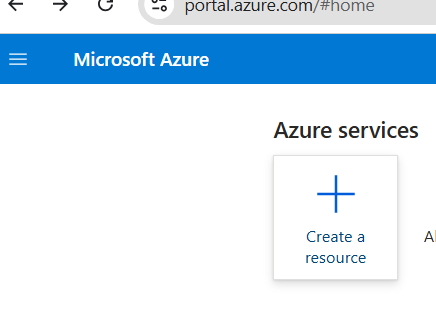
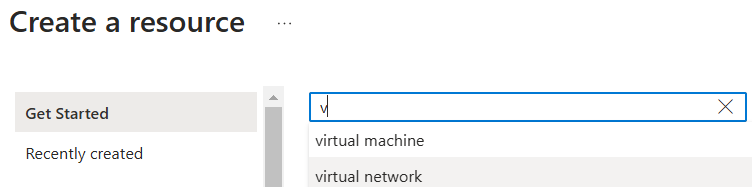
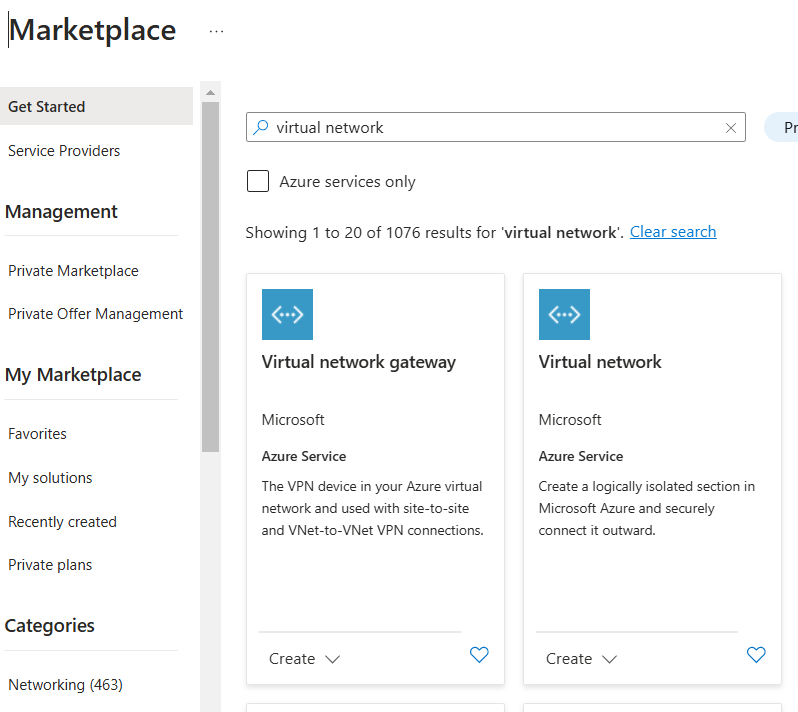
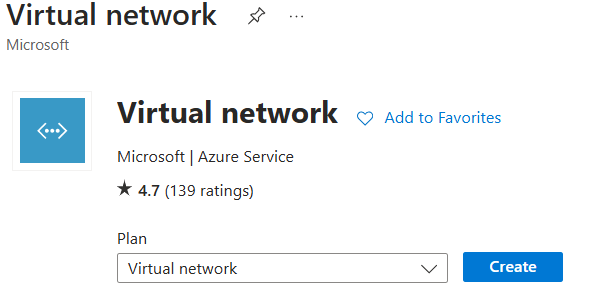
**Connecting Internet workloads using Vnet peering and Assigning a Custom Role for Operating these workloads**

**Task1. Create Vnet -1 in the Azure portal:**

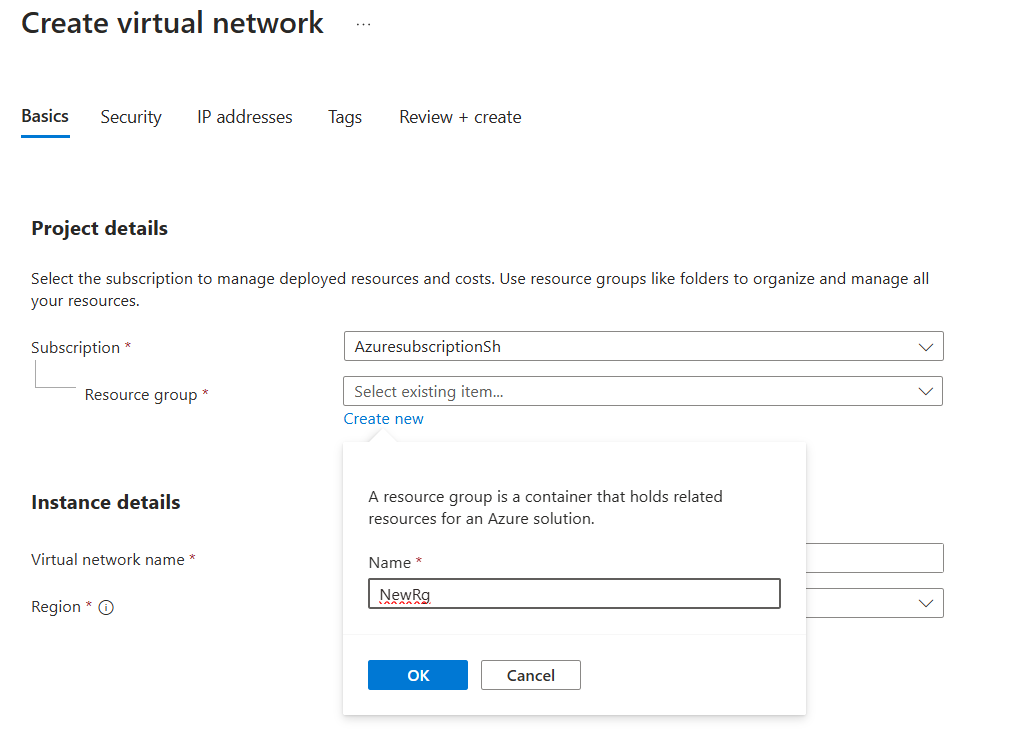
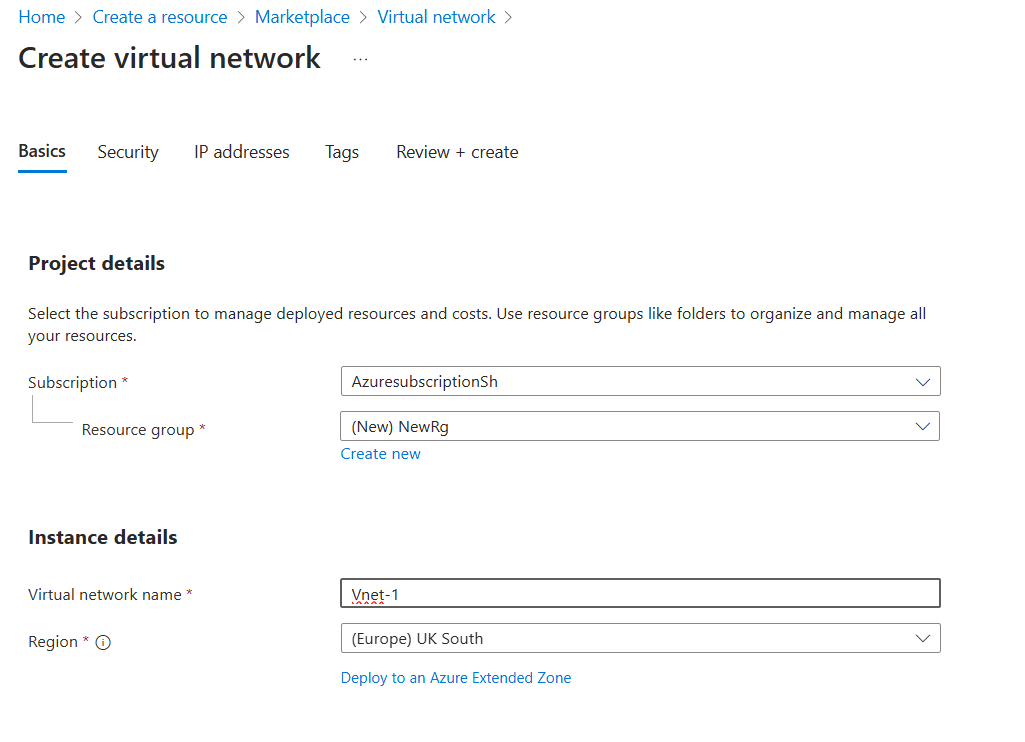
Step1: Login to Azure Portal and click on create new resource and search for Virtual network as shown below.



Step2: It will open Marketplace and show below screen, now click on Virtual Network and hit create.



Step3: After hitting Create, it will open vizard as shown below.

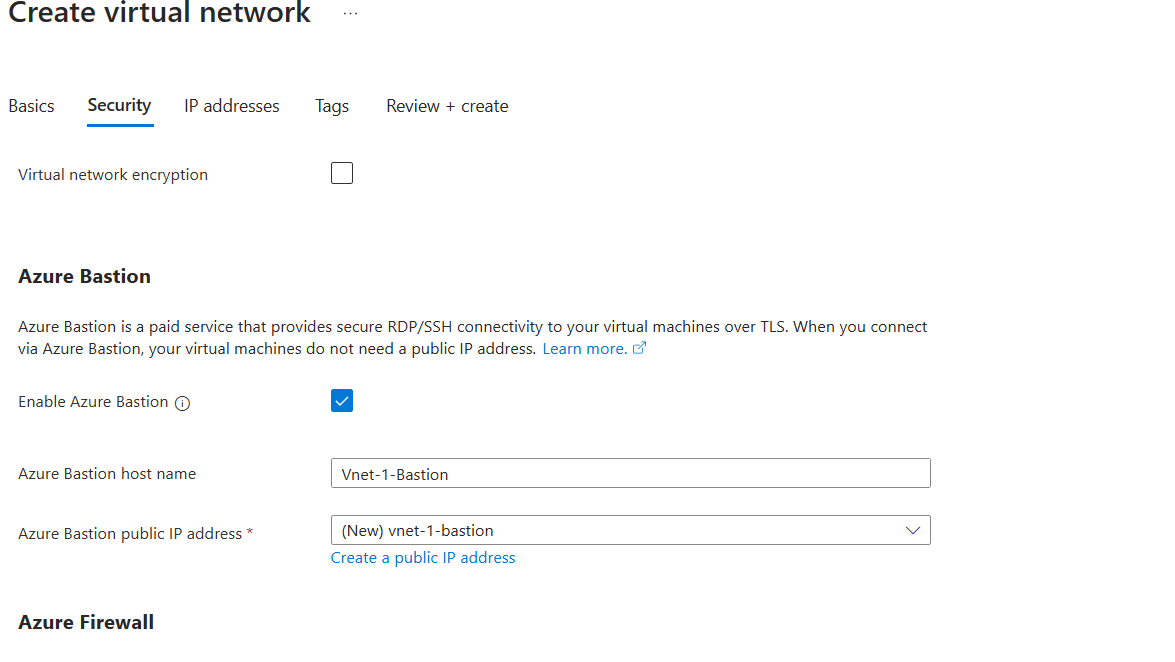


**In basic tab:**

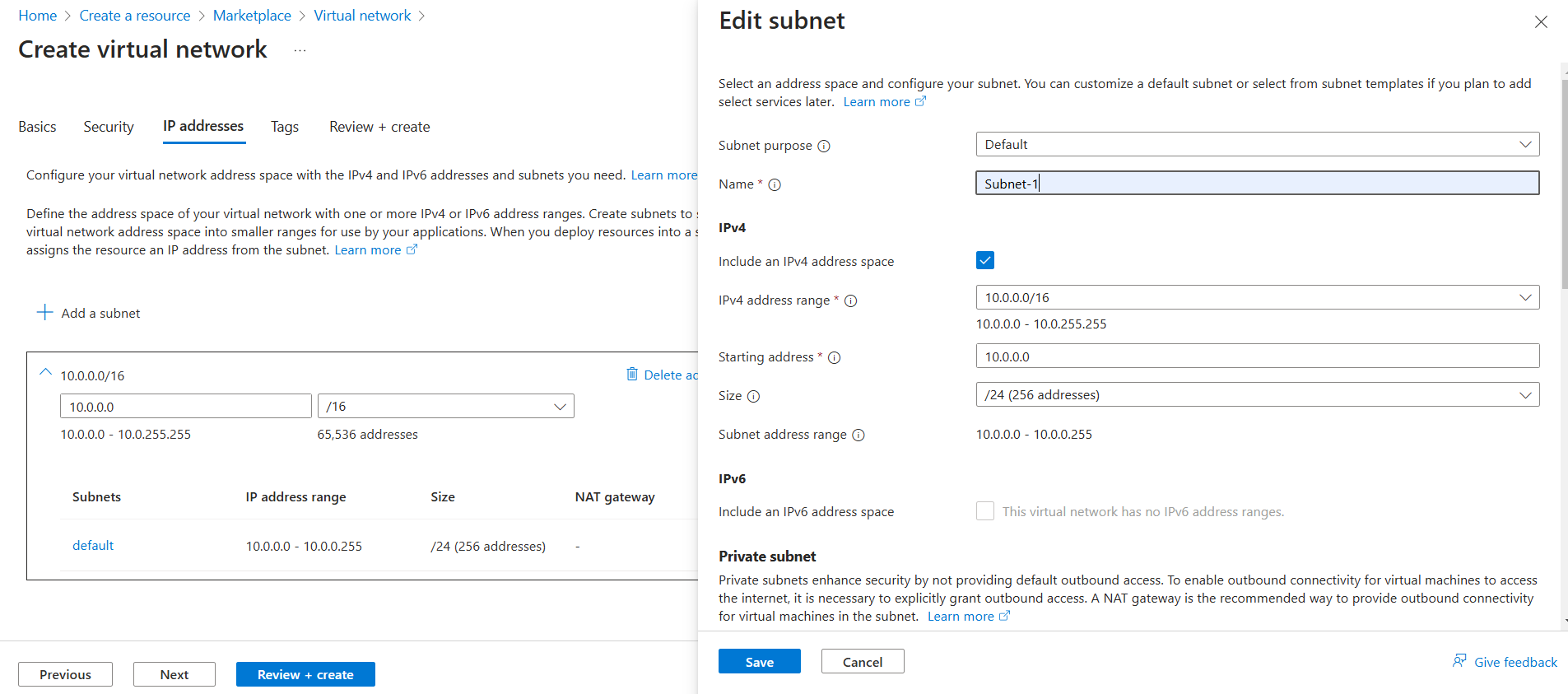
In Project Details, provide the subscription and resource group name that we use, if there is no resource group created, add new resource group with a new name in the resource group.

In Instance Details, provide a name to the Virtual network and select region in which we need to create the virtual network.

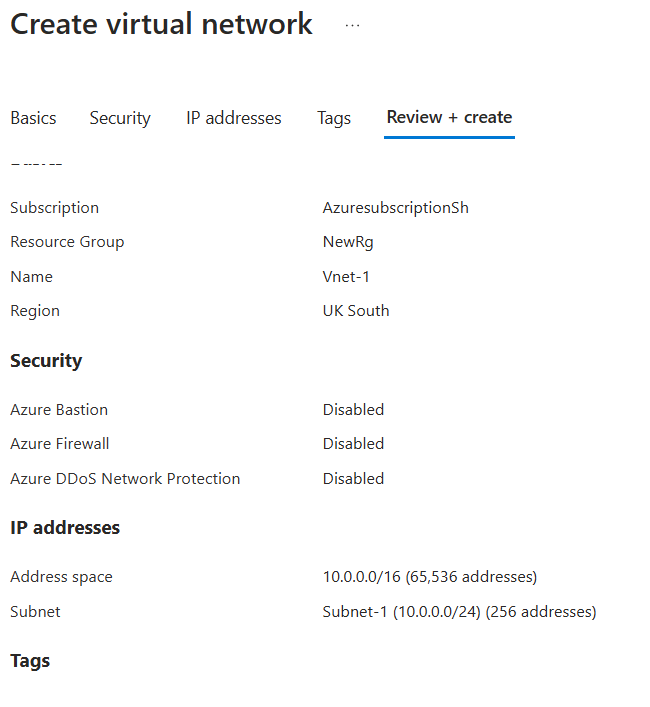
Step4: In the Security section, add Azure bastion as shown below:



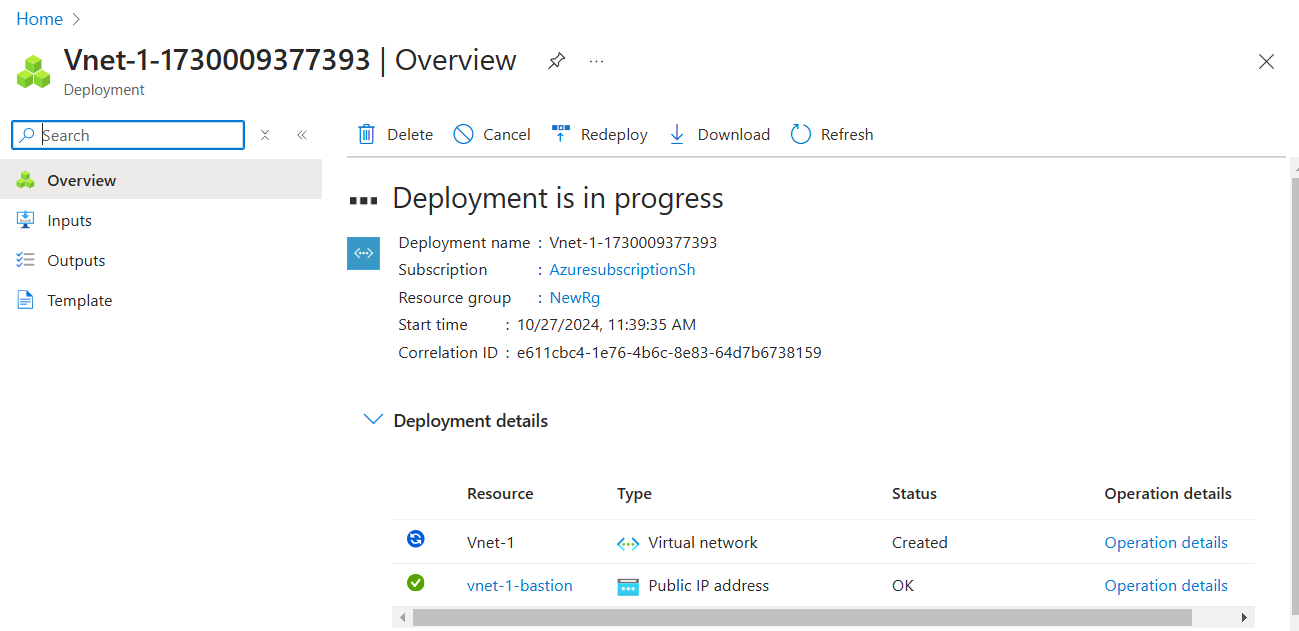
Step5: Go to Ip Address tab and add subnet-1 as shown below by adding Ip address range, Starting address and size.



Step6: now click Review+ create button as shown here.

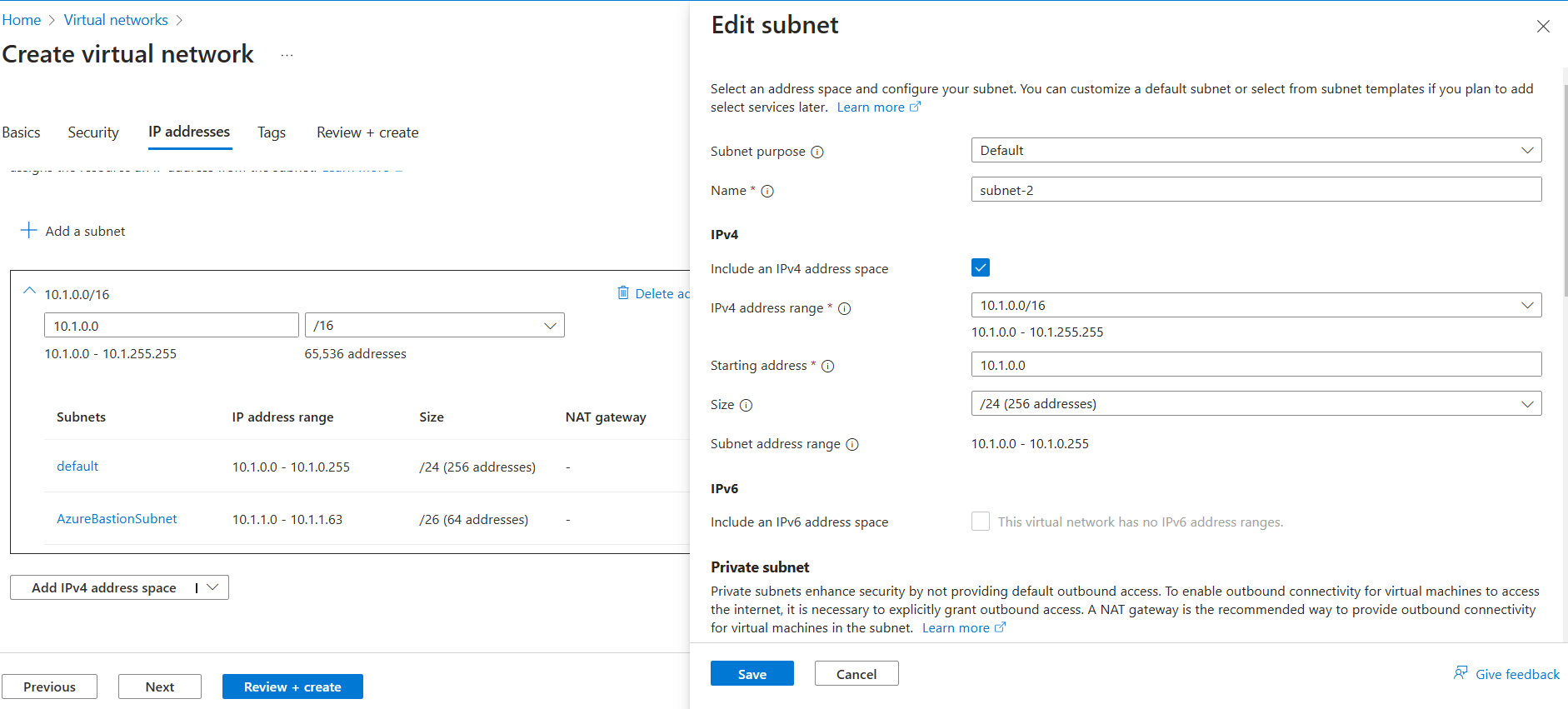
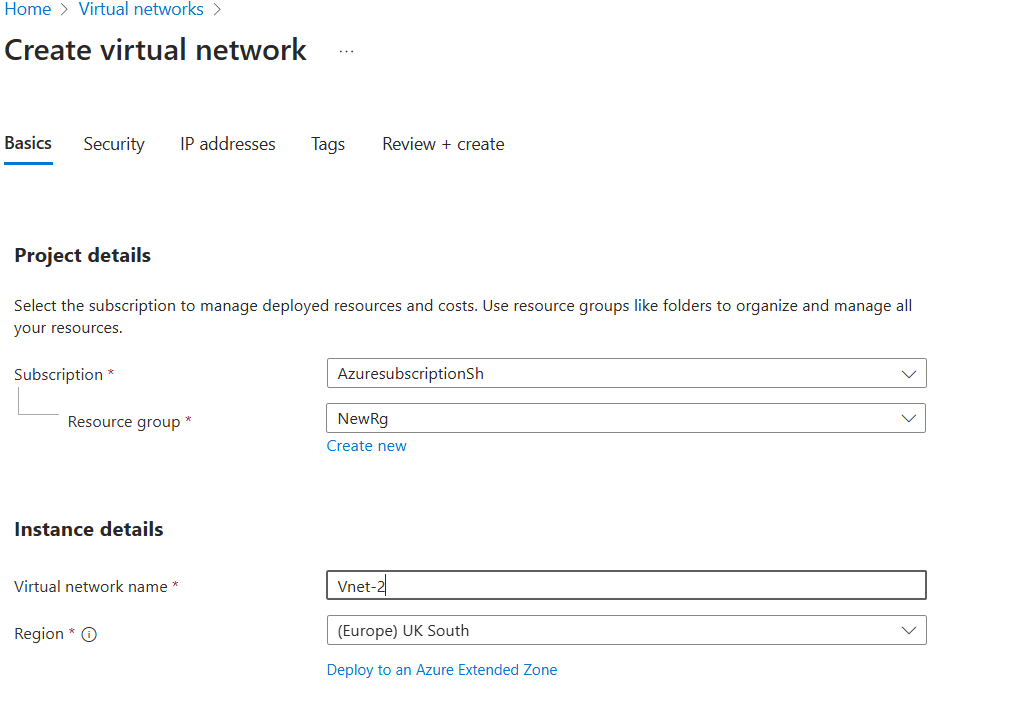


Now the virtual network will be deployed and ready to use as shown below.



**Task2: Create another Virtual Network (Vnet-2)**

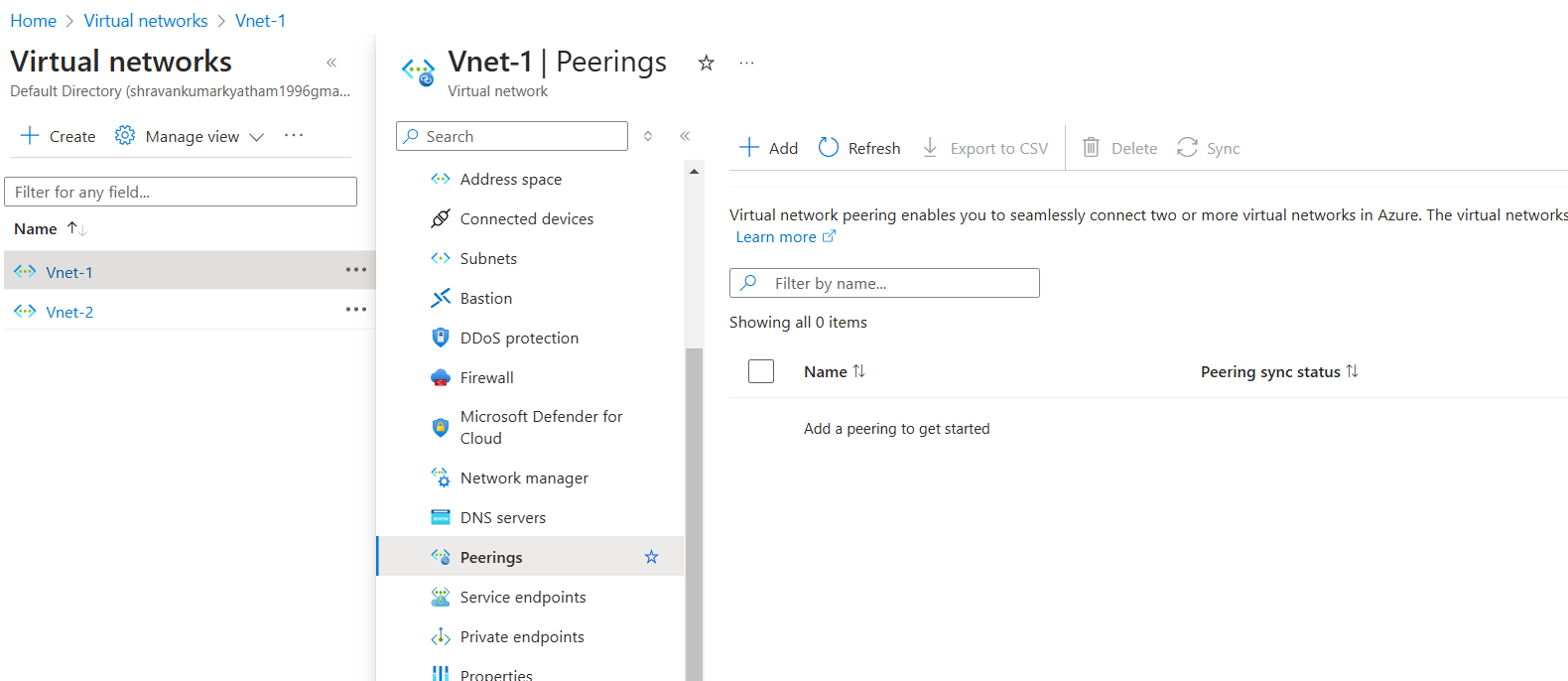
By repeating the process for creating Vnet-1 create Vnet-2 except name and Subnet are different for Vnet-2 as given below:



**Task 3: Virtual network Peering:**

Step1:

Go to Virtual networks sections and select Vnet-1, we can see one of the setting as “Peerings” select it, it will show below vizard.

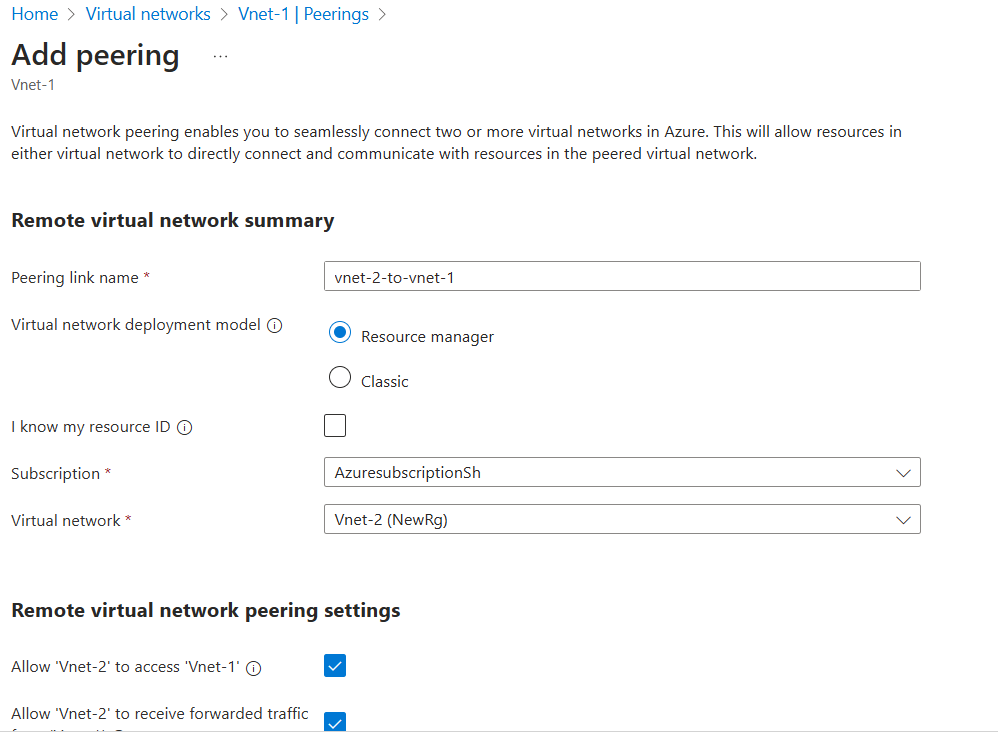


Step2:

Click on add, then under Remote Virtual network summary add:

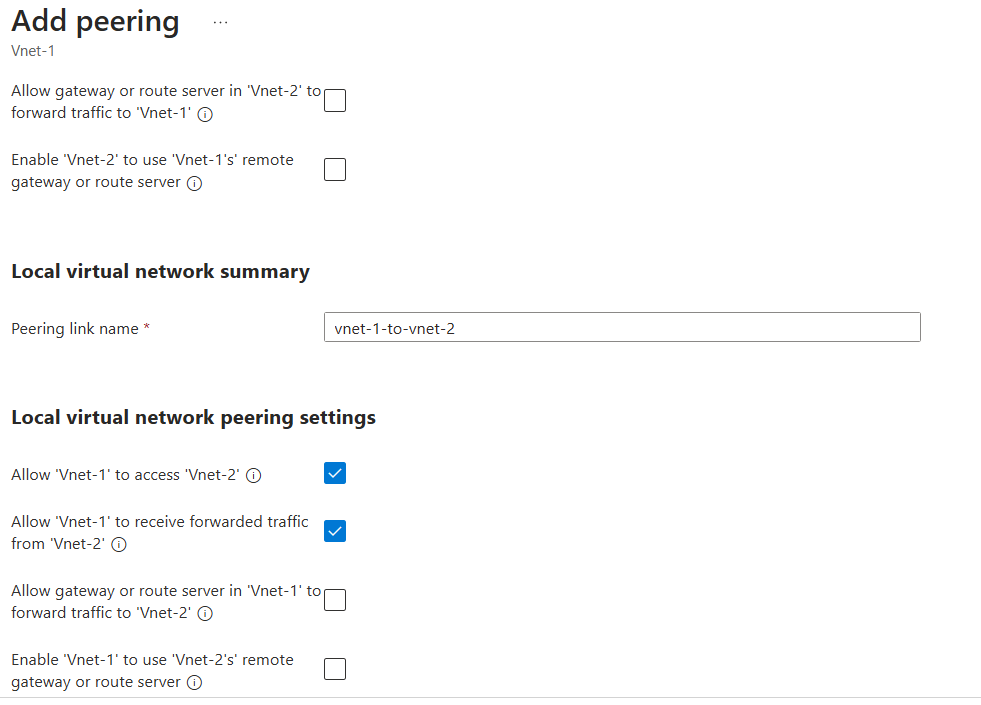
peering link name as “Vnet-1 to Vnet-2”, virtual network deployment model as “Resource Manager” and select subscription and Virtual network to which you want to give access i.e Vnet-2 and

Remote Virtual network summary check the check boxes for both 1.Allow Vnet-2 to access to Vnet-1 and 2.Allow Vnet-2 to receive forward traffic from Vnet-1 as show below:

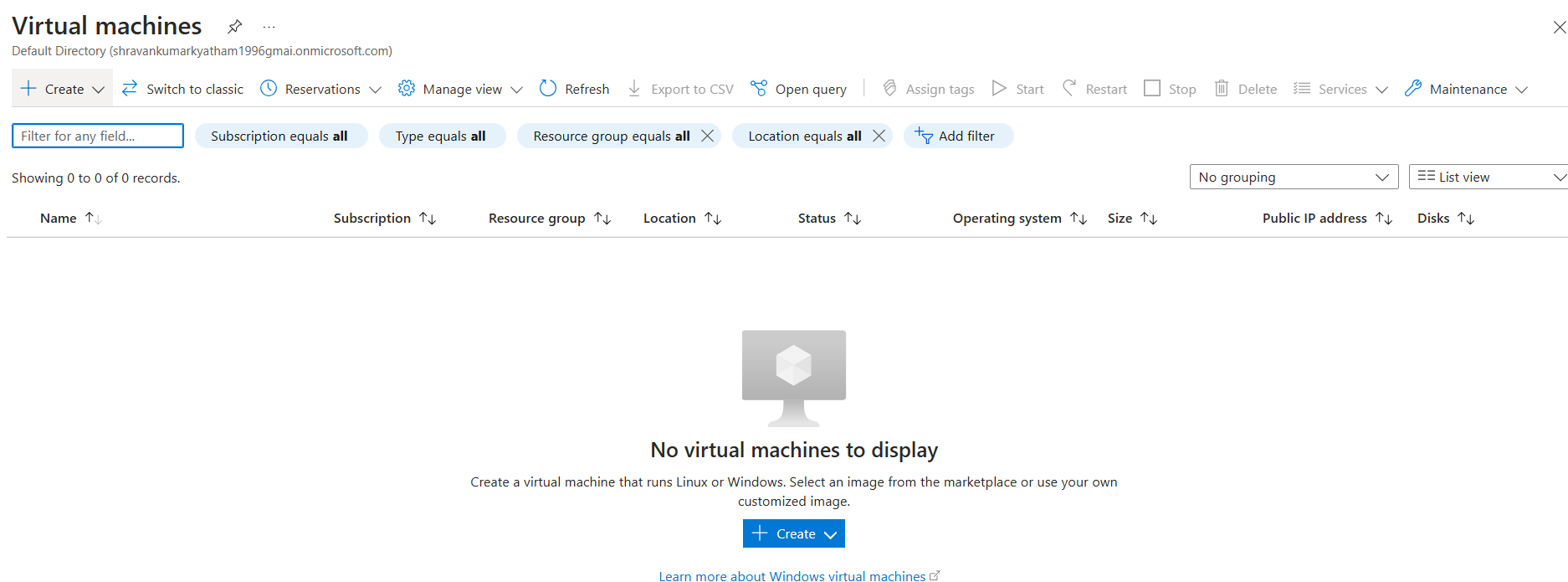


Under Local network summary :

Add peering link name as “vnet-1 to vnet-2”, under Local virtual network peering settings check the check boxes for both 1.Allow Vnet-1 to access to Vnet-2 and 2.Allow Vnet-1 to receive forward traffic from Vnet-2 as show below:

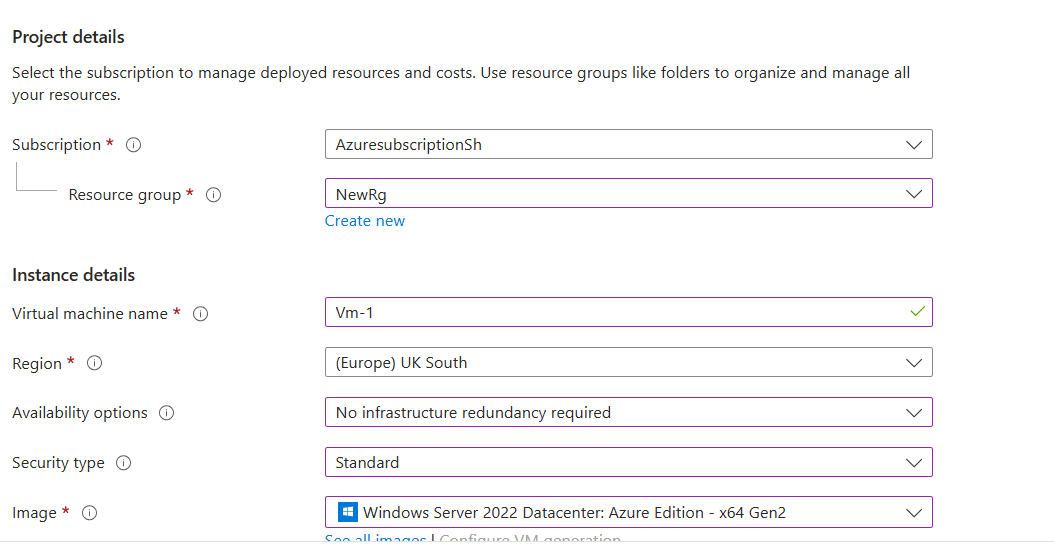


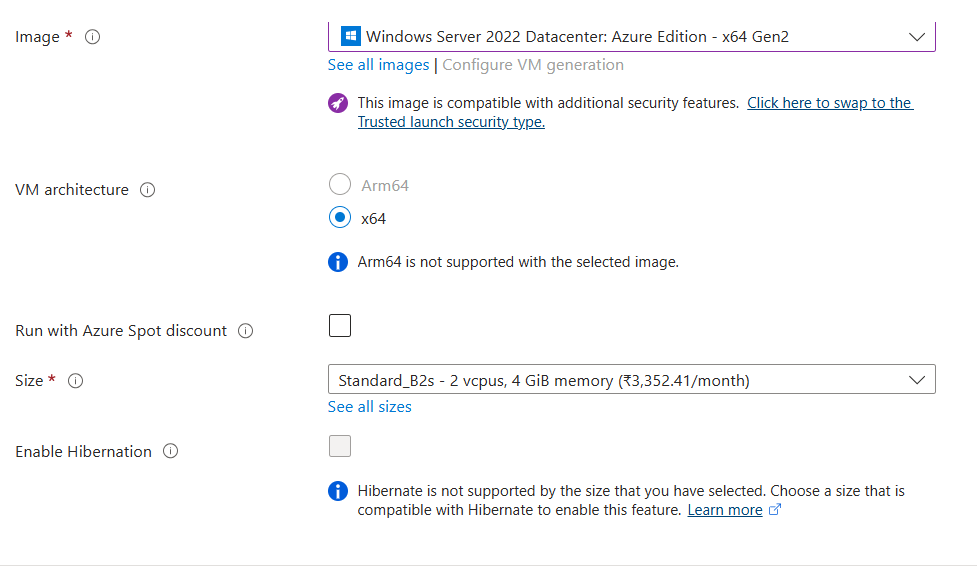
**Task 4 : Creating Virtual Machines (Vm-1 and Vm-2)**

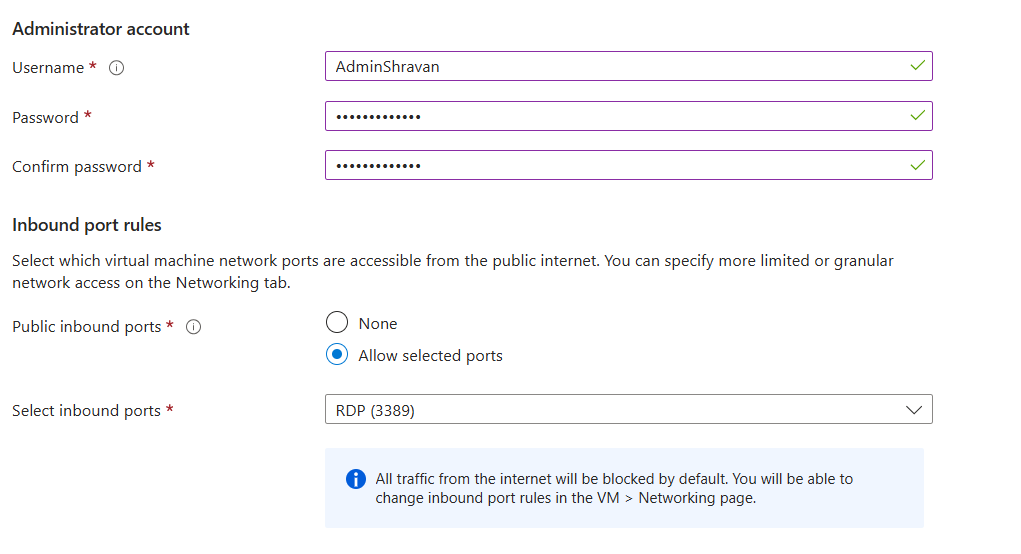
Step1: To create Virtual machine click on create resource and search for Virtual machines, portal will show wizard as shown below:

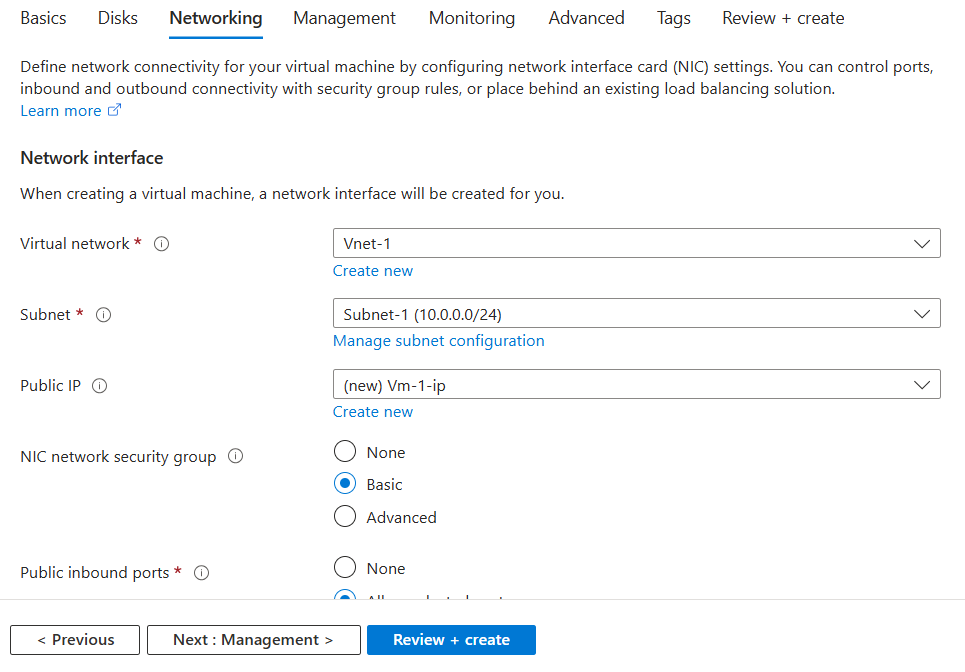
Step2: In basic tab, under project details give the subscription and resource group used to when we created the Vnets.

In instance details, give virtual machine name Vm-1 and select the region and specify the availability options as “No infrastructure redundancy required” and security type as “standard” and select image (windows or ubuntu) as shown here.

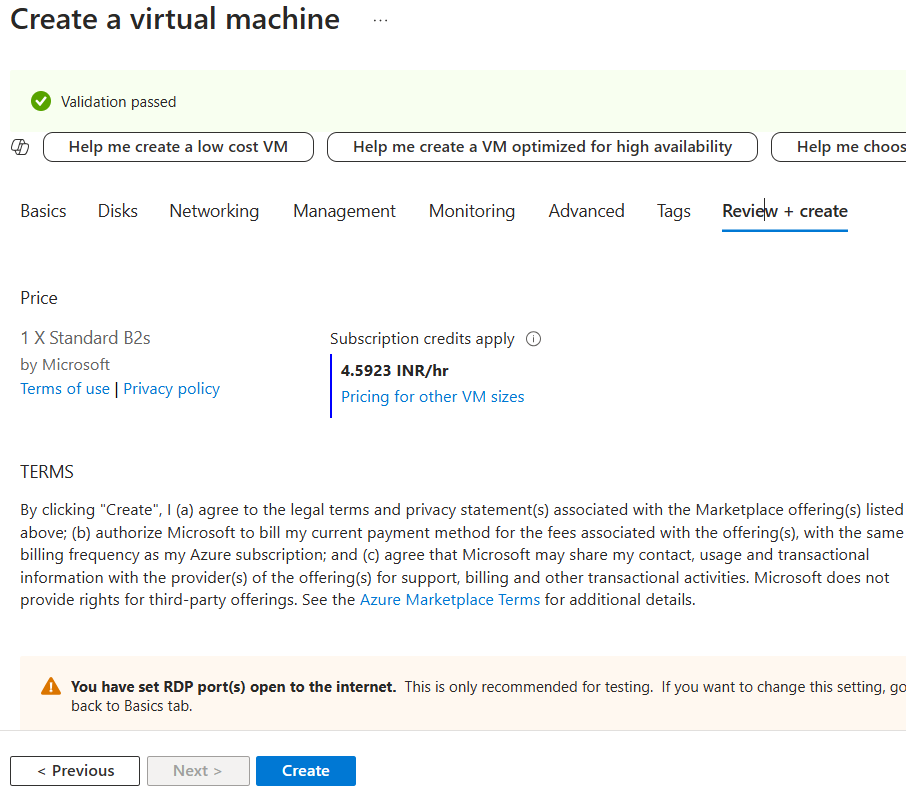


Step3: select size of the CPU and provide admin account credentials of your wish and in In bound rules select RDP in inbound ports and click allow selected ports radio button as shown

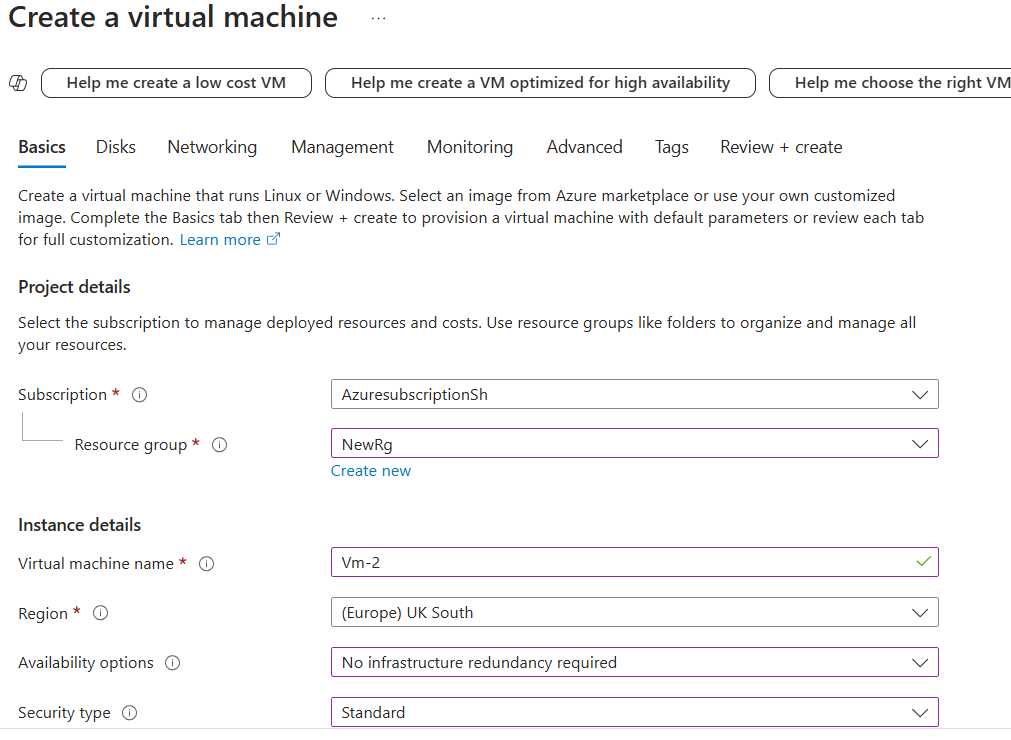
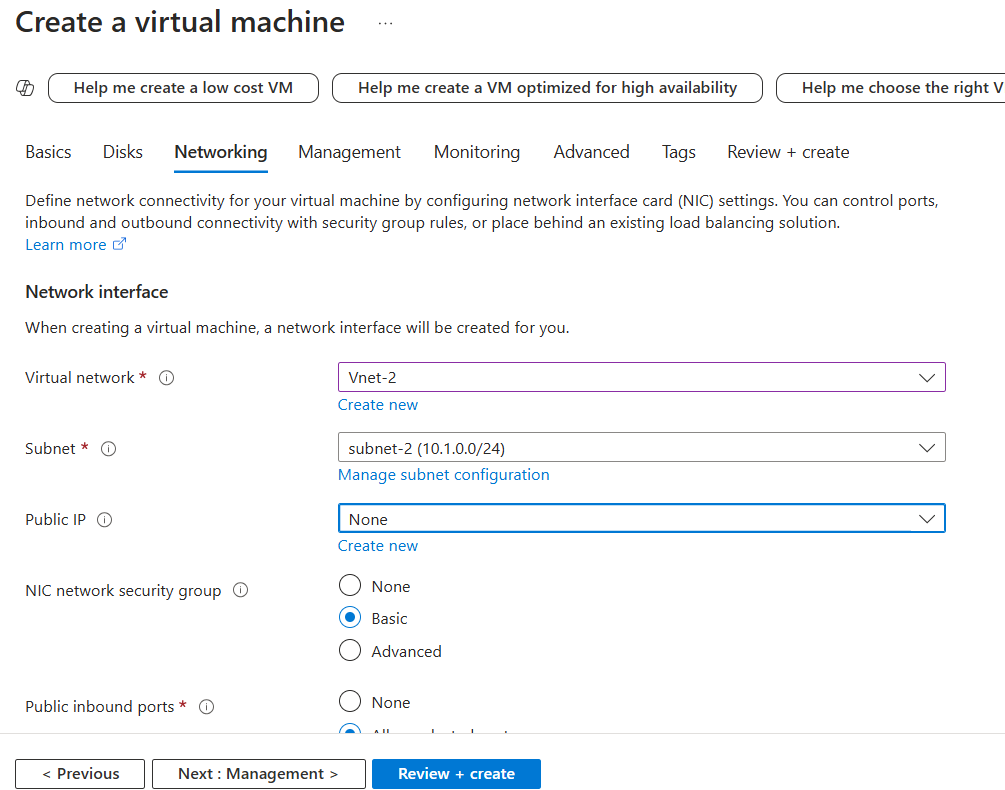


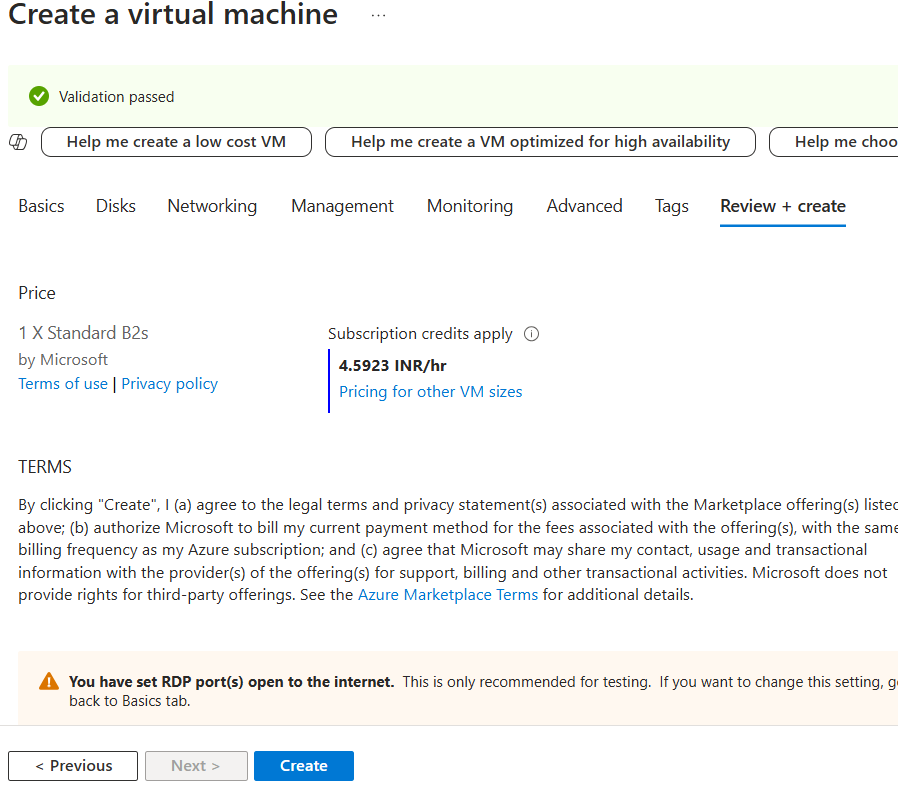
Step4**:** In networking Section, provide Virtual network as Vnet-1 and subnet as Subnet-1 and in public IP put new Vm -1 so it will create Public IP for this VM and put other default settings as shown here:

Step5: Now click on review + create, now portal will do validations of the details we entered and after validation passed click on create button as shown below, it will deploy our Virtual machine.



Step6: Create another Virtual Machine (Vm-2) in the same way, but we need to give Virtual network (Vnet-2) and subnet-2 in the network section as shown below:

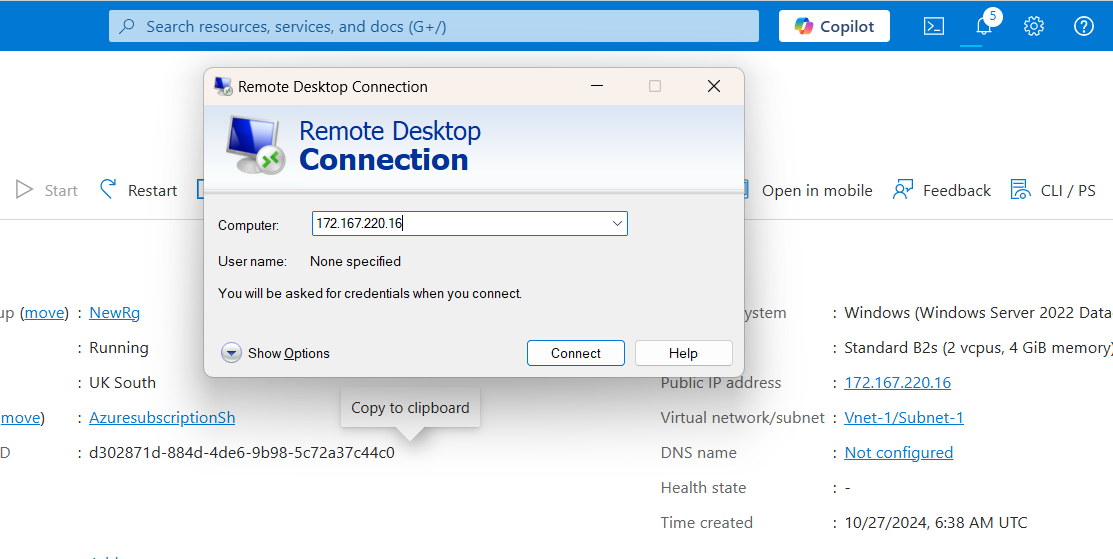


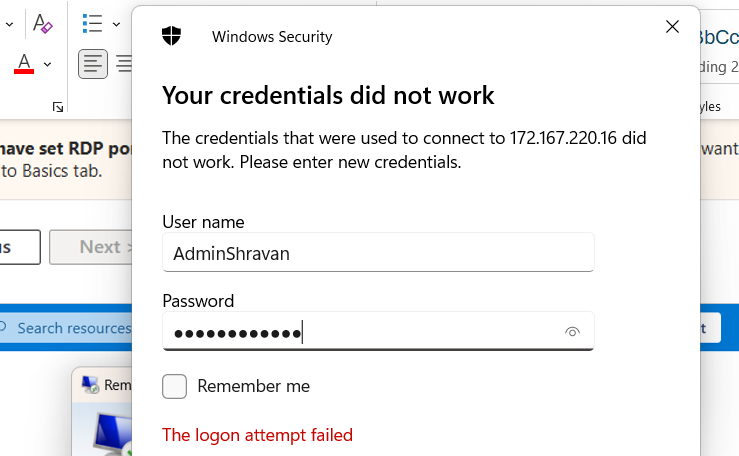


**Task 5: Checking Virtual machine connection: Vm2 from Vm1 using Vnet peering.**

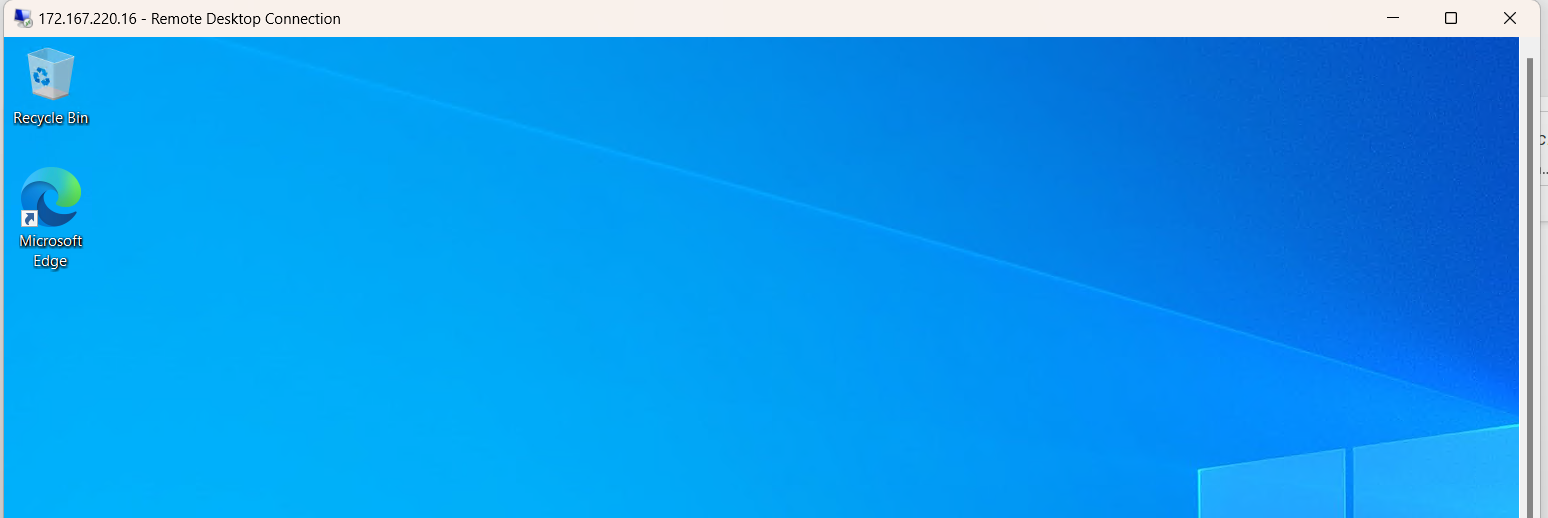
Step1:

Go to resources and click on Vm-1 and take the Public IP of the Vm-1 and RDP the public IP and enter the credentials that we gave while creating the Vm-1 as shown below.



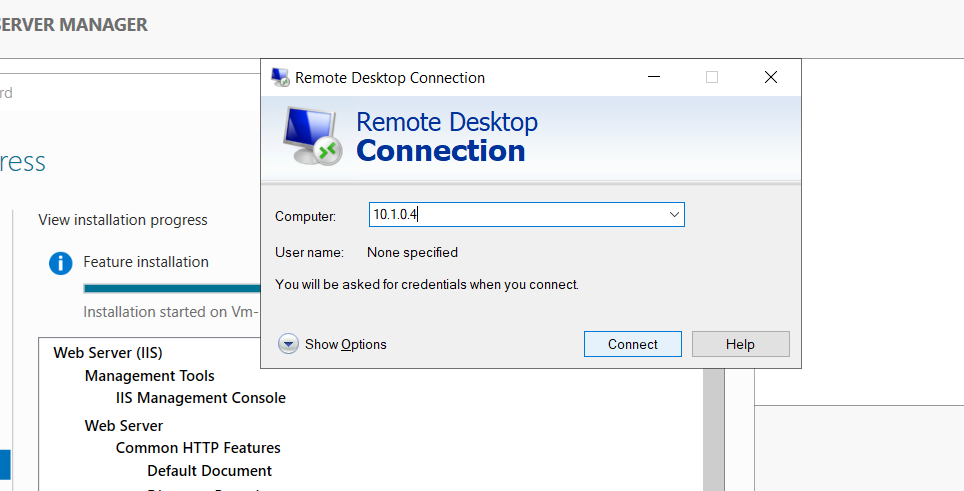
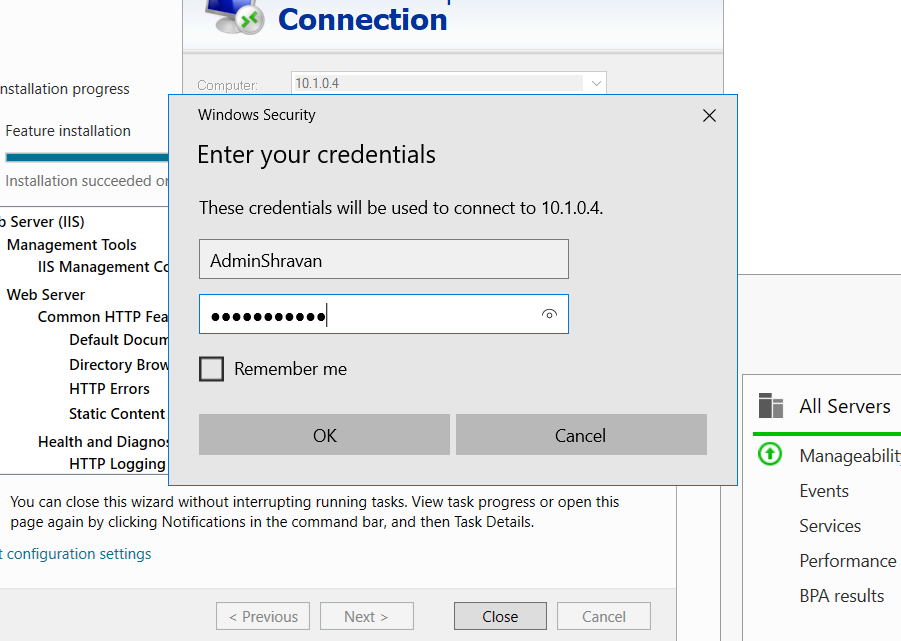


Step2: After connecting to the Server, it will show the below screen.



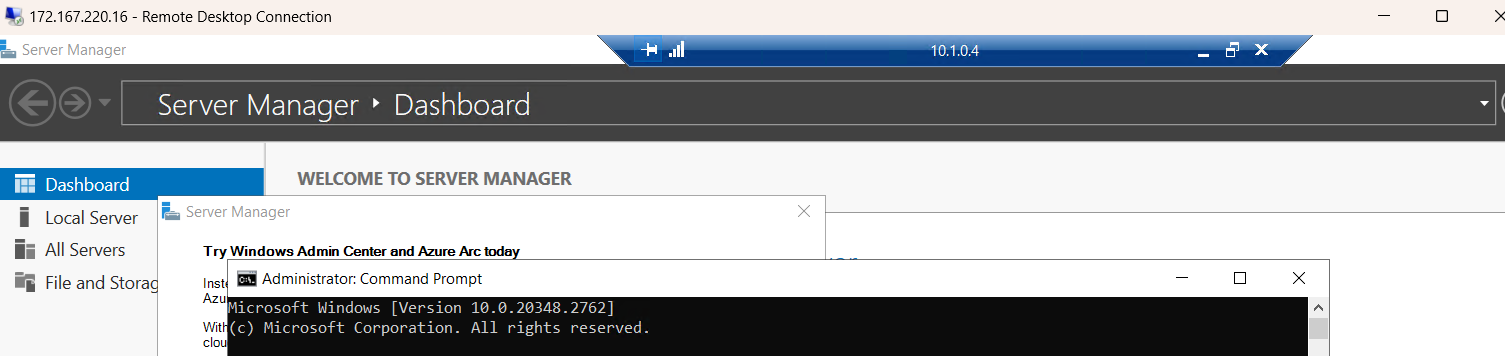
Step3: To check whether Vm2 can be connecting from Vm2:

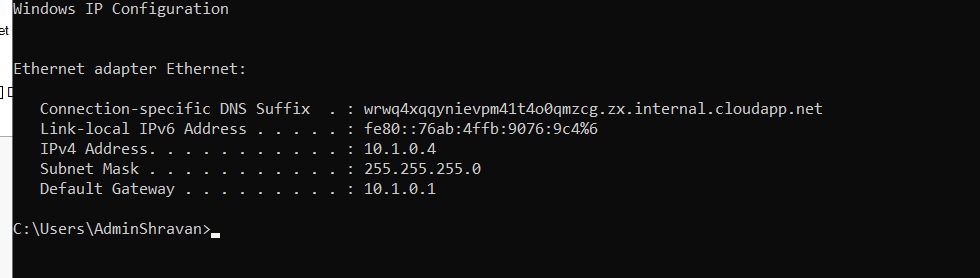
Take the private IP of the Vm-2 and from Vm-1 that we connected earlier RDP the Vm-2 as shown below, we need to provide the credentials that we gave when we created the Vm-2.

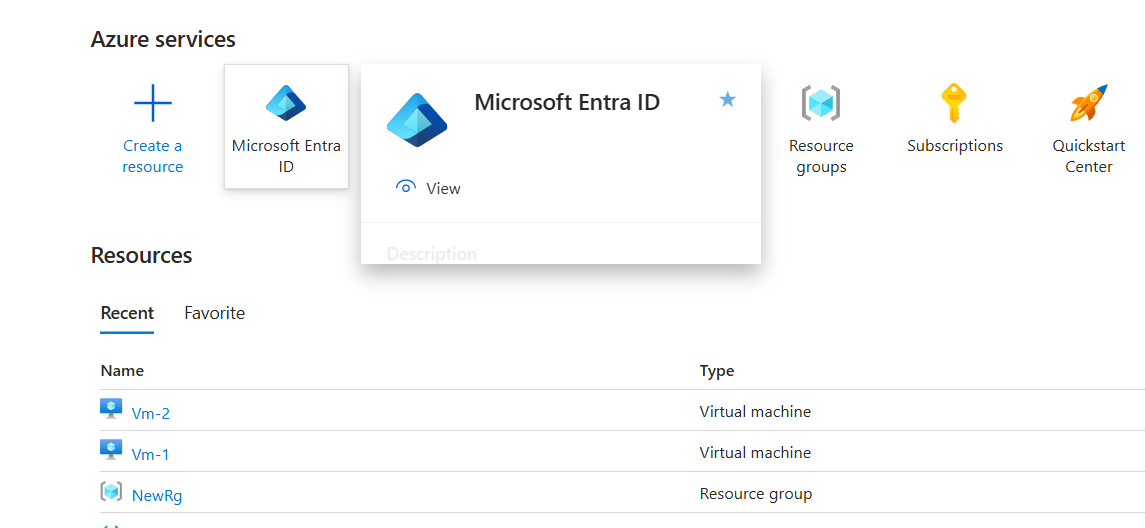


Step4:

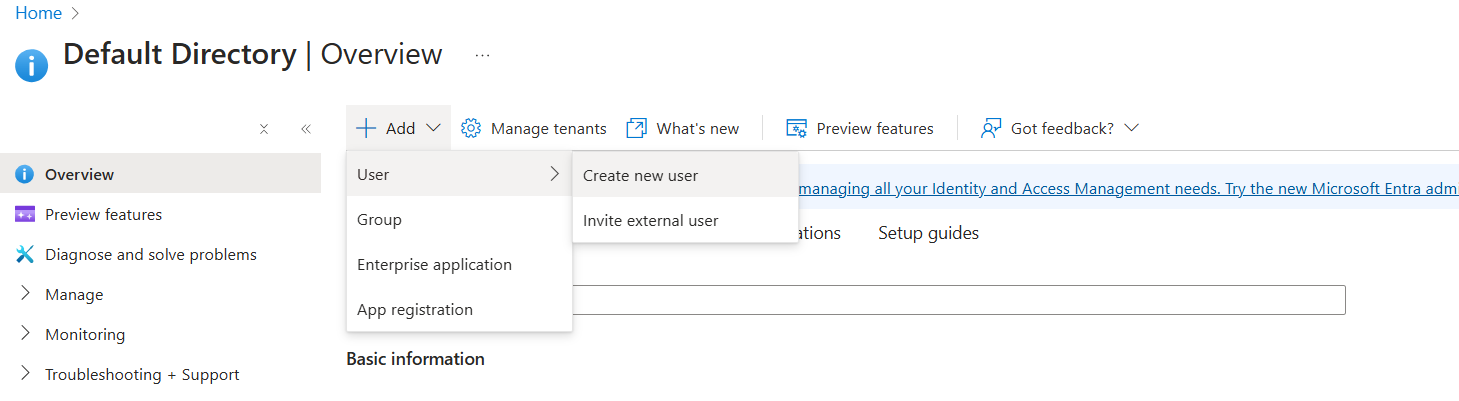
We can verify that we connected to Vm-2 by using Command prompt and checking the IP config , we will see the Ip address of the Vm-2 in the CMD as shown below.





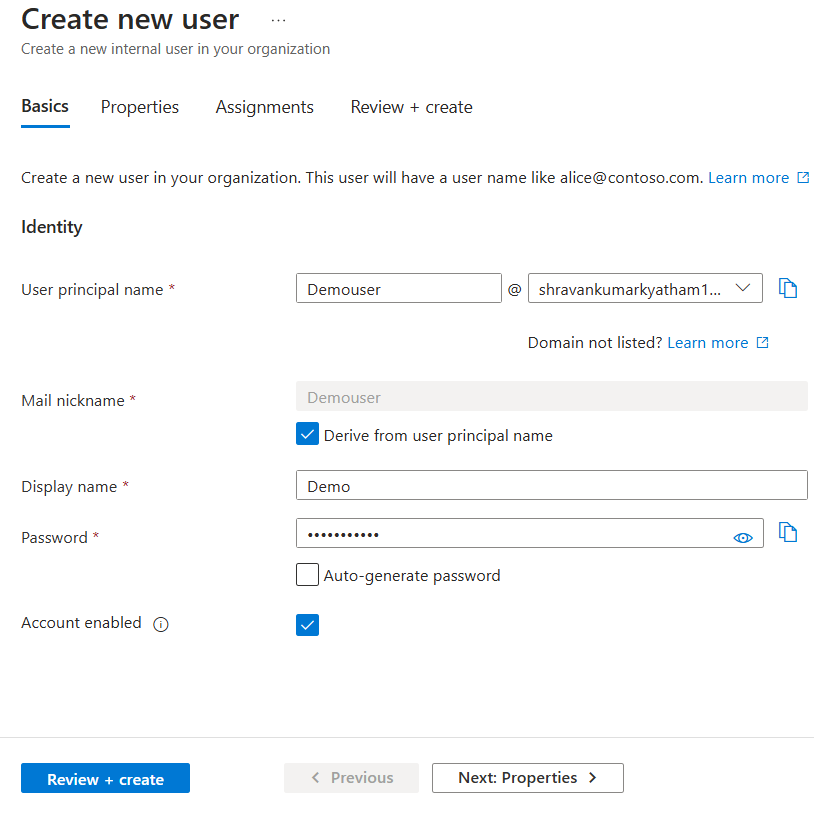
**Task 6: Create user In Azure Active Directory (Microsoft EntraID)**

Step1: Click on Microsoft Entra ID as shown above and click on “ Add” then select user from the dropdown as shown below and choose “ Create new user”.



Step2:

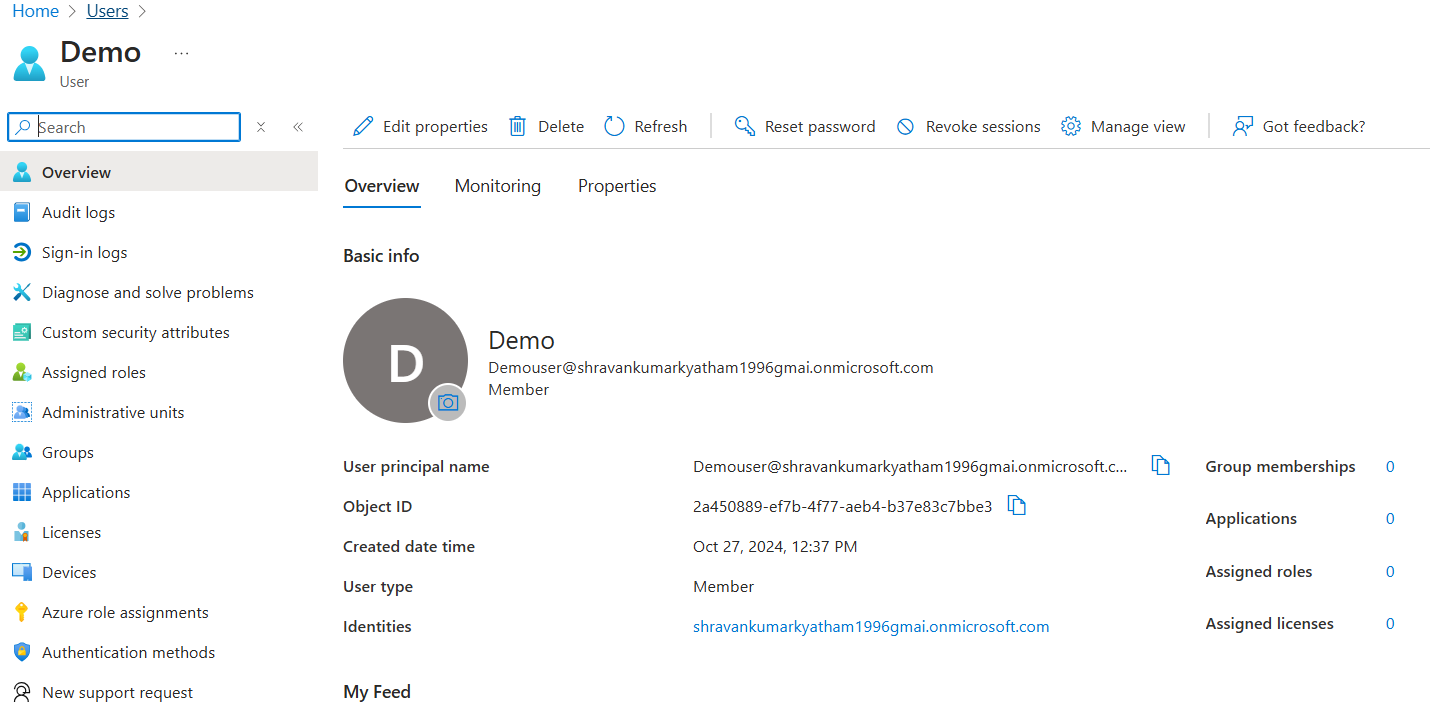
After clicking create new user, below given prompt is shown where we can provide details like , User principal name, display name, set password and enable the account and then click on create button, User will be created.



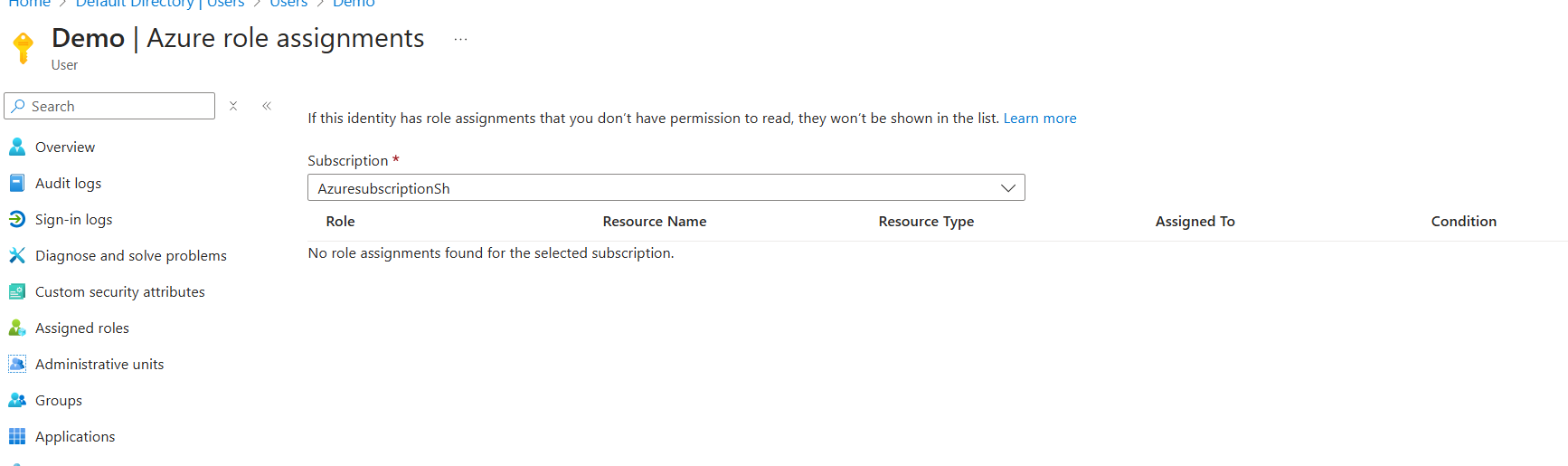
Step3:

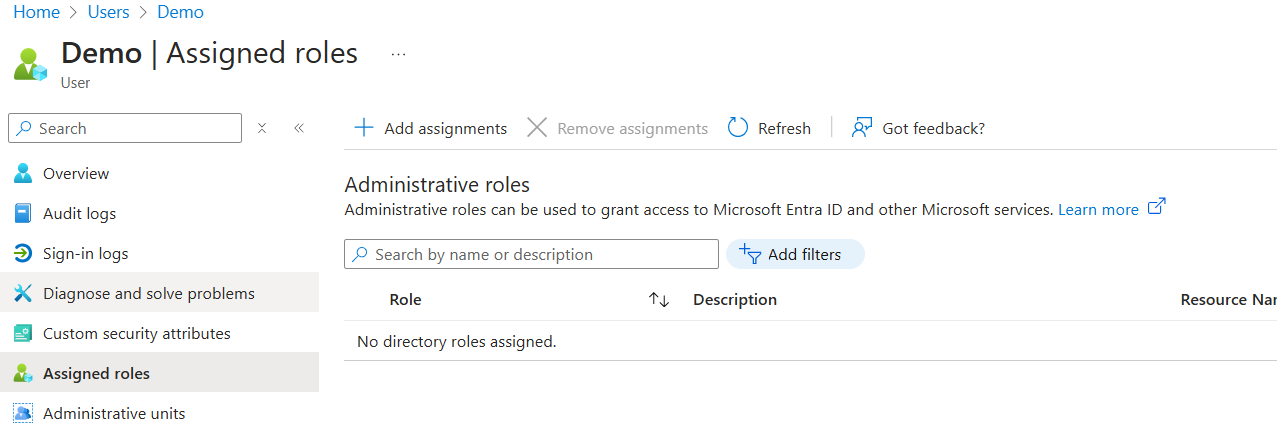
Step3:

Step3:

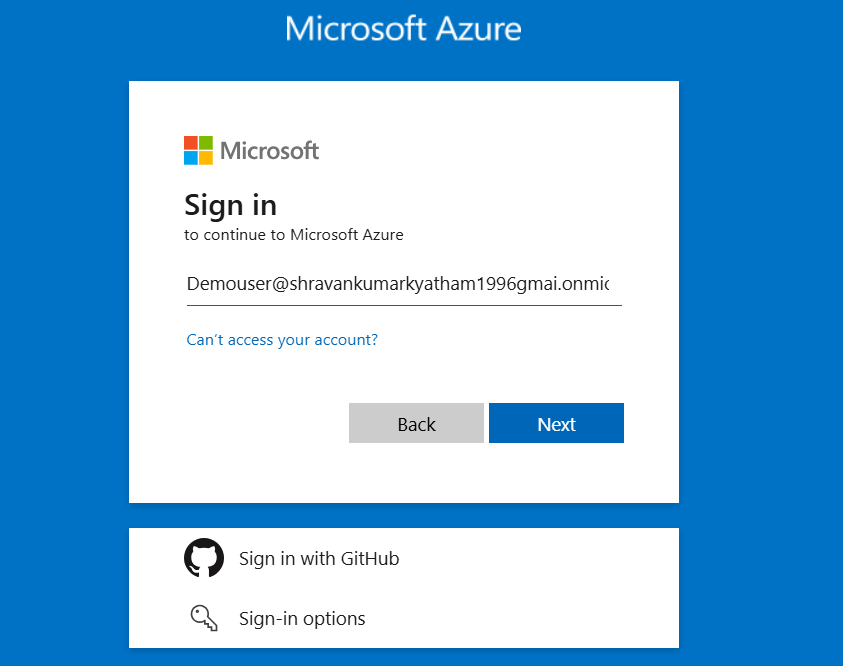
Go to users and check user created as shown below, verify that user is not given any access and having no roles assigned.

We can check here that Demo user is not assigned any role yet from below screenshots.

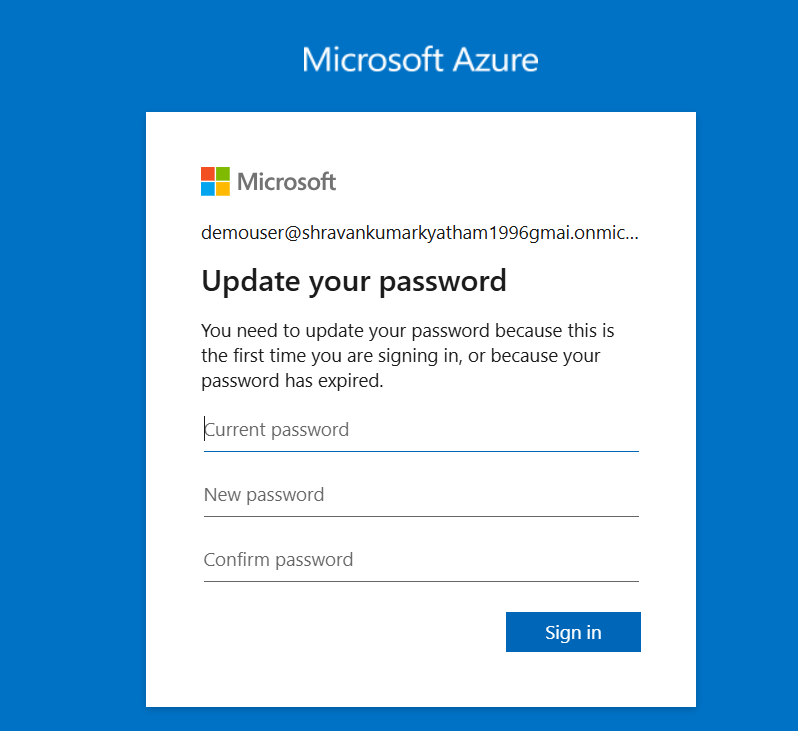
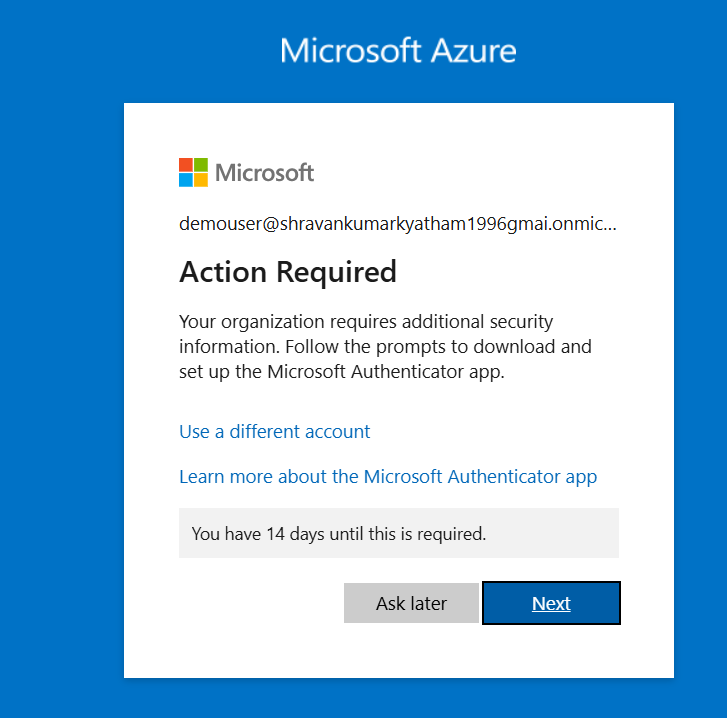


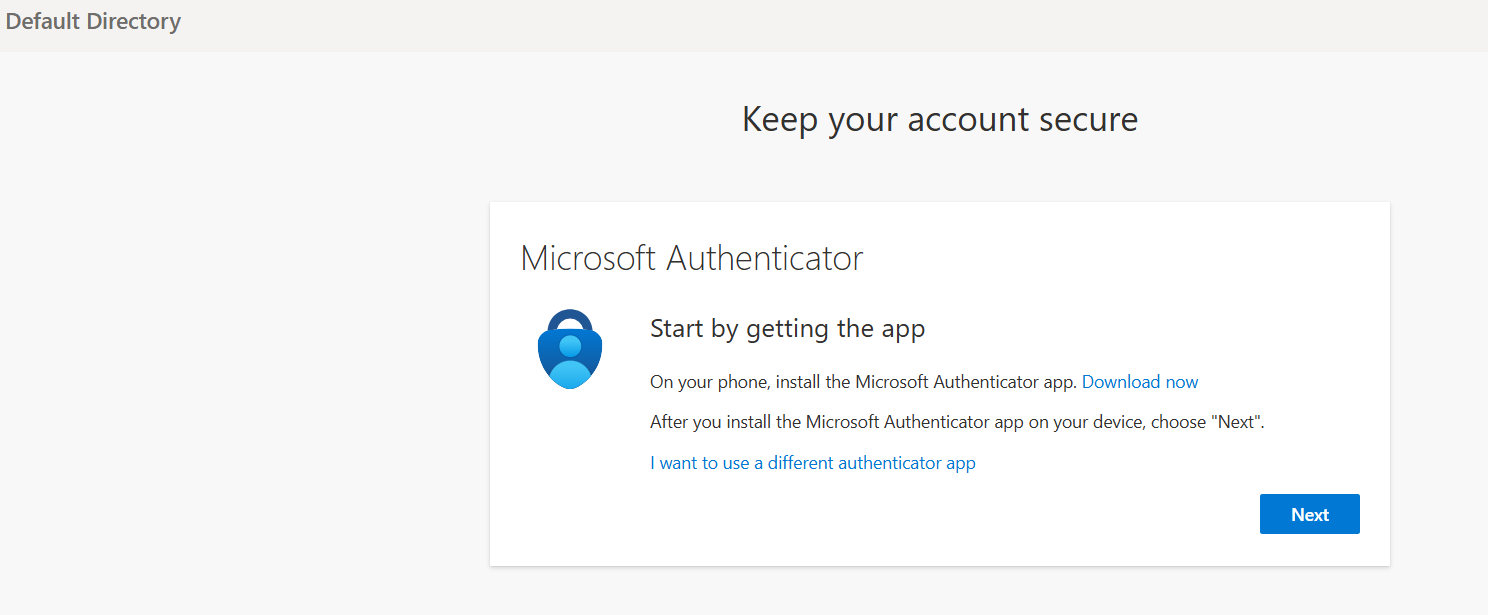


Step5: Logging to Azure portal using demo user to check access. Take the email related to the Demo user from Users in your Microsoft entra Id users. Go to new login page of Azure portal and enter the demo user email as shown here and click next.

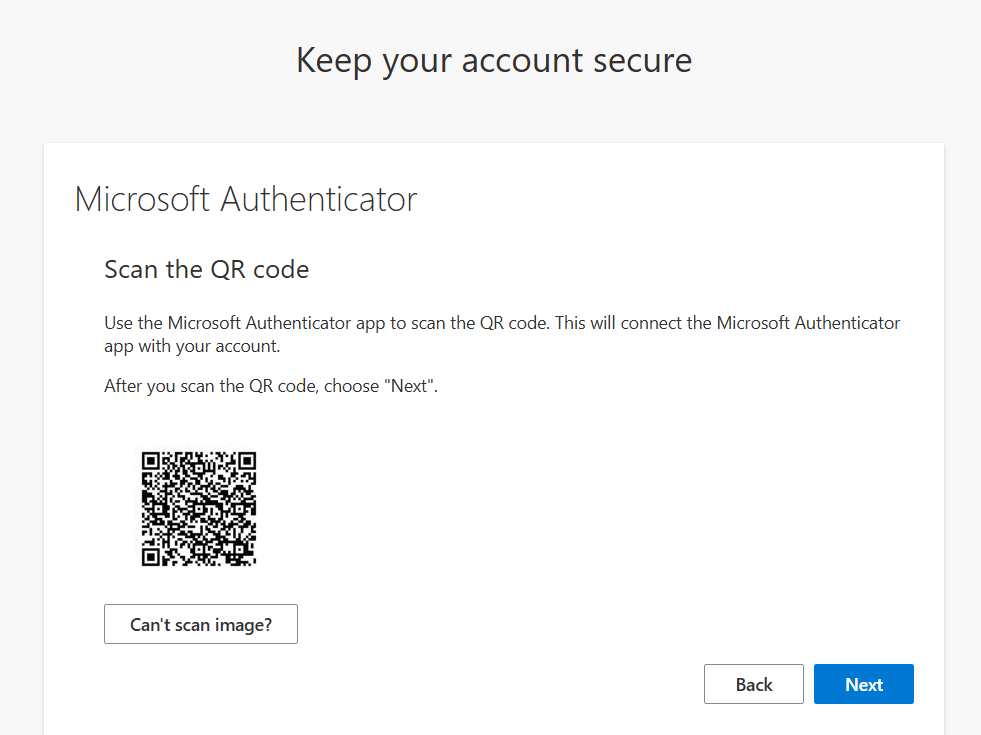


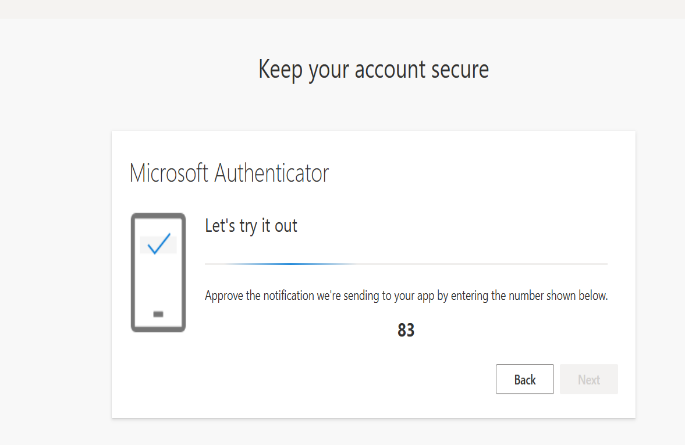
For the first time portal will ask to reset password as security measures, enter the password of the demo user that we gave while creating the user in “current password” and create your own password as shown here and click next in the next screen

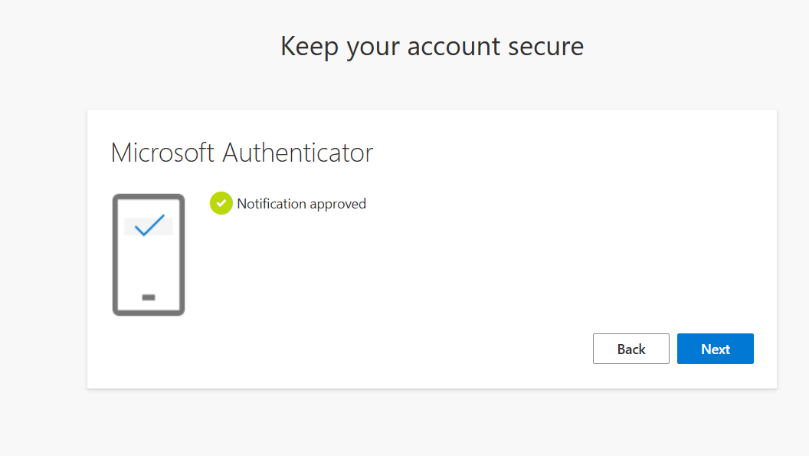


For safety and security, Microsoft Entra ID asks for multifactor authentication as shown below, we need to have authenticator app in mobile to access the portal. Click on next.

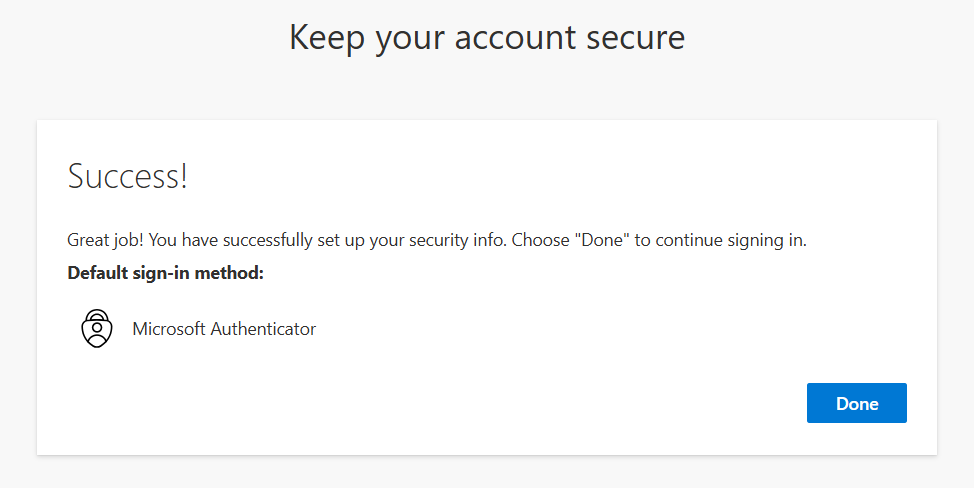
Then the portal will show QR code as shown below, we need scan that QR code by work or school account in authenticator app in mobile.



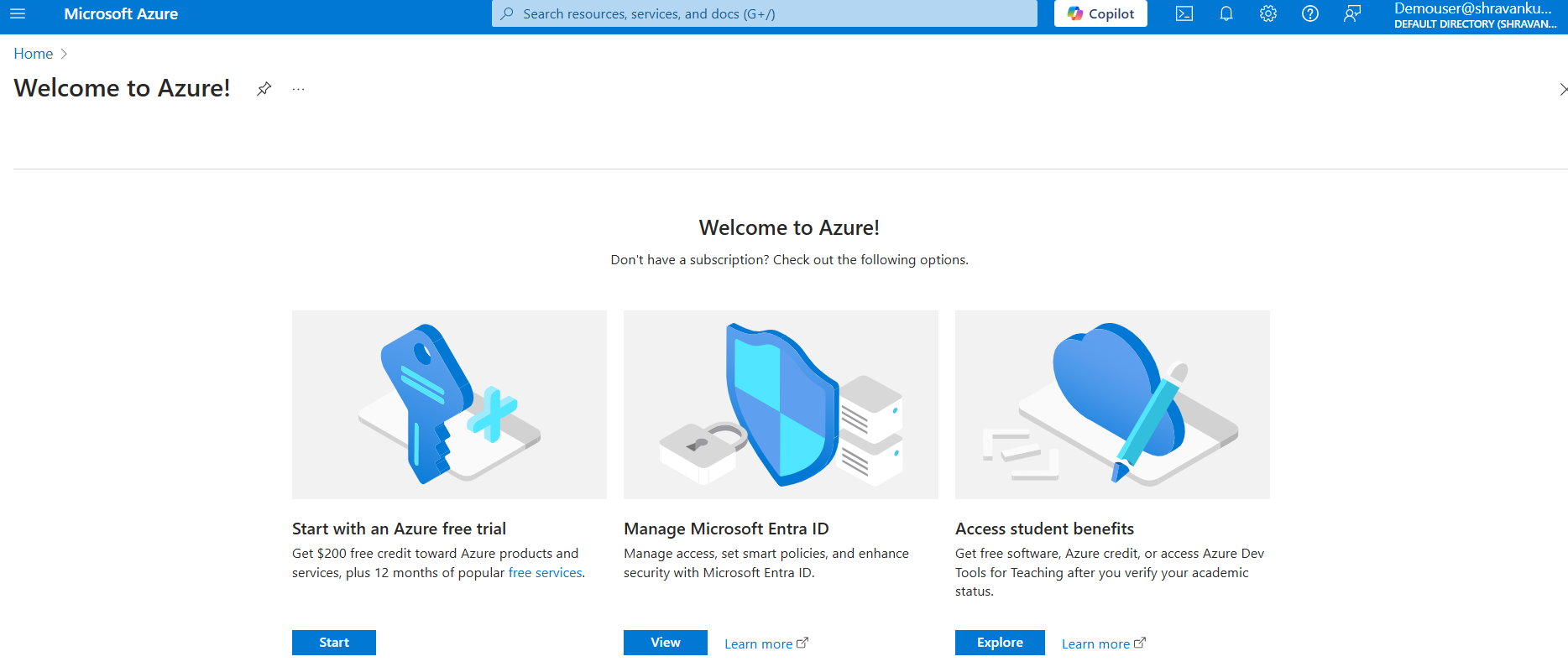
After scanning the QR code, portal will display a number as shown below which we need to enter in the authenticator app and approve the request.



Once the request is approved , then we will receive success message as shown here , click on done, now we can login with new demo user tpo Azure portal.

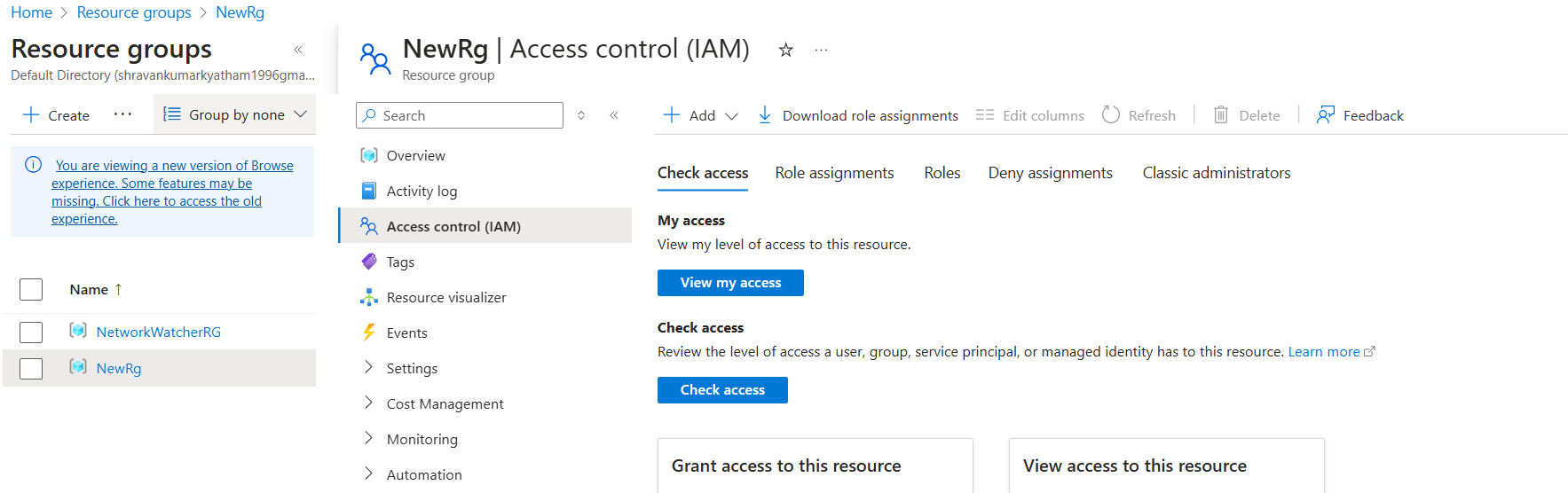


Demo User without any permission we can see any resources because demo user have no access as of now:



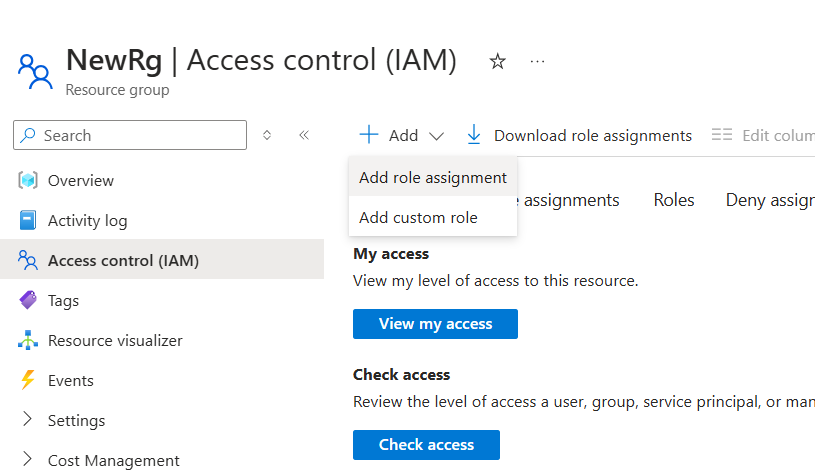
**Task 7: Create Custom Role and Assign to Demo user**

Step1: Go to resource group and select the resource group we created (NewRg)as shown here.

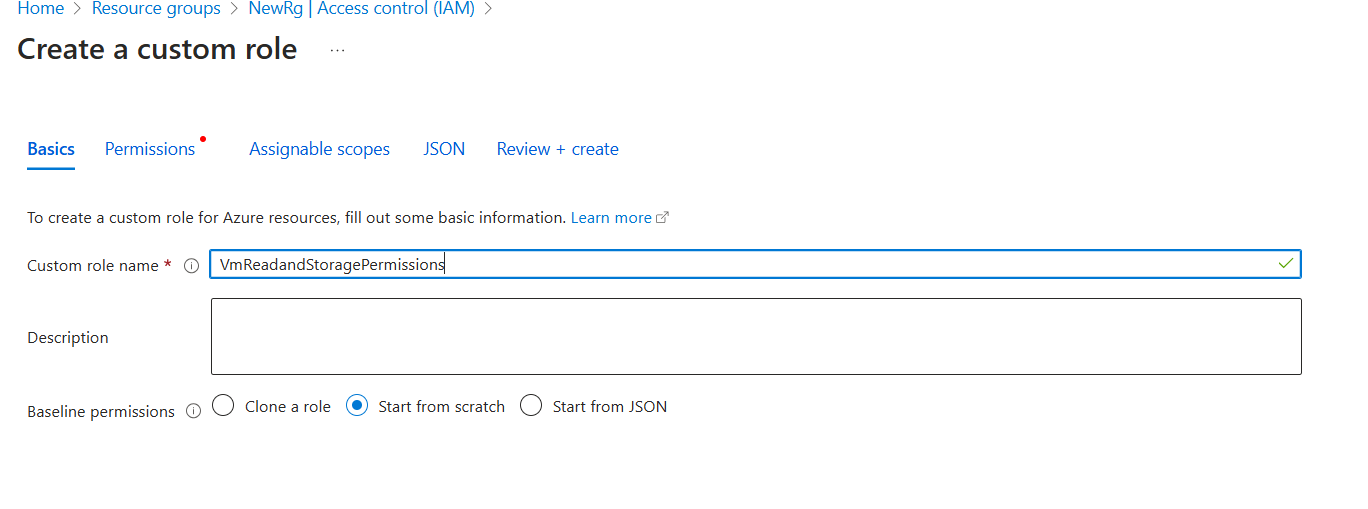


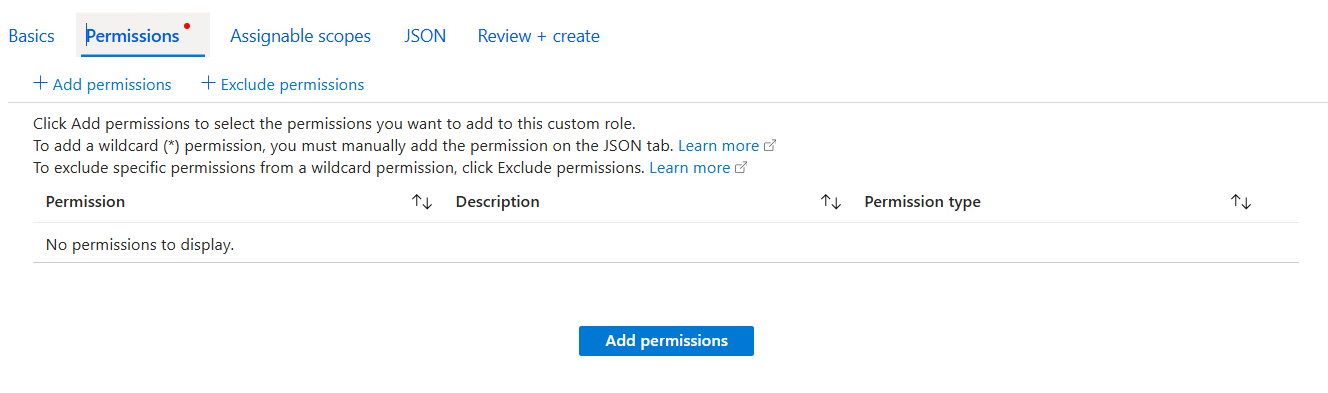
Step2:

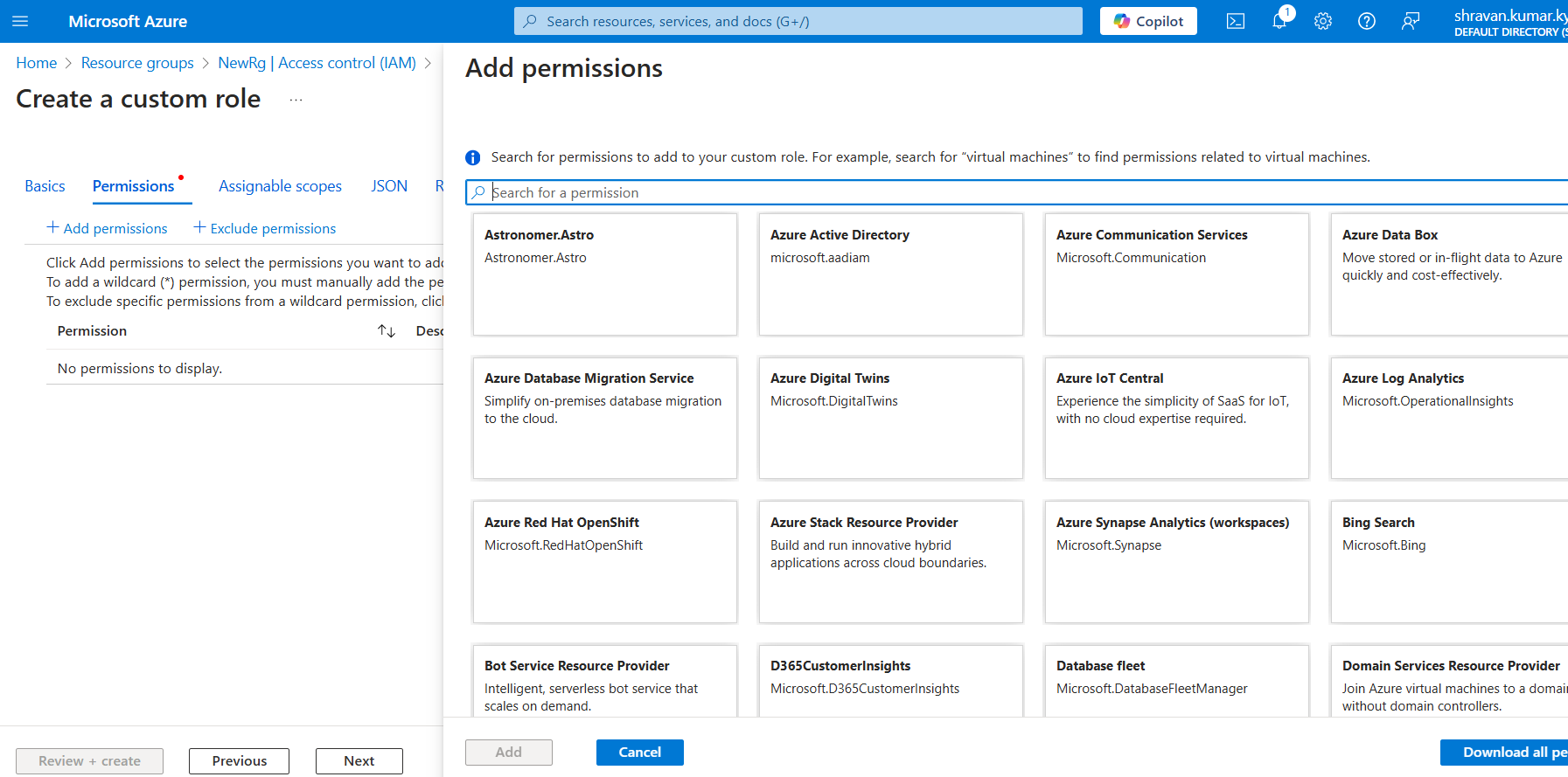
Go to Acess control (IAM) from the menu options and click on Add and select Add custom role as shown below:



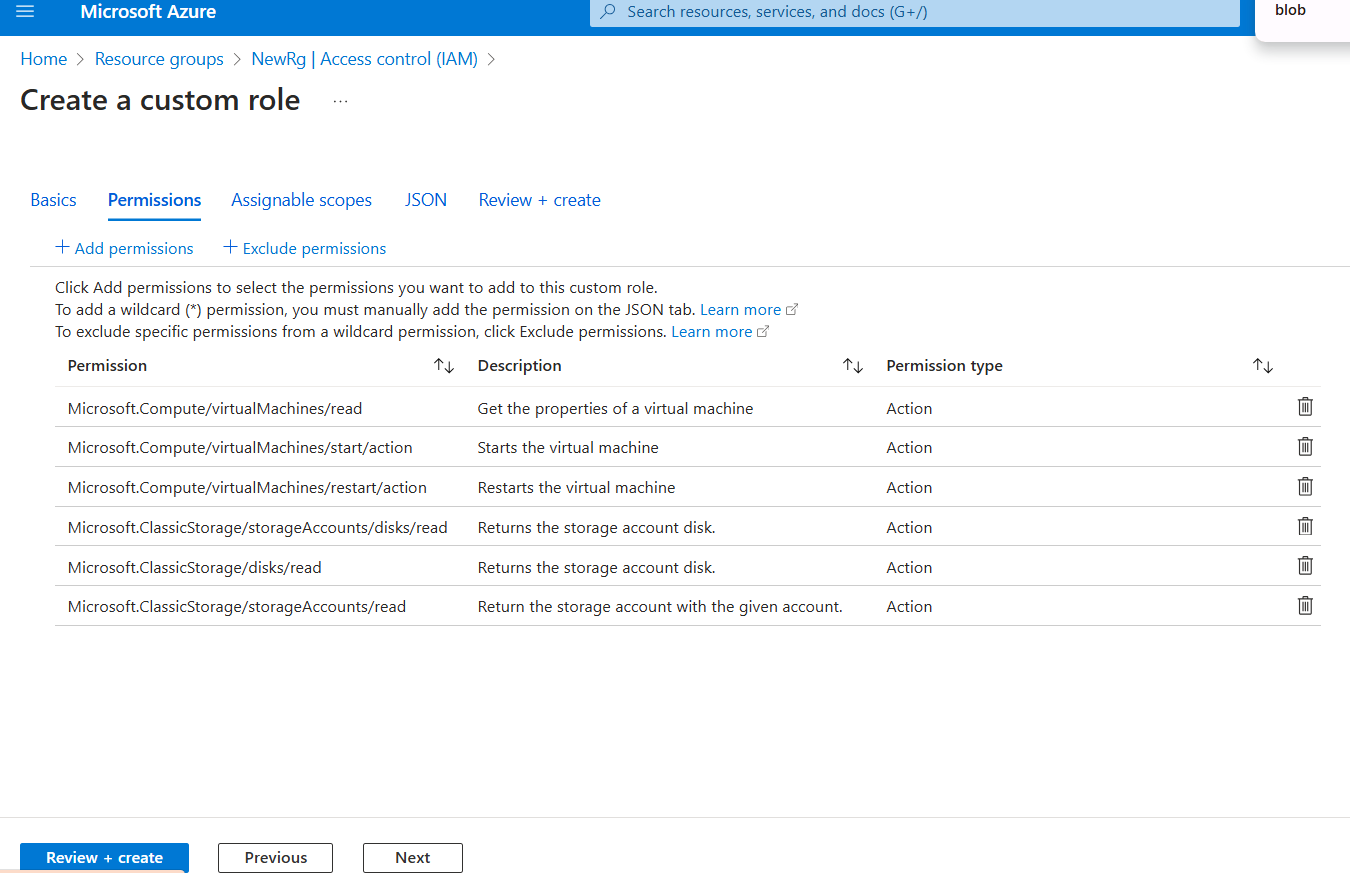
Step3:

When we click on Create custom role, we will get below prompt, here we need to provide role name, description and baseline permissions ( from scratch for new setup) in the basic section as shown here.

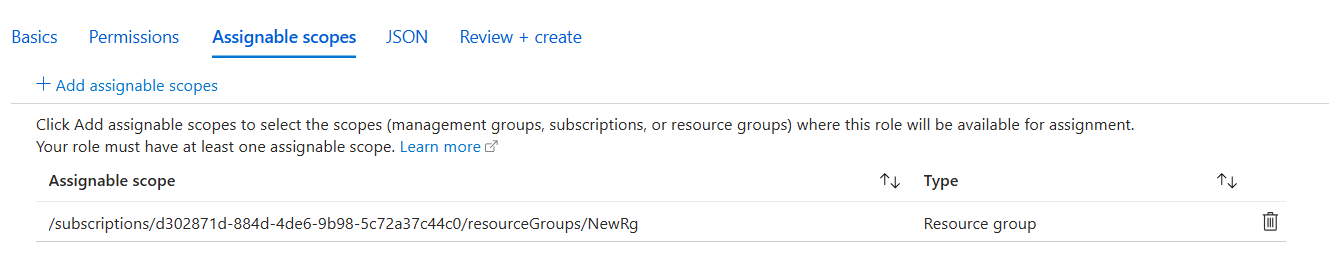
In the next step, go to permissions sections and click on add permissions

The page which allow to search the permissions available and to assign them will look as shown below. Select the required permissions from them.

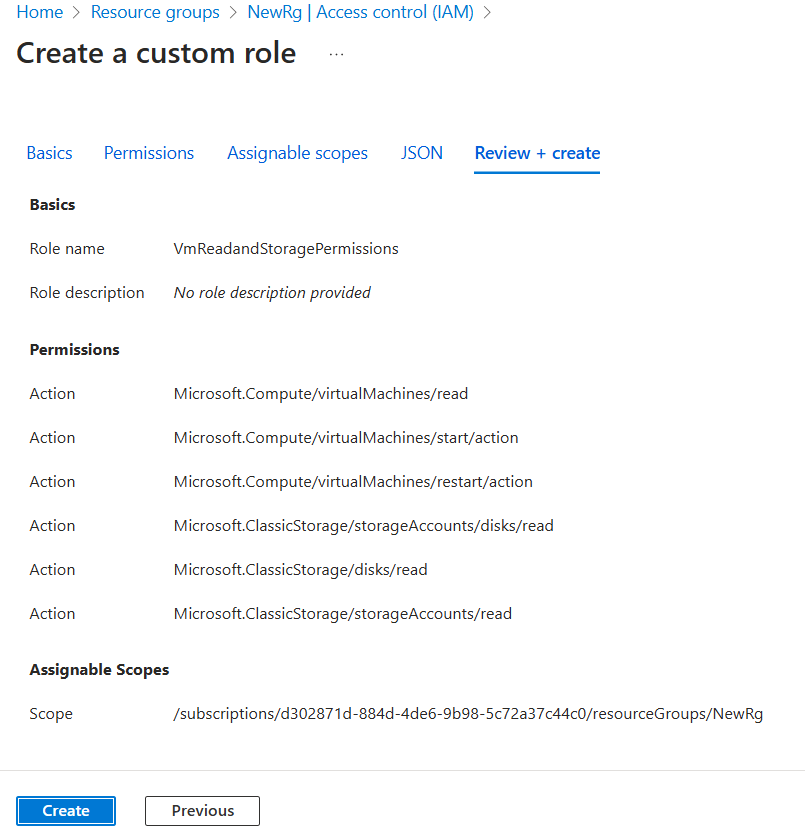
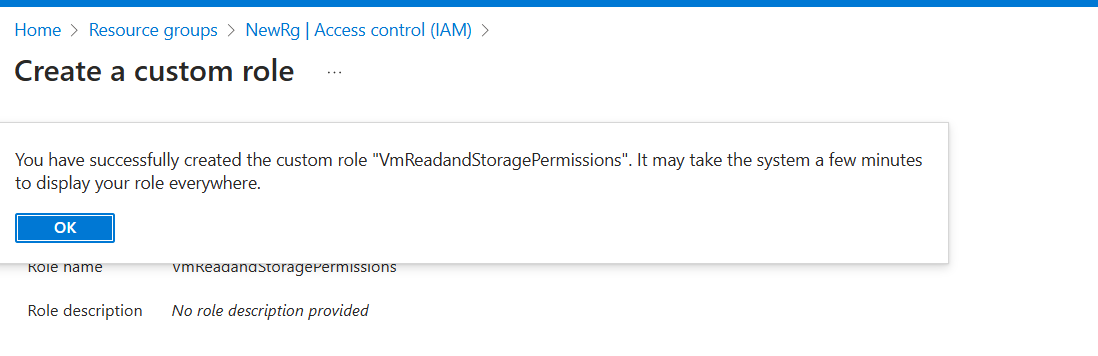
To give access to Start and restart Virtual machines to the users, go to compute permissions ->Microsoft compute/VirtualMachines and add the below mentioned ones and storage read access search for storage and click on Microsoft.Classic.Storage and add read access to storage accounts.



Now go to Assignable Scope and check if we have the resource group in it , if we need to give this role to any other group we can add it here as shown.

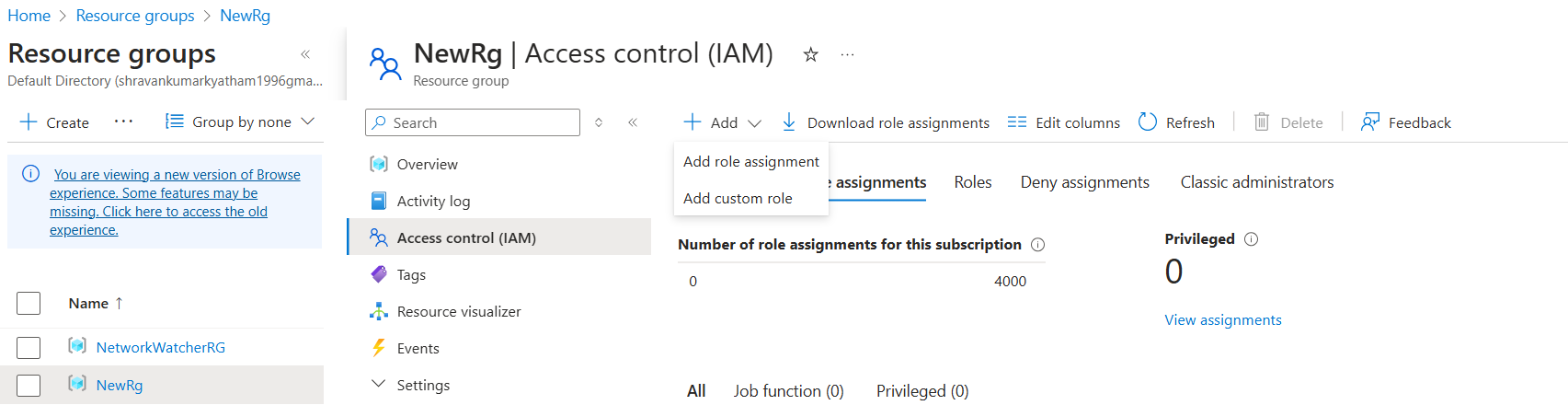


Click on review and create as given below, custom role is created successfully as shown.

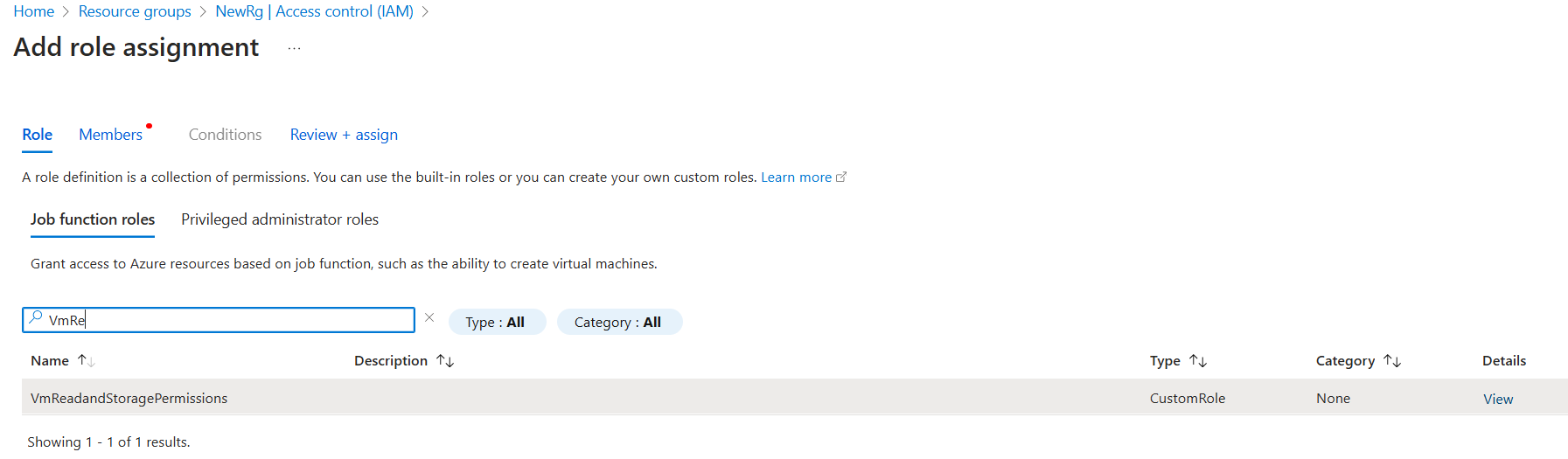


**Task 8: Assigning role to demo User:**

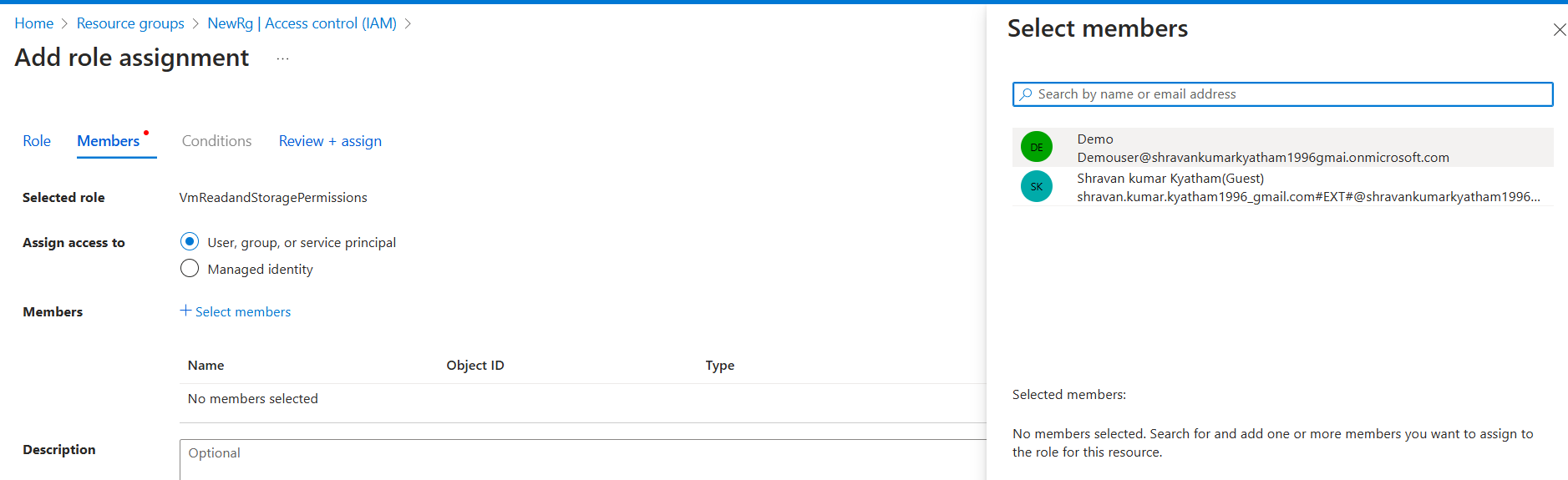
Go to Resource group (NewRg) and click on Access control (IAM) and select “Add role assignment” from dropdown. The screen will be looking like this.



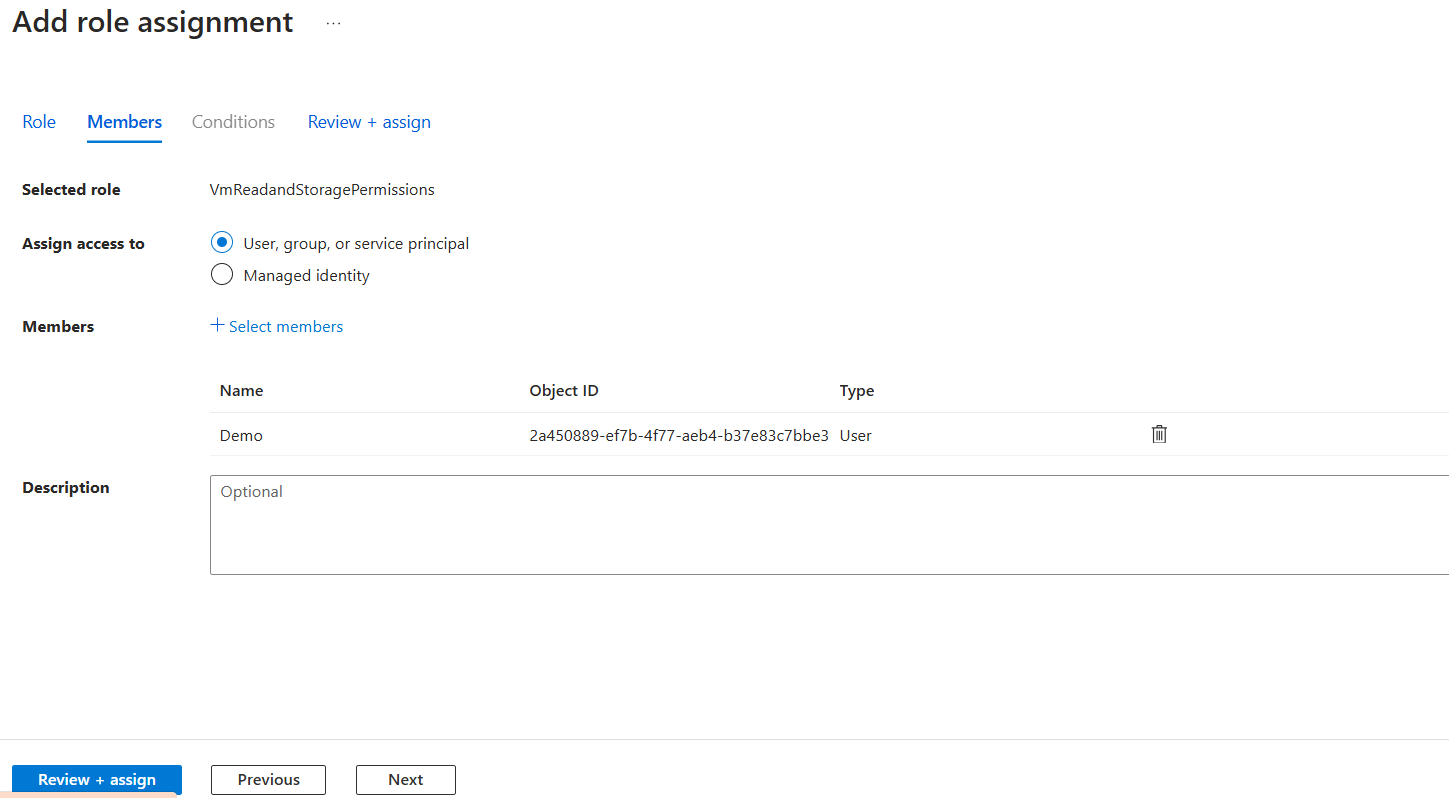
After clicking “Add role assignment, under roles search for the role we created and select it as shown here.



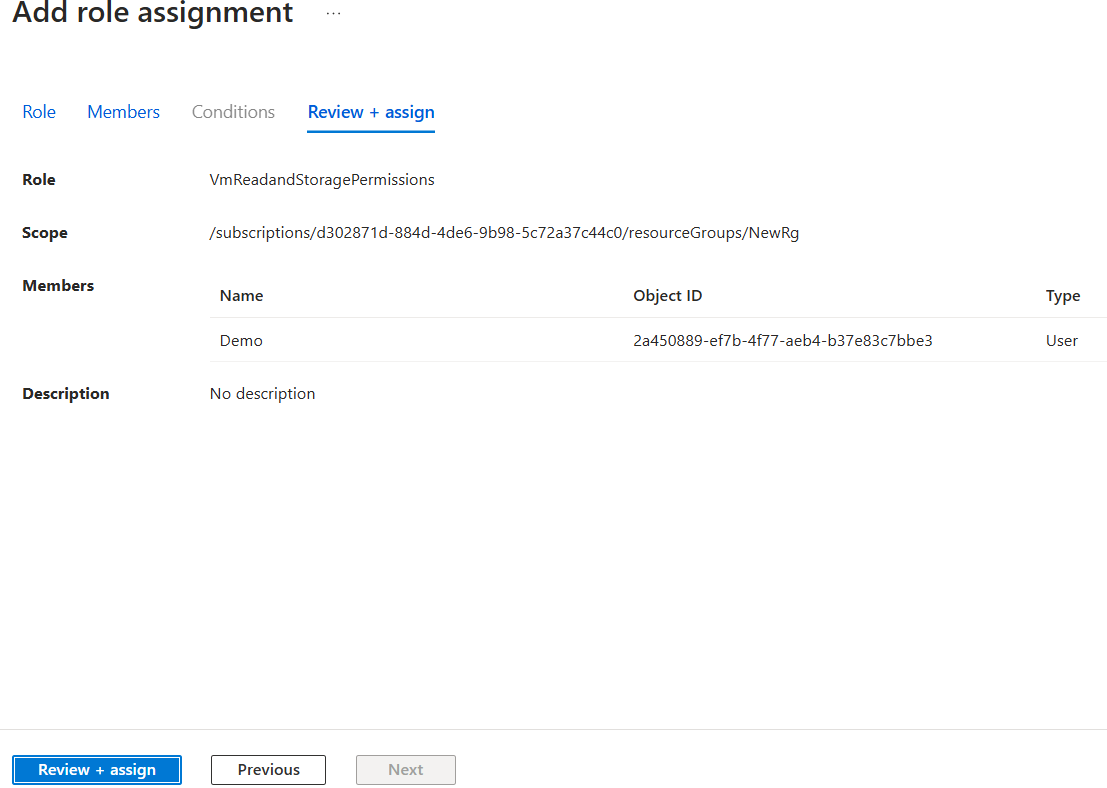
Go to members sections, we can see the role we selected and assign access to either user,group or managed identity, select user, group and click select members, there we see a pop-up with the users present in the Microsoft Entra ID.



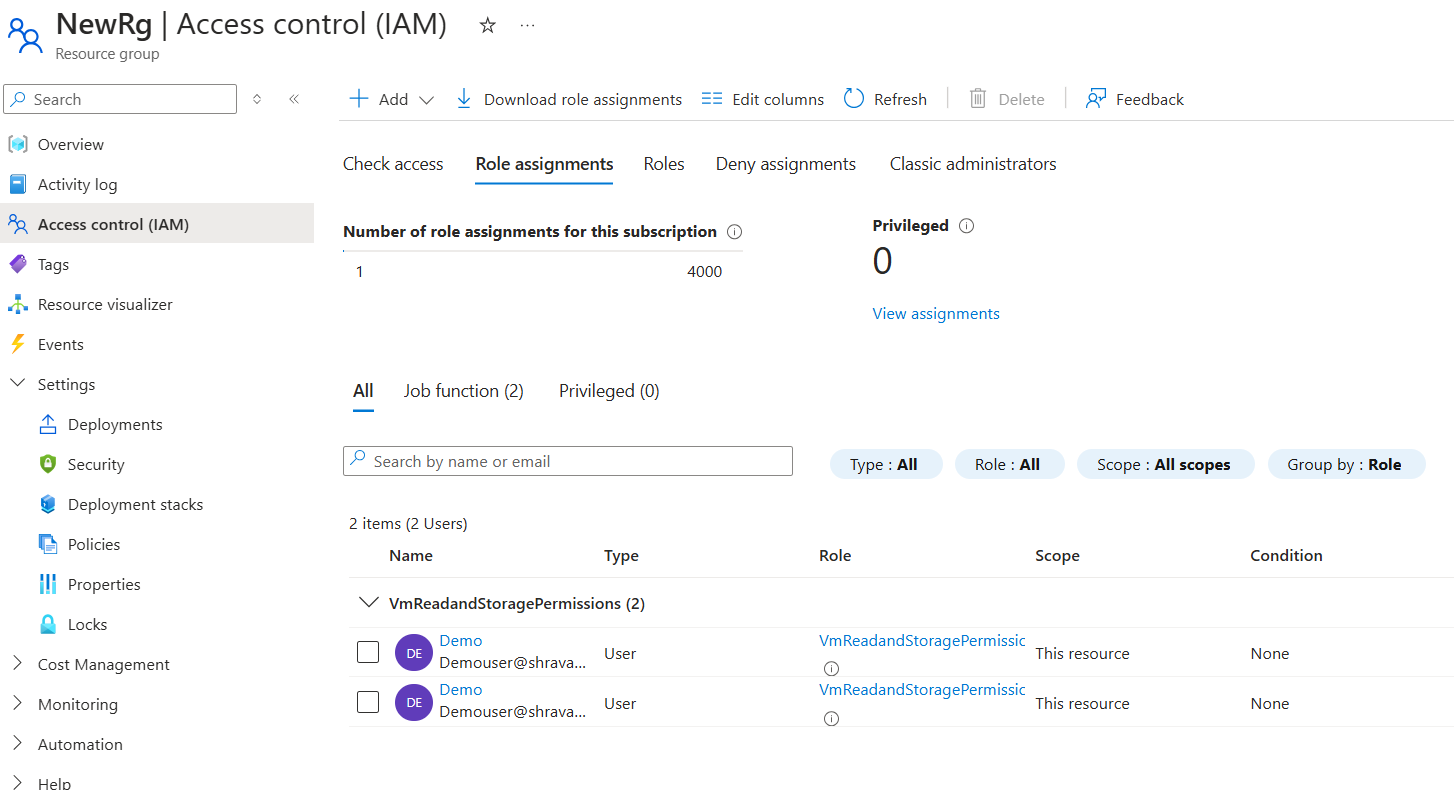
Select demo user and that user will be added under member as given below.



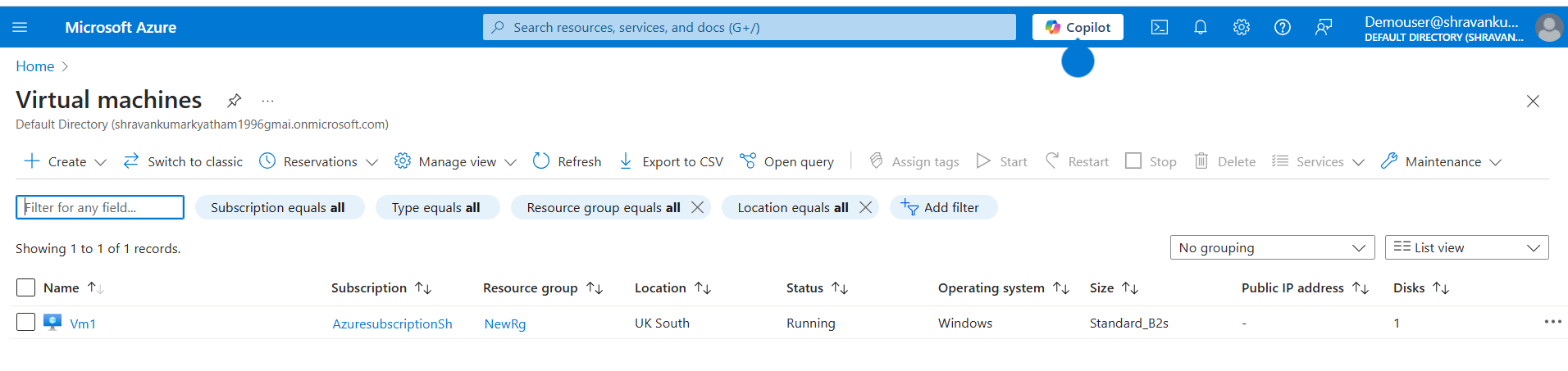
Now review and create and assign the role as shown here.



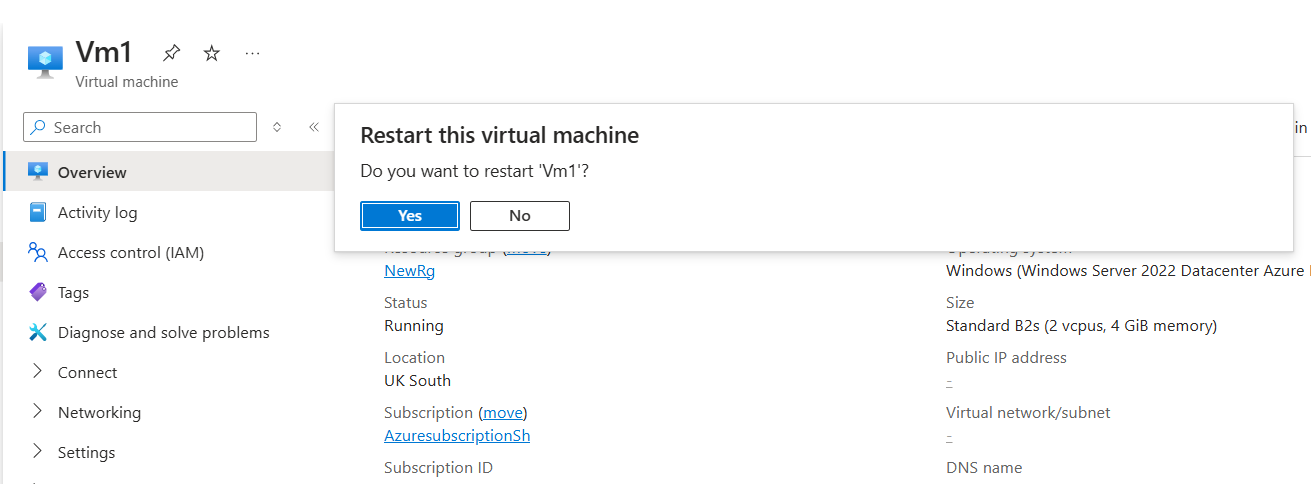
We can see here, in the resource group role assignments, demo user is assigned some roles that we created. It is shown here.



**Verification of Custom role access given to Demo User:**

We can verify that demo user got access by login with refreshing the browser where we logged in to azure portal using demo user credentials and we can see now demo user is able to access the Virtual machine shown in below screenshots.

The scenario where demo user is able to restart the Virtual machine is shown here.



If we try to delete the Virtual machine using demo user, we will get error as shown here, as the user is not having access to perform this action. Demo user have only read access to Virtual machines.

