**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](https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits?toc=%2fazure%2fvirtual-network%2ftoc.json#networking-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](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services#services-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](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings?toc=%2fazure%2fvirtual-network%2ftoc.json#gwsub).
* 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](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-vnet-plan-design-arm#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](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview), 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](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-vnet-plan-design-arm#traffic-filtering).

**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:



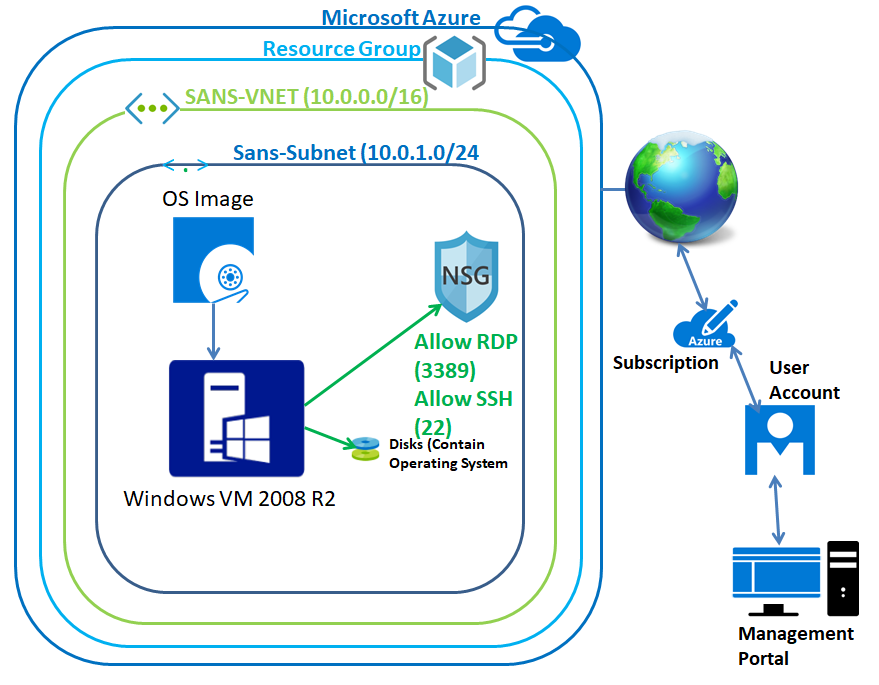
**Azure Locations:** <https://azure.microsoft.com/en-in/global-infrastructure/locations/>

**Resource Group:**

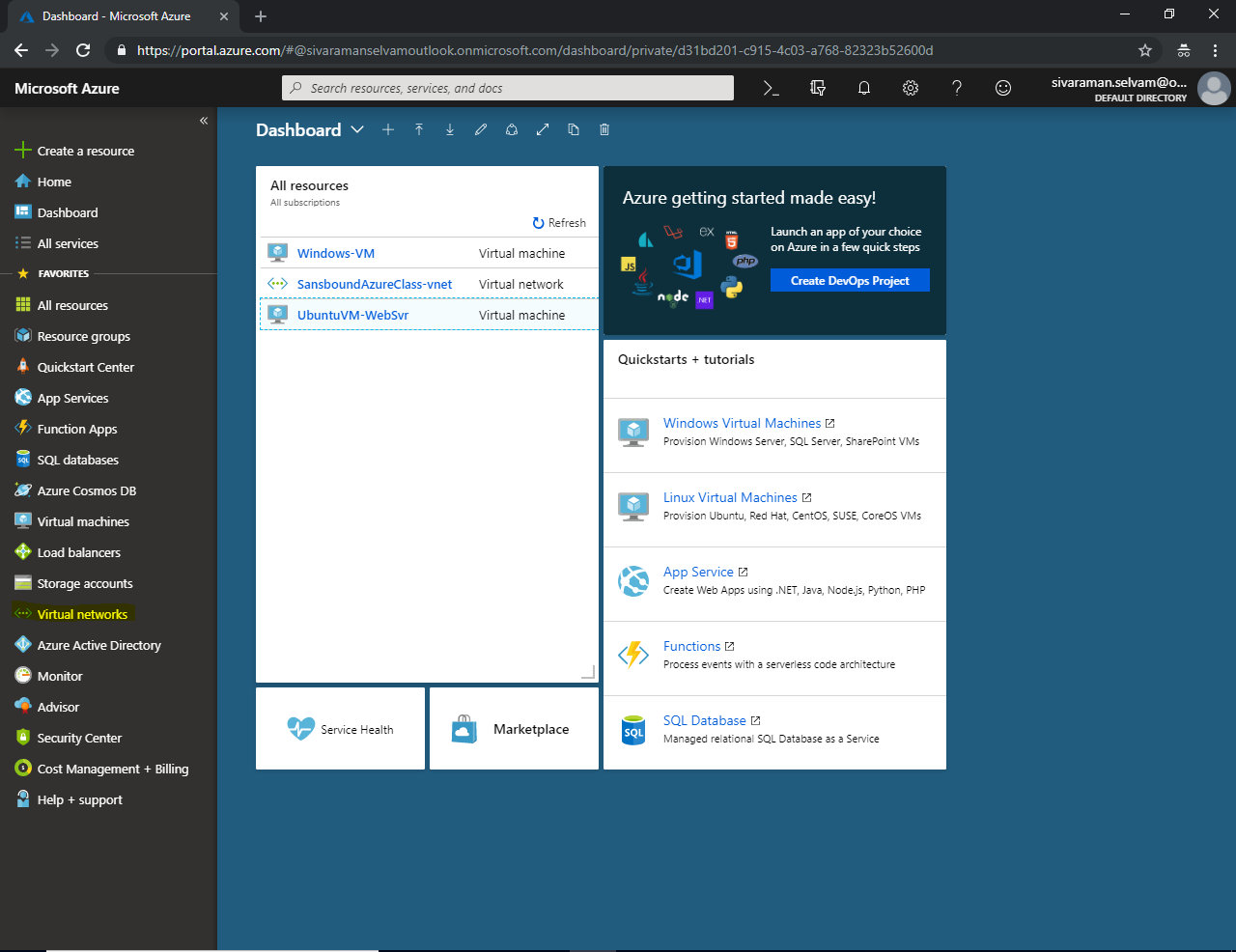
Since the introduction of the Azure preview portal in 2014, resource groups are automatically created for virtual machines, databases, and other assets, no matter how they are added to the cloud fabric. Resource groups provide a way to monitor, control access, provision and manage billing for collections 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](https://manage.windowsazure.com/), and select **Switch to new portal** from the menu. You can log in directly to the [new portal](https://portal.azure.com/).

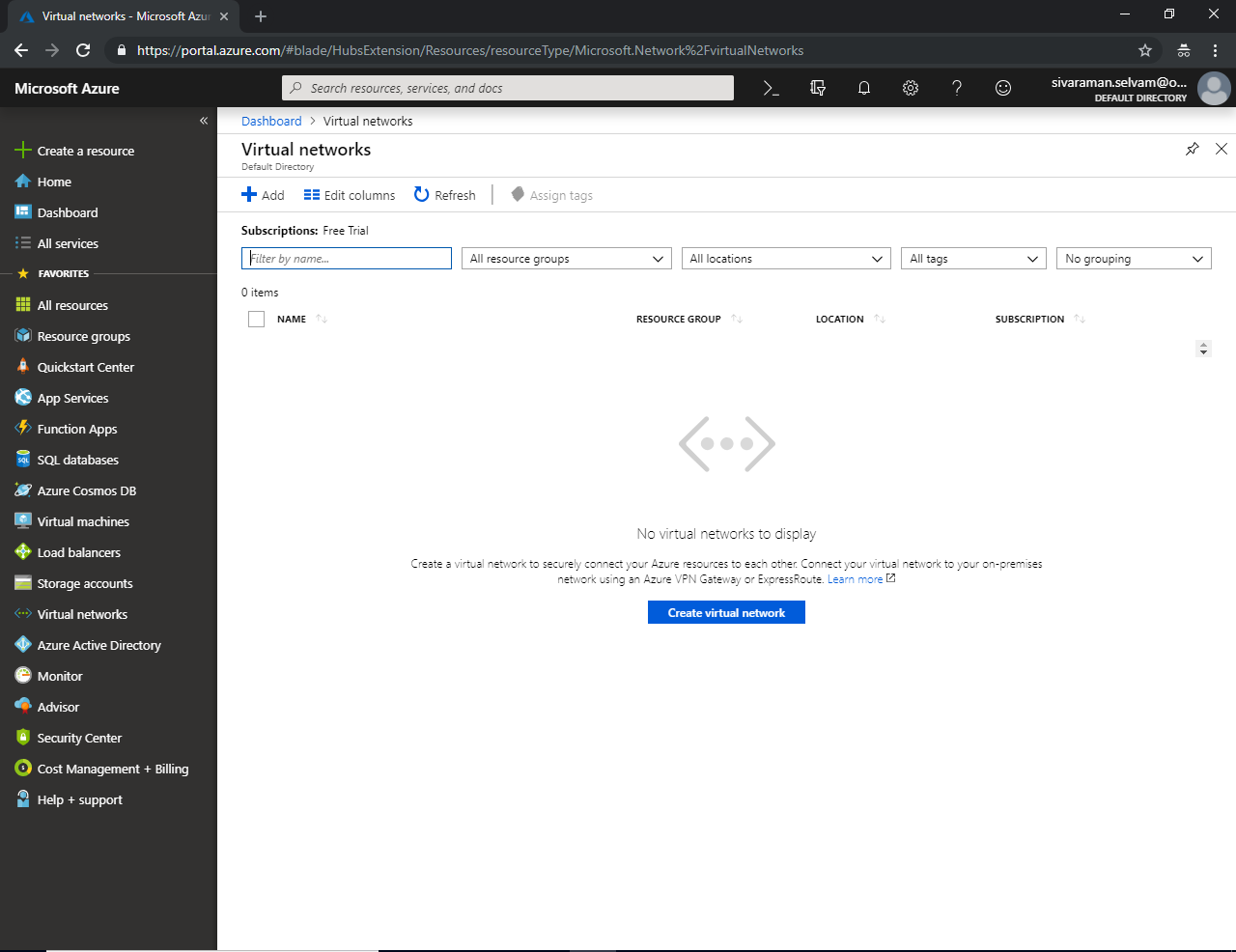
**Topology**



In Azure portal, click “Virtual networks”.

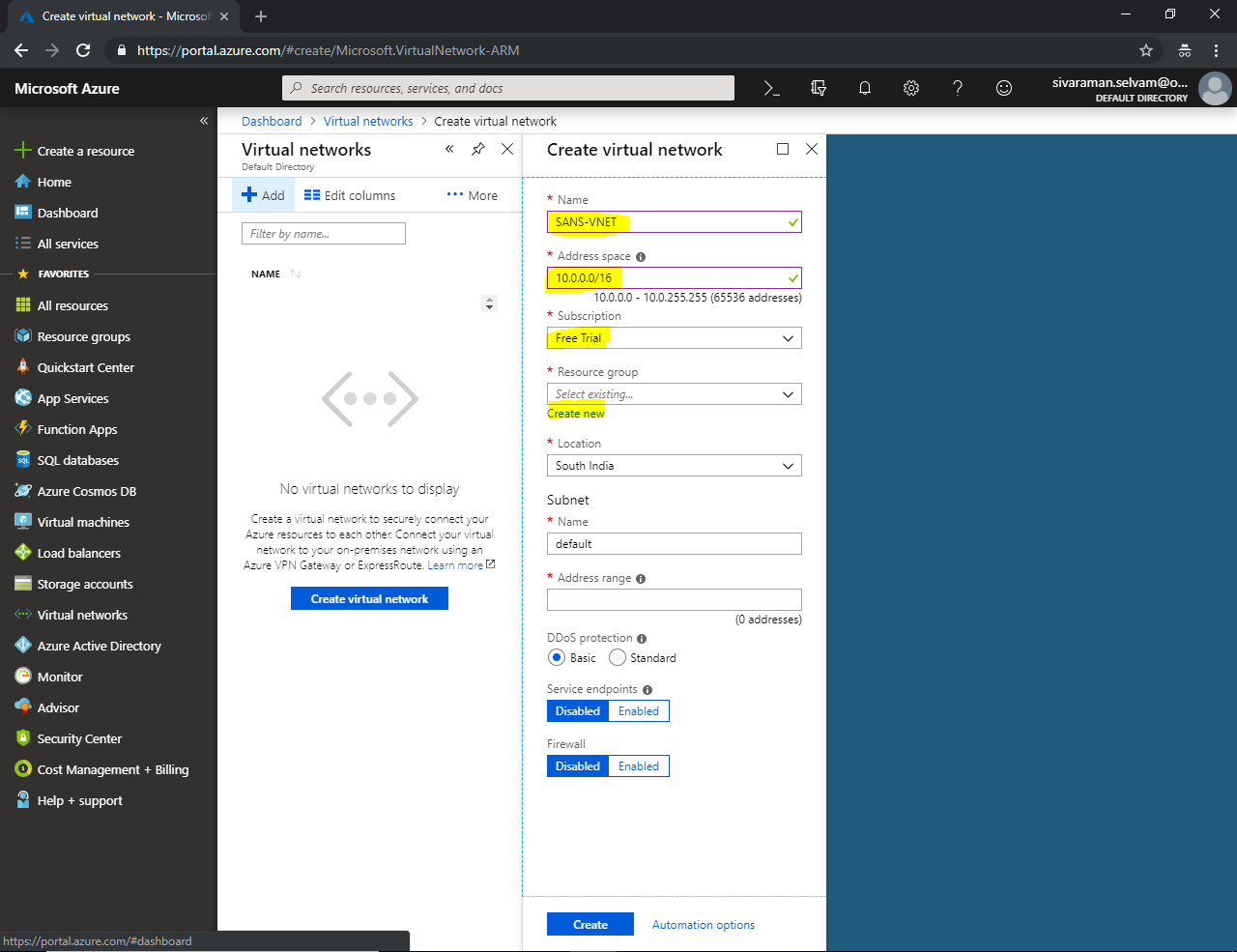


In **“Virtual networks”** click **“Add”.**

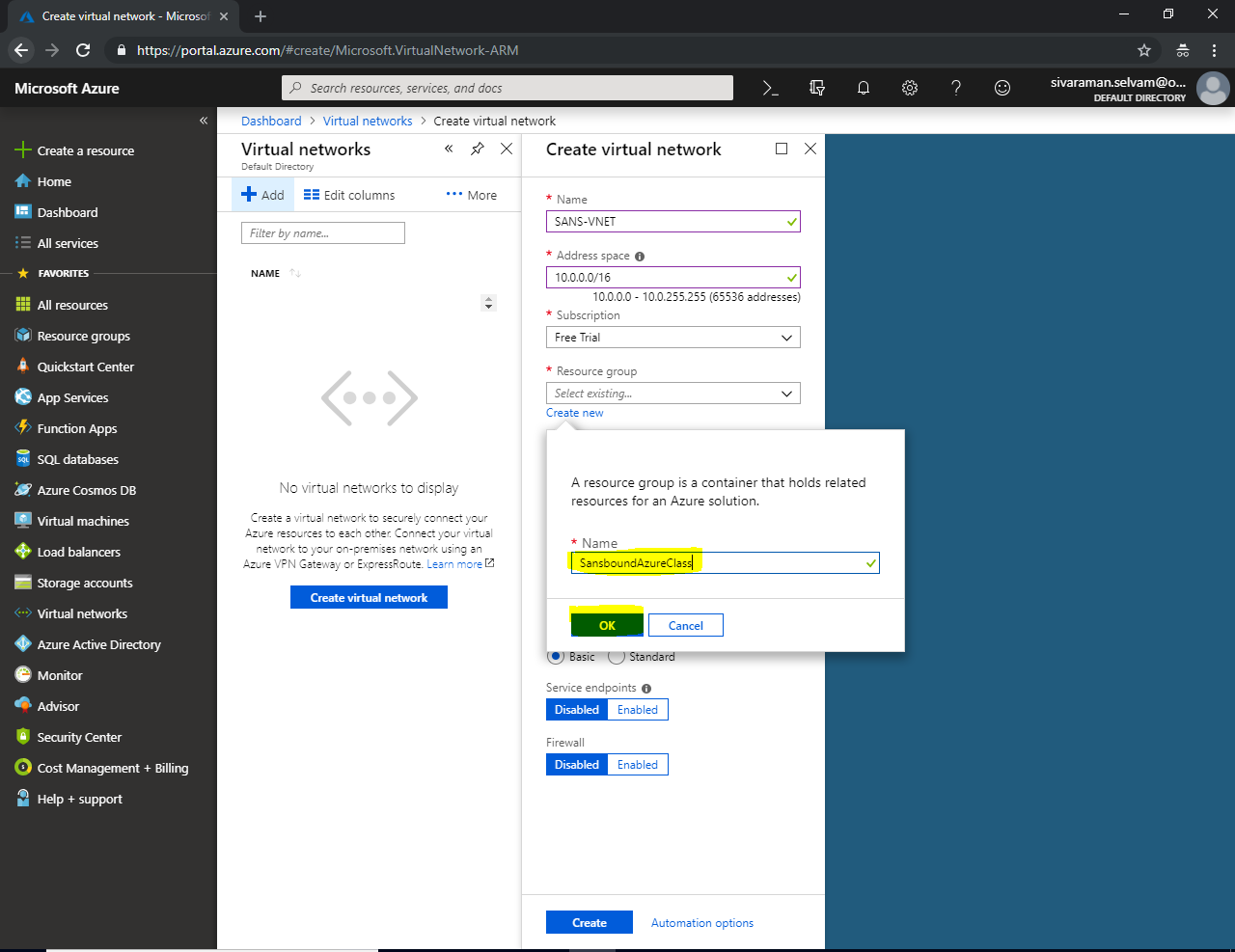


While creating virtual network, it has required the virtual network name specify it as “SANS-VNET” and specify the address space as **10.0.0.0/16,** select **“Subscription”** as **“Free Trial”.**

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



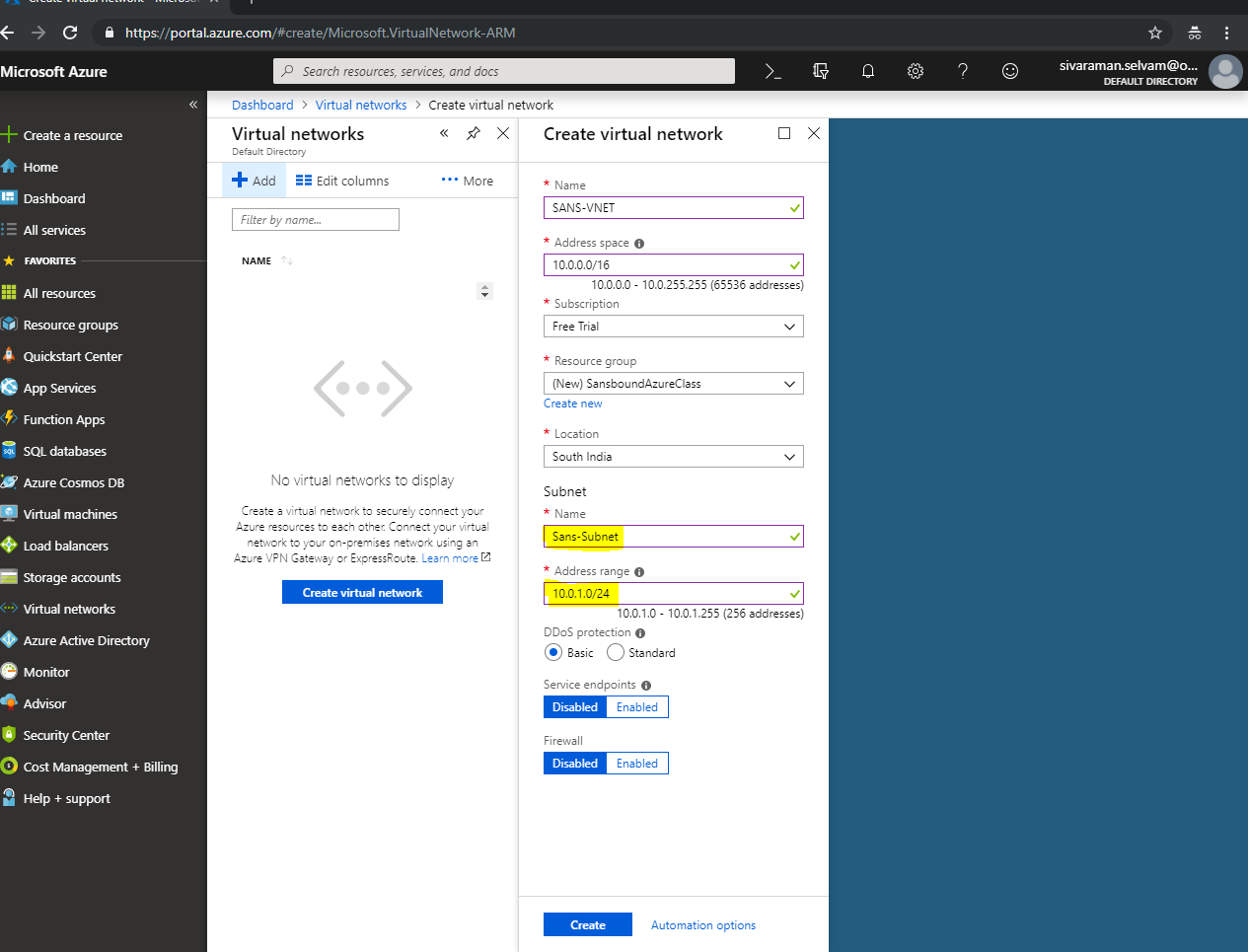
In Resource Group name type “SansboundAzureClass” and click “Ok”.



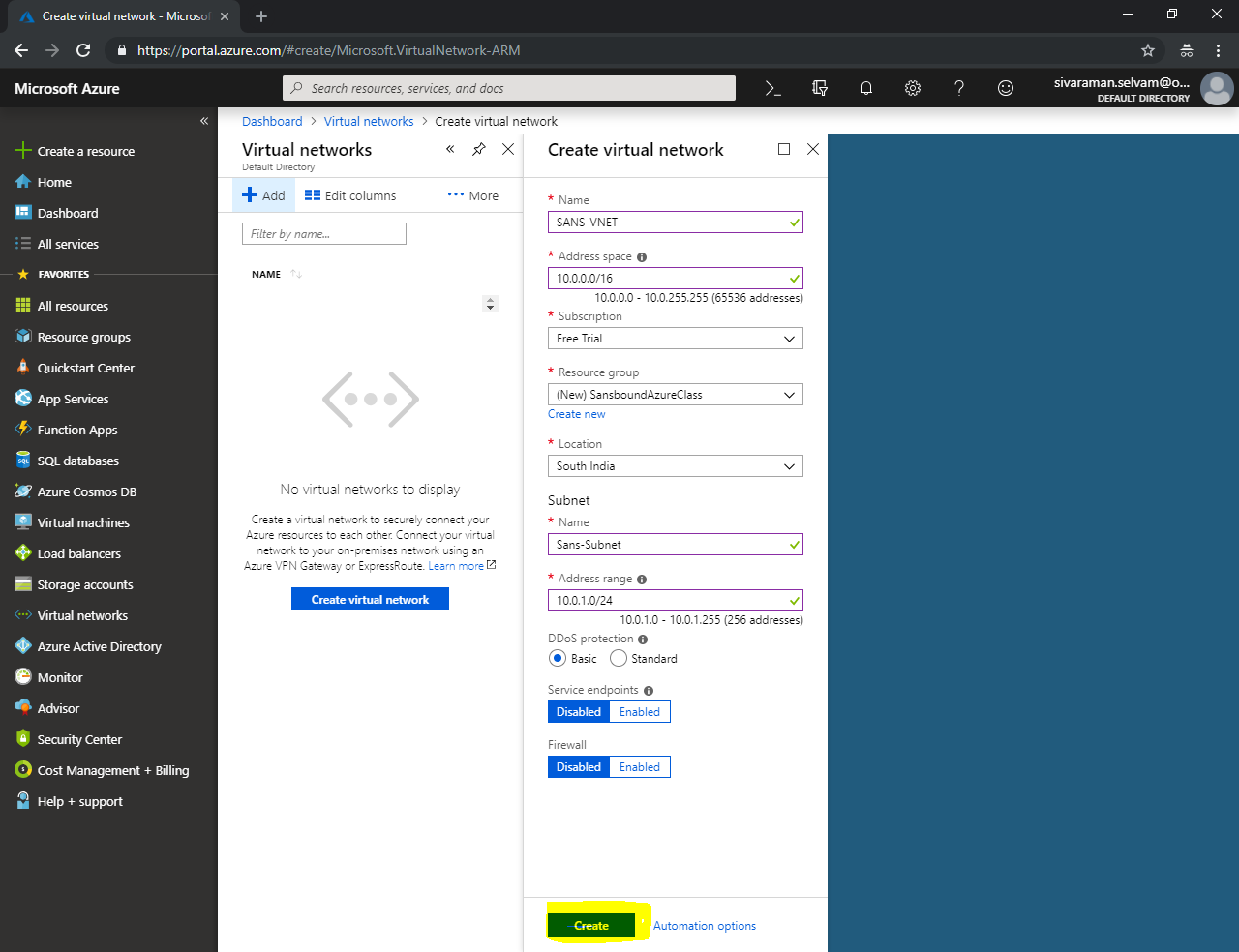
In **“Subnet”**,

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

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



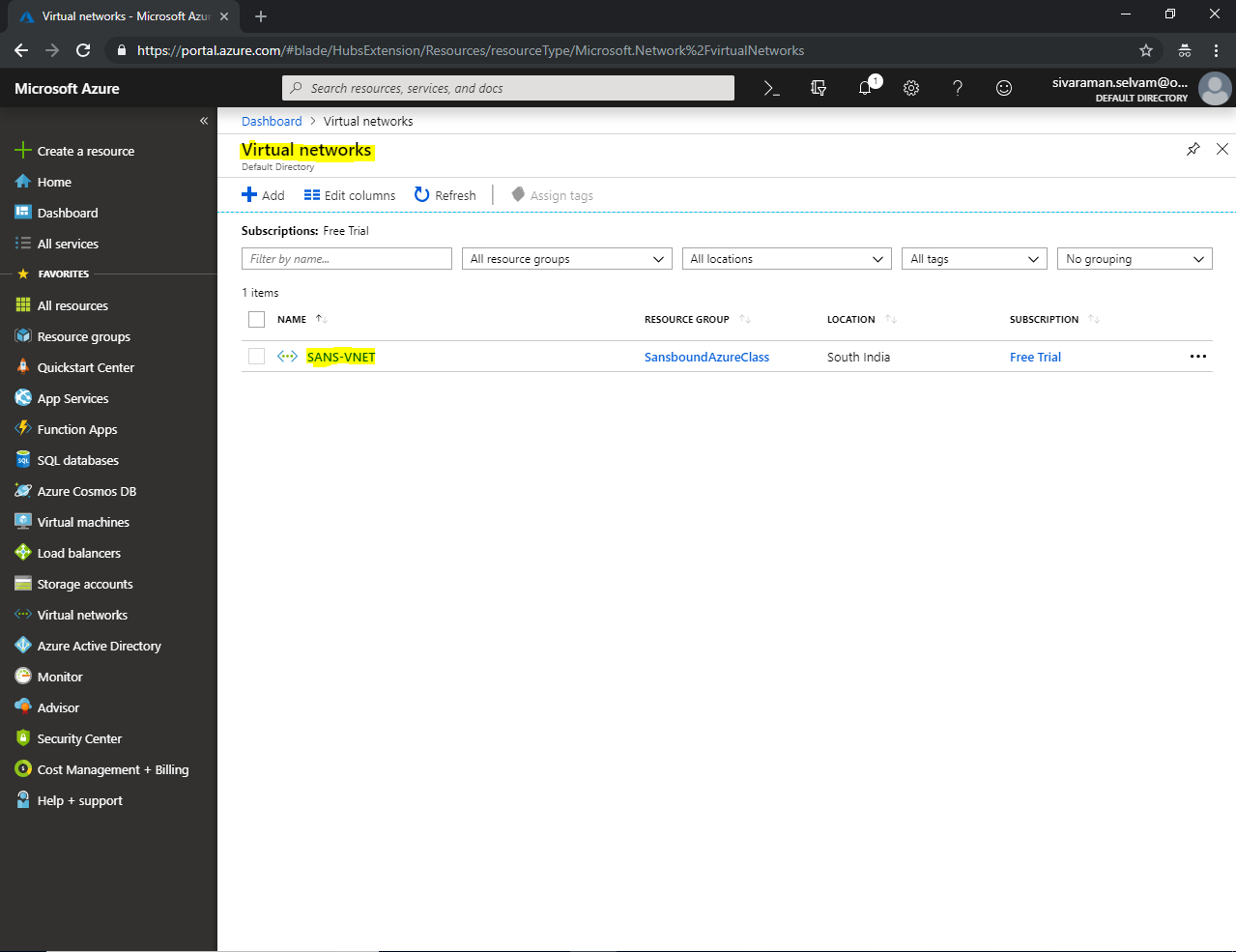
Click **“Create”.**



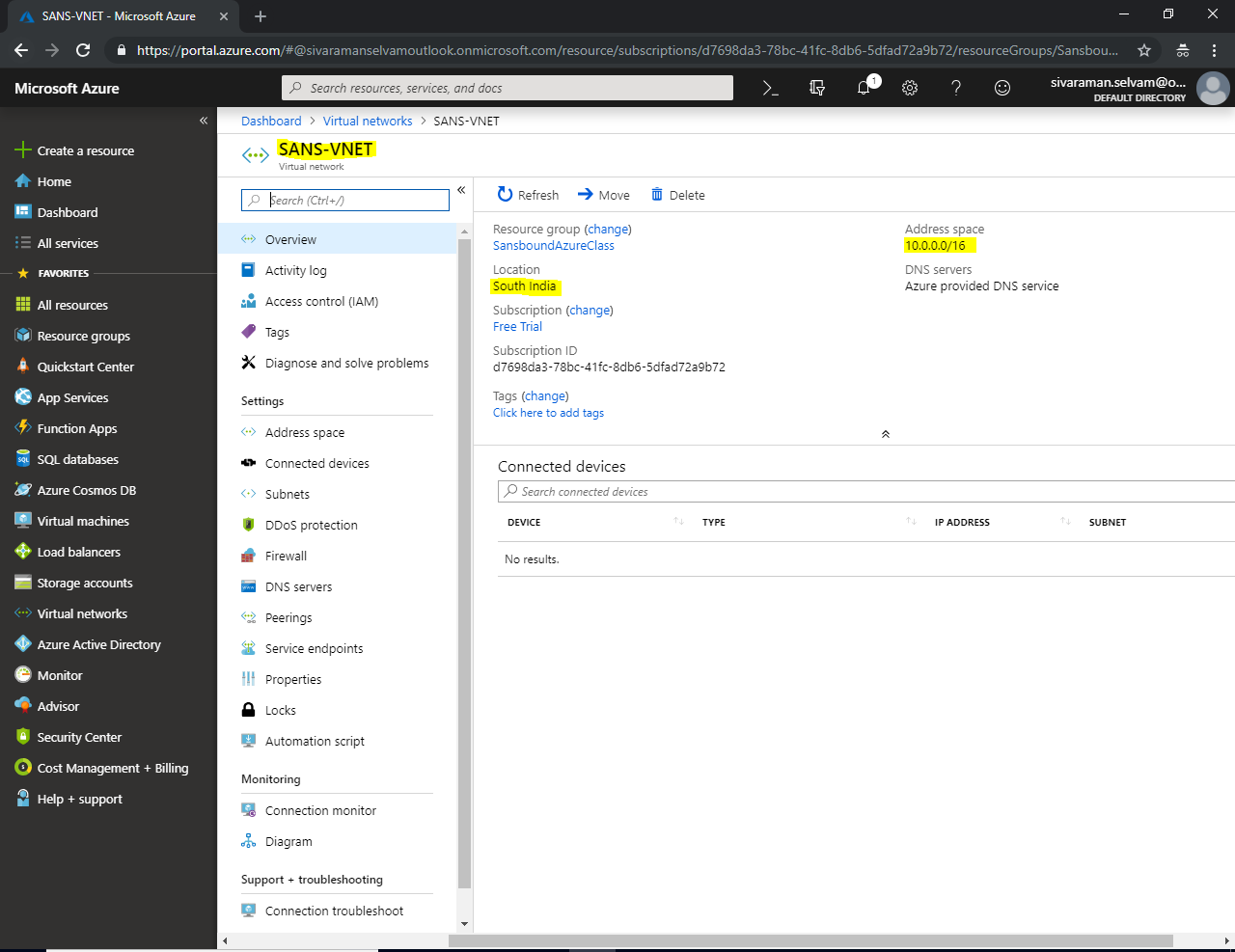
In “Virtual Networks”, click “Refresh” to view the newly created Vnet.

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

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

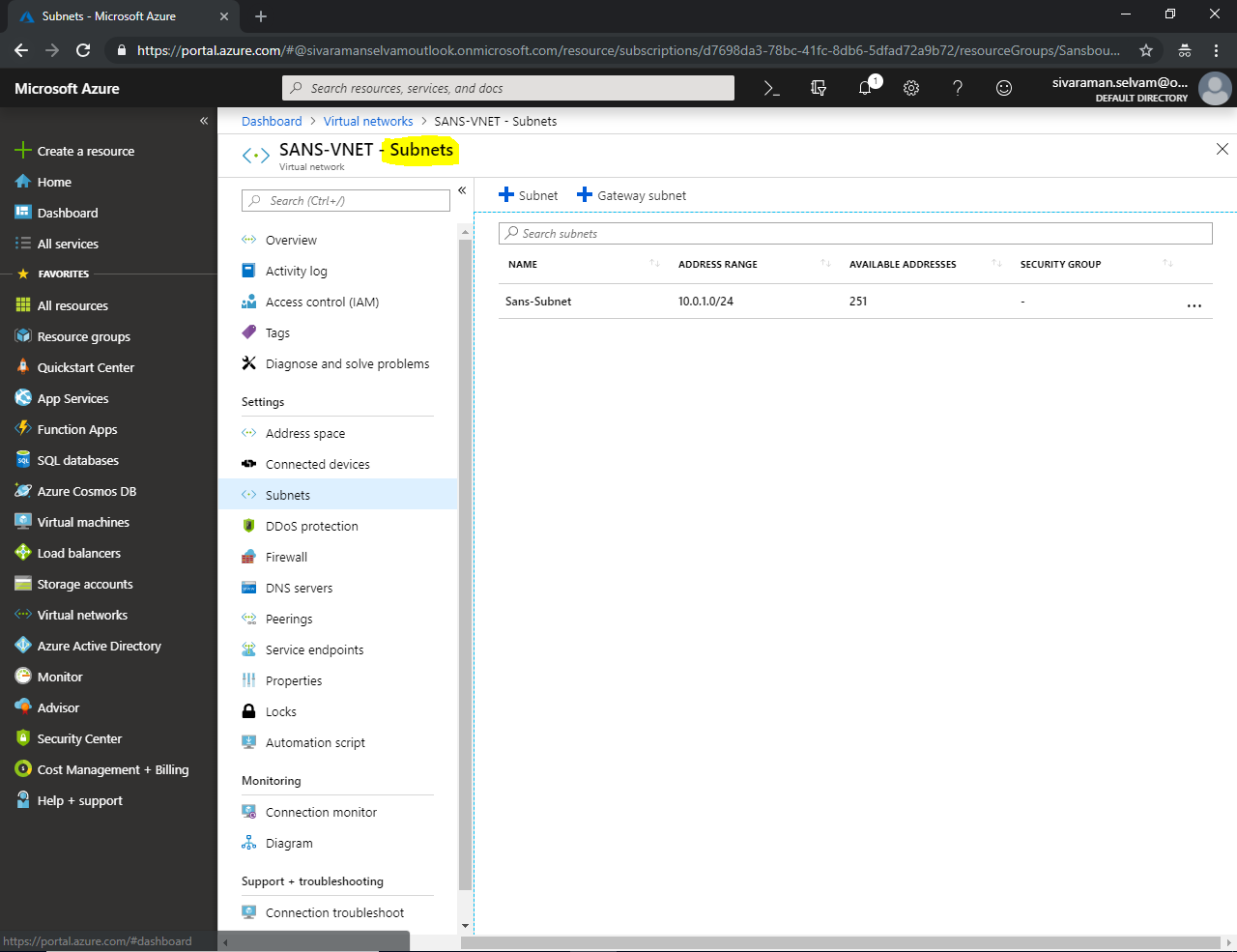


In **“SANS-VNET”**, you are able to see the address space details **10.0.0.0/16** and **“Region”**



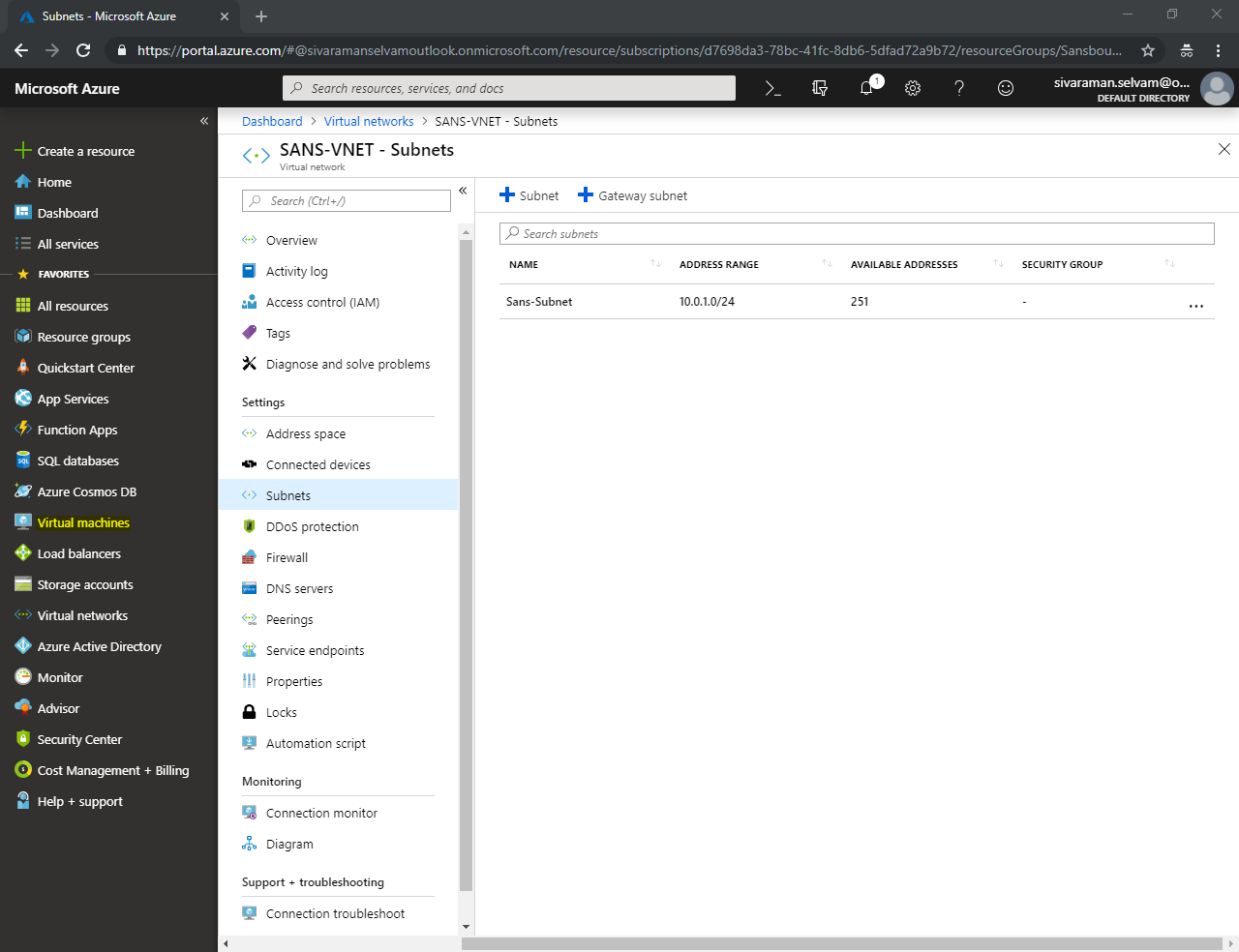
In **“SANS-VNET”** click on **“Subnets”** to get the details.

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

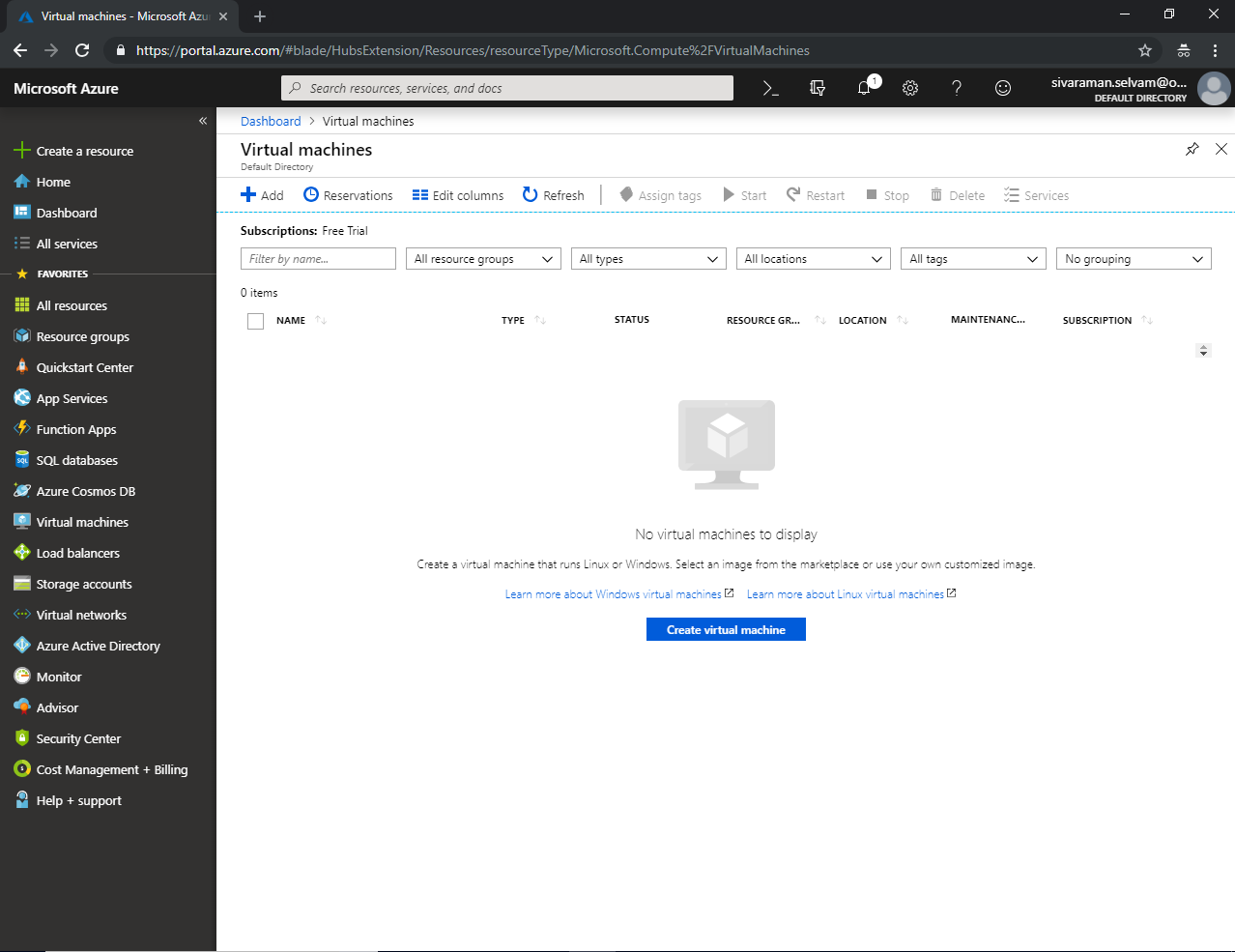


Now we have required to launch the virtual machine with Windows Server 2008 R2 Sp1.

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



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



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

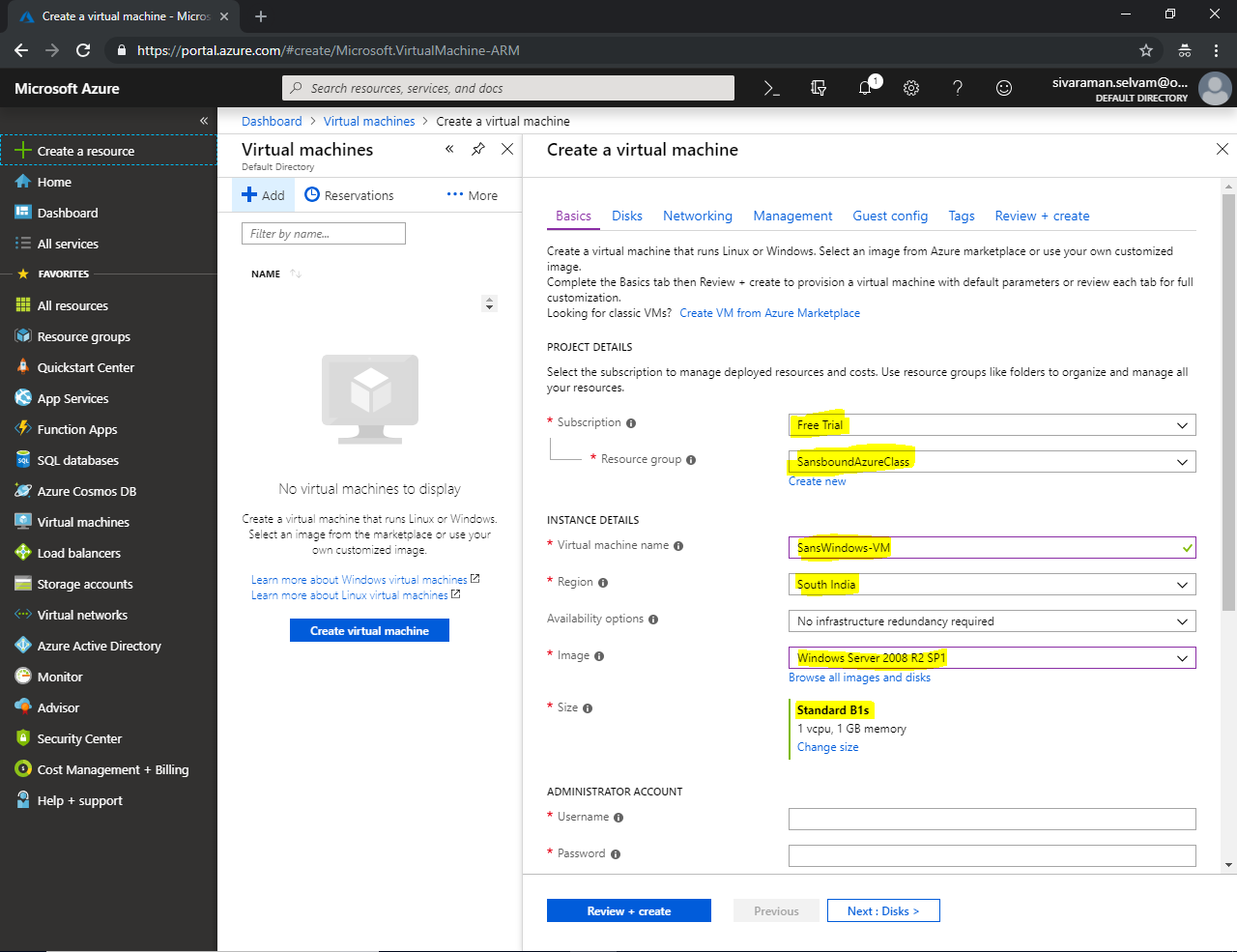
**“Resource Group”** as **“SansboundAzureClass”**.

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”**.

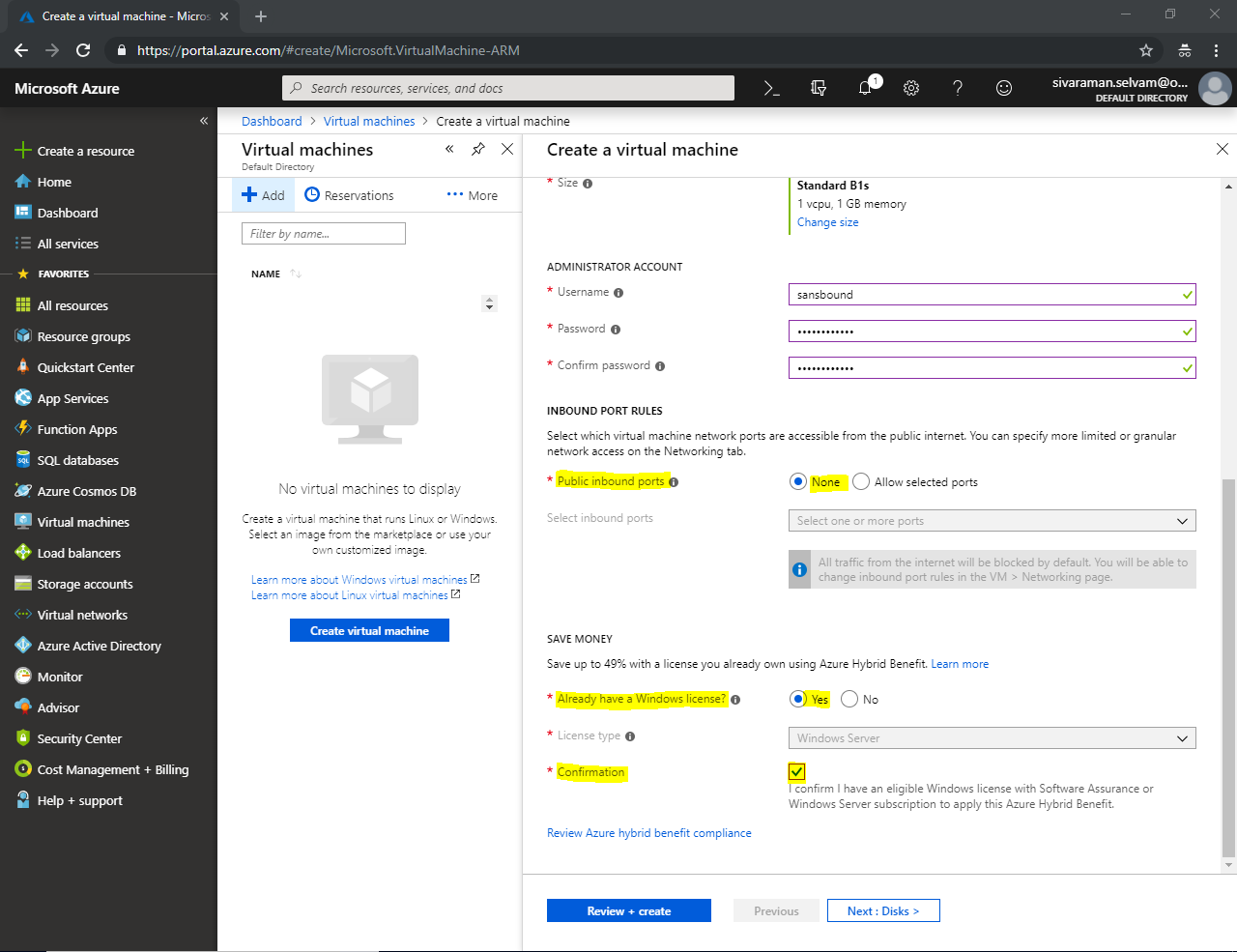


In **“Save Money”**

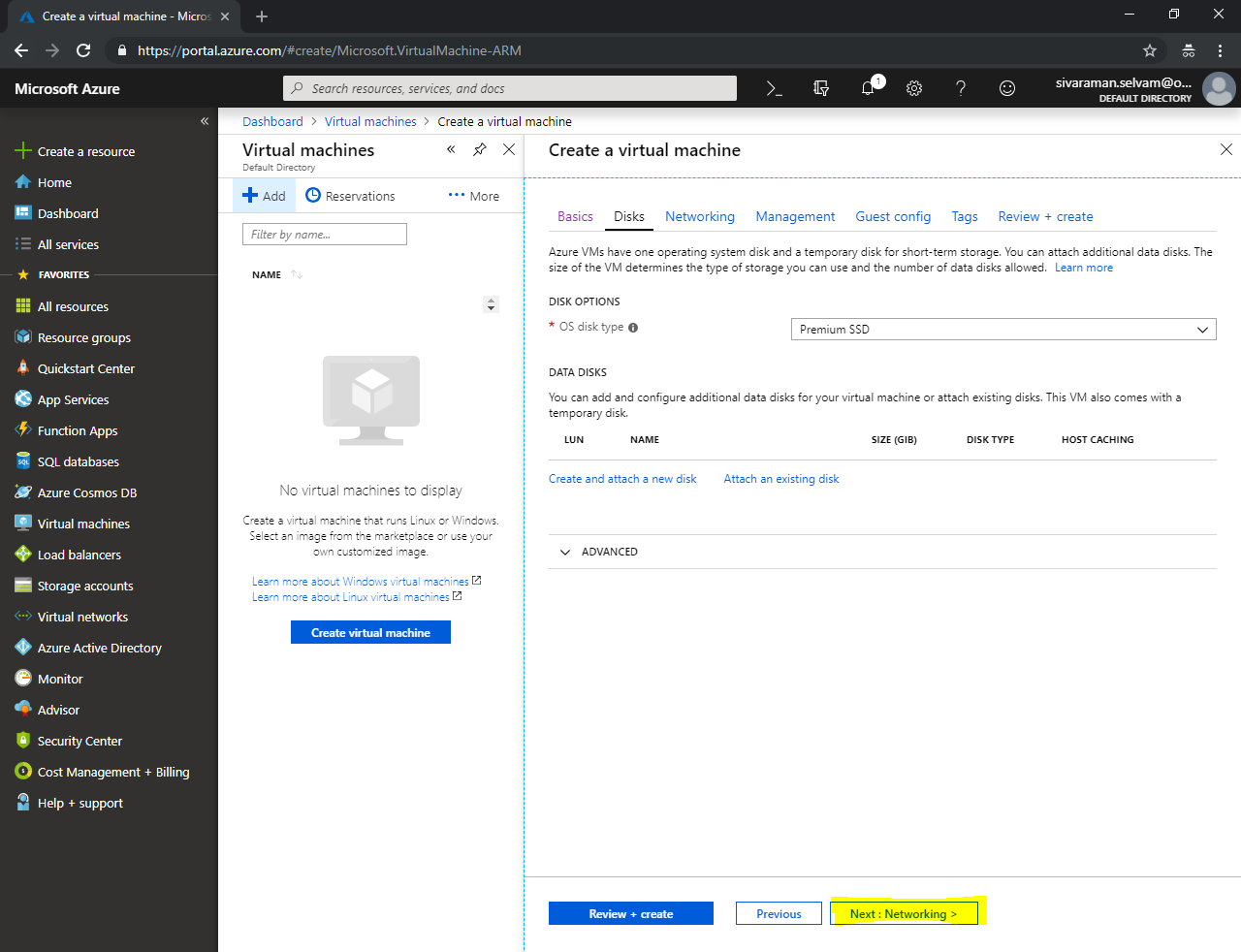
Click **“Yes”** for **“Already have a Windows license”**.

Need to check **“Confirmation”** box.

Click **“Next : Disks >”**.



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



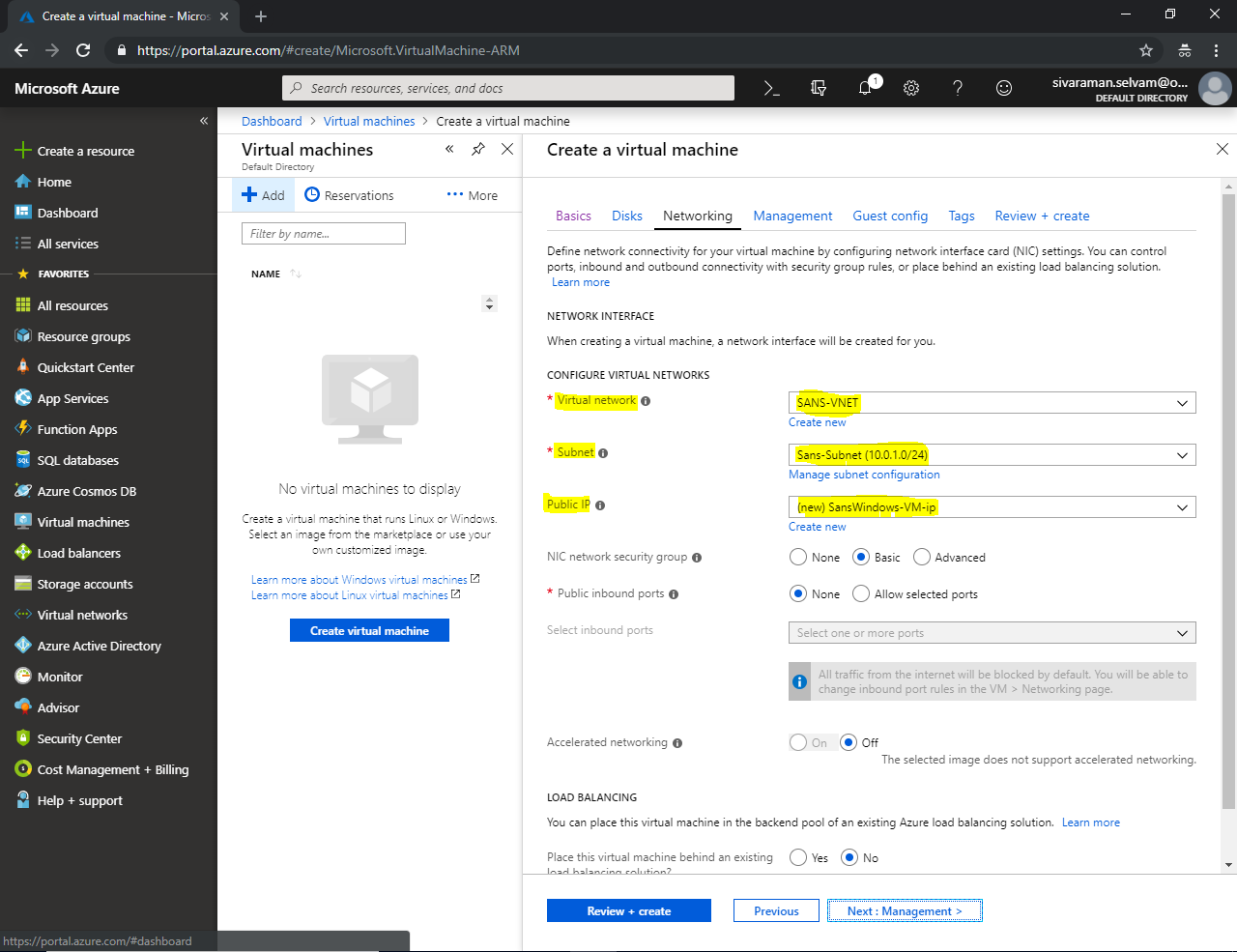
In **“Networking”**

At **“Configure virtual networks”**.

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

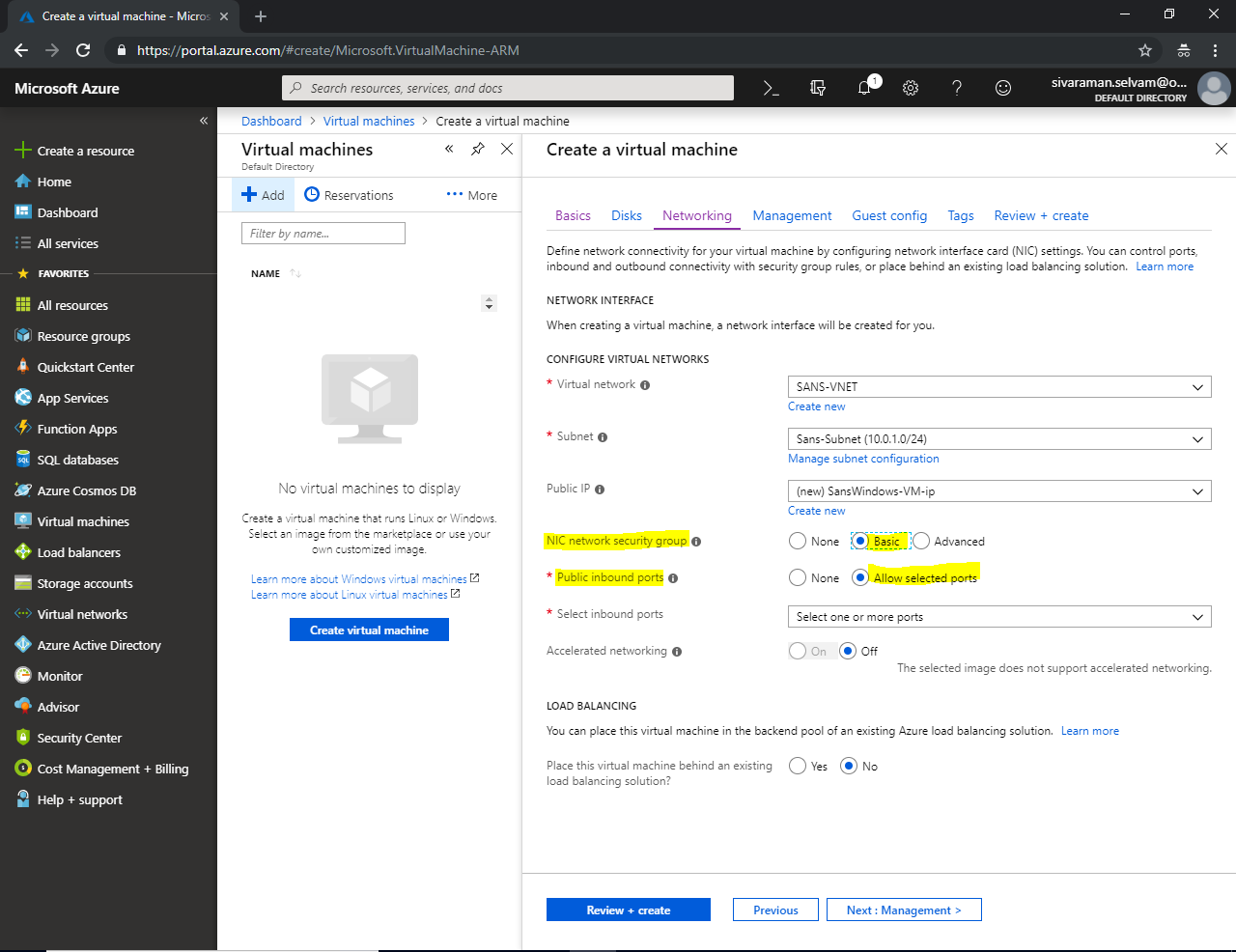
Ensure that **“Sans-Subnet (10.0.1.0/24)”**.

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

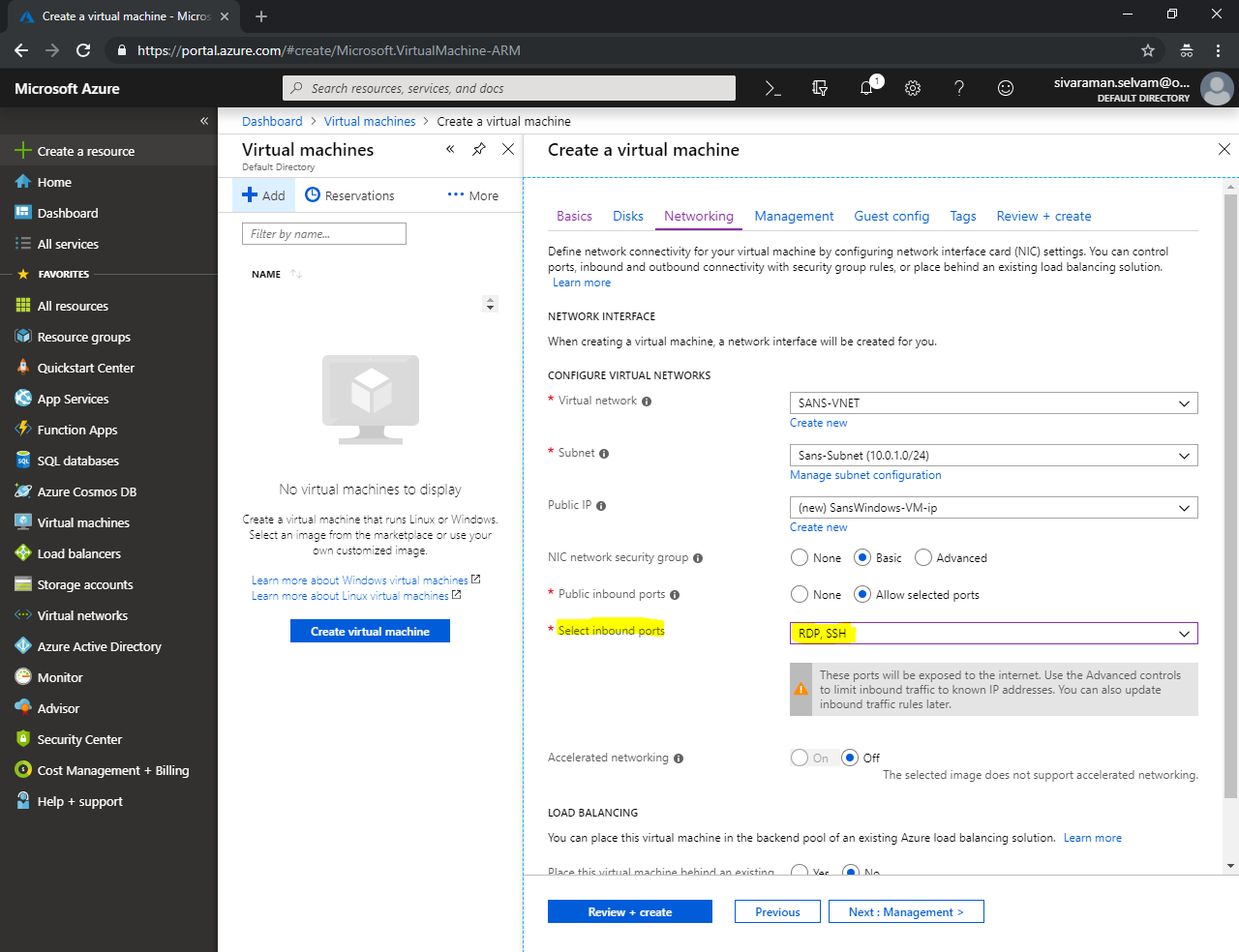


Click **“NIC network security group”** as **“Basic”**.

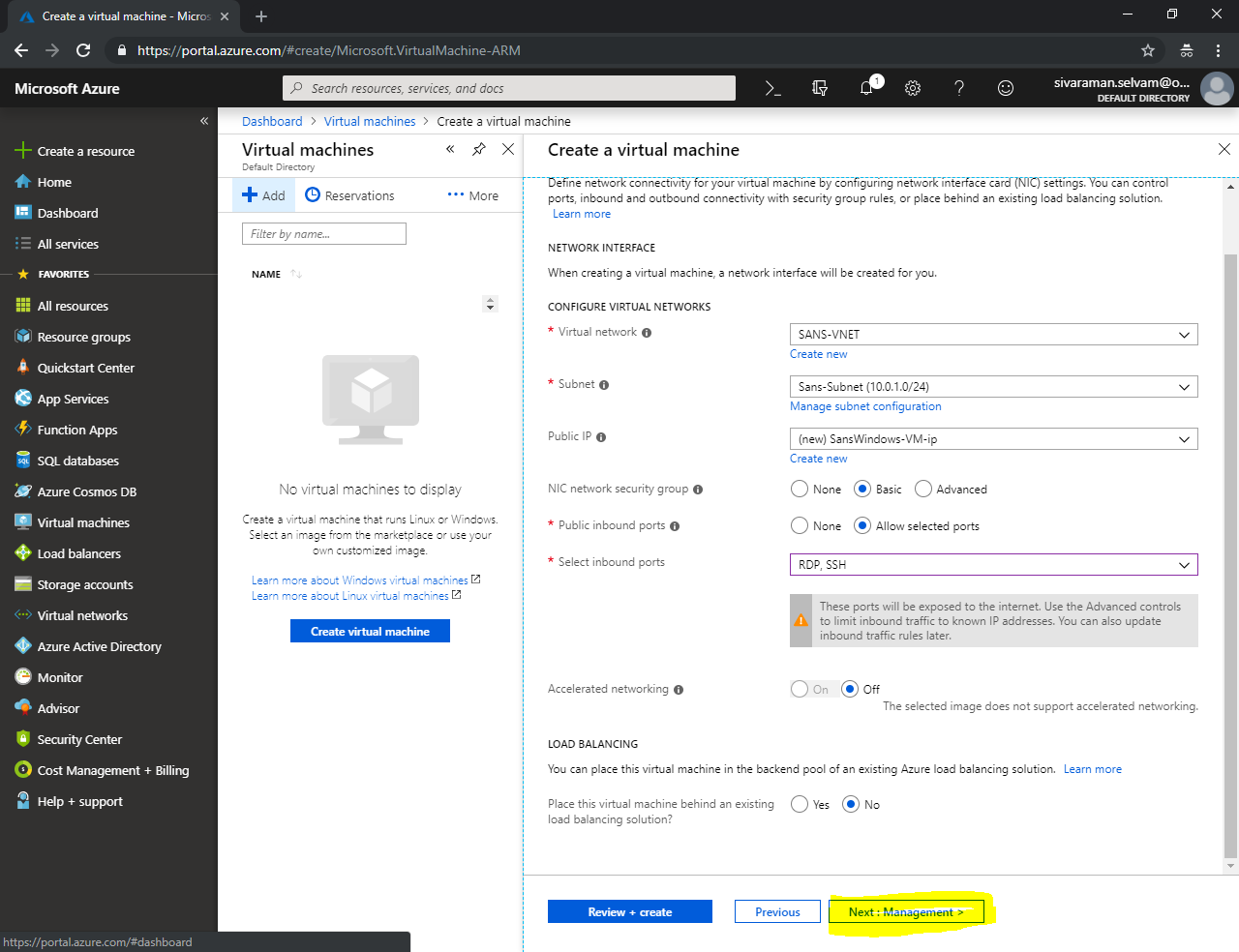
Click **“Public inbound ports”** as **“Allowed selected ports”**.



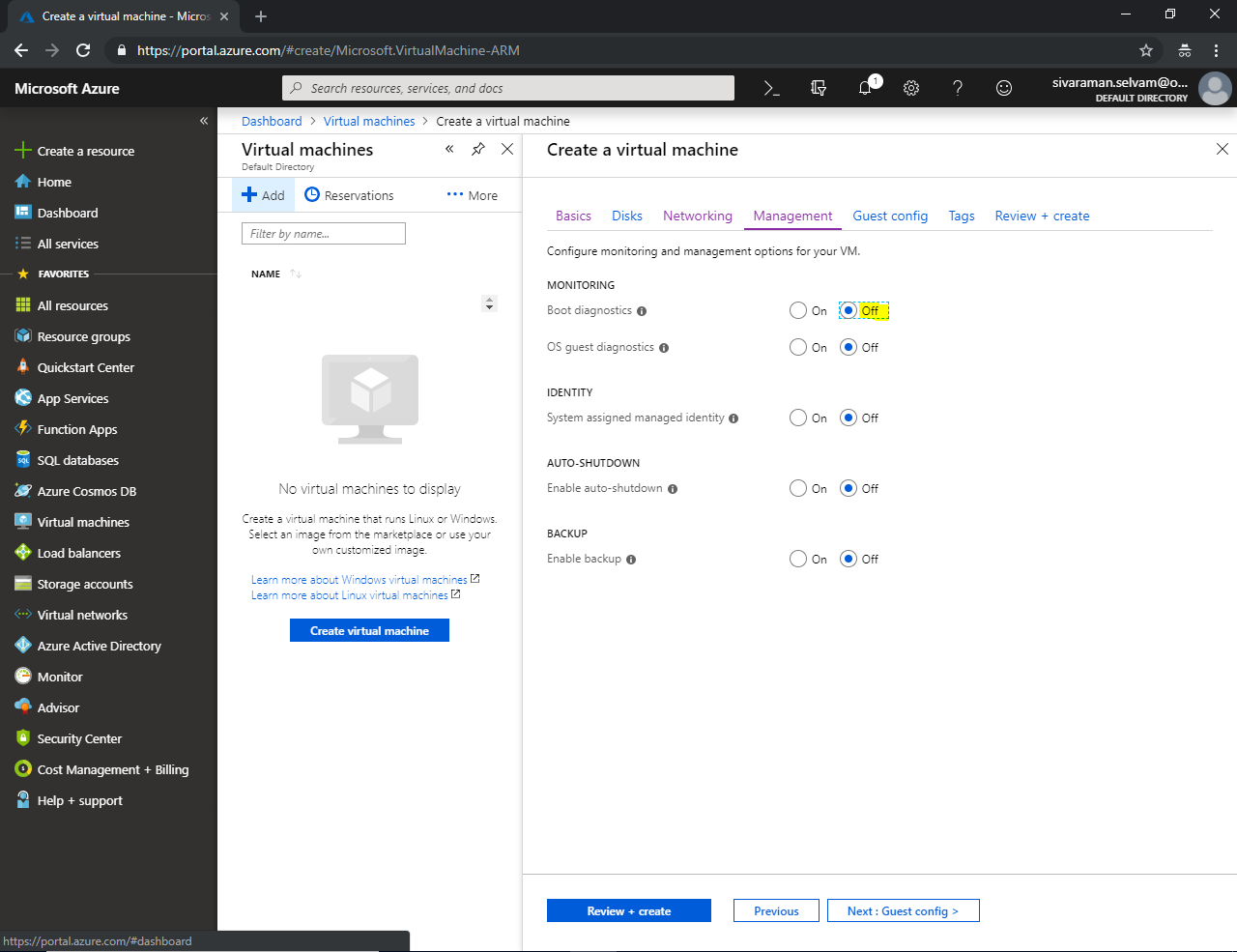
In **“Select inbound ports”** Allow **“RDP and SSH”**.



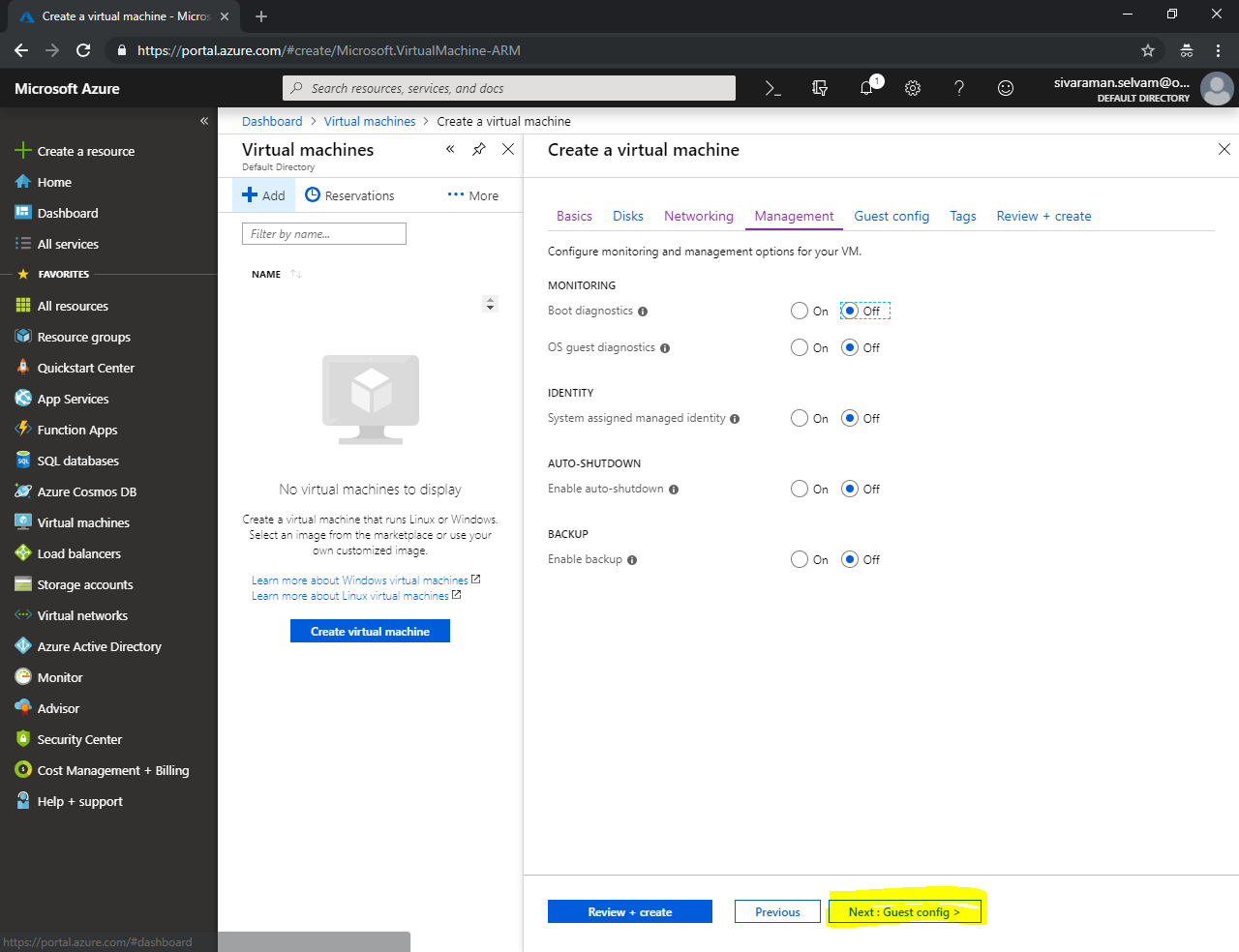
Click **“Next : Management >”**.



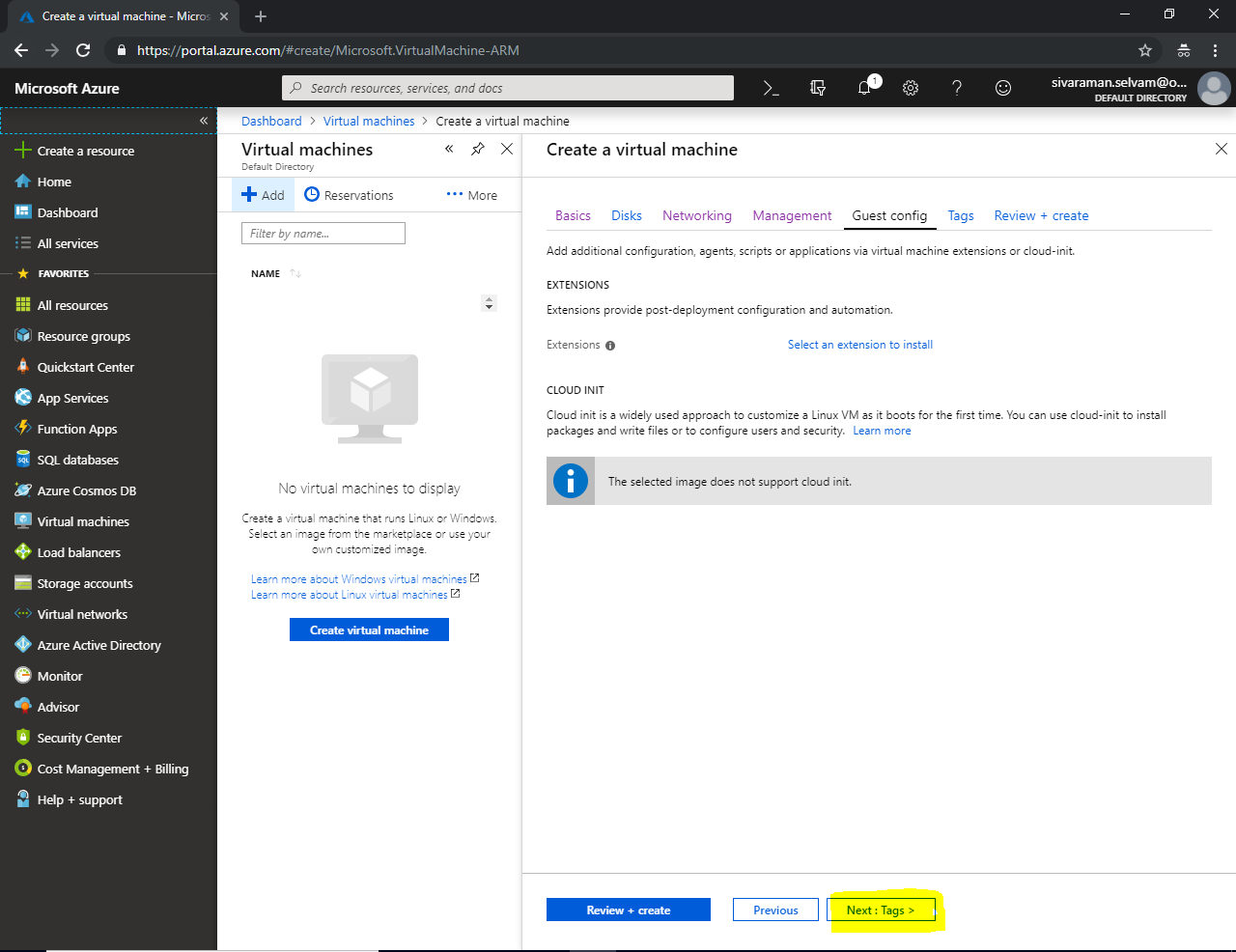
In Management, click **“Boot diagnostics”** as **“off”**.



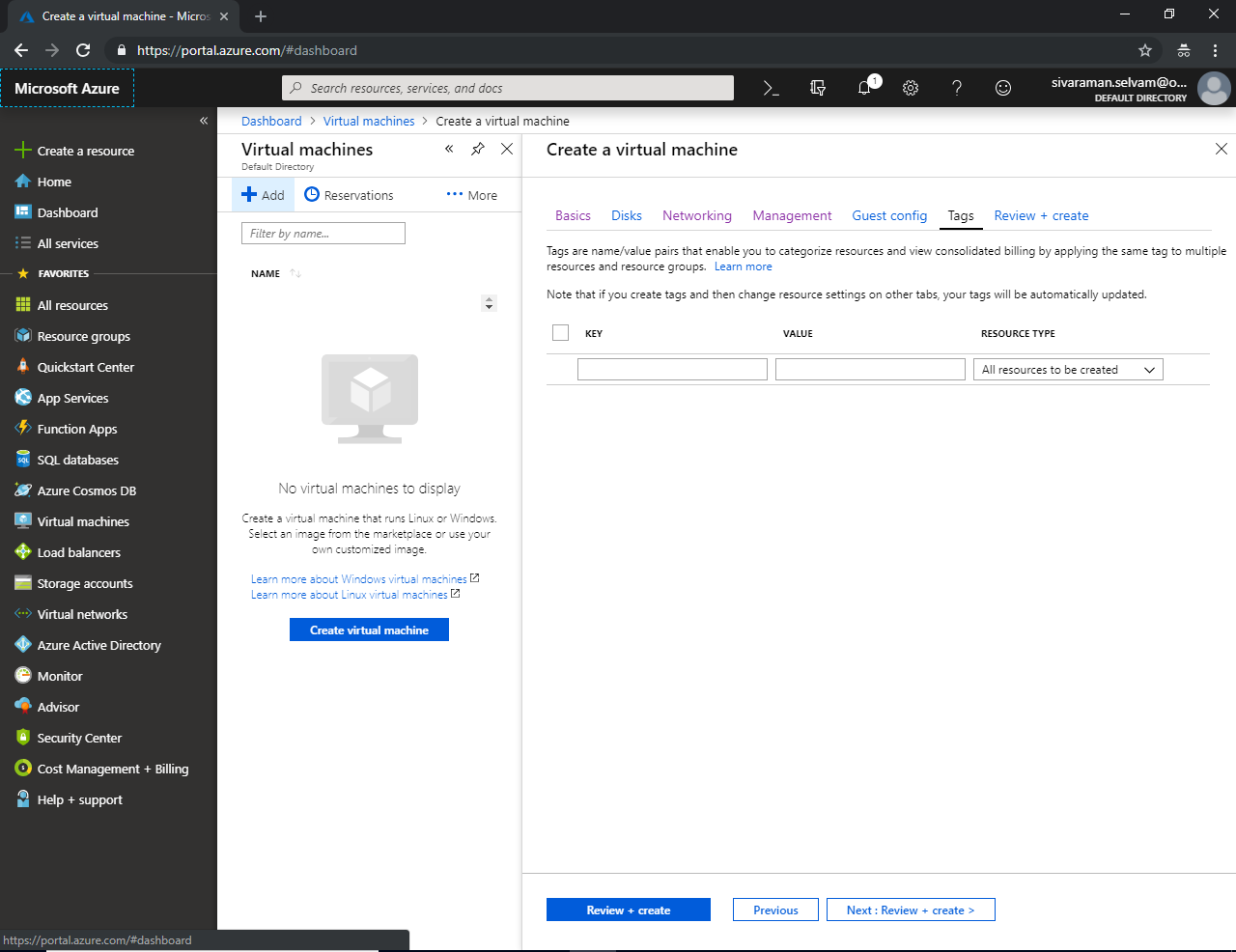
Click **“Next : Guest config >”**.



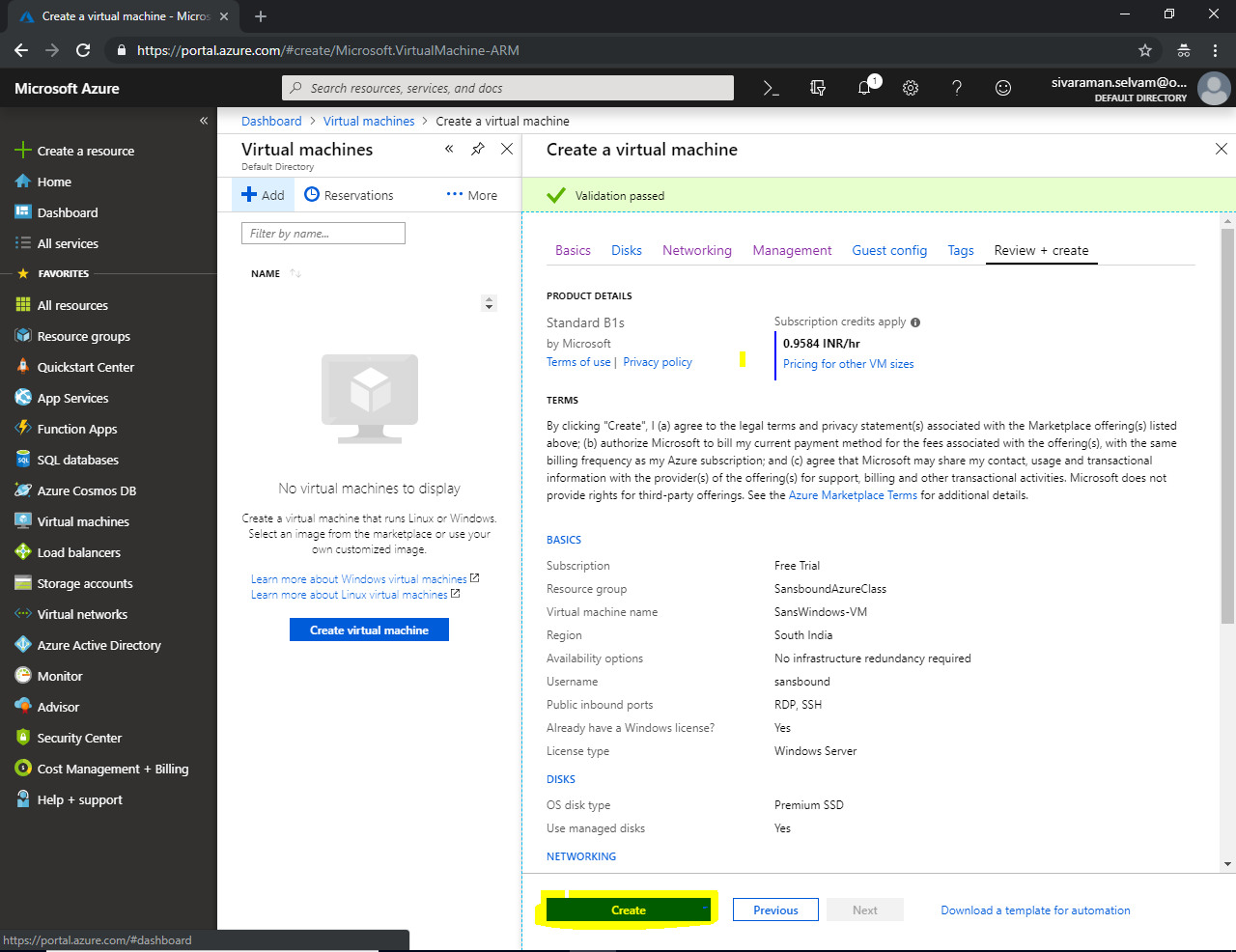
Leave default and click **“Next : Tags >”**.



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

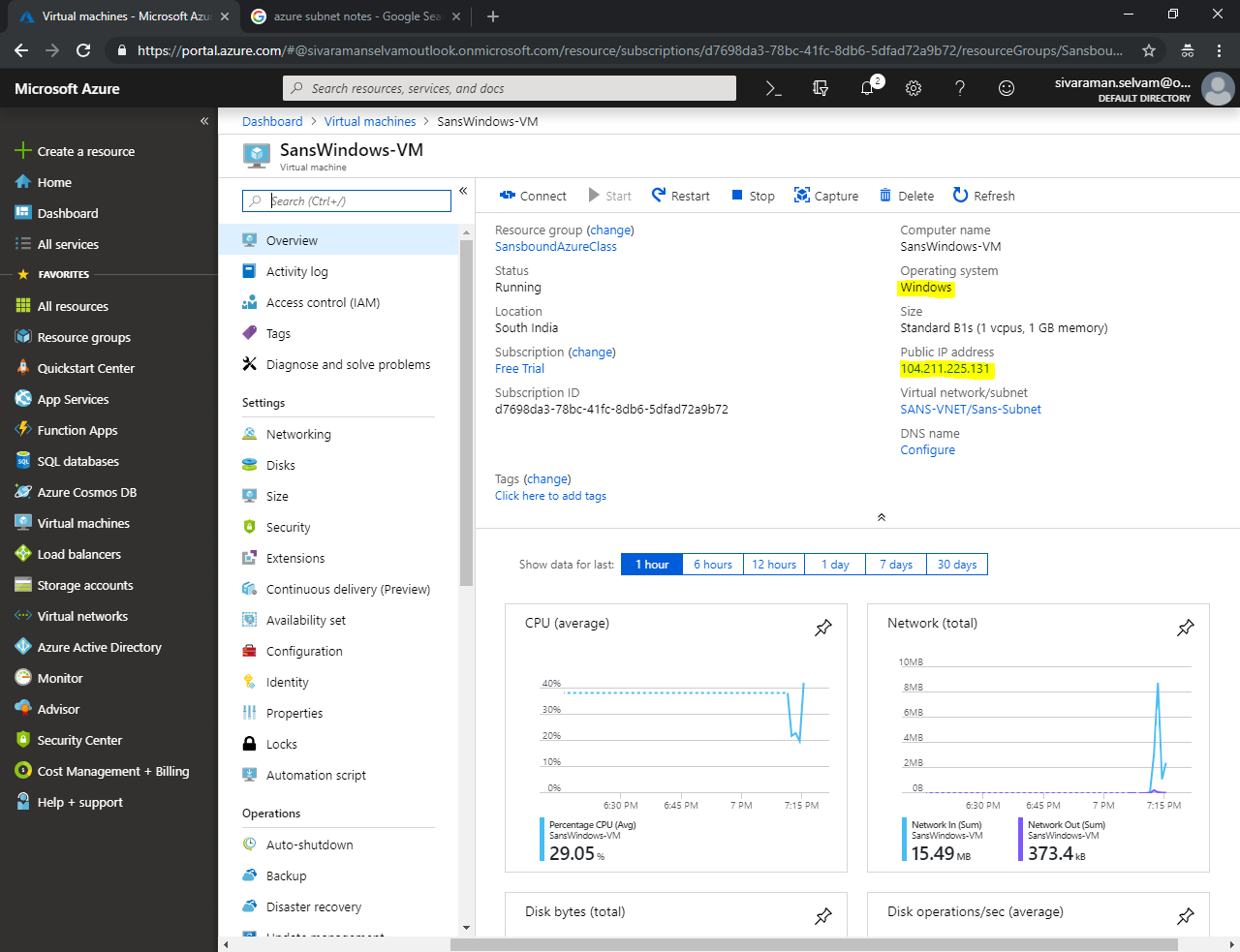


Click **“Create”**.



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

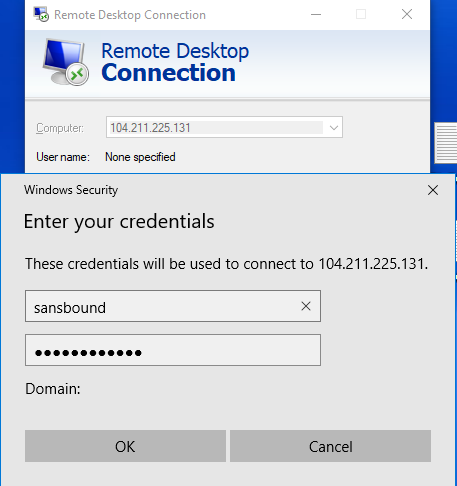
Note the public IP address of Windows Server.



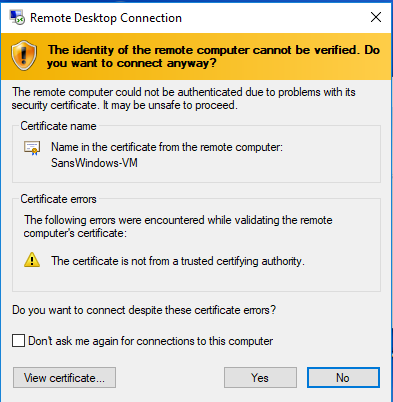
Type “mstsc” in Run box and click “OK”.

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

Provide the login credentials of Windows server.



Click **“Yes”**.



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).**

