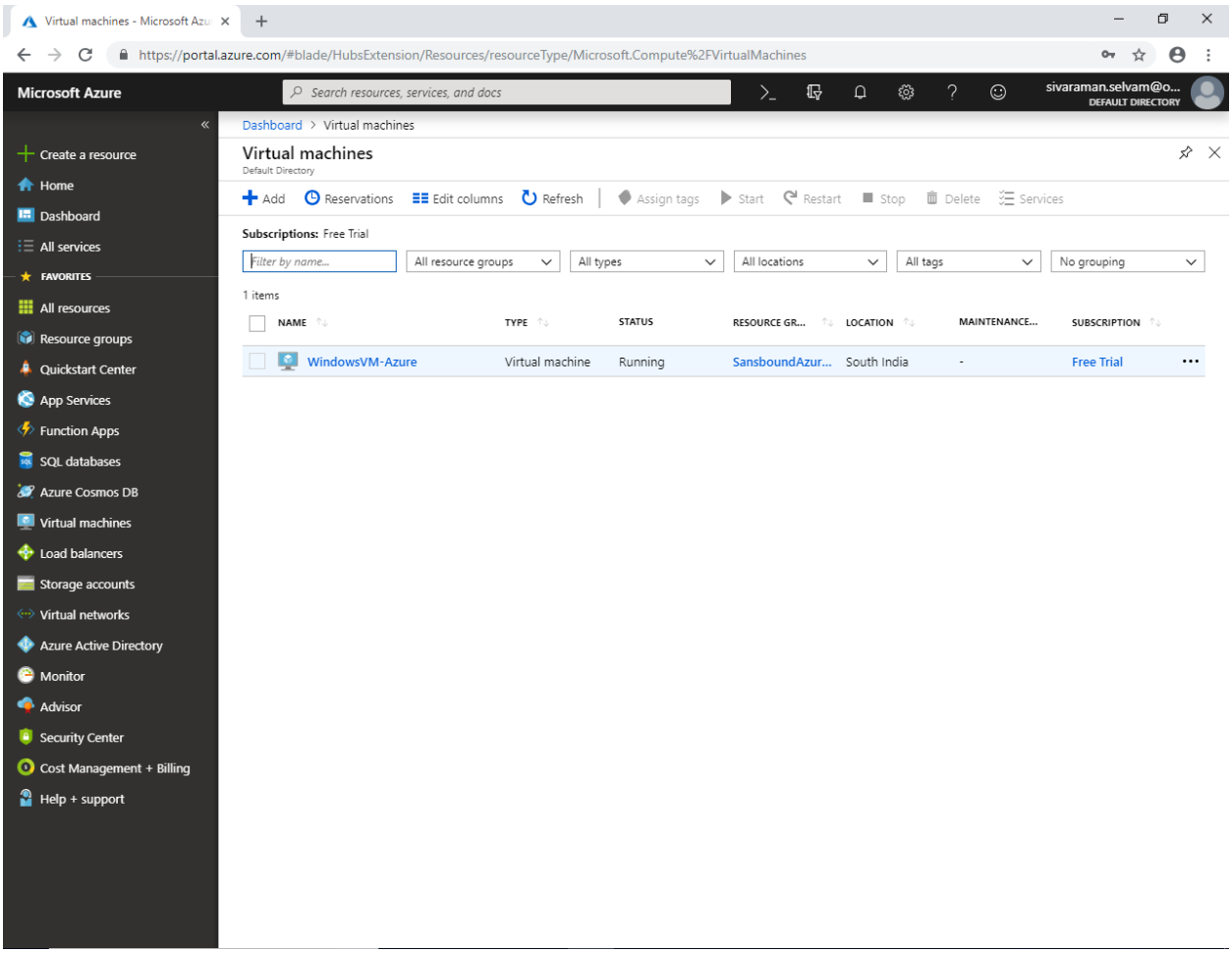


Once you have successfully deployed Virtual machine, then click **“Virtual machines”**.



In **“Virtual machines”**,

Click **“Add”** to create new virtual machine.



While creating Virtual machine,

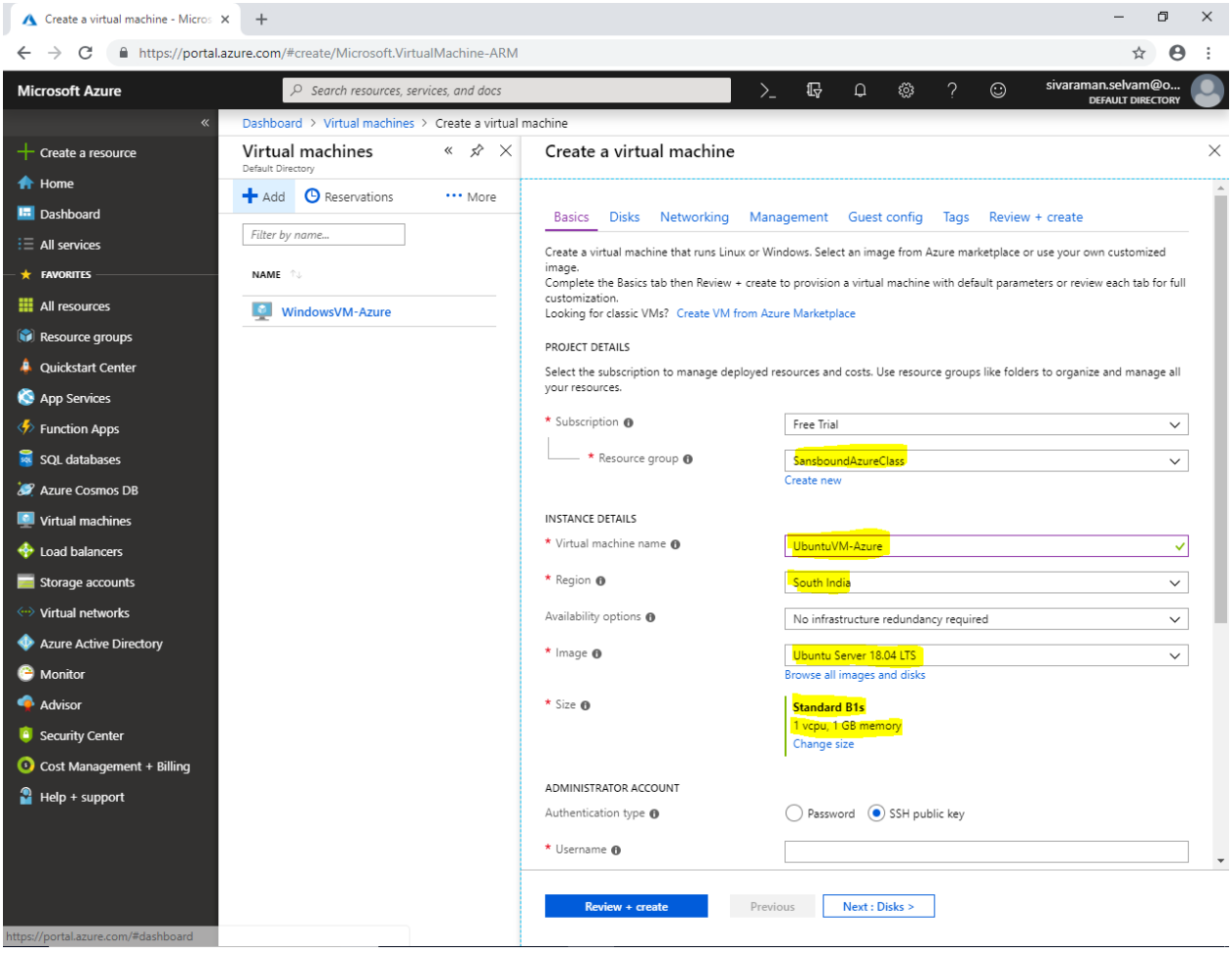
Select **“Resource Group”** as **“SansboundAzureClass”**.

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

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

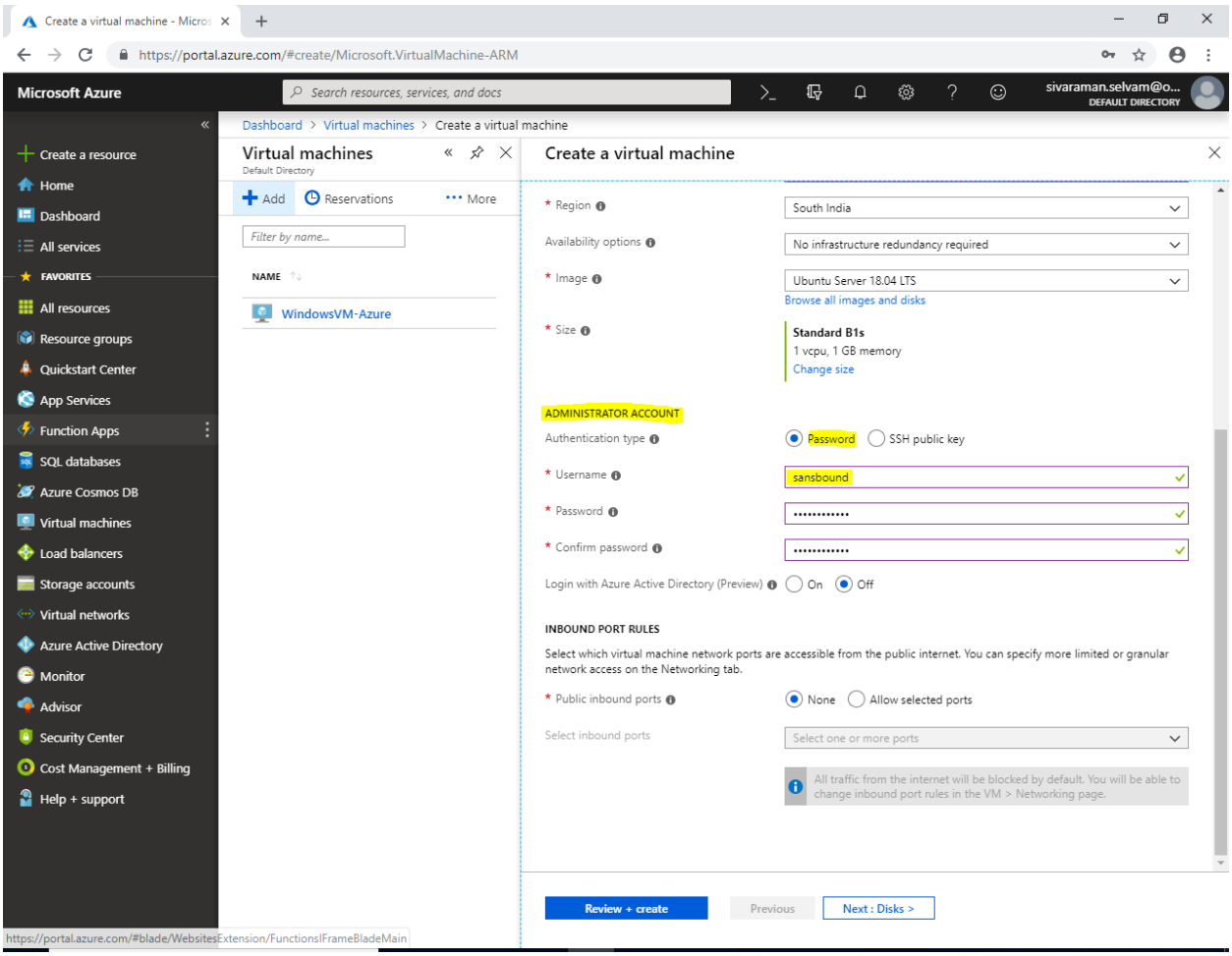
Select **“Image”** as **“Ubuntu Server 18.04 LTS”**.

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

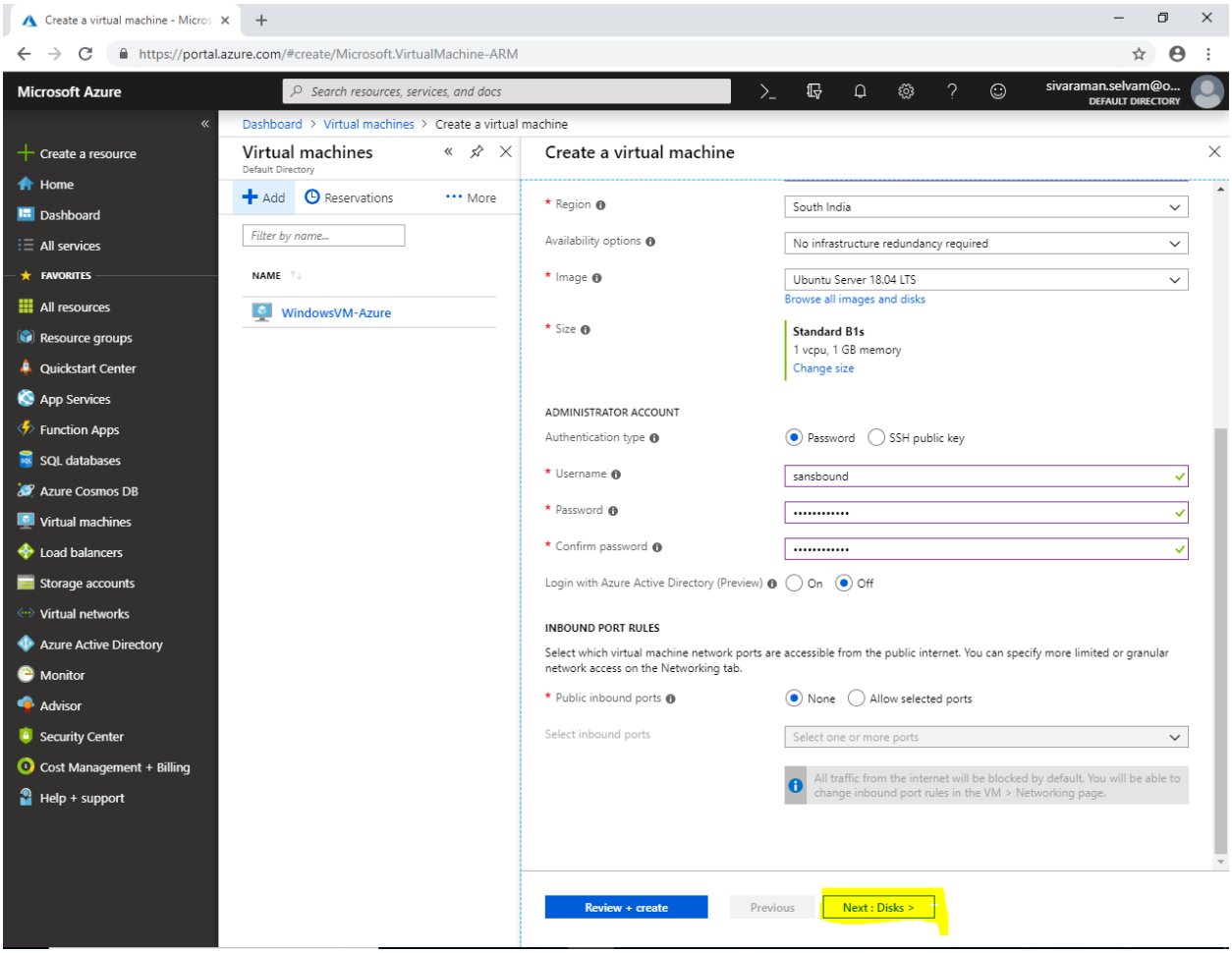


In **“Administrator Account”** set authentication type as **“Password”**.

Type **“Username”** as **“sansbound”**.

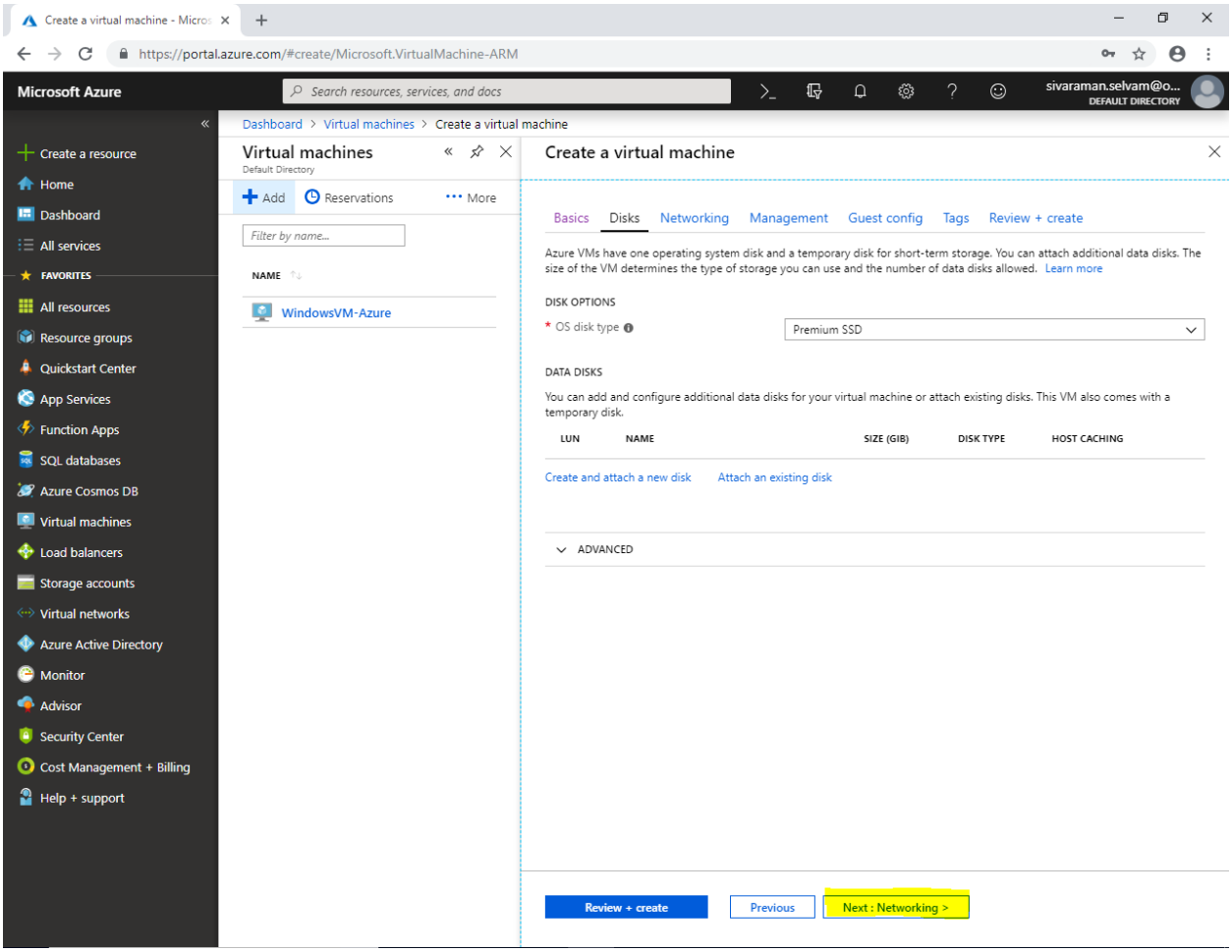


Click **“Next : Disks>”**.



In **“Disks”**

Click **“Next : Networking >”**.

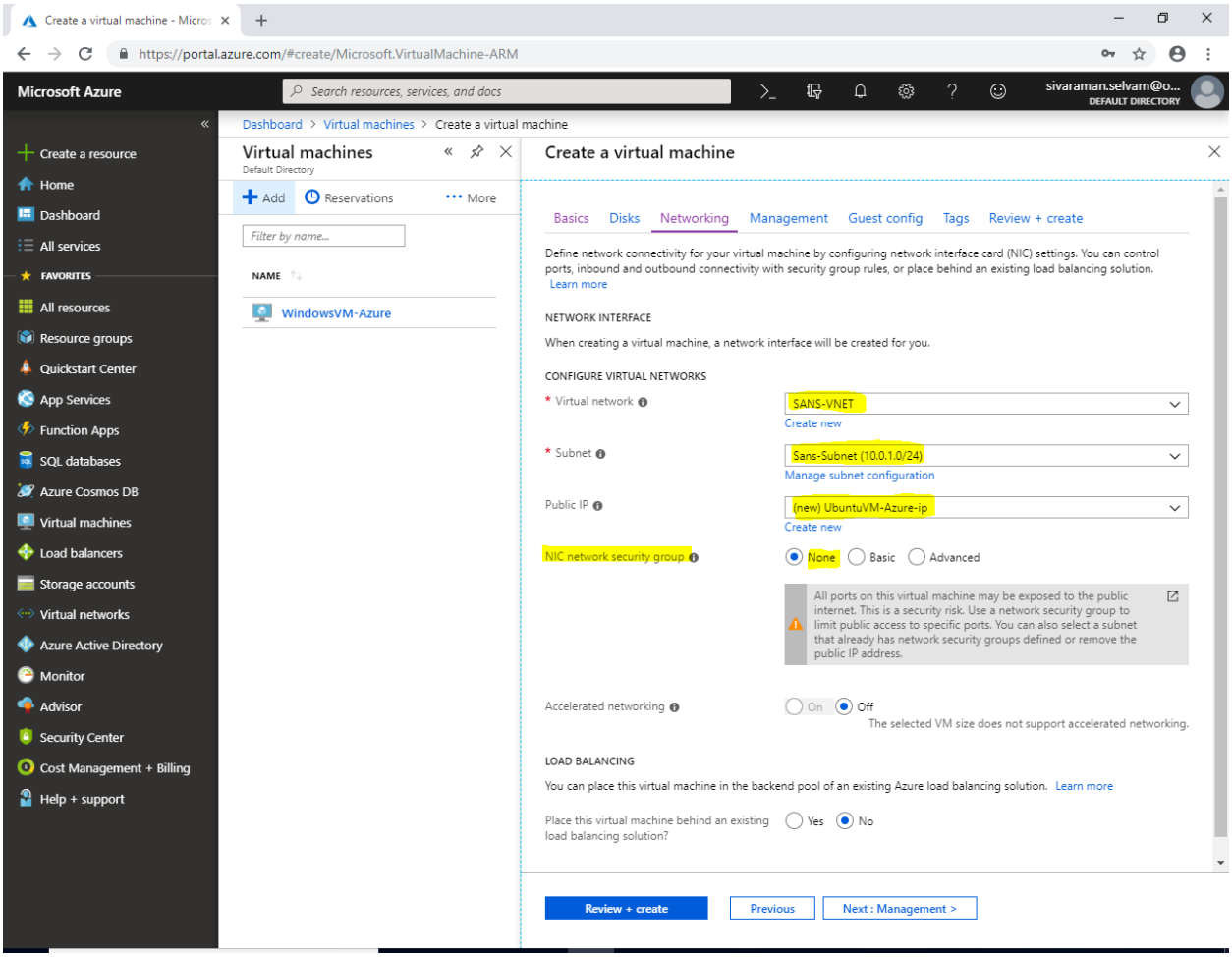


Ensure that Virtual network as **"SANS-VNET"**.

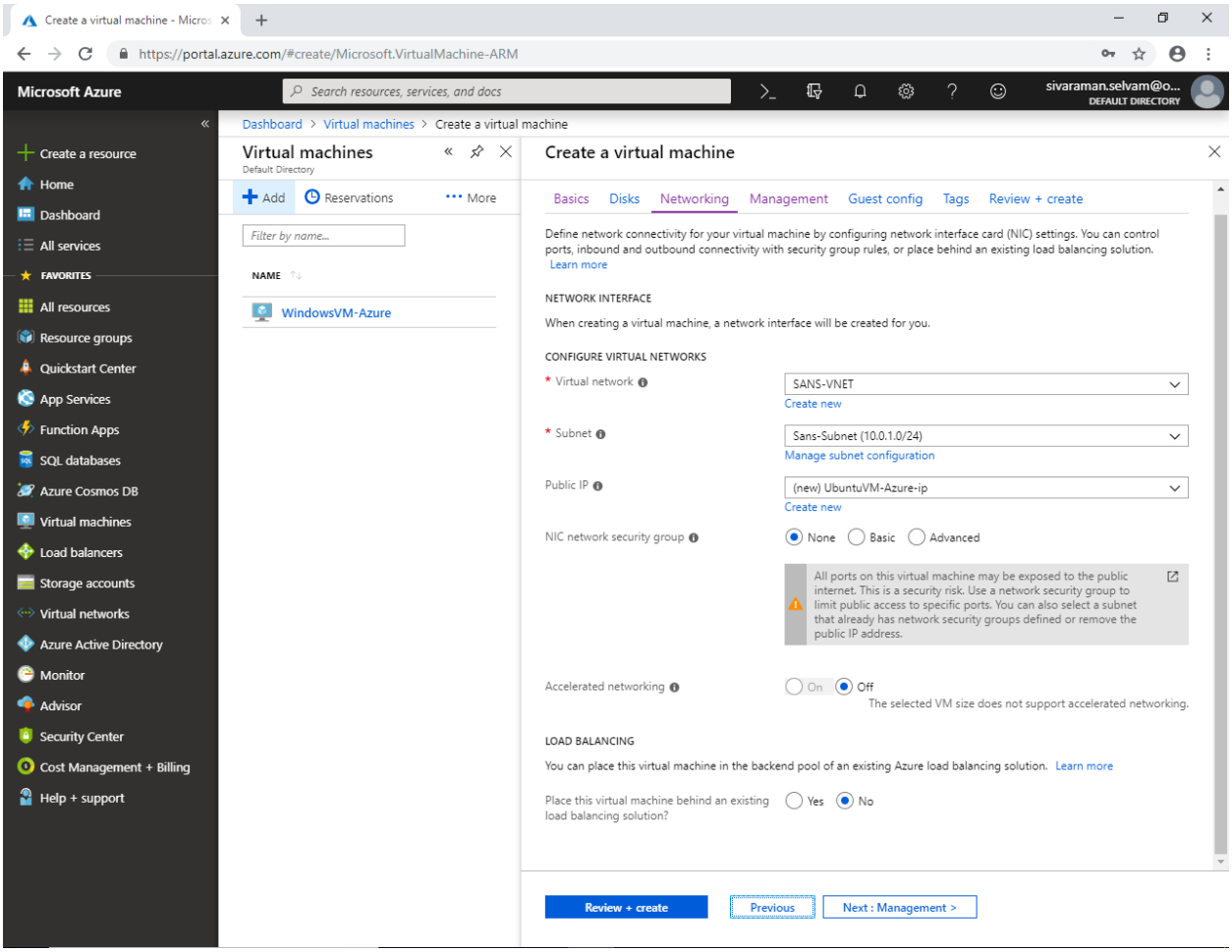
Subnet **"Sans-Subnet"**.

Public IP as new IP for Ubuntu VM

In Network Security Group click as **"None"**.

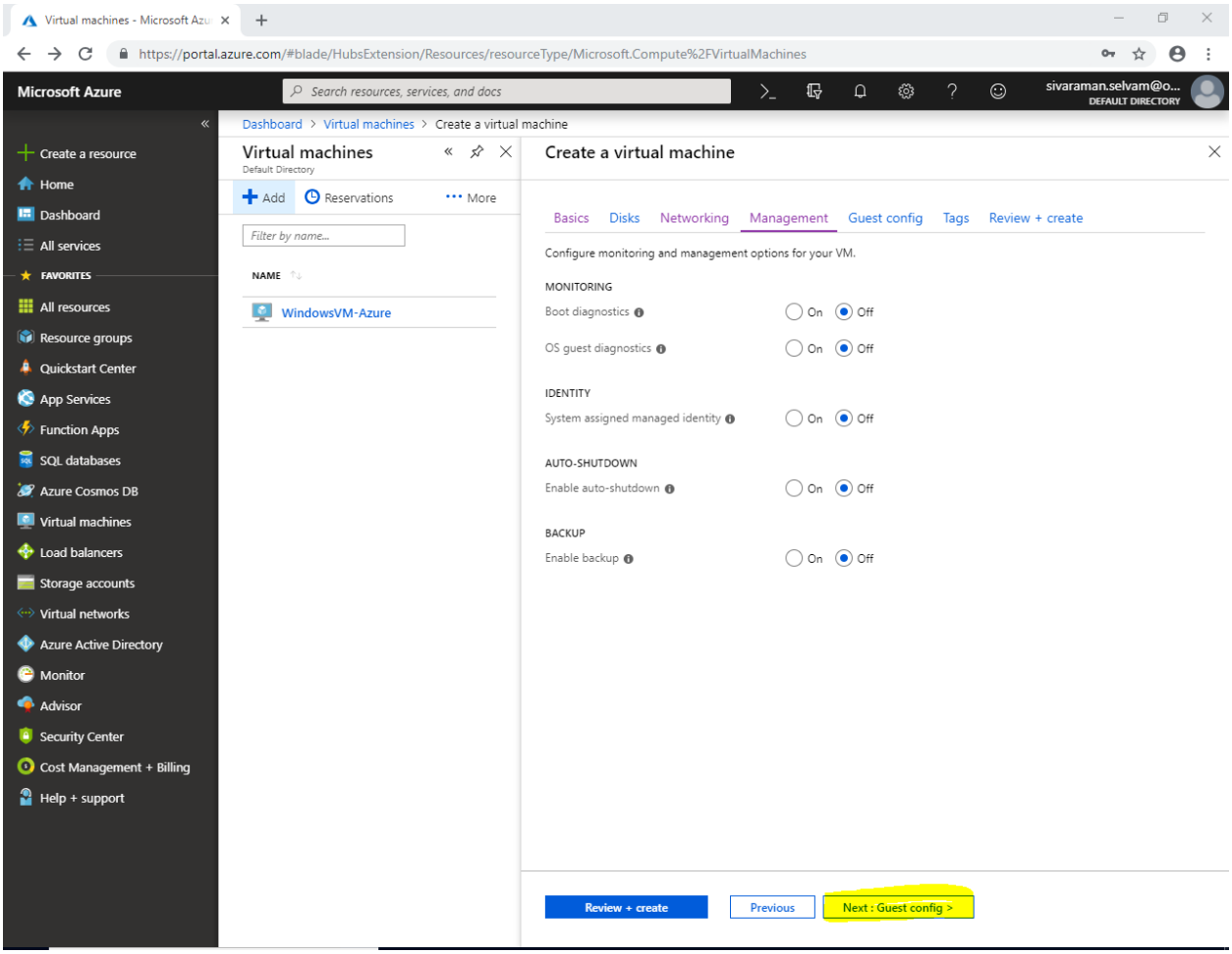


Click **“Next : Management>”**.



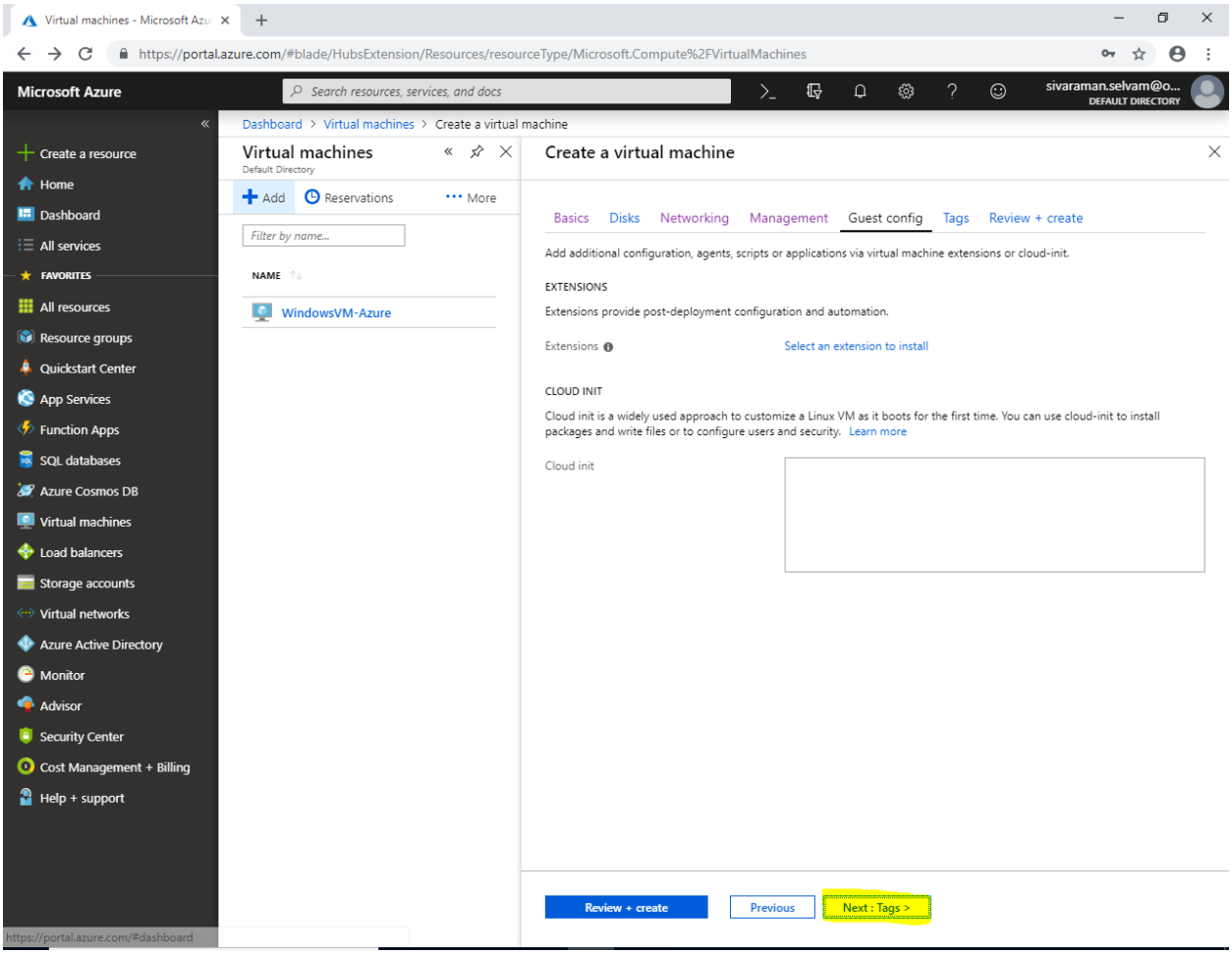
In **“Management”**

Click **“Next : Guest config >”**.



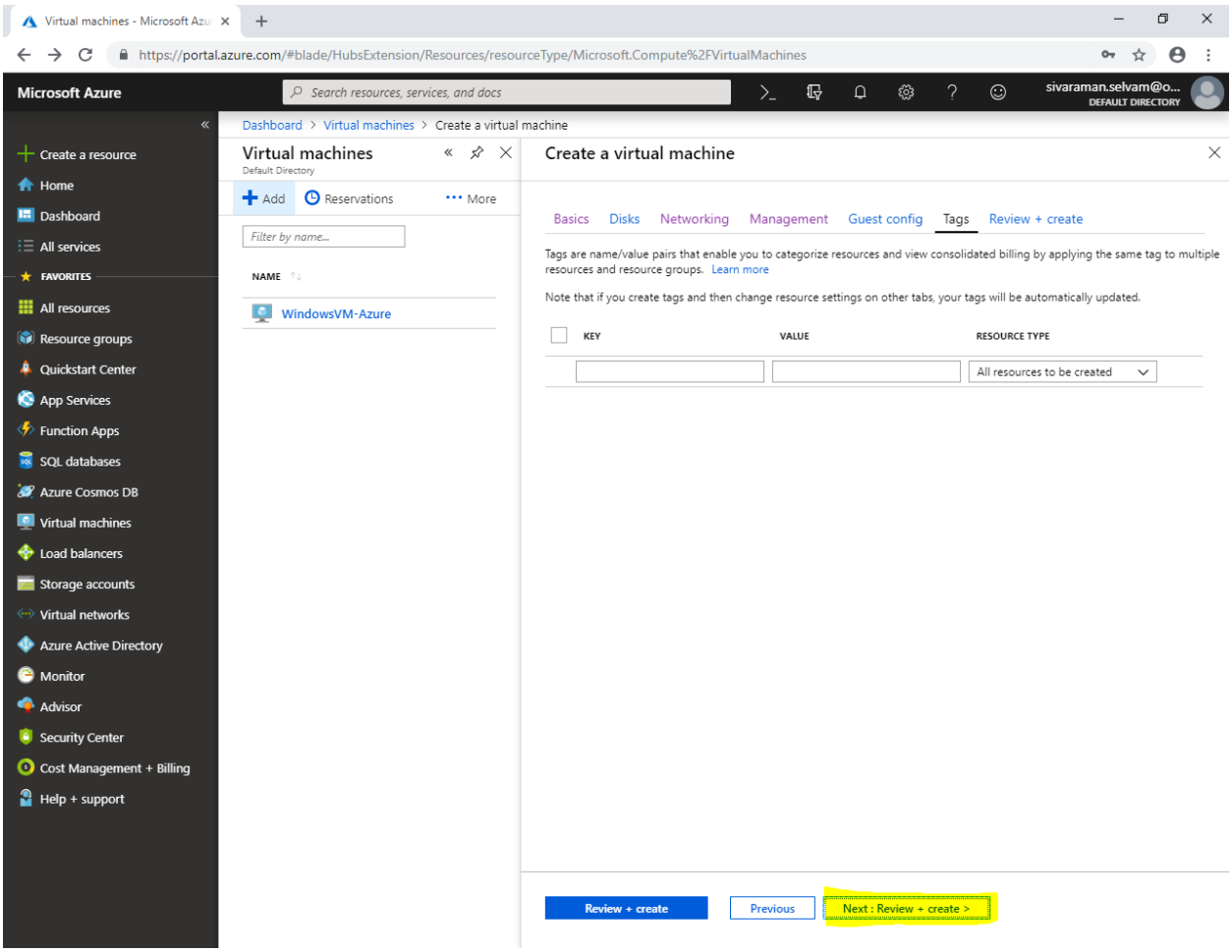
In “Guest config”.

Click **“Next : Tags>”**.

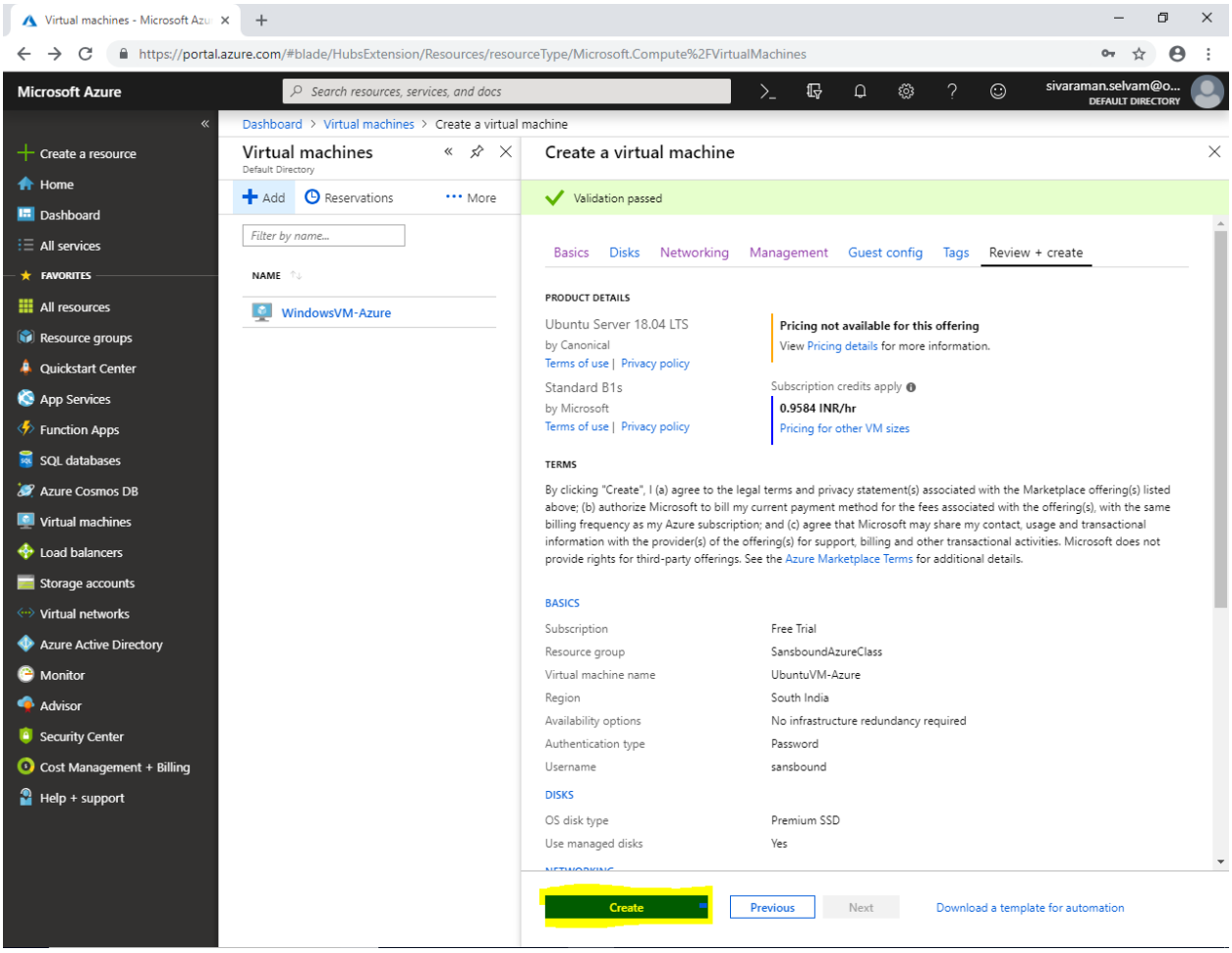


Click “Tags”.

Click **“Next : Review + Create>”**.

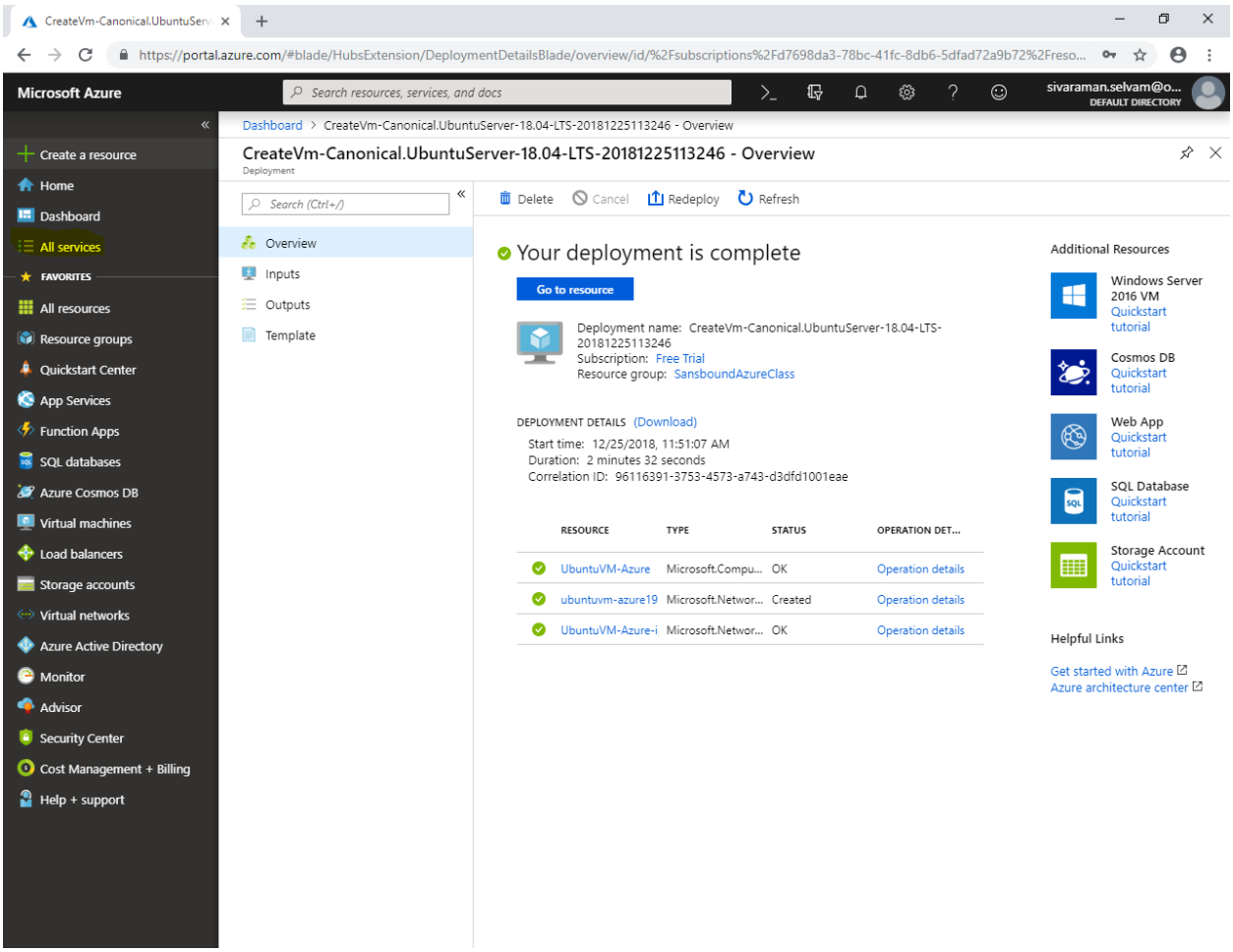


Click **"Create"**.

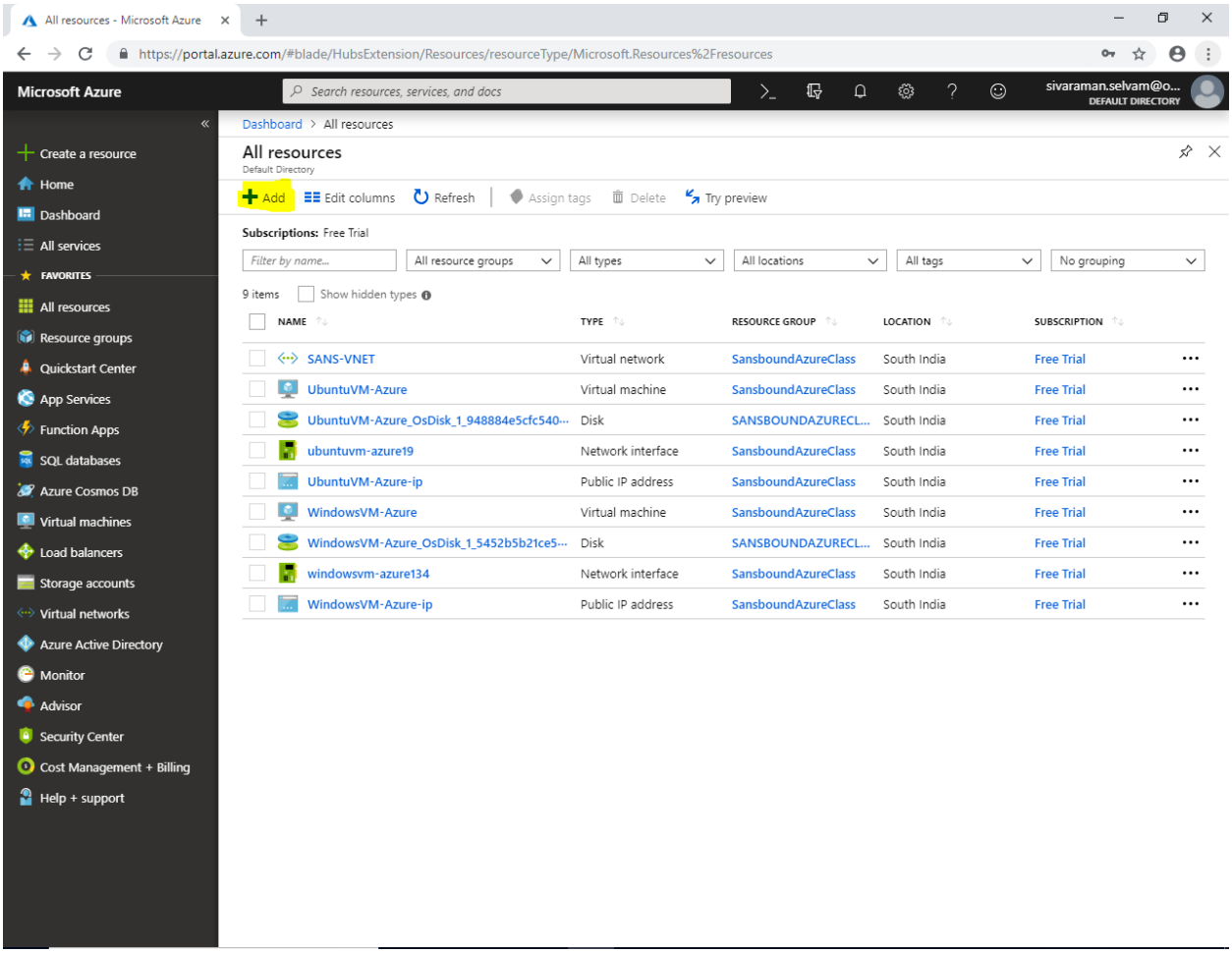


You have successfully deployed.

Click **“All Services”** in left side panel of Azure portal.

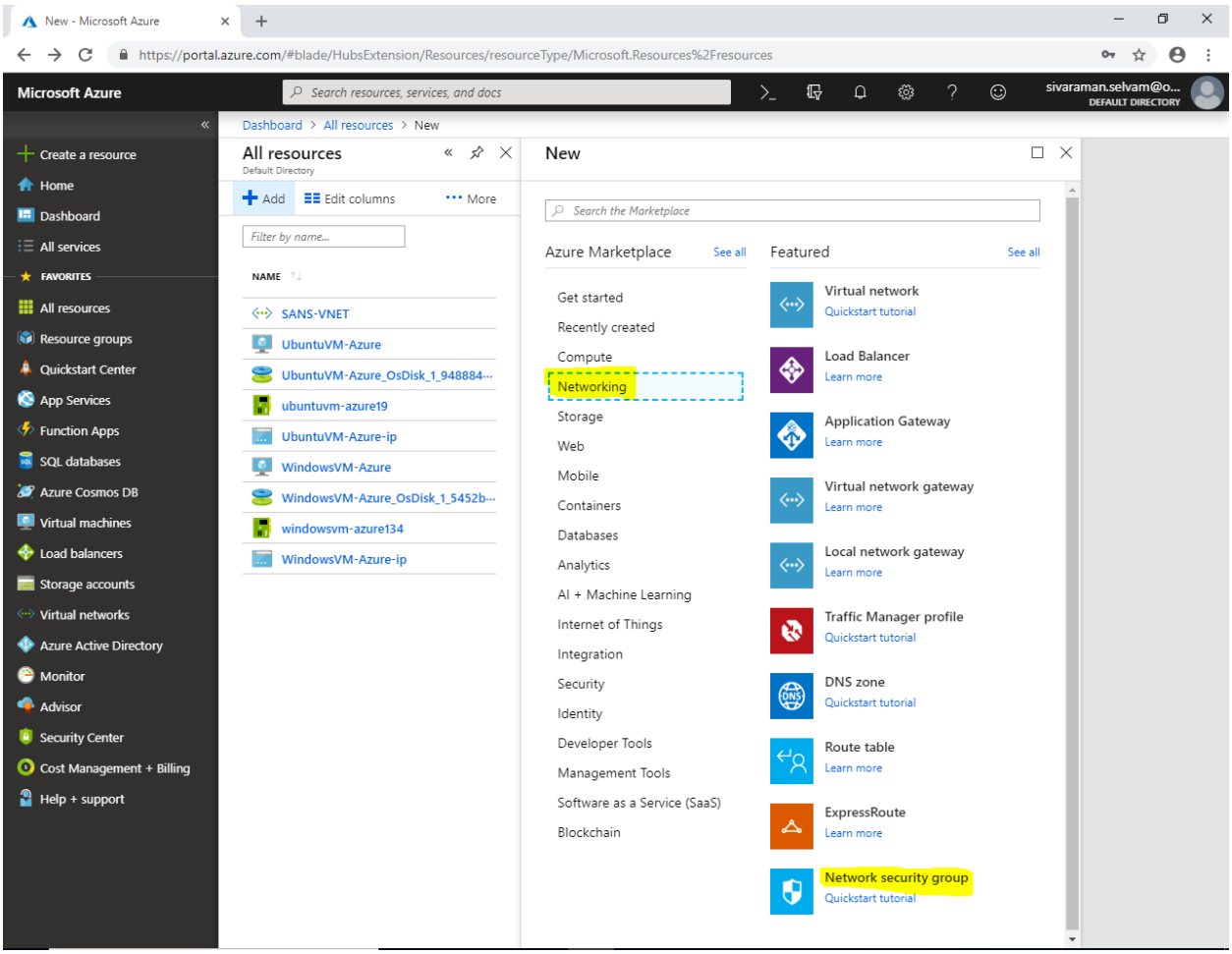


In **“All resources”** click **“Add”**.



In **“Azure Marketplace”**

Click **“Networking”** → **“Network Security Group”**

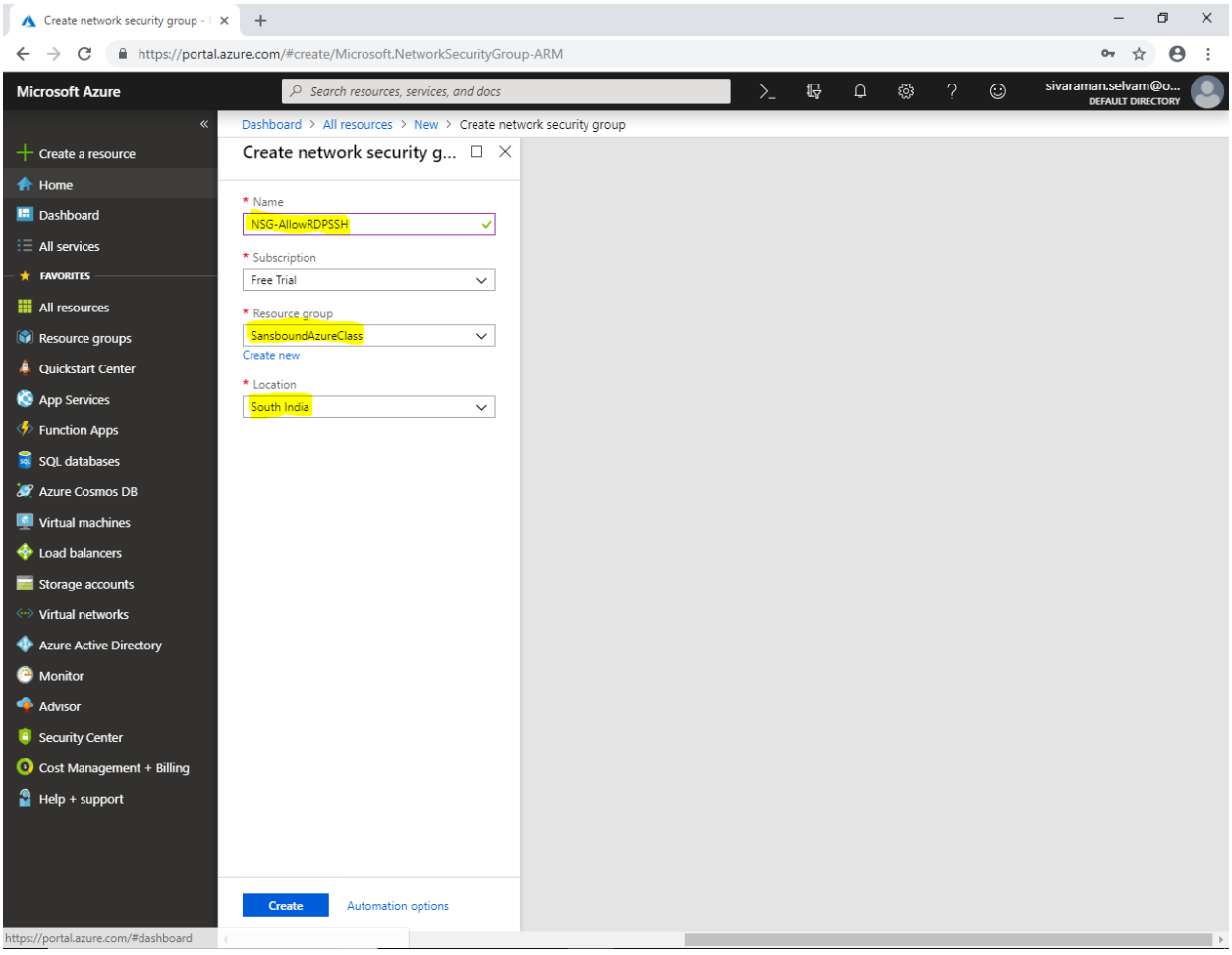


While creating **“Network Security Group”**

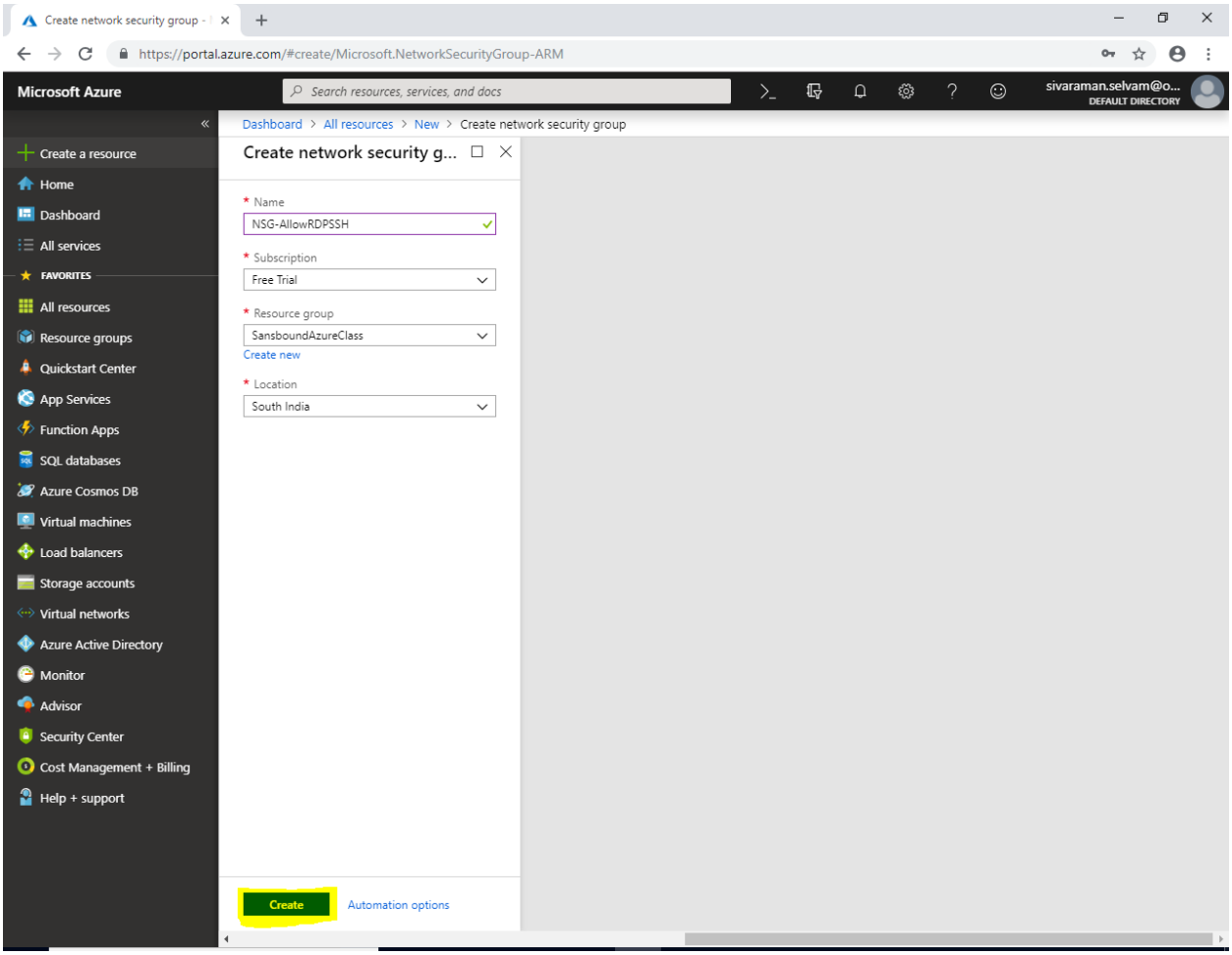
Type **“Network Security Group”** name as **“NSG-AllowRDPSSH”**.

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

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



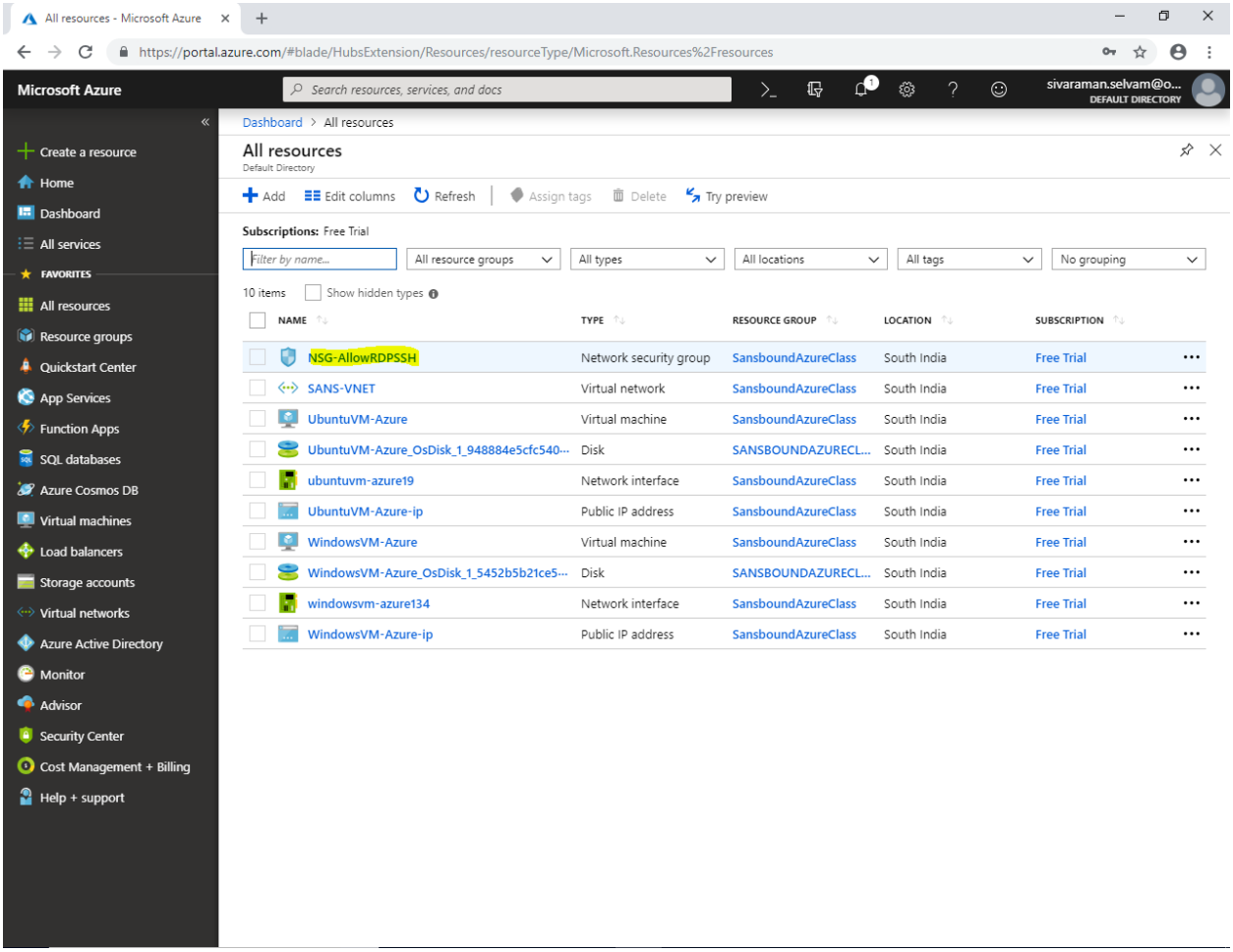
Click **"Create"**.



In **“All resources”**.

You are able to see the Network Security group.

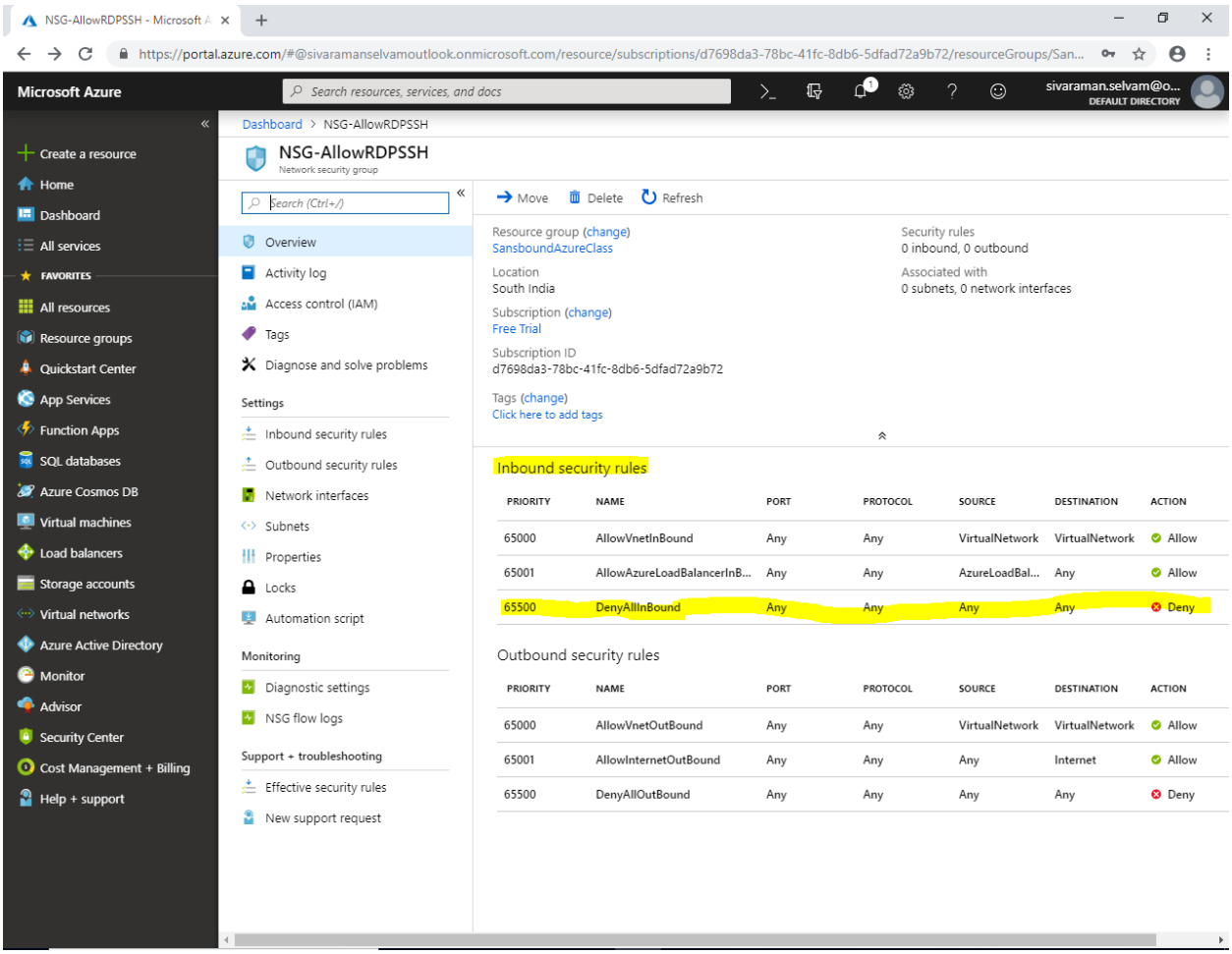
Click **“NSG-AllowRDPSSH”**.



In **“NSG-AllowRDPSSH”** network security group.

In **“Inbound security rules”** is a rule which allows user specified traffic from public network.

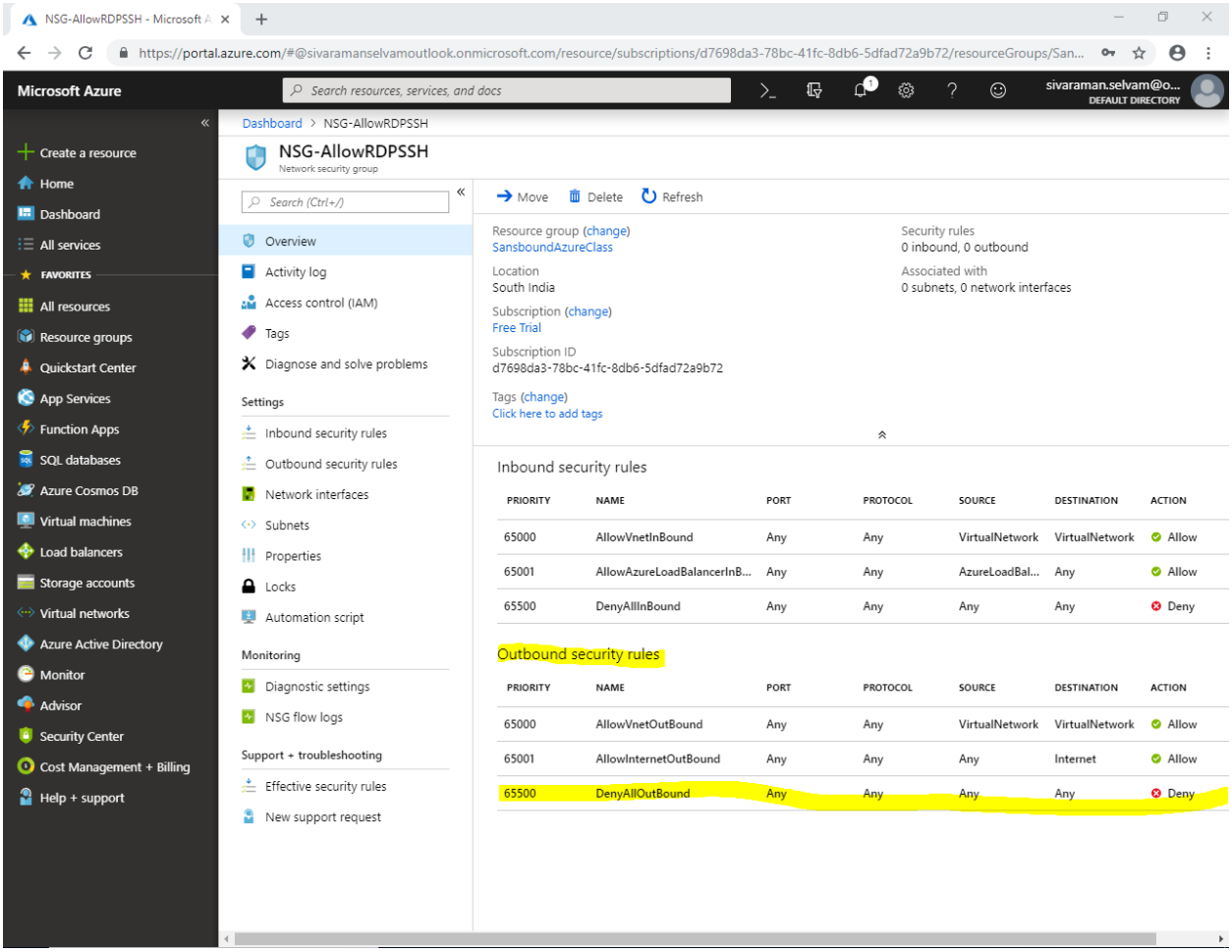
By default, it will deny all inbound traffic.



In **“Outbound Security rules”**

In “Outbound security rules” is a rule which allows user specified traffic from internal network of Azure (Private) to public network for access internet.

By default, it will deny all outbound traffic except Internet access and VNet outbound traffic.

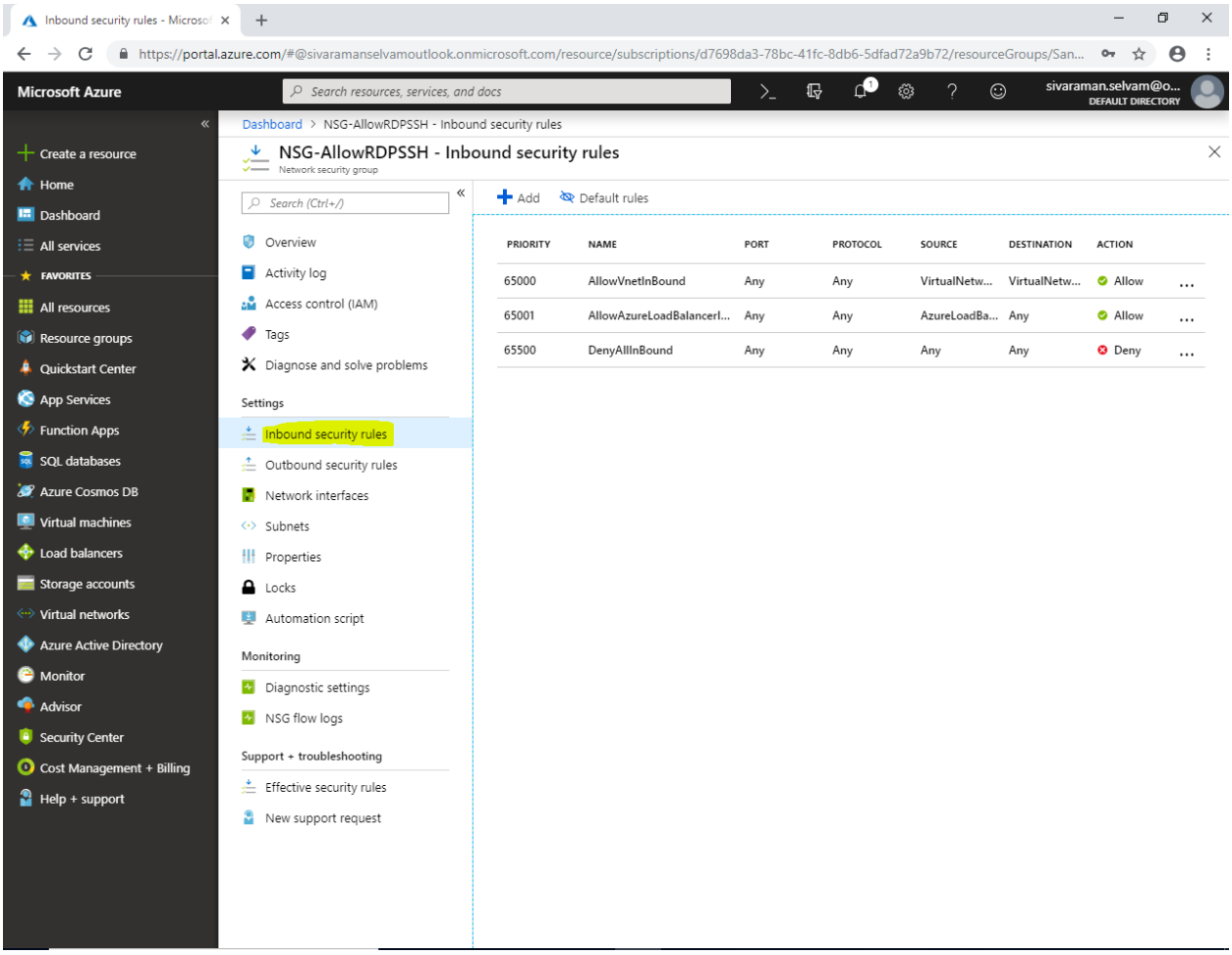


In **“Network Security Group”**

Click **“Inbound security rules”**.

Click **“Add”**.

I have required to create rules for **allow RDP (3389) and SSH (22) Ports** for this Network security group.



While creating inbound security rule

Source : Any

Source port ranges : *

Destination : Any

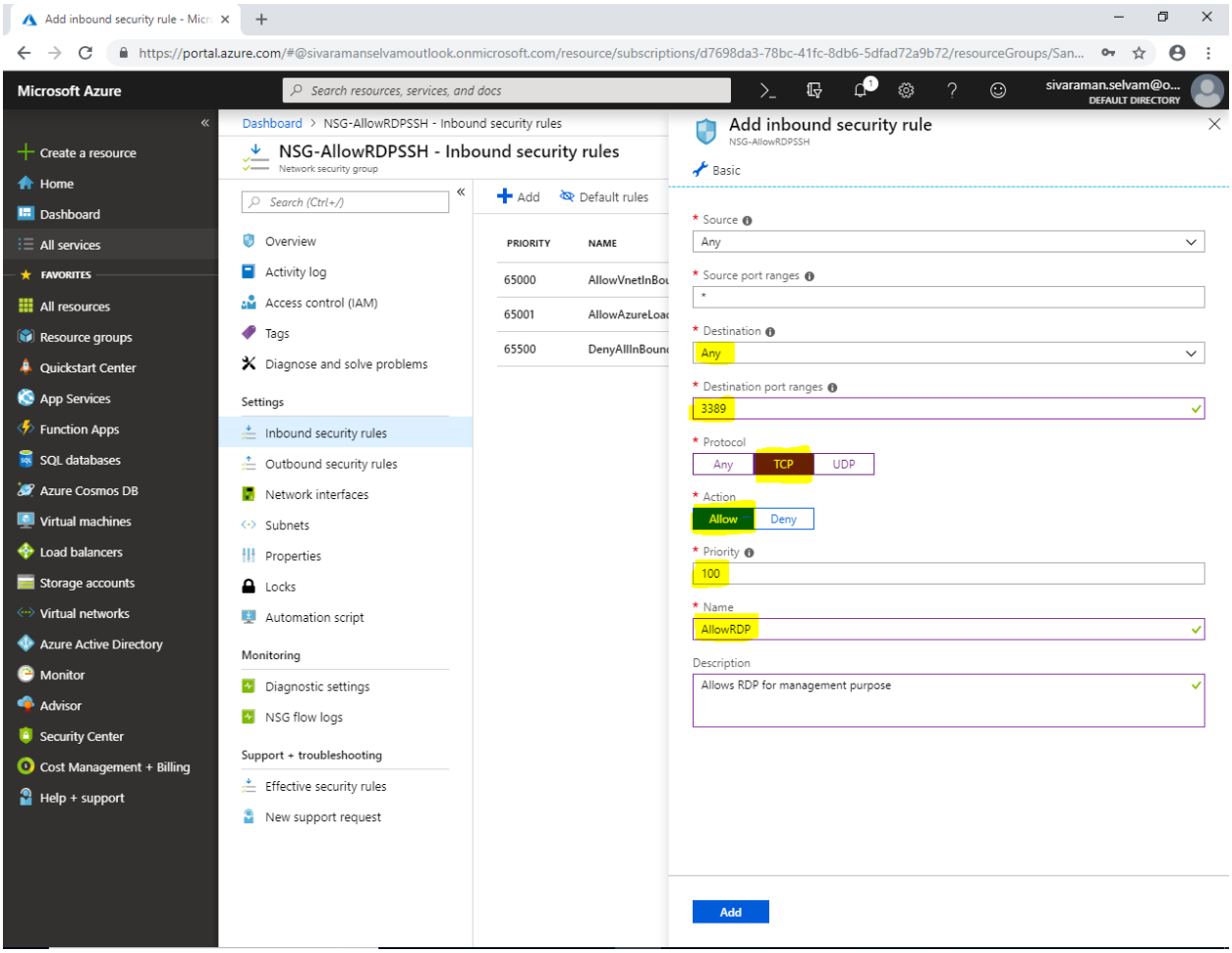
Destination port ranges : 3389

Protocol : TCP

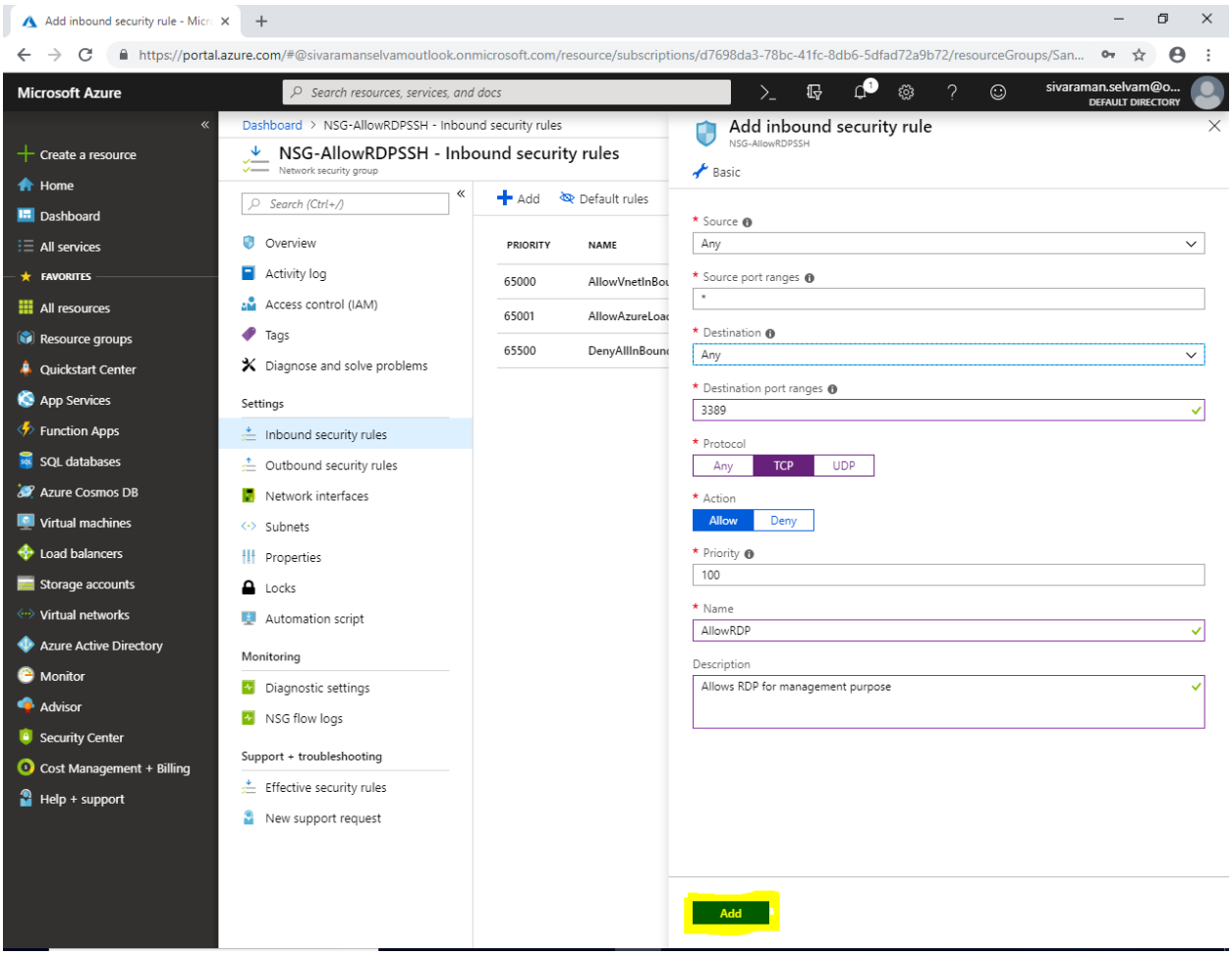
Action : Allow

Priority : 100

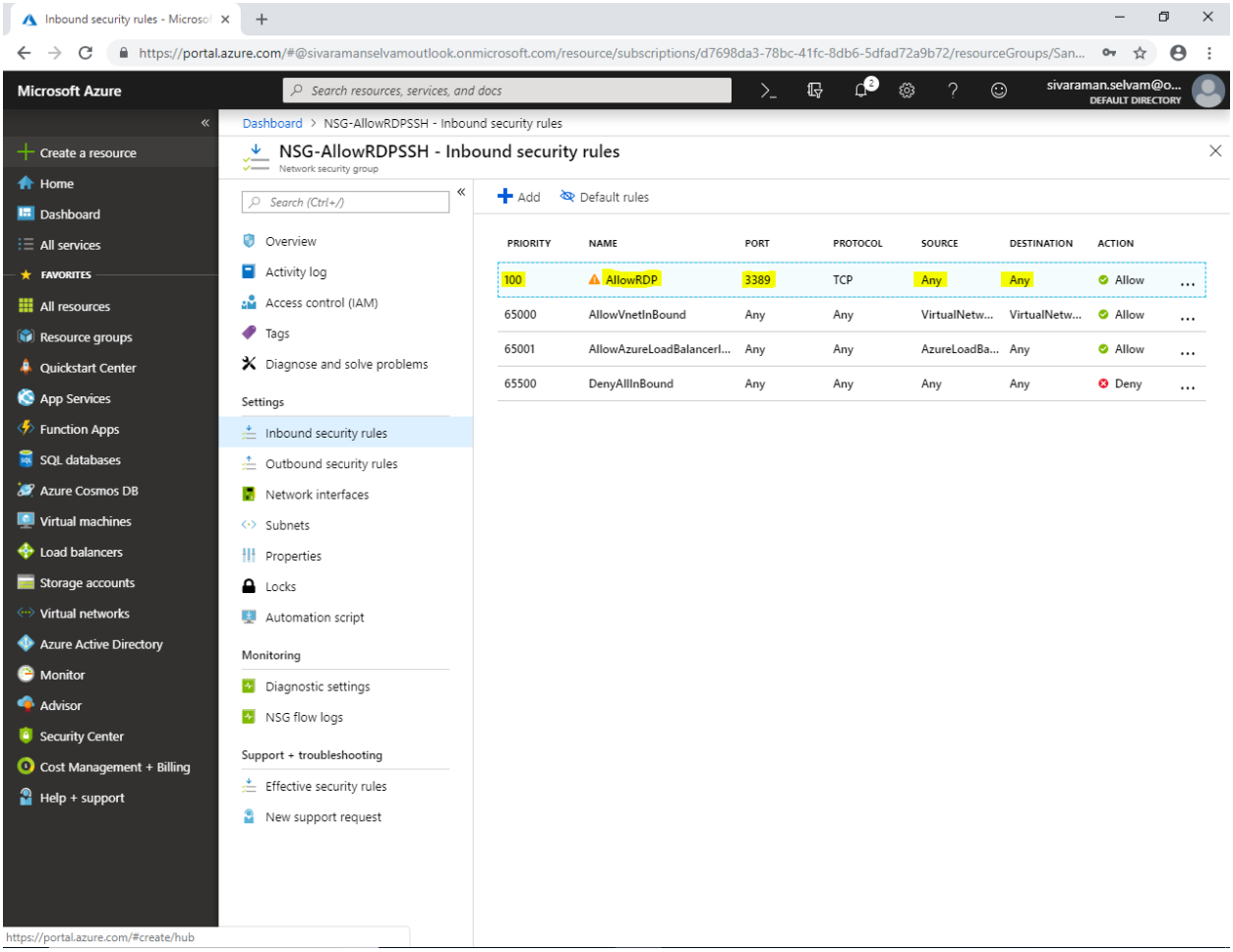
Name : AllowRDP :



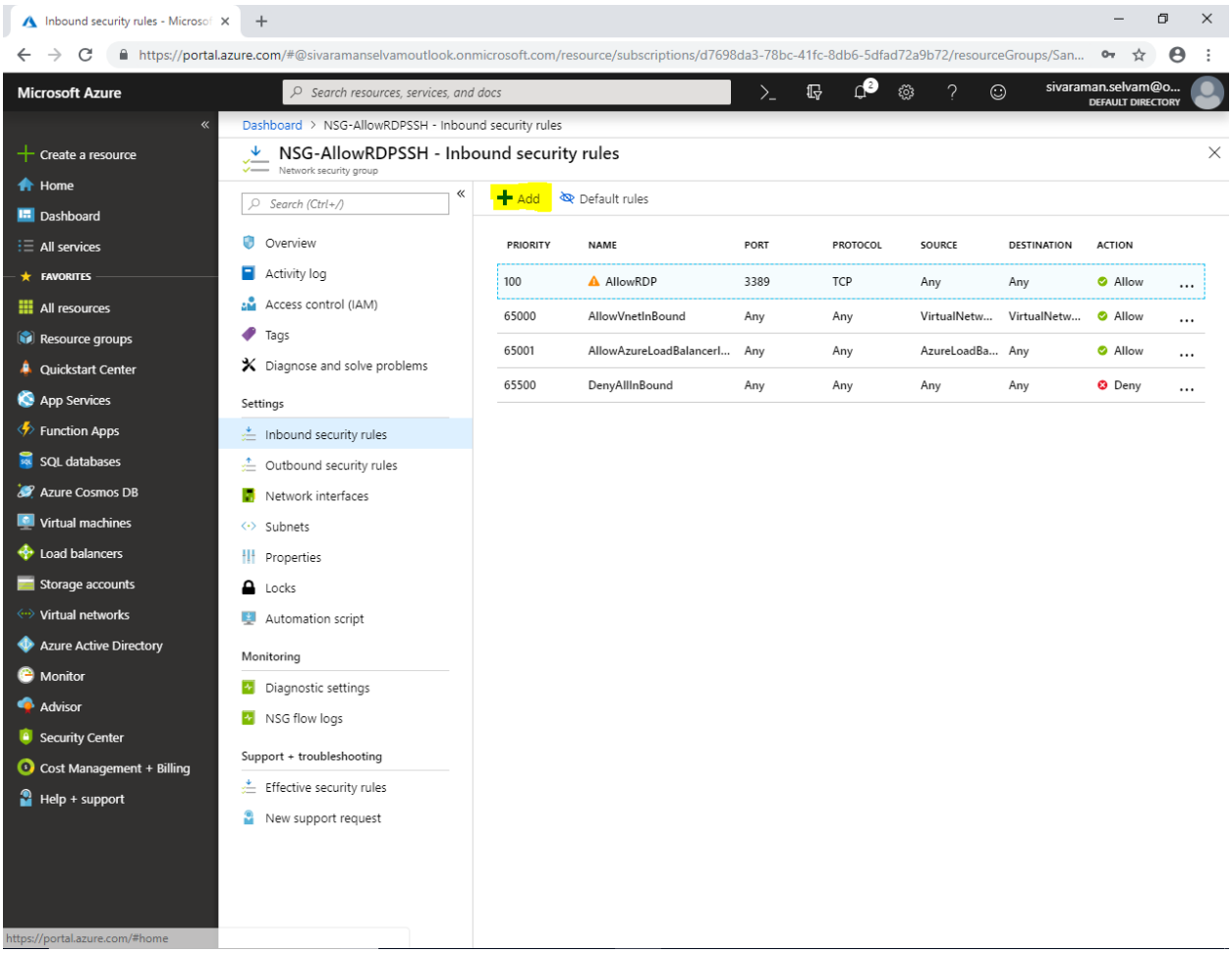
Click **“Add”**.


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 > NSG-AllowRDPSSH - Inbound security rules
NSG-AllowRDPSSH - 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
NSG-AllowRDPSSH
Basic
* Source
Any
* Source port ranges
*
* Destination
Any
* Destination port ranges
3389
* Protocol
Any
TCP
UDP
* Action
Allow
Deny
* Priority
100
* Name
AllowRDP
Description
Allows RDP for management purpose
Add

You are able to see that Inbound security rules has been created with priority “100”. RDP is not recommended to access the server through public. That is the reason it shows warning.



Click “Add”.


Inbound security rules - Microsof
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
Dashboard > NSG-AllowRDPSSH - Inbound security rules
NSG-AllowRDPSSH - Inbound security rules
Network security group
Search (Ctrl+/)
Add
Default rules
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
PRIORITY
NAME
PORT
PROTOCOL
SOURCE
DESTINATION
ACTION
100
AllowRDP
3389
TCP
Any
Any
Allow
65000
AllowVnetInBound
Any
Any
VirtualNetw...
VirtualNetw...
Allow
65001
AllowAzureLoadBalancerI...
Any
Any
AzureLoadBa...
Any
Allow
65500
DenyAllInBound
Any
Any
Any
Any
Deny
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
https://portal.azure.com/#home

While creating inbound security rule

Source : Any

Source port ranges : *

Destination : Any

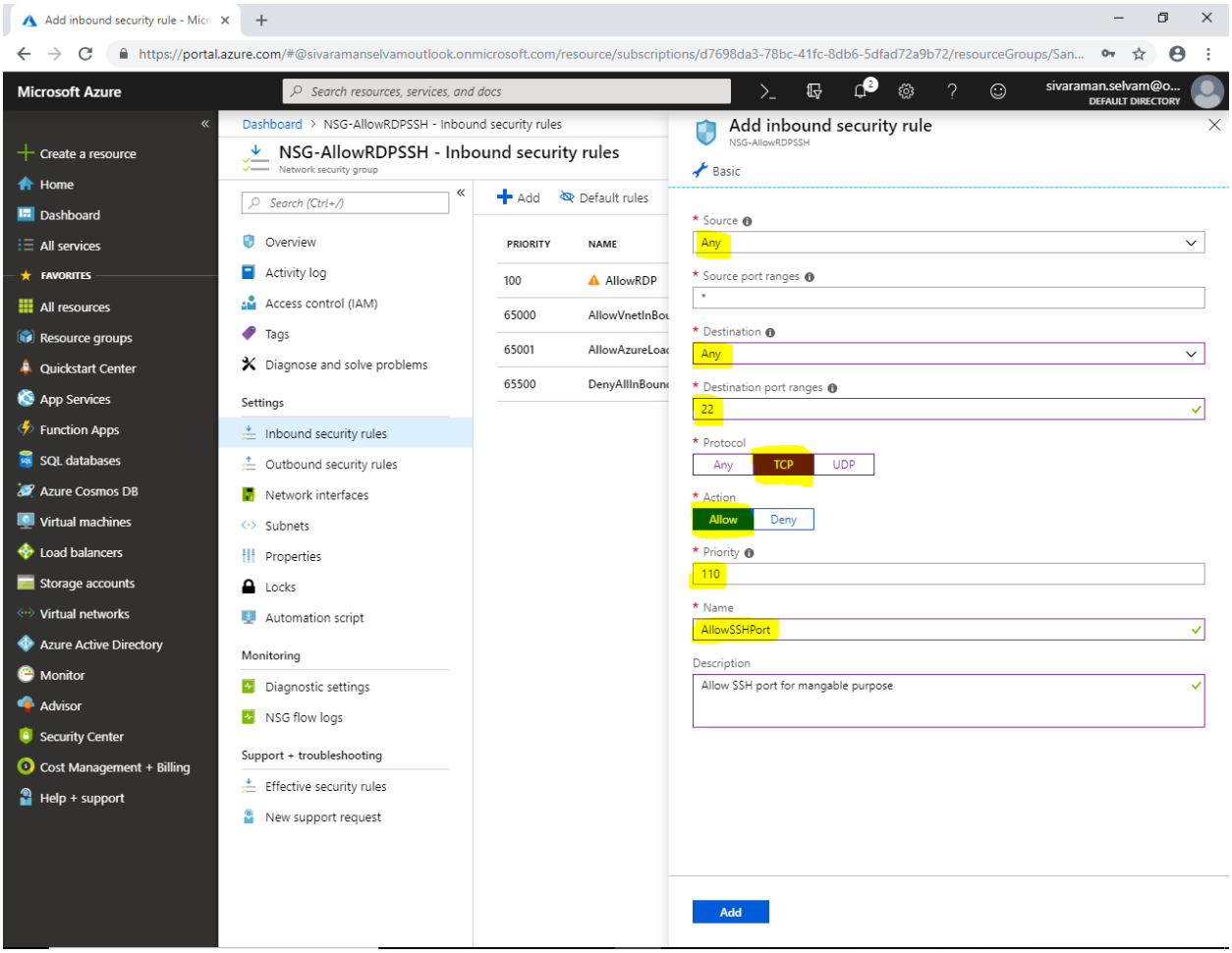
Destination port ranges : 22

Protocol : TCP

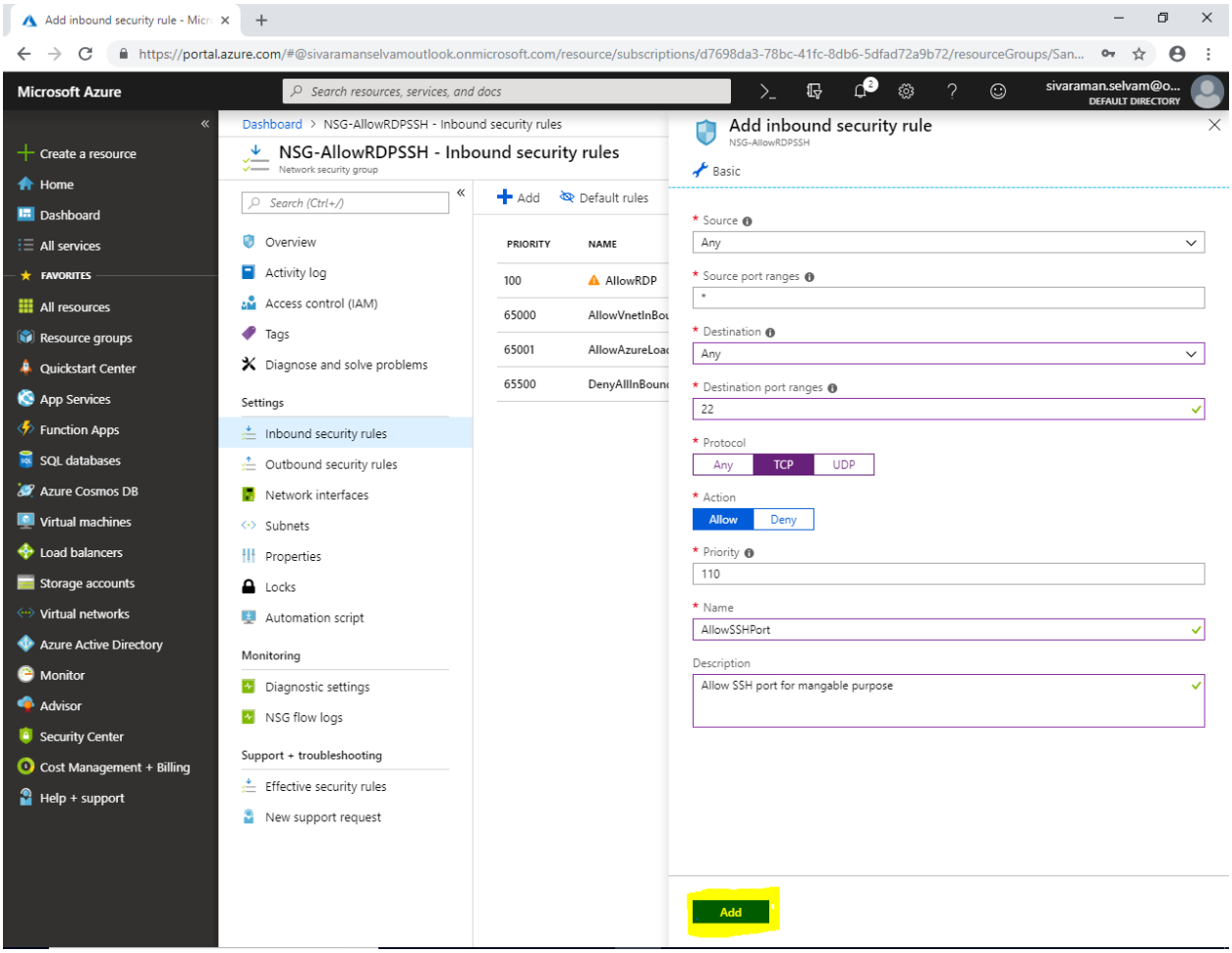
Action : Allow

Priority : 110

Name : AllowSSH

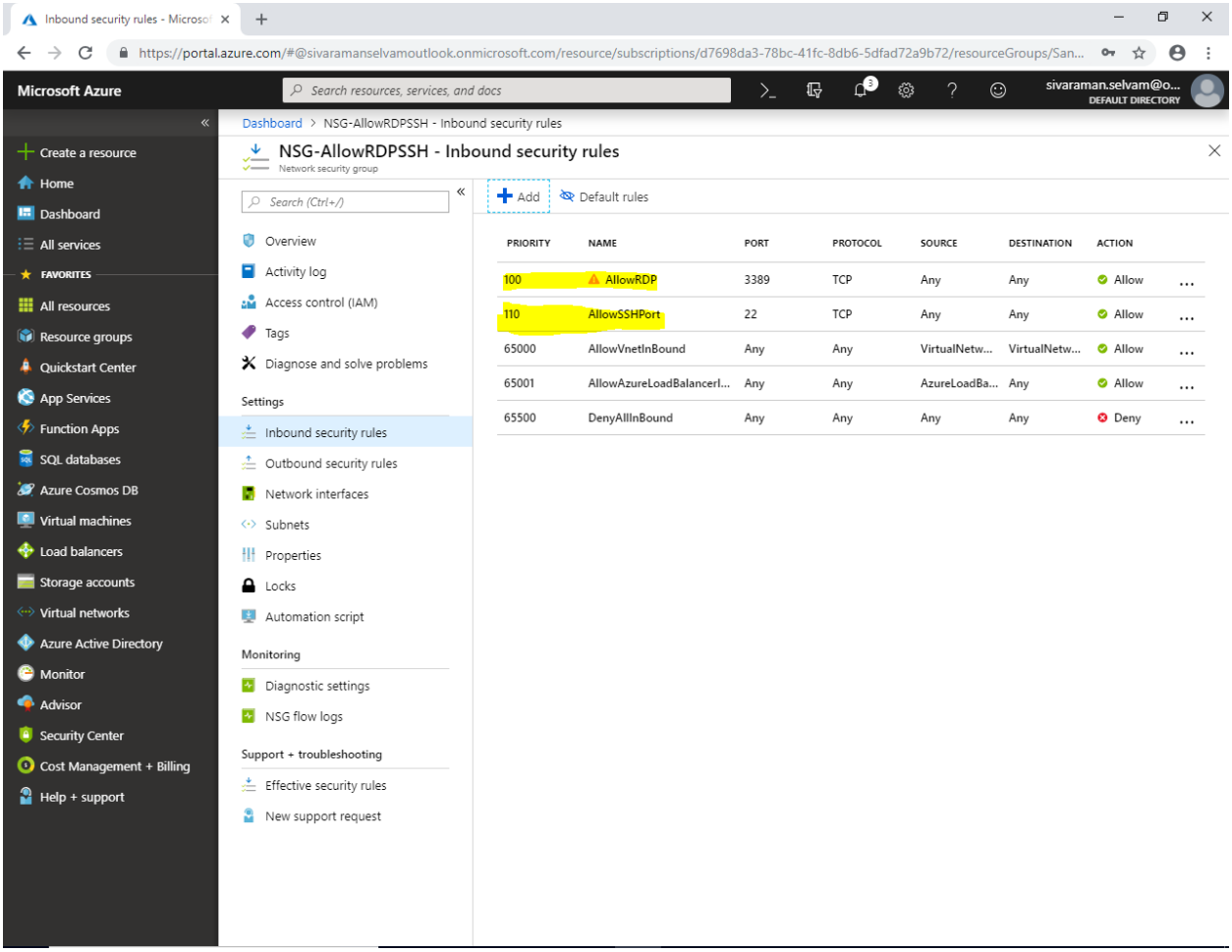


Click **“Add”**.


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 > NSG-AllowRDPSSH - Inbound security rules
NSG-AllowRDPSSH - 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
100
AllowRDP
65000
65001
65500
Add inbound security rule
NSG-AllowRDPSSH
Basic
* Source
Any
* Source port ranges
*
* Destination
Any
* Destination port ranges
22
* Protocol
Any
TCP
UDP
* Action
Allow
Deny
* Priority
110
* Name
AllowSSHPort
Description
Allow SSH port for mangable purpose
Add

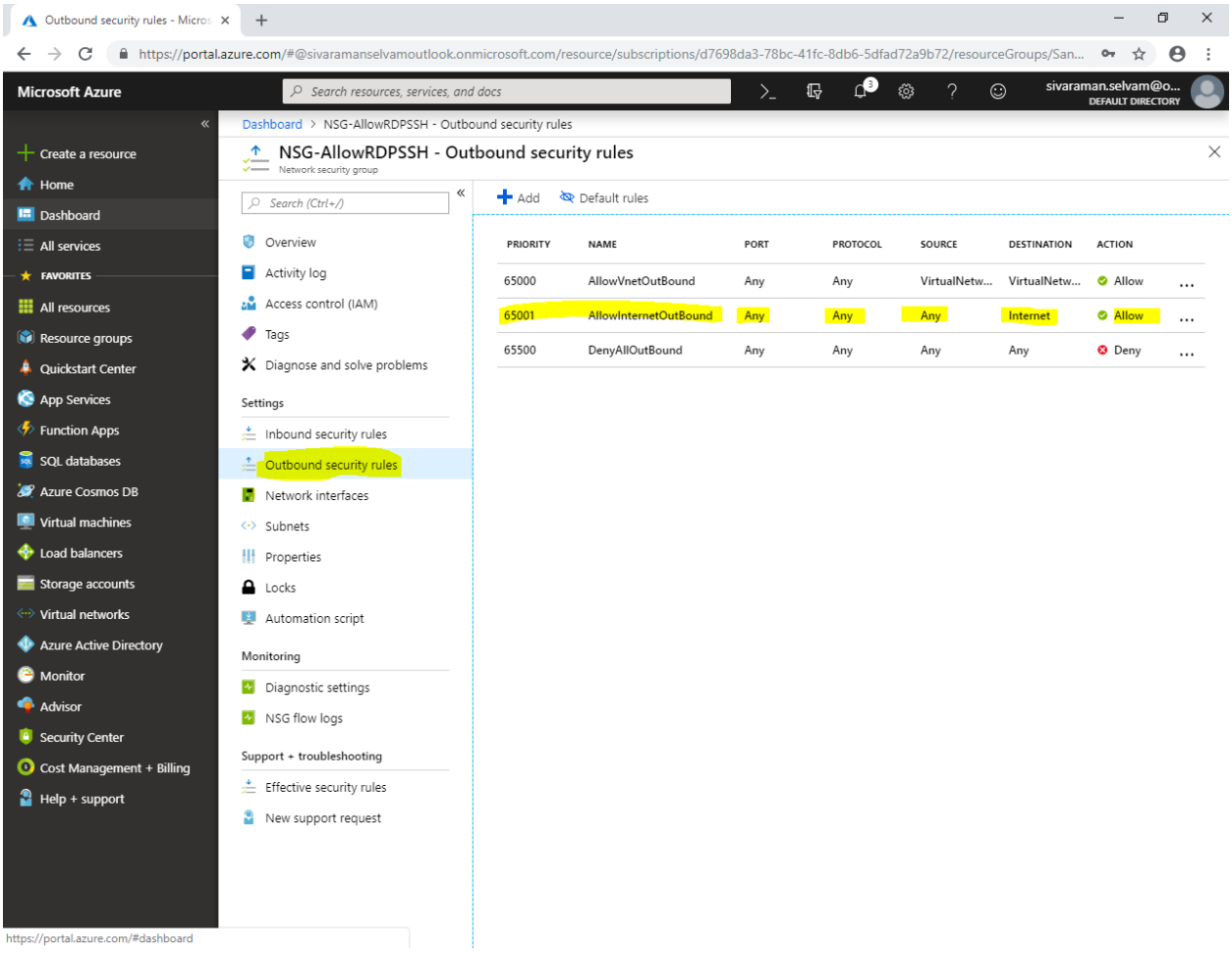
You are able to see 100 & 110 inbound security rules are created.

While any inbound traffic come from outside first it will check the lowest priority rule “100” if the traffic is allowed in that rule it will match and allow. Otherwise it will check next priority rule.



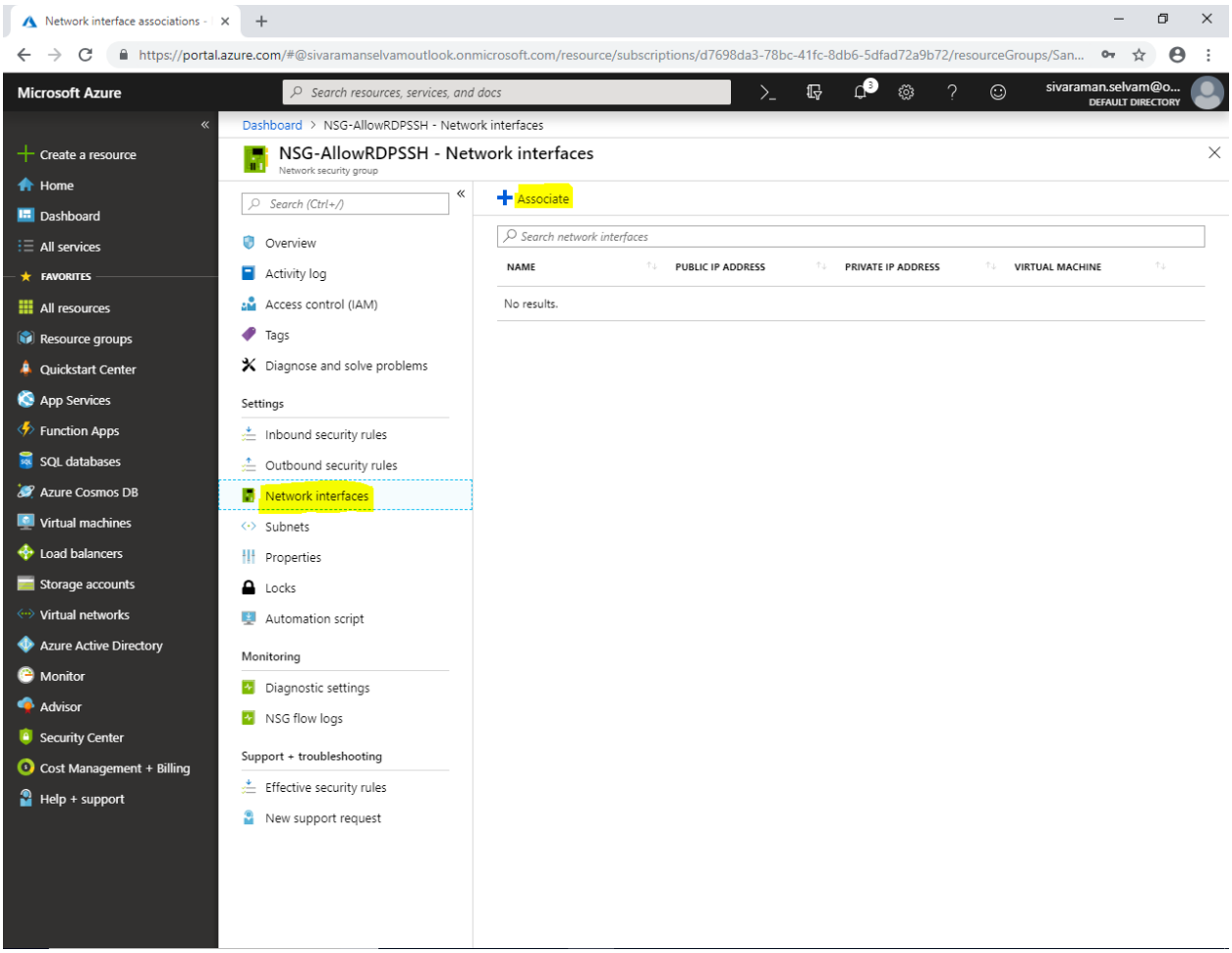
Click on **"Outbound security Rules"**

By default it will allow Internet (any protocol and and any port) from azure virtual machine to public.



Click **“Network interfaces”**.

Click **“Associate”**.

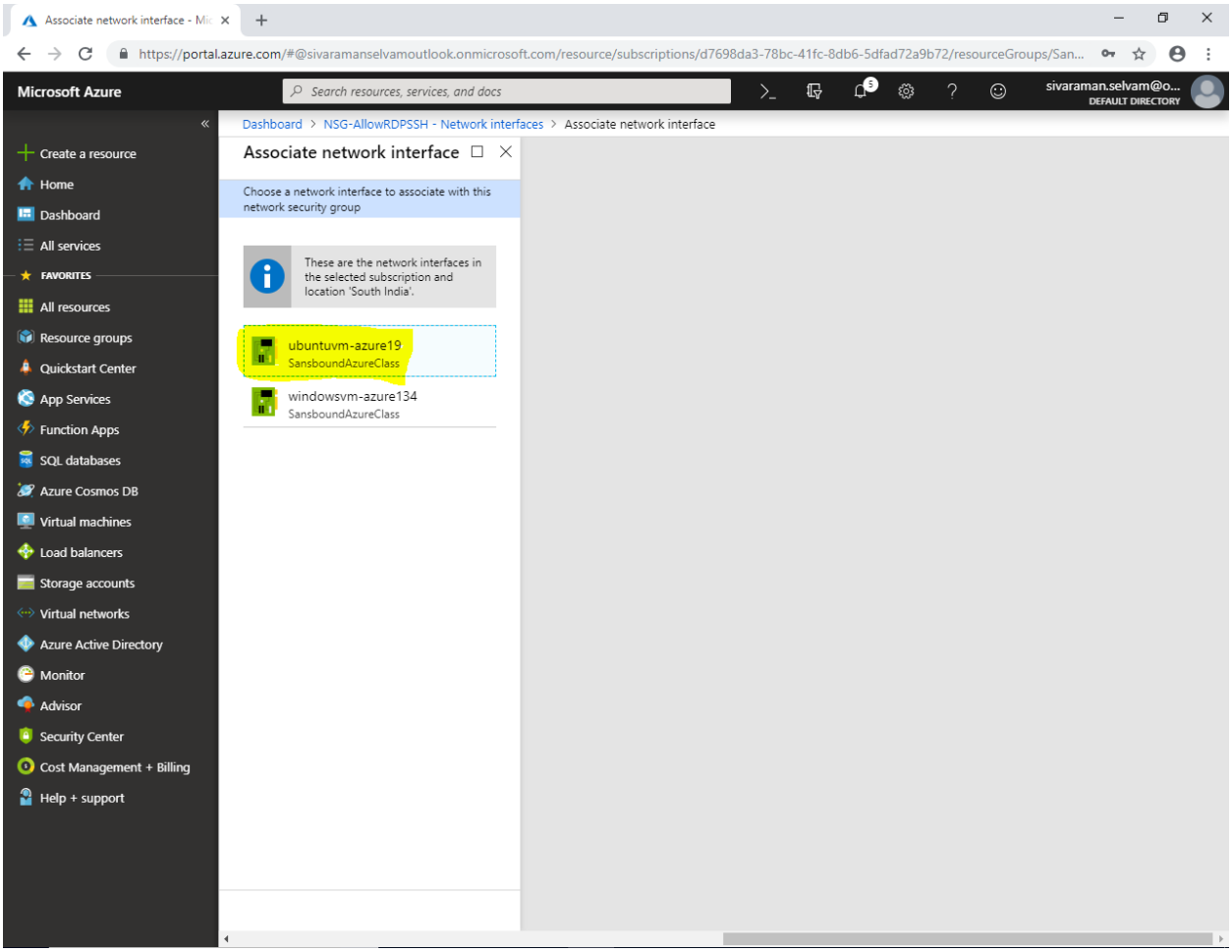


In **“Associate network interface”**

You are able to see list of VM’s Network interface(s) which you have created.

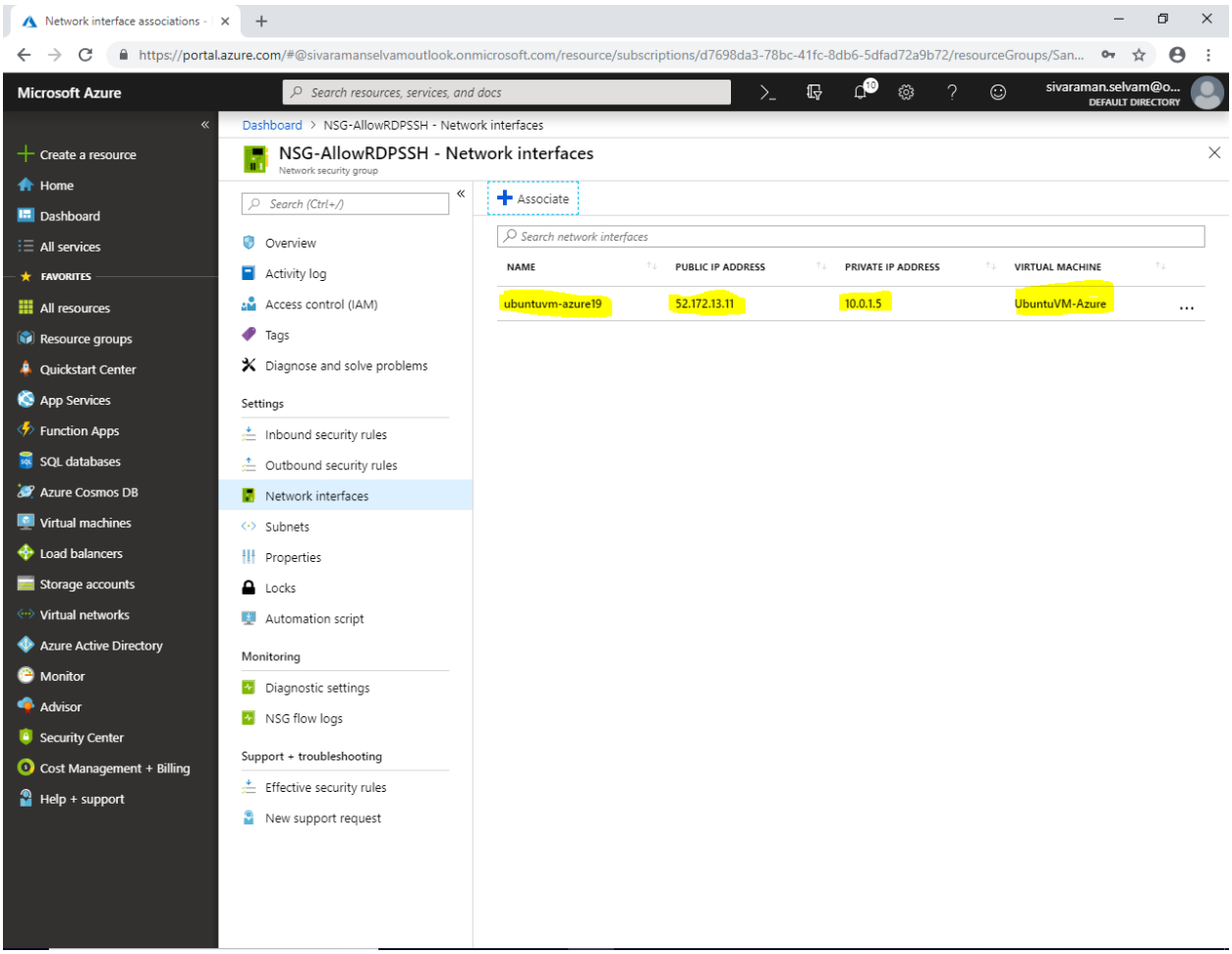
Now am able to see the Ubuntu VM and Windows VM network interface.

Note: If you have checked any one of the network interface, NSG (Network Security Group) will be associated only for that particular network interface simultaneously. If you have required to apply the same NSG to other VM(s) also, in that case you will click on the “Network interface” named manually. I will click on “Ubuntuvm-azure19”.

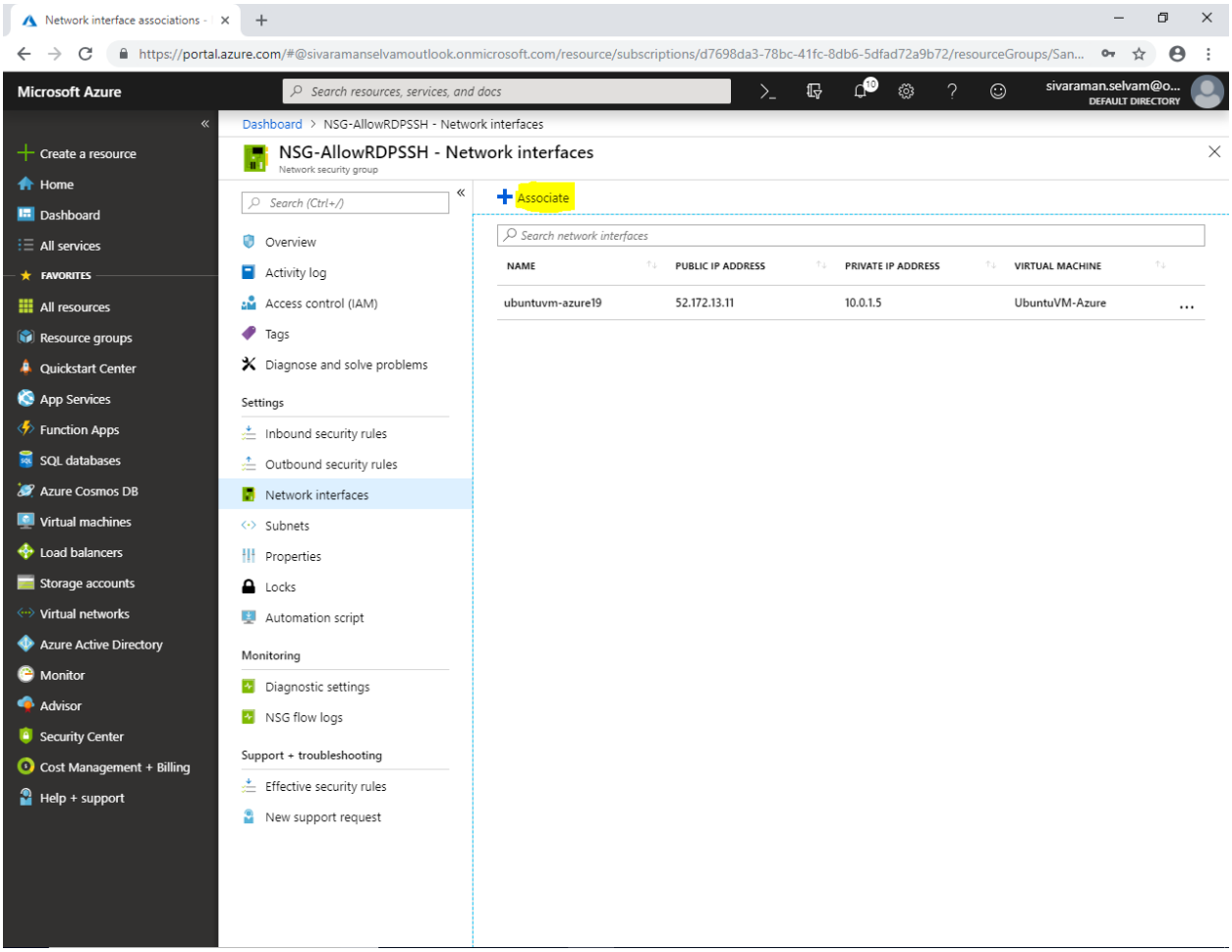


In **“Network Interfaces”**

You are able to see that “**UbuntuVM-Azure”** has been successfully associated.

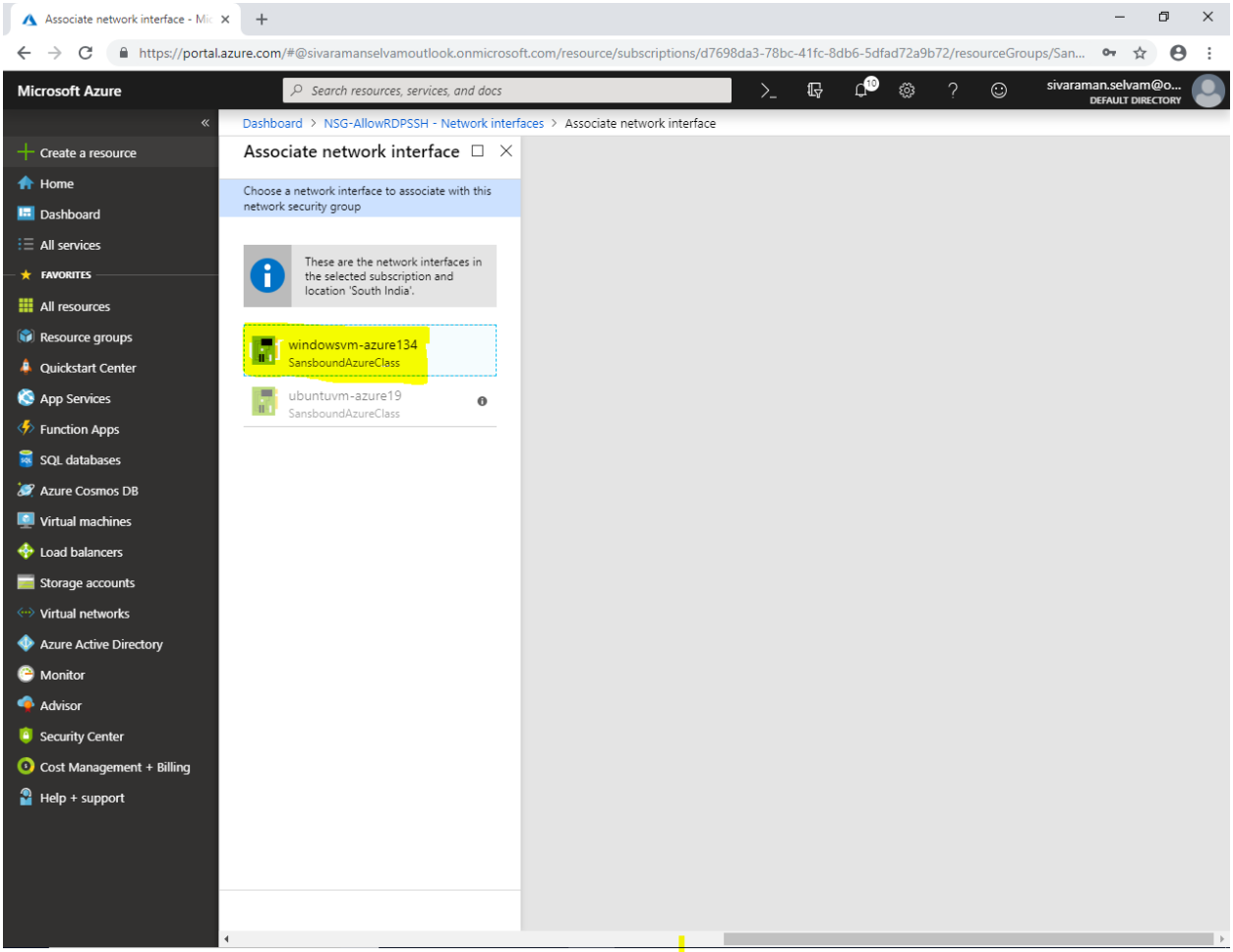


In **“Network Interfaces”** click **“Associate”**

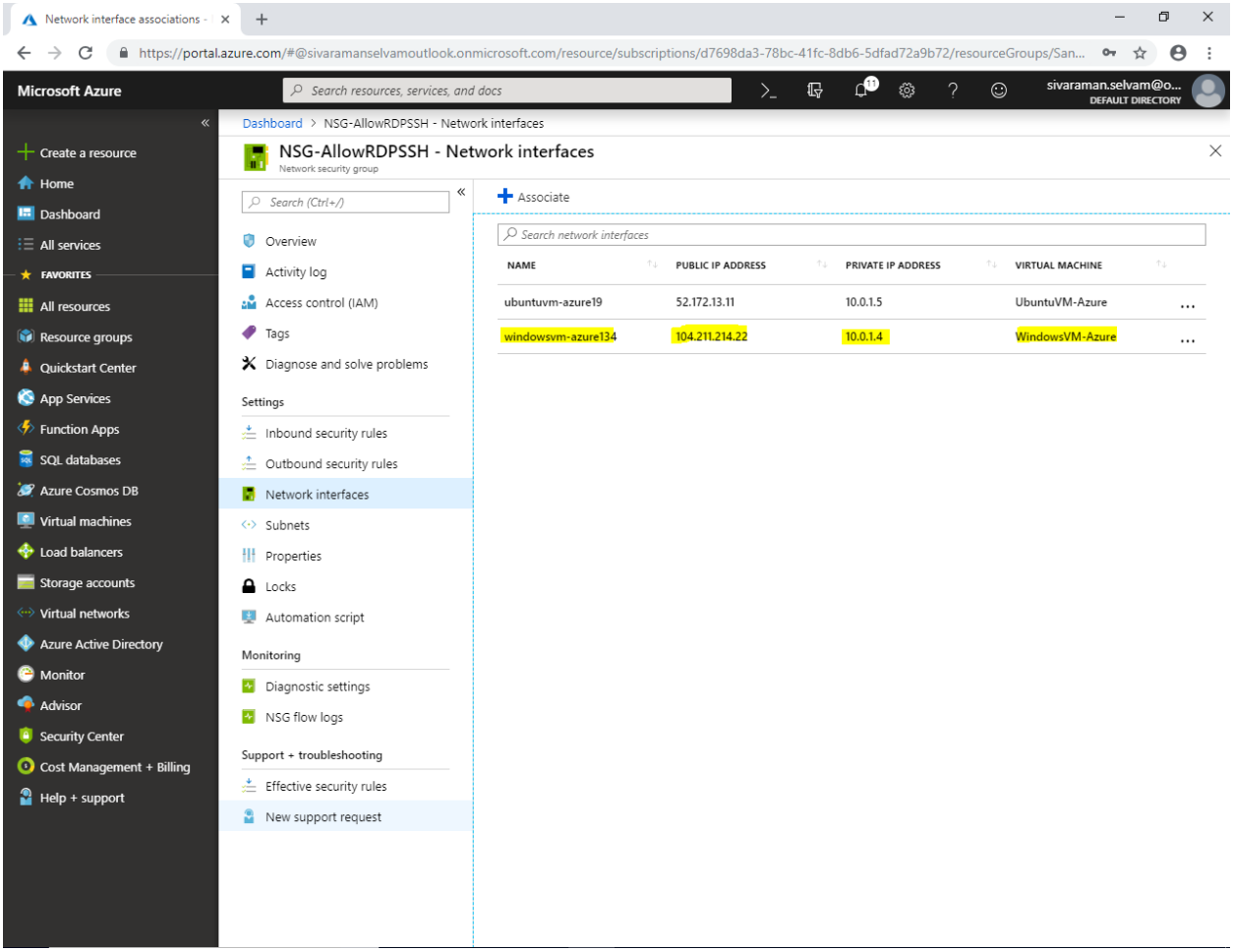


By default “Windows-VM” network interface has been selected. Because existing network interface has been already associated.

Click on **“windowsvm-azure134”**.

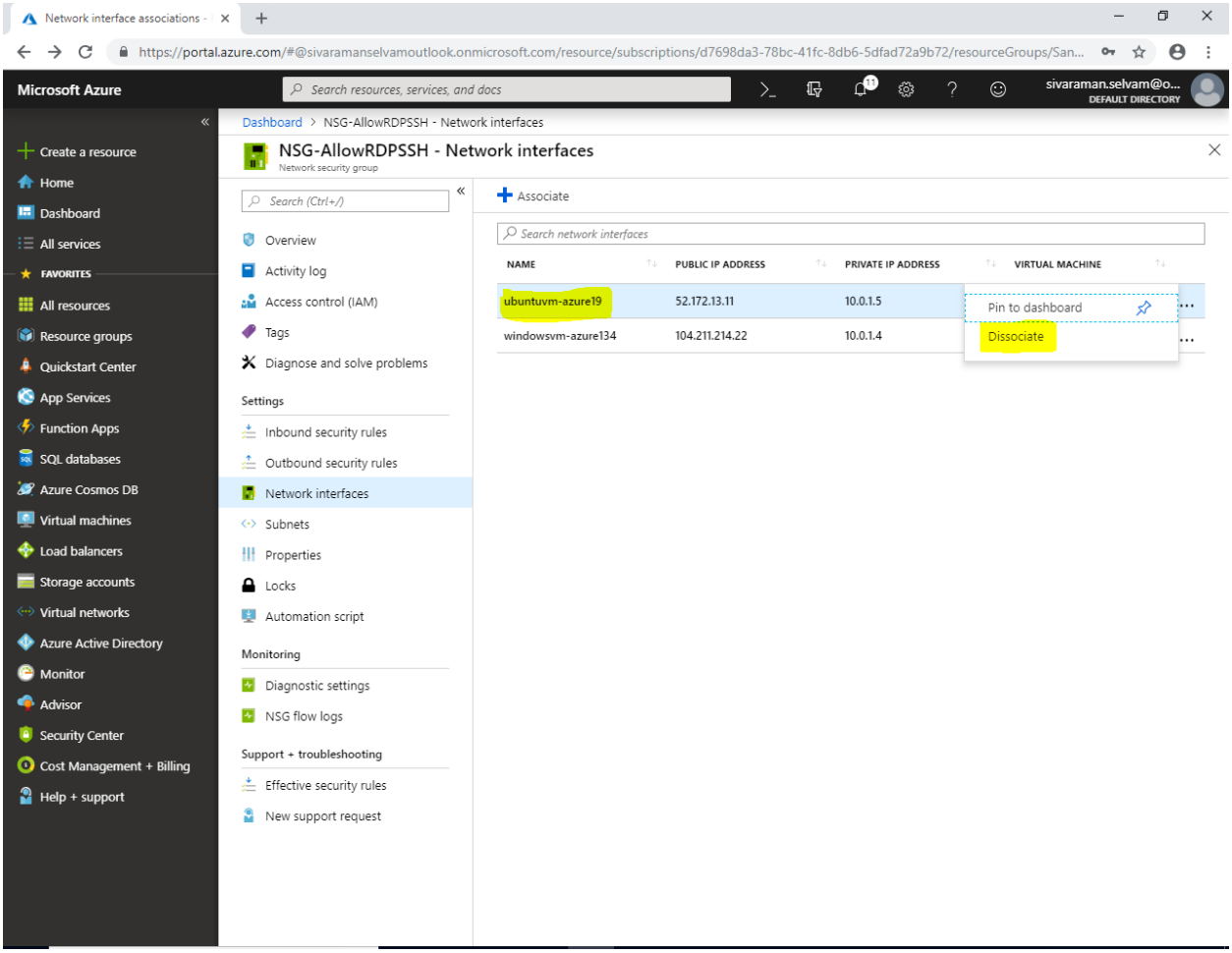


Now you are able to see that Windows VM network interface also associated with **"NSG-AllowRDPSSH"** network security group.

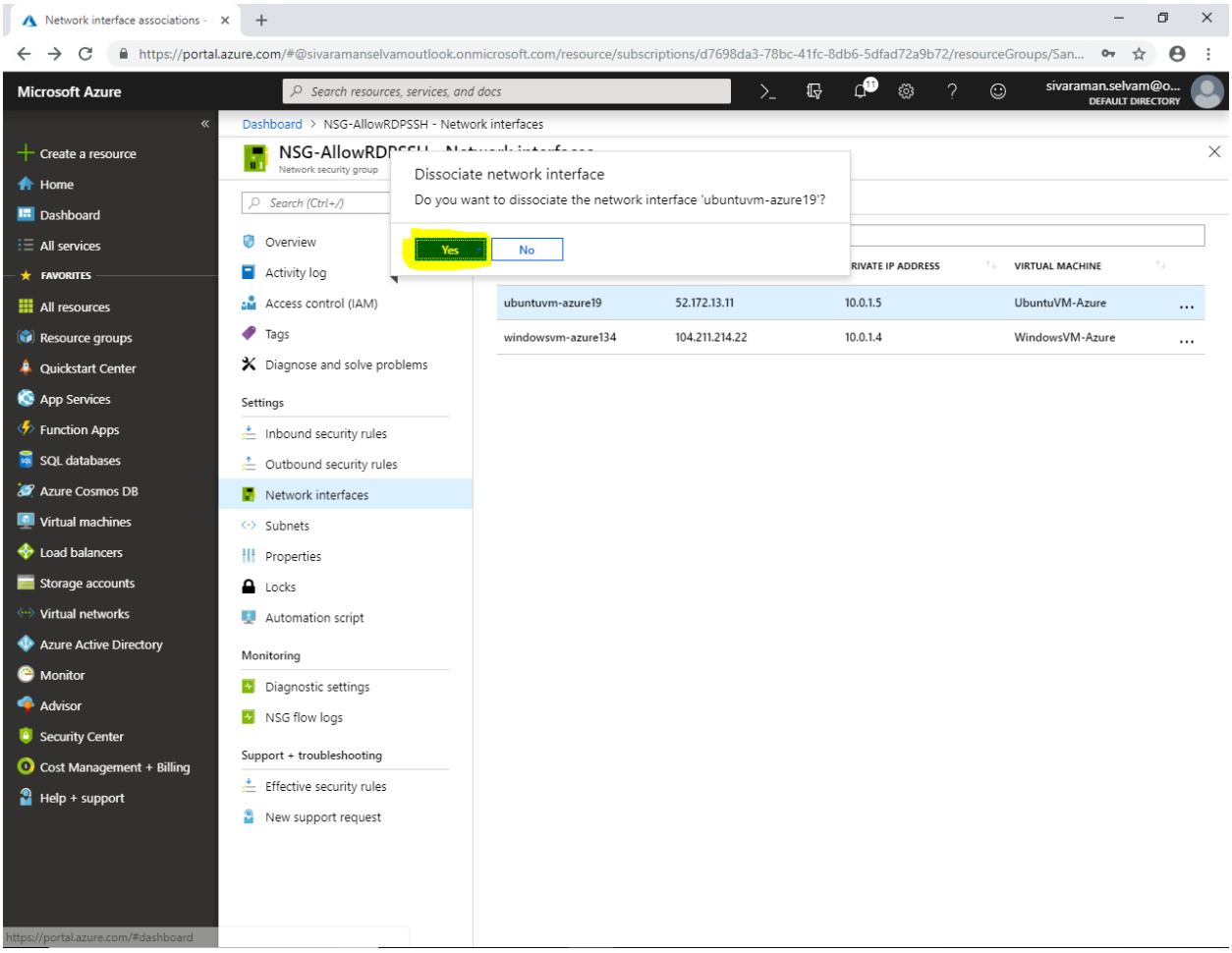


We have understood the features of **“Network Interfaces”** in **“Network Security Group”**.

Select **“ubuntuvm-azure19”** and click on ”…” you need to click **“Dissociate”**.

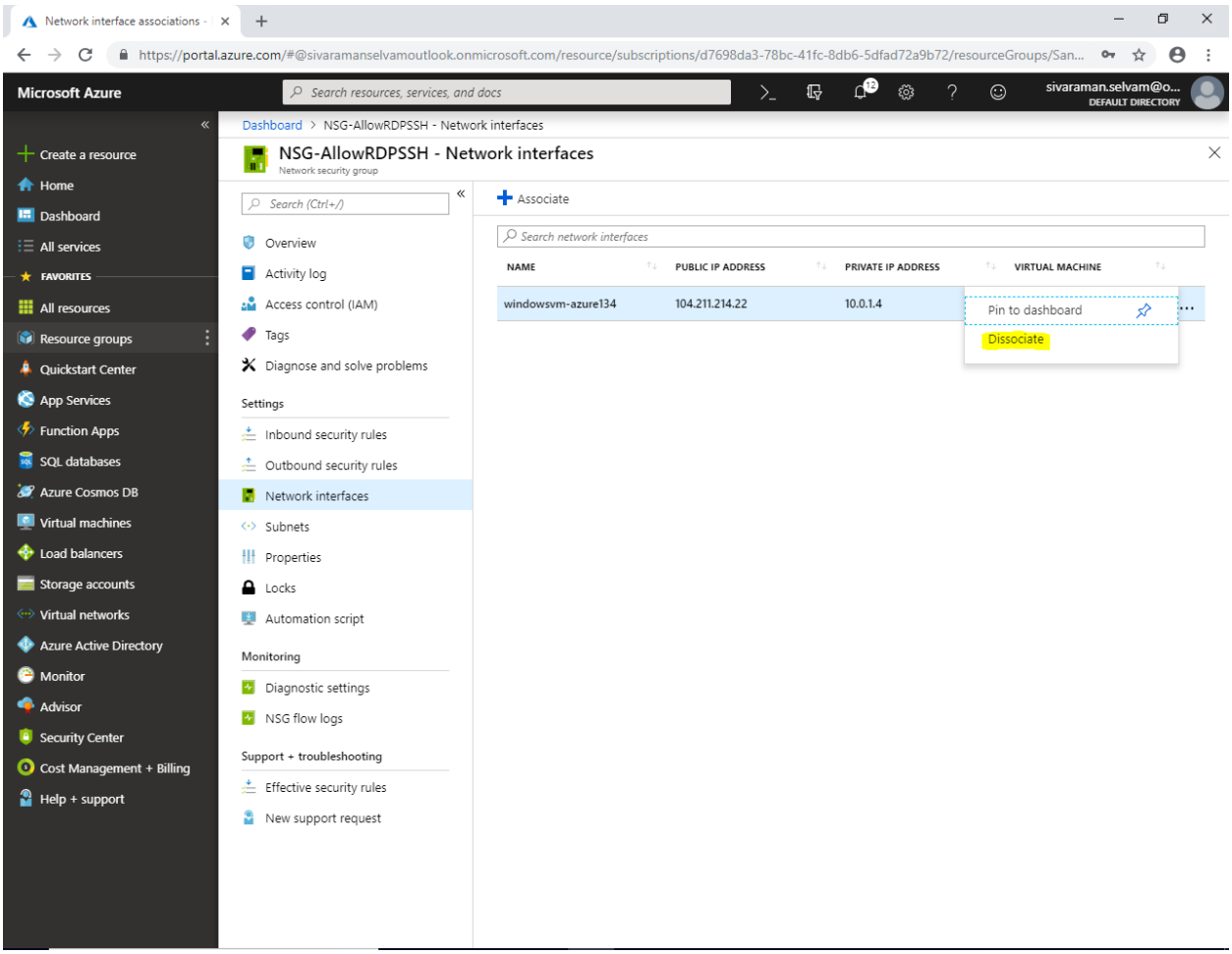


Click **"Yes"** to dissociate the network from ubuntuvm.

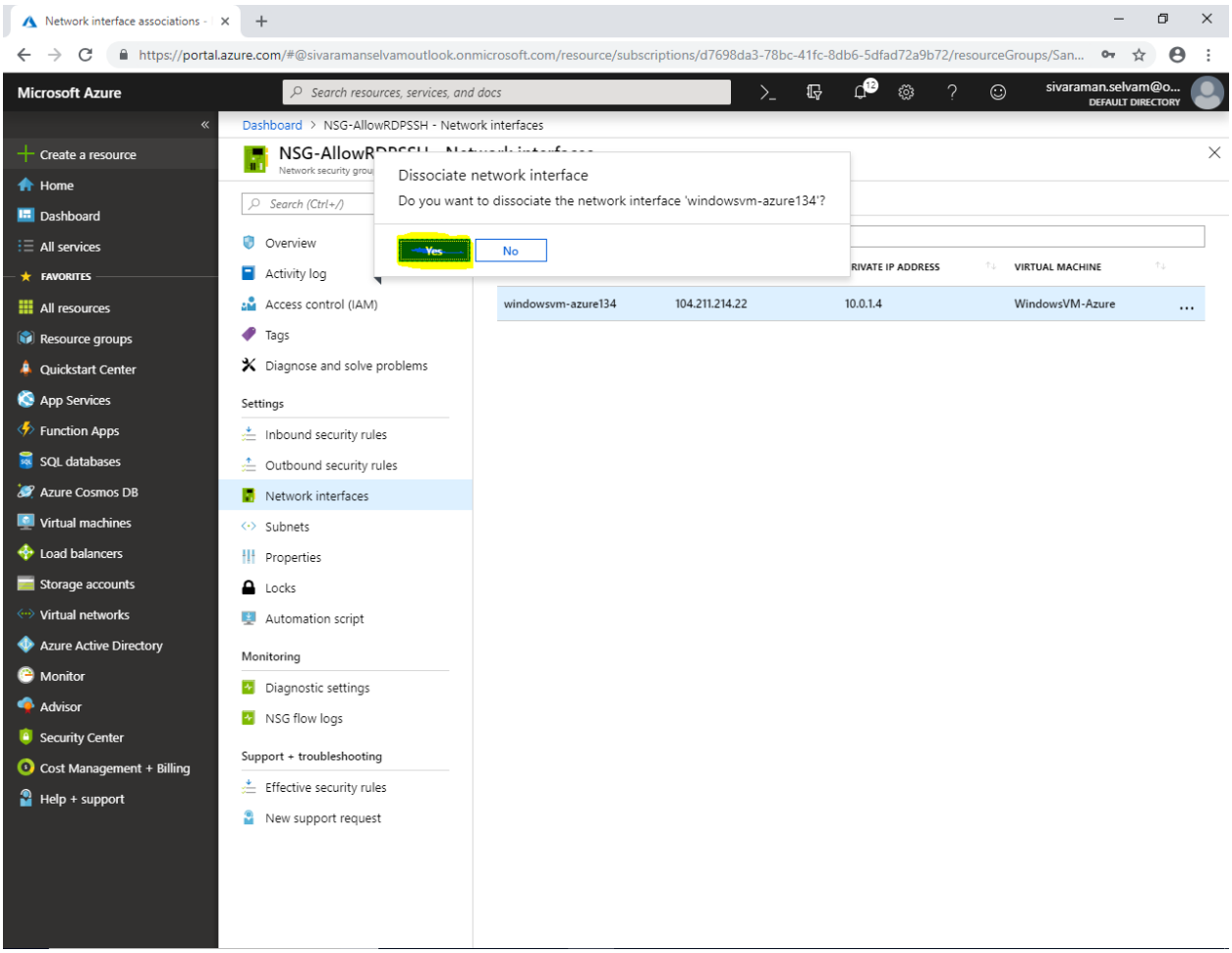


Select **“windowsvm”** and click on “…”

Click **“Dissociate”**.

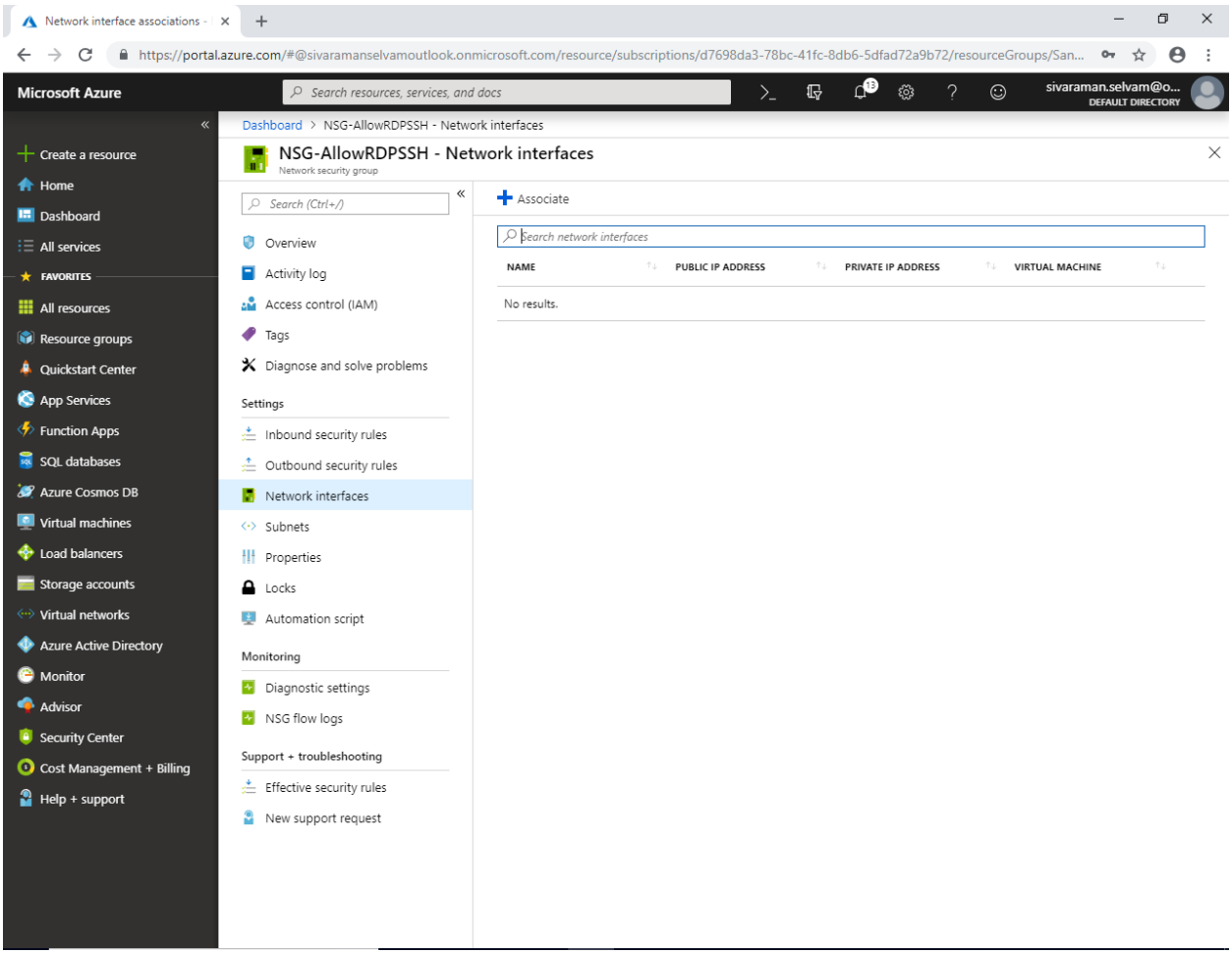


Click **"Yes"**.


Network interface associations -
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 > NSG-AllowRDPSSH - Network interfaces
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
Dissociate network interface
Do you want to dissociate the network interface 'windowsvm-azure134'?
Yes
No
RIVATE IP ADDRESS
VIRTUAL MACHINE
windowsvm-azure134
104.211.214.22
10.0.1.4
WindowsVM-Azure

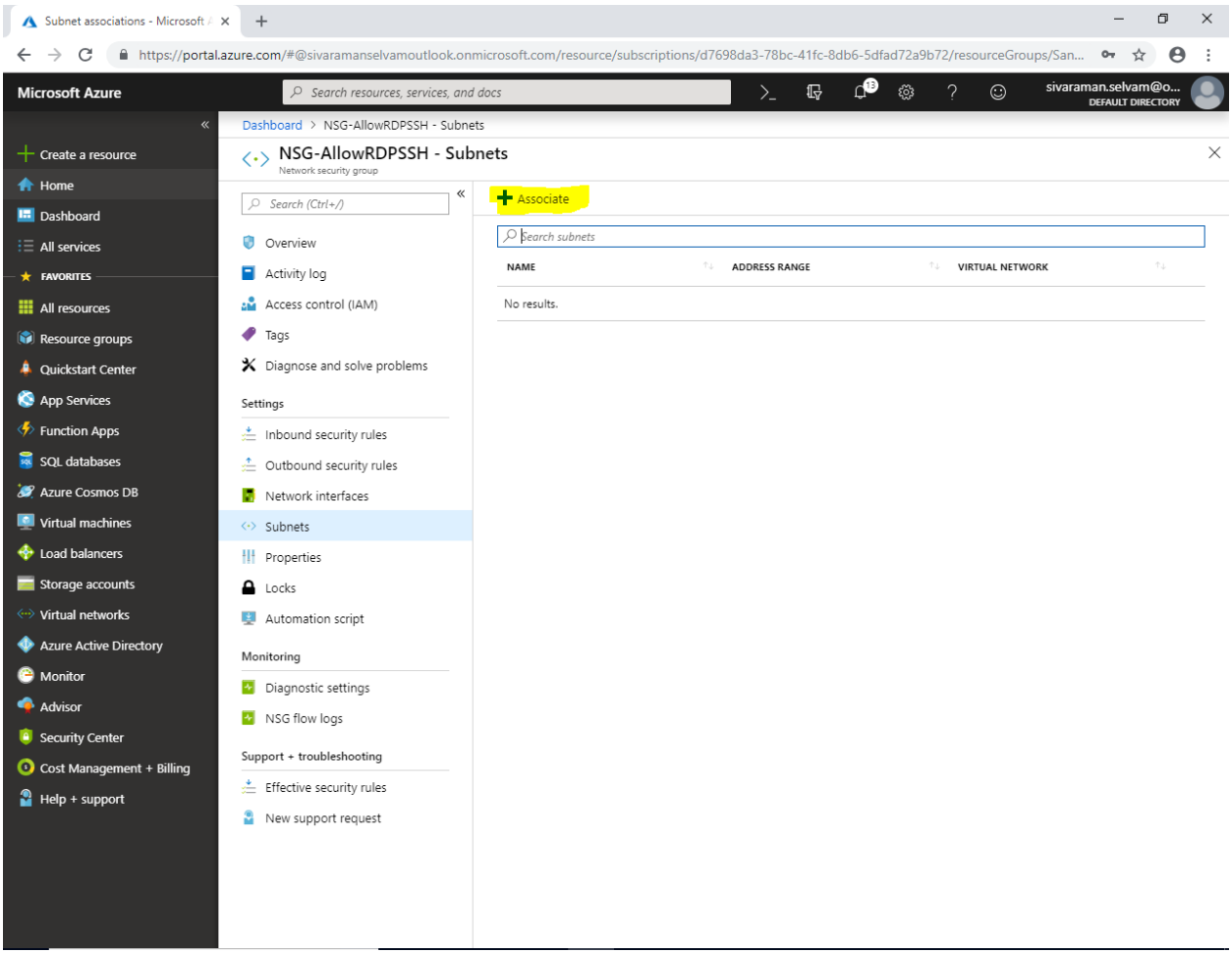
In **“Network Interfaces”**

There is no network interfaces are associated with Network Security Group (NSG).



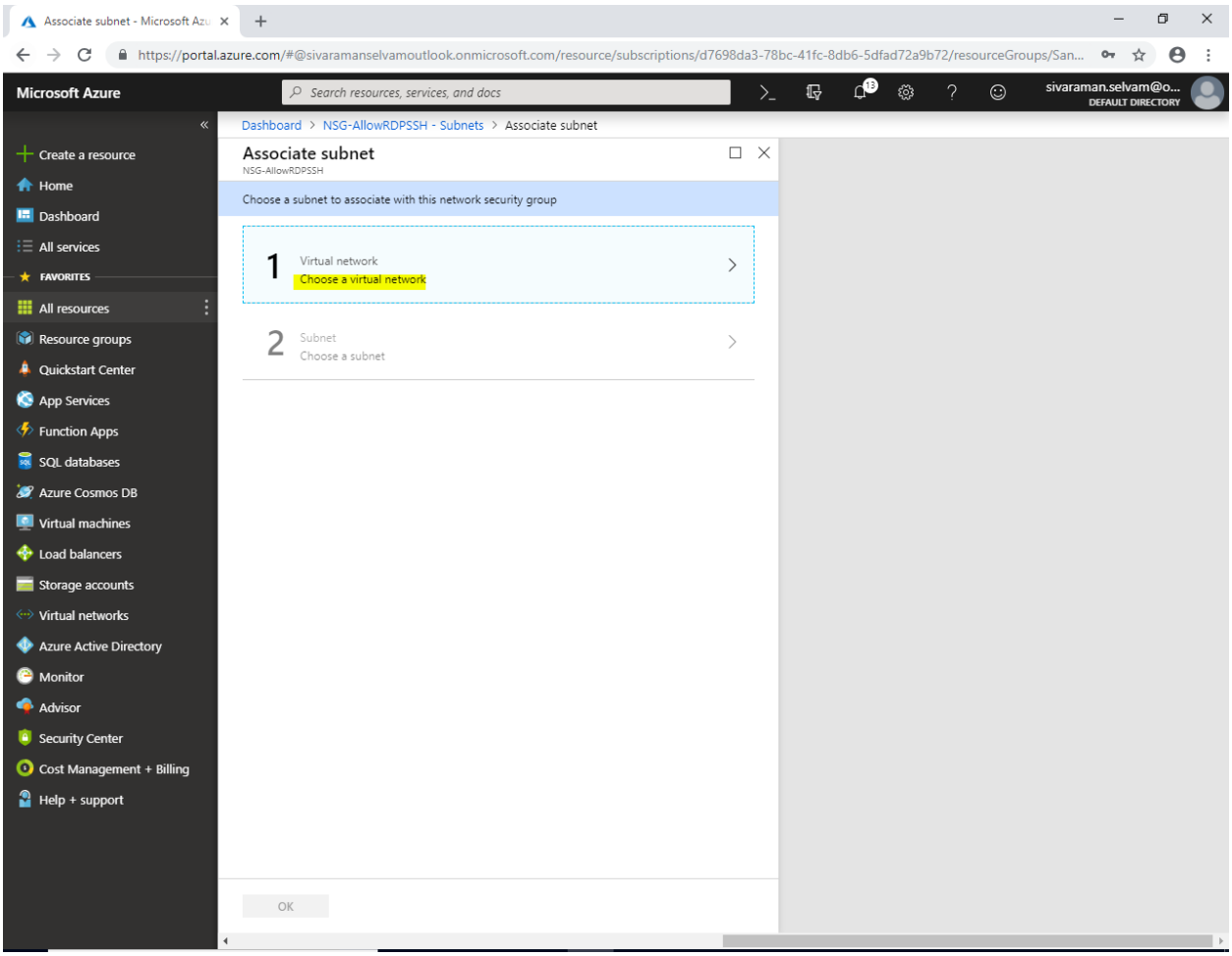
In **“Network Security Group”** click **“Subnets”**

In **“Subnets”** click **“Associate”**.

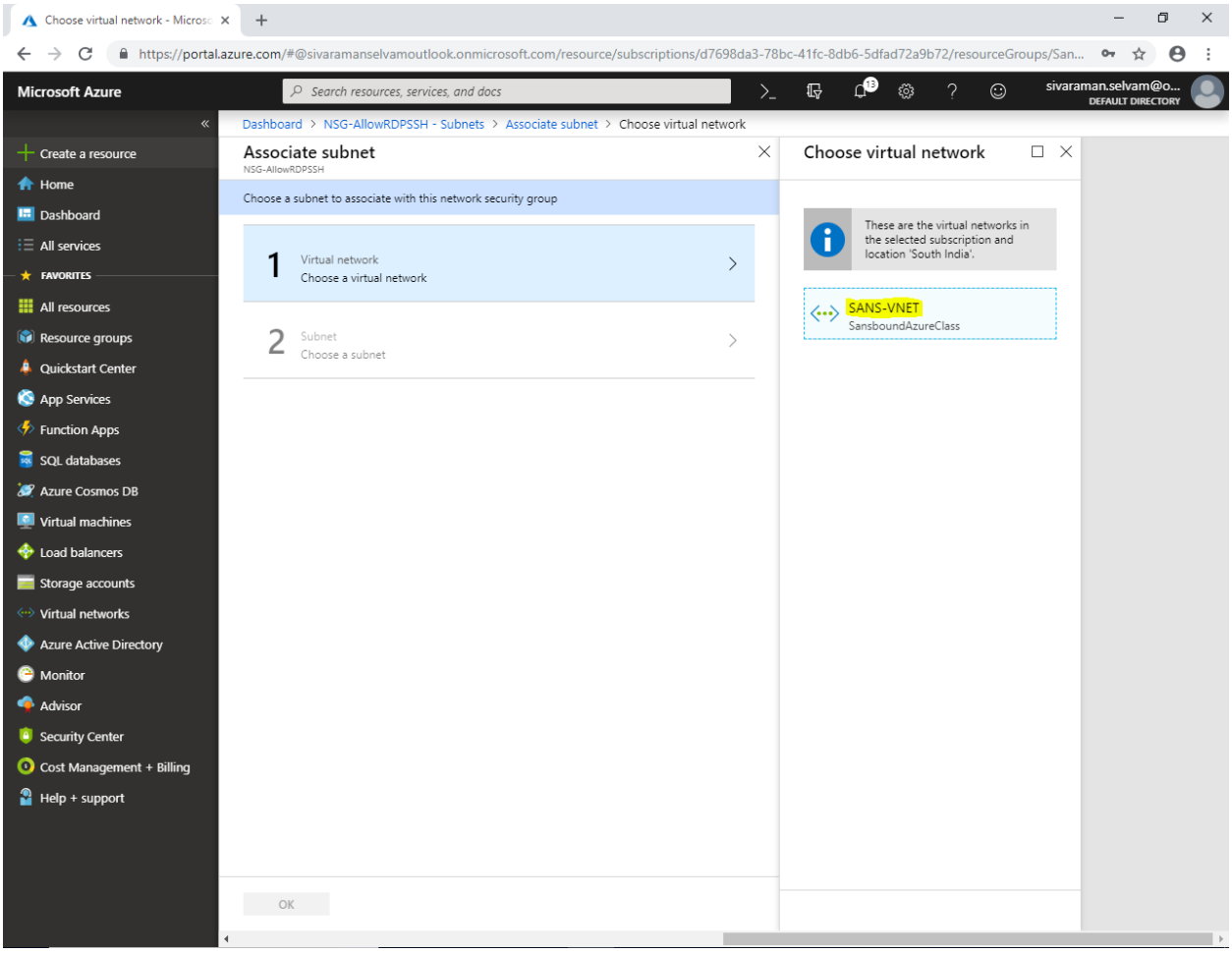


In **“Associate subnet”**

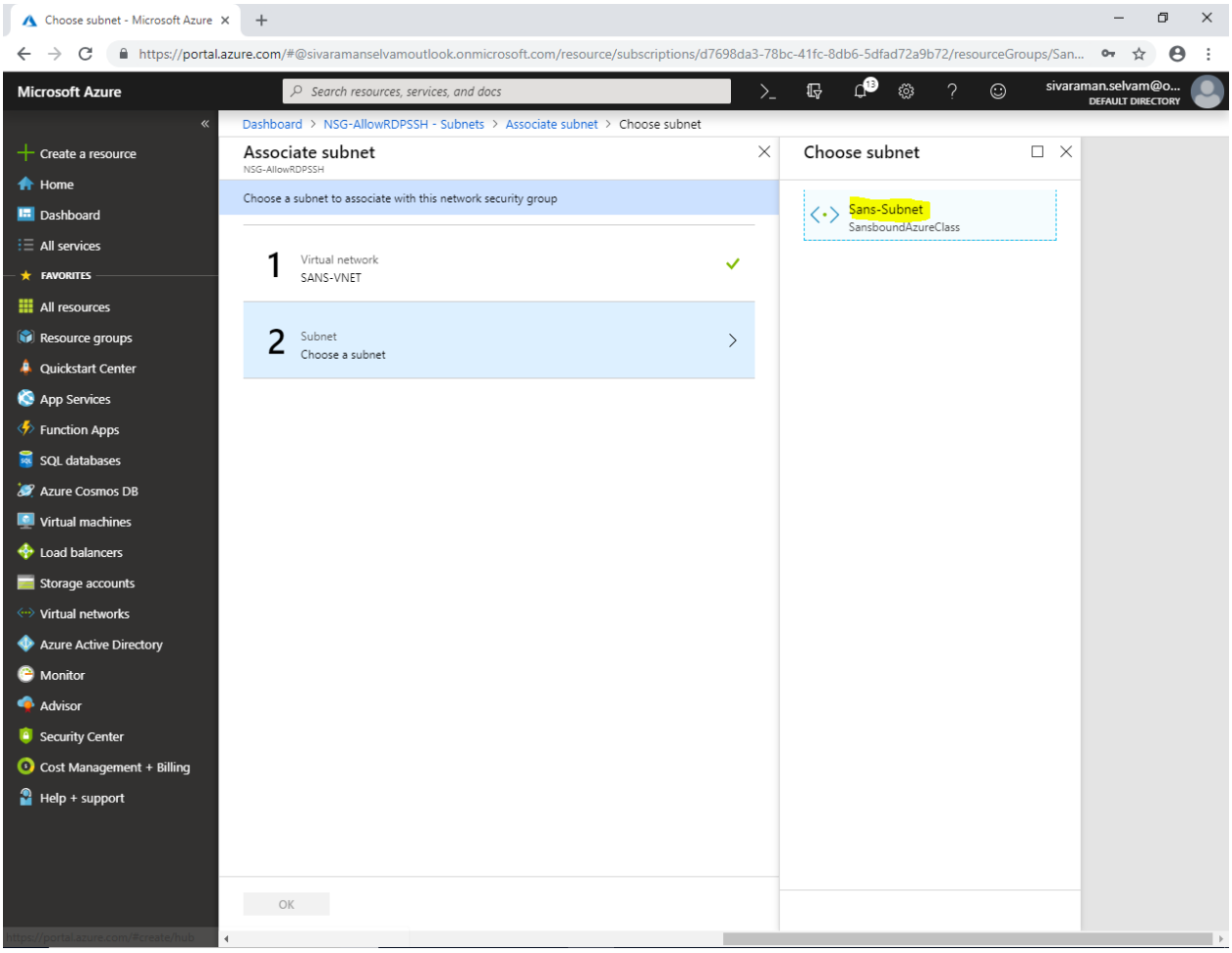
Click on **“Choose a virtual network”**.



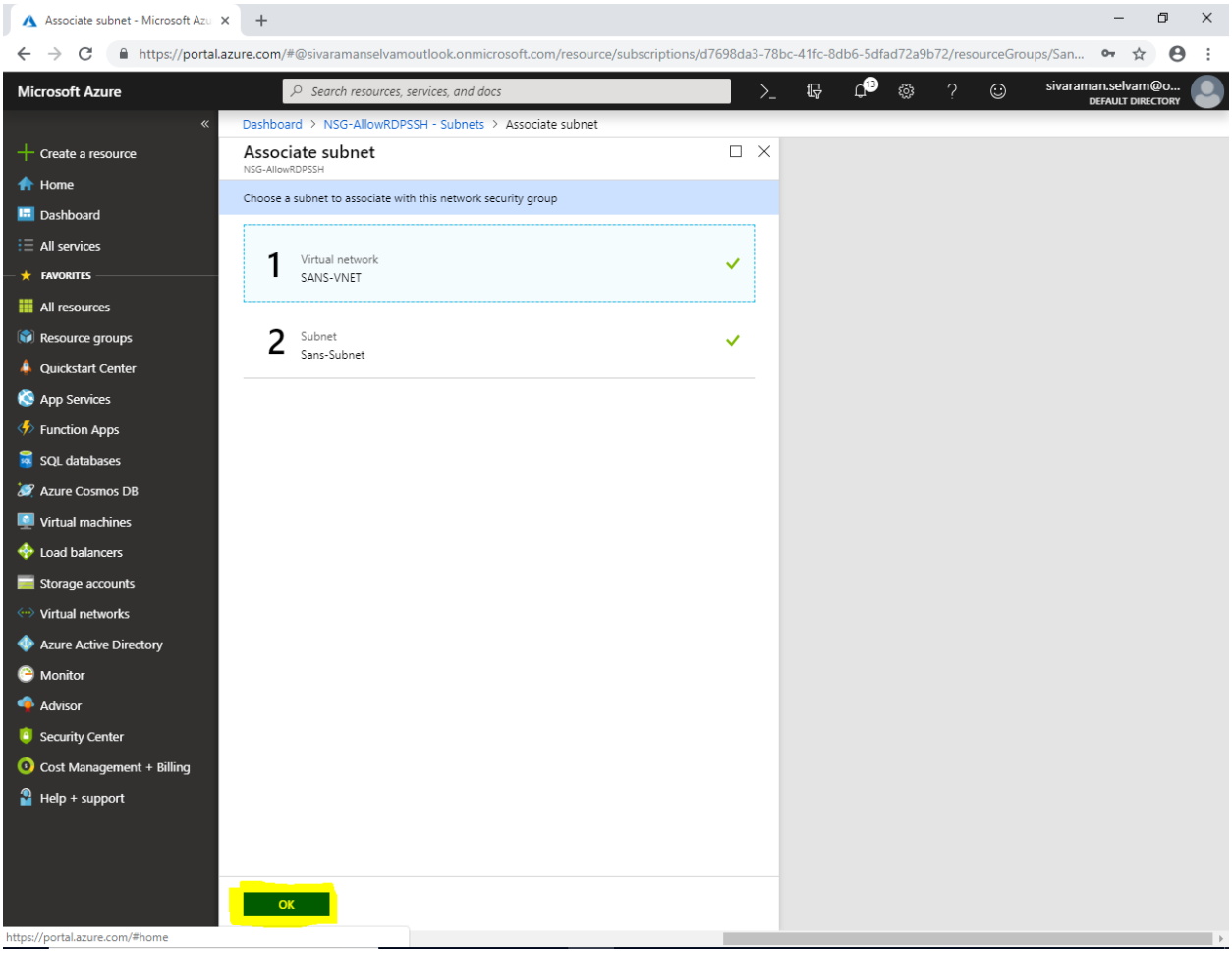
Click on **"SANS-VNET"**.



In **“Choose a subnet”** Click on **“Sans-Subnet”**.

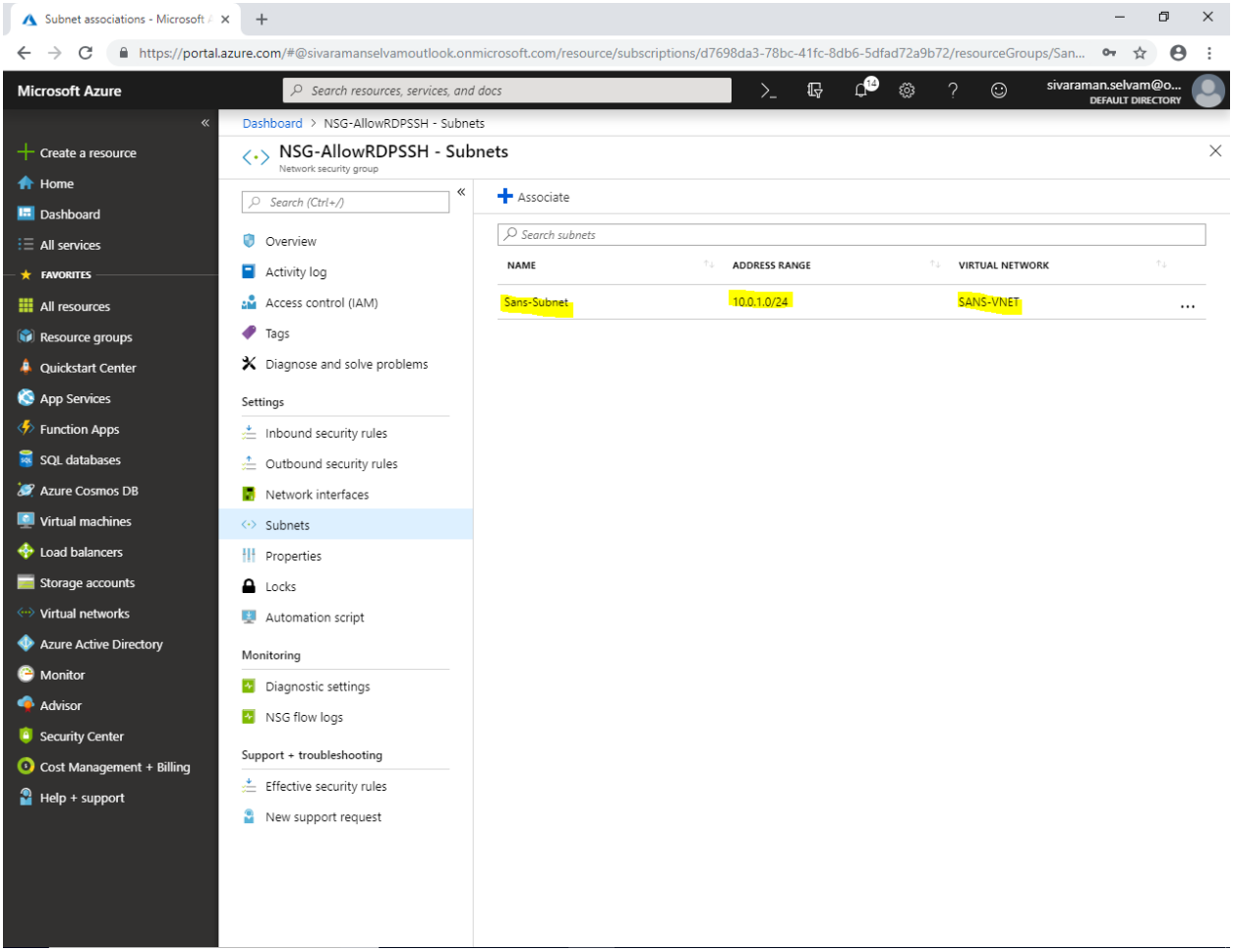


Click **“Ok”**.


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 > NSG-AllowRDPSSH - Subnets > Associate subnet
Associate subnet
NSG-AllowRDPSSH
Choose a subnet to associate with this network security group
1 Virtual network
SANS-VNET
2 Subnet
Sans-Subnet
OK
https://portal.azure.com/#home

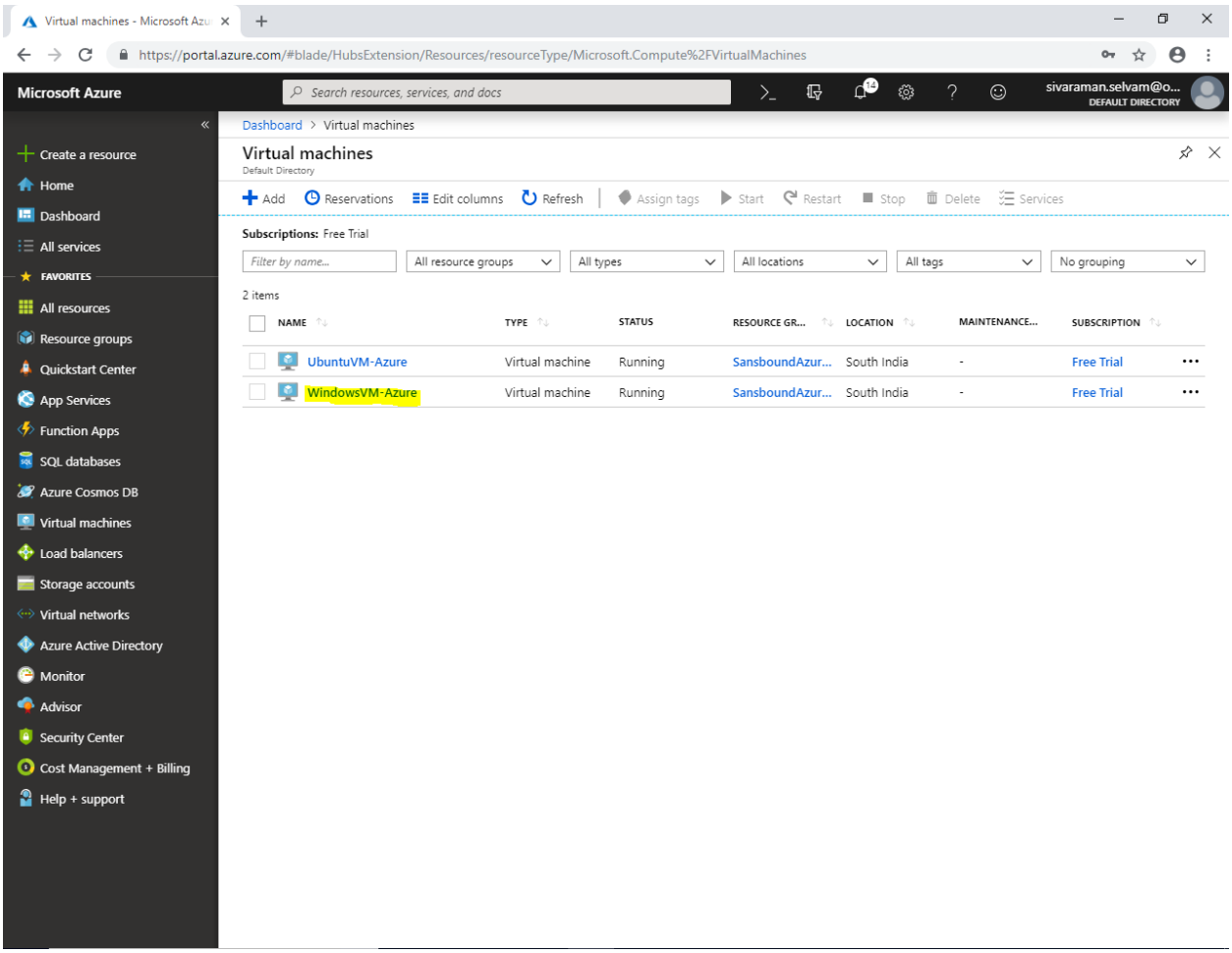
In **“Network Security Group”**

“NSG-AllowRDPSSH” Network Security Group has been associated with **Sans-Subnet (10.0.1.0/24)** of **“SANS-VNET”.**

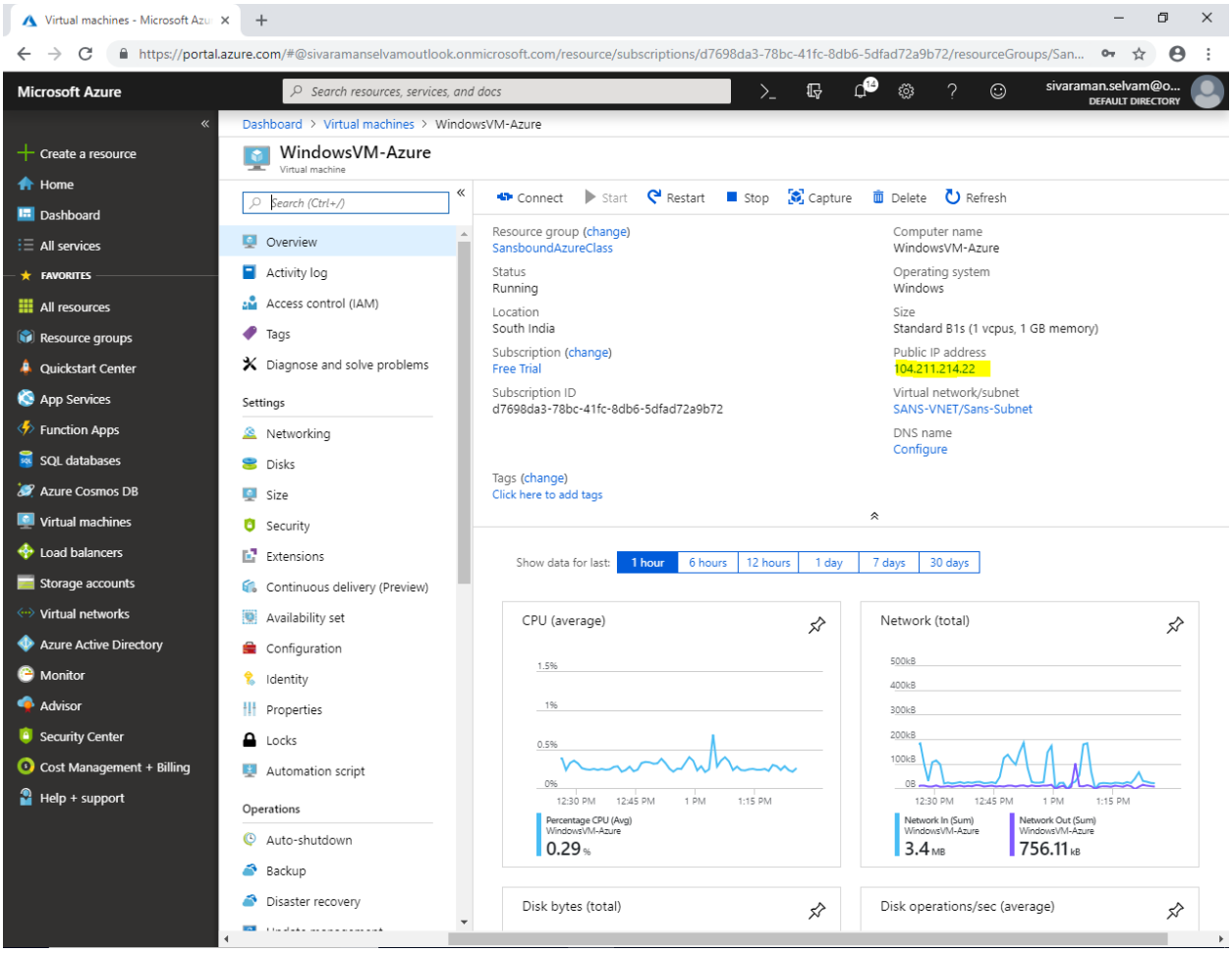


In Dashboard, click **"Virtual machines"**.

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

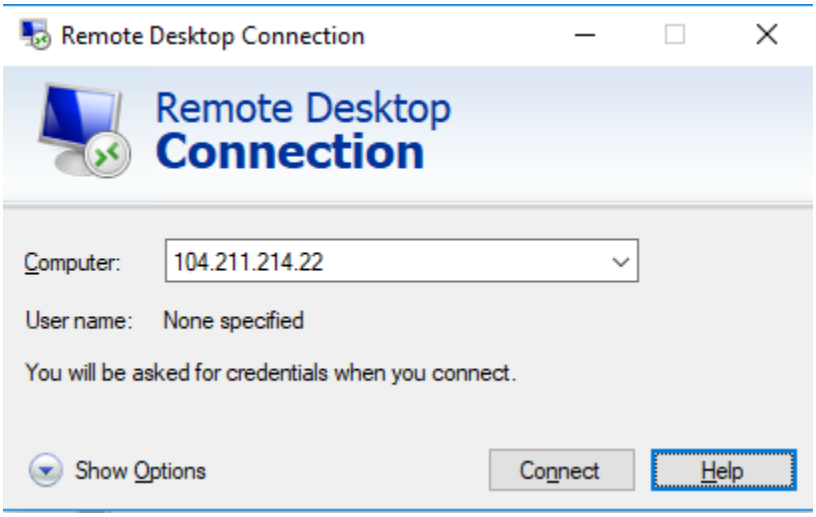


Kindly note the public IP address of **"Windows Server 2008 R2"**.

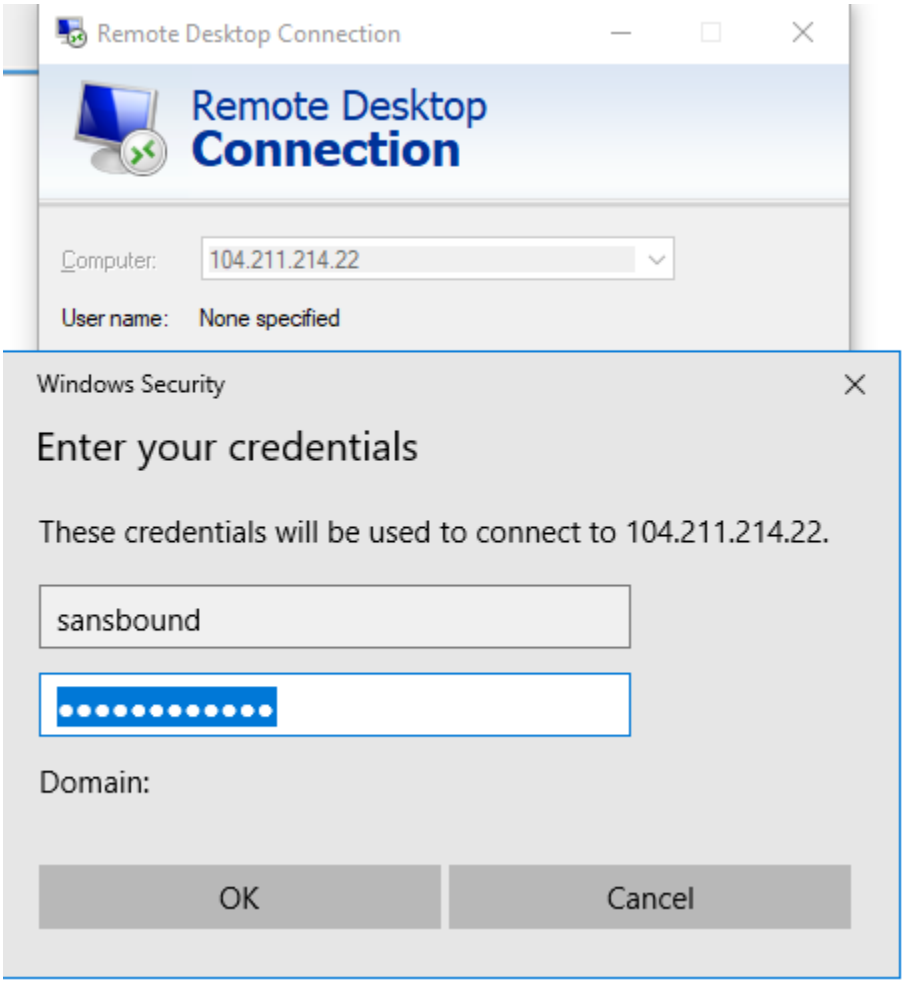


Type **“mstsc”** in your local machine to access the **“Windows Server 2008 R2”** remotely.

Type the public IP address of Windows server in Remote Desktop Connection console and click **“Connect”.**

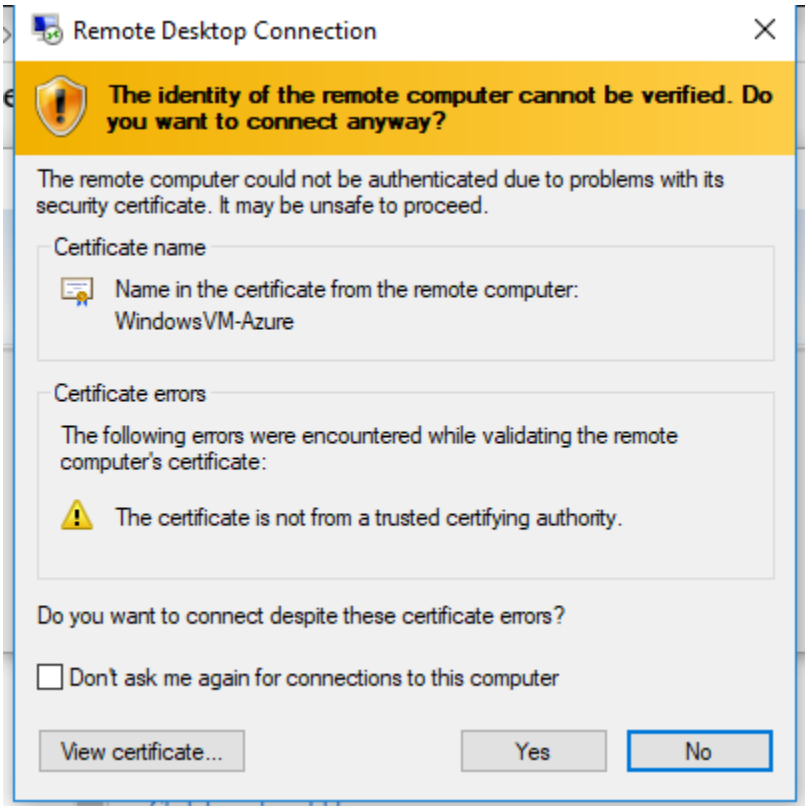


Type **Username and Password** for the Windows 2008 Server R2 which you have provided in Azure portal while creating a virtual machine.



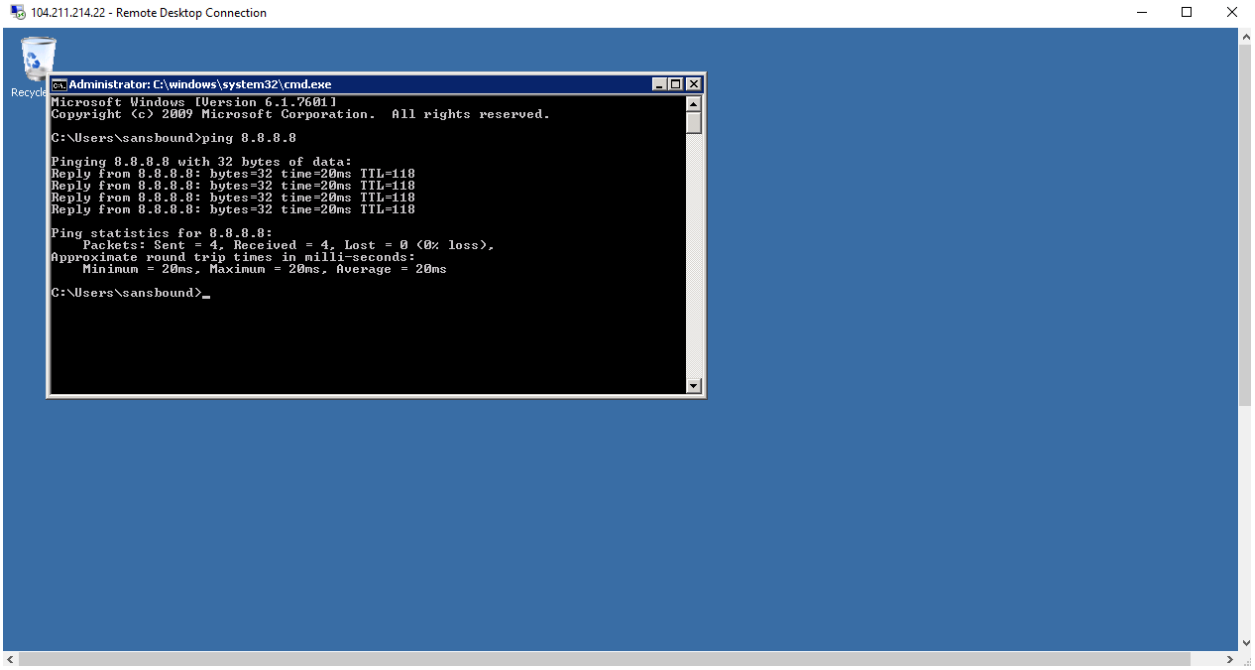
Click **"Ok".**

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

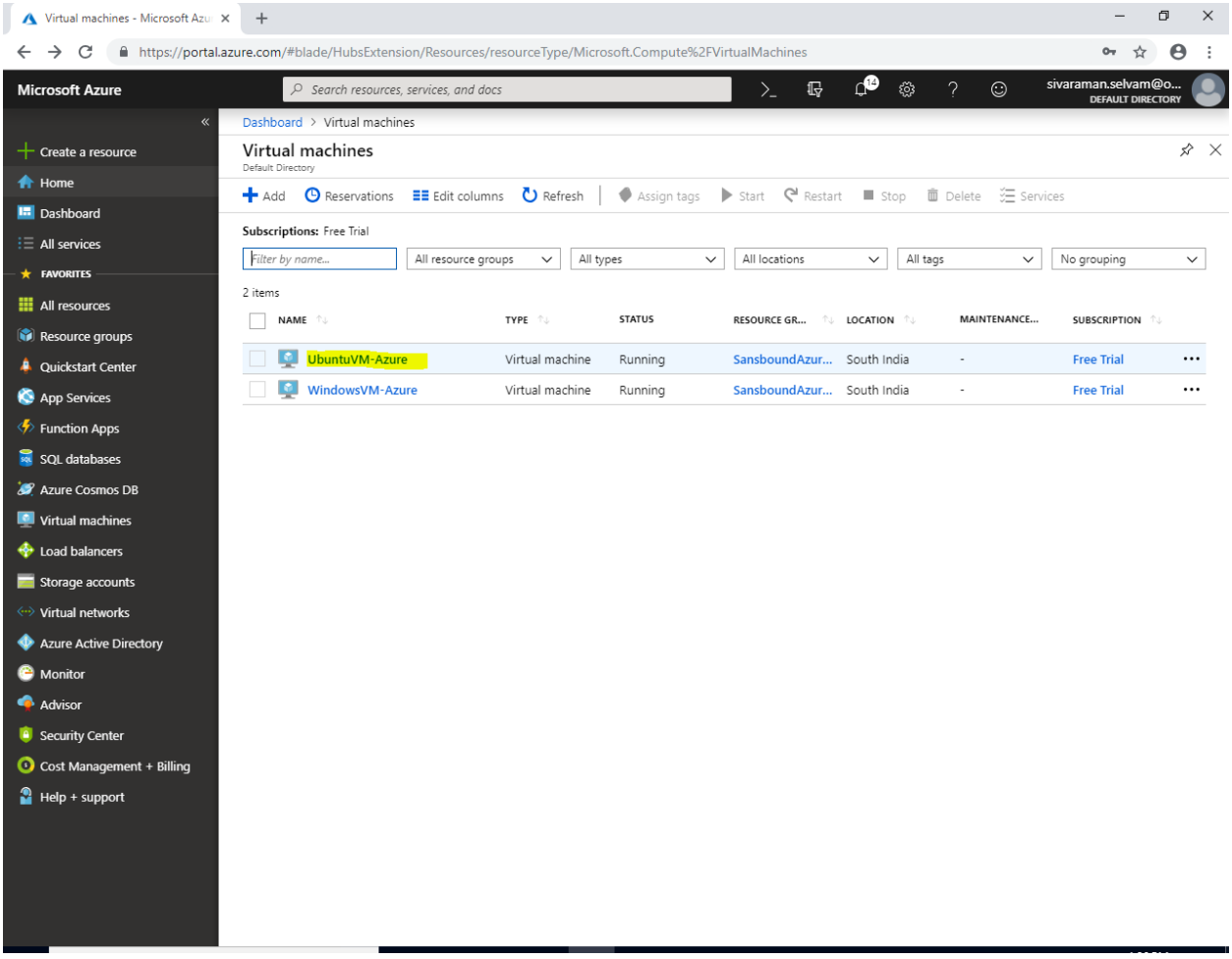
You have accessed windows server through remote successfully.

In Windows Server 2008 R2, I can able to access the internet because the network **10.0.1.0/24** subnet is belongs to Public Network (publicly accessible).

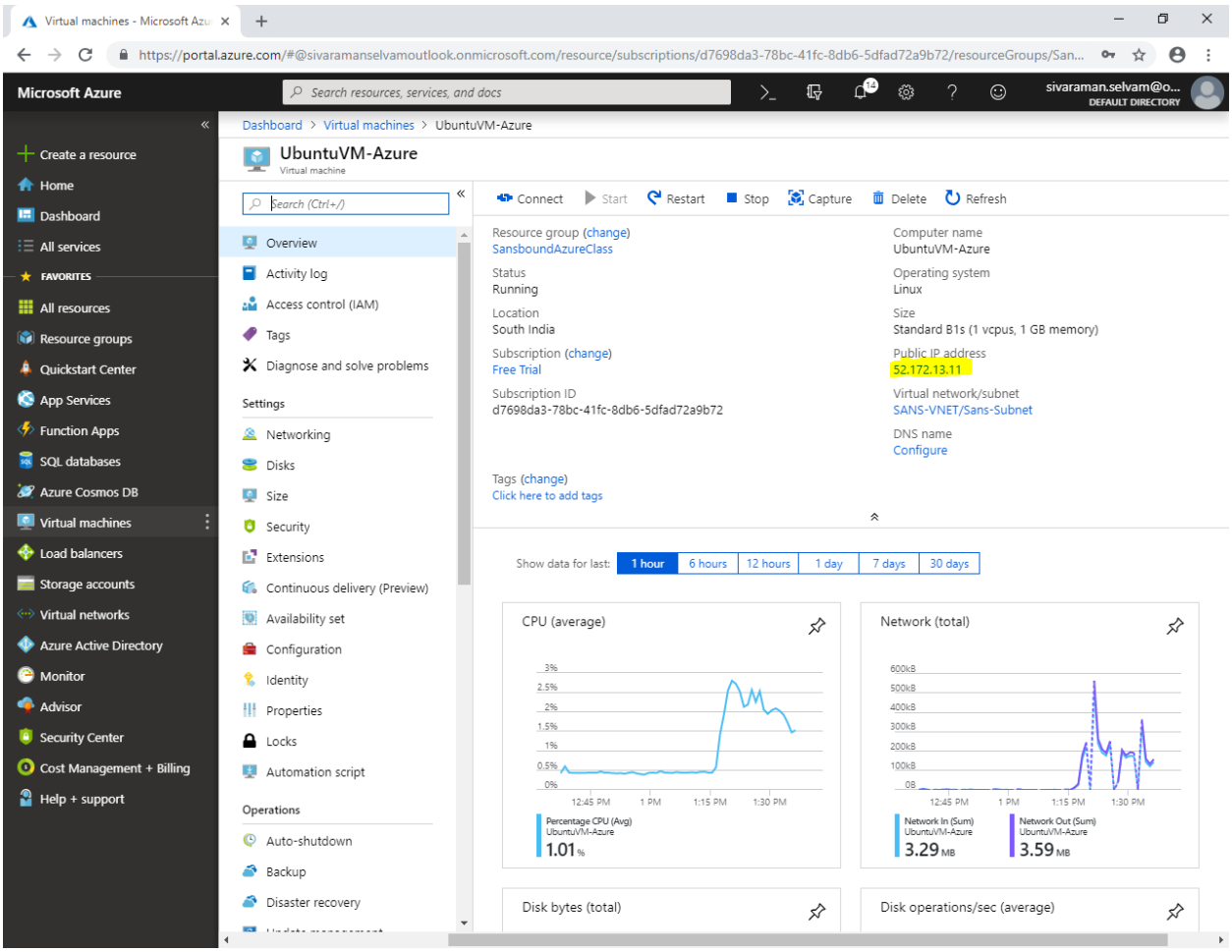


In Dashboard, click **"Virtual machines"**.

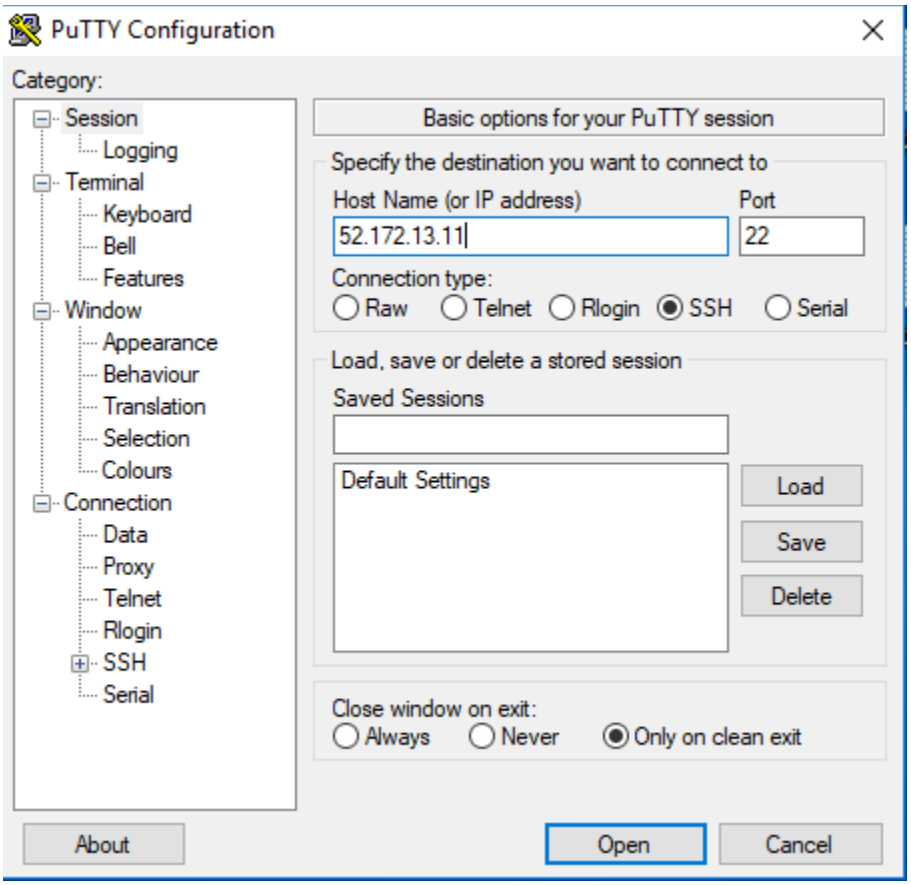
In **"Virtual machines"**, click on **"UbuntuVM-Azure"**.



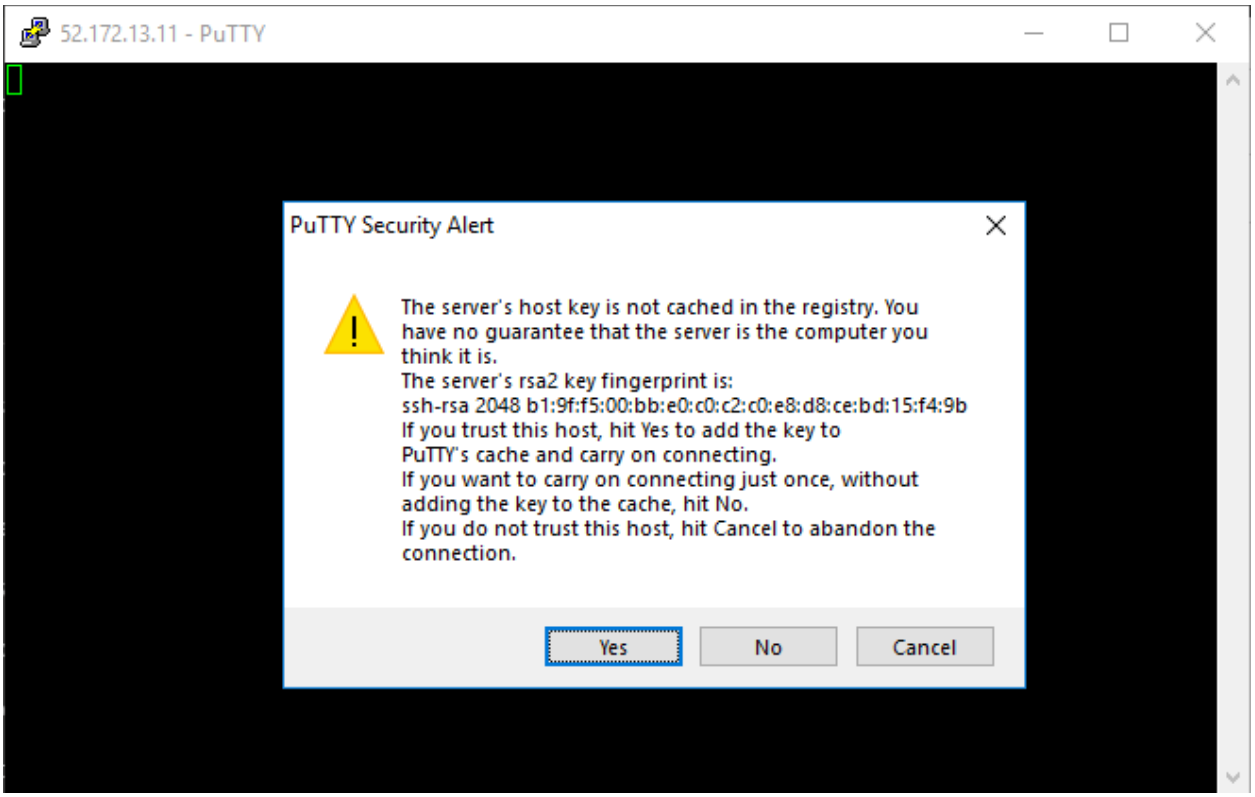
Kindly note the public address provided by azure to access the Ubuntu through SSH.



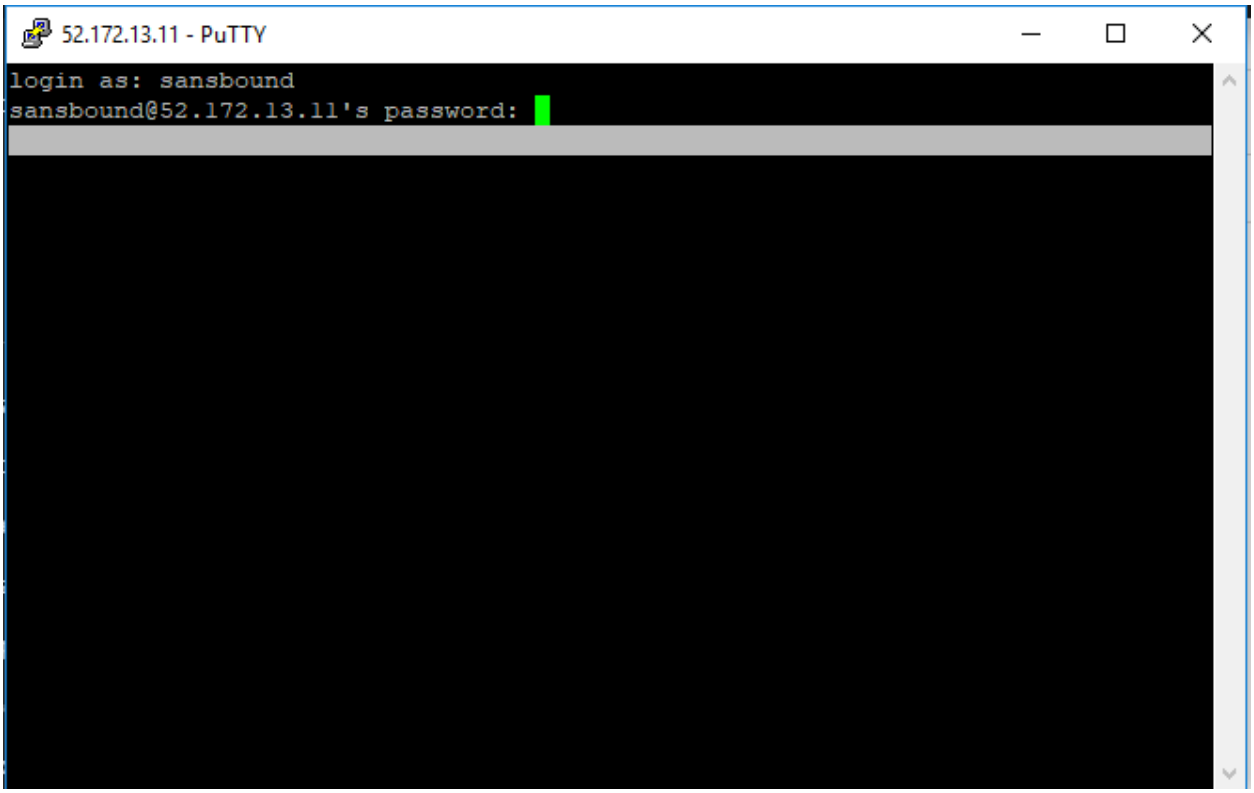
Click **“Open”** to connect “Ubuntu”.



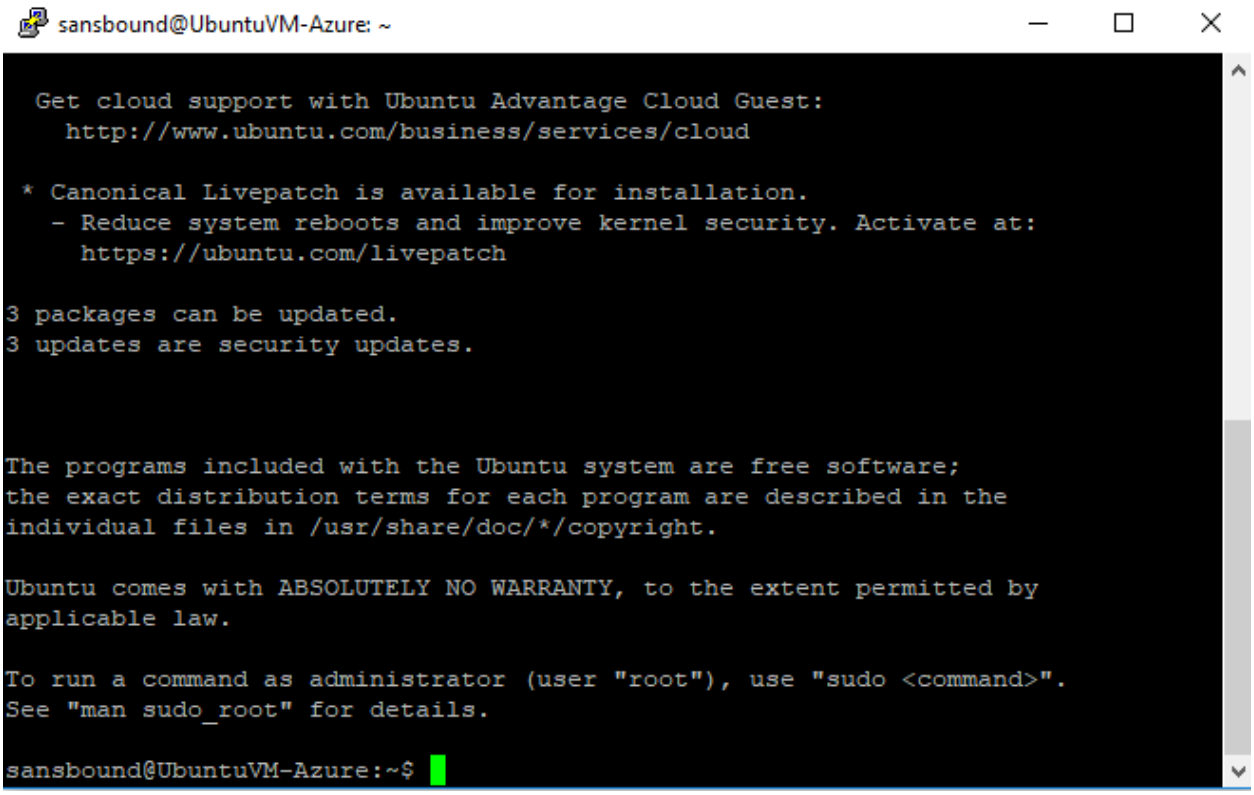
Click **"Yes"**.


52.172.13.11 - 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 rsa2 key fingerprint is:
ssh-rsa 2048 b1:9f:f5:00:bb:e0:c0:c2:c0:e8:d8:ce:bd:15:f4:9b
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

Type user name of the Ubuntu server as **“sansbound”** and press **“Enter”**.



I have successfully logged into the Ubuntu VM successfully.



Earlier days we have created Network Security Group and Allow the required ports while creating the Virtual machine.

But, today we have created Network Security Group manually and understood its features like associate the Network Security Group with Network Interface / Subnet. If we associate the Network Security Group it will applicable for the VM's in entire subnet.