

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 [limits](#) to 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.

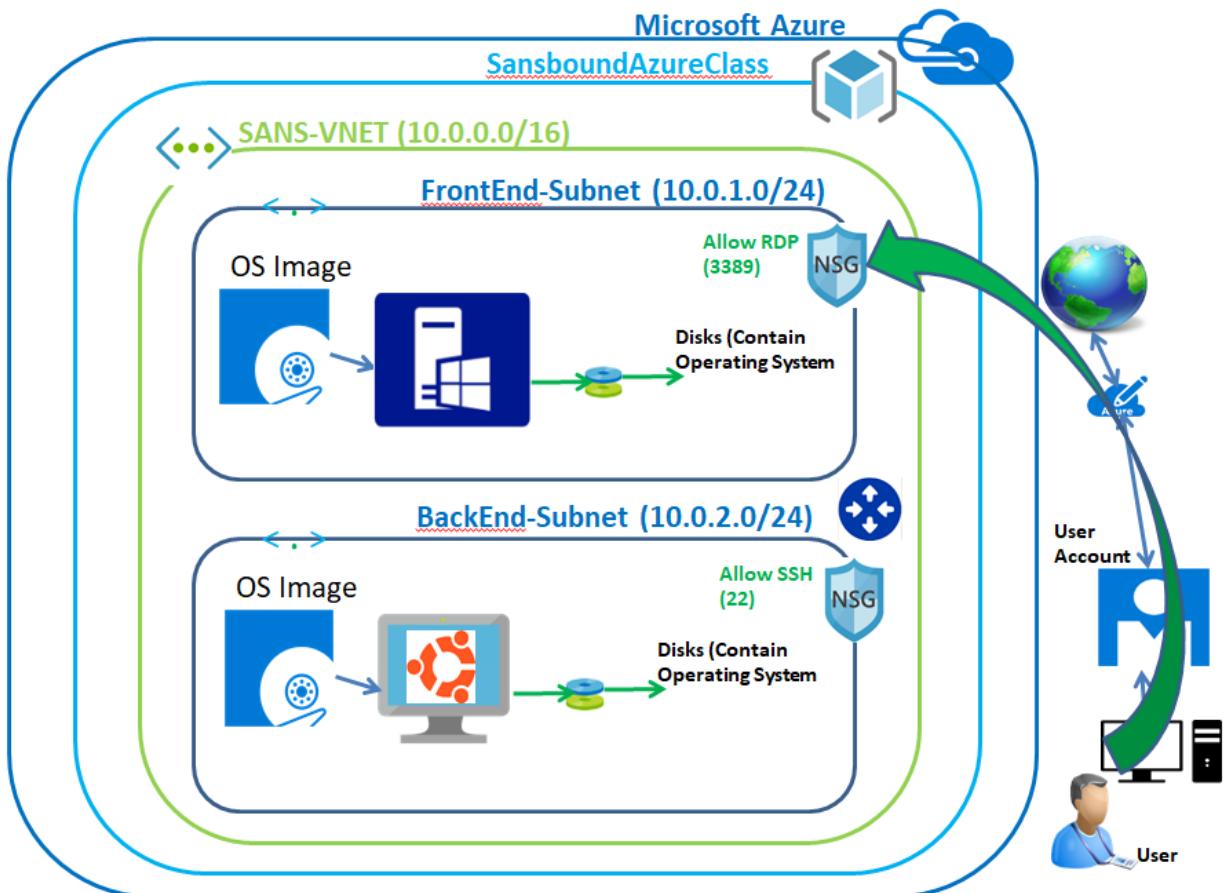
- When you deploy some Azure service resources into a virtual network, they create their own virtual network. To determine whether an Azure service creates its own virtual network, see information for each [Azure service that can be deployed into a virtual network](#).

Subnets

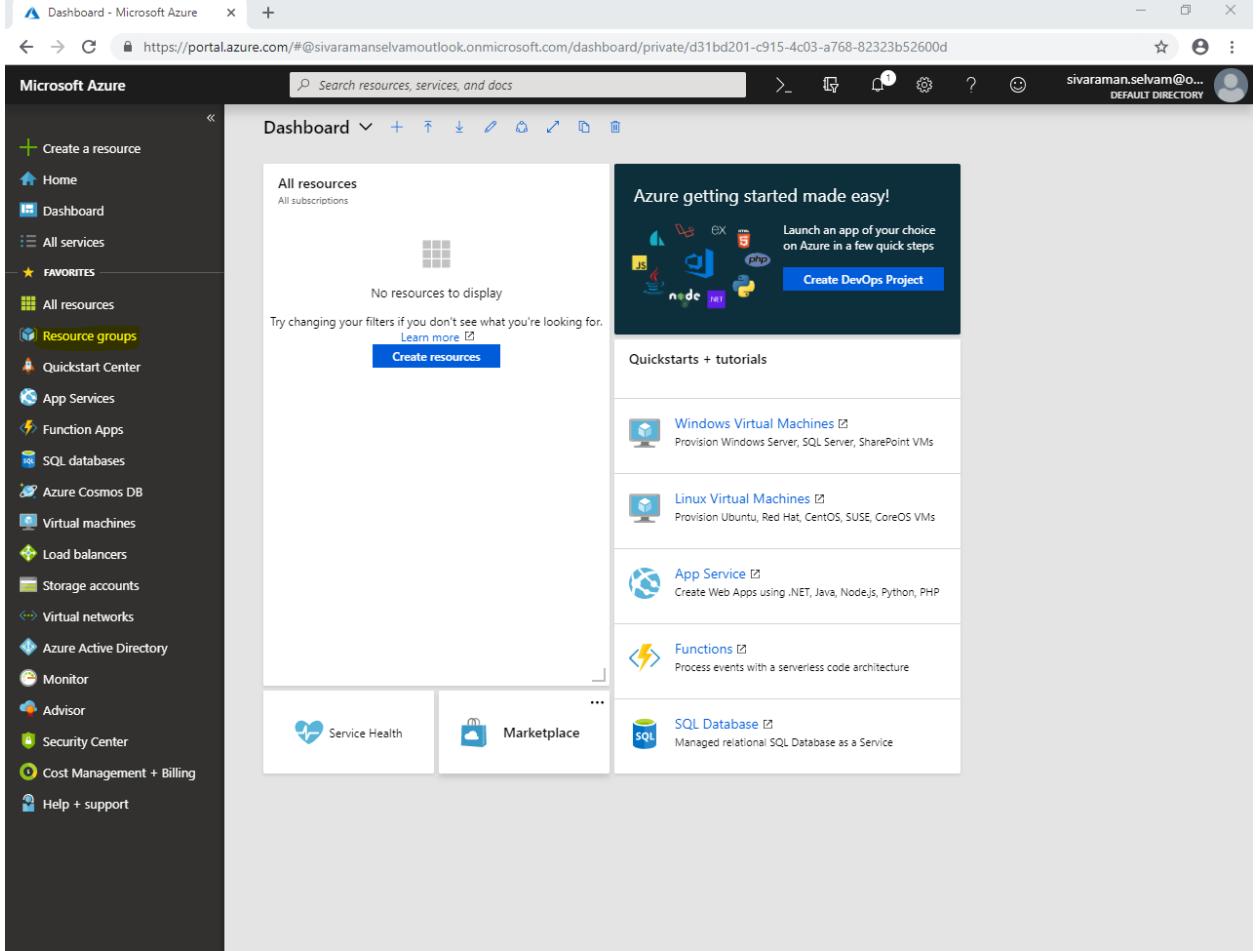
A virtual network can be segmented into one or more subnets up to the [limits](#). Things to consider when deciding whether to create one subnet, or multiple virtual networks in a subscription:

- 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

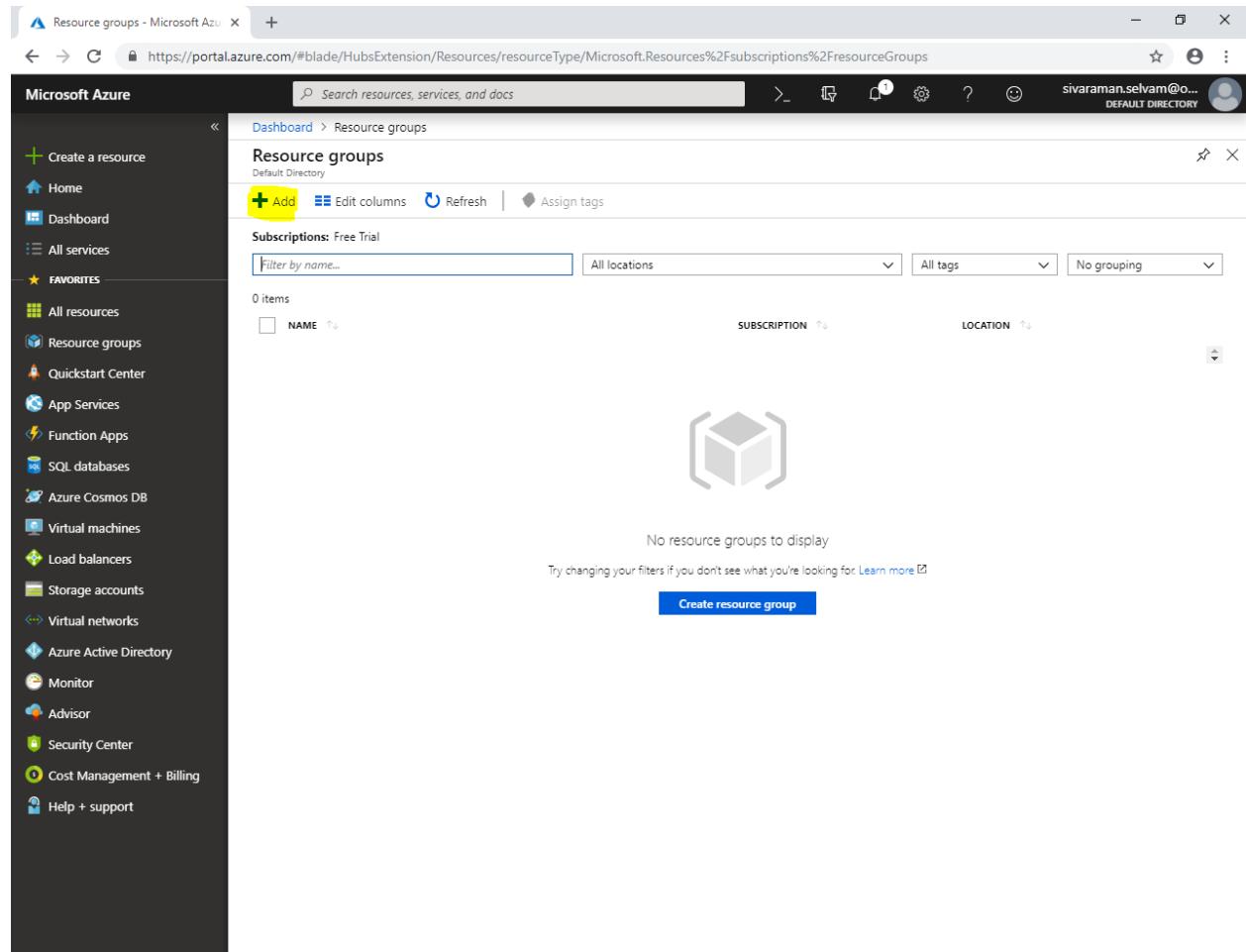


In Azure portal, click “**Resource groups**”.



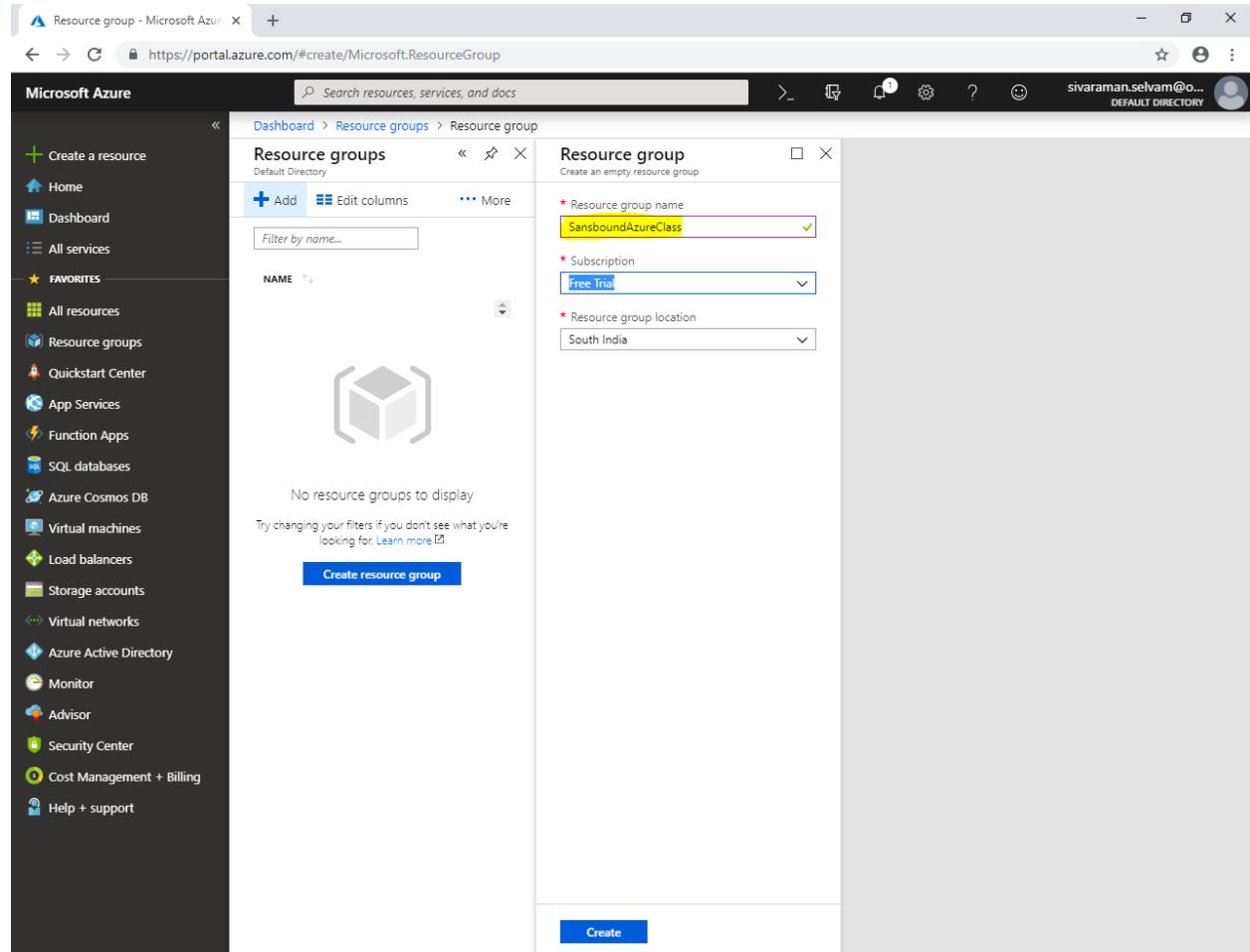
The screenshot shows the Microsoft Azure portal dashboard. On the left, a dark sidebar lists various services, with 'Resource groups' highlighted under the 'FAVORITES' section. The main content area has a heading 'All resources' and a message 'No resources to display'. Below this, there's a 'Create DevOps Project' button and a 'Learn more' link. To the right, a 'Quickstarts + tutorials' section is displayed, featuring links to 'Windows Virtual Machines', 'Linux Virtual Machines', 'App Service', 'Functions', and 'SQL Database', each with a brief description and a small icon.

In “Resource groups” click “Add”.



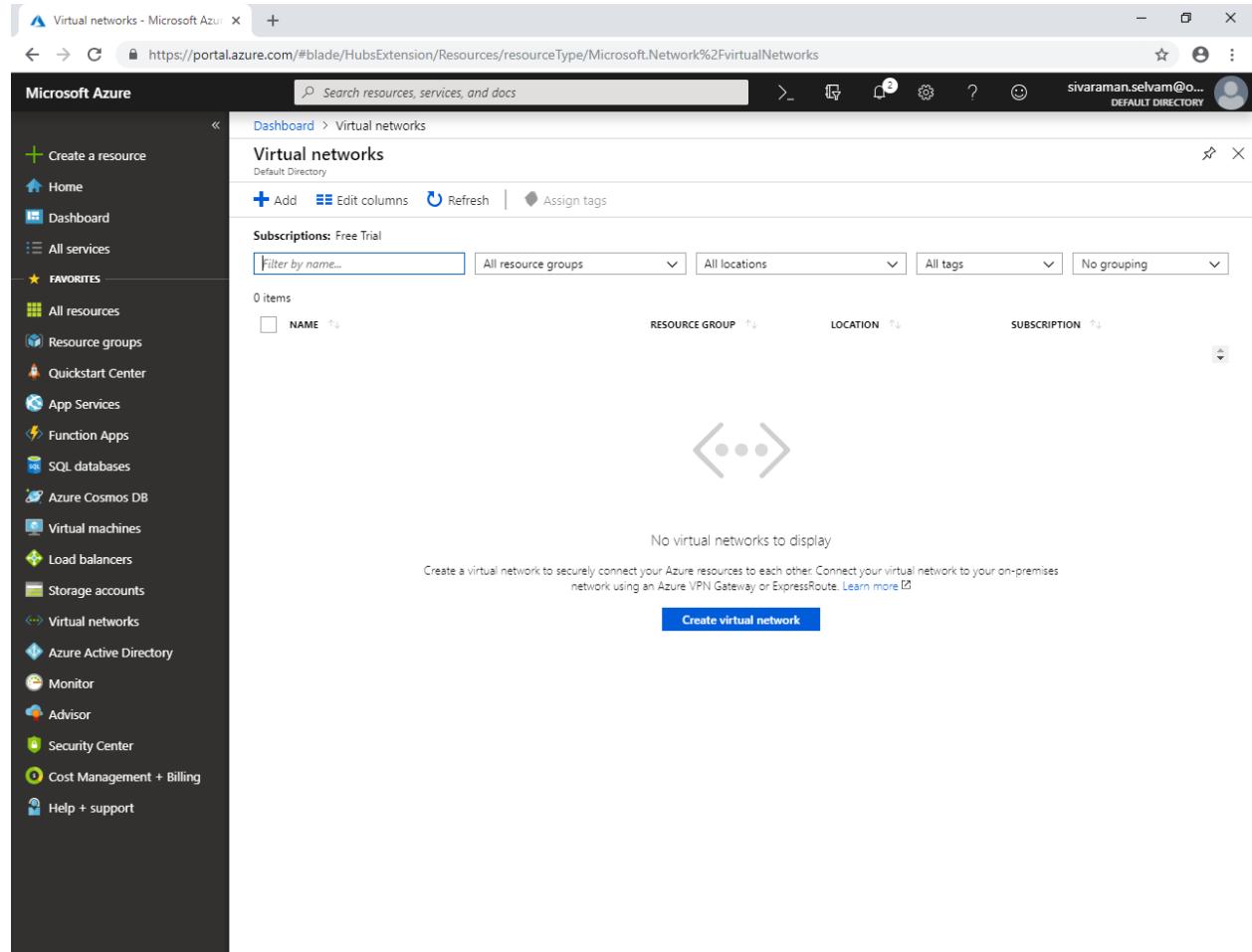
The screenshot shows the Microsoft Azure portal interface. The left sidebar is dark-themed and includes a 'FAVORITES' section with links to various services like All resources, Resource groups, App Services, etc. The main content area is titled 'Resource groups' under 'Dashboard > Resource groups'. It shows a table with one column, 'NAME', which is currently empty. At the top of the table are filters for 'SUBSCRIPTION' and 'LOCATION'. A large, light-gray 3D cube icon is centered above the table. Below the table, a message says 'No resource groups to display' and 'Try changing your filters if you don't see what you're looking for. Learn more'. A prominent blue button at the bottom right of the table area says 'Create resource group'.

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



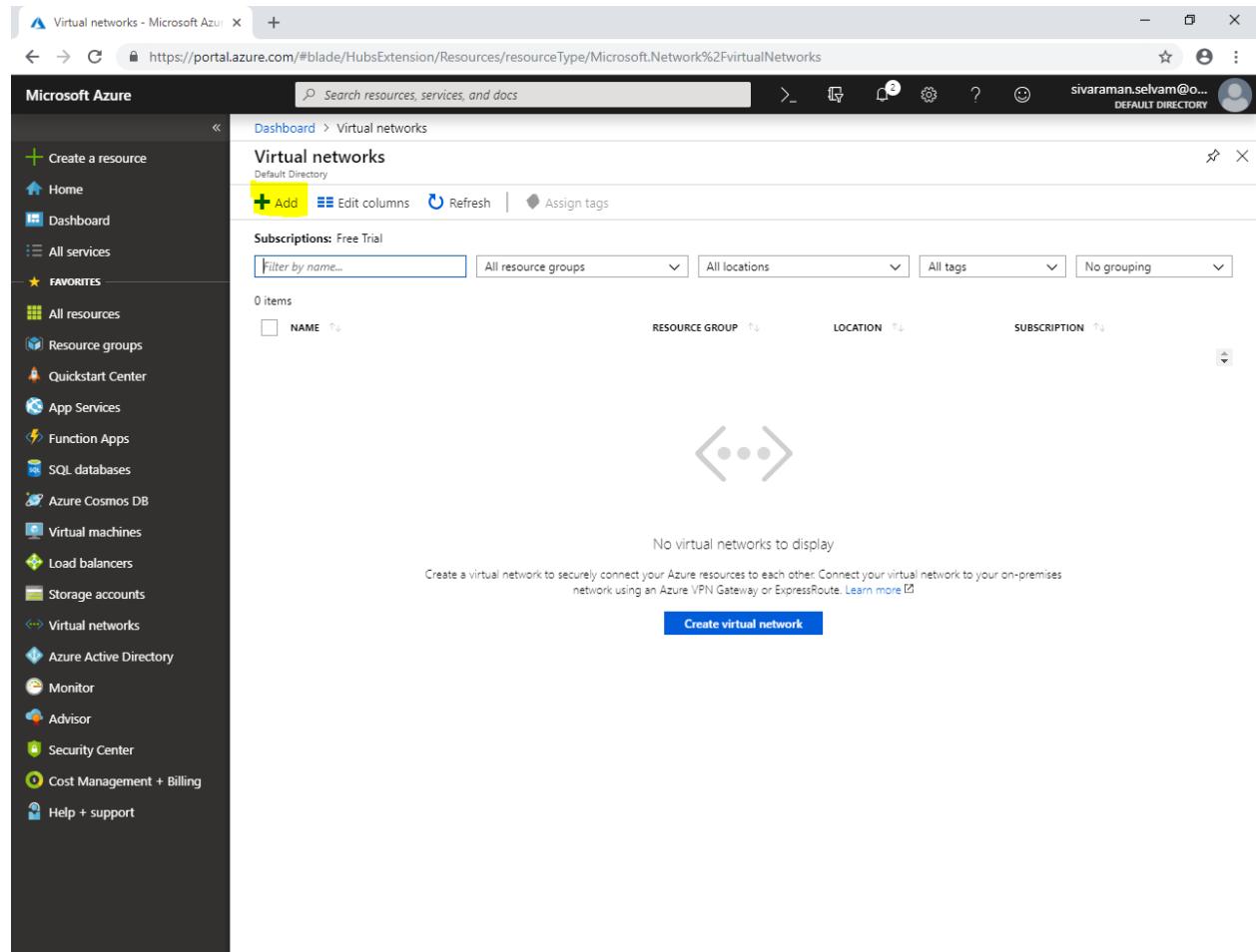
The screenshot shows the Microsoft Azure portal interface for creating a new Resource Group. The left sidebar contains various service links like Home, Dashboard, All services, and Favorites. The main area shows the 'Resource groups' blade with a single resource group listed. A modal window titled 'Resource group' is open, prompting for the 'Resource group name' (set to 'SansboundAzureClass'), 'Subscription' (set to 'Free Trial'), and 'Resource group location' (set to 'South India'). A large blue 'Create' button is at the bottom of the modal.

Click on “Virtual networks” in left side panel.



The screenshot shows the Microsoft Azure portal interface. The left sidebar is dark-themed and includes a 'FAVORITES' section with links to 'Virtual machines', 'Virtual networks', 'Azure Active Directory', 'Monitor', 'Advisor', 'Security Center', 'Cost Management + Billing', and 'Help + support'. The main content area is titled 'Virtual networks' under 'Dashboard > Virtual networks'. It shows a table with one row labeled '0 items'. The columns are 'NAME' (with a sorting arrow), 'RESOURCE GROUP' (with a sorting arrow), 'LOCATION' (with a sorting arrow), and 'SUBSCRIPTION' (with a sorting arrow). Below the table, there is a large placeholder icon with three dots and the text 'No virtual networks to display'. A descriptive message encourages creating a virtual network: '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.' A blue 'Create virtual network' button is located at the bottom right of this message area.

Click “Add”.



The screenshot shows the Microsoft Azure portal interface for managing Virtual networks. The left sidebar contains a navigation menu with various service icons. The main content area is titled "Virtual networks" under the "Dashboard > Virtual networks" path. At the top of the main area, there is a search bar and several filter options: "Filter by name...", "All resource groups", "All locations", "All tags", and "No grouping". Below these filters, a message states "0 items" and includes columns for "NAME", "RESOURCE GROUP", "LOCATION", and "SUBSCRIPTION". A large, semi-transparent "Create virtual network" button is centered at the bottom of the page, with a callout arrow pointing towards it from the text above.

While creating virtual network,

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

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

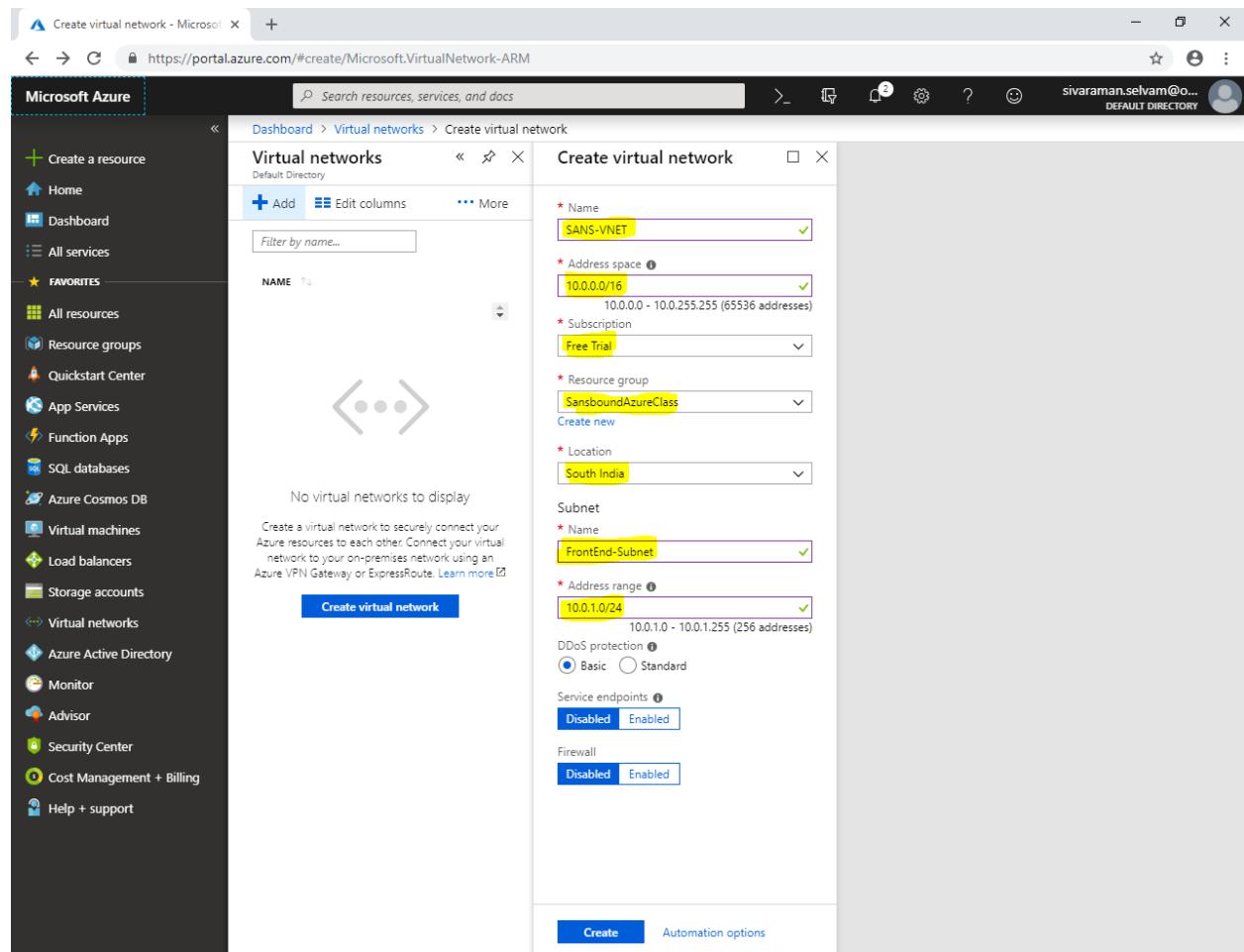
Select “**Subscription**” as “**Free Trial**”.

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**”.

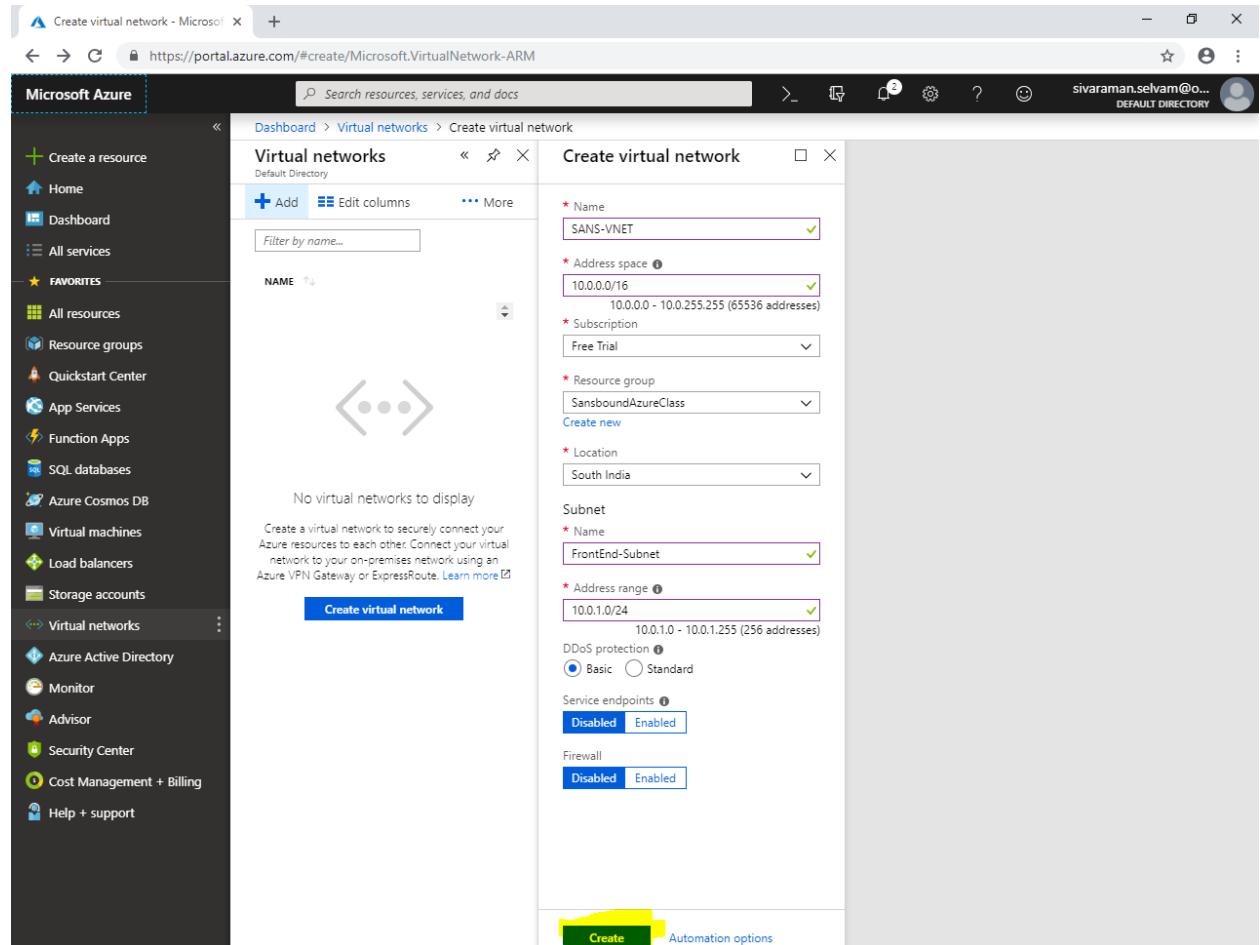


The screenshot shows the Azure portal interface for creating a virtual network. The left sidebar lists various services like Home, Dashboard, All services, Favorites, and Virtual machines. The main area shows the 'Virtual networks' blade with a table of existing networks and a 'Create virtual network' wizard. In the wizard, the following details are entered:

- Name:** SANS-VNET
- Address space:** 10.0.0.0/16
- Subscription:** Free Trial
- Resource group:** SansboundAzureClass
- Location:** South India
- Subnet:** FrontEnd-Subnet
- Address range:** 10.0.1.0/24

At the bottom of the wizard, there are 'Create' and 'Automation options' buttons.

Click “Create”.

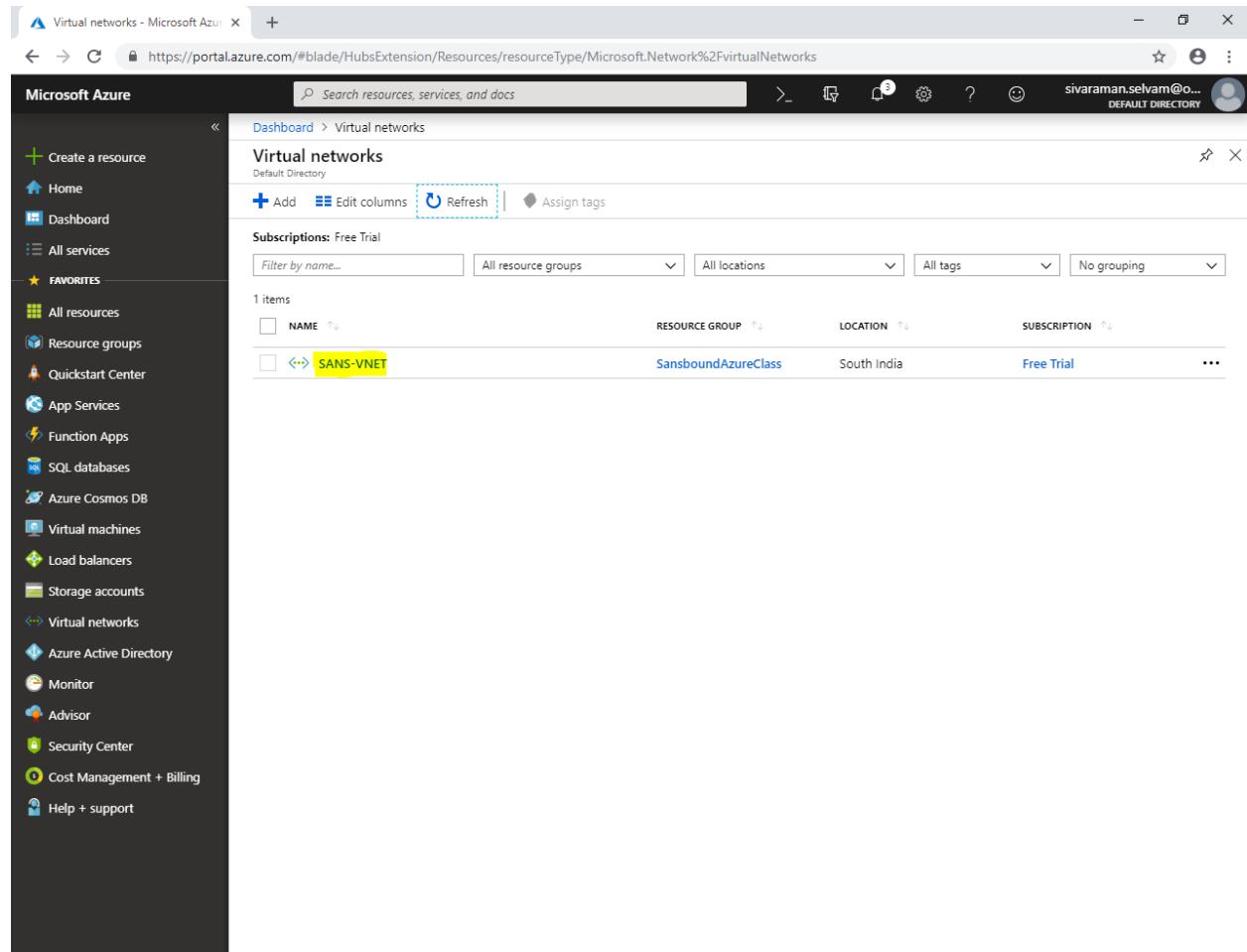


The screenshot shows the Microsoft Azure portal interface for creating a virtual network. The left sidebar contains various service links like Home, Dashboard, All services, Favorites, and Virtual networks. The main area is titled 'Create virtual network' under 'Virtual networks'. The form fields are filled as follows:

- Name:** SANS-VNET
- Address space:** 10.0.0/16 (10.0.0.0 - 10.0.255.255)
- Subscription:** Free Trial
- Resource group:** SansboundAzureClass
- Location:** South India
- Subnet:**
 - Name:** FrontEnd-Subnet
 - Address range:** 10.0.1.0/24 (10.0.1.0 - 10.0.1.255)
 - DDoS protection:** Basic (radio button selected)
 - Service endpoints:** Disabled
 - Firewall:** Disabled

The 'Create' button at the bottom left of the form is highlighted with a yellow box.

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

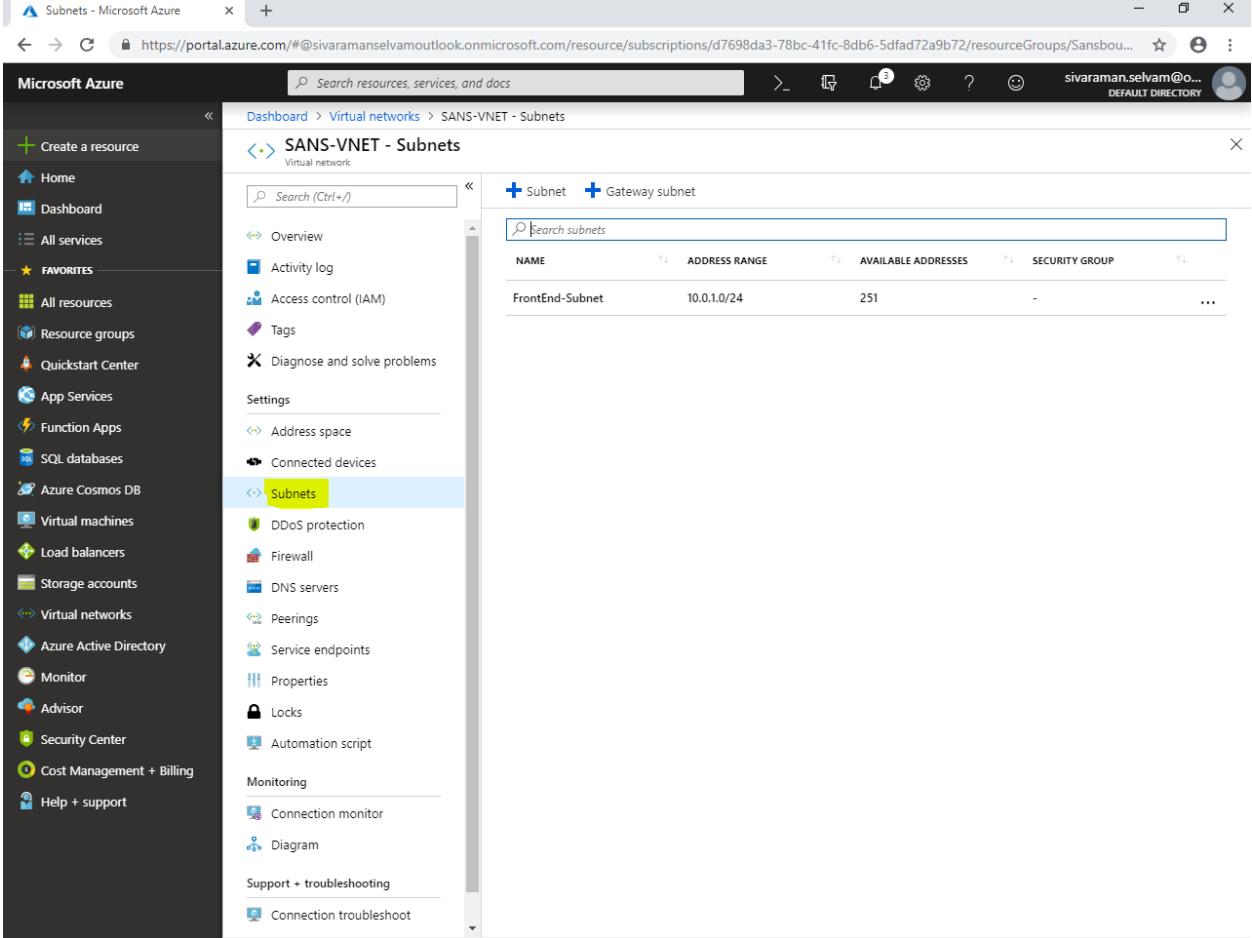


The screenshot shows the Microsoft Azure portal interface. The left sidebar is collapsed, and the main content area is titled "Virtual networks". The URL in the browser bar is <https://portal.azure.com/#blade/HubsExtension/Resources/resourceType/Microsoft.Network%2FvirtualNetworks>. The user's email, "sivaraman.selvam@o...", is visible in the top right corner. The table below lists one item:

NAME	RESOURCE GROUP	LOCATION	SUBSCRIPTION
SANS-VNET	SansboundAzureClass	South India	Free Trial

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

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

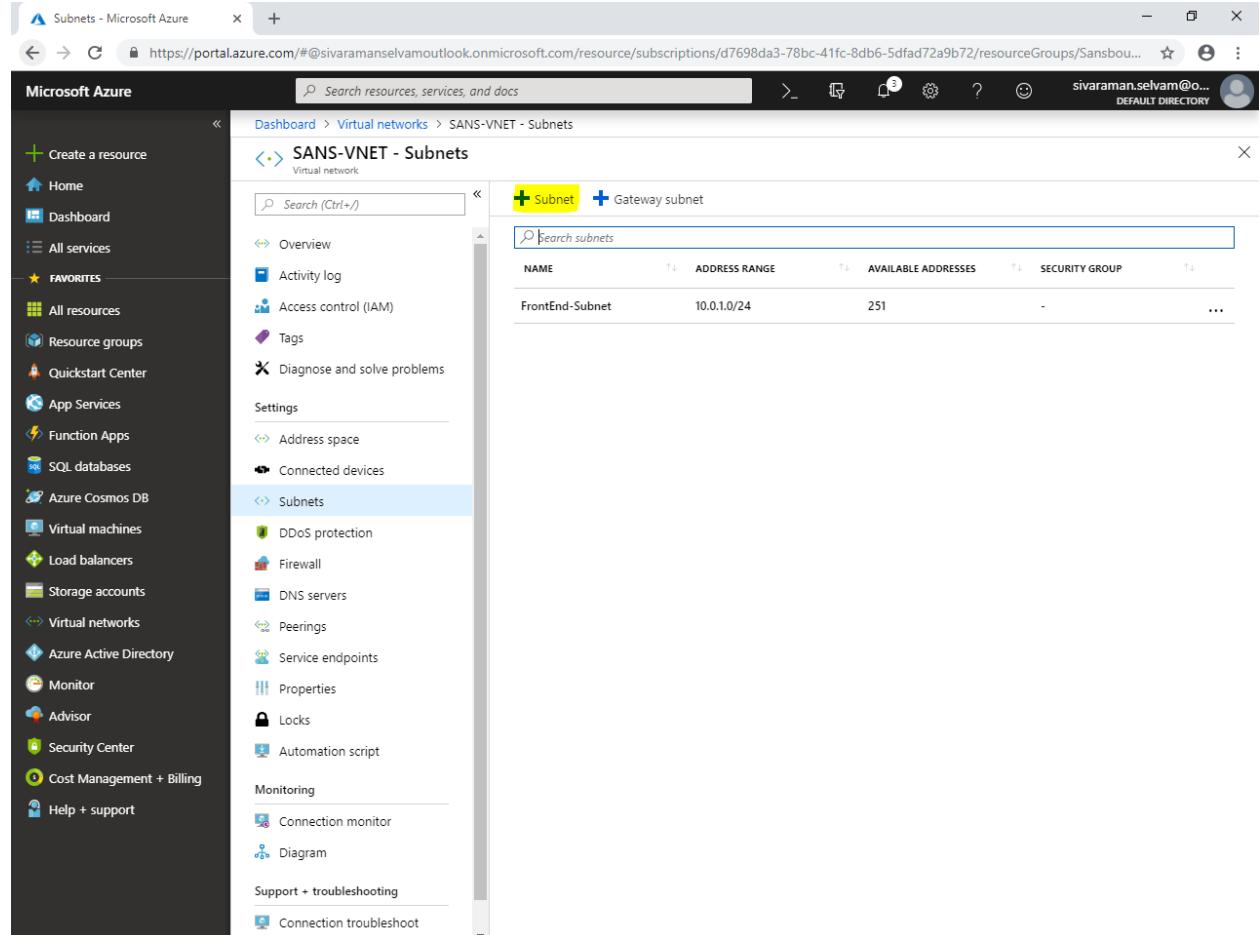


The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation bar is visible, showing various service categories like Home, Dashboard, All services, Favorites, All resources, Resource groups, Quickstart Center, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Billing, and Help + support. Under the Virtual networks section, the 'Subnets' option is highlighted with a yellow box. The main content area displays the 'SANS-VNET - Subnets' page. At the top, there are 'Search resources, services, and docs' and a user profile. Below that, there are 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Settings' (with 'Address space', 'Connected devices', and 'Subnets' selected), 'DDoS protection', 'Firewall', 'DNS servers', 'Peerings', 'Service endpoints', 'Properties', 'Locks', and 'Automation script'. A 'Monitoring' section includes 'Connection monitor' and 'Diagram'. A 'Support + troubleshooting' section has 'Connection troubleshoot'. On the right, there is a table titled 'Search subnets' with columns: NAME, ADDRESS RANGE, AVAILABLE ADDRESSES, and SECURITY GROUP. It lists one entry: 'FrontEnd-Subnet' with '10.0.1.0/24' as the address range and '251' available addresses. There is also a '... more' button.

NAME	ADDRESS RANGE	AVAILABLE ADDRESSES	SECURITY GROUP
FrontEnd-Subnet	10.0.1.0/24	251	-

In “Subnets”

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



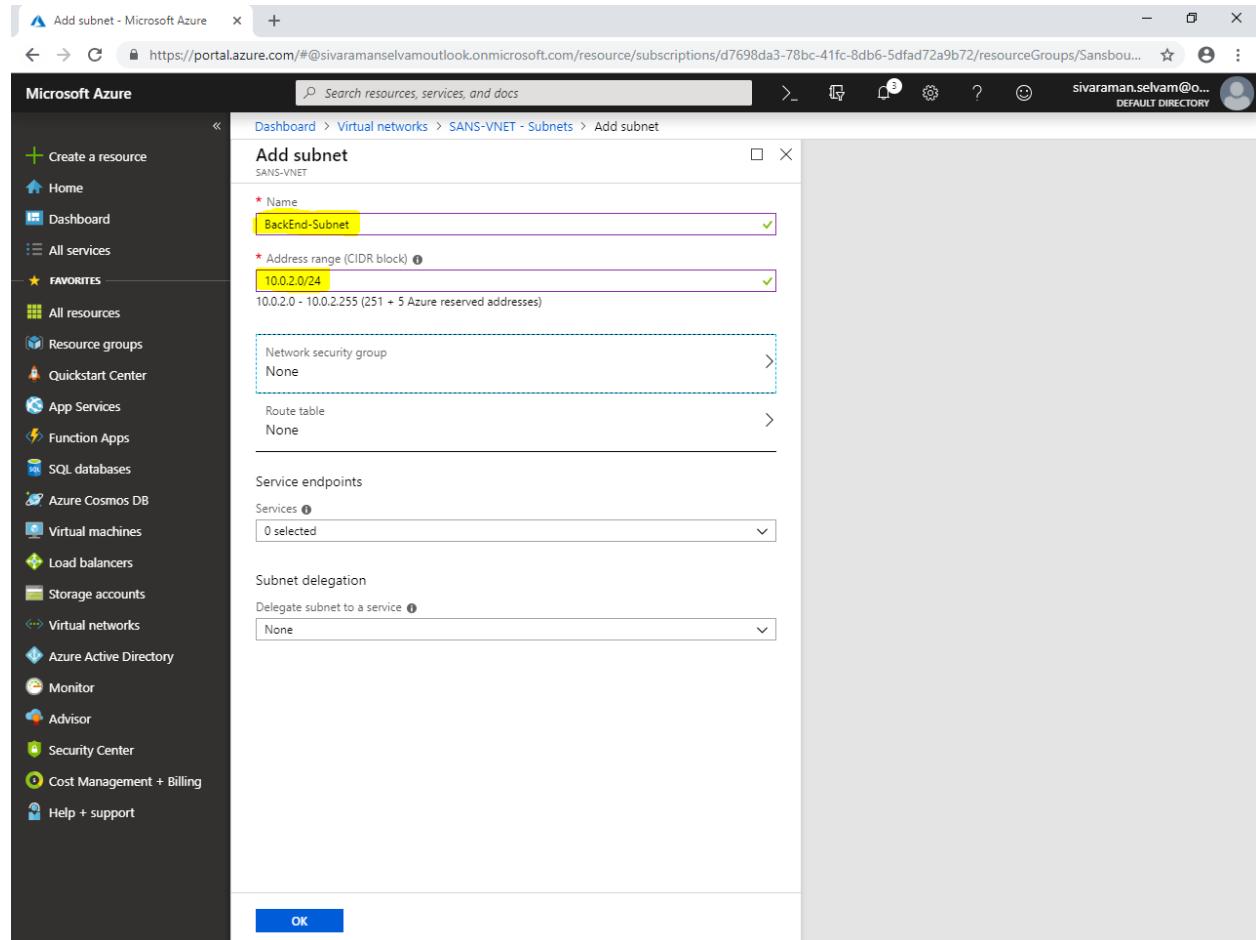
The screenshot shows the Microsoft Azure portal interface for managing subnets. The left sidebar contains a navigation menu with various service icons. The main content area is titled "SANS-VNET - Subnets" under the "Virtual networks" section. A search bar at the top right says "Search resources, services, and docs". Below the title, there are two buttons: "+ Subnet" and "+ Gateway subnet". A table lists the existing subnet "FrontEnd-Subnet" with details: NAME, ADDRESS RANGE (10.0.1.0/24), AVAILABLE ADDRESSES (251), and SECURITY GROUP (-). The "Subnets" option in the sidebar is highlighted with a blue background.

NAME	ADDRESS RANGE	AVAILABLE ADDRESSES	SECURITY GROUP
FrontEnd-Subnet	10.0.1.0/24	251	-

While “Add subnet”.

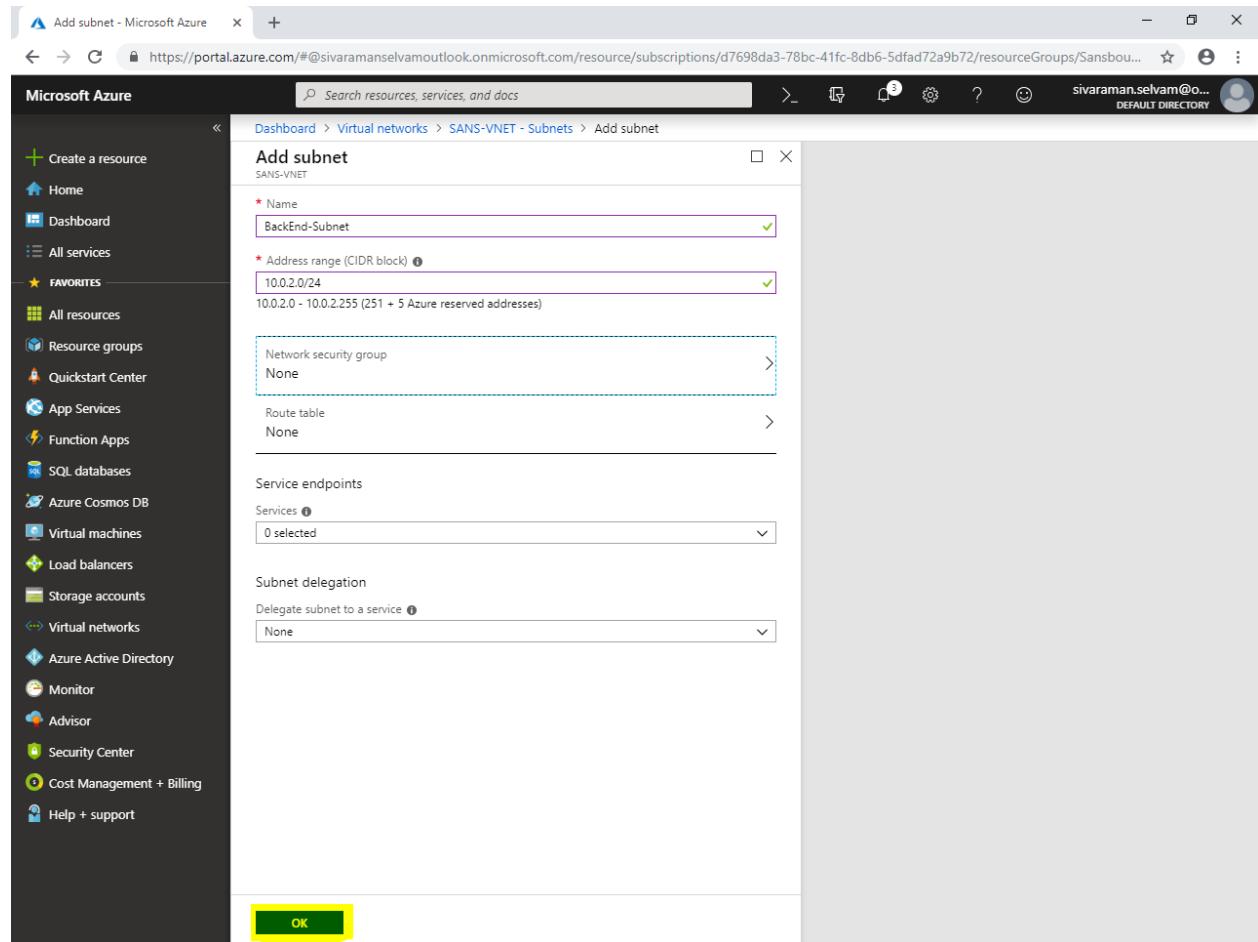
Type “Subnet name” as “**BackEnd-Subnet**”.

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



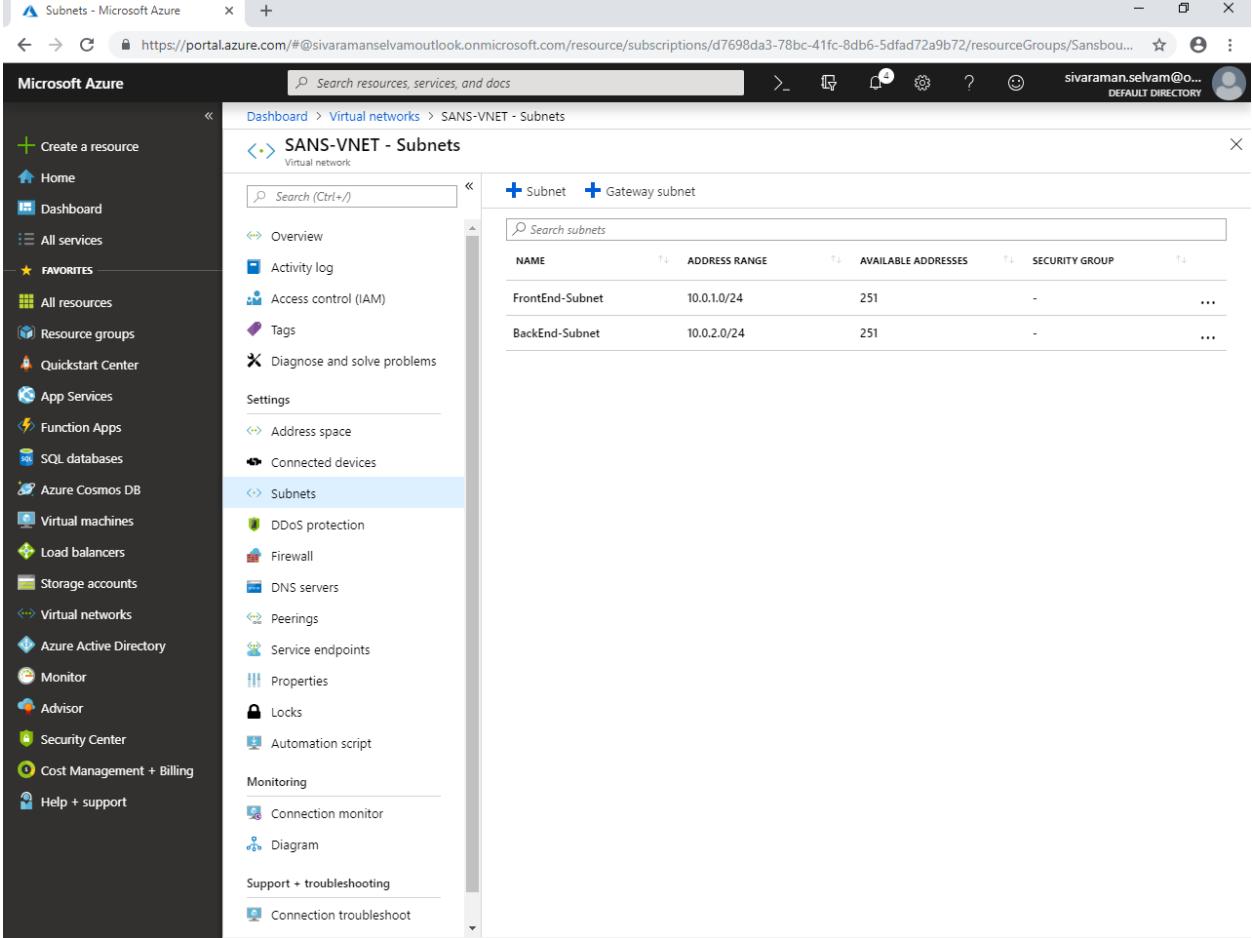
The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons. The main area is titled "Add subnet" under "SANS-VNET". The "Name" field is populated with "BackEnd-Subnet". The "Address range (CIDR block)" field is populated with "10.0.2.0/24". Below these fields, there are sections for "Network security group" (set to "None"), "Route table" (set to "None"), "Service endpoints" (with a dropdown showing "0 selected"), and "Subnet delegation" (with a dropdown showing "None"). At the bottom right of the dialog is a blue "OK" button.

Click “OK”.



In “Subnets”.

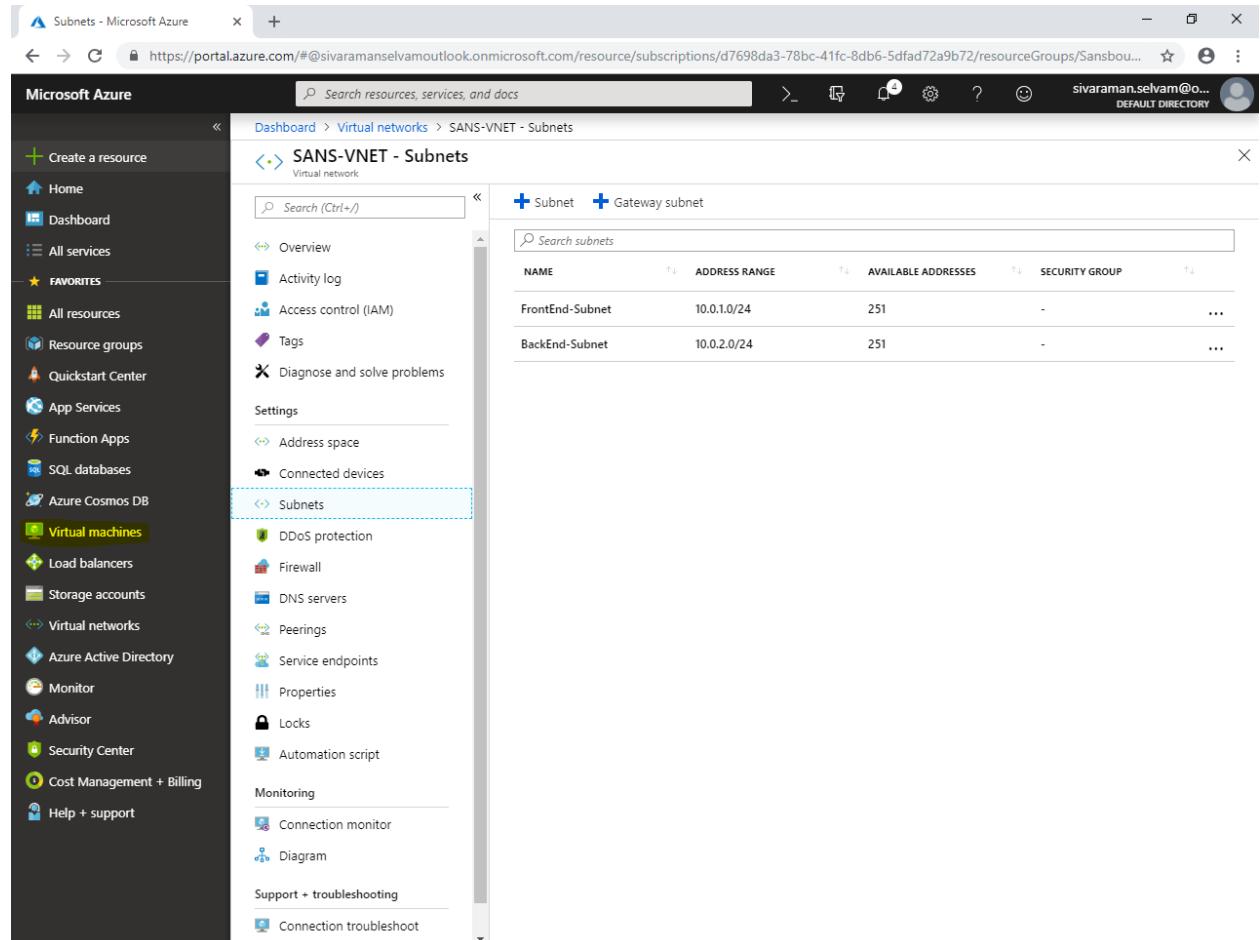
You have created “FrontEnd-Subnet” and “BackEndSubnet”.



The screenshot shows the Microsoft Azure portal interface for managing subnets. The left sidebar contains a navigation menu with various services like 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, and Help + support. The 'Virtual networks' section is expanded, showing options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (with Address space, Connected devices, Subnets selected), Monitoring (with Connection monitor, Diagram), and Support + troubleshooting (with Connection troubleshoot). The main content area displays the 'SANS-VNET - Subnets' page for the 'SANS-VNET' virtual network. It shows a table with two subnets:

NAME	ADDRESS RANGE	AVAILABLE ADDRESSES	SECURITY GROUP
FrontEnd-Subnet	10.0.1.0/24	251	-
BackEnd-Subnet	10.0.2.0/24	251	-

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

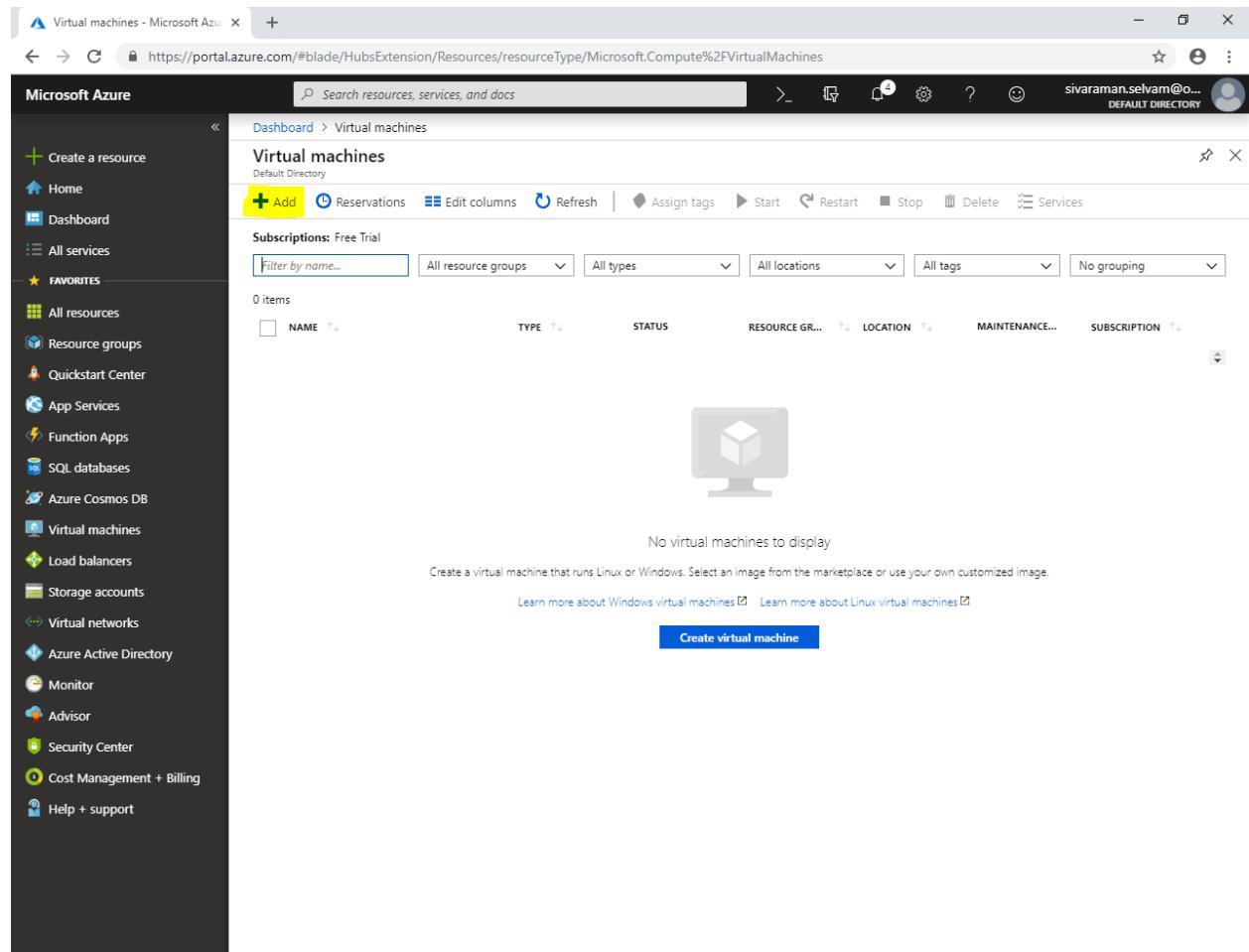


The screenshot shows the Microsoft Azure portal interface. The left sidebar is open, displaying various service categories. The "Virtual machines" icon is highlighted with a yellow box, indicating it is the active section. The main content area is titled "SANS-VNET - Subnets" under the "Virtual networks" section. It shows a list of subnets with the following details:

NAME	ADDRESS RANGE	AVAILABLE ADDRESSES	SECURITY GROUP
FrontEnd-Subnet	10.0.1.0/24	251	-
BackEnd-Subnet	10.0.2.0/24	251	-

In “Virtual machines”,

Click “Add”.



The screenshot shows the Microsoft Azure portal interface. The left sidebar is dark-themed and includes a 'Create a resource' button, followed by a list of services: Home, Dashboard, All services, Favorites (with 'All resources' selected), Resource groups, Quickstart Center, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines (which is the current page), Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Billing, and Help + support. The main content area is titled 'Virtual machines' and shows a table header with columns: NAME, TYPE, STATUS, RESOURCE GRP., LOCATION, MAINTENANCE..., and SUBSCRIPTION. Below the table, there is a large gray placeholder icon of a computer monitor. A message says 'No virtual machines to display'. Below the message, it says 'Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.' and provides links to 'Learn more about Windows virtual machines' and 'Learn more about Linux virtual machines'. At the bottom of the content area is a blue 'Create virtual machine' button.

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

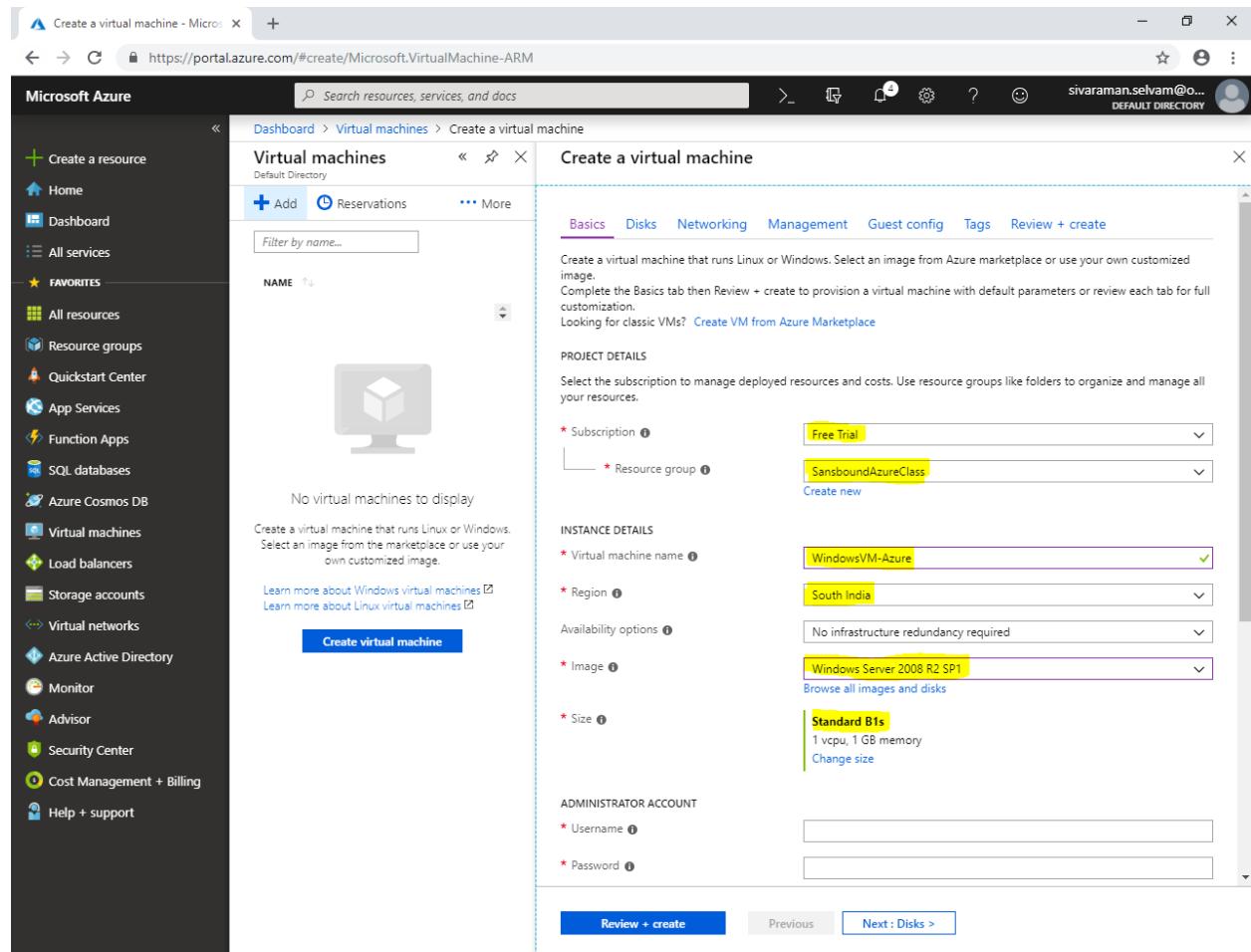
Select “Resource group” as “SansboundAzureClass”.

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”.

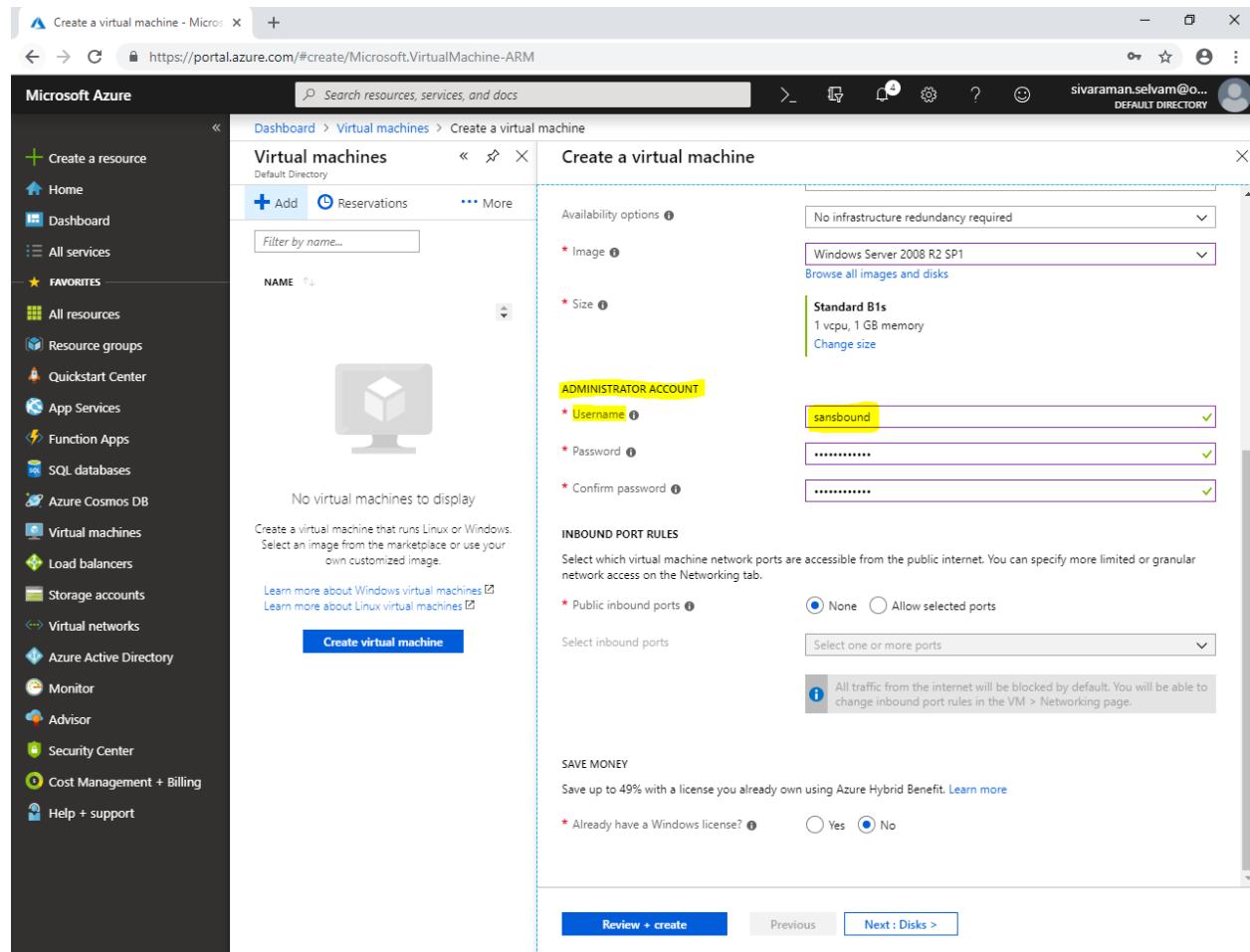


The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar lists various services like Home, Dashboard, and All services. The main area shows the 'Create a virtual machine' wizard. The 'Basics' tab is active, displaying fields for NAME, PROJECT DETAILS (Subscription: Free Trial, Resource group: SansboundAzureClass), INSTANCE DETAILS (Virtual machine name: WindowsVM-Azure, Region: South India, Image: Windows Server 2008 R2 SP1, Size: Standard B1s), and ADMINISTRATOR ACCOUNT (Username and Password fields). The 'Review + create' button is at the bottom.

In “Administrator Account”

Type “username” as “sansbound”.

Type “password” for Windows Server 2008 R2.



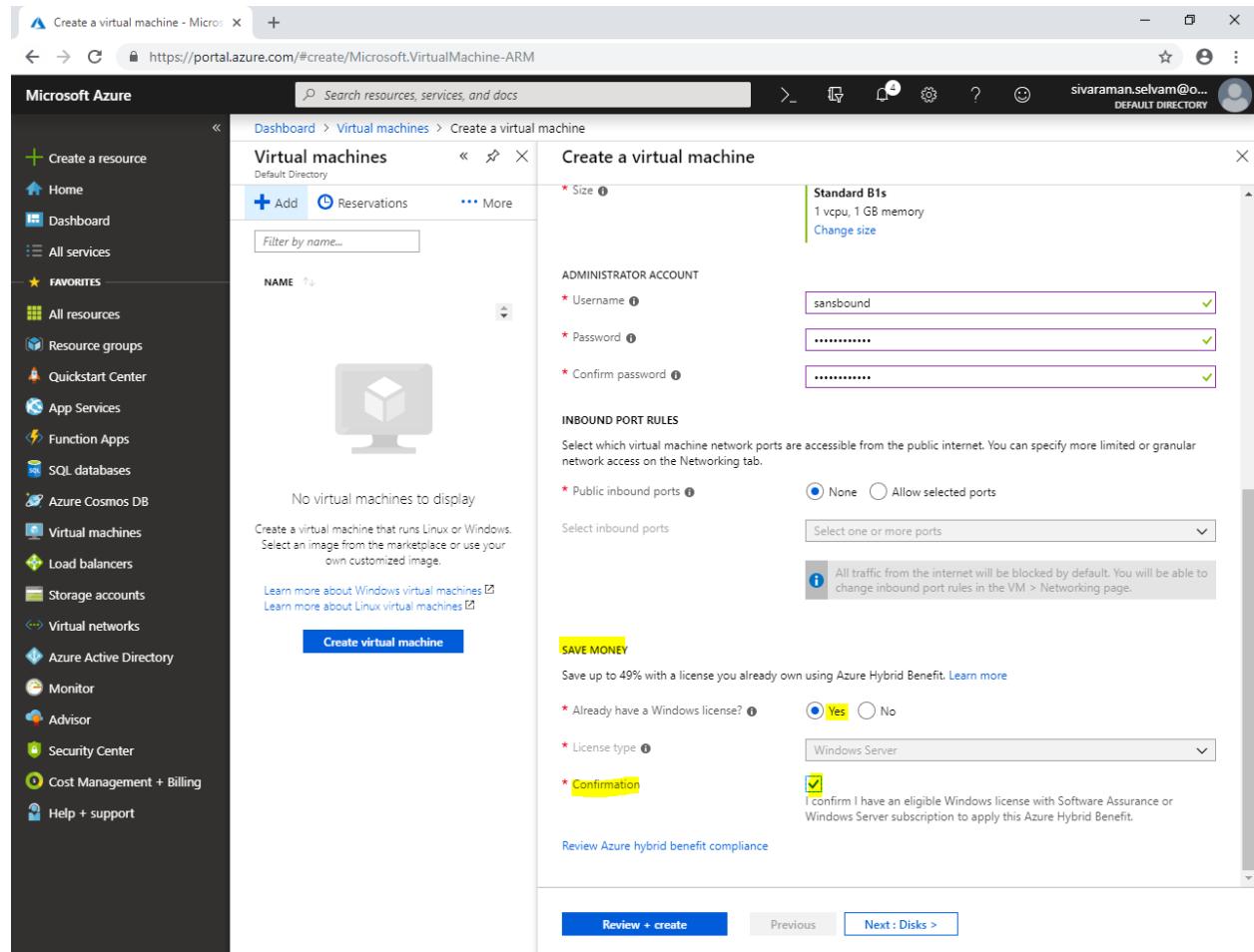
The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar lists various services like Home, Dashboard, All services, and Virtual machines. The main area shows the 'Virtual machines' blade with a 'Create a virtual machine' dialog open. In the 'ADMINISTRATOR ACCOUNT' section, the 'Username' field is set to 'sansbound'. The 'Image' dropdown is set to 'Windows Server 2008 R2 SP1'. Other settings like 'Size' (Standard B1s), 'Availability options', and 'Inbound port rules' are also visible.

In “Save Money”.

Click “Yes” for already have a windows license.

In “Confirmation” need to check.

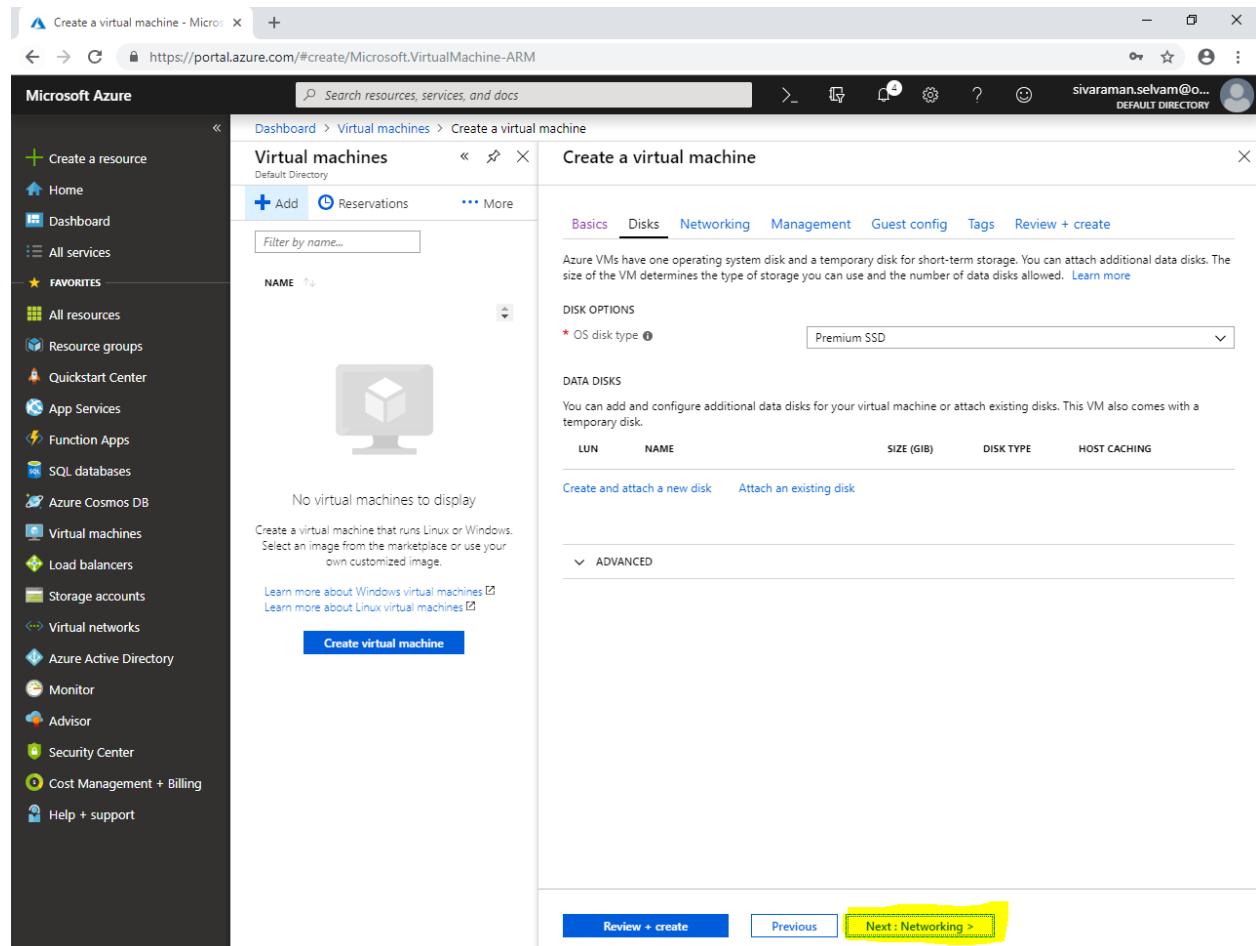
Click “Next : Disks >”.



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar shows various service categories like Home, Dashboard, and Virtual machines. The main area is titled 'Create a virtual machine' under 'Virtual machines'. It's set to 'Standard B1s' (1 vcpu, 1 GB memory). The 'Administrator Account' section has 'Username' set to 'sansbound' and 'Password' and 'Confirm password' both set to '*****'. Under 'INBOUND PORT RULES', 'Public inbound ports' is set to 'None'. A note says 'All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.' In the 'SAVE MONEY' section, 'Already have a Windows license?' has 'Yes' selected. 'License type' is set to 'Windows Server'. 'Confirmation' is checked. At the bottom, there are buttons for 'Review + create', 'Previous', and 'Next : Disks >'.

In “Disks”,

Click “Next : Networking >”.



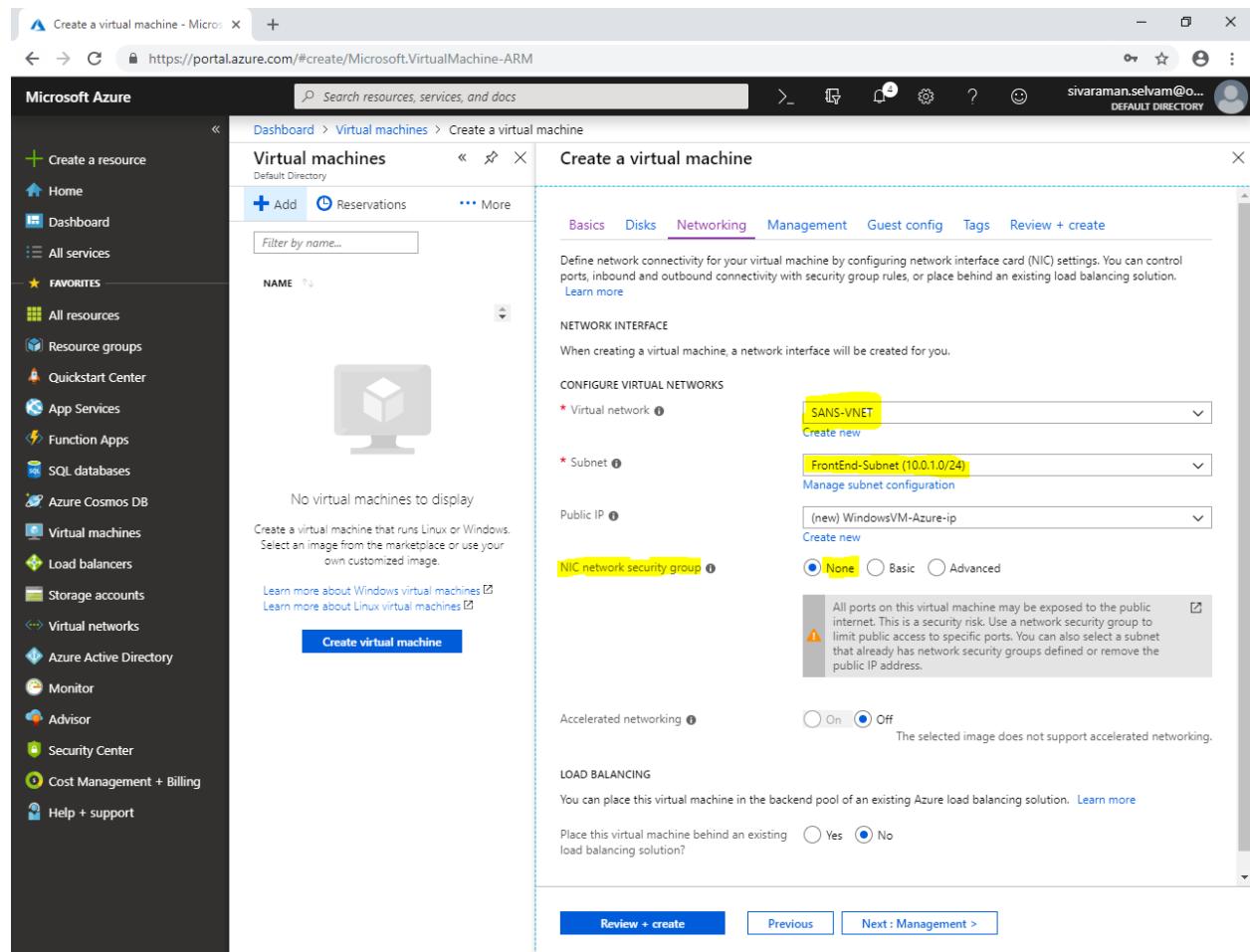
The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains various service icons like Home, Dashboard, All services, Favorites, and more. The main area is titled 'Virtual machines' and shows a list of existing VMs. A 'Create a virtual machine' dialog box is open, currently on the 'Basics' tab. The 'Networking' tab is highlighted with a yellow box. In the 'Networking' section, there's a note about OS disk type, with 'Premium SSD' selected. Below that, under 'DATA DISKS', it says you can add and configure additional data disks or attach existing ones. At the bottom of the dialog, there are buttons for 'Review + create', 'Previous', and 'Next : Networking >' (which is also highlighted with a yellow box).

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.

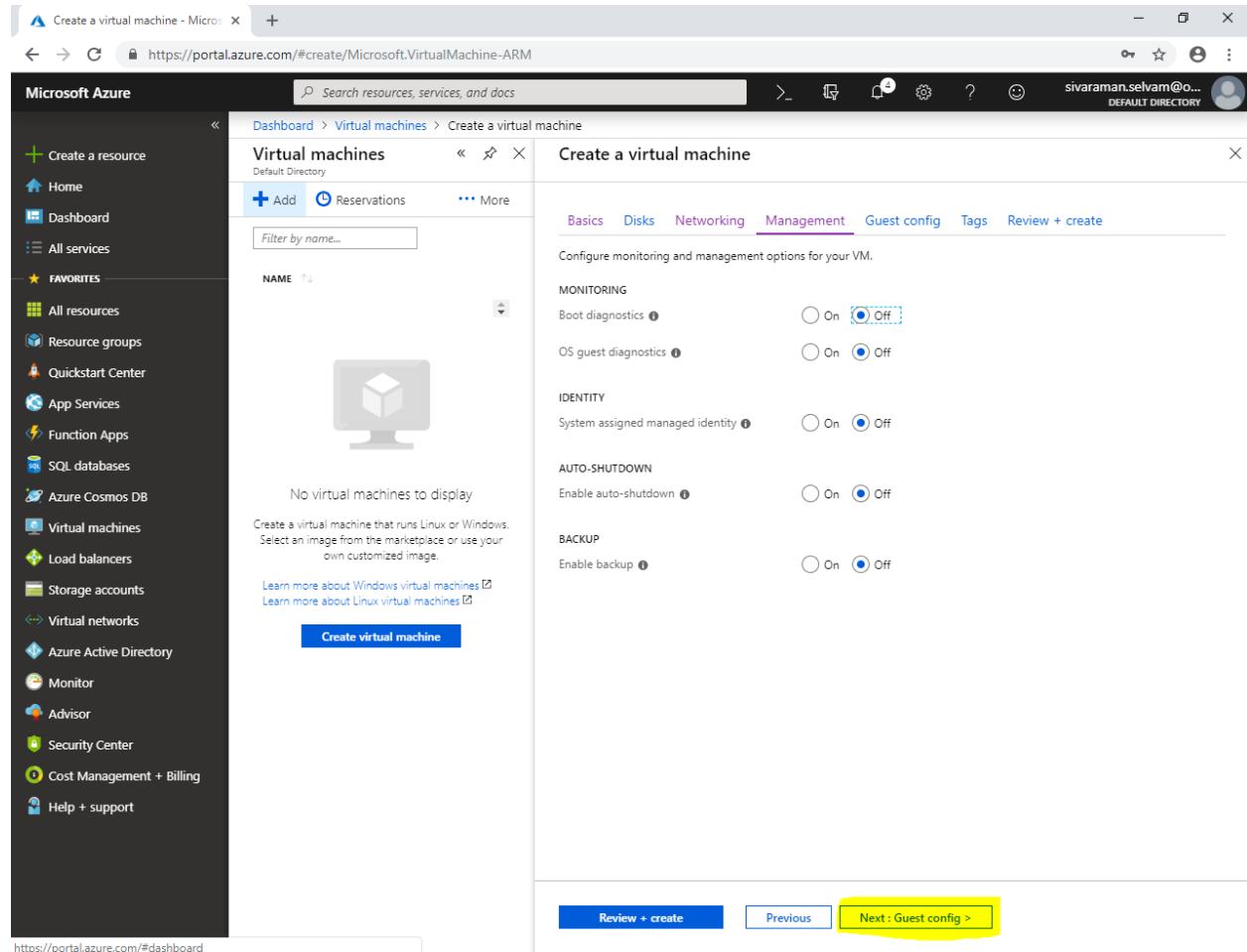
In “NIC network security group” as “**None**”.



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar lists various services like Home, Dashboard, and Virtual machines. The main area is titled 'Create a virtual machine' under 'Virtual machines'. The 'Networking' tab is selected. In the 'CONFIGURE VIRTUAL NETWORKS' section, the 'Virtual network' dropdown is set to 'SANS-VNET' and the 'Subnet' dropdown is set to 'FrontEnd-Subnet (10.0.1.0/24)'. The 'Public IP' dropdown shows '(new) WindowsVM-Azure-ip'. Under 'NIC network security group', the 'None' radio button is selected. A note below states: 'All ports on this virtual machine may be exposed to the public internet. This is a security risk. Use a network security group to limit public access to specific ports. You can also select a subnet that already has network security groups defined or remove the public IP address.' At the bottom, 'Accelerated networking' is turned off ('Off') and there's a note that the selected image does not support accelerated networking. The 'LOAD BALANCING' section is collapsed. At the very bottom are 'Review + create', 'Previous', and 'Next : Management >' buttons.

In “Management”

Click “Next : Guest config >”.



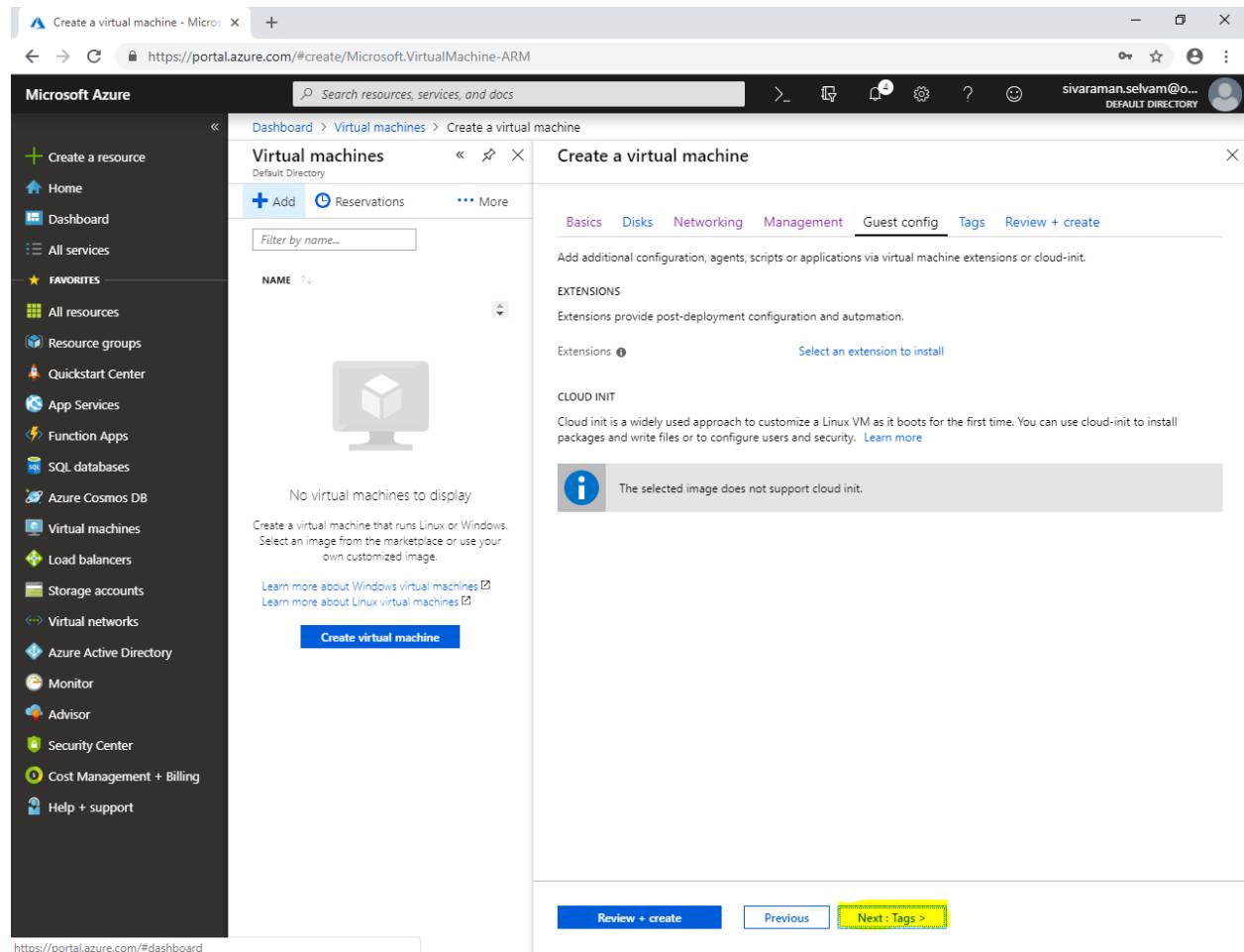
The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains various service icons like Home, Dashboard, and Resource groups. The main area is titled 'Create a virtual machine' and is currently on the 'Guest config' tab. The configuration options shown include:

- MONITORING:** Boot diagnostics (radio button set to Off), OS guest diagnostics (radio button set to Off).
- IDENTITY:** System assigned managed identity (radio button set to Off).
- AUTO-SHUTDOWN:** Enable auto-shutdown (radio button set to Off).
- BACKUP:** Enable backup (radio button set to Off).

At the bottom of the wizard, there are three buttons: 'Review + create' (blue), 'Previous' (gray), and 'Next : Guest config >' (highlighted with a yellow box). The URL in the browser bar is <https://portal.azure.com/#create/Microsoft.VirtualMachine-ARM>.

In “Guest config”.

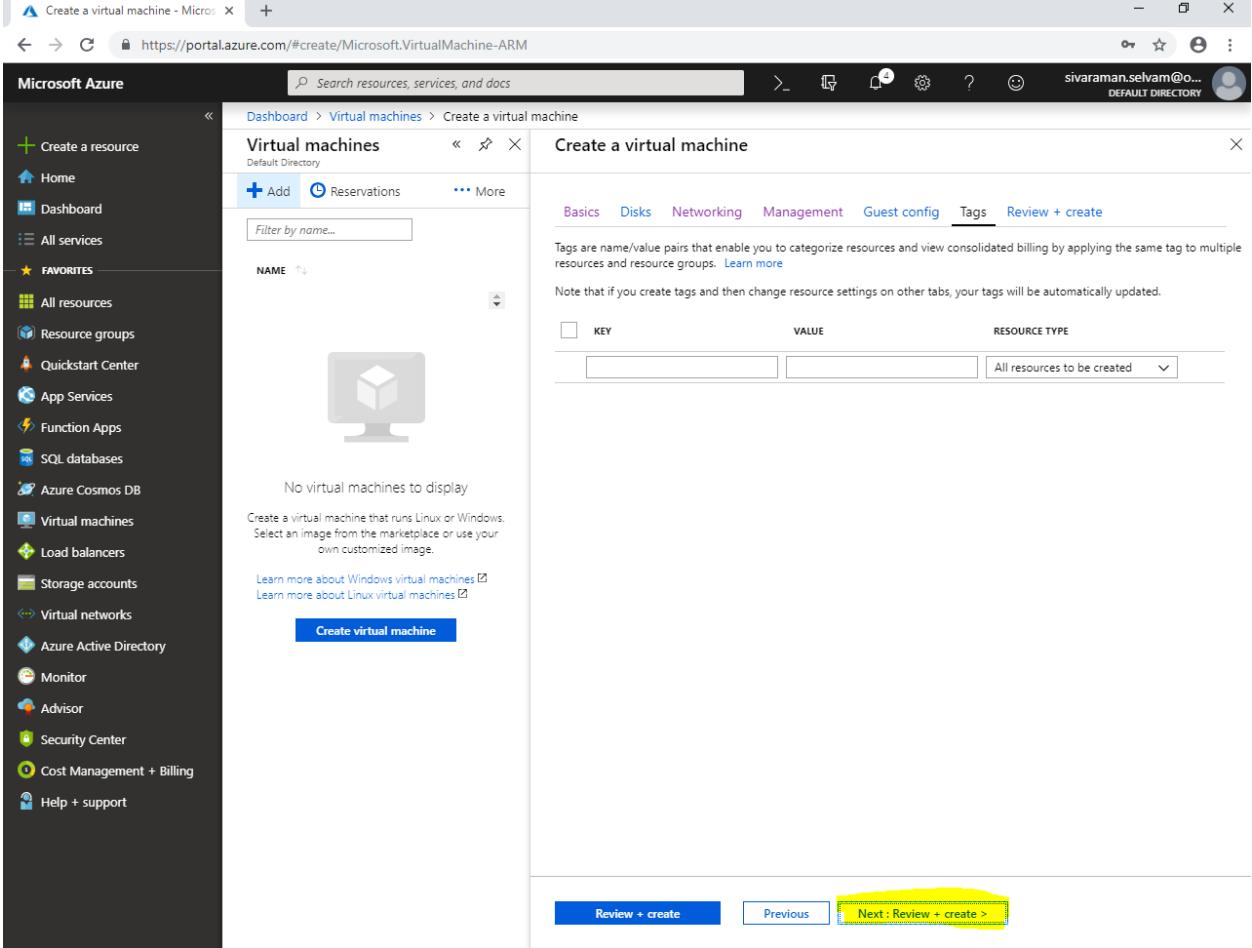
Click “Next : Tags >”.



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar lists various services like Home, Dashboard, and Virtual machines. The main area shows the 'Virtual machines' blade with a 'Create a virtual machine' wizard open. The 'Guest config' tab is currently selected. A note in the center says 'The selected image does not support cloud init.' At the bottom, there are buttons for 'Review + create', 'Previous', and 'Next : Tags >'. The 'Next : Tags >' button is highlighted with a yellow box.

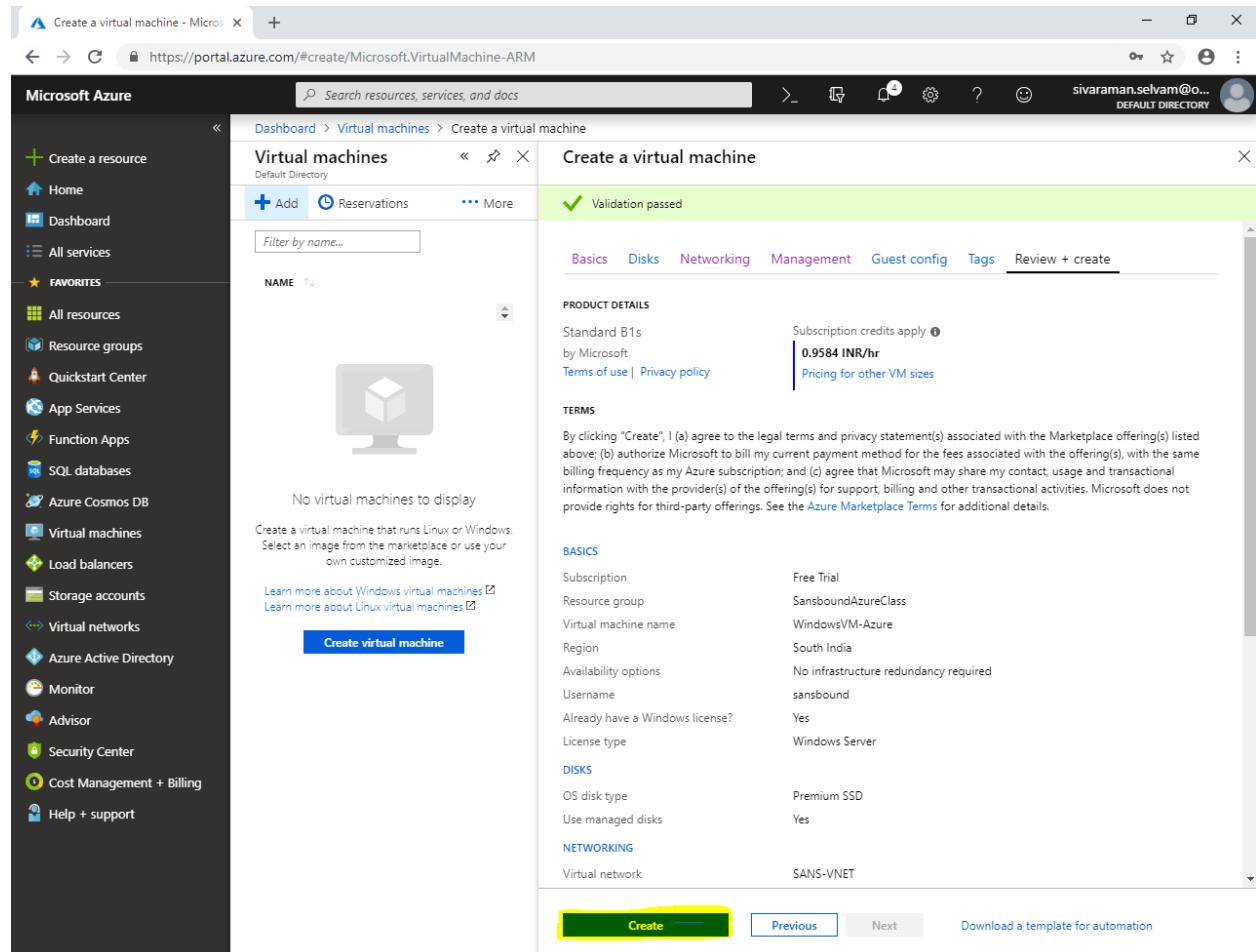
In “Tags”.

Click “Review + create”.



The screenshot shows the Microsoft Azure portal interface for creating a virtual machine. The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, Favorites, 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, and Help + support. The main content area is titled "Create a virtual machine" under "Virtual machines". It shows a section for "Tags" where users can add key-value pairs. The "Tags" tab is currently selected. At the bottom of the page, there are three buttons: "Review + create" (highlighted in blue), "Previous", and "Next : Review + create >".

Click “Create”.



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains various service links like Home, Dashboard, and Resource groups. The main area shows a summary of the creation process:

- Virtual machines**: Default Directory
- Add Reservations**
- More**
- Validation passed** (indicated by a green checkmark)

The configuration details are as follows:

PRODUCT DETAILS	
Standard B1s	Subscription credits apply ⓘ
by Microsoft	0.9584 INR/hr
Terms of use Privacy policy	Pricing for other VM sizes

TERMS (Legal terms and privacy statement are listed here).

BASICS (Configuration details):

- Subscription: Free Trial
- Resource group: SansboundAzureClass
- Virtual machine name: WindowsVM-Azure
- Region: South India
- Availability options: No infrastructure redundancy required
- Username: sansbound
- Already have a Windows license?: Yes
- License type: Windows Server

DISKS (Disk settings):

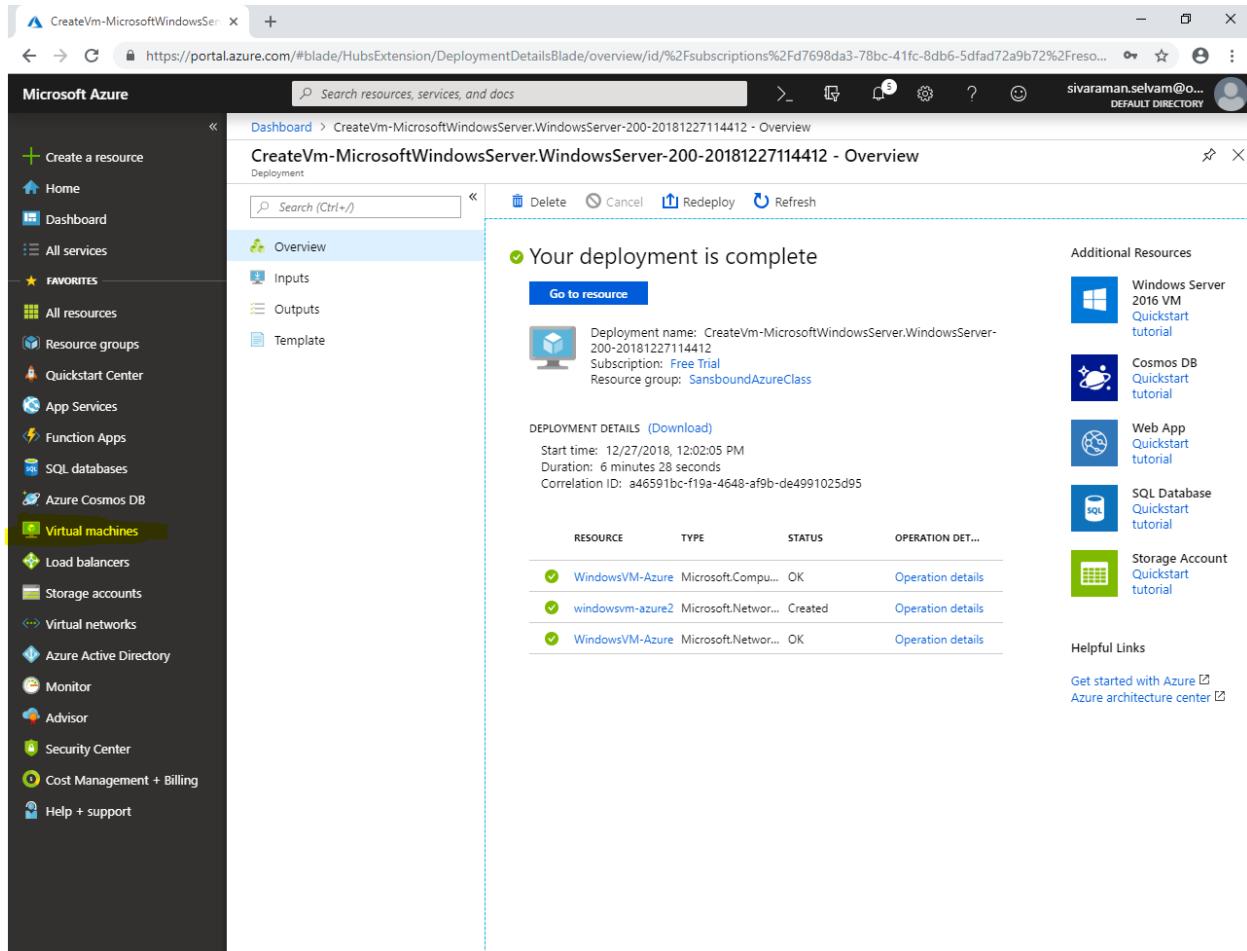
- OS disk type: Premium SSD
- Use managed disks: Yes

NETWORKING (Networking settings):

- Virtual network: SANS-VNET

At the bottom, there are buttons for **Create** (highlighted in yellow), **Previous**, **Next**, and **Download a template for automation**.

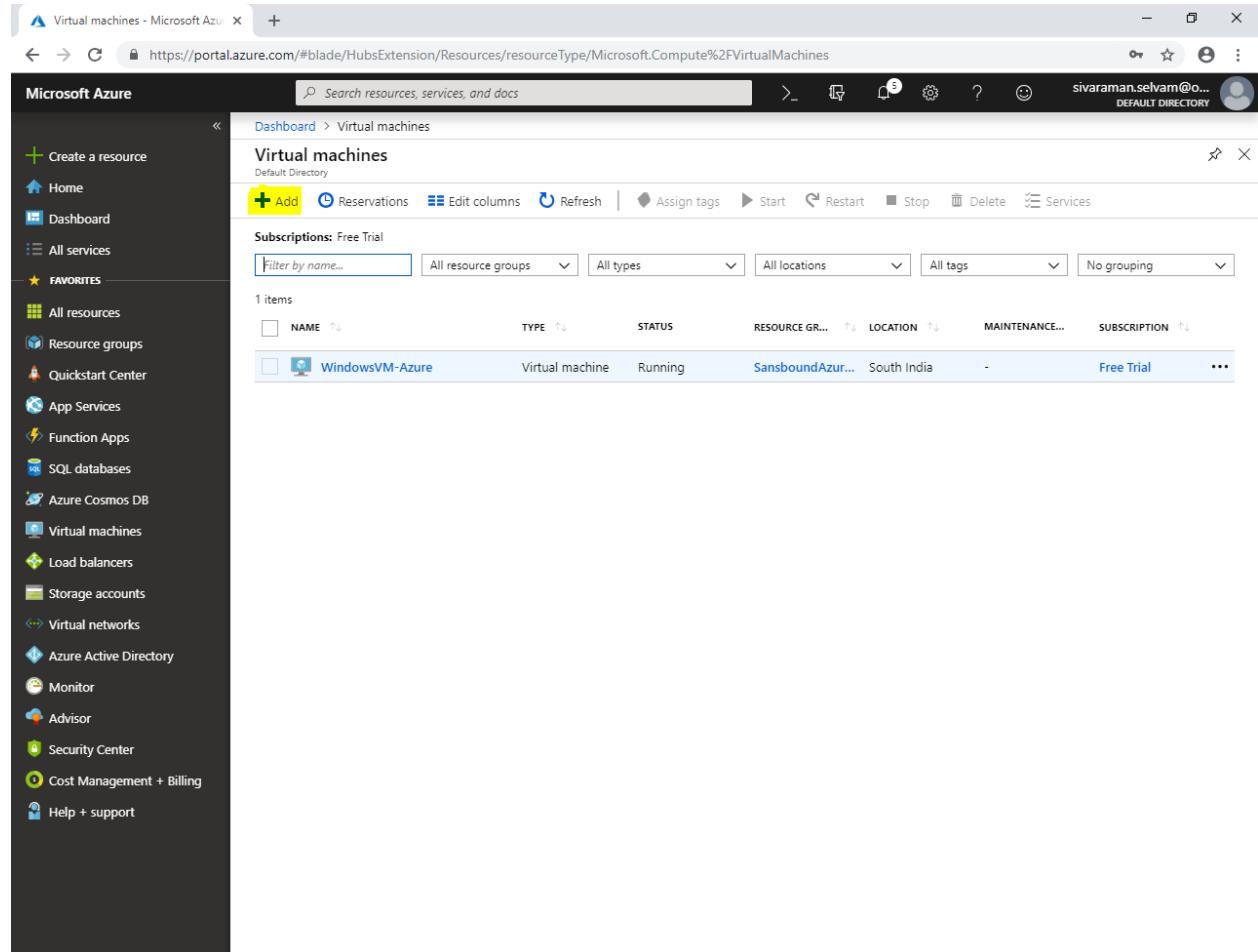
Click “Virutal machine”.



The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation bar is visible, with the "Virtual machines" option highlighted under the "Compute" category. The main content area displays the "CreateVm-MicrosoftWindowsServer.WindowsServer-200-20181227114412 - Overview" page. A prominent message states "Your deployment is complete". Below this, deployment details are listed: Deployment name: CreateVm-MicrosoftWindowsServer.WindowsServer-200-20181227114412, Subscription: Free Trial, Resource group: SansboundAzureClass. A table titled "DEPLOYMENT DETAILS" shows three resources: WindowsVM-Azure (Microsoft.Compu...), windowsvm-azure2 (Microsoft.Networ...), and WindowsVM-Azure (Microsoft.Networ...). All resources are marked as "OK" with "Operation details" links. To the right, there are sections for "Additional Resources" (Windows Server 2016 VM Quickstart tutorial, Cosmos DB Quickstart tutorial, Web App Quickstart tutorial, SQL Database Quickstart tutorial, Storage Account Quickstart tutorial) and "Helpful Links" (Get started with Azure, Azure architecture center).

RESOURCE	TYPE	STATUS	OPERATION DET...
WindowsVM-Azure	Microsoft.Compu...	OK	Operation details
windowsvm-azure2	Microsoft.Networ...	Created	Operation details
WindowsVM-Azure	Microsoft.Networ...	OK	Operation details

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



The screenshot shows the Microsoft Azure portal interface for managing virtual machines. The left sidebar contains a navigation menu with various services like Create a resource, Home, Dashboard, All services, and Favorites. Under Favorites, the Virtual machines option is selected. The main content area is titled "Virtual machines" and shows a single item in the list:

NAME	TYPE	STATUS	RESOURCE GR...	LOCATION	MAINTENANCE...	SUBSCRIPTION
WindowsVM-Azure	Virtual machine	Running	SansboundAzu...	South India	-	Free Trial

While create Virtual machine,

Select “Subscription” as “Free Trial”.

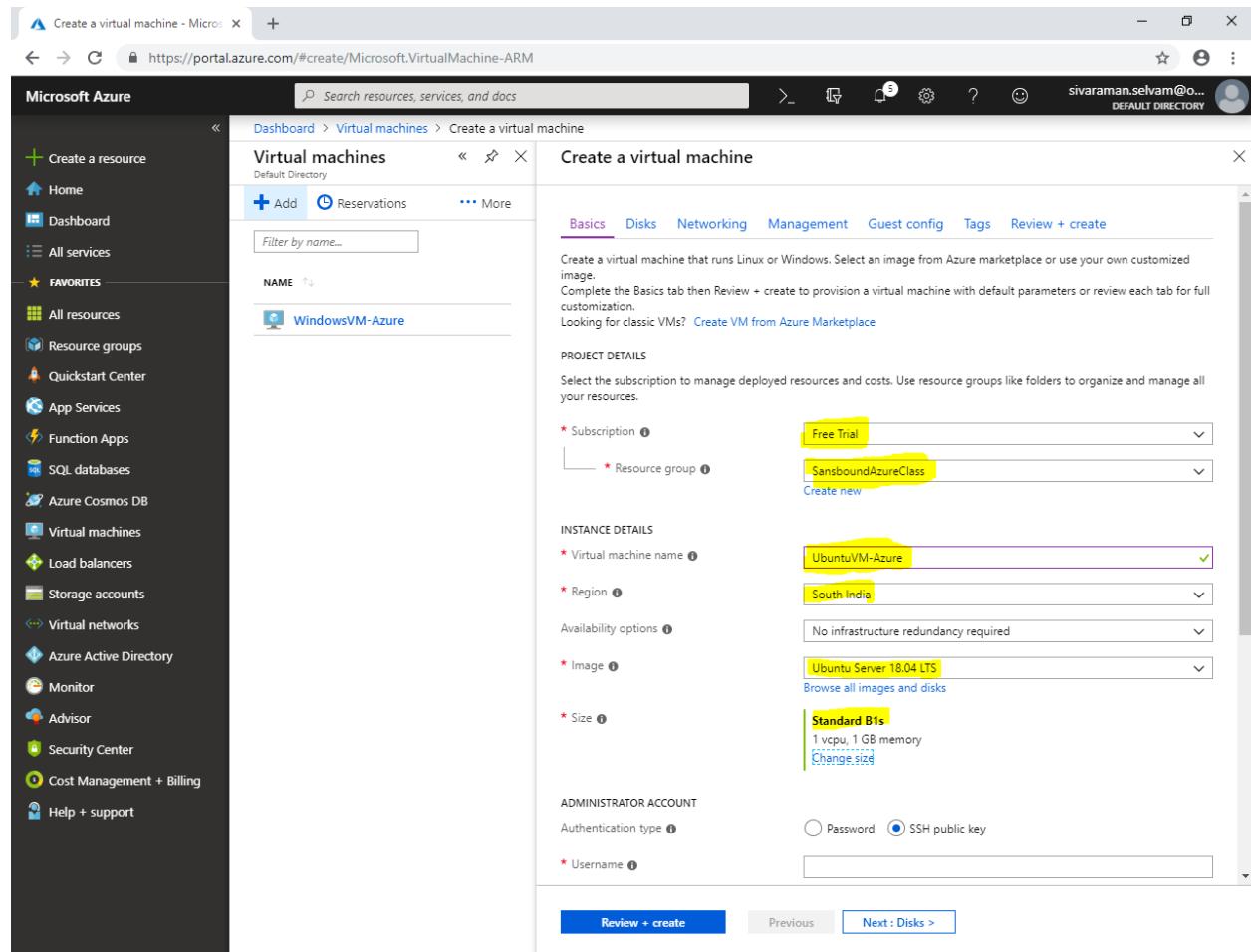
Select “Resource group” as “SansboundAzureClass”.

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

Select “Region” as “South India”.

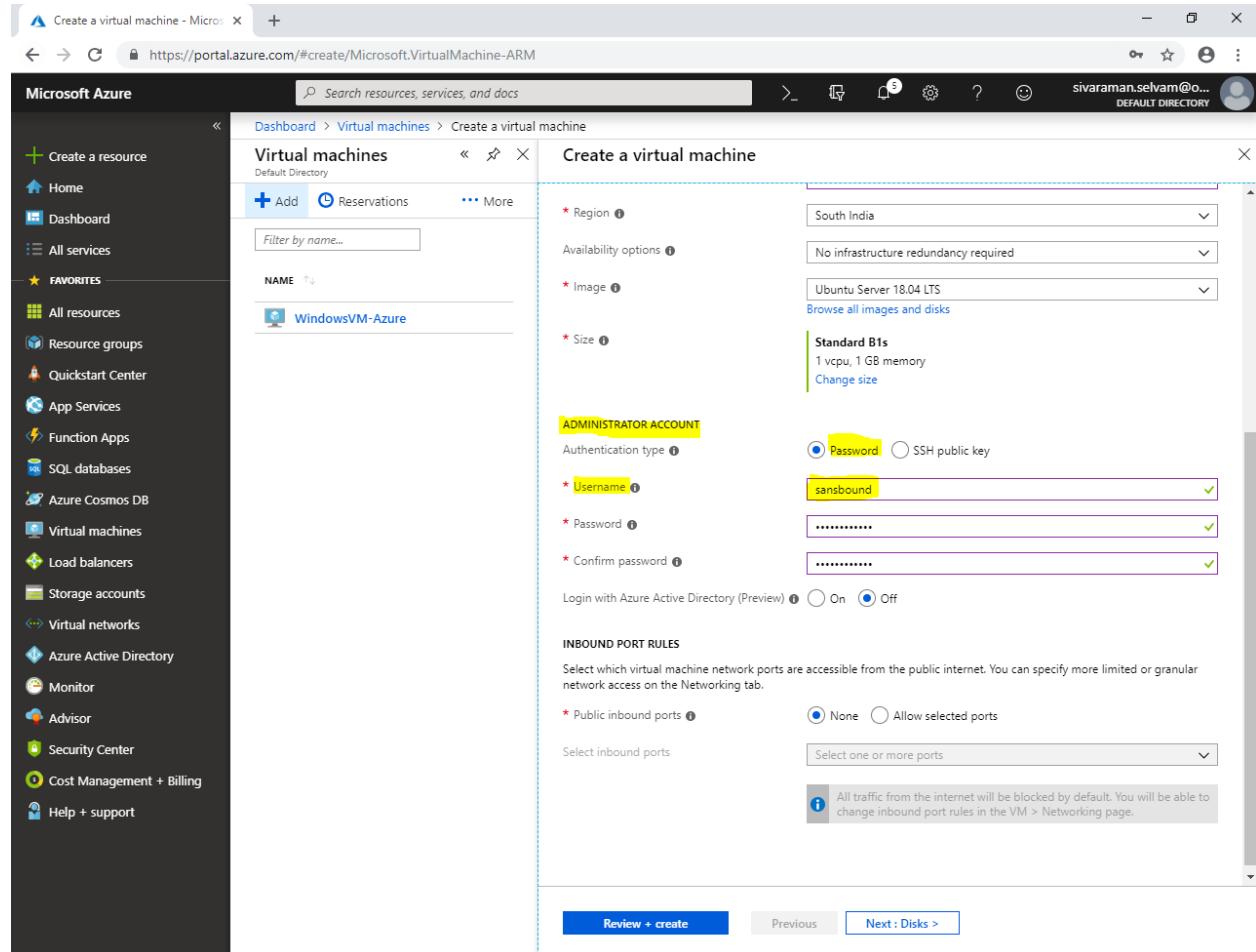
Select “Image” as “Ubuntu Server 18.04 LTS”.

Change “VM Size” as “Standard B1s”.



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains various service icons like Home, Dashboard, and Resource groups. The main area is titled 'Create a virtual machine' under 'Virtual machines'. The 'Basics' tab is active, showing fields for 'NAME' (WindowsVM-Azure), 'Subscription' (Free Trial), 'Resource group' (SansboundAzureClass), 'Virtual machine name' (UbuntuVM-Azure), 'Region' (South India), 'Image' (Ubuntu Server 18.04 LTS), and 'Size' (Standard B1s). The 'Administrator account' section has 'SSH public key' selected. At the bottom, there are 'Review + create', 'Previous', and 'Next : Disks >' buttons.

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

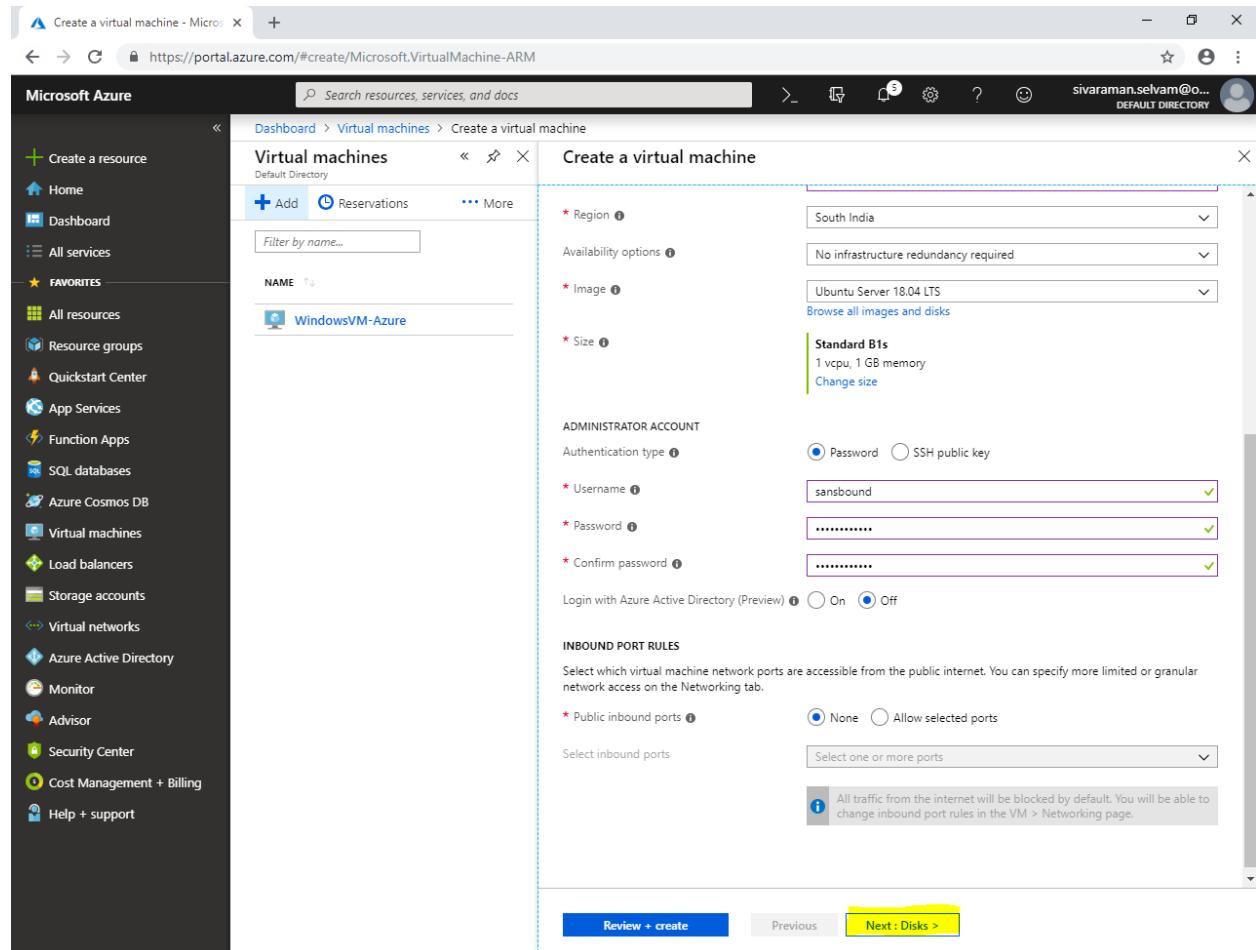


The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar lists various services under 'Virtual machines'. The main area is titled 'Create a virtual machine' and shows the configuration steps:

- Region:** South India
- Availability options:** No infrastructure redundancy required
- Image:** Ubuntu Server 18.04 LTS (Browse all images and disks)
- Size:** Standard B1s (1 vcpu, 1 GB memory) - Change size
- ADMINISTRATOR ACCOUNT:** Authentication type set to Password (radio button selected). Username: sansbound, Password: [REDACTED], Confirm password: [REDACTED]
- INBOUND PORT RULES:** Public inbound ports set to None (radio button selected). A note states: "All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page."

At the bottom, there are 'Review + create' and 'Next : Disks >' buttons.

Click “Next : Disks >”.



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar lists various services like Home, Dashboard, and Virtual machines. The main area shows the 'Create a virtual machine' wizard. The 'Virtual machines' blade is selected. The configuration steps are as follows:

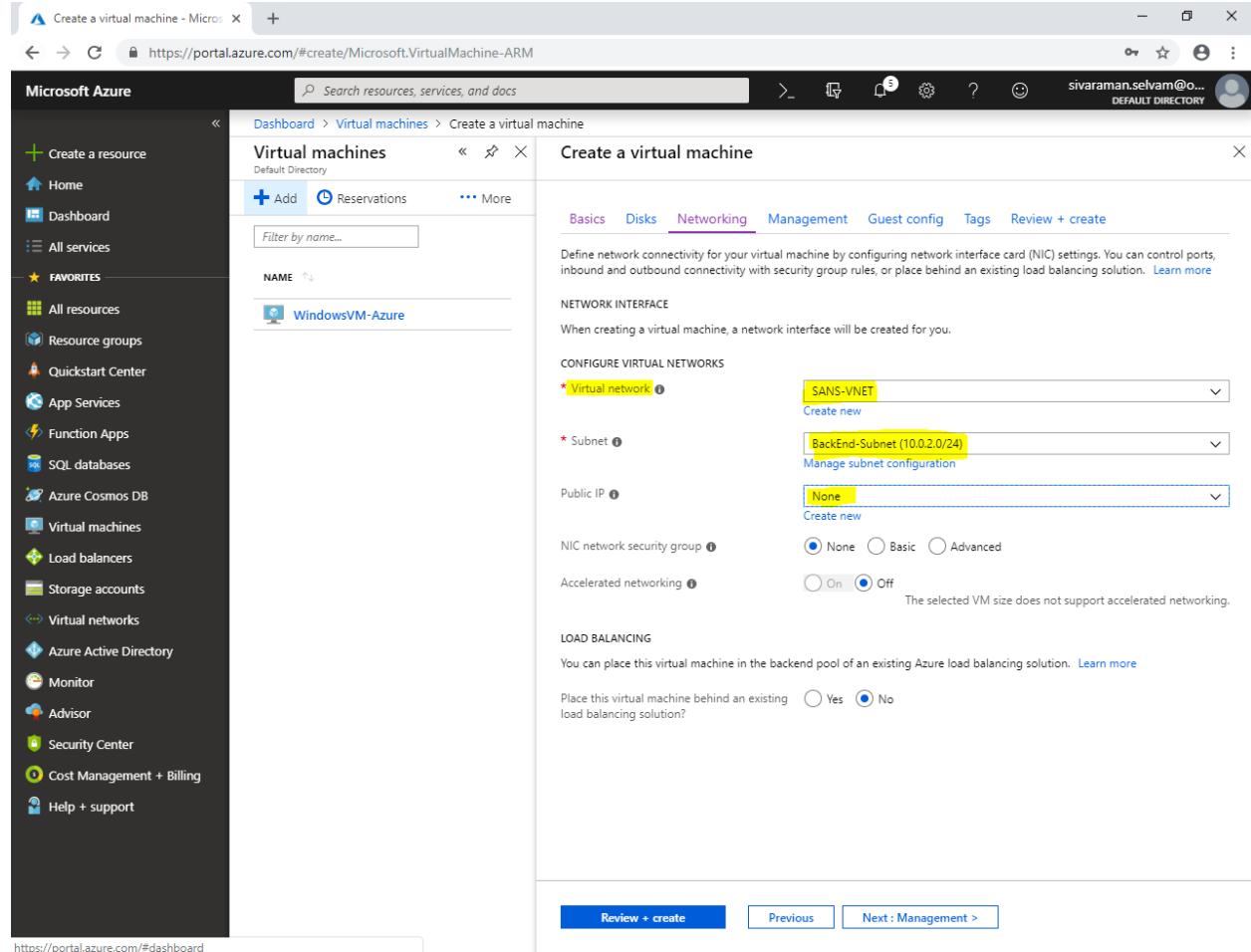
- Region:** South India
- Image:** Ubuntu Server 18.04 LTS
- Size:** Standard B1s (1 vcpu, 1 GB memory)
- Administrator Account:**
 - Authentication type: Password (selected)
 - Username: sansbound
 - Password: (redacted)
 - Confirm password: (redacted)
- Inbound Port Rules:** Public inbound ports: None

At the bottom, there are 'Review + create' and 'Next : Disks >' buttons. The 'Next : Disks >' button is highlighted with a yellow box.

In “Networking”,

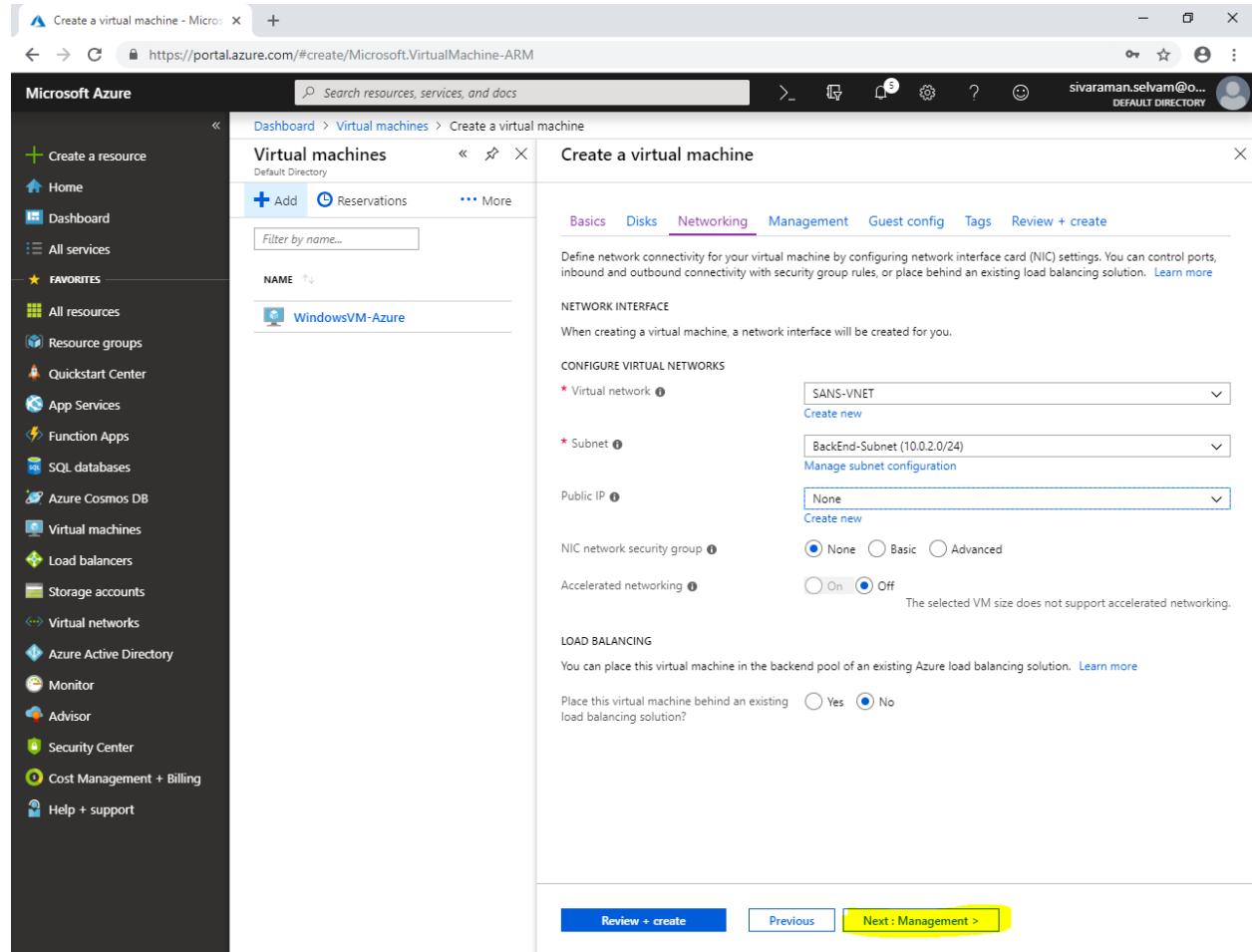
In “Virtual network” select as “**SANS-VNET**”.

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



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, Favorites, and Virtual machines. The main area is titled 'Create a virtual machine' under 'Virtual machines'. The 'Networking' tab is currently selected. In the 'NETWORK INTERFACE' section, the 'Virtual network' is set to 'SANS-VNET' and the 'Subnet' is set to 'BackEnd-Subnet (10.0.2.0/24)'. Under 'Public IP', it is set to 'None'. There are options for 'NIC network security group' (set to 'None'), 'Accelerated networking' (set to 'Off'), and 'LOAD BALANCING' (set to 'No'). At the bottom, there are buttons for 'Review + create', 'Previous', and 'Next : Management >'. The URL in the browser bar is https://portal.azure.com/#create/Microsoft.VirtualMachine-ARM

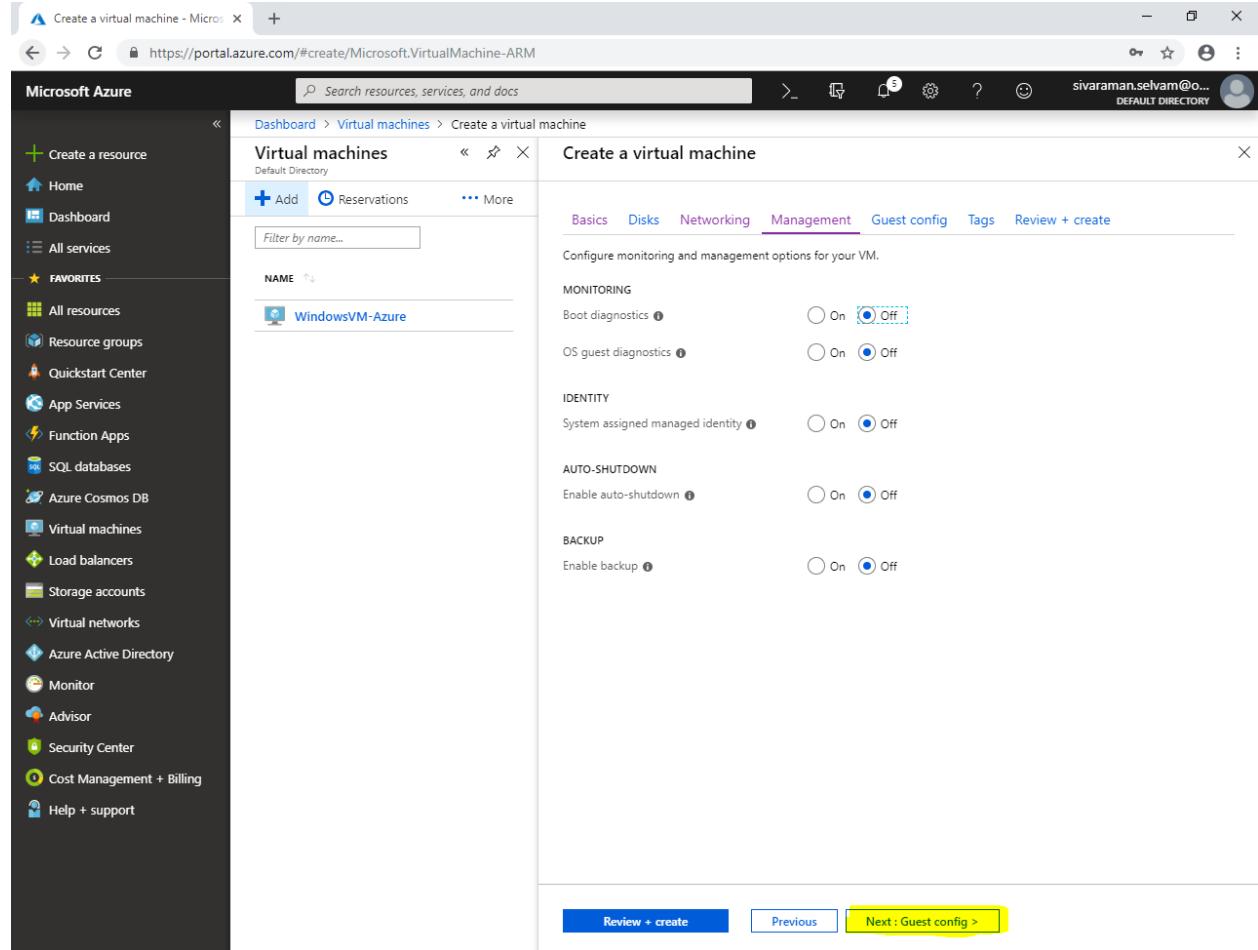
Click "Next : Management >".



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains various service links like Home, Dashboard, All services, and Favorites. The main area shows a list of existing virtual machines, with one named 'WindowsVM-Azure' selected. On the right, the 'Create a virtual machine' wizard is open, specifically the 'Networking' configuration step. It includes fields for selecting a Virtual network (set to 'SANS-VNET'), Subnet (set to 'BackEnd-Subnet (10.0.2.0/24)'), and Public IP (set to 'None'). Below these, there are options for NIC network security group (set to 'None') and Accelerated networking (set to 'Off'). Under 'LOAD BALANCING', it asks if the VM should be placed behind an existing load balancing solution, with 'No' selected. At the bottom, there are three buttons: 'Review + create', 'Previous', and 'Next : Management >'. The 'Next : Management >' button is highlighted with a yellow box.

In “Management”.

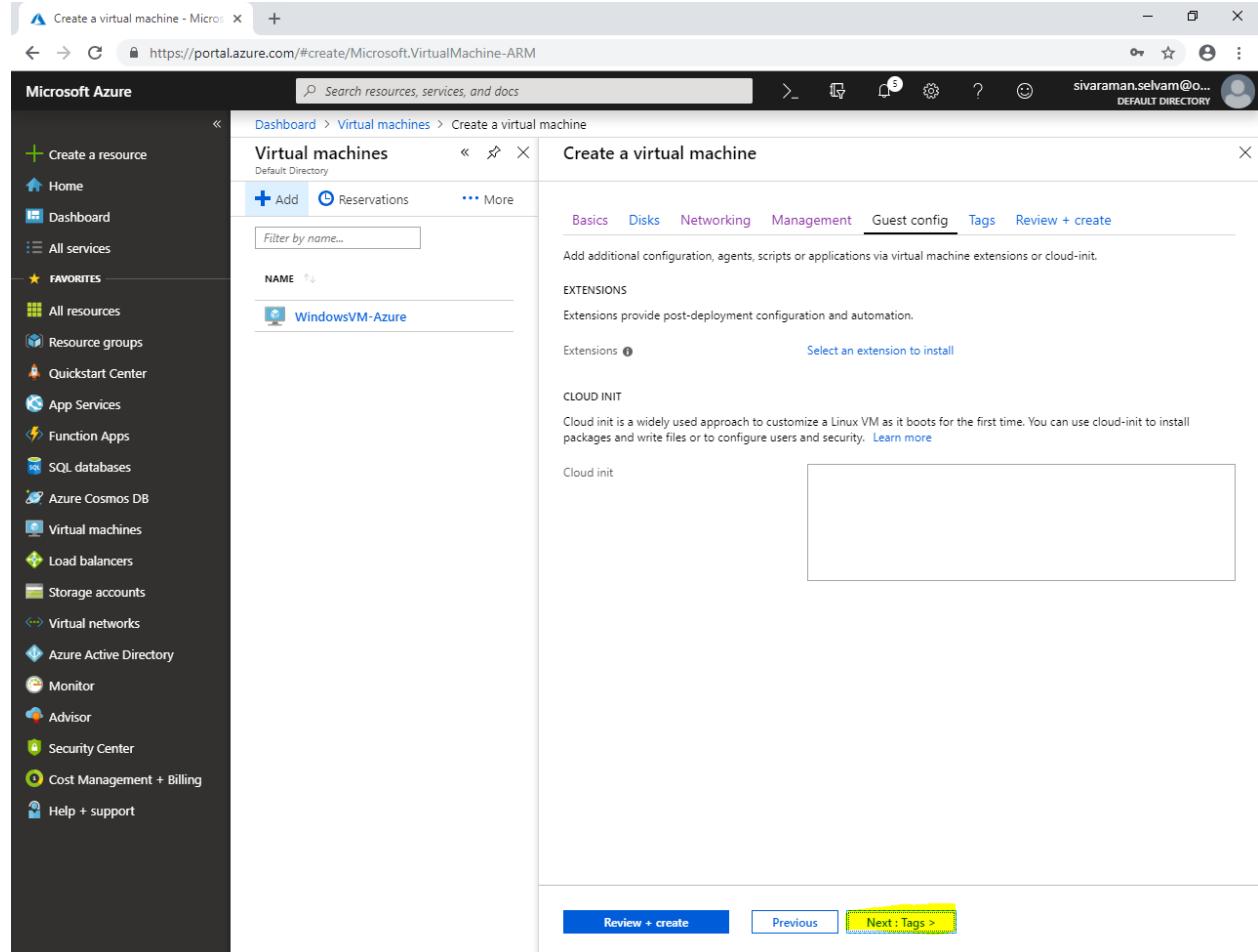
Click “Next : Guest config >”.



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, Favorites, and more. The main area is titled 'Create a virtual machine' under 'Virtual machines'. The 'Guest config' tab is currently selected. The configuration section includes options for Monitoring, Identity, Auto-shutdown, and Backup, each with 'On' or 'Off' radio button choices. The 'WindowsVM-Azure' name is already entered in the NAME field. At the bottom, there are three buttons: 'Review + create' (blue), 'Previous' (light blue), and 'Next : Guest config >' (yellow, indicating it's the current step). The URL in the browser bar is https://portal.azure.com/#create/Microsoft.VirtualMachine-ARM.

In “Guest config”

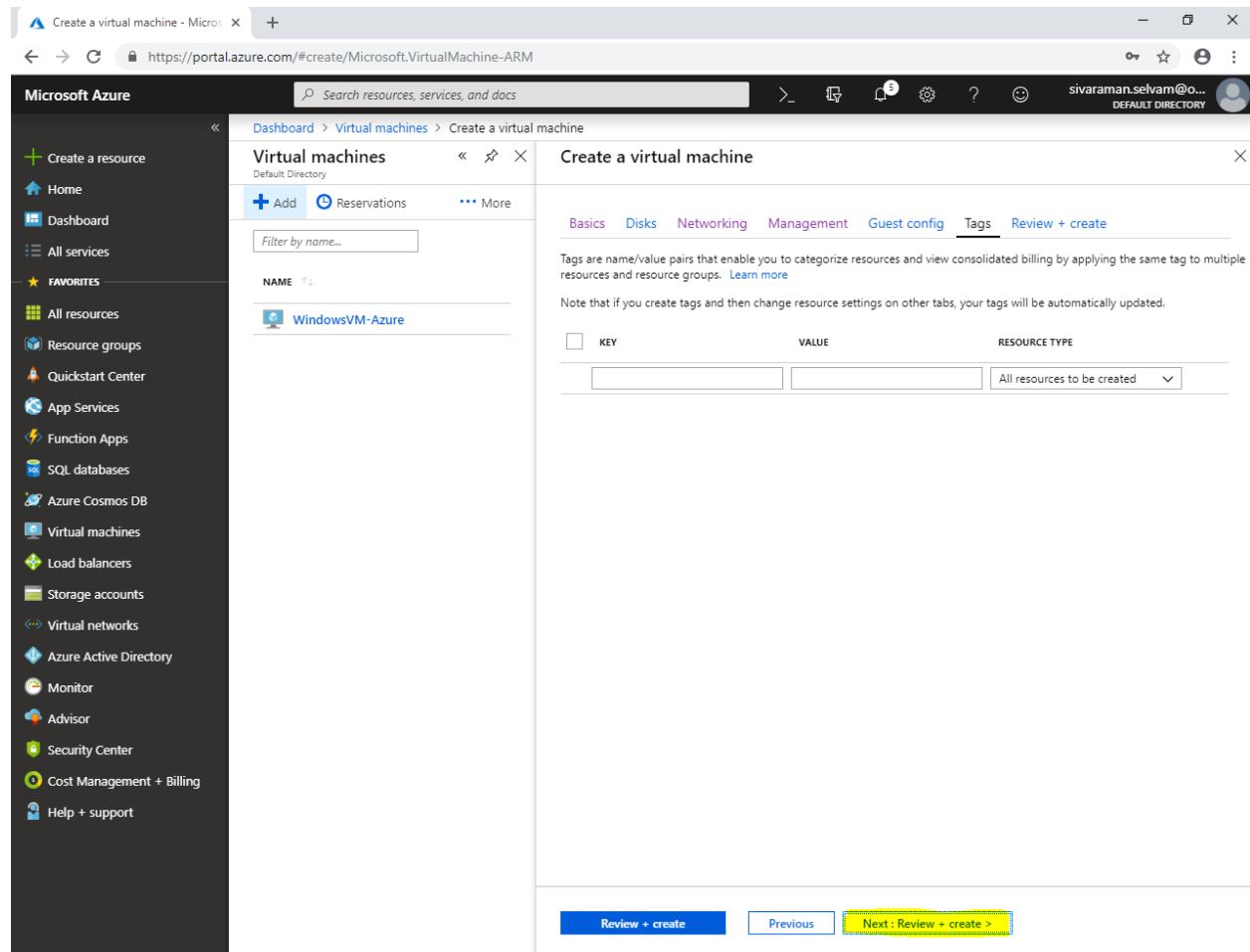
Click “**Next : Tags >**”.



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, Favorites, and more. The main area is titled 'Virtual machines' and shows a list of existing VMs, with one named 'WindowsVM-Azure' selected. The central part of the screen is the 'Create a virtual machine' wizard, currently on the 'Guest config' tab. This tab allows users to add additional configuration, agents, scripts, or applications via virtual machine extensions or cloud-init. Below the tabs, there's a section for 'EXTENSIONS' with a link to 'Select an extension to install'. Under 'CLOUD INIT', there's a brief description and a note about using cloud-init to customize a Linux VM. At the bottom of the wizard, there are three buttons: 'Review + create' (blue), 'Previous' (light blue), and 'Next : Tags >' (yellow, highlighted with a yellow box).

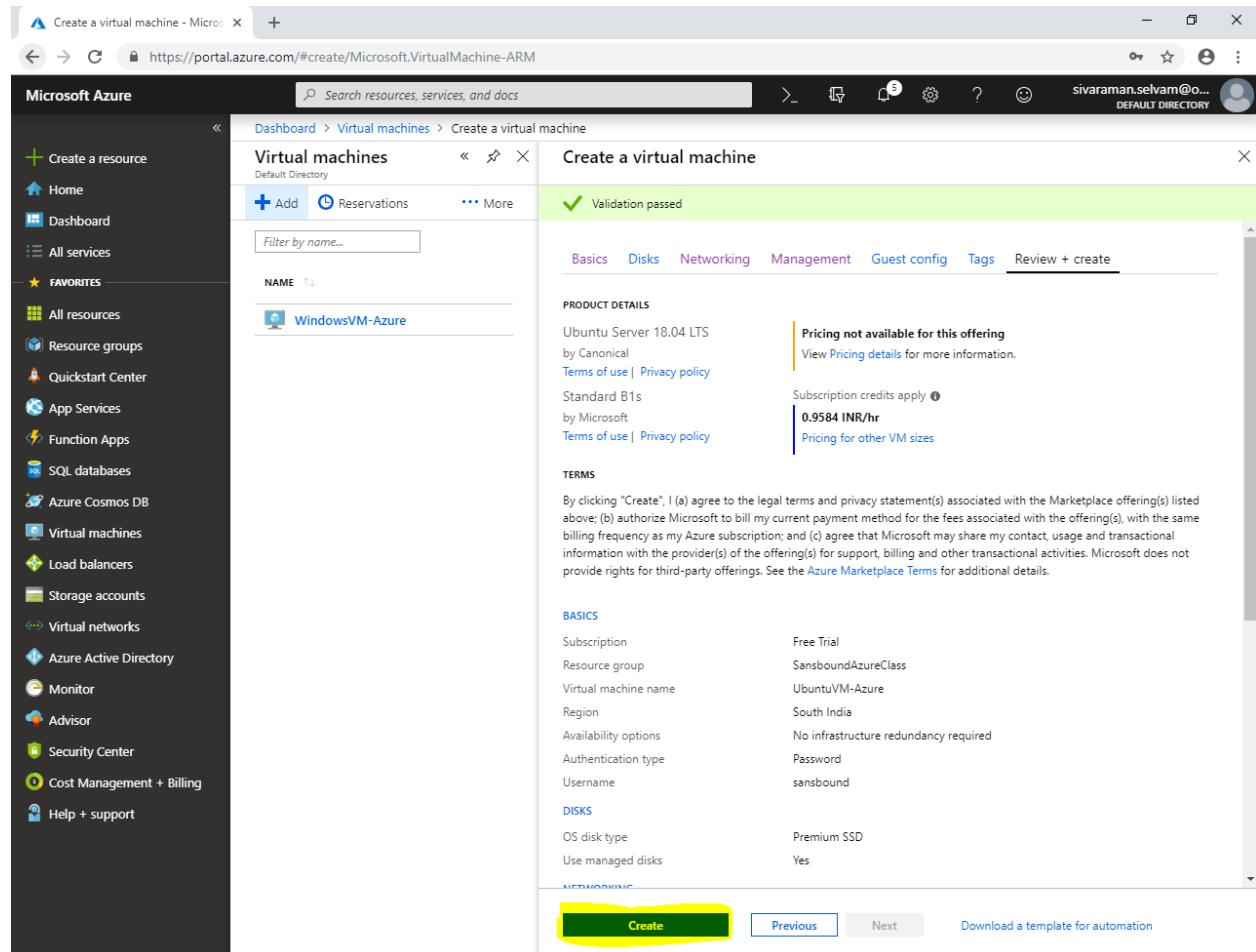
In “Tags”.

Click “Review + create”.



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, Favorites, 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, and Help + support. The main content area is titled "Create a virtual machine" and shows the "Virtual machines" blade. The "Tags" tab is currently selected. A table allows adding key-value pairs for tags. The table has columns for KEY, VALUE, and RESOURCE TYPE, with a dropdown set to "All resources to be created". At the bottom, there are buttons for "Review + create", "Previous", and "Next : Review + create >".

Click “Create”.

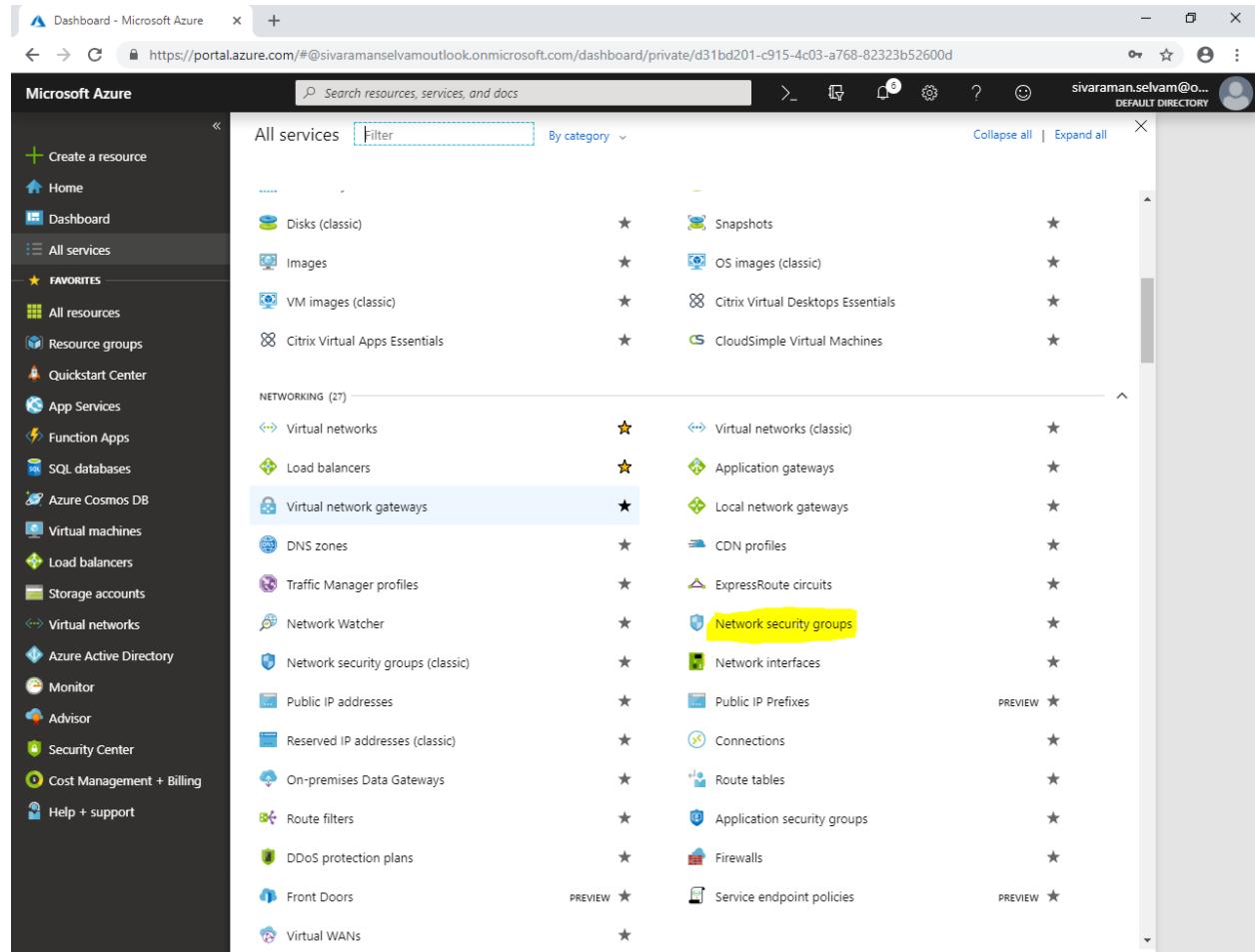


The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains navigation links for resources like Home, Dashboard, and Virtual machines. The main area is titled 'Create a virtual machine' and shows a validation message 'Validation passed'. The configuration tabs include Basics, Disks, Networking, Management, Guest config, Tags, and Review + create. Under 'PRODUCT DETAILS', it lists Ubuntu Server 18.04 LTS as the offering, with a note that pricing is not available. It also shows the price of 0.9584 INR/hr and a link to view pricing details. The 'TERMS' section contains legal disclaimers. The 'BASICS' tab shows subscription details: Free Trial, Resource group SansboundAzureClass, Virtual machine name UbuntuVM-Azure, Region South India, Availability options No infrastructure redundancy required, Authentication type Password, and Username sansbound. The 'DISKS' tab shows OS disk type Premium SSD and Use managed disks Yes. At the bottom, there are 'Create', 'Previous', 'Next', and 'Download a template for automation' buttons. The 'Create' button is highlighted with a yellow box.

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

In “**Networking**”.

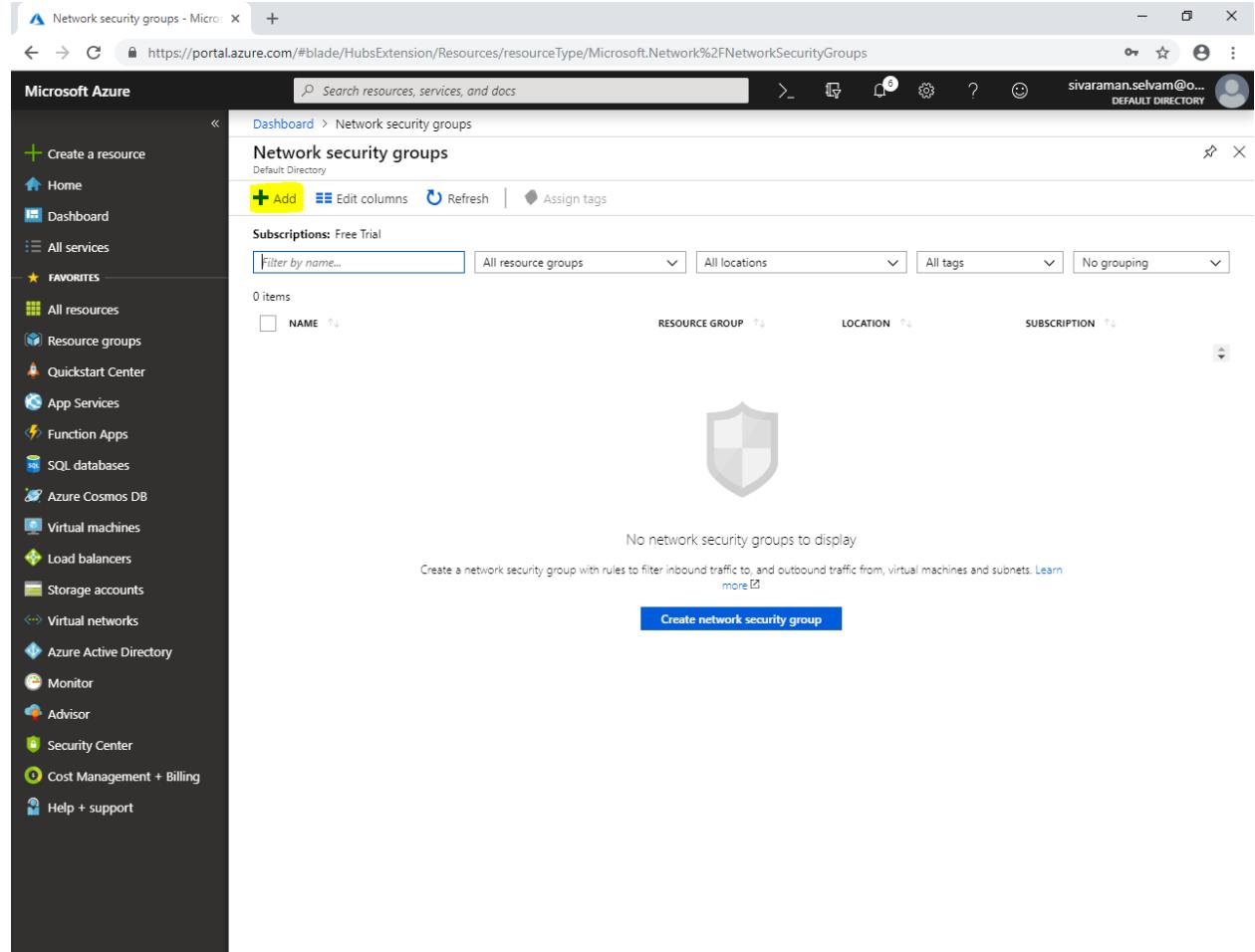
Click “**Network security groups**”.



The screenshot shows the Microsoft Azure All Services dashboard. On the left sidebar, under the “FAVORITES” section, the “All services” item is selected. In the main content area, the “NETWORKING (27)” section is expanded. Within this section, the “Network security groups” item is highlighted with a yellow box. Other items in the list include Virtual networks, Load balancers, Virtual network gateways, DNS zones, Traffic Manager profiles, Network Watcher, Network security groups (classic), Public IP addresses, Reserved IP addresses (classic), On-premises Data Gateways, Route filters, DDoS protection plans, Front Doors, and Virtual WANs.

In “Network security groups”.

Click “Add”.



The screenshot shows the Microsoft Azure portal interface. The left sidebar is filled with various service icons under the 'FAVORITES' section. The main content area is titled 'Network security groups' and shows a single large shield icon in the center. Below the icon, the text 'No network security groups to display' is visible. At the bottom of the page, there is a blue button labeled 'Create network security group'.

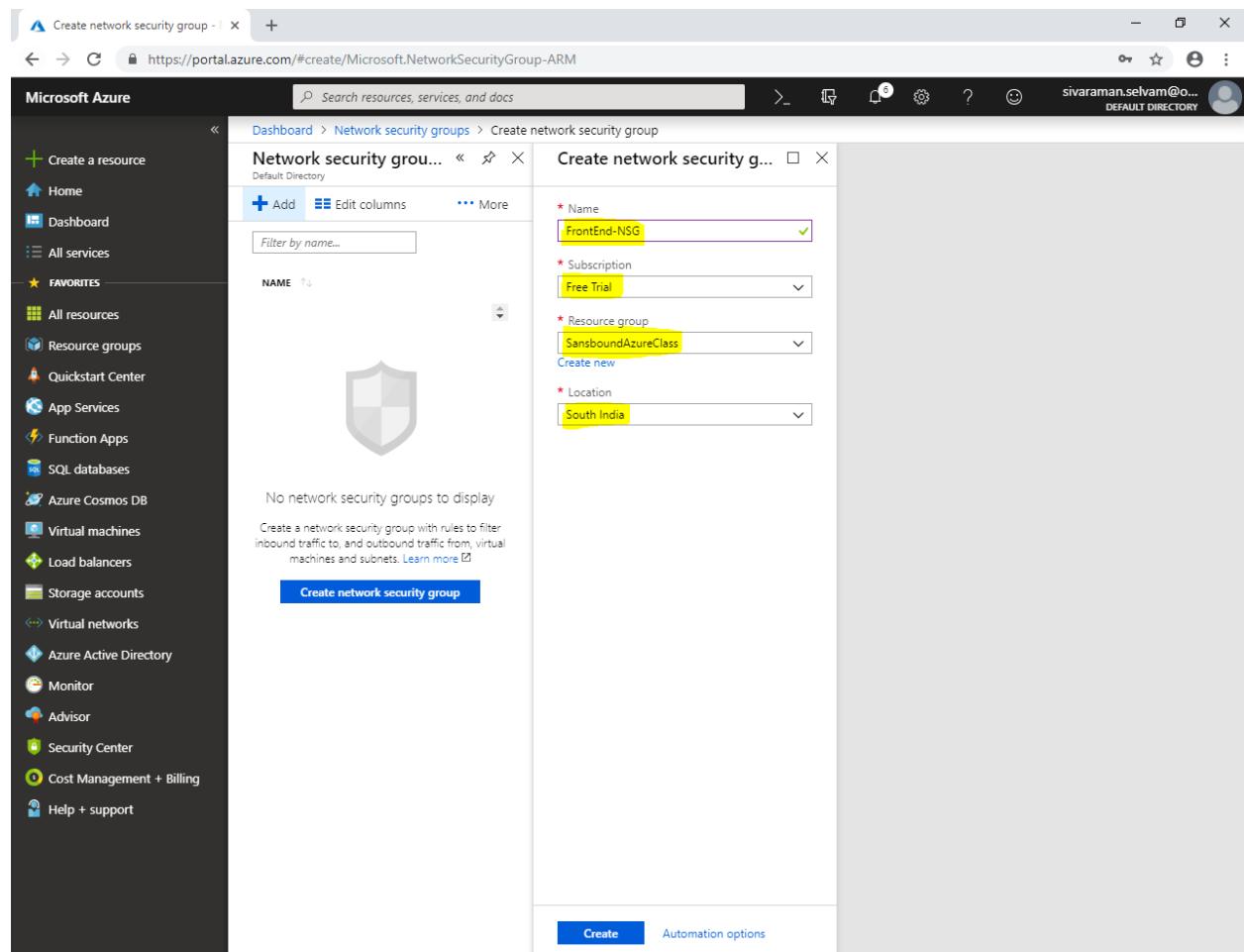
While creating “**Network Security Group**” it requires,

Name “**FrontEnd-NSG**”.

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

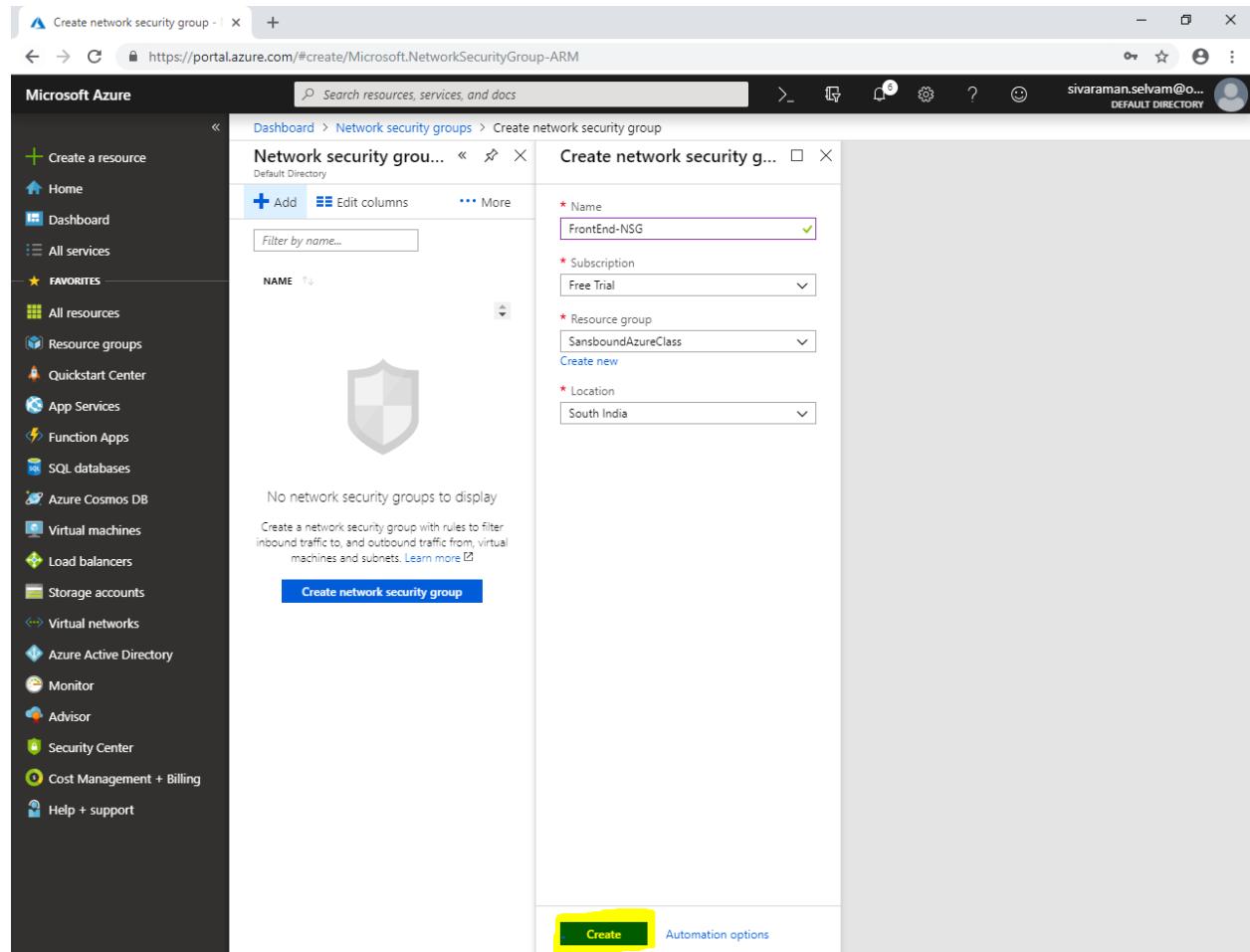
Select “**Resource group**” as “**SansboundAzureClass**”.

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



The screenshot shows the Microsoft Azure portal interface for creating a Network Security Group (NSG). The left sidebar lists various services like Home, Dashboard, All resources, and others. The main area shows the 'Create network security group' wizard. The 'Name' field is filled with 'FrontEnd-NSG'. The 'Subscription' dropdown is set to 'Free Trial'. The 'Resource group' dropdown is set to 'SansboundAzureClass'. The 'Location' dropdown is set to 'South India'. At the bottom, there is a large blue 'Create network security group' button.

Click "Create".



The screenshot shows the Microsoft Azure portal interface for creating a Network Security Group (NSG). The left sidebar contains various service links like Home, Dashboard, and Resource groups. The main area shows a 'Network security group...' blade with a 'Create network security group...' sub-blade. The 'Create' button at the bottom of the sub-blade is highlighted with a yellow box.

Create network security group

Name: FrontEnd-NSG

Subscription: Free Trial

Resource group: SansboundAzureClass

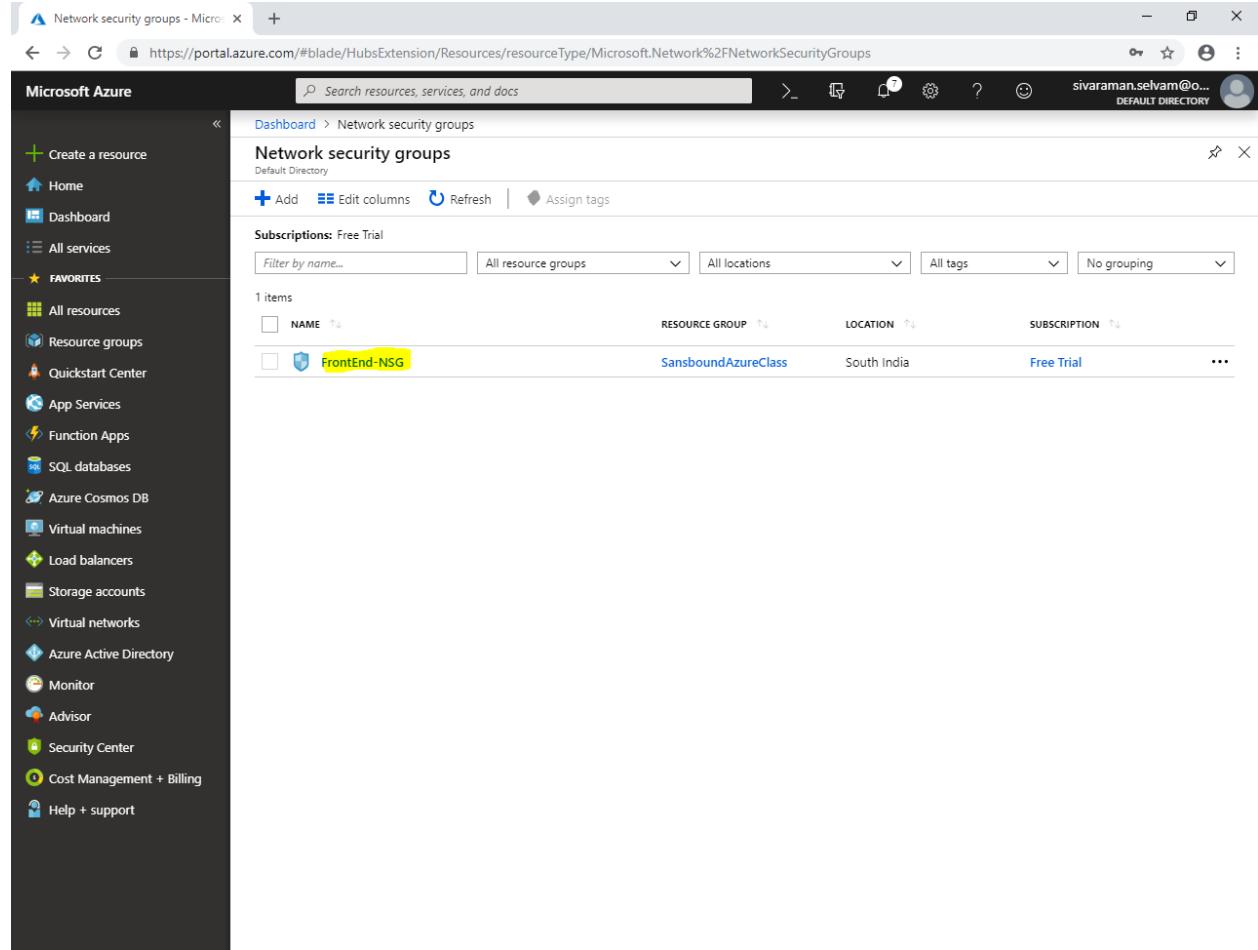
Location: South India

Create network security group

Create Automation options

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

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



The screenshot shows the Microsoft Azure portal interface. The left sidebar is filled with various service icons under the 'FAVORITES' section. The main content area is titled 'Network security groups' and shows a single item in the list:

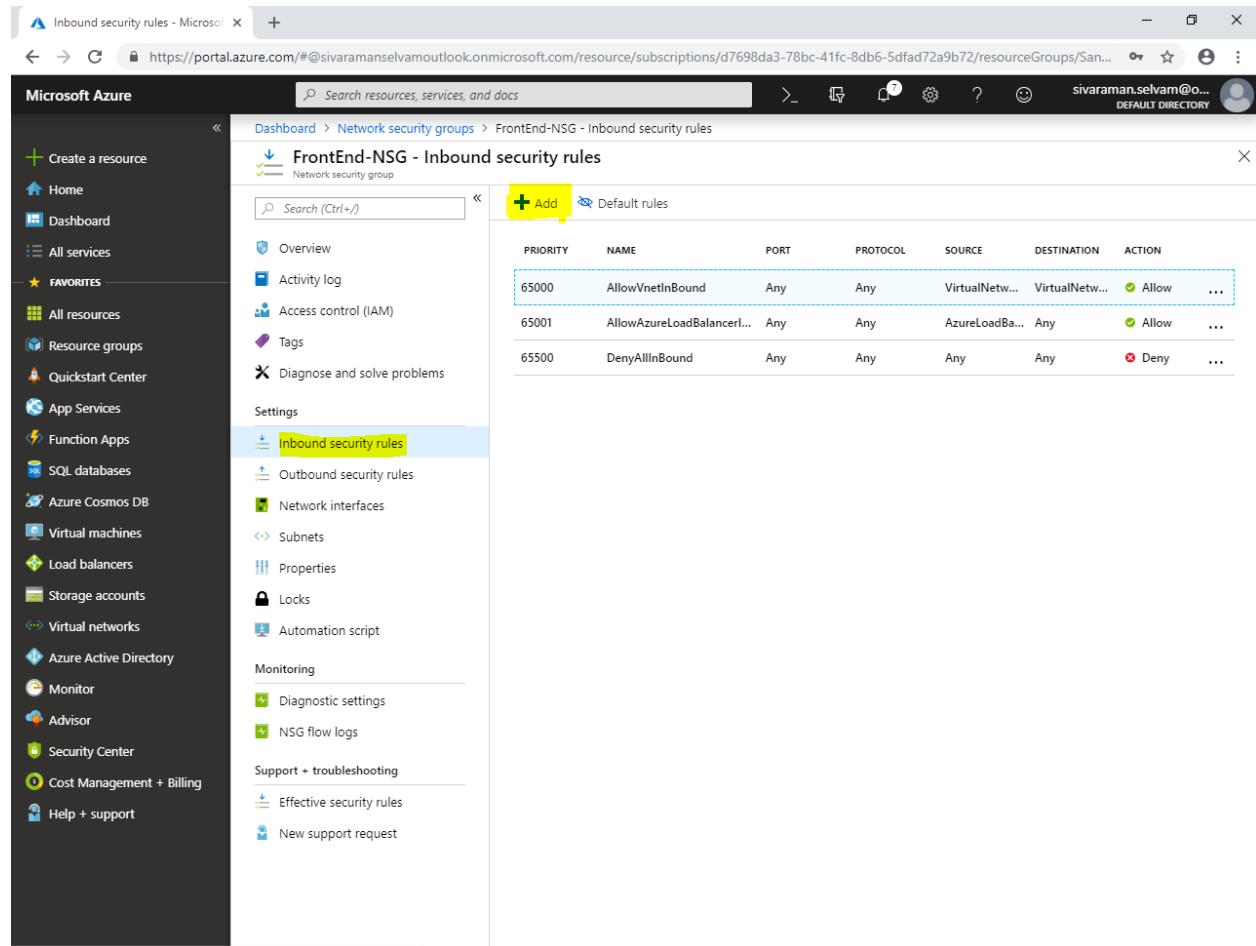
NAME	RESOURCE GROUP	LOCATION	SUBSCRIPTION
FrontEnd-NSG	SansboundAzureClass	South India	Free Trial

A yellow box highlights the 'NAME' column for the 'FrontEnd-NSG' entry. The URL in the browser bar is https://portal.azure.com/#blade/HubsExtension/Resources/resourceType/Microsoft.Network%2FNetworkSecurityGroups.

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”.



PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetInBound	Any	Any	VirtualNetw...	VirtualNetw...	Allow
65001	AllowAzureLoadBalancer...	Any	Any	AzureLoadBa...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

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

In “**Source**” as “**Any**”.

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

In “**Destination**” as “**Any**”.

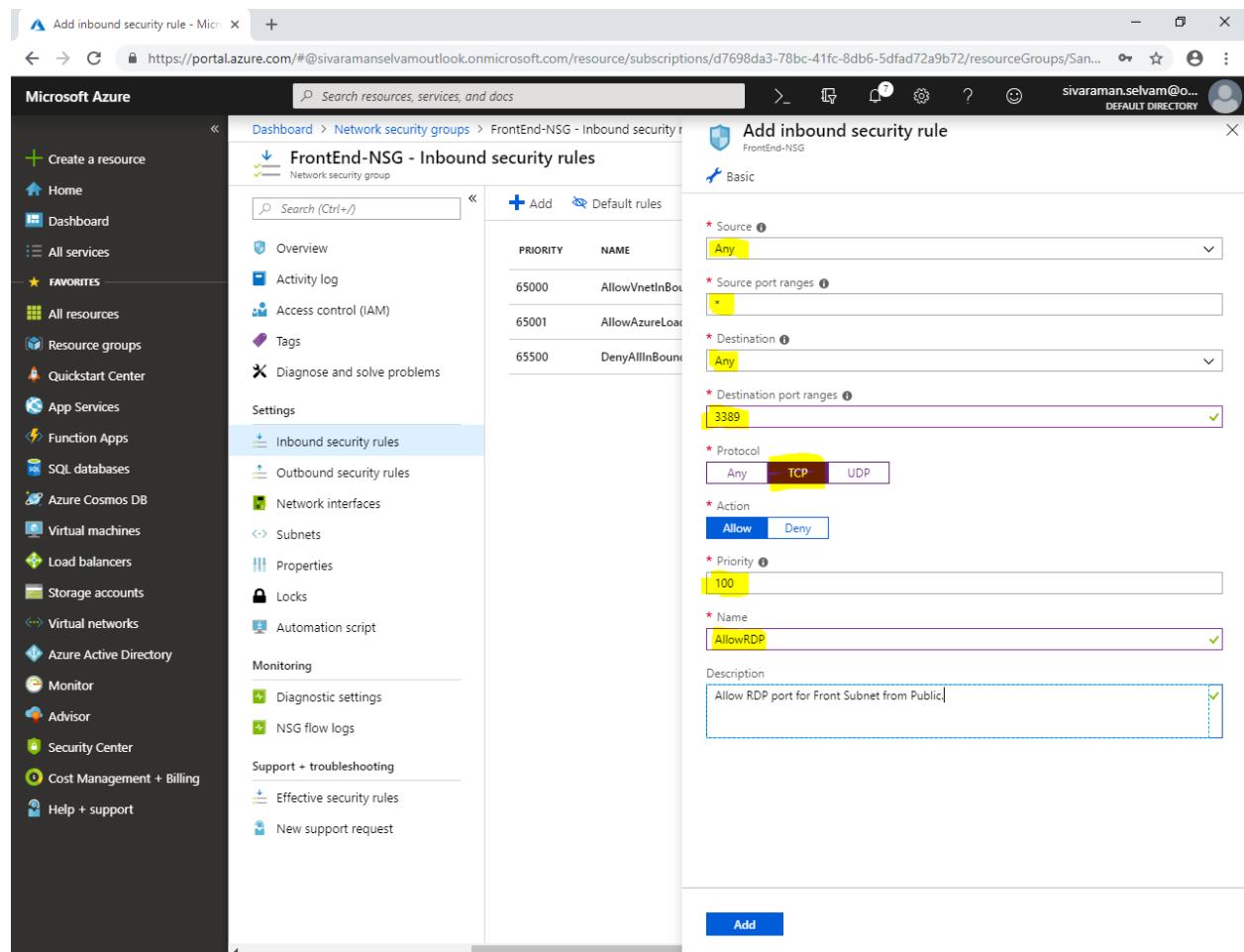
In “**Destination port ranges**” as “**3389**” (To Allow RDP port to access the server through remotely).

“**Protocol**” click on “**TCP**”.

“**Action**” as “**Allow**”.

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

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



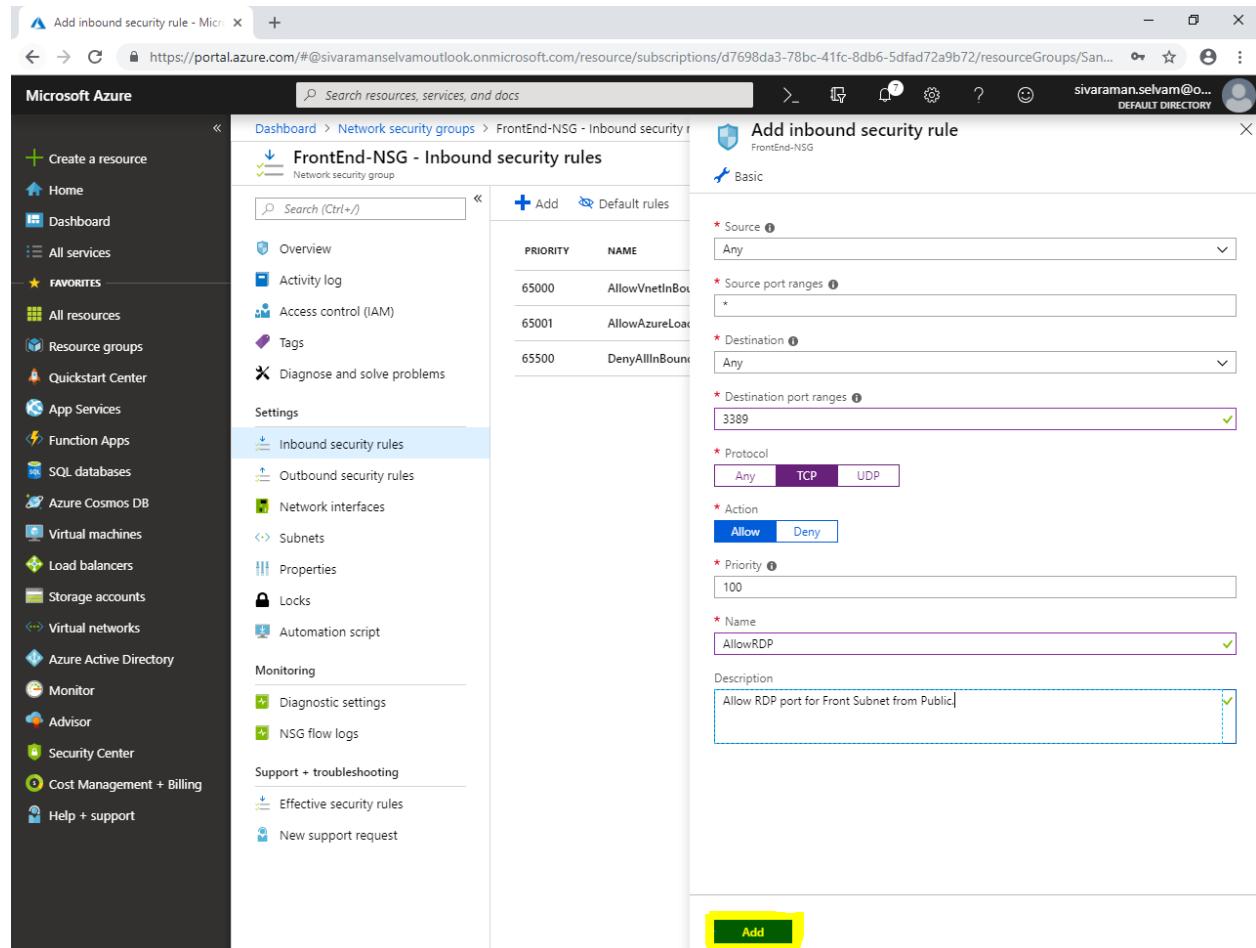
PRIORITY	NAME
65000	AllowVnetInBou
65001	AllowAzureLoad
65500	DenyAllInBound

Basic

- * Source **Any**
- * Source port ranges *****
- * Destination **Any**
- * Destination port ranges **3389**
- * Protocol **TCP**
- * Action **Allow**
- * Priority **100**
- * Name **AllowRDP**

Description
Allow RDP port for Front Subnet from Public

Click “Add”.

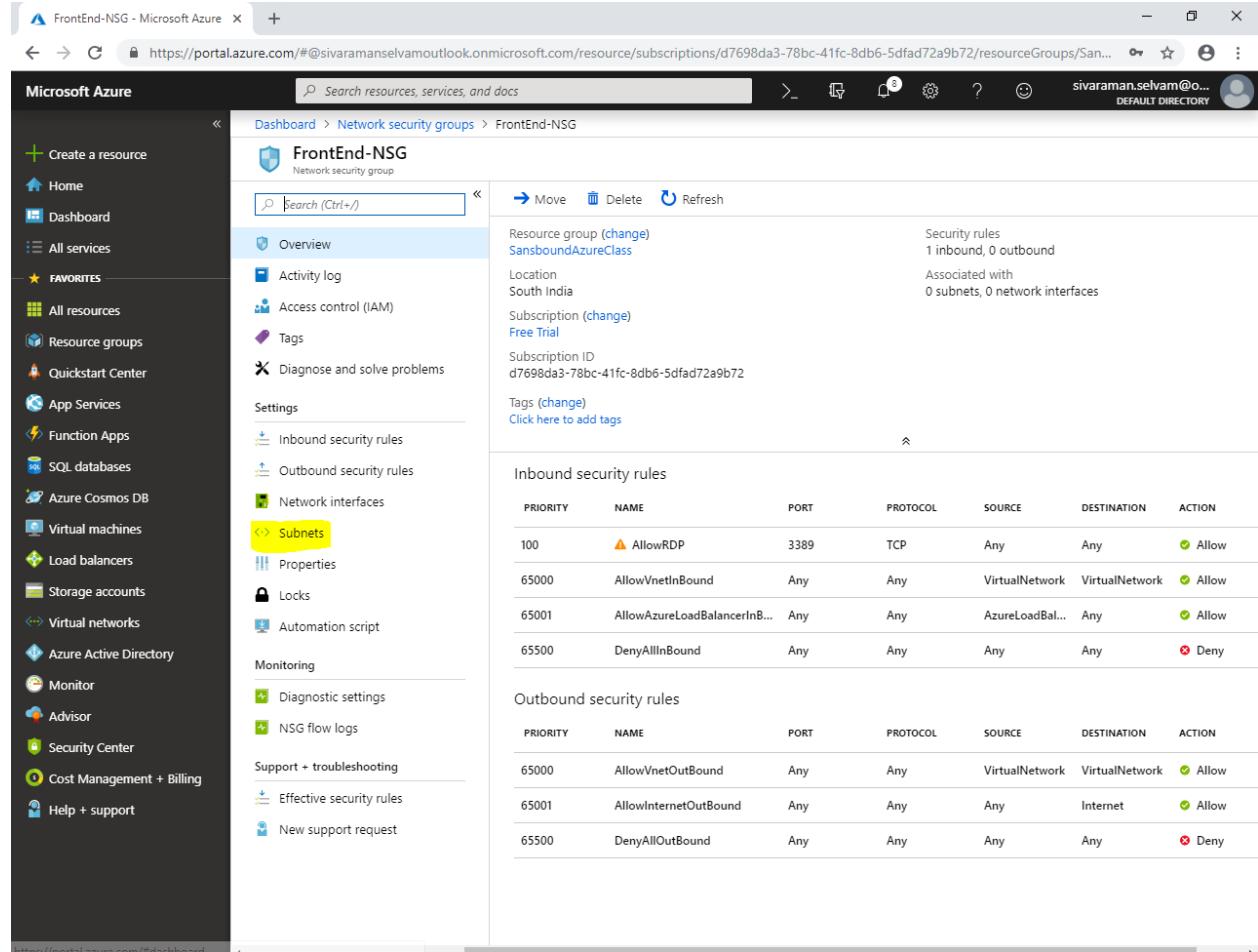


The screenshot shows the Microsoft Azure portal interface for managing Network Security Groups (NSGs). The left sidebar contains various service links, and the main area shows the 'FrontEnd-NSG - Inbound security rules' page. A new rule is being added, with the following details:

- Source:** Any
- Source port ranges:** *
- Destination:** Any
- Destination port ranges:** 3389
- Protocol:** TCP
- Action:** Allow
- Priority:** 100
- Name:** AllowRDP
- Description:** Allow RDP port for Front Subnet from Public

In “FrontEnd-NSG”,

Click “Subnets”.



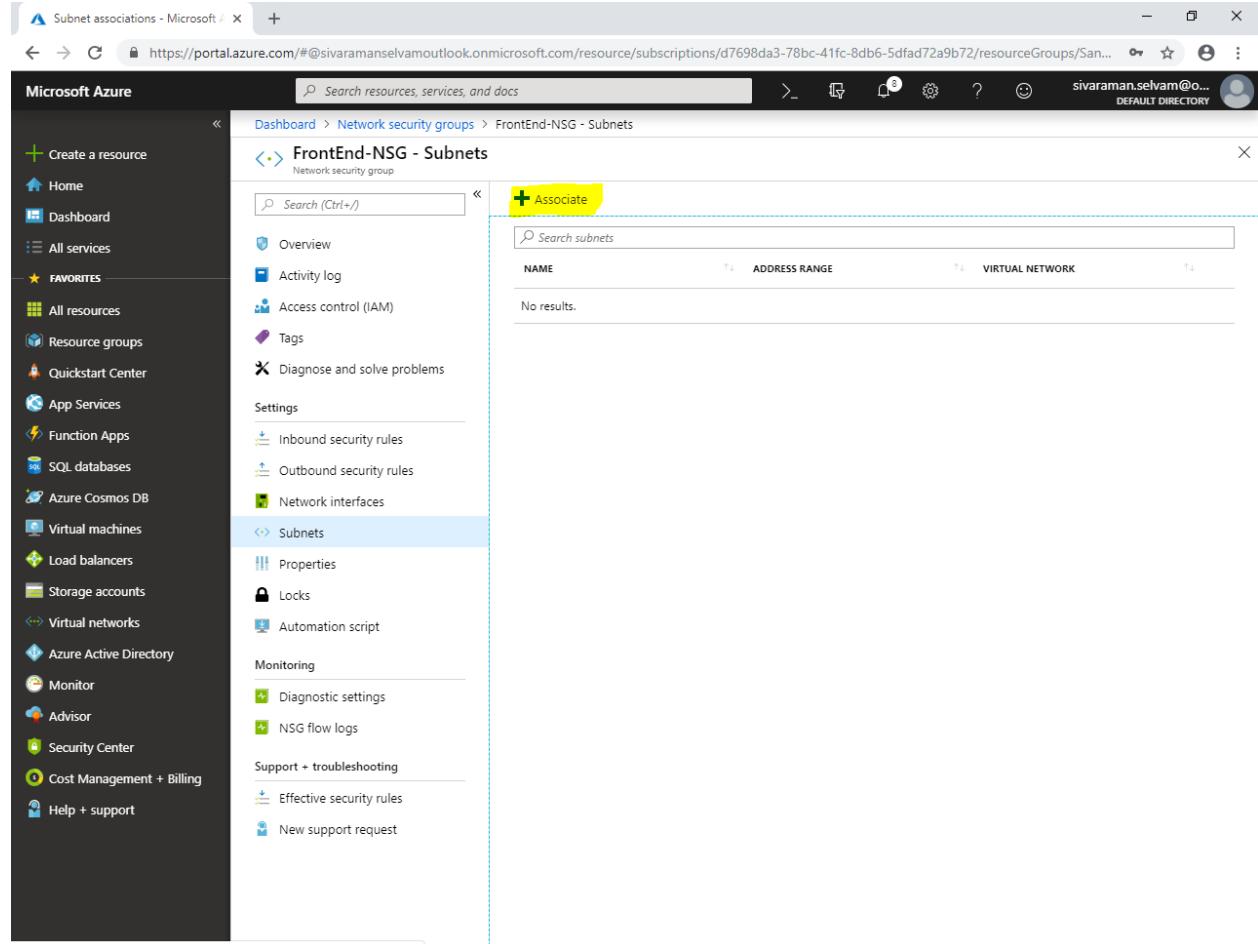
The screenshot shows the Microsoft Azure portal interface for the 'FrontEnd-NSG' Network Security Group. The left sidebar contains various service links like Home, Dashboard, All services, and Favorites. The main content area displays the NSG overview with tabs for Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. Under Settings, there are sections for Inbound security rules, Outbound security rules, Network interfaces, and Subnets. The 'Subnets' link is highlighted with a yellow box. To the right, detailed information about the NSG is shown, including its resource group, location, subscription, and security rules. Below this are tables for Inbound and Outbound security rules, each listing priority, name, port, protocol, source, destination, and action.

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	AllowRDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBal...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowNetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

In “FrontEnd-NSG – Subnets”.

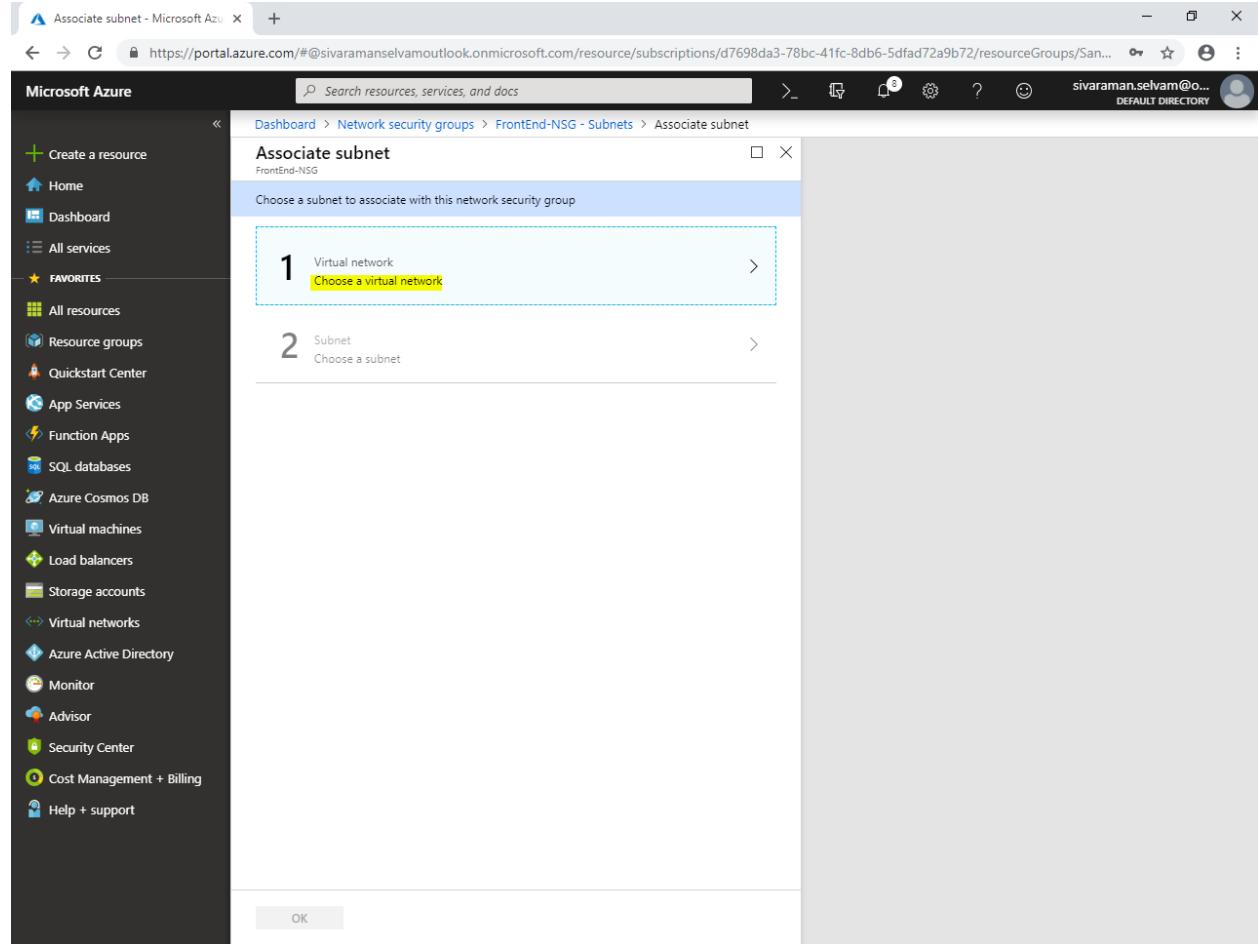
Click “Associate”.



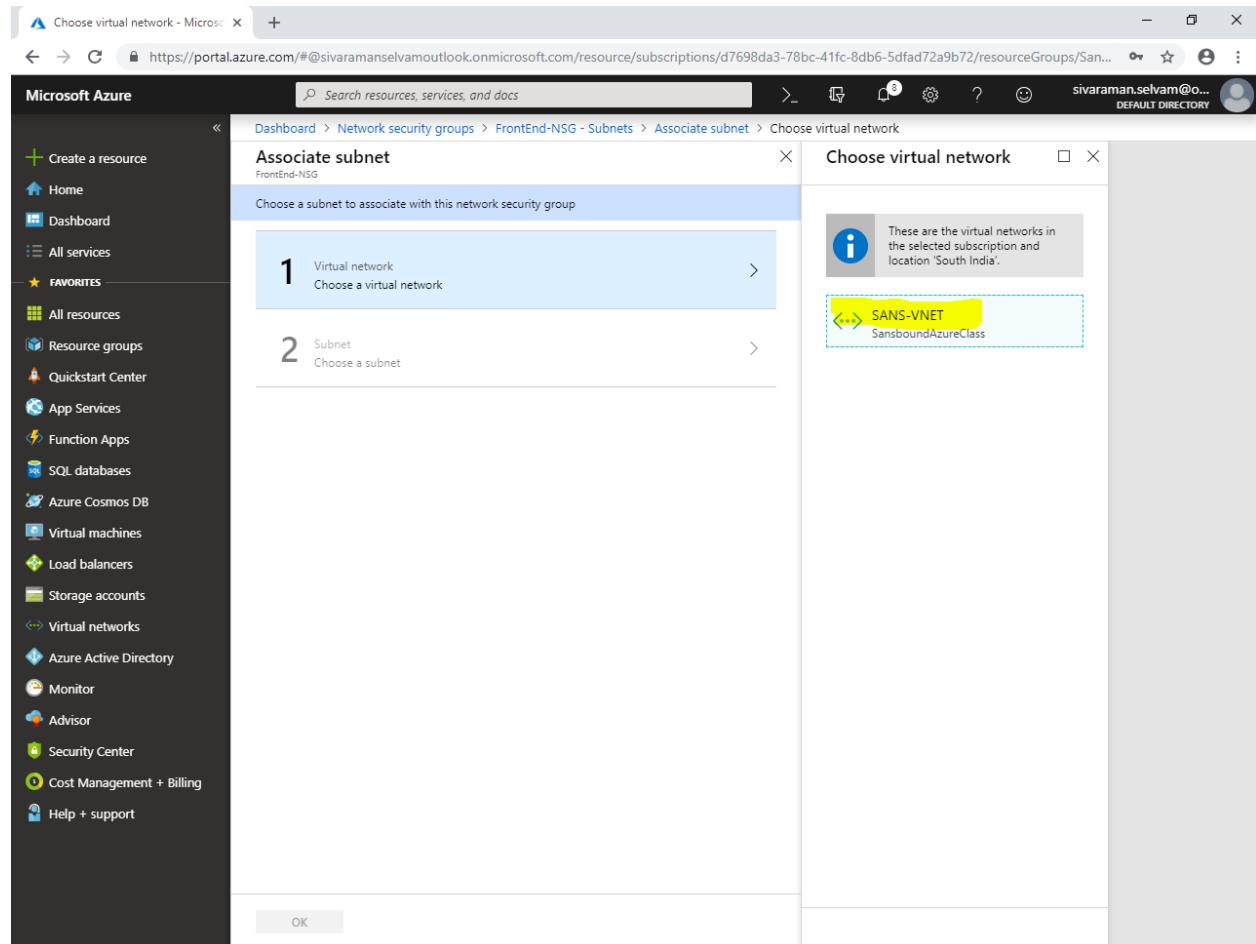
The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a list of services under 'FAVORITES'. The main content area is titled 'FrontEnd-NSG - Subnets' and shows a list of subnets with columns for NAME, ADDRESS RANGE, and VIRTUAL NETWORK. A large yellow box highlights the '+ Associate' button at the top right of the subnet list.

While “Associate subnet”

Click on “Choose a virtual network”.

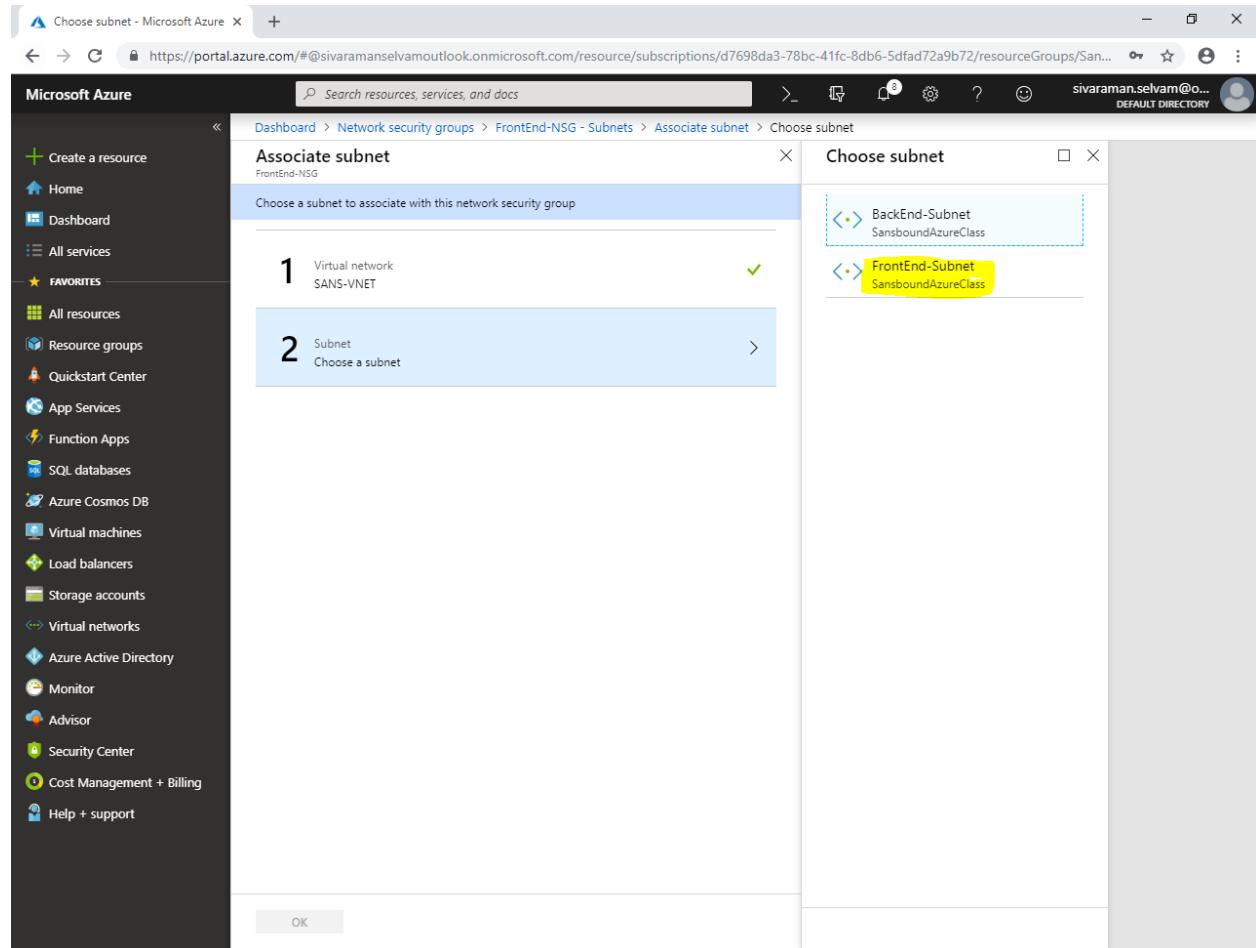


Click on “**SANS-VNET**” to select the Virtual network for the Network Security Group.



The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu is visible with various service icons. The main area displays a step-by-step wizard titled "Associate subnet". Step 1, "Virtual network", has a callout pointing to the "SANS-VNET" entry in the "Choose virtual network" dialog box. Step 2, "Subnet", is also shown. The "Choose virtual network" dialog includes an informational message about the selected subscription and location, and a list of available virtual networks, with "SANS-VNET" highlighted.

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**.

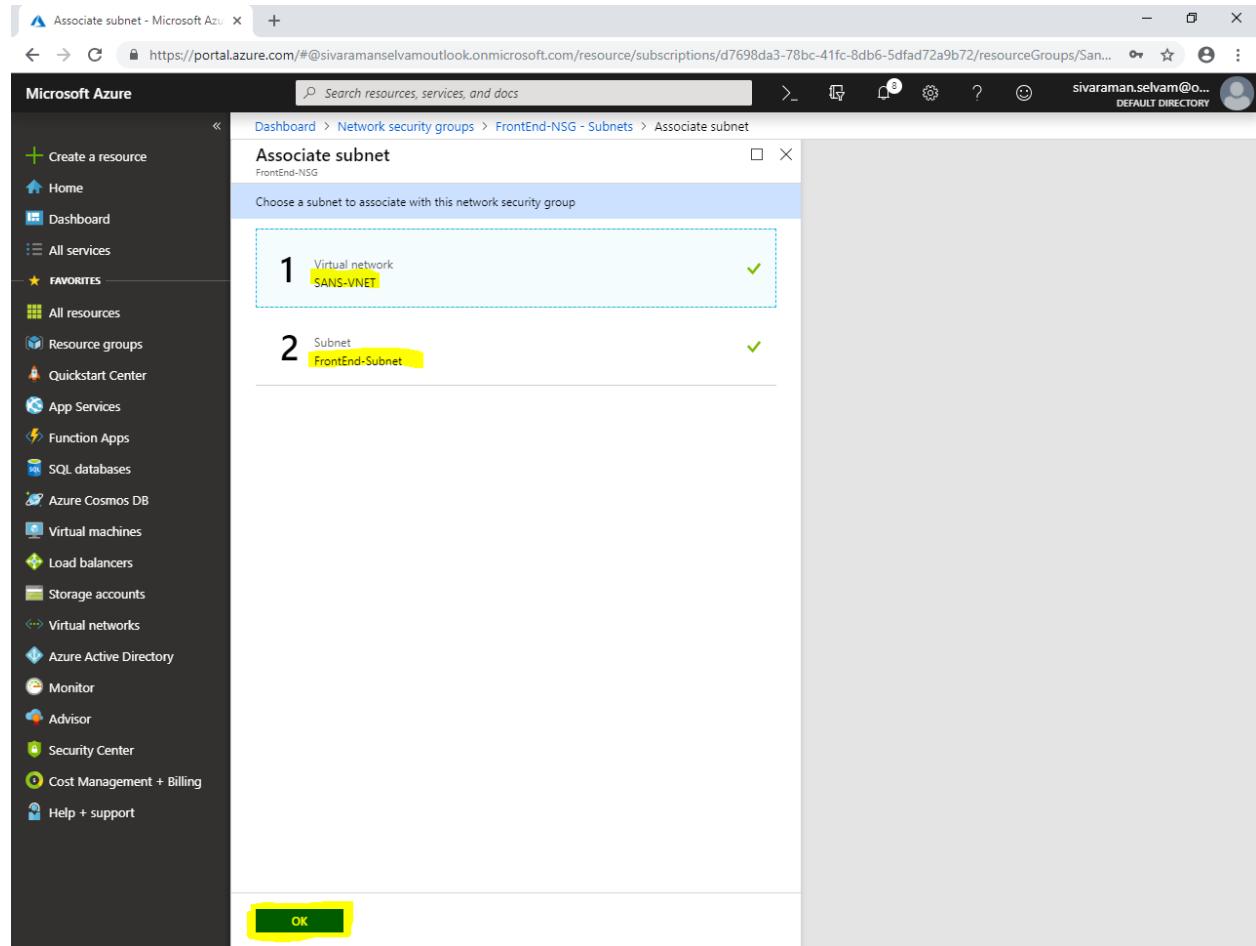


The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu is visible with various service icons. The main area displays a 'Associate subnet' dialog box. The dialog has two steps: Step 1 shows a 'Virtual network' named 'SANS-VNET' with a checkmark. Step 2 shows a 'Subnet' section with the instruction 'Choose a subnet'. Two subnets are listed: 'BackEnd-Subnet' and 'FrontEnd-Subnet'. The 'FrontEnd-Subnet' is highlighted with a yellow box. At the bottom of the dialog, there is an 'OK' button.

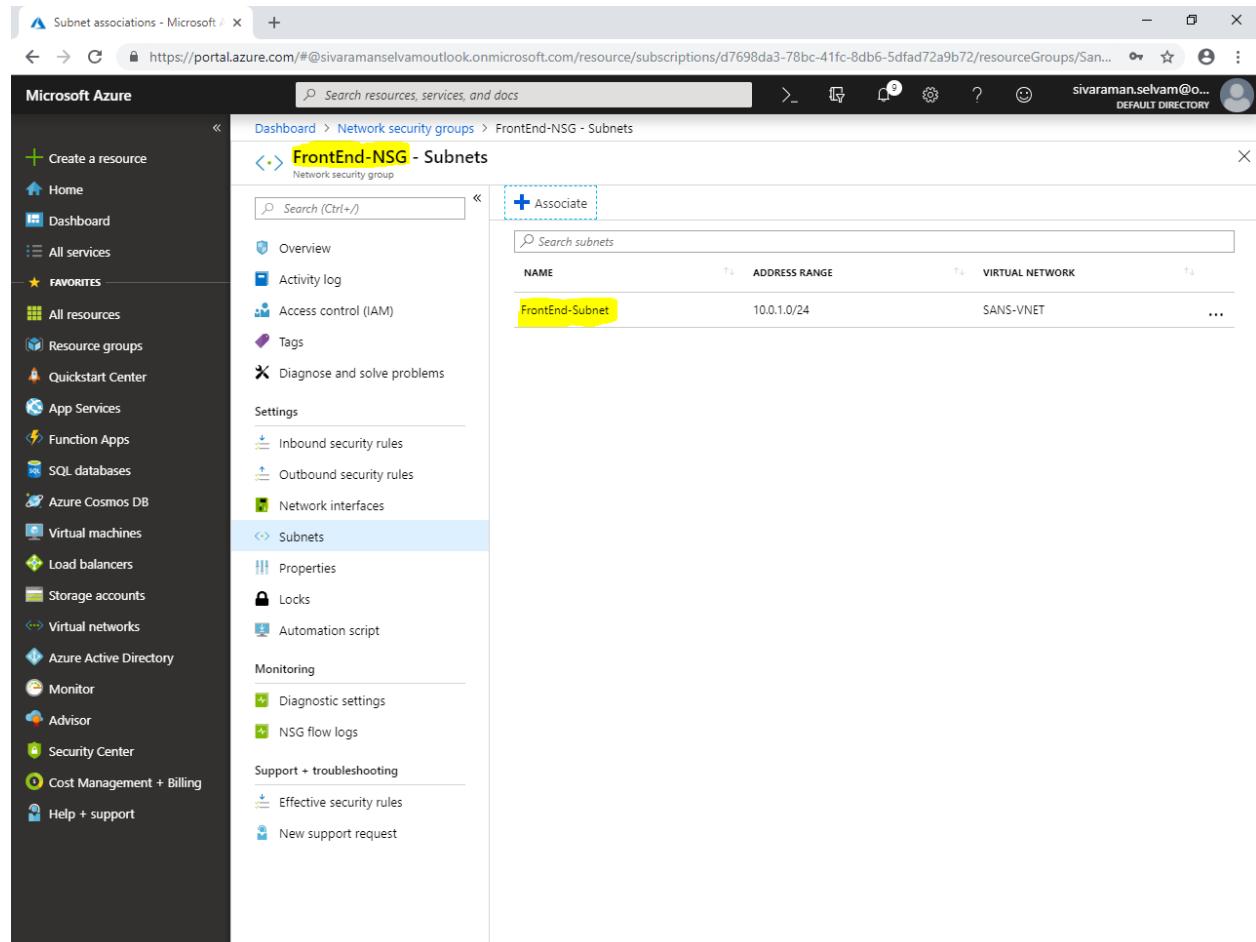
Ensure that “Virtual network” as “**SANS-VNET**”.

Ensure that “Subnet” as “**FrontEnd-Subnet**”.

Click “**Ok**”.



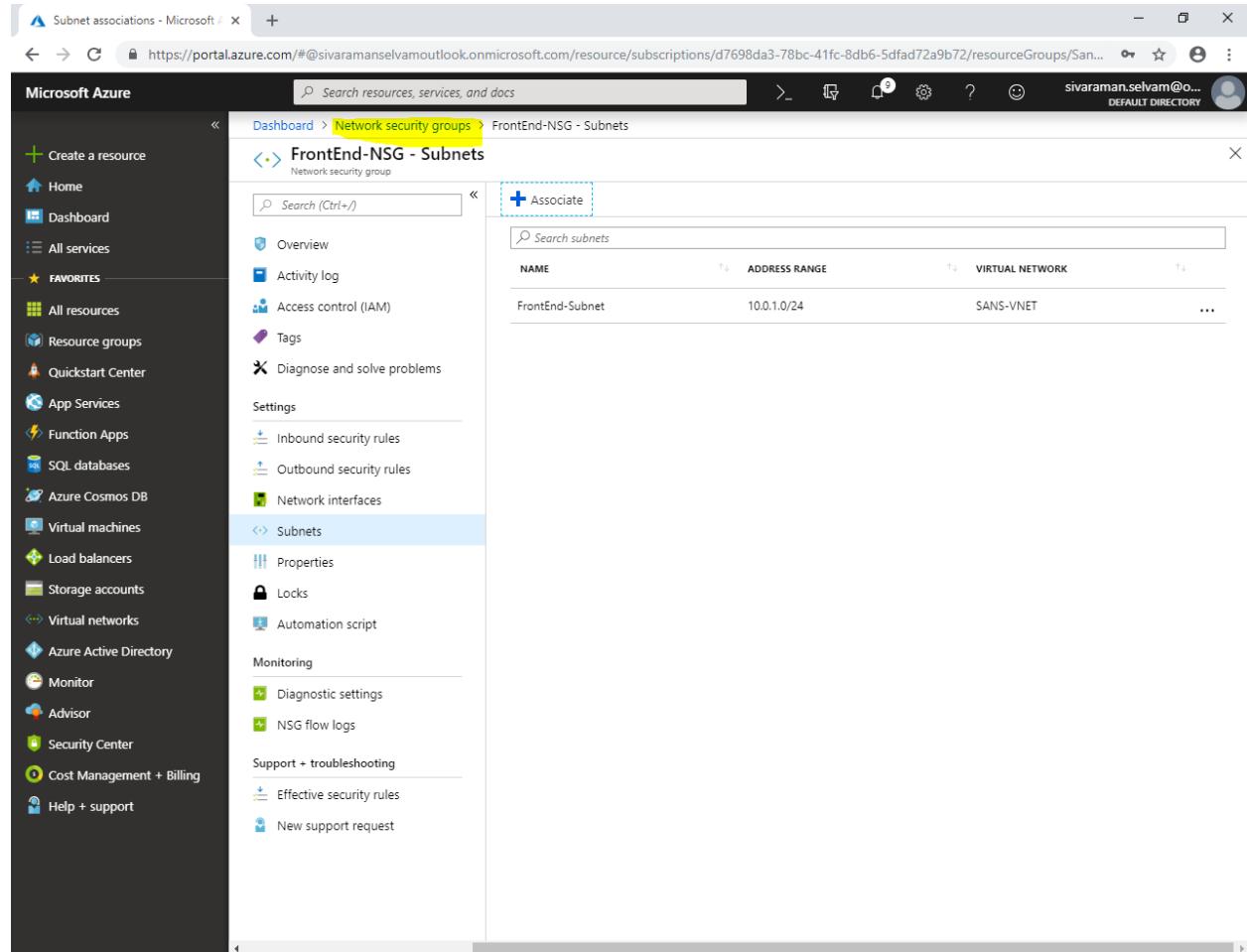
In “FrontEnd-NSG” we have associated FrontEnd-Subnet.



The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, and Favorites. Under Favorites, the 'Virtual networks' section is expanded, showing options like Subnets, Virtual machines, Load balancers, and Storage accounts. The main content area is titled 'FrontEnd-NSG - Subnets' and shows a table of associated subnets:

NAME	ADDRESS RANGE	VIRTUAL NETWORK
FrontEnd-Subnet	10.0.1.0/24	SANS-VNET

Click on “Network security groups”.

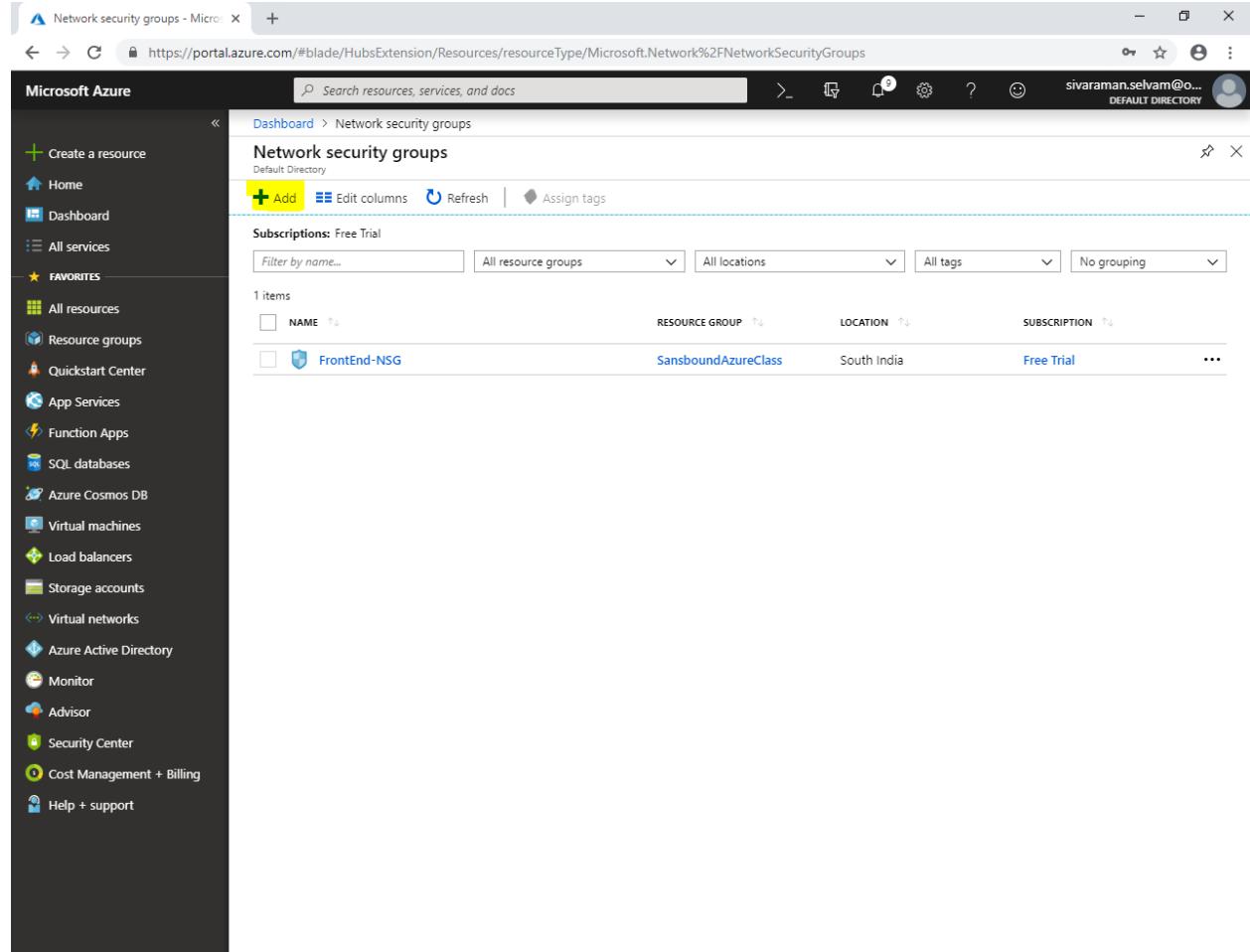


The screenshot shows the Microsoft Azure portal interface. The left sidebar is filled with various service icons under categories like Favorites, All services, and Favorites. The main content area is titled 'FrontEnd-NSG - Subnets' and shows a list of subnets. One subnet, 'FrontEnd-Subnet', is listed with its details: NAME: FrontEnd-Subnet, ADDRESS RANGE: 10.0.1.0/24, and VIRTUAL NETWORK: SANS-VNET. There is also a 'Associate' button above the subnet table.

NAME	ADDRESS RANGE	VIRTUAL NETWORK
FrontEnd-Subnet	10.0.1.0/24	SANS-VNET

In “Network Security groups”.

Click “Add”.



The screenshot shows the Microsoft Azure portal interface. The left sidebar is filled with various service icons under the 'All services' category. The main content area is titled 'Network security groups' and shows one item listed:

NAME	RESOURCE GROUP	LOCATION	SUBSCRIPTION
FrontEnd-NSG	SansboundAzureClass	South India	Free Trial

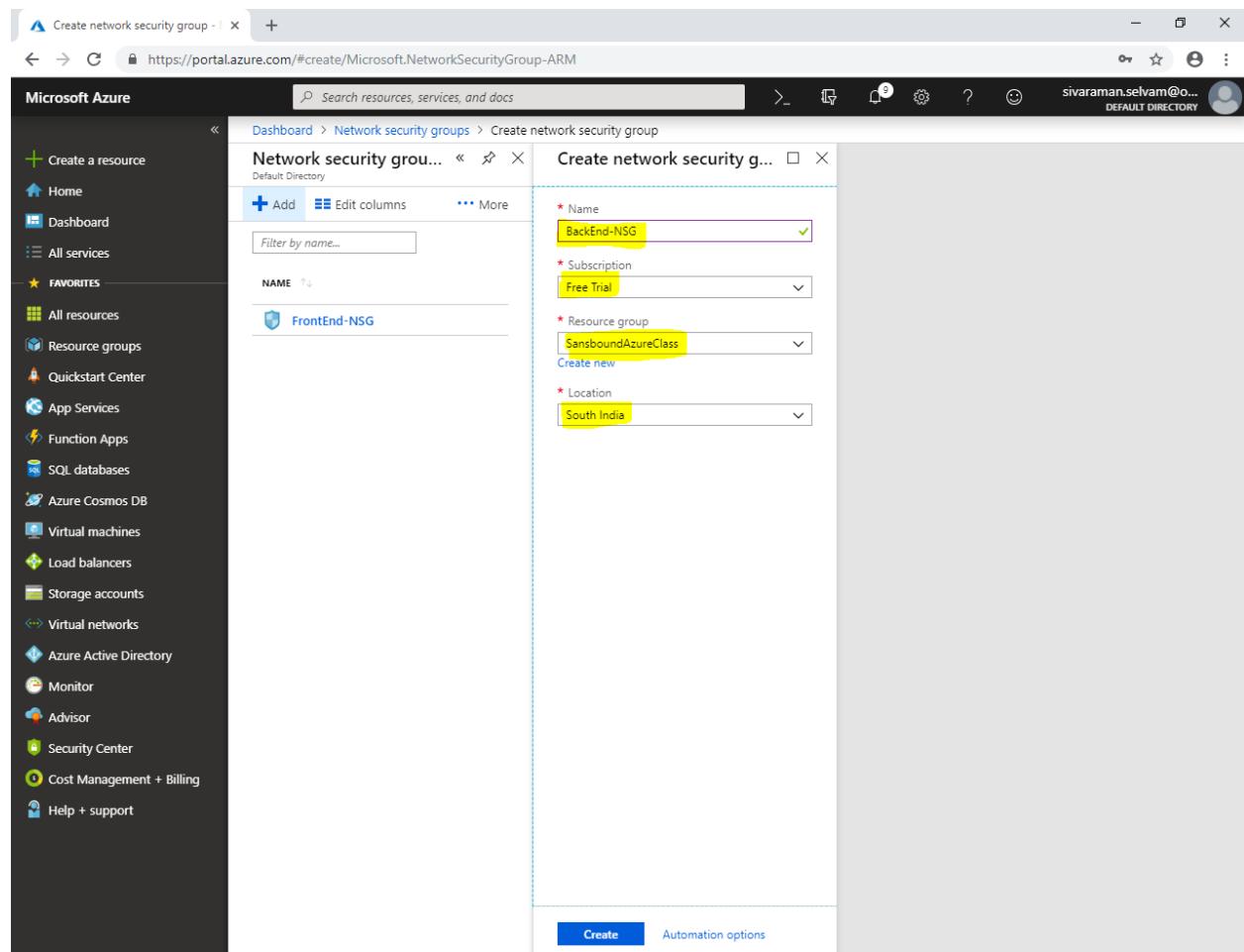
While creating “**Network security group**”

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

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

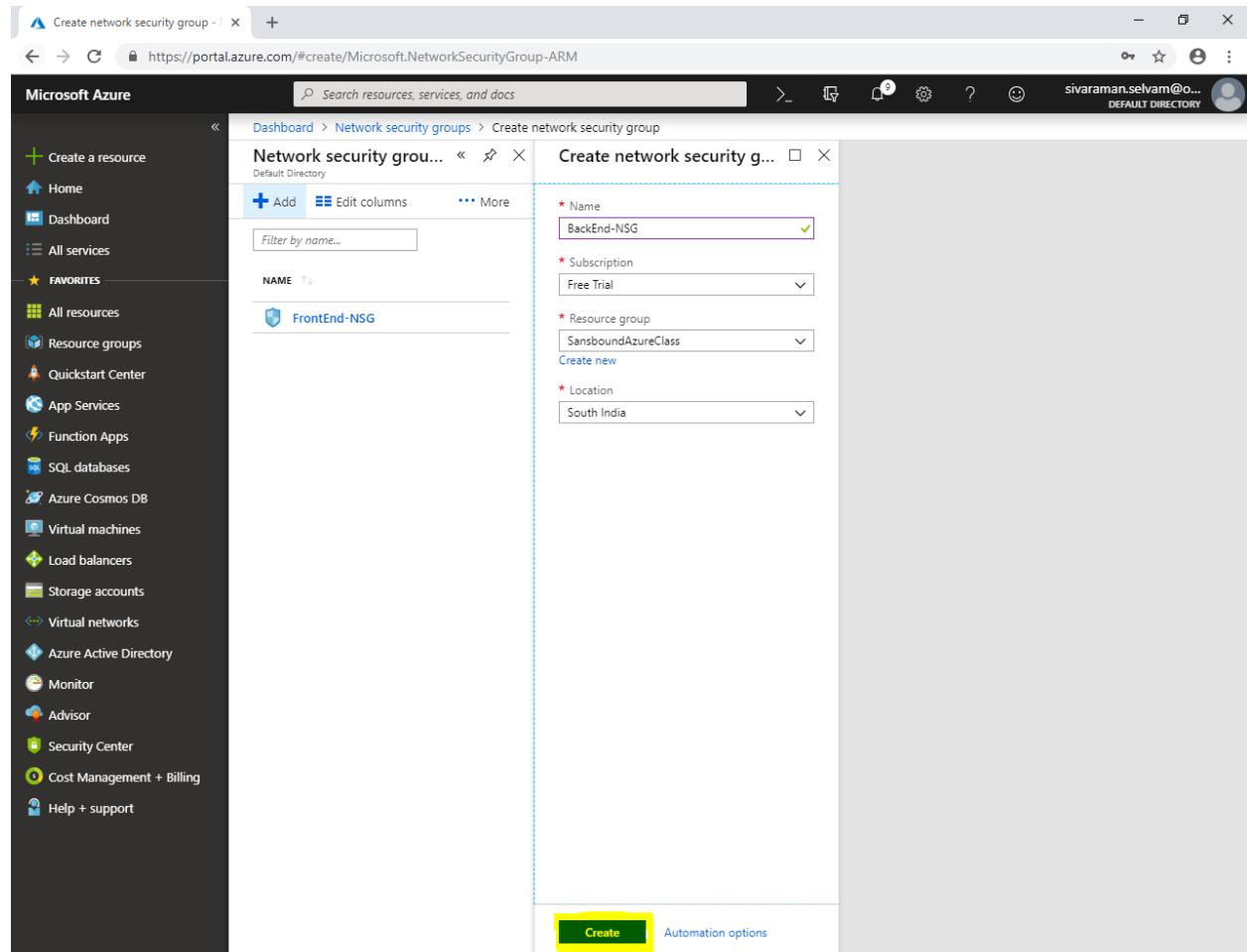
Select “**Resource group**” as “**SansboundAzureClass**”.

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



The screenshot shows the Azure portal interface for creating a Network Security Group (NSG). The left sidebar lists various Azure services. The main area shows the 'Create network security group' wizard. The 'Name' field is filled with 'BackEnd-NSG'. The 'Subscription' dropdown is set to 'Free Trial'. The 'Resource group' dropdown is set to 'SansboundAzureClass'. The 'Location' dropdown is set to 'South India'. At the bottom, there are 'Create' and 'Automation options' buttons.

Click "Create".



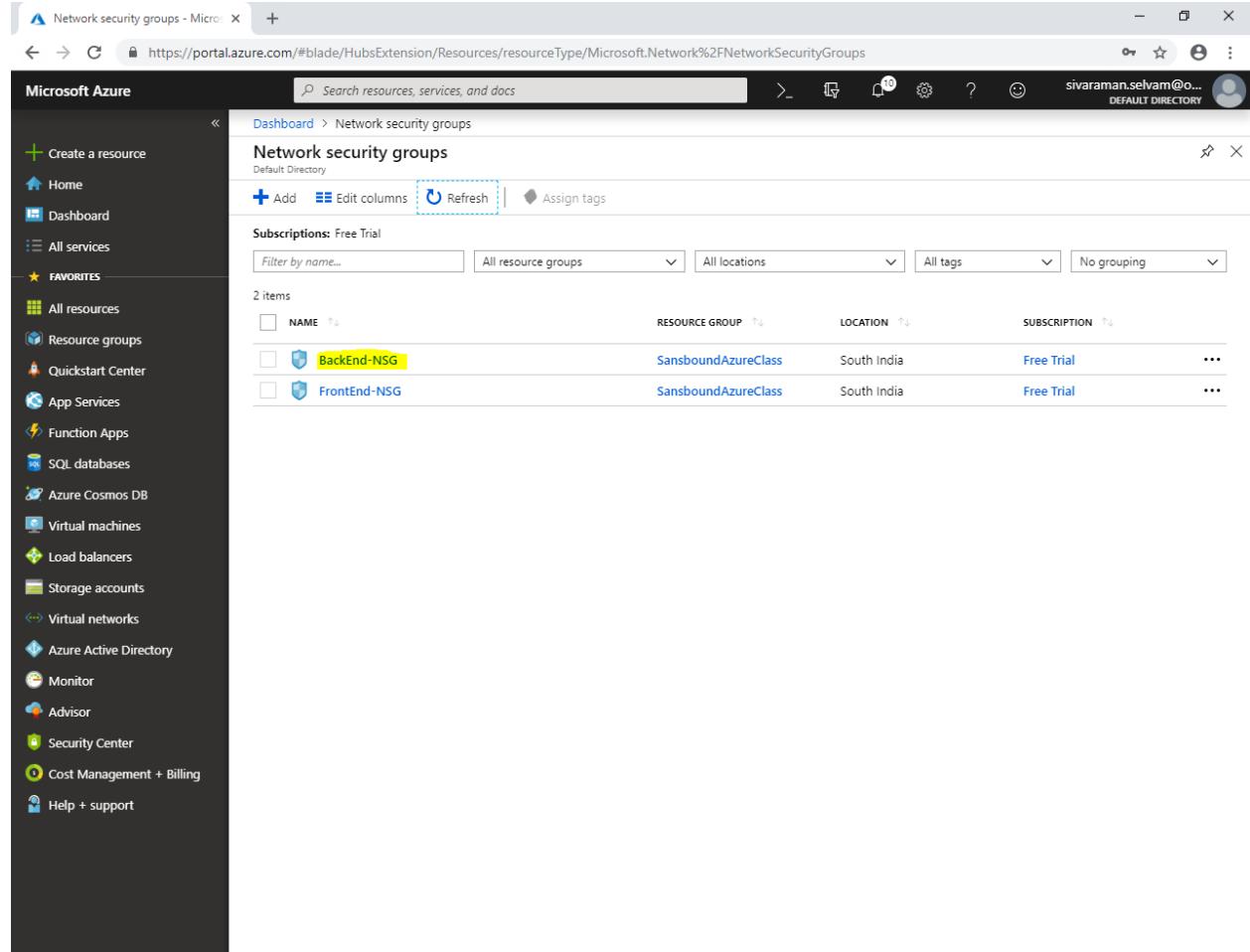
The screenshot shows the Microsoft Azure portal interface for creating a Network Security Group (NSG). The left sidebar contains various service icons under 'FAVORITES'. The main area shows a list of existing NSGs, with 'FrontEnd-NSG' selected. A 'Create network security g...' dialog box is open on the right, prompting for configuration details:

- Name: BackEnd-NSG
- Subscription: Free Trial
- Resource group: SansboundAzureClass
- Location: South India

The 'Create' button at the bottom of the dialog box is highlighted with a yellow box.

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

Click on “**BackEnd-NSG**”.



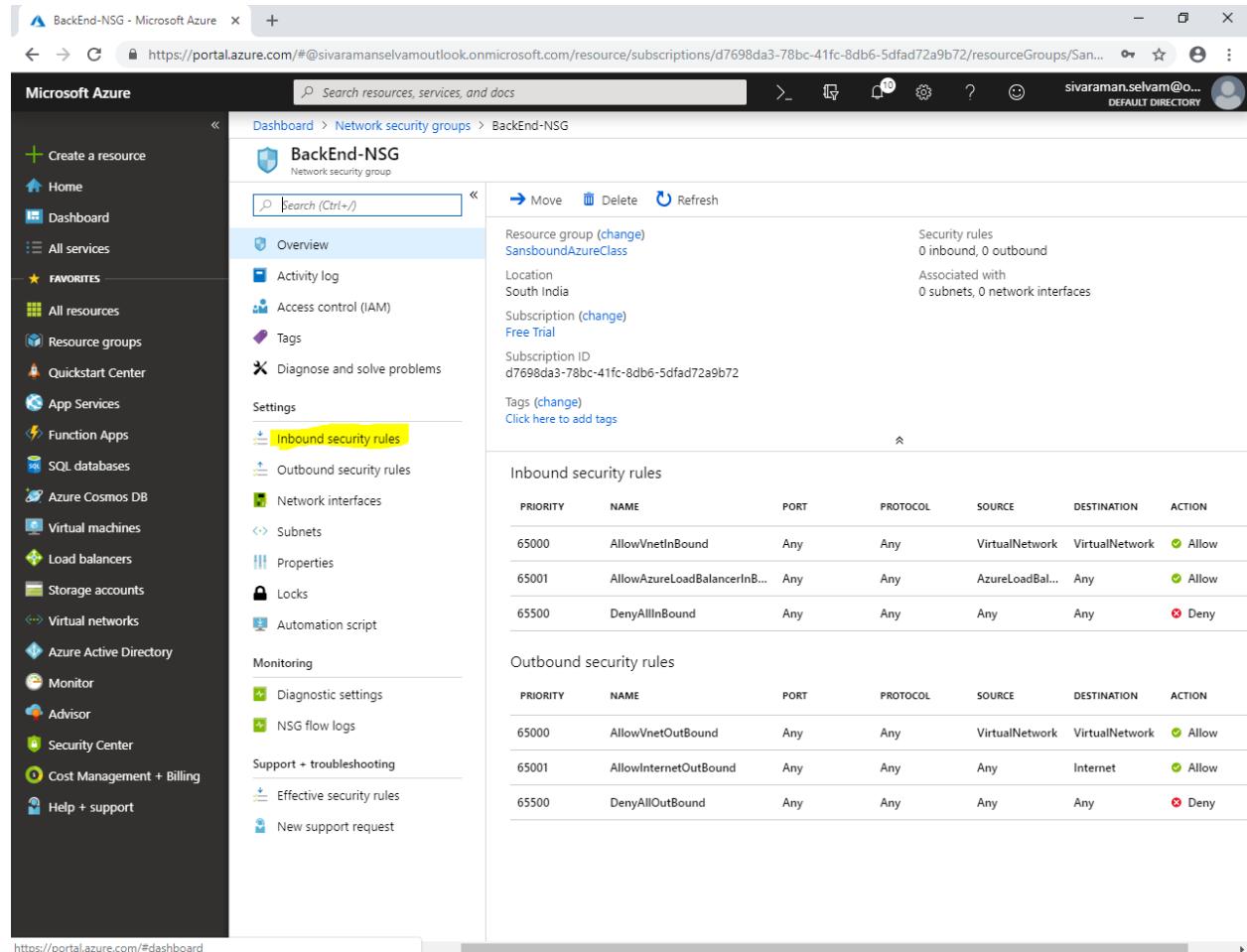
The screenshot shows the Microsoft Azure portal interface. The left sidebar is the navigation menu with various service icons. The main content area is titled "Network security groups". At the top, there are buttons for "+ Add", "Edit columns", "Refresh" (which is highlighted with a dashed blue border), and "Assign tags". Below this, a section titled "Subscriptions: Free Trial" shows filter options: "Filter by name...", "All resource groups", "All locations", "All tags", and "No grouping". A table lists two items:

NAME	RESOURCE GROUP	LOCATION	SUBSCRIPTION
BackEnd-NSG	SansboundAzureClass	South India	Free Trial
FrontEnd-NSG	SansboundAzureClass	South India	Free Trial

In “Network Security groups”.

In “BackEnd-NSG”.

Click “Inbound security rules”.



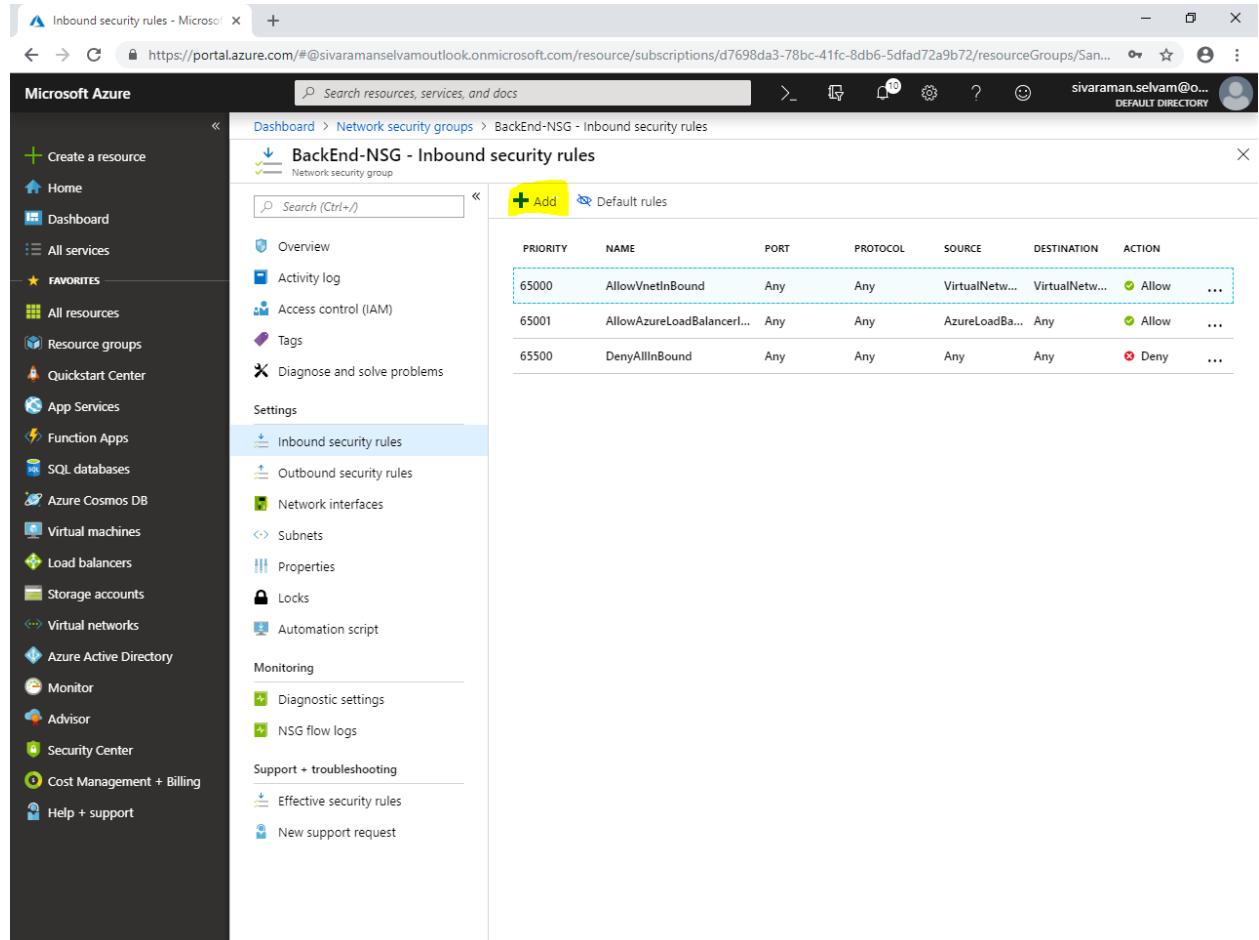
The screenshot shows the Azure portal interface for managing a Network Security Group (NSG). The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, Favorites, All resources, Resource groups, Quickstart Center, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Billing, and Help + support. The main content area is titled "BackEnd-NSG" and shows the "Overview" tab selected. It displays basic information such as the resource group (change), location (South India), subscription (change), and tags. Below this, under "Settings", the "Inbound security rules" link is highlighted with a yellow box. The "Inbound security rules" table lists three entries:

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBal...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Below the inbound rules, there is a section for "Outbound security rules" which also lists three entries:

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Click “Add”.



The screenshot shows the Microsoft Azure portal interface for managing Network Security Groups (NSGs). The left sidebar contains a navigation menu with various service icons. The main content area is titled "BackEnd-NSG - Inbound security rules" under "Network security group". A search bar is at the top. Below it, there are two buttons: "+ Add" (highlighted with a yellow box) and "Default rules". A table lists three existing inbound security rules:

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetInBound	Any	Any	VirtualNetw...	VirtualNetw...	Allow
65001	AllowAzureLoadBalancer...	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.

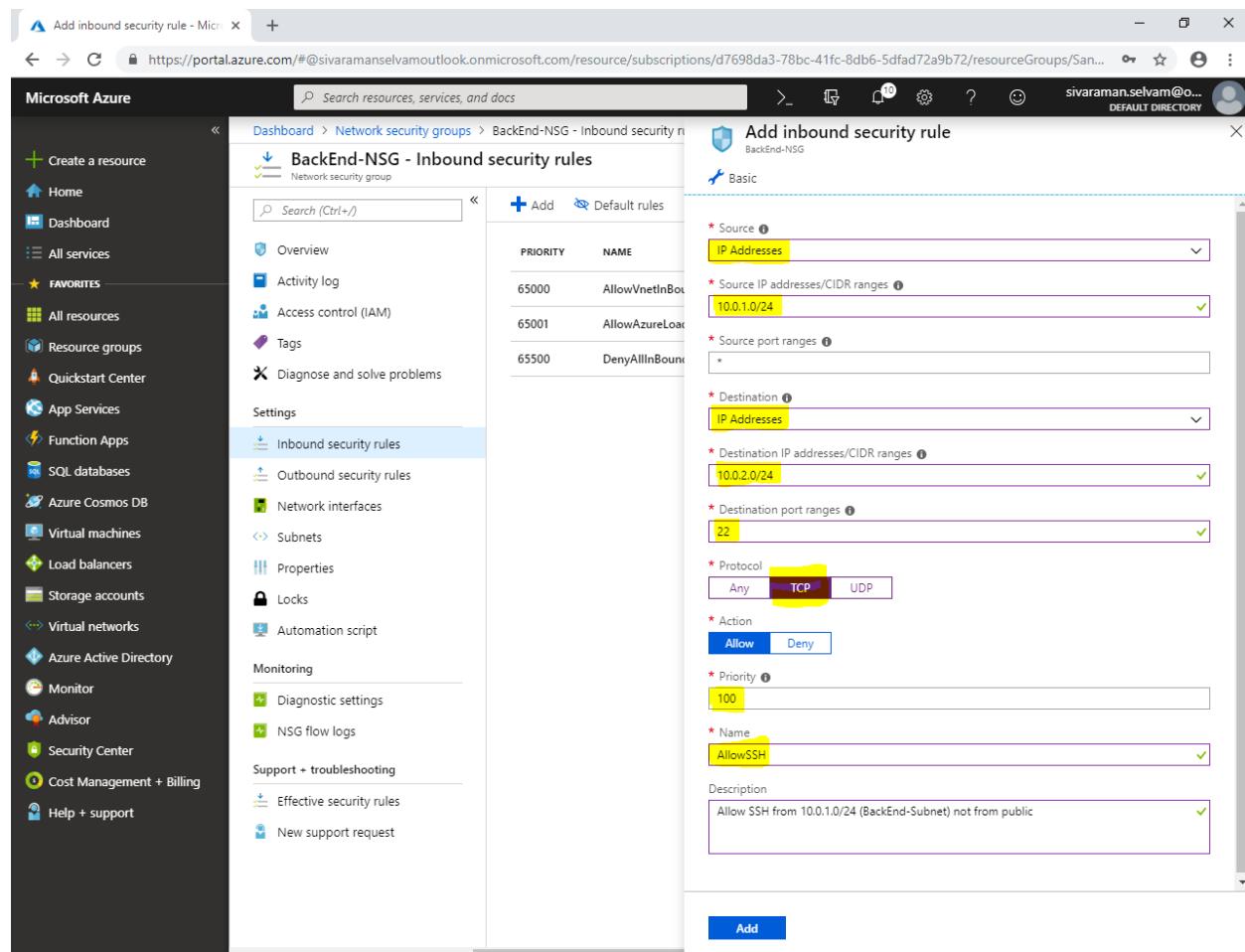
Type “**Destination port ranges**” as “**22**”.

Protocol “**TCP**”.

Click “**Allow**”.

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

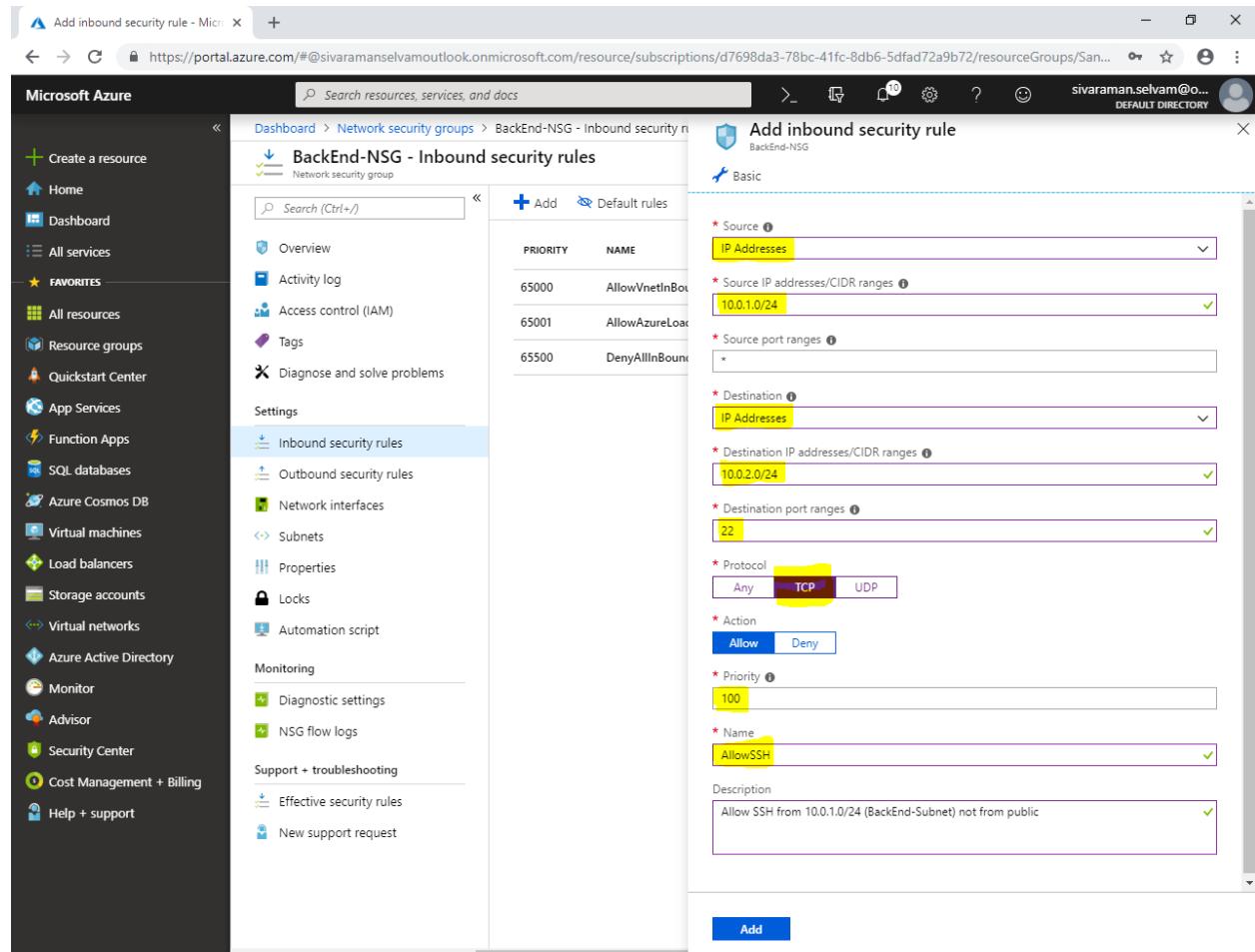
Name as “**AllowSSH**”.



The screenshot shows the Microsoft Azure portal interface for managing Network Security Groups (NSGs). On the left, the navigation menu includes options like 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, and Help + support. The main area displays the 'BackEnd-NSG - Inbound security rules' section under the 'Network security group' settings. A new rule is being added with the following details:

- Source:** IP Addresses (10.0.1.0/24)
- Destination:** IP Addresses (10.0.2.0/24)
- Destination port ranges:** 22
- Protocol:** TCP
- Action:** Allow
- Priority:** 100
- Name:** AllowSSH
- Description:** Allow SSH from 10.0.1.0/24 (BackEnd-Subnet) not from public

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



Add inbound security rule

Basic

PRIORITY	NAME
65000	AllowVnetInBound
65001	AllowAzureLoadBalancer
65500	DenyAllInBound

Inbound security rules

Source
IP Addresses: 10.0.1.0/24

Destination
IP Addresses: 10.0.2.0/24

Protocol
TCP

Action
Allow

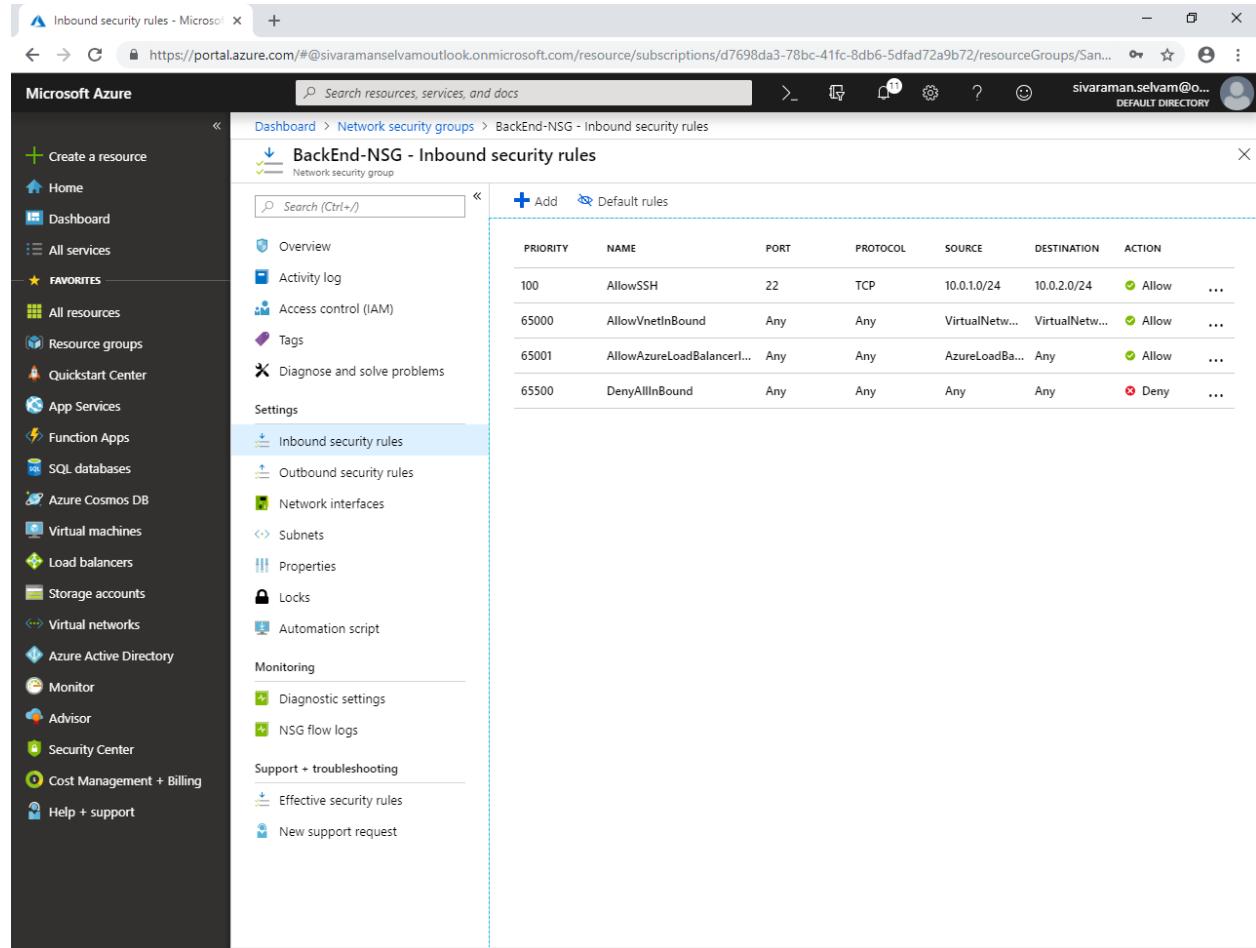
Priority
100

Name
AllowSSH

Description
Allow SSH from 10.0.1.0/24 (BackEnd-Subnet) not from public

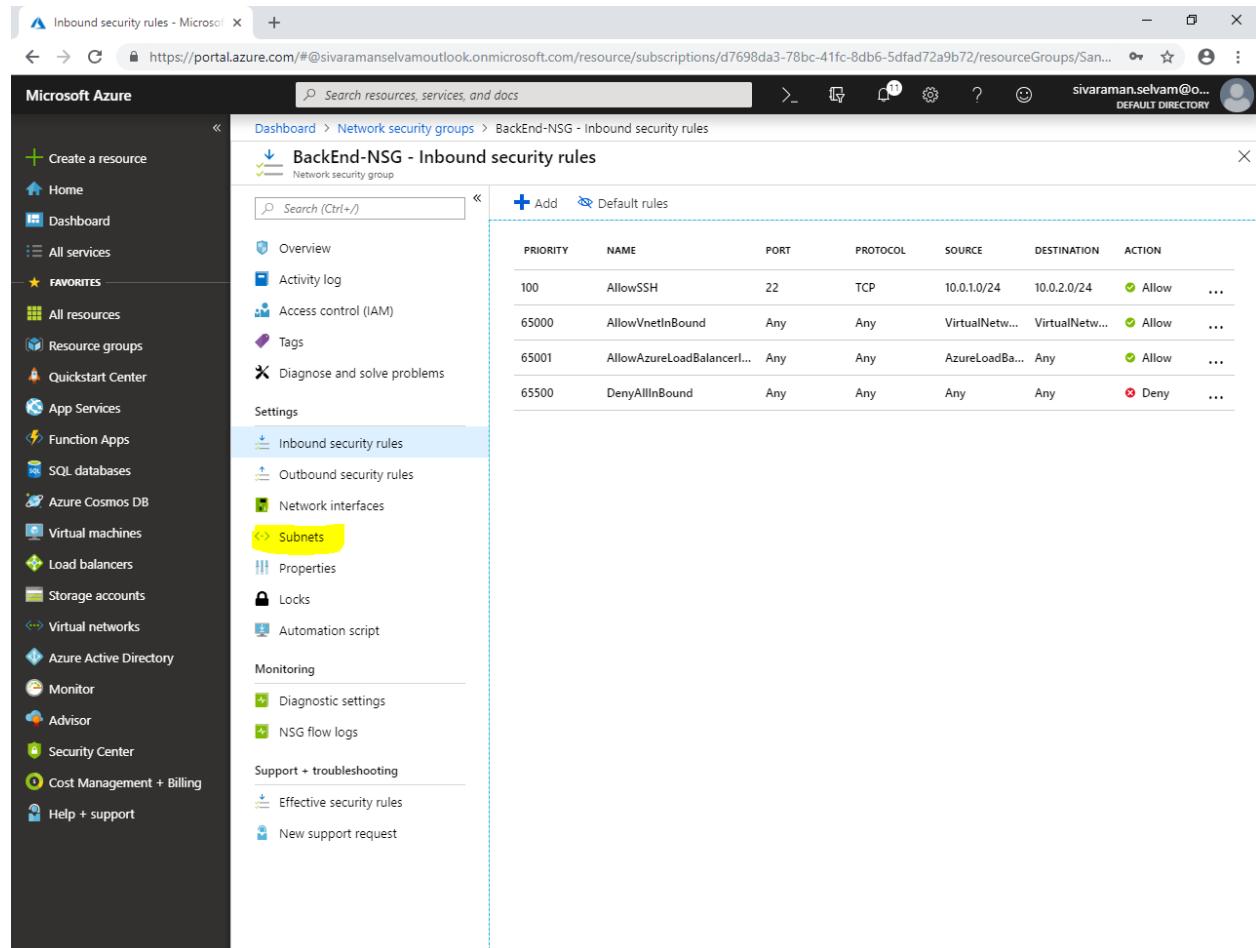
Add

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



PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	AllowSSH	22	TCP	10.0.1.0/24	10.0.2.0/24	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetw...	VirtualNetw...	Allow
65001	AllowAzureLoadBalancer...	Any	Any	AzureLoadBa...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

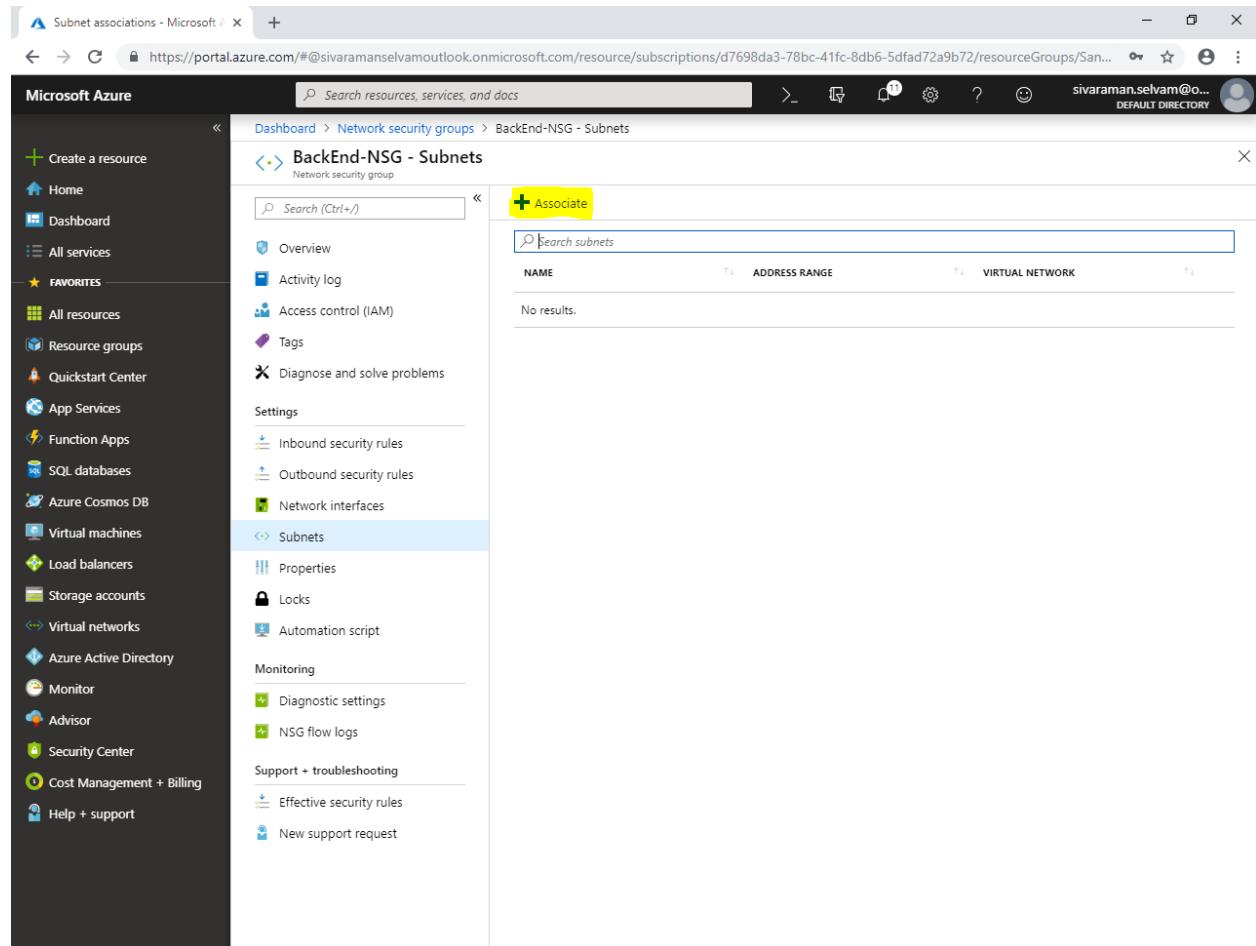
Click “Subnets”.



The screenshot shows the Microsoft Azure portal interface. The user is navigating through the Network security groups section, specifically the BackEnd-NSG - Inbound security rules page. On the left sidebar, under the 'Subnets' section, the 'Subnets' option is highlighted with a yellow box. The main pane displays a table of inbound security rules with the following data:

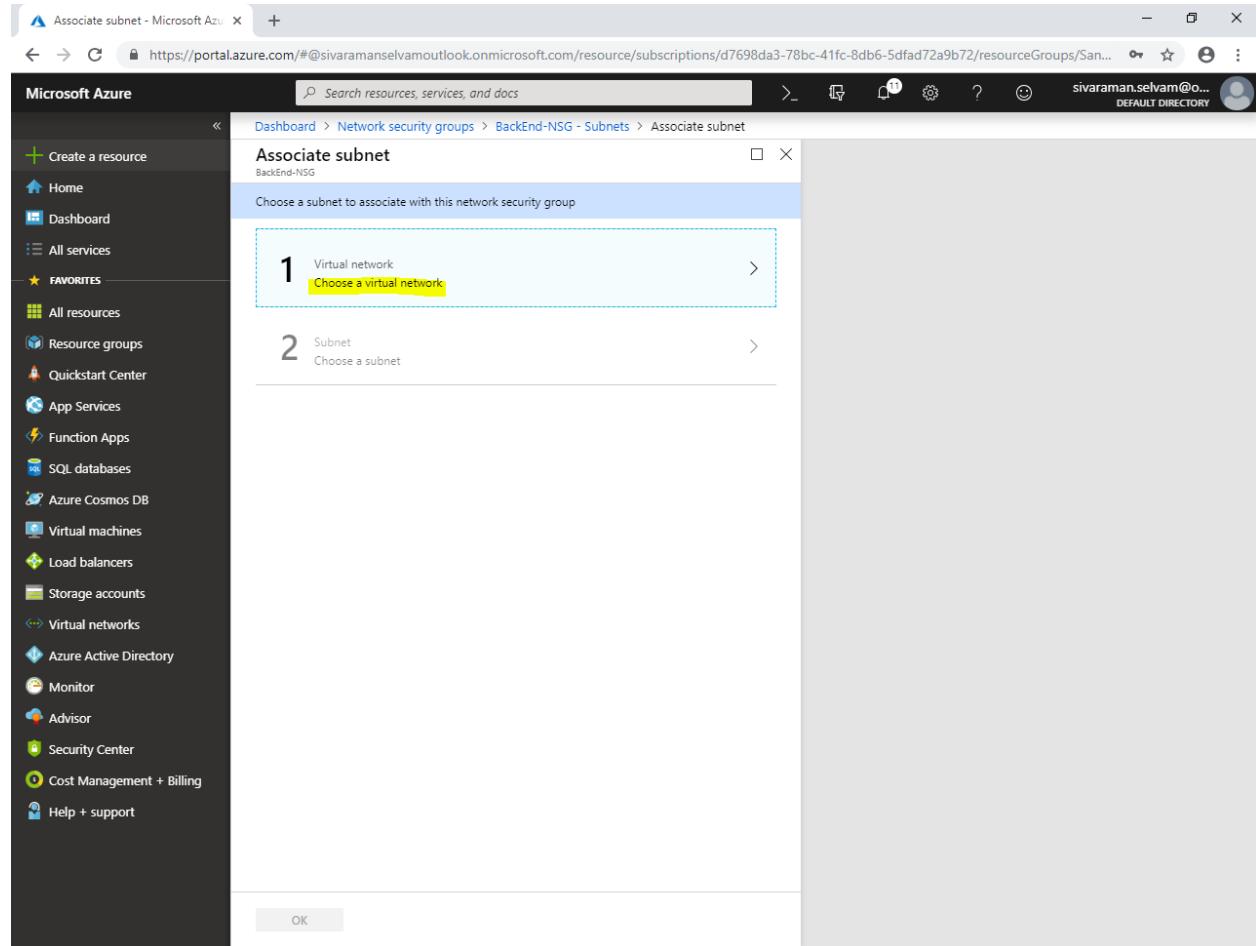
PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	AllowSSH	22	TCP	10.0.1.0/24	10.0.2.0/24	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetw...	VirtualNetw...	Allow
65001	AllowAzureLoadBalancerI...	Any	Any	AzureLoadBa...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Click “Associate” to associate the subnet to “Network Security Group”.



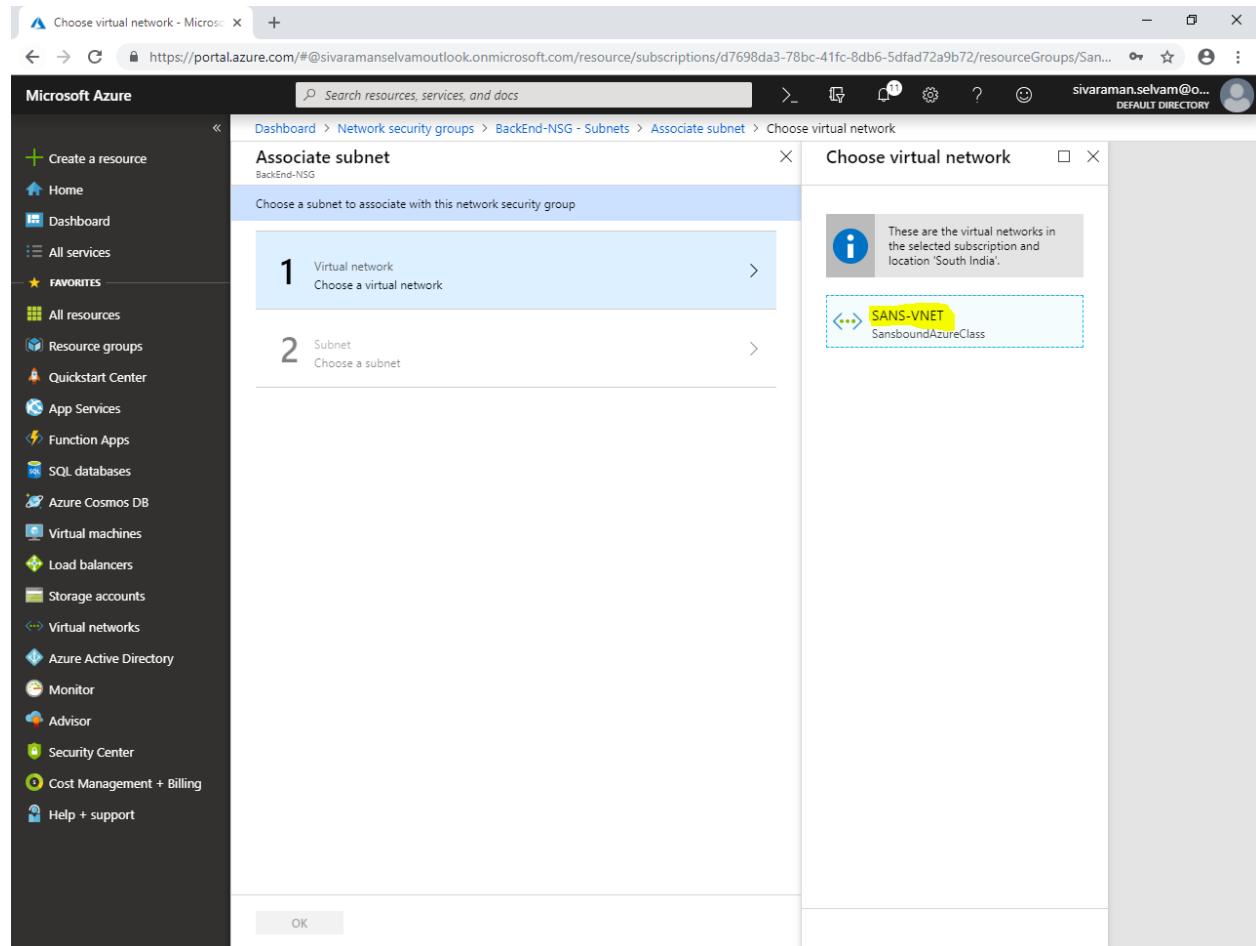
The screenshot shows the Microsoft Azure portal interface. The left sidebar is filled with various service icons under categories like Favorites, All resources, and Virtual networks. The main content area is titled "BackEnd-NSG - Subnets". On the left of this area, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (with Inbound security rules, Outbound security rules, Network interfaces, and Subnets selected), Properties, Locks, Automation script, Monitoring (Diagnostic settings, NSG flow logs), and Support + troubleshooting (Effective security rules, New support request). At the top right of the main content area, there's a yellow button labeled "+ Associate". Below it is a search bar with placeholder text "Search subnets". A table header is visible with columns for NAME, ADDRESS RANGE, and VIRTUAL NETWORK. The message "No results." is displayed below the table.

While “Associate subnet” click on “Choose a virtual network” to select “Virtual Network”.



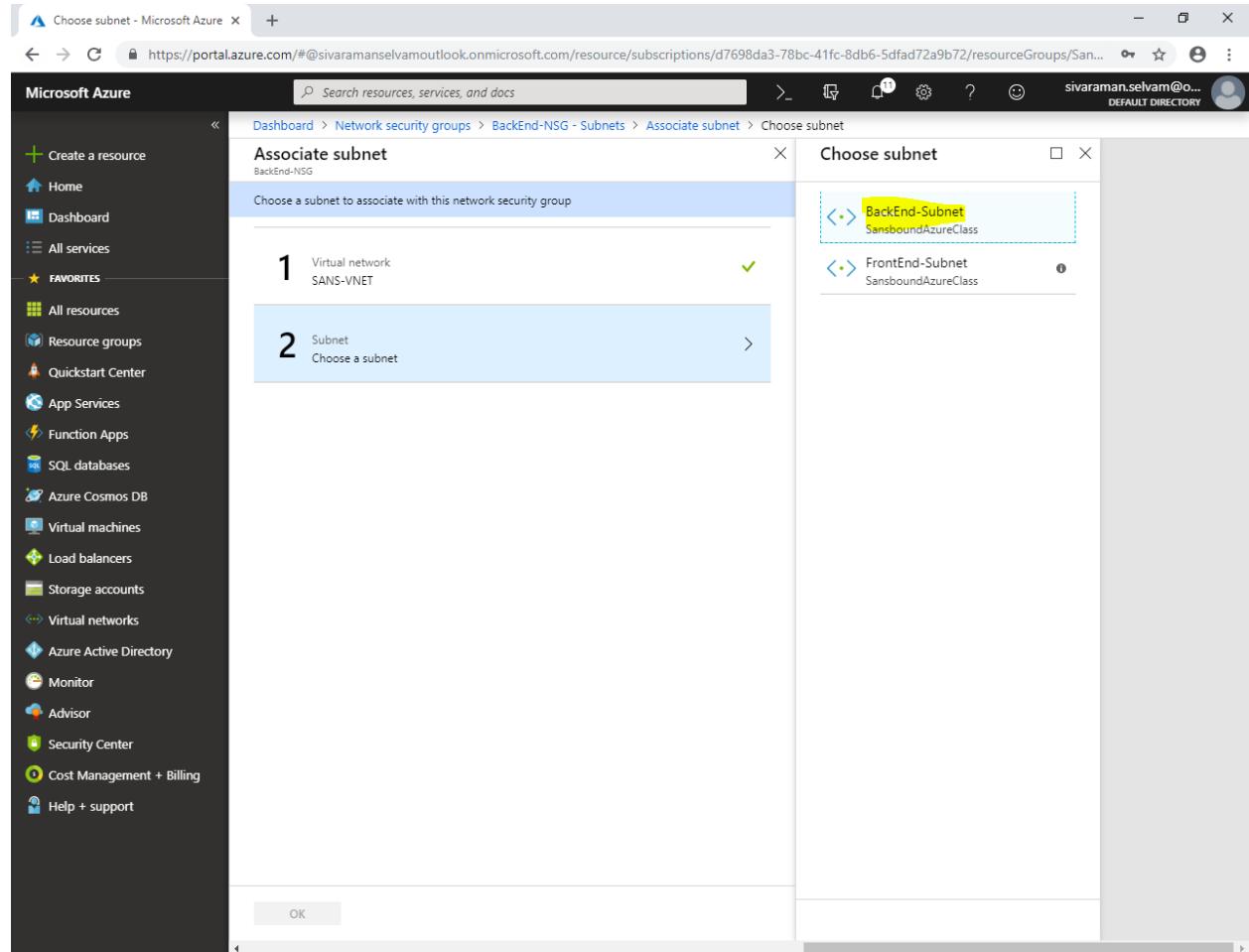
The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a list of services: Create a resource, Home, Dashboard, All services, Favorites (All resources, Resource groups, Quickstart Center, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts), and links to Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Billing, and Help + support. The main content area is titled "Associate subnet" under "BackEnd-NSG". It displays two steps: Step 1, "Choose a subnet to associate with this network security group", which is currently selected and highlighted with a yellow box around the "Choose a virtual network" button; Step 2, "Choose a subnet". At the bottom right of the dialog is an "OK" button.

Click on "SANS-VNET".



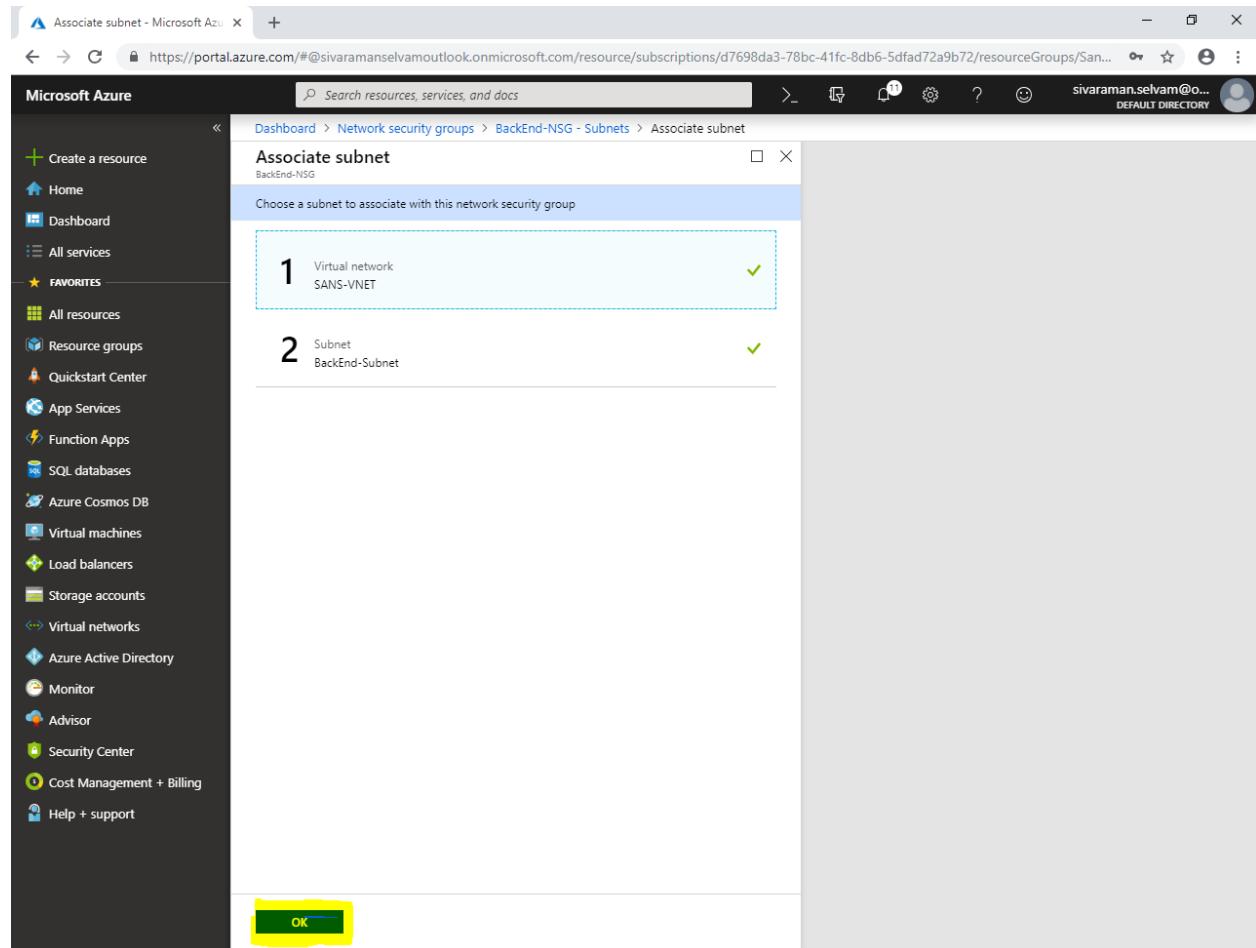
The screenshot shows the Microsoft Azure portal interface. The user is navigating through the Network security groups section to associate a subnet with a specific NSG. The current step is 'Choose a virtual network'. A callout box highlights the 'SANS-VNET' option, which is associated with the resource group 'SansboundAzureClass'. The left sidebar contains a list of favorite services, including App Services, Function Apps, SQL databases, and Virtual machines.

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



The screenshot shows the Microsoft Azure portal interface. The left sidebar is filled with various service icons under the 'All services' category. The main area displays a 'Associate subnet' dialog for a 'BackEnd-NSG'. Step 1 shows a 'Virtual network' named 'SANS-VNET' with a green checkmark. Step 2 shows a 'Subnet' section with a blue arrow pointing right, labeled 'Choose a subnet'. To the right, a 'Choose subnet' pane lists two subnets: 'BackEnd-Subnet' (highlighted with a yellow box) and 'FrontEnd-Subnet'. Both subnets are associated with the 'SansboundAzureClass' security group. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

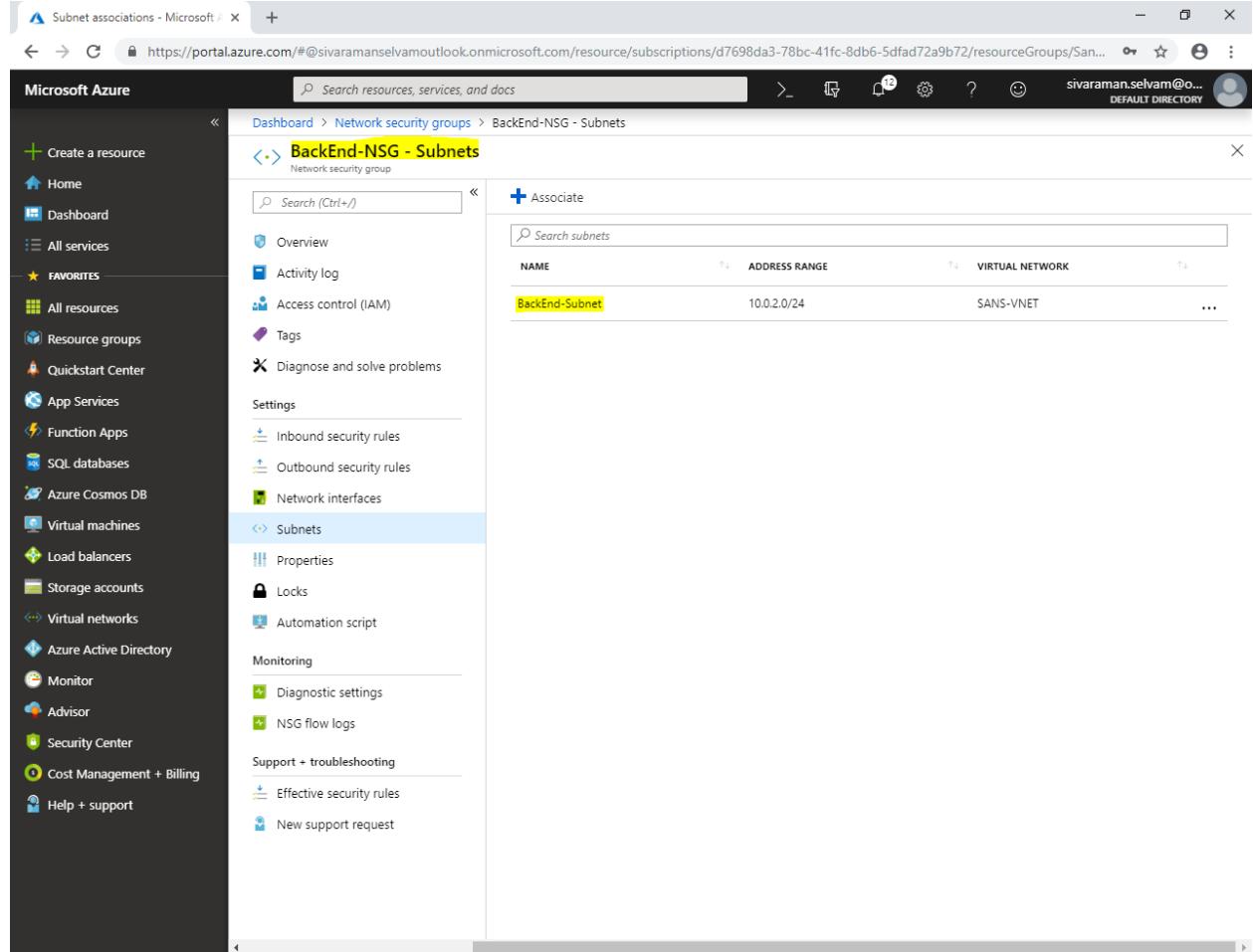
Click "OK".



The screenshot shows the Microsoft Azure portal interface. The user is in the 'Associate subnet' step of associating a Network Security Group (NSG) with a subnet. Two items are selected: 'Virtual network SANS-VNET' and 'Subnet BackEnd-Subnet'. Both items have a green checkmark next to them. At the bottom of the dialog, there is a large 'OK' button, which is highlighted with a yellow box to indicate it should be clicked.

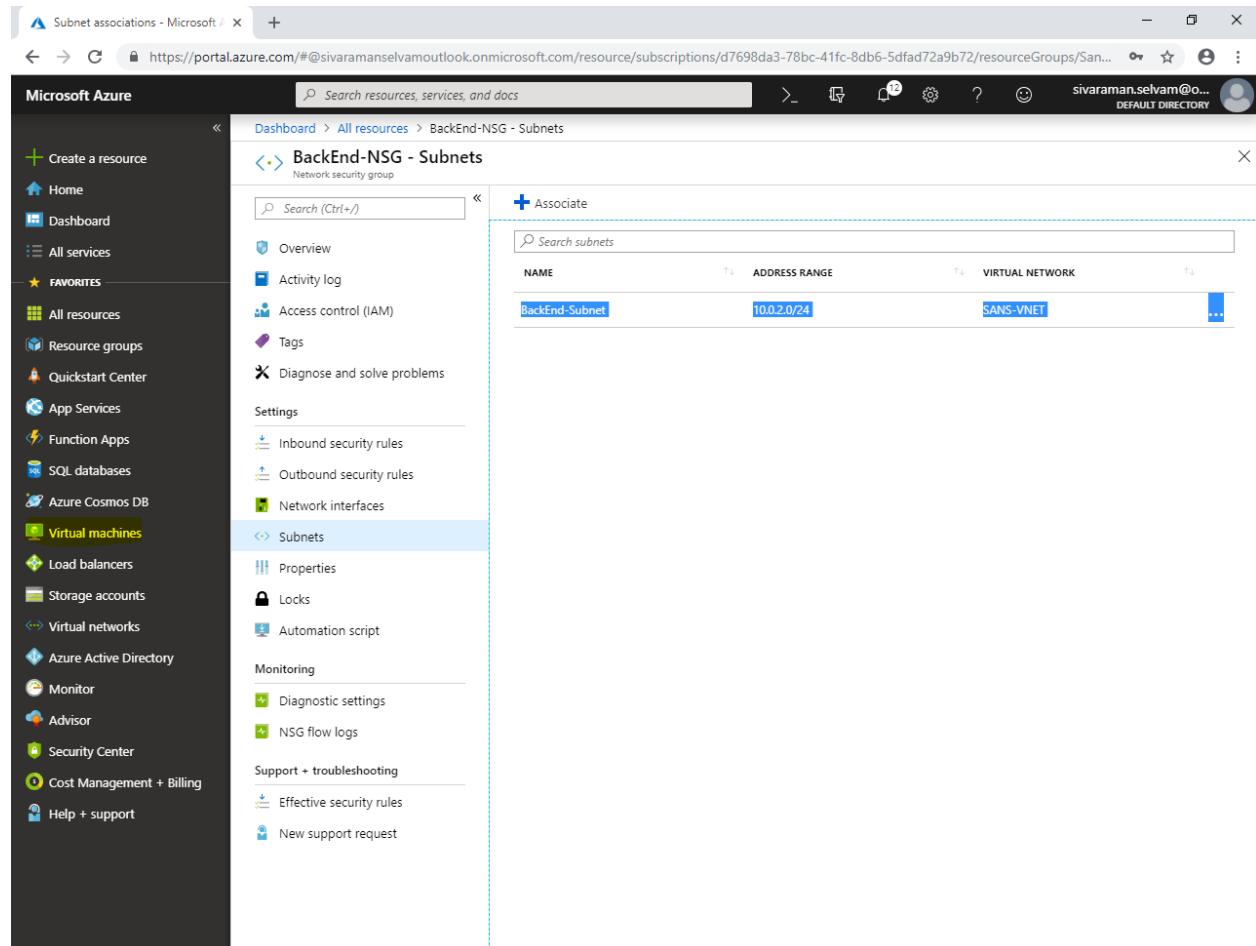
In “BackEnd-NSG – Subnets”.

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



NAME	ADDRESS RANGE	VIRTUAL NETWORK
BackEnd-Subnet	10.0.2.0/24	SANS-VNET

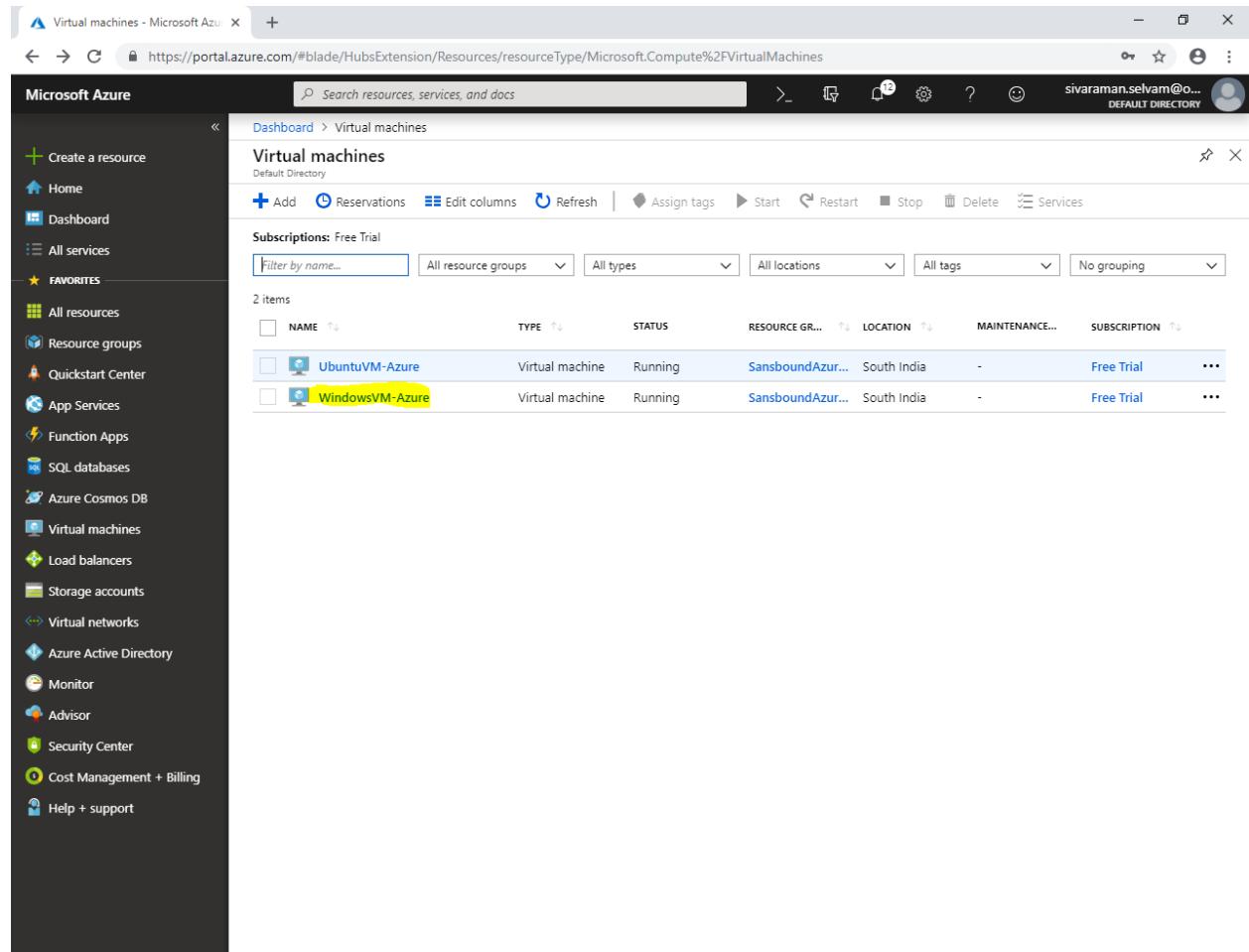
Click on “Virtual machines” in left side panel.



The screenshot shows the Microsoft Azure portal interface. The left sidebar is open, displaying various service options. The 'Virtual machines' option is highlighted with a yellow background. The main content area shows the 'BackEnd-NSG - Subnets' page for a Network Security Group. The subnets table lists one subnet named 'BackEnd-Subnet' with an address range of '10.0.2.0/24' and associated with the 'SANS-VNET' virtual network. A blue dashed box highlights the 'Associate' button and the subnets table.

NAME	ADDRESS RANGE	VIRTUAL NETWORK
BackEnd-Subnet	10.0.2.0/24	SANS-VNET

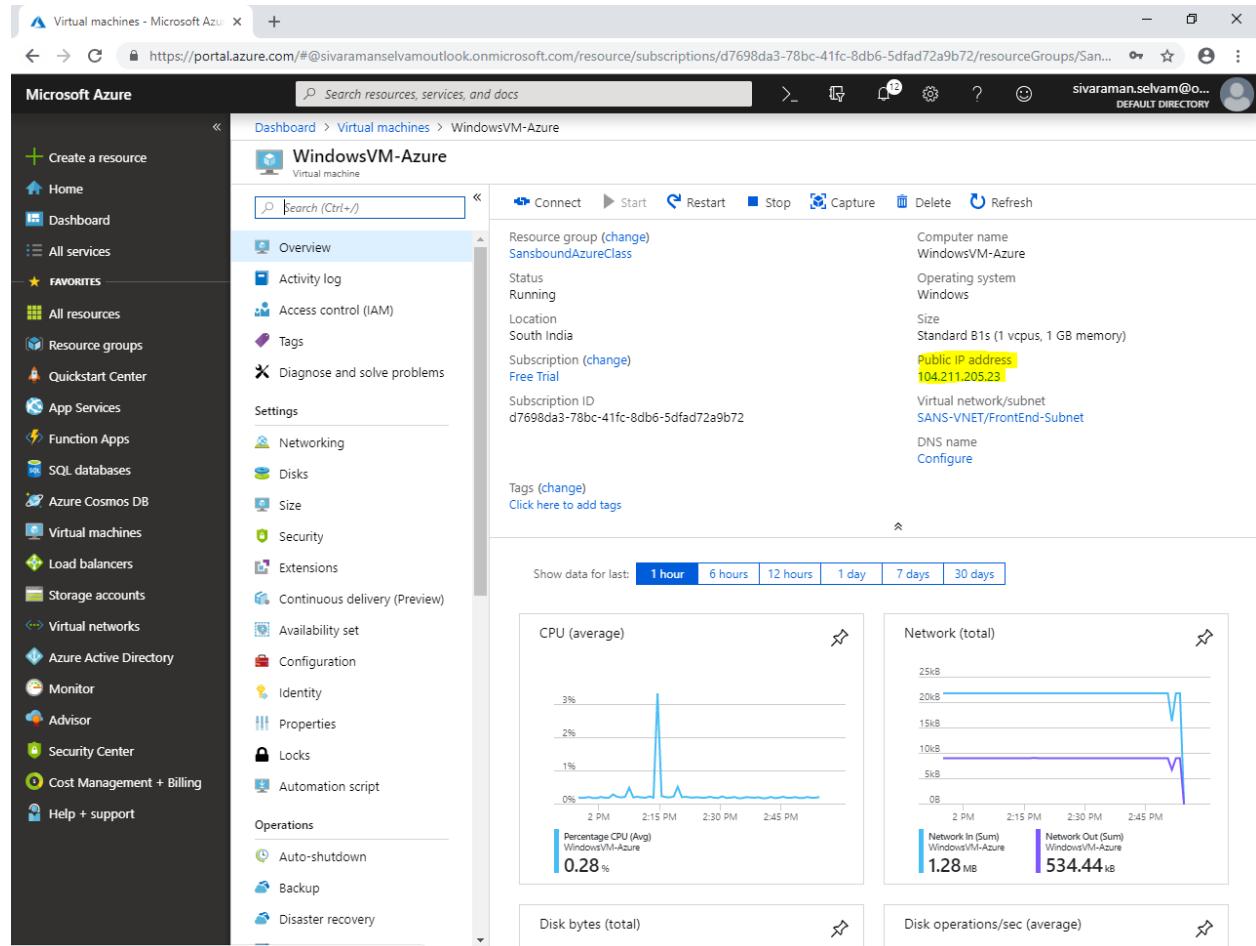
Click on "WindowsVM-Azure".



The screenshot shows the Microsoft Azure portal interface. The left sidebar is titled "Microsoft Azure" and contains a "FAVORITES" section with links to various services: Create a resource, Home, Dashboard, All services, 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, and Help + support. The main content area is titled "Virtual machines" and shows a list of "2 items". The table has columns: NAME, TYPE, STATUS, RESOURCE GR., LOCATION, MAINTENANCE..., and SUBSCRIPTION. The first item is "UbuntuVM-Azure" (Virtual machine, Running, SansboundAzur..., South India, -, Free Trial). The second item is "WindowsVM-Azure" (Virtual machine, Running, SansboundAzur..., South India, -, Free Trial). The URL in the browser bar is https://portal.azure.com/#blade/HubsExtension/Resources/resourceType/Microsoft.Compute%2FVirtualMachines.

NAME	TYPE	STATUS	RESOURCE GR...	LOCATION	MAINTENANCE...	SUBSCRIPTION
UbuntuVM-Azure	Virtual machine	Running	SansboundAzur...	South India	-	Free Trial
WindowsVM-Azure	Virtual machine	Running	SansboundAzur...	South India	-	Free Trial

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



The screenshot shows the Microsoft Azure portal interface for a virtual machine named "WindowsVM-Azure".

Resource Group: SansboundAzureClass

Status: Running

Location: South India

Subscription: Free Trial

Public IP Address: 104.211.205.23

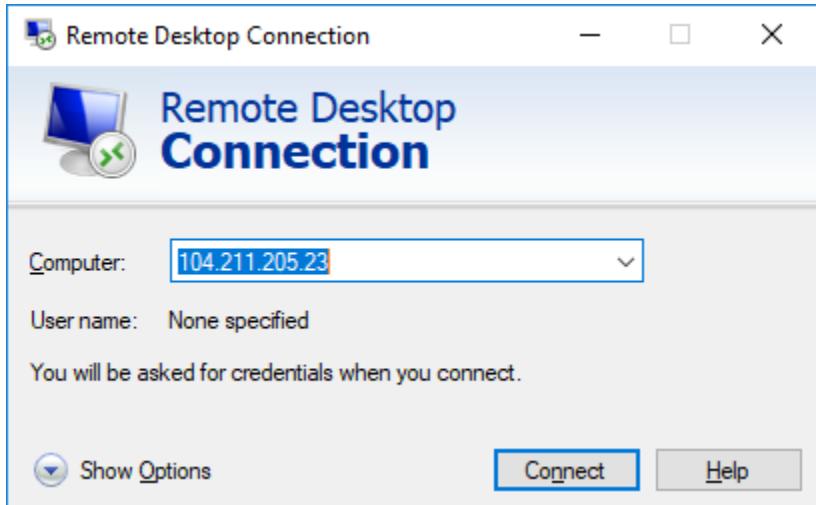
Virtual Network/Subnet: SANS-VNET/FrontEnd-Subnet

DNS Name: Configure

Performance Metrics (Last 1 hour):

- CPU (average):** Percentage CPU (Avg) WindowsVM-Azure 0.28 %
- Network (total):** Network In (Sum) WindowsVM-Azure 1.28 MB, Network Out (Sum) WindowsVM-Azure 534.44 kB
- Disk bytes (total):**
- Disk operations/sec (average):**

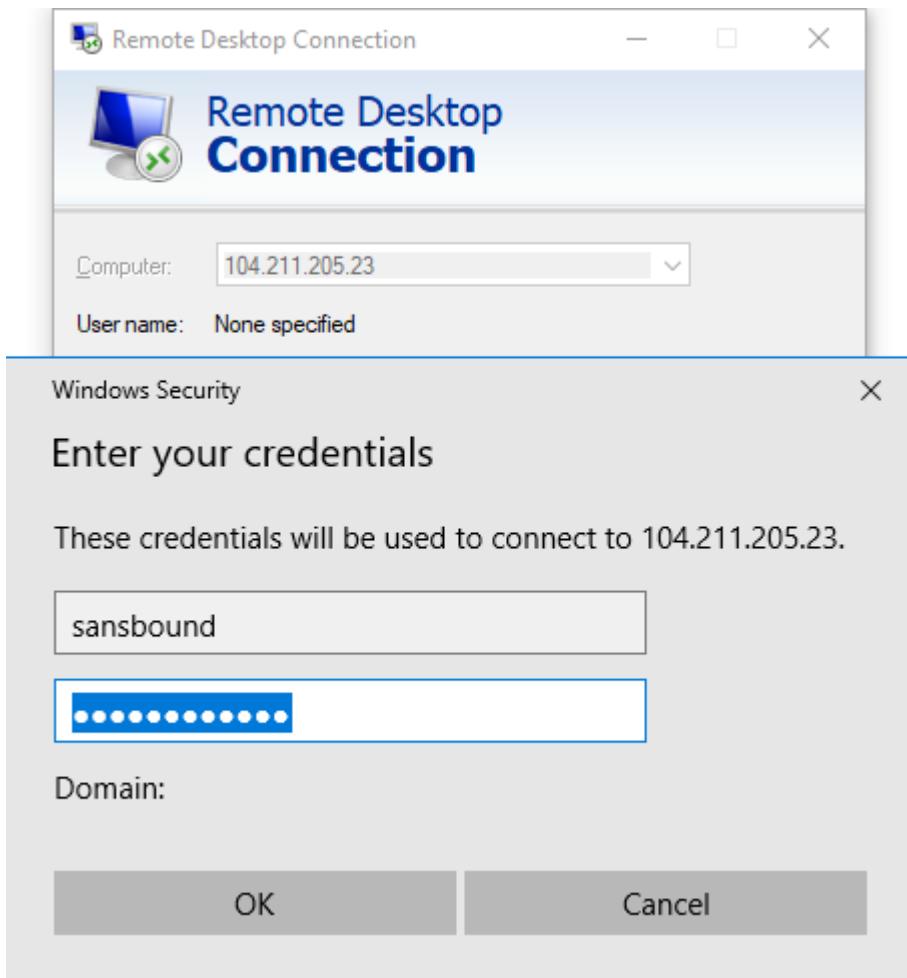
Type “**mstsc**” in your local machine, and type the Public IP address of the Windows Server 2008 R2.



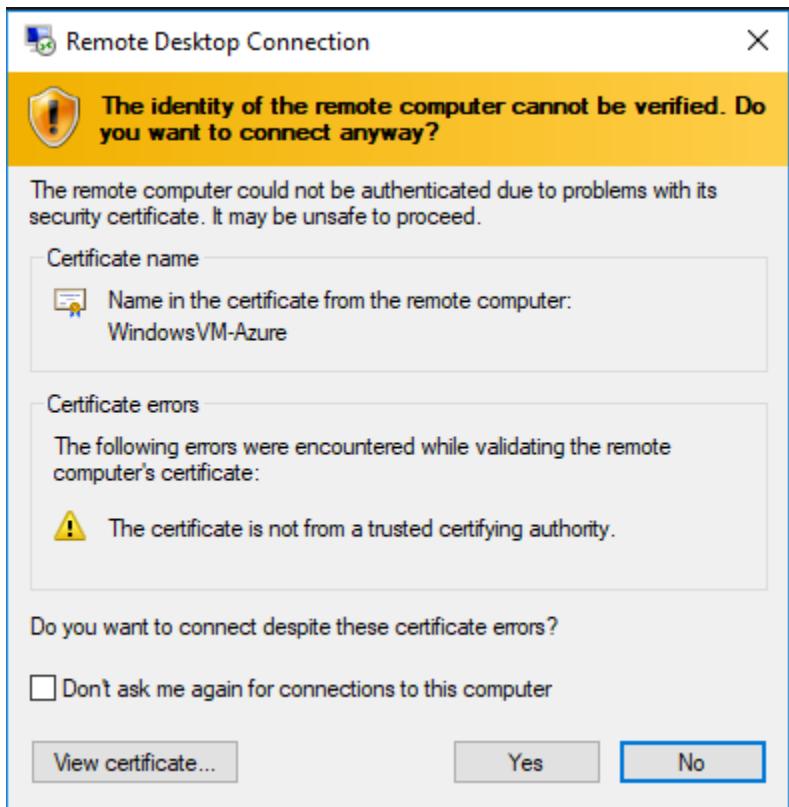
Click “**Connect**”.

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

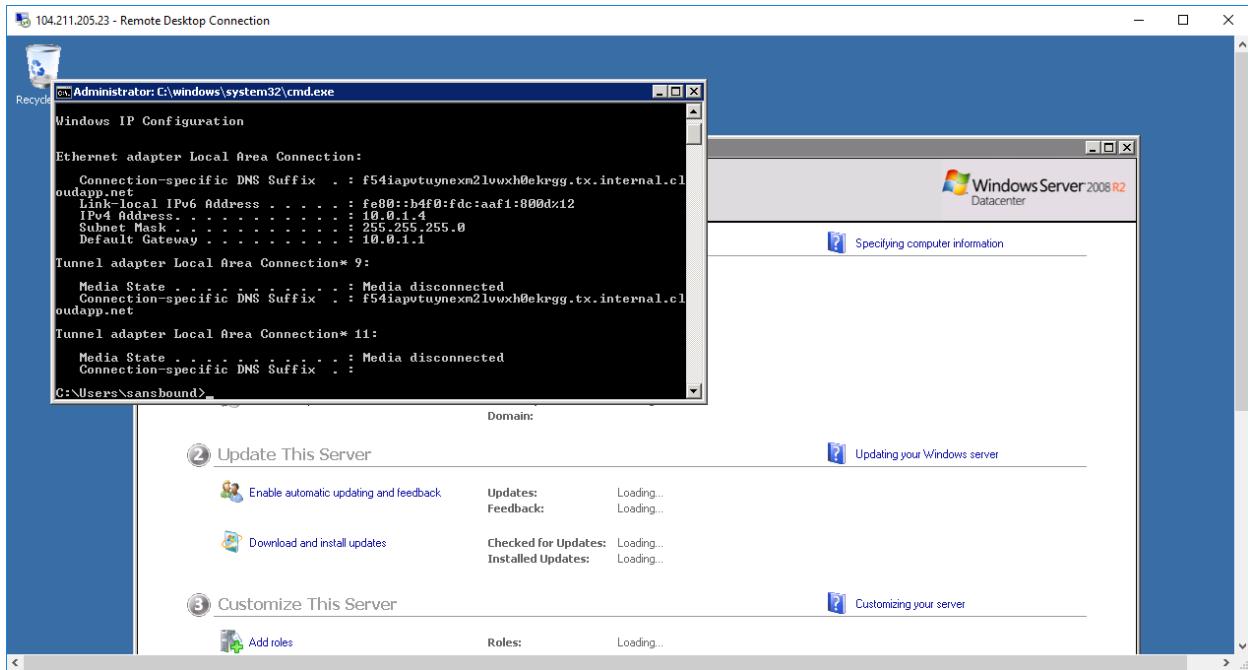
Click “Ok”.



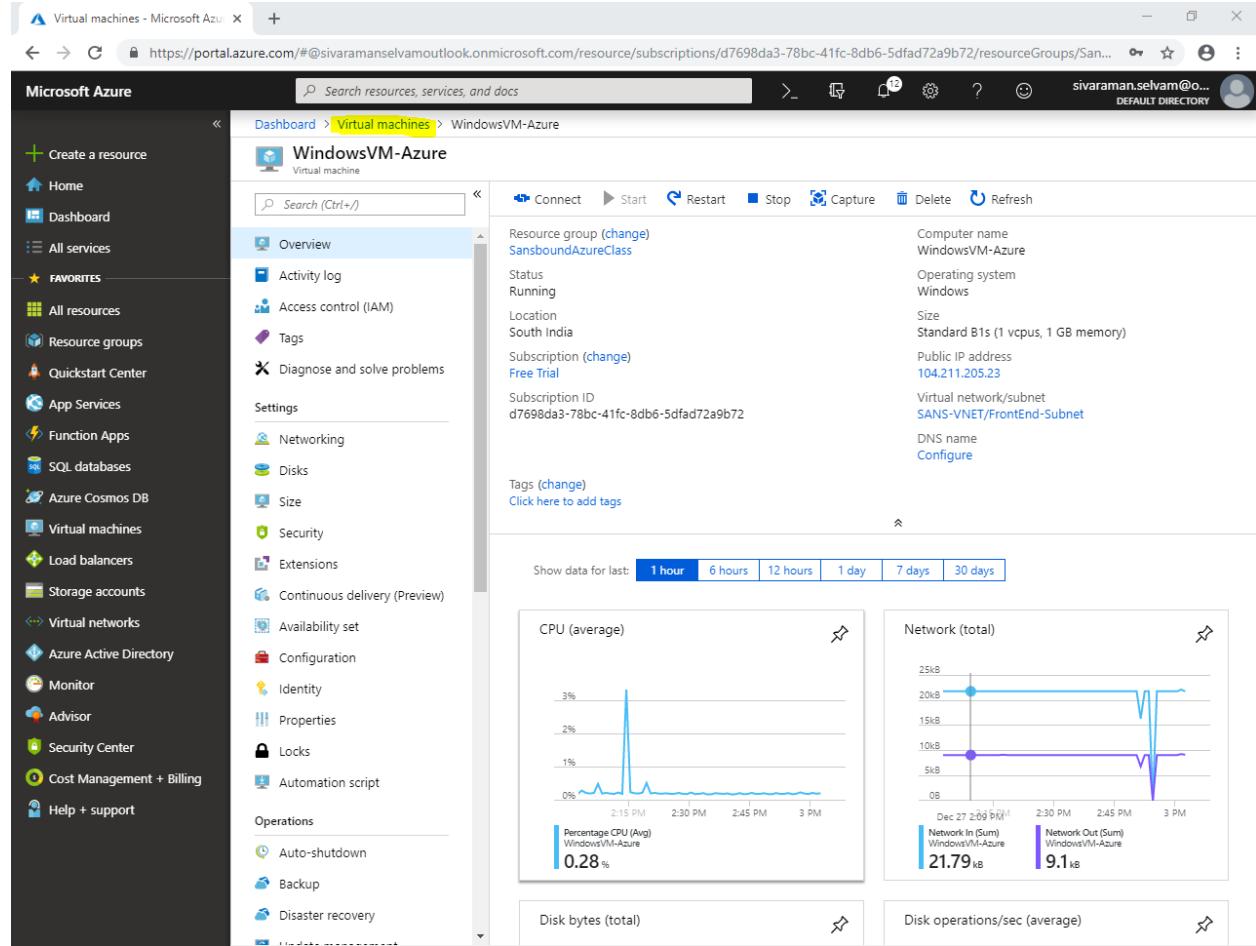
Click "Yes".



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



Click on “Virtual machines” in top.



The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation bar is visible, showing various service categories like Home, Dashboard, All services, Favorites, and Virtual machines, which is highlighted in yellow. The main content area displays the details for a specific virtual machine named "WindowsVM-Azure".

Virtual machine Overview:

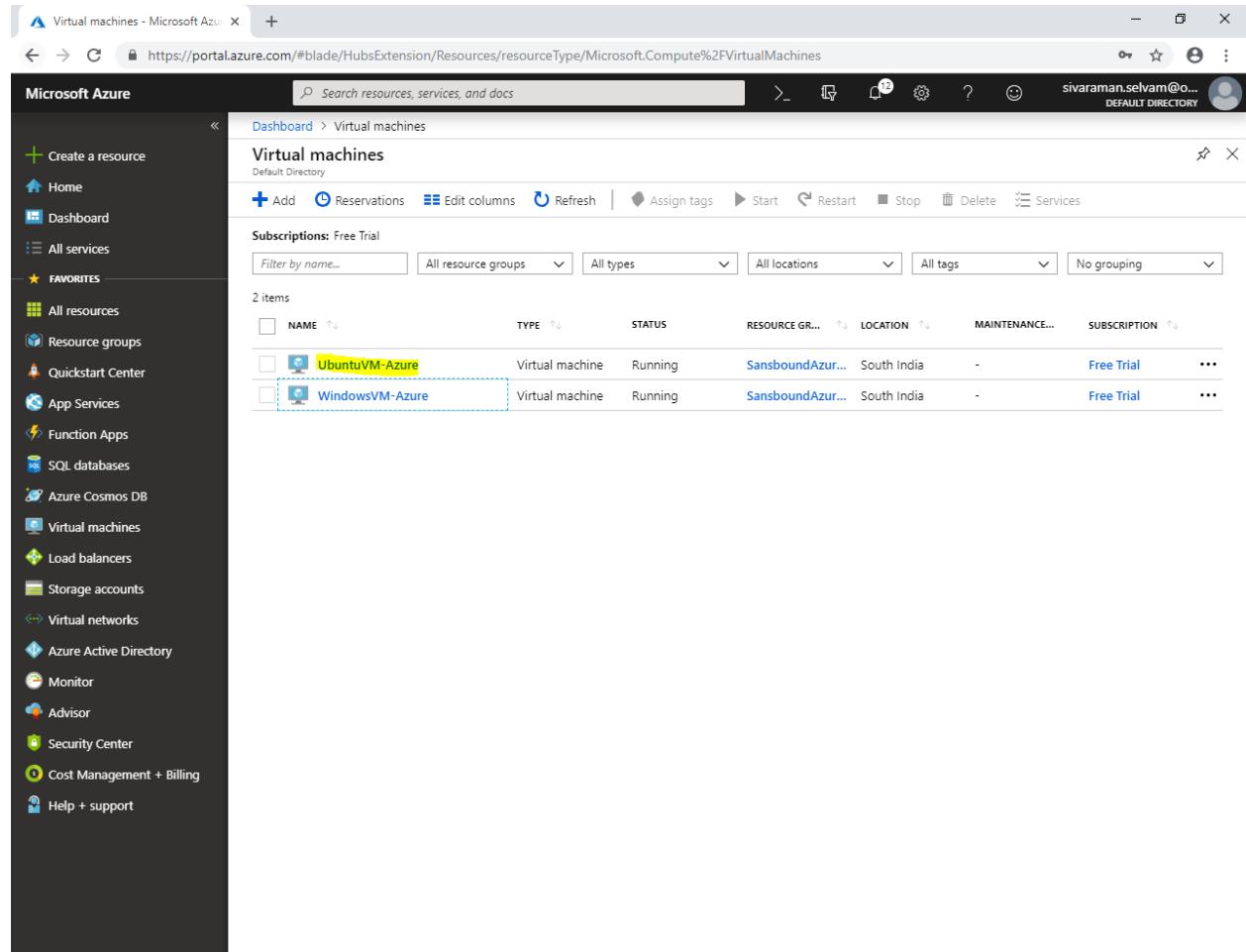
- Resource group: SansboundAzureClass
- Status: Running
- Location: South India
- Subscription: Free Trial
- Subscription ID: d7698da3-78bc-41fc-8db6-5dfad72a9b72
- Computer name: WindowsVM-Azure
- Operating system: Windows
- Size: Standard B1s (1 vcpus, 1 GB memory)
- Public IP address: 104.211.205.23
- Virtual network/subnet: SANS-VNET/FrontEnd-Subnet
- DNS name: Configure

Tags: Click here to add tags

Metrics:

- CPU (average): Percentage CPU Avg: 0.28 %
- Network (total): Network In (Sum) 21.79 kB, Network Out (Sum) 9.1 kB
- Disk bytes (total)
- Disk operations/sec (average)

Click on “UbuntuVM-Azure” virtual machine.

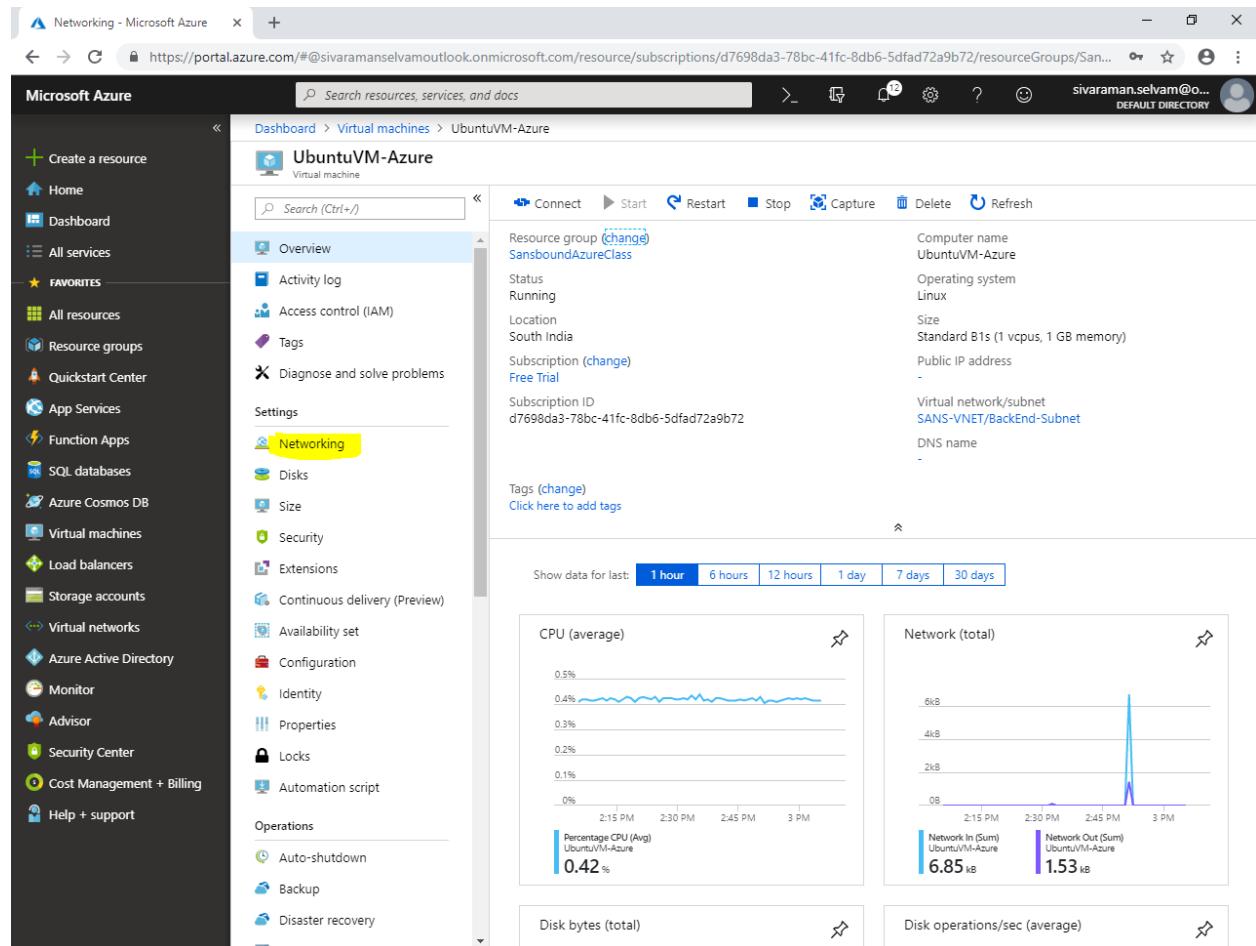


The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, and Favorites. Under Favorites, the Virtual machines option is selected. The main content area is titled "Virtual machines" and shows a list of resources. The list includes columns for NAME, TYPE, STATUS, RESOURCE GRP..., LOCATION, MAINTENANCE..., and SUBSCRIPTION. There are two items listed:

NAME	TYPE	STATUS	RESOURCE GRP...	LOCATION	MAINTENANCE...	SUBSCRIPTION
UbuntuVM-Azure	Virtual machine	Running	SansboundAzur...	South India	-	Free Trial
WindowsVM-Azure	Virtual machine	Running	SansboundAzur...	South India	-	Free Trial

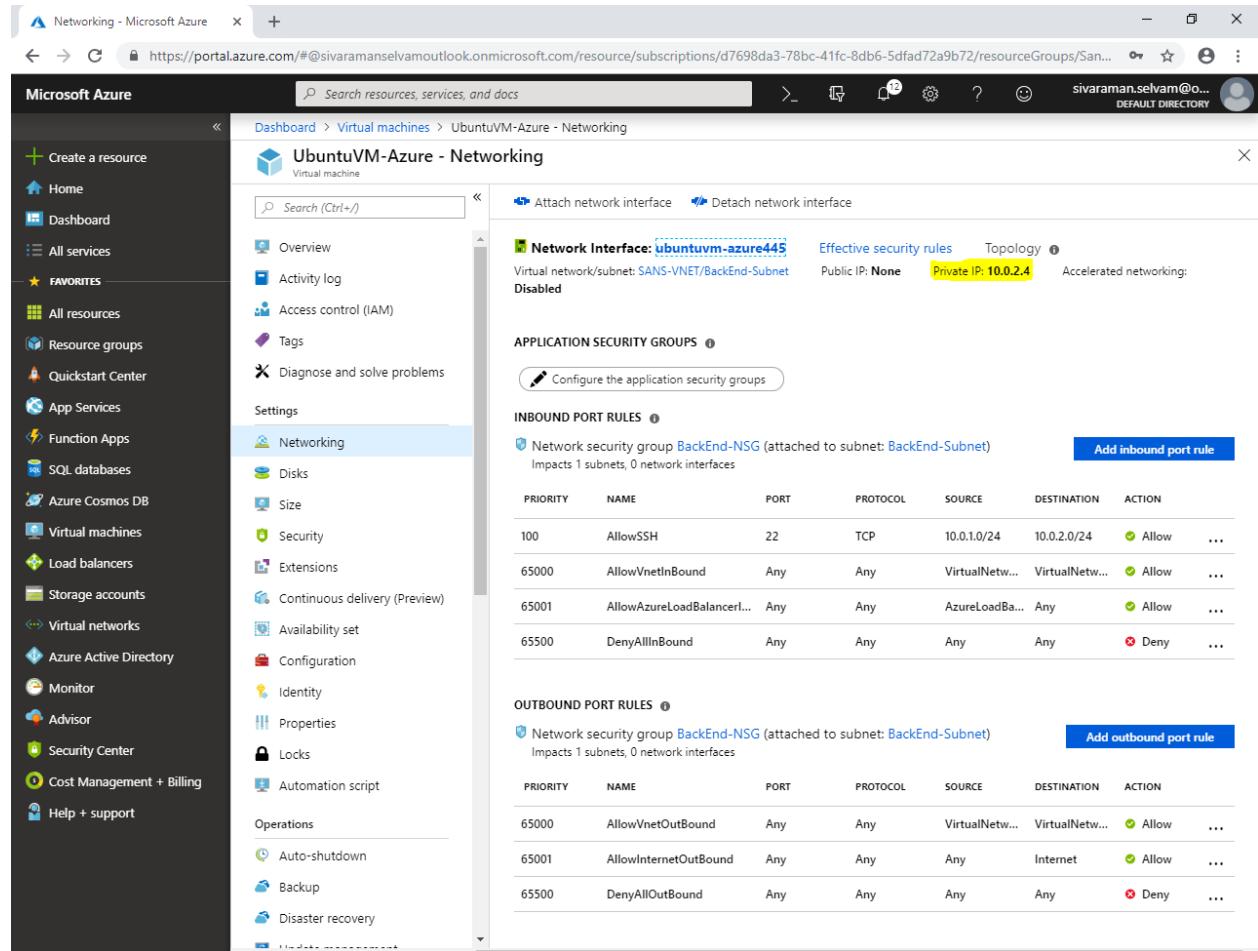
In “UbuntuVM-Azure”.

Click on “Networking”.



The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu is visible with various service icons. In the center, the details for a virtual machine named "UbuntuVM-Azure" are displayed under the "Virtual machines" section. The "Networking" tab is highlighted with a yellow box. Below the tabs, there are several sections: "Overview", "Activity log", "Access control (IAM)", "Tags", "Diagnose and solve problems", "Settings", "Networking" (which is active), "Disks", "Size", "Security", "Extensions", "Continuous delivery (Preview)", "Availability set", "Configuration", "Identity", "Properties", "Locks", and "Automation script". To the right of these settings, detailed information about the VM is shown, including its resource group ("SansboundAzureClass"), status ("Running"), location ("South India"), subscription ("Free Trial"), and public IP address. Below this, there are sections for "Tags" and "Metrics". At the bottom, four performance charts are displayed: "CPU (average)", "Network (total)", "Disk bytes (total)", and "Disk operations/sec (average)". The "Networking" chart shows a sharp spike in network traffic around 2:45 PM.

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



The screenshot shows the Microsoft Azure portal interface. The left sidebar is the navigation menu, and the main area is the networking configuration for a virtual machine named "UbuntuVM-Azure - Networking".

Network Interface: **ubuntuvm-azure445** (highlighted in yellow)

- Virtual network/subnet: SANS-VNET/BackEnd-Subnet
- Public IP: None
- Private IP: **10.0.2.4** (highlighted in yellow)
- Topology: Disabled

APPLICATION SECURITY GROUPS

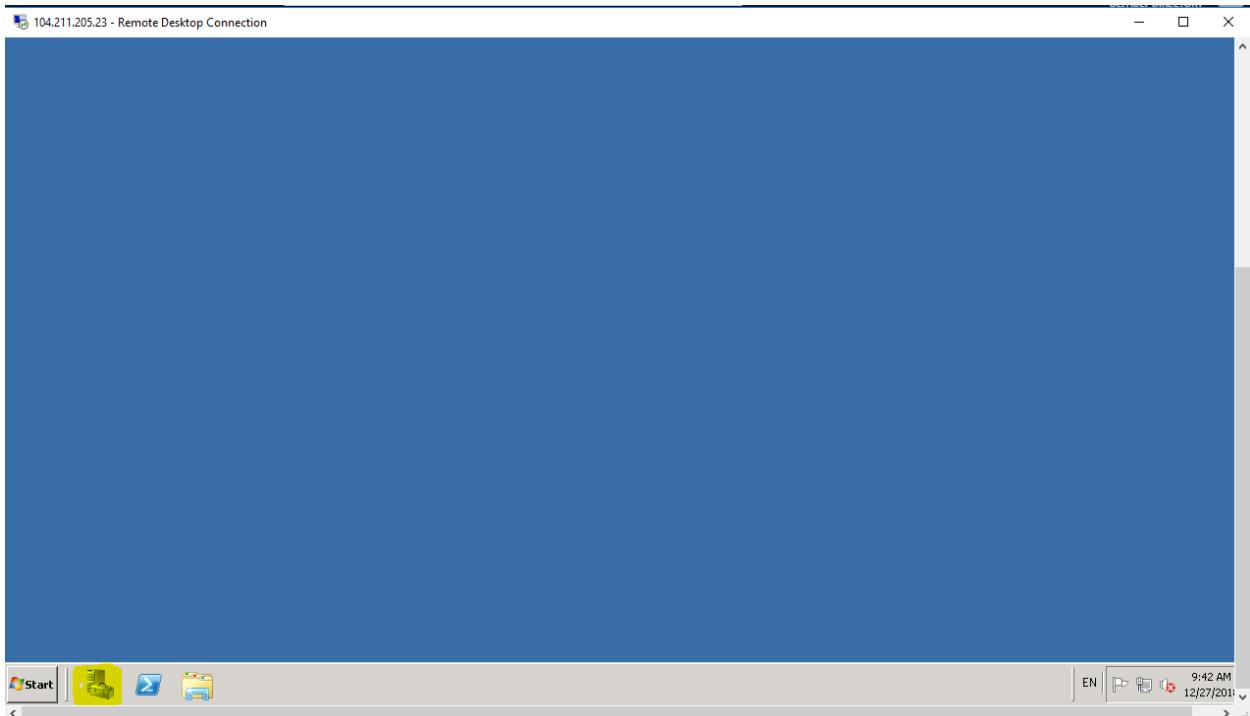
INBOUND PORT RULES

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	AllowSSH	22	TCP	10.0.1.0/24	10.0.2.0/24	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetw...	VirtualNetw...	Allow
65001	AllowAzureLoadBalancer...	Any	Any	AzureLoadBa...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

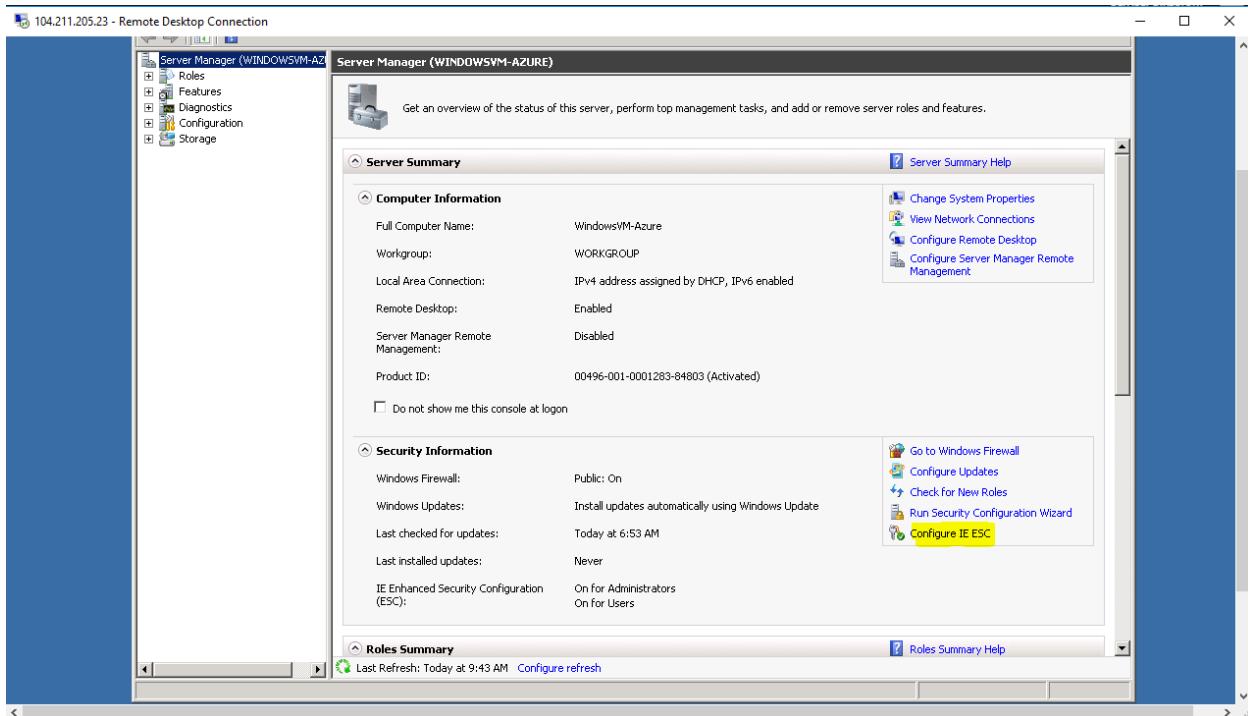
OUTBOUND PORT RULES

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetOutBound	Any	Any	VirtualNetw...	VirtualNetw...	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

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

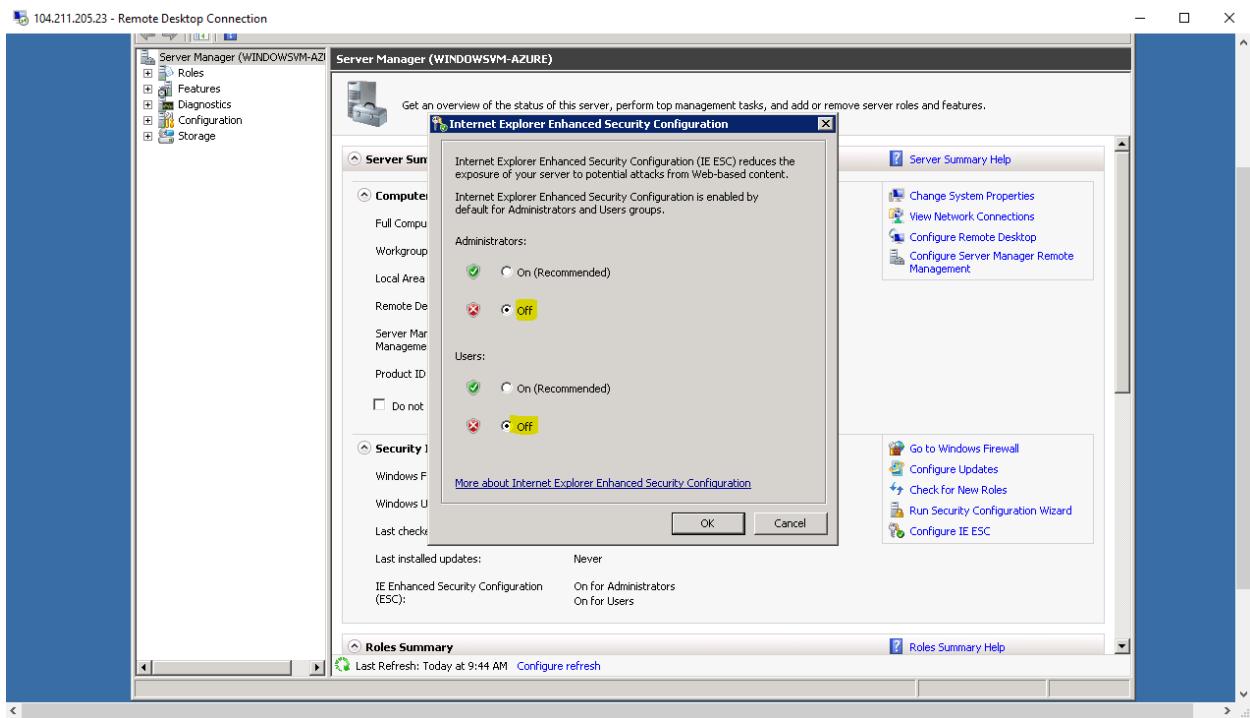


In “Server manager”, click “Configure IE ESC”.



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

Click “**Ok**”.

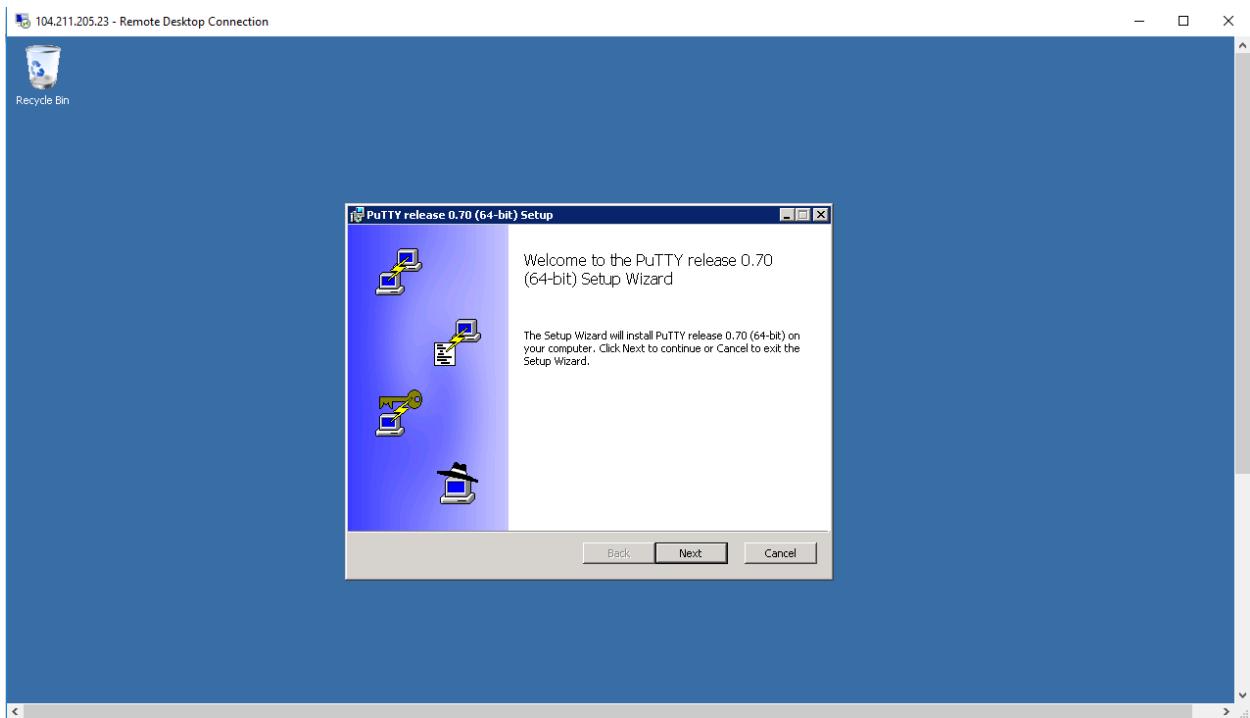


In “Windows Server 2008 R2”,

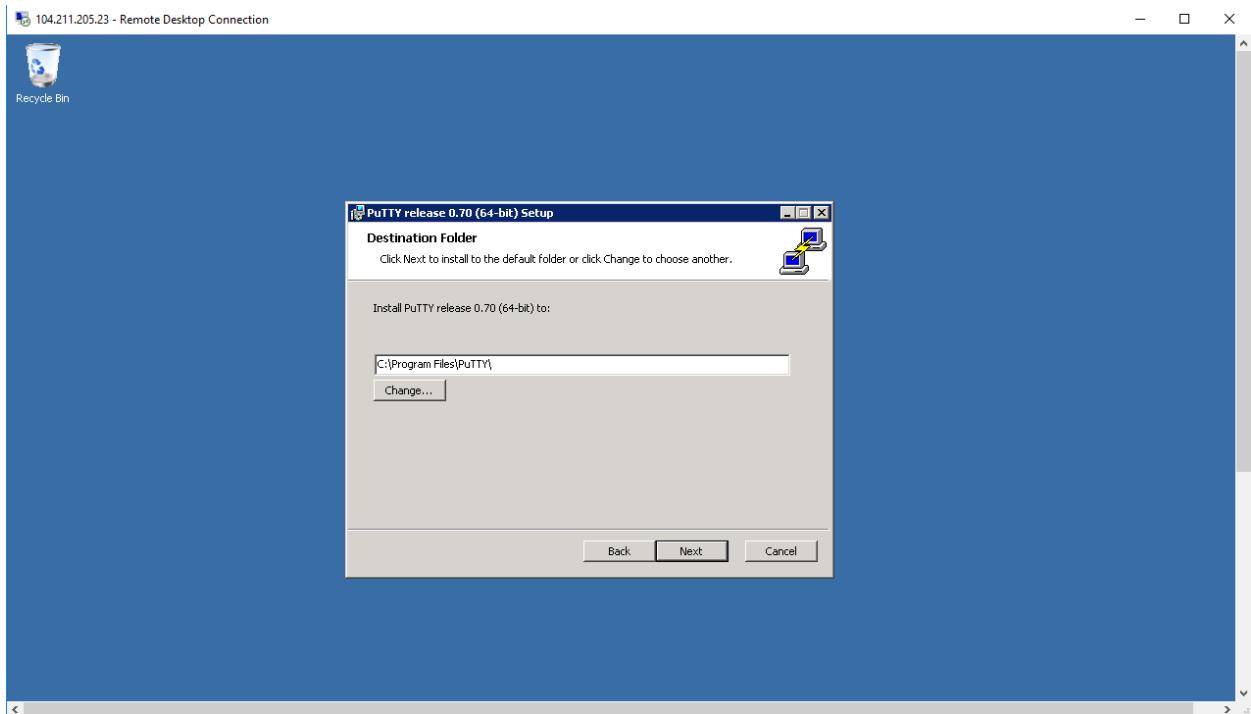
You have required to download “[Putty.exe](#)” for access the Ubuntu through SSH.

Run the putty setup.

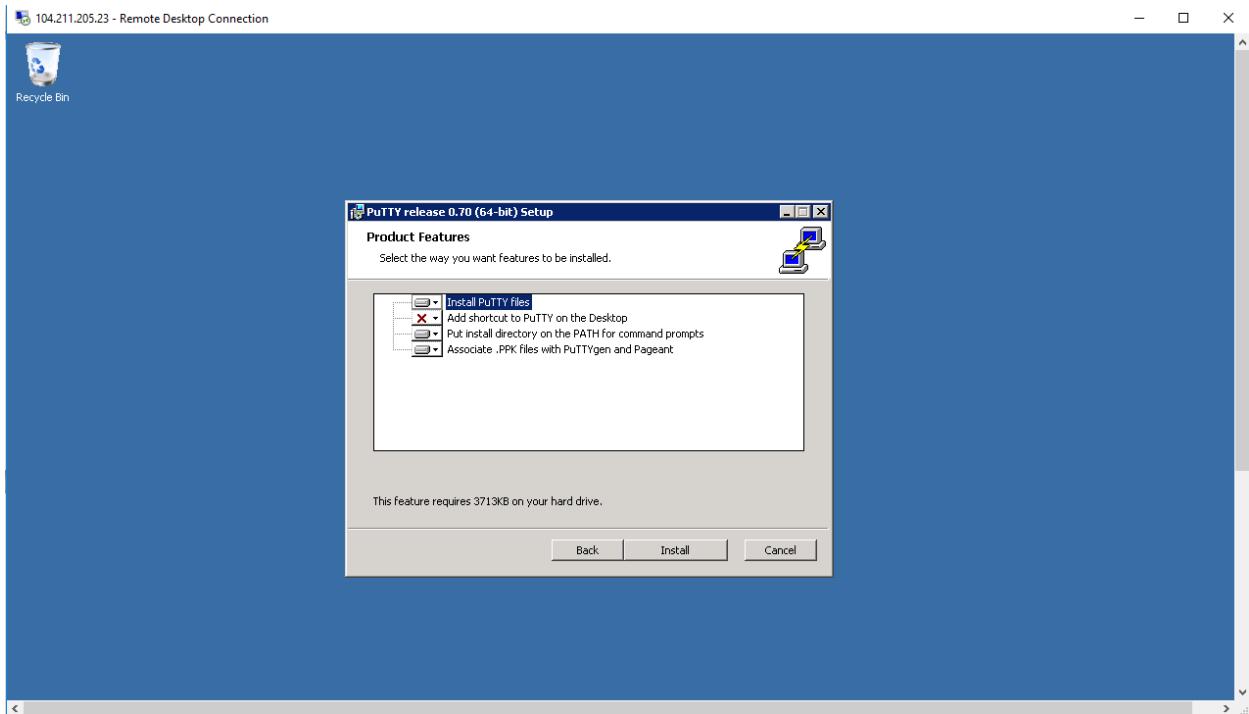
Click “Next” to continue.



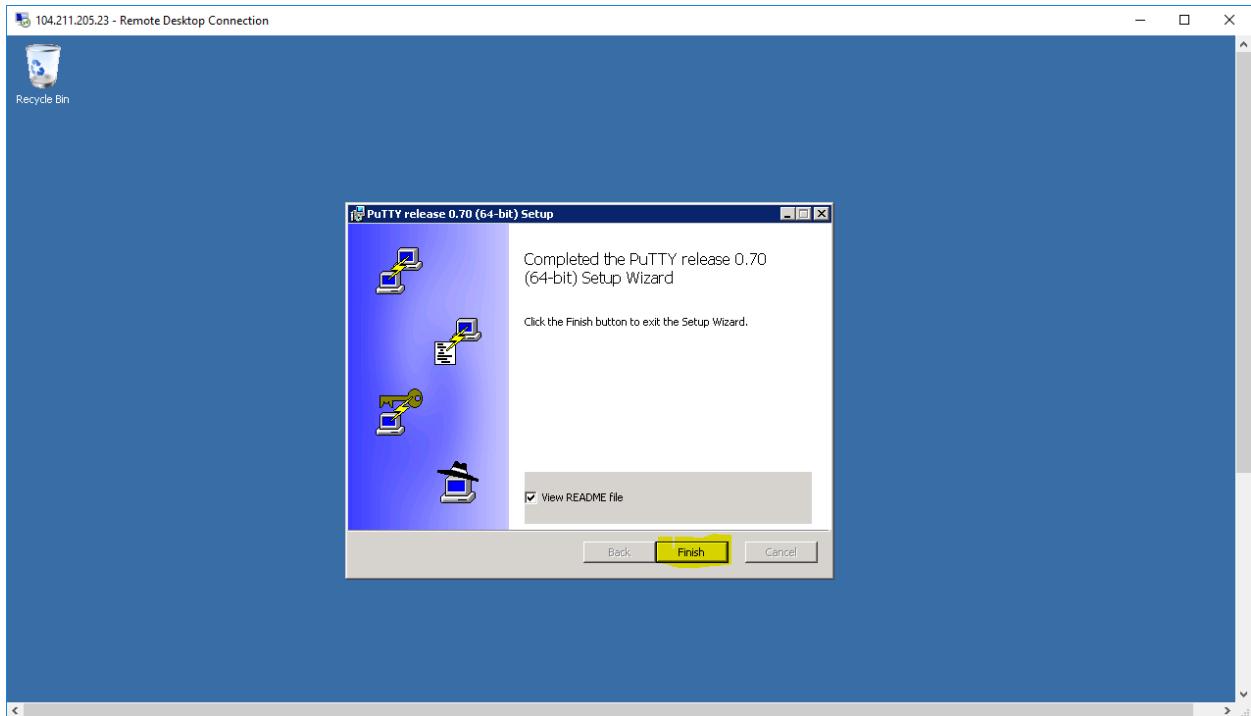
Click “Next”.



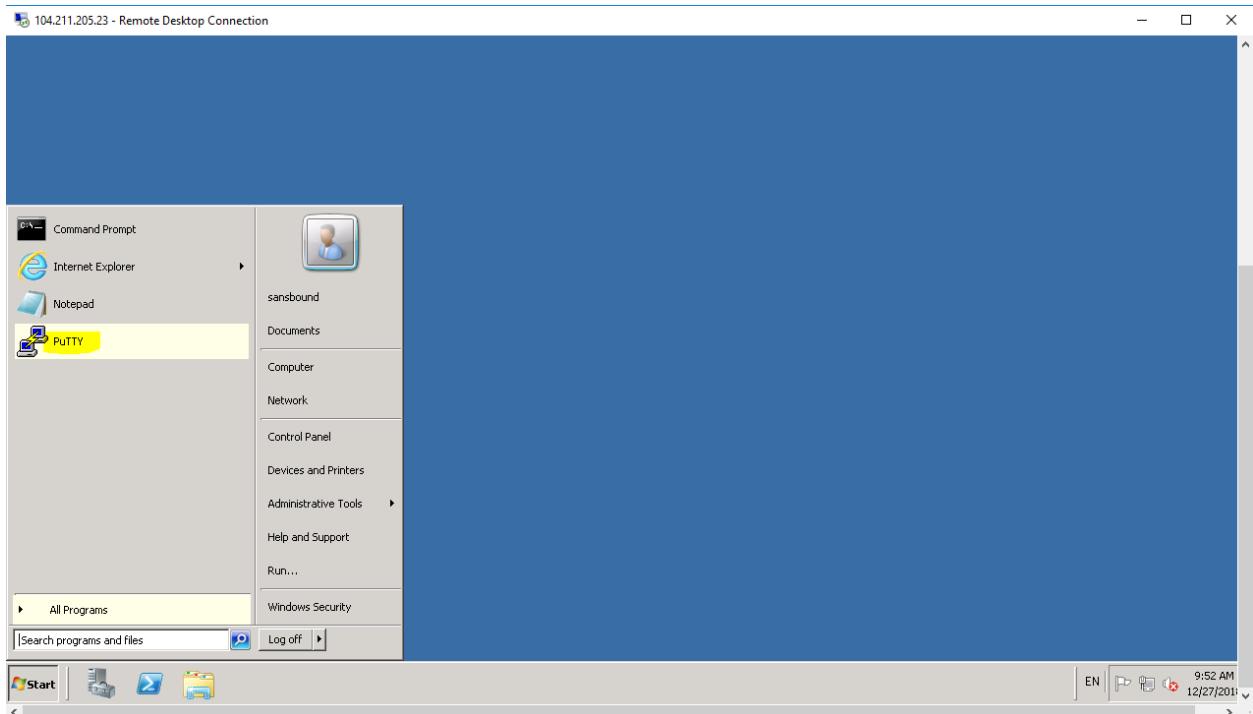
Click “Install”.



Click “**Finish**”.

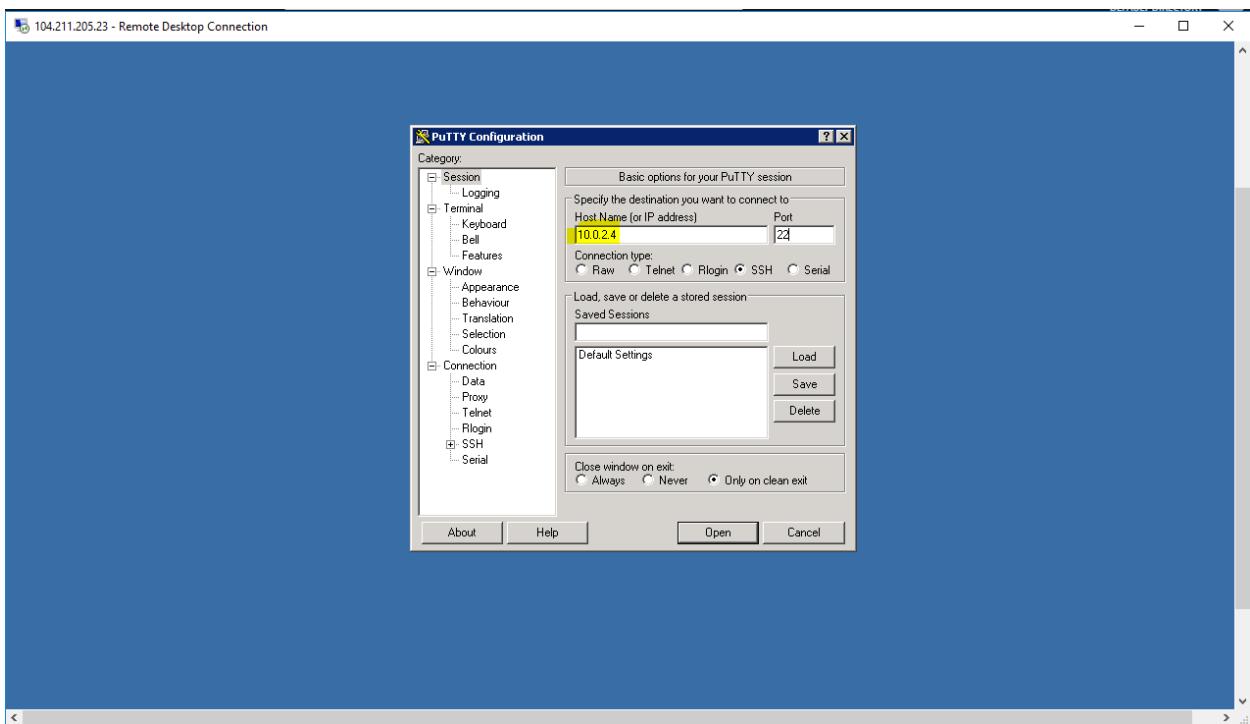


In “Start” you are able to see the “**putty.exe**” click it.

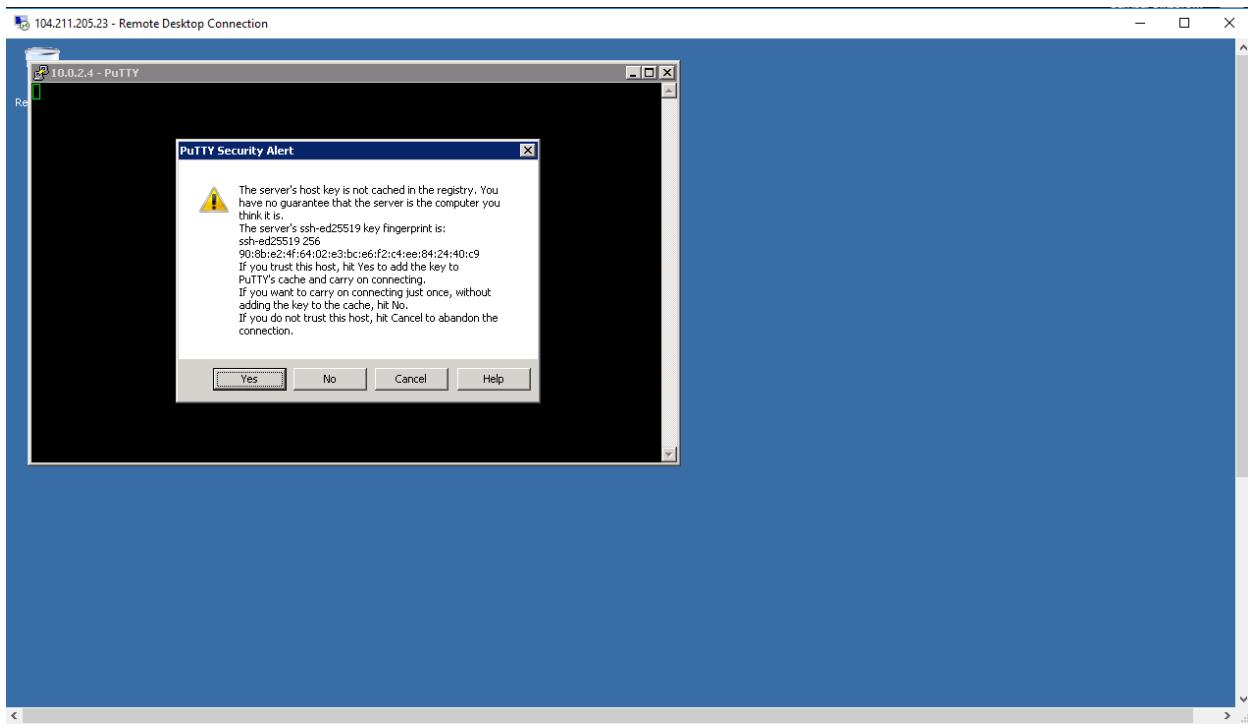


In Putty, Private IP address of as “**10.0.2.4**” Ubuntu Server which belongs to BackEnd-Subnet (10.0.2.0/24).

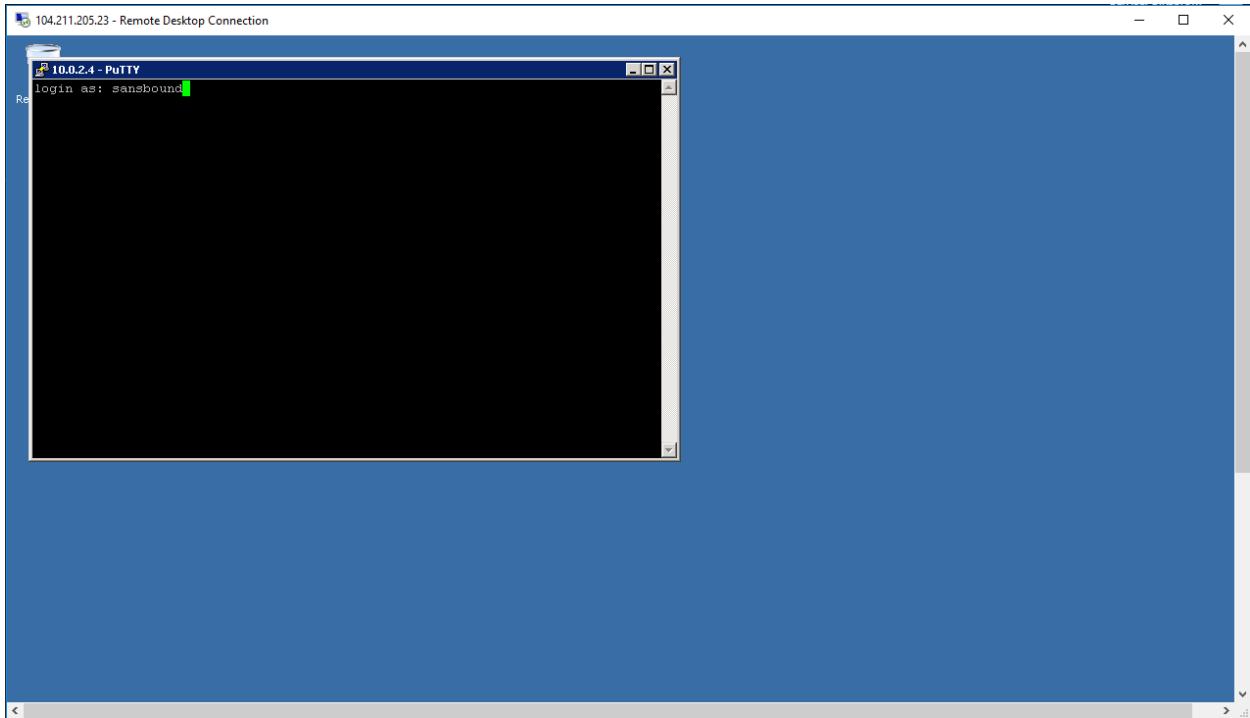
Click “**Open**” to connect to Ubuntu.



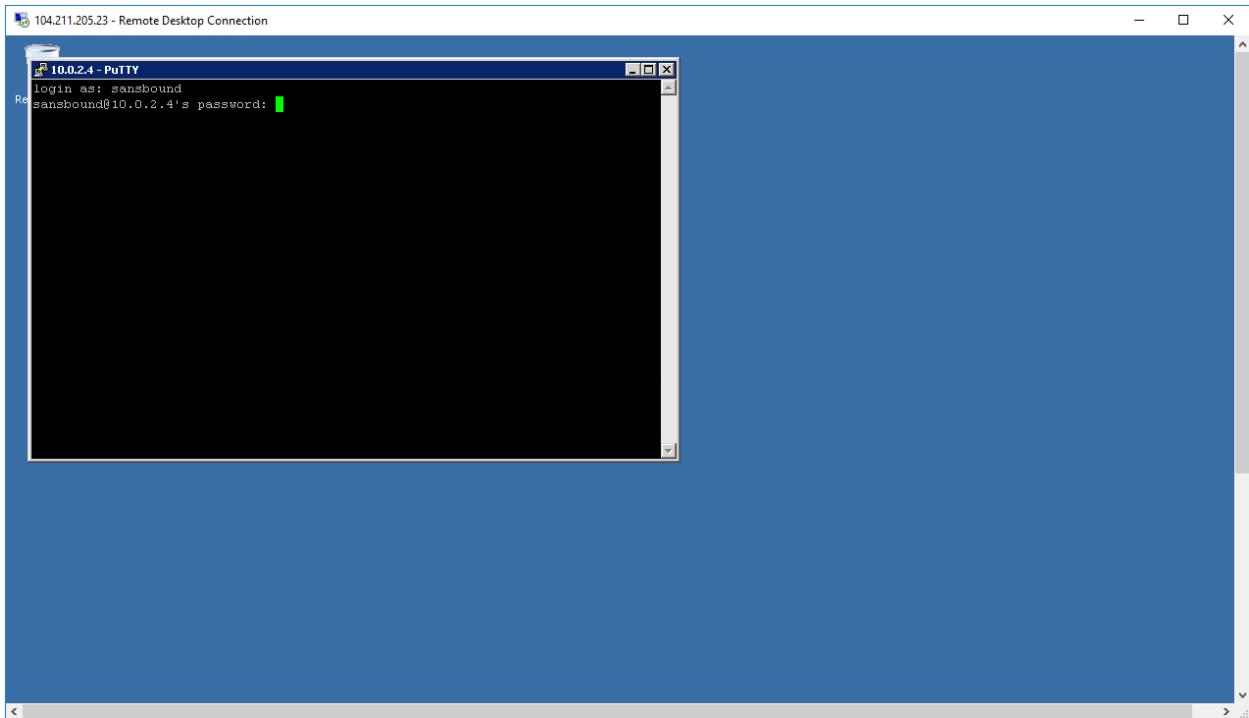
Click "Yes".



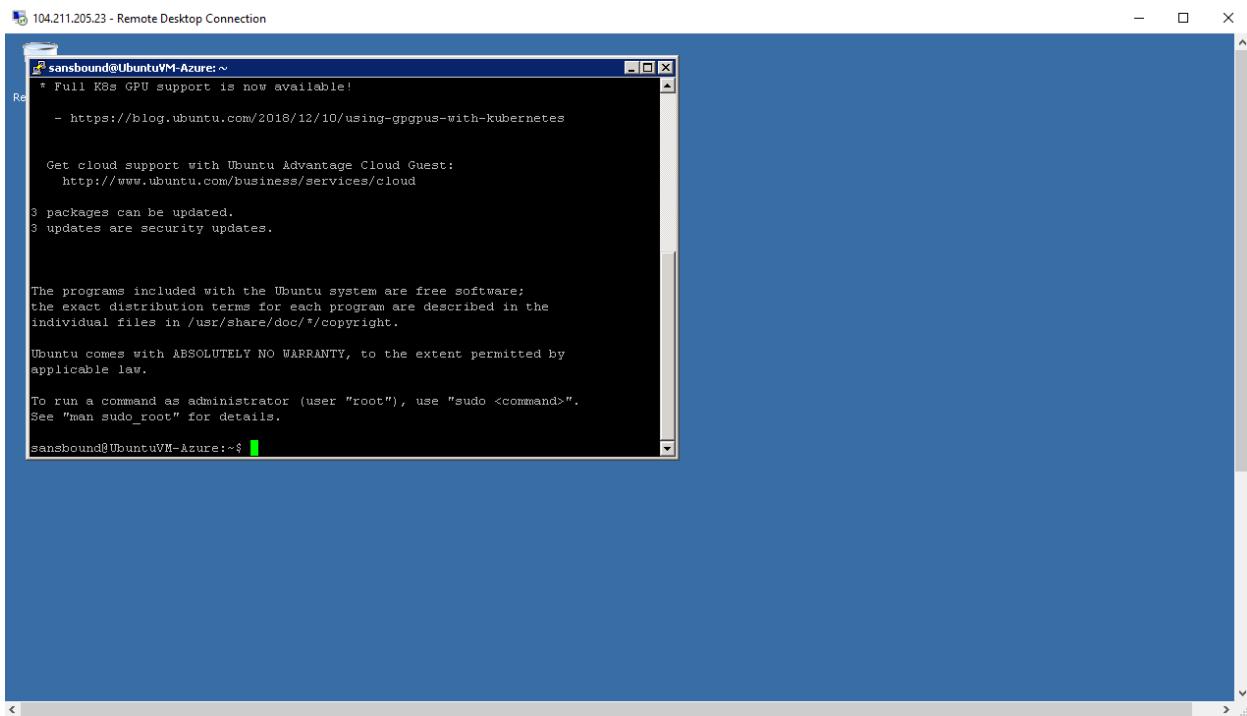
Type username of Ubuntu server as “**sansbound**”and press “**Enter**”.



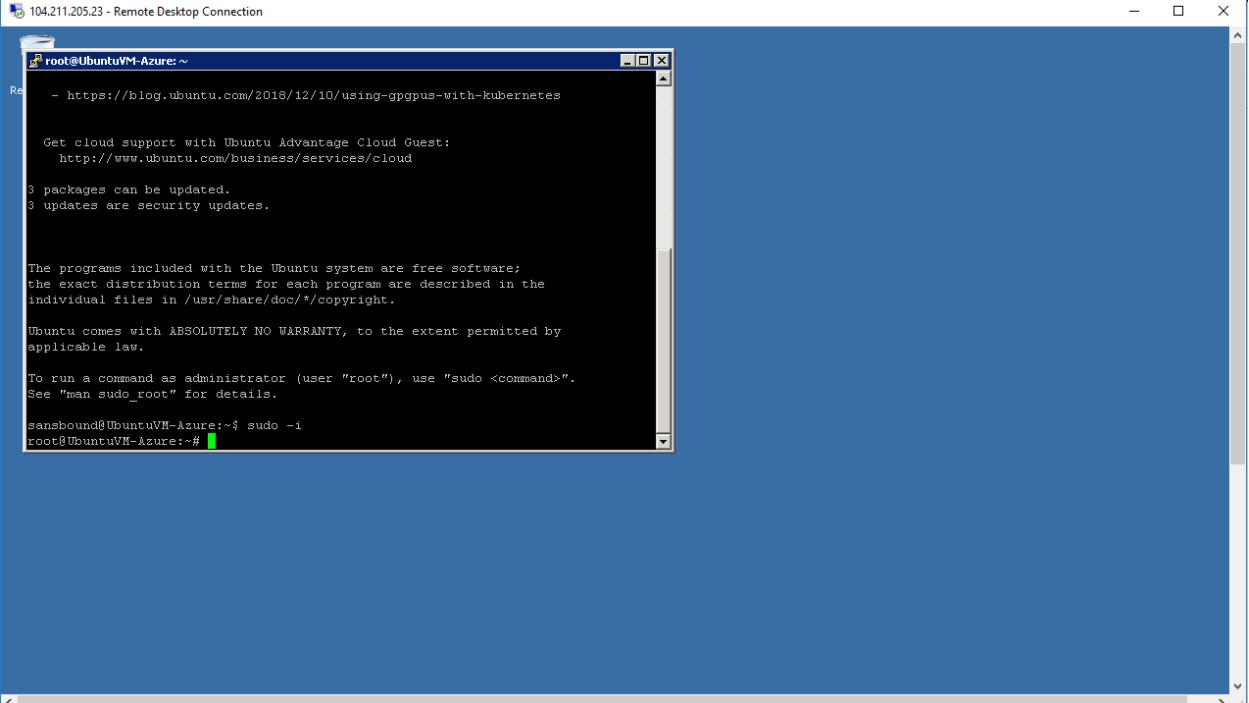
And type password for Ubuntu server and press “Enter”.



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.



```
104.211.205.23 - Remote Desktop Connection

root@UbuntuVM-Azure: ~
Re
- https://blog.ubuntu.com/2018/12/10/using-gpgpus-with-kubernetes

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

3 packages can be updated.
3 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

sansbound@UbuntuVM-Azure:~$ sudo -i
root@UbuntuVM-Azure:~#
```

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