

Lab21 – Understanding VNET Peering between Two VNET's in same Region – Azure

Virtual network (VNET) peering:

Virtual network peering enables you to seamlessly connect two Azure [virtual networks](#). Once peered, the virtual networks appear as one, for connectivity purposes. The traffic between virtual machines in the peered virtual networks is routed through the Microsoft backbone infrastructure, much like traffic is routed between virtual machines in the same virtual network, through *private* IP addresses only. Azure supports:

- VNet peering - connecting VNets within the same Azure region
- Global VNet peering - connecting VNets across Azure regions

The benefits of using virtual network peering, whether local or global, include:

- Network traffic between peered virtual networks is private. Traffic between the virtual networks is kept on the Microsoft backbone network. No public Internet, gateways, or encryption is required in the communication between the virtual networks.
- A low-latency, high-bandwidth connection between resources in different virtual networks.
- The ability for resources in one virtual network to communicate with resources in a different virtual network, once the virtual networks are peered.
- The ability to transfer data across Azure subscriptions, deployment models, and across Azure regions.
- The ability to peer virtual networks created through the Azure Resource Manager or to peer one virtual network created through Resource Manager to a virtual network created through the classic deployment model. To learn more about Azure deployment models, see [Understand Azure deployment models](#).
- No downtime to resources in either virtual network when creating the peering, or after the peering is created.

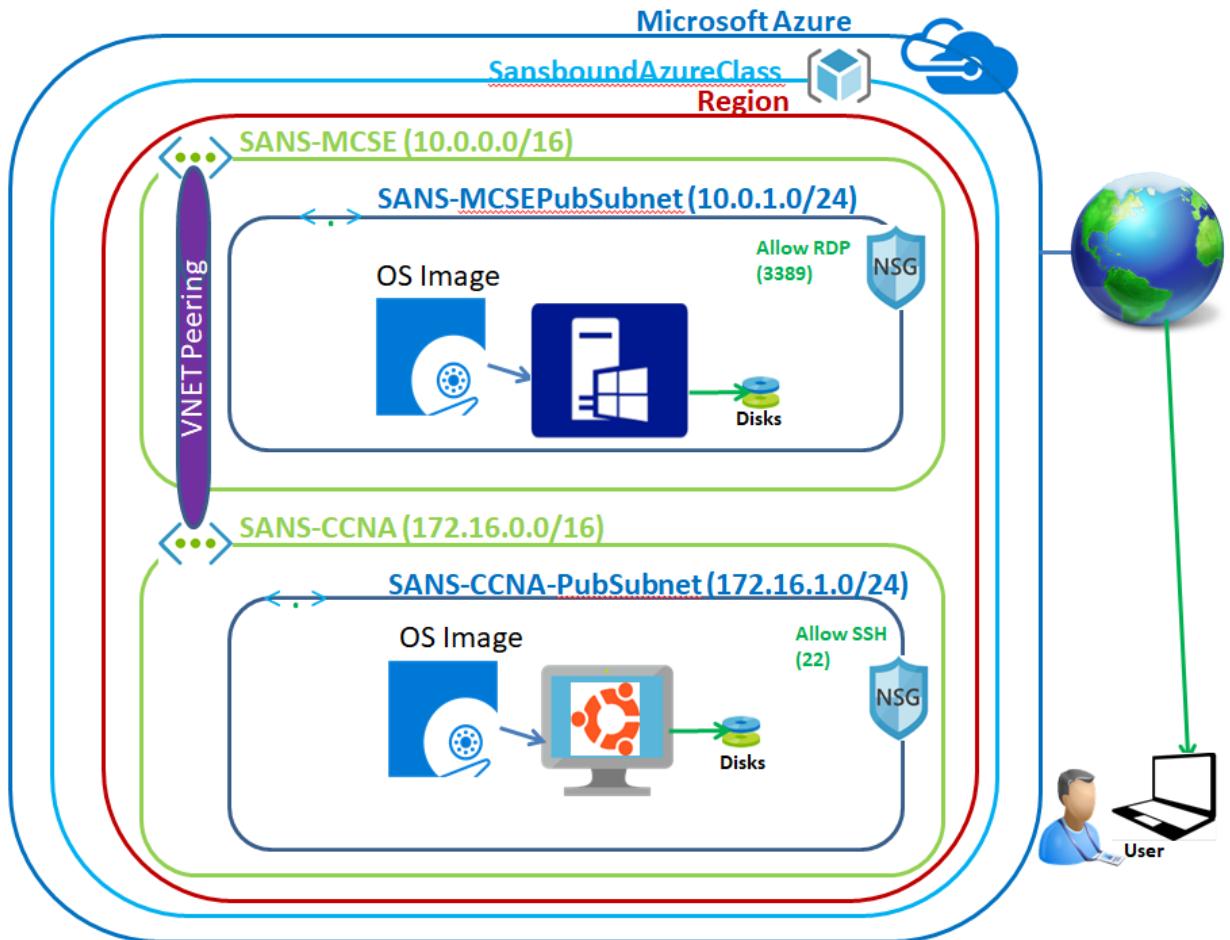
Connectivity

After virtual networks are peered, resources in either virtual network can directly connect with resources in the peered virtual network.

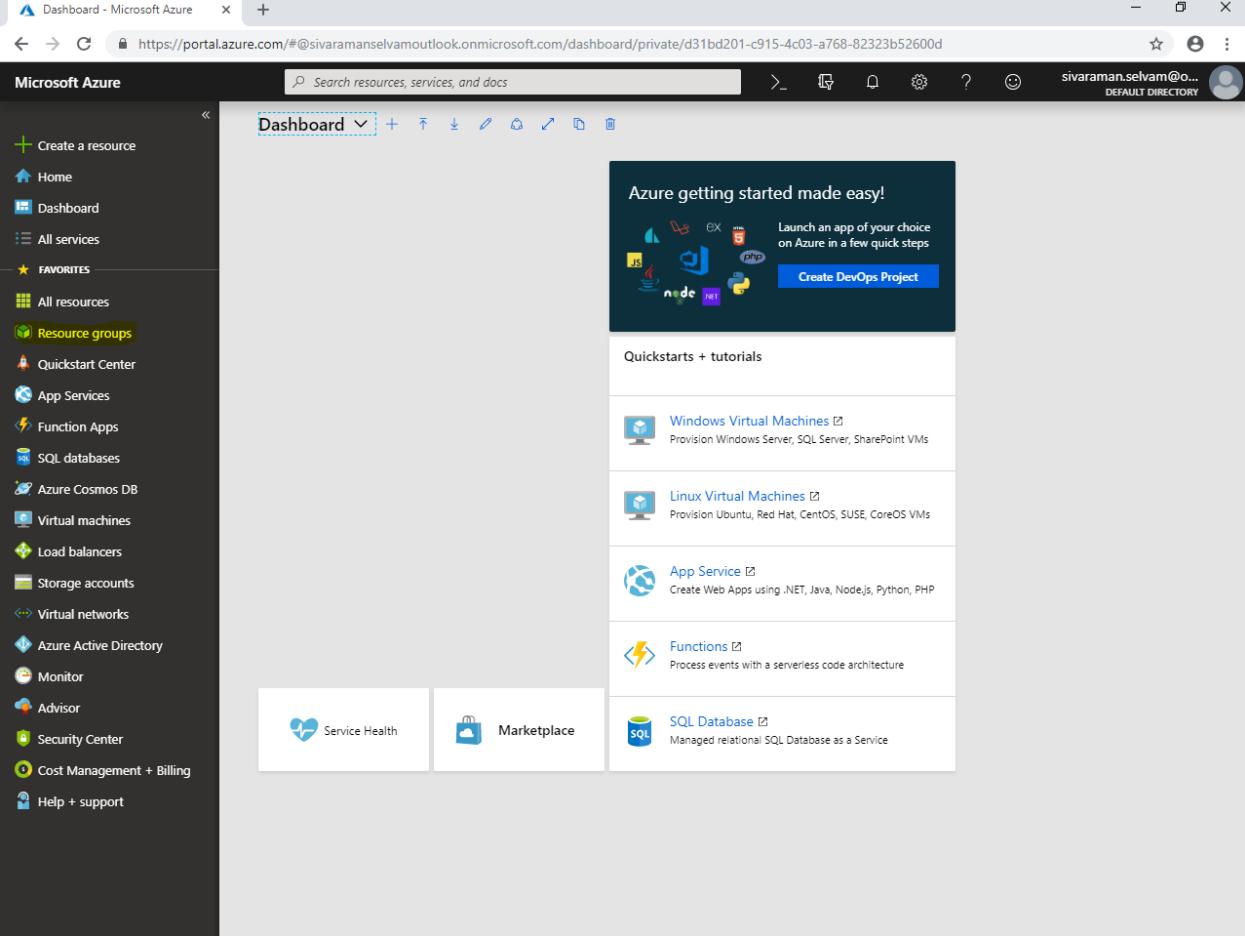
The network latency between virtual machines in peered virtual networks in the same region is the same as the latency within a single virtual network. The network throughput is based on the bandwidth that's allowed for the virtual machine, proportionate to its size. There isn't any additional restriction on bandwidth within the peering.

The traffic between virtual machines in peered virtual networks is routed directly through the Microsoft backbone infrastructure, not through a gateway or over the public Internet.

Network security groups can be applied in either virtual network to block access to other virtual networks or subnets, if desired. When configuring virtual network peering, you can either open or close the network security group rules between the virtual networks. If you open full connectivity between peered virtual networks (which is the default option), you can apply network security groups to specific subnets or virtual machines to block or deny specific access.

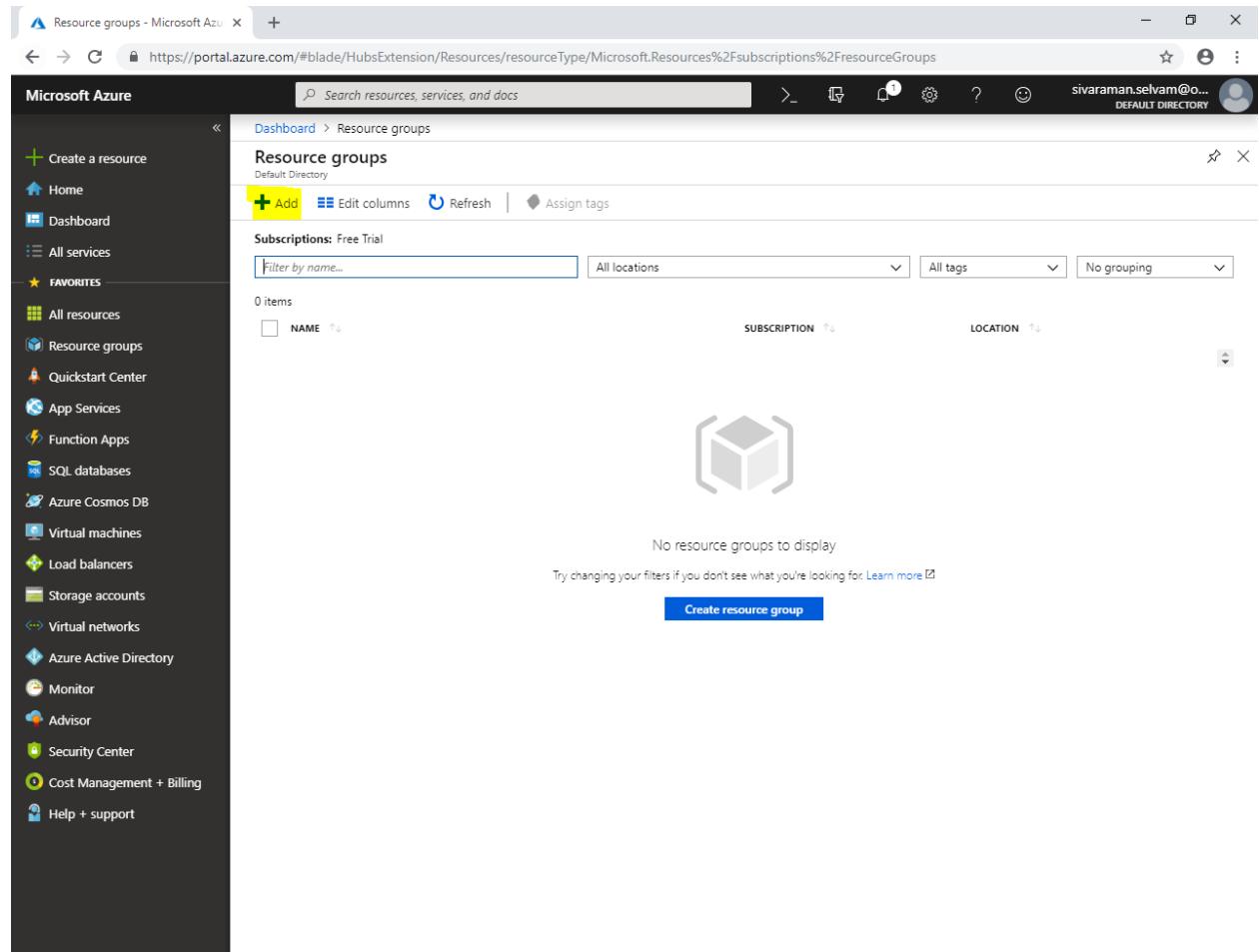
Topology:

In Azure portal, click “Resource group”.



The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various options like Home, Dashboard, All services, Favorites, Resource groups (which is highlighted), 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 features a "Dashboard" header with a search bar and several quick access icons. Below the dashboard is a large promotional box titled "Azure getting started made easy!" with a "Create DevOps Project" button. To the right of this is a "Quickstarts + tutorials" section containing links to Windows Virtual Machines, Linux Virtual Machines, App Service, Functions, and SQL Database. At the bottom of the main content area are two buttons: "Service Health" and "Marketplace".

Click “Add”.



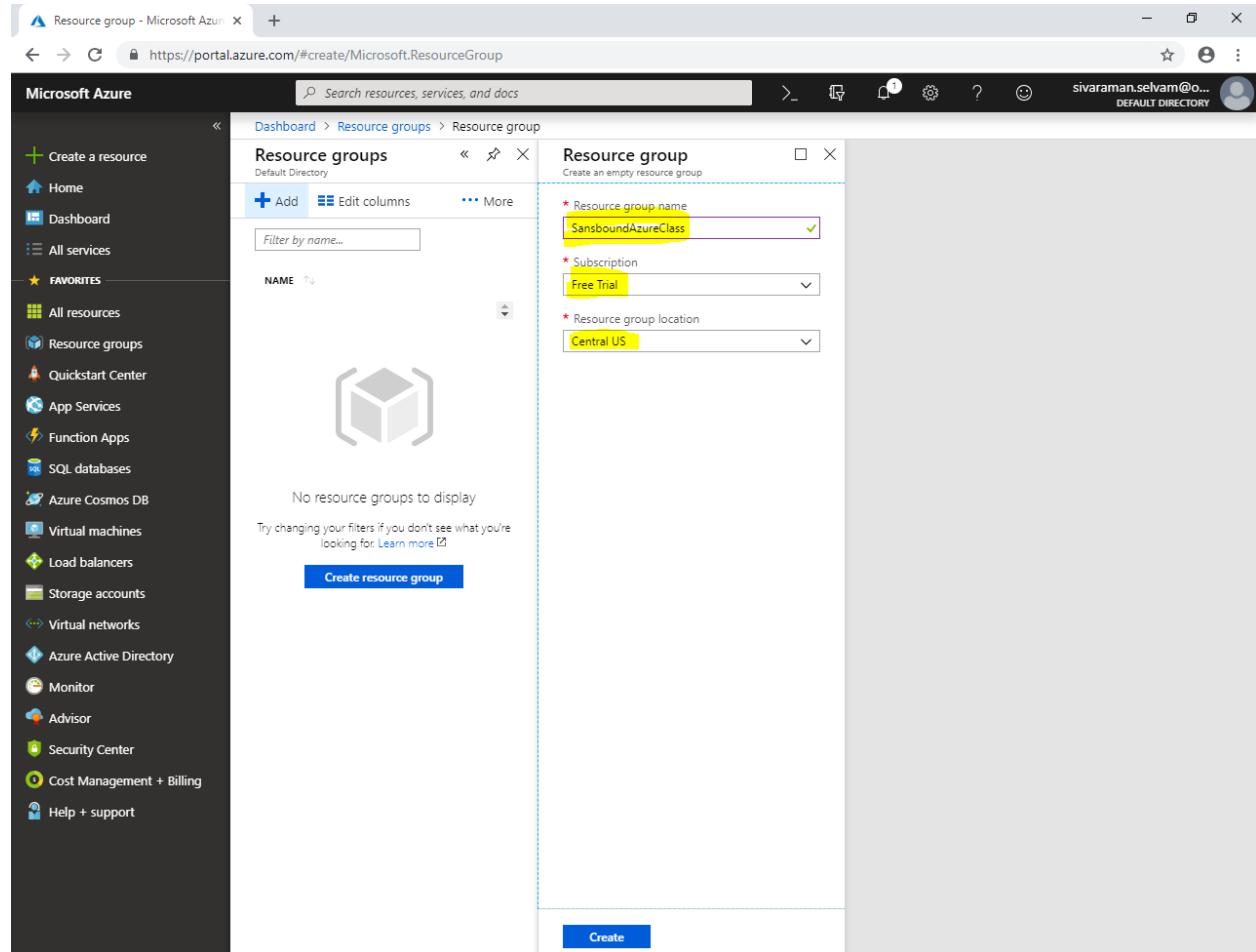
The screenshot shows the Microsoft Azure Resource Groups page. The left sidebar contains a navigation menu with various service icons and links. The main content area is titled "Resource groups" and shows a table with one row. The row has a yellow background and contains the text "+ Add". The table has columns for NAME, SUBSCRIPTION, and LOCATION. A large gray cube icon is centered below the table. Below the table, the text "No resource groups to display" is displayed, followed by a link "Try changing your filters if you don't see what you're looking for." At the bottom right of the main content area is a blue button labeled "Create resource group".

While create “Resource group”,

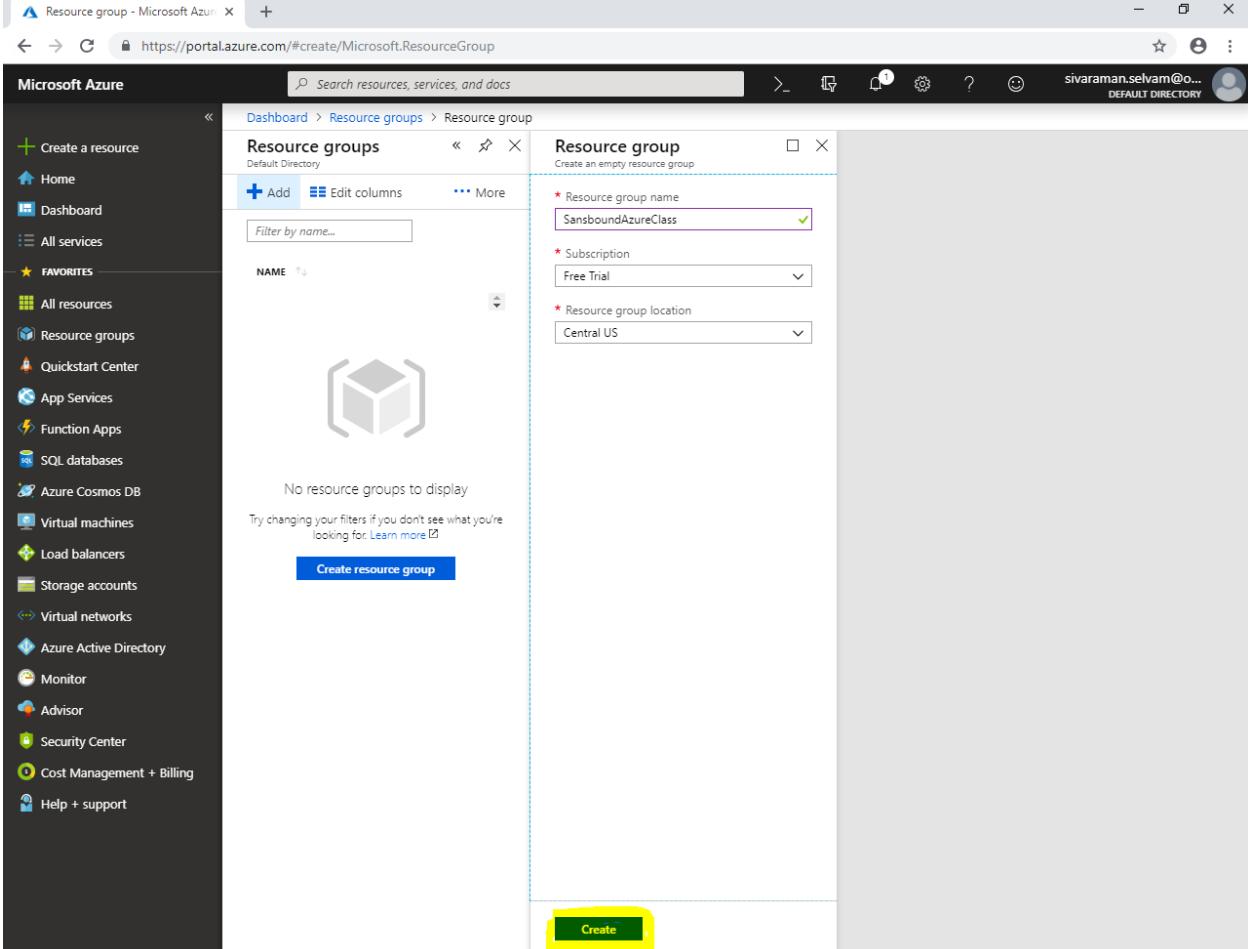
Type “Resource group name” as “**SansboundAzureClass**”.

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

Select “Resource group location” as “**Central US**”.

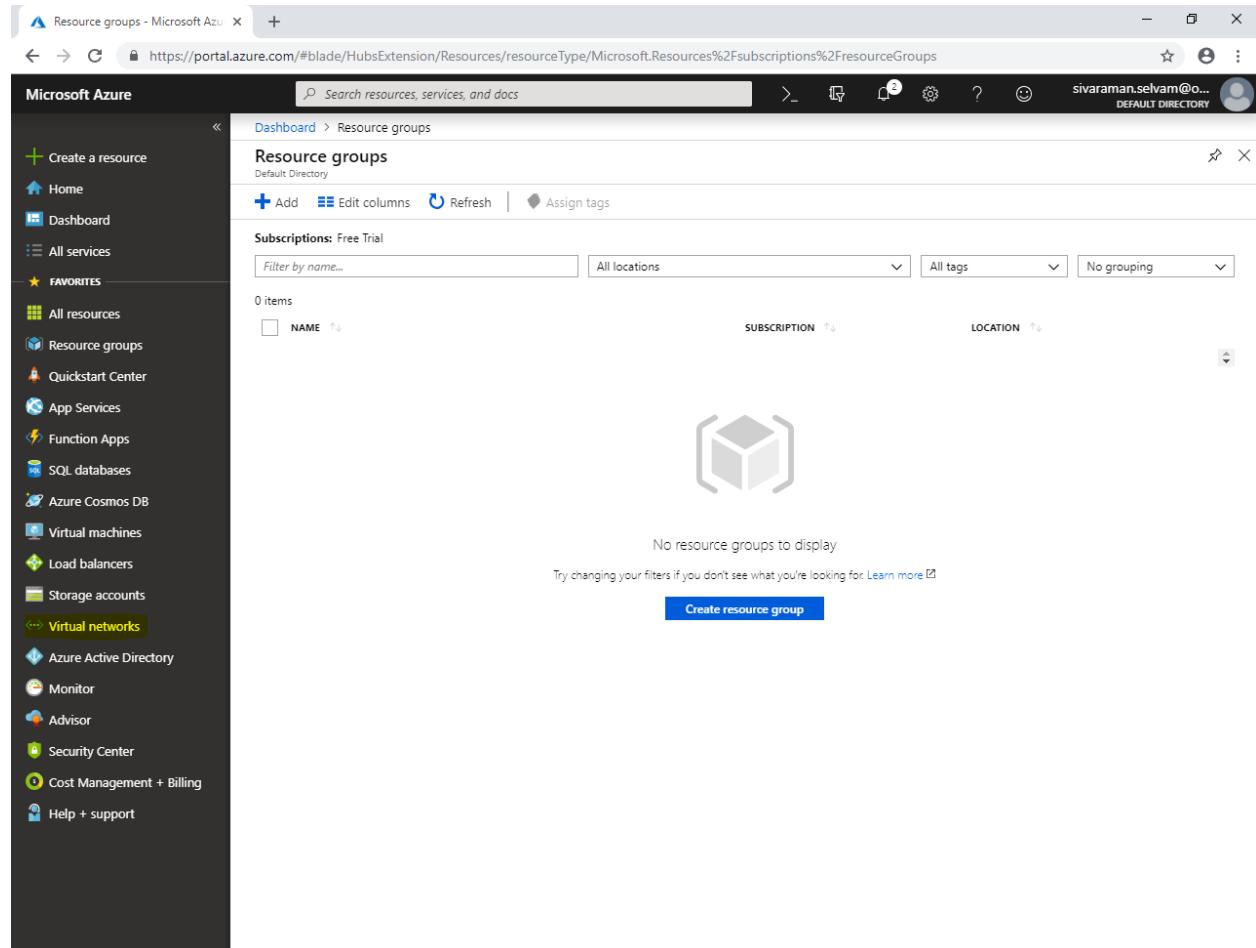


Click “Create”.



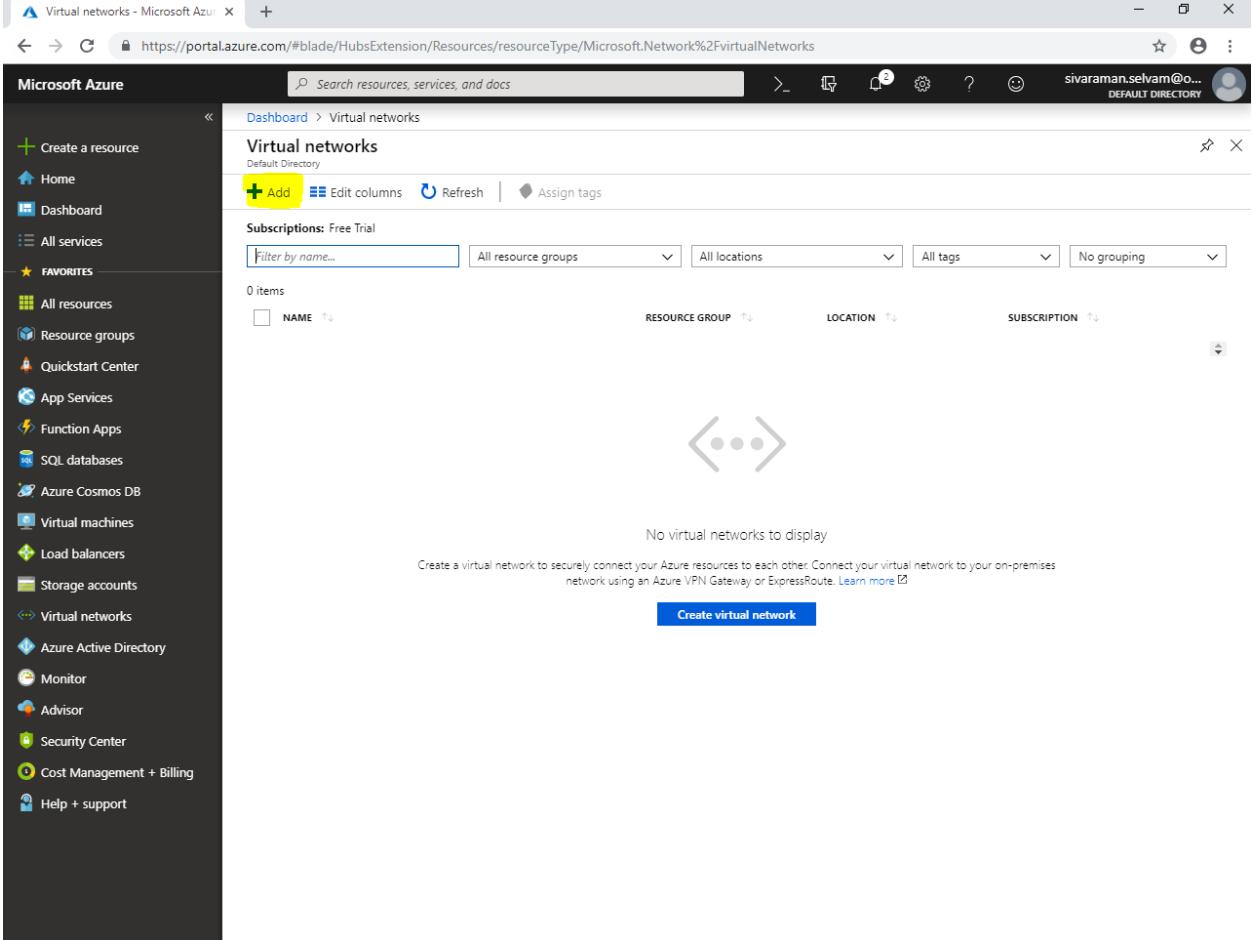
The screenshot shows the Microsoft Azure portal interface for creating a new resource group. The left sidebar contains various service links like Home, Dashboard, and Resource groups. The main area shows a 'Resource groups' table with one entry and a 'Create resource group' button. A detailed 'Resource group' configuration dialog is open on the right, prompting for a name ('SansboundAzureClass'), subscription ('Free Trial'), and location ('Central US'). A yellow box highlights the 'Create' button at the bottom of the dialog.

Click "Virtual Networks".



The screenshot shows the Microsoft Azure portal interface. The left sidebar is open, displaying various service categories. The 'Virtual networks' option is highlighted with a yellow box, indicating it is the selected item. The main content area is titled 'Resource groups' and shows a message stating 'No resource groups to display'. It includes a 'Create resource group' button and filter options for 'NAME', 'SUBSCRIPTION', and 'LOCATION'.

Click "Add".



The screenshot shows the Microsoft Azure portal interface for managing virtual networks. The left sidebar contains a navigation menu with various service icons. The main content area is titled 'Virtual networks' and displays a table with one row, indicating '0 items'. The table has columns for NAME, RESOURCE GROUP, LOCATION, and SUBSCRIPTION. At the top of the table, there are buttons for '+ Add', 'Edit columns', 'Refresh', and 'Assign tags'. A search bar at the top of the page includes filters for 'Filter by name...', 'All resource groups', 'All locations', 'All tags', and 'No grouping'. Below the table, a message encourages creating a virtual network to securely connect resources. A prominent blue 'Create virtual network' button is located at the bottom right of the page.

While create “Virtual network”.

Type “Name” as “**SANS-MCSE**”.

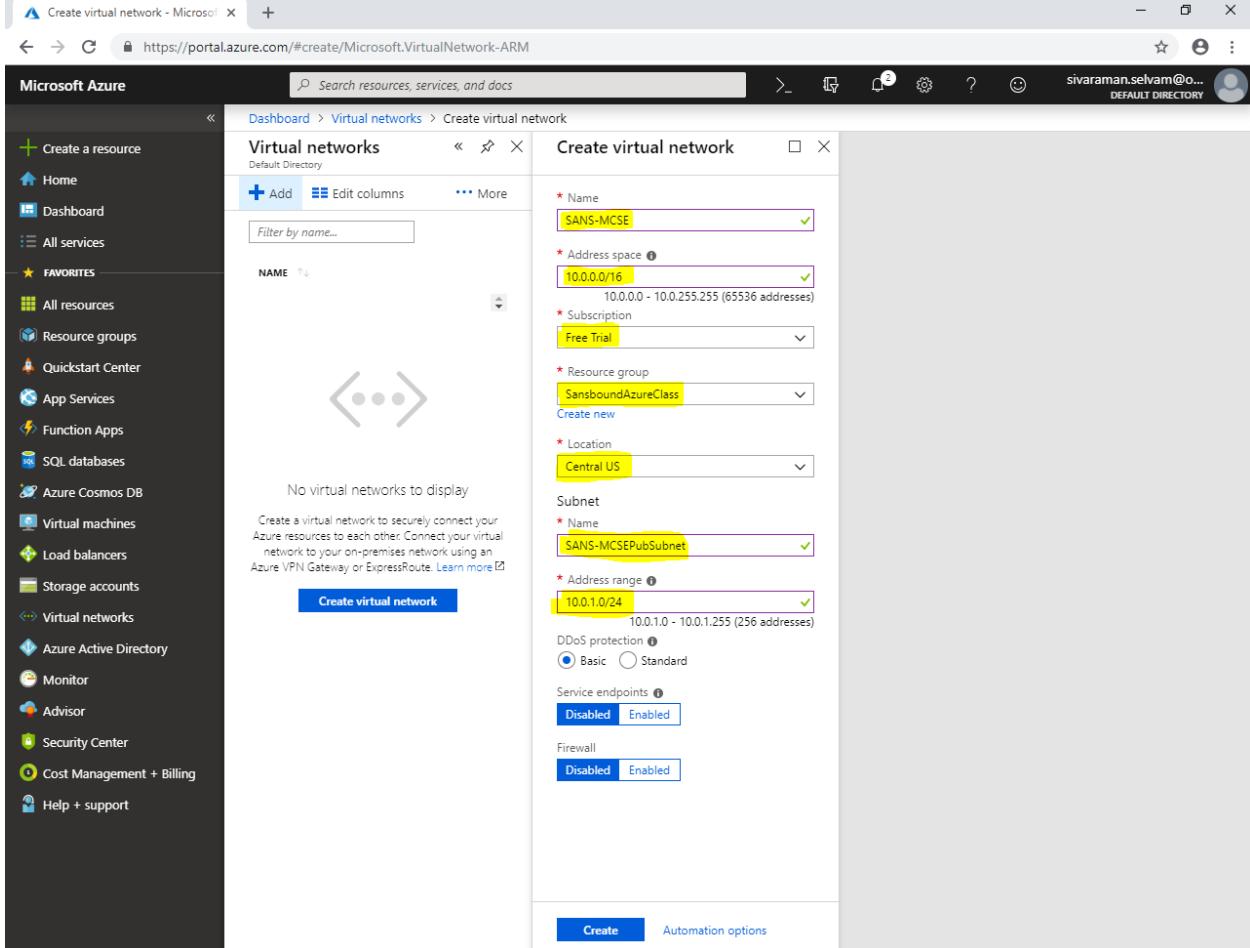
Type “Address space” as “**10.0.0.0/16**”.

Select “Subscription” as “**SansboundAzureClass**”.

Select “Location” as “**Central US**”.

Type “Subnet” name as “**SANS-MCSEPubSubnet**”.

Type “Address range” as “**10.0.1.0/24**”.

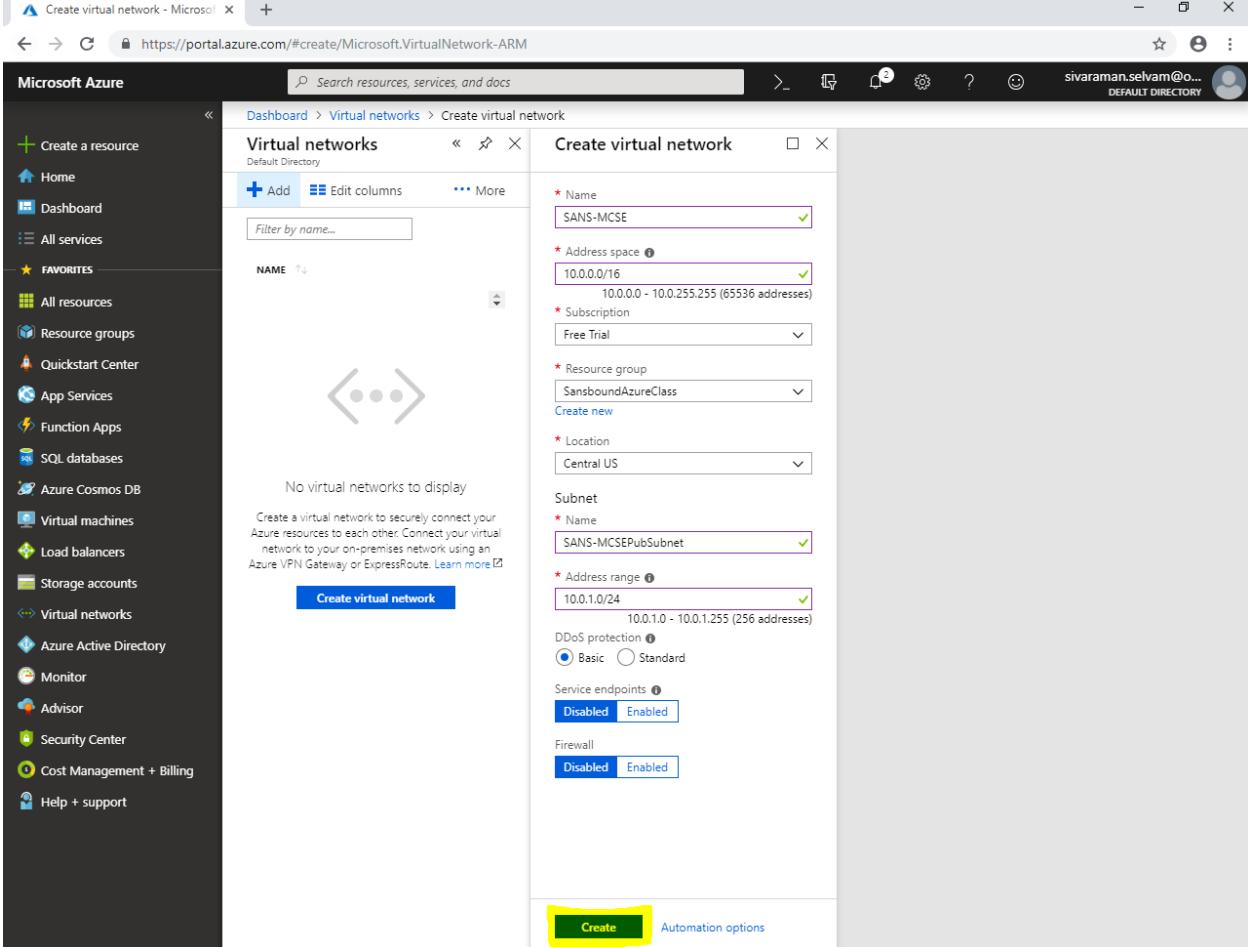


The screenshot shows the Microsoft Azure portal interface for creating a virtual network. The left sidebar navigation includes 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES' (with 'Virtual networks' selected), 'All resources', 'Resource groups', 'Quickstart Center', 'App Services', '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', and 'Help + support'. The main content area is titled 'Create virtual network' under 'Virtual networks'. It displays the following configuration:

- Name:** SANS-MCSE
- Address space:** 10.0.0.0/16 (10.0.0.0 - 10.0.255.255 (65536 addresses))
- Subscription:** Free Trial
- Resource group:** SansboundAzureClass
- Location:** Central US
- Subnet:**
 - Name:** SANS-MCSEPubSubnet
 - Address range:** 10.0.1.0/24 (10.0.1.0 - 10.0.1.255 (256 addresses))
 - DDoS protection:** Basic (radio button selected)
 - Service endpoints:** Disabled (radio button selected)
 - Firewall:** Disabled (radio button selected)

At the bottom of the form are 'Create' and 'Automation options' buttons.

Click “Create”.

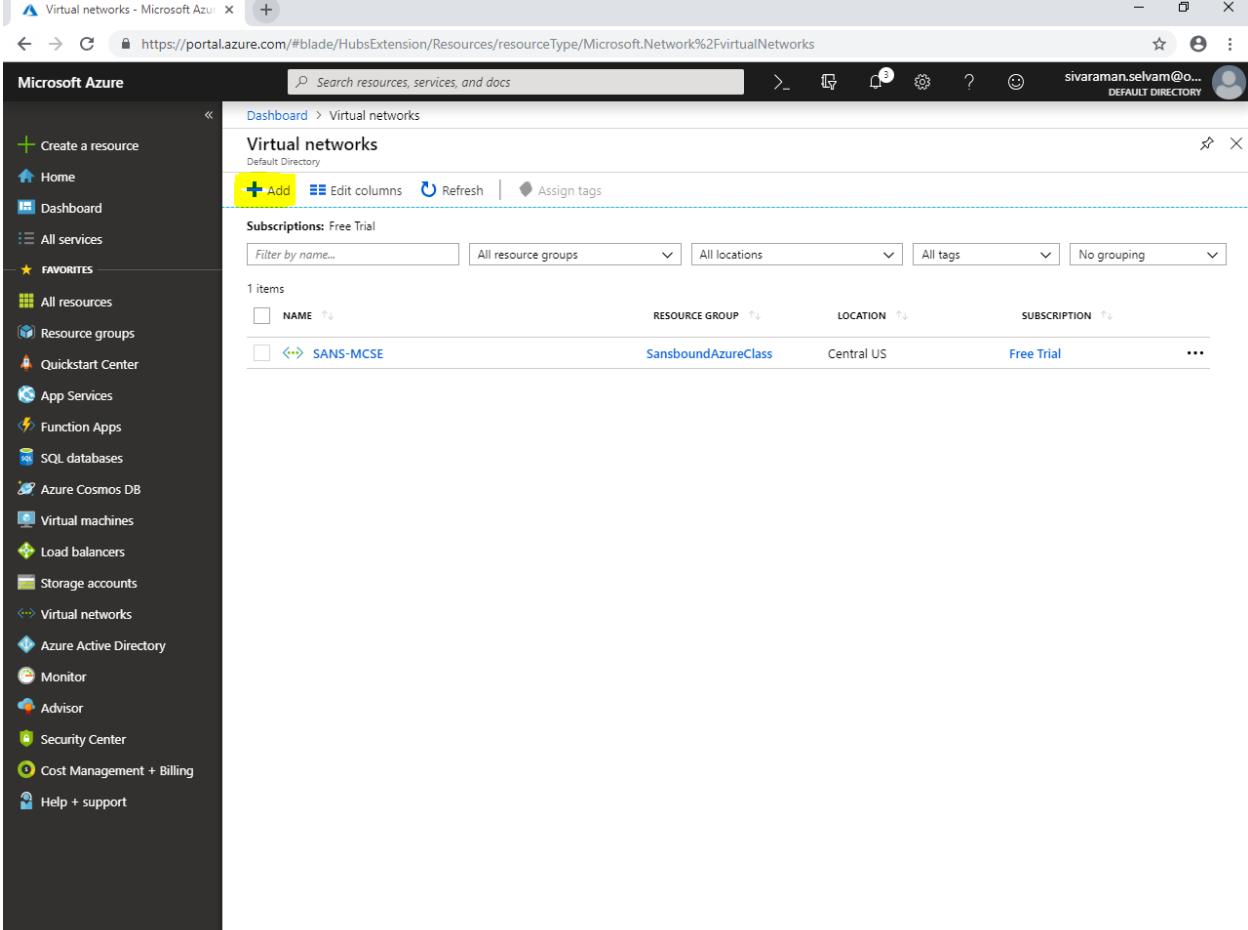


The screenshot shows the Microsoft Azure portal interface for creating a virtual network. The left sidebar contains various service icons, and the main area is titled "Create virtual network". The "Virtual networks" table on the left has one entry: "NAME" (SANS-MCSE). The right panel is titled "Create virtual network" and contains the following fields:

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

At the bottom right of the right panel, there is a large green "Create" button, which is highlighted with a yellow box. Below it is a link for "Automation options".

Click "Add".



The screenshot shows the Microsoft Azure portal interface. The left sidebar is open, showing various service categories like Home, Dashboard, All services, and Favorites. Under Favorites, the 'Virtual networks' option is selected. The main content area is titled 'Virtual networks' and shows a single item named 'SANS-MCSE' under the 'Subscriptions: Free Trial' section. The 'Add' button, located at the top left of the list, is highlighted with a yellow box.

NAME	RESOURCE GROUP	LOCATION	SUBSCRIPTION
SANS-MCSE	SansboundAzureClass	Central US	Free Trial

While create “Virtual network”,

Type “Name” as “**172.16.0.0/16**”.

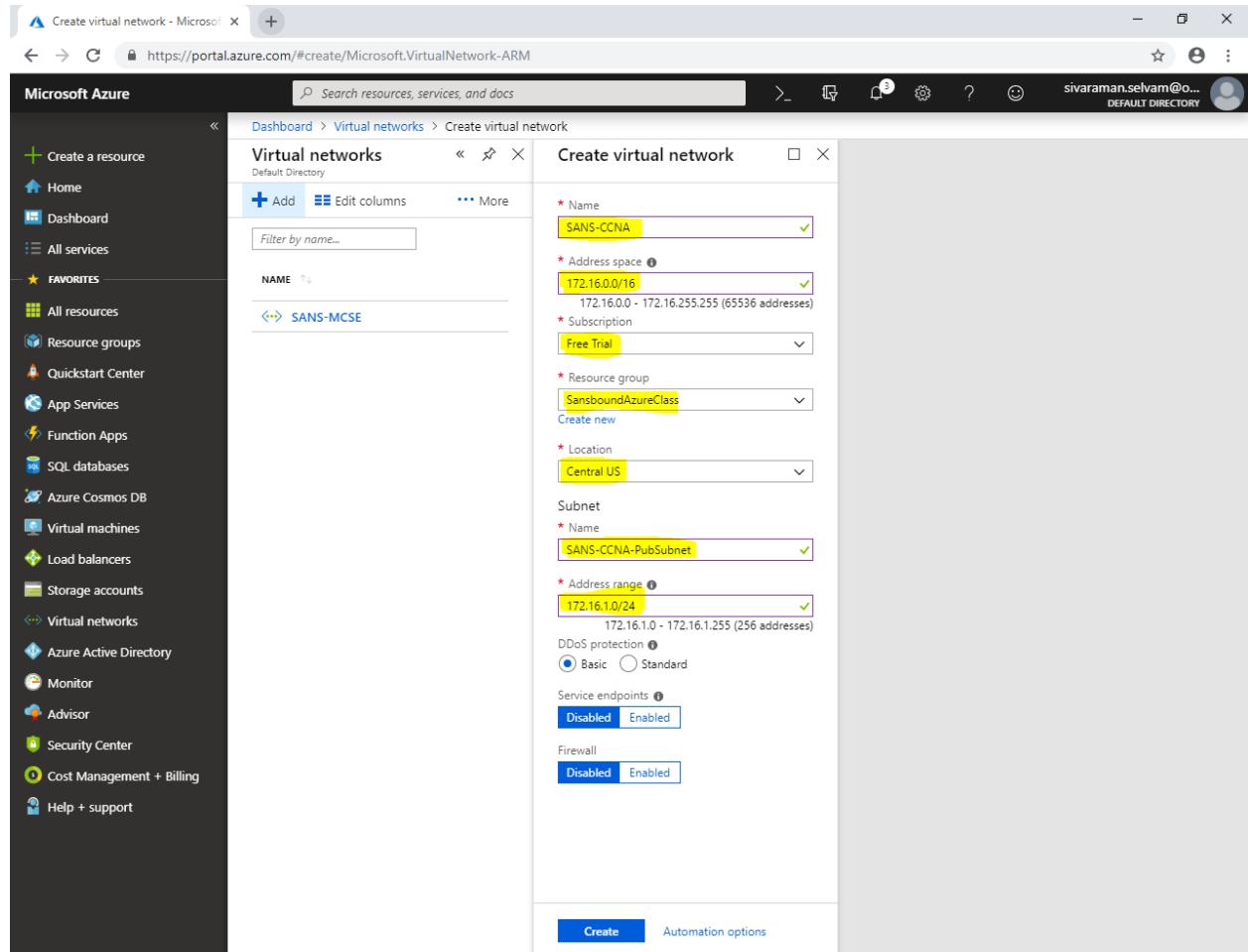
Select “Subscription” as “**Free Trial**”.

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

Select “Location” as “**Central US**”.

Type “Subnet” name as “**SANS-CCNA-PubSubnet**”.

Type “Address range” as “**172.16.1.0/24**”.

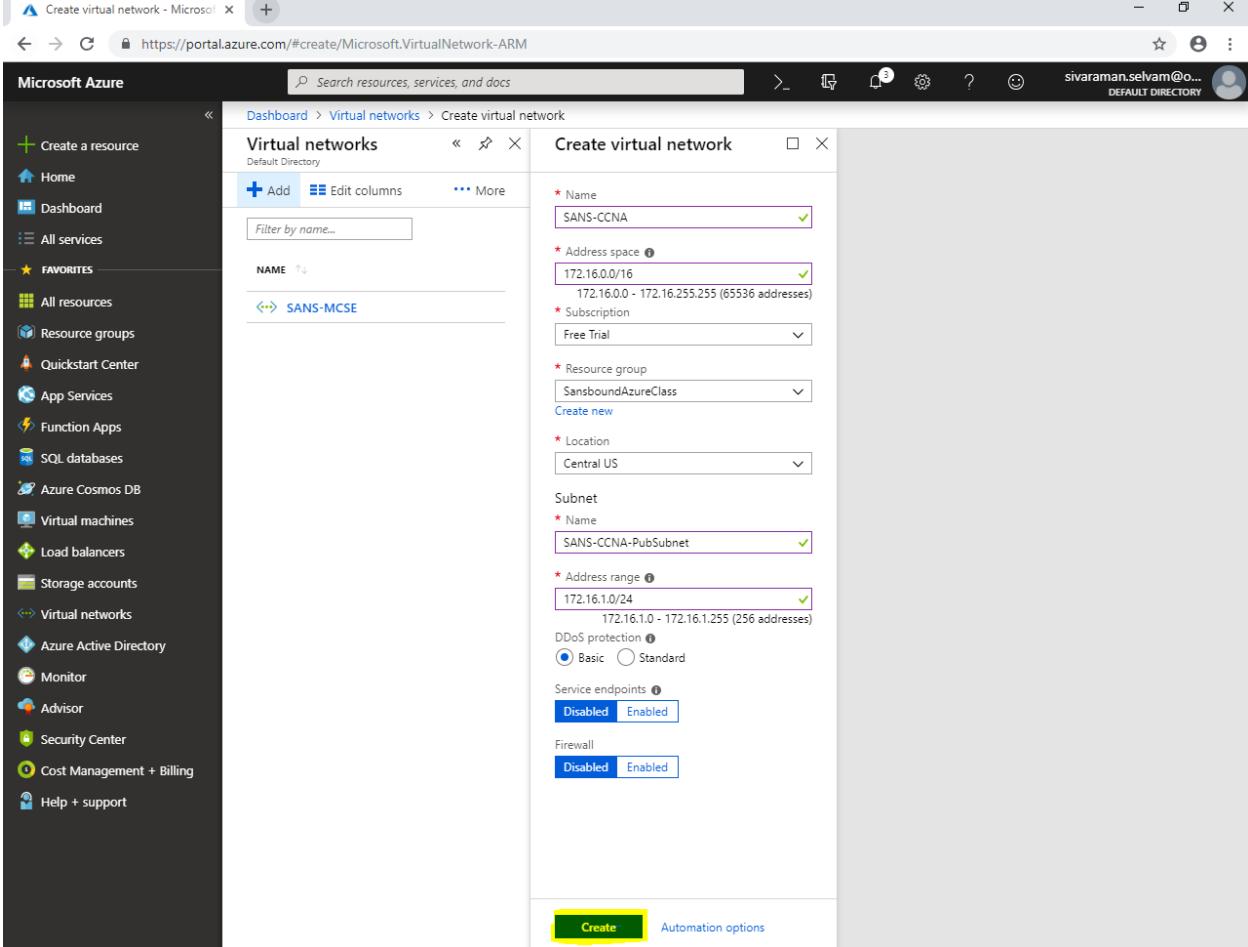


The screenshot shows the Microsoft Azure portal interface for creating a new virtual network. The left sidebar contains navigation links for creating resources, home, dashboard, and various services like app services, function apps, and storage accounts. The main area shows the 'Virtual networks' blade with a table of existing networks and a 'Create virtual network' wizard on the right. In the wizard, the following details are entered:

- Name:** SANS-CCNA
- Address space:** 172.16.0.0/16 (172.16.0.0 - 172.16.255.255, 65536 addresses)
- Subscription:** Free Trial
- Resource group:** SansboundAzureClass
- Location:** Central US
- Subnet:** SANS-CCNA-PubSubnet
- Address range:** 172.16.1.0/24 (172.16.1.0 - 172.16.1.255, 256 addresses)
- DDoS protection:** Basic (radio button selected)
- Service endpoints:** Disabled (radio button selected)
- Firewall:** Enabled

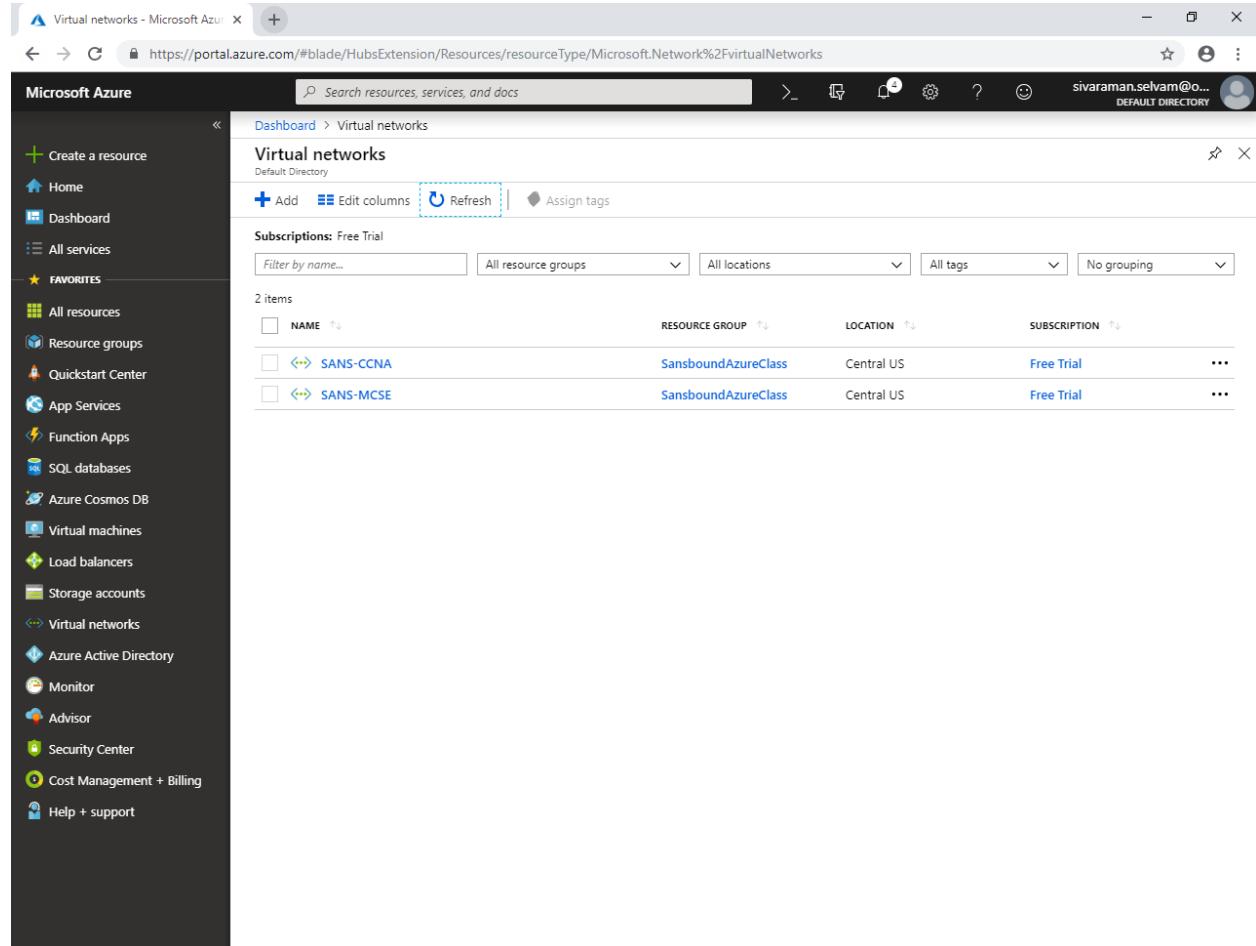
At the bottom of the wizard, there are 'Create' and 'Automation options' buttons.

Click “Create”.



The screenshot shows the Microsoft Azure portal interface for creating a virtual network. The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, Favorites, Resource groups, Quickstart Center, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Billing, and Help + support. The main content area is titled "Create virtual network" under "Virtual networks". It includes fields for Name (SANS-CCNA), Address space (172.16.0.0/16), Subscription (Free Trial), Resource group (SansboundAzureClass), Location (Central US), Subnet (Name: SANS-CCNA-PubSubnet, Address range: 172.16.1.0/24), DDoS protection (Basic selected), Service endpoints (Disabled selected), and Firewall (Enabled selected). At the bottom, there are "Create" and "Automation options" buttons, with the "Create" button highlighted in yellow.

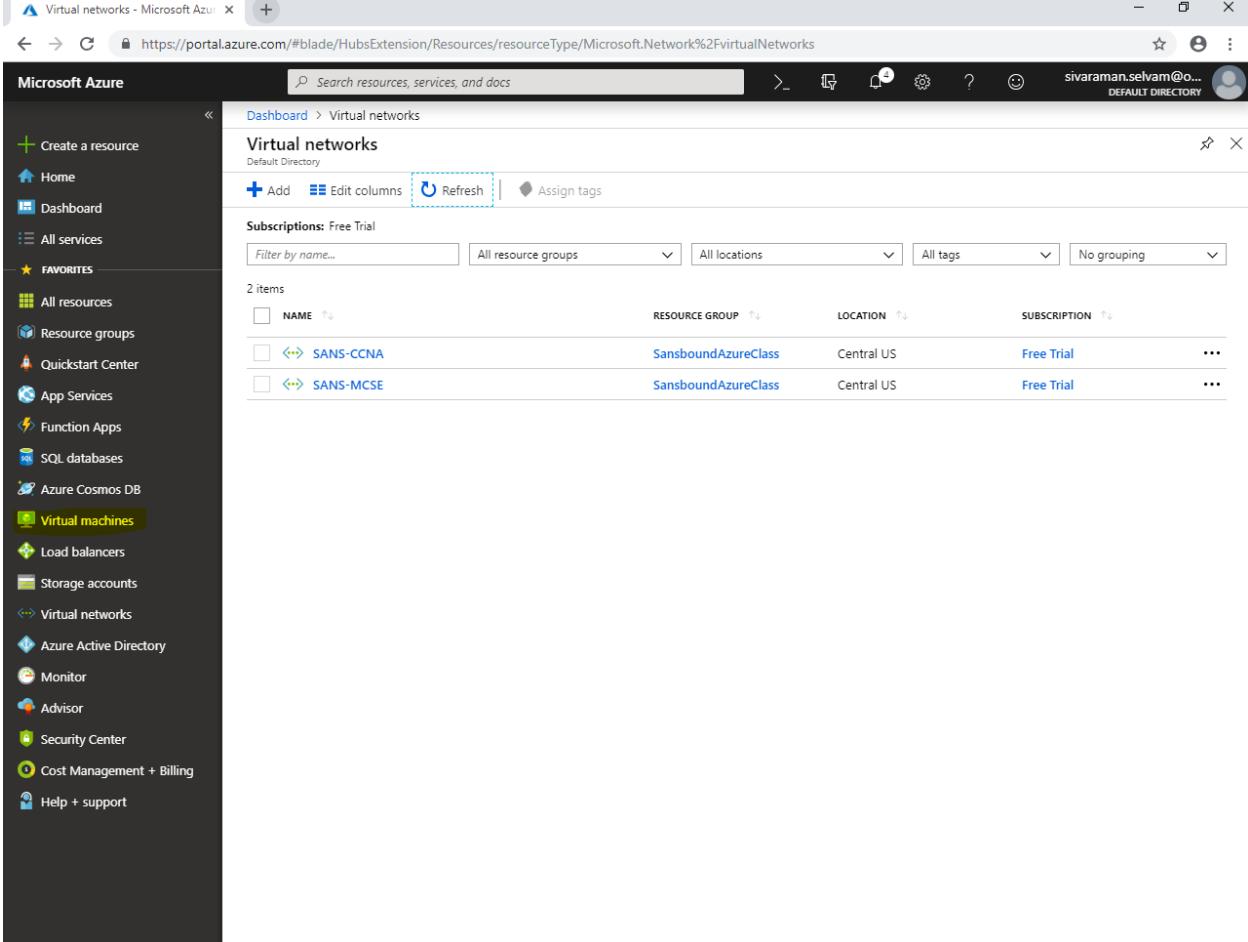
Click “Refresh” to view the newly created Virtual network.



The screenshot shows the Microsoft Azure portal interface for managing Virtual networks. The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, and Favorites. Under Favorites, the 'Virtual networks' option is selected. The main content area is titled 'Virtual networks' and shows a list of resources. At the top of the list, there are buttons for '+ Add', 'Edit columns', 'Refresh' (which is highlighted with a dashed blue border), and 'Assign tags'. Below this, a search bar says 'Filter by name...' and dropdown menus for 'All resource groups', 'All locations', 'All tags', and 'No grouping'. The table lists two items:

NAME	RESOURCE GROUP	LOCATION	SUBSCRIPTION	...
SANS-CCNA	SansboundAzureClass	Central US	Free Trial	...
SANS-MCSE	SansboundAzureClass	Central US	Free Trial	...

Click “Virtual machines”.

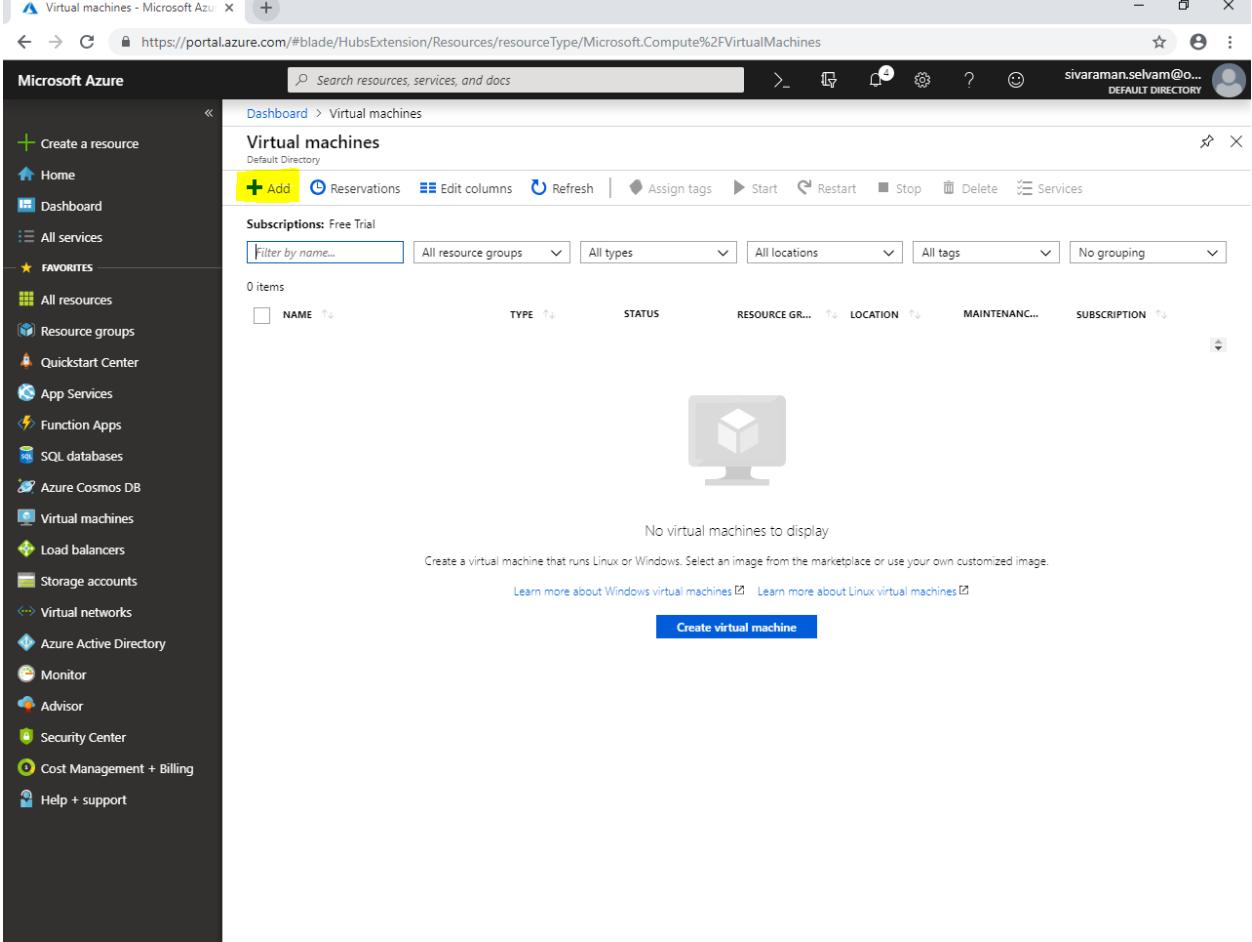


The screenshot shows the Microsoft Azure portal interface. The left sidebar is open, displaying various service categories. The 'Virtual machines' option is highlighted with a yellow background, indicating it is the active section. The main content area shows the 'Virtual networks' blade, which lists two resources: 'SANS-CCNA' and 'SANS-MCSE'. Both resources belong to the 'SansboundAzureClass' resource group, are located in 'Central US', and are associated with the 'Free Trial' subscription. The 'NAME' column is sorted in ascending order, and the 'SUBSCRIPTION' column is also visible.

NAME	RESOURCE GROUP	LOCATION	SUBSCRIPTION
SANS-CCNA	SansboundAzureClass	Central US	Free Trial
SANS-MCSE	SansboundAzureClass	Central US	Free Trial

In “Virtual machines”,

Click “Add”.



The screenshot shows the Microsoft Azure portal interface. The left sidebar is visible with various service icons. The main content area is titled "Virtual machines". At the top of the list, there is a yellow-highlighted "Add" button. Below the header, there are several filter and search options. A message states "No virtual machines to display" and provides links to learn more about Windows and Linux virtual machines. A prominent blue "Create virtual machine" button is located at the bottom of the list.

While create virtual machine,

Select “Subscription” as “Free Trial”.

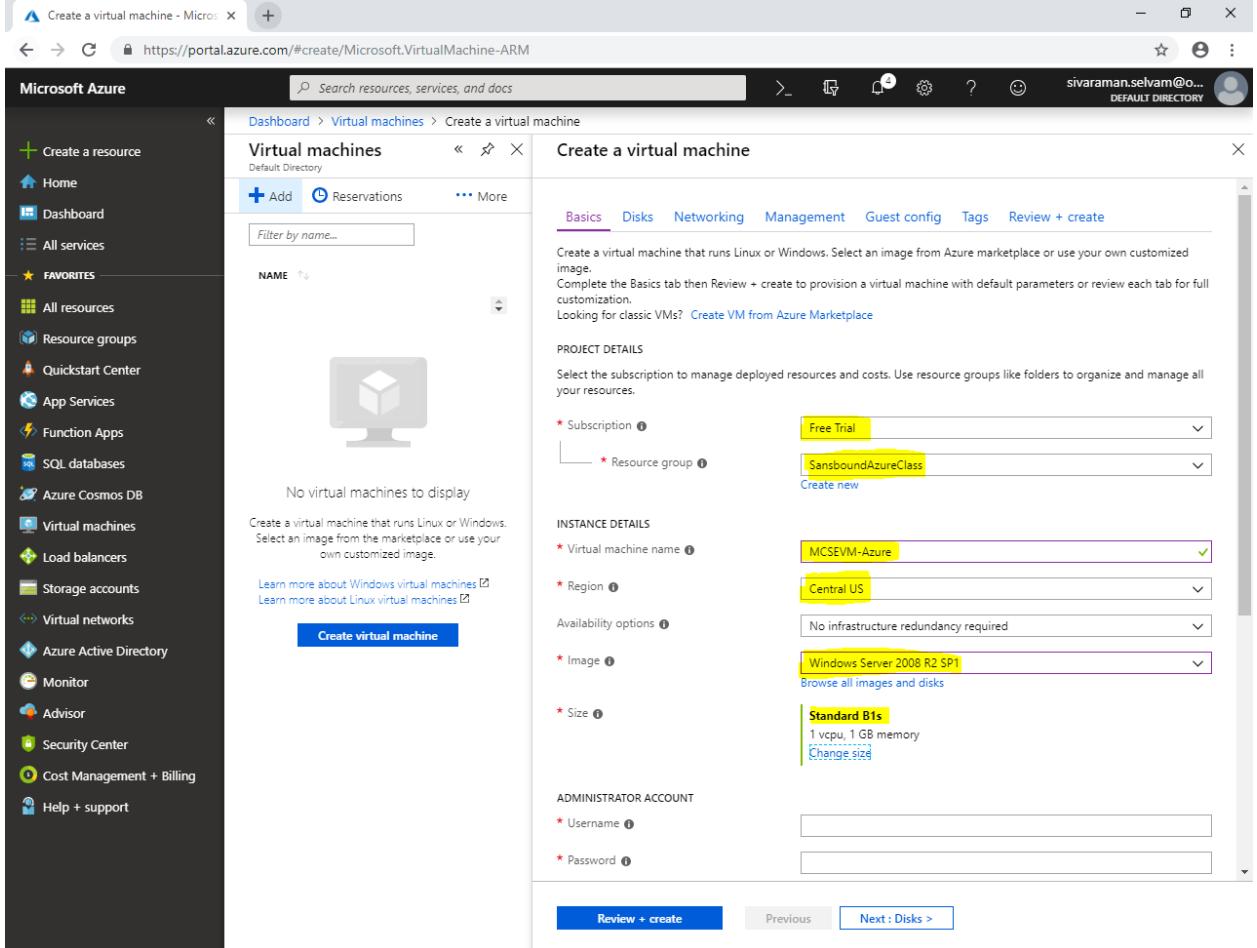
Select “Resource group” as “SansboundAzureClass”.

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

Select “Region” as “Central US”.

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

Change “Virtual machine size” as “Standard B1s”.



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 is titled 'Create a virtual machine' under 'Virtual machines'. The 'PROJECT DETAILS' tab is active, showing the following configuration:

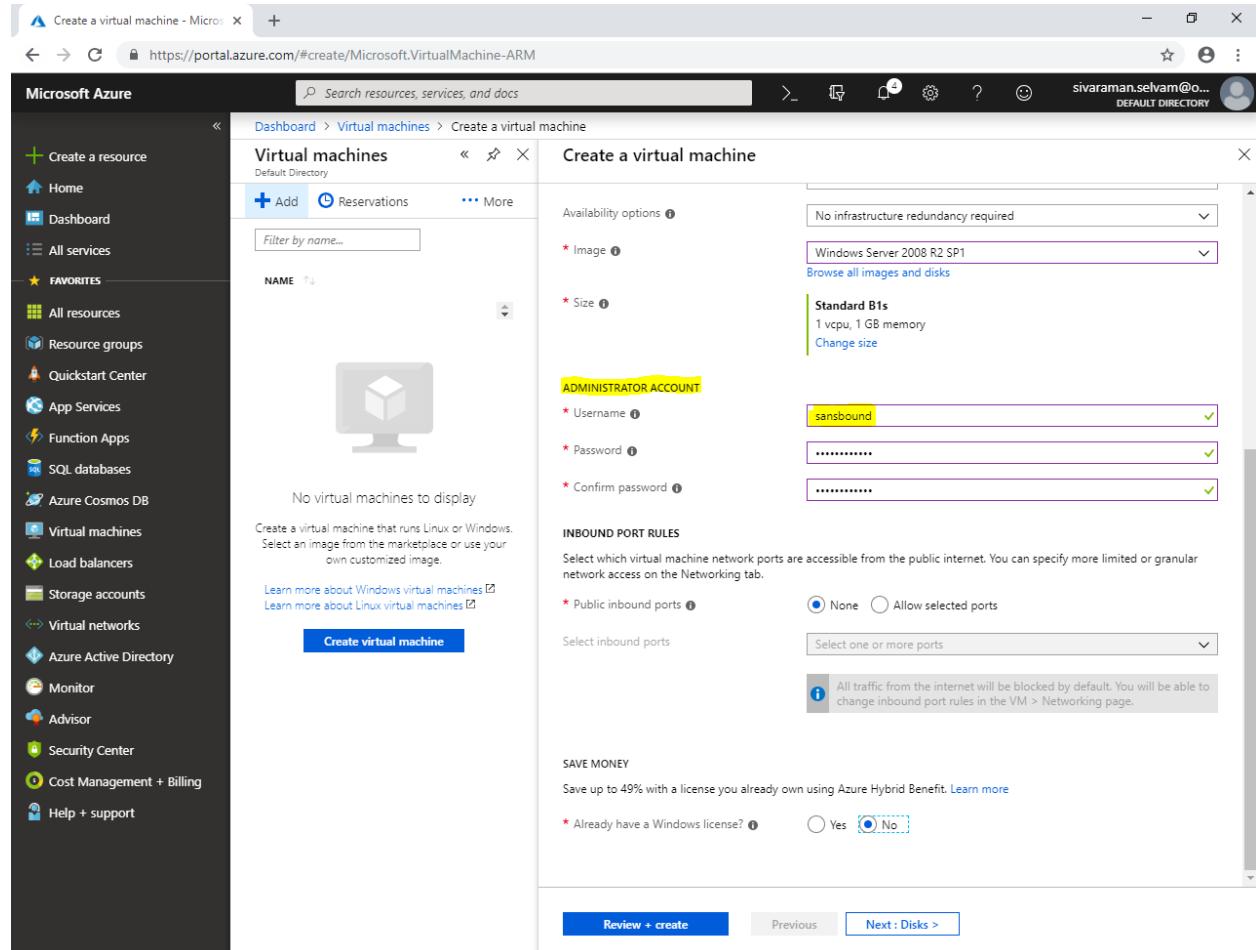
- Subscription:** Free Trial
- Resource group:** SansboundAzureClass
- Virtual machine name:** MCSEVM-Azure
- Region:** Central US
- Image:** Windows Server 2008 R2 SP1
- Size:** Standard B1s

The 'INSTANCE DETAILS' tab shows 'Availability options' set to 'No infrastructure redundancy required'. The 'Create virtual machine' button is visible at the bottom left of the form.

In “Administrator Account”,

In “Username” type as “sansbound”.

In “Password” of virtual machine.

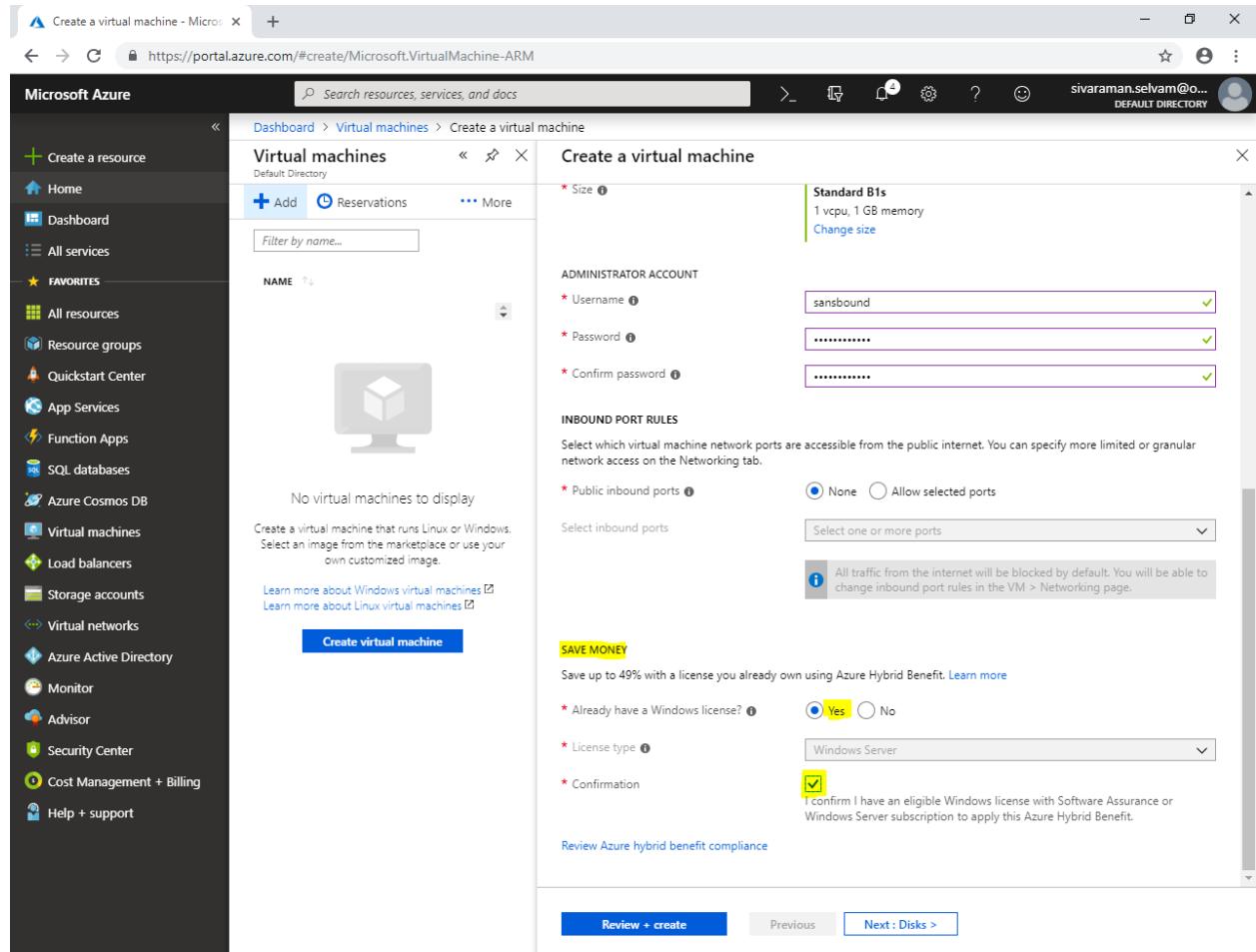


The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains various service icons such as Home, Dashboard, All services, Favorites, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Billing, and Help + support. The main panel is titled "Create a virtual machine" and shows the "Virtual machines" blade. It includes sections for "Availability options", "Image", "Size", and "ADMINISTRATOR ACCOUNT". In the "ADMINISTRATOR ACCOUNT" section, the "Username" field is highlighted with a yellow box and contains the value "sansbound". The "Password" and "Confirm password" fields are also present. Below this, there are sections for "INBOUND PORT RULES" (with "None" selected) and "SAVE MONEY" (with "No" selected for "Already have a Windows license?"). At the bottom, there are buttons for "Review + create", "Previous", and "Next : Disks >".

In “Save Money”,

Click “Yes” to “Already have a windows license”.

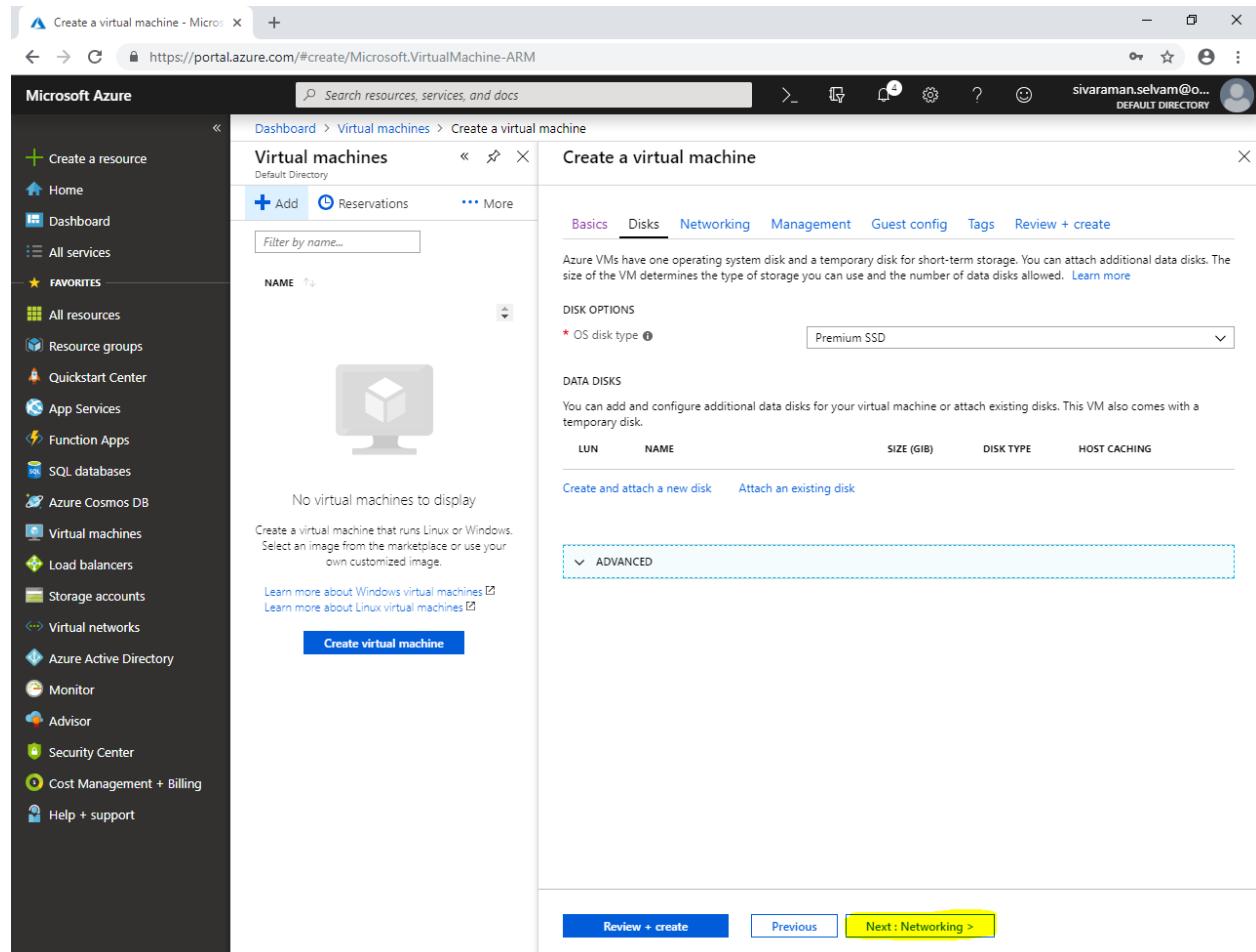
Need to check “Confirmation” box.



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. On the left, there's a sidebar with various service icons like Home, Dashboard, and Storage accounts. The main area is titled 'Create a virtual machine' and shows a step-by-step process. In the 'SAVE MONEY' section, there are two radio buttons: 'Yes' (selected) and 'No'. Below them is a checkbox labeled 'Confirmation' which is also checked. At the bottom of the screen, there are navigation buttons for 'Review + create', 'Previous', and 'Next : Disks >'. The URL in the browser bar is <https://portal.azure.com/#create/Microsoft.VirtualMachine-ARM>.

In “Disks”,

Click “Next : Networking >”.



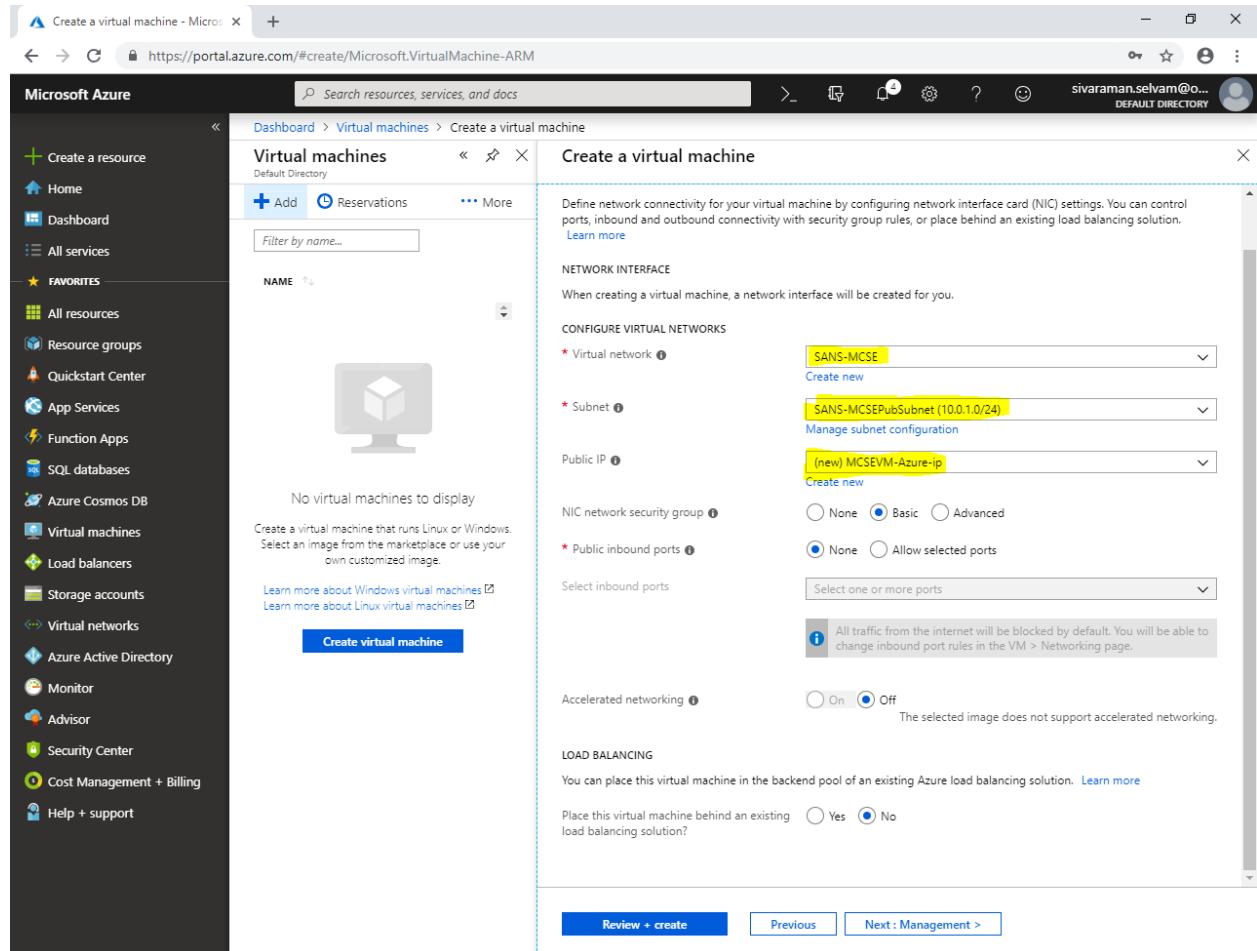
The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar lists various services like Home, Dashboard, and Storage accounts. The main area is titled 'Create a virtual machine' under 'Virtual machines'. The 'Disks' tab is currently selected. It shows disk options: 'OS disk type' is set to 'Premium SSD'. Below this, there's a section for 'DATA DISKS' with a table header: LUN, NAME, SIZE (GiB), DISK TYPE, and HOST CACHING. At the bottom, there are buttons for 'Create and attach a new disk' and 'Attach an existing disk'. A collapsed 'ADVANCED' section is also present. At the very bottom, there are navigation buttons: 'Review + create', 'Previous', and 'Next : Networking >' (which is highlighted with a yellow box).

In “Networking”,

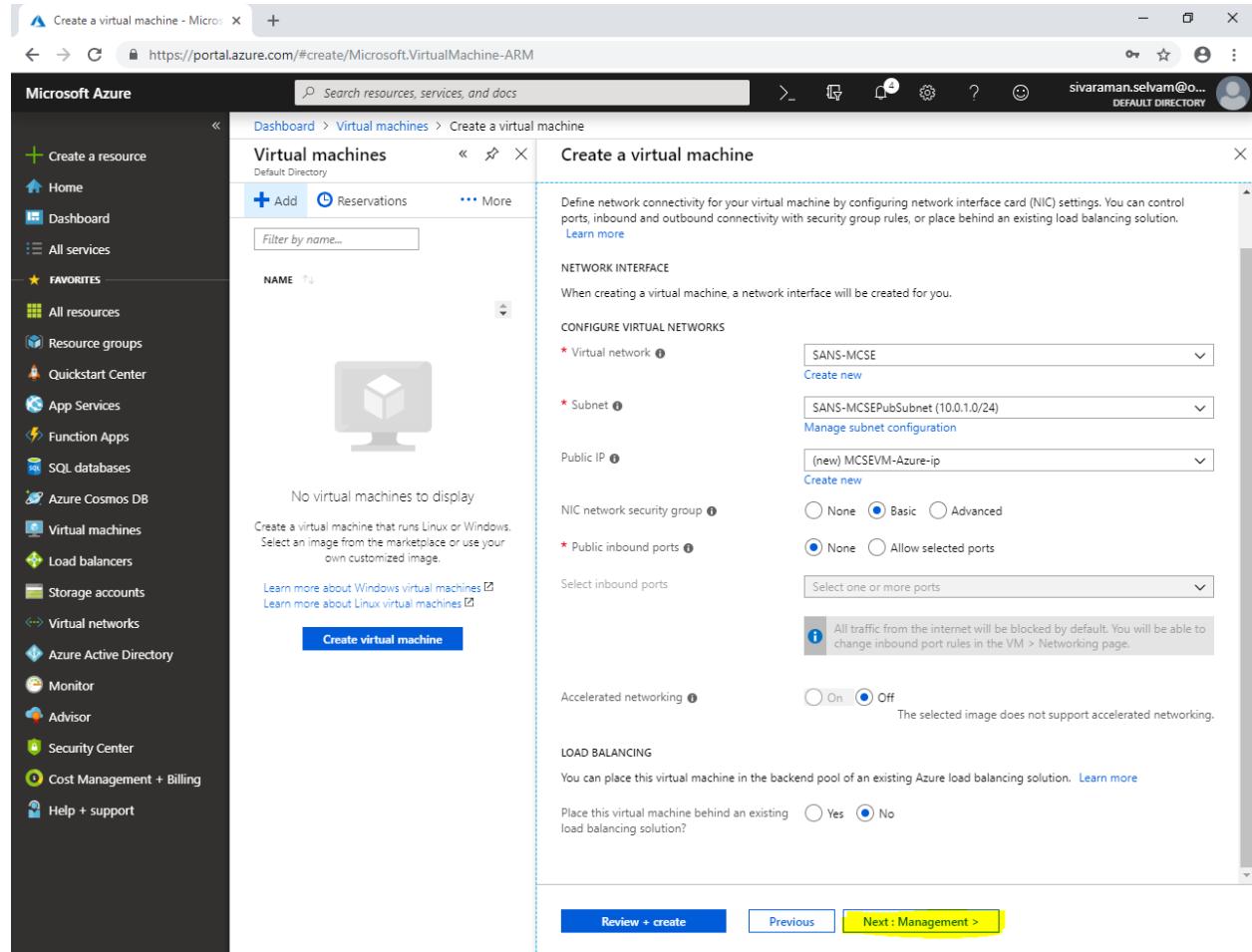
Create “Virtual machine”

Select “Virtual network” as “**SANS-MCSE**”.

Select “Subnet” as “**SANS-MCSEPubSubet**”.



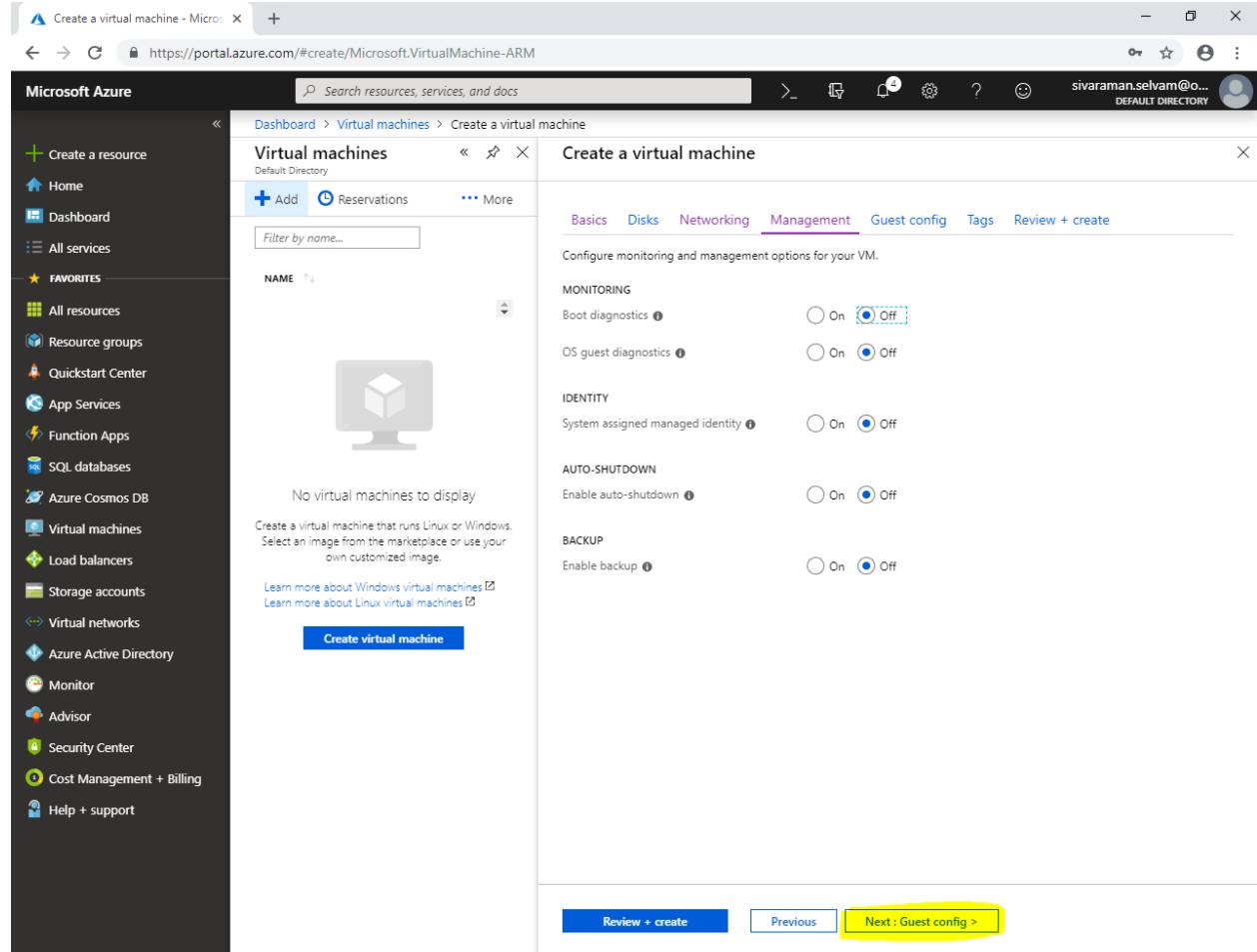
Click "Next : Management".



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, Favorites, Resource groups, Quickstart Center, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Billing, and Help + support. The main area is titled 'Virtual machines' and shows a 'Create a virtual machine' wizard. The current step is 'Configure Virtual Networks'. It asks for a 'Virtual network' (selected as 'SANS-MCSE'), a 'Subnet' ('SANS-MCSEPubSubnet (10.0.1.0/24)'), and a 'Public IP' ('(new) MCSEVM-Azure-ip'). Under 'NIC network security group', 'Basic' is selected. Under 'Public inbound ports', 'Allow selected ports' is chosen, and a dropdown menu is open. The 'Accelerated networking' section has 'Off' selected. The 'LOAD BALANCING' section has 'No' selected. At the bottom, there are buttons for 'Review + create', 'Previous', and 'Next : Management >' (which is highlighted with a yellow box).

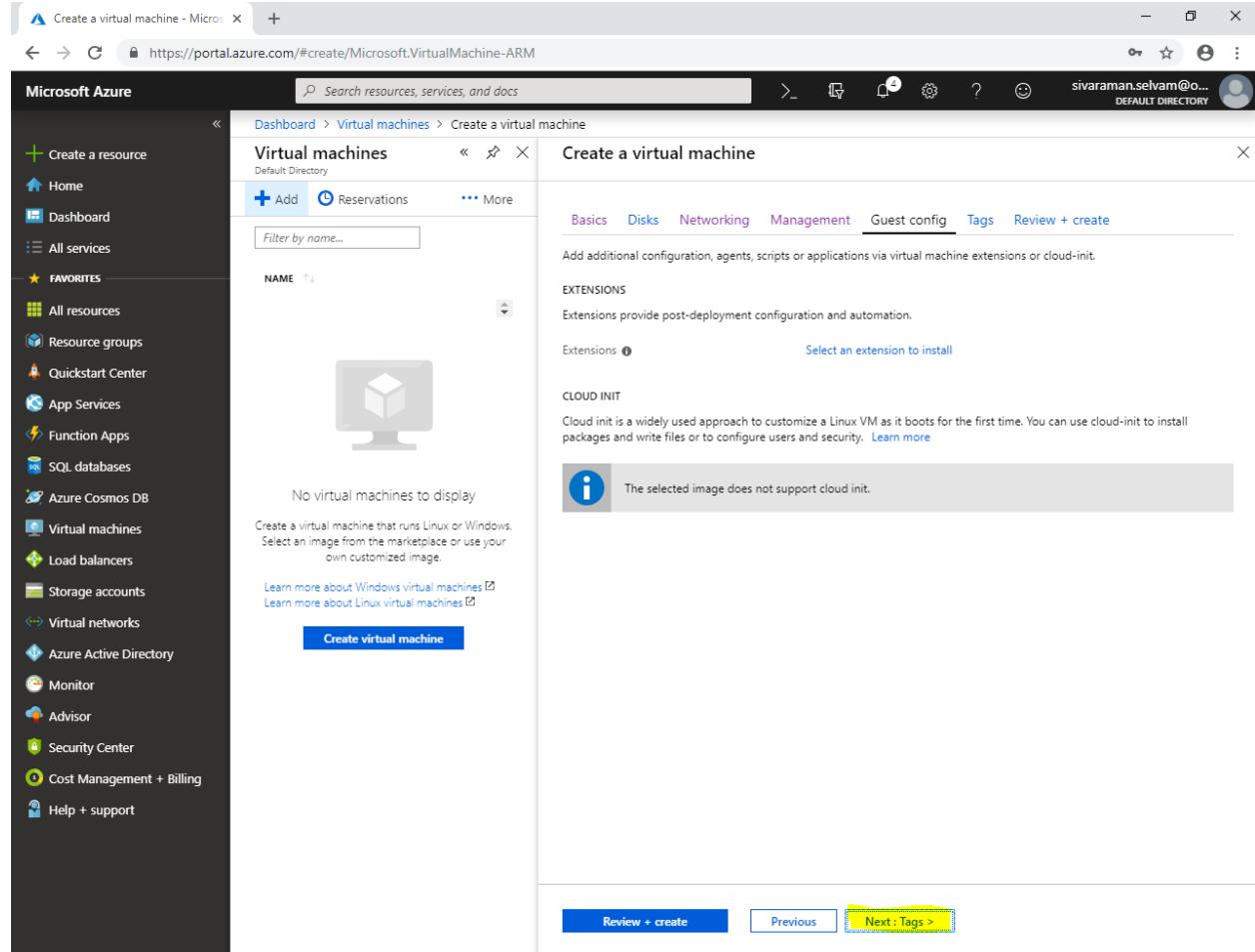
In “Management”,

Click “Next : Guest config”.



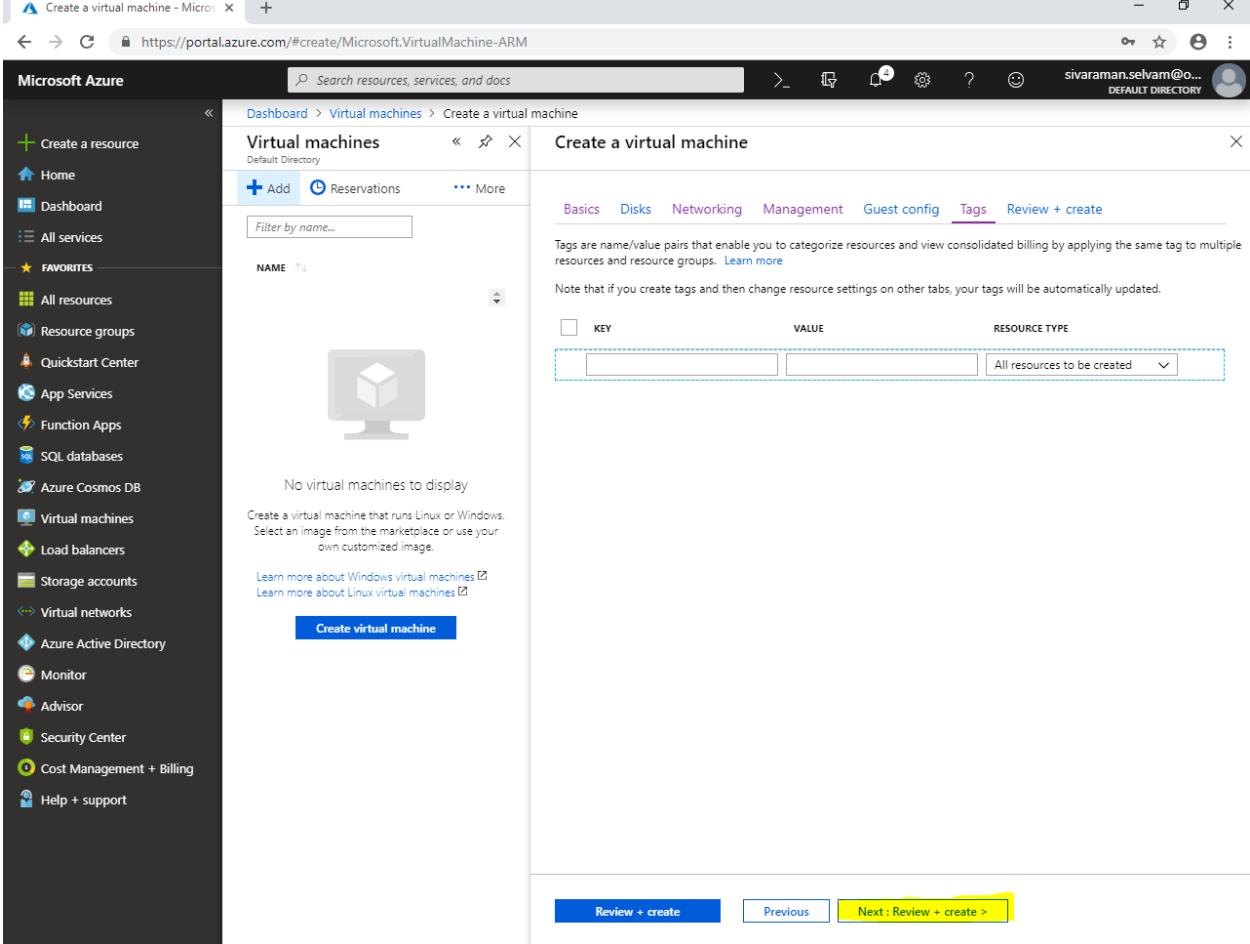
In “Guest config”,

Click “Next : Tags >”.



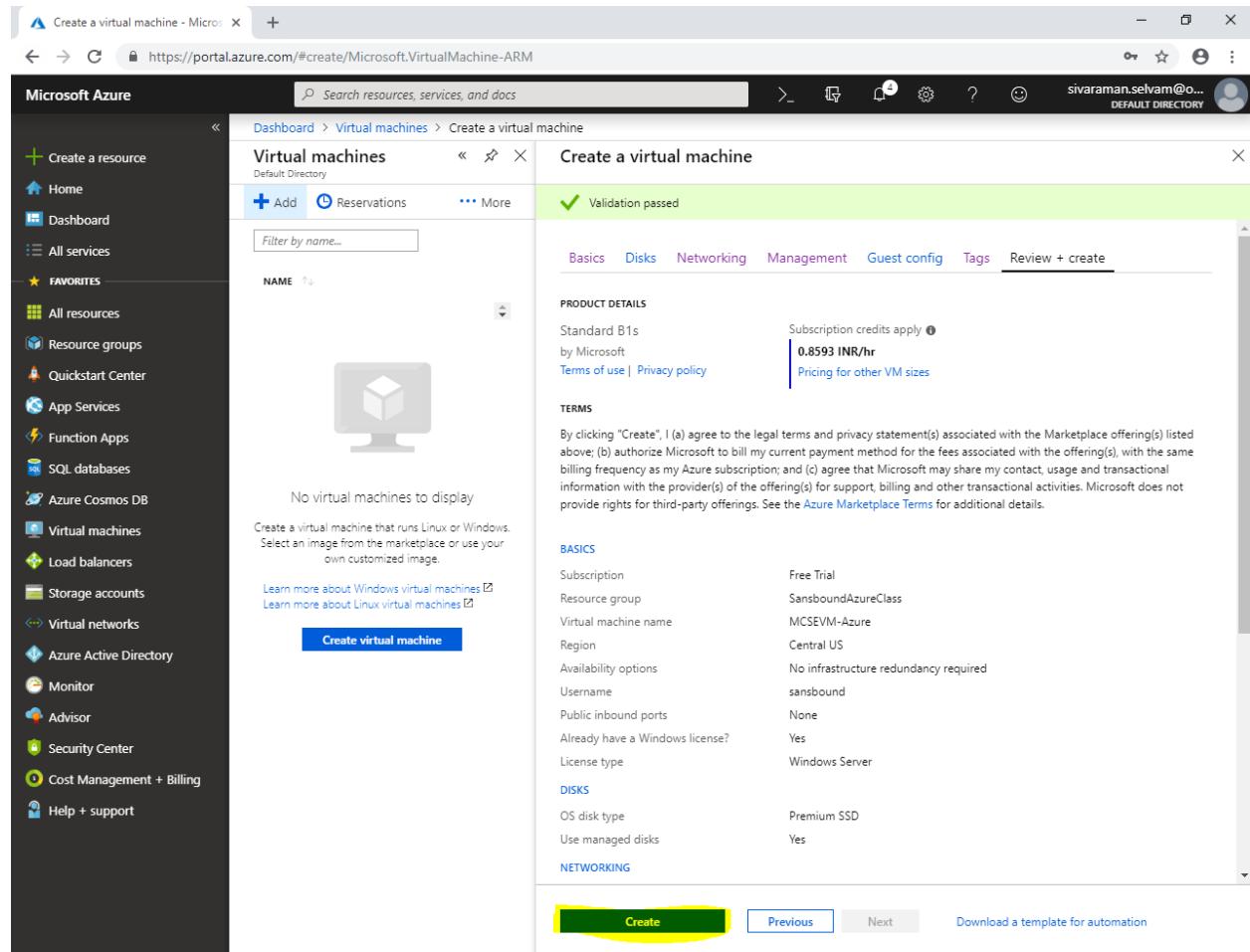
In “Tags”,

Click “Next : Review + create >”.



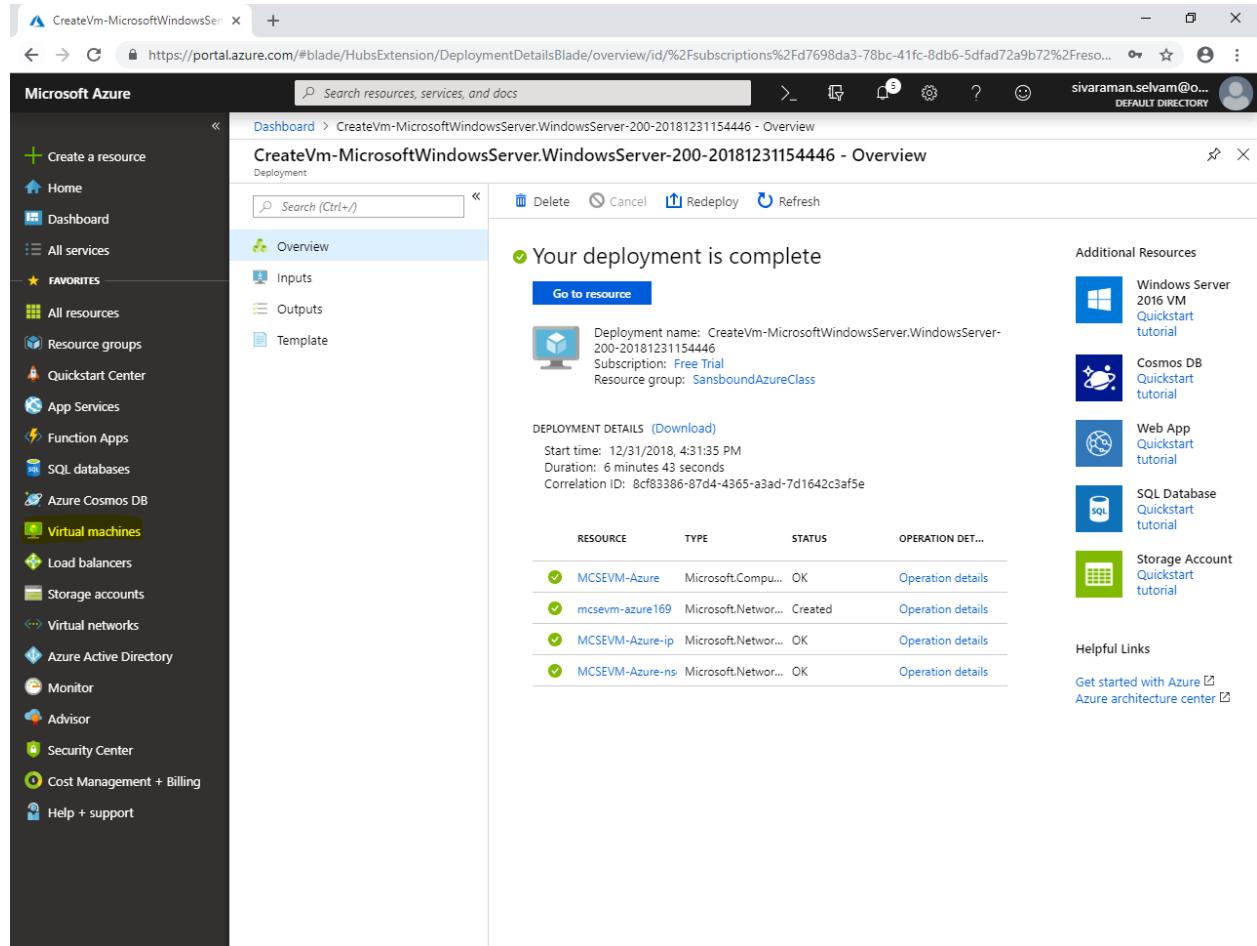
The screenshot shows the Microsoft Azure portal interface for creating a virtual machine. The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, Favorites, All resources, Resource groups, Quickstart Center, App Services, Function Apps, SQL databases, Azure 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 'Create a virtual machine' under 'Virtual machines'. It shows a summary of the configuration: 'NAME' is 'Windows VM', 'IMAGE' is 'Windows Server 2019 Datacenter', 'SIZE' is 'Standard DS1 v2', 'DISK' is 'Standard LRS', 'NETWORK' is 'VNET1', and 'LOCATION' is 'South Central US'. Below this, there's a section for 'Tags' where a single tag 'All resources to be created' is listed. At the bottom, there are three buttons: 'Review + create' (highlighted in blue), 'Previous', and 'Next : Review + create >' (highlighted in yellow).

Click “Create”.



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains navigation links for Home, Dashboard, All services, Favorites, All resources, Resource groups, Quickstart Center, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Billing, and Help + support. The main area displays the 'Virtual machines' blade, which includes a search bar, a 'Create' button, and a 'Reservations' section. Below these are tabs for 'Basics', 'Disks', 'Networking', 'Management', 'Guest config', 'Tags', and 'Review + create'. The 'Review + create' tab is selected, showing validation status ('Validation passed'), product details (Standard B1s by Microsoft), subscription credits apply (0.8593 INR/hr), terms of use, and privacy policy. The 'TERMS' section contains legal text about agreeing to terms and conditions. The 'BASICS' section lists configuration details: Subscription (Free Trial), Resource group (SansboundAzureClass), Virtual machine name (MCSEVM-Azure), Region (Central US), Availability options (No infrastructure redundancy required), Username (sansbound), Public inbound ports (None), Already have a Windows license? (Yes), License type (Windows Server). 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 with a yellow box), 'Previous', 'Next', and 'Download a template for automation' buttons.

Click “Virtual machines” in left side panel.



The screenshot shows the Microsoft Azure portal interface. The left sidebar is dark-themed and includes the following navigation items:

- 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** (highlighted)
 - Load balancers
 - Storage accounts
 - Virtual networks
 - Azure Active Directory
 - Monitor
 - Advisor
 - Security Center
 - Cost Management + Billing
 - Help + support

The main content area displays the deployment details for a VM named "CreateVm-MicrosoftWindowsServer.WindowsServer-200-20181231154446". The "Overview" tab is selected. A prominent message states "Your deployment is complete". Below it, a "Go to resource" button is available. Deployment details include:

- Deployment name: CreateVm-MicrosoftWindowsServer.WindowsServer-200-20181231154446
- Subscription: Free Trial
- Resource group: SansboundAzureClass

Deployment details also show:

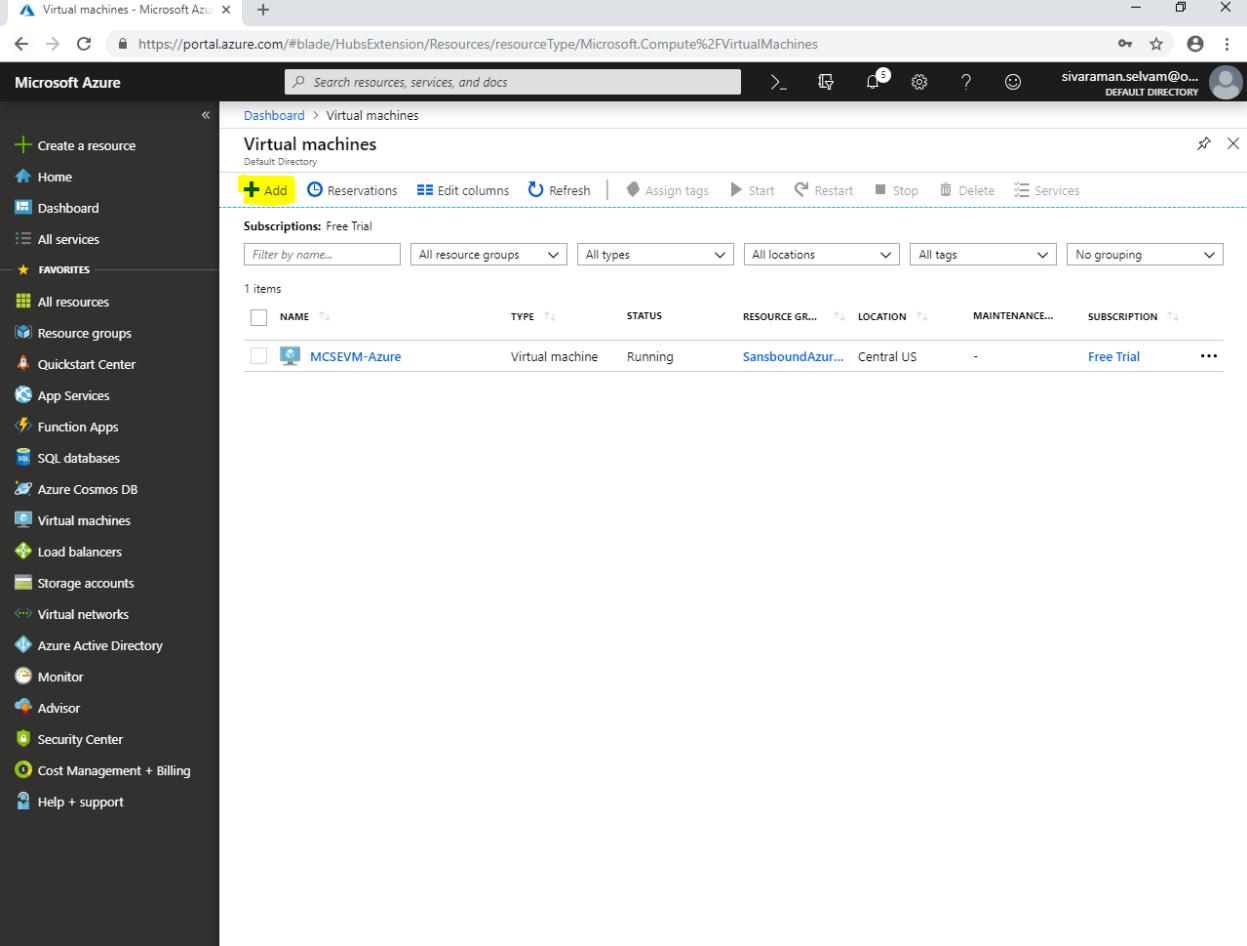
- Start time: 12/31/2018, 4:31:35 PM
- Duration: 6 minutes 43 seconds
- Correlation ID: 8cf83386-87d4-4365-a3ad-7d1642c3af5e

A table lists the resources created during the deployment:

RESOURCE	TYPE	STATUS	OPERATION DET...
MCSEVM-Azure	Microsoft.Compu...	OK	Operation details
mcesvm-azure169	Microsoft.Networ...	Created	Operation details
MCSEVM-Azure-ip	Microsoft.Networ...	OK	Operation details
MCSEVM-Azure-ns	Microsoft.Networ...	OK	Operation details

Additional Resources and Helpful Links are also present on the right side of the page.

In “Virtual machines”, click “Add”.



The screenshot shows the Microsoft Azure portal interface. The left sidebar is visible with various service icons. The main content area is titled "Virtual machines". At the top of the list, there is a blue "Add" button with a plus sign, which is highlighted with a yellow box. Below the button, there are several filter options: "Filter by name...", "All resource groups", "All types", "All locations", "All tags", and "No grouping". A table lists one item: "MCSEVM-Azure" (Virtual machine, Running, SansboundAzur..., Central US, Free Trial). The "NAME" column is sorted in ascending order.

NAME	TYPE	STATUS	RESOURCE GR...	LOCATION	MAINTENANCE...	SUBSCRIPTION
MCSEVM-Azure	Virtual machine	Running	SansboundAzur...	Central US	-	Free Trial

While create virtual machine,

Select “Subscription” as “Free Trial”.

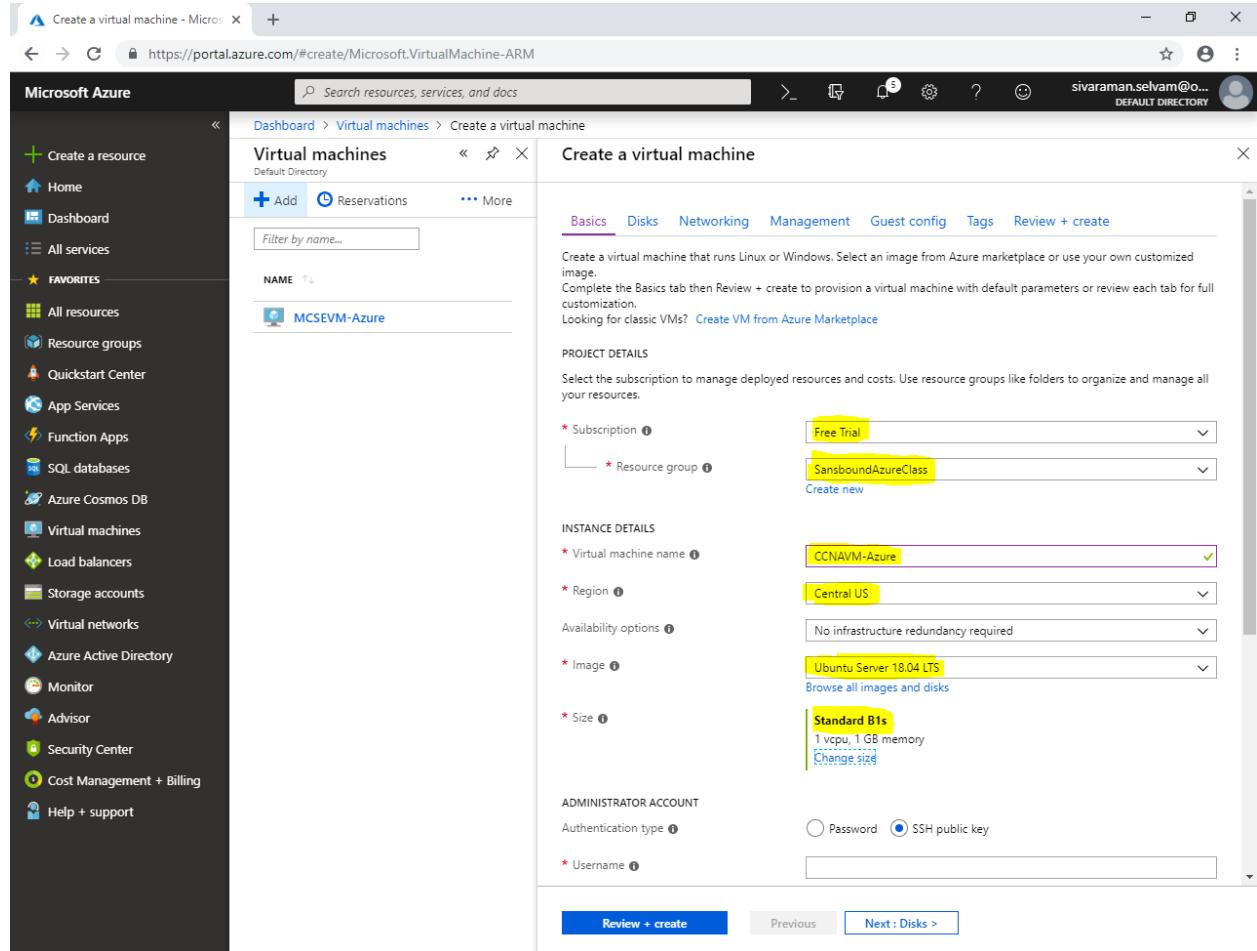
Select “Resource group” as “SansboundAzureClass”.

In “Virtual machine name” as “CCNAVM-Azure”.

Select “Region” as “Central US”.

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

Change “Virtual machine Size” as “Standard B1s”.



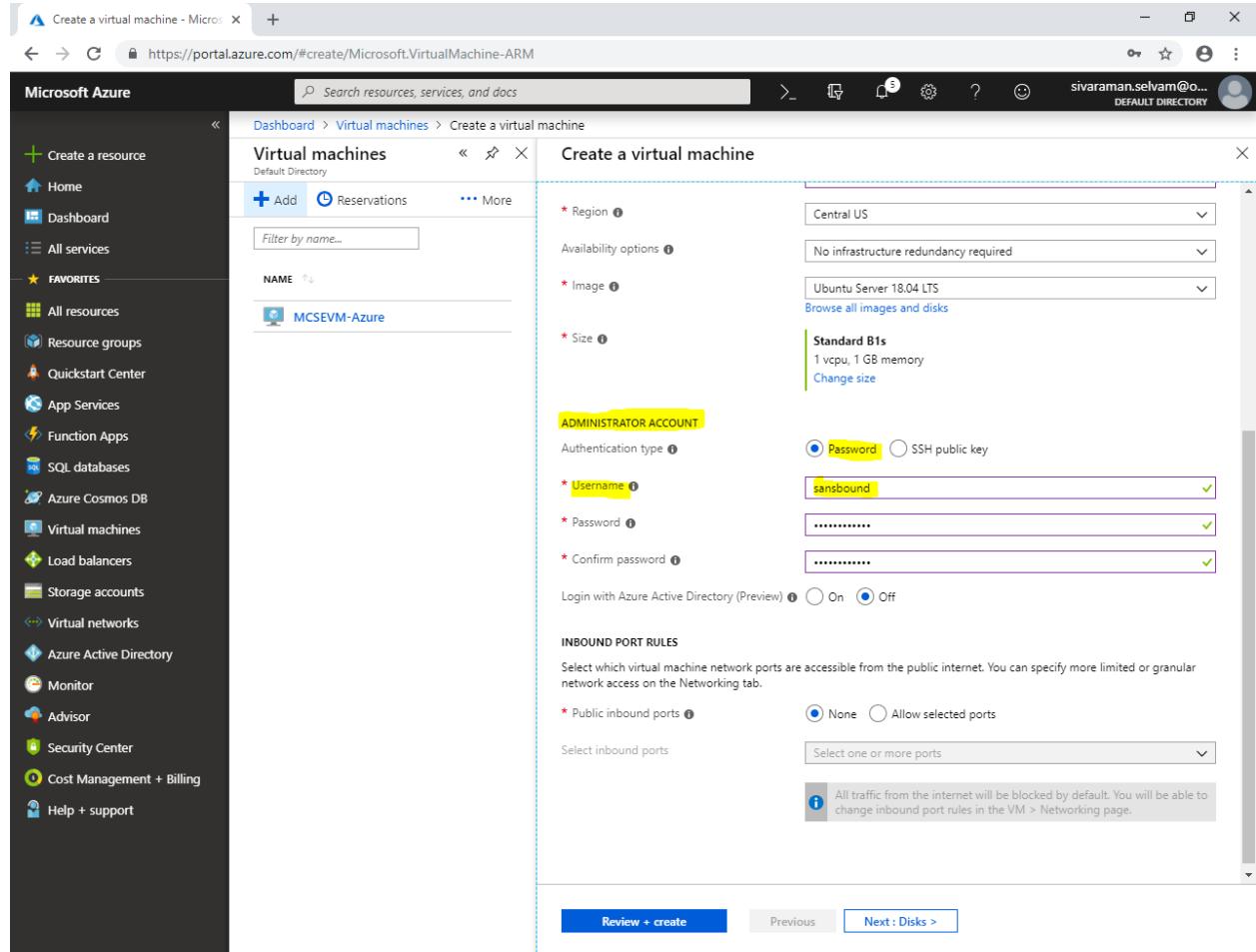
The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar lists various services like Home, Dashboard, All services, Favorites, All resources, Resource groups, Quickstart Center, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual 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'. The 'Basics' tab is active. In the 'PROJECT DETAILS' section, the 'Subscription' is set to 'Free Trial' and the 'Resource group' is set to 'SansboundAzureClass'. In the 'INSTANCE DETAILS' section, the 'Virtual machine name' is 'CCNAVM-Azure', 'Region' is 'Central US', 'Image' is 'Ubuntu Server 18.04 LTS', and 'Size' is 'Standard B1s' (1 vcpu, 1 GB memory). Under 'ADMINISTRATOR ACCOUNT', 'SSH public key' is selected. At the bottom, there are buttons for 'Review + create', 'Previous', and 'Next : Disks >'. The URL in the browser bar is https://portal.azure.com/#create/Microsoft.VirtualMachine-ARM.

In “Administrator Account”,

Click “Authentication type” as “Password”.

Type “Username” as “sansbound”.

Type “Password” for virtual machine.

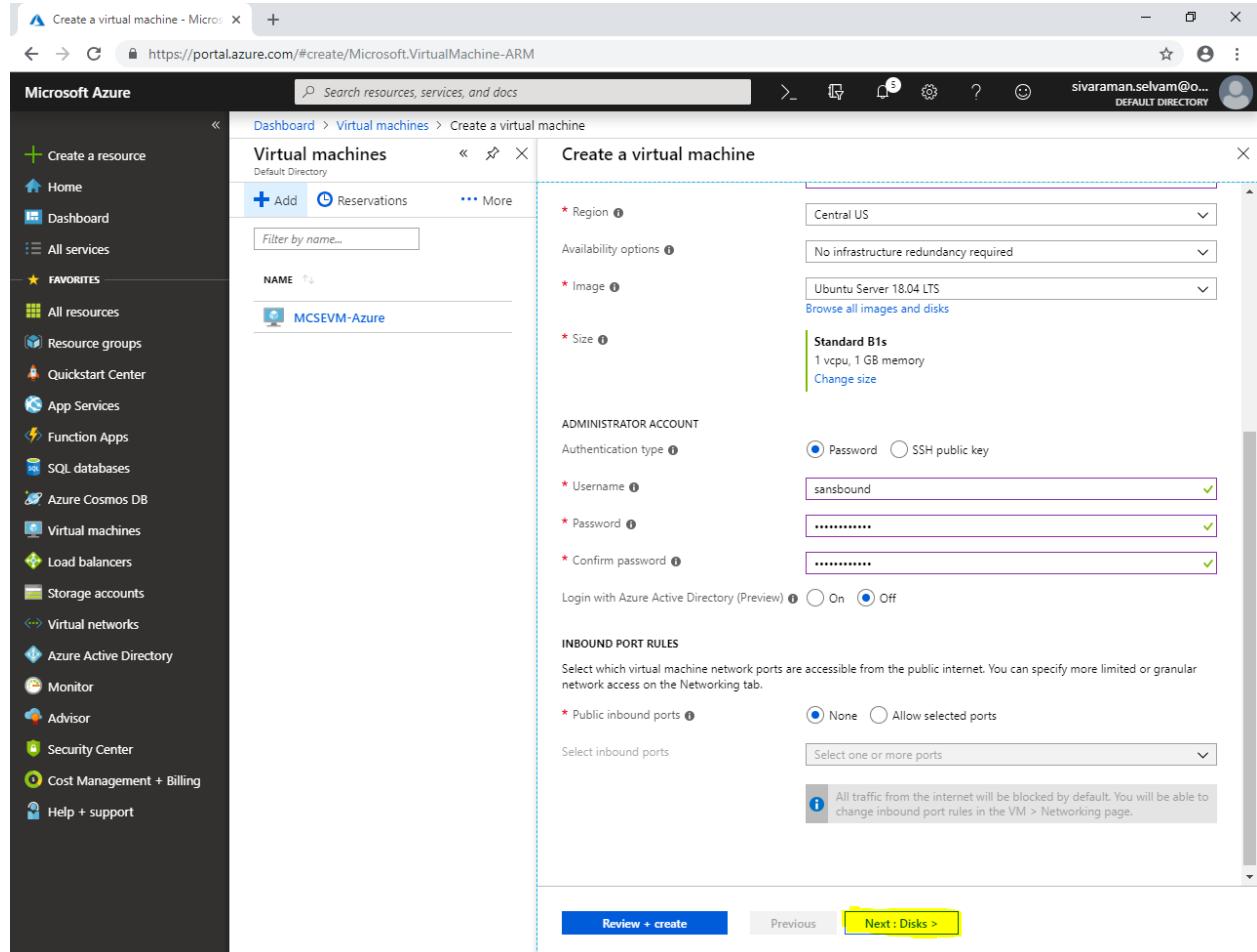


The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains various service icons and navigation links. The main area is titled "Create a virtual machine" and includes sections for "Virtual machines" and "Create a virtual machine". The "Create a virtual machine" section is active, showing the following configuration:

- Region:** Central US
- Availability options:** No infrastructure redundancy required
- Image:** Ubuntu Server 18.04 LTS
- Size:** Standard B1s (1 vcpu, 1 GB memory)
- ADMINISTRATOR ACCOUNT:**
 - Authentication type: Password (selected)
 - Username: sansbound
 - Password: (redacted)
 - Confirm password: (redacted)
- INBOUND PORT RULES:**
 - Public inbound ports: None (selected)
 - Select inbound ports: Select one or more ports
 - 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, there are "Review + create", "Previous", and "Next : Disks >" buttons.

Click “Next : Disks >”.



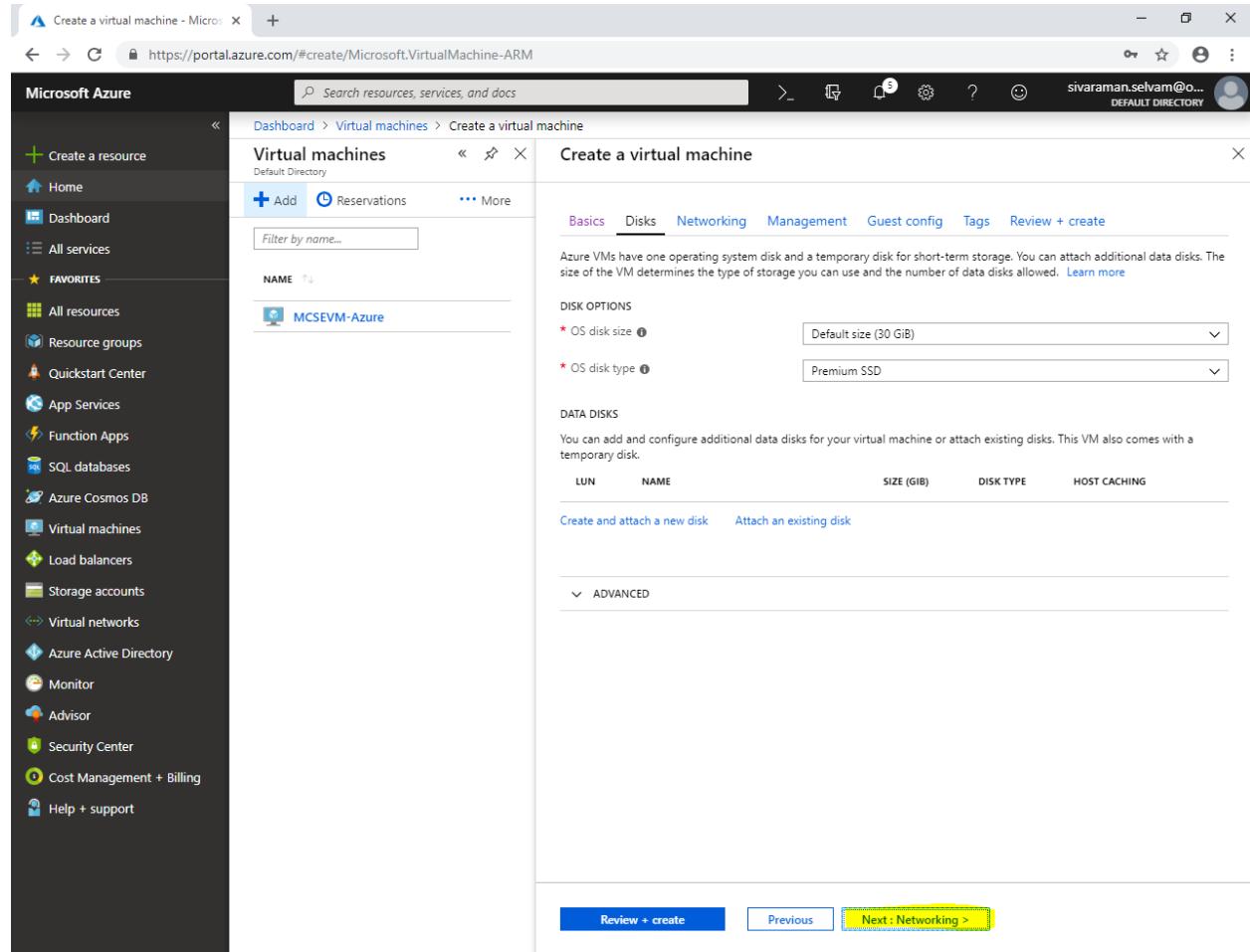
The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains various service icons under 'FAVORITES'. The main area shows a list of existing virtual machines, with one named 'MCSEVM-Azure' selected. The right panel is titled 'Create a virtual machine' and is currently on the second step, 'Configure VM settings'. The configuration fields include:

- Region:** Central US
- Availability options:** No infrastructure redundancy required
- Image:** Ubuntu Server 18.04 LTS (Browse all images and disks)
- Size:** Standard B1s (1 vcpu, 1 GB memory) - Change size
- Administrator Account:**
 - Authentication type: 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
 - A 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 wizard, the 'Review + create' and 'Previous' buttons are on the left, and the 'Next : Disks >' button is highlighted with a yellow box on the right.

In “Disks”

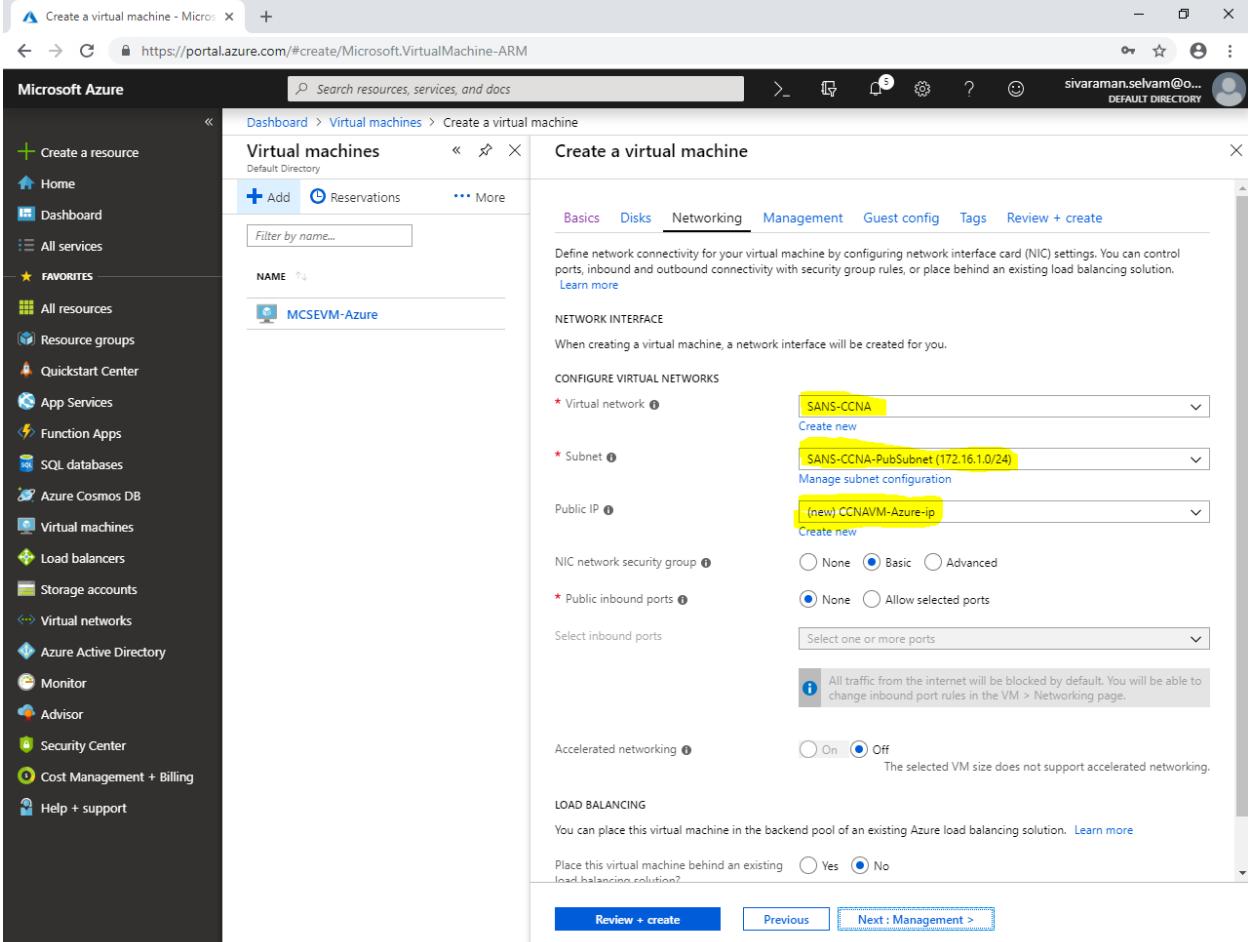
Click “Next : Networking >”.



In “Networking”,

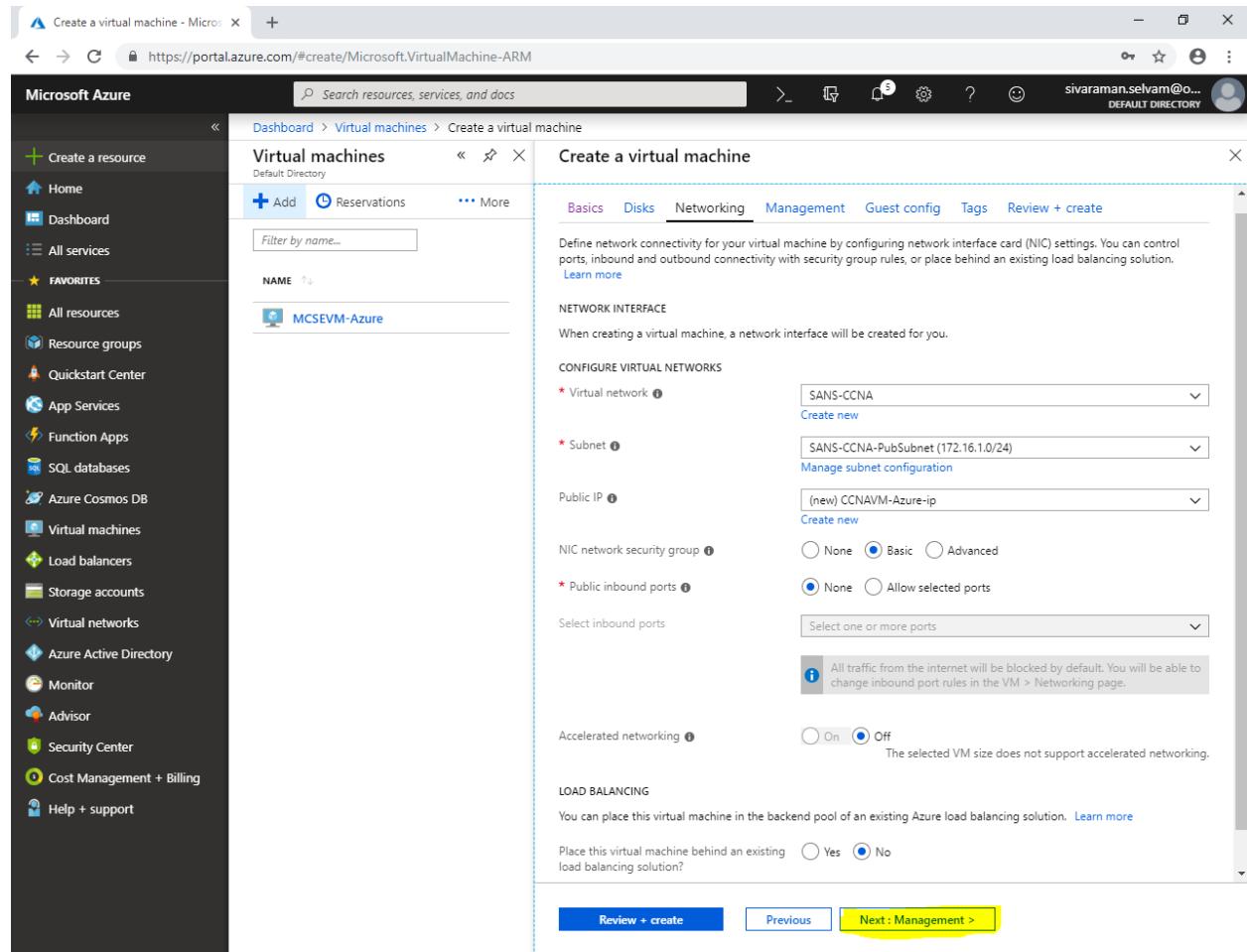
Select “Virtual network” as “**SANS-CCNA**”.

Click “Subnet” as “**SANS-CCNA-PubSubnet**”.



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 'Networking' tab is selected. In the 'CONFIGURE VIRTUAL NETWORKS' section, the 'Virtual network' dropdown is set to 'SANS-CCNA' (highlighted in yellow). The 'Subnet' dropdown is set to 'SANS-CCNA-PubSubnet (172.16.1.0/24)' (also highlighted in yellow). The 'Public IP' dropdown shows '(new) CCNAVVM-Azure-ip' (highlighted in yellow). Other networking options like 'NIC network security group', 'Public inbound ports', and 'Accelerated networking' are also visible. At the bottom, there are buttons for 'Review + create', 'Previous', and 'Next : Management >'.

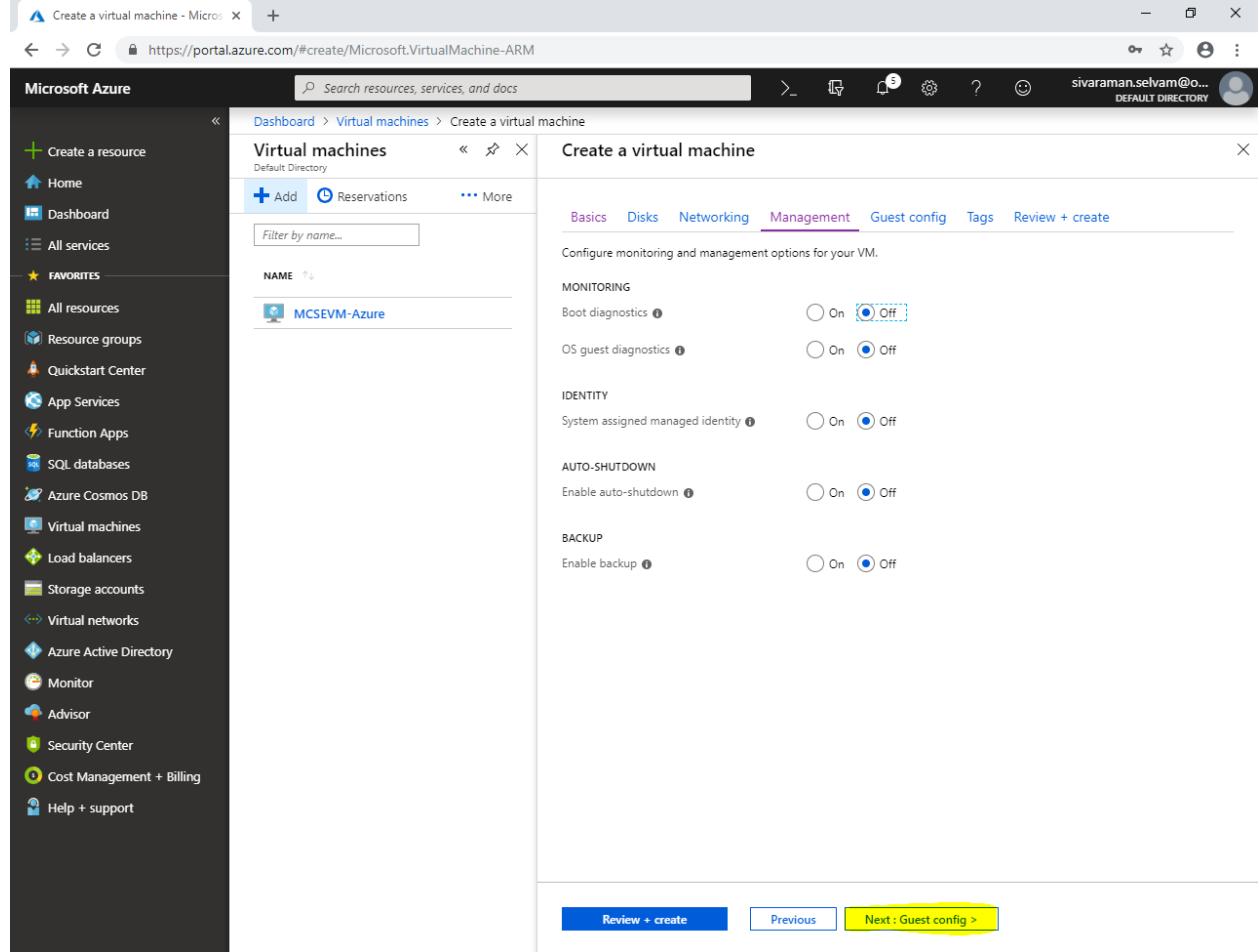
Click “Next : Management”.



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains various service links like Home, Dashboard, All services, Favorites, and Virtual machines. The main area shows the 'Virtual machines' blade with a list of existing VMs and a 'Create a virtual machine' button. The 'Create a virtual machine' wizard is open, showing the 'Management' tab. This tab allows configuring network connectivity, including selecting a virtual network (SANS-CCNA), subnet (SANS-CCNA-PubSubnet), and public IP (new CCNAVVM-Azure-ip). It also includes options for network security groups (Basic selected) and public inbound ports (None selected). Accelerated networking is turned off. In the 'LOAD BALANCING' section, it asks if the VM should be placed behind an existing 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”,

Click “Next : Guest config”.



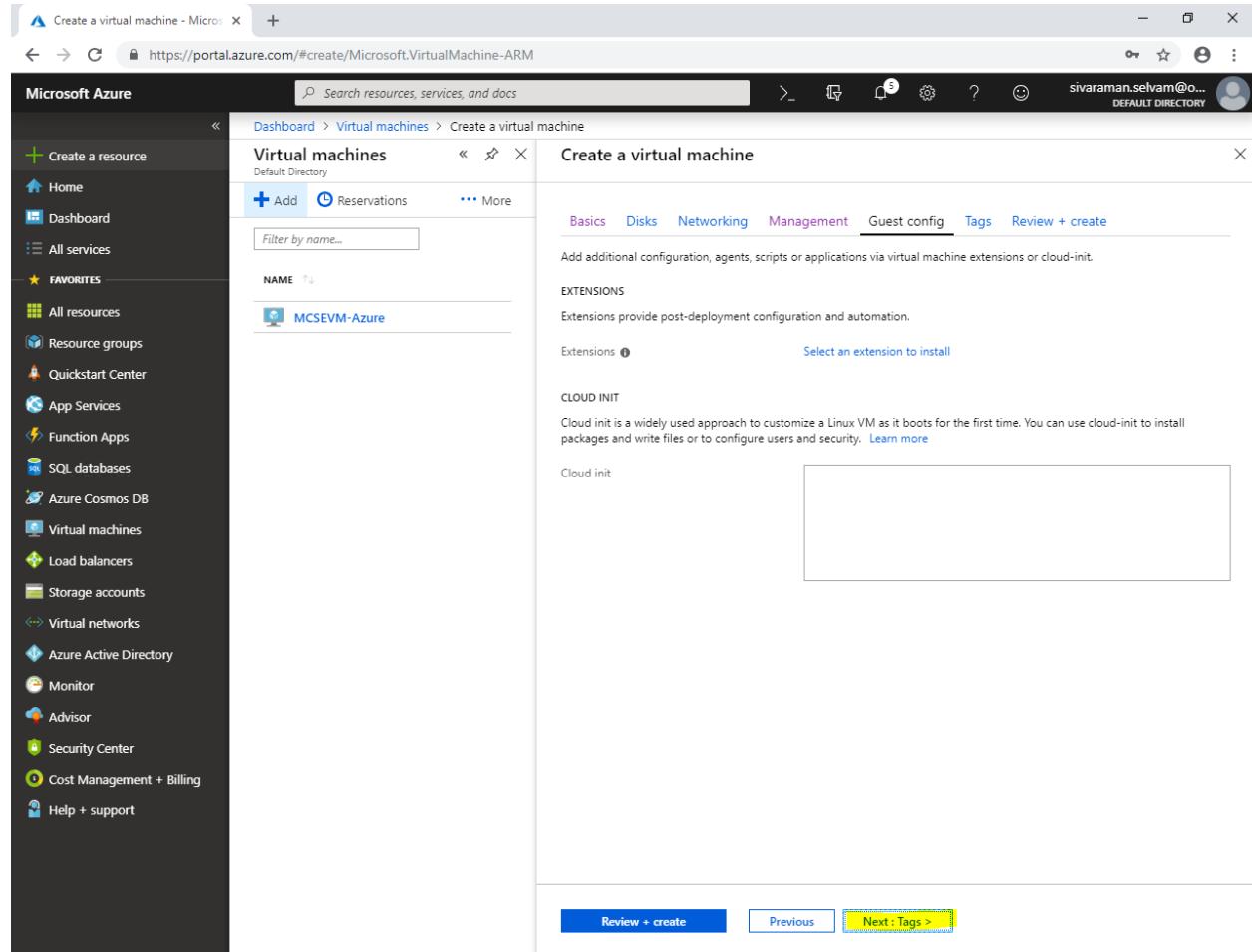
The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, Favorites, and Virtual machines. The main area is titled 'Create a virtual machine' under 'Virtual machines'. On the right, the 'Guest config' tab is selected from a series of tabs: Basics, Disks, Networking, Management, Guest config, Tags, and Review + create. Under the 'Management' section, there are several configuration options with radio buttons:

- 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 page, 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/#create/Microsoft.VirtualMachine-ARM>.

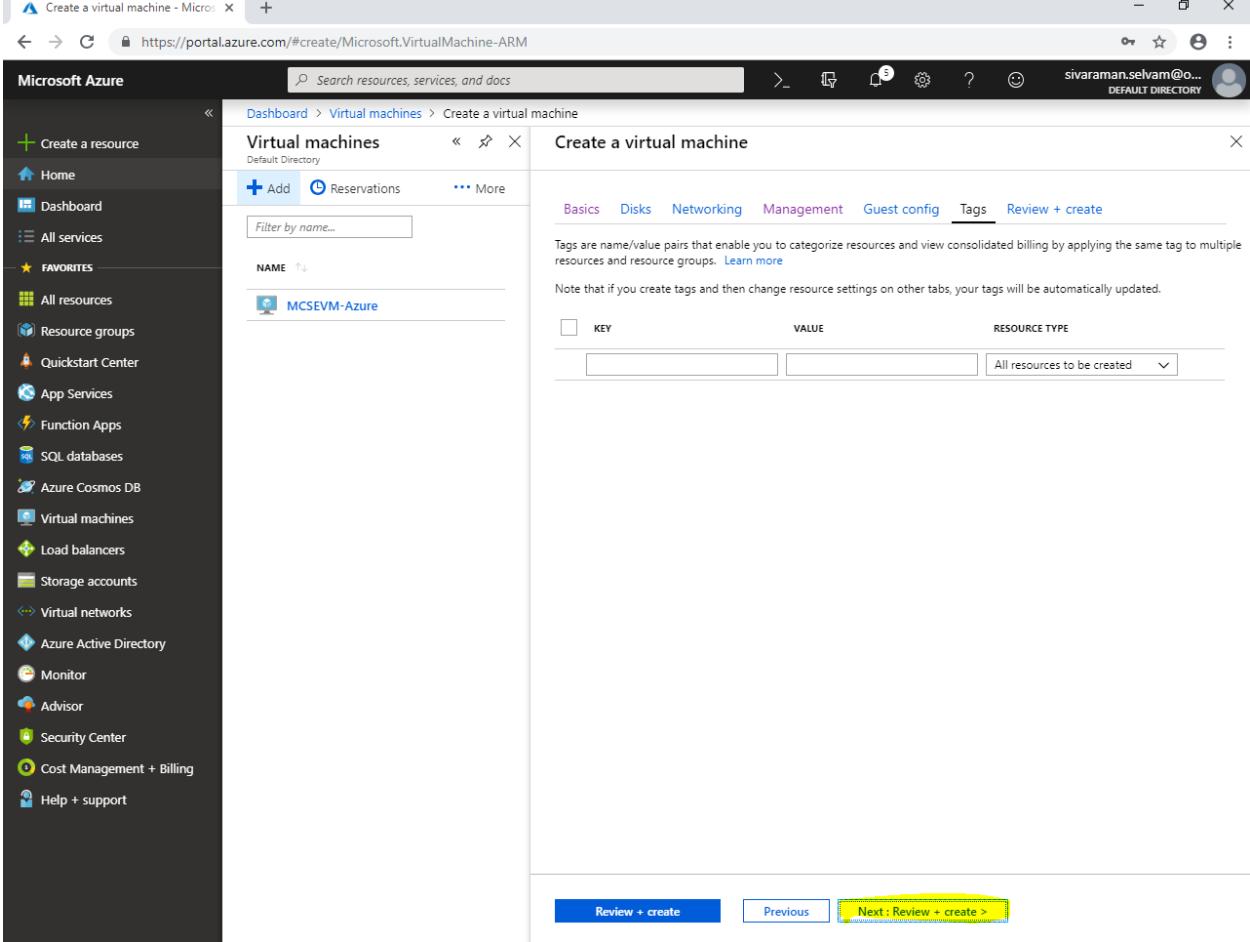
In “Guest config”,

Click “Next : Tags >”.



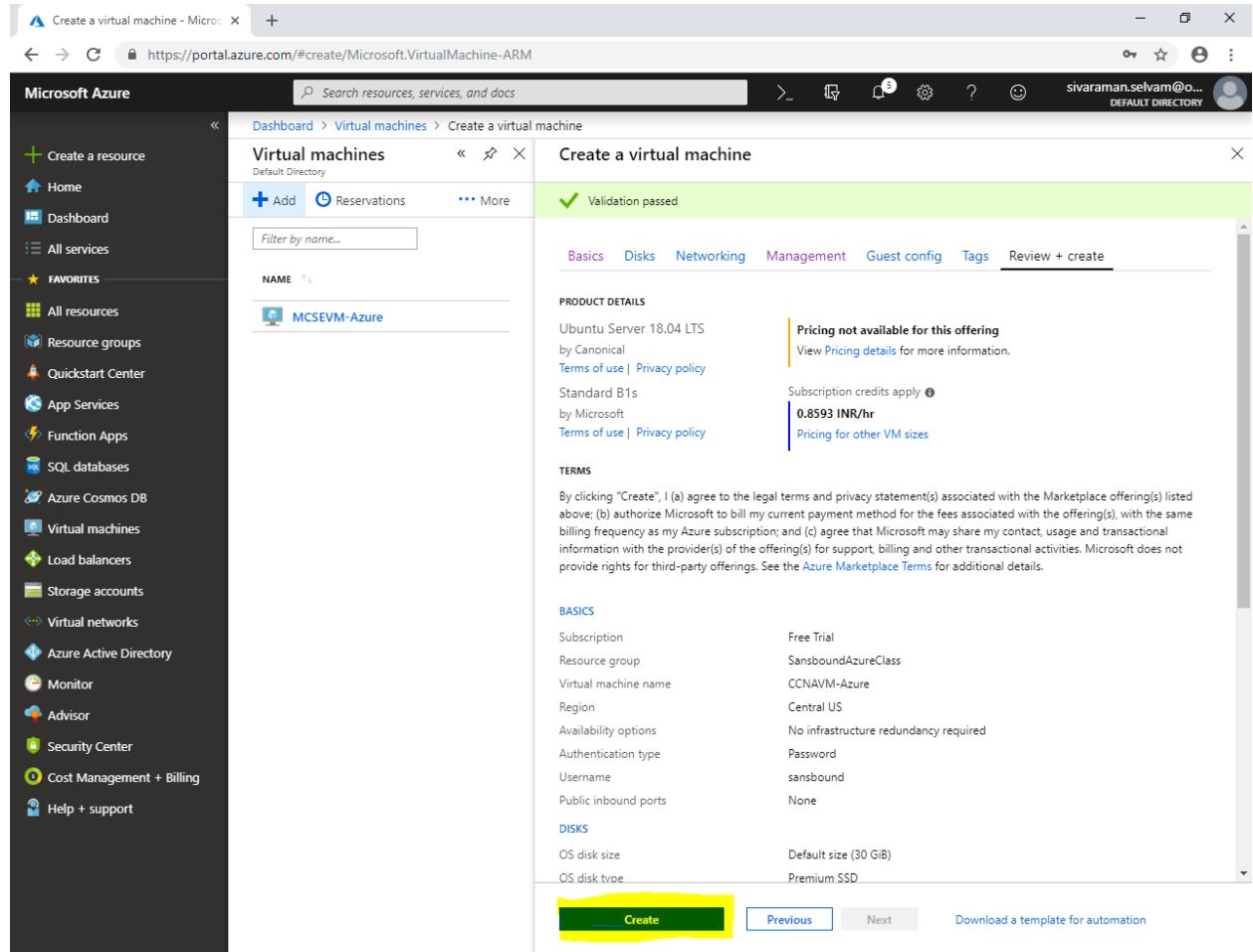
In “Tags”,

Click “Next : Review + create”.



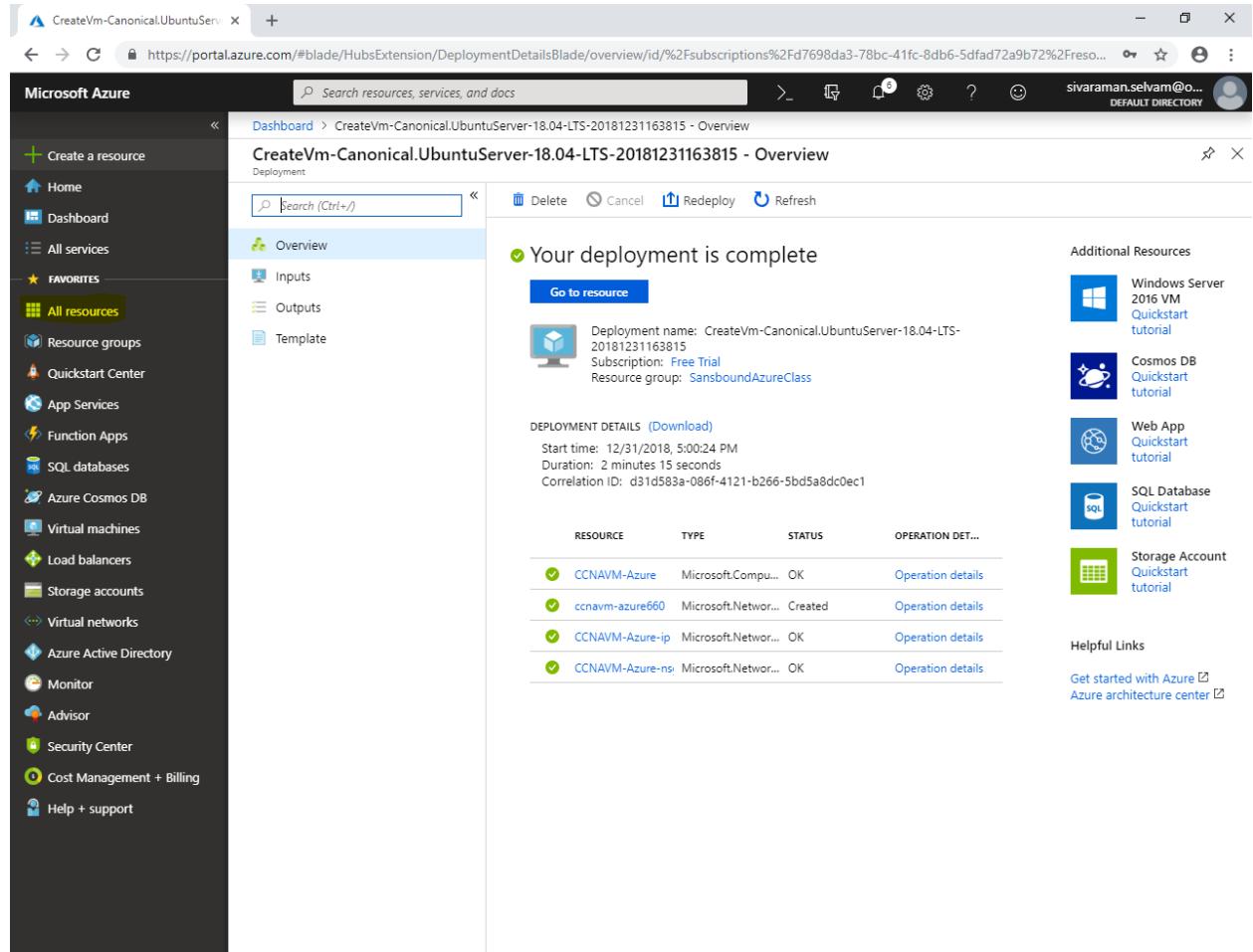
The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, Favorites, All resources, Resource groups, Quickstart Center, App Services, Function Apps, SQL databases, 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 "Create a virtual machine" under "Virtual machines". It shows a list of existing VMs, including "MCSEVM-Azure". Below this is a "Tags" section with a table header for KEY, VALUE, and RESOURCE TYPE. A note states: "Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more". A note also says: "Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated." At the bottom, there are three buttons: "Review + create" (highlighted in yellow), "Previous", and "Next : Review + create >" (also highlighted in yellow).

Click “Create”.



The screenshot shows the Microsoft Azure portal interface for creating a virtual machine. The left sidebar contains navigation links for various services like Home, Dashboard, All services, and Virtual machines. The main area is titled 'Create a virtual machine' under 'Virtual machines'. A green header bar indicates 'Validation passed'. The 'Basics' tab is selected, showing product details for 'Ubuntu Server 18.04 LTS by Canonical'. It notes that pricing is not available for this offering and lists a standard B1s size at 0.8593 INR/hr. The 'TERMS' section contains legal agreement text. The 'DISKS' section shows default settings for OS disk size (30 GB) and Premium SSD. At the bottom right, there are 'Create', 'Previous', 'Next', and 'Download a template for automation' buttons. The 'Create' button is highlighted with a yellow box.

Click “All resources”.



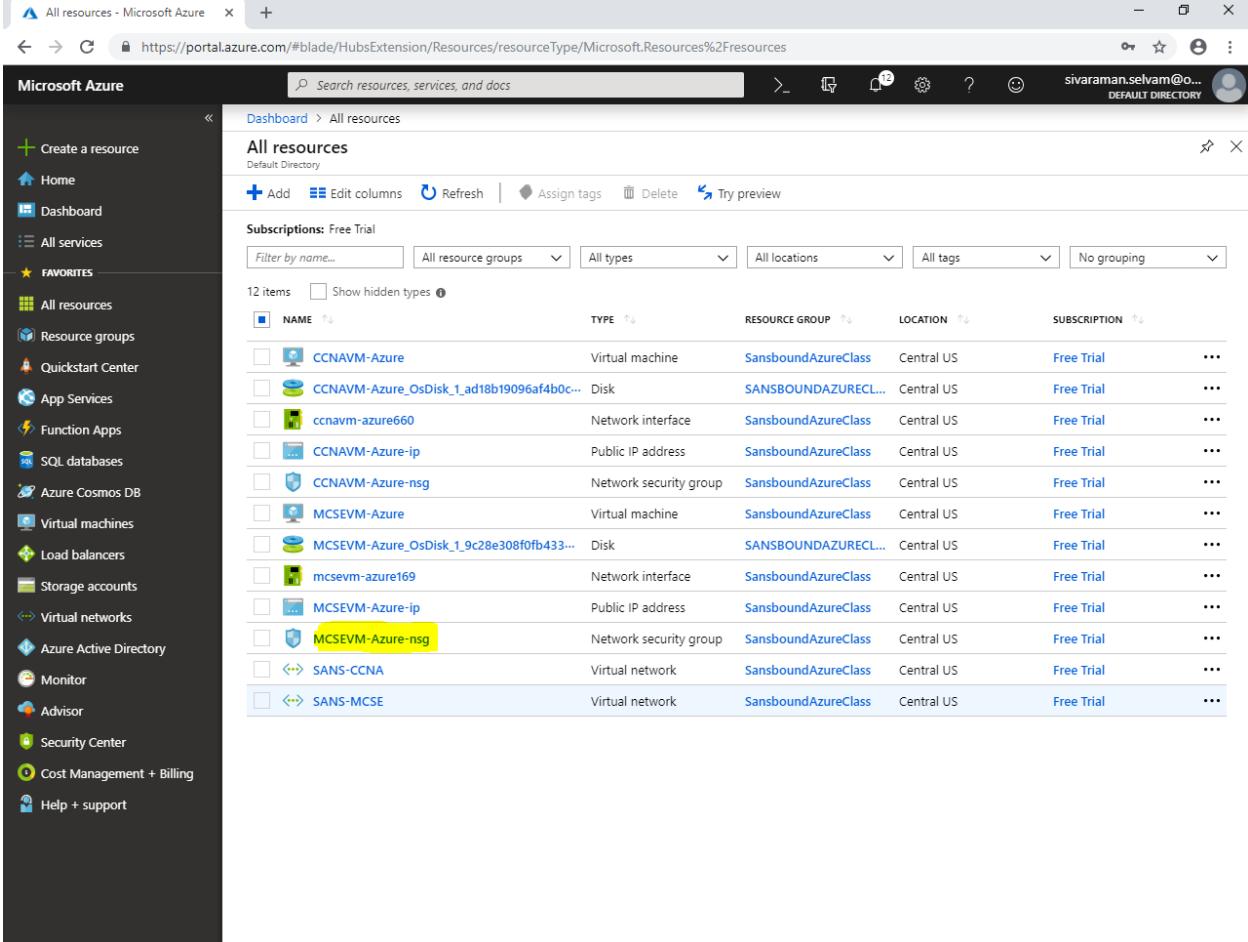
The screenshot shows the Microsoft Azure portal interface. The left sidebar is titled "Microsoft Azure" and includes a "Create a resource" button, followed by a list of services: Home, Dashboard, All services, FAVORITES (with "All resources" selected), Resource groups, Quickstart Center, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, 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 "CreateVm-Canonical.UbuntuServer-18.04-LTS-20181231163815 - Overview". It displays a summary of the deployment, stating "Your deployment is complete" with a green checkmark. Below this, it shows deployment details: Deployment name: CreateVm-Canonical.UbuntuServer-18.04-LTS-20181231163815, Subscription: Free Trial, Resource group: SansboundAzureClass. It also lists four resources created during the deployment:

RESOURCE	TYPE	STATUS	OPERATION DET...
CCNAVM-Azure	Microsoft.Compu...	OK	Operation details
ccnavm-azure660	Microsoft.Networ...	Created	Operation details
CCNAVM-Azure-ip	Microsoft.Networ...	OK	Operation details
CCNAVM-Azure-ns	Microsoft.Networ...	OK	Operation details

On the right side, there is a "Additional Resources" section with links to Windows Server 2016 VM Quickstart tutorial, Cosmos DB Quickstart tutorial, Web App Quickstart tutorial, SQL Database Quickstart tutorial, and Storage Account Quickstart tutorial. At the bottom, there is a "Helpful Links" section with links to Get started with Azure and Azure architecture center.

In “All resources”,

Click “Network security group” named as “**MCSEVM-Azure-nsg**”.

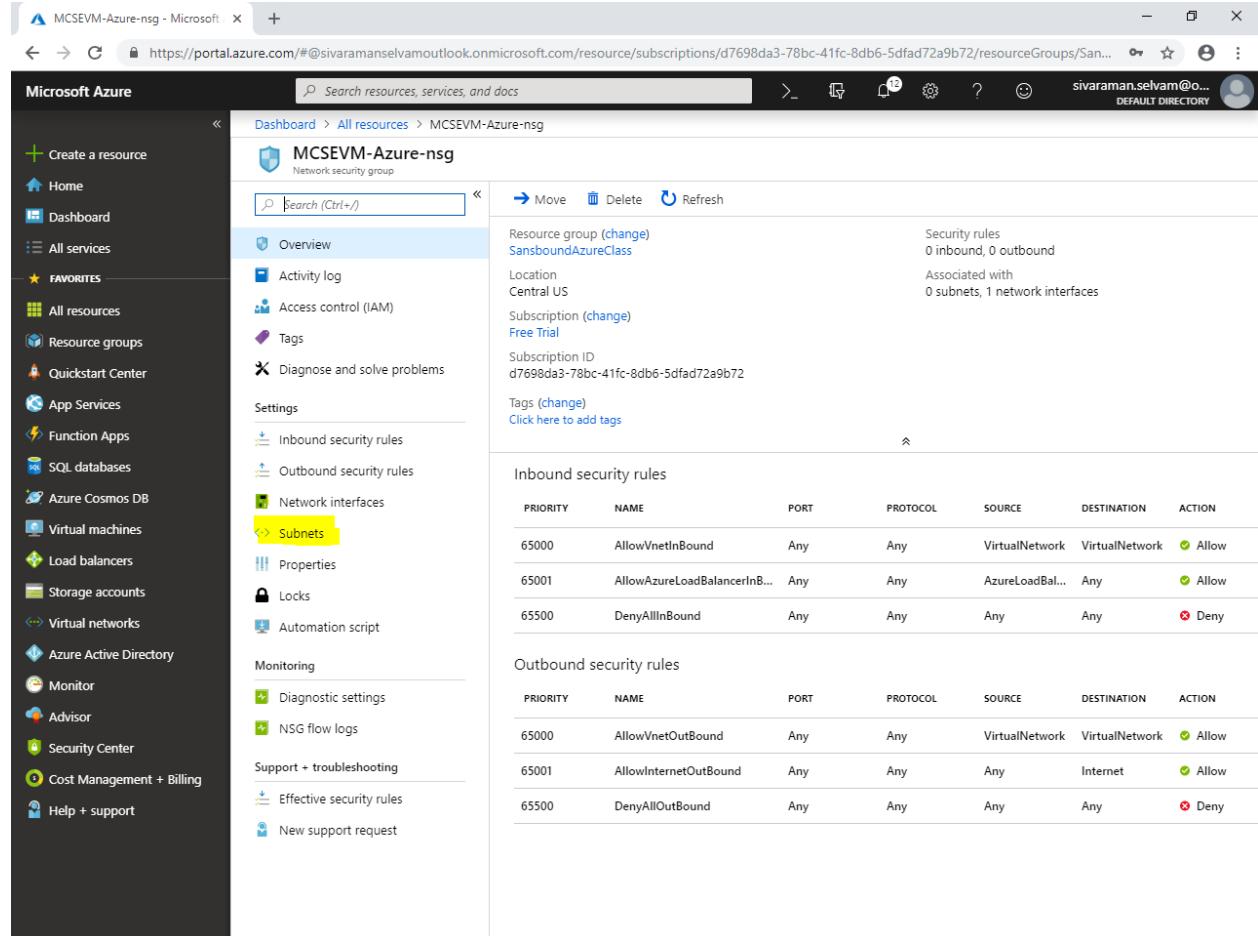


The screenshot shows the Microsoft Azure portal's "All resources" blade. The left sidebar has "All resources" selected under "FAVORITES". The main area displays a table of resources with columns: NAME, TYPE, RESOURCE GROUP, LOCATION, and SUBSCRIPTION. A filter bar at the top allows filtering by name, resource group, type, location, tags, and grouping. The "NAME" column is sorted by name. The "MCSEVM-Azure-nsg" network security group is highlighted with a yellow background. Other visible resources include various virtual machines, disks, network interfaces, and public IP addresses.

NAME	TYPE	RESOURCE GROUP	LOCATION	SUBSCRIPTION
CCNAVM-Azure	Virtual machine	SansboundAzureClass	Central US	Free Trial
CCNAVM-Azure_OsDisk_1_ad18b19096af4b0c...	Disk	SANSBOUNDAZURECL...	Central US	Free Trial
cnnavm-azure660	Network interface	SansboundAzureClass	Central US	Free Trial
CCNAVM-Azure-ip	Public IP address	SansboundAzureClass	Central US	Free Trial
CCNAVM-Azure-nsg	Network security group	SansboundAzureClass	Central US	Free Trial
MCSEVM-Azure	Virtual machine	SansboundAzureClass	Central US	Free Trial
MCSEVM-Azure_OsDisk_1_9c28e308f0fb433...	Disk	SANSBOUNDAZURECL...	Central US	Free Trial
mcsevm-azure169	Network interface	SansboundAzureClass	Central US	Free Trial
MCSEVM-Azure-ip	Public IP address	SansboundAzureClass	Central US	Free Trial
MCSEVM-Azure-nsg	Network security group	SansboundAzureClass	Central US	Free Trial
SANS-CCNA	Virtual network	SansboundAzureClass	Central US	Free Trial
SANS-MCSE	Virtual network	SansboundAzureClass	Central US	Free Trial

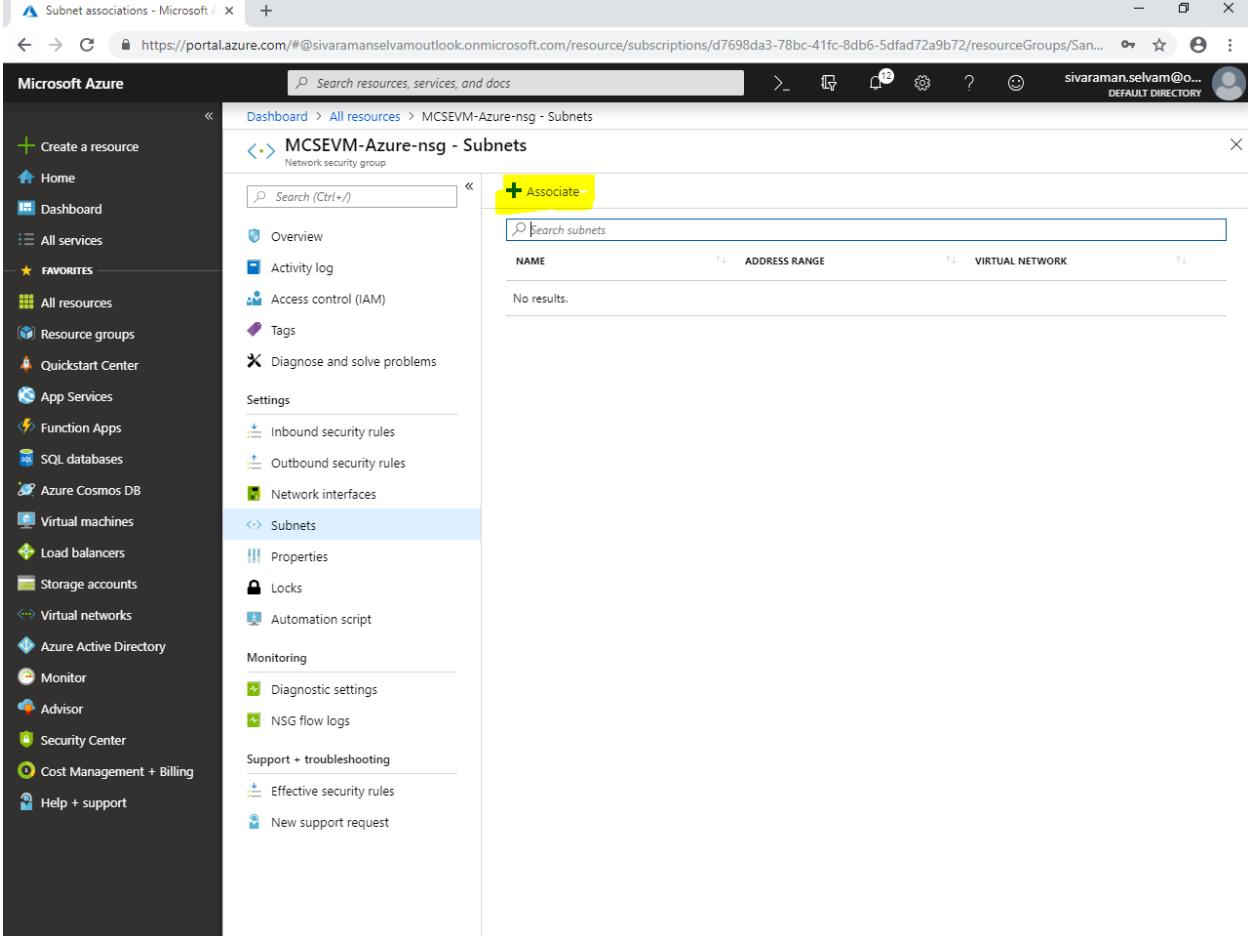
In “MCSEVM-Azure-nsg” network security group,

Click “Subnets”.



The screenshot shows the Azure portal interface for managing a Network Security Group (NSG). The left sidebar navigation includes options like Home, Dashboard, All services, Favorites, All resources, Resource groups, Quickstart Center, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Billing, and Help + support. The main content area displays the 'MCSEVM-Azure-nsg' NSG settings. The 'Overview' tab is selected. Key details shown include the resource group (SansboundAzureClass), location (Central US), subscription (Free Trial), and tags. The 'Inbound security rules' section lists three rules: AllowVnetInBound (Priority 65000, Allow), AllowAzureLoadBalancerInB... (Priority 65001, Allow), and DenyAllInBound (Priority 65500, Deny). The 'Outbound security rules' section lists three rules: AllowVnetOutBound (Priority 65000, Allow), AllowInternetOutBound (Priority 65001, Allow), and DenyAllOutBound (Priority 65500, Deny). The 'Subnets' option in the left sidebar is highlighted with a yellow box.

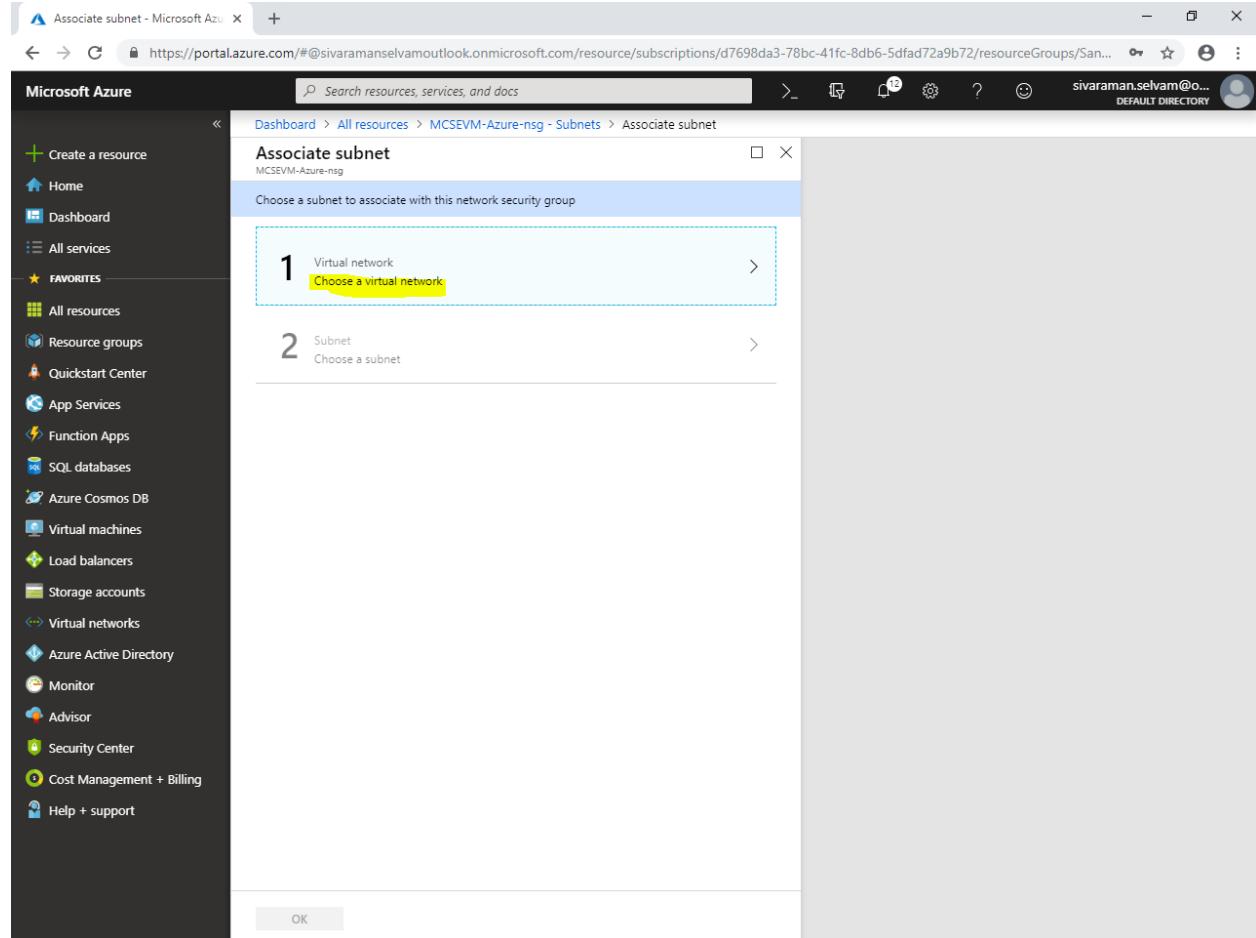
We have required to associate the “SANS-MCSEPubSubnet” to “MCSEVM-Azure-nsg” network security group.



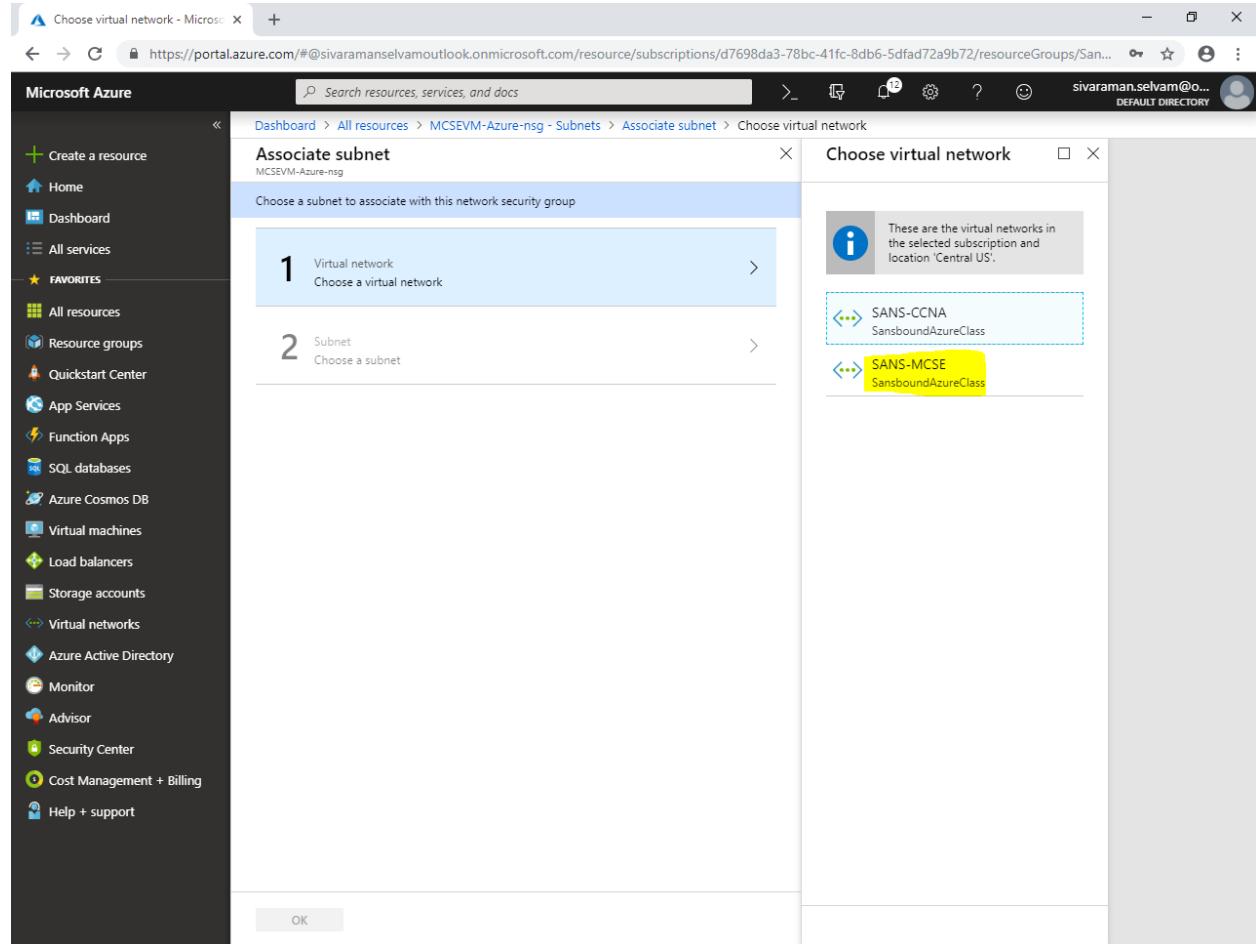
The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various service icons. The main content area is titled "MCSEVM-Azure-nsg - Subnets" and shows a list of subnets. At the top right of this list, there is a yellow-highlighted button labeled "+ Associate". Below this button is a search bar with the placeholder "Search subnets". The table below has columns for NAME, ADDRESS RANGE, and VIRTUAL NETWORK. A message "No results." is displayed in the table body.

While “Associate subnet”,

Click “Choose a virtual network”.

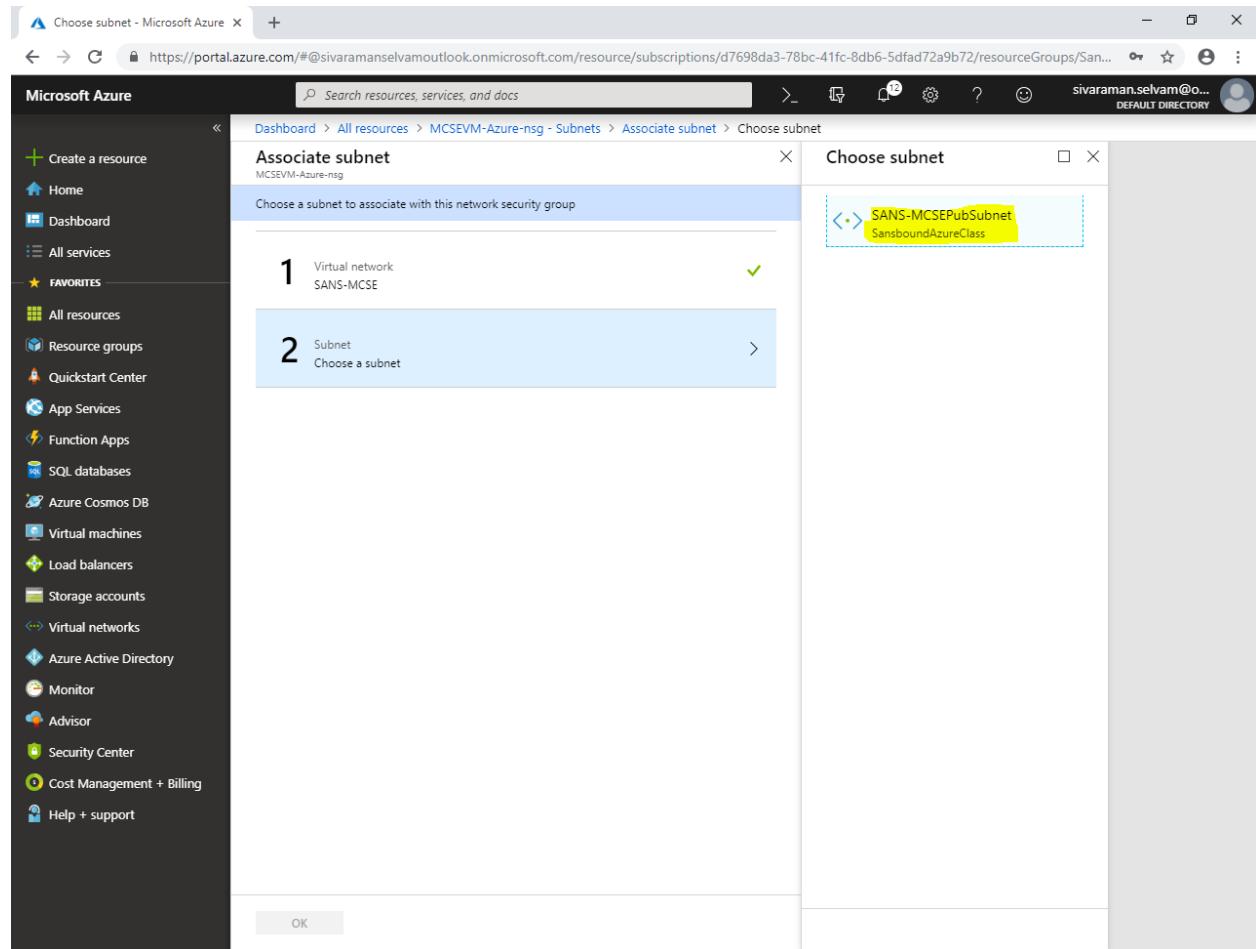


Click “**SANS-MCSE**” to select the Virtual network.



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 "MCSEVM-Azure-nsg". The first step, "Choose a virtual network", is active, showing a list of available virtual networks. The second step, "Choose a subnet", is shown below it. A modal window titled "Choose virtual network" is overlaid on the page. This modal contains an information icon and text stating, "These are the virtual networks in the selected subscription and location 'Central US'." It lists two options: "SANS-CCNA SansboundAzureClass" and "SANS-MCSE SansboundAzureClass". The "SANS-MCSE SansboundAzureClass" option is highlighted with a yellow box. At the bottom of the modal, there is an "OK" button.

In “Choose a subnet” click on “**SANS-MCSEPubSubnet**”.

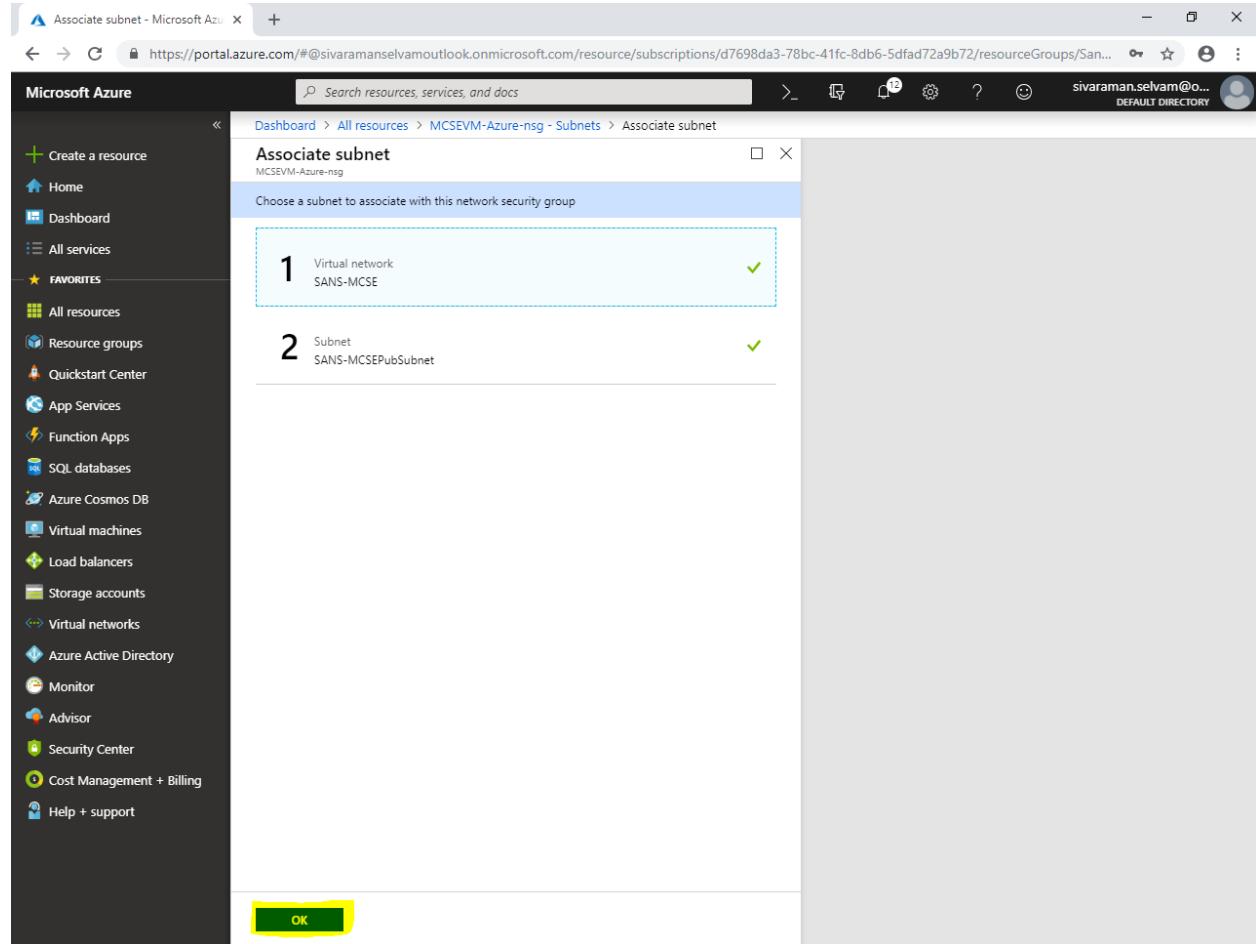


The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu is visible with various service icons and names. The main area displays a two-step process for associating a subnet with a network security group:

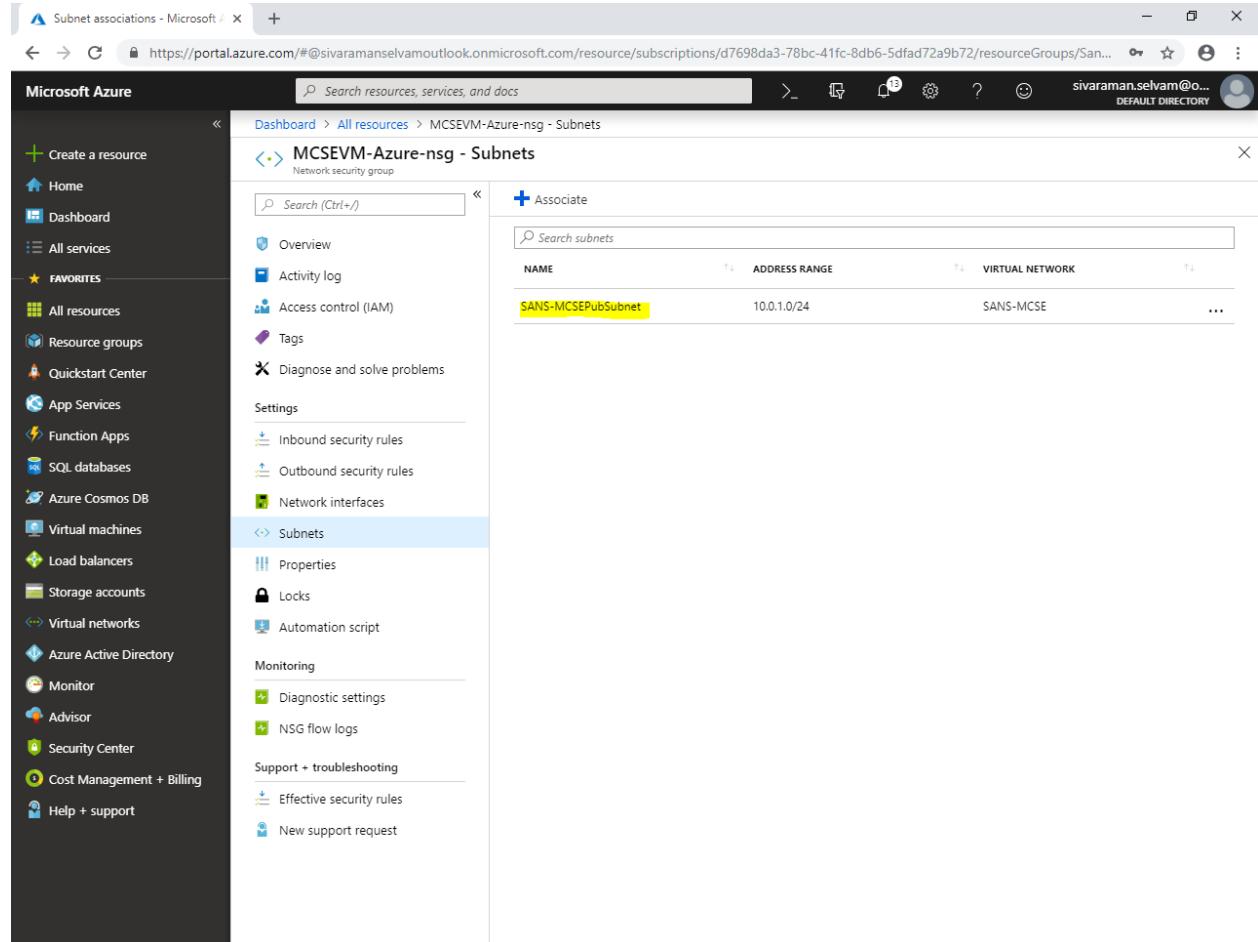
- Associate subnet**: A step titled "Choose a subnet to associate with this network security group". It lists one item:
 - 1 Virtual network SANS-MCSE
- Choose subnet**: A step titled "Choose a subnet". It lists one item:
 - 2 Subnet Choose a subnet

A yellow box highlights the text "SANS-MCSEPubSubnet" in the "Choose a subnet" list, indicating it is the target for selection.

Click "OK".



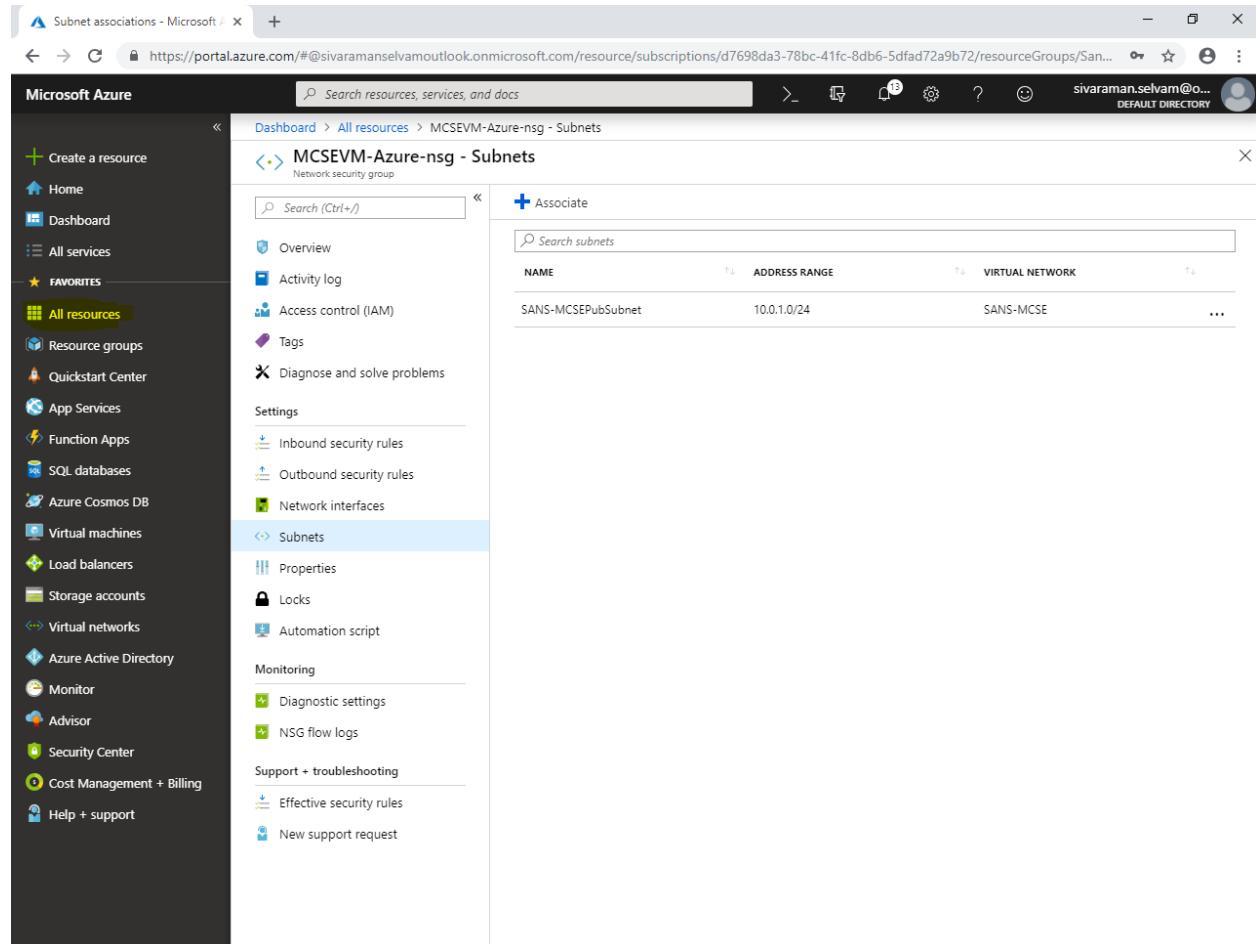
You have successfully associated the “**SANS-MCSEPubSubnet**” subnet with “**MCSEVM-Azure-nsg**” network security group.



The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various service icons. The main content area is titled "MCSEVM-Azure-nsg - Subnets" and shows a list of subnets. One subnet, "SANS-MCSEPubSubnet", is highlighted with a yellow background. The table columns are NAME, ADDRESS RANGE, and VIRTUAL NETWORK. The subnet details are: NAME: SANS-MCSEPubSubnet, ADDRESS RANGE: 10.0.1.0/24, VIRTUAL NETWORK: SANS-MCSE.

NAME	ADDRESS RANGE	VIRTUAL NETWORK
SANS-MCSEPubSubnet	10.0.1.0/24	SANS-MCSE

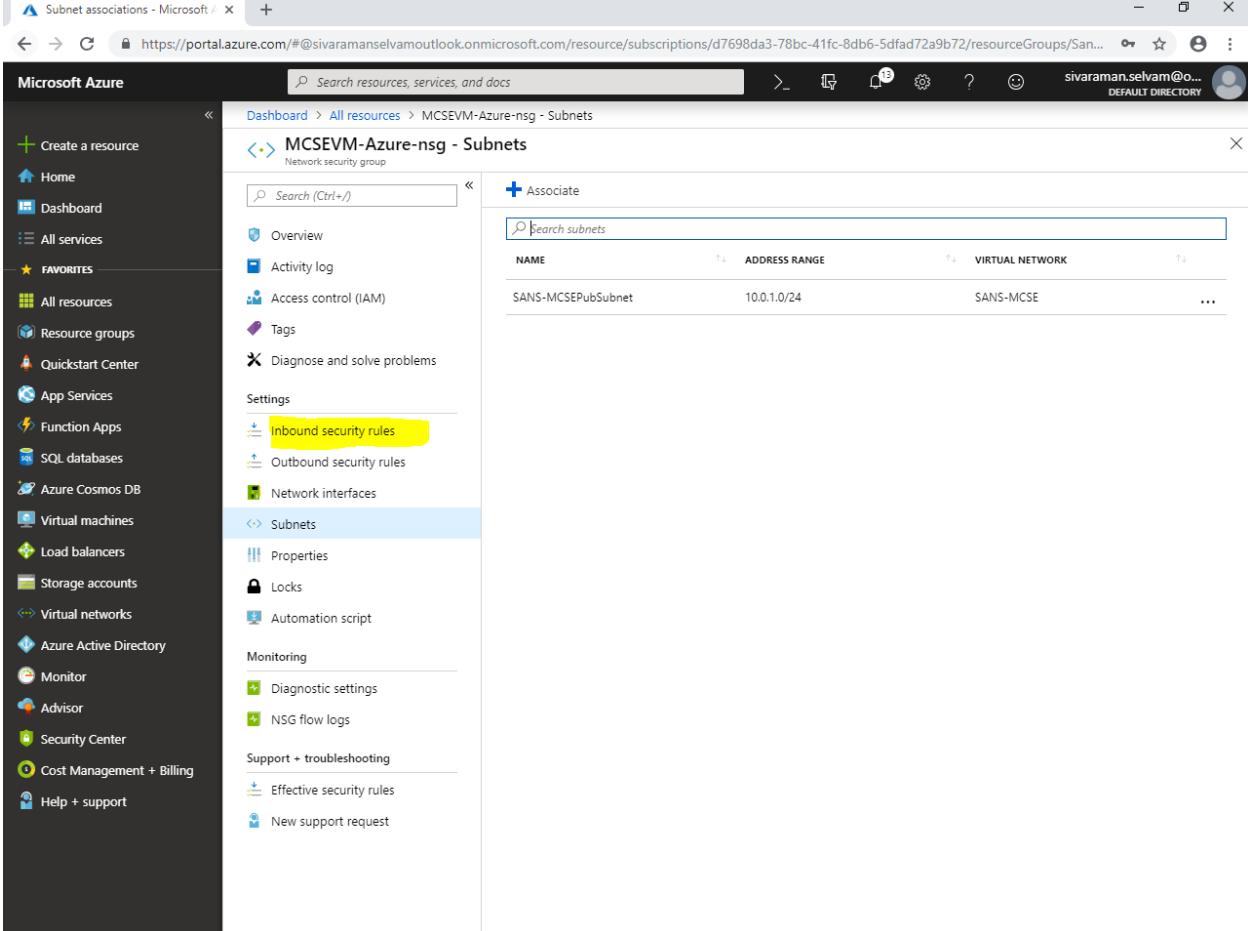
Click "All resources".



The screenshot shows the Microsoft Azure portal interface. The left sidebar is the navigation menu with various service icons. The main content area shows the 'MCSEVM-Azure-nsg - Subnets' page. The 'Subnets' tab is selected. A table lists one subnet:

NAME	ADDRESS RANGE	VIRTUAL NETWORK
SANS-MCSEPubSubnet	10.0.1.0/24	SANS-MCSE

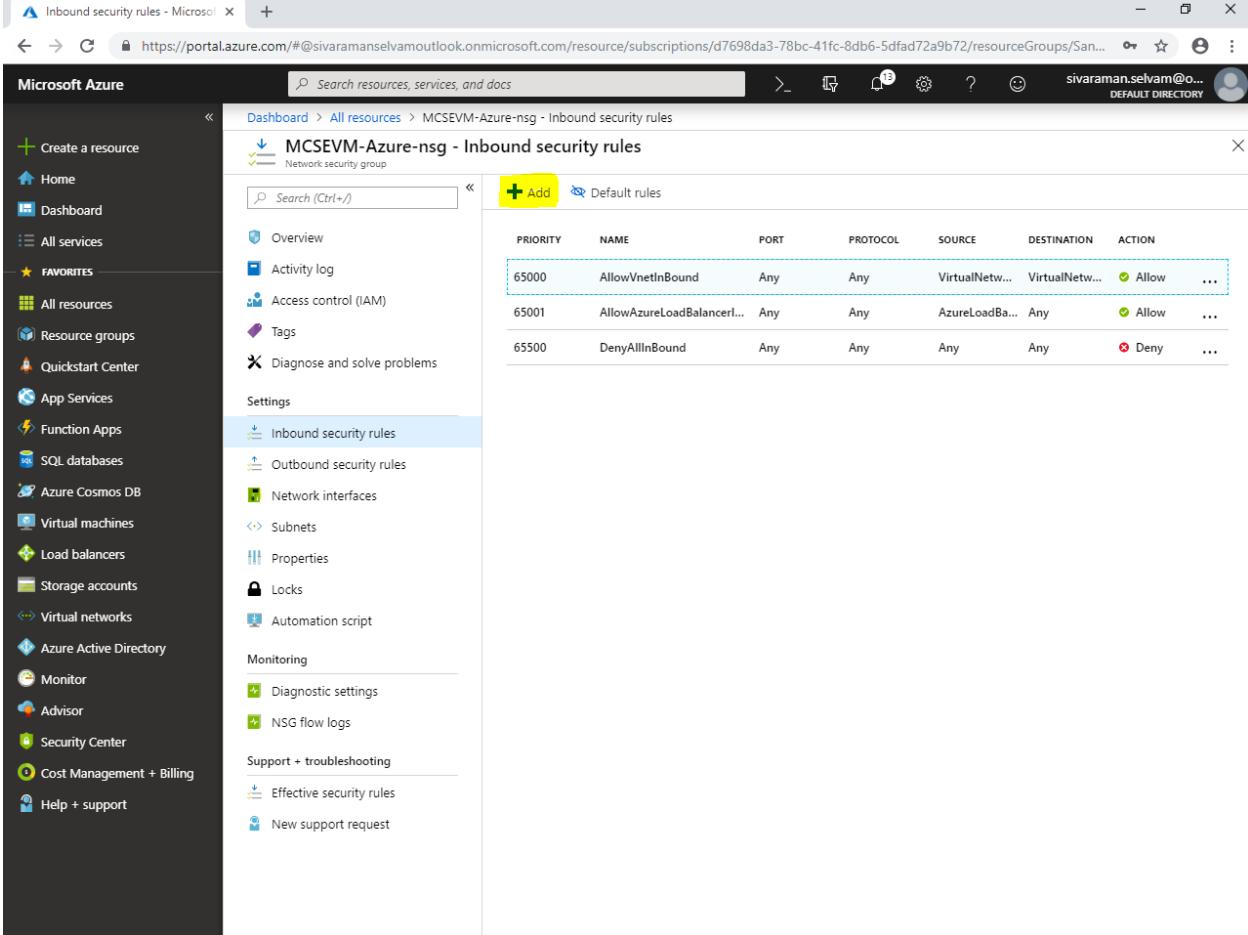
Click "Inbound security rules"



The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various service icons. The main content area displays the 'Subnets' page for a specific Network Security Group (NSG). The left sidebar has a section titled 'Settings' which includes 'Inbound security rules'. This section is highlighted with a yellow box. The main content area shows a table of subnets associated with the NSG, with one entry visible:

NAME	ADDRESS RANGE	VIRTUAL NETWORK
SANS-MCSEPubSubnet	10.0.1.0/24	SANS-MCSE

Click “Add”.



The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a list of services and resources. The main content area is titled "MCSEVM-Azure-nsg - Inbound security rules". It displays a table of existing security rules:

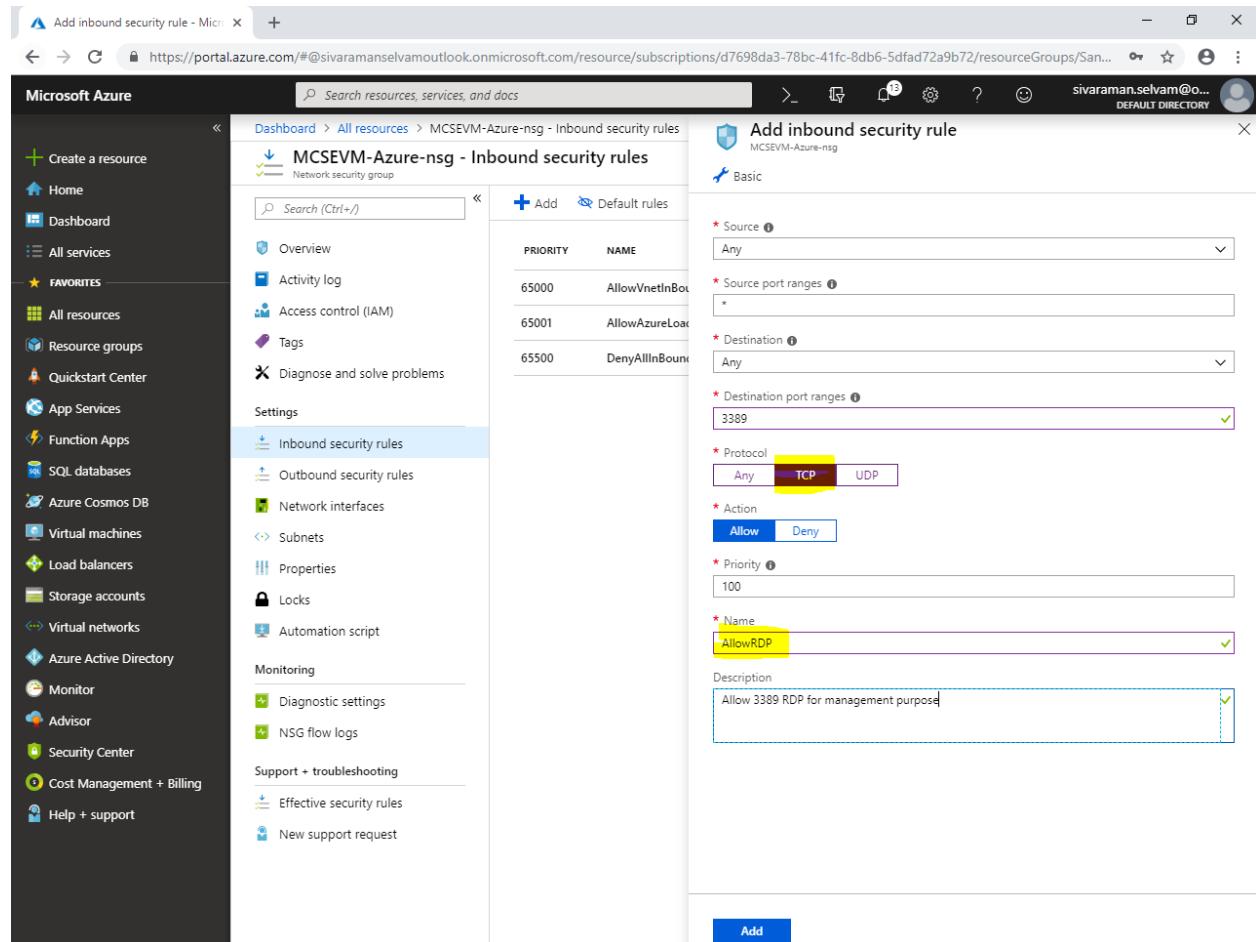
PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetInBound	Any	Any	VirtualNetw...	VirtualNetw...	Allow
65001	AllowAzureLoadBalancer...	Any	Any	AzureLoadBa...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

A yellow box highlights the "Add" button at the top right of the table header. The URL in the browser address bar is <https://portal.azure.com/#@sivaraman selvam outlook.onmicrosoft.com/resource/subscriptions/d7698da3-78bc-41fc-8db6-5dfad72a9b72/resourceGroups/San...>.

While “Add inbound security rule”,

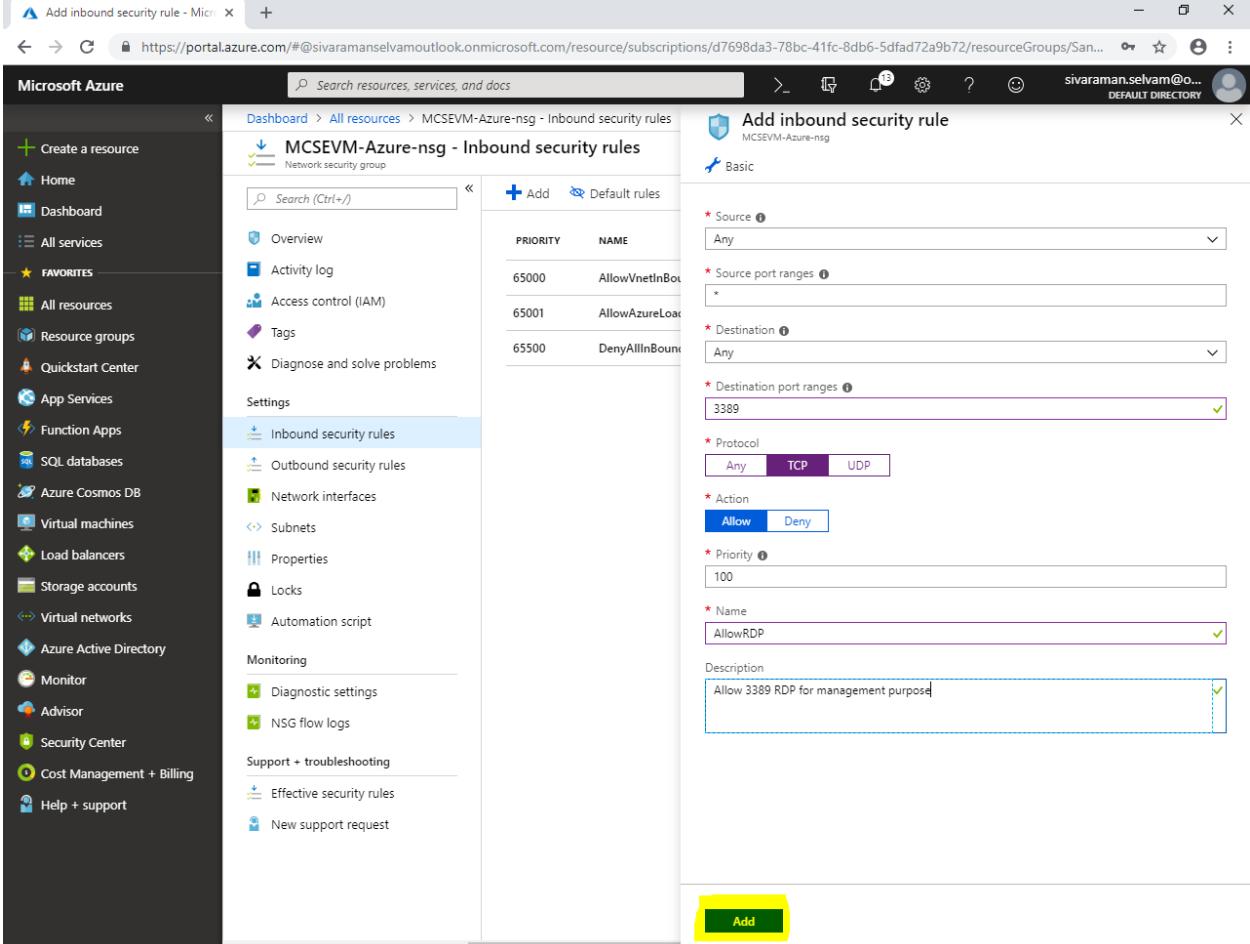
Select “Protocol” as “TCP”.

Type Rule “Name” as “AllowRDP”.



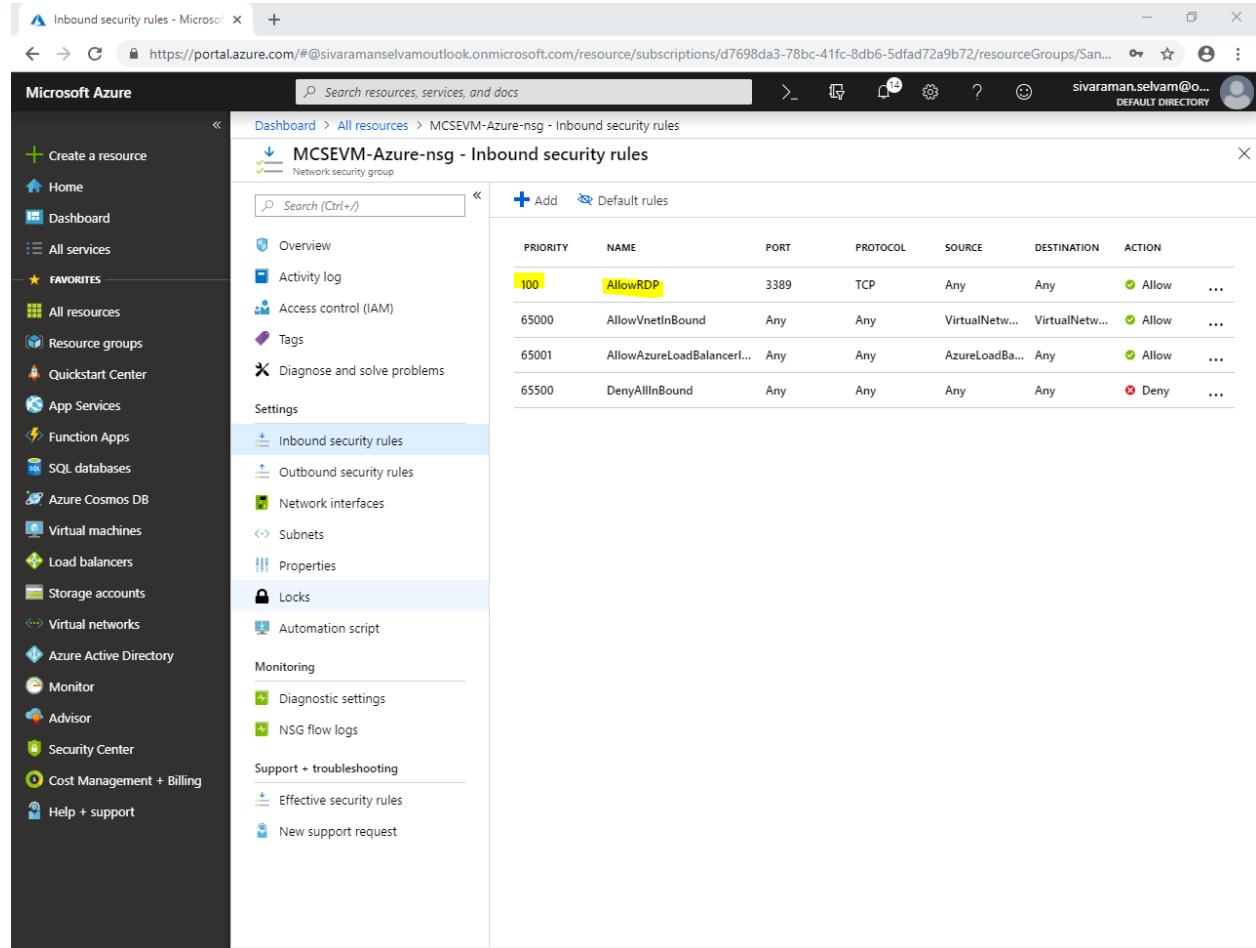
The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu includes options like Create a resource, Home, Dashboard, All services, Favorites (All resources, Resource groups, Quickstart Center, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Billing, Help + support). The main content area shows the 'MCSEVM-Azure-nsg - Inbound security rules' section under 'MCSEVM-Azure-nsg - Network security group'. A table lists existing rules: Priority 65000 (AllowVnetInbound), Priority 65001 (AllowAzureLoadBalanced), and Priority 65500 (DenyAllInbound). To the right, a 'Basic' configuration pane is open for adding a new rule. It includes fields for Source (Any), Source port ranges (3389), Destination (Any), Destination port ranges (3389), Protocol (TCP selected), Action (Allow), Priority (100), Name (AllowRDP), and Description (Allow 3389 RDP for management purpose). The 'Protocol' dropdown has 'TCP' highlighted.

Click "Add".



The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu includes options like 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES' (with 'All resources' selected), '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 'MCSEVM-Azure-nsg - Inbound security rules' page under 'All resources'. A sub-menu on the right lists 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Settings' (with 'Inbound security rules' selected), 'Outbound security rules', 'Network interfaces', 'Subnets', 'Properties', 'Locks', 'Automation script', 'Monitoring' (with 'Diagnostic settings' and 'NSG flow logs' selected), 'Support + troubleshooting' (with 'Effective security rules' and 'New support request' selected), and 'Description'. A modal dialog box titled 'Add inbound security rule' is open on the right, showing fields for 'Source' (Any), 'Source port ranges' (*), 'Destination' (Any), 'Destination port ranges' (3389), 'Protocol' (TCP selected), 'Action' (Allow selected), 'Priority' (100), 'Name' (AllowRDP), and 'Description' (Allow 3389 RDP for management purpose). The 'Add' button at the bottom of the dialog is highlighted with a yellow box.

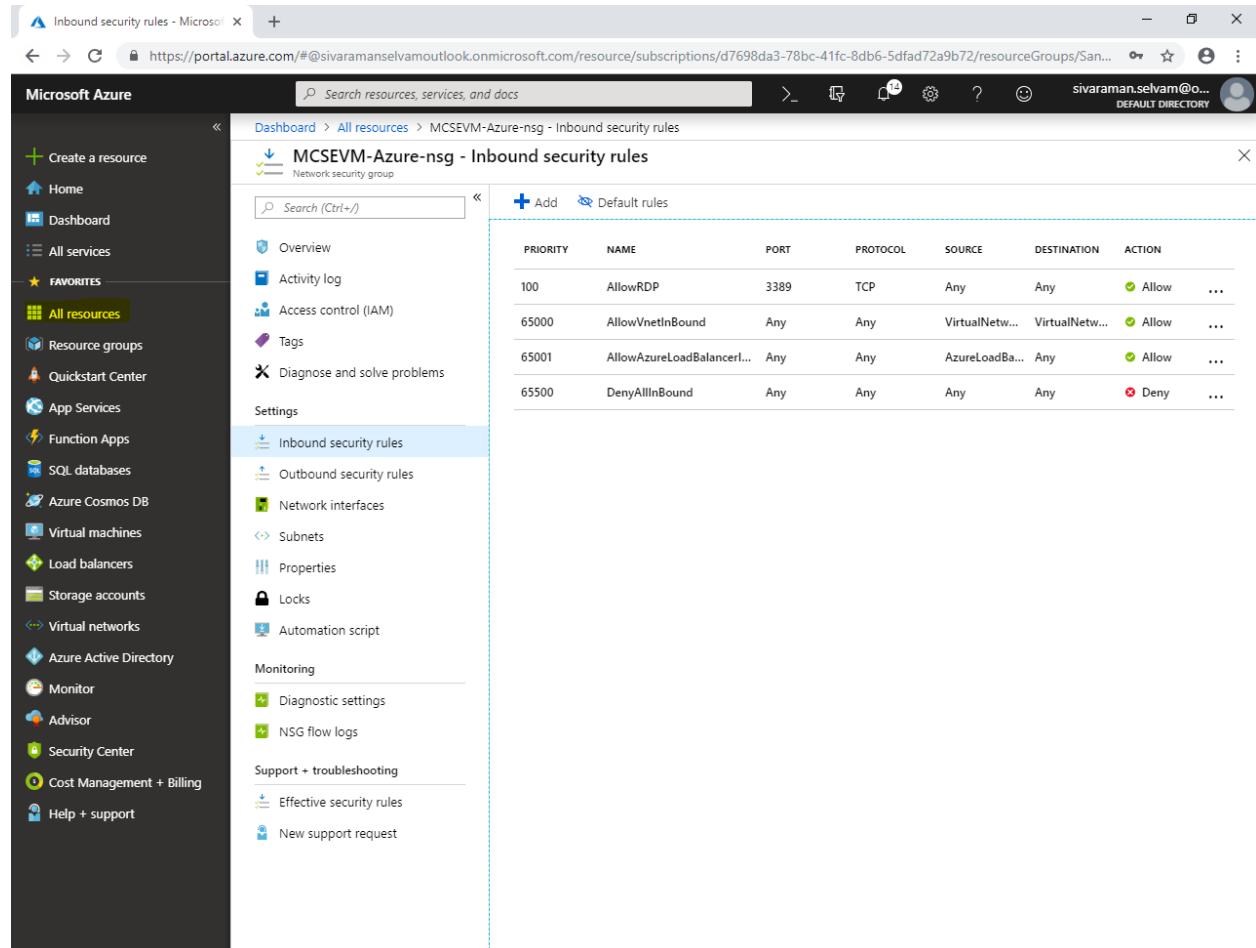
We have allowed “RDP” port to manage the Windows Servers remotely.



The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a list of services and favorites. The main content area is titled "MCSEVM-Azure-nsg - Inbound security rules". On the right, there is a table of security rules:

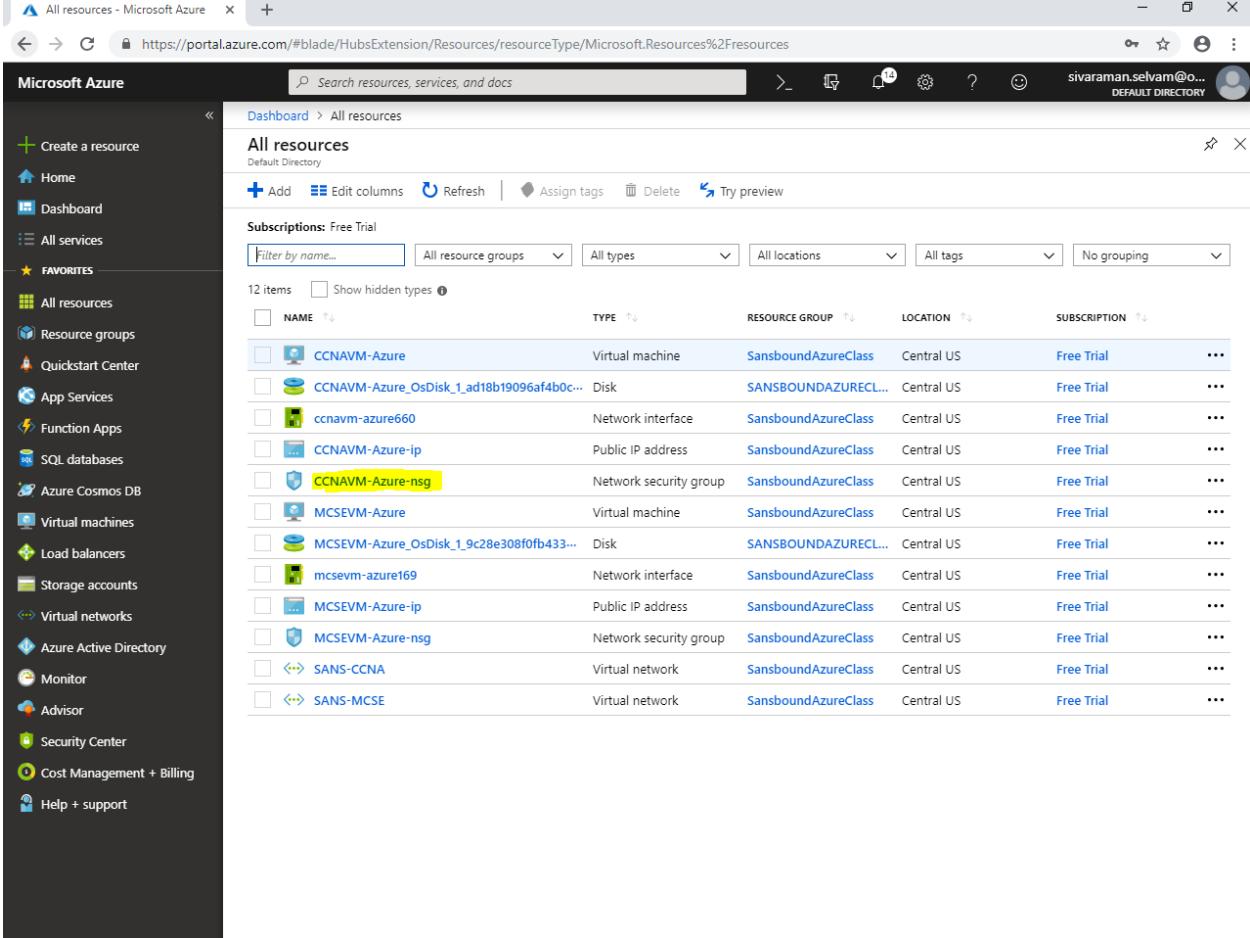
PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	AllowRDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetw...	VirtualNetw...	Allow
65001	AllowAzureLoadBalancerI...	Any	Any	AzureLoadBa...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Click "All resources".



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

Click “CCNAVM-Azure-nsg” Network security group.

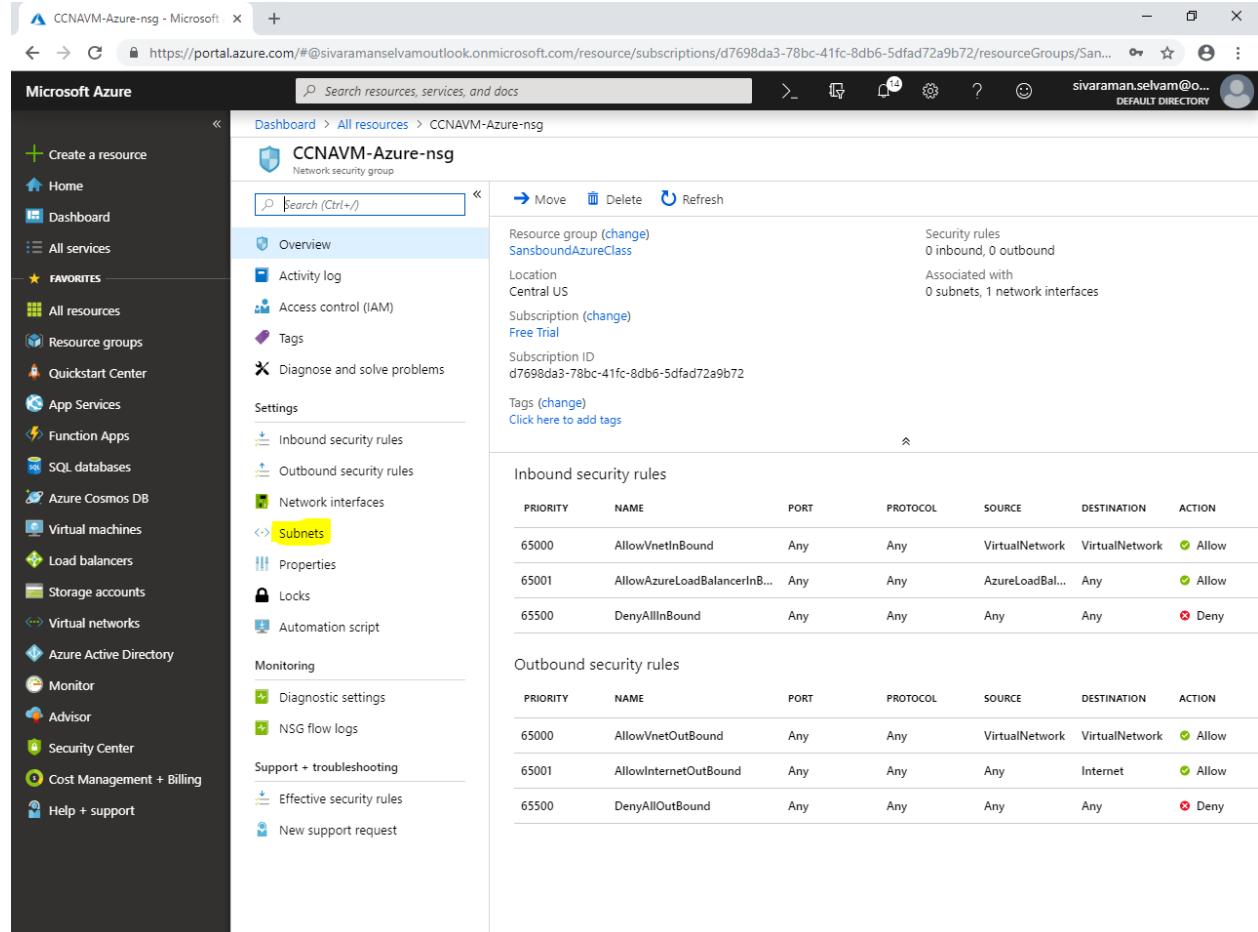


The screenshot shows the Microsoft Azure portal's "All resources" blade. The left sidebar contains a "FAVORITES" section with various service icons. The main area displays a table of 12 items, with the "CCNAVM-Azure-nsg" row highlighted by a yellow box. The columns in the table are NAME, TYPE, RESOURCE GROUP, LOCATION, and SUBSCRIPTION. The "CCNAVM-Azure-nsg" entry is listed under the "Network security group" type, located in the "SansboundAzureClass" resource group, in Central US, and associated with the "Free Trial" subscription.

NAME	TYPE	RESOURCE GROUP	LOCATION	SUBSCRIPTION
CCNAVM-Azure	Virtual machine	SansboundAzureClass	Central US	Free Trial
CCNAVM-Azure_OsDisk_1_ad18b19096af4b0c...	Disk	SANSONDAZURECL...	Central US	Free Trial
ccnavm-azure660	Network interface	SansboundAzureClass	Central US	Free Trial
CCNAVM-Azure-ip	Public IP address	SansboundAzureClass	Central US	Free Trial
CCNAVM-Azure-nsg	Network security group	SansboundAzureClass	Central US	Free Trial
MCSEVM-Azure	Virtual machine	SansboundAzureClass	Central US	Free Trial
MCSEVM-Azure_OsDisk_1_9c28e308f0fb433...	Disk	SANSONDAZURECL...	Central US	Free Trial
mcsevm-azure169	Network interface	SansboundAzureClass	Central US	Free Trial
MCSEVM-Azure-ip	Public IP address	SansboundAzureClass	Central US	Free Trial
MCSEVM-Azure-nsg	Network security group	SansboundAzureClass	Central US	Free Trial
SANS-CCNA	Virtual network	SansboundAzureClass	Central US	Free Trial
SANS-MCSE	Virtual network	SansboundAzureClass	Central US	Free Trial

In “CCNAVM-Azure-nsg” network security group,

Click “Subnets”.

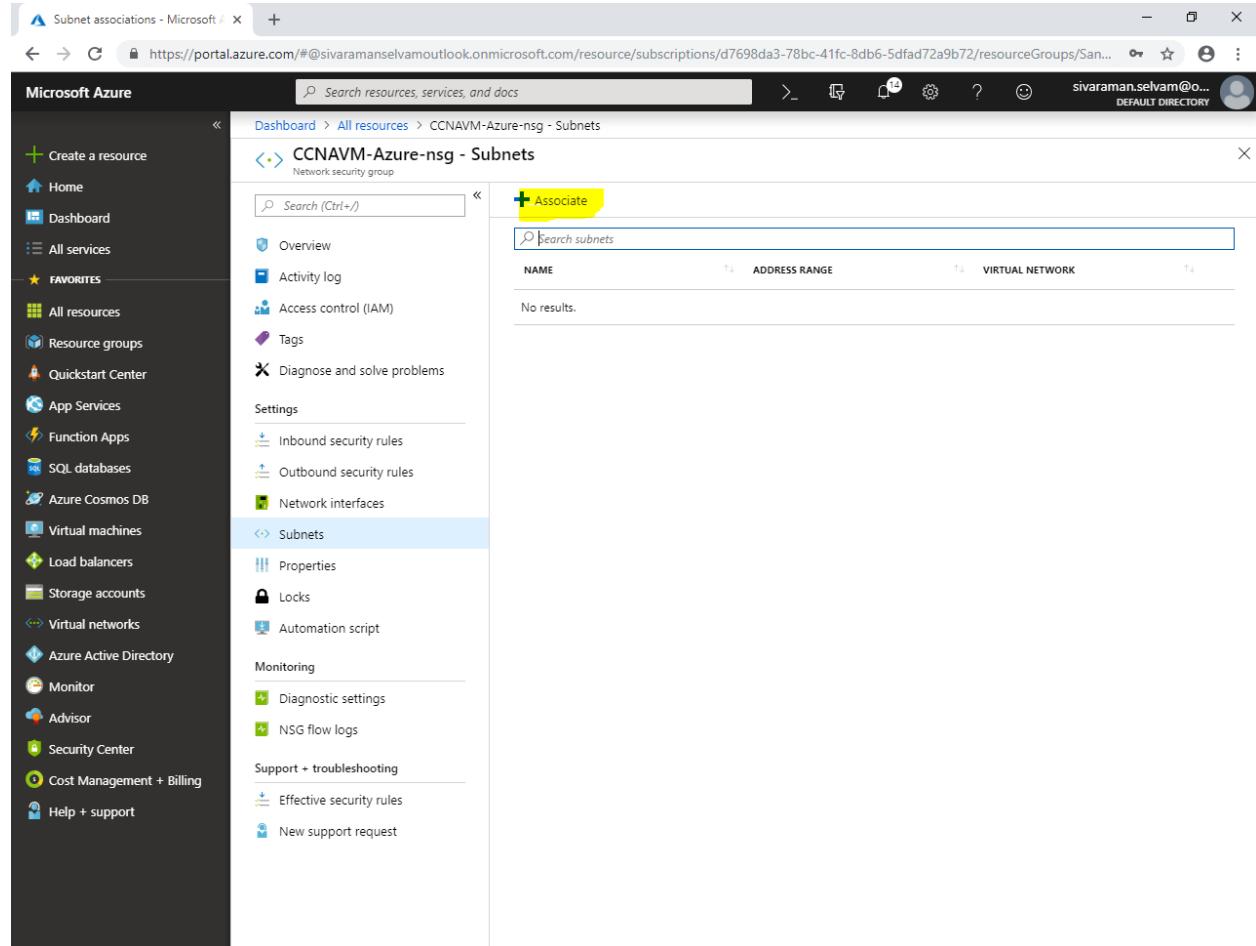


The screenshot shows the Microsoft Azure portal interface. The left sidebar is filled with various service icons. In the main content area, the title bar says "CCNAVM-Azure-nsg - Microsoft" and the URL is "https://portal.azure.com/#@sivaramselvamoutlook.onmicrosoft.com/resource/subscriptions/d7698da3-78bc-41fc-8db6-5dfad72a9b72/resourceGroups/San...". The main content is titled "CCNAVM-Azure-nsg" and "Network security group". The "Overview" tab is selected. On the right, there are sections for "Resource group (change)", "Subscription (change)", and "Tags". Below these are two tables: "Inbound security rules" and "Outbound security rules", both of which are currently empty.

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

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

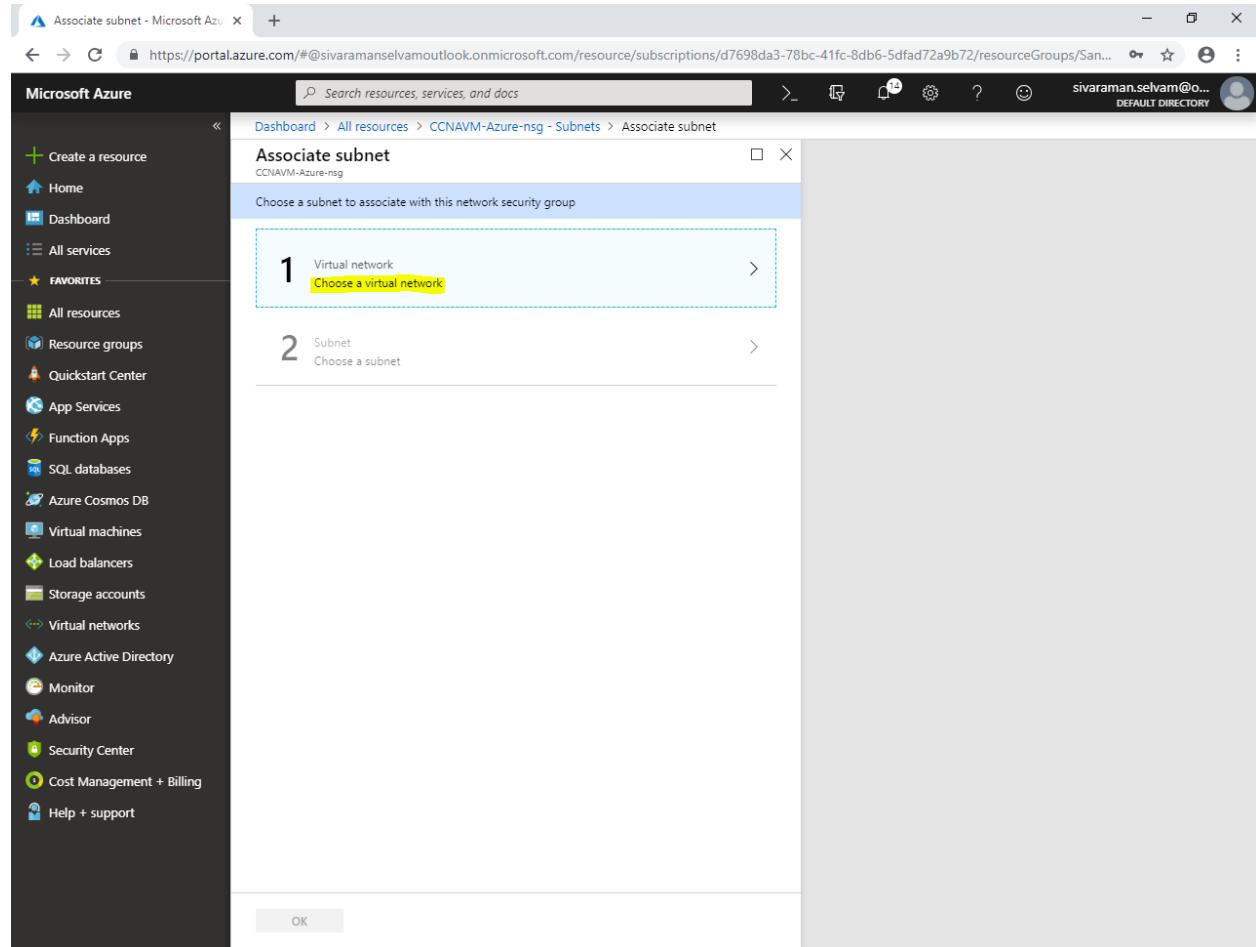
In “Subnets” click “Associate” to associate the subnet to network security group.



The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various service icons. The main content area is titled "CCNAVM-Azure-nsg - Subnets". On the left, there is a sidebar with several options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Inbound security rules, Outbound security rules, Network interfaces, Subnets, Properties, Locks, Automation script), Monitoring (Diagnostic settings, NSG flow logs), Support + troubleshooting (Effective security rules, New support request), and Help + support. A large yellow box highlights the "Associate" button at the top right of the main content area. Below it is a search bar labeled "Search subnets" and a table with columns: NAME, ADDRESS RANGE, and VIRTUAL NETWORK. The table displays the message "No results."

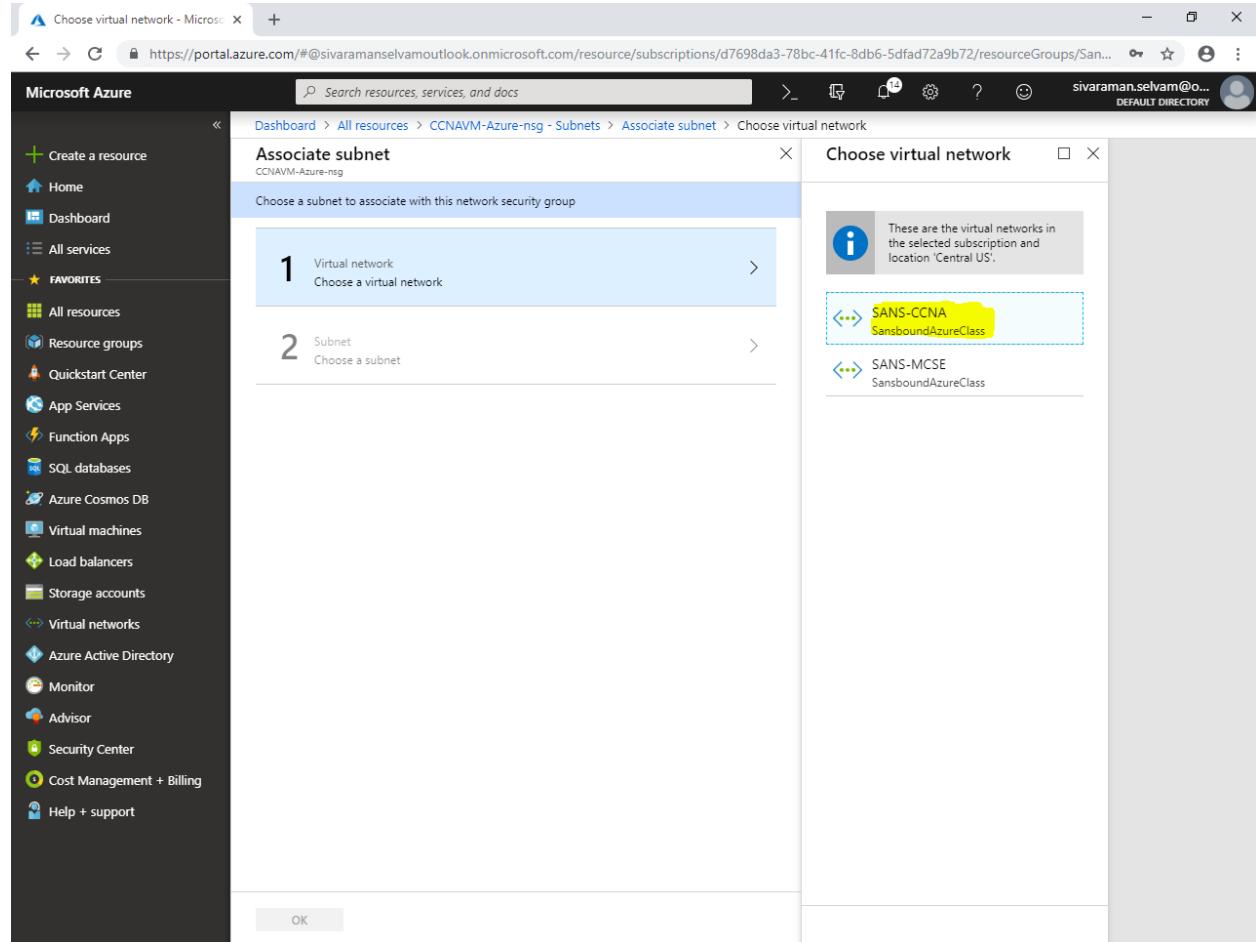
While associate subnet,

Click **"Choose a virtual network"**



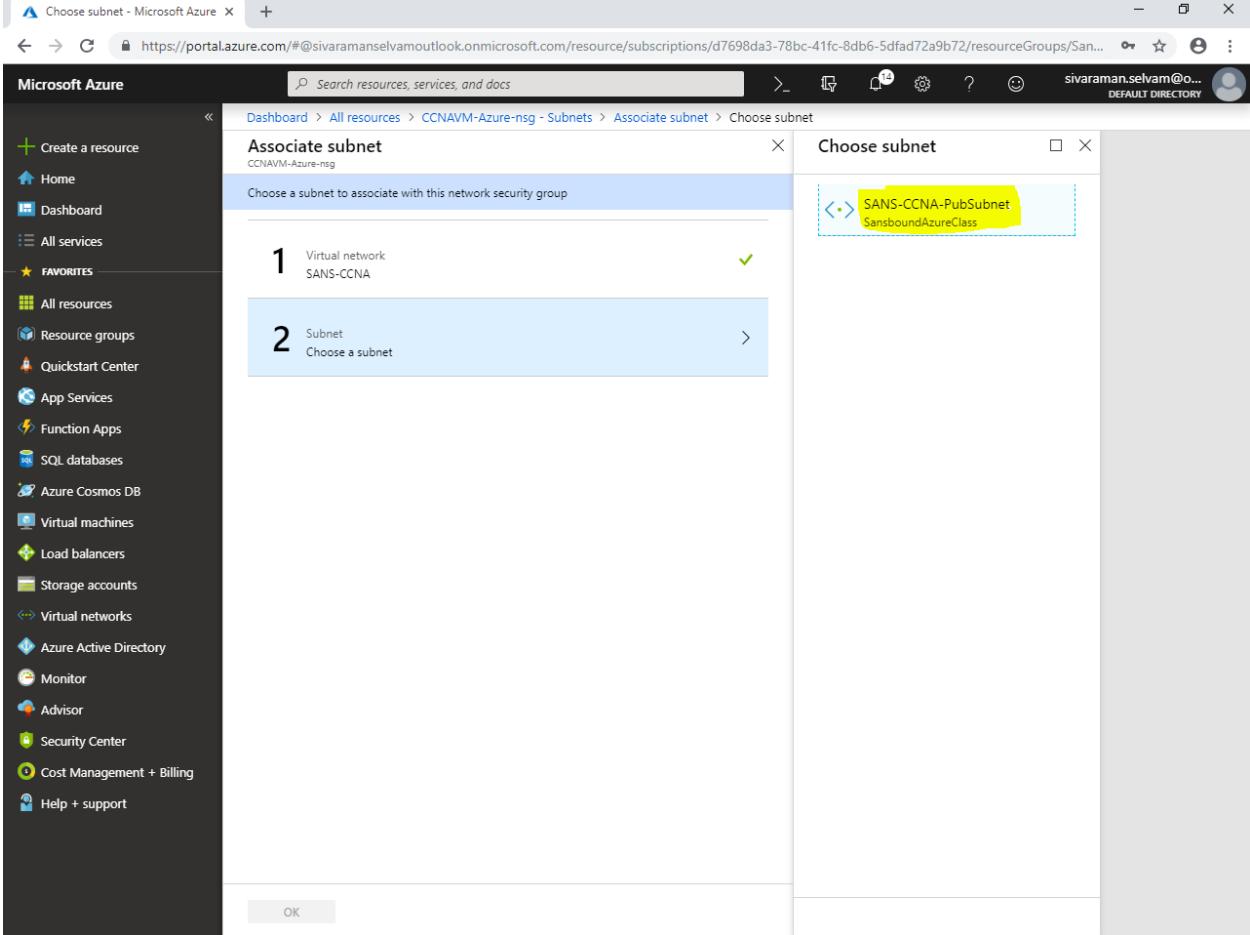
The screenshot shows the 'Associate subnet' dialog box in the Microsoft Azure portal. The URL in the browser is <https://portal.azure.com/#@sivaramselvamoutlook.onmicrosoft.com/resource/subscriptions/d7698da3-78bc-41fc-8db6-5dfad72a9b72/resourceGroups/San...>. The dialog box is titled 'Associate subnet' and shows two steps: 1. Virtual network (with 'Choose a virtual network' highlighted) and 2. Subnet (with 'Choose a subnet'). The left sidebar shows various Azure services like Home, Dashboard, All services, and Virtual machines.

Click on "SANS-CCNA" to select Virtual network.



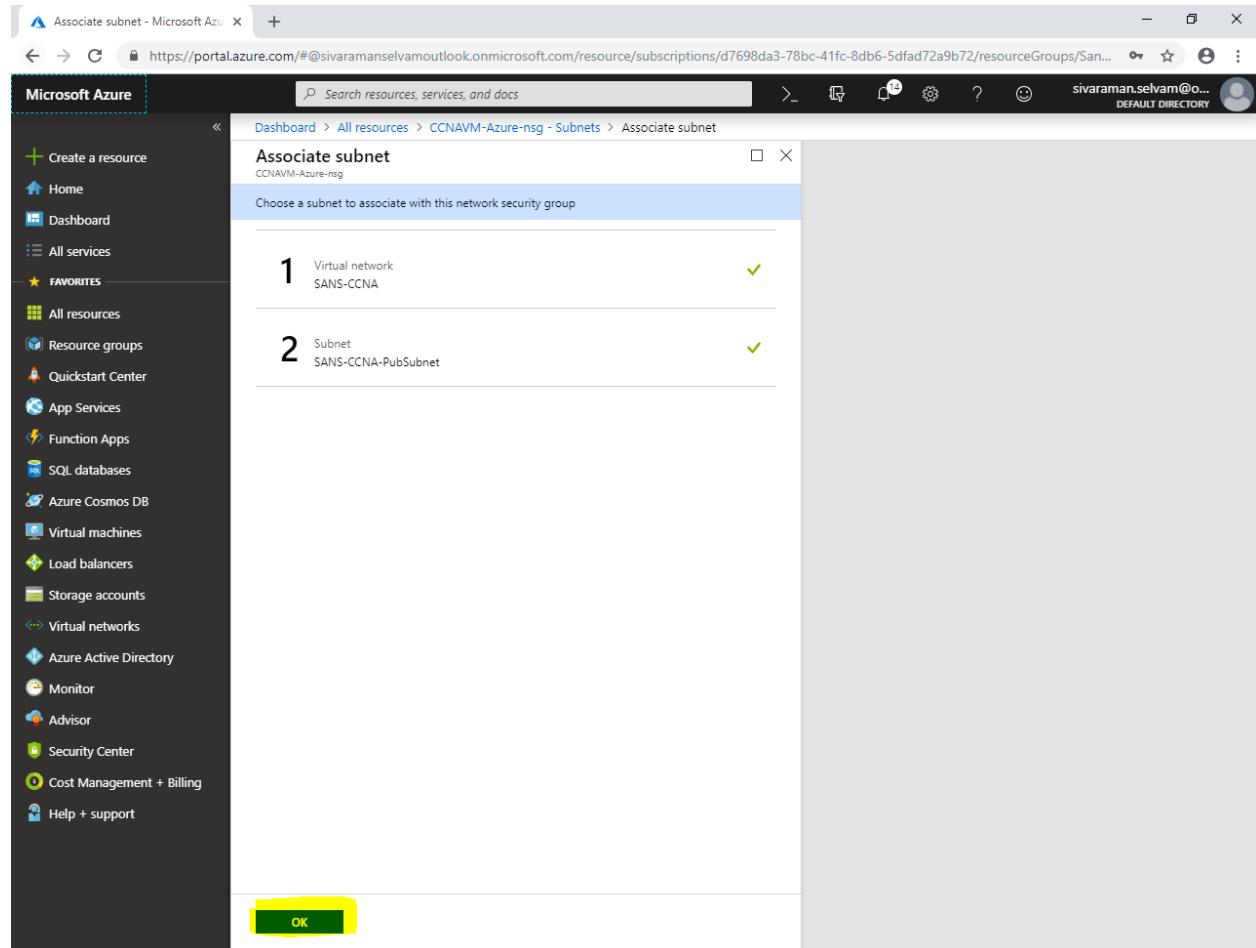
The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu is visible with various service icons. The main area displays a step-by-step wizard titled 'Associate subnet'. Step 1, 'Virtual network', shows the user choosing a virtual network from a list. Step 2, 'Subnet', shows the user choosing a subnet from a list. To the right, a modal window titled 'Choose virtual network' lists available virtual networks. One entry, 'SANS-CCNA SansboundAzureClass', is highlighted with a yellow box. An information icon in the modal window states: 'These are the virtual networks in the selected subscription and location 'Central US''. Other entries in the list include 'SANS-MCSE SansboundAzureClass'.

In “Choose a subnet” click on “**SANS-CCNA-PubSubnet**”.



The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons and links 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 shows a "Associate subnet" wizard. Step 1, "Virtual network", has "SANS-CCNA" selected. Step 2, "Subnet", has "Choose a subnet" selected. A yellow box highlights the option "SANS-CCNA-PubSubnet" in the list of subnets. At the bottom right of the wizard, there's an "OK" button.

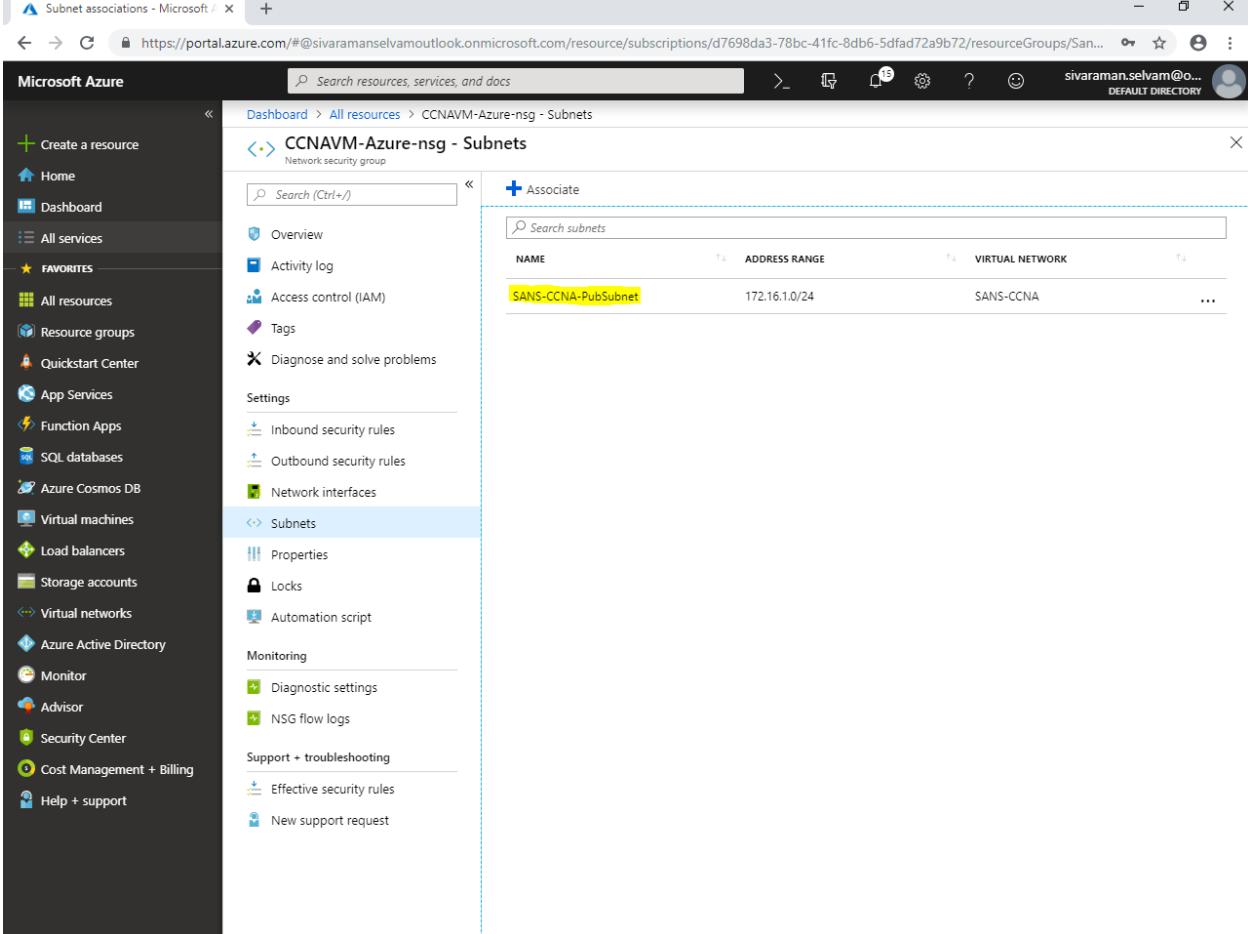
Click "OK".



The screenshot shows the Microsoft Azure portal interface. On the left is the navigation sidebar with various service icons. The main area displays a 'Associate subnet' dialog box. Inside the dialog, under the heading 'Choose a subnet to associate with this network security group', there are two entries: '1 Virtual network SANS-CCNA' and '2 Subnet SANS-CCNA-PubSubnet', both of which have green checkmarks next to them. At the bottom of the dialog is a prominent yellow 'OK' button.

In Network security group “**Subnets**”,

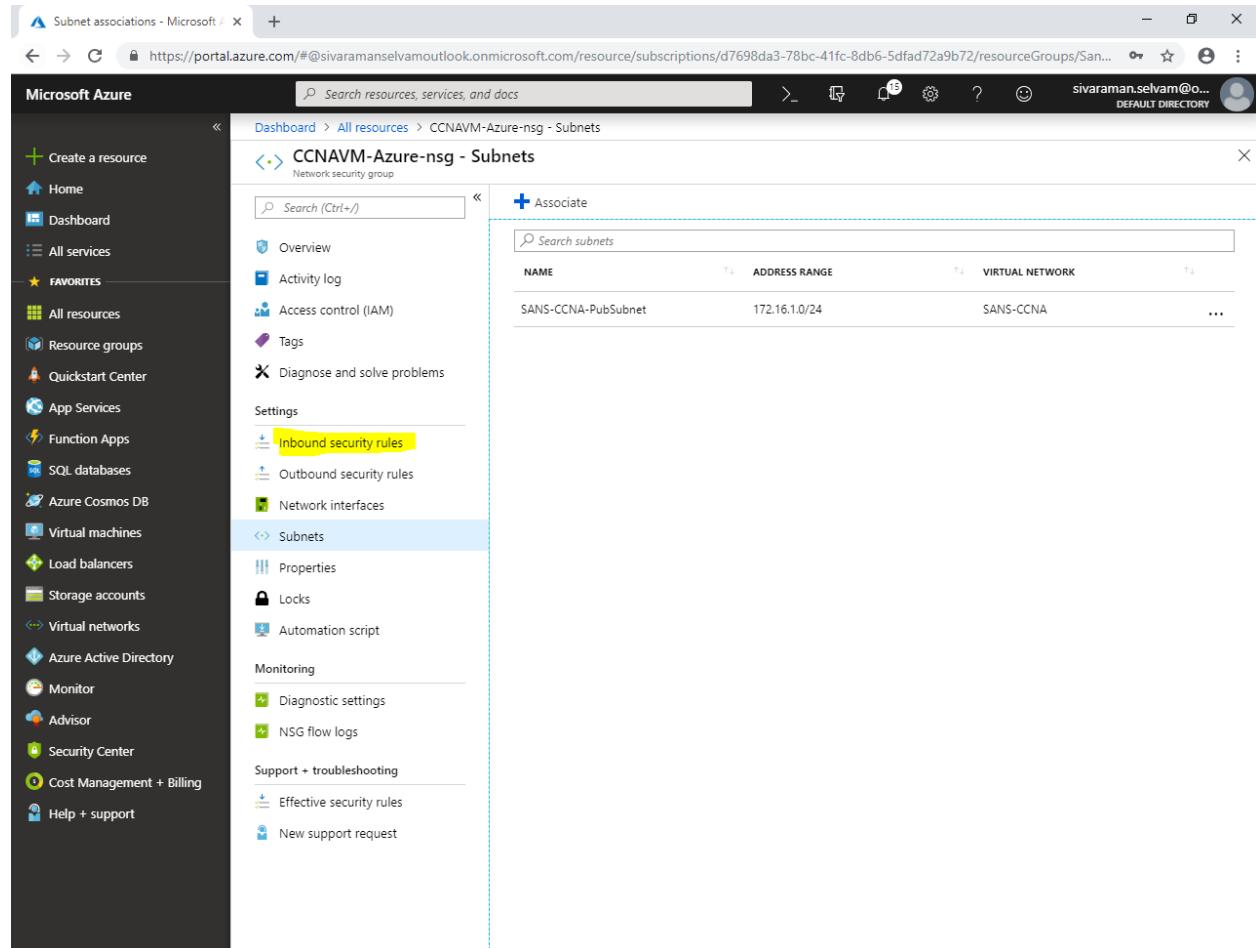
We are able see that “**SANS-CCNA-PubSubnet**” has been successfully associated with “**CCNAVM-Azure-nsg**” network security group.



The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a list of services under 'FAVORITES'. The main area shows the 'Subnets' page for the 'CCNAVM-Azure-nsg' network security group. The table lists one subnet:

NAME	ADDRESS RANGE	VIRTUAL NETWORK
SANS-CCNA-PubSubnet	172.16.1.0/24	SANS-CCNA

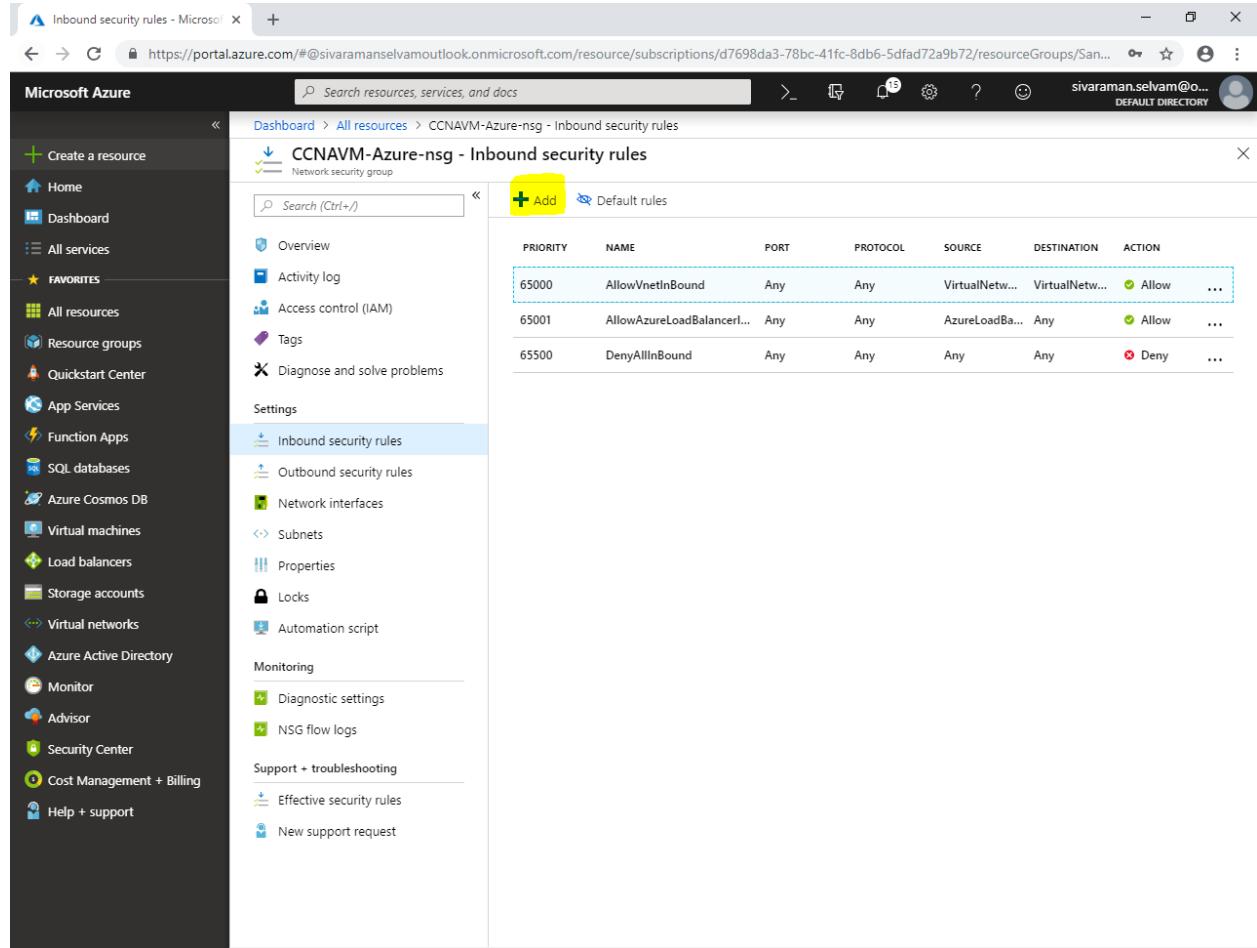
Click "Inbound security rules",



The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various service icons. The main content area displays the 'Subnets' section of a Network Security Group (NSG). The 'Associate' tab is selected, showing a table of subnets associated with the NSG. One row is visible: 'SANS-CCNA-PubSubnet' with address range '172.16.1.0/24' and virtual network 'SANS-CCNA'. On the left, a detailed sidebar for the 'Subnets' section is open, listing options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (with 'Inbound security rules' highlighted in yellow), Outbound security rules, Network interfaces, Properties, Locks, Automation script, Monitoring (Diagnostic settings, NSG flow logs), Support + troubleshooting (Effective security rules, New support request), and Help + support.

In “Inbound security rules”,

Click “Add”.



The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various service icons. The main content area is titled "CCNAVM-Azure-nsg - Inbound security rules". On the right, there is a table listing three existing 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	...

A yellow box highlights the "Add" button located at the top right of the rule list. The URL in the browser address bar is: https://portal.azure.com/#@sivaramselvamoutlook.onmicrosoft.com/resource/subscriptions/d7698da3-78bc-41fc-8db6-5dfad72a9b72/resourceGroups/San...

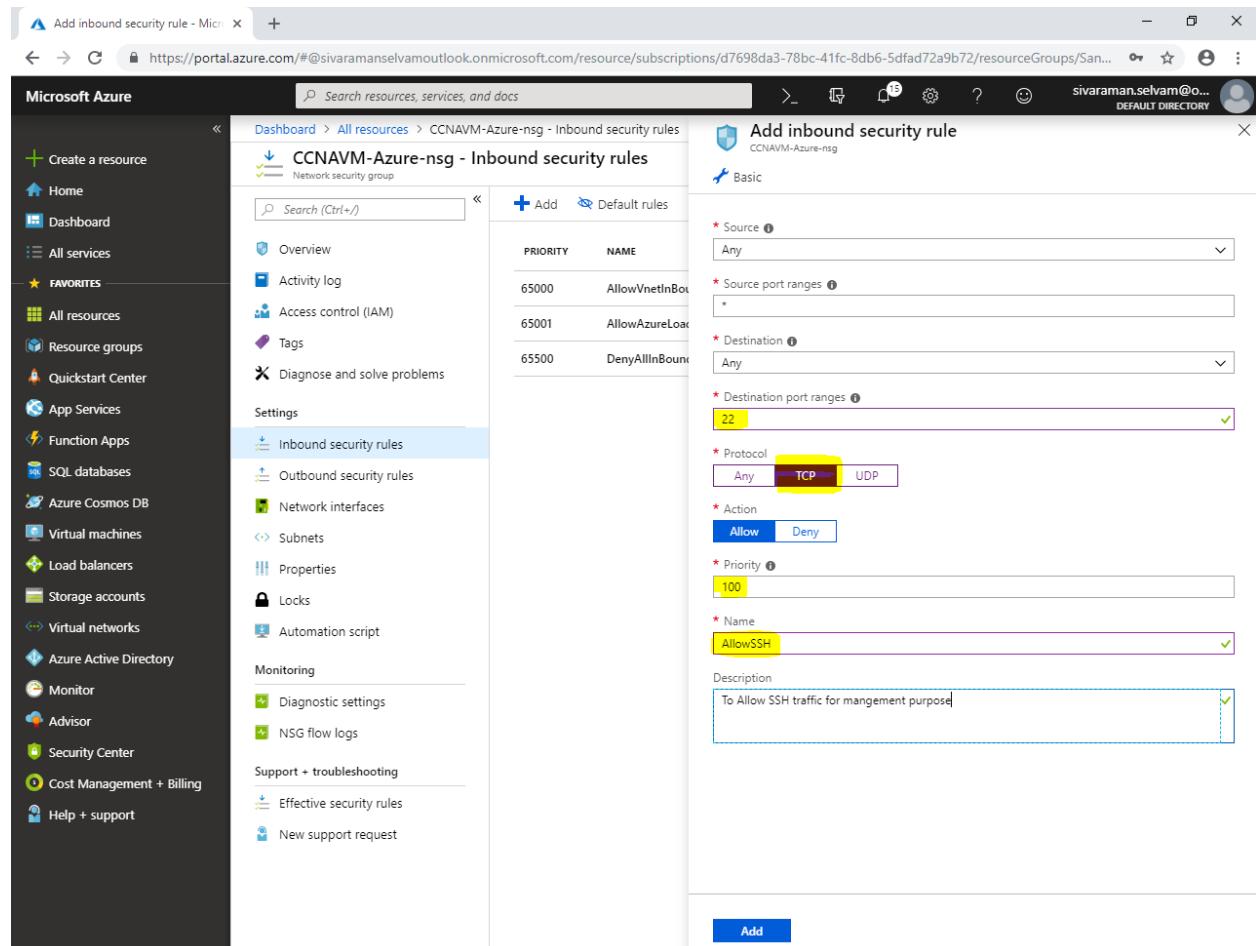
While “**Add inbound security rule**”,

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

In “**Protocol**” select “**TCP**”.

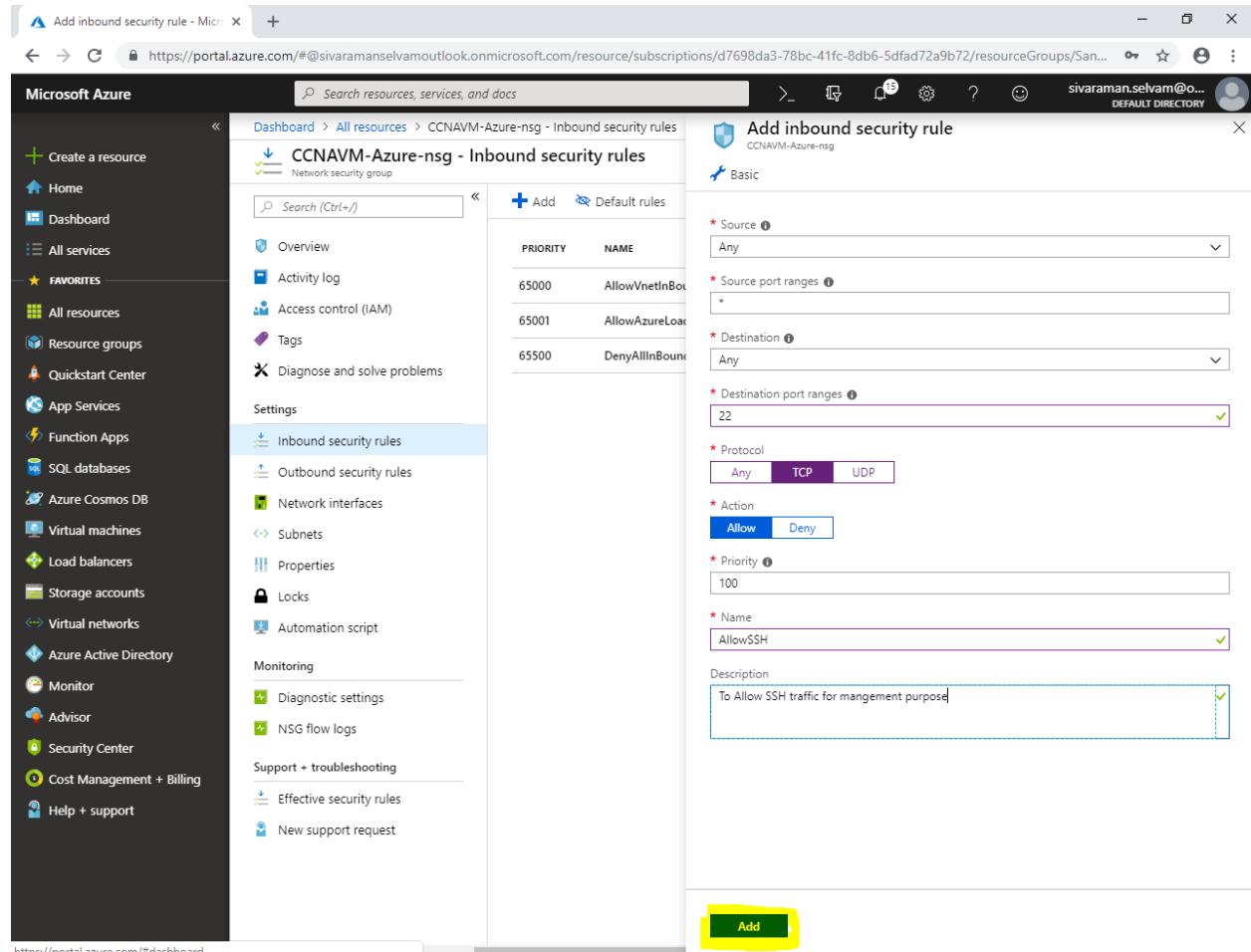
Set “**Priority**” as “**100**”.

Type “**Name**” as “**AllowSSH**”.



The screenshot shows the Azure portal interface for managing an NSG. On the left, the navigation menu includes options like Home, Dashboard, All services, and Favorites. Under Favorites, 'All resources' is selected, showing a list of services including 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 'Inbound security rules' section for the 'CCNAVM-Azure-nsg' NSG. A table lists three existing rules: 'AllowVnetInBound' (Priority 65000), 'AllowAzureLoadBalancer' (Priority 65001), and 'DenyAllInBound' (Priority 65500). To the right, a 'Basic' configuration pane is open for adding a new rule. It includes fields for Source (Any), Source port ranges (22), Destination (Any), Destination port ranges (22), Protocol (TCP), Action (Allow), Priority (100), Name (AllowSSH), and a Description field containing 'To Allow SSH traffic for management purpose'. The 'Protocol' field has 'TCP' highlighted in yellow.

Click "Add".



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 'Inbound security rules' section for a specific Network Security Group (CCNAVM-Azure-nsg). A new rule is being added, as indicated by the 'Add' button at the top right of the dialog. The dialog form includes fields for priority, source, destination, protocol, action, name, and description.

PRIORITY	NAME
65000	AllowVnetInBound
65001	AllowAzureLoadBalancing
65500	DenyAllInBound

Add inbound security rule

Basic

* Source: Any

* Source port ranges: *

* Destination: Any

* Destination port ranges: 22

* Protocol: Any TCP UDP

* Action: Allow Deny

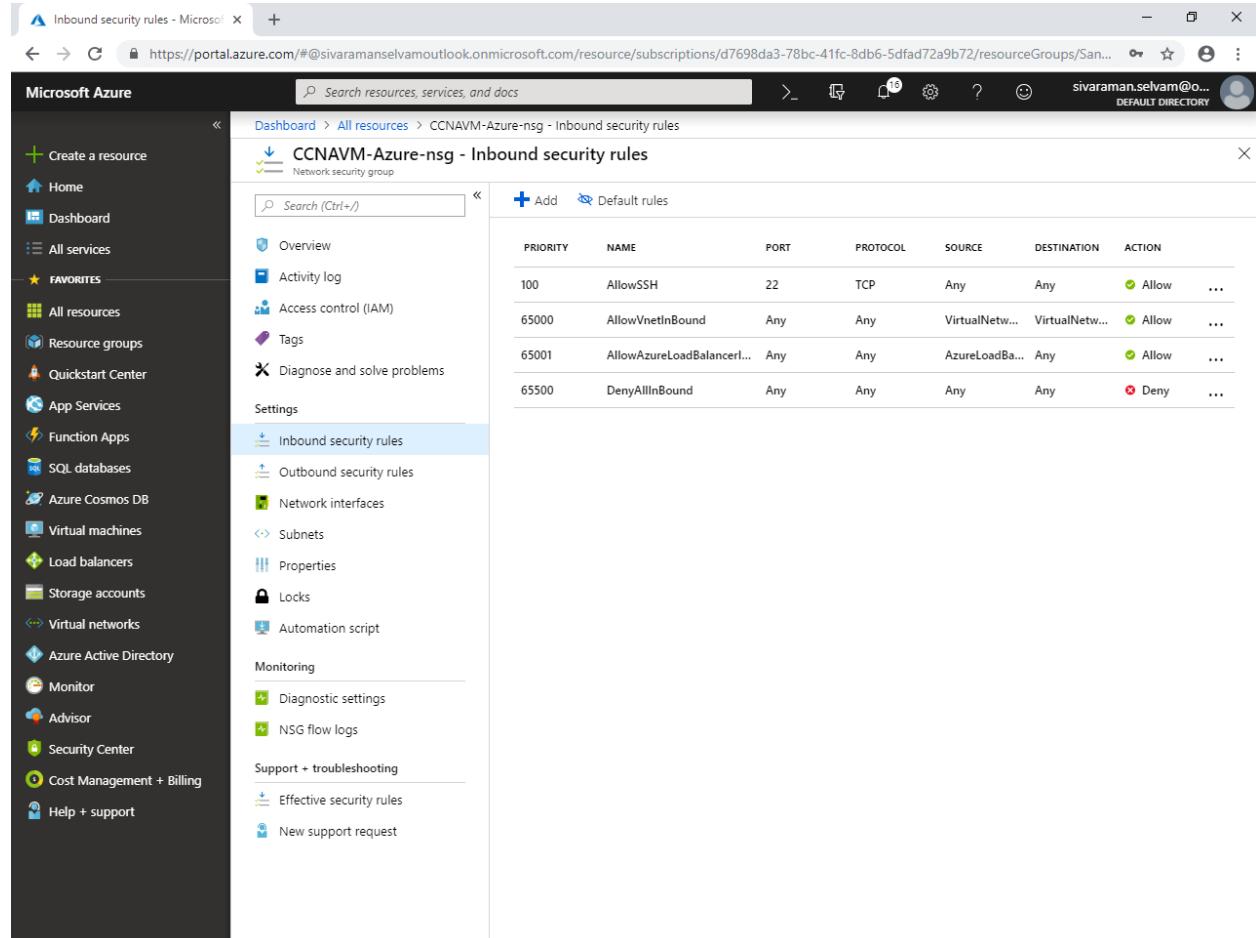
* Priority: 100

* Name: AllowSSH

Description: To Allow SSH traffic for management purpose

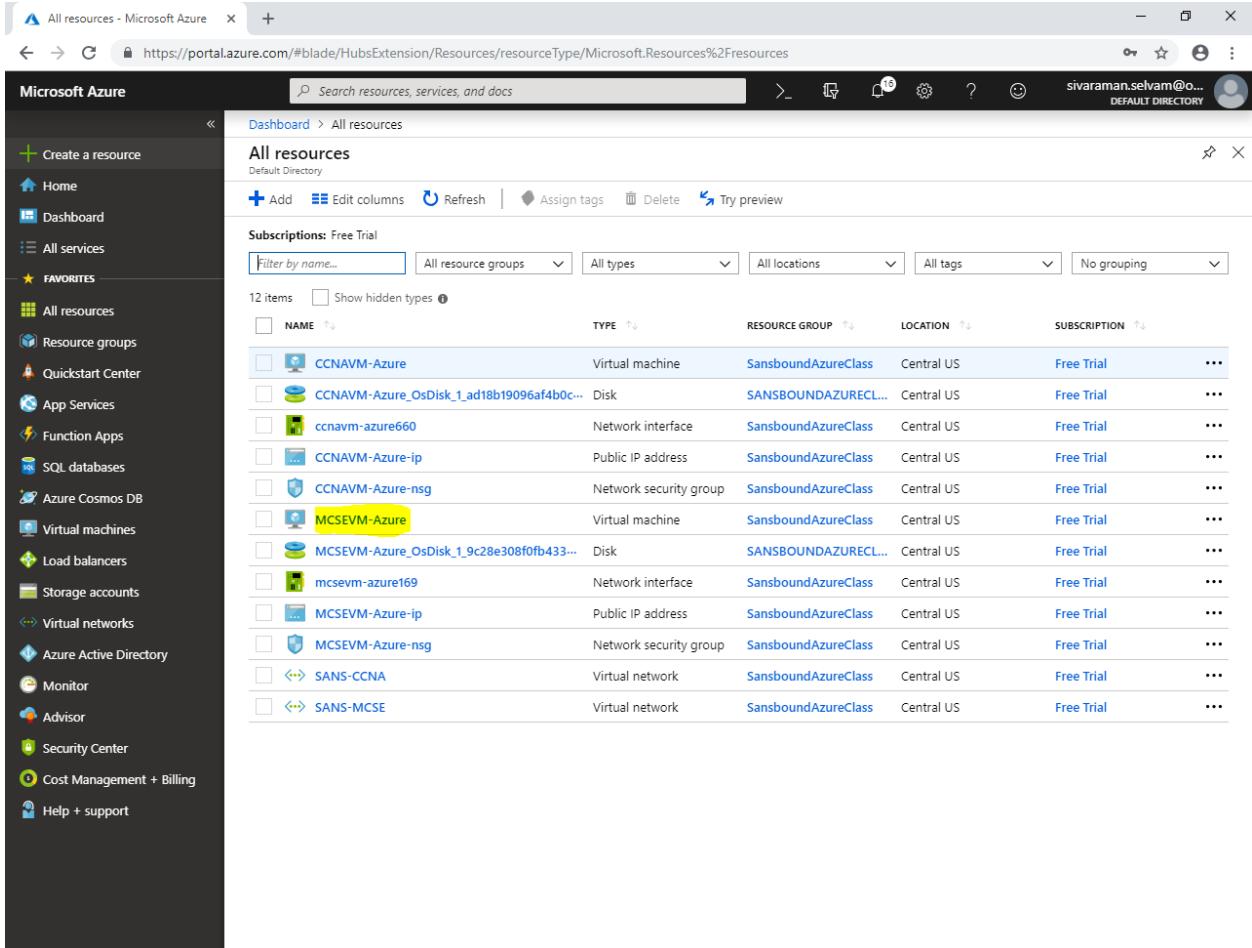
Add

You are able to see that inbound rule has been created for "**CCNAVM-Azure-nsg**" successfully.



PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	AllowSSH	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 Virtual machine named “**MCSEVM-Azure**” which belongs to “**SANS-MCSE**” Virtual network as well as “**SANS-MCSE-PubSubnet**”.

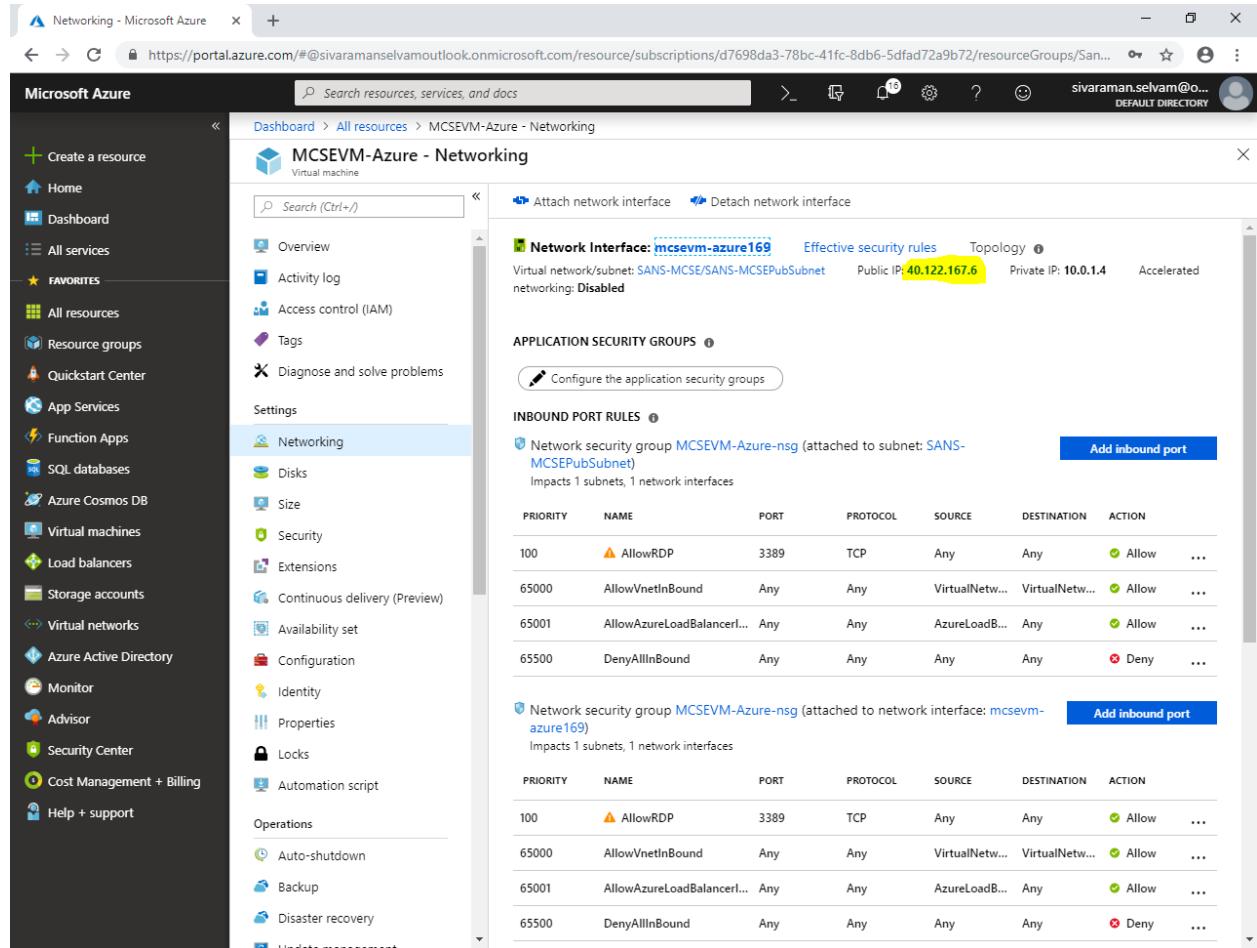


The screenshot shows the Microsoft Azure portal's "All resources" blade. The left sidebar contains a "FAVORITES" section with links to various Azure services. The main area displays a table of 12 resources. The columns are: NAME, TYPE, RESOURCE GROUP, LOCATION, and SUBSCRIPTION. The "NAME" column is sorted by name. The "MCSEVM-Azure" resource is highlighted with a yellow box. The table data is as follows:

NAME	TYPE	RESOURCE GROUP	LOCATION	SUBSCRIPTION
CCNAVM-Azure	Virtual machine	SansboundAzureClass	Central US	Free Trial
CCNAVM-Azure_OsDisk_1_ad18b19096af4b0c...	Disk	SANSBOUNDAZURECL...	Central US	Free Trial
cnnavm-azure660	Network interface	SansboundAzureClass	Central US	Free Trial
CCNAVM-Azure-ip	Public IP address	SansboundAzureClass	Central US	Free Trial
CCNAVM-Azure-nsg	Network security group	SansboundAzureClass	Central US	Free Trial
MCSEVM-Azure	Virtual machine	SansboundAzureClass	Central US	Free Trial
MCSEVM-Azure_OsDisk_1_9c28e308f0fb433...	Disk	SANSBOUNDAZURECL...	Central US	Free Trial
mcsevm-azure169	Network interface	SansboundAzureClass	Central US	Free Trial
MCSEVM-Azure-ip	Public IP address	SansboundAzureClass	Central US	Free Trial
MCSEVM-Azure-nsg	Network security group	SansboundAzureClass	Central US	Free Trial
SANS-CCNA	Virtual network	SansboundAzureClass	Central US	Free Trial
SANS-MCSE	Virtual network	SansboundAzureClass	Central US	Free Trial

In “MCSEVM-Azure”Click on “**Networking**”,

Kindly note the Public and Private IP address of the Virtual machine.



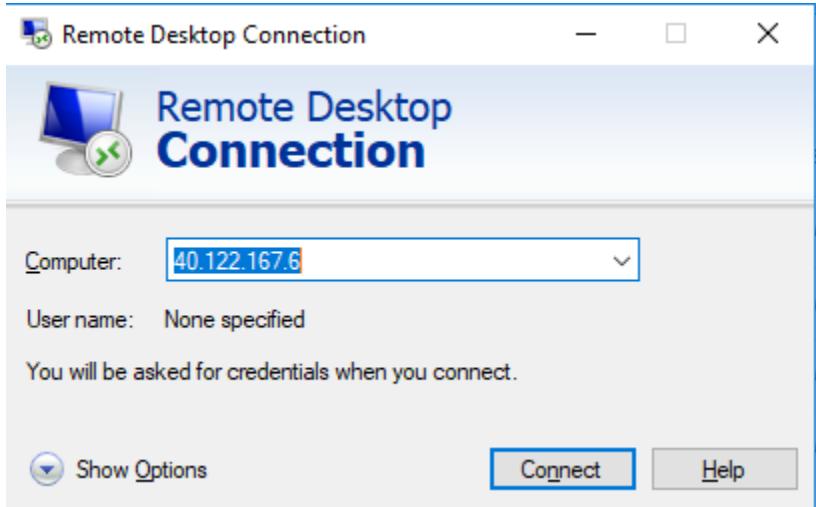
The screenshot shows the Microsoft Azure portal interface for managing the networking of a virtual machine named "MCSEVM-Azure". The left sidebar lists various services like Home, Dashboard, All Services, and Favorites. The main content area shows the "Networking" tab selected under the "Settings" section. Key details visible include:

- Network Interface:** mcsevm-azure169 (highlighted in yellow)
- Effective security rules:** Enabled
- Topology:** Accelerated
- Public IP:** 40.122.167.6 (highlighted in yellow)
- Private IP:** 10.0.1.4
- Networking:** Disabled
- APPLICATION SECURITY GROUPS:** Configure application security groups (button)
- INBOUND PORT RULES:** Two tables of rules:
 - Network security group MCSEVM-Azure-nsg (attached to subnet: SANS-MCSEPubSubnet):** Impacts 1 subnets, 1 network interfaces.

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	AzureLoadB...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
 - Network security group MCSEVM-Azure-nsg (attached to network interface: mcsevm-azure169):** Impacts 1 subnets, 1 network interfaces.

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	AzureLoadB...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

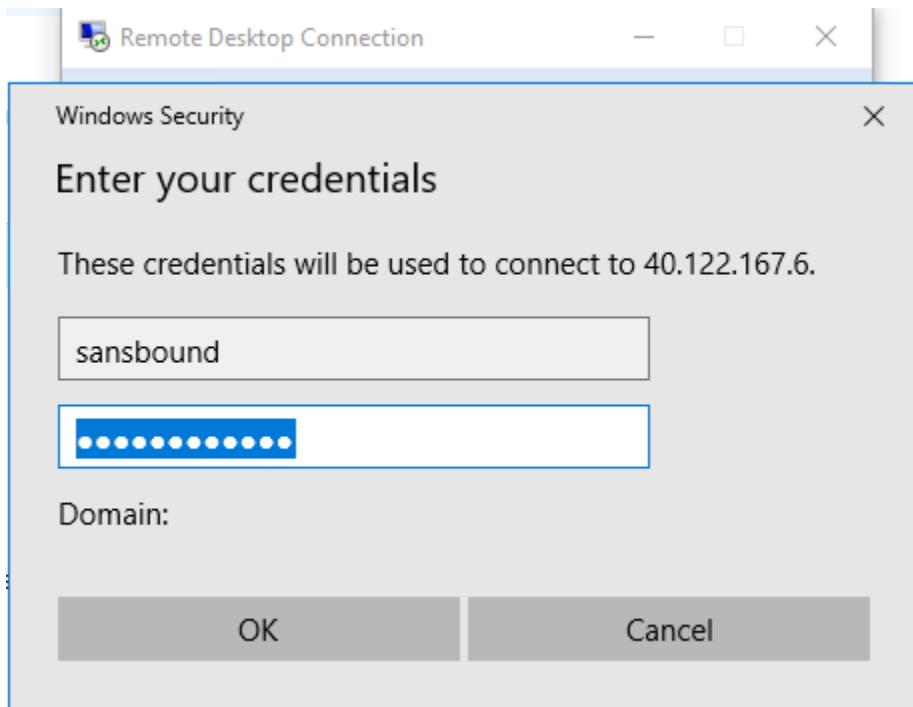
From your local machine, type “**mstsc**” in run box, and press “**Enter**”.



Click "**Connect**".

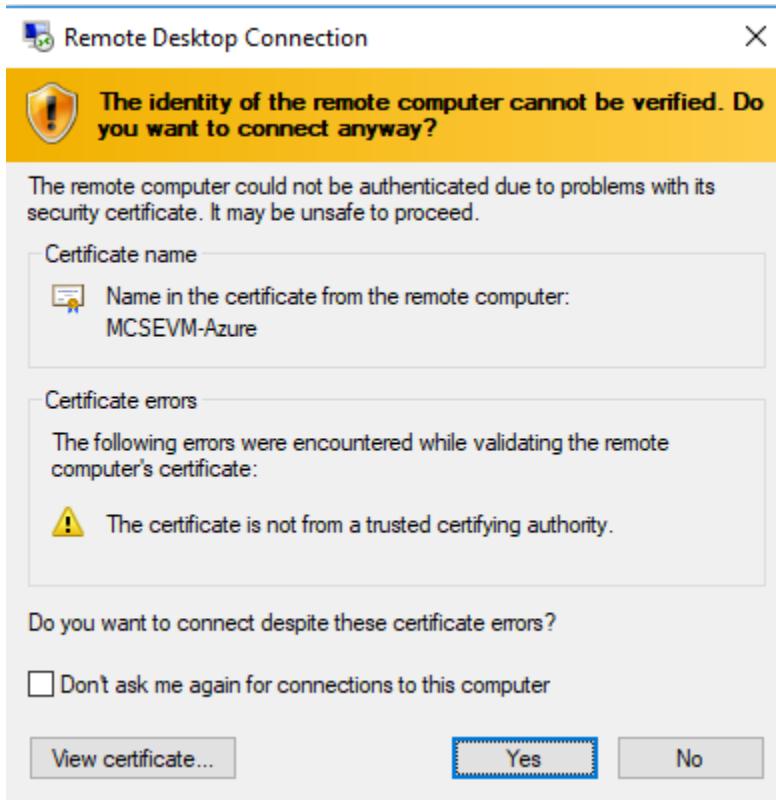
Type username as sansbound

Type password for the Windows 2008 R2 server.

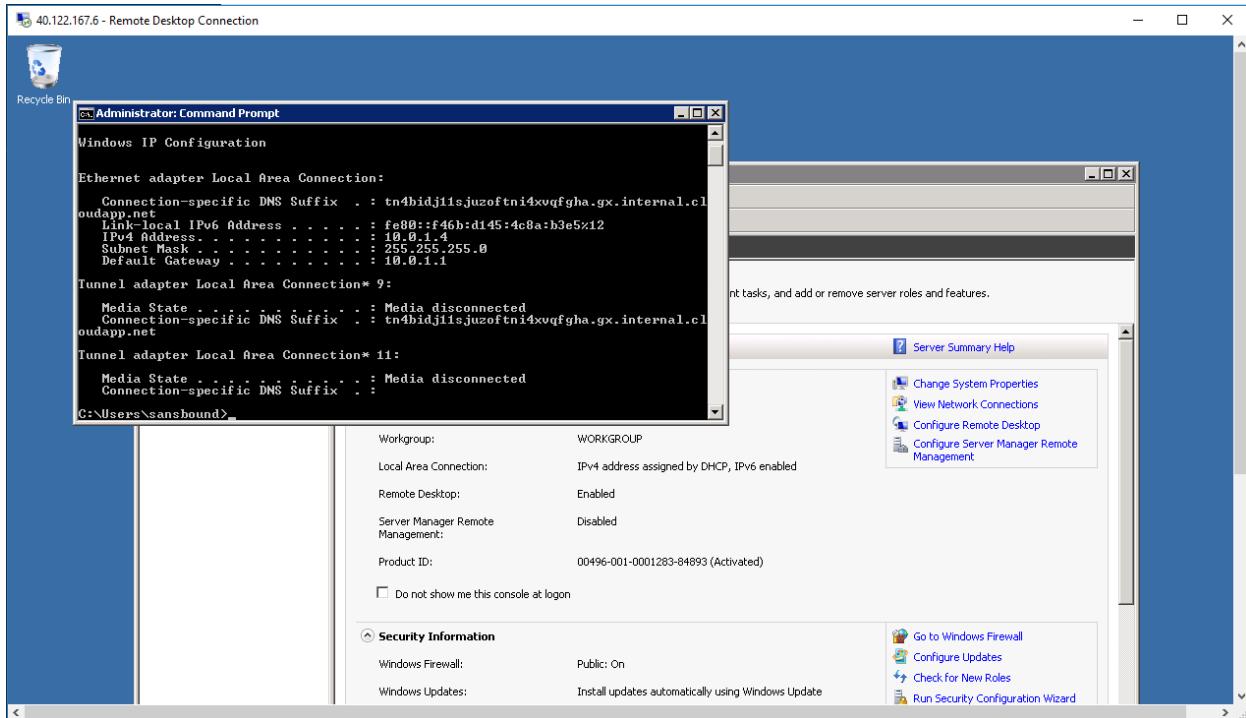


Click "Ok".

Click "Yes".

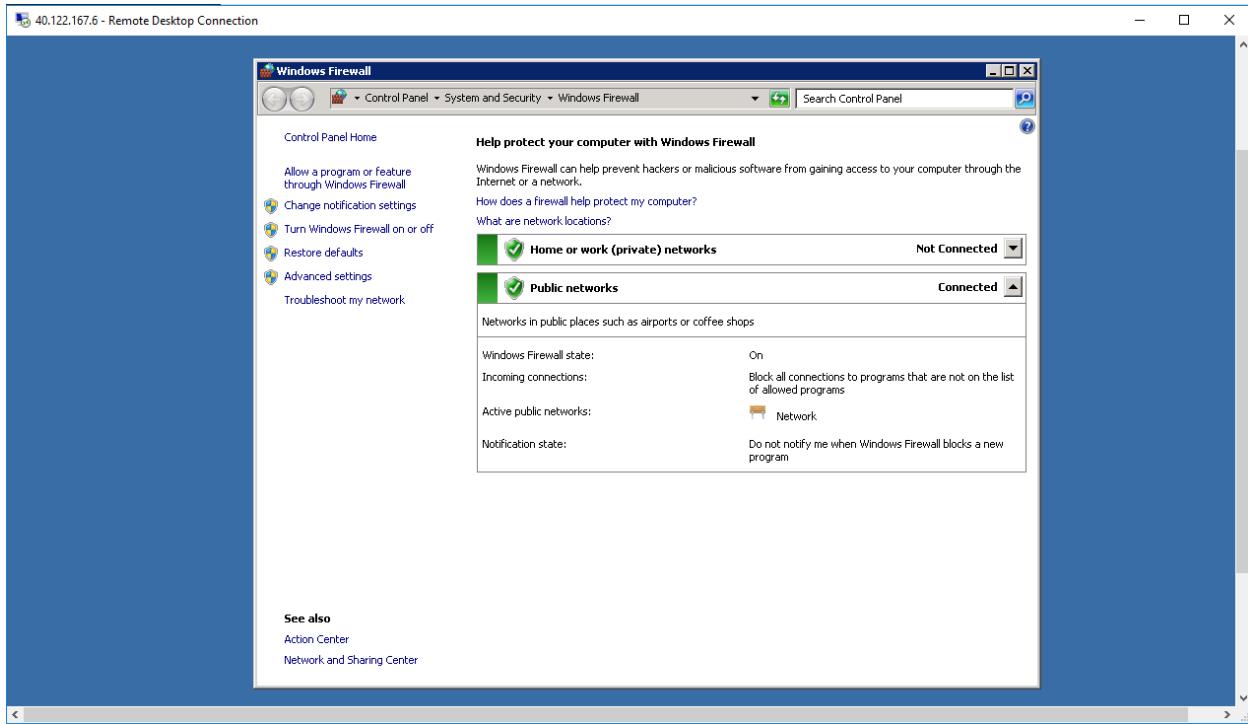


You have successfully logged into the “Windows 2008 R2 Server”.

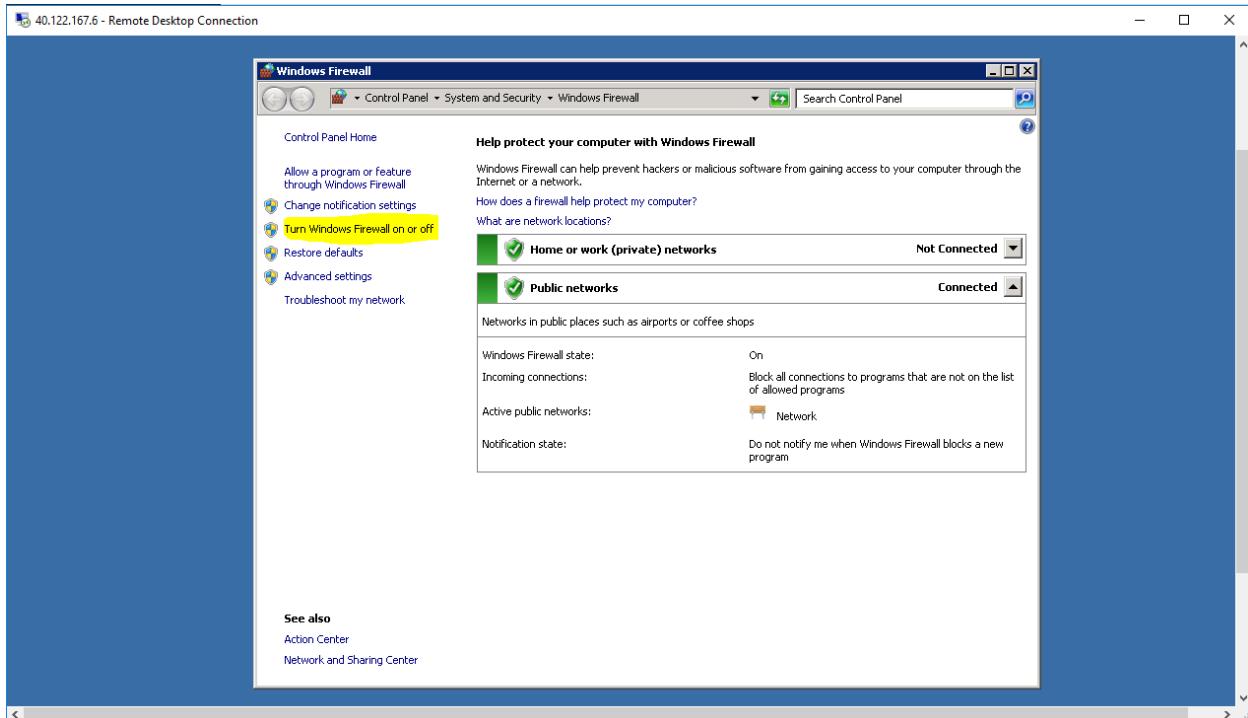


In “Windows 2008 R2 server”,

Type “firewall.cpl” in Run box and press “Enter”.

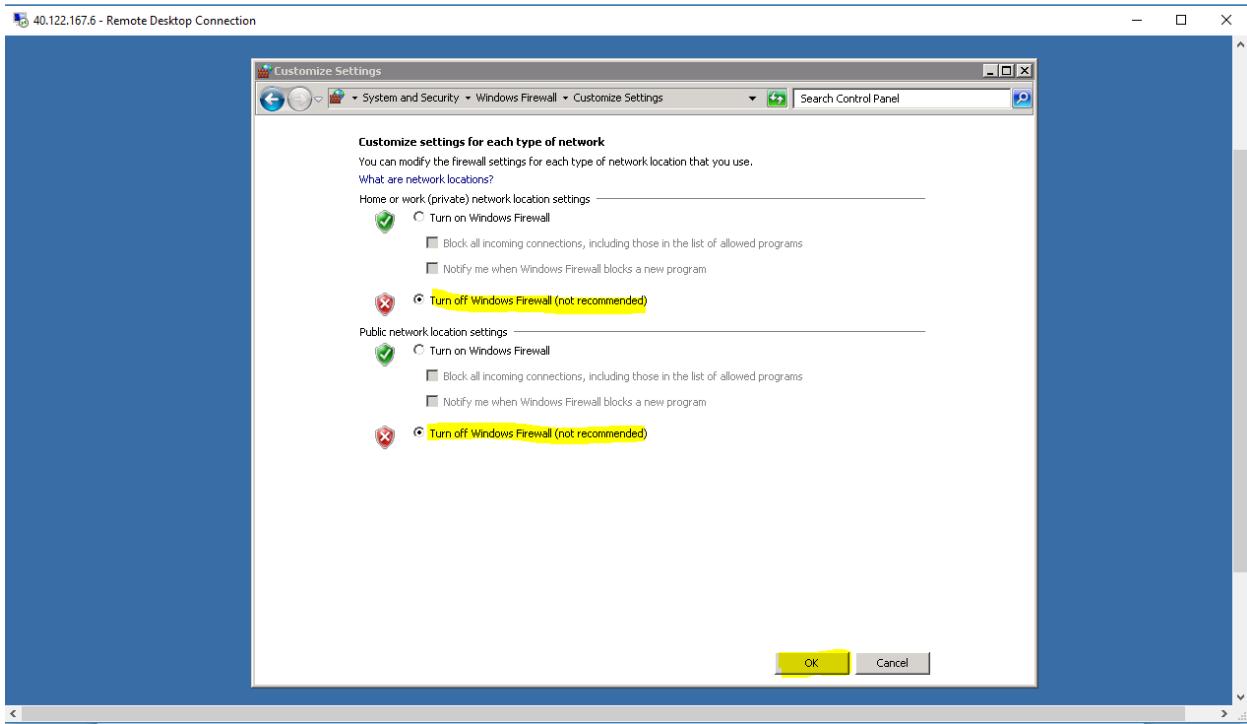


Click “Turn Windows Firewall on or off”.



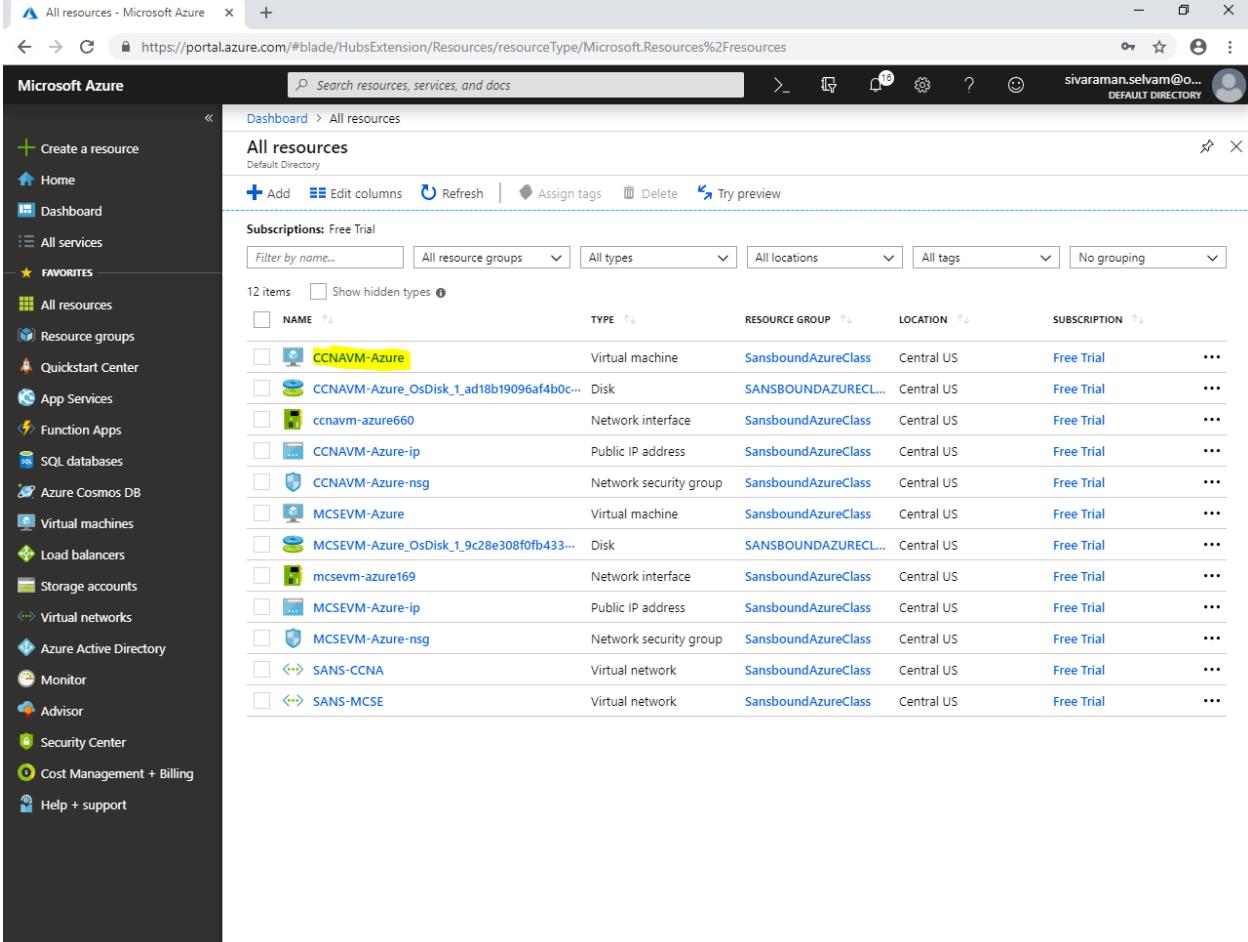
Click “**Turn off**” on both.

Click “Ok”.



In “All resources”.

Click virtual machine named “**CCNAVM-Azure**”.



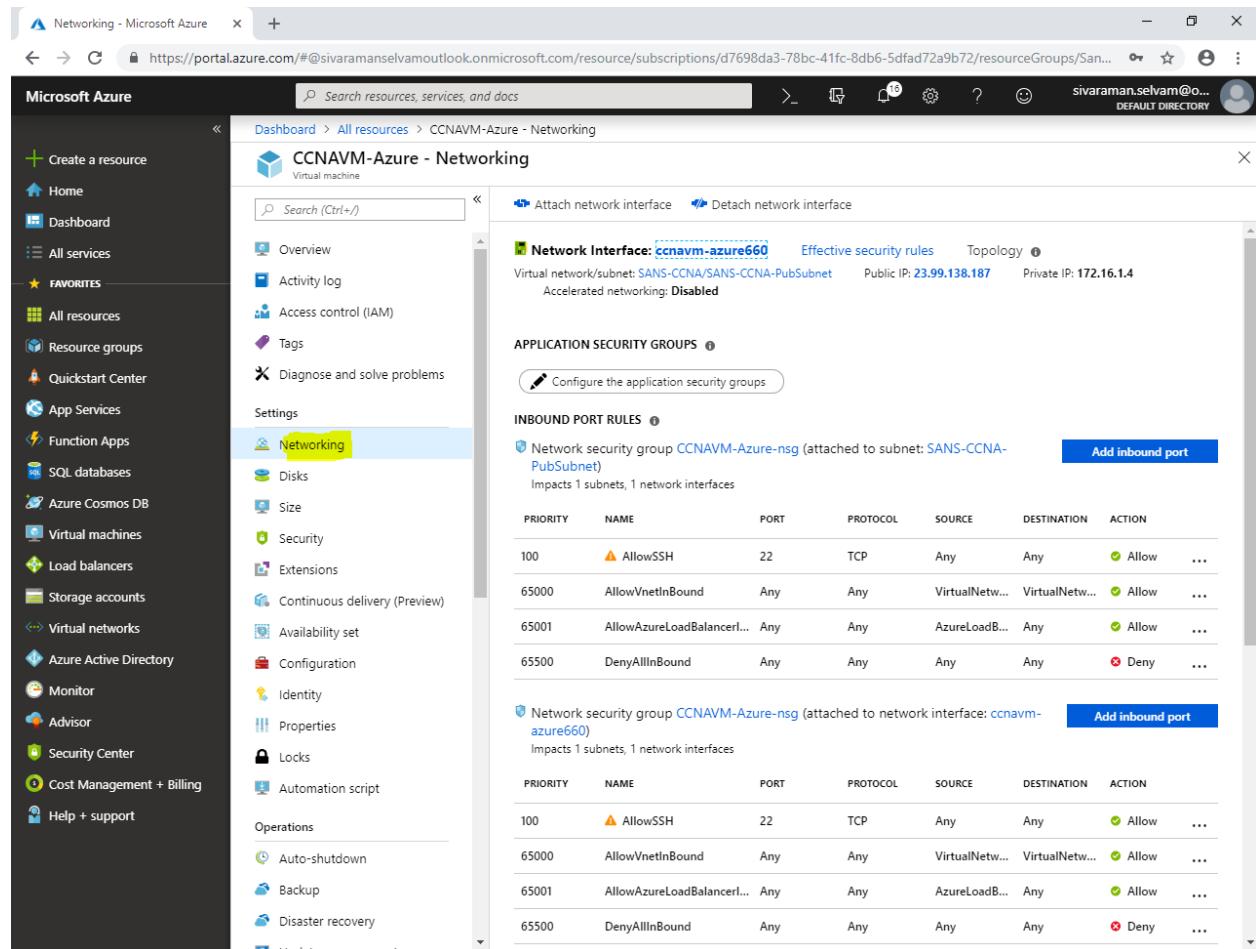
The screenshot shows the Microsoft Azure portal interface. The left sidebar is filled with various service icons under categories like Favorites, All services, and Monitoring. The main content area is titled "All resources" and displays a list of 12 items. The columns are labeled NAME, TYPE, RESOURCE GROUP, LOCATION, and SUBSCRIPTION. The first item, "CCNAVM-Azure", is highlighted with a yellow background and has a yellow border around its icon. Other items listed include "CCNAVM-Azure_OsDisk_1_ad18b19096af4b0c...", "cnnavm-azure660", "CCNAVM-Azure-ip", "CCNAVM-Azure-nsg", "MCSEVM-Azure", "MCSEVM-Azure_OsDisk_1_9c28e308f0fb433...", "mcsevm-azure169", "MCSEVM-Azure-ip", "MCSEVM-Azure-nsg", "SANS-CCNA", and "SANS-MCSE".

NAME	TYPE	RESOURCE GROUP	LOCATION	SUBSCRIPTION
CCNAVM-Azure	Virtual machine	SansboundAzureClass	Central US	Free Trial
CCNAVM-Azure_OsDisk_1_ad18b19096af4b0c...	Disk	SANSBOUNDAZURECL...	Central US	Free Trial
cnnavm-azure660	Network interface	SansboundAzureClass	Central US	Free Trial
CCNAVM-Azure-ip	Public IP address	SansboundAzureClass	Central US	Free Trial
CCNAVM-Azure-nsg	Network security group	SansboundAzureClass	Central US	Free Trial
MCSEVM-Azure	Virtual machine	SansboundAzureClass	Central US	Free Trial
MCSEVM-Azure_OsDisk_1_9c28e308f0fb433...	Disk	SANSBOUNDAZURECL...	Central US	Free Trial
mcsevm-azure169	Network interface	SansboundAzureClass	Central US	Free Trial
MCSEVM-Azure-ip	Public IP address	SansboundAzureClass	Central US	Free Trial
MCSEVM-Azure-nsg	Network security group	SansboundAzureClass	Central US	Free Trial
SANS-CCNA	Virtual network	SansboundAzureClass	Central US	Free Trial
SANS-MCSE	Virtual network	SansboundAzureClass	Central US	Free Trial

In virtual machine named "**CCNAVM-Azure**",

Click "**Networking**".

Kindly note the Public and Private IP address of the Virtual machine of Ubuntu.



The screenshot shows the Microsoft Azure portal interface. The left sidebar is the navigation menu, and the main content area is titled "CCNAVM-Azure - Networking". The "Networking" tab is selected in the left sidebar. The main pane displays the network interface configuration for the virtual machine, showing the public IP (23.99.138.187) and private IP (172.16.1.4). It also lists application security groups and inbound port rules for two Network Security Groups (NSGs): "CCNAVM-Azure-nsg" and "CCNAVM-Azure-nsg".

Network Interface: ccnavm-azure660
Virtual network/subnet: SANS-CCNA/SANS-CCNA-PubSubnet
Public IP: 23.99.138.187
Private IP: 172.16.1.4
Accelerated networking: Disabled

APPLICATION SECURITY GROUPS

INBOUND PORT RULES

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	AllowSSH	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetw...	VirtualNetw...	Allow
65001	AllowAzureLoadBalancer...	Any	Any	AzureLoadB...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Network security group CCNAVM-Azure-nsg (attached to subnet: SANS-CCNA-PubSubnet)
Impacts 1 subnets, 1 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	AllowSSH	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetw...	VirtualNetw...	Allow
65001	AllowAzureLoadBalancer...	Any	Any	AzureLoadB...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Network security group CCNAVM-Azure-nsg (attached to network interface: ccnavm-azure660)
Impacts 1 subnets, 1 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	AllowSSH	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetw...	VirtualNetw...	Allow
65001	AllowAzureLoadBalancer...	Any	Any	AzureLoadB...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

In “Windows server 2008 R2” machine,

Try to ping IP address of the Ubuntu (172.16.1.4)

But, we have got **request timed out**.

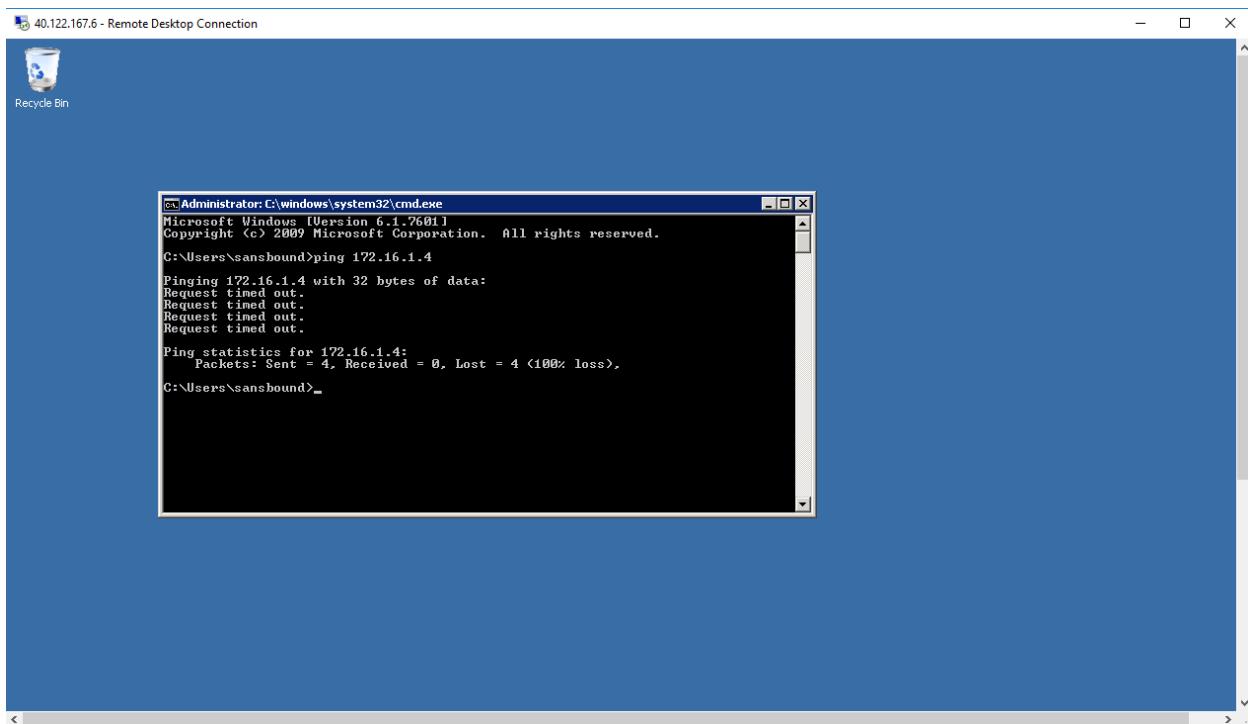
What is the reason?

Windows 2008 R2 server is belongs to “**SANS-MCSEPubSubnet**” of “**SANS-MCSE**” virtual network.

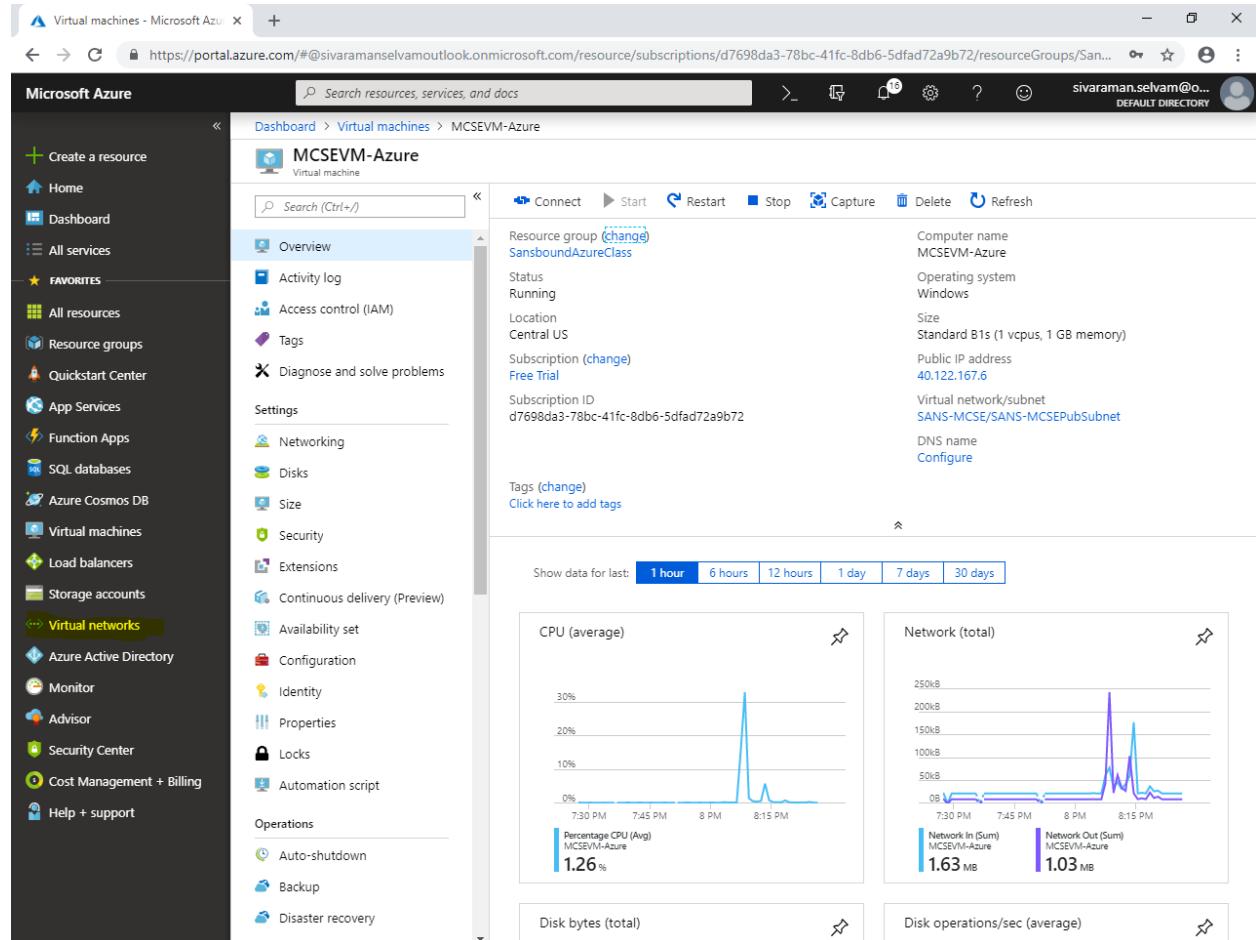
But Ubuntu machine which you are trying to connect is belongs to “**SANS-CCNA-PubSubnet**” of “**SANS-CCNA**” virtual network.

That is the reason, two different virtual networks are will not communicate with each other by default.

So that, we have required to configure Vnet peering on both Virtual networks.

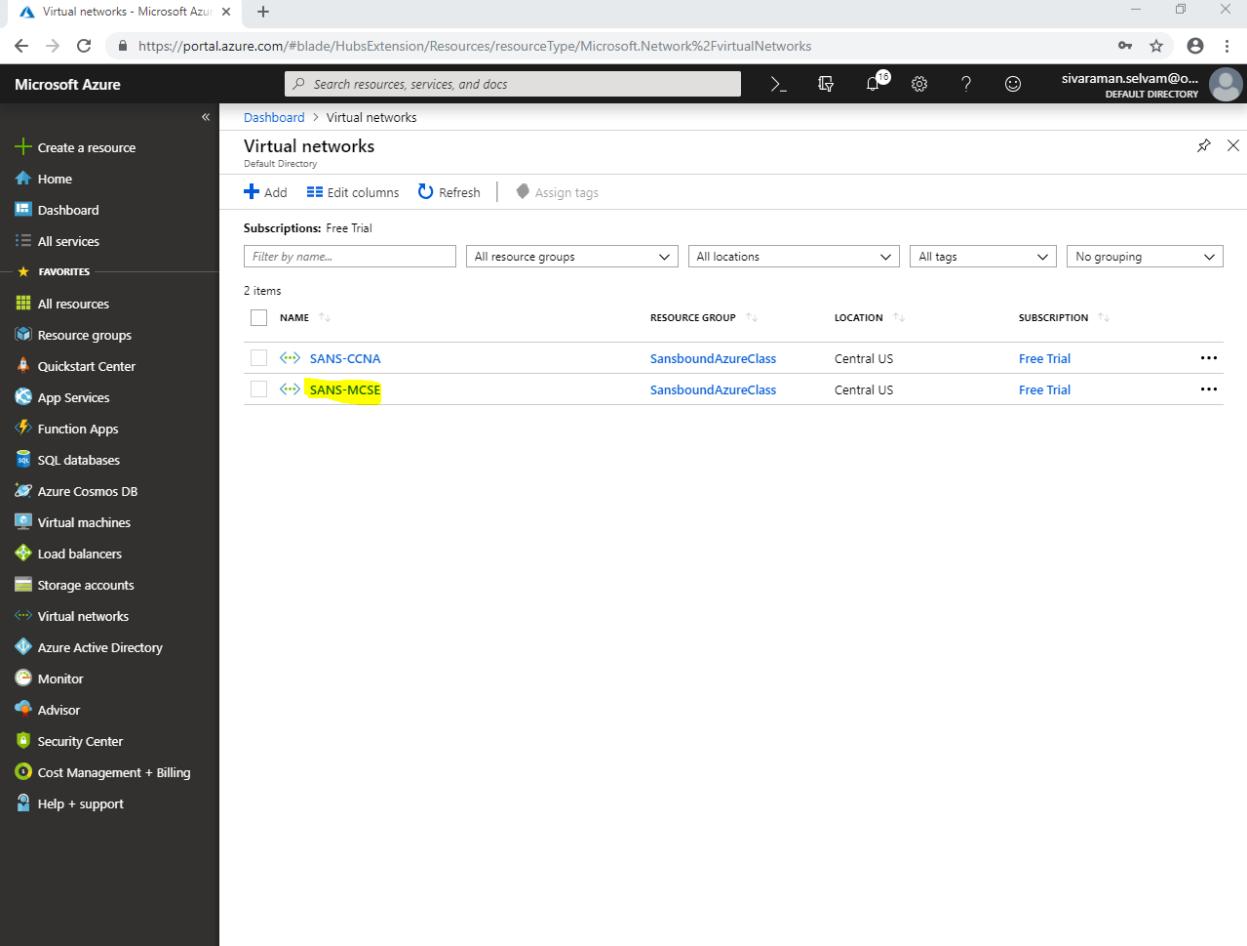


Click “Virtual networks” in left side panel.



The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation bar is visible, with the 'Virtual networks' option highlighted under the 'Compute' category. The main content area displays the details for a virtual machine named 'MCSEVM-Azure'. The 'Overview' tab is selected, showing basic information like the resource group ('SansboundAzureClass'), status ('Running'), location ('Central US'), and subscription ('Free Trial'). The 'Networking' section is expanded, showing the public IP address (40.122.167.6) and the virtual network/subnet (SANS-MCSE/SANS-MCSEPubSubnet). Below this, there are four performance charts: CPU (average), Network (total), Disk bytes (total), and Disk operations/sec (average). The CPU chart shows a spike of 1.26% around 8 PM. The Network chart shows Network In (Sum) at 1.63 MB and Network Out (Sum) at 1.03 MB, both with significant spikes around 8 PM.

Click “**SANS-MCSE**” virtual network.



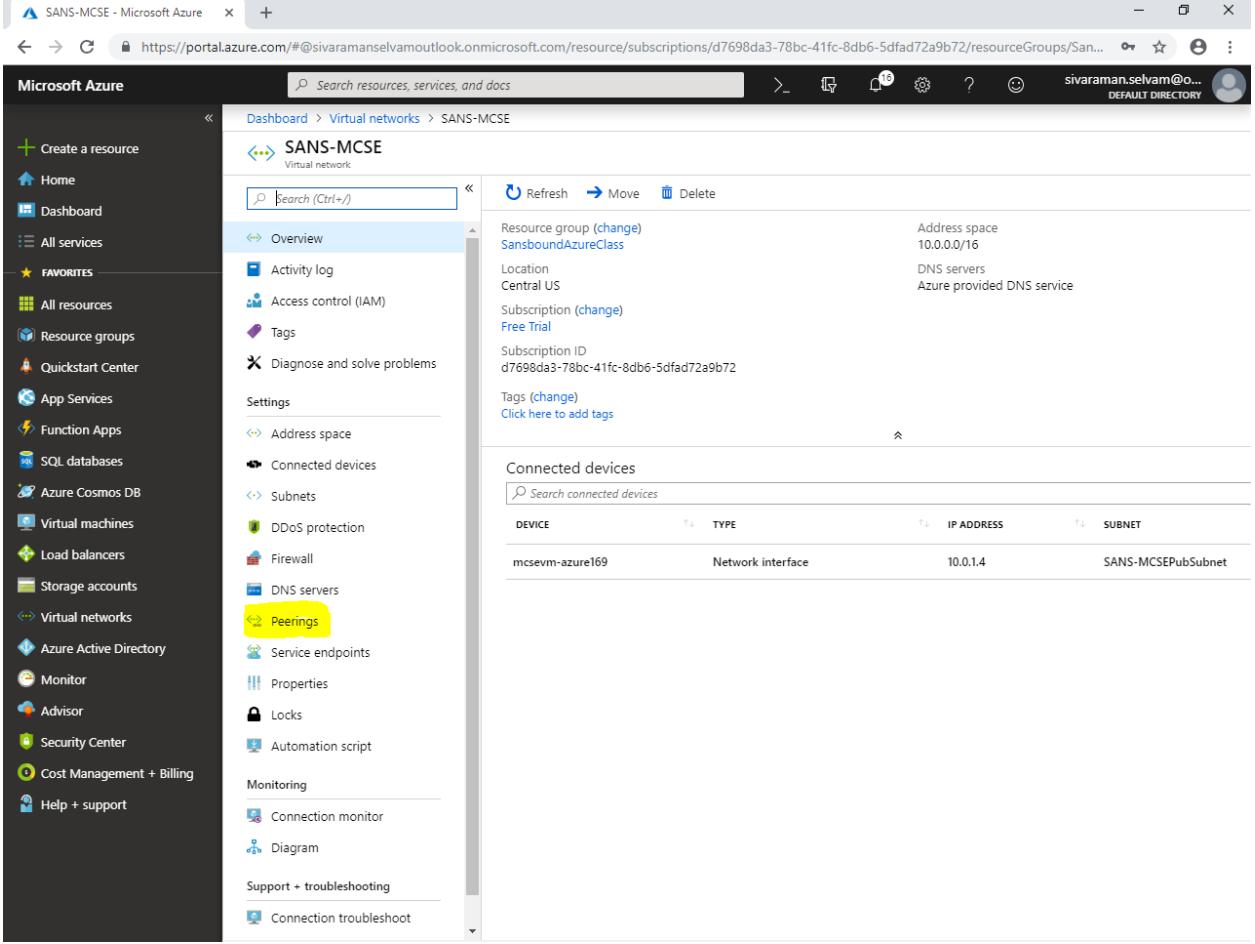
The screenshot shows the Microsoft Azure portal interface. The left sidebar is the navigation menu, and the main area is the "Virtual networks" blade under the "Virtual networks" section of the navigation bar. The blade displays a table of virtual networks with the following data:

NAME	RESOURCE GROUP	LOCATION	SUBSCRIPTION
SANS-CCNA	SansboundAzureClass	Central US	Free Trial
SANS-MCSE	SansboundAzureClass	Central US	Free Trial

The row for "SANS-MCSE" is highlighted with a yellow box. The URL in the browser address bar is <https://portal.azure.com/#blade/HubsExtension/Resources/resourceType/Microsoft.Network%2FVirtualNetworks>.

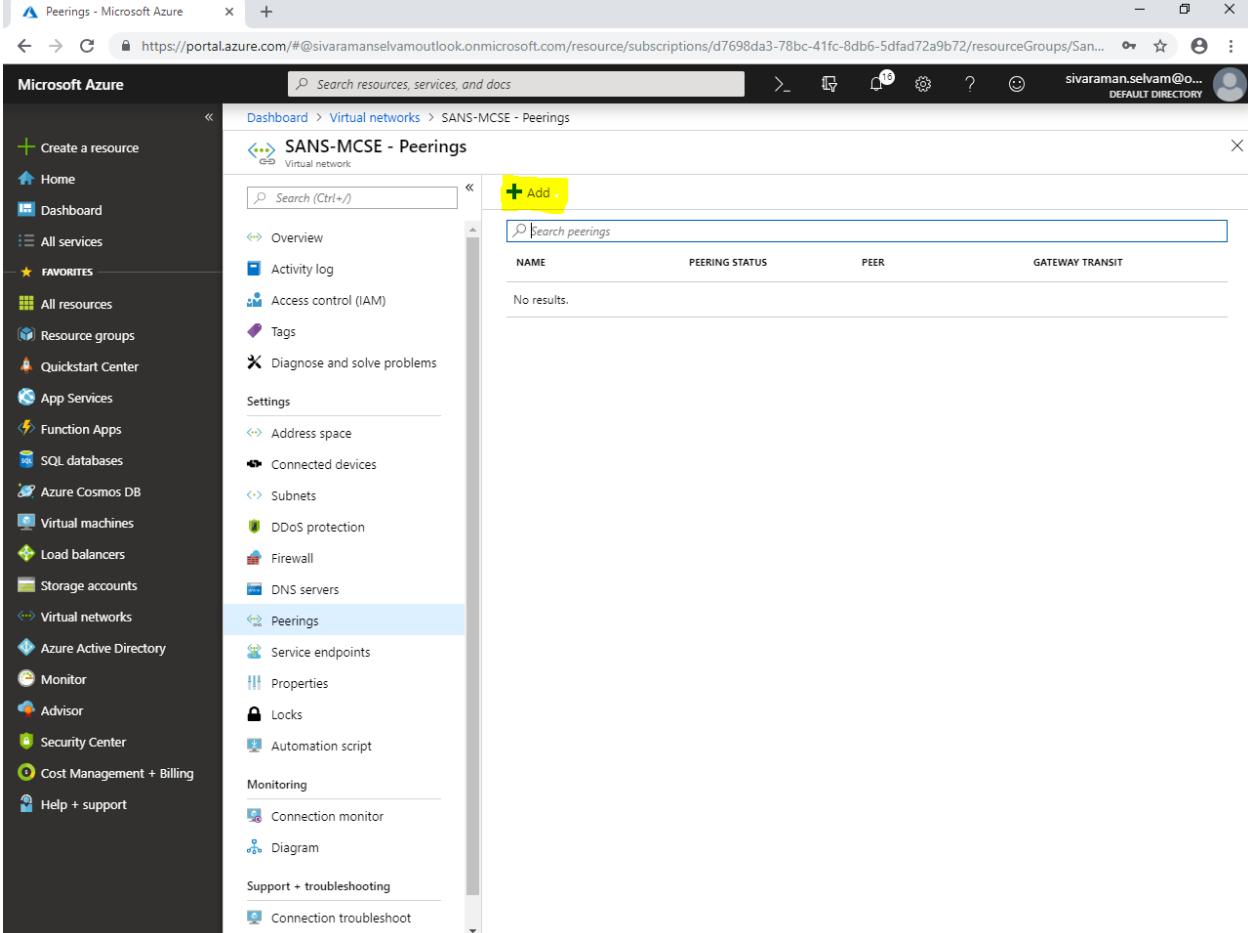
In “SANS-MCSE” virtual network,

Click on “Peerings”.



The screenshot shows the Microsoft Azure portal interface. The left sidebar is the navigation menu, and the main content area is the 'Virtual networks' blade for the 'SANS-MCSE' resource group. The 'Peerings' option in the 'Peering' section of the sidebar is highlighted with a yellow box. The main pane displays the 'Overview' of the virtual network, including details like Resource group, Address space (10.0.0.0/16), Location (Central US), Subscription (Free Trial), and a list of connected devices. One device, 'mcsevm-azure169', is listed as a Network interface with IP address 10.0.1.4 and subnet SANS-MCSEPubSubnet.

Click "Add".



The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various service icons and links. The main content area is titled 'SANS-MCSE - Peerings' under 'Virtual networks'. A search bar at the top right says 'Search resources, services, and docs'. Below it, a large yellow box highlights the '+ Add' button. To the right of the button is a search bar with the placeholder 'Search peerings'. A table below the search bar has columns: NAME, PEERING STATUS, PEER, and GATEWAY TRANSIT. The table displays the message 'No results.'

While “Add peering”

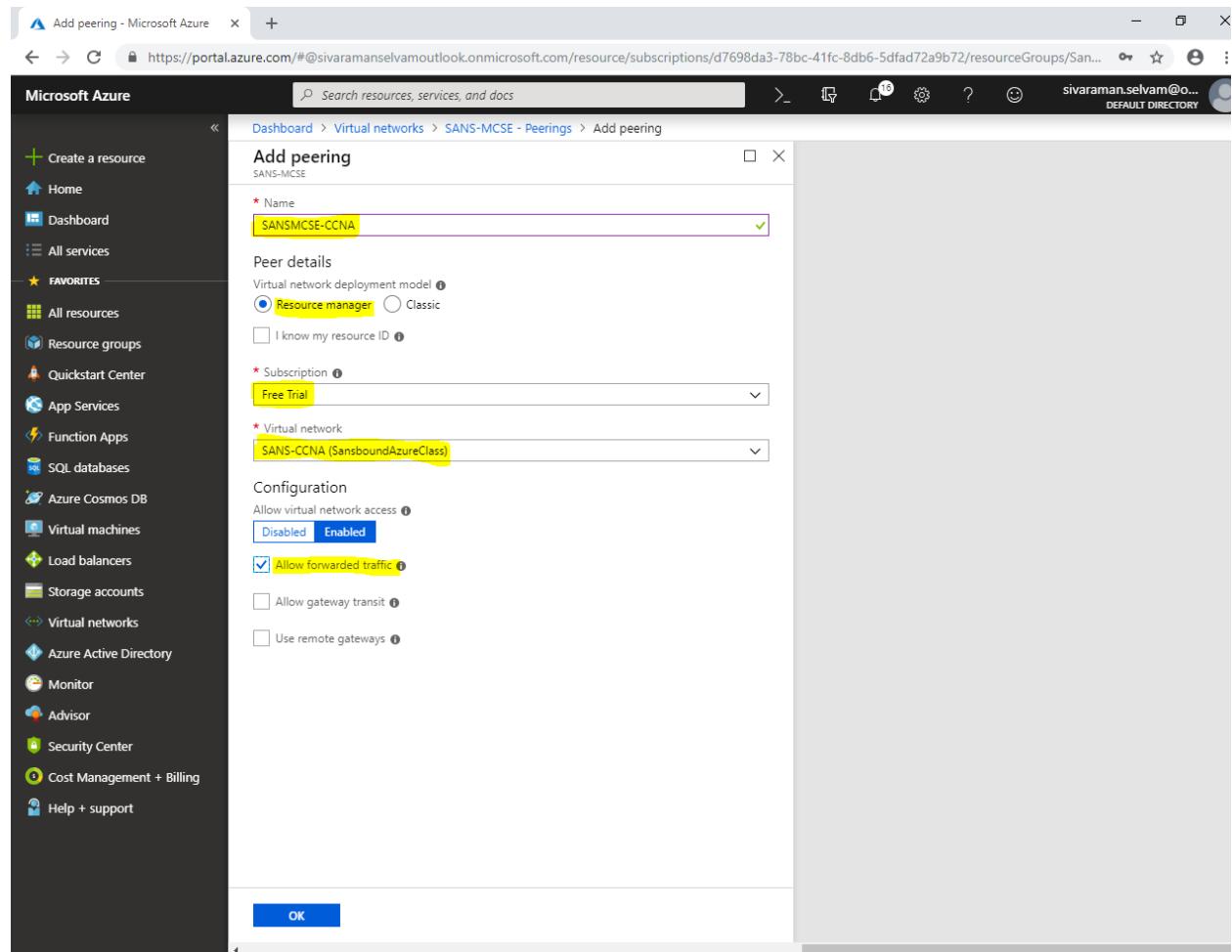
Type “Name” as “**SANSMCSE-CCNA**”.

In “Peer details” as “**Resource manager**”.

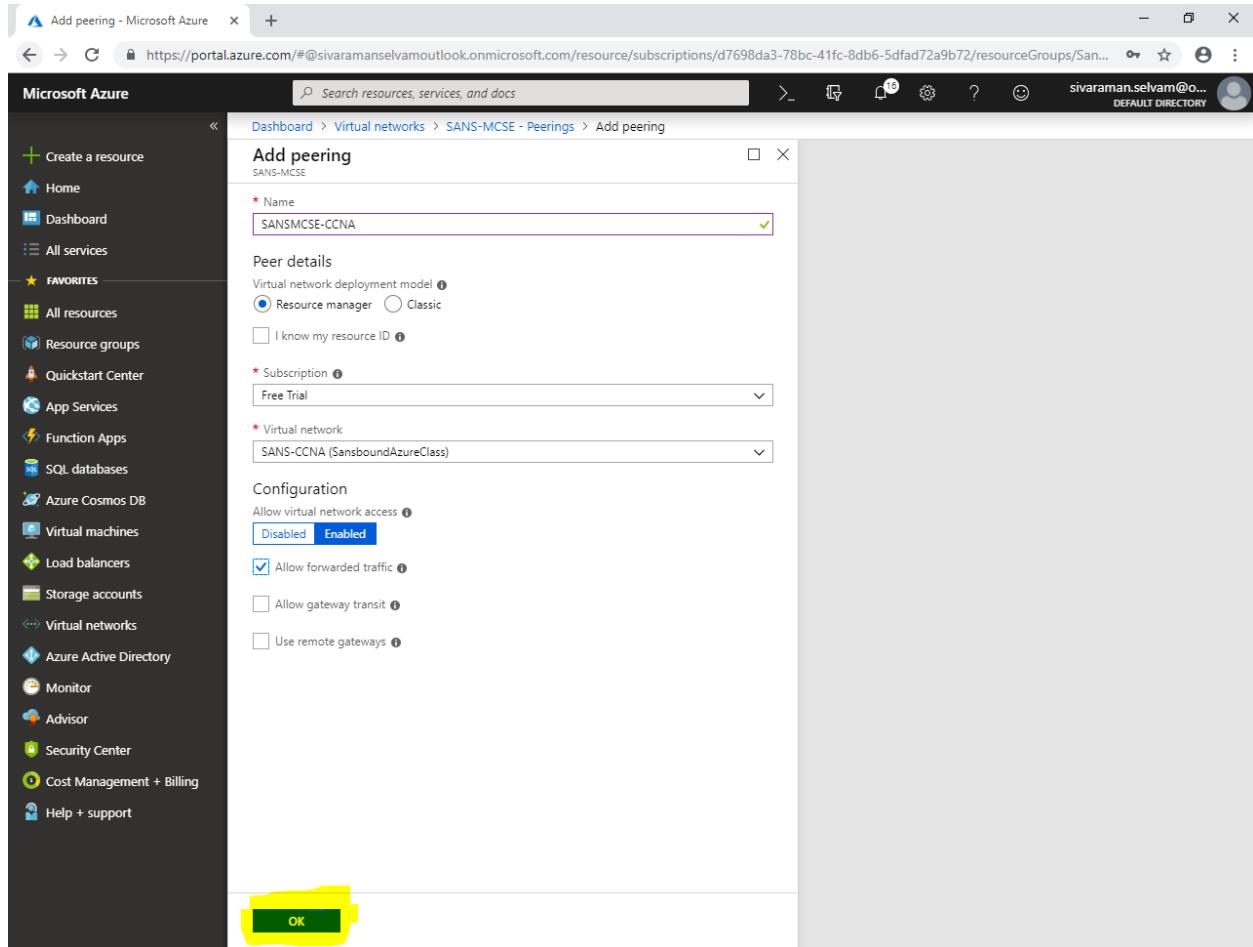
Select “**Subscription**” as “**Free Trial**”.

Select “**Virtual network**” of Remote Virtual network.

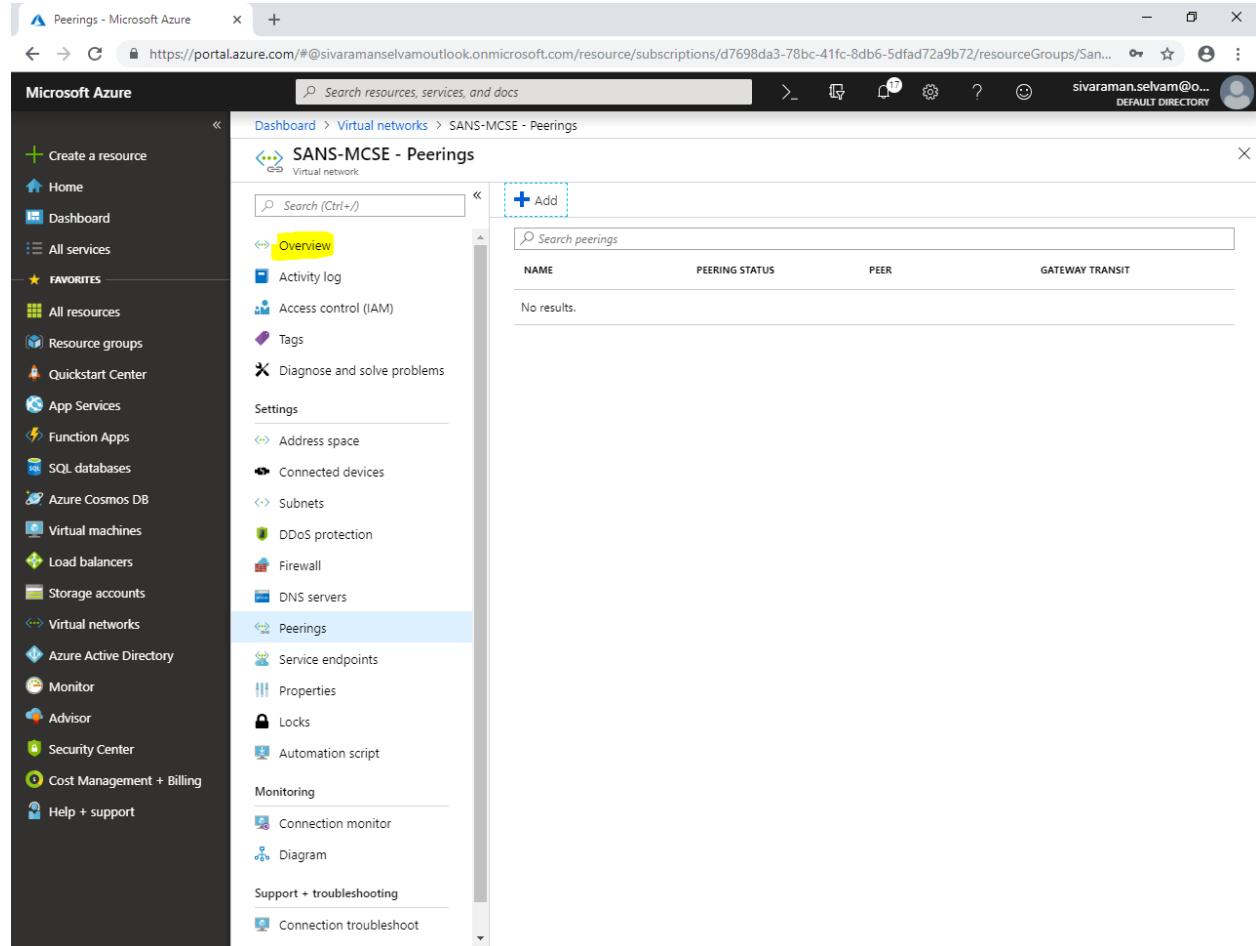
In “**Configuration**” need to check “**Allow forwarded traffic**”.



Click "Ok".

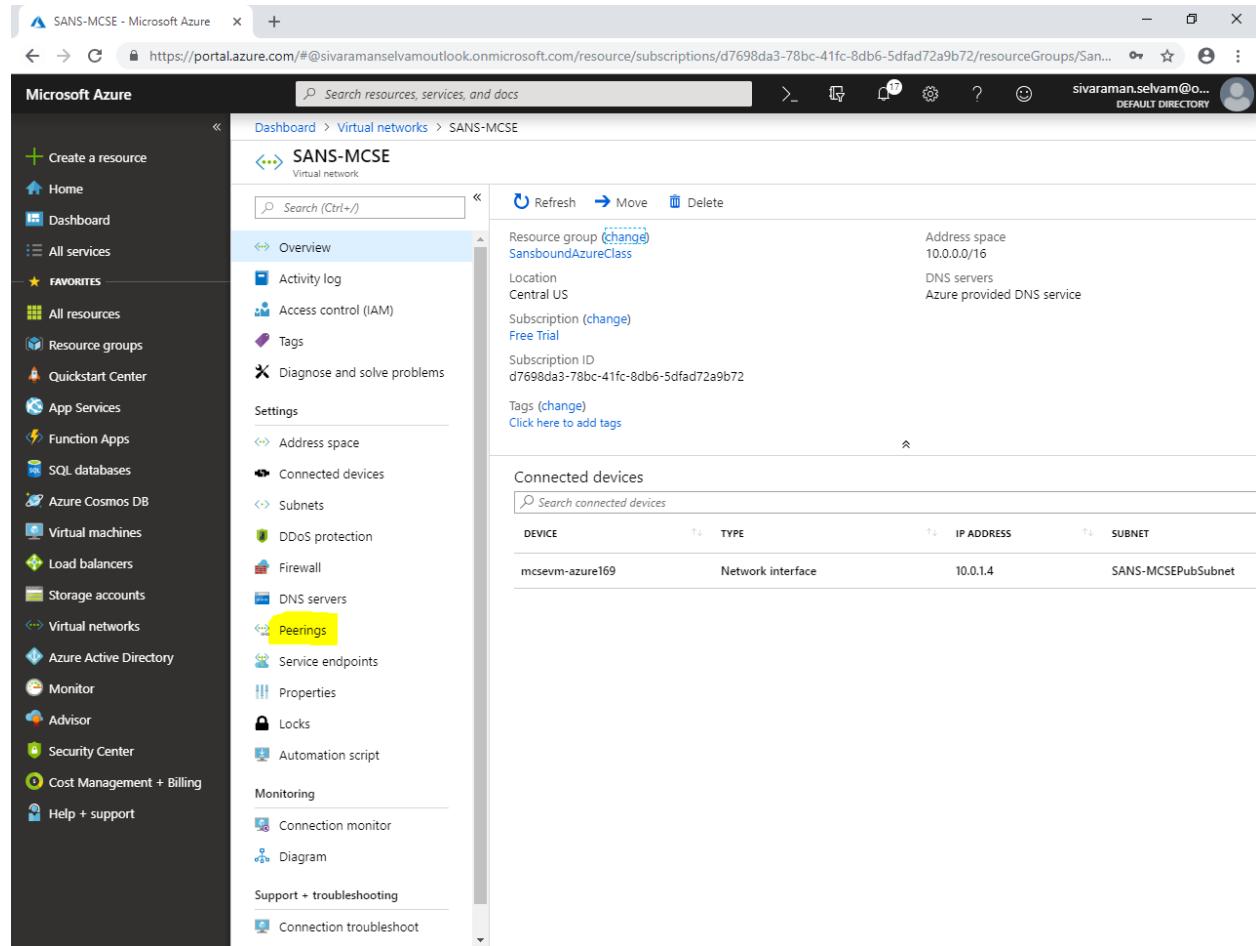


By default you are not able to view “**Peering**” details, click on any other option like “**Options**”.



The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, Favorites, and many others. Under the 'Virtual networks' section, the 'Peerings' option is highlighted with a yellow box. The main content area shows the 'SANS-MCSE - Peerings' page for a specific virtual network. It includes a search bar, a 'Add' button, and a table with columns: NAME, PEERING STATUS, PEER, and GATEWAY TRANSIT. A message at the top right says 'No results.'

Click "Peerings".



The screenshot shows the Microsoft Azure portal interface. The left sidebar is the navigation menu, and the main area is the 'Virtual networks' blade for the 'SANS-MCSE' resource group. The 'Peerings' link in the 'Settings' section is highlighted with a yellow box.

Microsoft Azure

SANS-MCSE - Microsoft Azure

https://portal.azure.com/#@sivaramselvamoutlook.onmicrosoft.com/resource/subscriptions/d7698da3-78bc-41fc-8db6-5dfad72a9b72/resourceGroups/Sans... 17 sivaramselvam@o... DEFAULT DIRECTORY

Microsoft Azure

Dashboard > Virtual networks > SANS-MCSE

SANS-MCSE

Virtual network

Search resources, services, and docs

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

DDoS protection

Firewall

DNS servers

Peerings

Service endpoints

Properties

Locks

Automation script

Monitoring

Connection monitor

Diagram

Support + troubleshooting

Connection troubleshoot

Resource group: SansboundAzureClass

Location: Central US

Subscription: Free Trial

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

Tags: Click here to add tags

Address space: 10.0.0.0/16

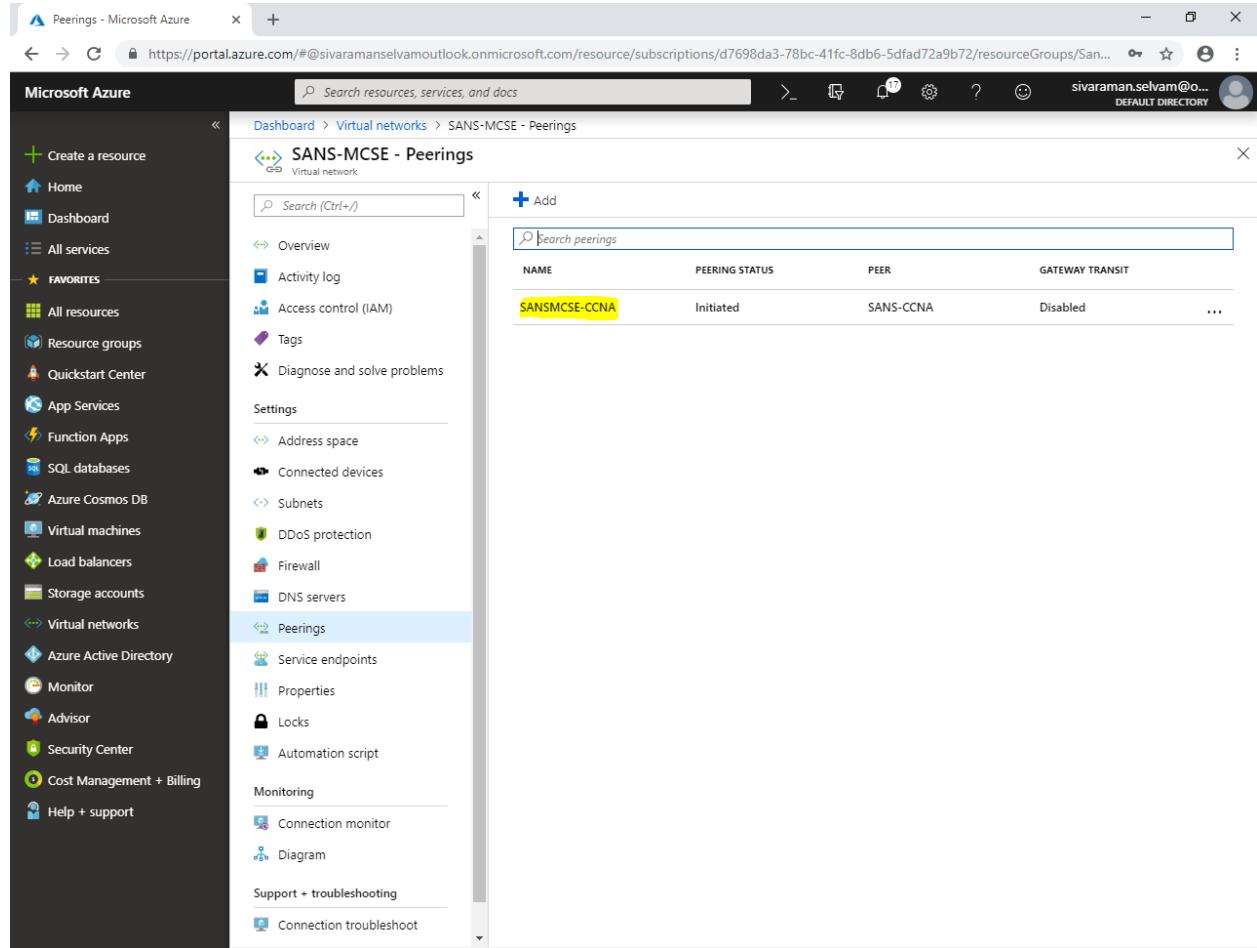
DNS servers: Azure provided DNS service

Connected devices:

DEVICE	TYPE	IP ADDRESS	SUBNET
mcsevm-azure169	Network interface	10.0.1.4	SANS-MCSEPubSubNet

In “Peerings”,

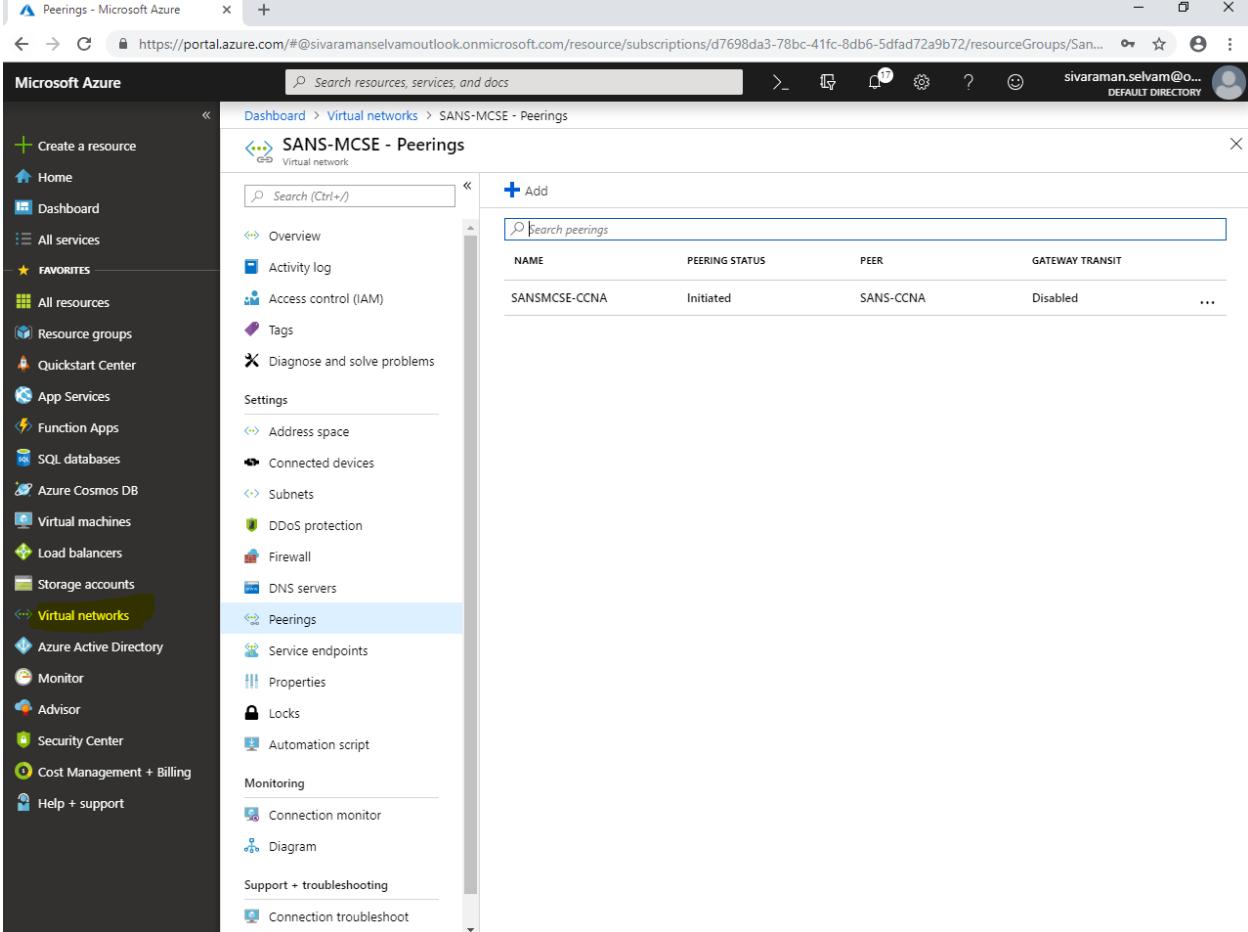
You are able to see that you have successfully added peering in “**SANS-MCSE**” virtual network.



The screenshot shows the Microsoft Azure portal interface. The left sidebar is filled with various service icons under categories like Home, Dashboard, All services, Favorites, and Virtual networks. The 'Virtual networks' category is expanded, and 'Peerings' is selected, highlighted with a blue background. The main content area is titled 'SANS-MCSE - Peerings' and shows a table of peerings. The table has columns: NAME, PEERING STATUS, PEER, and GATEWAY TRANSIT. There is one entry: 'SANSMCSE-CCNA' with 'Initiated' status, 'SANS-CCNA' as the peer, and 'Disabled' gateway transit. A search bar at the top right of the content area contains the placeholder 'Search peerings'.

NAME	PEERING STATUS	PEER	GATEWAY TRANSIT
SANSMCSE-CCNA	Initiated	SANS-CCNA	Disabled

Click “Virtual networks” in left side panel.

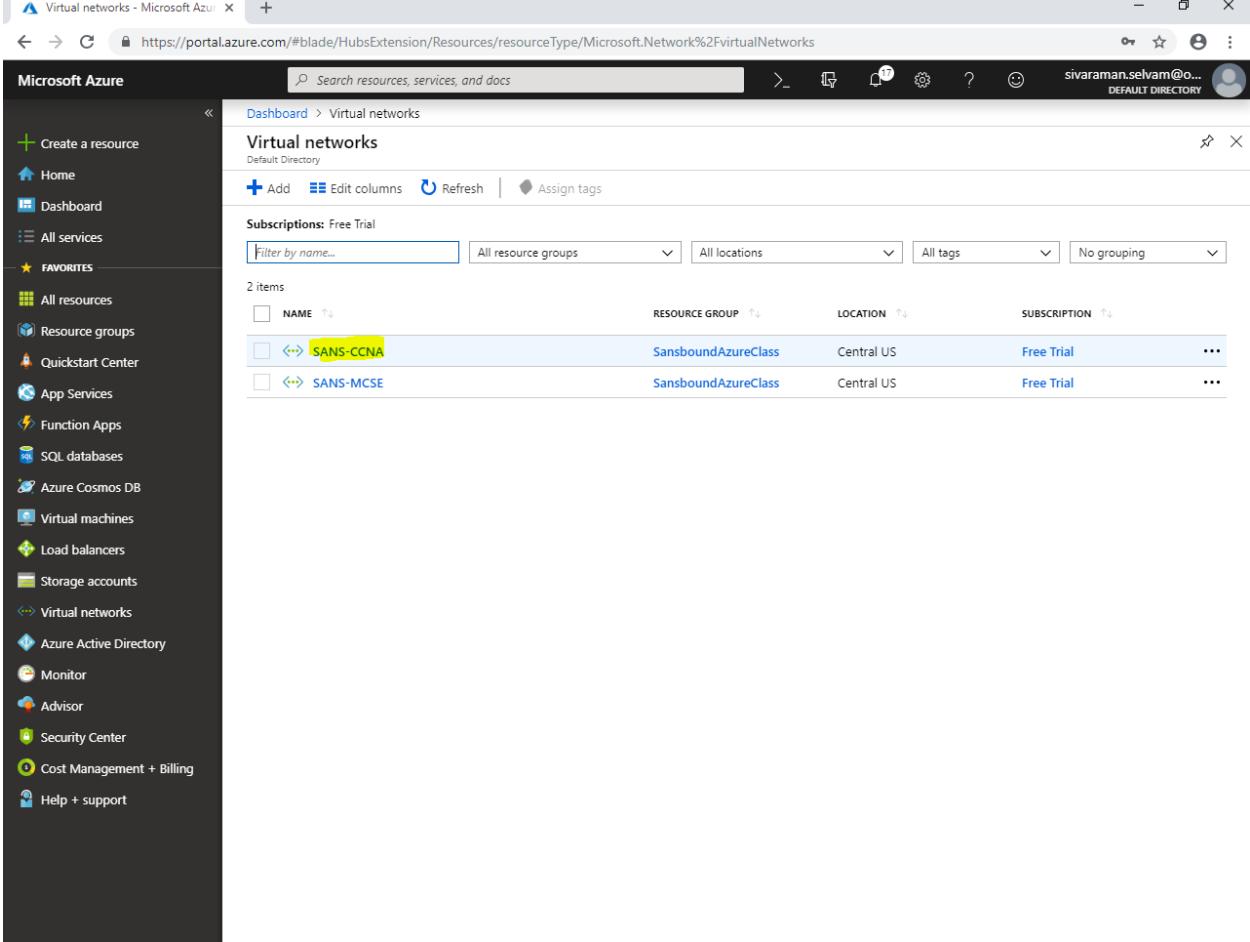


The screenshot shows the Microsoft Azure portal interface. The left sidebar is open, displaying various service categories. The "Virtual networks" option is highlighted with a yellow box. The main content area shows the "Peering" blade for a resource group named "SANS-MCSE - Peering". The blade includes a search bar, a navigation menu with links like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, and Peering, and a table listing a single peering entry. The table has columns for NAME, PEERING STATUS, PEER, and GATEWAY TRANSIT. The entry listed is "SANSMCSE-CCNA" with status "Initiated", peer "SANS-CCNA", and gateway transit "Disabled".

NAME	PEERING STATUS	PEER	GATEWAY TRANSIT
SANSMCSE-CCNA	Initiated	SANS-CCNA	Disabled

In “Virtual networks”,

Click “**SANS-CCNA**” virtual network.

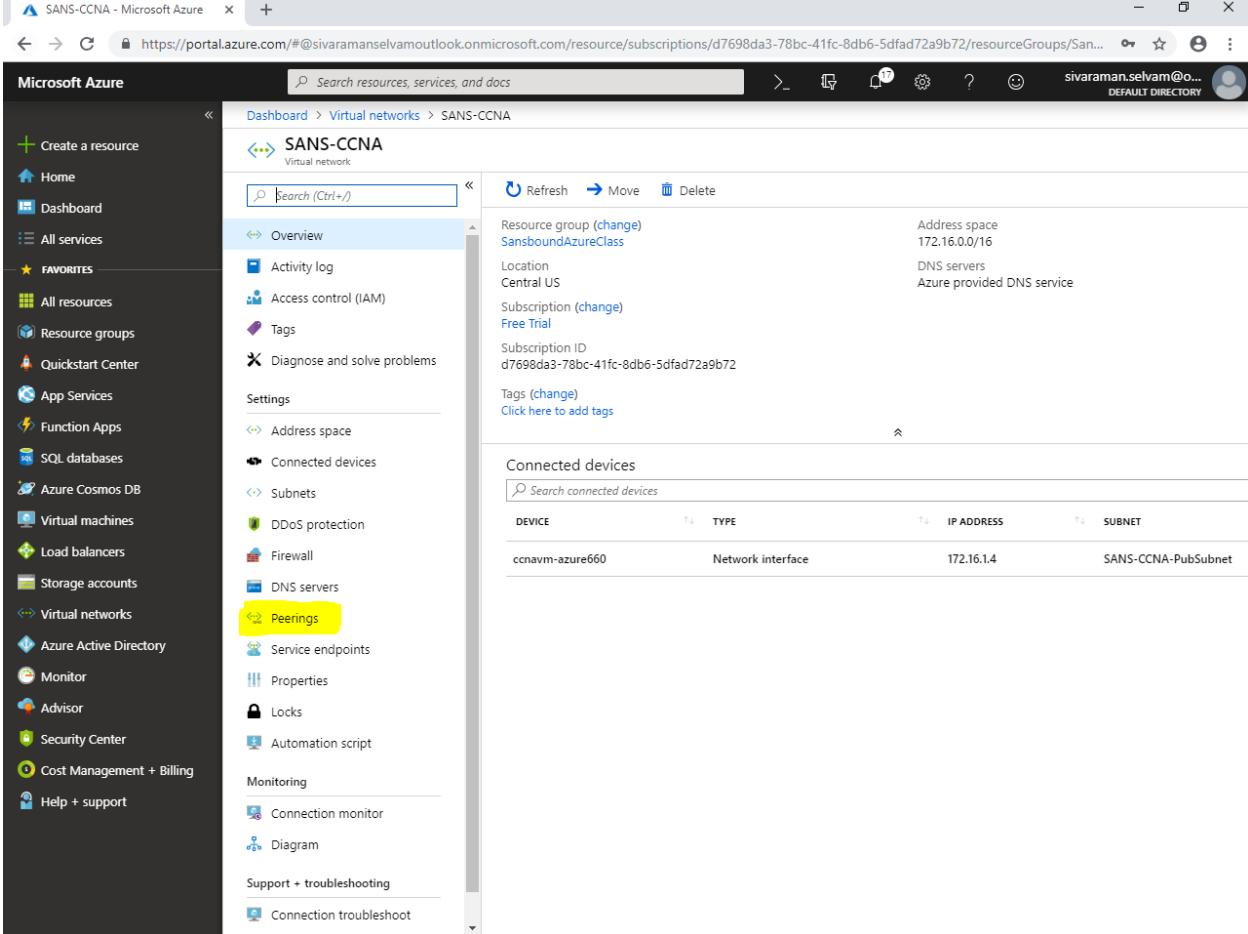


The screenshot shows the Microsoft Azure portal interface. The left sidebar is the navigation menu with various service icons. The main content area is titled "Virtual networks". It displays a table with two items:

NAME	RESOURCE GROUP	LOCATION	SUBSCRIPTION	...
SANS-CCNA	SansboundAzureClass	Central US	Free Trial	...
SANS-MCSE	SansboundAzureClass	Central US	Free Trial	...

In “**SANS-CCNA**” virtual network,

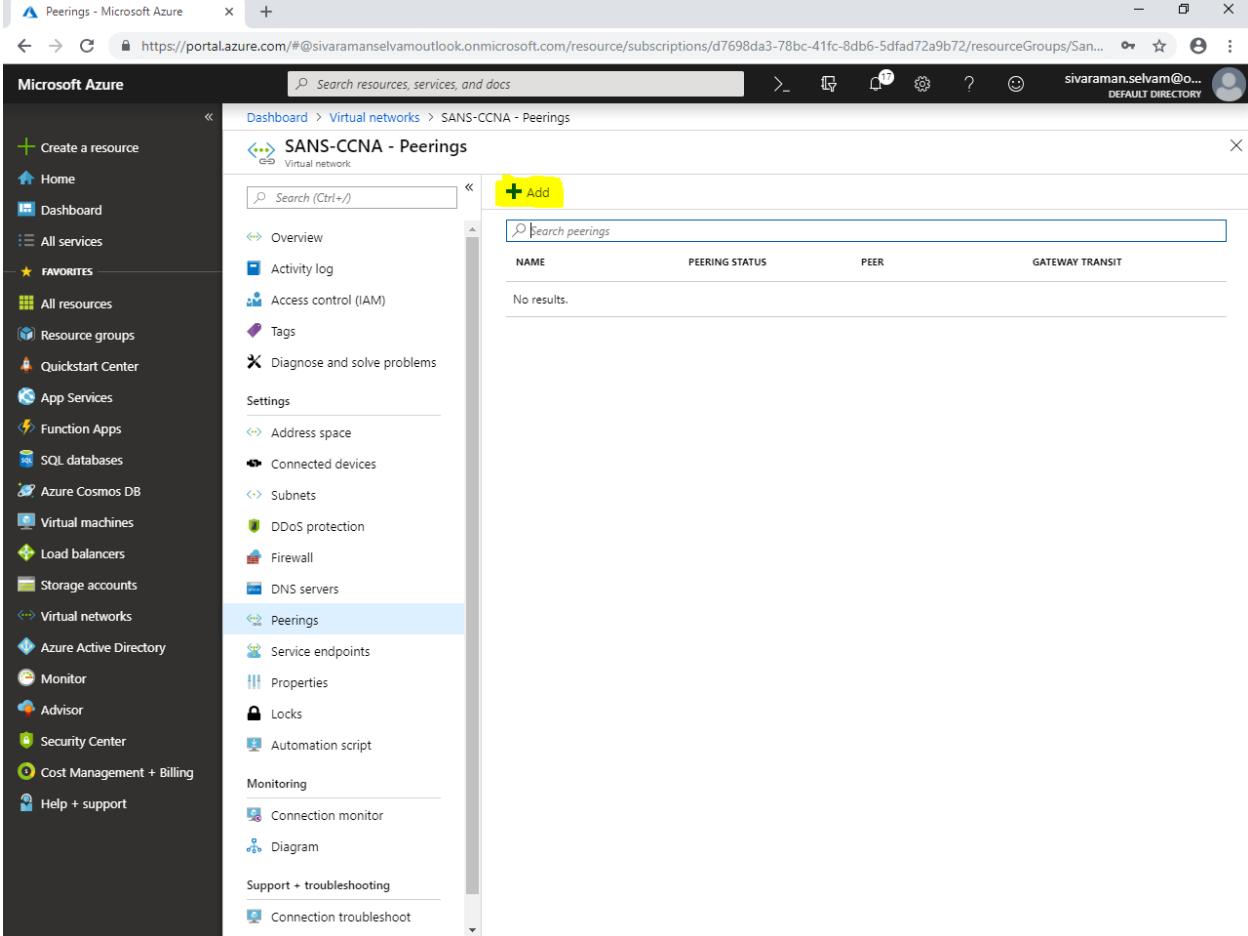
Click “**Peerings**”.



The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu is visible with various service icons. Under the "Virtual networks" section, the "Peerings" option is highlighted with a yellow box. The main content area displays the "SANS-CCNA" virtual network settings. It includes sections for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Address space, Connected devices, Subnets, DDoS protection, Firewall, DNS servers), and Connected devices. A table lists one connected device: "ccnavm-azure660" (Network interface, IP ADDRESS: 172.16.1.4, SUBNET: SANS-CCNA-PubSubnet).

DEVICE	TYPE	IP ADDRESS	SUBNET
ccnavm-azure660	Network interface	172.16.1.4	SANS-CCNA-PubSubnet

Click “Add” to add remote virtual network.



The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, Favorites, Resource groups, Quickstart Center, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Billing, and Help + support. The 'Virtual networks' option is selected. The main content area shows the 'SANS-CCNA - Peerings' page for a specific virtual network. The top navigation bar includes a search bar, dashboard, and user information. A large yellow box highlights the '+ Add' button in the top right corner of the main content area. Below it is a search bar labeled 'Search peerings'. A table below shows columns for NAME, PEERING STATUS, PEER, and GATEWAY TRANSIT, with a message 'No results.' at the bottom.

NAME	PEERING STATUS	PEER	GATEWAY TRANSIT
No results.			

While “**Add peering**”,

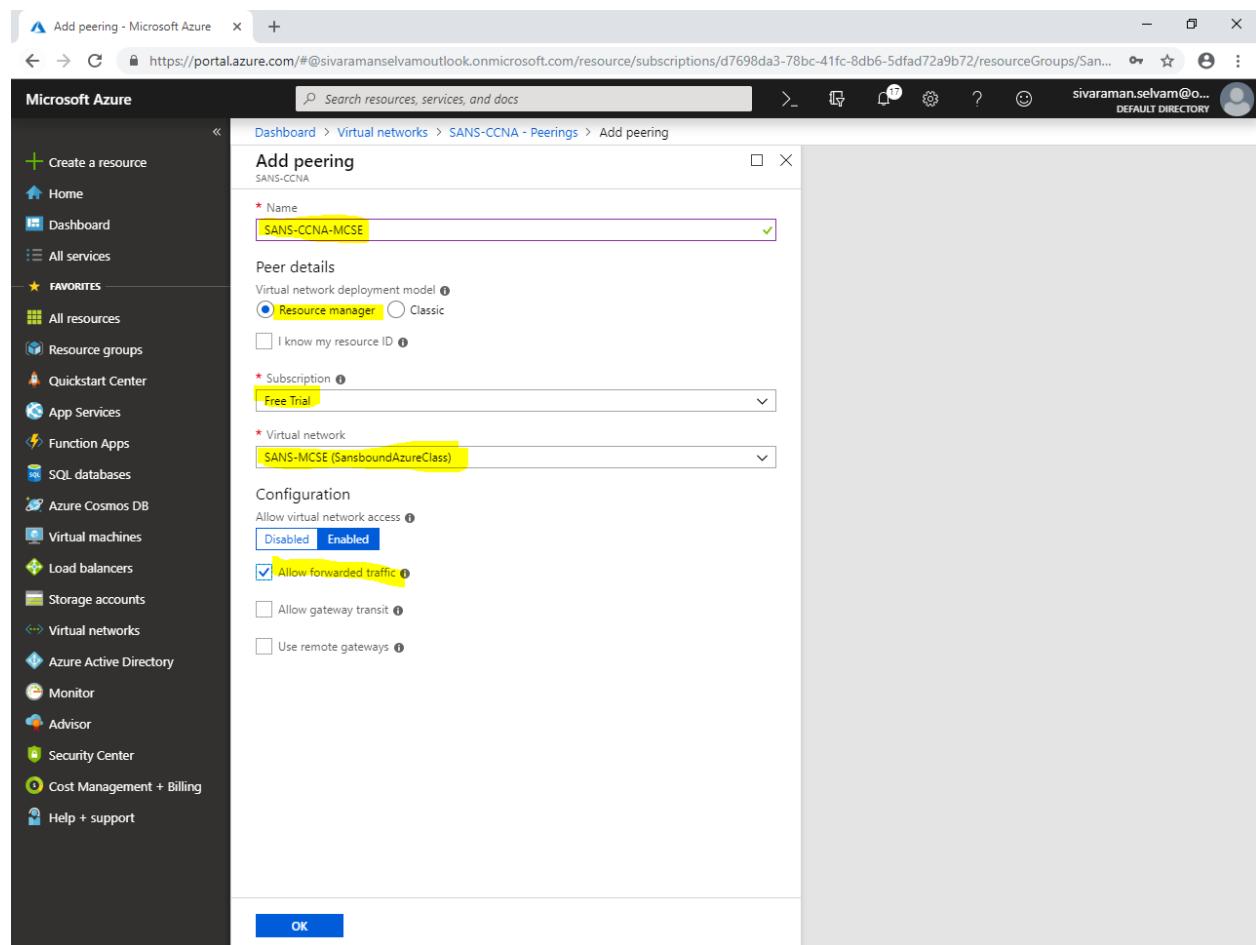
Type peering “**Name**” as “**SANS-CCNA-MCSE**”.

In “**Virtual network deployment model**” click on “**Resource manager**”.

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

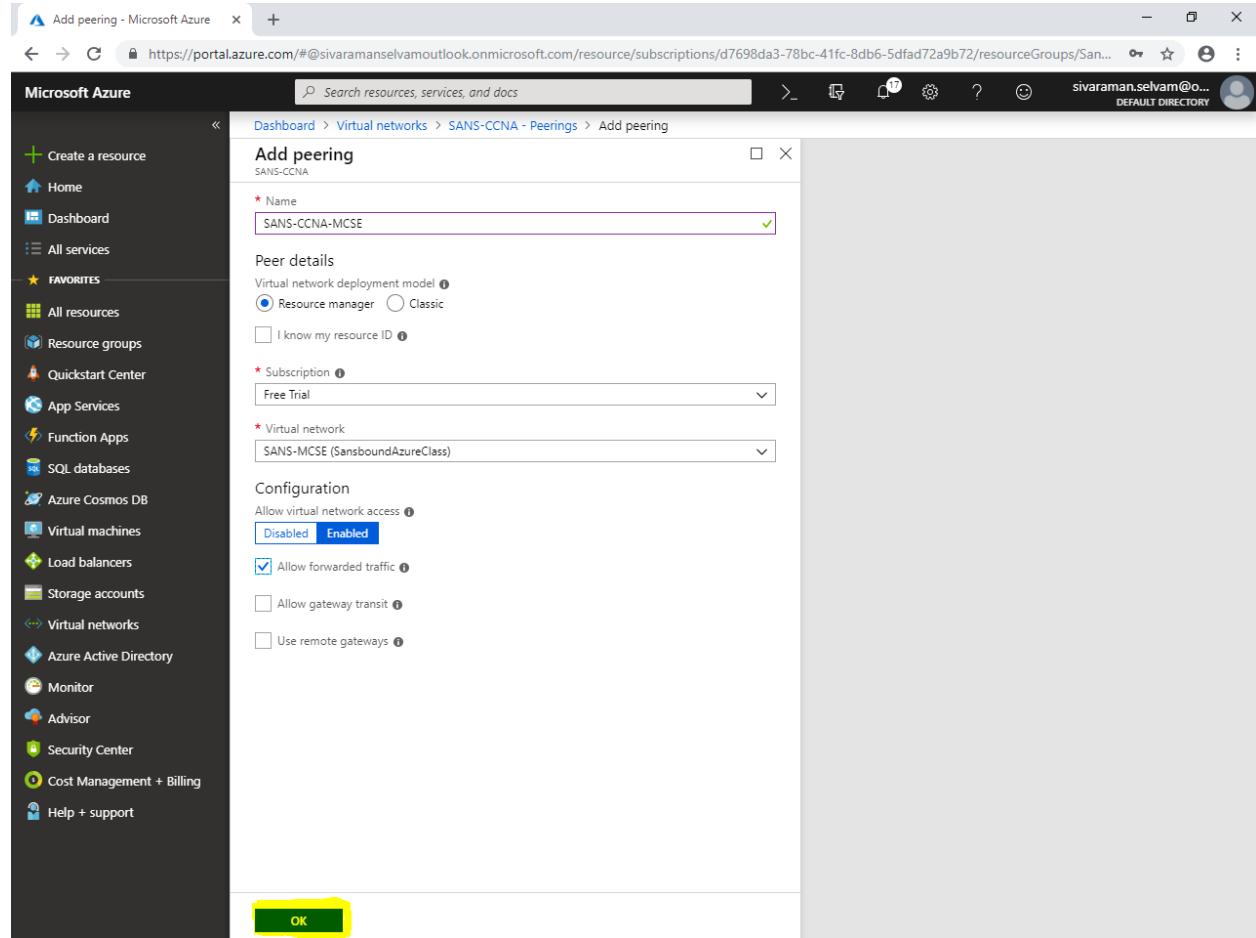
Select “**Virtual network**” as “**SANS-MCSE**” (which you have required to configure VNET peering).

In “**Configuration**”, need to check “**Allow forwarded traffic**”.



The screenshot shows the 'Add peering' dialog in the Microsoft Azure portal. The 'Name' field is set to 'SANS-CCNA-MCSE'. The 'Virtual network deployment model' is set to 'Resource manager'. The 'Subscription' dropdown shows 'Free Trial'. The 'Virtual network' dropdown shows 'SANS-MCSE (SansboundAzureClass)'. Under 'Configuration', the 'Allow virtual network access' section has 'Enabled' selected. The 'Allow forwarded traffic' checkbox is checked. There are also other configuration options like 'Allow gateway transit' and 'Use remote gateways' which are unchecked. At the bottom right is a blue 'OK' button.

Click "OK".



Add peering - Microsoft Azure

Microsoft Azure

Dashboard > Virtual networks > SANS-CCNA - Peering > Add peering

Name: SANS-CCNA-MCSE

Peer details

Virtual network deployment model:

- Resource manager
- Classic

I know my resource ID:

Subscription: Free Trial

Virtual network: SANS-MCSE (SansboundAzureClass)

Configuration

Allow virtual network access:

- Disabled
- Enabled

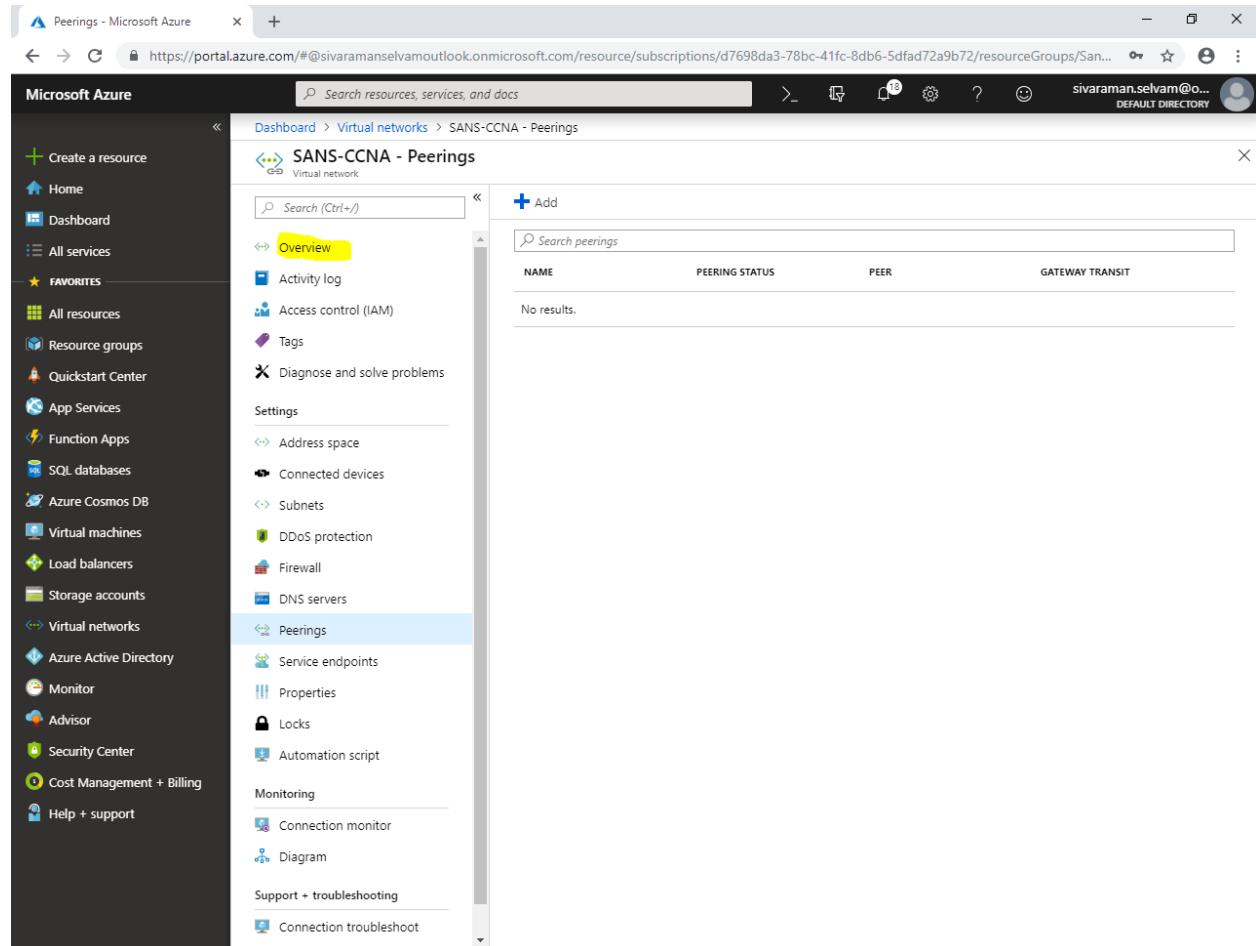
Allow forwarded traffic:

Allow gateway transit:

Use remote gateways:

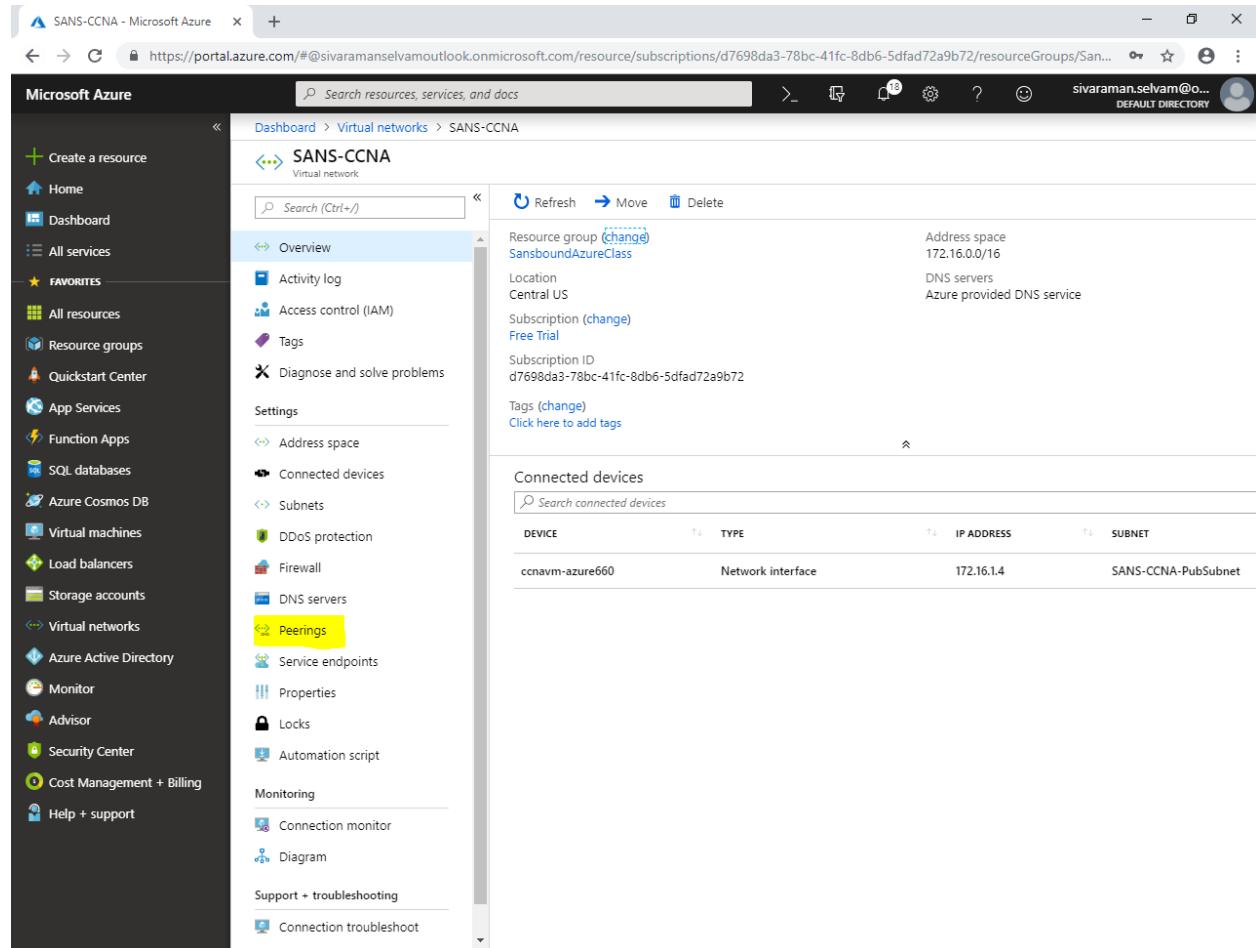
OK

Click “Overview”.



The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various service icons and links. The main content area is titled "SANS-CCNA - Peerings" and shows the "Virtual network" section. The "Overview" tab is highlighted with a yellow box. Below it, other tabs include "Activity log", "Access control (IAM)", "Tags", "Diagnose and solve problems", "Settings" (with sub-options like "Address space", "Connected devices", "Subnets", "DDoS protection", "Firewall", and "DNS servers"), "Peerings" (which is also highlighted with a blue box), "Service endpoints", "Properties", "Locks", "Automation script", "Monitoring" (with "Connection monitor" and "Diagram" sub-options), and "Support + troubleshooting" (with "Connection troubleshoot" sub-option). To the right, there is a search bar labeled "Search peerings" and a table with columns: NAME, PEERING STATUS, PEER, and GATEWAY TRANSIT. The table displays the message "No results."

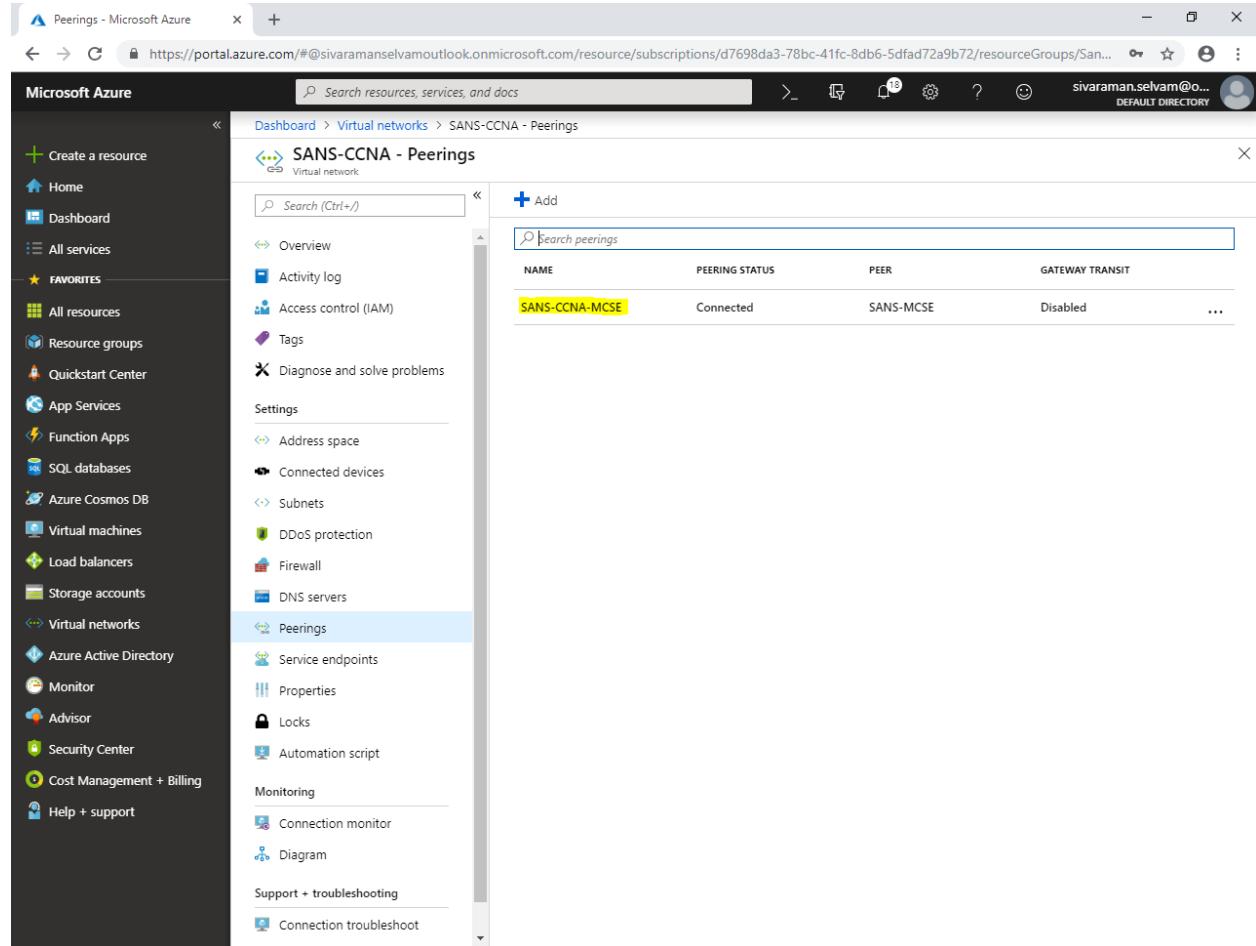
Click “**Peerings**” to view the remote virtual network details.



The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu is open, showing various services like Home, Dashboard, All services, Favorites, and Virtual networks. Under Virtual networks, the 'Peerings' link is highlighted with a yellow box. The main content area displays the 'SANS-CCNA' Virtual network blade. It shows basic information such as Resource group (SansboundAzureClass), Location (Central US), Subscription (Free Trial), and Address space (172.16.0.0/16). It also lists connected devices, including 'ccnavm-azure660' which is a Network interface with IP address 172.16.1.4 in the SANS-CCNA-PubSubnet.

DEVICE	TYPE	IP ADDRESS	SUBNET
ccnavm-azure660	Network interface	172.16.1.4	SANS-CCNA-PubSubnet

You are able see that “**SANS-CCNA-MCSE**” peering.



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 is titled "SANS-CCNA - Peerings" under "Virtual networks". It displays a table with one row:

NAME	PEERING STATUS	PEER	GATEWAY TRANSIT
SANS-CCNA-MCSE	Connected	SANS-MCSE	Disabled

In Windows 2008 R2 server, try to **ping 172.16.1.4** (Ubuntu IP) of “**SANS-CCNA**” virtual network from **10.0.1.4** of “**SANS-MCSE**” virtual network.

Now we can able to access the resources between **two different Virtual networks (VNET's)** from same region.

