Lab6 – Understanding Features of Virtual Network - Azure

Azure Virtual Network (VNet)?

An Azure Virtual Network (VNet) is a representation of your own network in the cloud. It is a logical isolation of the Azure cloud dedicated to your subscription. You can use VNets to provision and manage virtual private networks (VPNs) in Azure and, optionally, link the VNets with other VNets in Azure, or with your on-premises IT infrastructure to create hybrid or cross-premises solutions. Each VNet you create has its own CIDR block, and can be linked to other VNets and on-premises networks as long as the CIDR blocks do not overlap. You also have control of DNS server settings for VNets, and segmentation of the VNet into subnets.

Use VNets to:

- Create a dedicated private cloud-only VNet Sometimes you don't require a cross-premises configuration for your solution. When you create a VNet, your services and VMs within your VNet can communicate directly and securely with each other in the cloud. You can still configure endpoint connections for the VMs and services that require Internet communication, as part of your solution.
- Securely extend your data center With VNets, you can build traditional site-to-site (S2S) VPNs to securely scale your datacenter capacity. S2S VPNs use IPSEC to provide a secure connection between your corporate VPN gateway and Azure.
- Enable hybrid cloud scenarios VNets give you the flexibility to support a range of hybrid cloud scenarios. You can securely connect cloud-based applications to any type of on-premises system such as mainframes and Unix systems.

  For more infor go through below URL:

  https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-faq

Subnets

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

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

Network Secuirty Group (NSG)

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

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

Security rules

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

Property

Explanation

Name

A unique name within the network security group.

Priority

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

Source or destination

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

Protocol

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

Direction

Whether the rule applies to inbound, or outbound traffic.

Port range

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

Action

Allow or deny

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

A network security group (NSG) is a networking filter (firewall) containing a list of security rules allowing or denying network traffic to resources connected to Azure VNets. These rules can manage both inbound and outbound traffic. NSGs can be associated to subnets and/or individual Network Interfaces attached to ARM VMs and Classic VMs. Each NSG has the following properties regardless of where it is associated:

- Name for the NSG
- Azure region where the NSG is located
- resource group
- Rules either Inbound or Outboard defining what traffic is allowed or denied

When a NSG is associated to a subnet, the rules apply to all resources connected to the subnet. Traffic can be further restricted by also associating a NSG to a VM or NIC. NSGs that are associated to subnets are said to be filtering “North/South” traffic (in other words, packets flowing in and out of a subnet). NSGs that are associated to Network Interfaces are said to be filtering “East/West” traffic (in other words, how the VMs within the subnet connect to each other).

NSG Rules

NSG Rules are the mechanism defining traffic the administrator is looking to control. All NSGs have a set of default rules. These default rules cannot be deleted, but since they have the lowest possible priority, they can be overridden by the rules that you create. The lower the number, the sooner it will take precedence. The default rules allow and disallow traffic as follows:

- **Virtual network:** Traffic originating and ending in a virtual network is allowed both in inbound and outbound directions.
- **Internet:** Outbound traffic is allowed, but inbound traffic is blocked.
- **Load balancer:** Allow Azure's load balancer to probe the health of your VMs and role instances. If you are not using a load balanced set, you can override this rule.

NSG Rules are enforced based on their Priority. Priority values start from 100 and go to 4096. Rules will be read and enforced starting with 100 then 101, 102 etc., until all rules have been evaluated in this order. Rules with the priority "closest" to 100 will be enforced. For example, if you had an inbound rule that allowed TCP traffic on Port 80 with a priority of 250 and another that denied TCP traffic on Port 80 with a priority of 125, the NSG rule of deny would be put in place. This is because the "deny rule", with a priority of 125 is closer to 100 than the "allow rule", containing a priority of 250.

Associating NSGs

NSGs are used to define the rules of how traffic is filtered for your IaaS deployments in Azure. NSGs by themselves are not implemented until they are "associated", with a resource in Azure. NSGs can be associated to ARM network interfaces (NIC), which are associated to the VMs, or subnets.

For NICs associated to VMs, the rules are applied to all traffic to/from that Network Interface where it is associated. It is possible to have a multi-NIC VM, and you can associate the same or different NSG to each Network Interface. When NSGs are applied to subnets, rules are applied to traffic to/from all resources connect to that subnet.

In what order are NSGs enforced?

Understanding the effective rules of NSGs is critical. Security rules are applied to the traffic by priority in each NSG in the following order:

Inbound Traffic:

1. NSG applied to subnet: If a subnet NSG has a matching rule to deny traffic, the packet is dropped.

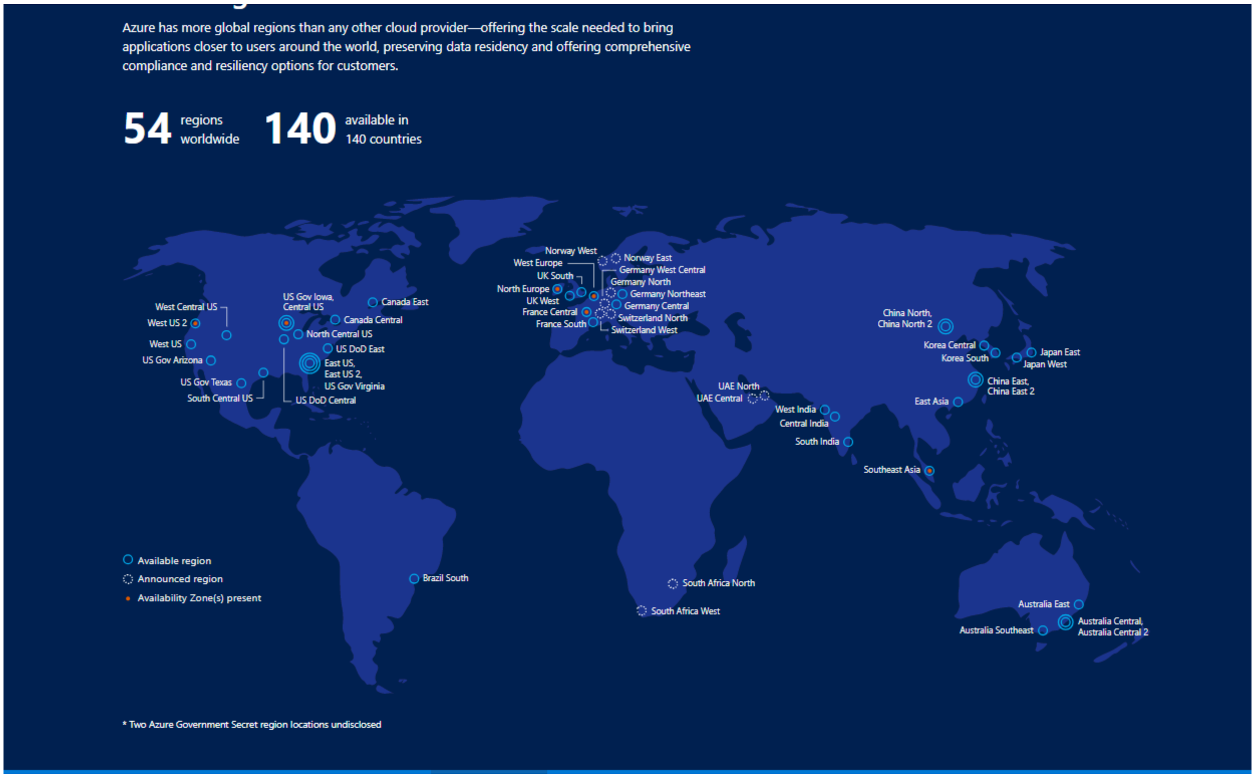
2. NSG applied to NIC: If VM\NIC NSG has a matching rule that denies traffic, packets are dropped at the VM\NIC, even if a subnet NSG has a matching rule that allows traffic.

Outbound Traffic:

1. NSG applied to NIC: If a VM\NIC NSG has a matching rule that denies traffic, packets are dropped.

2. NSG applied to subnet: If a subnet NSG has a matching rule that denies traffic, packets are dropped, even if a VM\NIC NSG has a matching rule that allows traffic.

Regions:



Azure has more global regions than any other cloud provider—offering the scale needed to bring applications closer to users around the world, preserving data residency and offering comprehensive compliance and resiliency options for customers.

54 regions worldwide

140 available in 140 countries

○ Available region

◌ Announced region

● Availability Zone(s) present

* Two Azure Government Secret region locations undisclosed

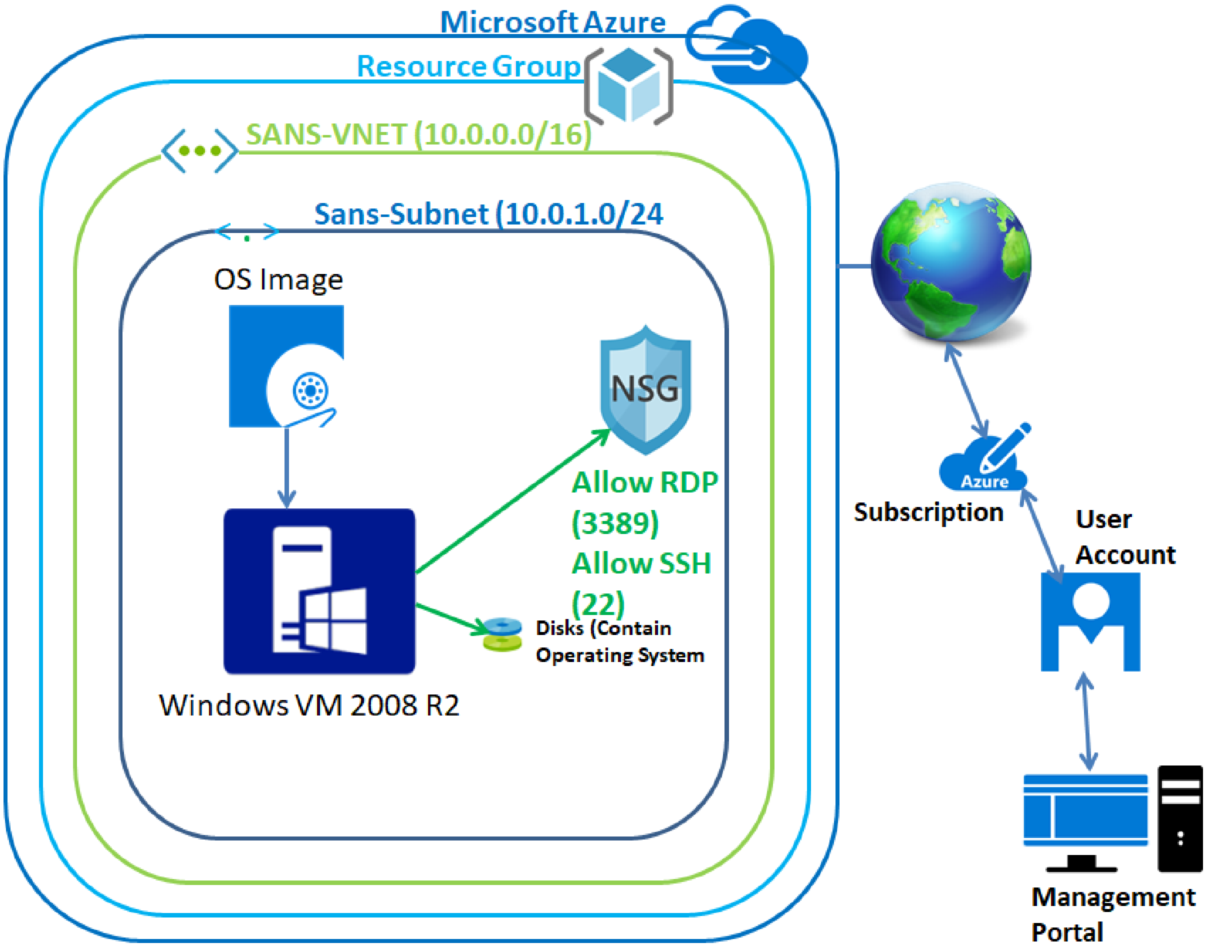
Azure Locations: https://azure.microsoft.com/en-in/global-infrastructure/locations/

Resource Group:

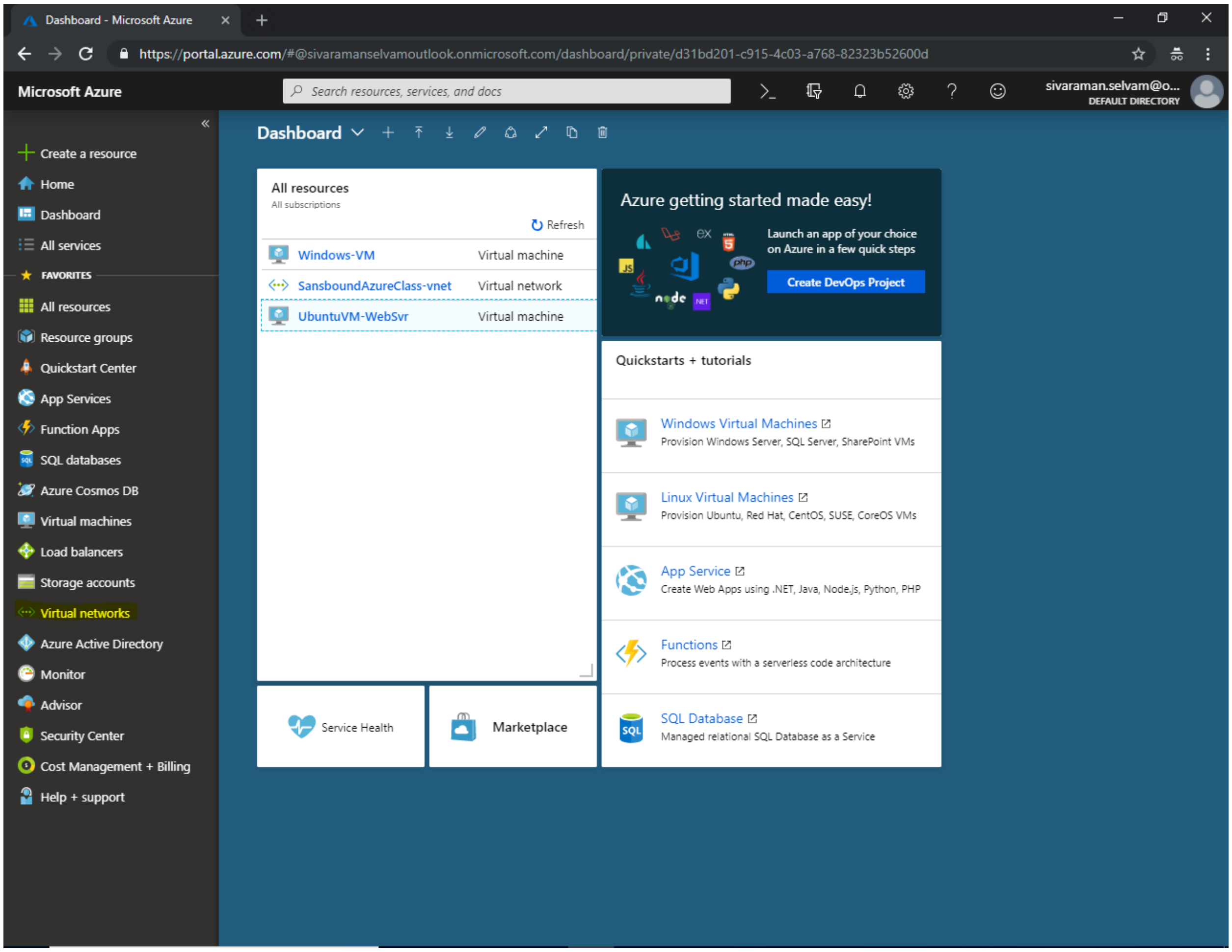
Since the introduction of the Azure preview portal in 2014, resource groups are automatically created for virtual machines, databases, and other assets, no matter how they are added to the cloud fabric. Resource groups provide a way to monitor, control access, provision and manage billing for collections of assets that are required to run an application, or used by a client or company department. Azure Resource Manager (ARM) is the technology that works behind the scenes so that you can administer assets using these logical containers.

Resource groups can only be managed using the preview portal or PowerShell, and as you might expect, there are no plans to add support to the old management portal. If you haven’t yet discovered the preview portal, click the user icon in the far top-right corner of the old portal, and select **Switch to new portal** from the menu. You can log in directly to the new portal.

Topology

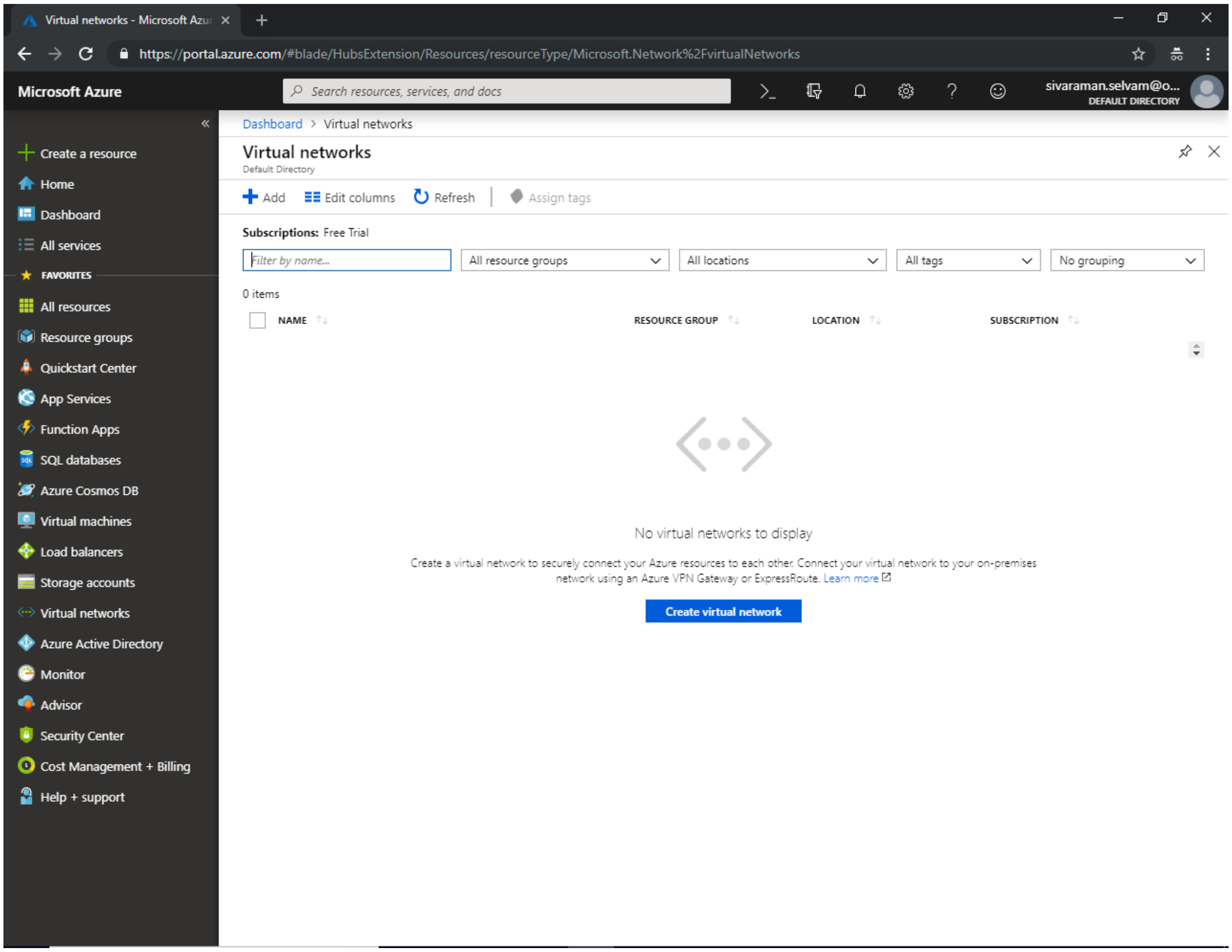

Microsoft Azure
Resource Group
SANS-VNET (10.0.0.0/16)
Sans-Subnet (10.0.1.0/24
OS Image
NSG
Allow RDP (3389)
Allow SSH (22)
Disks (Contain Operating System
Windows VM 2008 R2
Azure
Subscription
User Account
Management Portal

In Azure portal, click “Virtual networks”.


Dashboard - Microsoft Azure
https://portal.azure.com/#@sivaramanselvamoutlook.onmicrosoft.com/dashboard/private/d31bd201-c915-4c03-a768-82323b52600d
Microsoft Azure
Search resources, services, and docs
sivaraman.selvam@o...
DEFAULT DIRECTORY
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
Quickstart Center
App Services
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
Dashboard
All resources
All subscriptions
Refresh
Azure getting started made easy!
Launch an app of your choice on Azure in a few quick steps
Create DevOps Project
Quickstarts + tutorials
Windows Virtual Machines
Provision Windows Server, SQL Server, SharePoint VMs
Linux Virtual Machines
Provision Ubuntu, Red Hat, CentOS, SUSE, CoreOS VMs
App Service
Create Web Apps using .NET, Java, Node.js, Python, PHP
Functions
Process events with a serverless code architecture
SQL Database
Managed relational SQL Database as a Service
Service Health
Marketplace

Windows-VM	Virtual machine
SansboundAzureClass-vnet	Virtual network
UbuntuVM-WebSvr	Virtual machine

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



Subscriptions: Free Trial

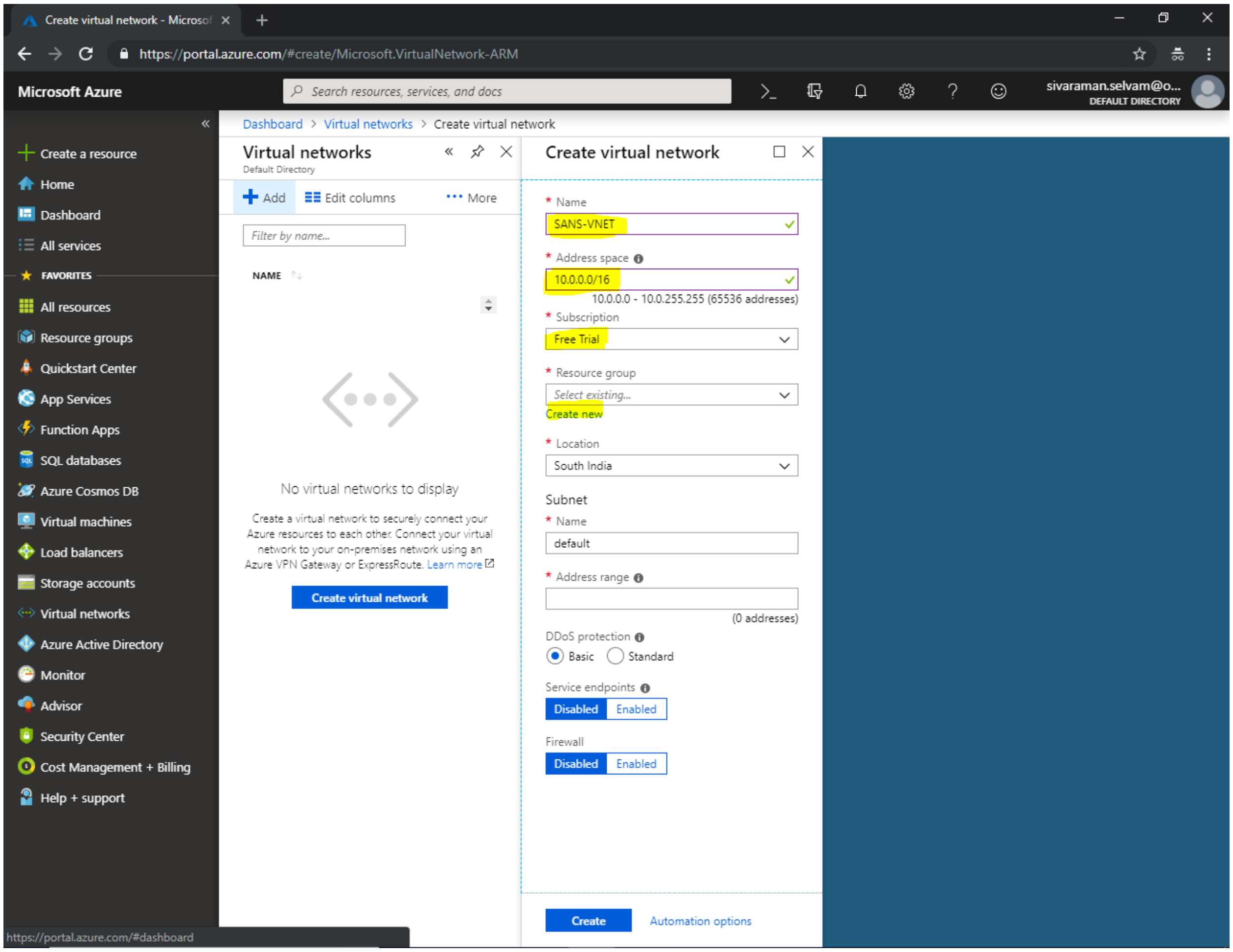
0 items

No virtual networks to display

Create a virtual network to securely connect your Azure resources to each other. Connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute. Learn more

While creating virtual network, it has required the virtual network name specify it as “SANS-VNET” and specify the address space as **10.0.0.0/16,** select **“Subscription”** as **“Free Trial”.**

We have required to create the “Resource group” click “Create new”.



No virtual networks to display

Create a virtual network to securely connect your Azure resources to each other. Connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute. Learn more

Create virtual network

* Name: SANS-VNET

* Address space: 10.0.0.0/16
10.0.0.0 - 10.0.255.255 (65536 addresses)

* Subscription: Free Trial

* Resource group: Select existing...
Create new

* Location: South India

Subnet

* Name: default

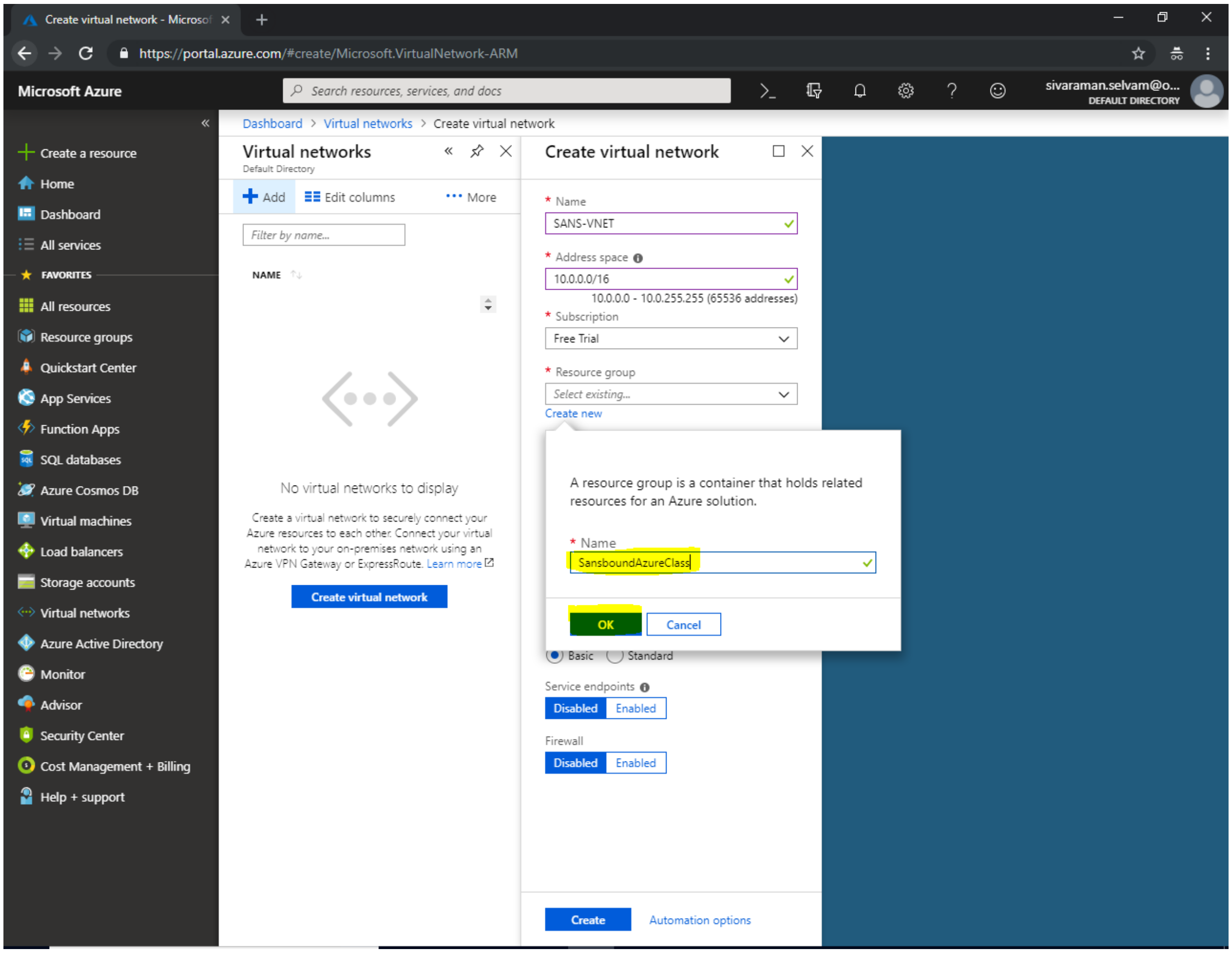
* Address range:
(0 addresses)

DDoS protection: ● Basic ○ Standard

Service endpoints: Disabled | Enabled

Firewall: Disabled | Enabled

In Resource Group name type “SansboundAzureClass” and click “Ok”.



Create virtual network

* Name
SANS-VNET ✓

* Address space
10.0.0.0/16 ✓
10.0.0.0 - 10.0.255.255 (65536 addresses)

* Subscription
Free Trial

* Resource group
Select existing...
Create new

A resource group is a container that holds related resources for an Azure solution.

* Name
SansboundAzureClass ✓

OK Cancel

● Basic ○ Standard

Service endpoints
Disabled Enabled

Firewall
Disabled Enabled

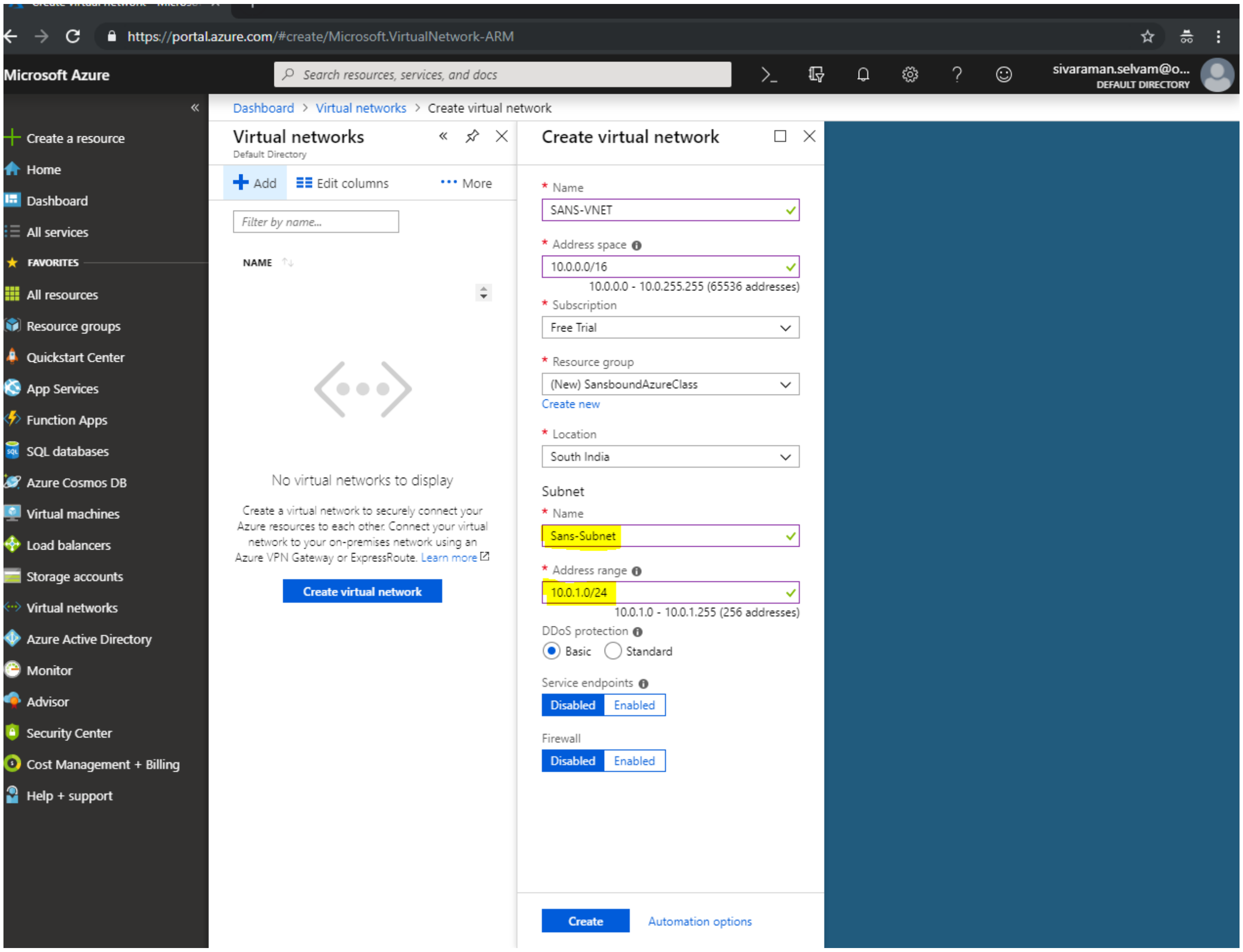
Create Automation options

Create virtual network - Microsof ×
https://portal.azure.com/#create/Microsoft.VirtualNetwork-ARM
Microsoft Azure
Search resources, services, and docs
sivaraman.selvam@o...
DEFAULT DIRECTORY
Dashboard > Virtual networks > Create virtual network
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
Quickstart Center
App Services
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
Virtual networks
Default Directory
Add
Edit columns
More
Filter by name...
NAME
No virtual networks to display
Create a virtual network to securely connect your Azure resources to each other. Connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute. Learn more
Create virtual network

In **“Subnet”**,

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

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



No virtual networks to display

Create a virtual network to securely connect your Azure resources to each other. Connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute. Learn more

Create virtual network

* Name: SANS-VNET

* Address space: 10.0.0.0/16
10.0.0.0 - 10.0.255.255 (65536 addresses)

* Subscription: Free Trial

* Resource group: (New) SansboundAzureClass
Create new

* Location: South India

Subnet

* Name: Sans-Subnet

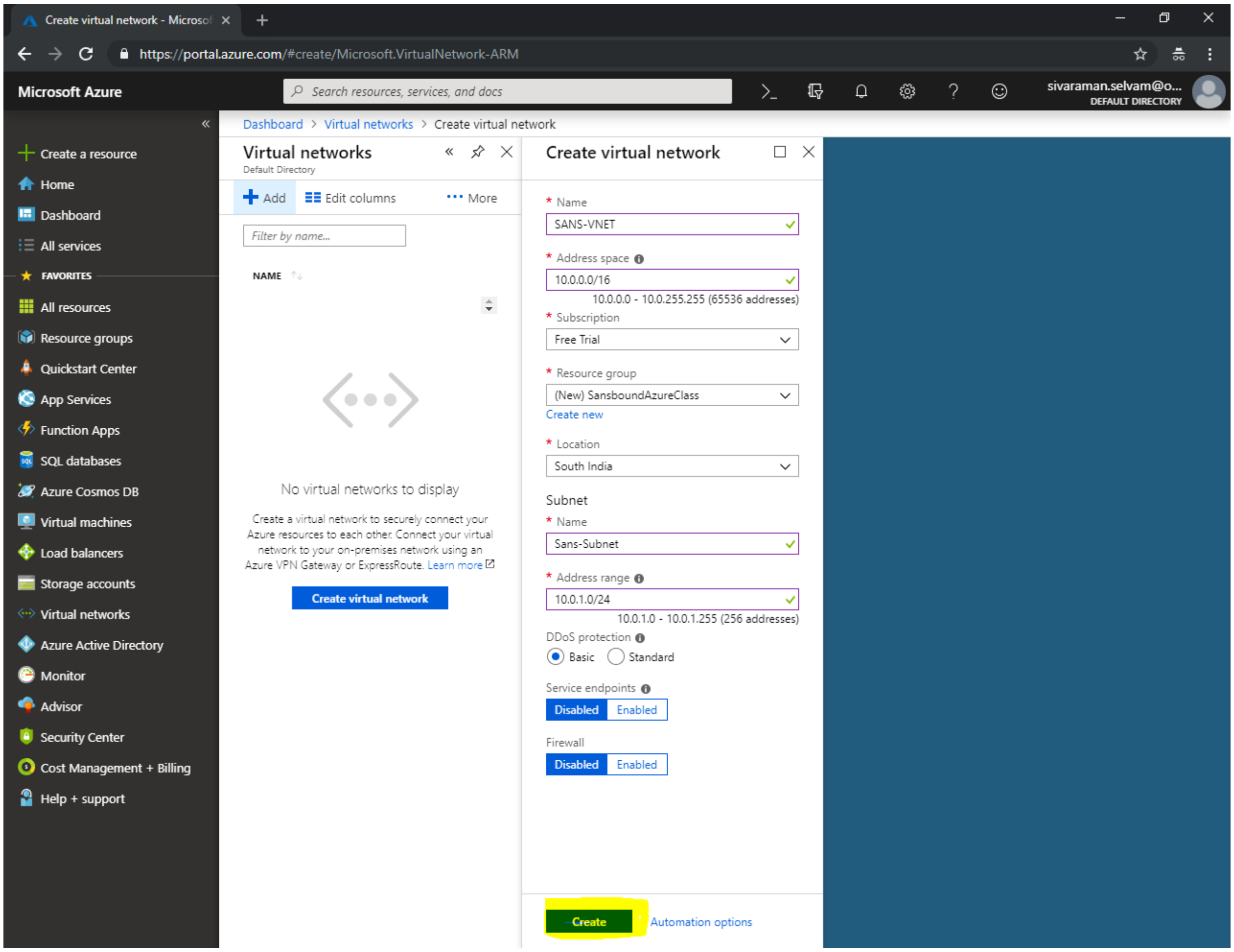
* Address range: 10.0.1.0/24
10.0.1.0 - 10.0.1.255 (256 addresses)

DDoS protection: ● Basic ○ Standard

Service endpoints: [✓ Disabled] Enabled

Firewall: [✓ Disabled] Enabled

Click **"Create".**



Create virtual network

- Name: SANS-VNET
- Address space: 10.0.0.0/16
  - 10.0.0.0 - 10.0.255.255 (65536 addresses)
- Subscription: Free Trial
- Resource group: (New) SansboundAzureClass
- Location: South India

Subnet

- Name: Sans-Subnet
- Address range: 10.0.1.0/24
  - 10.0.1.0 - 10.0.1.255 (256 addresses)
- DDoS protection: ● Basic ○ Standard
- Service endpoints: Disabled
- Firewall: Disabled

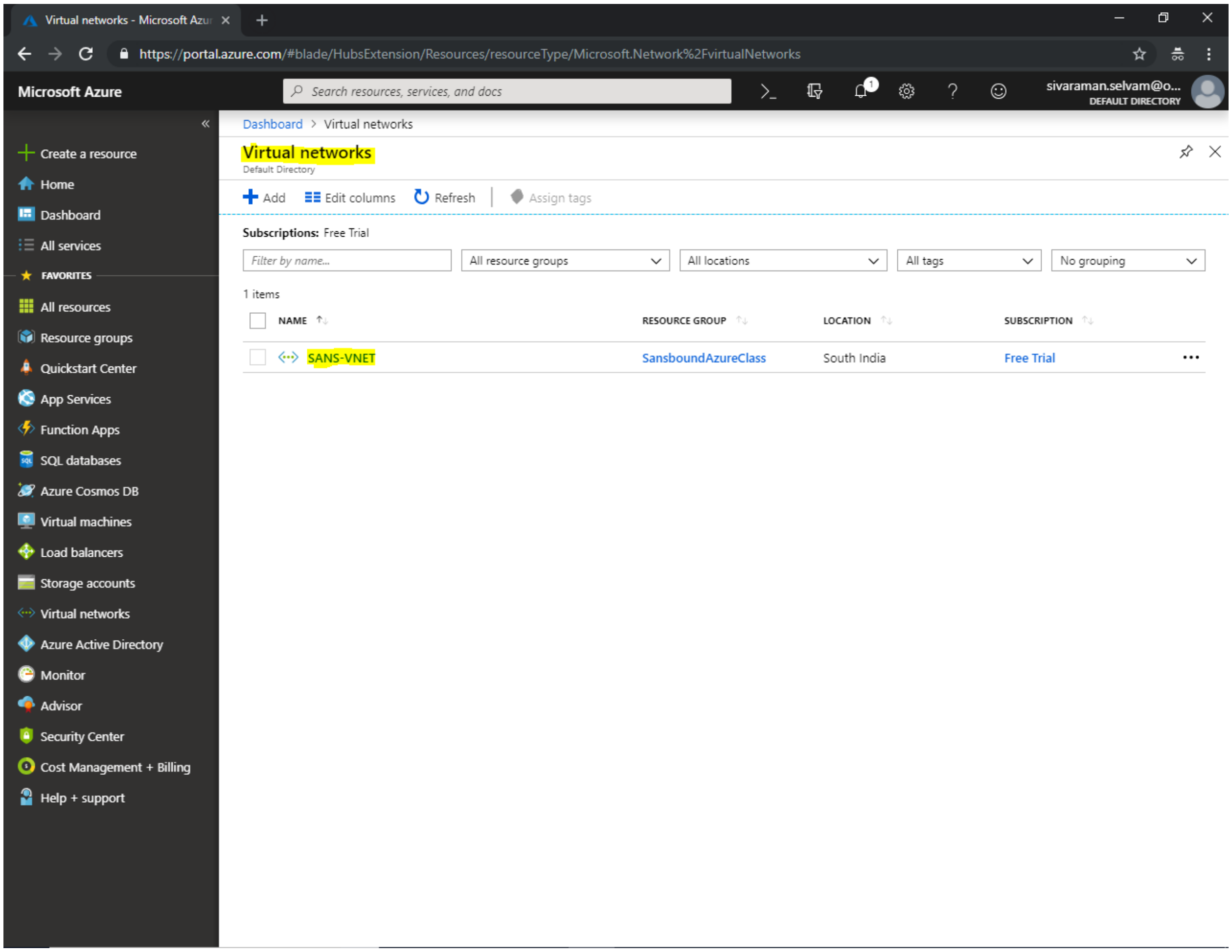
No virtual networks to display

Create a virtual network to securely connect your Azure resources to each other. Connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute. Learn more

In “Virtual Networks”, click “Refresh” to view the newly created Vnet.

Now you are able to see the VNet named **“SANS-VNET”**.

Click on **“SANS-VNET”** to view it details.

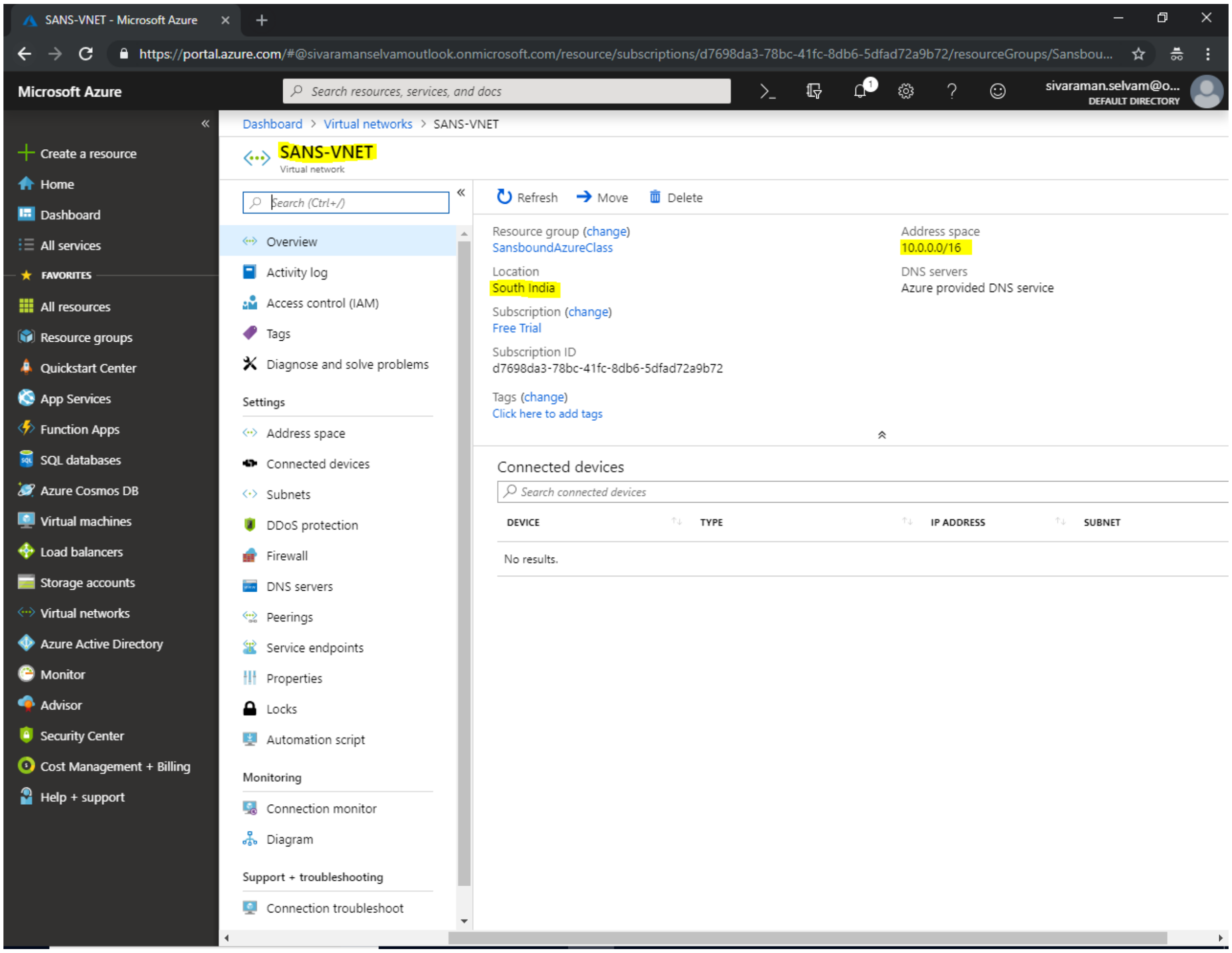


Subscriptions: Free Trial

1 items

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

In **“SANS-VNET”**, you are able to see the address space details **10.0.0.0/16** and **“Region”**



Resource group (change)
SansboundAzureClass

Location
South India

Subscription (change)
Free Trial

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

Tags (change)
Click here to add tags

Address space
10.0.0.0/16

DNS servers
Azure provided DNS service

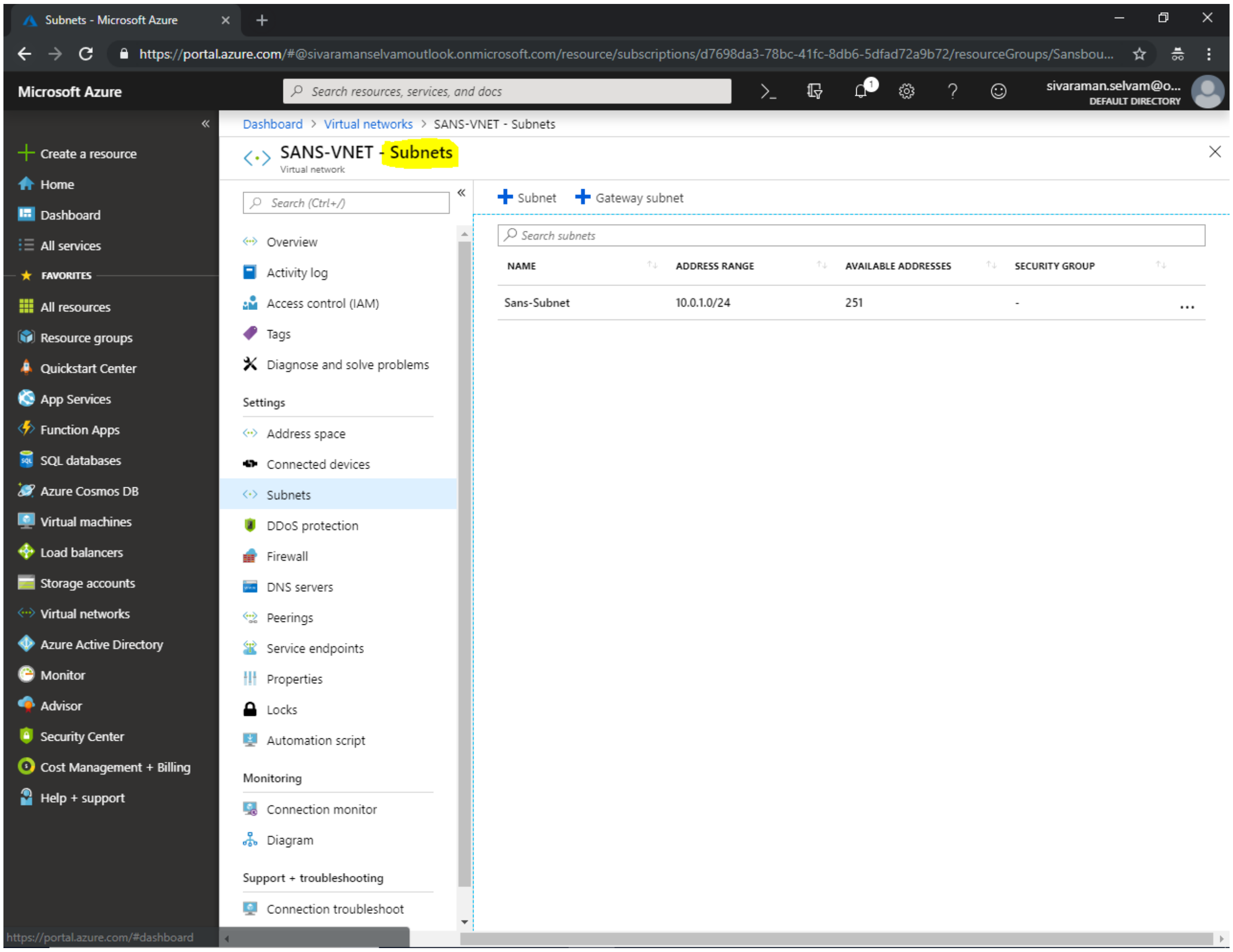
Connected devices

Search connected devices

DEVICE	TYPE	IP ADDRESS	SUBNET
No results.			

In **“SANS-VNET”** click on **“Subnets”** to get the details.

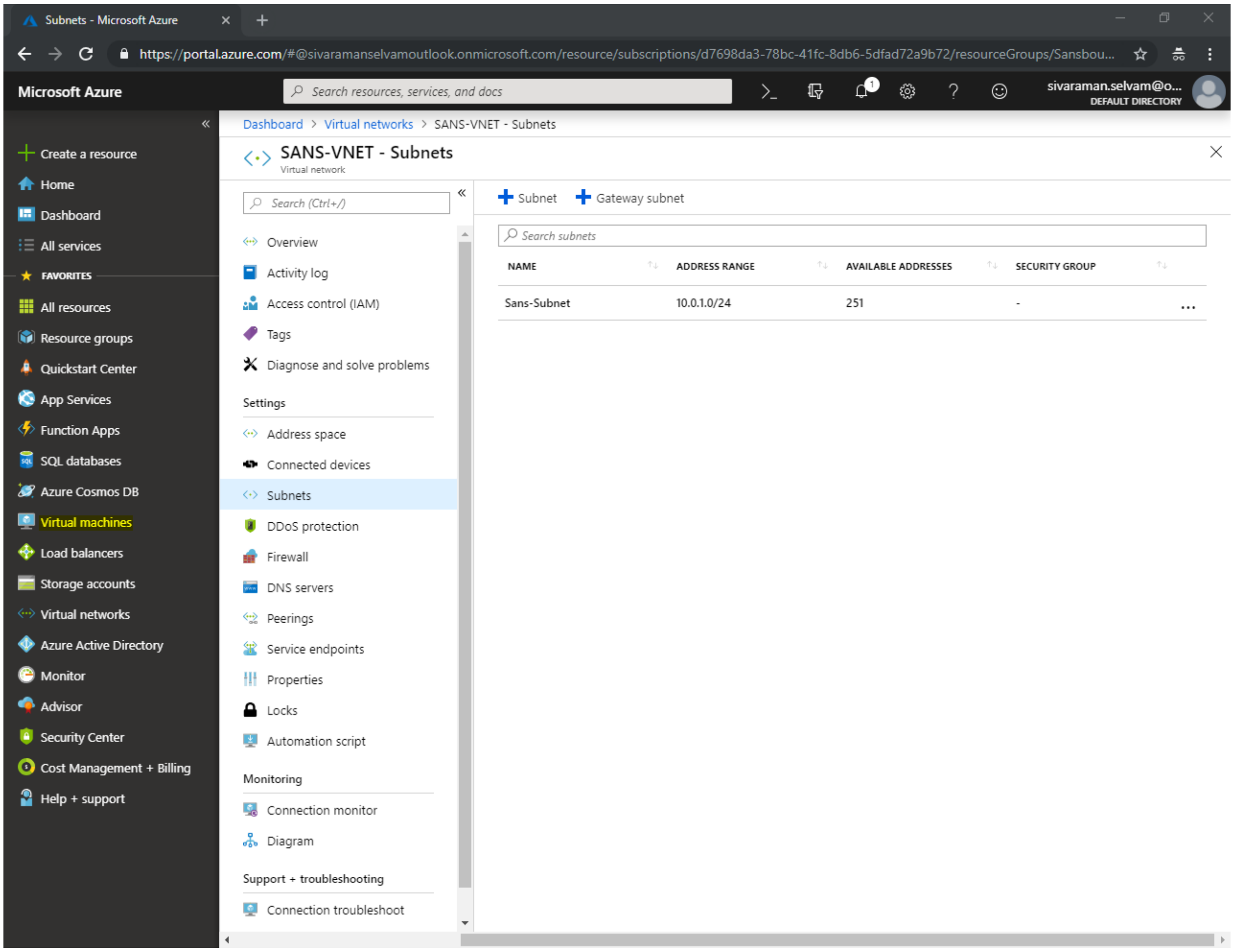
As of now, we have only one **“Subnet”** named **“Sans-Subnet” and it’s range is 10.0.1.0/24.**



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

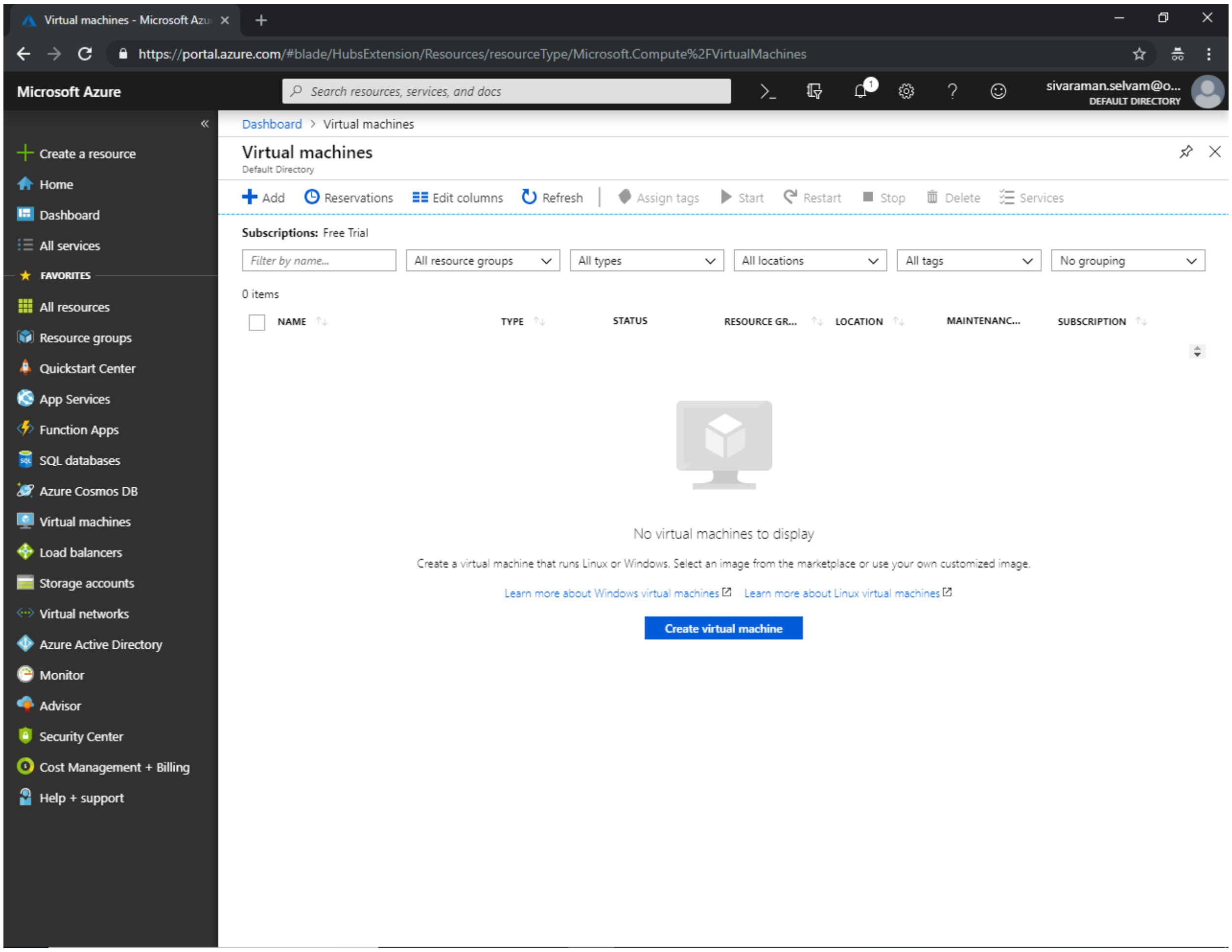
Now we have required to launch the virtual machine with Windows Server 2008 R2 Sp1.

Click **"Virtual machines"** in left side panel.



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

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



Subscriptions: Free Trial

0 items

No virtual machines to display

Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.

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

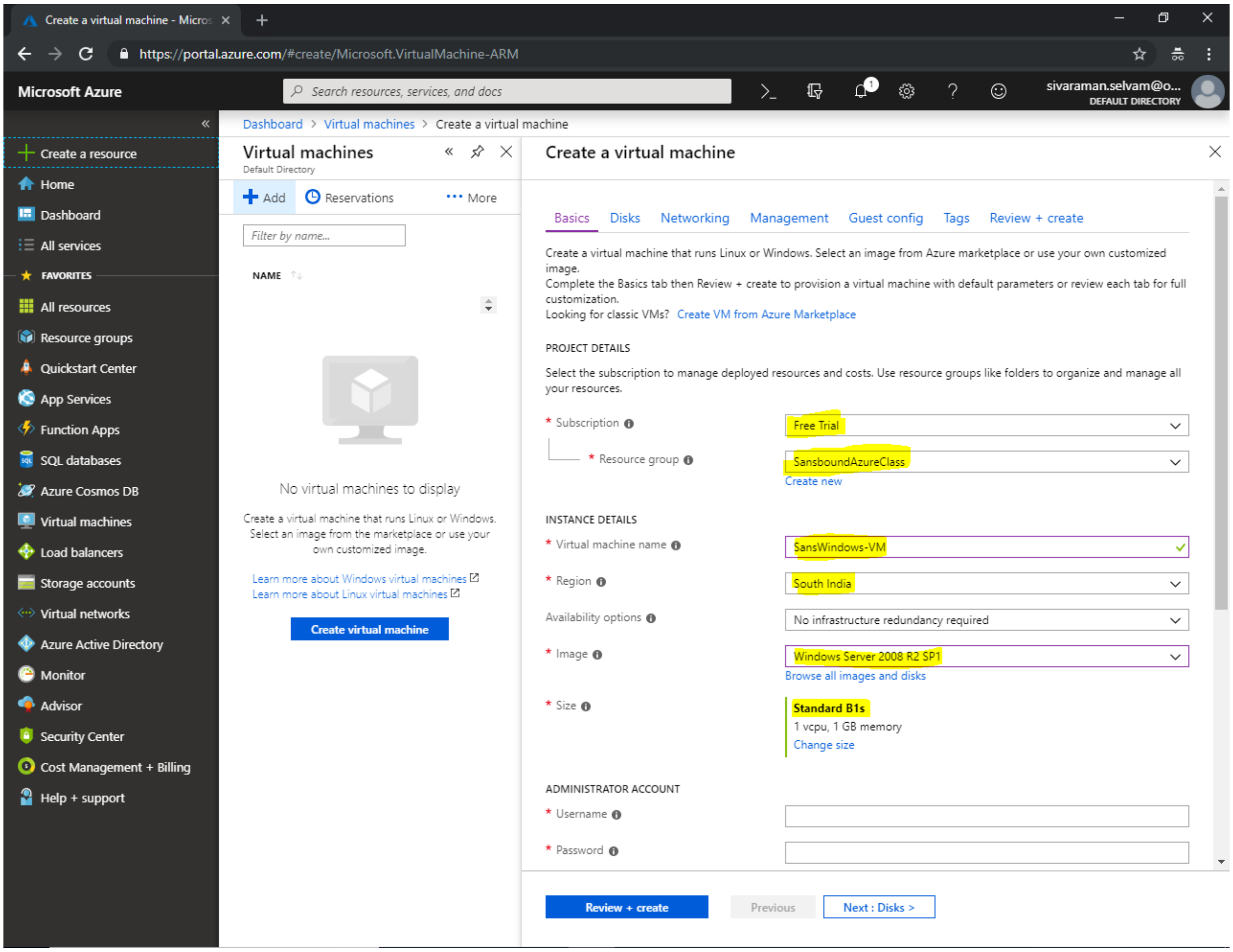
“Resource Group” as **“SansboundAzureClass”**.

Type **“Virtual machine name”** as **“SansWindows-VM”**

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

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

“VM Size” should be changed as **“Standard B1s”**.



No virtual machines to display

Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.

Learn more about Windows virtual machines
Learn more about Linux virtual machines

Create a virtual machine

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image.
Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.
Looking for classic VMs? Create VM from Azure Marketplace

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription	Free Trial
* Resource group	SansboundAzureClass Create new

INSTANCE DETAILS

* Virtual machine name	SansWindows-VM
* Region	South India
Availability options	No infrastructure redundancy required
* Image	Windows Server 2008 R2 SP1 Browse all images and disks
* Size	Standard B1s 1 vcpu, 1 GB memory Change size

ADMINISTRATOR ACCOUNT

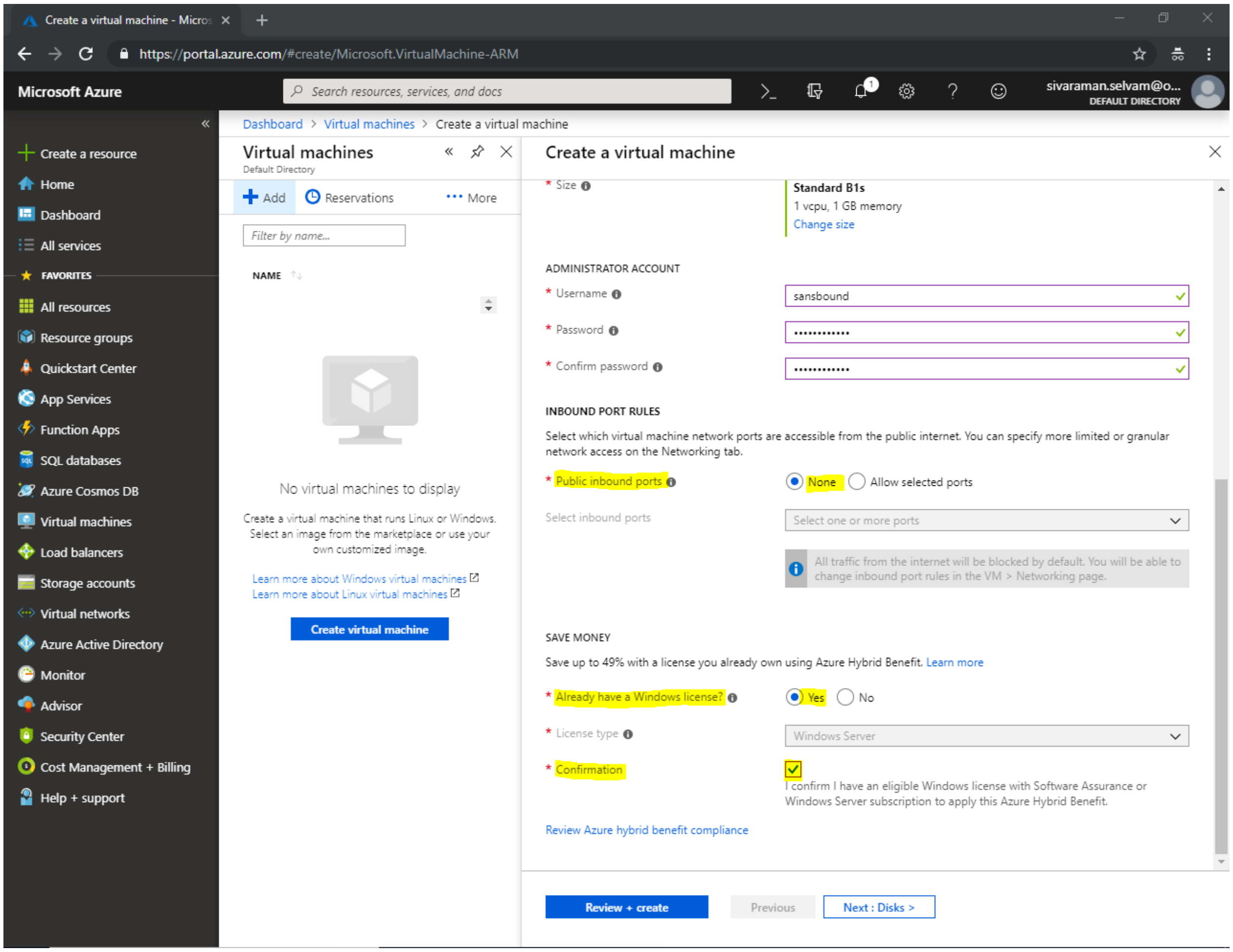
* Username	
* Password	

In **“Save Money”**

Click **“Yes”** for **“Already have a Windows license”**.

Need to check **“Confirmation”** box.

Click **“Next : Disks >”**.



Create a virtual machine

* Size: Standard B1s, 1 vcpu, 1 GB memory, Change size

ADMINISTRATOR ACCOUNT

* Username: sansbound

* Password: ••••••••••••

* Confirm password: ••••••••••••

INBOUND PORT RULES

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

* Public inbound ports: ● None ○ Allow selected ports

Select inbound ports: Select one or more ports

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

SAVE MONEY

Save up to 49% with a license you already own using Azure Hybrid Benefit. Learn more

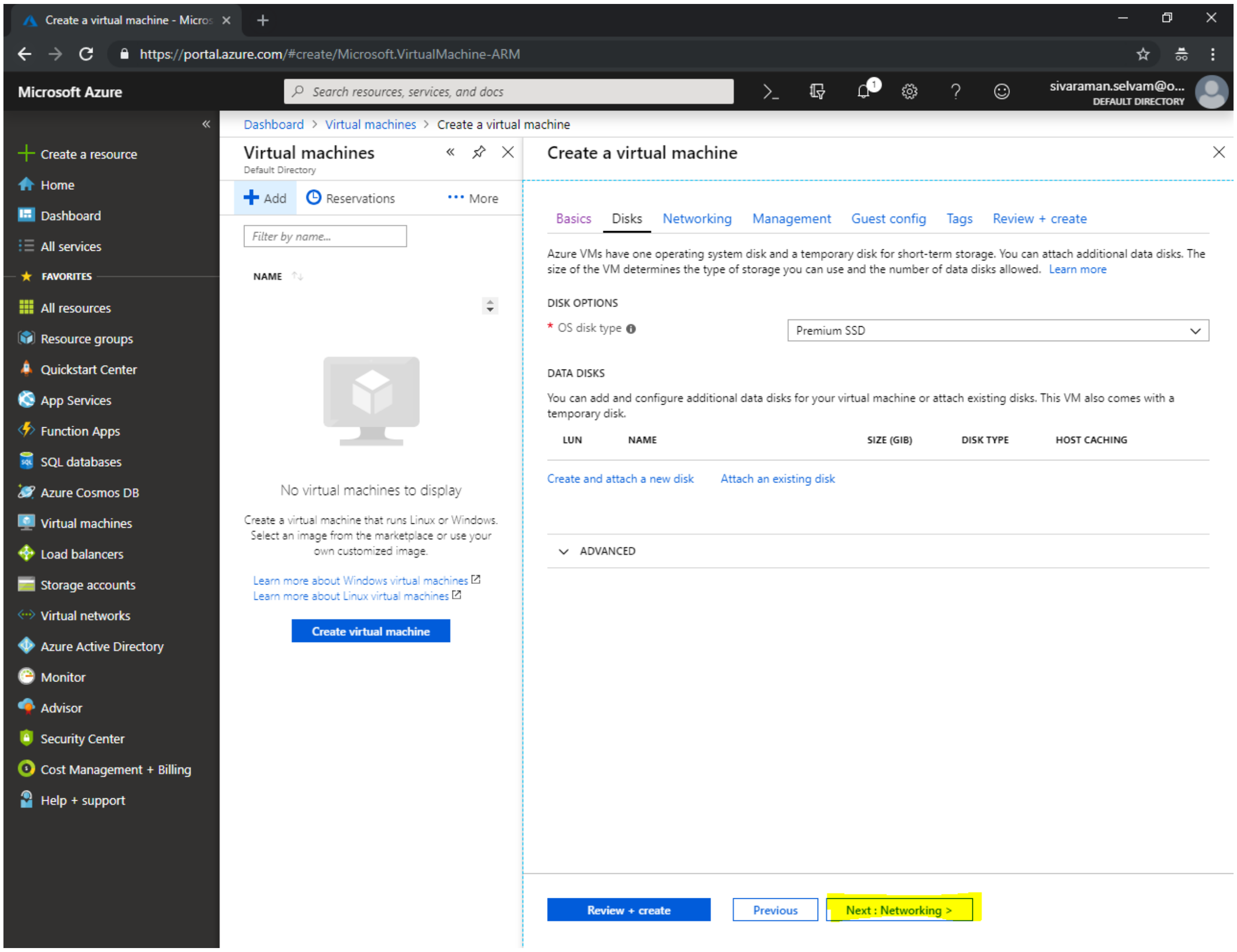
* Already have a Windows license? ● Yes ○ No

* License type: Windows Server

* Confirmation: ☑ I confirm I have an eligible Windows license with Software Assurance or Windows Server subscription to apply this Azure Hybrid Benefit.

Review Azure hybrid benefit compliance

Leave default and click **"Next : Networking >"**.



Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed.

DISK OPTIONS

* OS disk type: Premium SSD

DATA DISKS

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	NAME	SIZE (GIB)	DISK TYPE	HOST CACHING

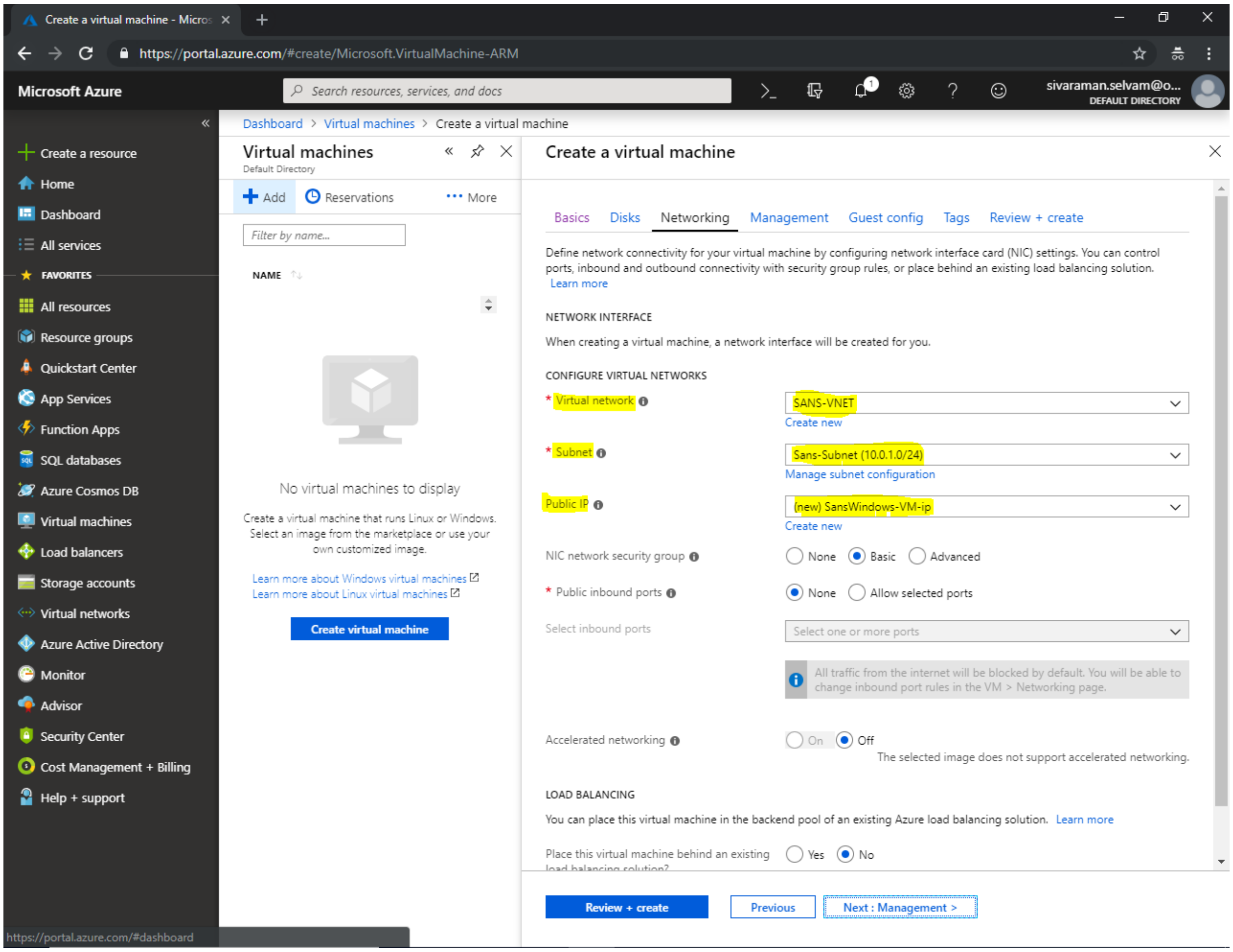
In **"Networking"**

At **"Configure virtual networks"**.

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

Ensure that **"Sans-Subnet (10.0.1.0/24)"**.

Public IP for Windows VM: (new) **"SansWindows-VM-Ip"**


Create a virtual machine - Micros ×
https://portal.azure.com/#create/Microsoft.VirtualMachine-ARM
Microsoft Azure
Search resources, services, and docs
sivaraman.selvam@o...
DEFAULT DIRECTORY
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
Quickstart Center
App Services
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
https://portal.azure.com/#dashboard
Dashboard > Virtual machines > Create a virtual machine
Virtual machines
Default Directory
Add
Reservations
More
Filter by name...
NAME
No virtual machines to display
Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.
Learn more about Windows virtual machines
Learn more about Linux virtual machines
Create virtual machine

Create a virtual machine

Basics | Disks | Networking | Management | Guest config | Tags | Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

NETWORK INTERFACE

When creating a virtual machine, a network interface will be created for you.

CONFIGURE VIRTUAL NETWORKS

* Virtual network: SANS-VNET
Create new

* Subnet: Sans-Subnet (10.0.1.0/24)
Manage subnet configuration

Public IP: (new) SansWindows-VM-ip
Create new

NIC network security group: ○ None ● Basic ○ Advanced

* Public inbound ports: ● None ○ Allow selected ports

Select inbound ports: Select one or more ports

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Accelerated networking: ○ On ● Off
The selected image does not support accelerated networking.

LOAD BALANCING

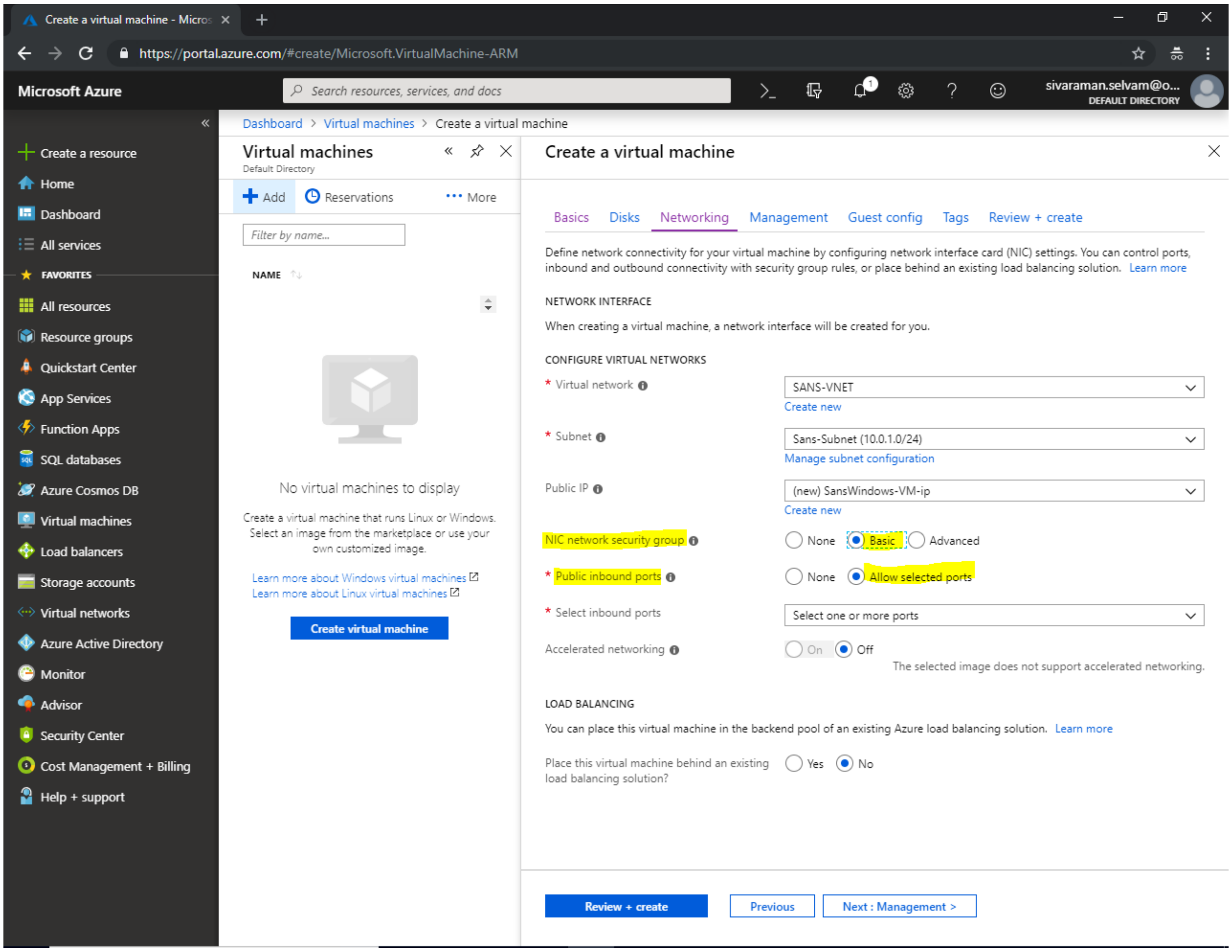
You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

Place this virtual machine behind an existing load balancing solution? ○ Yes ● No

Review + create | Previous | Next : Management >

Click **“NIC network security group”** as **“Basic”**.

Click **“Public inbound ports”** as **“Allowed selected ports”**.



No virtual machines to display

Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.

Learn more about Windows virtual machines
Learn more about Linux virtual machines

Create a virtual machine

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

NETWORK INTERFACE

When creating a virtual machine, a network interface will be created for you.

CONFIGURE VIRTUAL NETWORKS

- * Virtual network: SANS-VNET (Create new)
- * Subnet: Sans-Subnet (10.0.1.0/24) (Manage subnet configuration)
- Public IP: (new) SansWindows-VM-ip (Create new)
- NIC network security group: ○ None ● Basic ○ Advanced
- * Public inbound ports: ○ None ● Allow selected ports
- * Select inbound ports: Select one or more ports
- Accelerated networking: ○ On ● Off

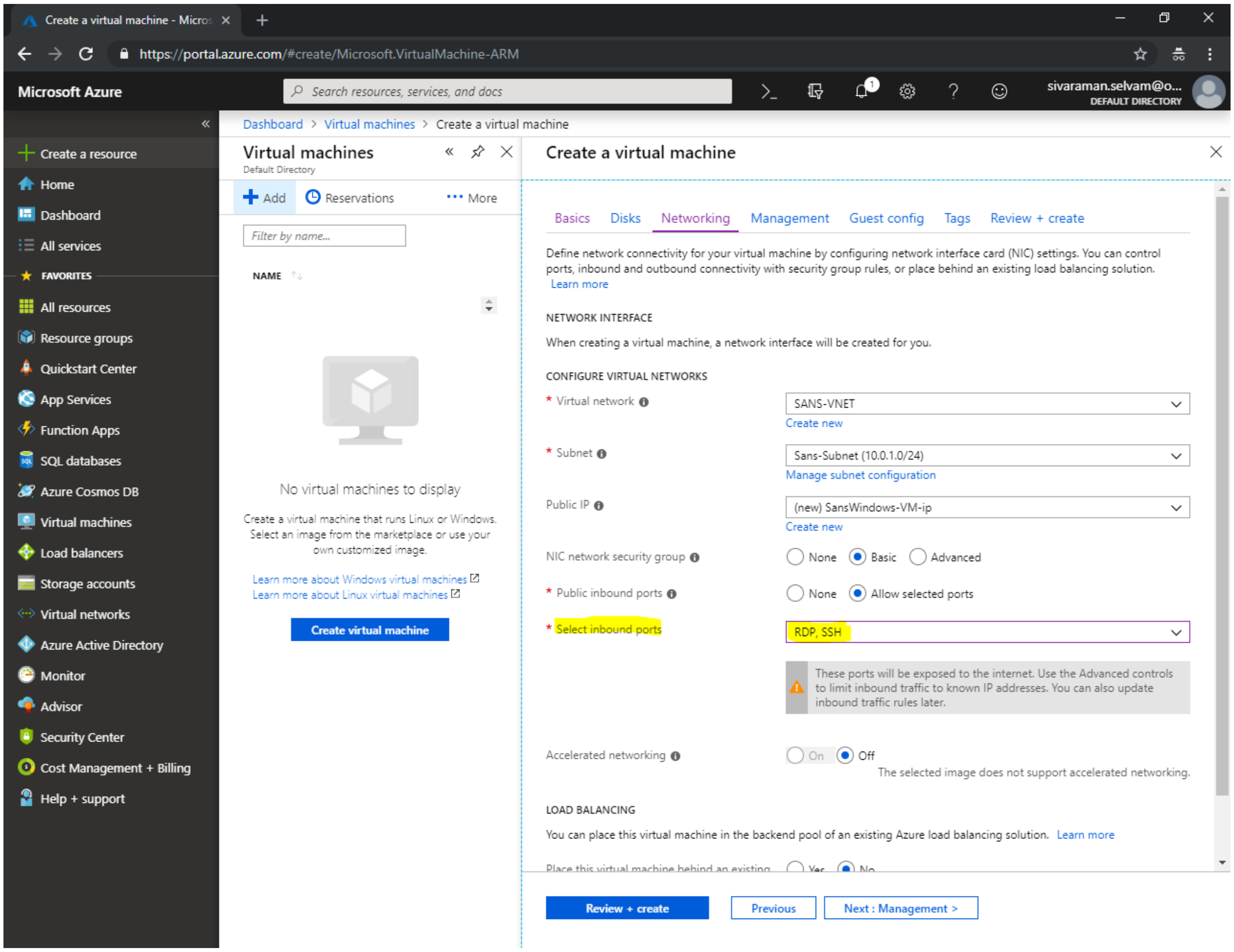
The selected image does not support accelerated networking.

LOAD BALANCING

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

Place this virtual machine behind an existing load balancing solution? ○ Yes ● No

In **“Select inbound ports”** Allow **“RDP and SSH”**.



No virtual machines to display

Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.

Learn more about Windows virtual machines
Learn more about Linux virtual machines

Create a virtual machine

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

NETWORK INTERFACE

When creating a virtual machine, a network interface will be created for you.

CONFIGURE VIRTUAL NETWORKS

* Virtual network: SANS-VNET
Create new

* Subnet: Sans-Subnet (10.0.1.0/24)
Manage subnet configuration

Public IP: (new) SansWindows-VM-ip
Create new

NIC network security group: ○ None ● Basic ○ Advanced

* Public inbound ports: ○ None ● Allow selected ports

* Select inbound ports: RDP, SSH

These ports will be exposed to the internet. Use the Advanced controls to limit inbound traffic to known IP addresses. You can also update inbound traffic rules later.

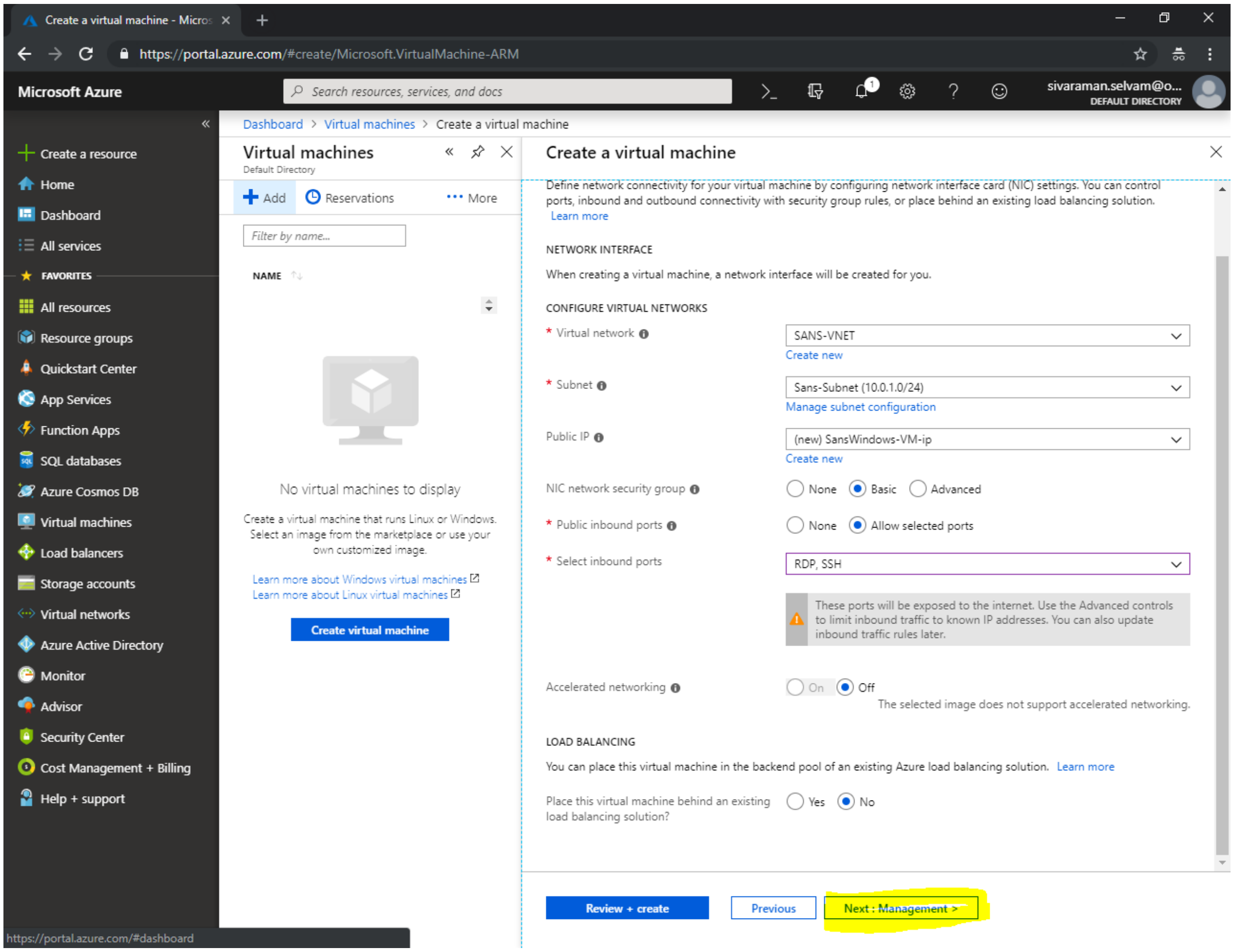
Accelerated networking: ○ On ● Off
The selected image does not support accelerated networking.

LOAD BALANCING

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

Place this virtual machine behind an existing ... ○ Yes ● No

Click **“Next : Management >”**.



Create a virtual machine

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

NETWORK INTERFACE

When creating a virtual machine, a network interface will be created for you.

CONFIGURE VIRTUAL NETWORKS

* Virtual network: SANS-VNET (Create new)
* Subnet: Sans-Subnet (10.0.1.0/24) (Manage subnet configuration)
Public IP: (new) SansWindows-VM-ip (Create new)
NIC network security group: ○ None ● Basic ○ Advanced
* Public inbound ports: ○ None ● Allow selected ports
* Select inbound ports: RDP, SSH

These ports will be exposed to the internet. Use the Advanced controls to limit inbound traffic to known IP addresses. You can also update inbound traffic rules later.

Accelerated networking: ○ On ● Off

The selected image does not support accelerated networking.

LOAD BALANCING

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

Place this virtual machine behind an existing load balancing solution? ○ Yes ● No

Virtual machines

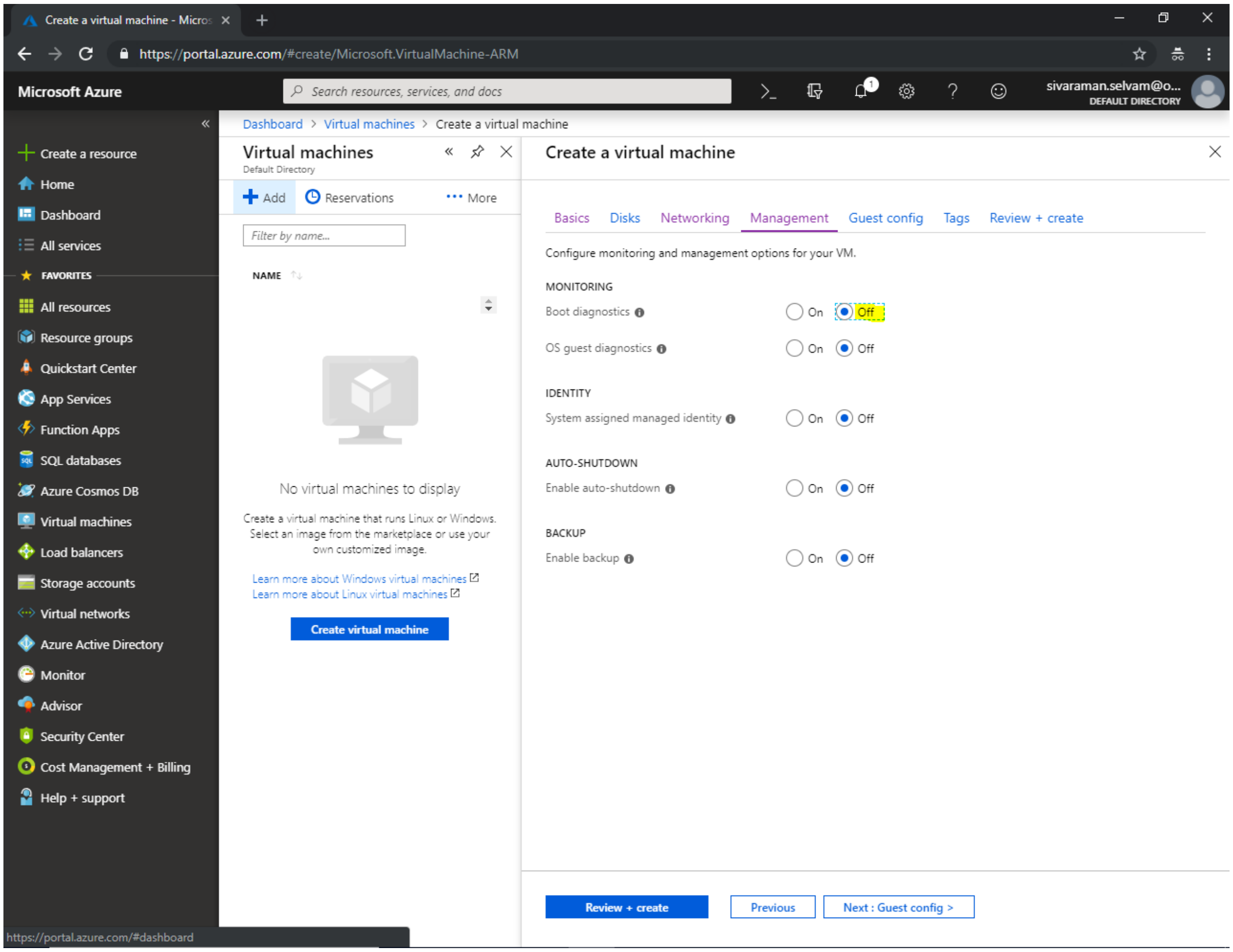
Default Directory

No virtual machines to display

Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.

Learn more about Windows virtual machines
Learn more about Linux virtual machines

In Management, click **“Boot diagnostics”** as **“off”**.



Create a virtual machine - Micros
https://portal.azure.com/#create/Microsoft.VirtualMachine-ARM
Microsoft Azure
Search resources, services, and docs
sivaraman.selvam@o...
DEFAULT DIRECTORY
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
Quickstart Center
App Services
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
Dashboard > Virtual machines > Create a virtual machine
Virtual machines
Default Directory
Add
Reservations
More
Filter by name...
NAME
No virtual machines to display
Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.
Learn more about Windows virtual machines
Learn more about Linux virtual machines
Create virtual machine
https://portal.azure.com/#dashboard

Create a virtual machine

Basics | Disks | Networking | Management | Guest config | Tags | Review + create

Configure monitoring and management options for your VM.

MONITORING

Boot diagnostics ○ On ● Off

OS guest diagnostics ○ On ● Off

IDENTITY

System assigned managed identity ○ On ● Off

AUTO-SHUTDOWN

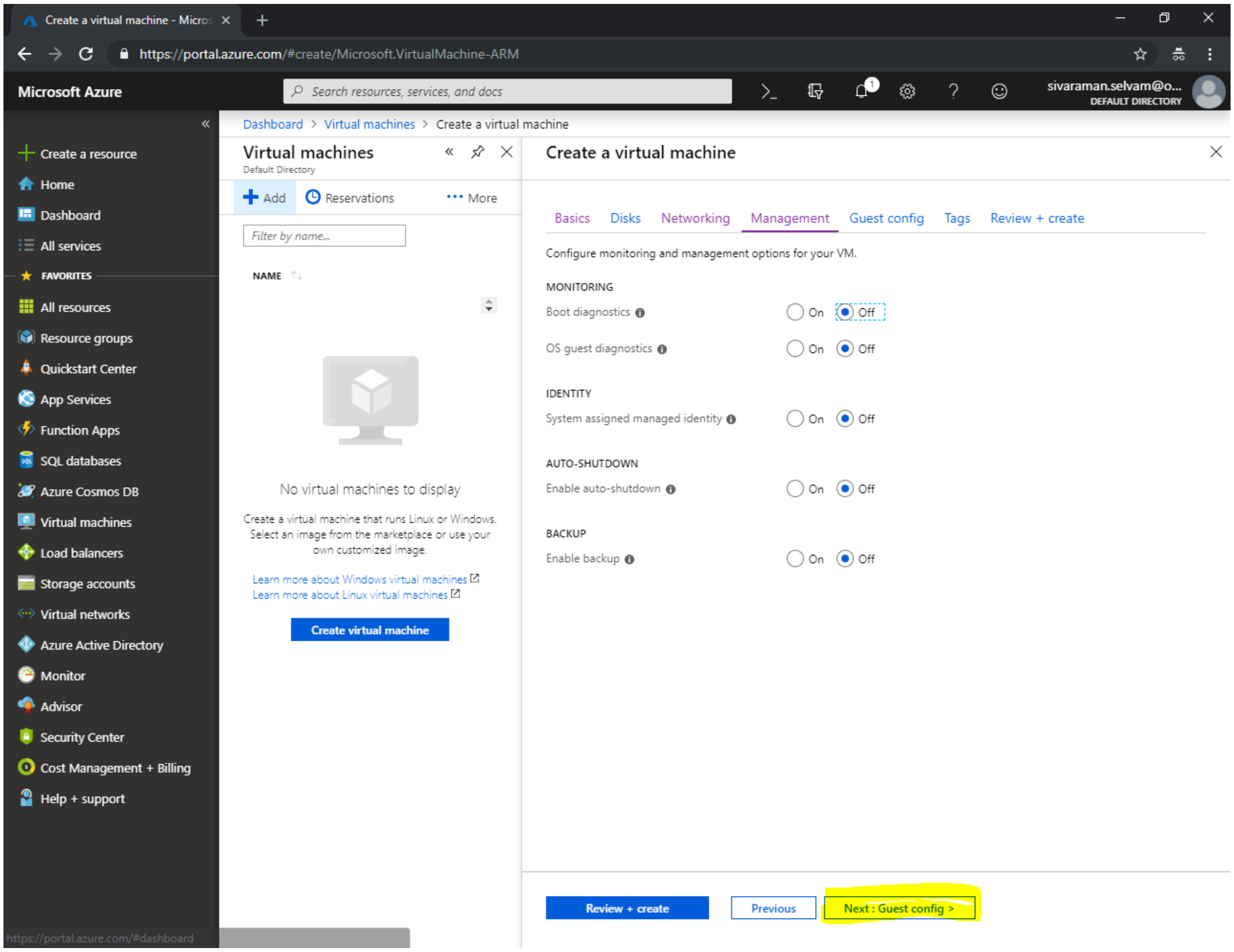
Enable auto-shutdown ○ On ● Off

BACKUP

Enable backup ○ On ● Off

Review + create
Previous
Next : Guest config >

Click **“Next : Guest config >”**.



Configure monitoring and management options for your VM.

MONITORING

Boot diagnostics ○ On ● Off

OS guest diagnostics ○ On ● Off

IDENTITY

System assigned managed identity ○ On ● Off

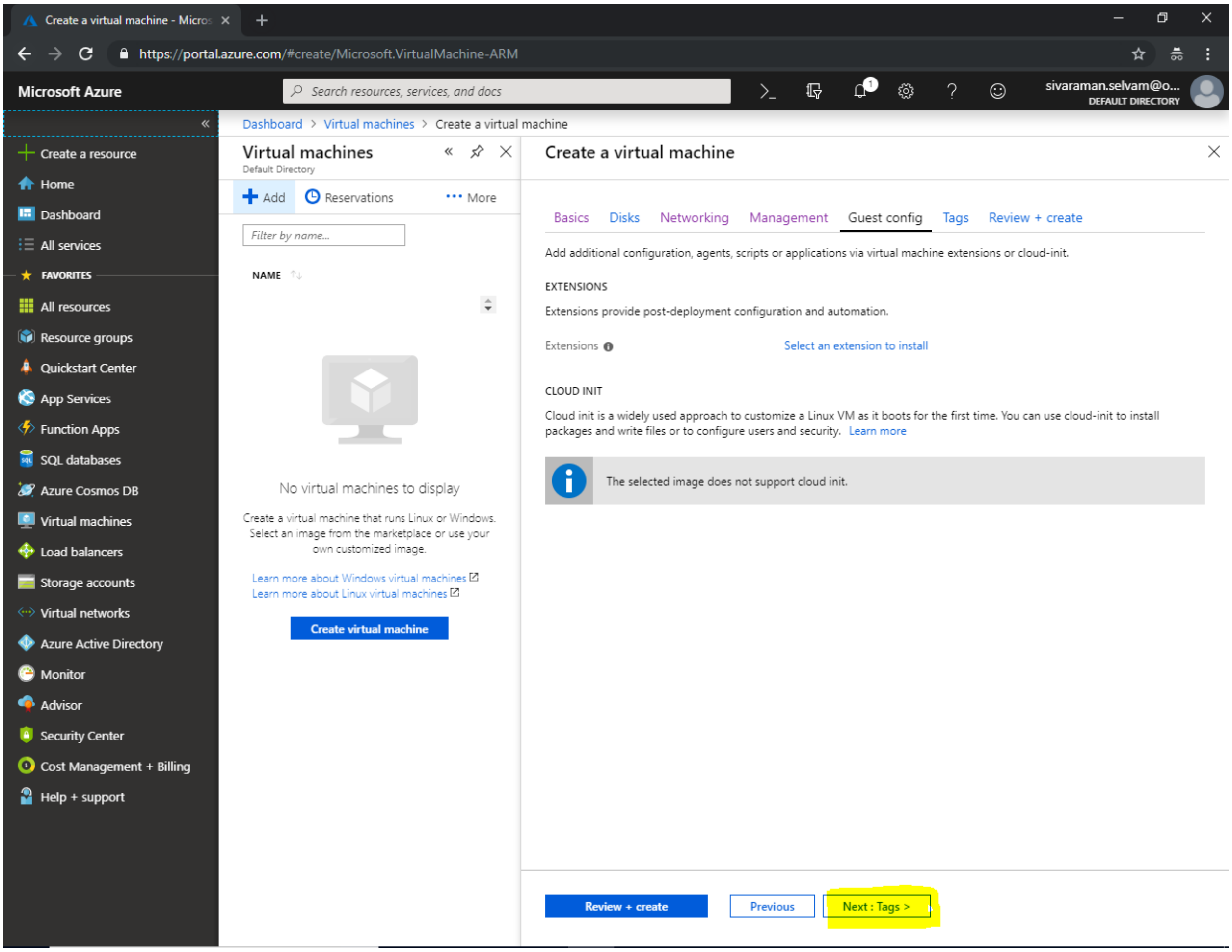
AUTO-SHUTDOWN

Enable auto-shutdown ○ On ● Off

BACKUP

Enable backup ○ On ● Off

Leave default and click **"Next : Tags >"**.



Create a virtual machine

Basics Disks Networking Management Guest config Tags Review + create

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

EXTENSIONS

Extensions provide post-deployment configuration and automation.

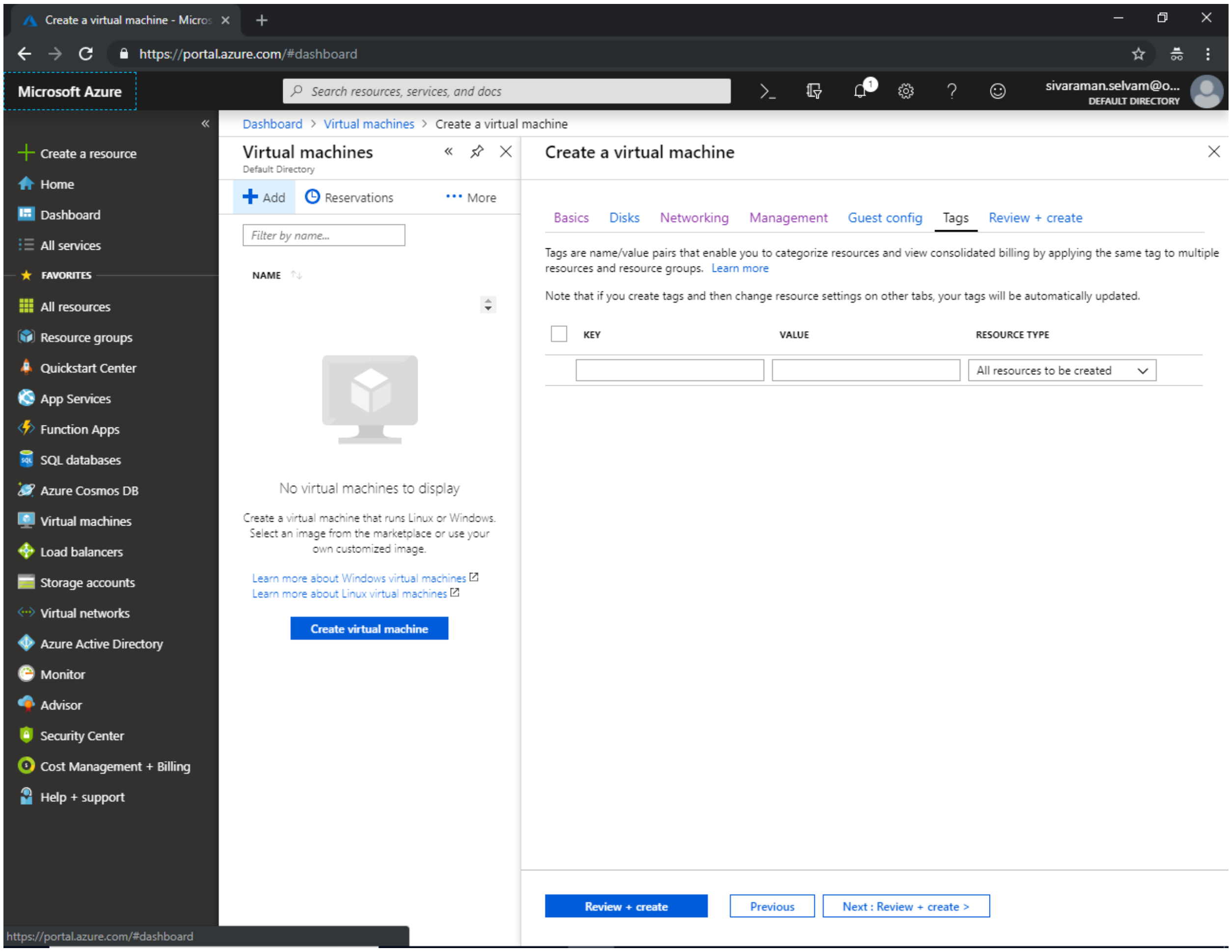
Extensions: Select an extension to install

CLOUD INIT

Cloud init is a widely used approach to customize a Linux VM as it boots for the first time. You can use cloud-init to install packages and write files or to configure users and security. Learn more

The selected image does not support cloud init.

Leave default and click **"Next : Review + Create >"**.



No virtual machines to display

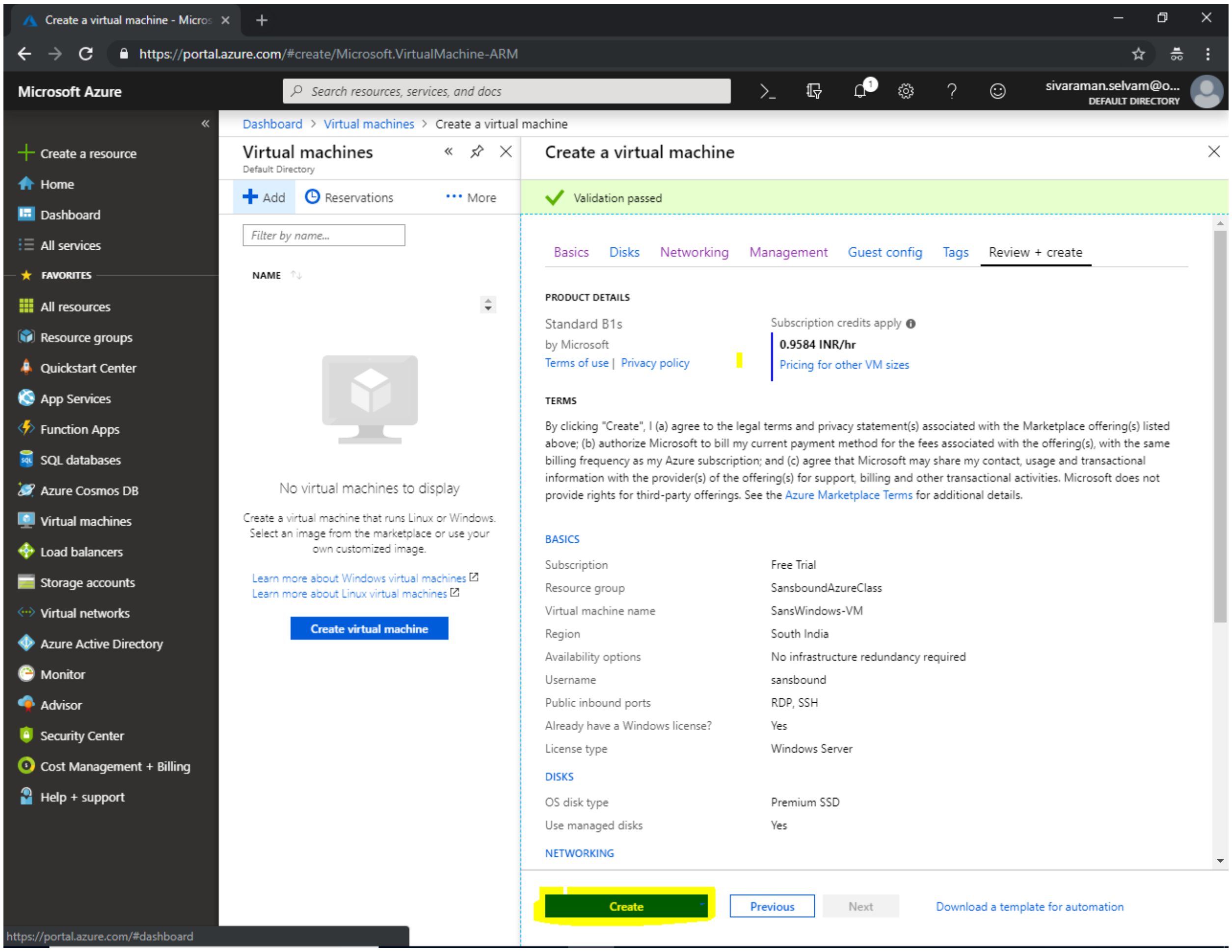
Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.

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

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

□	KEY	VALUE	RESOURCE TYPE
			All resources to be created

Click **"Create"**.



Create a virtual machine

Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.

✓ Validation passed

PRODUCT DETAILS

Standard B1s
by Microsoft
Terms of use | Privacy policy

Subscription credits apply
0.9584 INR/hr
Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

BASICS

Subscription	Free Trial
Resource group	SansboundAzureClass
Virtual machine name	SansWindows-VM
Region	South India
Availability options	No infrastructure redundancy required
Username	sansbound
Public inbound ports	RDP, SSH
Already have a Windows license?	Yes
License type	Windows Server

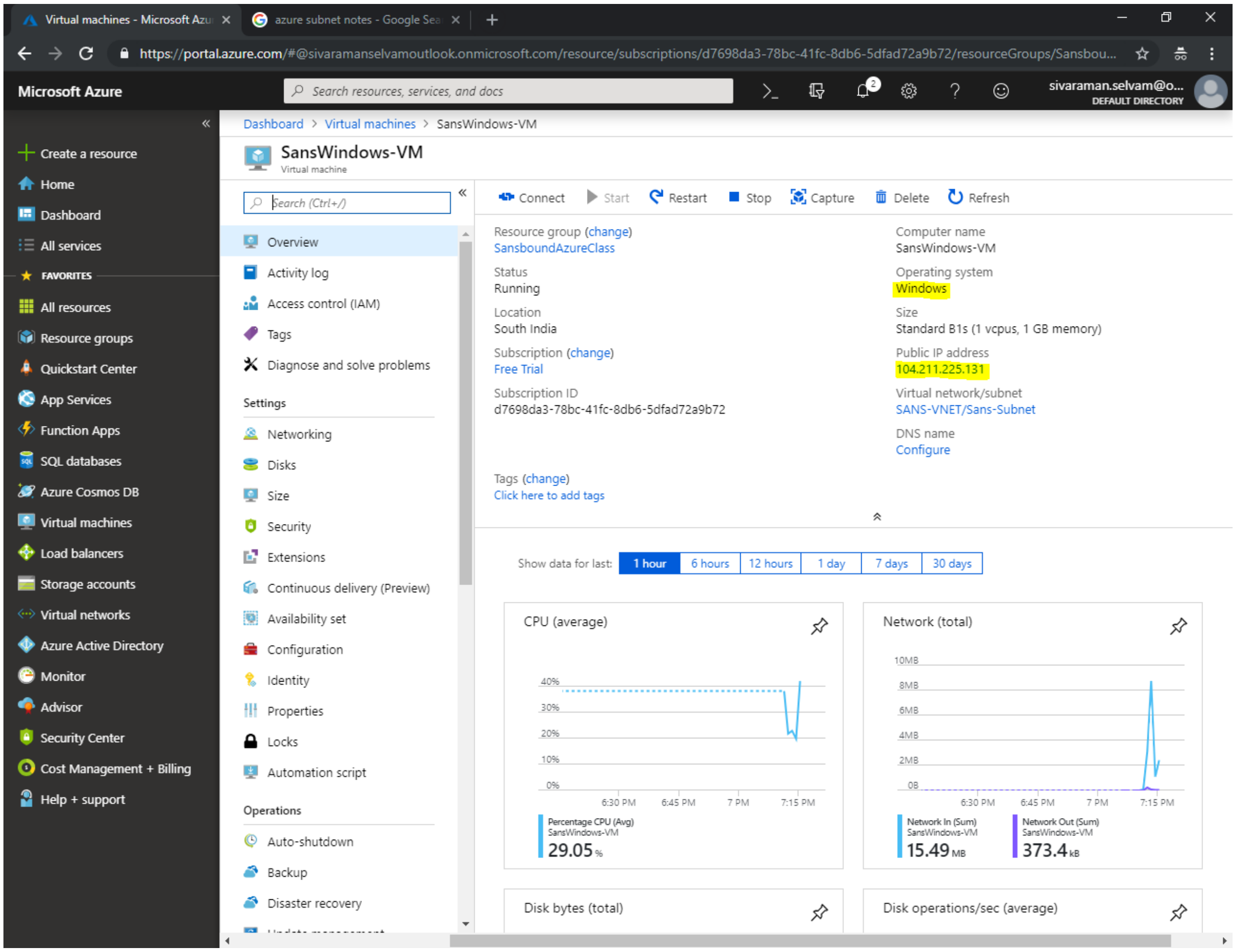
DISKS

OS disk type	Premium SSD
Use managed disks	Yes

NETWORKING

Once Virtual machine deployed successfully go the Virtual machine which you have created.

Note the public IP address of Windows Server.



https://portal.azure.com/#@sivaramanselvamoutlook.onmicrosoft.com/resource/subscriptions/d7698da3-78bc-41fc-8db6-5dfad72a9b72/resourceGroups/Sansbou...

Dashboard > Virtual machines > SansWindows-VM

SansWindows-VM
Virtual machine

Resource group (change)
SansboundAzureClass

Status
Running

Location
South India

Subscription (change)
Free Trial

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

Tags (change)
Click here to add tags

Computer name
SansWindows-VM

Operating system
Windows

Size
Standard B1s (1 vcpus, 1 GB memory)

Public IP address
104.211.225.131

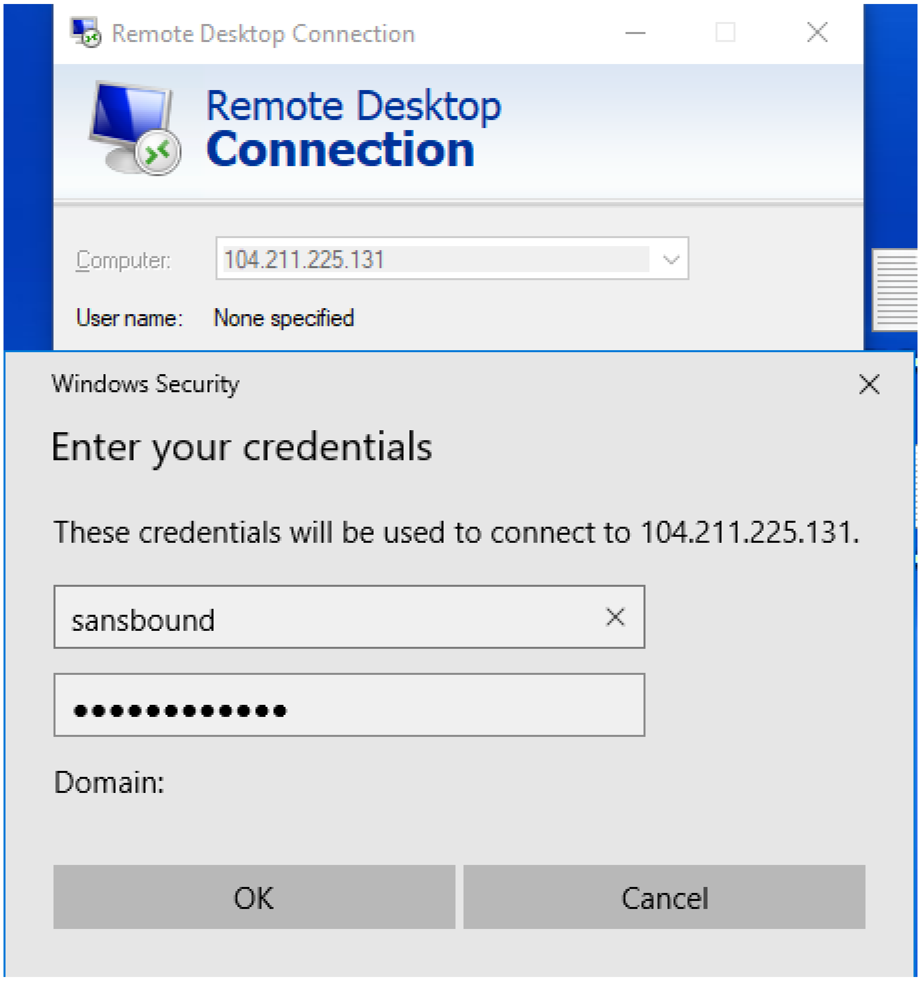
Virtual network/subnet
SANS-VNET/Sans-Subnet

DNS name
Configure

Type “mstsc” in Run box and click “OK”.

Type the public IP address of Windows Server in mstsc console and click “Connect”.

Provide the login credentials of Windows server.



Computer: 104.211.225.131

User name: None specified

Enter your credentials

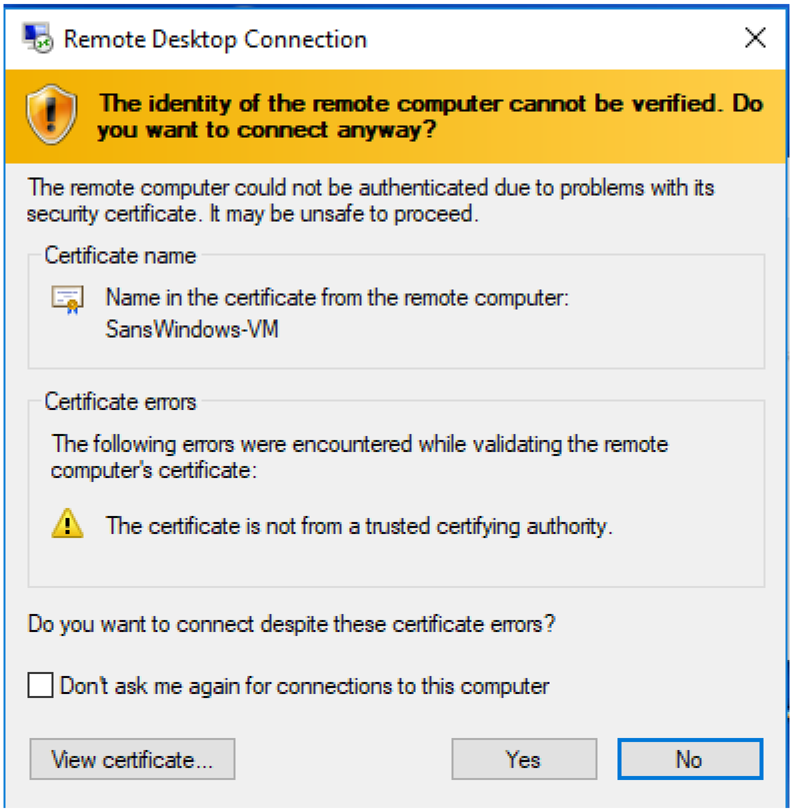
These credentials will be used to connect to 104.211.225.131.

sansbound

●●●●●●●●●●●●●

Domain:

Click **"Yes"**.



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
SansWindows-VM

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

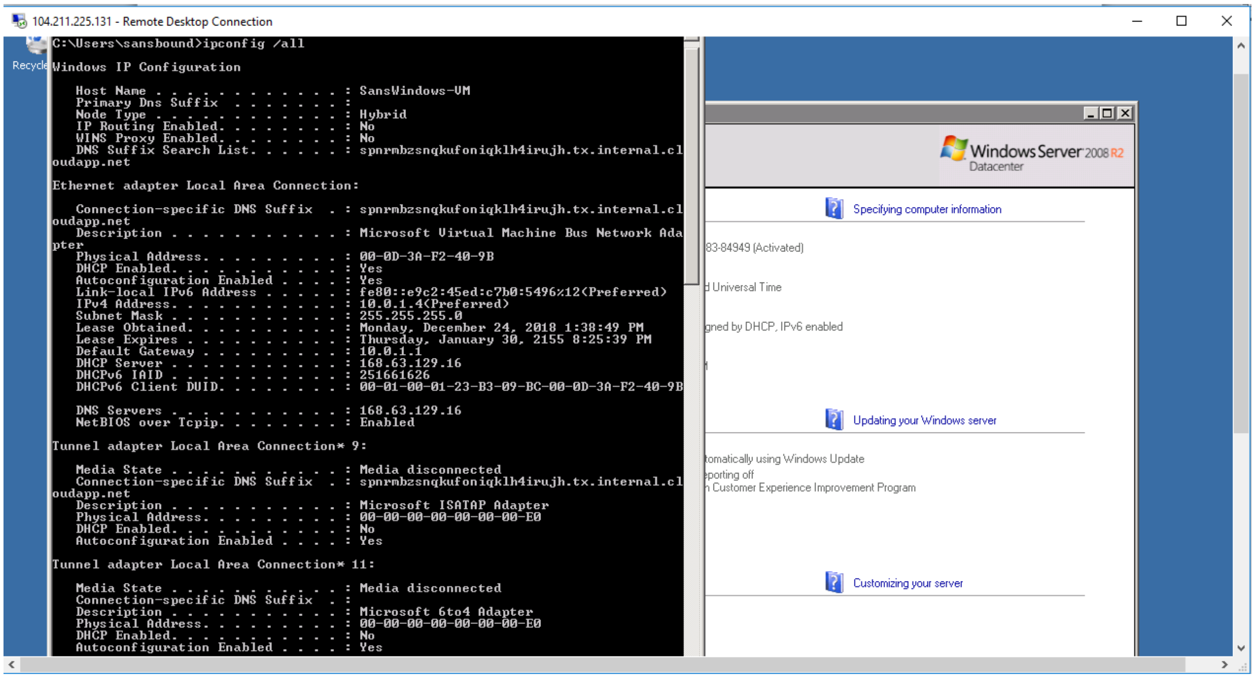
Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

In Windows Server, in command prompt type “ipconfig /all” and press “Enter”.

You will get IP details of Windows Server.

We have got IP address as 10.0.1.4 (Subnet which we have designed).


104.211.225.131 - Remote Desktop Connection
Recycle
Windows Server 2008 R2
Datacenter
Specifying computer information
83-84949 (Activated)
d Universal Time
gned by DHCP, IPv6 enabled
Updating your Windows server
tomatically using Windows Update
eporting off
n Customer Experience Improvement Program
Customizing your server

```
C:\Users\sansbound>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : SansWindows-VM
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : spnrmbzsnqkufoniqklh4irujh.tx.internal.cl
oudapp.net

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : spnrmbzsnqkufoniqklh4irujh.tx.internal.cl
oudapp.net
   Description . . . . . . . . . . . : Microsoft Virtual Machine Bus Network Ada
pter
   Physical Address. . . . . . . . . : 00-0D-3A-F2-40-9B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::e9c2:45ed:c7b0:5496%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.1.4(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, December 24, 2018 1:38:49 PM
   Lease Expires . . . . . . . . . . : Thursday, January 30, 2155 8:25:39 PM
   Default Gateway . . . . . . . . . : 10.0.1.1
   DHCP Server . . . . . . . . . . . : 168.63.129.16
   DHCPv6 IAID . . . . . . . . . . . : 251661626
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-23-B3-09-BC-00-0D-3A-F2-40-9B

   DNS Servers . . . . . . . . . . . : 168.63.129.16
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : spnrmbzsnqkufoniqklh4irujh.tx.internal.cl
oudapp.net
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Tunnel adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft 6to4 Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```