

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.

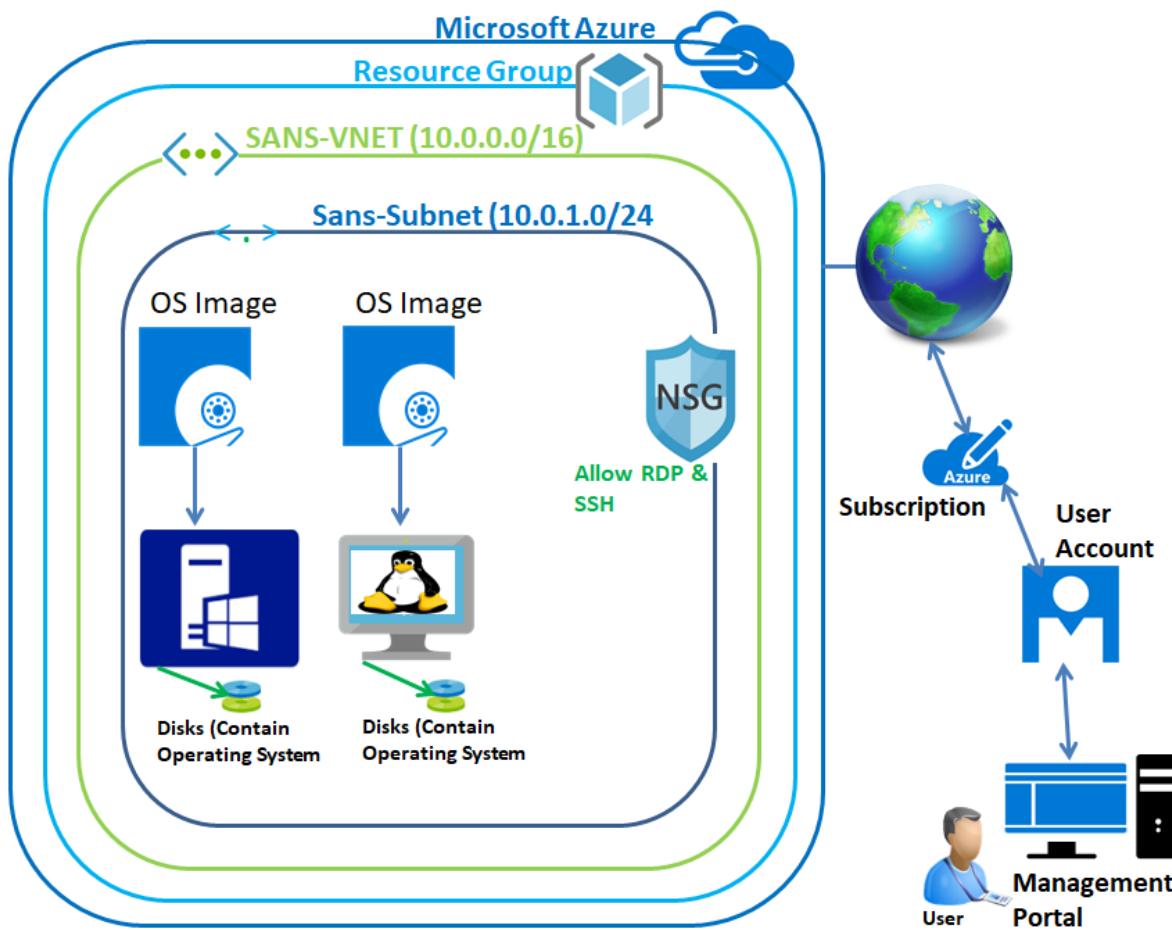
Port range

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.

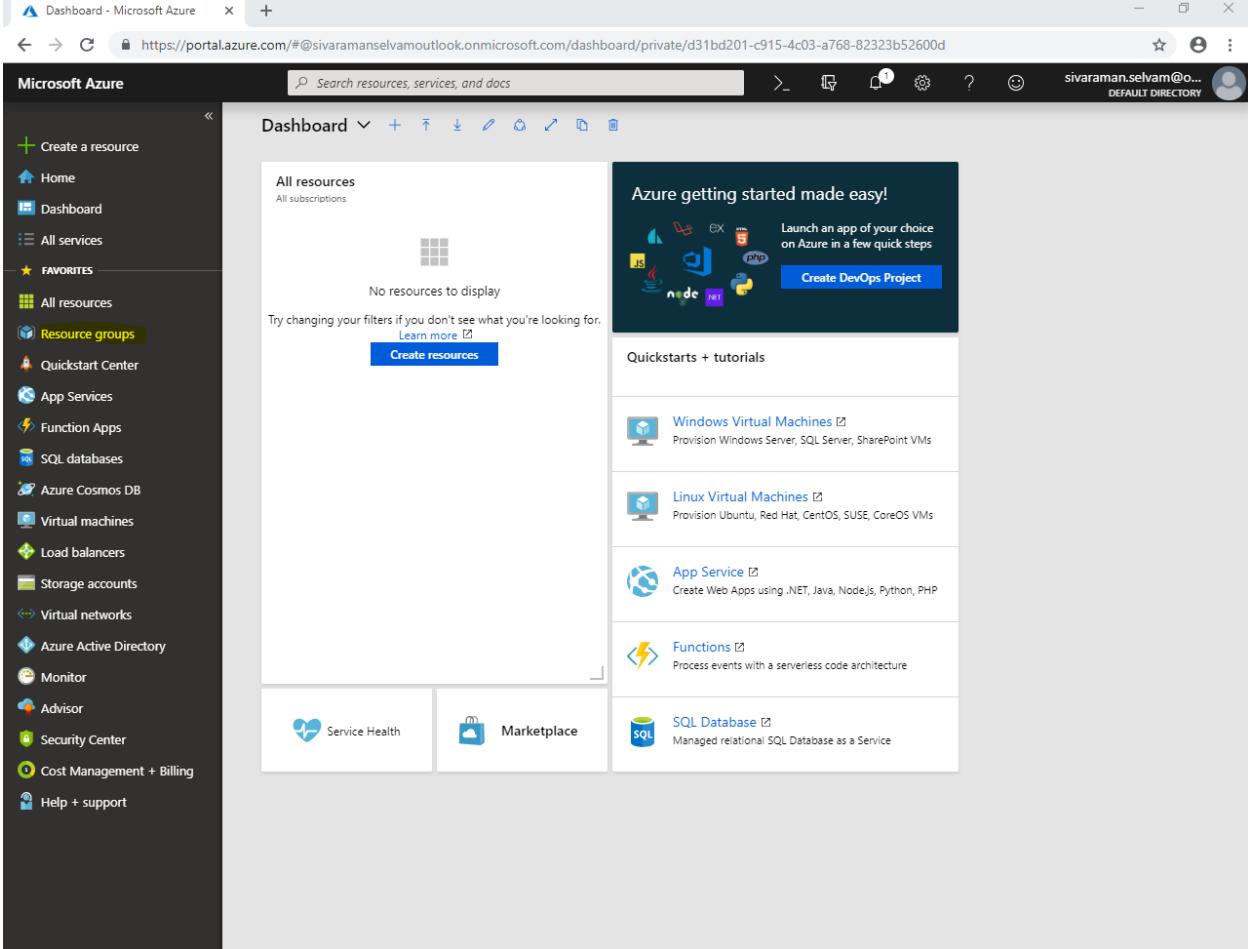
Action

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.

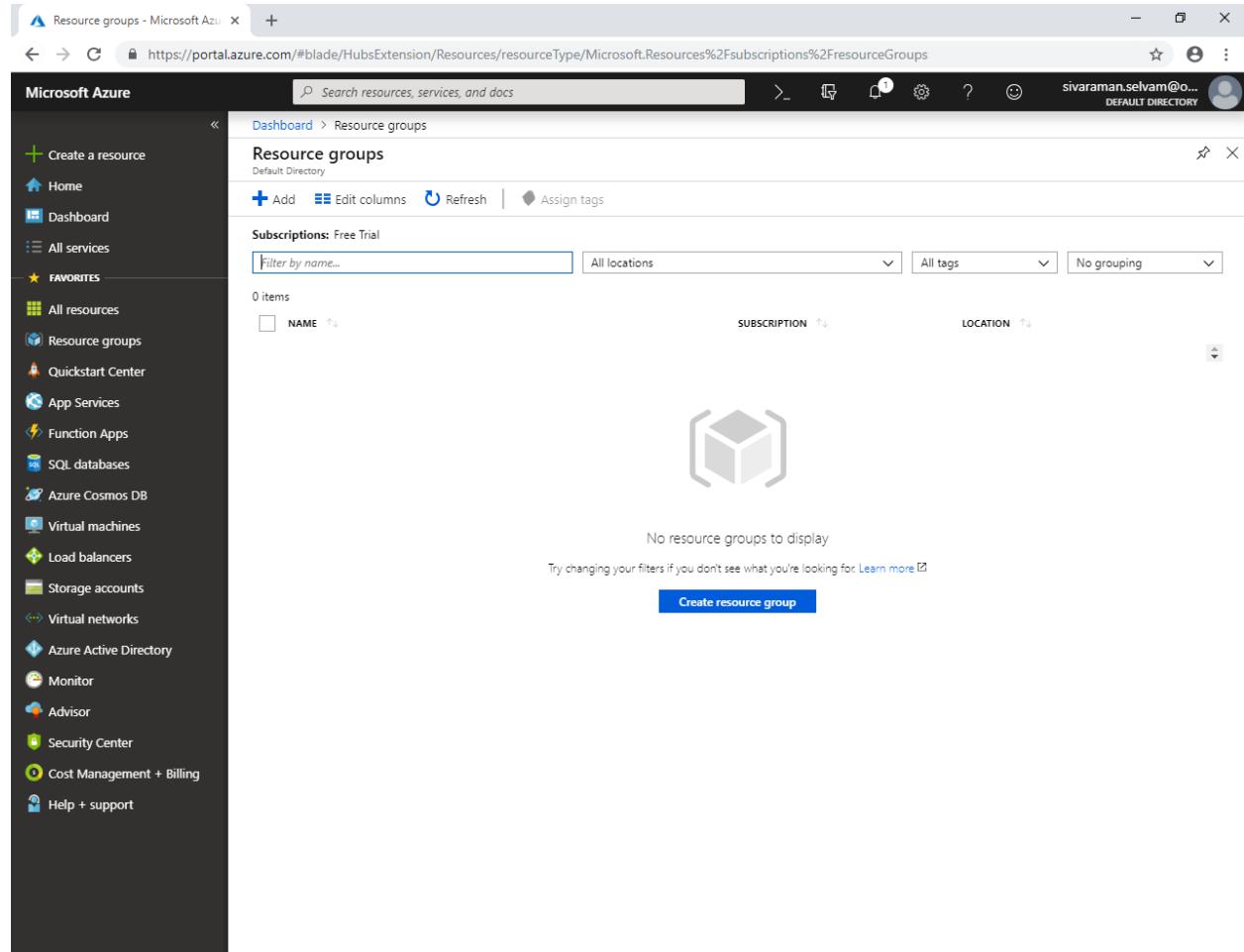
Topology:

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



The screenshot shows the Microsoft Azure portal dashboard. On the left, a dark sidebar lists various services under 'FAVORITES'. The 'Resource groups' option is highlighted with a yellow background. The main content area displays a 'Dashboard' view with a central message: 'No resources to display' and a 'Create resources' button. To the right, there's a 'Quickstarts + tutorials' section with links to 'Windows Virtual Machines', 'Linux Virtual Machines', 'App Service', 'Functions', and 'SQL Database'. At the bottom of the dashboard, there are 'Service Health' and 'Marketplace' buttons.

In “Resource Groups” click “Add”.



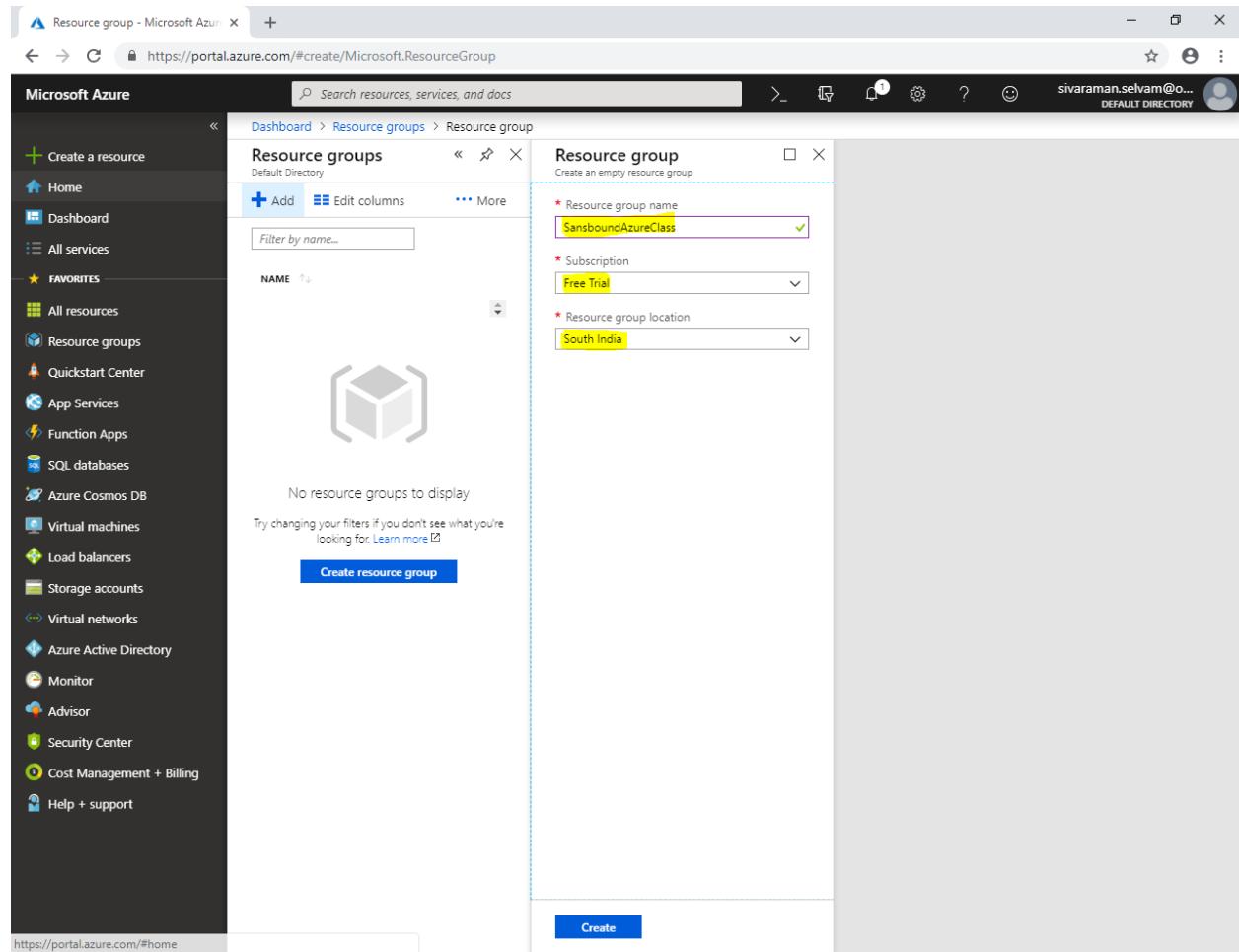
The screenshot shows the Microsoft Azure portal interface. The left sidebar is dark-themed and includes a 'FAVORITES' section with links to various services like All resources, Resource groups, App Services, and Help + support. The main content area is titled 'Resource groups' under 'Dashboard > Resource groups'. It shows a message 'No resource groups to display' with a note to 'Try changing your filters if you don't see what you're looking for.' A blue 'Create resource group' button is prominently displayed at the bottom. The top navigation bar shows the URL <https://portal.azure.com/#blade/HubsExtension/Resources/resourceType/Microsoft.Resources%2Fsubscriptions%2FresourceGroups>.

While creating “Resource Group”

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

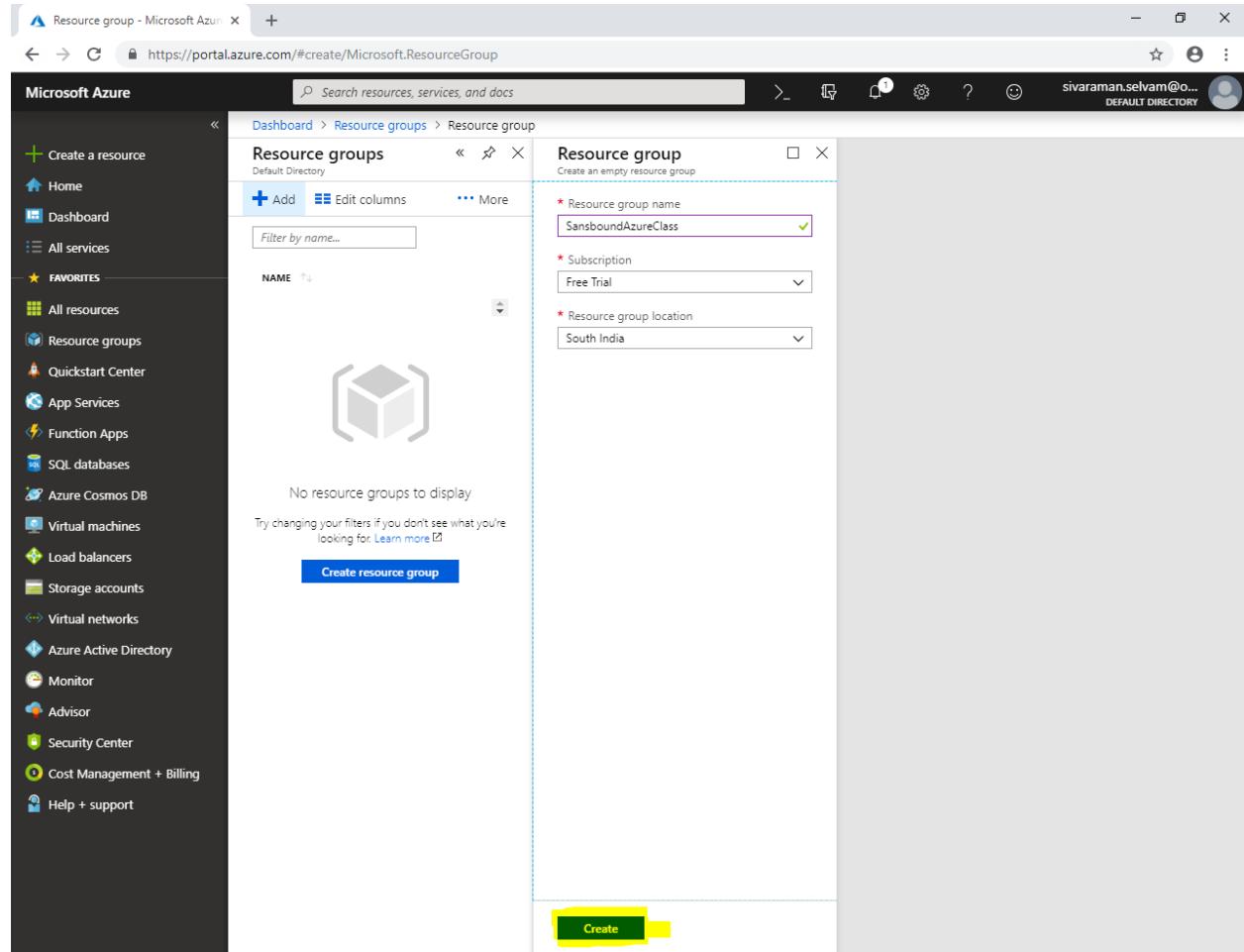
“Subscription” as “**Free Trial**”.

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



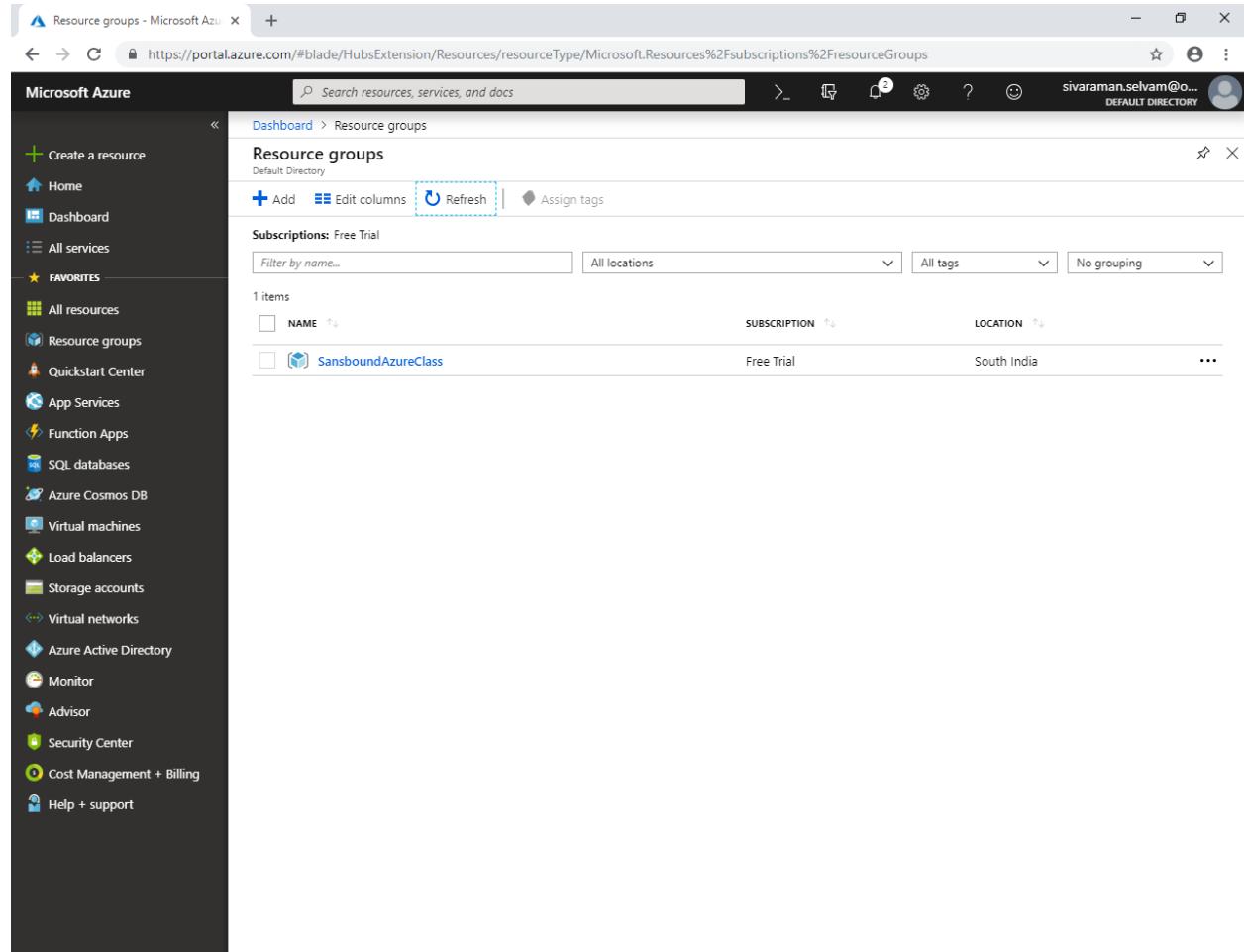
The screenshot shows the Microsoft Azure portal interface for creating a new resource group. On the left, there's a sidebar with various service icons like Home, Dashboard, All services, Favorites, and many others. The main area has a title bar "Resource group - Microsoft Azure" and a URL "https://portal.azure.com/#create/Microsoft.ResourceGroup". Below the title bar, it says "Microsoft Azure" and "Dashboard > Resource groups > Resource group". The central part of the screen is titled "Resource group" with the sub-instruction "Create an empty resource group". It contains three fields: "Resource group name" (set to "SansboundAzureClass"), "Subscription" (set to "Free Trial"), and "Resource group location" (set to "South India"). At the bottom right of this panel is a large blue "Create" button. To the left of the main panel, there's a preview section showing a 3D cube icon and the message "No resource groups to display". A "Create resource group" button is also located in this preview area.

Click “Create” to create a new “Resource Group”



The screenshot shows the Microsoft Azure portal interface for creating a new Resource Group. The left sidebar contains various service links like Home, Dashboard, and Resource groups. The main area shows a list of Resource Groups with a single entry: "SansboundAzureClass". A modal window is open for creating a new group, with fields for Name (set to "SansboundAzureClass"), Subscription (set to "Free Trial"), and Resource group location (set to "South India"). At the bottom right of this modal, a green "Create" button is highlighted with a yellow box.

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

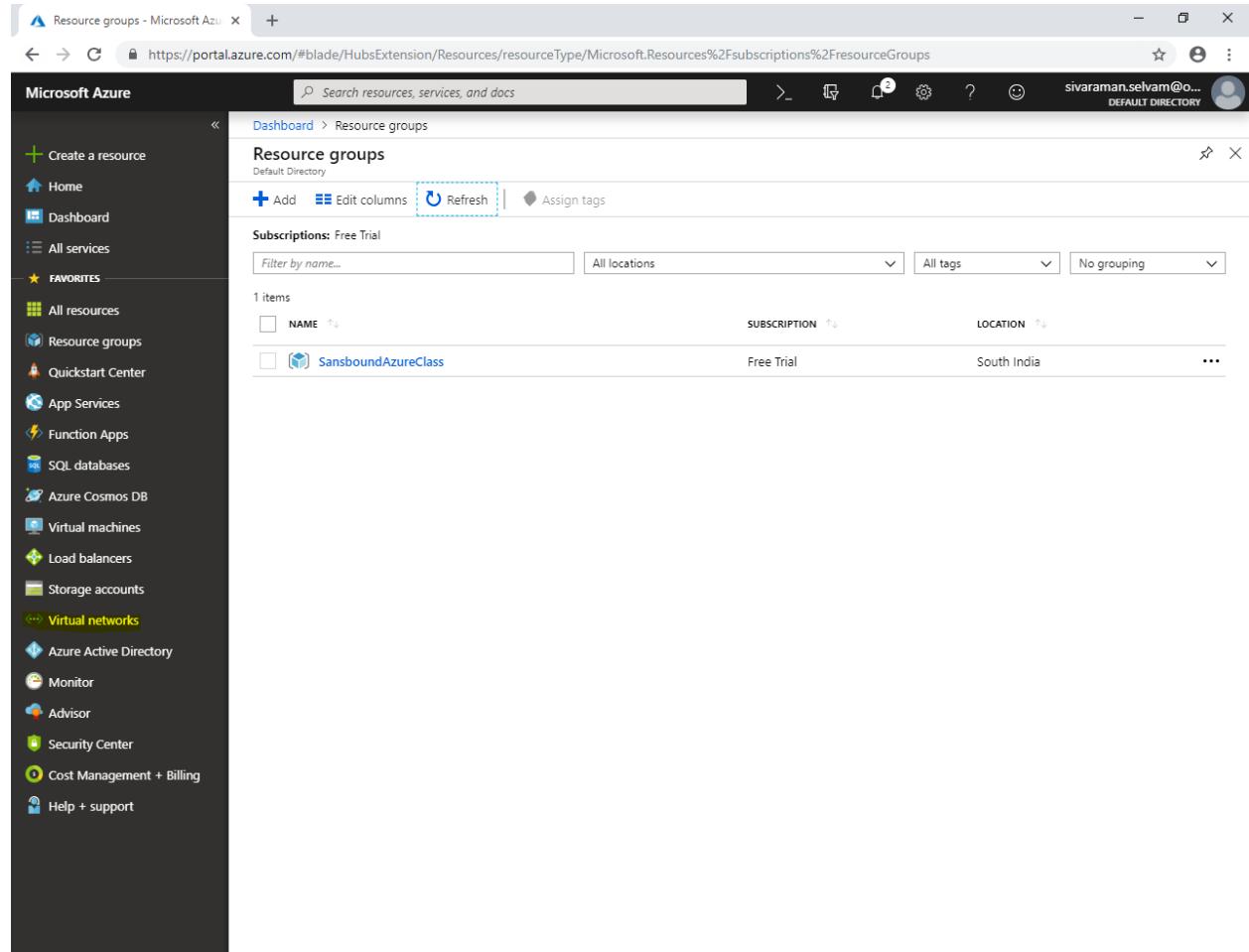


The screenshot shows the Microsoft Azure portal interface. The left sidebar is titled "Microsoft Azure" and includes a "FAVORITES" section with links to various services like Resource groups, App Services, and Virtual machines. The main content area is titled "Resource groups" and shows a table with one item:

NAME	SUBSCRIPTION	LOCATION
SansboundAzureClass	Free Trial	South India

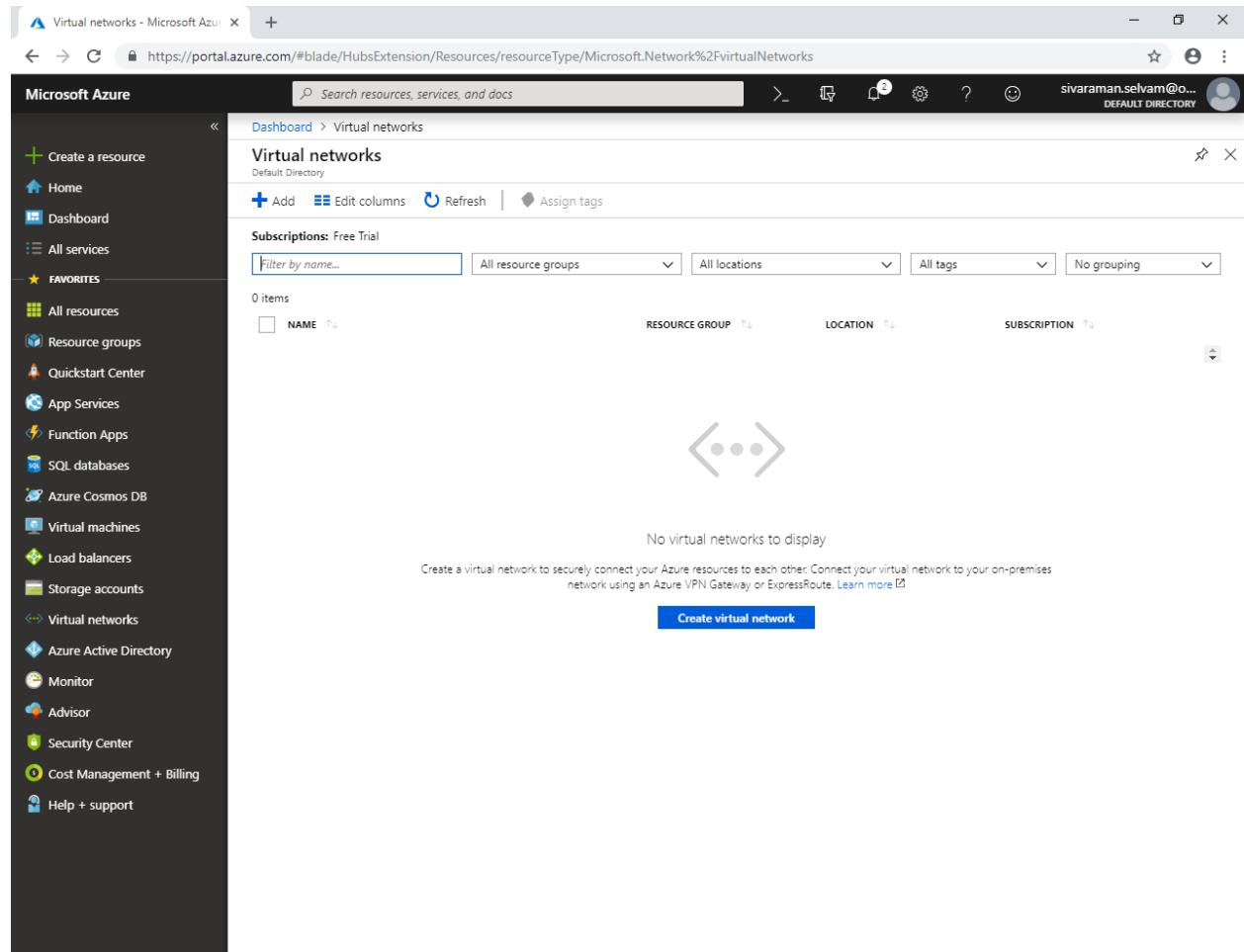
A blue dashed box highlights the "Refresh" button in the top navigation bar, which is located next to the "Edit columns" and "Assign tags" buttons.

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



NAME	SUBSCRIPTION	LOCATION
SansboundAzureClass	Free Trial	South India

In “Virtual networks” click “Add”.



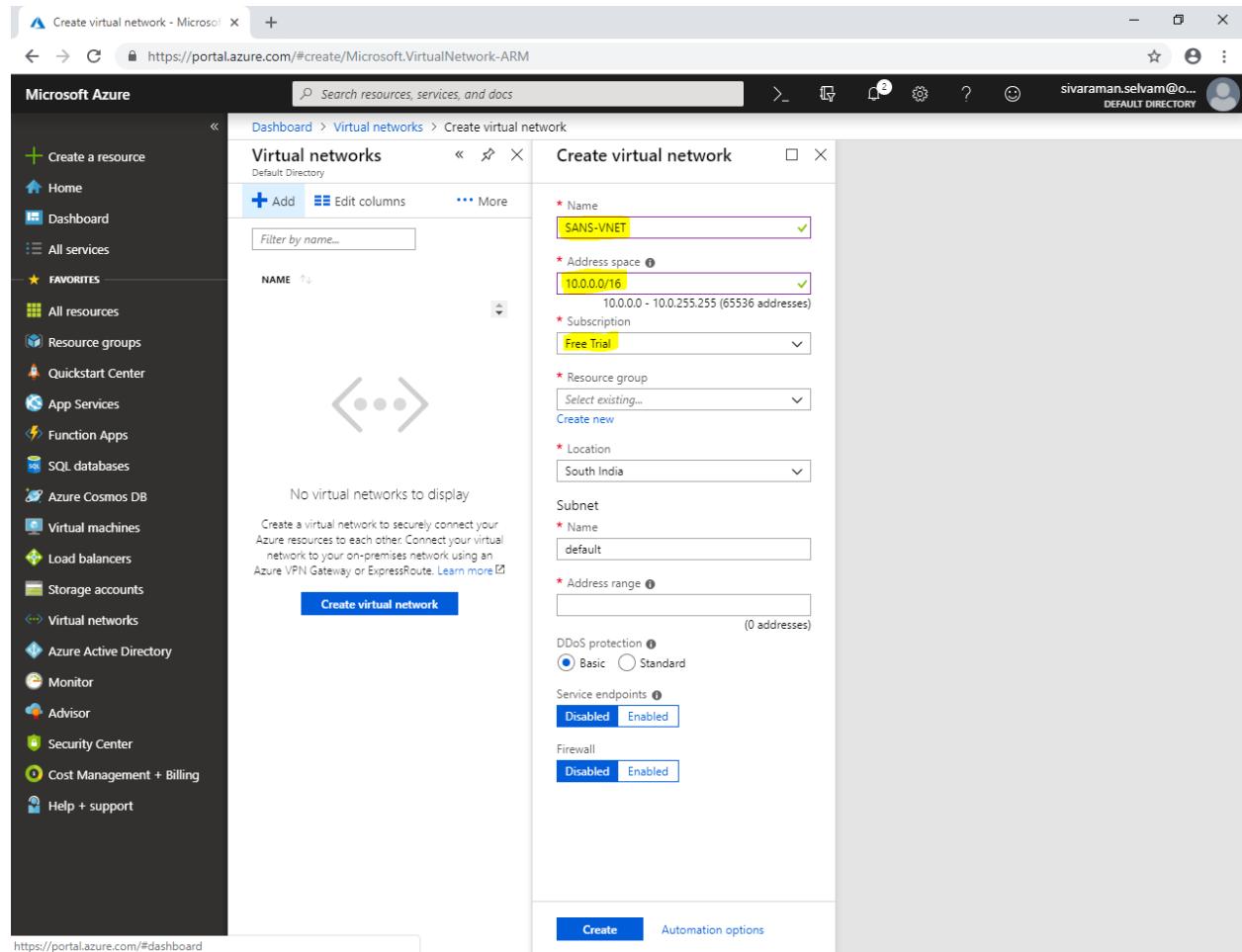
The screenshot shows the Microsoft Azure portal interface. The left sidebar is dark-themed and includes a 'Create a resource' button, 'Home', 'Dashboard', 'All services', and a 'Favorites' section with links to 'All resources', 'Resource groups', 'Quickstart Center', 'App Services', 'Function Apps', '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 has a light background. At the top, it says 'Virtual networks - Microsoft Azure' and shows the URL 'https://portal.azure.com/#blade/HubsExtension/Resources/resourceType/Microsoft.Network%2FvirtualNetworks'. Below this is the 'Virtual networks' heading with a 'Default Directory' dropdown. A search bar says 'Search resources, services, and docs'. There are buttons for '+ Add', 'Edit columns', 'Refresh', and 'Assign tags'. A 'Subscriptions' section shows 'Free Trial'. A table header row includes 'NAME', 'RESOURCE GROUP', 'LOCATION', and 'SUBSCRIPTION'. Below the table, a message says 'No virtual networks to display' and 'Create a virtual network to securely connect your Azure resources to each other. Connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute. [Learn more](#)'. A large blue 'Create virtual network' button is at the bottom.

While “Create virtual network”

Specify “Name” as “**SANS-VNET**”.

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

“Subscription” as “**Free Trial**”.

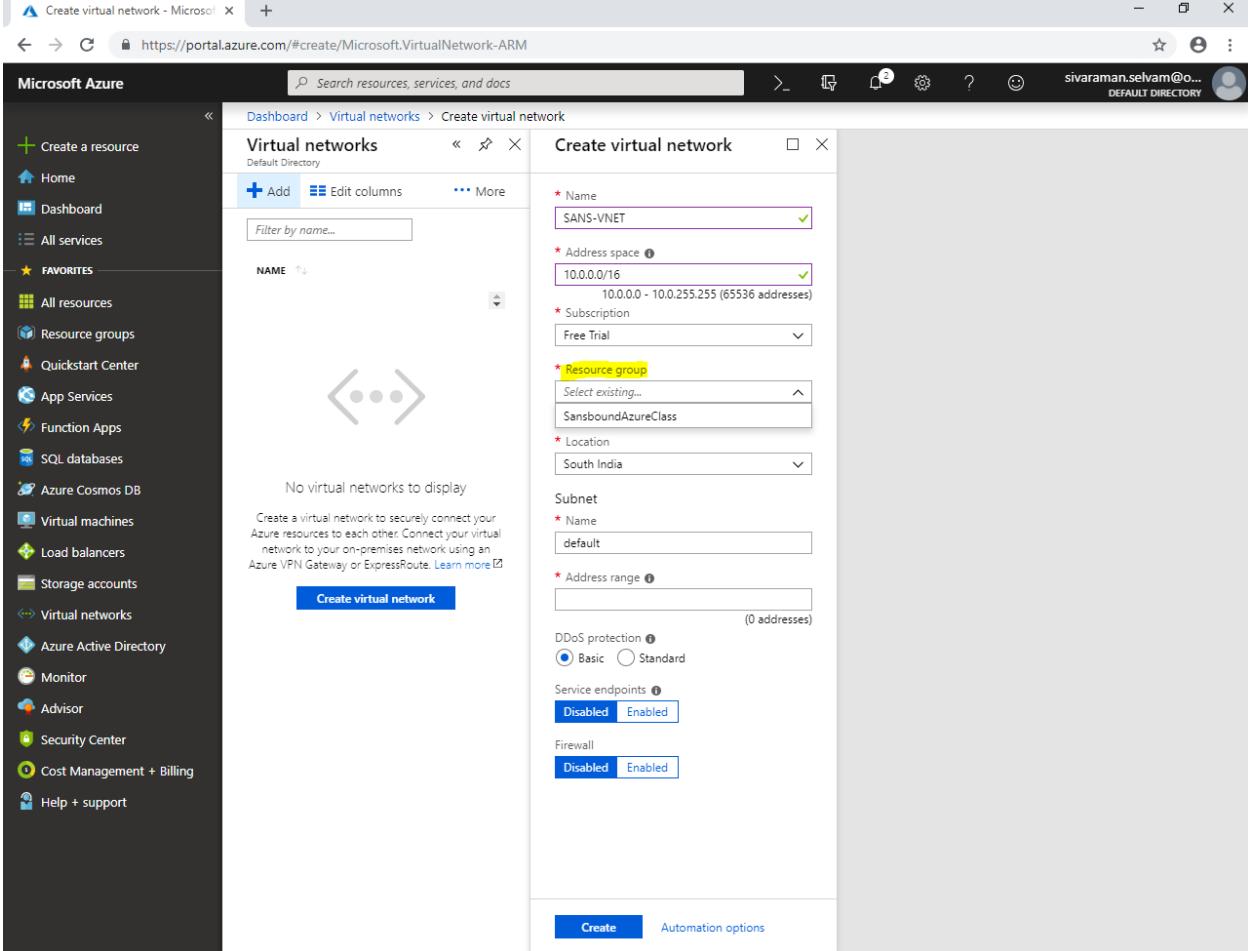


The screenshot shows the Microsoft Azure portal interface for creating a virtual network. The left sidebar contains navigation links for various services like Home, Dashboard, and Virtual networks. The main area is titled "Create virtual network" under "Virtual networks". The form fields are as follows:

- Name: SANS-VNET
- Address space: 10.0.0.0/16
- Subscription: Free Trial
- Resource group: Select existing... (with "Create new" option)
- Location: South India
- Subnet:
 - Name: default
 - Address range: (0 addresses)
 - DDoS protection: Basic (selected)
 - Service endpoints: Disabled
 - Firewall: Enabled

At the bottom, there are "Create" and "Automation options" buttons.

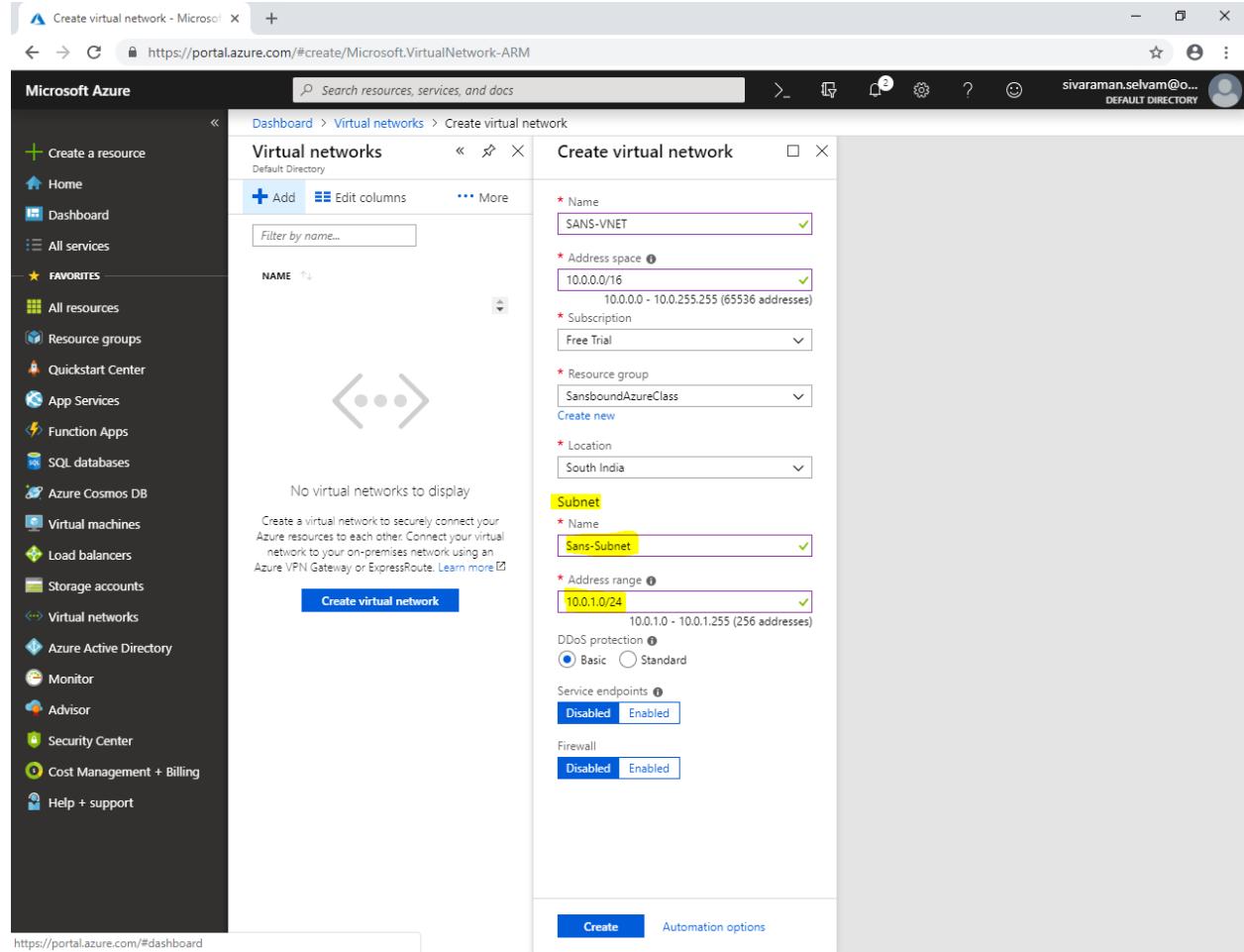
In “Resource group” click drop down list to select “**SansboundAzureClass**”.



The screenshot shows the Microsoft Azure portal interface for creating a virtual network. The left sidebar contains various service links, and the main area is titled 'Create virtual network'. The 'Resource group' field is highlighted with a yellow box, showing the dropdown menu with 'Select existing...' and 'SansboundAzureClass' selected. Other fields visible include 'Name' (SANS-VNET), 'Address space' (10.0.0.0/16), 'Subscription' (Free Trial), 'Location' (South India), and 'Subnet' settings.

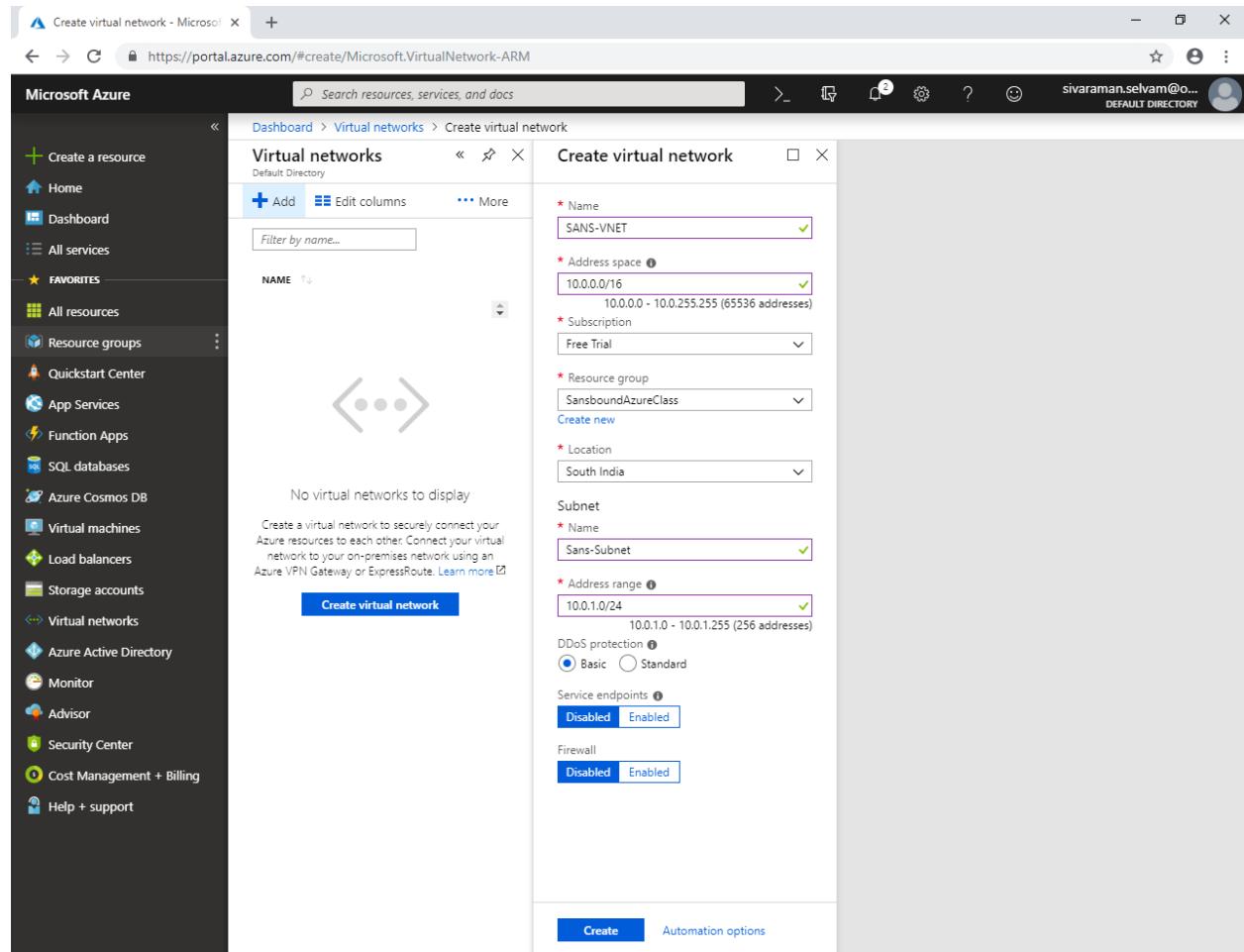
In “**Subnet**”, specify the Subnet name as “**Sans-Subnet**”.

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



The screenshot shows the Microsoft Azure portal interface for creating a virtual network. The left sidebar contains various service icons. The main area shows the 'Virtual networks' blade with the 'Create virtual network' step selected. The 'Name' field is filled with 'SANS-VNET'. The 'Address space' field is set to '10.0.0/16'. In the 'Subnet' section, 'Sans-Subnet' is listed under 'Name' and '10.0.1.0/24' is listed under 'Address range'. Other configuration options like 'Subscription', 'Resource group', 'Location', 'DDoS protection', 'Service endpoints', and 'Firewall' are also visible.

Click “Create”.



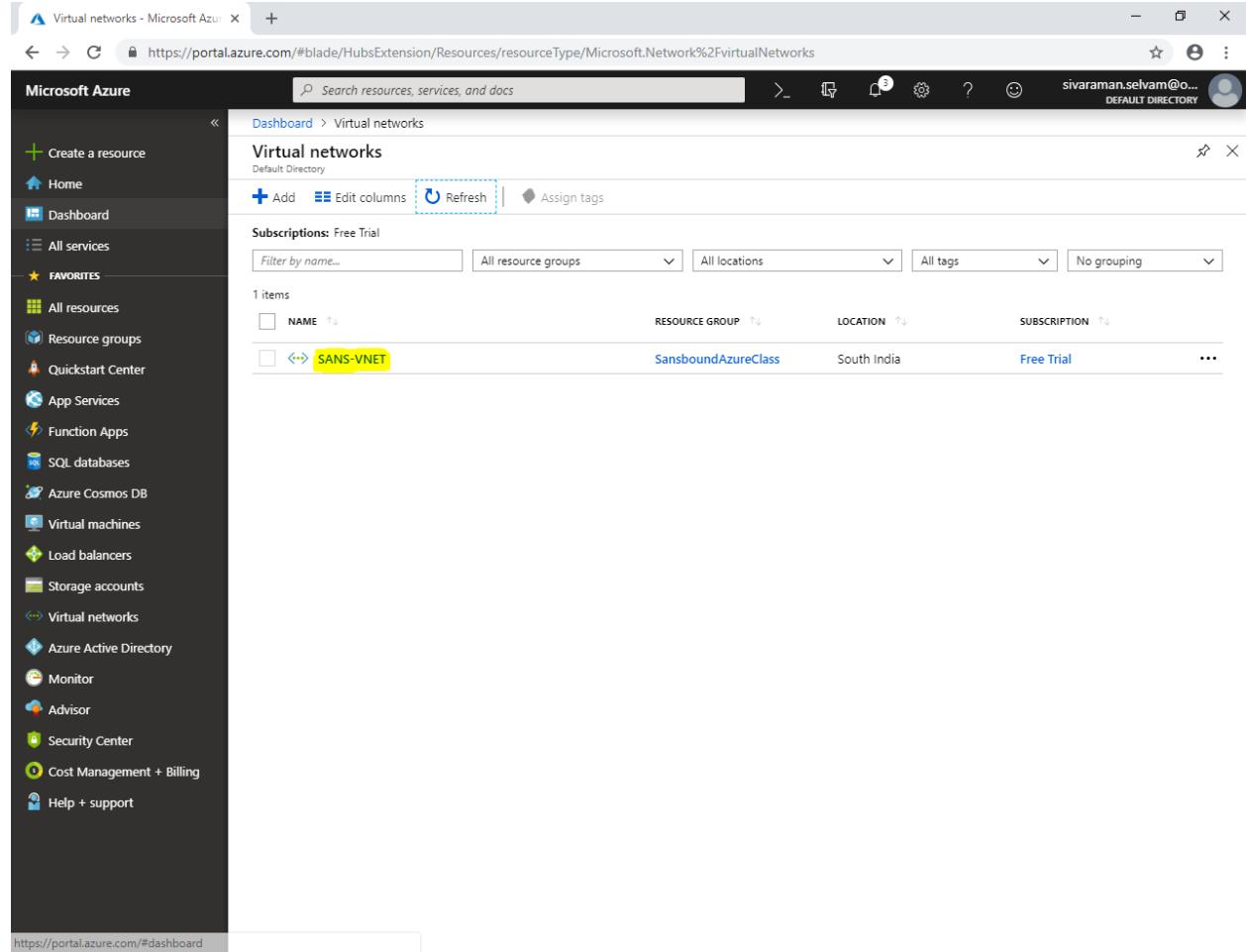
The screenshot shows the Microsoft Azure portal interface for creating a virtual network. The left sidebar contains navigation links for various services like Home, Dashboard, Resource groups, and Virtual networks. The main area is titled "Virtual networks" and shows a "Create virtual network" form. The form fields are 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:** Sans-Subnet
 - Address range:** 10.0.1.0/24 (10.0.1.0 - 10.0.1.255)
 - DDoS protection:** Basic (selected)
 - Service endpoints:** Disabled
 - Firewall:** Enabled

At the bottom of the form are two buttons: "Create" (highlighted in blue) and "Automation options".

In “Virtual networks”, click “Refresh”.

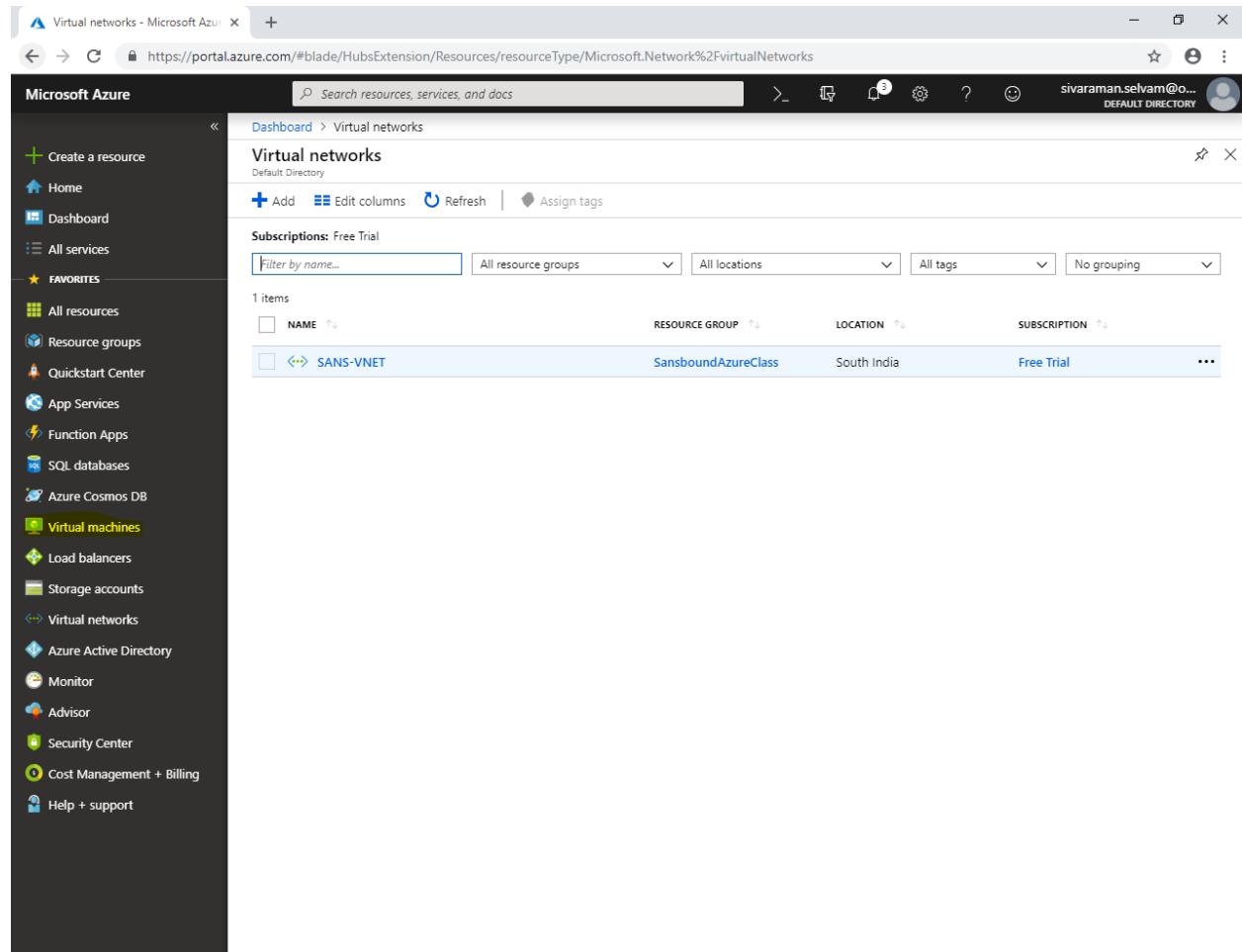
To view Virtual Network “**SANS-VNET**”



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 "Refresh" button in the top navigation bar is highlighted with a dashed blue border. The table below lists one item: "SANS-VNET", which is highlighted with a yellow box. The table columns are NAME, RESOURCE GROUP, LOCATION, and SUBSCRIPTION. The details for "SANS-VNET" are: NAME - SANS-VNET, RESOURCE GROUP - SansboundAzureClass, LOCATION - South India, and SUBSCRIPTION - Free Trial.

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

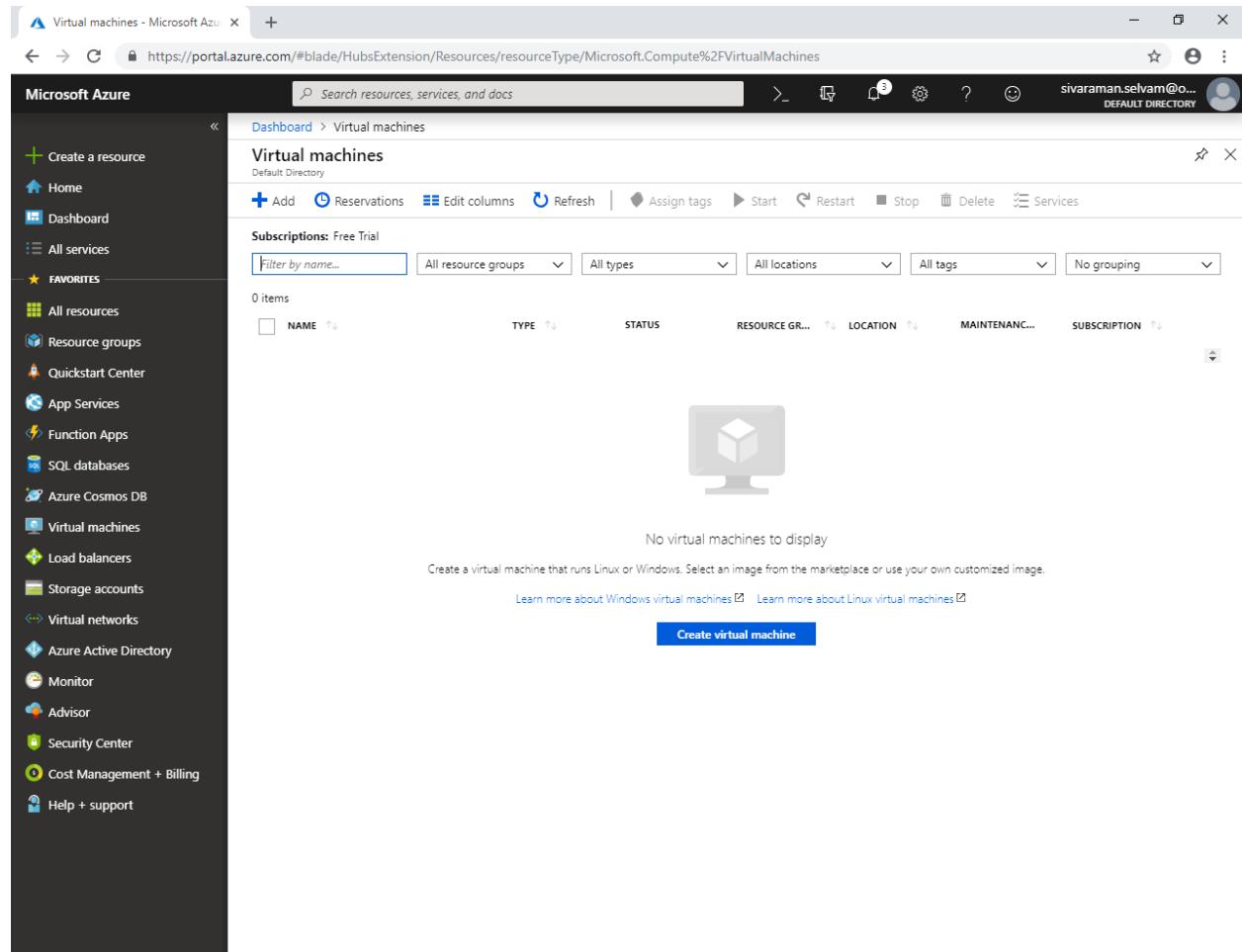
Click “Virtual machines” in left side panel.



The screenshot shows the Microsoft Azure portal interface. The left sidebar is titled "Microsoft Azure" and contains a list of services under "FAVORITES", including "Virtual machines", which is highlighted with a yellow background. The main content area is titled "Virtual networks" and shows a table of resources. The table has columns for NAME, RESOURCE GROUP, LOCATION, and SUBSCRIPTION. One item is listed: "SANS-VNET" under "NAME", "SansboundAzureClass" under "RESOURCE GROUP", "South India" under "LOCATION", and "Free Trial" under "SUBSCRIPTION".

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

In “Virtual machines” click “Add”.



The screenshot shows the Microsoft Azure portal interface. The left sidebar is the navigation menu with various services listed under 'FAVORITES'. The main content area is titled 'Virtual machines' and shows a message 'No virtual machines to display'. Below this, there is a callout with icons for Windows and Linux virtual machines, followed by links to 'Learn more about Windows virtual machines' and 'Learn more about Linux virtual machines'. At the bottom of the page is a prominent blue button labeled 'Create virtual machine'.

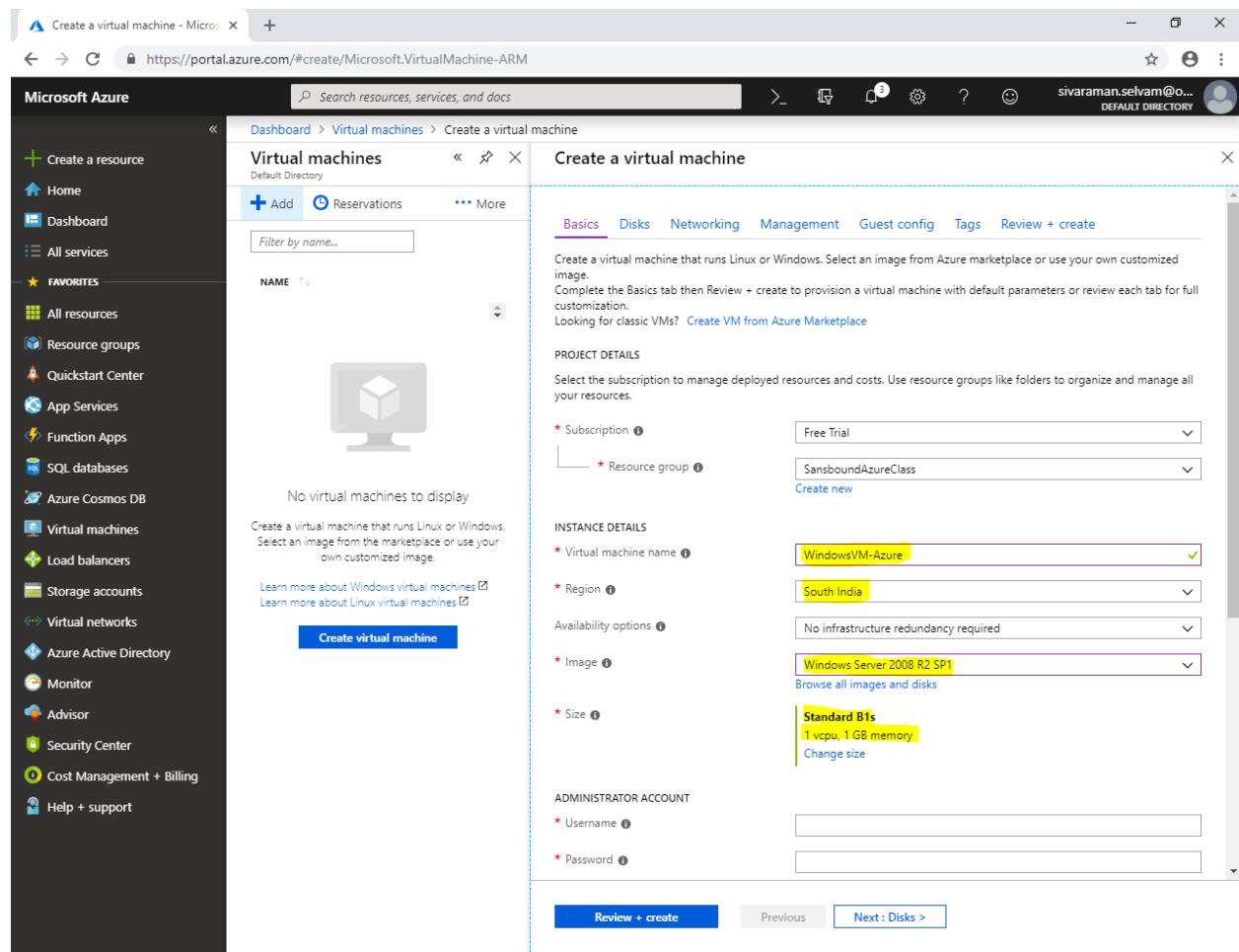
In “Instance details”

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

Select “Region” as “South India”.

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

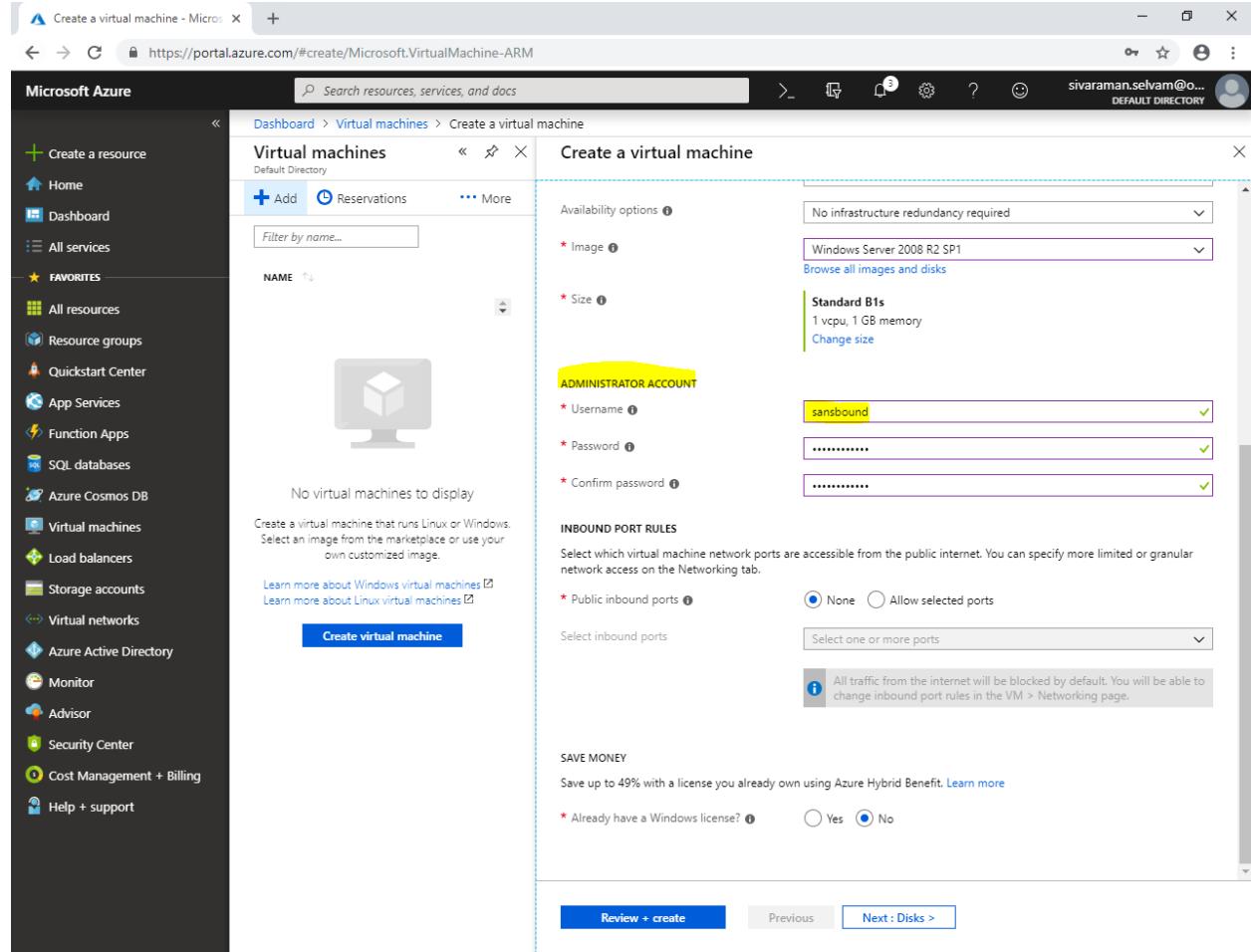
Change “VM Size” as “Standard B1s”.



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar lists various Azure services like Home, Dashboard, Resource groups, and App Services. The main area shows a 'Virtual machines' blade with a search bar and a 'Create a virtual machine' wizard. The 'Basics' tab is active, displaying fields for Subscription (Free Trial), Resource group (SansboundAzureClass), Virtual machine name (WindowsVM-Azure), Region (South India), Image (Windows Server 2008 R2 SP1), and Size (Standard B1s). Buttons for 'Review + create' and 'Next : Disks >' are at the bottom.

In “Administrator Account”.

Type “Username” as “sansbound”.



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, and Favorites. The main area shows the 'Virtual machines' blade with a search bar and a 'Create a virtual machine' button. The 'Create a virtual machine' wizard is open, showing the following steps:

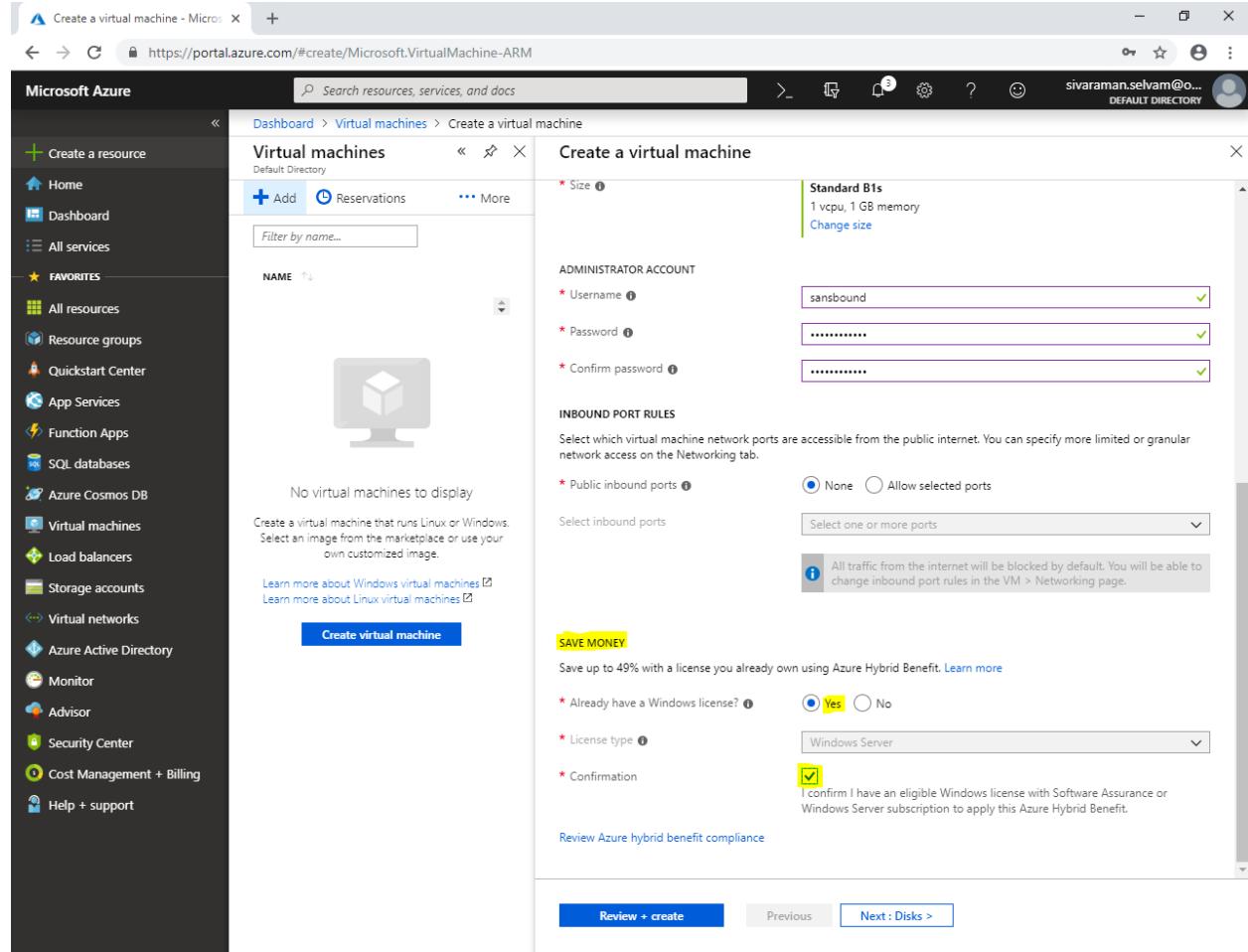
- Availability options:** No infrastructure redundancy required.
- Image:** Windows Server 2008 R2 SP1 selected.
- Size:** Standard B1s selected (1 vCPU, 1 GB memory).
- ADMINISTRATOR ACCOUNT:** The 'Username' field is highlighted and contains 'sansbound'. The 'Password' and 'Confirm password' fields are also visible.
- INBOUND PORT RULES:** Set to 'None'.
- SAVE MONEY:** A note about Azure Hybrid Benefit.
- Already have a Windows license?**: A radio button is selected for 'No'.

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

In “Save Money”

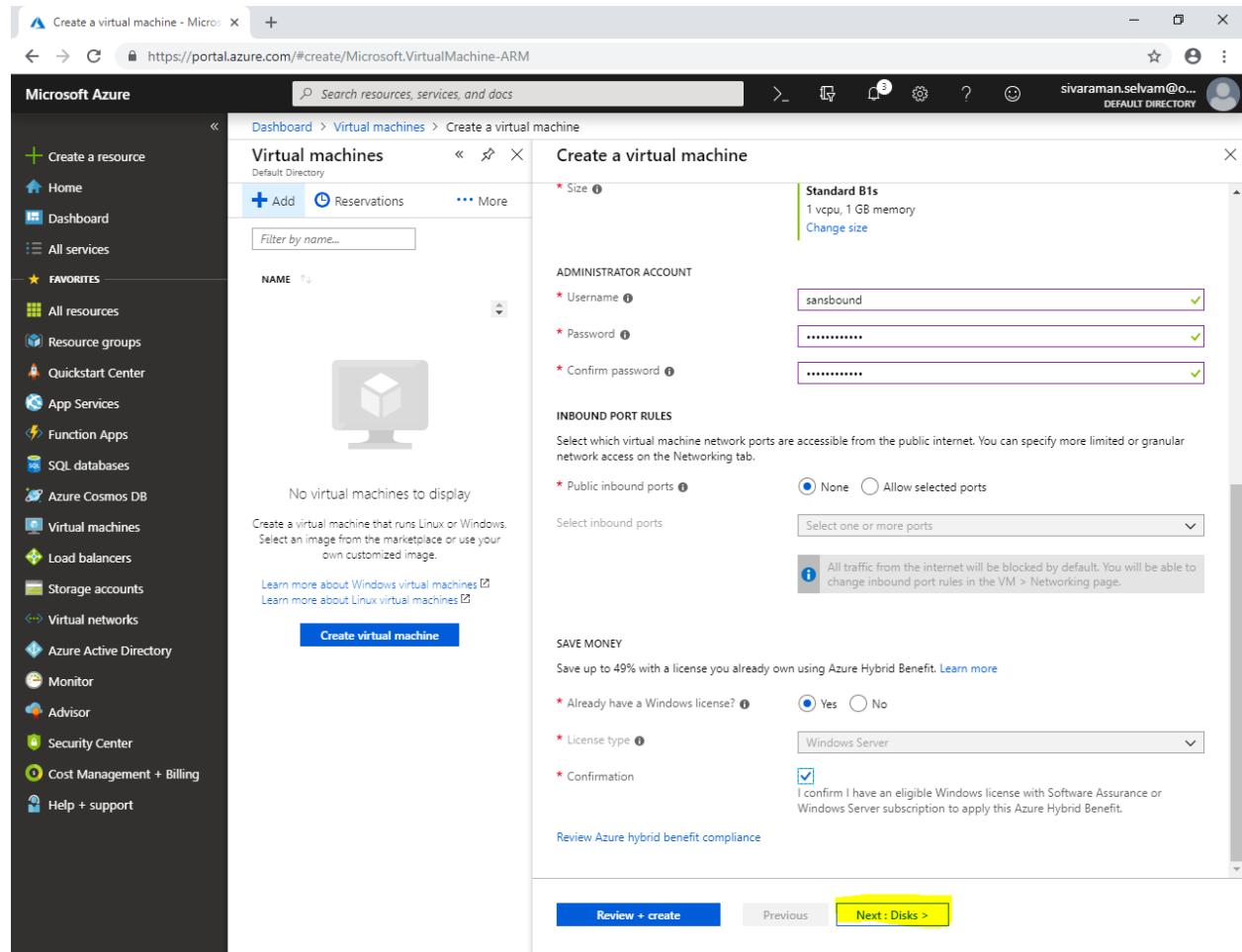
Click “Yes”.

Need to check “Confirmation” box.



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 (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 is titled "Create a virtual machine" under "Virtual machines". It shows a "Standard B1s" size (1 vcpu, 1 GB memory) selected. The "ADMINISTRATOR ACCOUNT" section requires a "Username" (sansbound), "Password", and "Confirm password". Under "INBOUND PORT RULES", it says "None" is selected. A "SAVE MONEY" section offers a 49% discount for using Azure Hybrid Benefit. It includes radio buttons for "Already have a Windows license? Yes" (selected) and "No", a dropdown for "License type" (Windows Server), and a checked checkbox for "Confirmation" which states: "I confirm I have an eligible Windows license with Software Assurance or Windows Server subscription to apply this Azure Hybrid Benefit." At the bottom, there are "Review + create", "Previous", and "Next: Disks >" buttons.

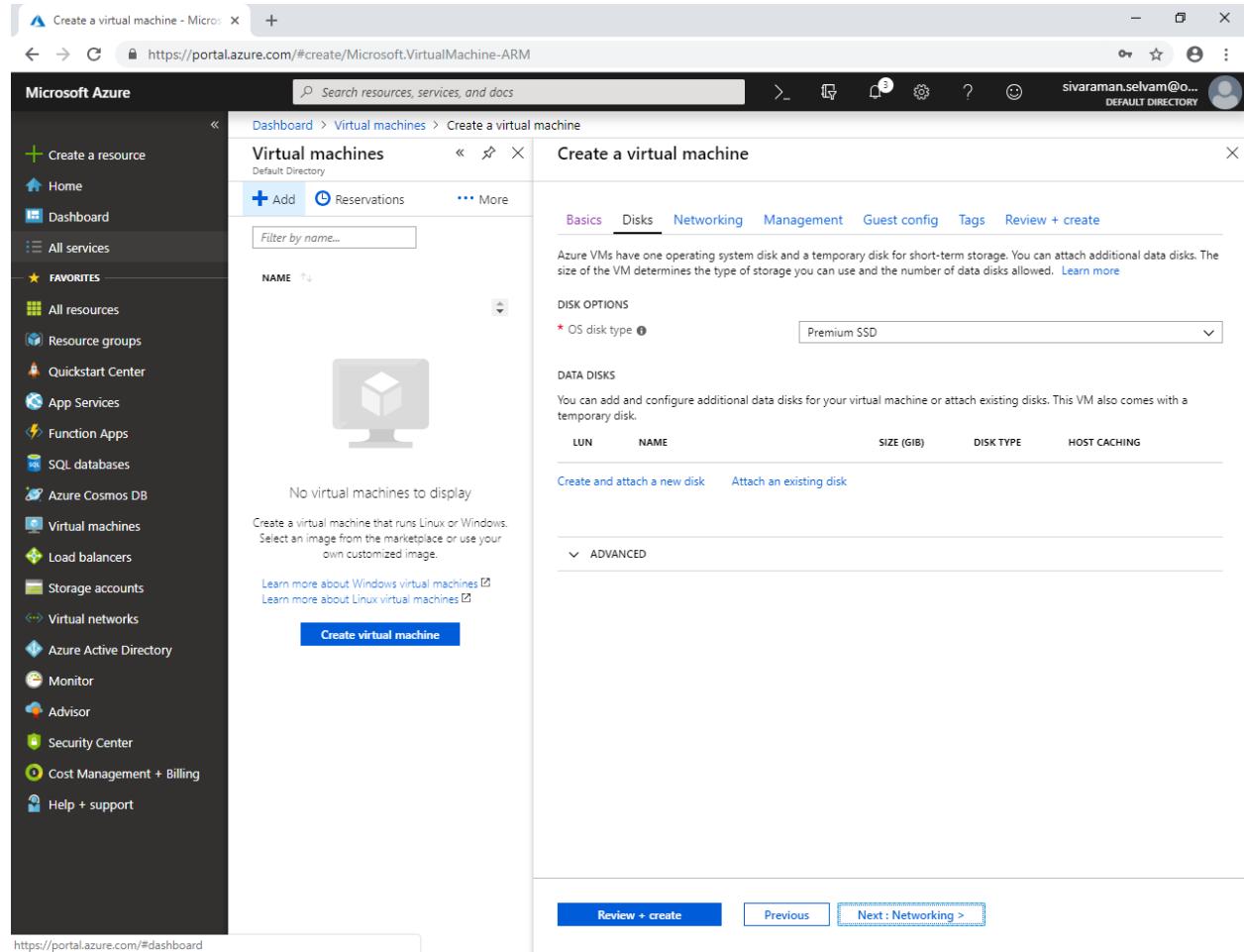
Click “Next : Disks >”.



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 'Virtual machines' blade is active, showing a list of existing VMs and a 'Create a virtual machine' button. The 'Create a virtual machine' page is the second step of the wizard. It asks for basic details: a name ('NAME'), size ('Standard B1s'), administrator account ('sansbound'), and inbound port rules ('None'). It also offers to save money by using an existing Windows license ('Yes', 'Windows Server'). A note at the bottom says 'I confirm I have an eligible Windows license with Software Assurance or Windows Server subscription to apply this Azure Hybrid Benefit.' The 'Next : Disks >' button is highlighted with a yellow box, indicating the next step in the process.

In “Disks”,

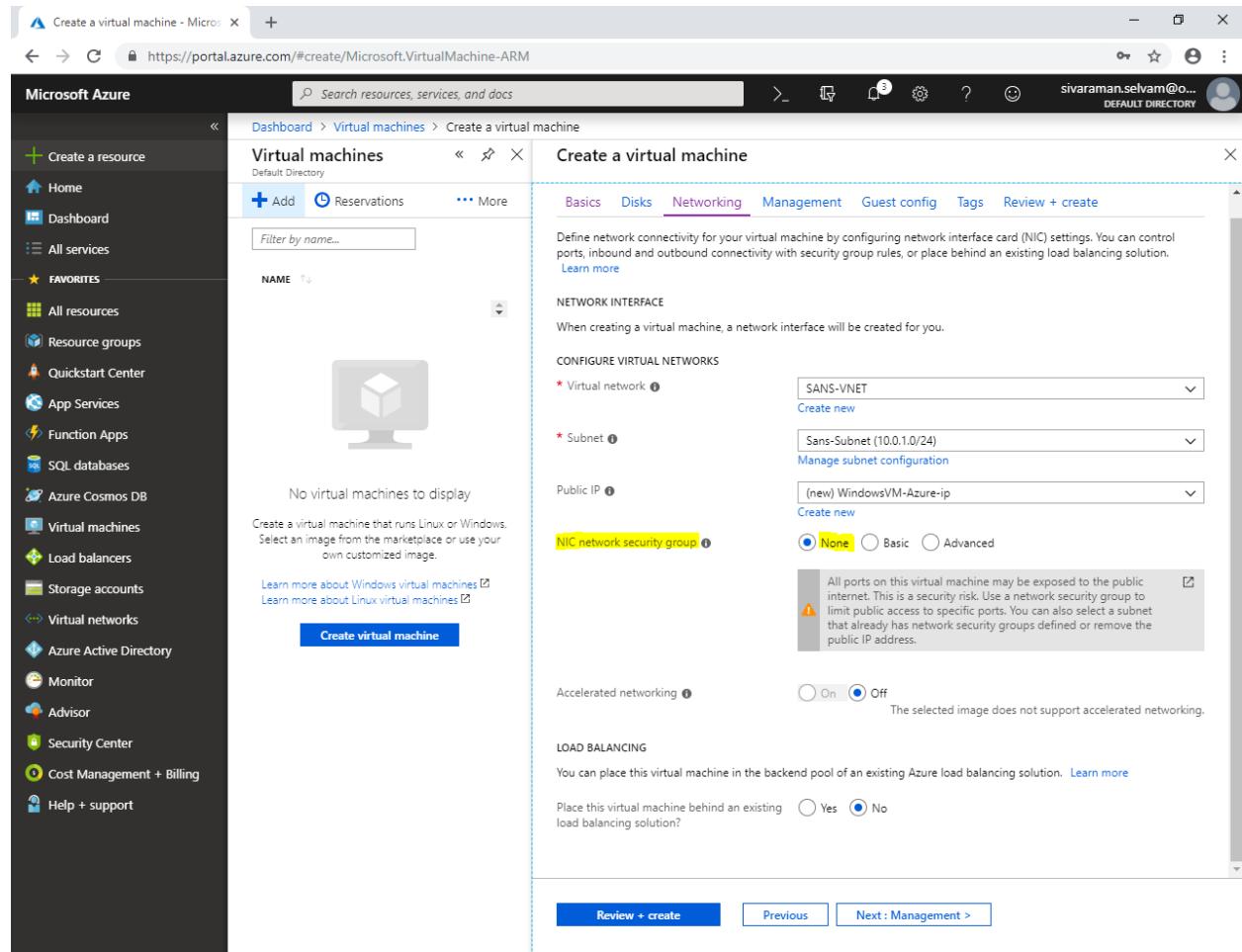
Leave default and click “**Next : Networking>**”.



The screenshot shows the Microsoft Azure portal interface for creating a virtual machine. The left sidebar contains various service icons under 'All services' and 'FAVORITES'. The main panel shows the 'Virtual machines' section with a 'Create a virtual machine' wizard. The 'Disks' tab is currently selected. Under 'DISK OPTIONS', the 'OS disk type' is set to 'Premium SSD'. Below that, the 'DATA DISKS' section allows adding additional disks. At the bottom of the wizard, there are three buttons: 'Review + create', 'Previous', and 'Next : Networking >'. The URL in the browser bar is <https://portal.azure.com/#create/Microsoft.VirtualMachine-ARM>.

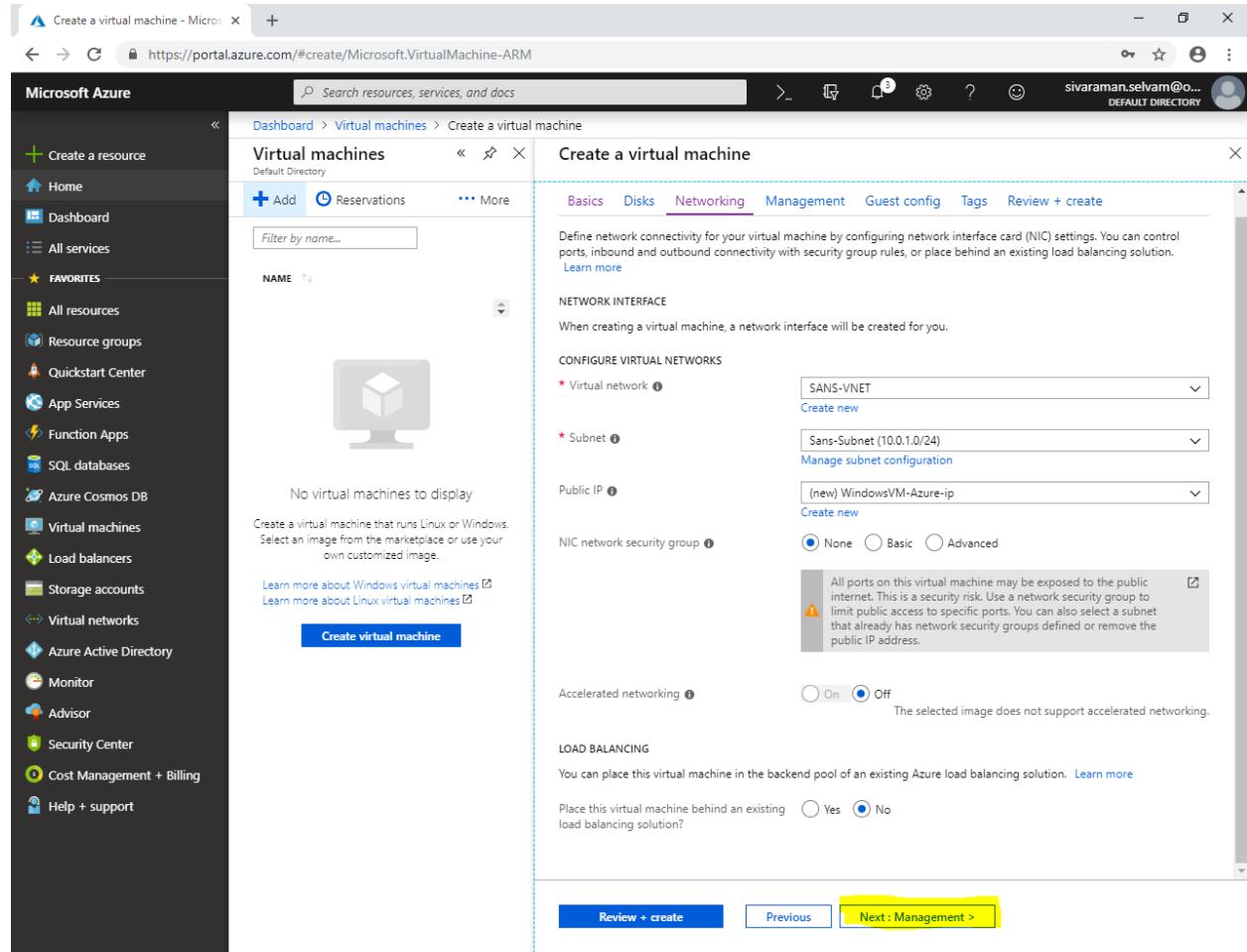
In “Networking”

Click “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 shows the 'Virtual machines' blade with a search bar and a 'Create a virtual machine' button. The 'Networking' tab is selected in the top navigation bar. In the 'CONFIGURE VIRTUAL NETWORKS' section, under 'Virtual network', the dropdown is set to 'SANS-VNET'. Under 'Subnet', it is set to 'Sans-Subnet (10.0.1.0/24)'. Under 'Public IP', it is set to '(new) WindowsVM-Azure-ip'. The 'NIC network security group' dropdown is highlighted with a yellow box and set to 'None'. A warning message 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, there are 'Review + create', 'Previous', and 'Next : Management >' buttons.

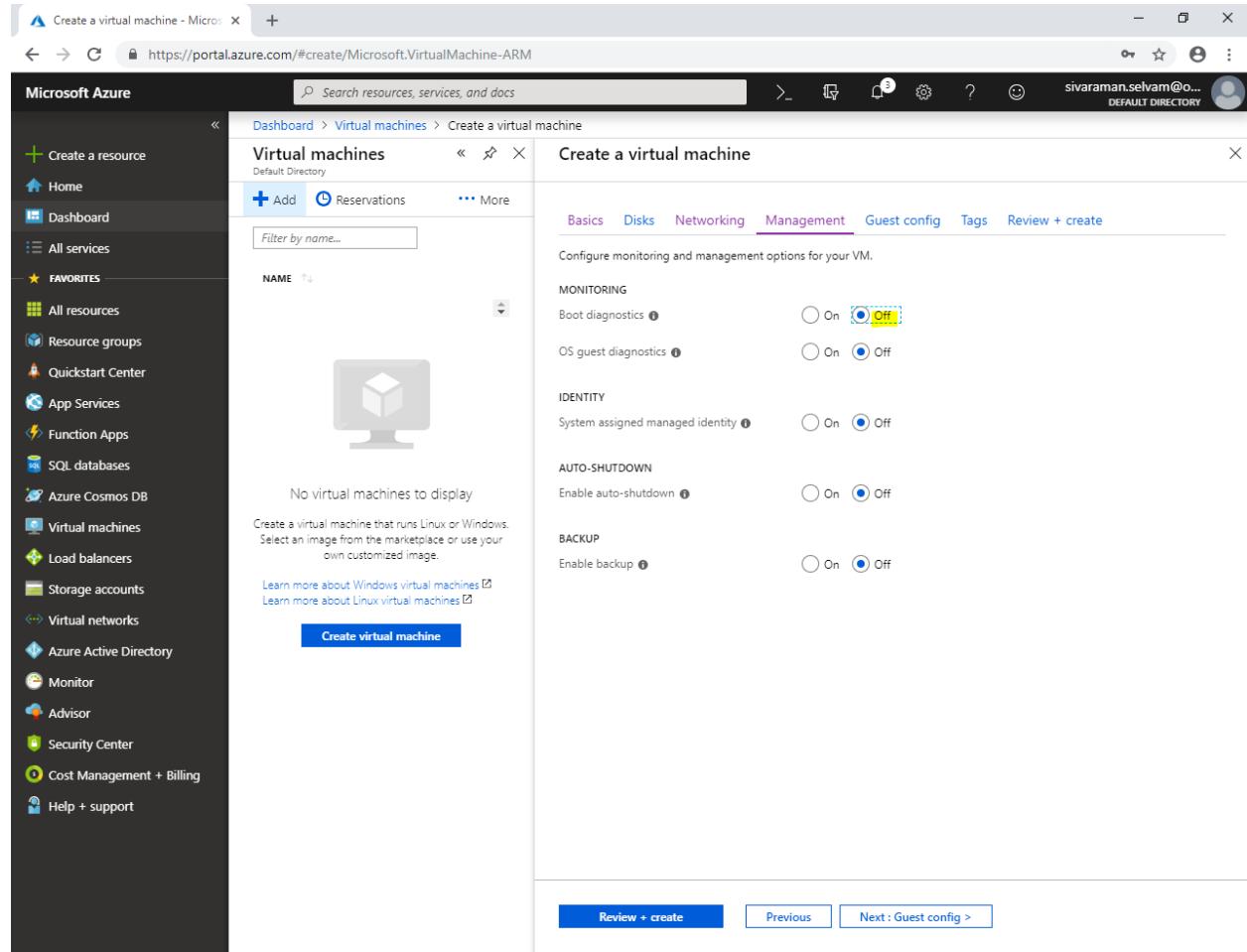
Click “Next : Management>”.



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains various service links like Home, Dashboard, and Resource groups. The main area shows a list of existing virtual machines with a 'Create virtual machine' button. The right panel is titled 'Create a virtual machine' and has tabs for Basics, Disks, Networking, Management, Guest config, Tags, Review + create, and a 'Management' tab which is currently active. Under the 'Networking' section, it asks to define network connectivity by configuring network interface card (NIC) settings. It shows a configuration for a Virtual network named 'SANS-VNET', a Subnet named 'Sans-Subnet (10.0.1.0/24)', and a Public IP address '(new) WindowsVM-Azure-ip'. A note states that all ports on the virtual machine may be exposed to the public internet, which is a security risk. Accelerated networking is turned off. In the 'LOAD BALANCING' section, it asks if the virtual machine should be placed behind an existing Azure load balancing solution, with 'No' selected. At the bottom, there are 'Review + create', 'Previous', and 'Next : Management >' buttons, with 'Next : Management >' being highlighted.

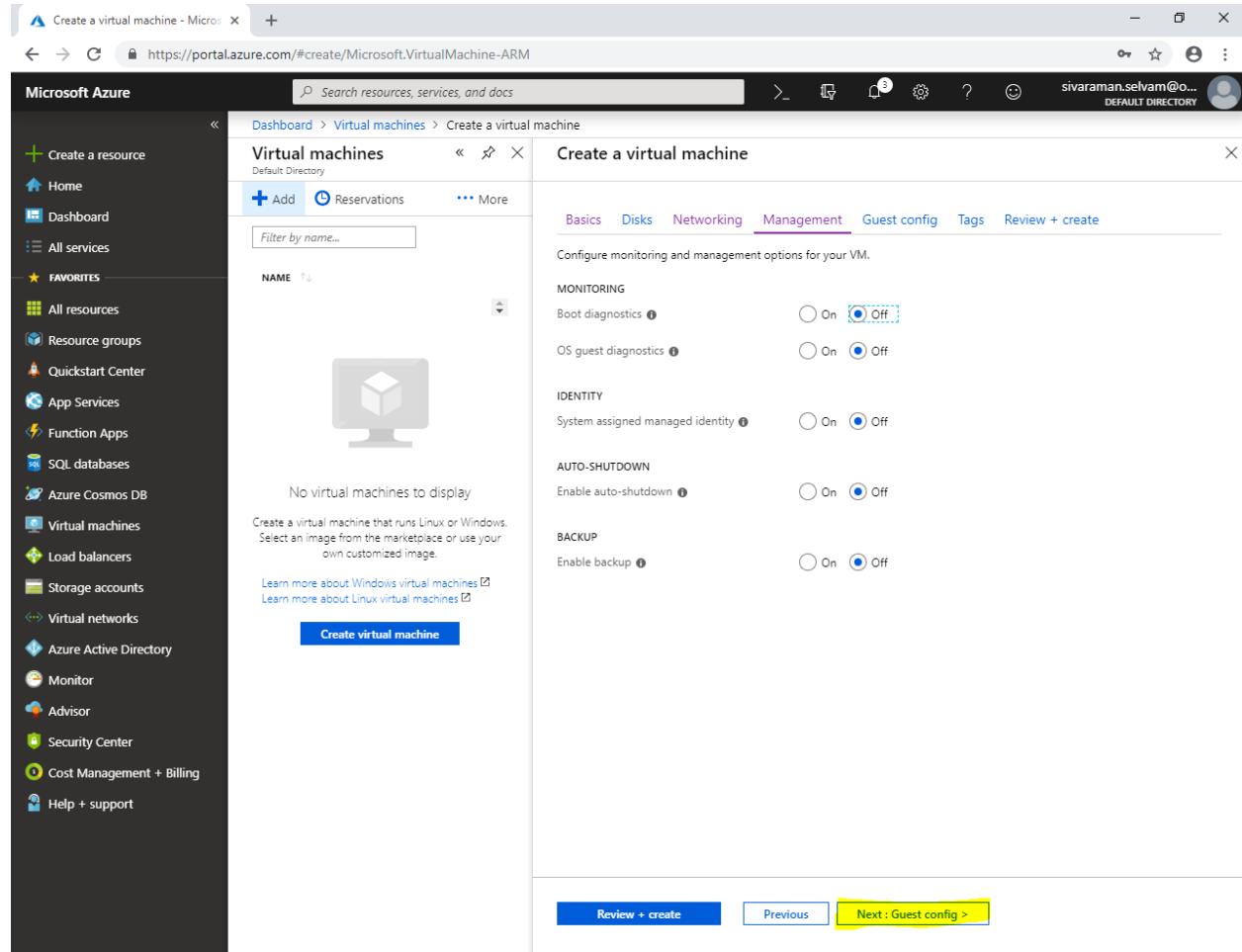
In “Management”.

Set “Boot Diagnostics” as “Off”.



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar lists various services under 'FAVORITES'. The main area shows the 'Virtual machines' blade with a 'Create a virtual machine' wizard. The 'Management' tab is currently selected. In the 'MONITORING' section, the 'Boot diagnostics' setting is configured to 'Off', indicated by a yellow box around the radio button. Other sections like 'IDENTITY', 'AUTO-SHUTDOWN', and 'BACKUP' are also visible with their respective configuration options.

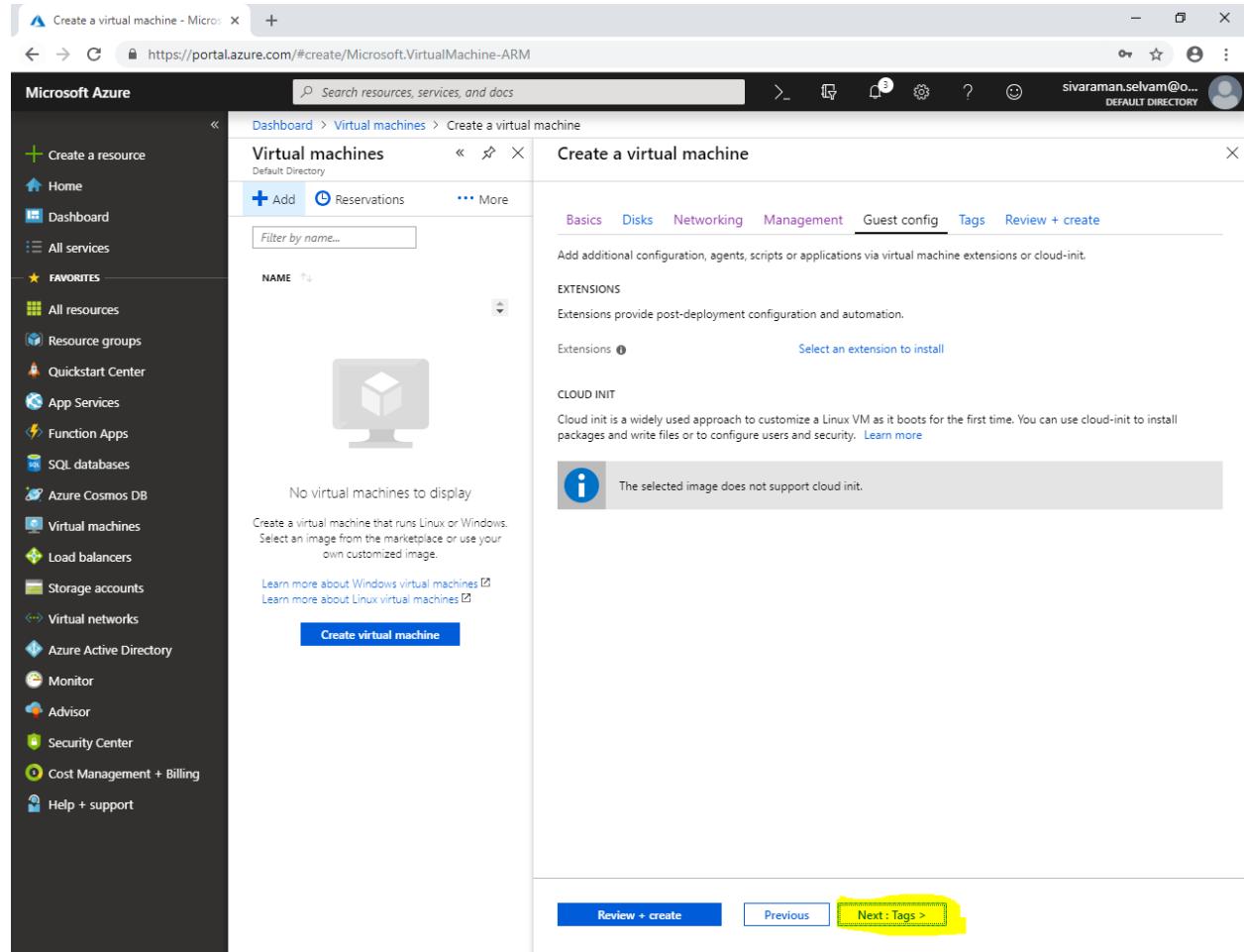
Click “**Next : Guest config>**”.



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains various service icons under 'FAVORITES'. The main area displays the 'Virtual machines' section with a search bar and a 'Create a virtual machine' button. The 'Management' tab is selected in the top navigation bar. The configuration pane shows several sections: 'MONITORING' (Boot diagnostics set to Off, OS guest diagnostics set to Off), 'IDENTITY' (System assigned managed identity set to Off), 'AUTO-SHUTDOWN' (Enable auto-shutdown set to Off), and 'BACKUP' (Enable backup set to Off). At the bottom, there are 'Review + create', 'Previous', and 'Next : Guest config >' buttons. The 'Next : Guest config >' button is highlighted with a yellow box.

In “Guest config”

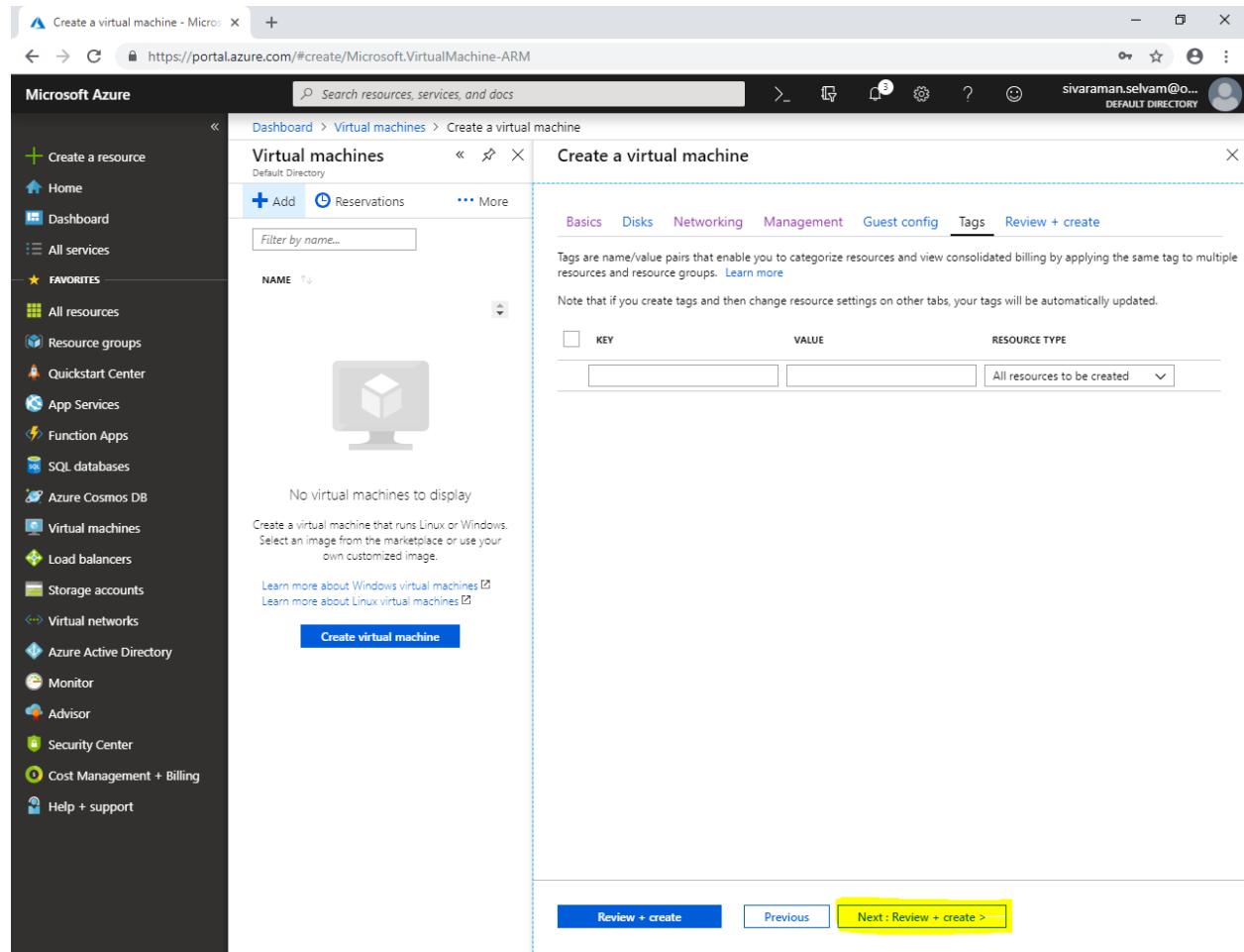
Click “Next : Tags >”.



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 various services. The main area is titled 'Create a virtual machine' under 'Virtual machines'. The 'Guest config' tab is currently selected, indicated by a blue underline. Below it, other tabs include Basics, Disks, Networking, Management, Tags, and Review + create. A note above the tabs says: 'Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.' Under 'EXTENSIONS', there's a link to 'Select an extension to install'. Under 'CLOUD INIT', it states: 'Cloud init is a widely used approach to customize a Linux VM as it boots for the first time. You can use cloud-init to install packages and write files or to configure users and security.' A note below says: 'The selected image does not support cloud init.' At the bottom, there are buttons for 'Review + create', 'Previous', and 'Next : Tags >' (the latter is highlighted with a yellow box).

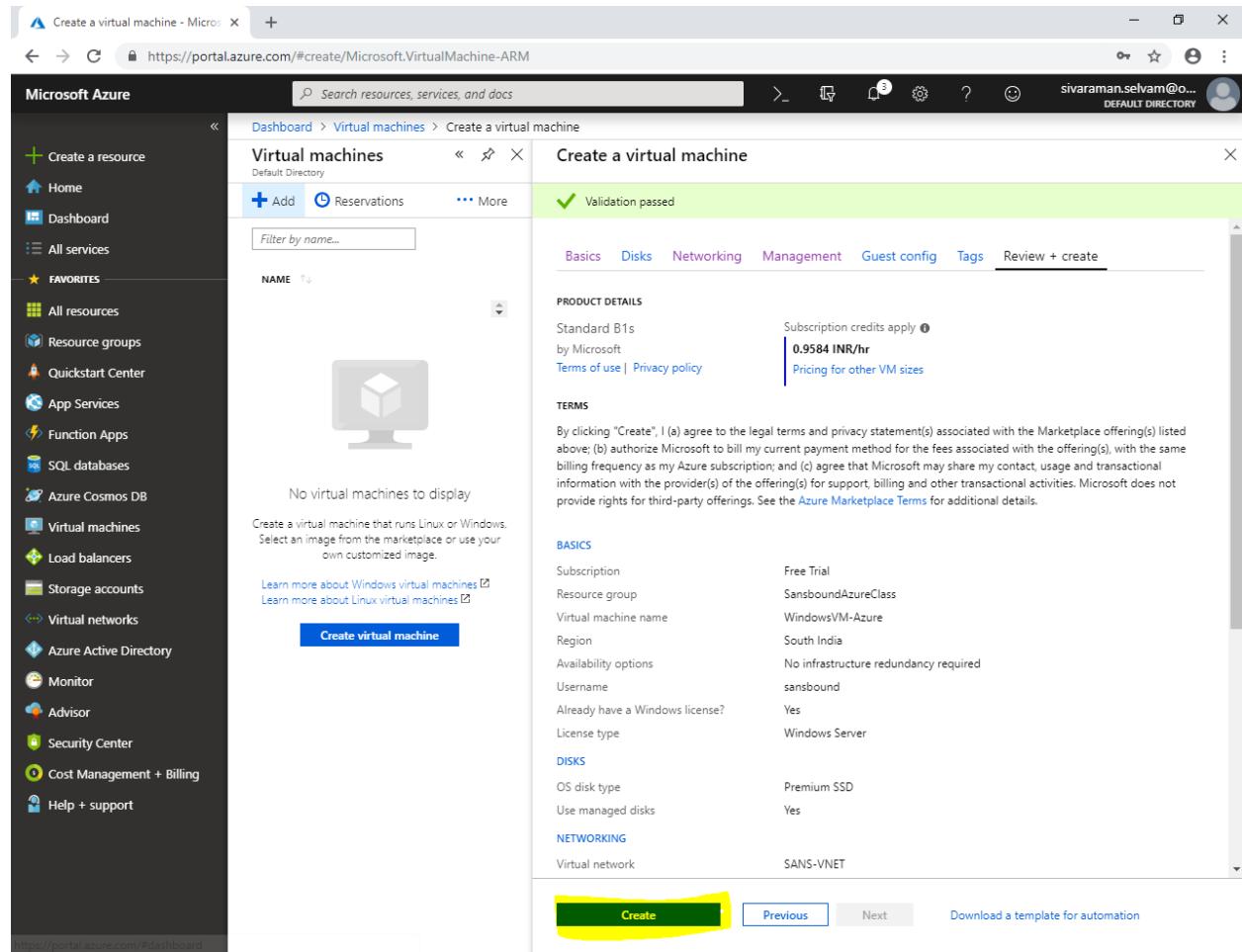
In “Tags”.

Click “Next : Review + Create”.



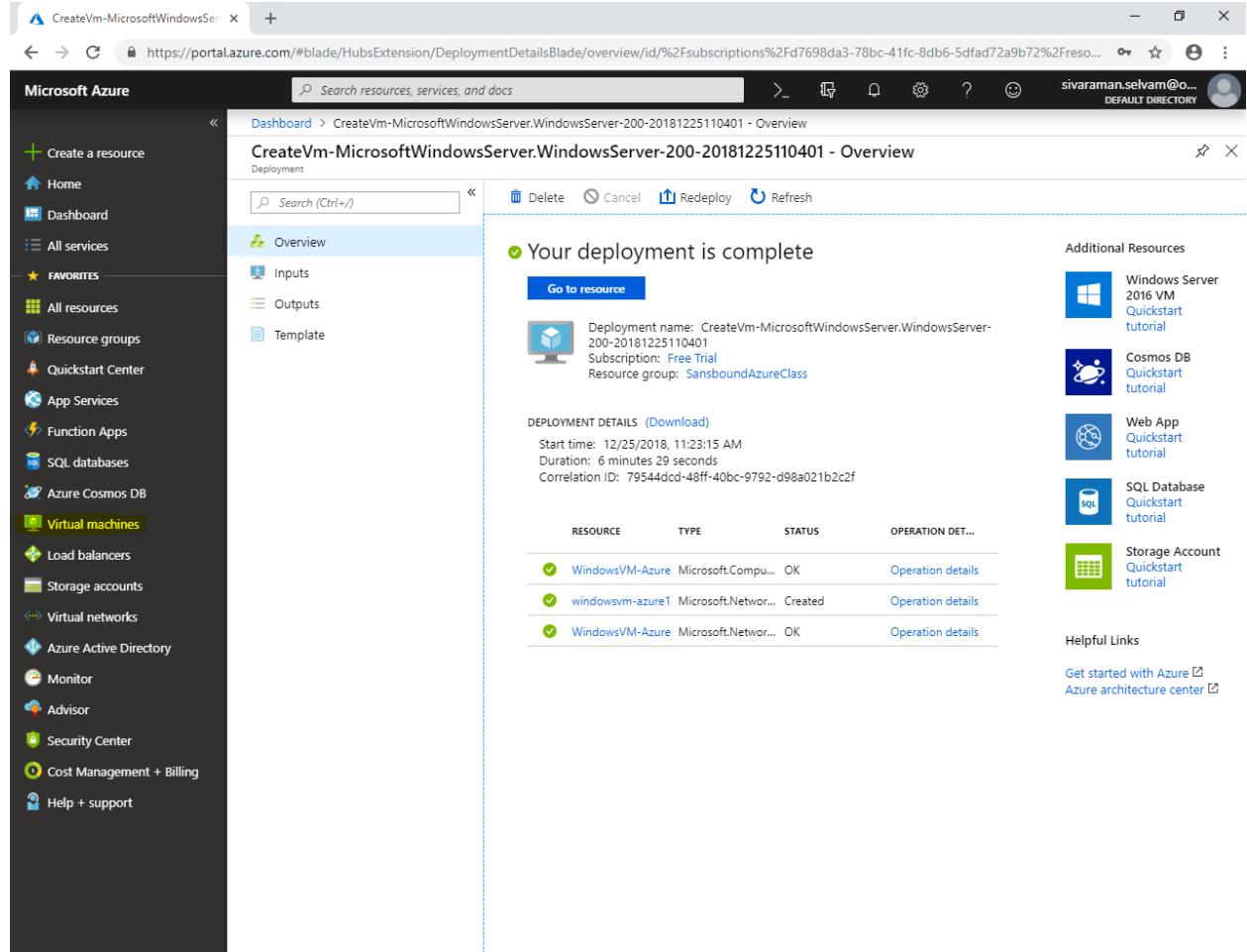
The screenshot shows the Microsoft Azure portal interface for creating a virtual machine. The left sidebar lists various services like Home, Dashboard, and Resource groups. The main area shows a list of virtual machines with a search bar and a 'Create a virtual machine' button. On the right, a detailed configuration pane is open for a new VM. The 'Tags' tab is currently active, showing a table where a single tag 'All resources to be created' is defined with the value 'All resources'. Below this table, there's a note about tags enabling categorized billing and resource grouping. At the bottom of the configuration pane, there are three buttons: 'Review + create' (highlighted with a yellow box), 'Previous', and 'Next: Review + create >'. The URL in the browser bar is https://portal.azure.com/#create/Microsoft.VirtualMachine-ARM.

Click “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, and more. The main area is titled 'Create a virtual machine' under 'Virtual machines'. A green banner at the top right says 'Validation passed'. Below it, there are tabs for Basics, Disks, Networking, Management, Guest config, Tags, and Review + create. The Basics tab is selected. Under 'PRODUCT DETAILS', it shows a Standard B1s VM by Microsoft, costing 0.9584 INR/hr. There's also a link to Pricing for other VM sizes. The 'TERMS' section contains legal agreement text. The 'BASICS' section includes fields for 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), and License type (Windows Server). The 'DISKS' section shows OS disk type as Premium SSD and Use managed disks as Yes. The 'NETWORKING' section lists the Virtual network as SANS-VNET. At the bottom, there are 'Create', 'Previous', 'Next', and 'Download a template for automation' buttons. The 'Create' button is highlighted with a yellow background.

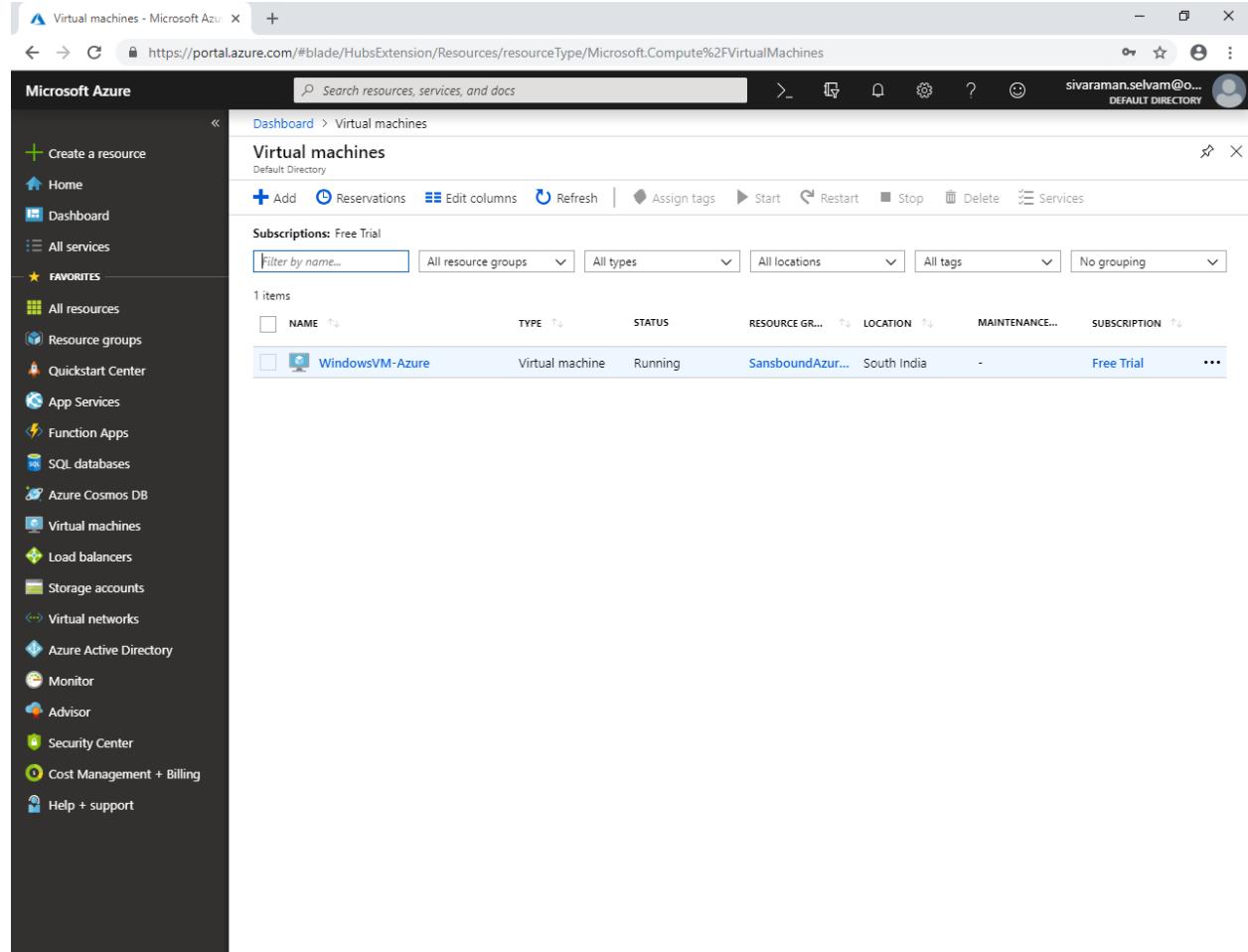
Once you have successfully deployed Virtual machine, then click “Virtual machines”.



The screenshot shows the Microsoft Azure portal interface. The left sidebar is dark-themed and includes the following navigation items under 'FAVORITES': Create a resource, Home, Dashboard, All services, Virtual machines (which is selected and highlighted in yellow), Resource groups, Quickstart Center, App Services, Function Apps, SQL databases, Azure Cosmos DB, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Billing, Help + support. The main content area shows the deployment details for 'CreateVm-MicrosoftWindowsServer.WindowsServer-200-20181225110401'. It displays a summary message: 'Your deployment is complete'. Below this, it lists deployment details: Deployment name: CreateVm-MicrosoftWindowsServer.WindowsServer-200-20181225110401, Subscription: Free Trial, Resource group: SansboundAzureClass. Under 'DEPLOYMENT DETAILS', it shows start time: 12/25/2018, 11:23:15 AM, duration: 6 minutes 29 seconds, and correlation ID: 79544dc4-40bc-9792-d98a021b2c2f. A table lists three resources: WindowsVM-Azure (Microsoft.Compute), windowsvm-azure1 (Microsoft.Network), and WindowsVM-Azure (Microsoft.Network), all in 'OK' status. To the right, there's a section for 'Additional Resources' with links to Quickstart tutorials for Windows Server 2016 VM, Cosmos DB, Web App, SQL Database, and Storage Account. At the bottom, there are 'Helpful Links' to 'Get started with Azure' and 'Azure architecture center'.

In “Virtual machines”,

Click “Add” to create new virtual machine.



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 "Virtual machines". At the top of the list, there is a single item: "WindowsVM-Azure" which is a "Virtual machine" in the "Running" status, located in "South India" under the "SansboundAzur..." resource group, and is associated with the "Free Trial" subscription. The "Add" button is visible at the top of the list.

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

While creating Virtual machine,

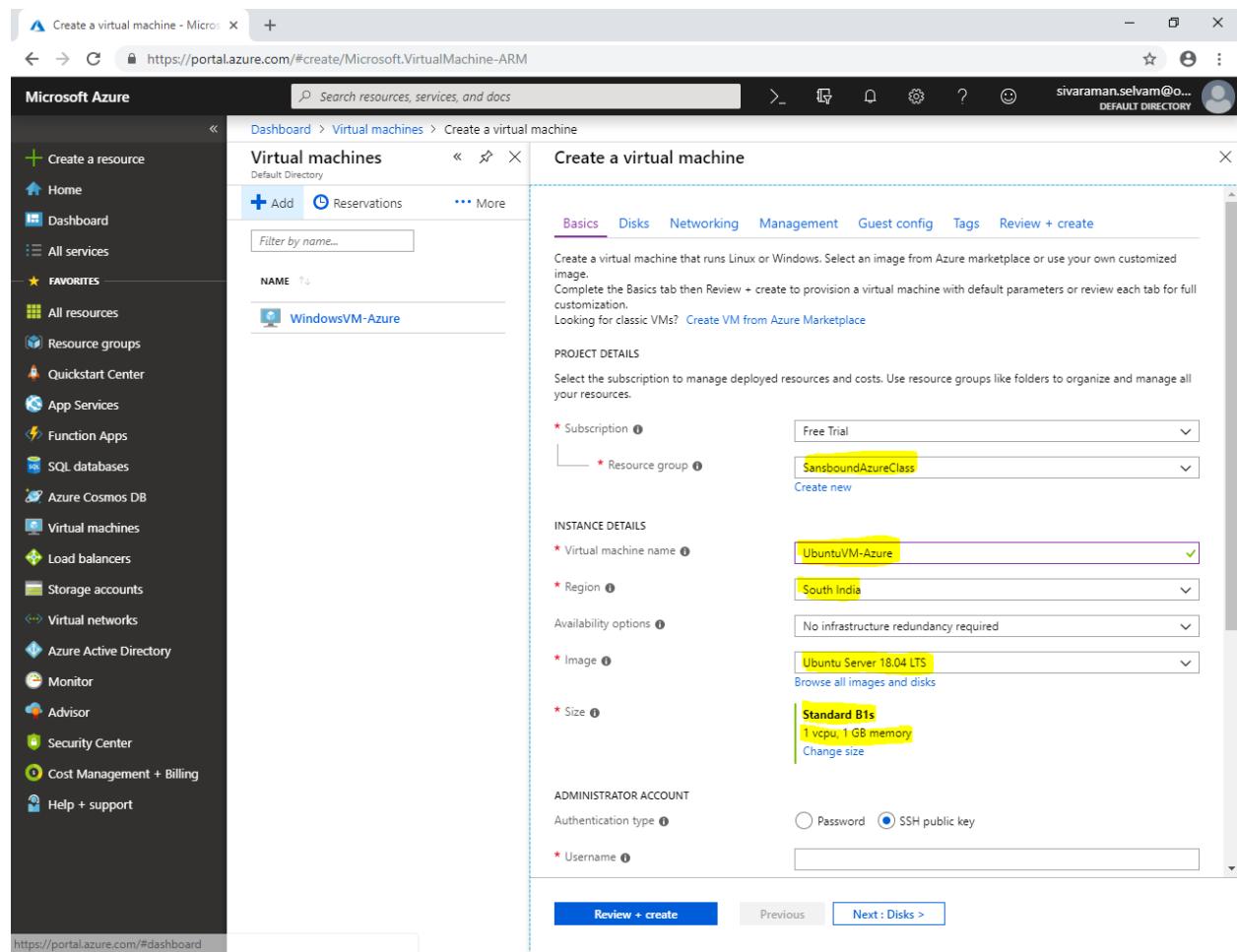
Select “**Resource Group**” as “**SansboundAzureClass**”.

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

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

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

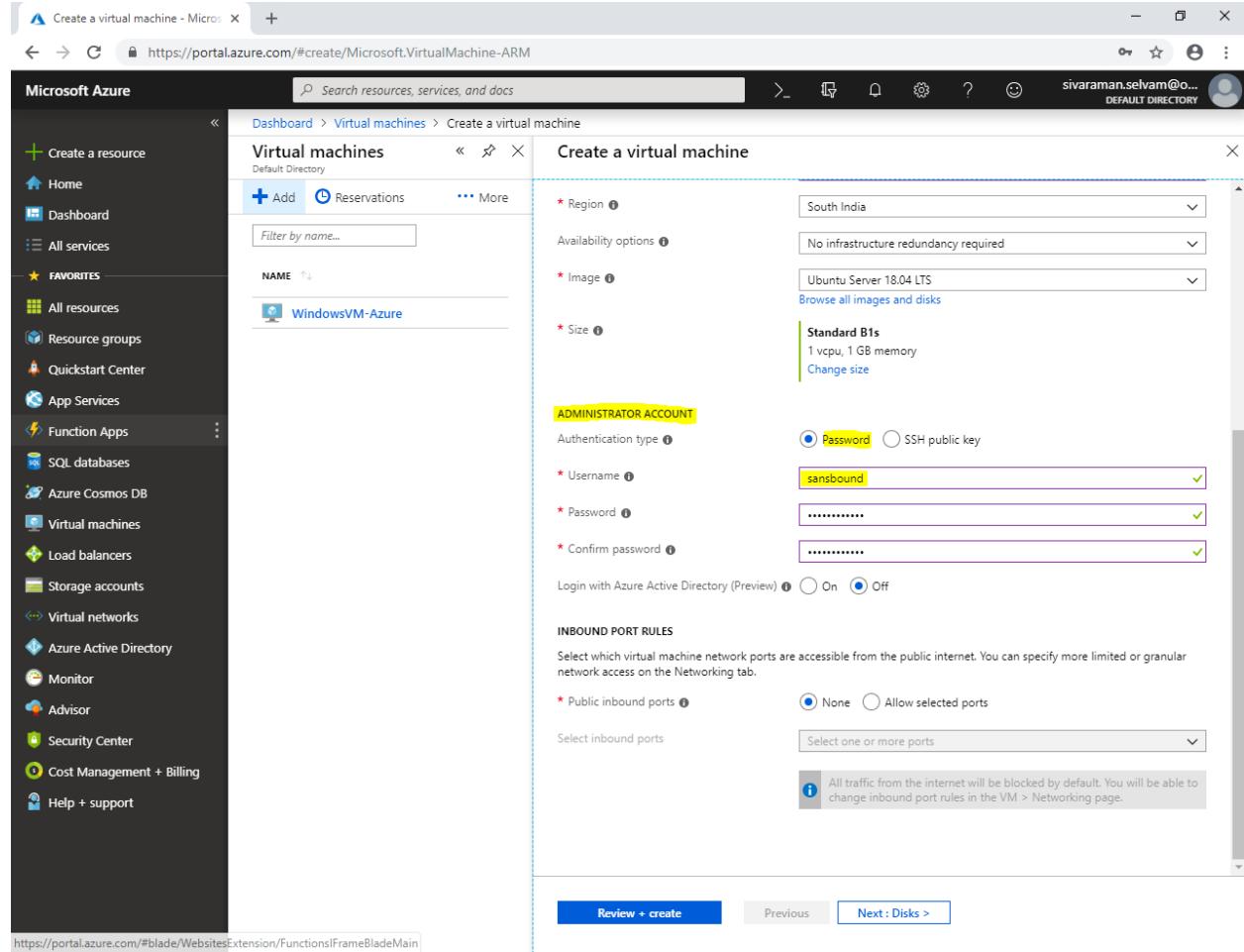
Change “**VM Size**” as “**Standard B1s**”.



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar lists various services under 'Favorites', including Home, Dashboard, All services, 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 shows the 'Virtual machines' section with a list of existing VMs and a 'Create a virtual machine' button. The 'Create a virtual machine' wizard is open, with the 'Basics' tab selected. The 'NAME' field contains 'WindowsVM-Azure'. The 'Region' field is set to 'South India'. The 'Image' field is set to 'Ubuntu Server 18.04 LTS'. The 'Size' field is set to 'Standard B1s'. The 'Resource group' dropdown is set to 'SansboundAzureClass'. Other tabs like Disks, Networking, Management, Guest config, Tags, and Review + create are visible. The URL in the browser is https://portal.azure.com/#create/Microsoft.VirtualMachine-ARM.

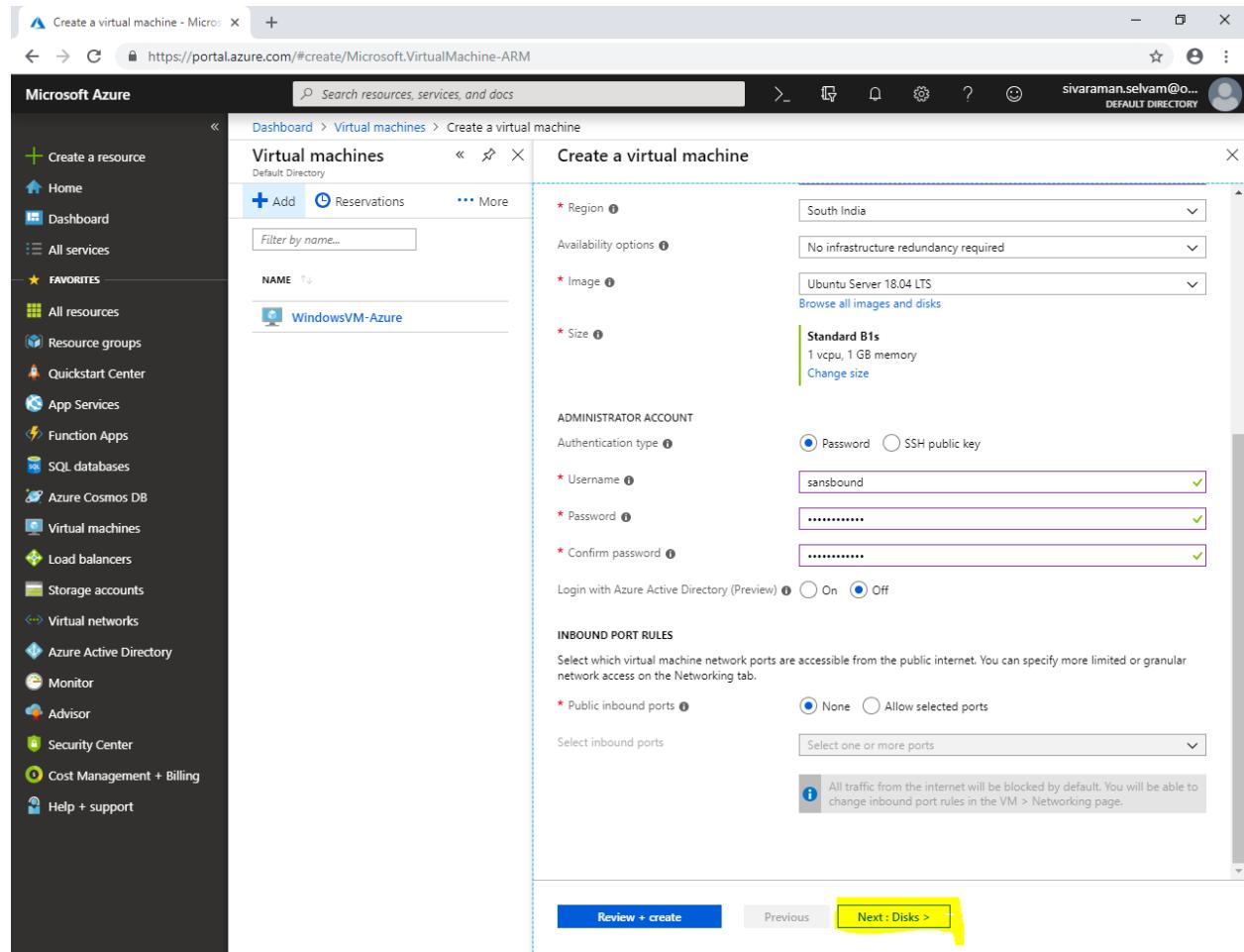
In “Administrator Account” set authentication type as “**Password**”.

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



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' dialog open. In the 'Create a virtual machine' dialog, the 'Administrator Account' section is highlighted with a yellow box. It shows the 'Authentication type' dropdown set to 'Password', with the value 'sansbound' entered in the 'Username' field. Other fields visible include 'Region' (South India), 'Image' (Ubuntu Server 18.04 LTS), and 'Size' (Standard B1s). The 'INBOUND PORT RULES' section is also partially visible at the bottom.

Click “Next : Disks>”.



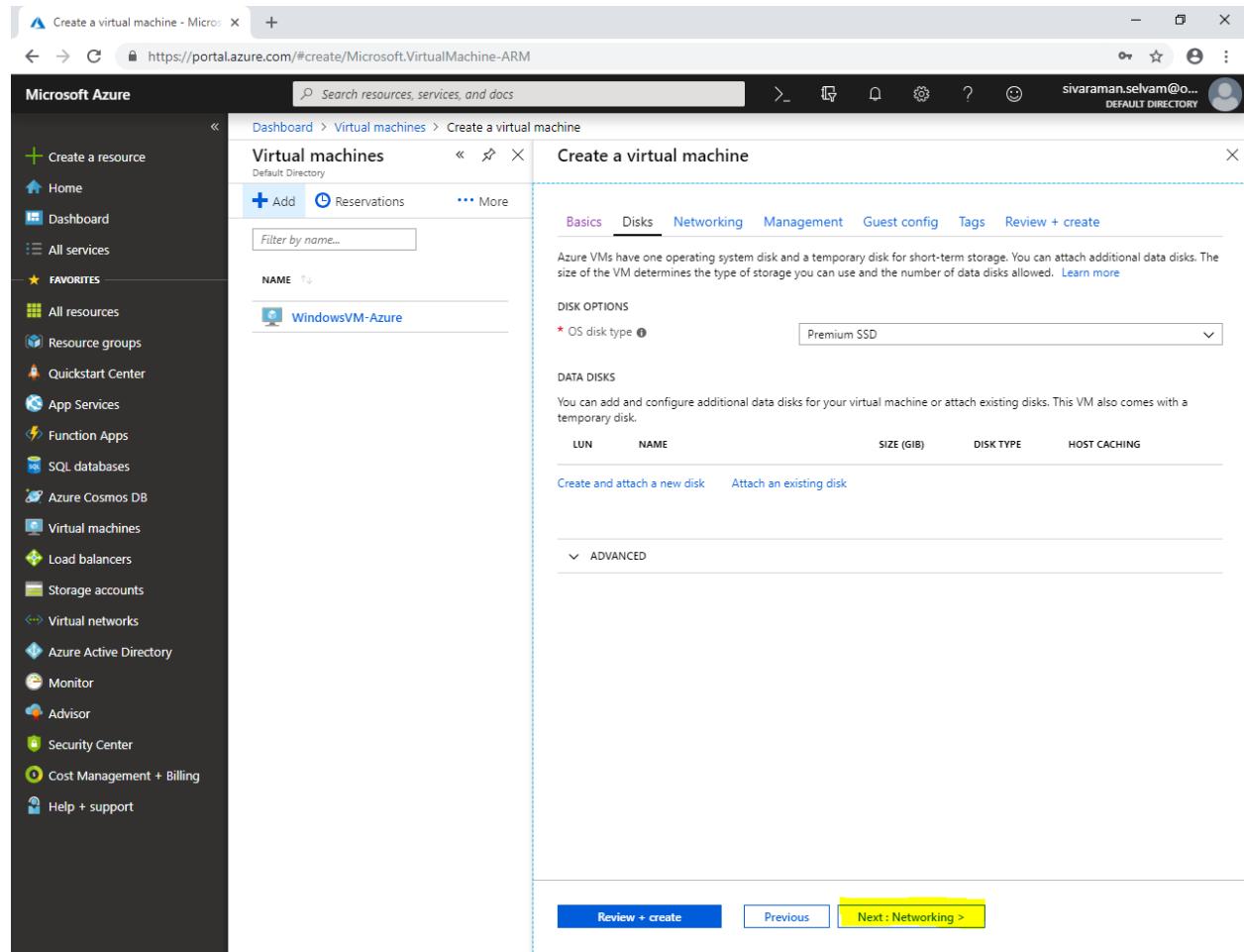
The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. On the left, the navigation menu is visible with various service icons. The main area displays the 'Virtual machines' blade under the 'Create a virtual machine' section. The 'Create a virtual machine' form is filled with the following details:

- 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)
- Administrator Account:**
 - Authentication type: Password (selected)
 - Username: sansbound
 - Password: [REDACTED]
 - Confirm password: [REDACTED]
- Inbound Port Rules:**
 - Public inbound ports: None (selected)
 - Select inbound ports: [Select one or more ports dropdown]
 - Note: 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 of the form, there are three buttons: 'Review + create', 'Previous', and 'Next : Disks >'. The 'Next : Disks >' button is highlighted with a yellow box.

In “Disks”

Click “Next : Networking >”.



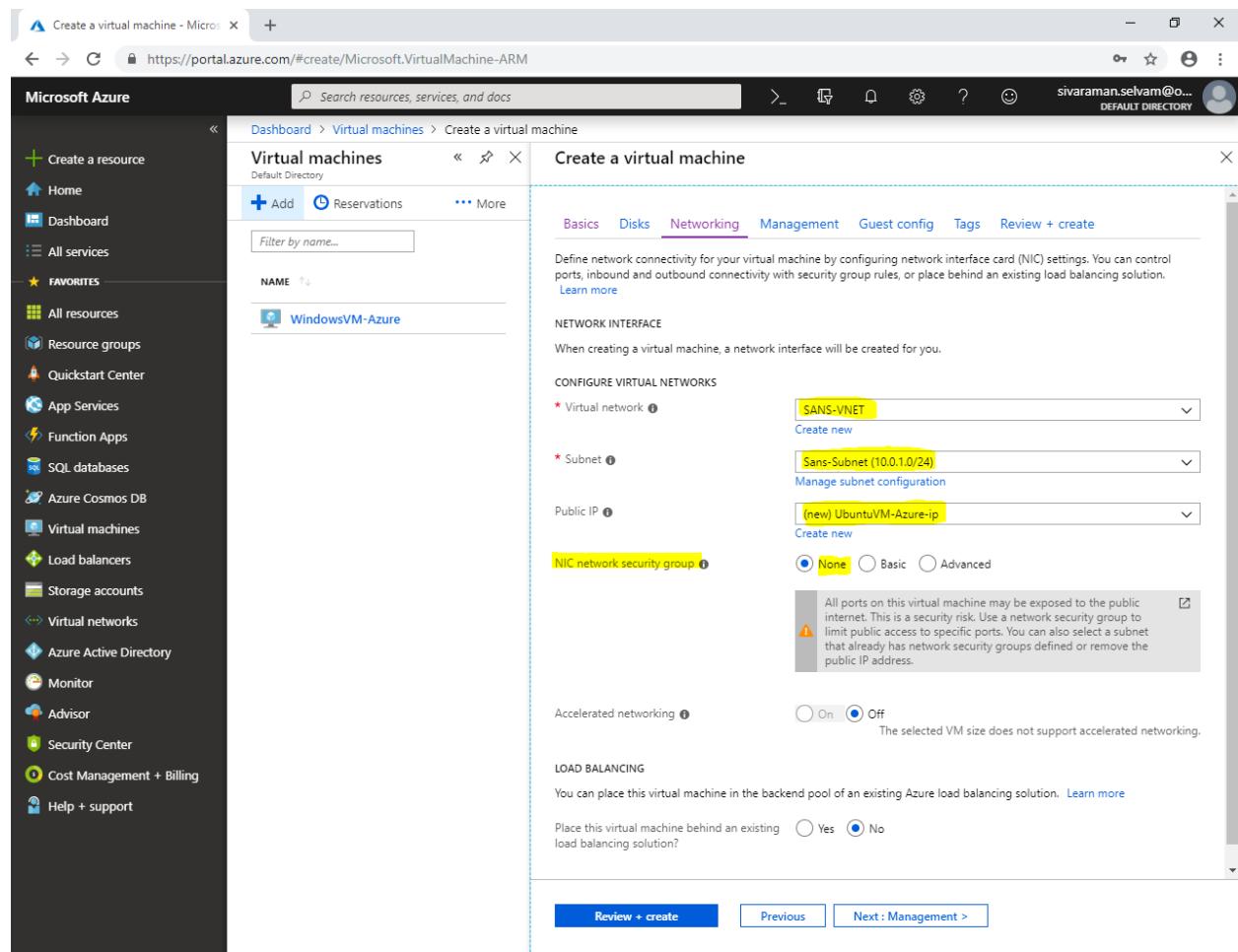
The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains various service icons under 'Virtual machines' and 'All services'. The main area shows a list of existing virtual machines, with one named 'WindowsVM-Azure' selected. A large central window is titled 'Create a virtual machine' and displays the configuration steps. The 'Disks' tab is currently active, showing options for the operating system disk (selected as 'Premium SSD') and data disks. Below this, there are buttons for 'Create and attach a new disk' and 'Attach an existing disk'. At the bottom of the window, there are three buttons: 'Review + create', 'Previous', and 'Next : Networking >'. The 'Next : Networking >' button is highlighted with a yellow box, indicating the next step in the process.

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

Subnet “**Sans-Subnet**”.

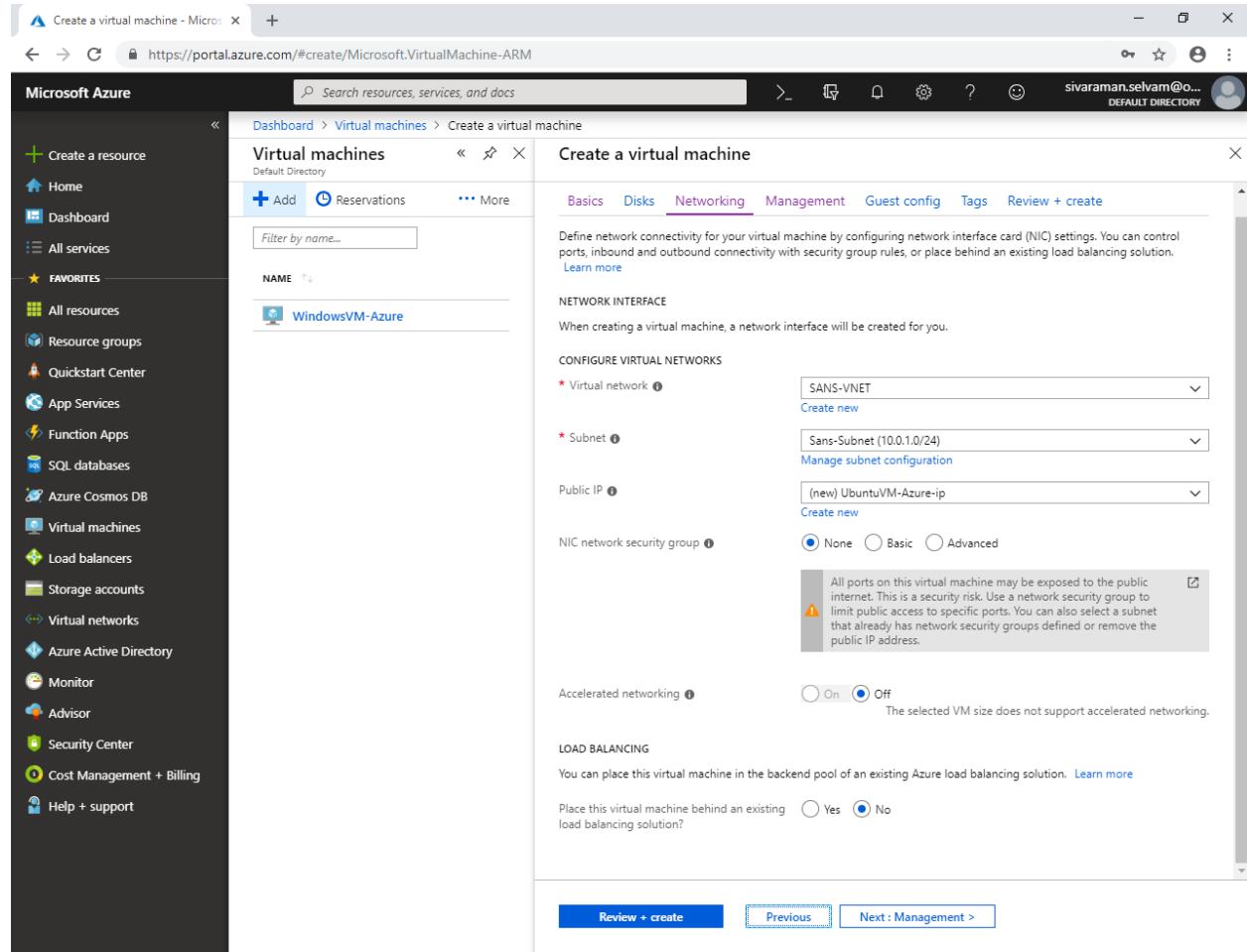
Public IP as new IP for Ubuntu VM

In Network Security Group click as “**None**”.



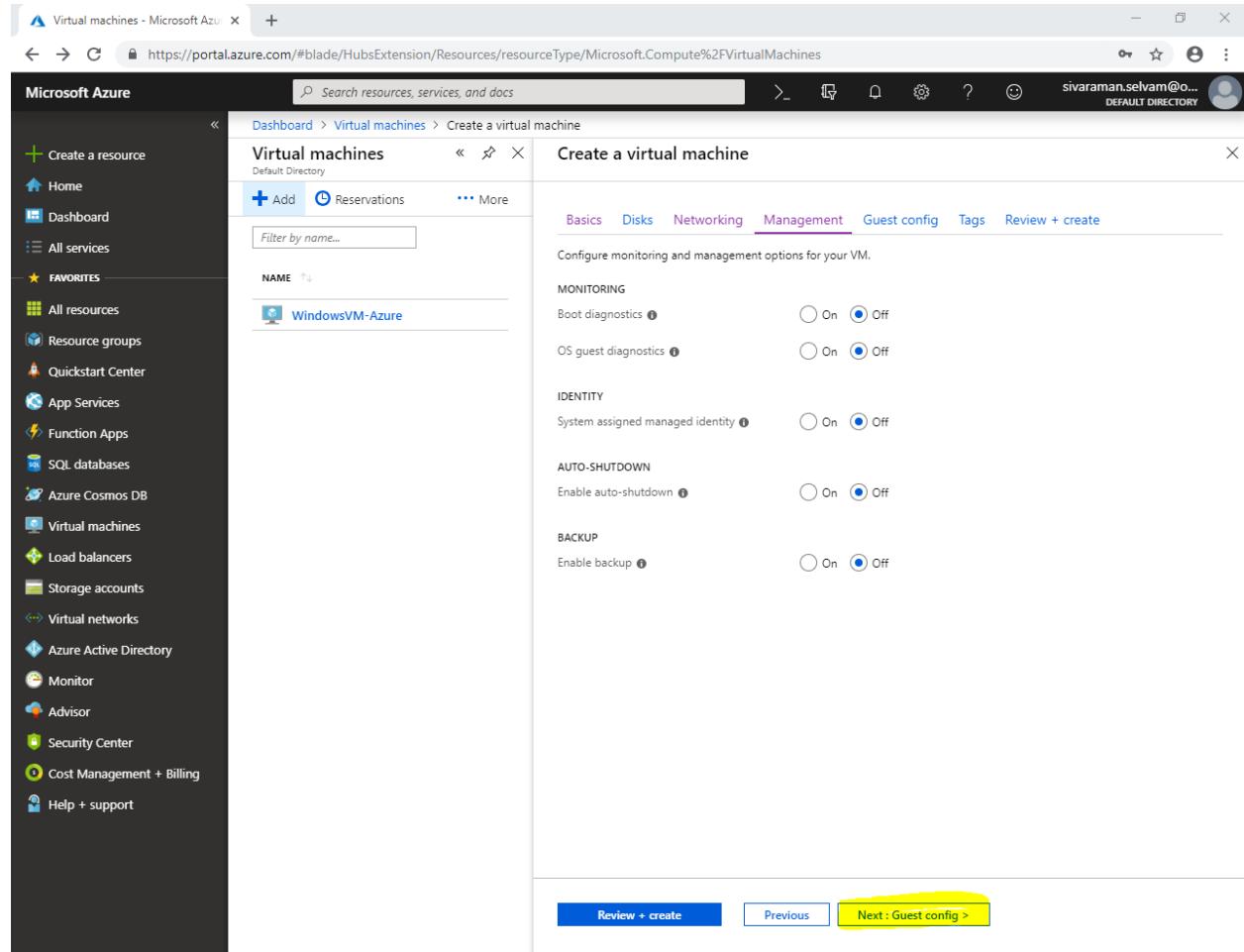
The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar lists various services like Home, Dashboard, All resources, and Virtual machines. The main window is titled 'Create a virtual machine' under the 'Virtual machines' section. The 'Networking' tab is active. In the 'CONFIGURE VIRTUAL NETWORKS' section, the 'Virtual network' dropdown is set to 'SANS-VNET' and the 'Subnet' dropdown is set to 'Sans-Subnet (10.0.1.0/24)'. Under 'Public IP', a new public IP address '(new) UbuntuVM-Azure-ip' is selected. In the 'NIC network security group' section, the 'None' radio button is selected. A warning message is displayed: '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.' Accelerated networking is turned off.

Click “Next : Management>”.



In “Management”

Click “Next : Guest config >”.



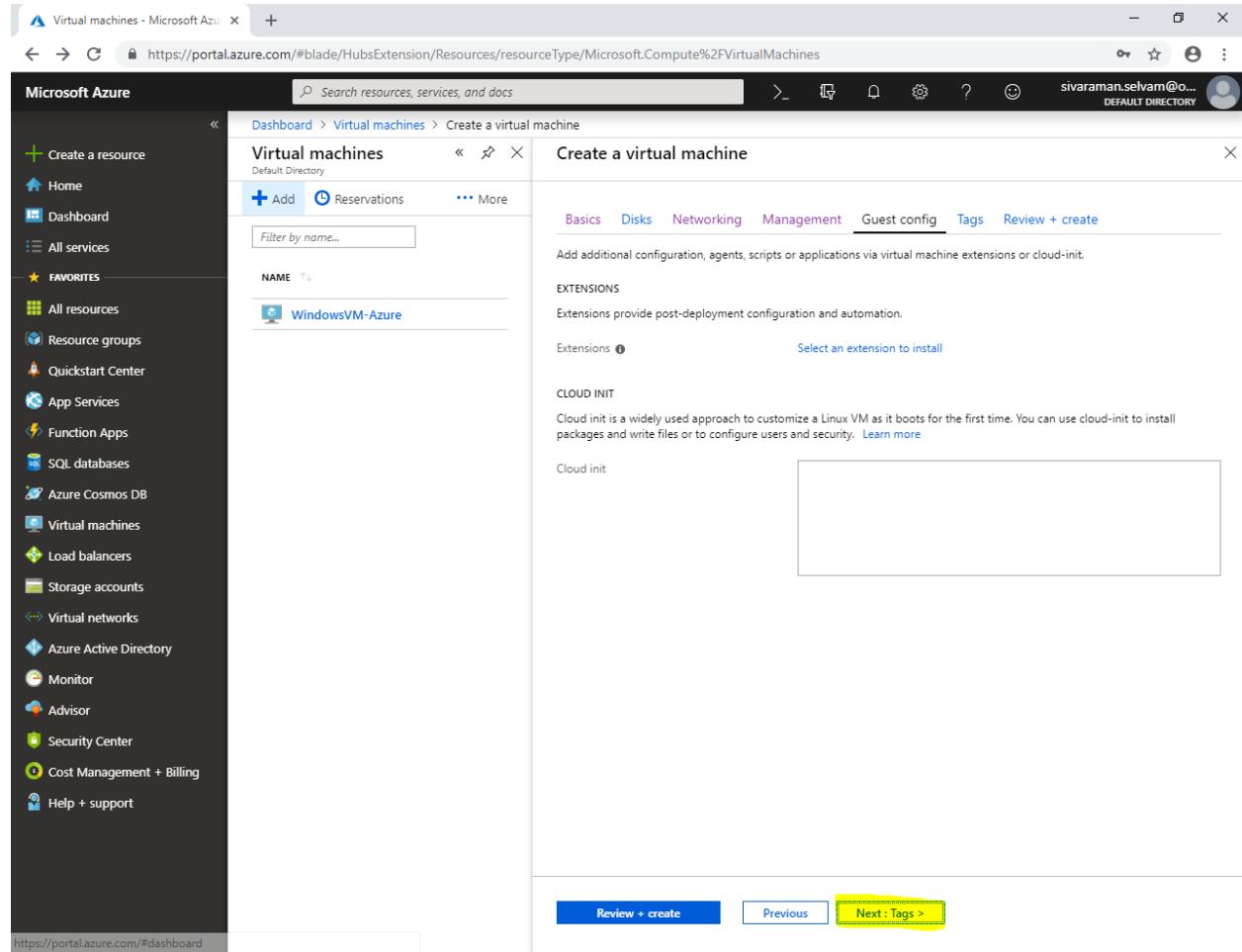
The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar lists various services like Home, Dashboard, and Virtual machines. The main area shows the 'Virtual machines' blade with a 'Create a virtual machine' wizard. The 'Management' tab is currently selected. On this tab, several options are available:

- MONITORING:** Boot diagnostics (On) and OS guest diagnostics (Off).
- IDENTITY:** System assigned managed identity (Off).
- AUTO-SHUTDOWN:** Enable auto-shutdown (Off).
- BACKUP:** Enable backup (Off).

At the bottom of the blade, there are three buttons: 'Review + create' (blue), 'Previous' (light blue), and 'Next : Guest config >' (yellow, indicating it is the current step). The URL in the browser bar is <https://portal.azure.com/#blade/HubsExtension/Resources/resourceType/Microsoft.Compute%2FVirtualMachines>.

In “Guest config”.

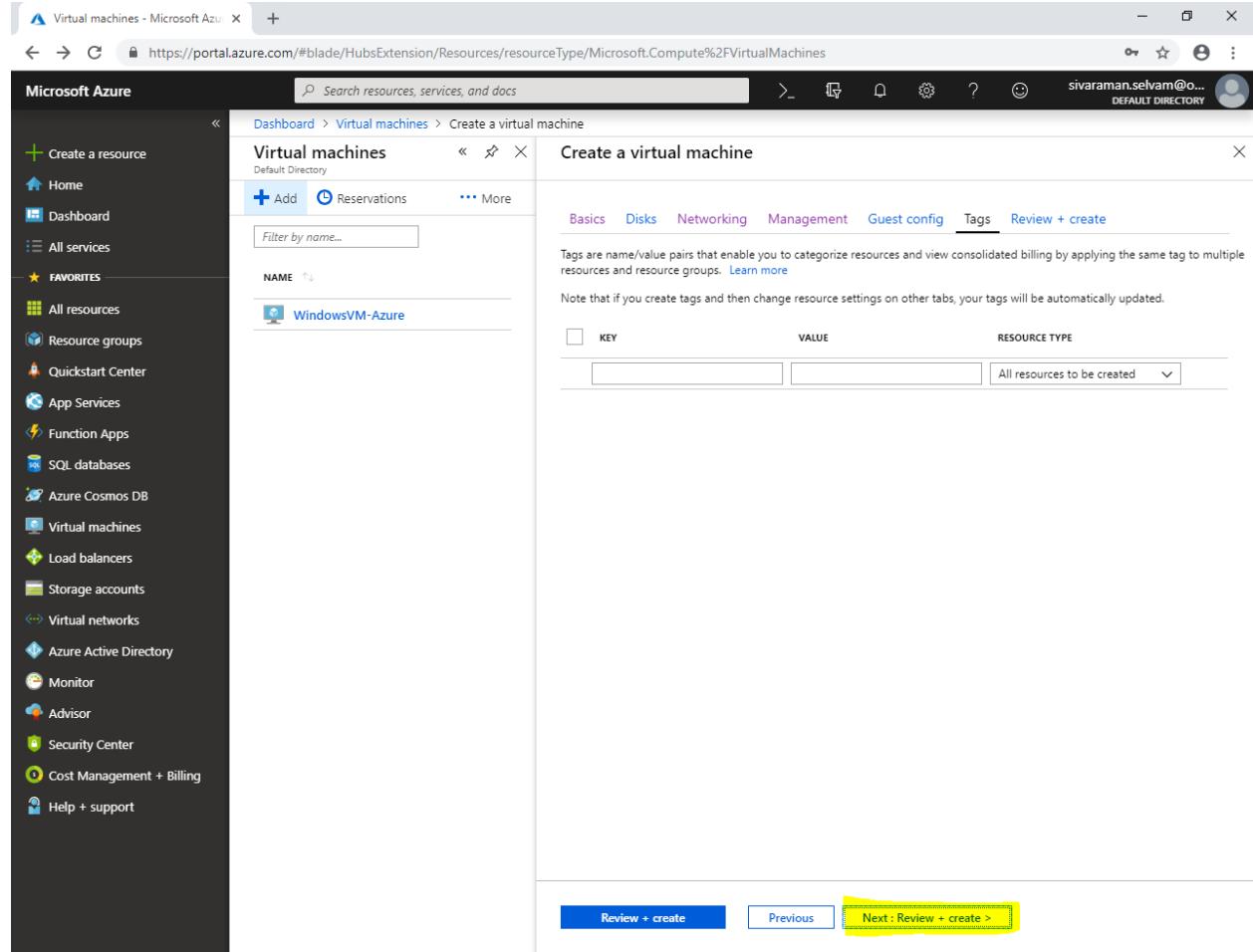
Click “**Next : Tags>**”.



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 'Create a virtual machine' under 'Virtual machines'. The 'Guest config' tab is currently selected. Below it, there's a section for adding extensions and cloud-init configurations. At the bottom of the page, there are three buttons: 'Review + create', 'Previous', and 'Next : Tags >'. The 'Next : Tags >' button is highlighted with a yellow box.

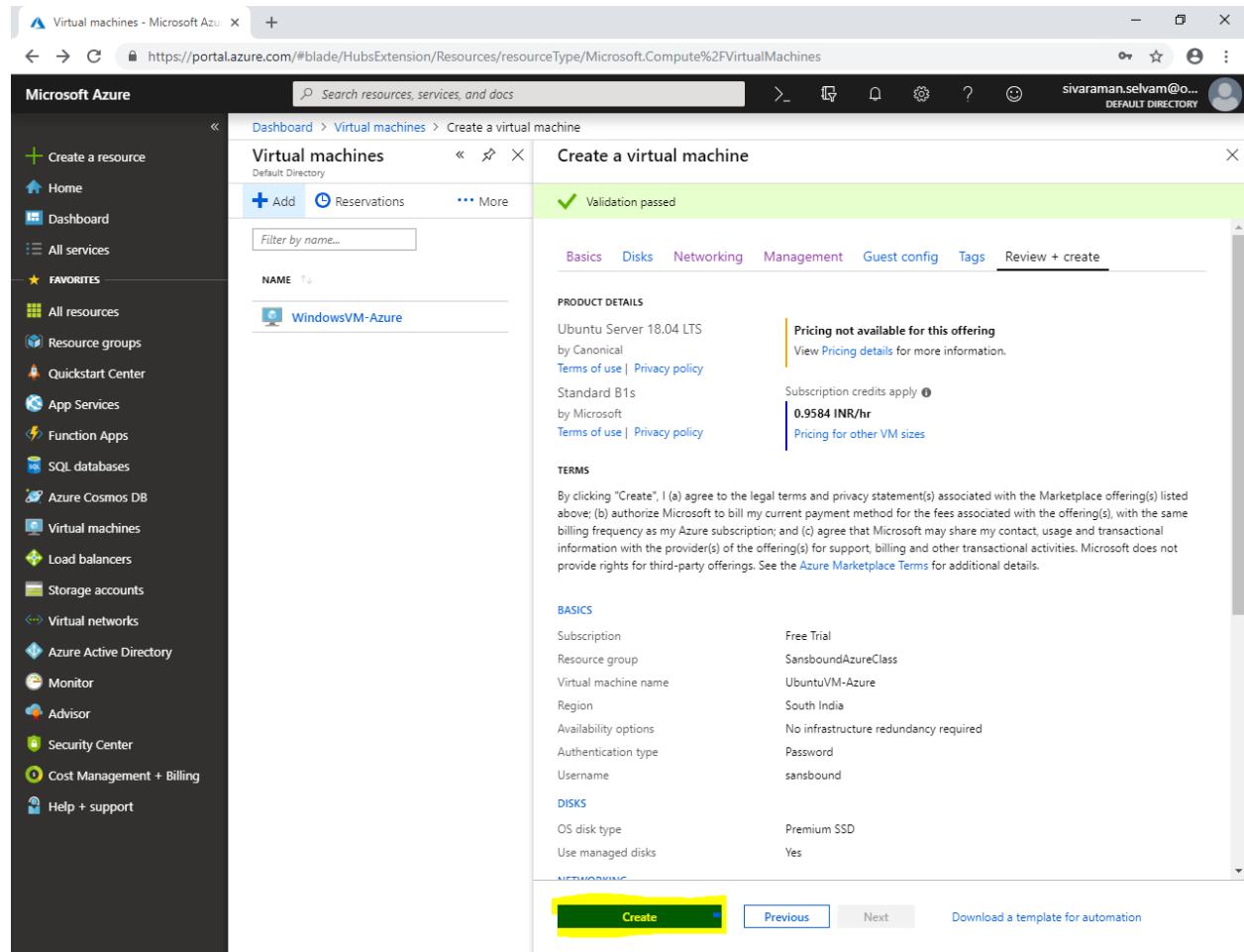
Click "Tags".

Click "Next : Review + Create".



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. On the left, the navigation menu is visible with various service icons. The main workspace is titled 'Create a virtual machine' under 'Virtual machines'. The 'Tags' tab is currently selected, showing a table where a single tag 'WindowsVM-Azure' is listed. The 'Review + create' button at the bottom is highlighted with a yellow box.

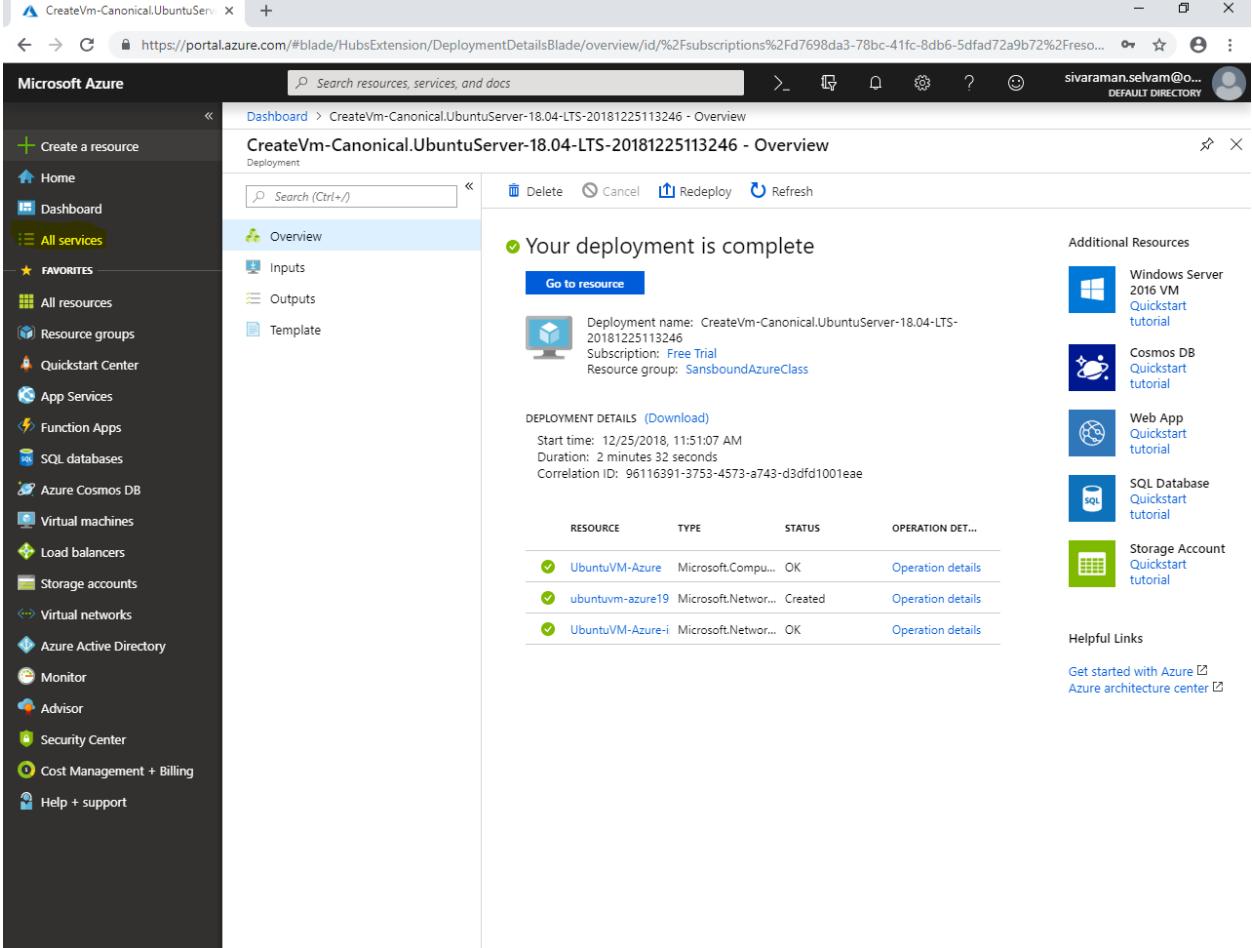
Click “Create”.



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 (Virtual machines, 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), and Create a resource. The main content area is titled 'Create a virtual machine' under 'Virtual machines'. A green validation message 'Validation passed' is displayed. The 'Basics' tab is selected, showing product details for 'Ubuntu Server 18.04 LTS' by Canonical. It includes terms of use, pricing information (0.9584 INR/hr), and subscription credits apply. The 'TERMS' section contains legal text about agreeing to terms and privacy statements. The 'BASICS' section lists configuration options: Subscription (Free Trial), Resource group (SansboundAzureClass), Virtual machine name (UbuntuVM-Azure), Region (South India), Availability options (No infrastructure redundancy required), Authentication type (Password), Username (sansbound). The 'DISKS' section shows OS disk type (Premium SSD) and Use managed disks (Yes). The 'NETWORKING' section is partially visible. At the bottom, there are 'Create' (highlighted in yellow), 'Previous', 'Next', and 'Download a template for automation' buttons.

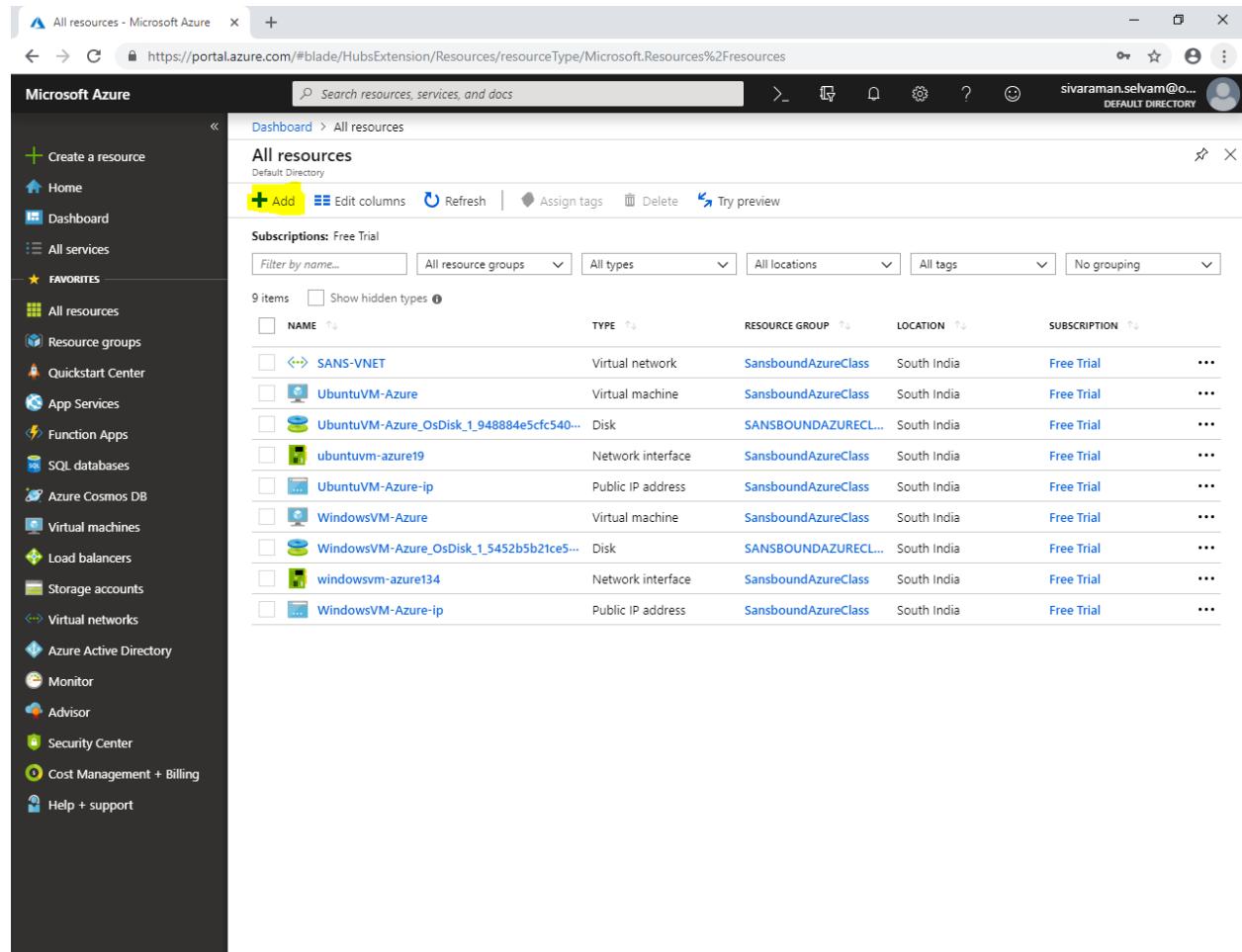
You have successfully deployed.

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



The screenshot shows the Microsoft Azure portal interface. The left sidebar is titled "Microsoft Azure" and includes a "Create a resource" button, "Home", "Dashboard", and a "All services" button which is highlighted. Below these are sections for "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). The main content area is titled "CreateVm-Canonical.UbuntuServer-18.04-LTS-20181225113246 - Overview". It displays a message "Your deployment is complete" with a "Go to resource" button. Below this, it shows deployment details: Deployment name: CreateVm-Canonical.UbuntuServer-18.04-LTS-20181225113246, Subscription: Free Trial, Resource group: SansboundAzureClass. It also lists DEPLOYMENT DETAILS with start time (12/25/2018, 11:51:07 AM), duration (2 minutes 32 seconds), and correlation ID (96116391-3753-4573-a743-d3dfd1001eae). A table lists three resources: UbuntuVM-Azure (Microsoft.Compu... OK), ubuntuvm-azure19 (Microsoft.Networ... Created), and UbuntuVM-Azure-i (Microsoft.Networ... OK). 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).

In “All resources” click “Add”.

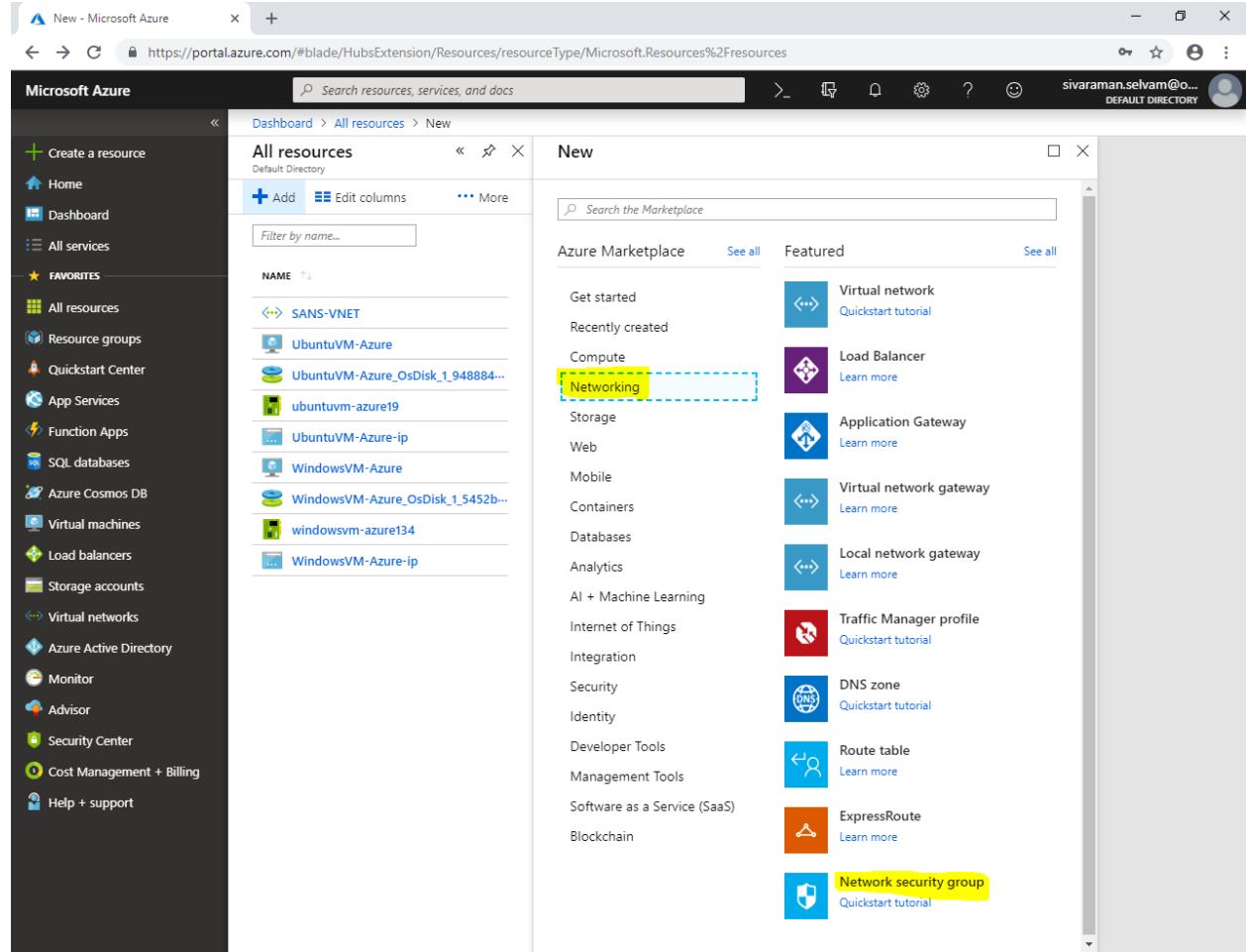


The screenshot shows the Microsoft Azure portal interface. The left sidebar is collapsed, showing a list of services under 'FAVORITES'. The main area is titled 'All resources' and shows a table of resources. The 'Add' button at the top left of the resource list is highlighted with a yellow box. The table columns are: NAME, TYPE, RESOURCE GROUP, LOCATION, and SUBSCRIPTION. The resources listed are:

NAME	TYPE	RESOURCE GROUP	LOCATION	SUBSCRIPTION
SANS-VNET	Virtual network	SansboundAzureClass	South India	Free Trial
UbuntuVM-Azure	Virtual machine	SansboundAzureClass	South India	Free Trial
UbuntuVM-Azure_OsDisk_1_948884e5fc540...	Disk	SANBOUNDAZURECL...	South India	Free Trial
ubuntuvm-azure19	Network interface	SansboundAzureClass	South India	Free Trial
UbuntuVM-Azure-ip	Public IP address	SansboundAzureClass	South India	Free Trial
WindowsVM-Azure	Virtual machine	SansboundAzureClass	South India	Free Trial
WindowsVM-Azure_OsDisk_1_5452b5b21ce5...	Disk	SANBOUNDAZURECL...	South India	Free Trial
windowsvm-azure134	Network interface	SansboundAzureClass	South India	Free Trial
WindowsVM-Azure-ip	Public IP address	SansboundAzureClass	South India	Free Trial

In “Azure Marketplace”

Click “Networking” → “Network Security Group”



The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons and a 'FAVORITES' section. The main area shows a list of resources under 'All resources'. On the right, a 'New' blade is open, featuring a search bar and a 'Featured' section. The 'Networking' category is highlighted with a yellow box, and the 'Network security group' item within it is also highlighted with a yellow box.

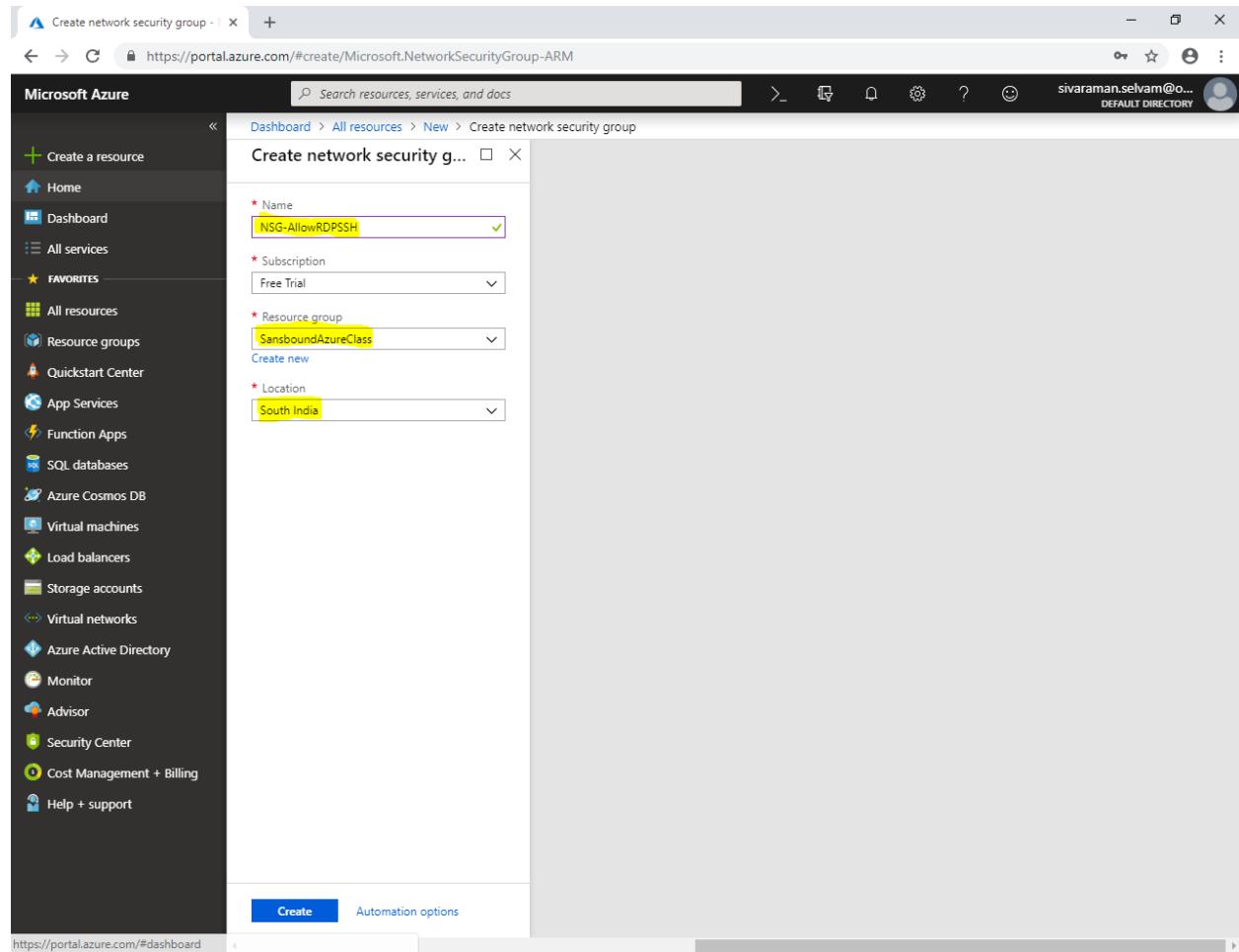
Azure Marketplace Category	Service	Description
Compute	Virtual network	Quickstart tutorial
Compute	Load Balancer	Learn more
Storage	Application Gateway	Learn more
Web	Virtual network gateway	Learn more
Mobile	Local network gateway	Learn more
Containers	Traffic Manager profile	Quickstart tutorial
Databases	DNS zone	Quickstart tutorial
Analytics	Route table	Learn more
AI + Machine Learning	ExpressRoute	Learn more
Internet of Things	Network security group	Quickstart tutorial
Integration		
Security		
Identity		
Developer Tools		
Management Tools		
Software as a Service (SaaS)		
Blockchain		

While creating “**Network Security Group**”

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

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

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

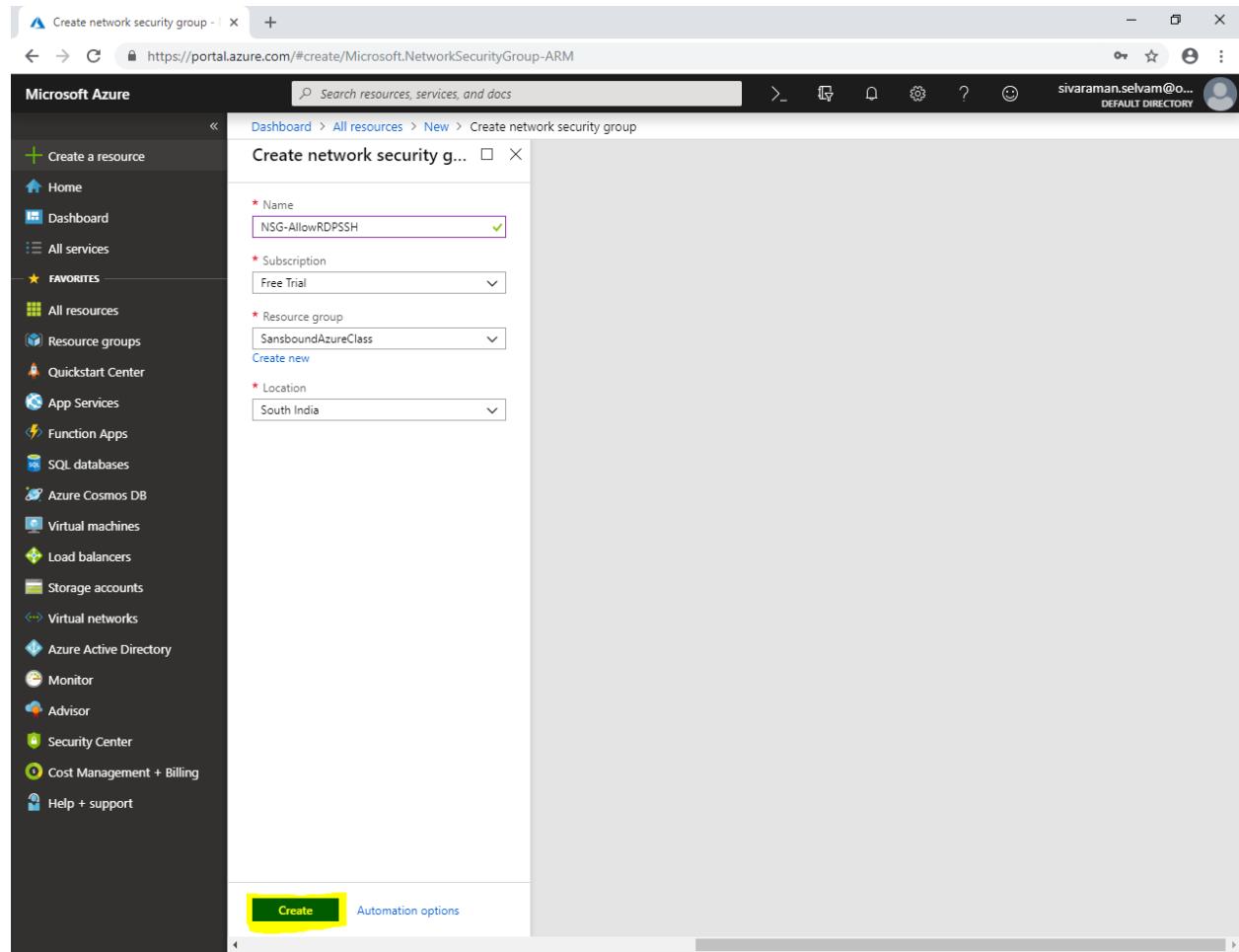


The screenshot shows the Microsoft Azure portal interface for creating a new Network Security Group (NSG). The left sidebar lists various services like Home, Dashboard, Resource groups, and Virtual machines. The main area is titled 'Create network security g...'. The configuration fields are as follows:

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

At the bottom of the form are two buttons: 'Create' (highlighted in blue) and 'Automation options'.

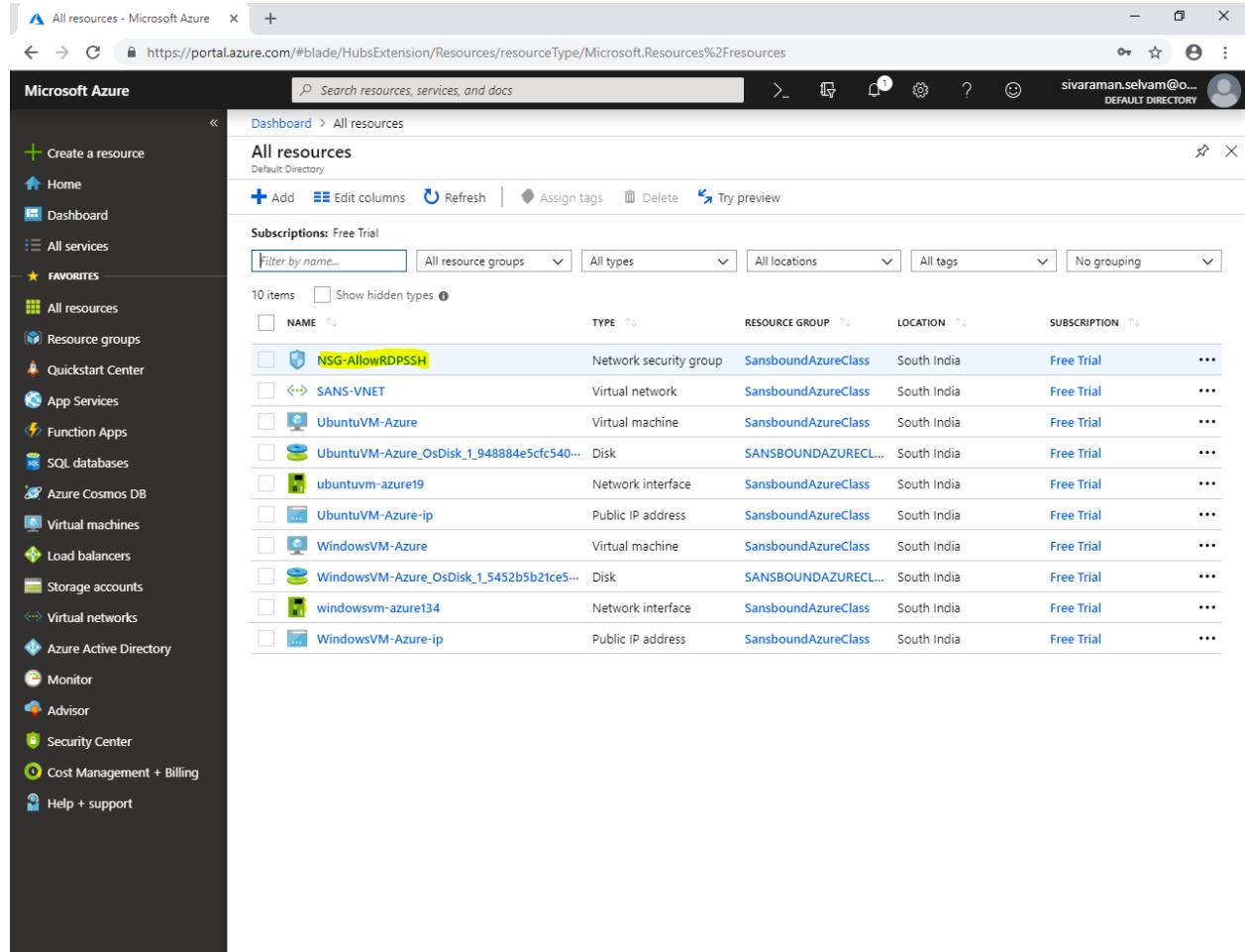
Click “Create”.



In “All resources”.

You are able to see the Network Security group.

Click “**NSG-AllowRDPSSH**”.



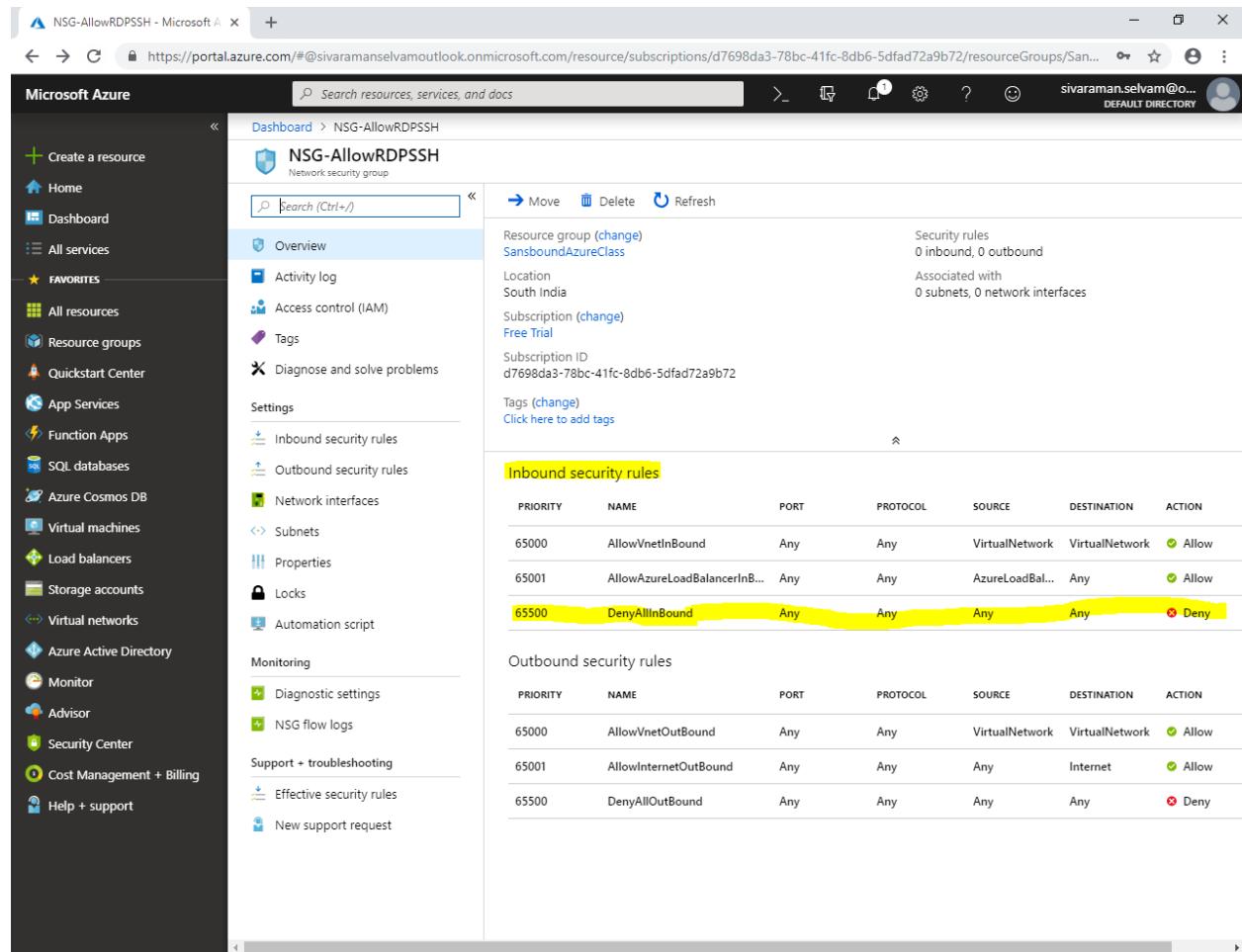
The screenshot shows the Microsoft Azure portal interface. The left sidebar has a dark theme with various service icons and links like Home, Dashboard, and Favorites. The Favorites section includes All services, All resources, Resource groups, Quickstart Center, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Billing, Help + support, and a plus icon for Create a resource. The main content area is titled "All resources" under "Default Directory". It shows a list of 10 items with columns: NAME, TYPE, RESOURCE GROUP, LOCATION, and SUBSCRIPTION. The first item in the list is "NSG-AllowRDPSSH", which is highlighted in yellow. Other items include SANS-VNET (Virtual network), UbuntuVM-Azure (Virtual machine), UbuntuVM-Azure_OsDisk_1_948884e5fc540... (Disk), ubuntuvm-azure19 (Network interface), UbuntuVM-Azure-ip (Public IP address), WindowsVM-Azure (Virtual machine), WindowsVM-Azure_OsDisk_1_5452b5b21ce5... (Disk), windowsvm-azure134 (Network interface), and WindowsVM-Azure-ip (Public IP address). Each item has a checkbox, a three-dot ellipsis menu, and a small icon representing its type.

NAME	TYPE	RESOURCE GROUP	LOCATION	SUBSCRIPTION
NSG-AllowRDPSSH	Network security group	SansboundAzureClass	South India	Free Trial
SANS-VNET	Virtual network	SansboundAzureClass	South India	Free Trial
UbuntuVM-Azure	Virtual machine	SansboundAzureClass	South India	Free Trial
UbuntuVM-Azure_OsDisk_1_948884e5fc540...	Disk	SANBOUNDAZURECL...	South India	Free Trial
ubuntuvm-azure19	Network interface	SansboundAzureClass	South India	Free Trial
UbuntuVM-Azure-ip	Public IP address	SansboundAzureClass	South India	Free Trial
WindowsVM-Azure	Virtual machine	SansboundAzureClass	South India	Free Trial
WindowsVM-Azure_OsDisk_1_5452b5b21ce5...	Disk	SANBOUNDAZURECL...	South India	Free Trial
windowsvm-azure134	Network interface	SansboundAzureClass	South India	Free Trial
WindowsVM-Azure-ip	Public IP address	SansboundAzureClass	South India	Free Trial

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.



NSG-AllowRDPSSH

Inbound security rules

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

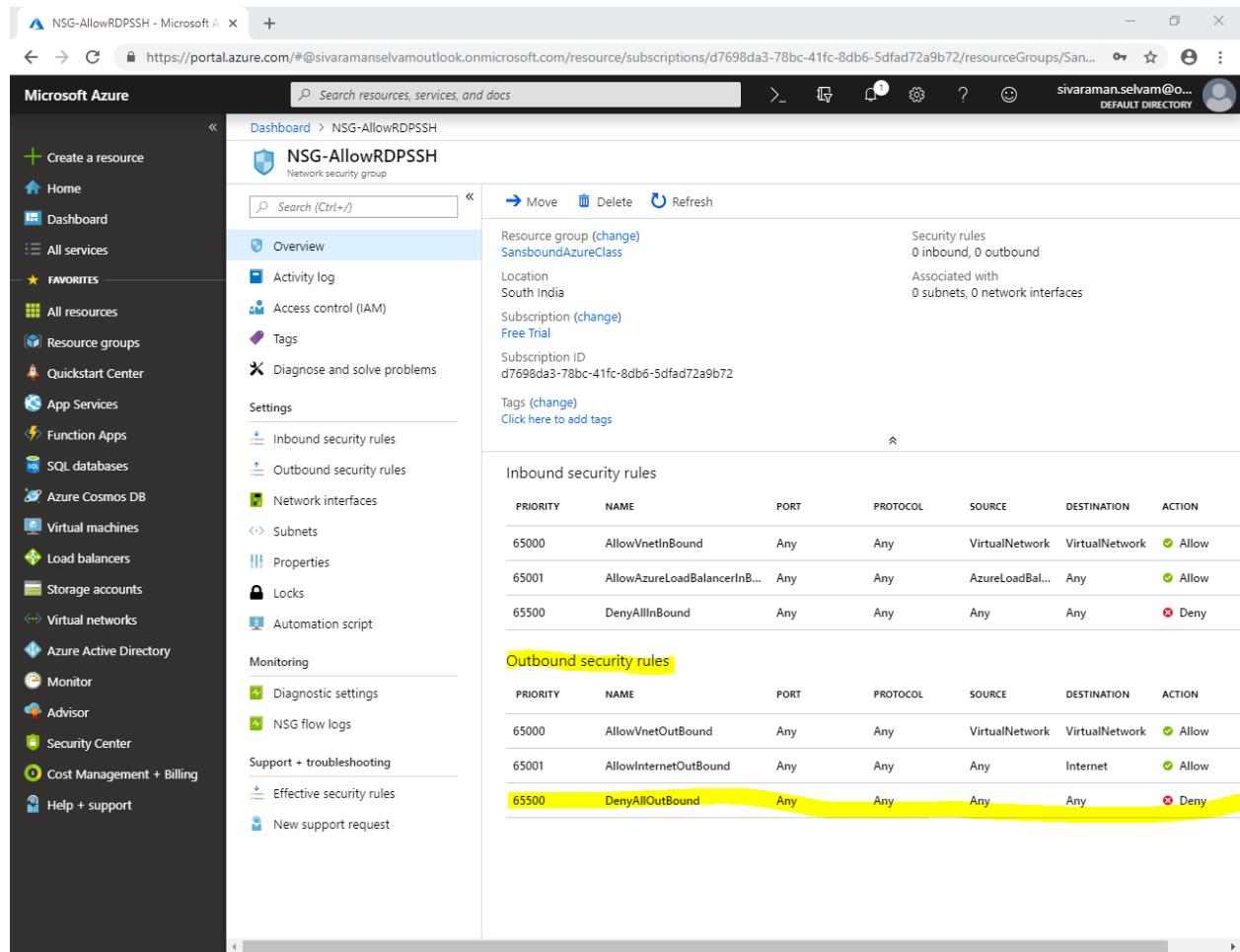
Outbound security rules

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

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.

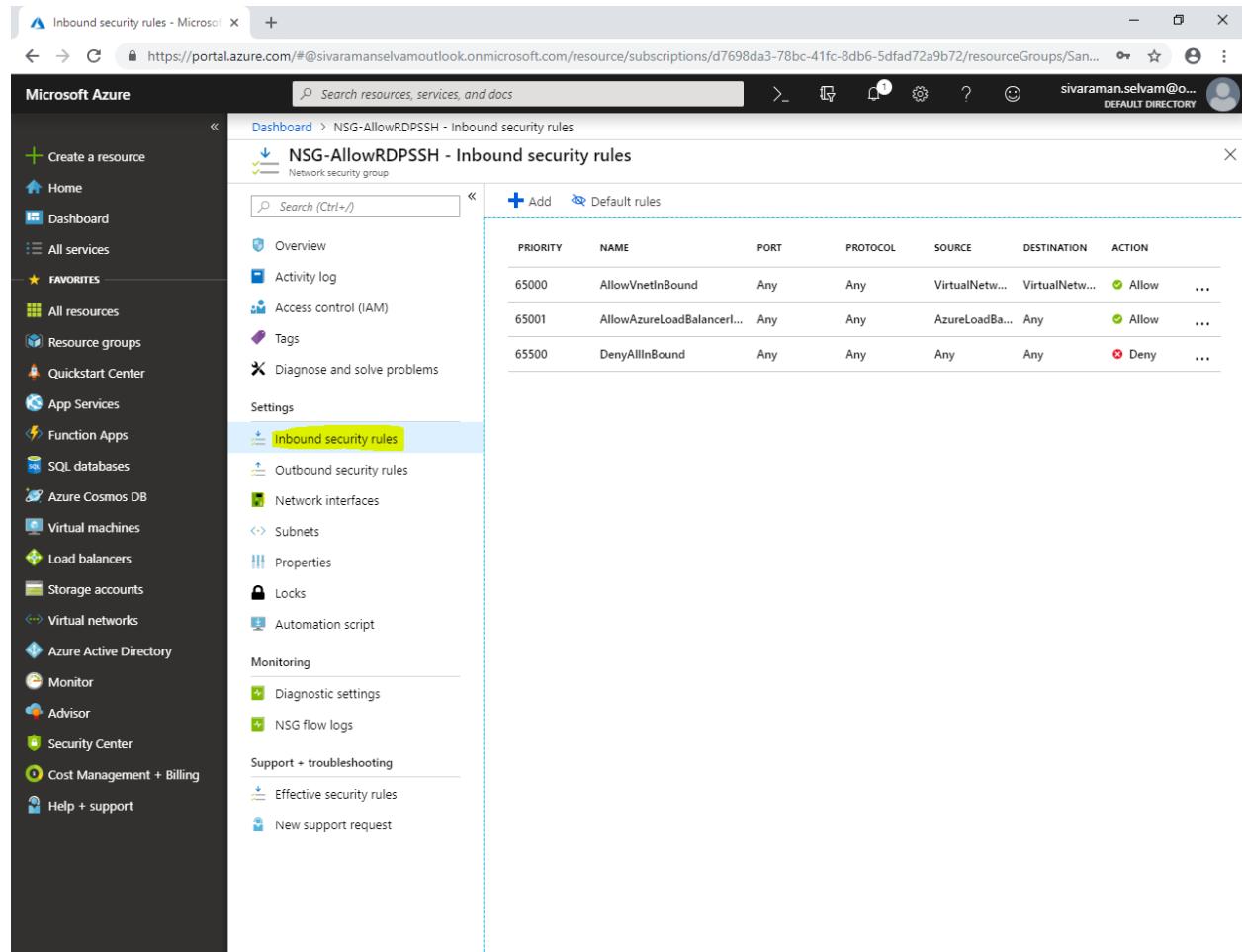


The screenshot shows the Azure portal interface for managing a Network Security Group (NSG). The left sidebar lists various Azure services. The main content area is titled "NSG-AllowRDPSSH" and displays the "Overview" tab. It shows basic information about the resource group, location (South India), and subscription. Under the "Settings" section, the "Outbound security rules" table is highlighted with a yellow box. This table lists three rules:

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

The "Outbound security rules" table also contains three rules:

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

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.

The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation bar 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. Under the Favorites section, 'Inbound security rules' is highlighted. The main content area displays the 'NSG-AllowRDPSSH - Inbound security rules' page. The left sidebar under 'NSG-AllowRDPSSH' lists 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), and Support + troubleshooting (Effective security rules, New support request). The right pane shows a table of inbound security rules:

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

While creating inbound security rule

Source : Any

Source port ranges : *

Destination : Any

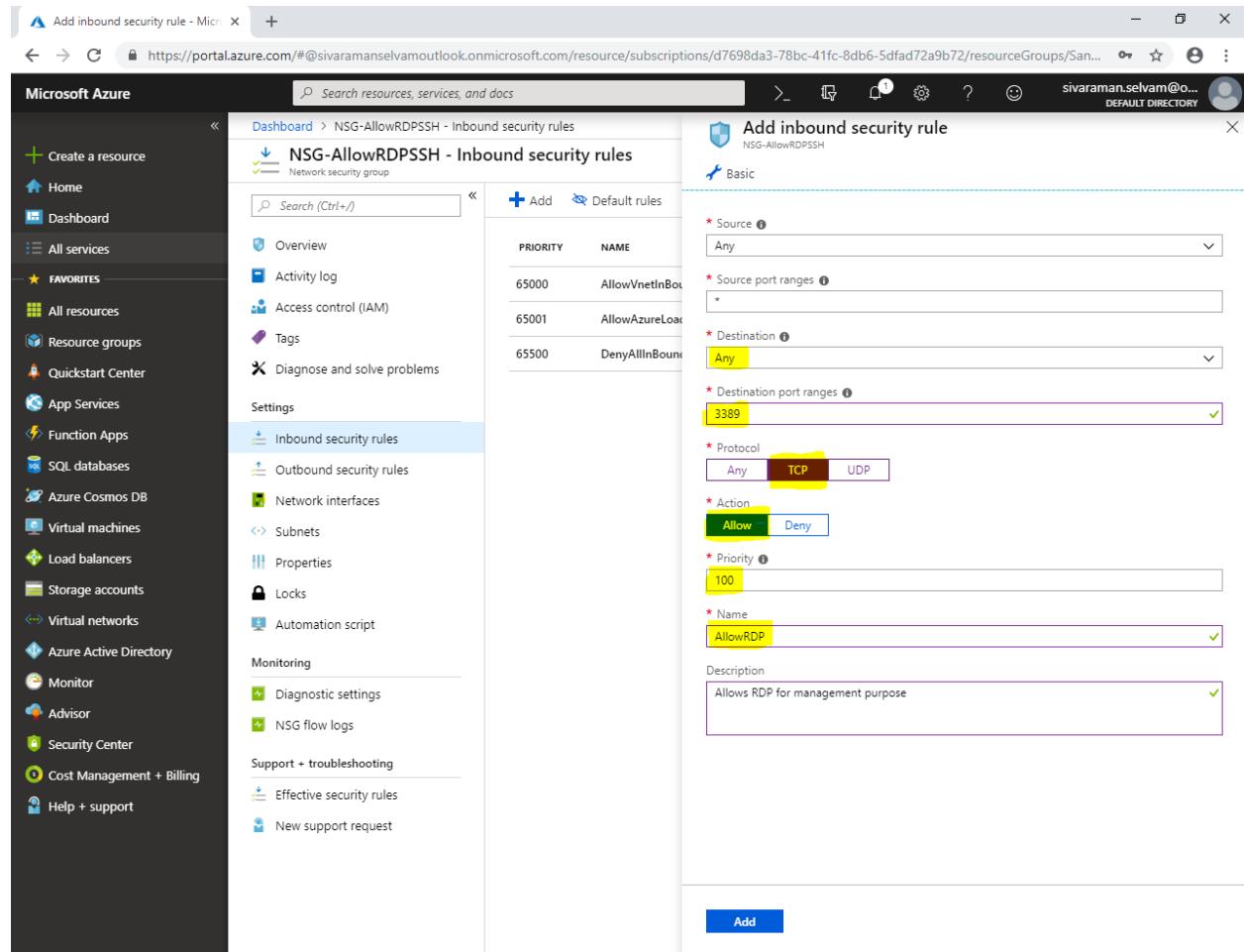
Destination port ranges : 3389

Protocol : TCP

Action : Allow

Priority : 100

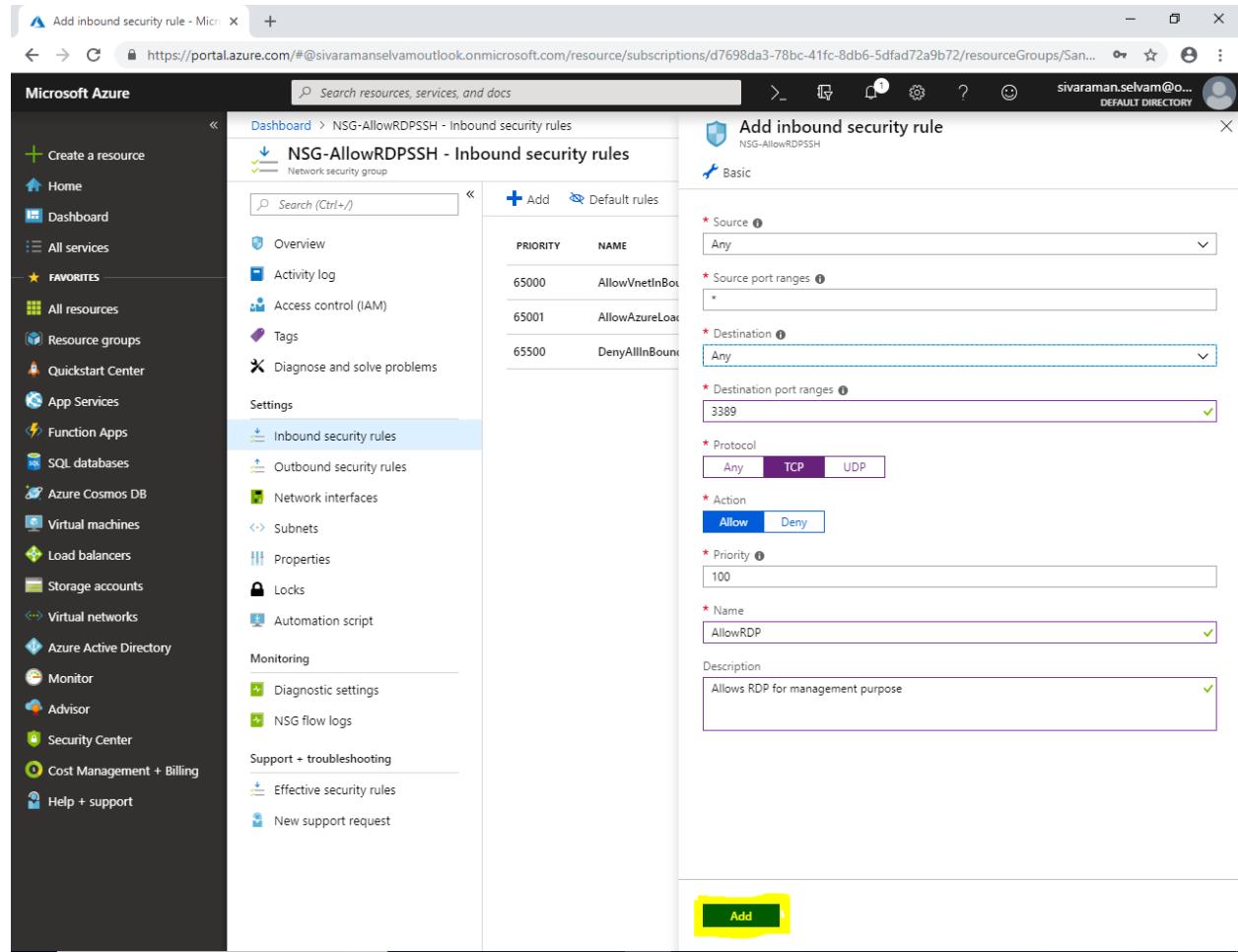
Name : AllowRDP :



The screenshot shows the Microsoft Azure portal interface for creating an inbound security rule. The left sidebar navigation includes '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 content area shows the 'NSG-AllowRDPSSH - Inbound security rules' section under 'NSG-AllowRDPSSH'. The 'Basic' tab is selected, displaying the following configuration:

- Source:** Any
- Source port ranges:** *
- Destination:** Any
- Destination port ranges:** 3389
- Protocol:** TCP
- Action:** Allow
- Priority:** 100
- Name:** AllowRDP
- Description:** Allows RDP for management purpose

Click “Add”.

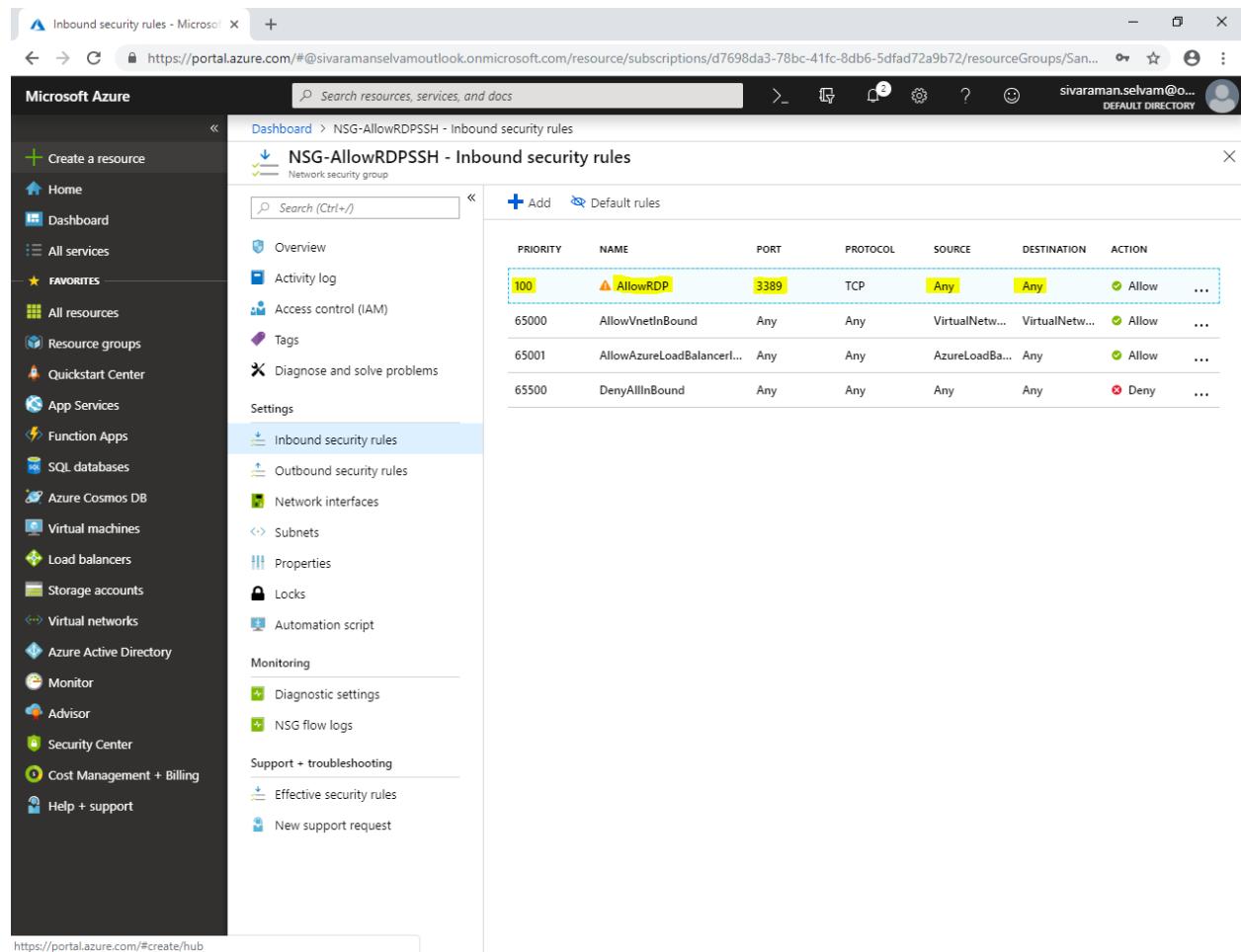


The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu is visible with various service icons. The main area displays the 'NSG-AllowRDPSSH - Inbound security rules' page under the 'Network security group' section. A search bar at the top right is present. The right side of the screen shows the 'Add inbound security rule' dialog box. The 'Basic' tab is selected. The configuration fields are as follows:

- Source:** Any
- Source port ranges:** *
- Destination:** Any
- Destination port ranges:** 3389
- Protocol:** TCP
- Action:** Allow
- Priority:** 100
- Name:** AllowRDP
- Description:** Allows RDP for management purpose

A yellow box highlights the 'Add' button at the bottom of the dialog box.

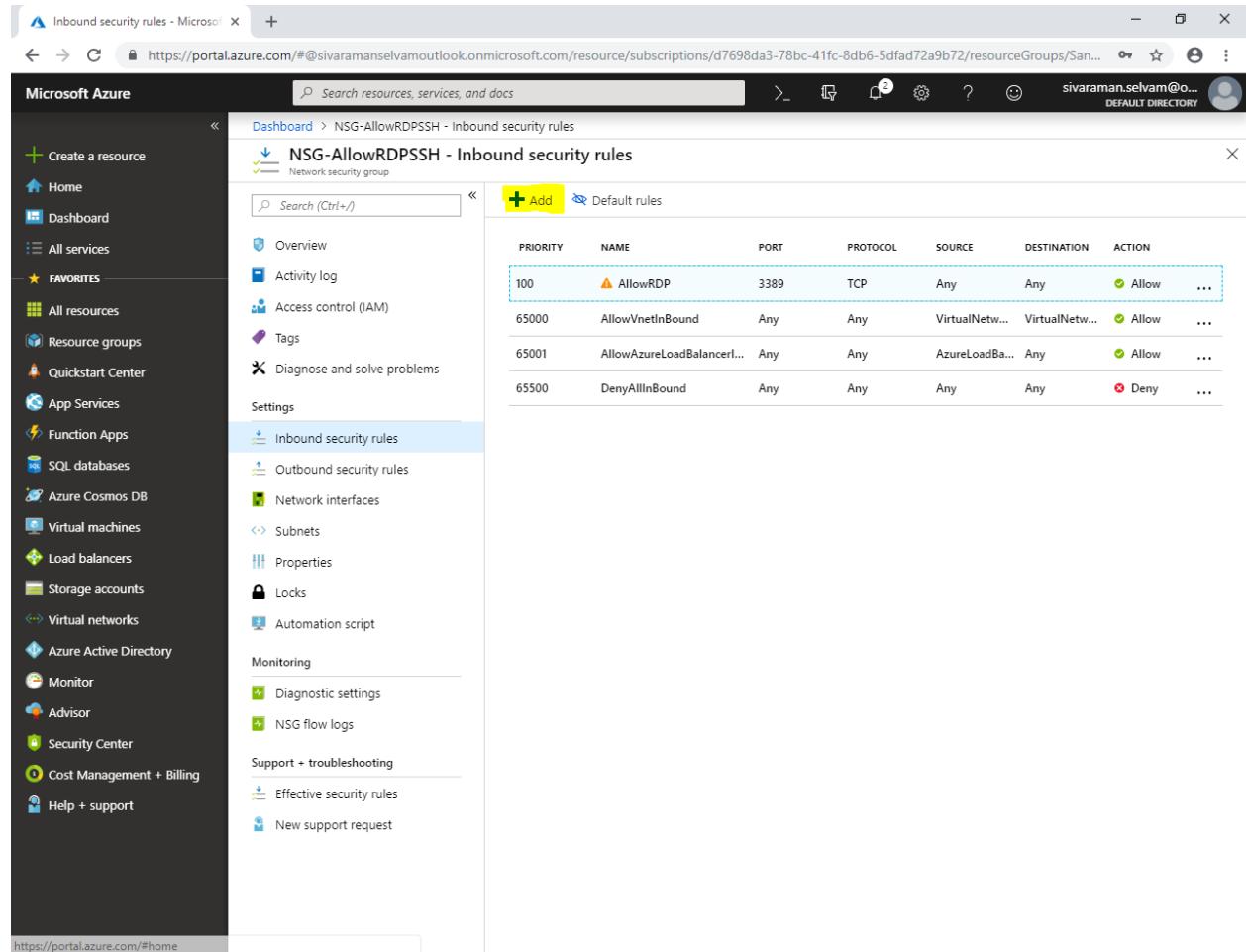
You are able to see that Inbound security rules has been created with priority “100”. RDP is not recommended to access the server through public. That is the reason it shows warning.



The screenshot shows the Microsoft Azure portal interface. The left sidebar contains various service icons under 'FAVORITES'. The main content area displays the 'NSG-AllowRDPSSH - Inbound security rules' page for a specific Network Security Group (NSG). The page title is 'NSG-AllowRDPSSH - Inbound security rules'. On the left, there's a navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Inbound security rules (which is selected and highlighted in blue), Outbound security rules, Network interfaces, Subnets, Properties, Locks, Automation script, Monitoring, Diagnostic settings, and NSG flow logs. Below these are sections for Support + troubleshooting, Effective security rules, and New support request. The main right panel shows a table of inbound security rules:

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	... (More)
100	AllowRDP	3389	TCP	Any	Any	Allow	...
65000	AllowVnetInBound	Any	Any	VirtualNetw...	VirtualNetw...	Allow	...
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBa...	Any	Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	Deny	...

Click “Add”.



The screenshot shows the Microsoft Azure portal interface for managing inbound security rules. The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, and Favorites. Under Favorites, 'Inbound security rules' is selected. The main content area displays a table of existing security rules under the heading 'NSG-AllowRDPSSH - Inbound security rules'. A yellow box highlights the '+ Add' button at the top right of the table header. The table columns are: PRIORITY, NAME, PORT, PROTOCOL, SOURCE, DESTINATION, and ACTION. The first rule listed is 'AllowRDP' with priority 100, port 3389, TCP protocol, and 'Allow' action.

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	AllowRDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetw...	VirtualNetw...	Allow
65001	AllowAzureLoadBalancer...	Any	Any	AzureLoadBa...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

While creating inbound security rule

Source : Any

Source port ranges : *

Destination : Any

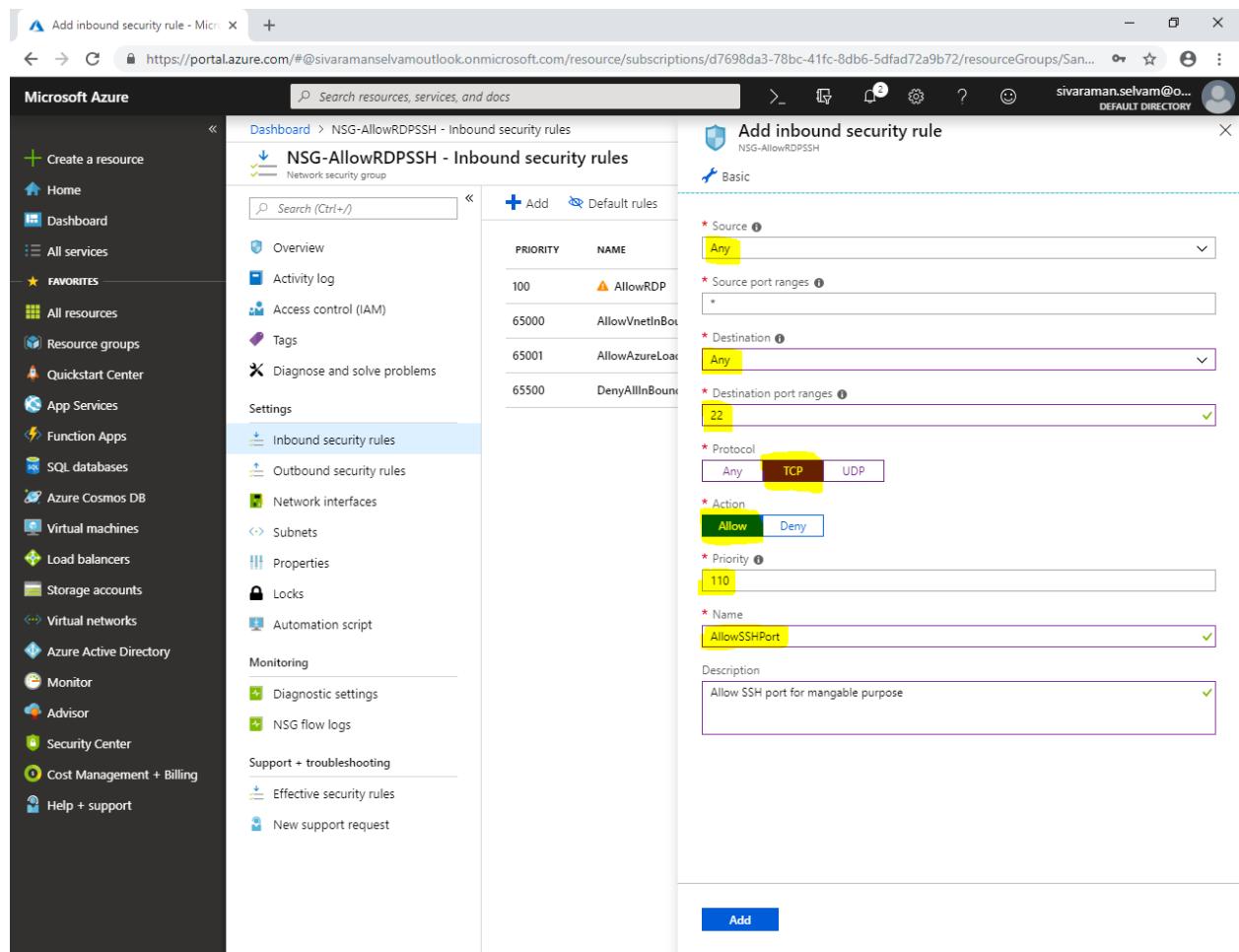
Destination port ranges : 22

Protocol : TCP

Action : Allow

Priority : 110

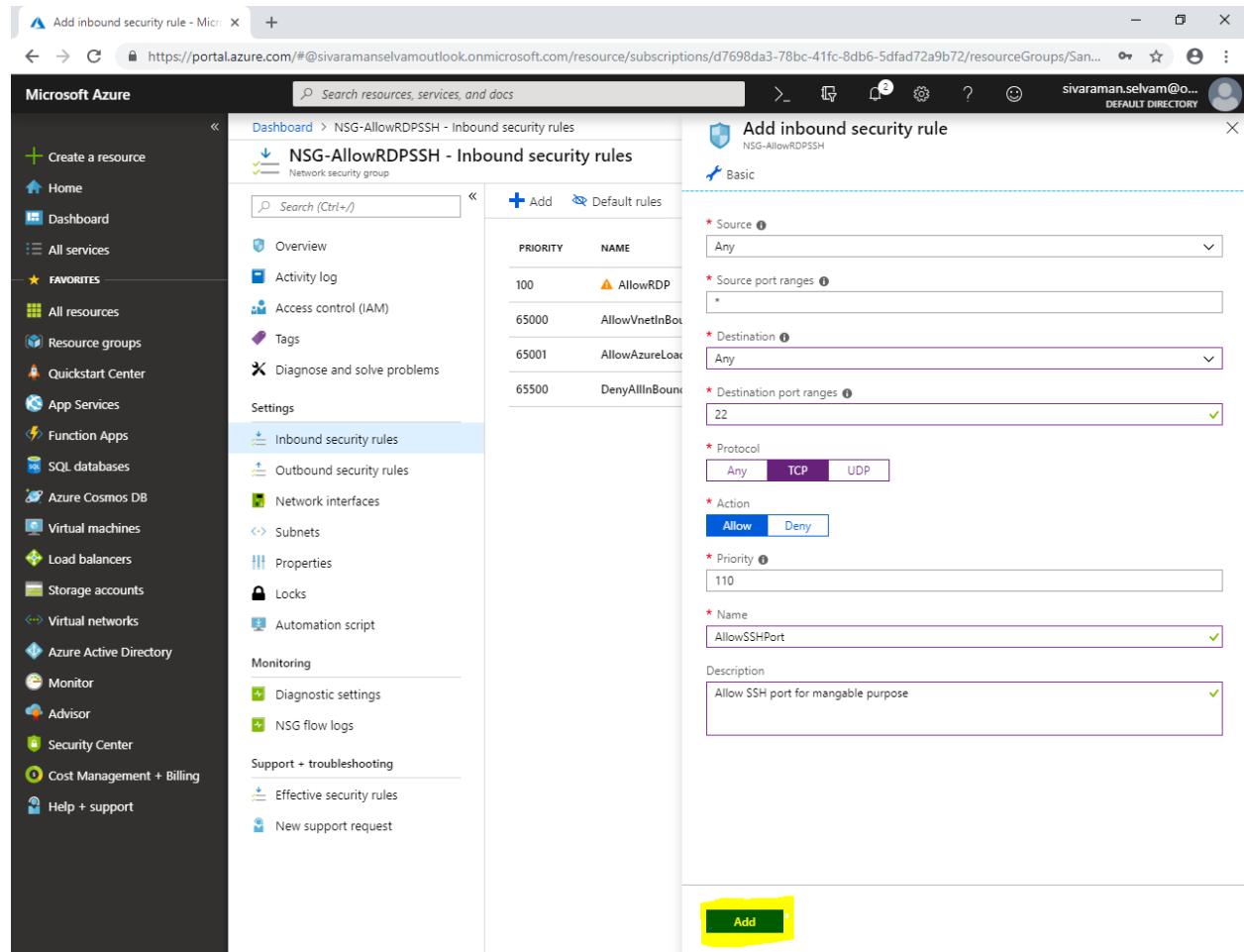
Name : AllowSSH



The screenshot shows the Azure portal interface for creating an inbound security rule. The left sidebar lists various Azure services, and the main area shows the 'NSG-AllowRDPSSH - Inbound security rules' blade. A new rule is being added with the following configuration:

- Source:** Any
- Source port ranges:** *
- Destination:** Any
- Destination port ranges:** 22
- Protocol:** TCP
- Action:** Allow
- Priority:** 110
- Name:** AllowSSHPort
- Description:** Allow SSH port for manageable purpose

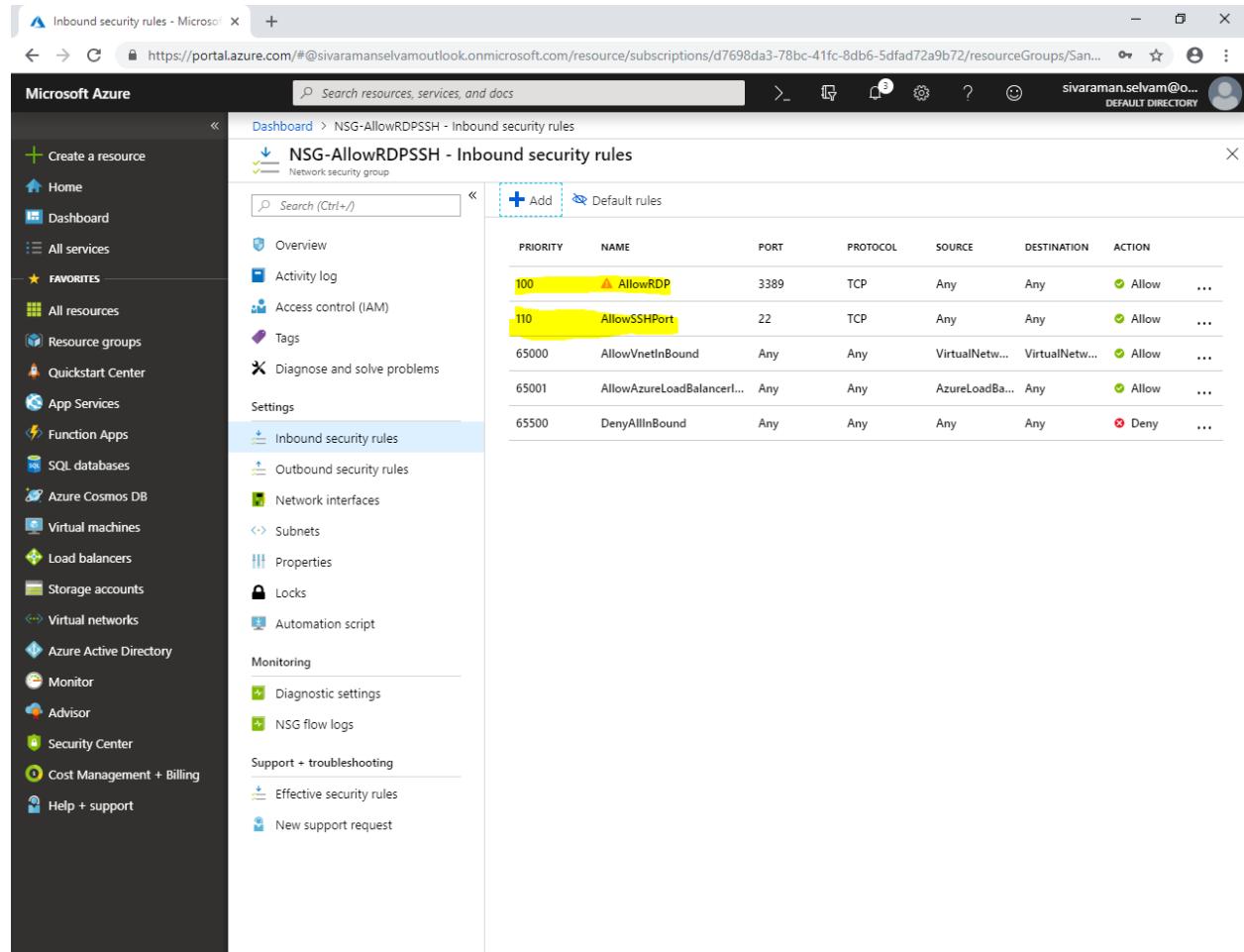
Click “Add”.



The screenshot shows the Microsoft Azure portal interface. The left sidebar is filled with various service icons under categories like Favorites, All resources, and Monitoring. The main content area is titled "NSG-AllowRDPSSH - Inbound security rules" and shows a list of existing rules with columns for Priority and Name. A new rule is being added, with fields for Source (Any), Destination (Any), Destination port ranges (22), Protocol (TCP), Action (Allow), Priority (110), and Name (AllowSSHPort). The "Add" button at the bottom is highlighted with a yellow box.

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.

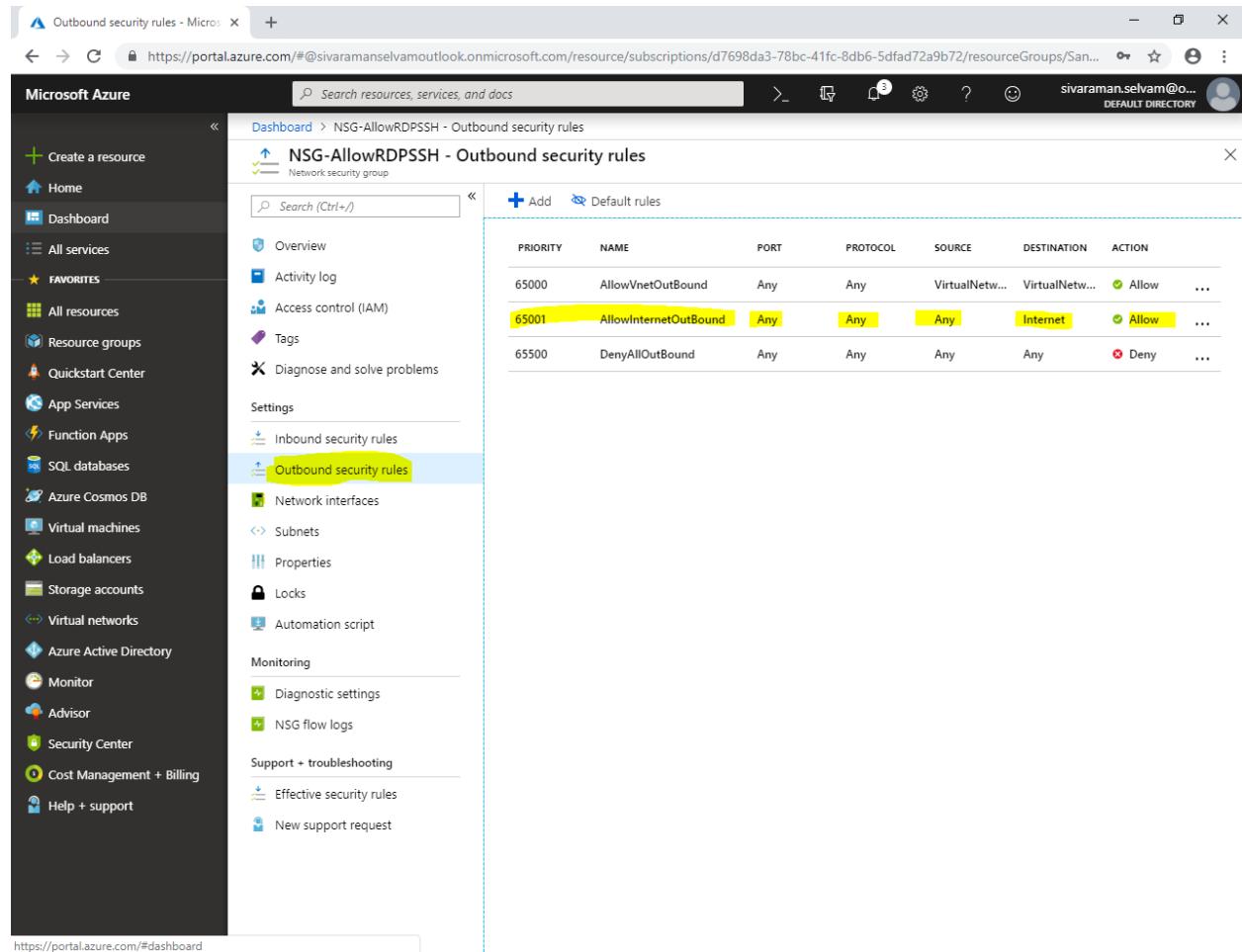


The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation bar includes options like Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, Quickstart Center, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Billing, and Help + support. The main content area displays the 'NSG-AllowRDPSSH - Inbound security rules' page under the 'NSG-AllowRDPSSH' network security group. The page has a search bar, a 'Default rules' button, and a table of rules:

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	AllowRDP	3389	TCP	Any	Any	Allow
110	AllowSSHPort	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetw...	VirtualNetw...	Allow
65001	AllowAzureLoadBalancerl...	Any	Any	AzureLoadBa...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Click on “Outbound security Rules”

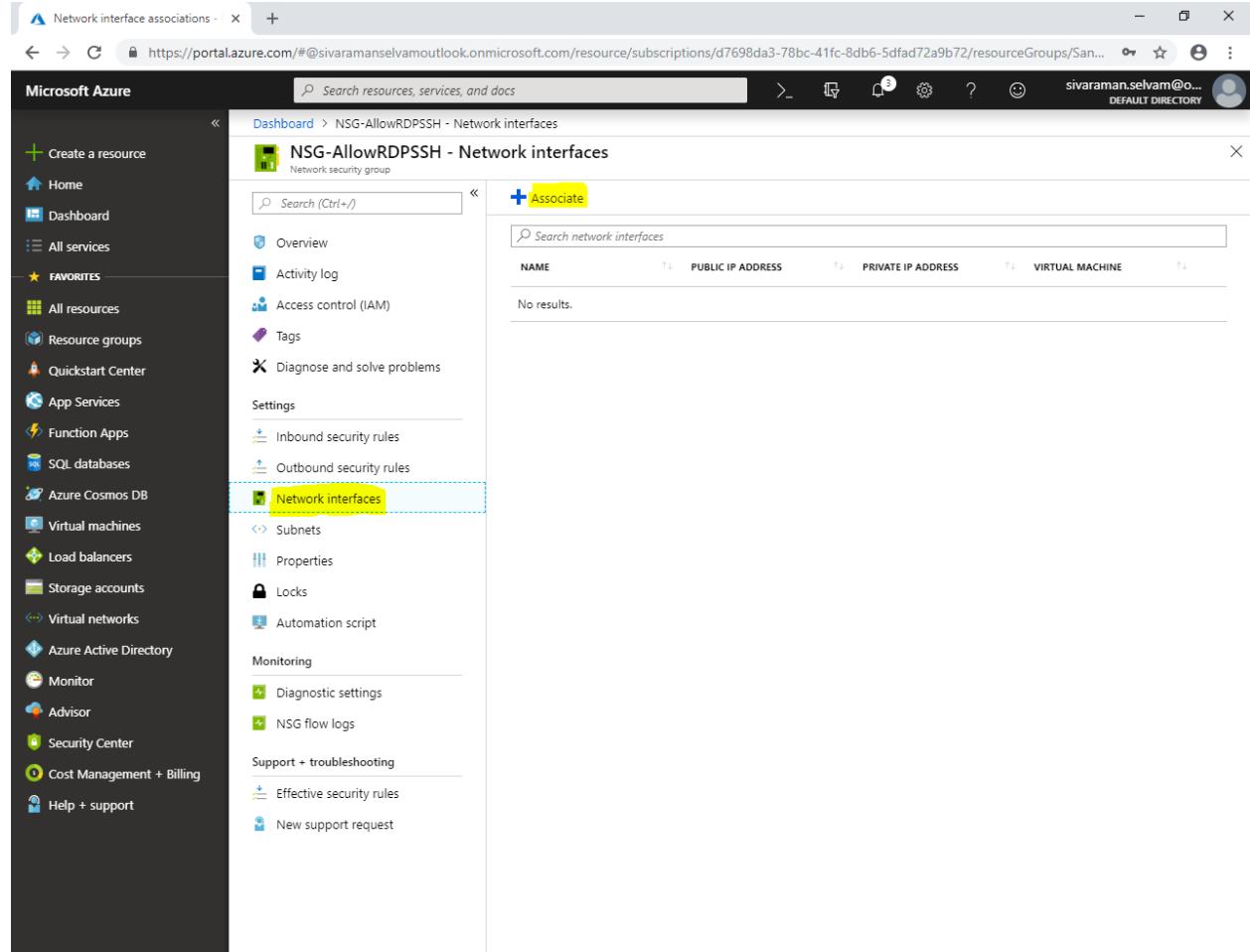
By default it will allow Internet (any protocol and any port) from azure virtual machine to public.



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 "Network interfaces".

Click "Associate".



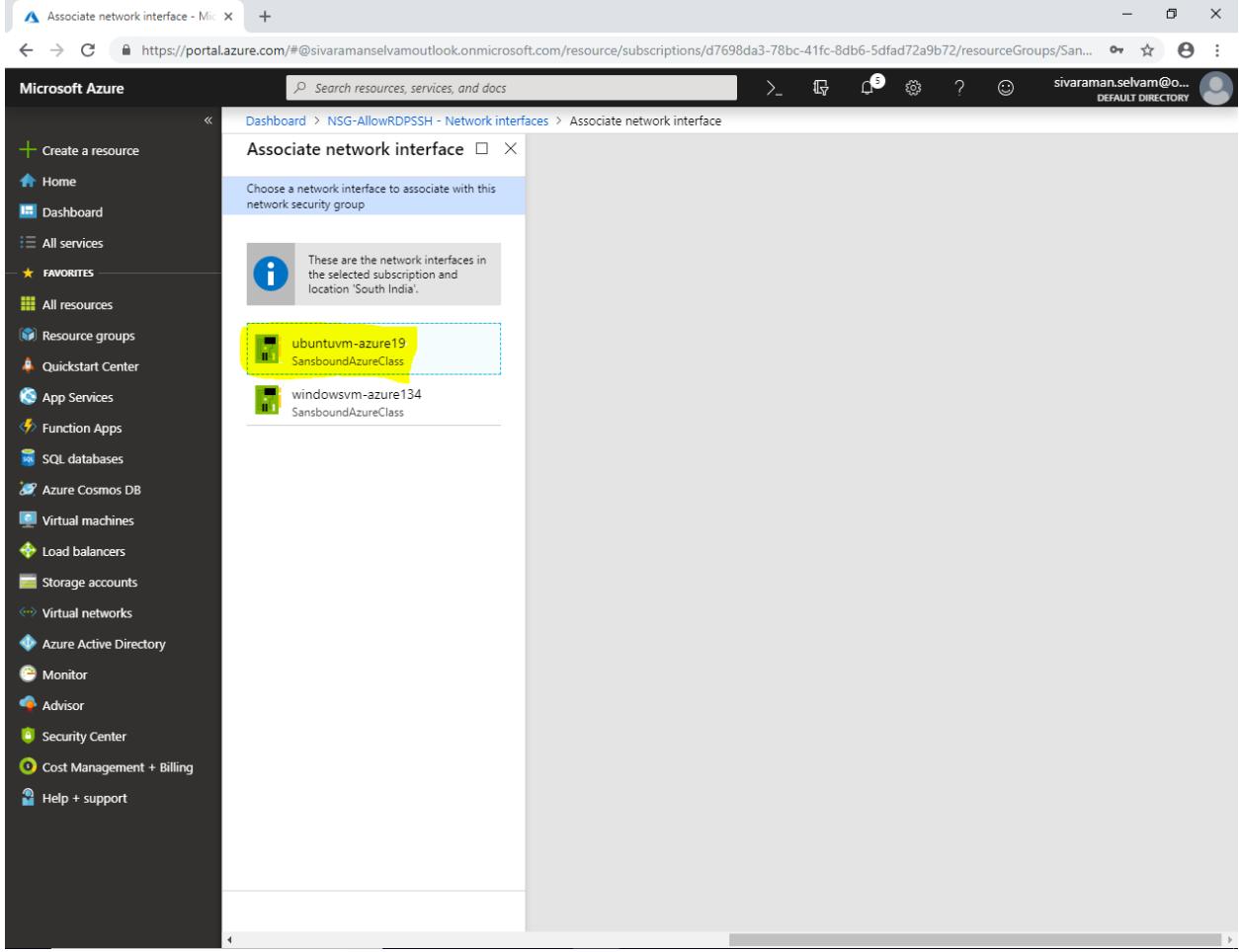
The screenshot shows the Microsoft Azure portal interface. The left sidebar is filled with various service icons under categories like Favorites, All resources, and Monitoring. The main content area is titled 'NSG-AllowRDPSSH - Network interfaces' and shows a list of network interfaces. At the top right of this area, there is a large yellow button labeled '+ Associate'. Below the title, there's a search bar and a table with columns for NAME, PUBLIC IP ADDRESS, PRIVATE IP ADDRESS, and VIRTUAL MACHINE. A message 'No results.' is displayed below the table. The 'Network interfaces' link in the sidebar is also highlighted with a yellow box.

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”.



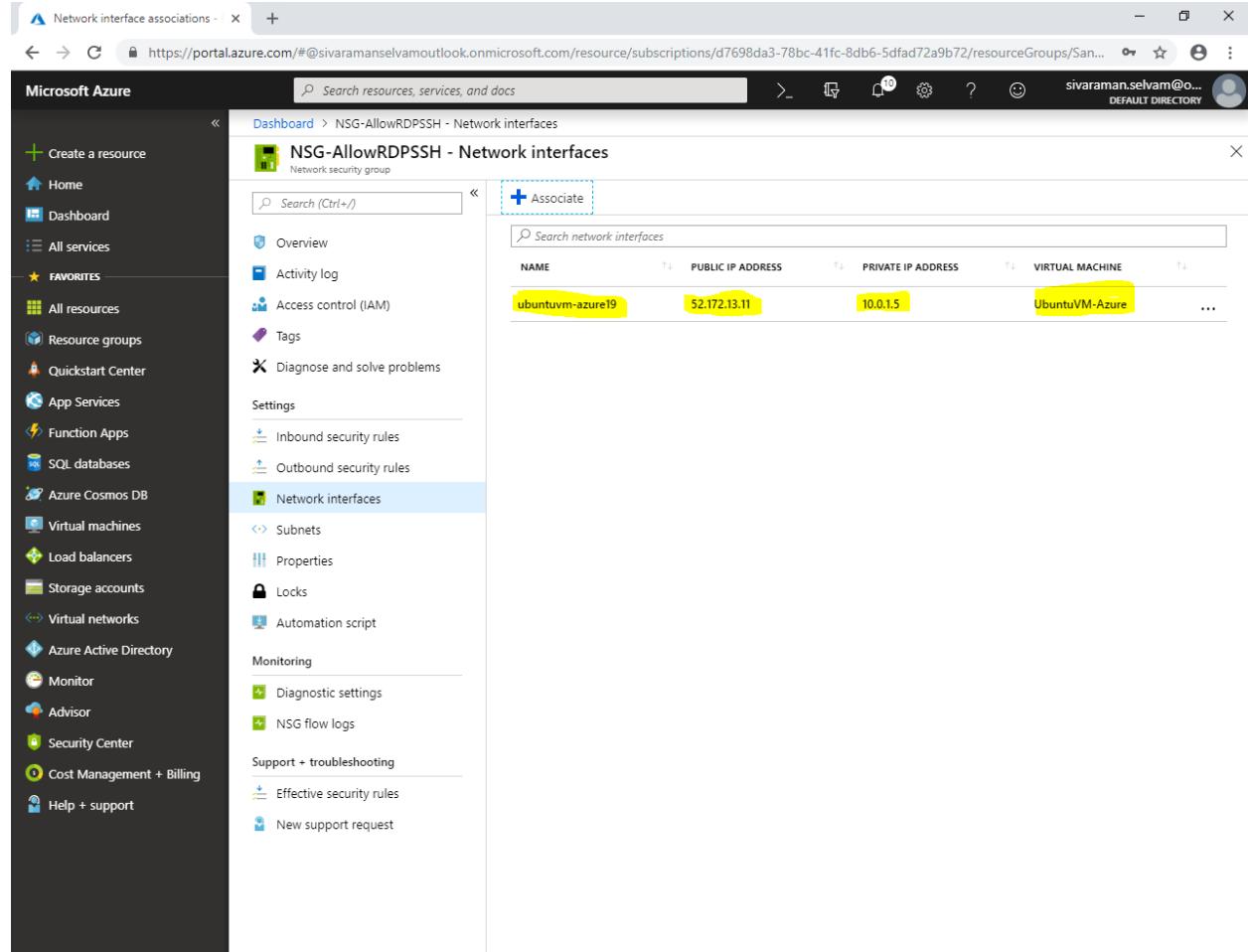
The screenshot shows the Microsoft Azure portal interface. The user is in the 'Associate network interface' section, specifically under the 'NSG-AllowRDPSSH' resource group. The left sidebar lists various Azure services. The main pane displays a list of network interfaces available for association:

- ubuntuvm-azure19 (highlighted with a yellow box)
- windowsvm-azure134

A tooltip above the list states: "These are the network interfaces in the selected subscription and location South India."

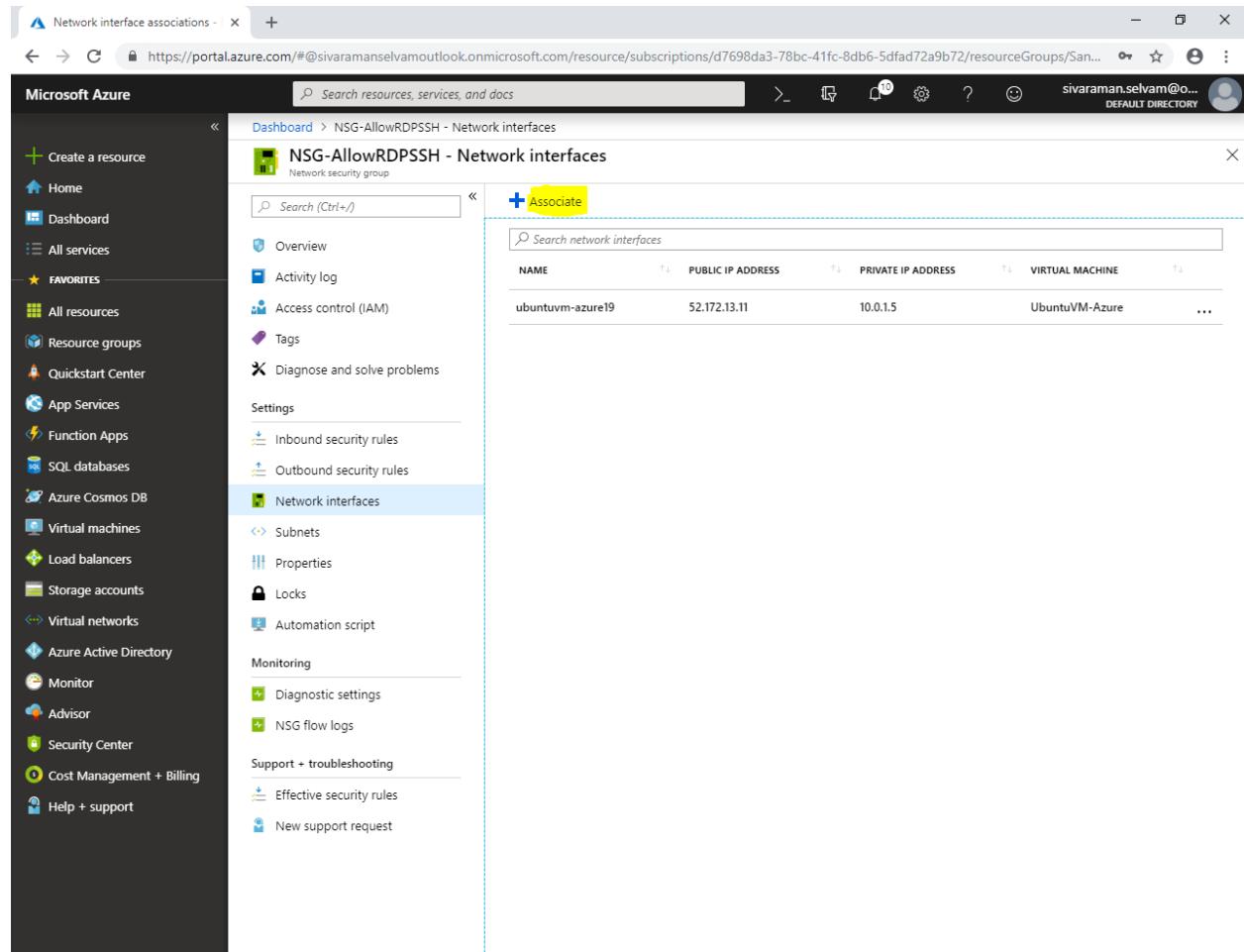
In “Network Interfaces”

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



NAME	PUBLIC IP ADDRESS	PRIVATE IP ADDRESS	VIRTUAL MACHINE
ubuntuvm-azure19	52.172.13.11	10.0.1.5	UbuntuVM-Azure

In “Network Interfaces” click “Associate”

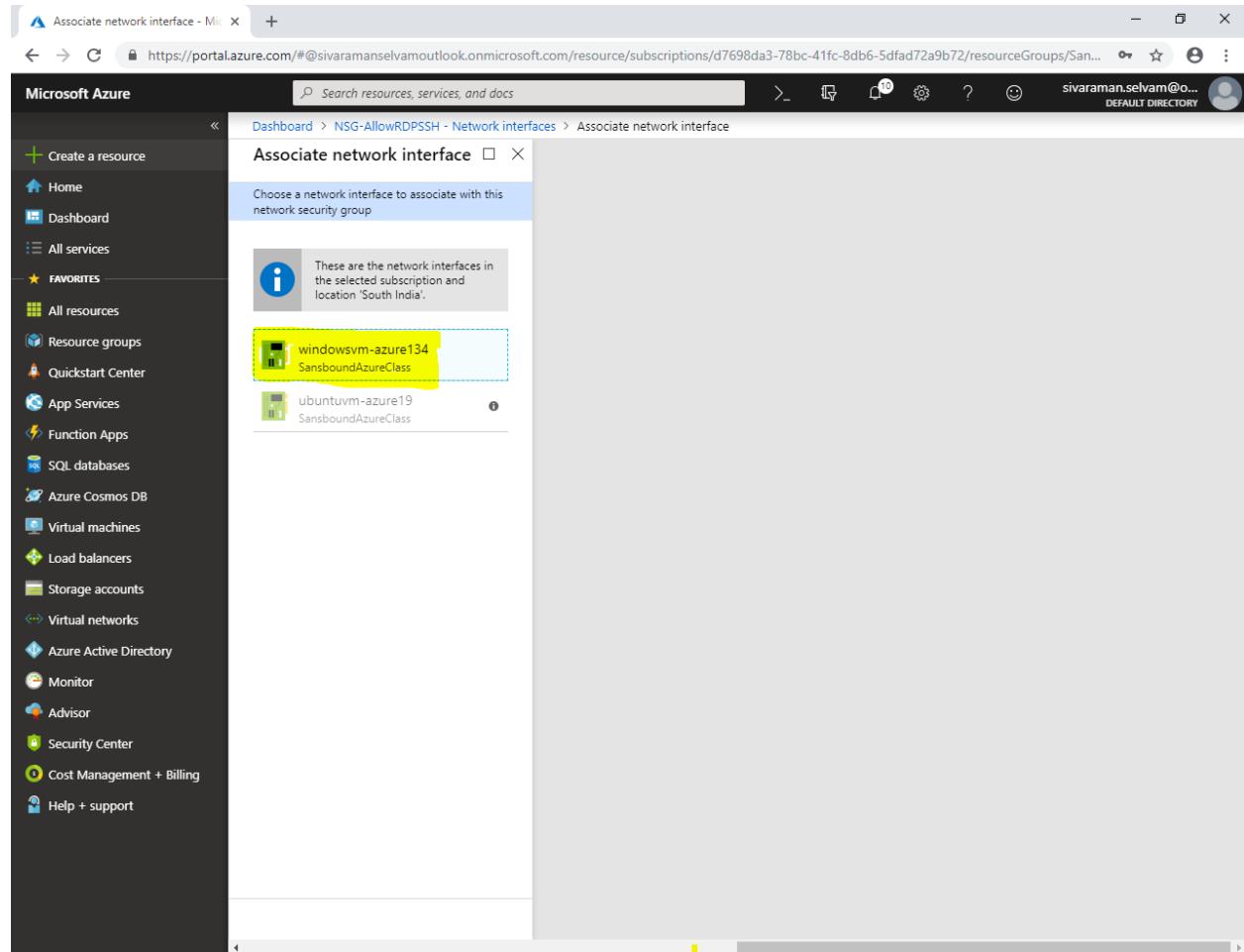


The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a list of services under 'FAVORITES'. The main content area is titled 'NSG-AllowRDPSSH - Network interfaces' and shows a table of network interfaces. A yellow box highlights the '+ Associate' button at the top right of the interface list.

NAME	PUBLIC IP ADDRESS	PRIVATE IP ADDRESS	VIRTUAL MACHINE
ubuntuvm-azure19	52.172.13.11	10.0.1.5	UbuntuVM-Azure

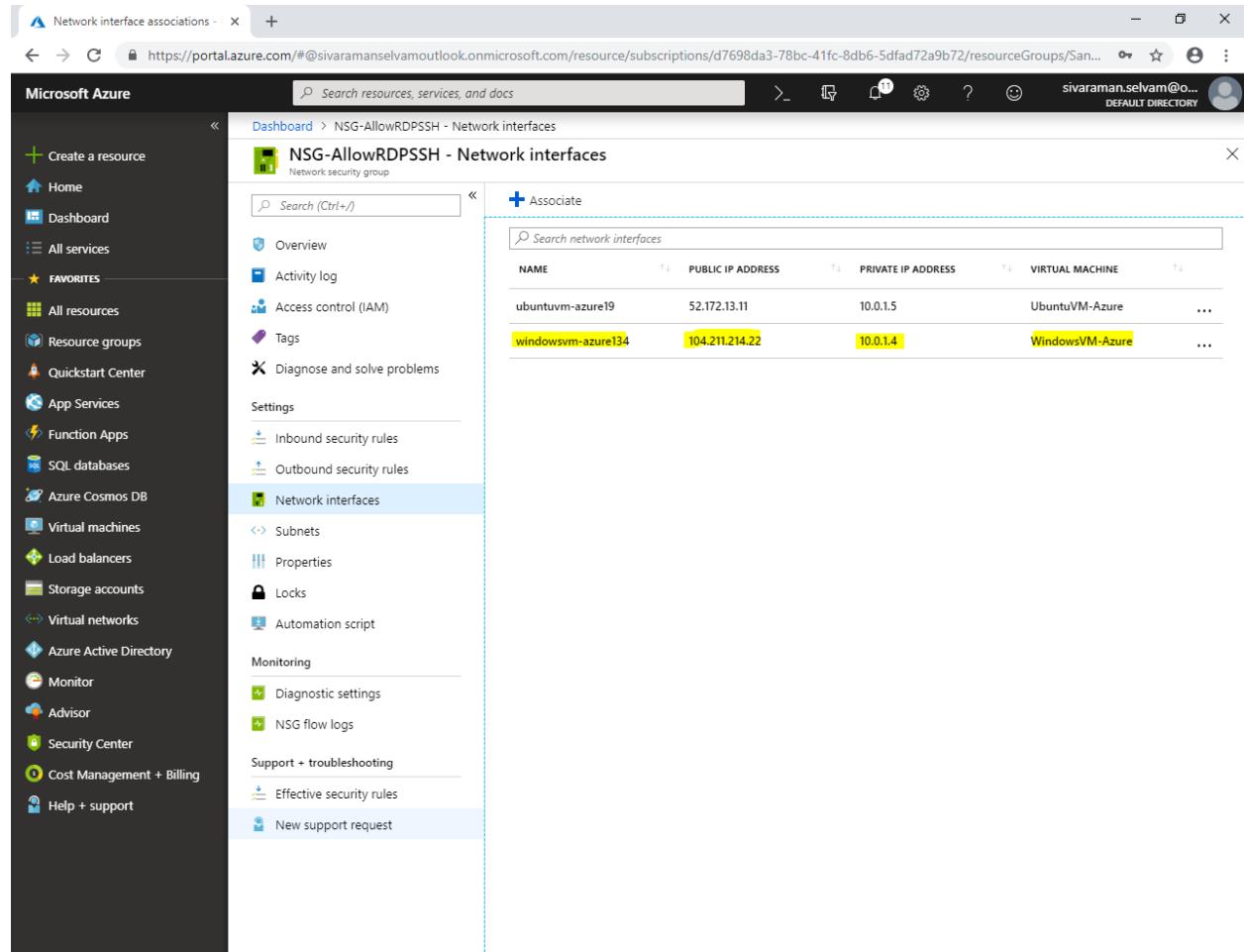
By default “Windows-VM” network interface has been selected. Because existing network interface has been already associated.

Click on “**windowsvm-azure134**”.



The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a list of services: 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). The main content area is titled "Associate network interface" and shows a list of network interfaces: "windowsvm-azure134" (highlighted with a yellow box) and "ubuntuvm-azure19". A tooltip indicates that these are the network interfaces in the selected subscription and location 'South India'.

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

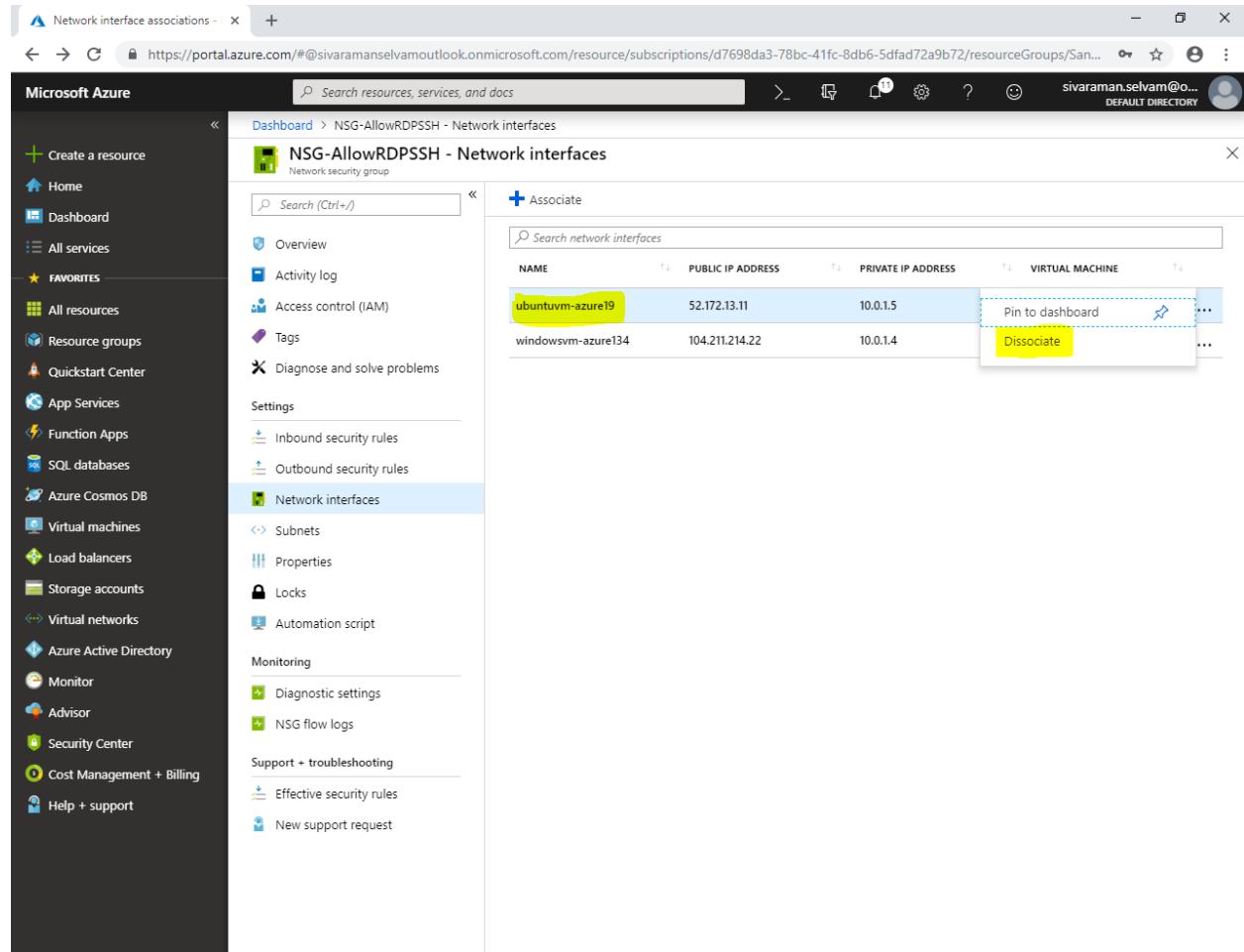


The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a list of services: Create a resource, Home, Dashboard, All services, Favorites (All resources, Resource groups, Quickstart Center, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Billing, Help + support. The main content area shows the 'NSG-AllowRDPSSH - Network interfaces' page under 'Dashboard > NSG-AllowRDPSSH - Network interfaces'. The left navigation pane for this page includes: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Inbound security rules, Outbound security rules, Network interfaces - selected), Subnets, Properties, Locks, Automation script, Monitoring (Diagnostic settings, NSG flow logs), and Support + troubleshooting (Effective security rules, New support request). The right pane displays a table titled 'Associate' with the following data:

NAME	PUBLIC IP ADDRESS	PRIVATE IP ADDRESS	VIRTUAL MACHINE
ubuntuvm-azure19	52.172.13.11	10.0.1.5	UbuntuVM-Azure
windowsvm-azure134	104.211.214.22	10.0.1.4	WindowsVM-Azure

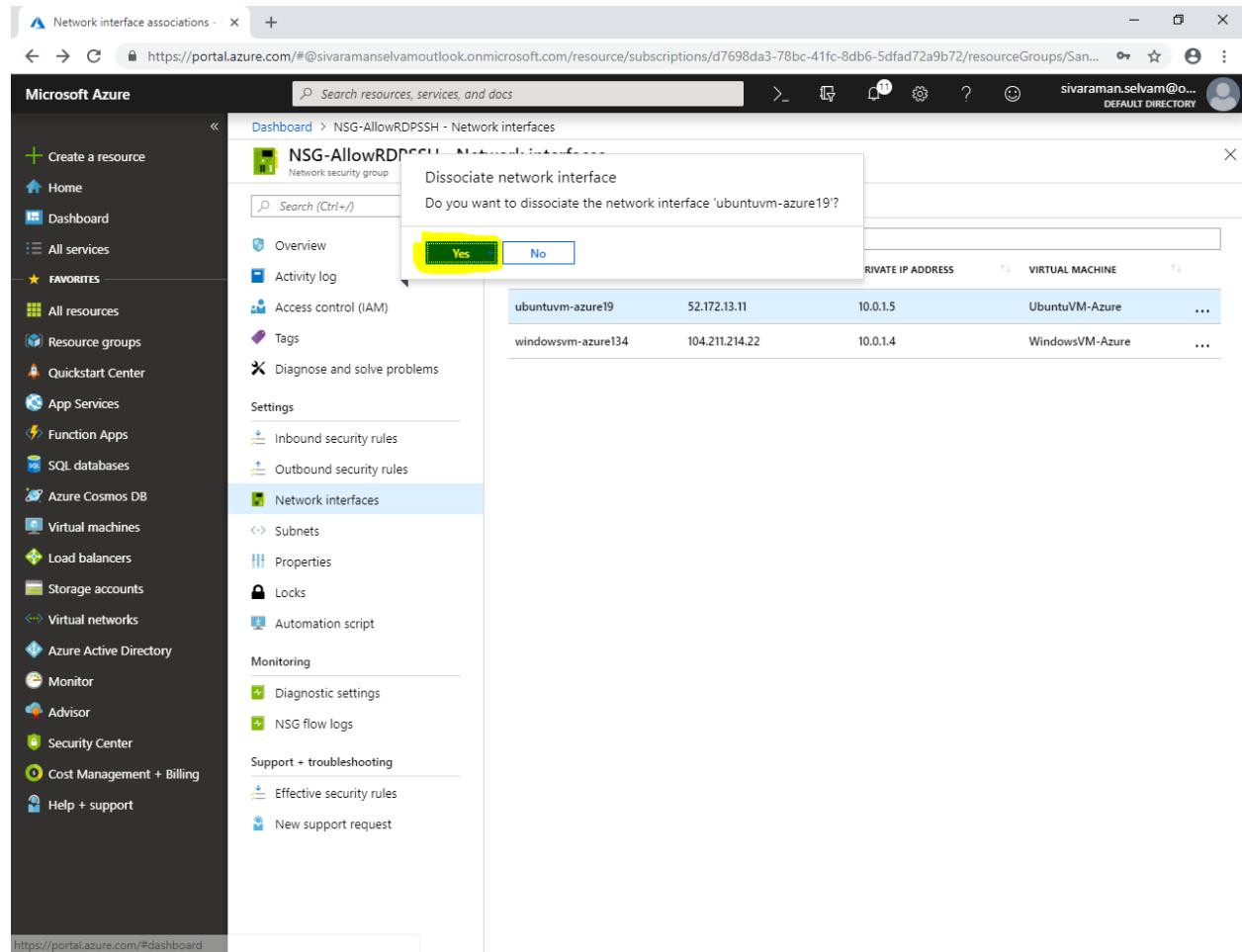
We have understood the features of “**Network Interfaces**” in “**Network Security Group**”.

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



NAME	PUBLIC IP ADDRESS	PRIVATE IP ADDRESS	VIRTUAL MACHINE
ubuntuvm-azure19	52.172.13.11	10.0.1.5	
windowsvm-azure134	104.211.214.22	10.0.1.4	

Click “**Yes**” to dissociate the network from ubuntuvm.

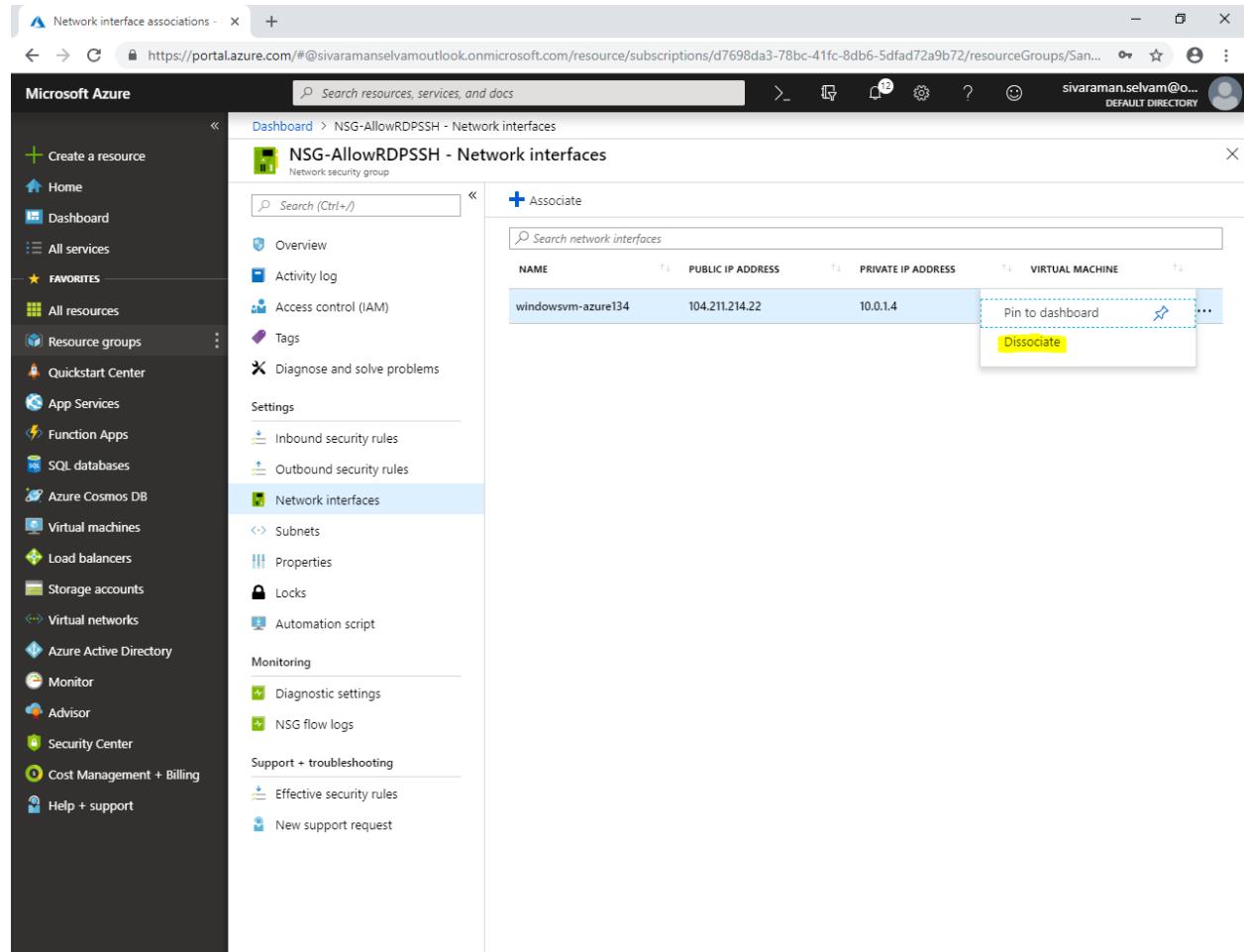


The screenshot shows the Microsoft Azure portal interface. The user is in the 'Network interface associations' section, specifically for the NSG-AllowRDPSSH network security group. A confirmation dialog box is open, asking if they want to dissociate the network interface 'ubuntuvm-azure19'. The 'Yes' button is highlighted with a yellow box. Below the dialog, there is a table listing two network interfaces:

	PRIVATE IP ADDRESS	VIRTUAL MACHINE	...
ubuntuvm-azure19	52.172.13.11	10.0.1.5	UbuntuVM-Azure
windowsvm-azure134	104.211.214.22	10.0.1.4	WindowsVM-Azure

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

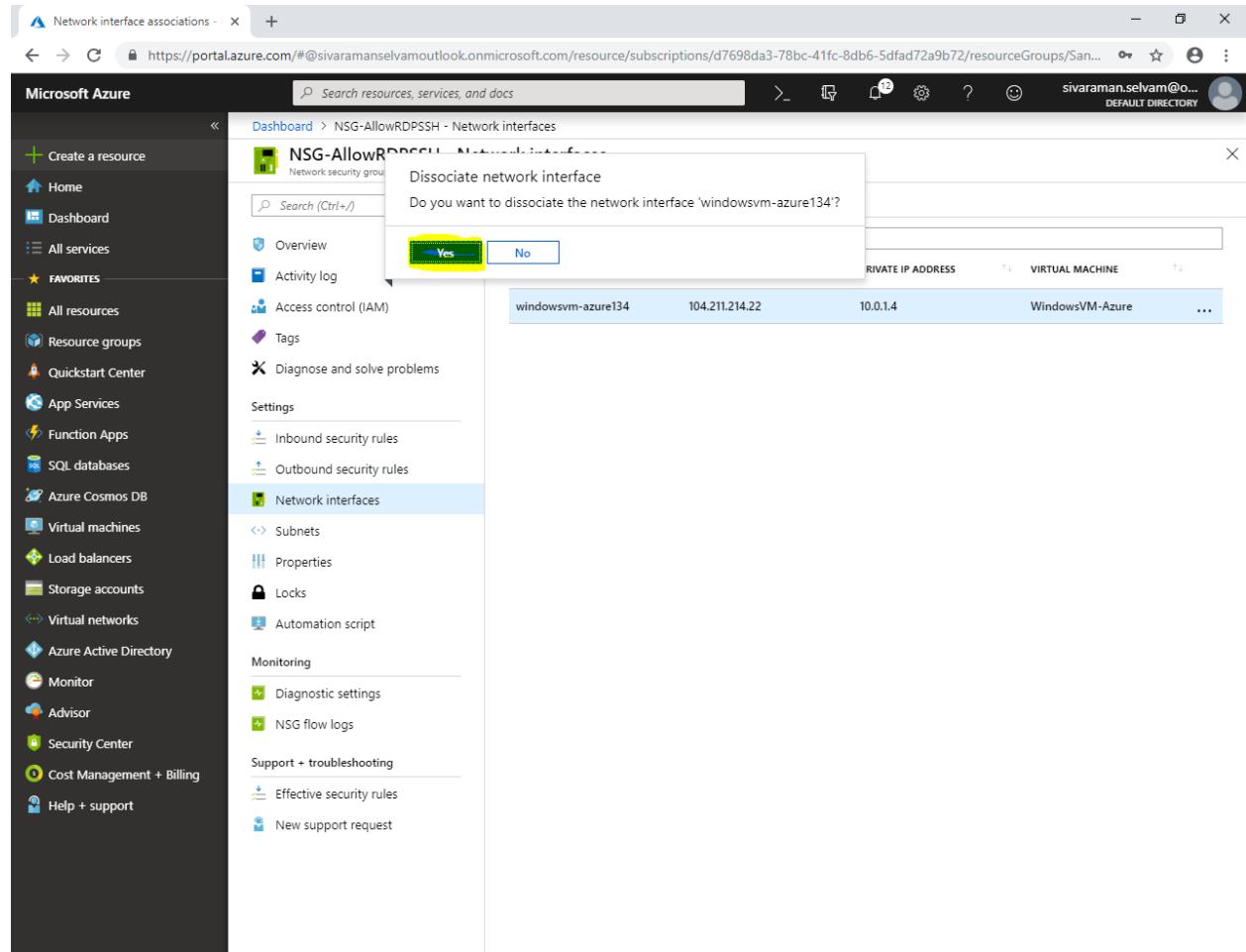
Click “**Dissociate**”.



The screenshot shows the Microsoft Azure portal interface. The left sidebar is filled with various service icons under categories like Home, All services, Favorites, and Resource groups. The main content area is titled "NSG-AllowRDPSSH - Network interfaces". It displays a table of network interfaces, with one row selected: "windowsvm-azure134". A context menu is open over this row, with the "Dissociate" option highlighted in yellow. Other options visible in the menu include "Pin to dashboard" and three dots (...).

NAME	PUBLIC IP ADDRESS	PRIVATE IP ADDRESS	VIRTUAL MACHINE
windowsvm-azure134	104.211.214.22	10.0.1.4	[Virtual Machine Icon]

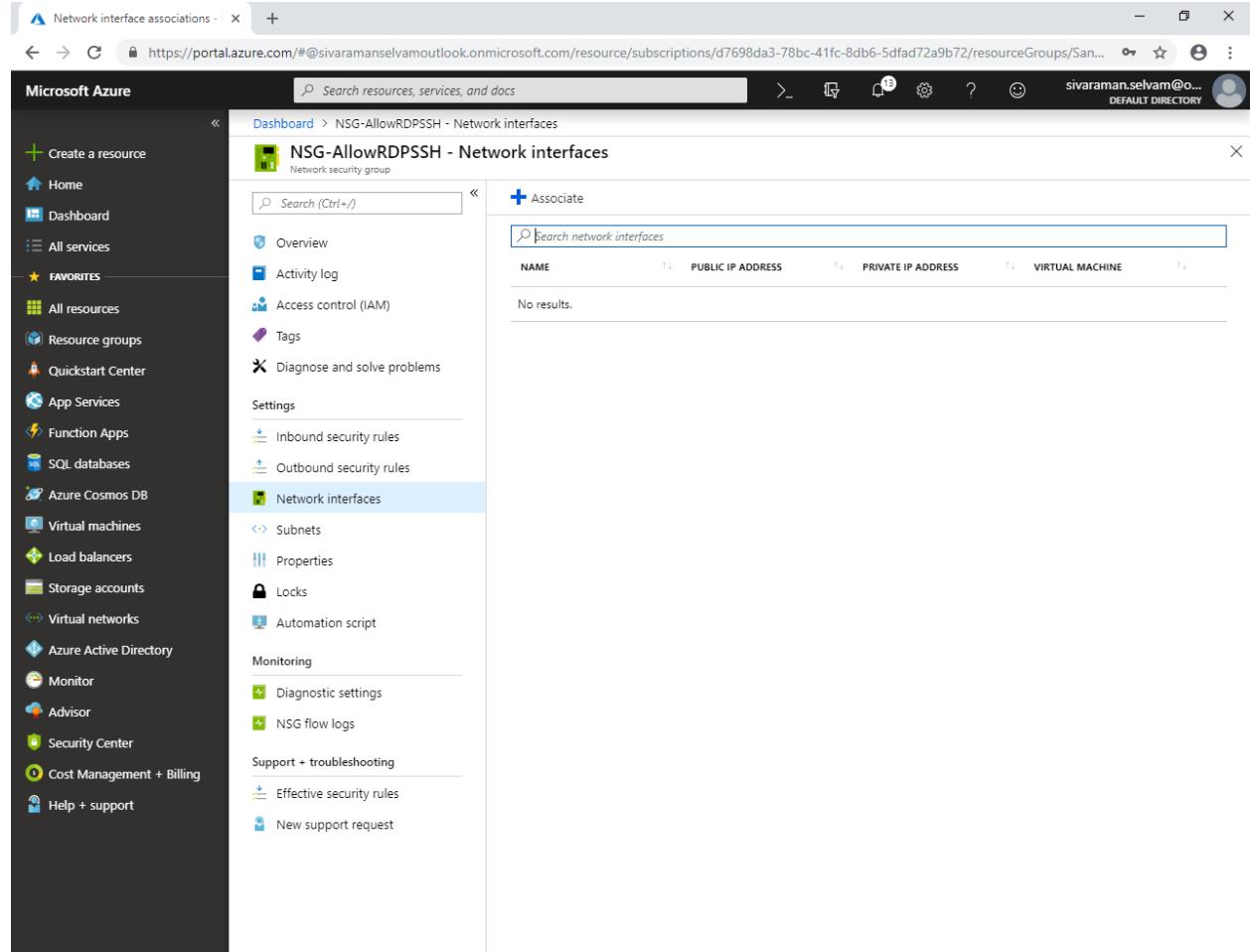
Click "Yes".



The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu is visible with various service icons. The main content area displays the 'Network interface associations' page for an NSG named 'NSG-AllowRDPSSH'. A modal dialog box is centered over the page, asking 'Do you want to dissociate the network interface 'windowsvm-azure134'?'. The 'Yes' button in the dialog is highlighted with a yellow box. Below the dialog, a table lists network interfaces, showing one entry: 'windowsvm-azure134' with 'PRIVATE IP ADDRESS' 104.211.214.22 and 'VIRTUAL MACHINE' WindowsVM-Azure.

In “Network Interfaces”

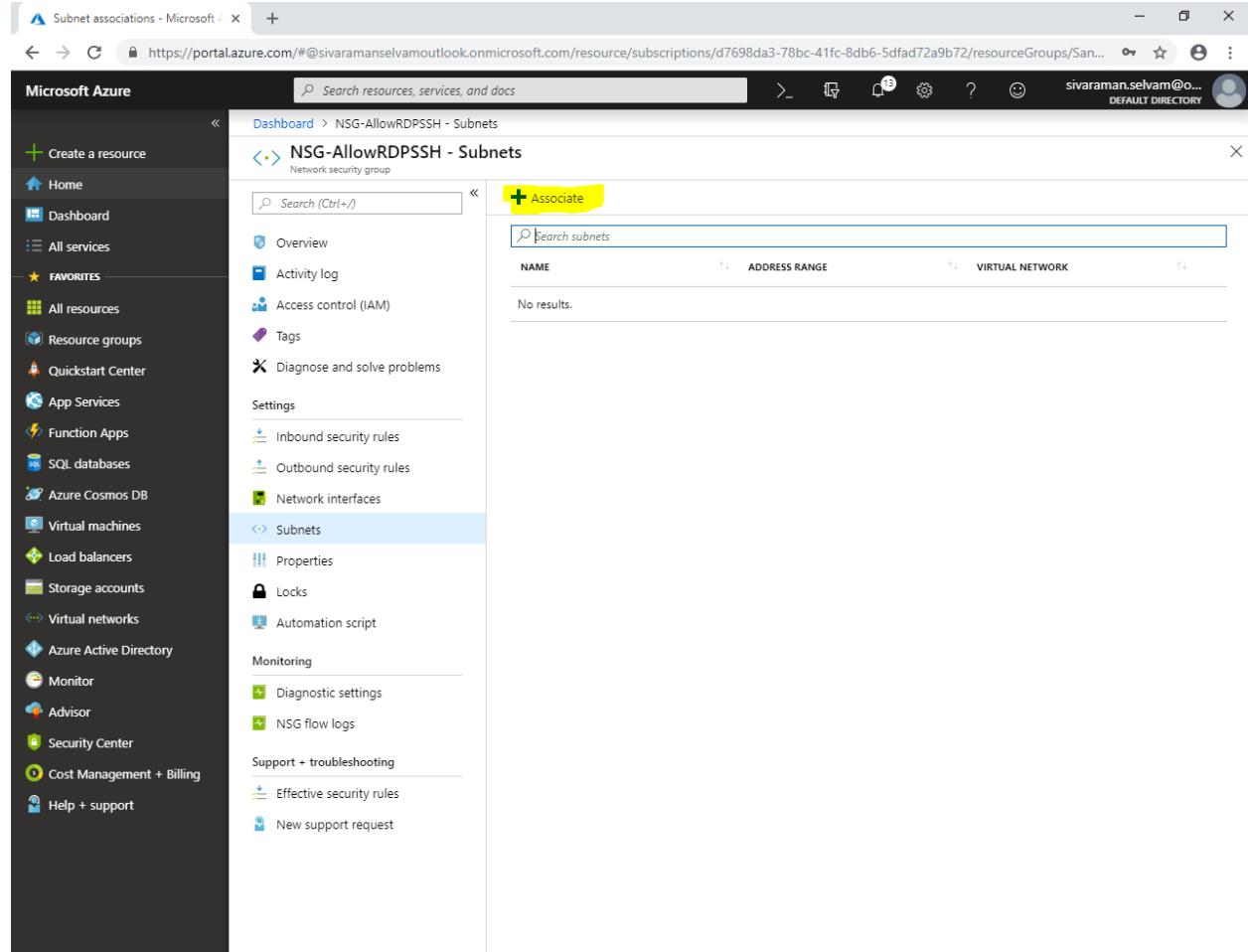
There is no network interfaces are associated with Network Security Group (NSG).



The screenshot shows the Microsoft Azure portal interface. The left sidebar is filled with various service icons under categories like Favorites, All resources, and All services. The main content area is titled "NSG-AllowRDPSSH - Network interfaces" and is under the "Network security group" category. On the left of this main area, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, and Network interfaces (which is currently selected and highlighted in blue). Below these are Subnets, Properties, Locks, and Automation script. Further down are Monitoring options for Diagnostic settings and NSG flow logs. At the bottom of this sidebar are Support + troubleshooting options for Effective security rules and New support request. The main right-hand pane has a search bar at the top labeled "Search network interfaces". Below it is a table with columns: NAME, PUBLIC IP ADDRESS, PRIVATE IP ADDRESS, and VIRTUAL MACHINE. A message "No results." is displayed below the table.

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

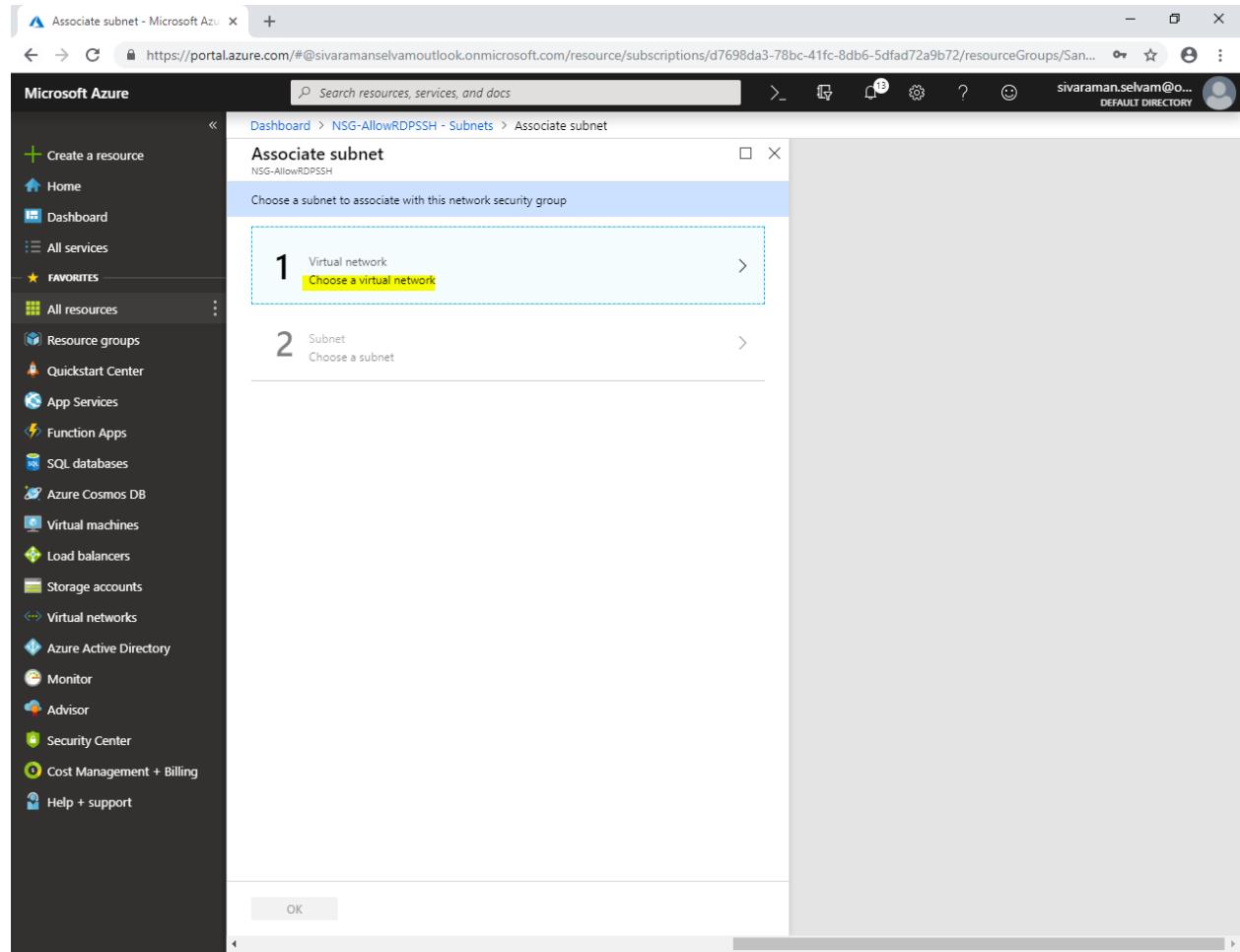
In “**Subnets**” click “**Associate**”.



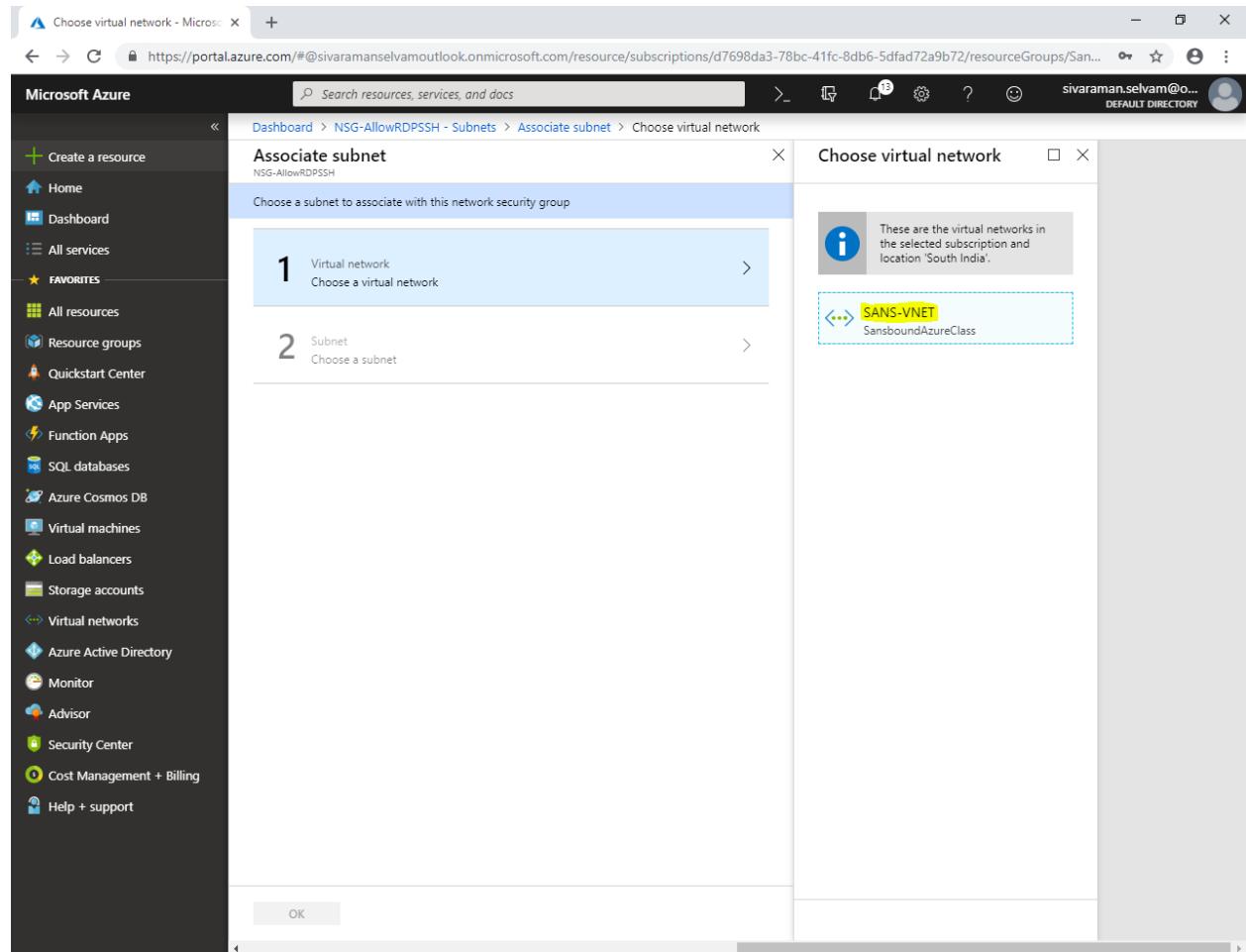
The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a list of services and resources. The main content area is titled "NSG-AllowRDPSSH - Subnets" under "Network security group". A sub-menu on the right lists options like "Overview", "Activity log", "Access control (IAM)", "Tags", "Diagnose and solve problems", "Settings" (which is expanded to show "Inbound security rules", "Outbound security rules", "Network interfaces", and "Subnets"), "Monitoring" (with "Diagnostic settings" and "NSG flow logs"), and "Support + troubleshooting" (with "Effective security rules" and "New support request"). A prominent yellow box highlights the "+ Associate" button at the top of the main content area, which has a search bar above it labeled "Search subnets".

In “Associate subnet”

Click on “Choose a virtual network”.

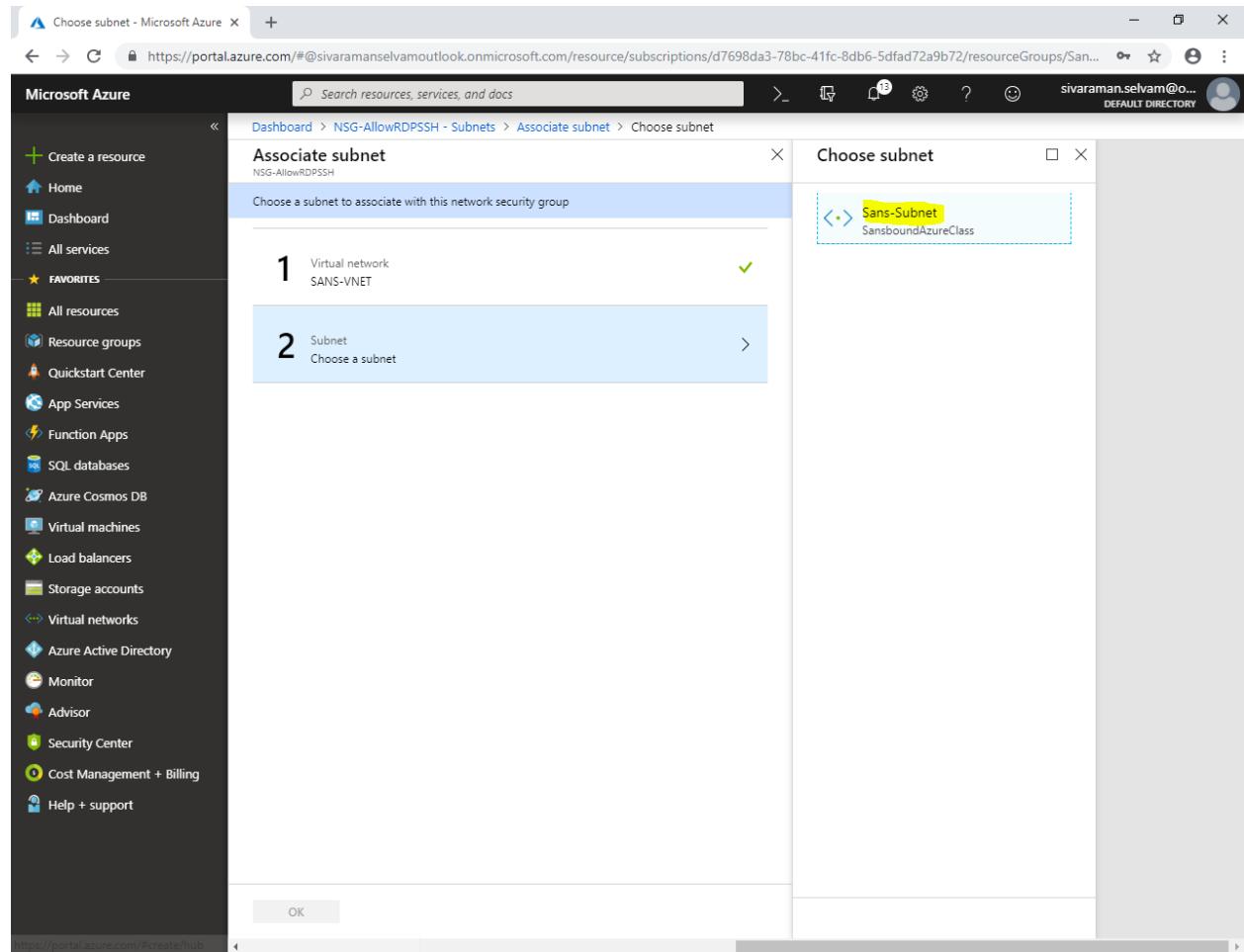


Click on "SANS-VNET".



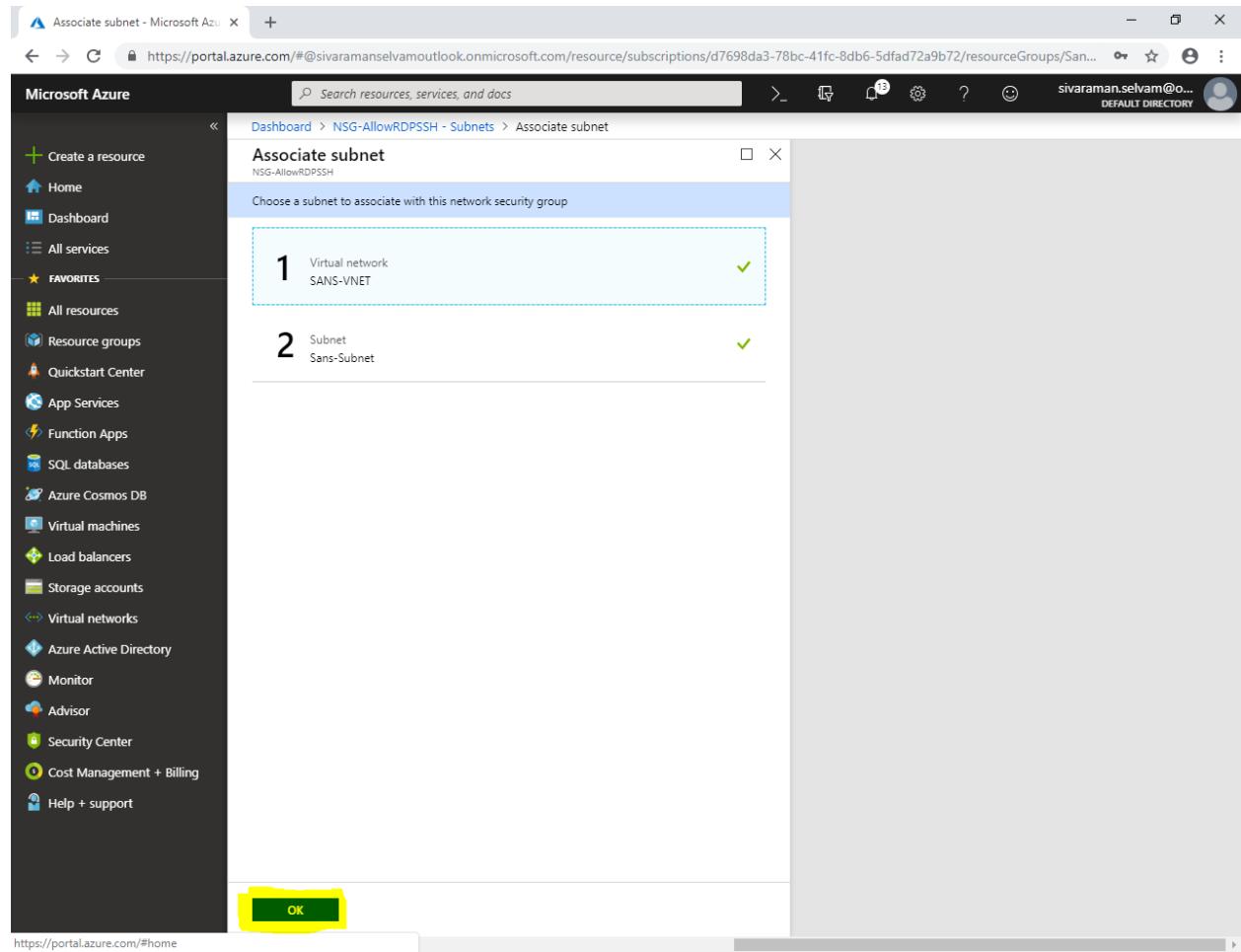
The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu is visible with various service icons. The main area displays a wizard titled 'Associate subnet' under 'NSG-AllowRDPSSH'. The first step, 'Choose a virtual network', is active, showing a list of virtual networks. One specific entry, 'SANS-VNET' from the 'SansboundAzureClass' resource group, is highlighted with a yellow dashed box. The second step, 'Choose a subnet', is shown below it. At the bottom of the wizard, there is an 'OK' button.

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



The screenshot shows the Microsoft Azure portal interface. The user is in the 'Associate subnet' step of a Network Security Group (NSG) configuration. The left sidebar shows various service icons under 'All services'. The main area displays 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'. A dropdown menu titled 'Choose subnet' is open, listing 'Sans-Subnet' under 'SansboundAzureClass'. This 'Sans-Subnet' option is highlighted with a yellow box. At the bottom of the screen, there is an 'OK' button.

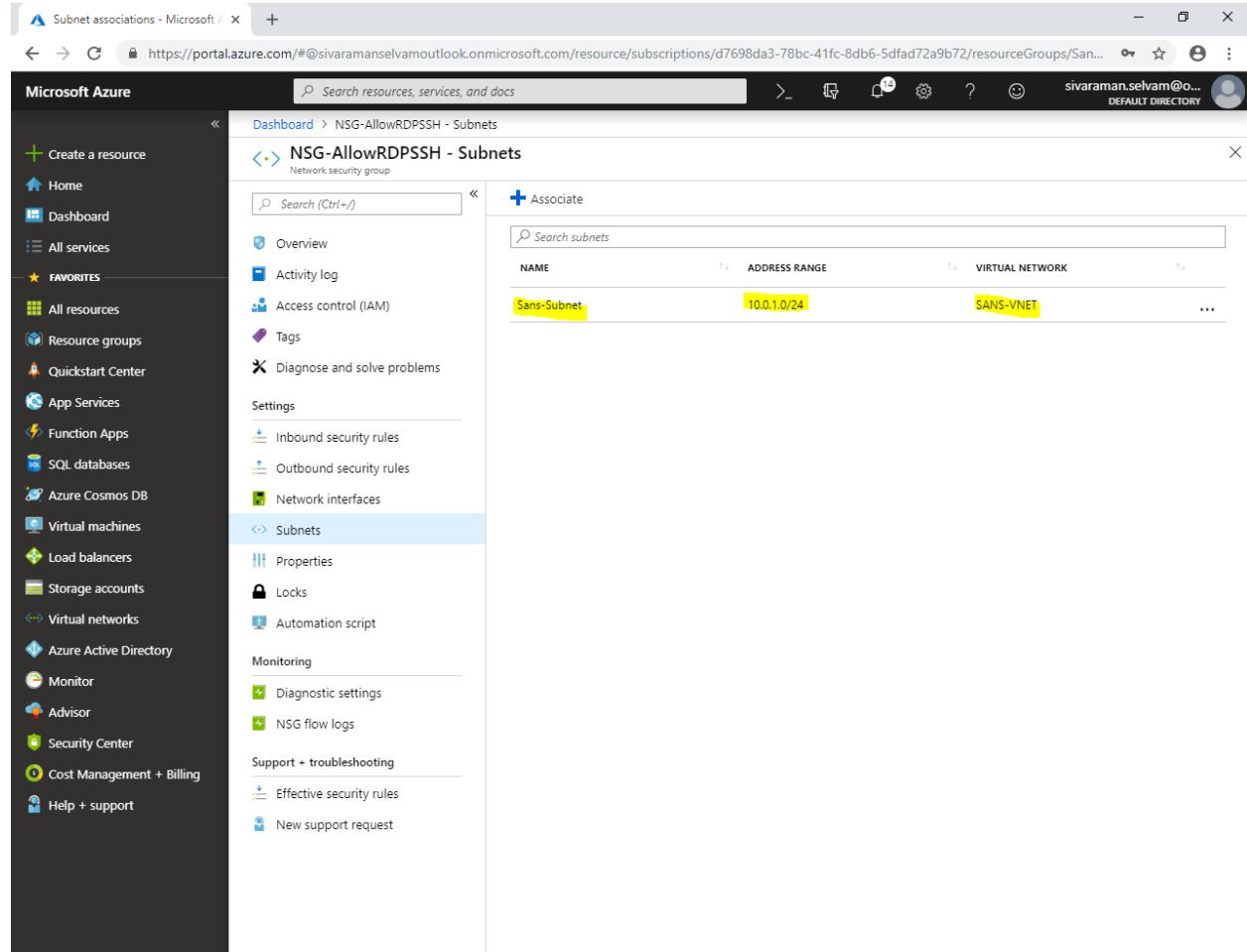
Click "OK".



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. The Favorites section is expanded, showing items such as 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 displays a 'Associate subnet' dialog for a resource group named 'NSG-AllowRDPSSH'. The dialog has two sections: 'Choose a subnet to associate with this network security group'. Section 1 shows a selected item 'Virtual network SANS-VNET' with a green checkmark. Section 2 shows a selected item 'Subnet Sans-Subnet' with a green checkmark. At the bottom of the dialog is a large yellow rectangular box highlighting the 'OK' button.

In “Network Security Group”

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

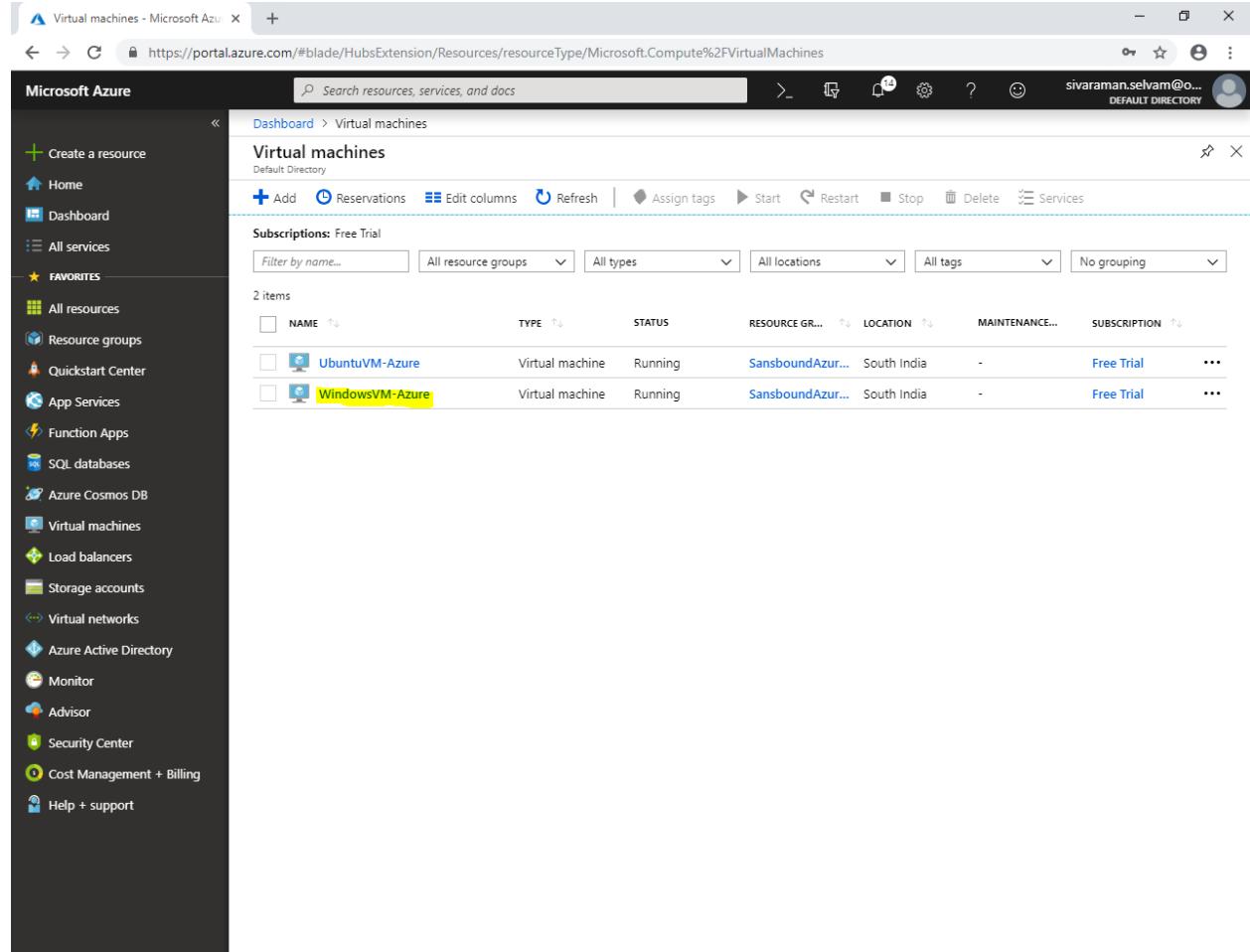


The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various service icons and links like 'Create a resource', 'Home', 'Dashboard', 'All services', 'Favorites' (which includes 'All resources', 'Resource groups', 'Quickstart Center', 'App Services', '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 'NSG-AllowRDPSSH - Subnets' under 'Network security group'. It displays a table with one row:

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

In Dashboard, click “Virtual machines”.

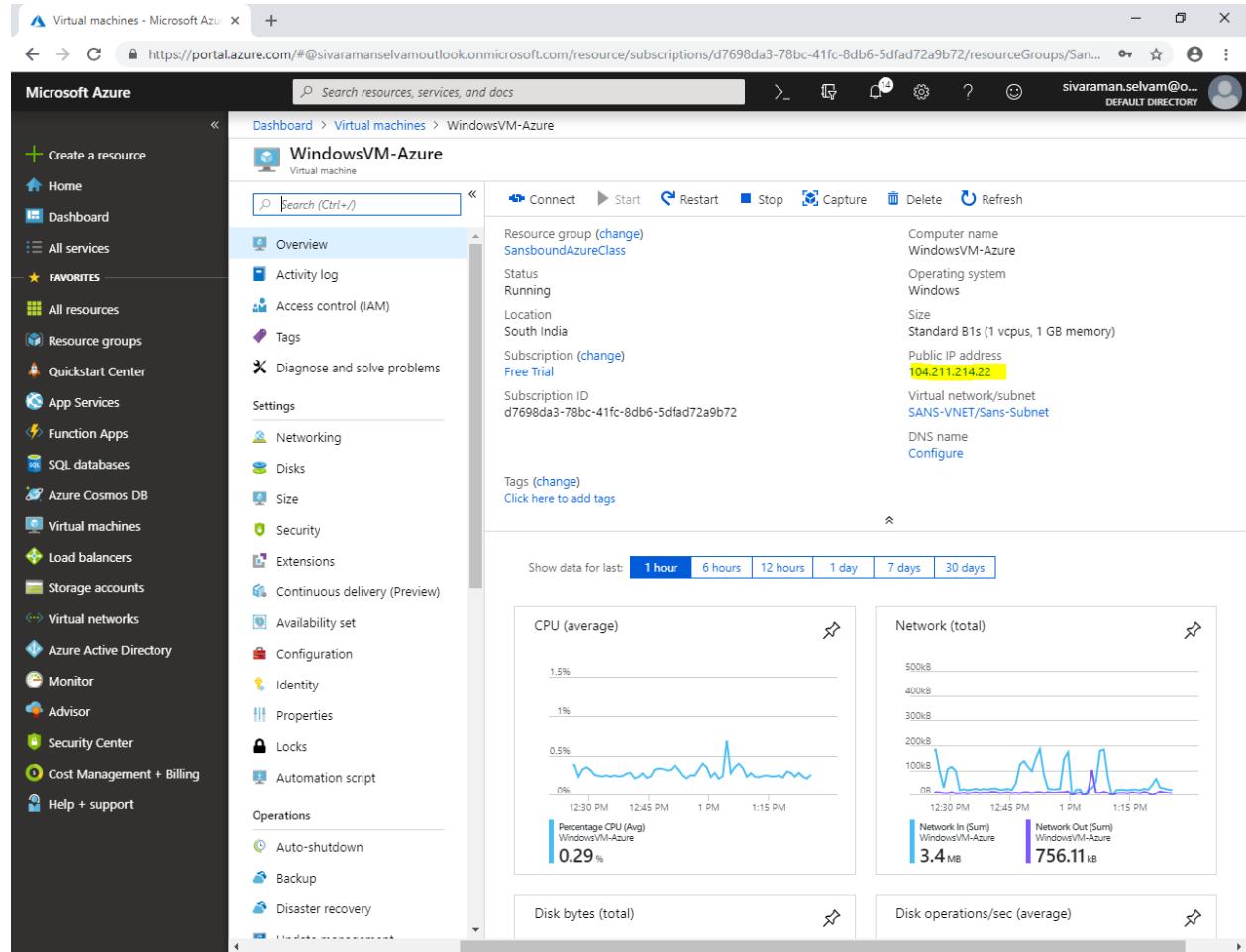
Click on “WindowsVM-Azure” virtual machine.



The screenshot shows the Microsoft Azure portal interface. The left sidebar is the navigation menu with various services like Home, Dashboard, All services, and Favorites. Under Favorites, the 'Virtual machines' icon is selected. The main content area is titled 'Virtual machines' and shows a list of 2 items. The table columns are NAME, TYPE, STATUS, RESOURCE GRP..., LOCATION, MAINTENANCE..., and SUBSCRIPTION. Two rows are 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

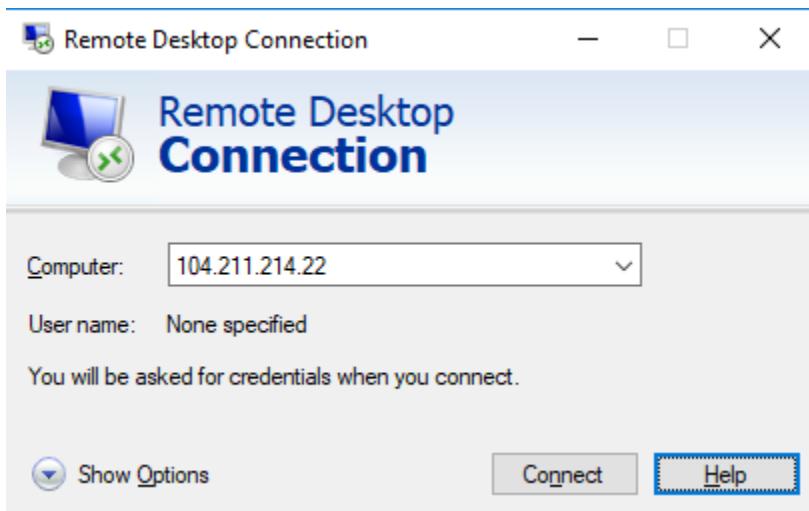
Kindly note the public IP address of “Windows Server 2008 R2”.



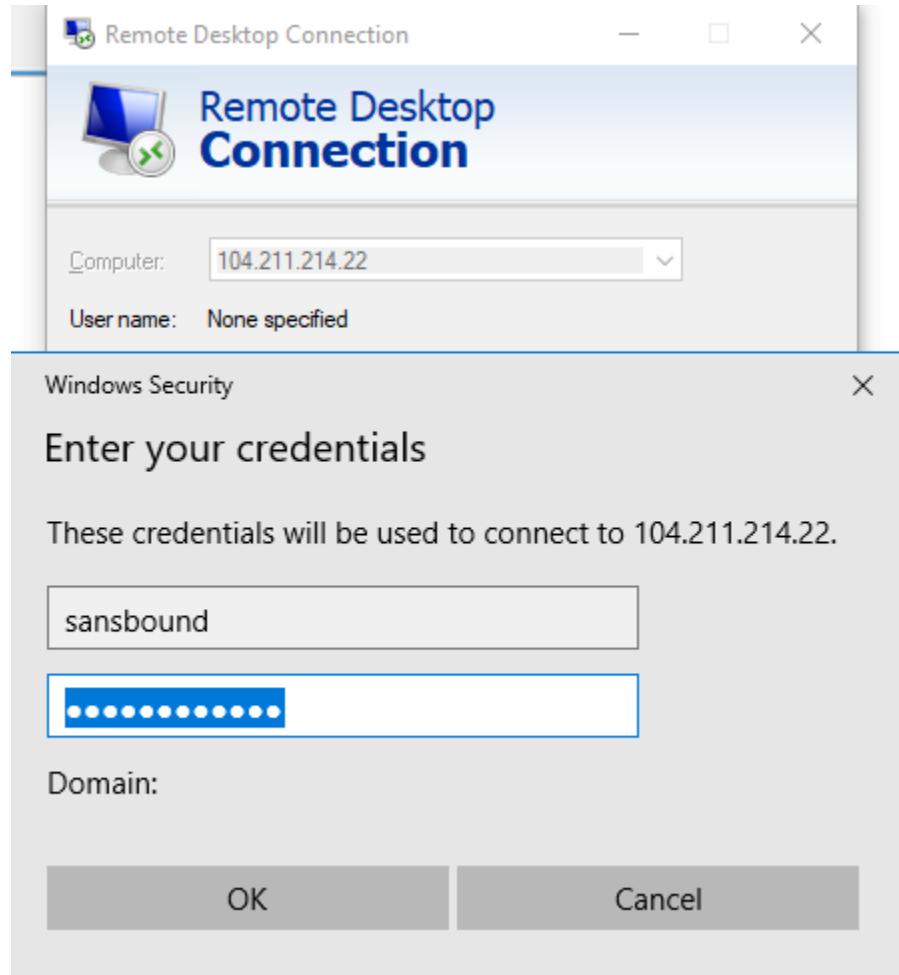
The screenshot shows the Microsoft Azure portal interface for a virtual machine named "WindowsVM-Azure". The left sidebar lists various services like Home, Dashboard, All services, and Favorites. The main content area shows the VM's details, including its resource group (SansboundAzureClass), status (Running), location (South India), and subscription (Free Trial). The Public IP address is prominently displayed as 104.211.214.22. Below the details, there are four performance charts: CPU (average), Network (total), Disk bytes (total), and Disk operations/sec (average), showing usage over the last hour.

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**”.

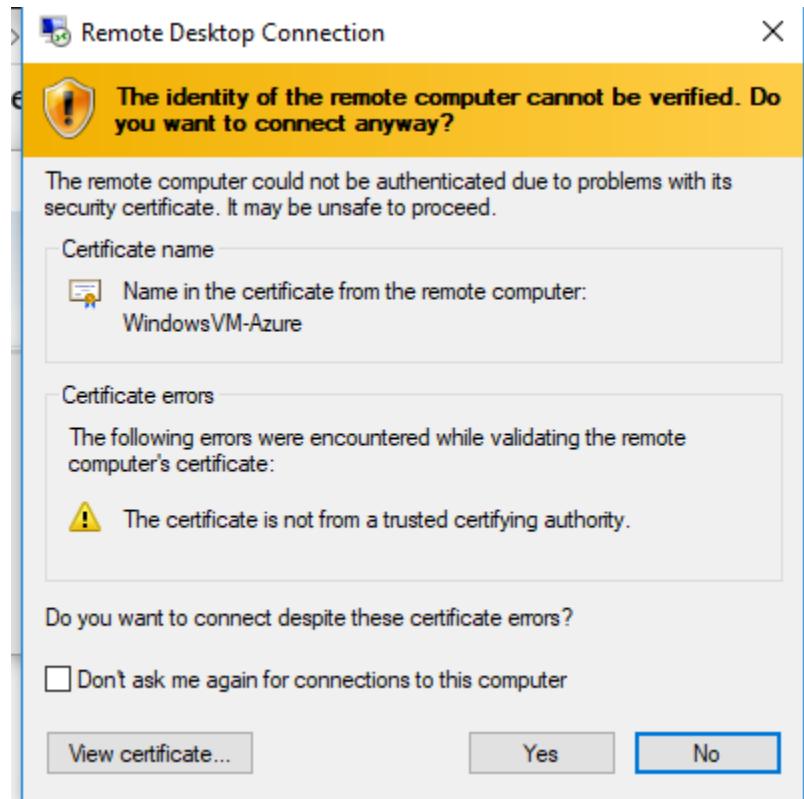


Type **Username and Password** for the Windows 2008 Server R2 which you have provided in Azure portal while creating a virtual machine.



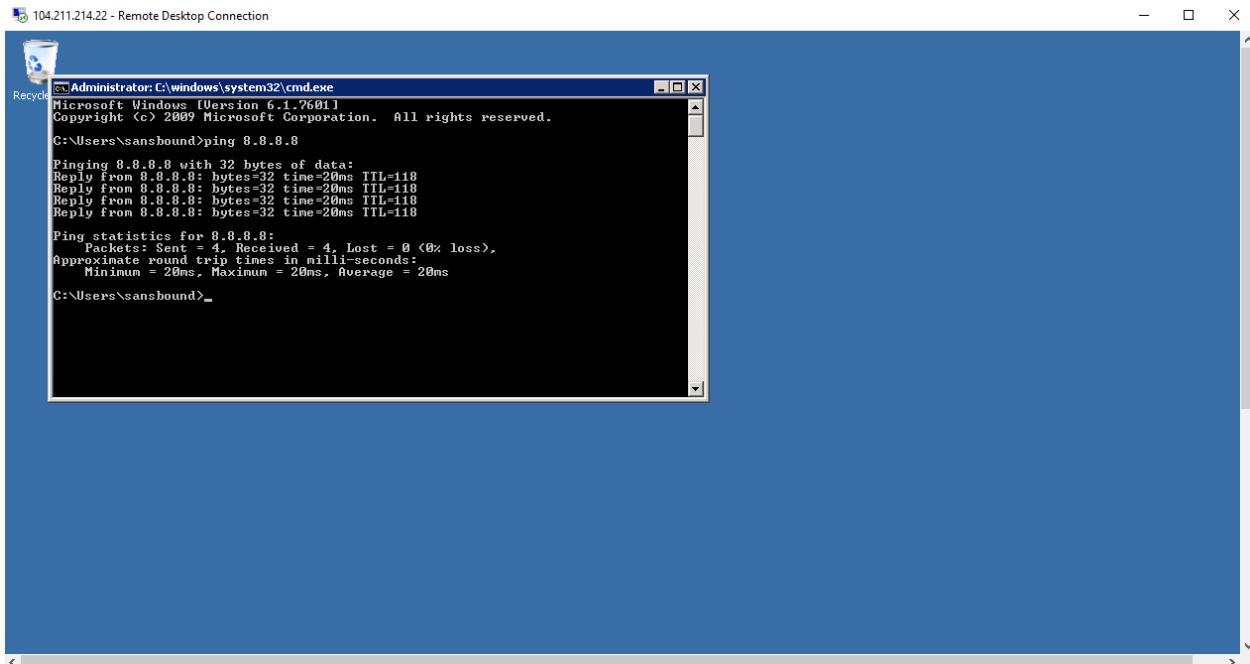
Click "Ok".

Click "Yes".



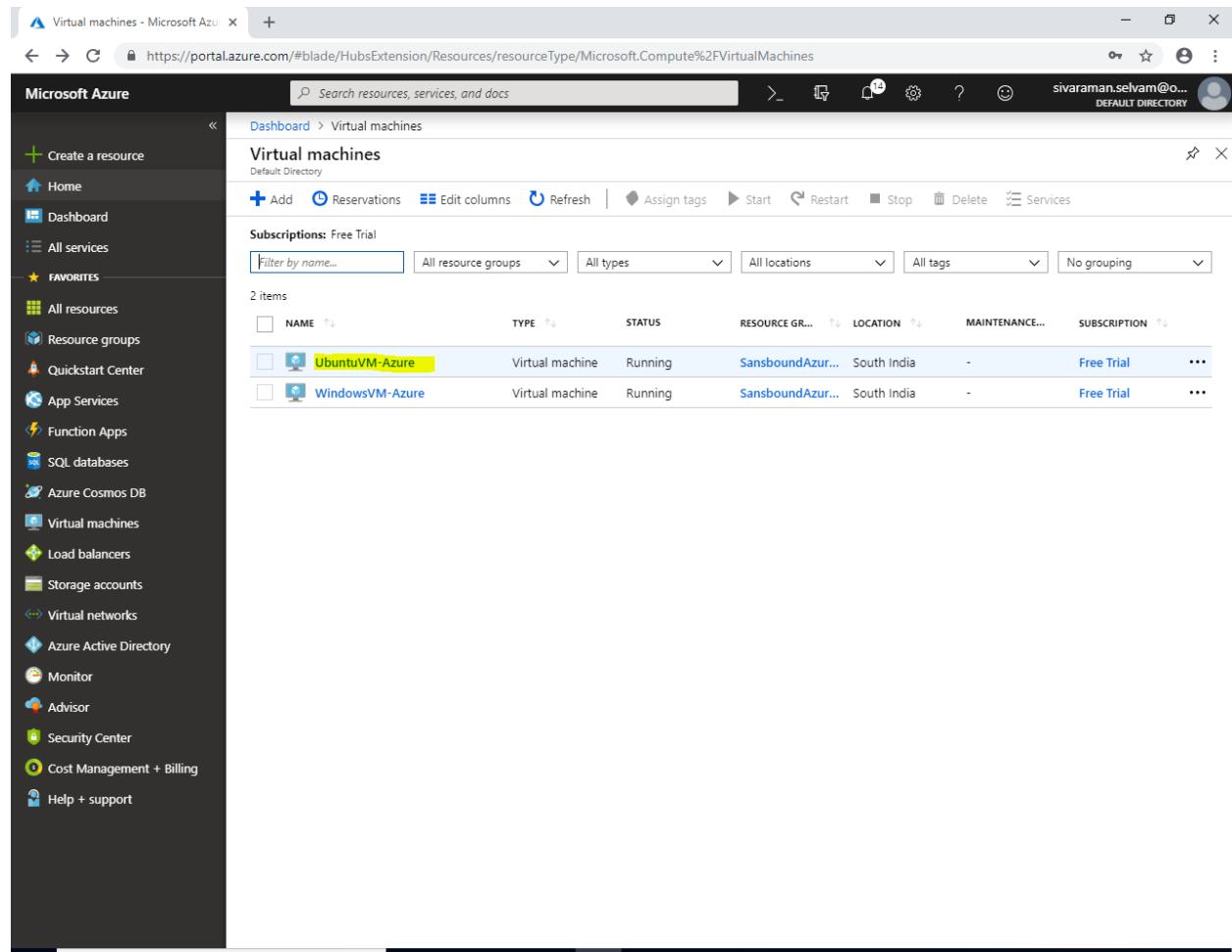
You have accessed windows server through remote successfully.

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”.

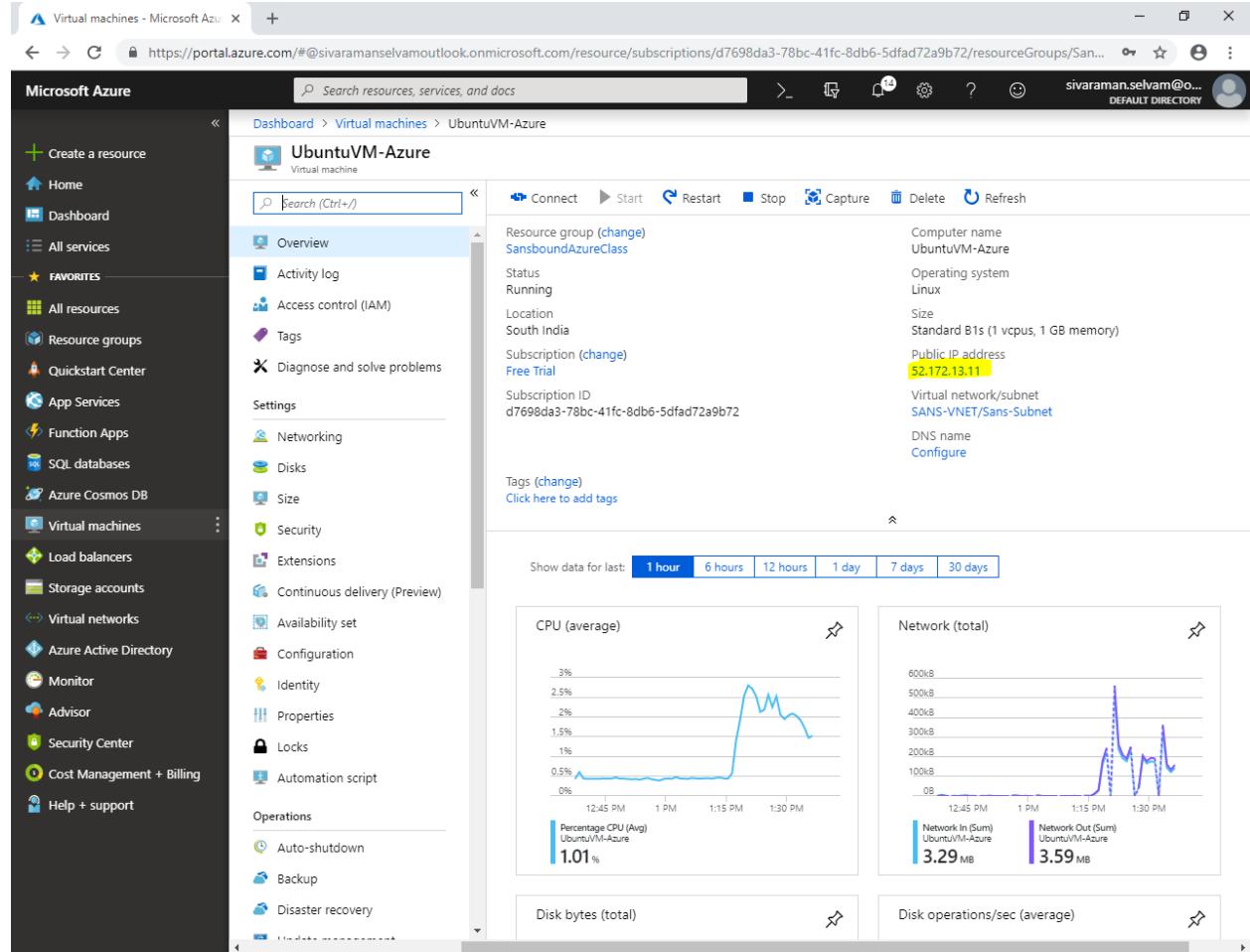
In “Virtual machines”, click on “UbuntuVM-Azure”.



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 "Virtual machines". It displays a table with two items:

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 address provided by azure to access the Ubuntu through SSH.



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

Left Sidebar (Favorites):

- Create a resource
- Home
- Dashboard
- All services
- Favorites** (selected)
- 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

Top Bar:

- Virtual machines - Microsoft Azure
- https://portal.azure.com/#@sivaramselvamoutlook.onmicrosoft.com/resource/subscriptions/d7698da3-78bc-41fc-8db6-5dfad72a9b72/resourceGroups/San...
- Microsoft Azure
- Search resources, services, and docs
- Dashboard > Virtual machines > UbuntuVM-Azure
- sivaraman.selvam@o...
DEFAULT DIRECTORY

UbuntuVM-Azure Overview Page:

Resource Group: SansboundAzureClass

Status: Running

Location: South India

Subscription: Free Trial

Subscription ID: d7698da3-78bc-41fc-8db6-5dfad72a9b72

Computer name: UbuntuVM-Azure

Operating system: Linux

Size: Standard B1s (1 vcpus, 1 GB memory)

Public IP address: 52.172.13.11

Virtual network/subnet: SANS-VNET/Sans-Subnet

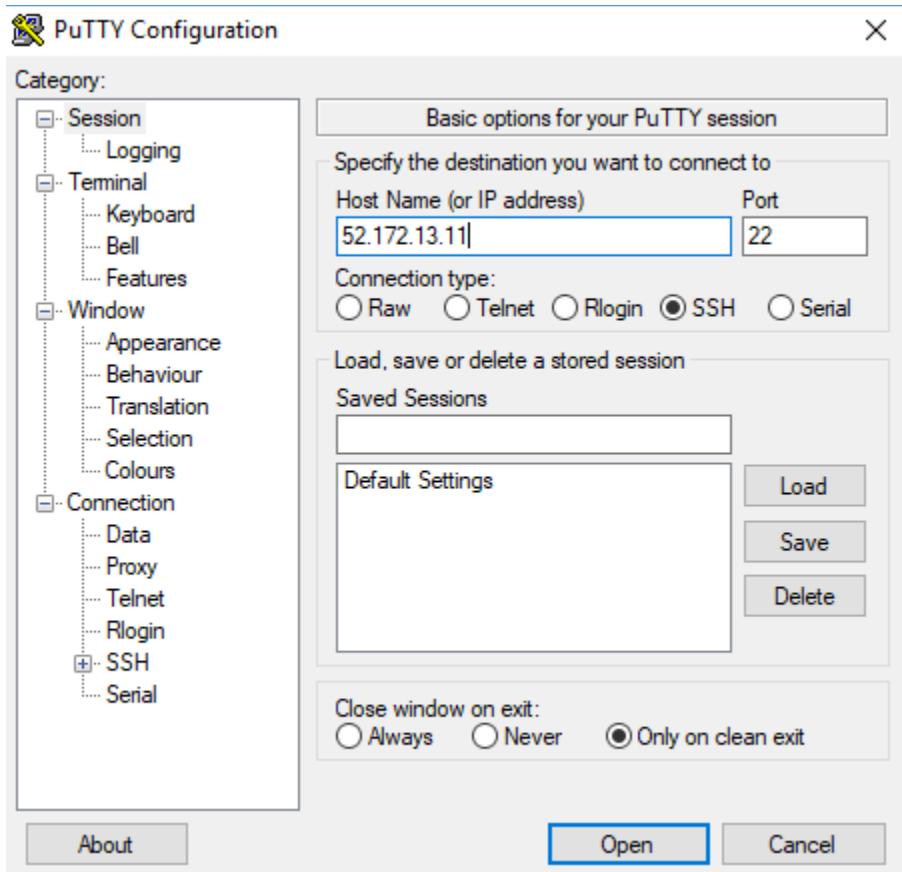
DNS name: Configure

Tags: Click here to add tags

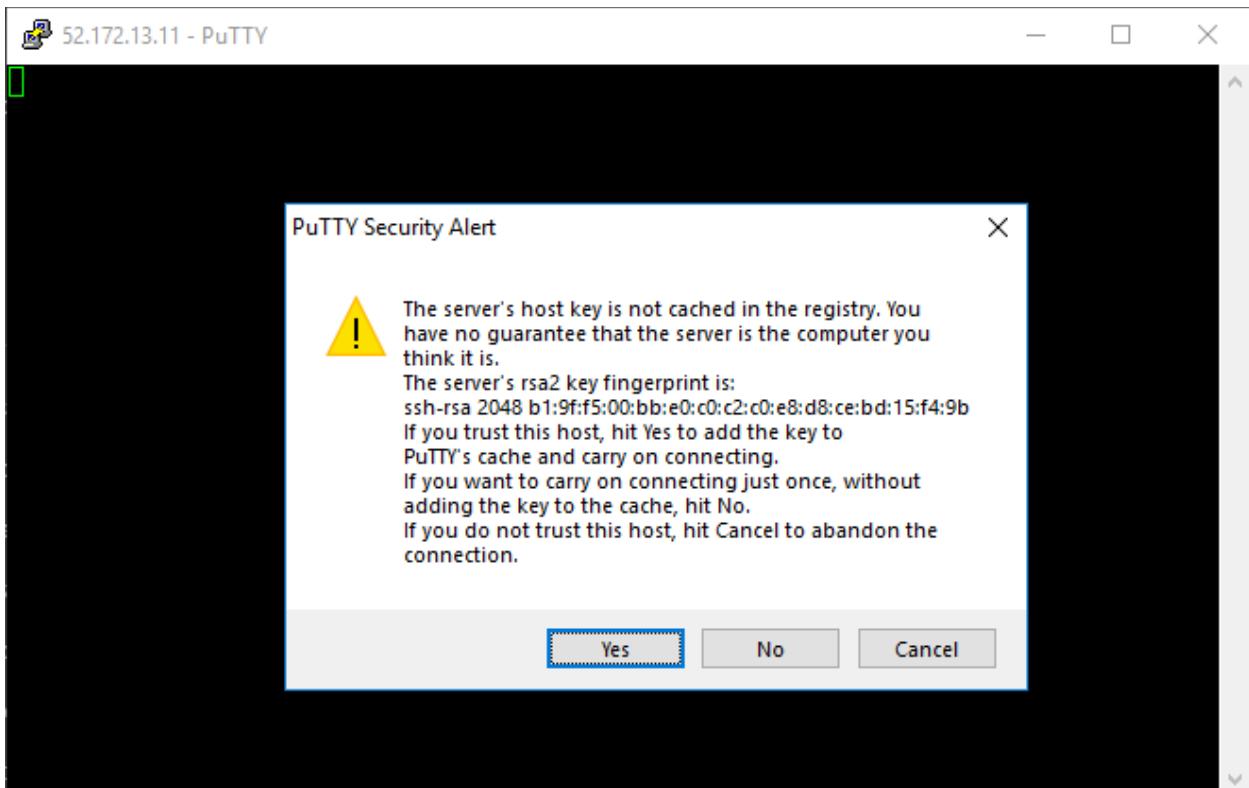
Metrics (Recent 1 hour):

- CPU (average):** Percentage CPU (Avg) UbuntuVM-Azure 1.01 %
- Network (total):** Network In (Sum) UbuntuVM-Azure 3.29 MB, Network Out (Sum) UbuntuVM-Azure 3.59 MB
- Disk bytes (total):**
- Disk operations/sec (average):**

Click “Open” to connect “Ubuntu”.



Click "Yes".

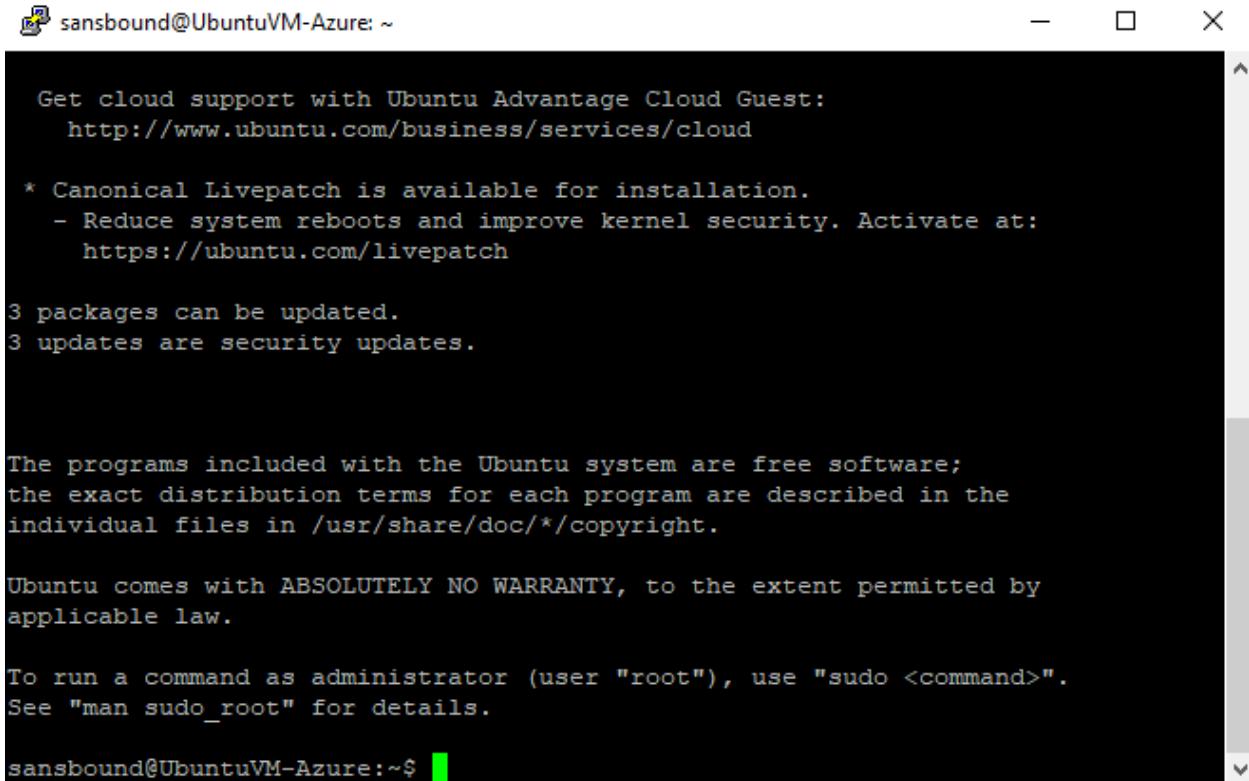


Type user name of the Ubuntu server as “**sansbound**” and press “**Enter**”.



A screenshot of a PuTTY terminal window titled "52.172.13.11 - PuTTY". The window shows a login prompt: "login as: sansbound" followed by "sansbound@52.172.13.11's password: [REDACTED]". The password field is redacted with a green bar. The rest of the window is blacked out.

I have successfully logged into the Ubuntu VM successfully.



```
sansbound@UbuntuVM-Azure: ~

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

* Canonical Livepatch is available for installation.
- Reduce system reboots and improve kernel security. Activate at:
  https://ubuntu.com/livepatch

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:~$
```

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.