**Azure Case study— **

Nilavembu Herbs provides a safer alternative to modern medicine wherever possible and to offer simple, effective and safe remedies for common problems. spreads awareness about the medicinal uses of these natural and safe herbs all over the world and to make it easily available through their online store for all those who want to enjoy its benefits

Nilavembu Herbs requires

* A low-cost solution based on demand of dynamic business conditions.
* As the business expands across EastUS and SEA, they would like to have their DataCenter virtualised using cloud computing.
* Critical Data should be made available in case of disaster

**Requirement for SEA region-**

* 2 web servers with 99.95% high availability
* These web services has to be utilised with proper balance with client affinity with Public IP
* Selected web servers should be reachable via RDP from internet
* A jump port should accessible from internet to upload contents to web servers.
* Protect web server traffic restricted to allowed based on ip addresses which will be updated as warranted
* Enable backup for WebServers
* Have alert generated in case of 80% above cpu usage

**Requirement for EUS region-**

* EastUS server (Server11) should be accessible from internet via public IP
* Establish secure Connection to SEA-EUS Azure sites
* All servers should be reachable with internal ip addresses

**Storage requirement-**

* EUS based resources should provide data resiliency in case of azure datacentre failure.
* The storage should be accessible by applications with secure access. provide access urls and keys.
* Sales manager should access his resource from windows explorer.
* SEA data resources must provide high resiliency in case of even multiple azure data center failures

**Resource management-**

* Create Vmadmin user who can manage all VM in the subscription
* Create Backup\_admin user who can manage backup only in EUS servers in EURG

**Deployment of SEA region requirements-**

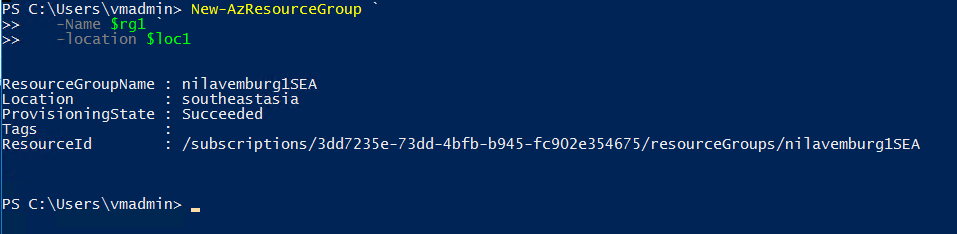
* 2 web servers with 99.95% high availability
* These web services has to be utilised with proper balance with client affinity with Public IP
* Selected web servers should be reachable via RDP from internet
* A jump port should accessible from internet to upload contents to web servers.
* Protect web server traffic restricted to allowed based on ip addresses which will be updated as warranted
* Enable backup for WebServers
* Have alert generated in case of 80% above cpu usage

**2 web servers with 99.95% high availability**

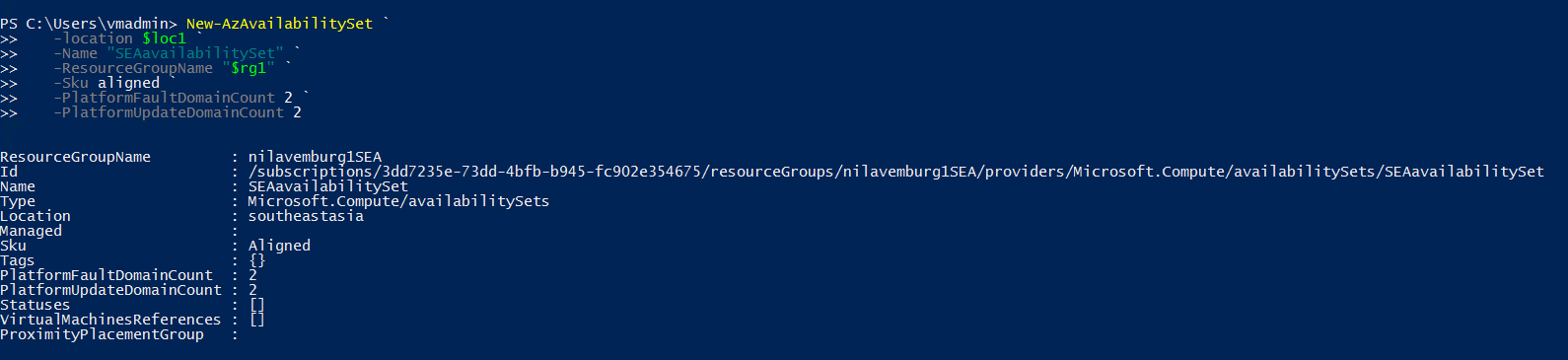
**Let’s create a Resource Group for SEA region, I have stored the value of resource group and location name as below -**



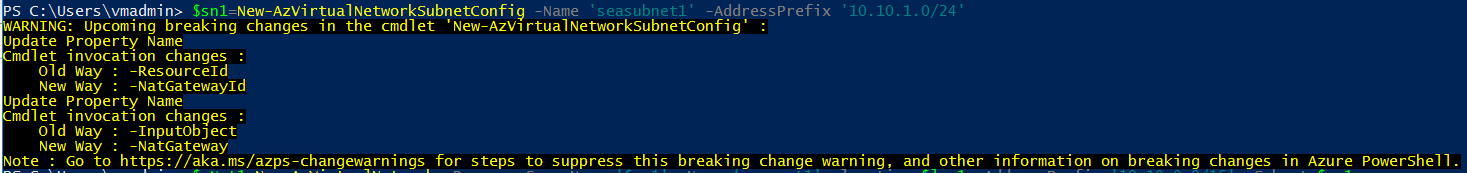
**We will create our first resource group (SEA resource group)-**



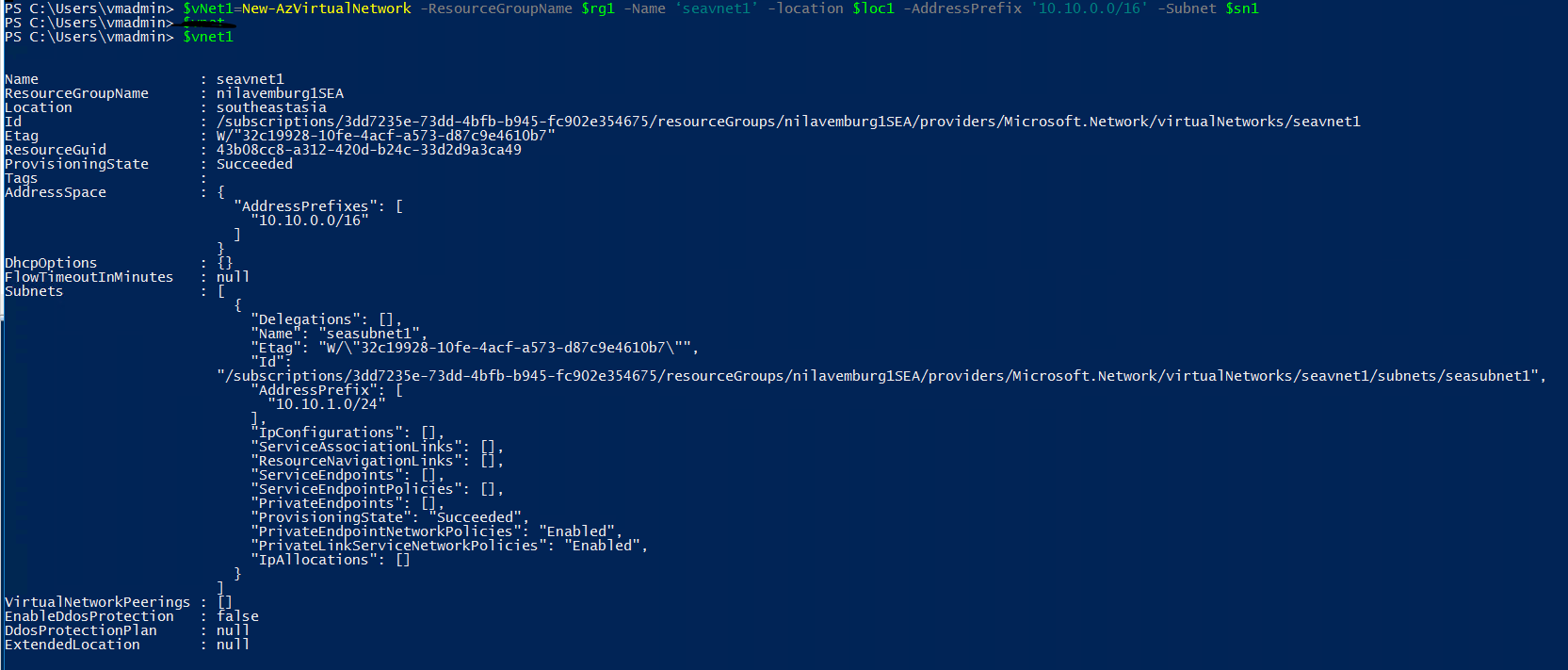
**As the requirement is 99.95% availability, we will configure an availability set and will add the web servers to the AvSet.**



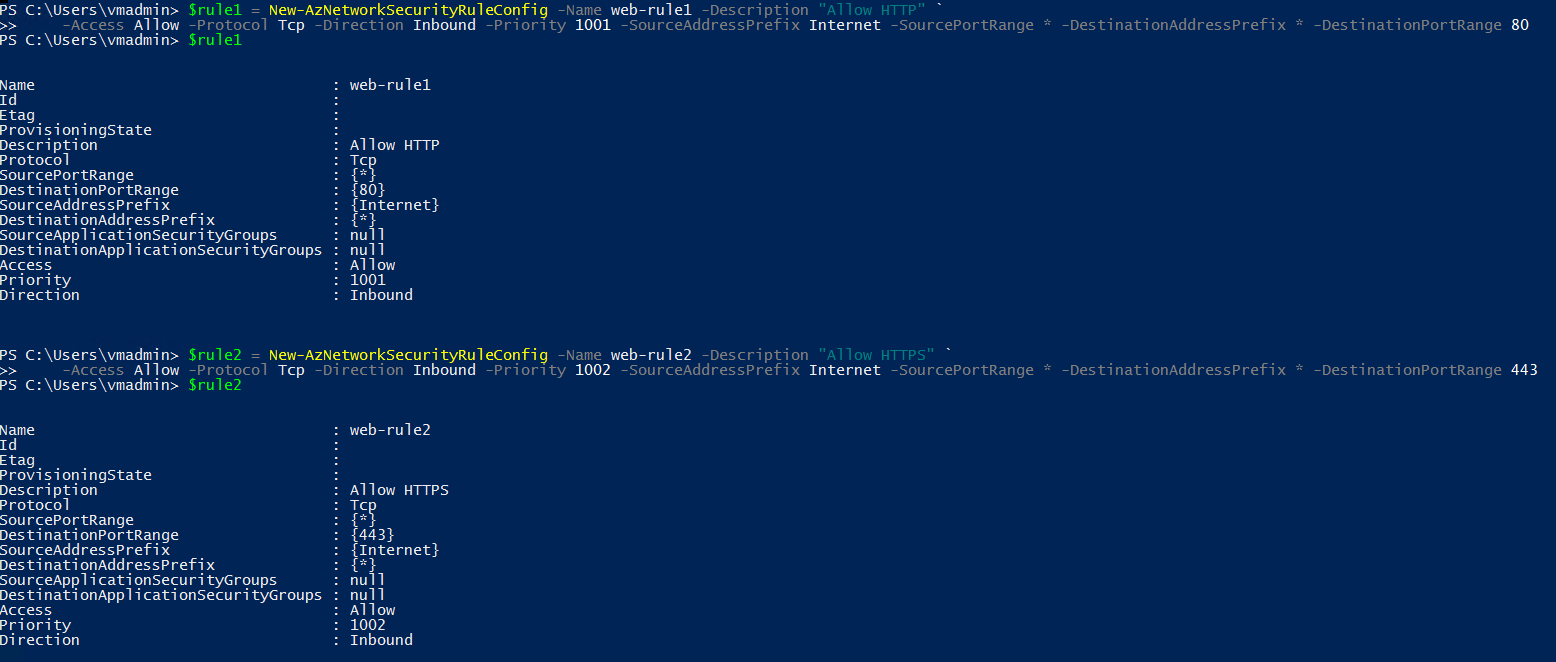
**I have created below subnet that I will associate with the SEA vNet-**



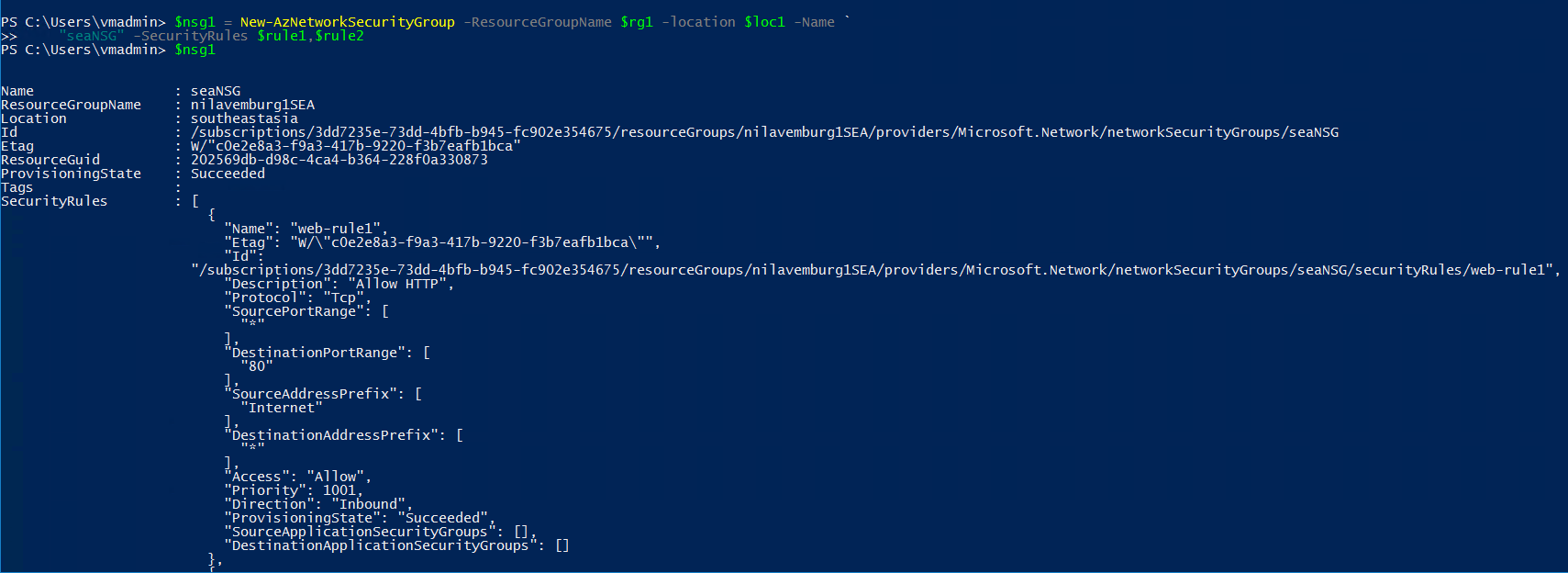
**Creating Virtual network for SEA region associating the subnet that we created in previous step-**



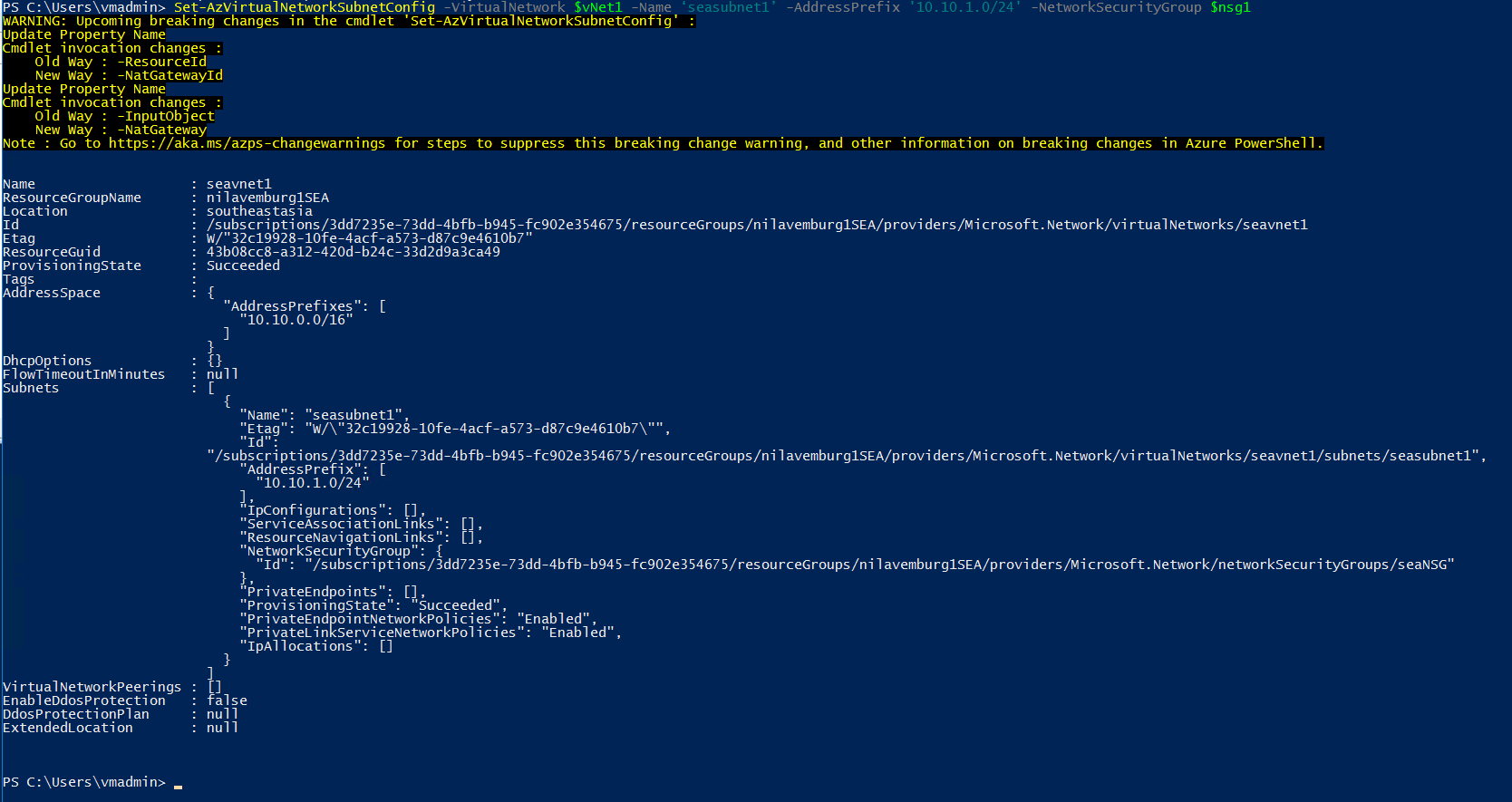
As we will require NSG for controlling the network traffic, we will create rules that we can later associate to the NSG.



We will add above rules to the NSG with inbound http, https Allow rules.



Now as we need to apply the NSG to both the webservers, we will associate the NSG created above to the subnet that we had created earlier.



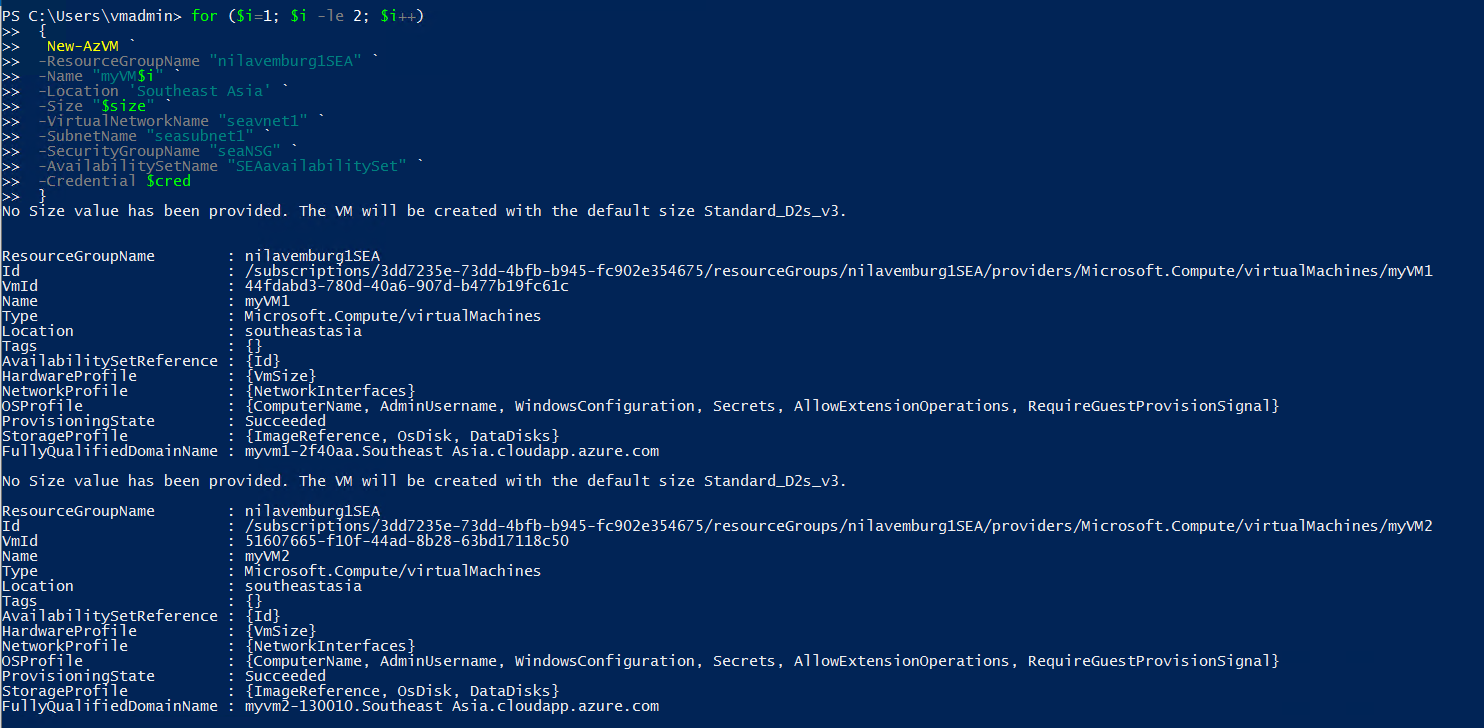
Input credentials for the VMs that are to be created.



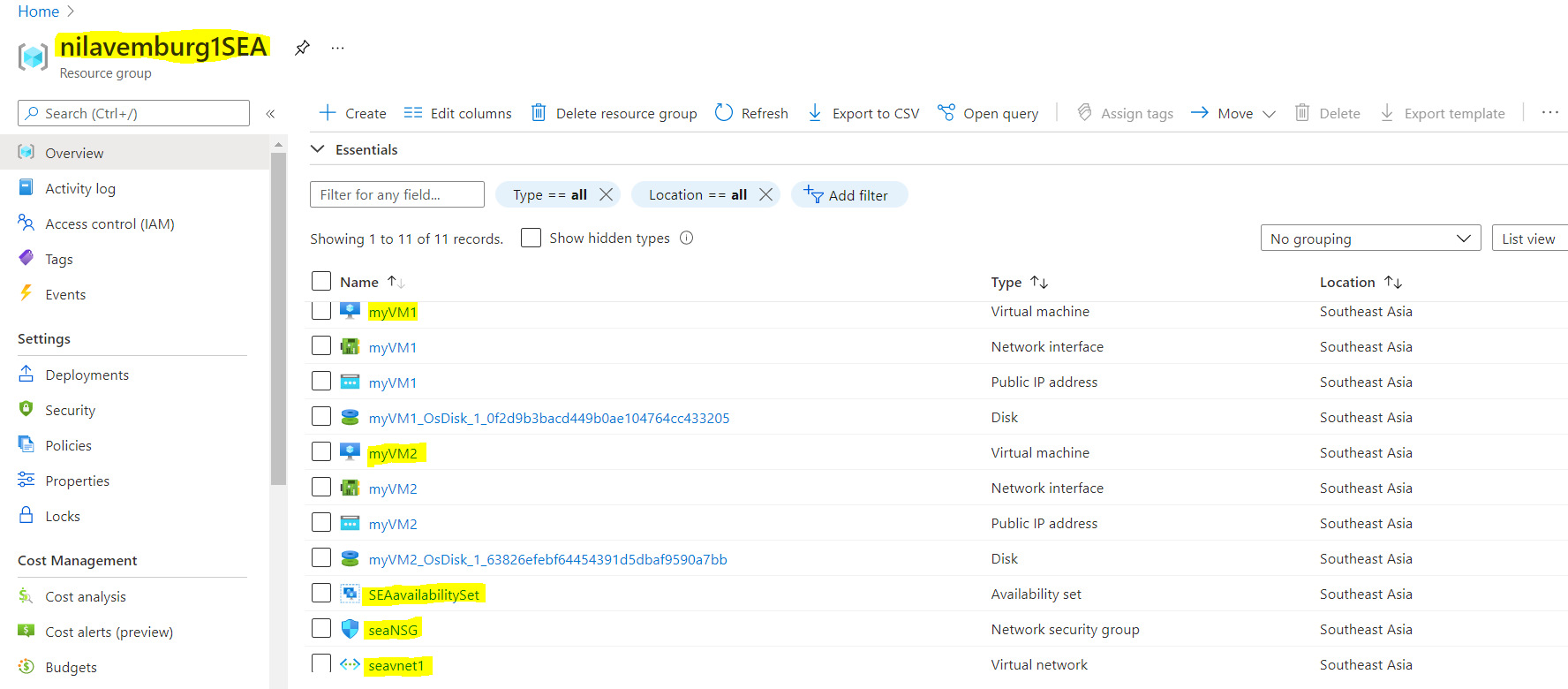
I have specified VM size as it the default VM size was not available.



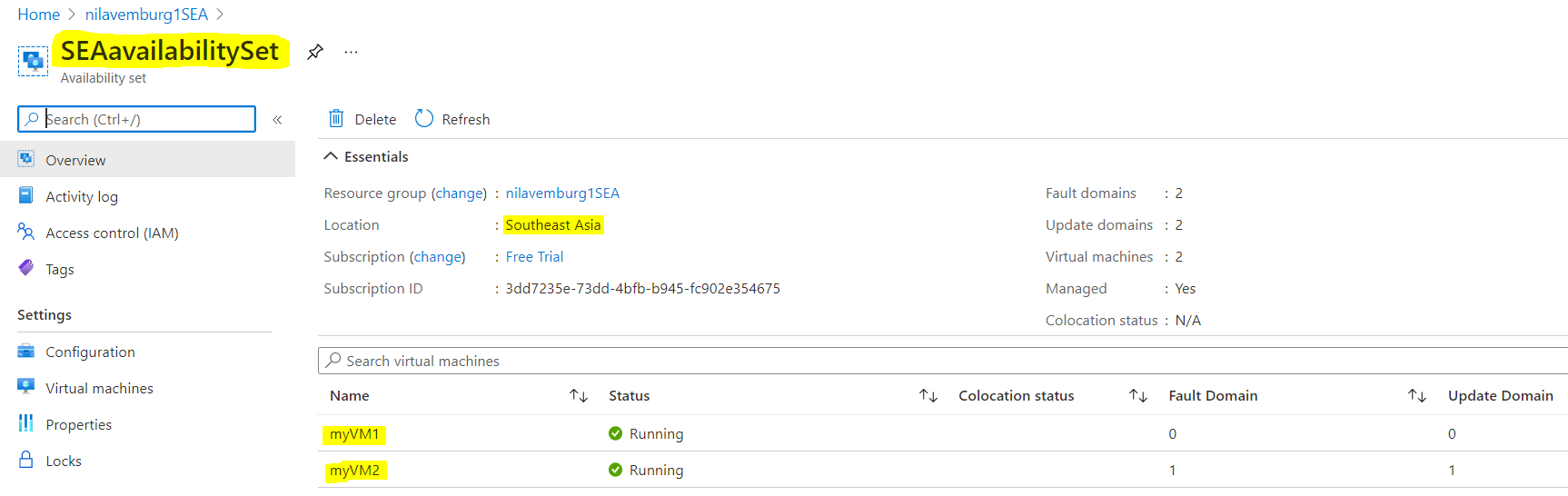
We will now create the virtual machines and will associate the above created parameters.



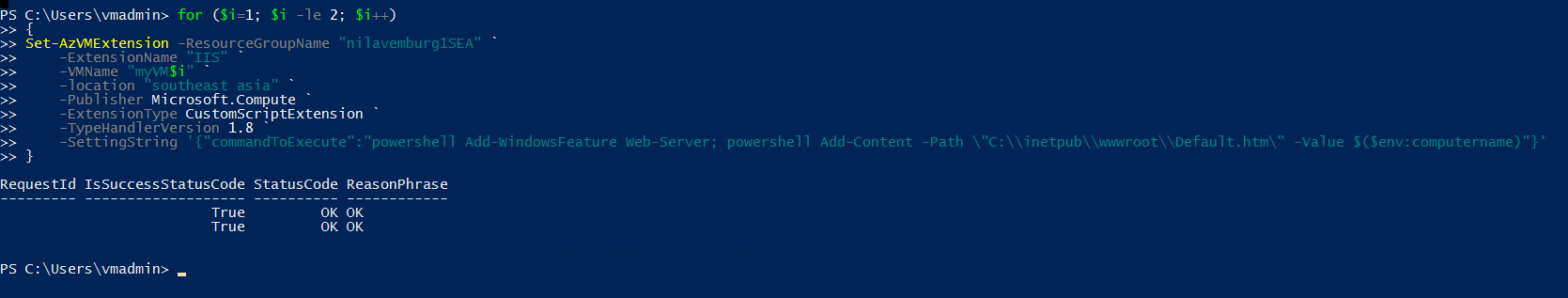
Hence the VMs have been created now-



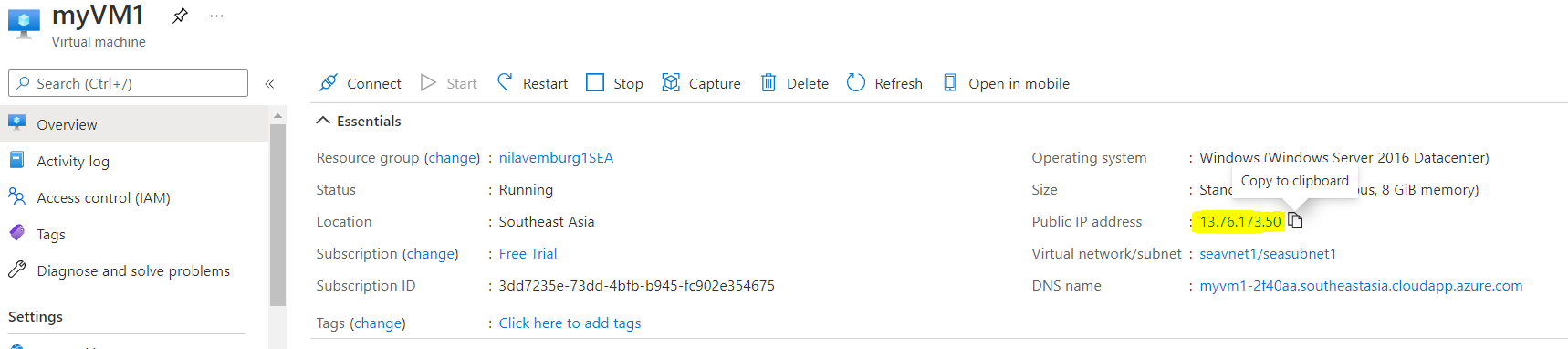
We can see that VMs have been created with the Availability set as required-



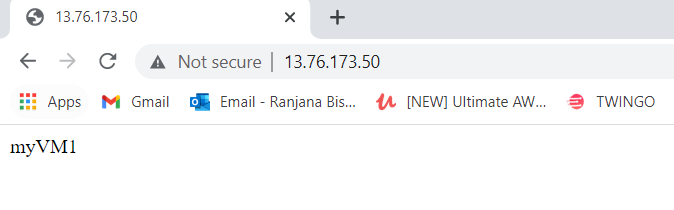
We will now install web-server feature on both the VMs-

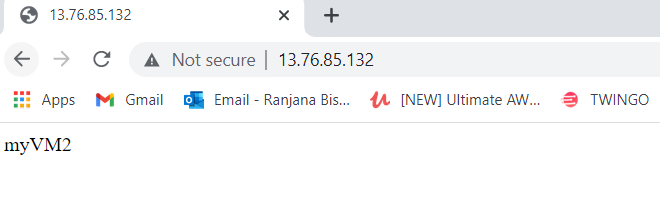


Copy the Public IP address of both the VMs to verify the IIS installation-



We can see that Web-server installation is successful for both the VMs.



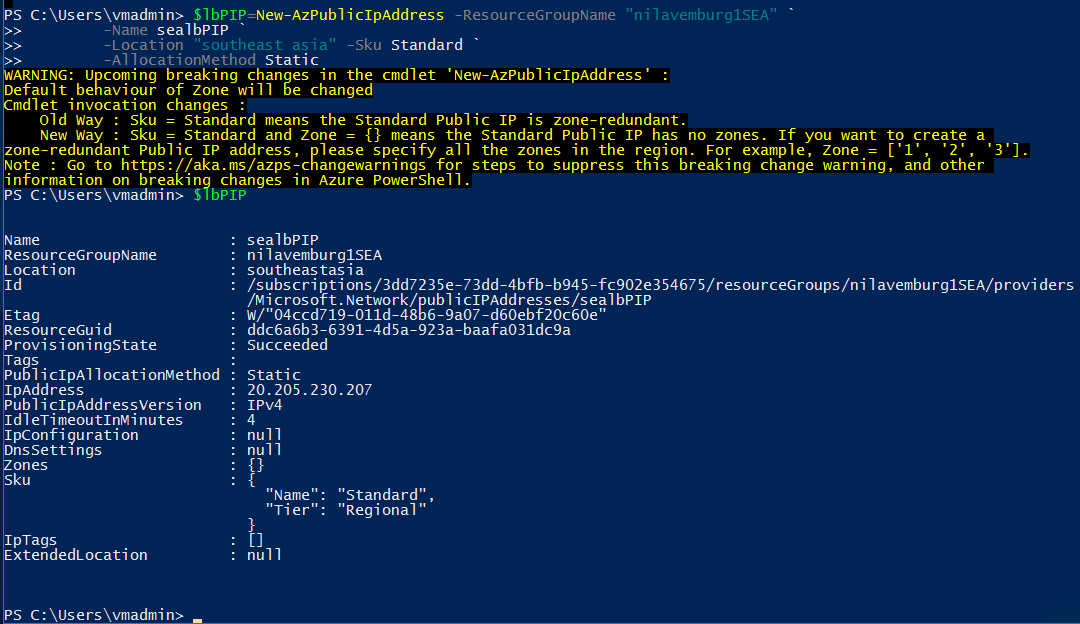


These web services has to be utilised with proper balance with client affinity with Public IP

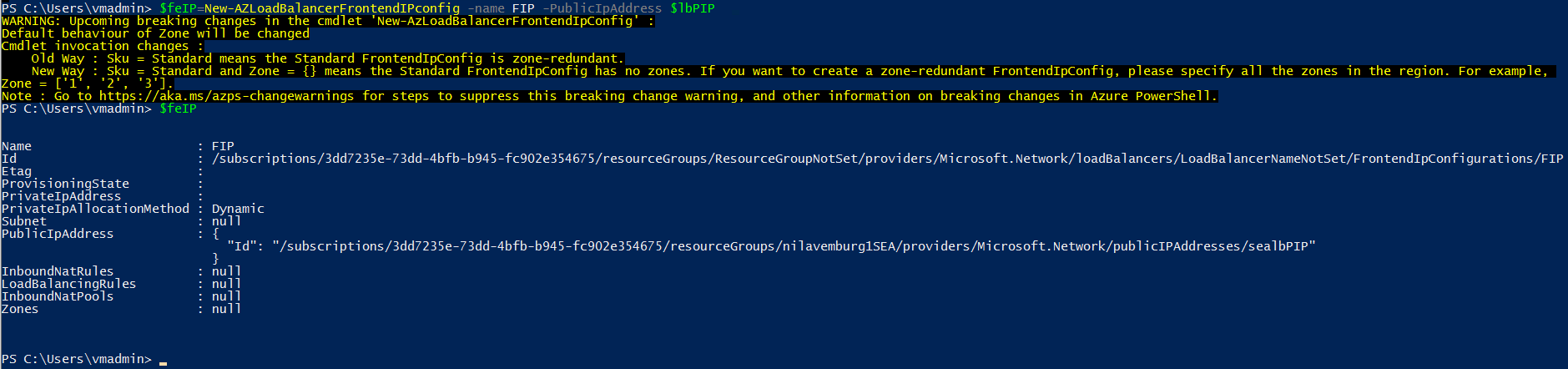
Selected web servers should be reachable via RDP from internet

**Deploying Load Balancer-**

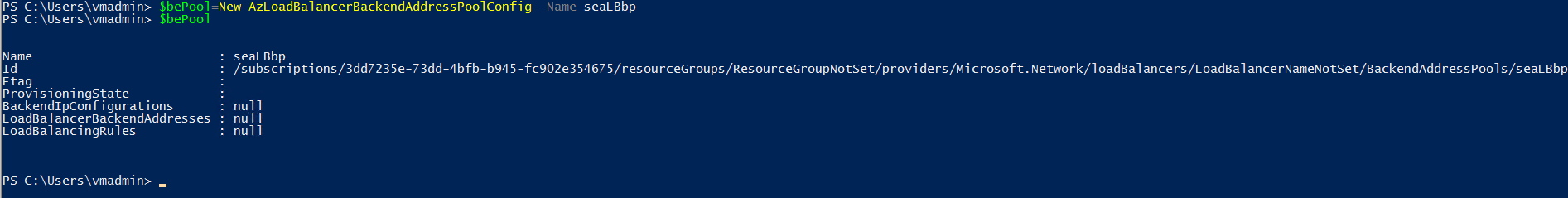
Creating Public IP for Load balancer that we will be associating with our Load balancer.



Creating Frontend IP config for the Load Balancer.

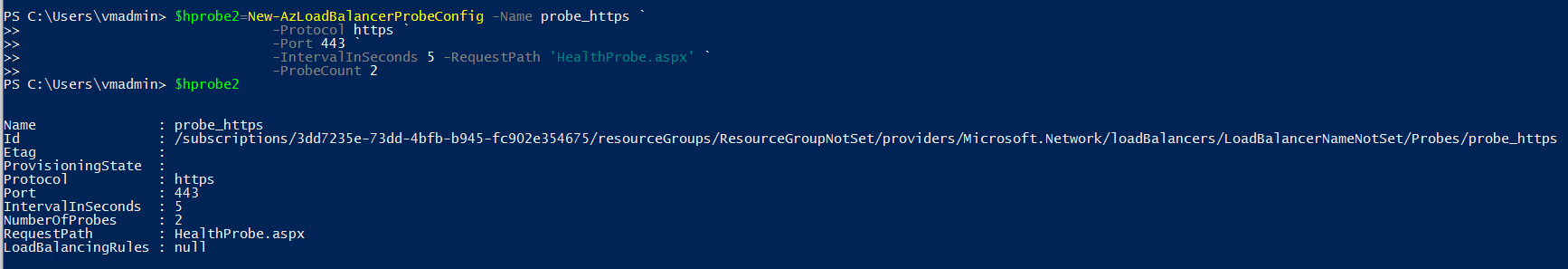


Creating Backend address pool for the Load Balancer-



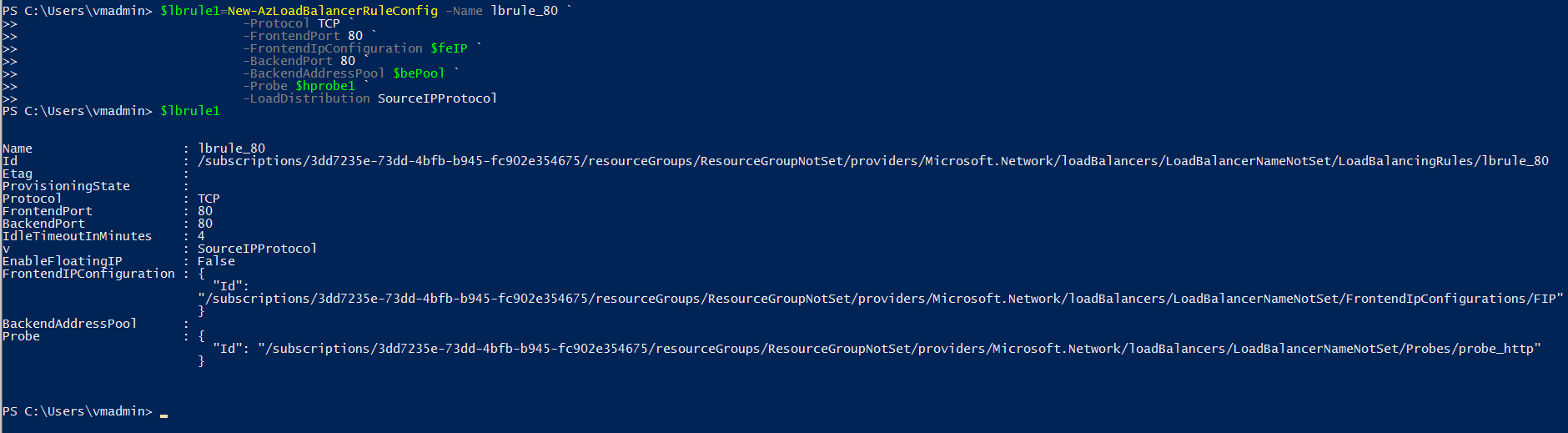
Creating Health Probes-



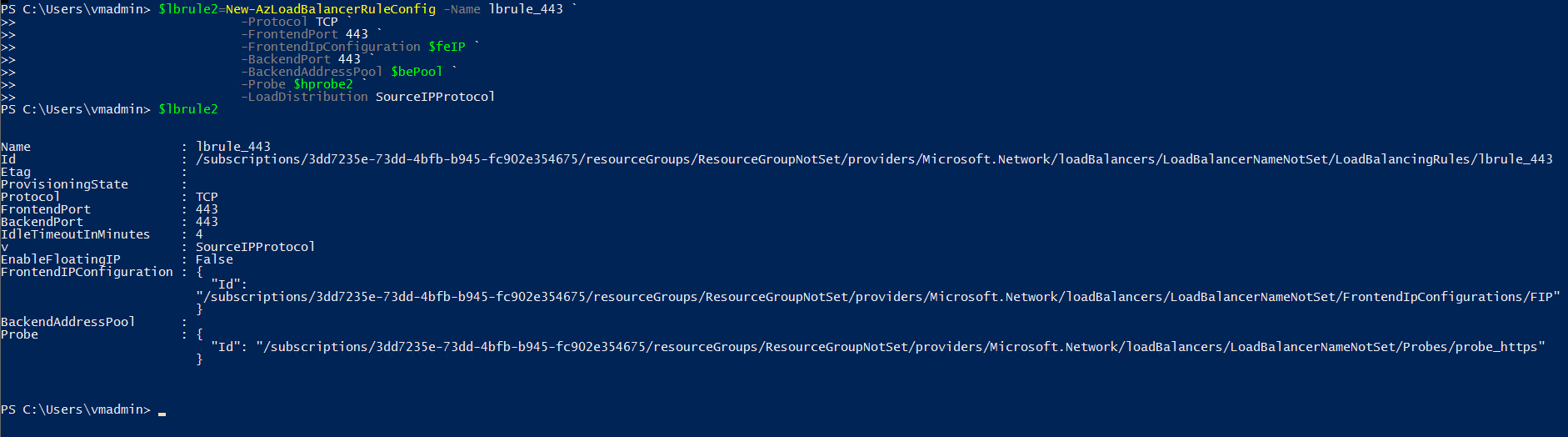


Creating Load Balancer rules-

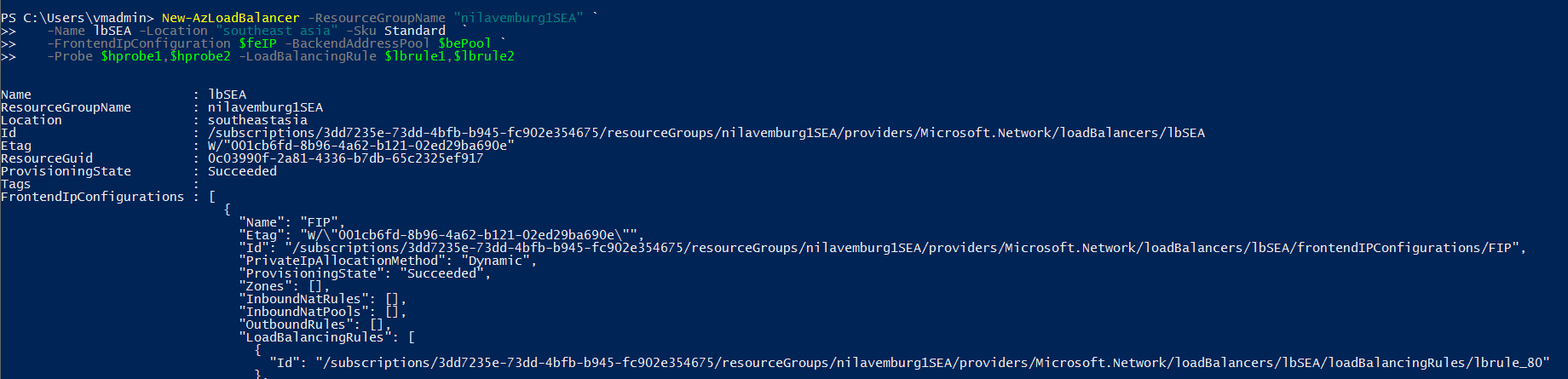
Rule1 - http



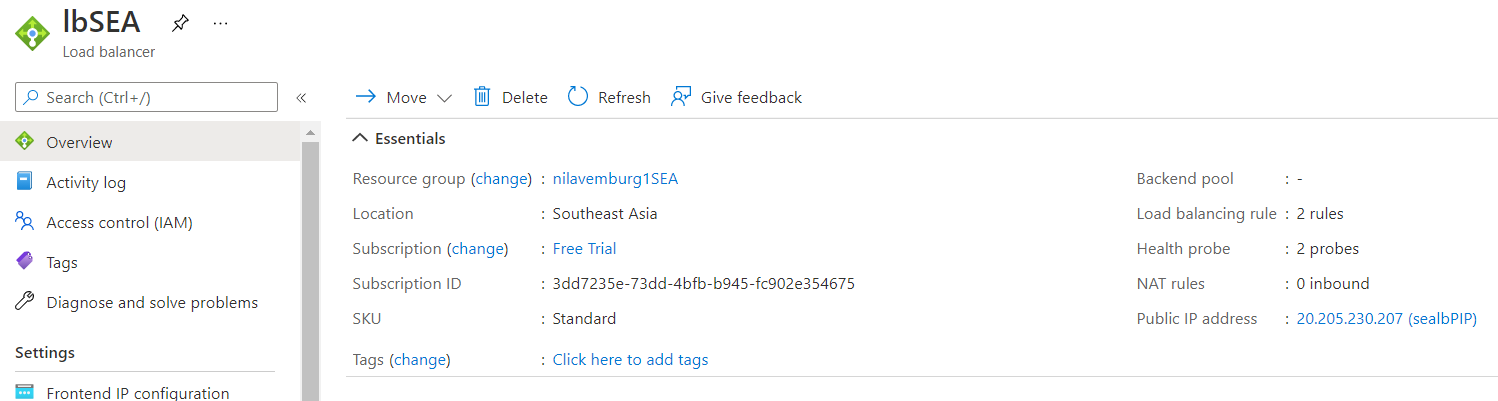
Rule 2 - https



Now we will create the Load Balancer and will associate the above created parameters-

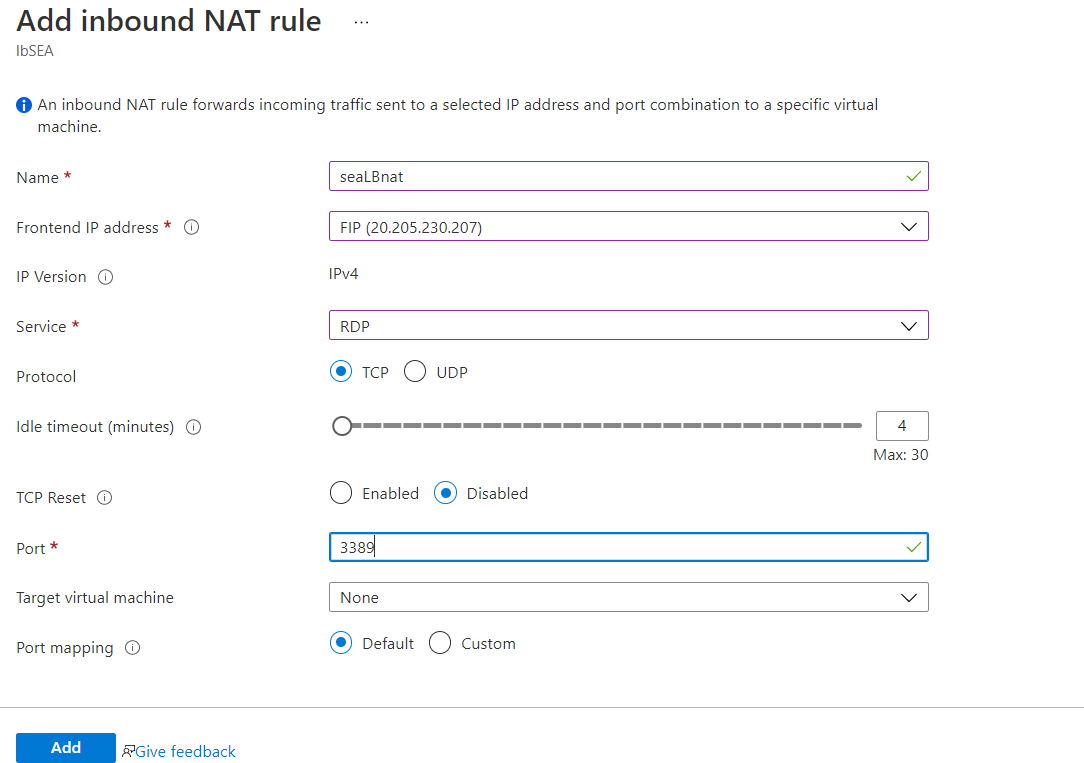


The load balancer has been created now-



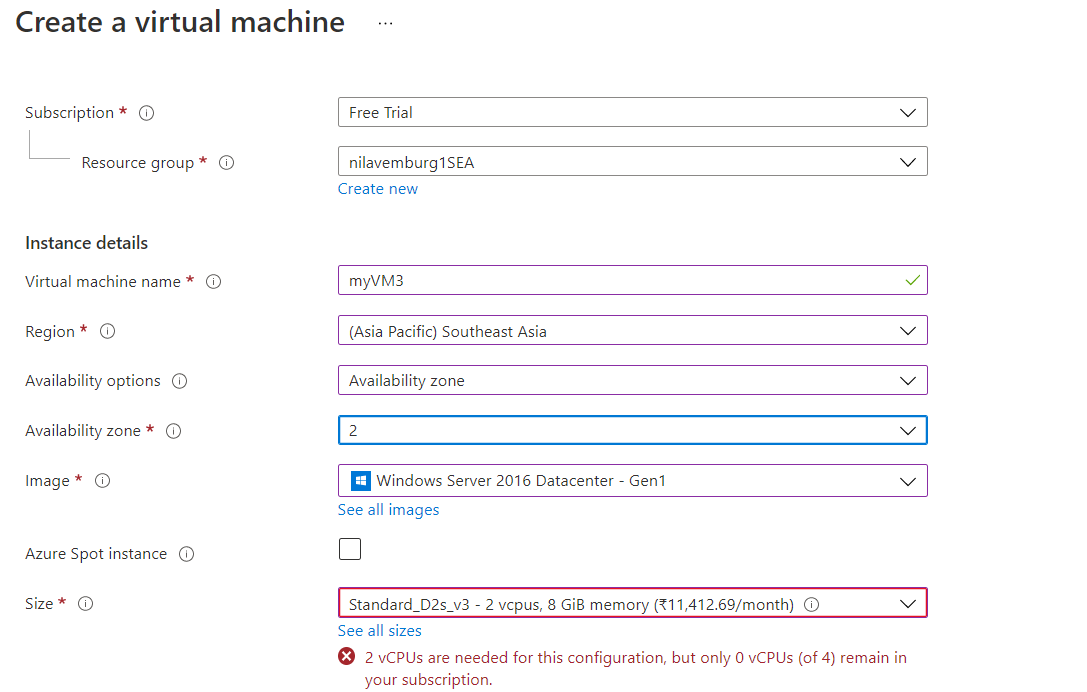
Selected web servers should be reachable via RDP from internet

We will create inbound NAT rule to direct the incoming traffic to a selected server-



A jump port should accessible from internet to upload contents to web servers.

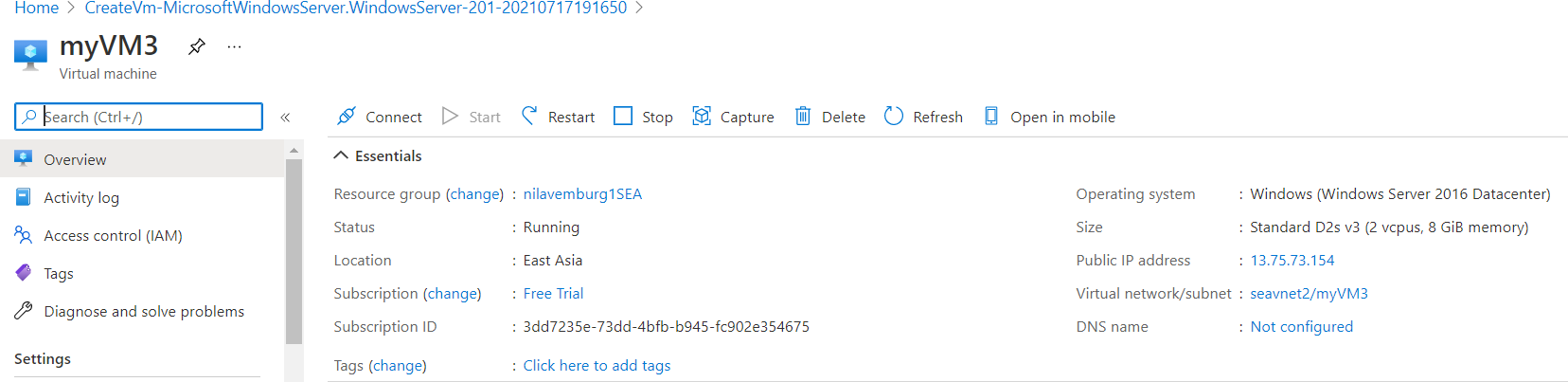
I had been facing issue with the SEA resource quota, I will try to create jump host in another region-



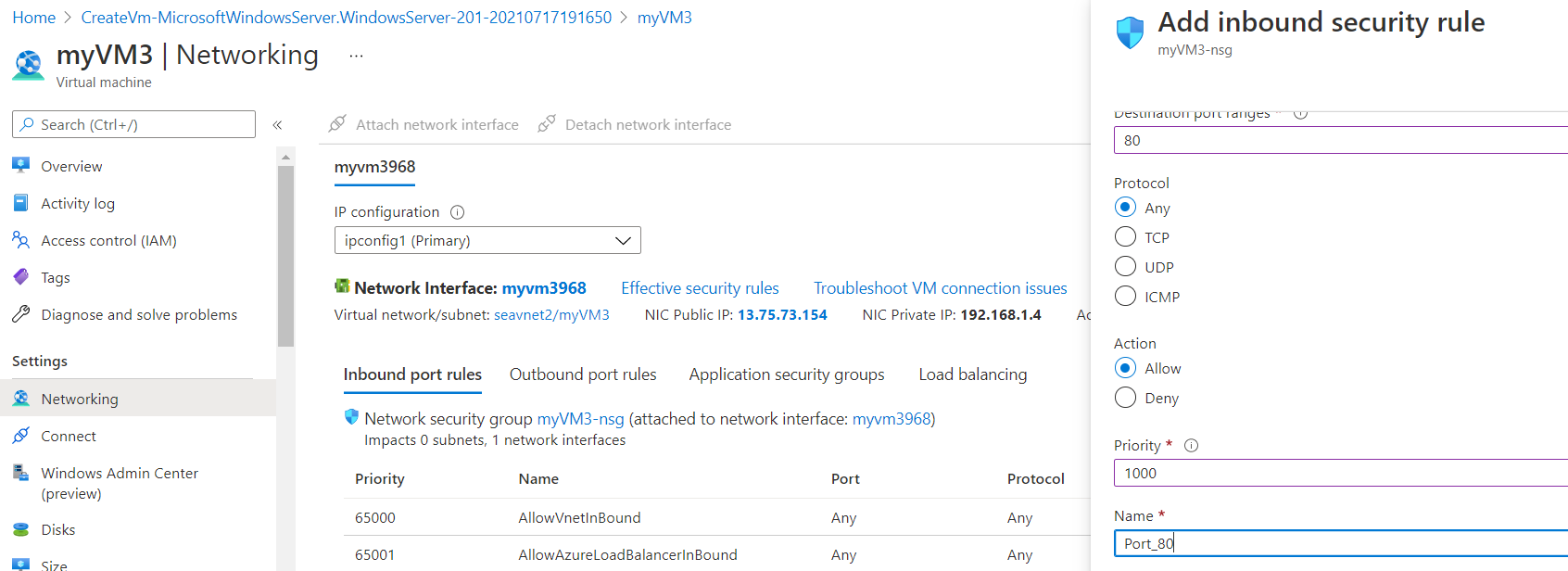
**Creating new VM (Jump host) in East Asia region-**



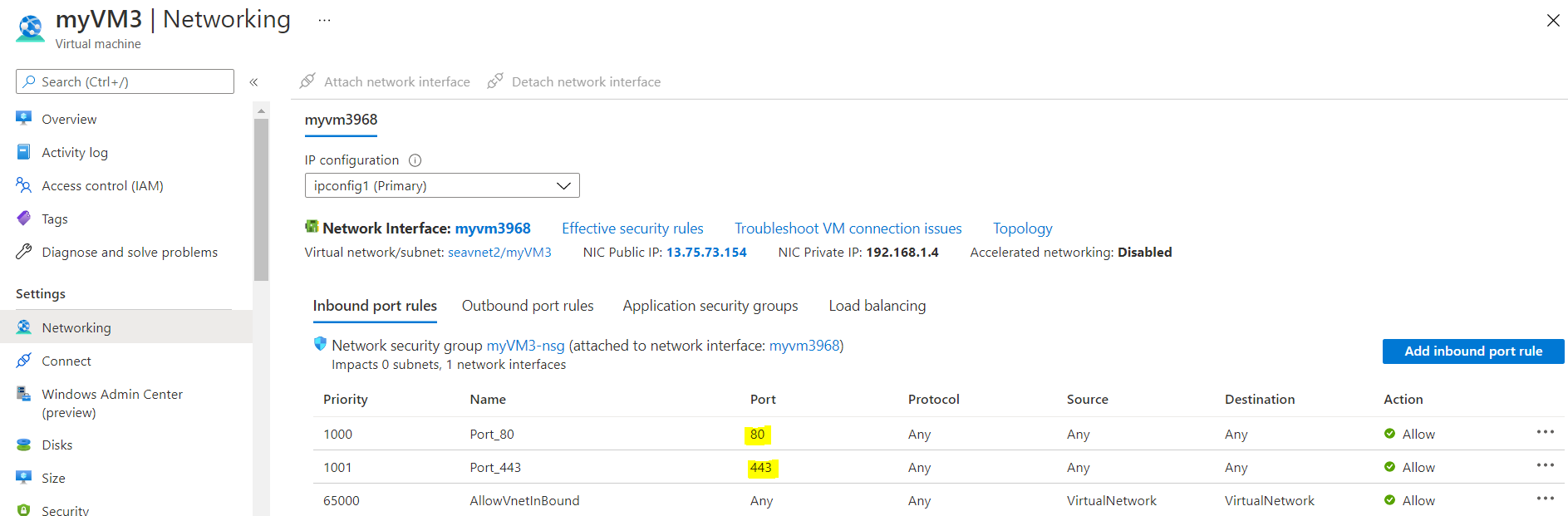
**The VM has been created now-**



**As the jump server must be accessible form internet, we will associate required rules using NSG-**

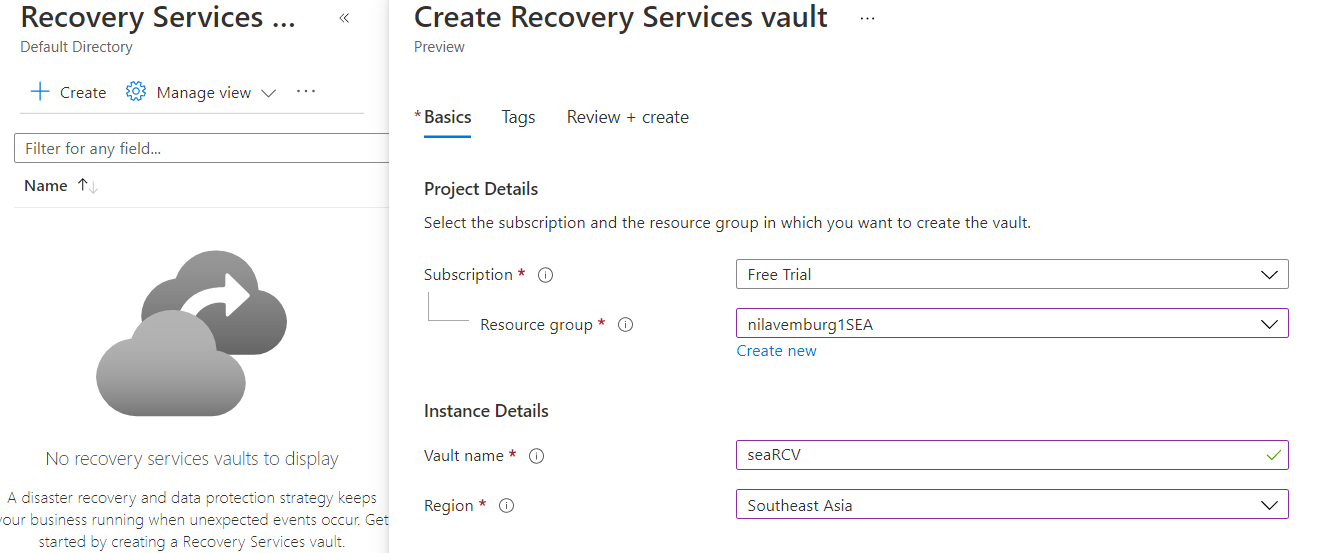


**Required rules have been configured on the VM-**

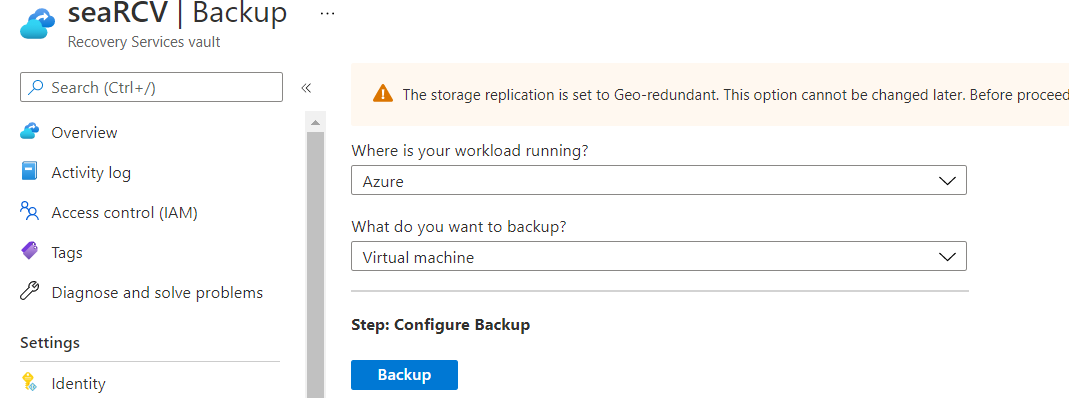


Enable backup for Webservers

To enable backup for the Web servers myVM1 and my VM2, firstly we will create a Recovery Services Vault. We will enter required details as below and proceed for RCV creation-



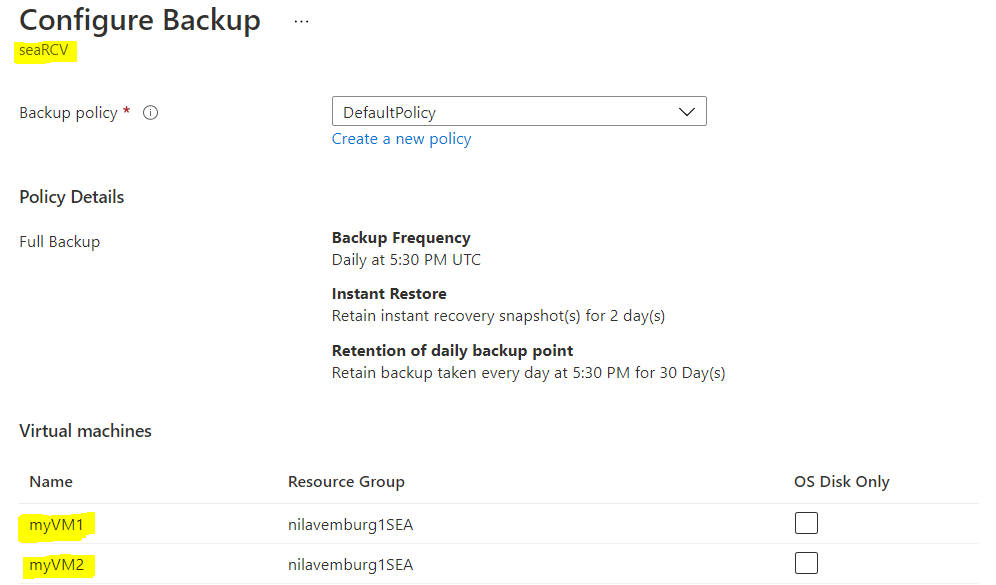
Select details as below-



Once we click on Backup, in the next window (Configure Backup) we can select the Default Policy or we can create a new Policy as per the requirement.

Also, we need to select the VMs for which we want the backup to be enabled.

Here I have accepted the default policy, and I have selected both Webservers as per the required scenario.

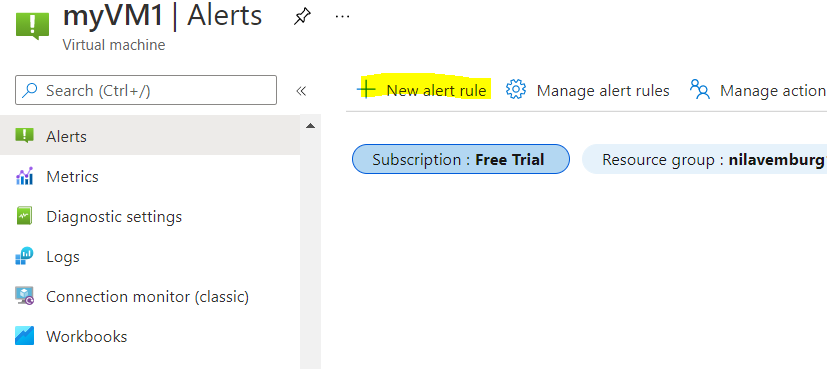


Backup is enabled now for both the Webservers -

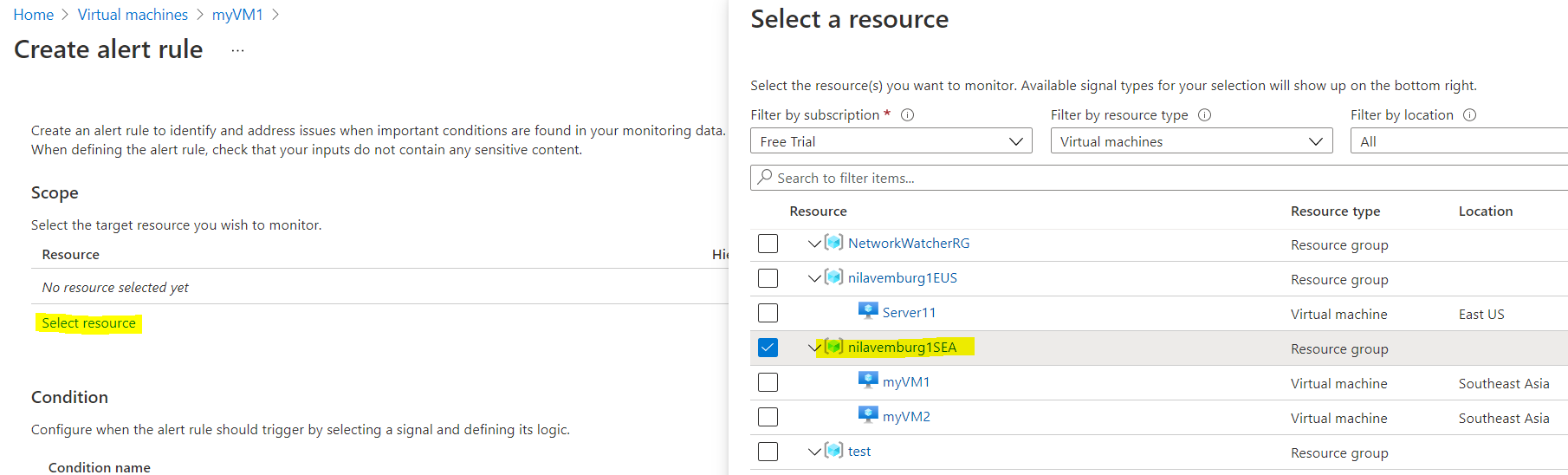


Have alert generated in case of 80% above cpu usage

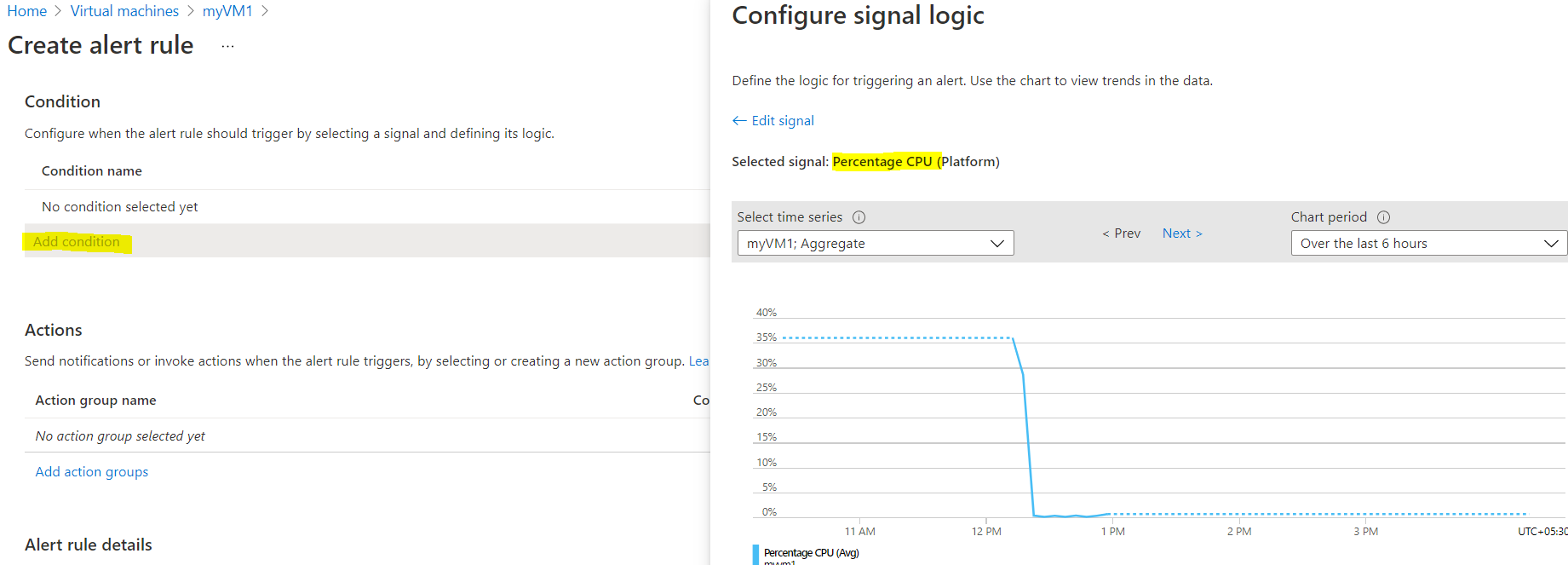
**As we need an alert to be generated if the CPU usage goes above 80% for our webservers, we will set up an alert on both the VMs. Click on +New alert rule to proceed-**

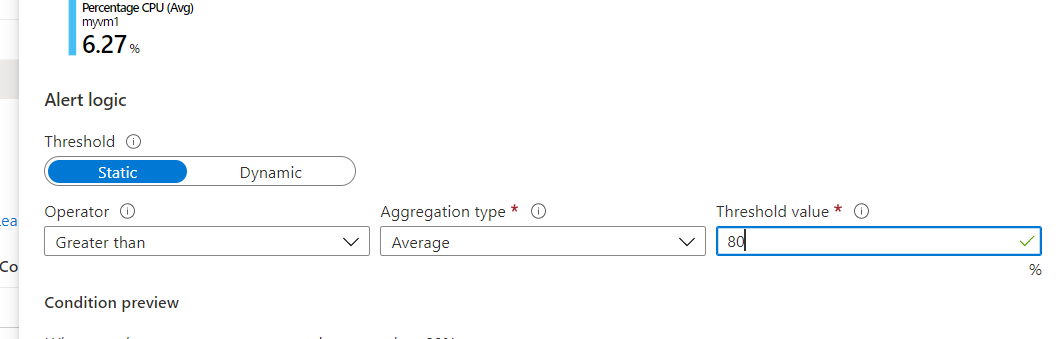


**Add the resources to be monitored, Here I have selected the RG name so that the alert can be configured both the VMs as required.**

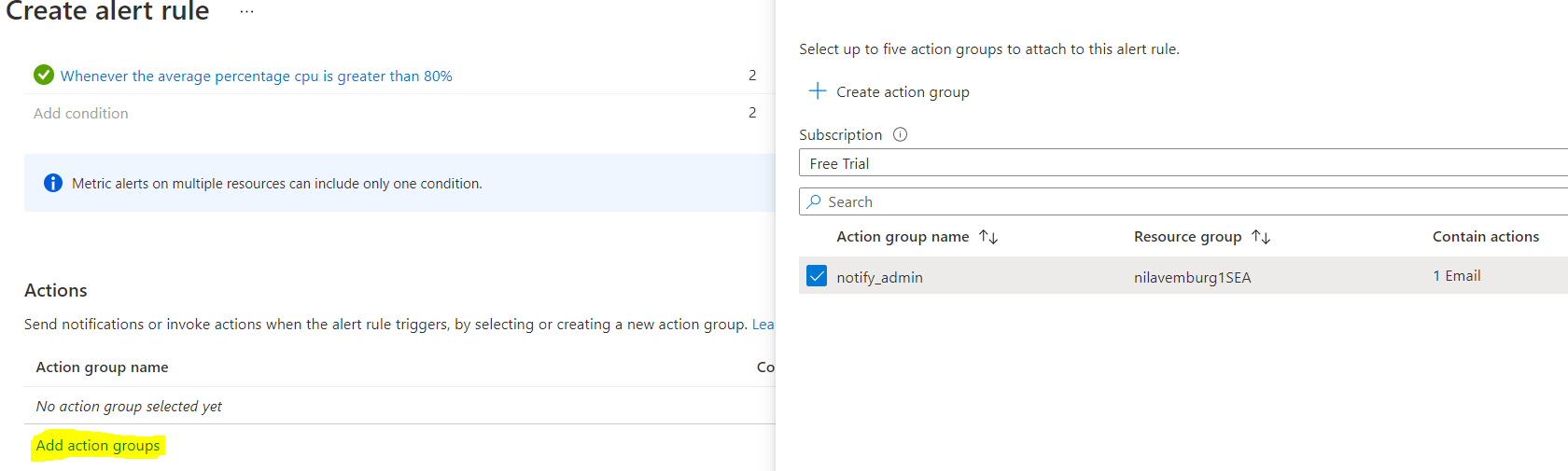


**Add the required condition (CPU usage>80%)-**

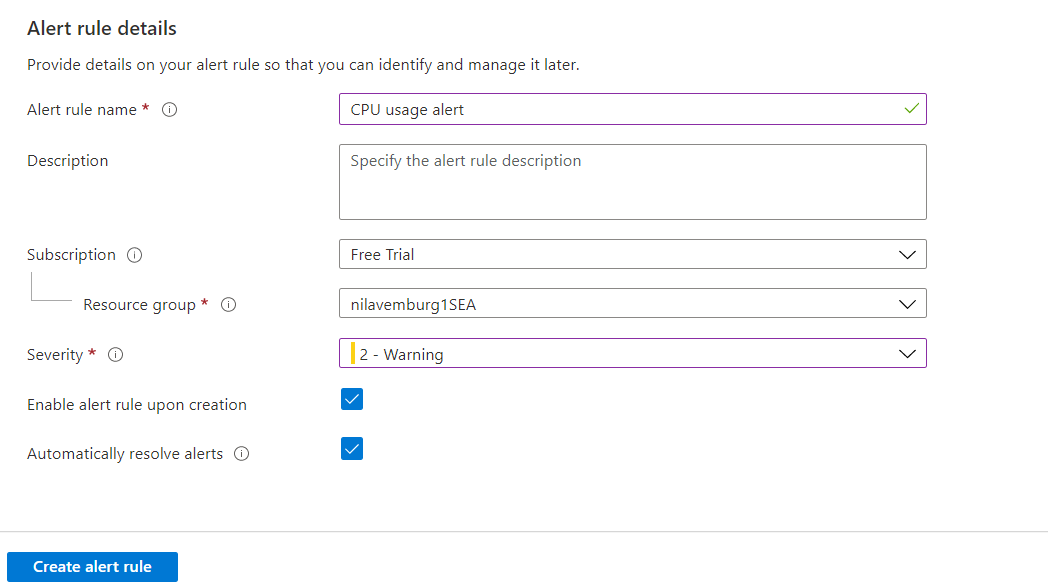




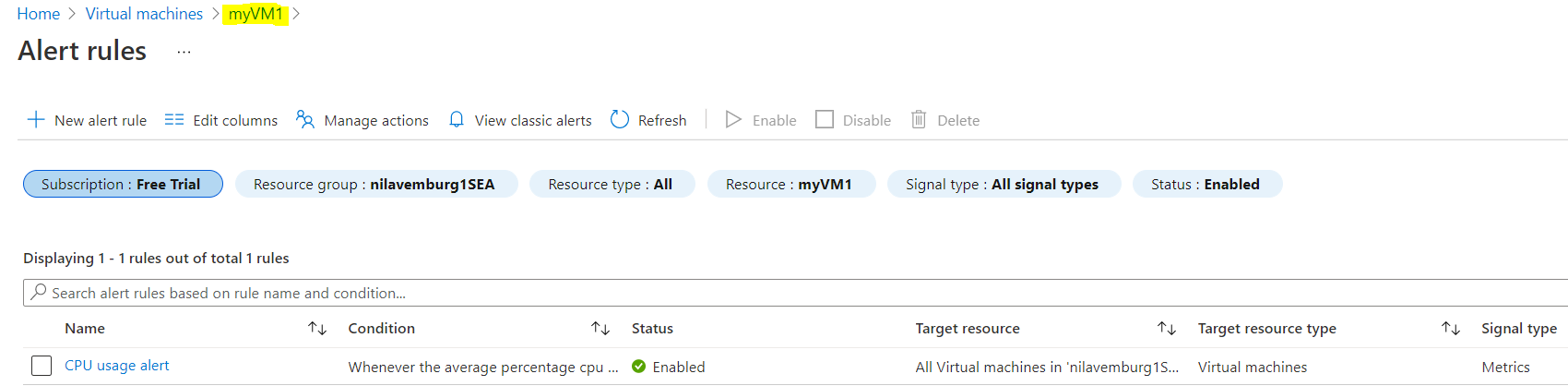
**Add an Action item i.e what happens when the CPU usage goes above 80%?**



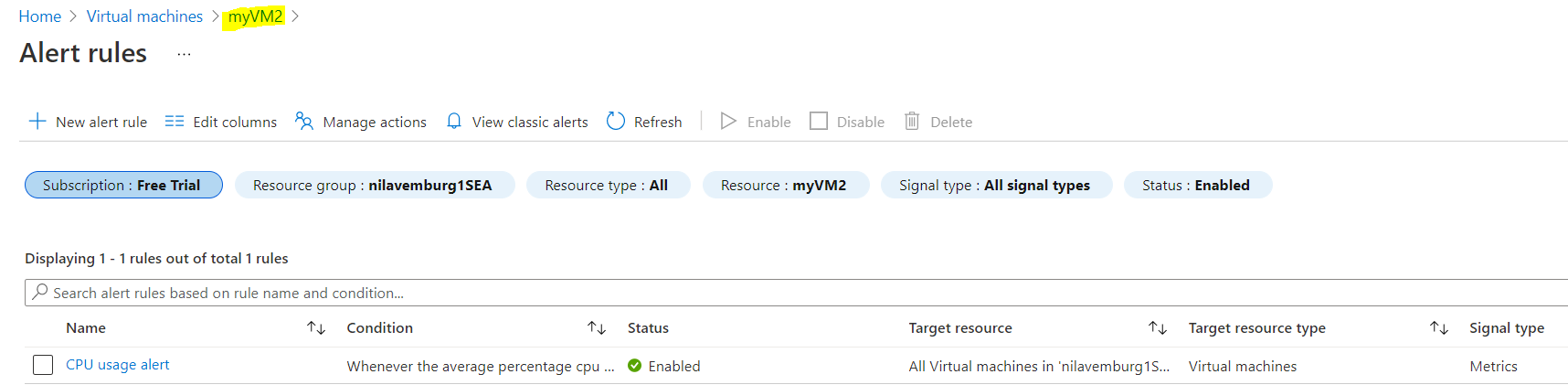
**Fill required details as below and click on Create alert rule-**



**The rule has been created as follows (VM1)-**



**The rule has been created as follows (VM2)-**

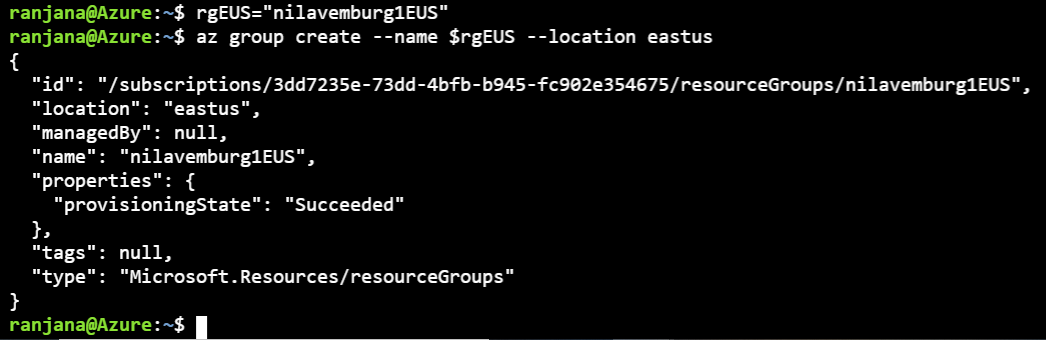


**Requirement for EUS region-**

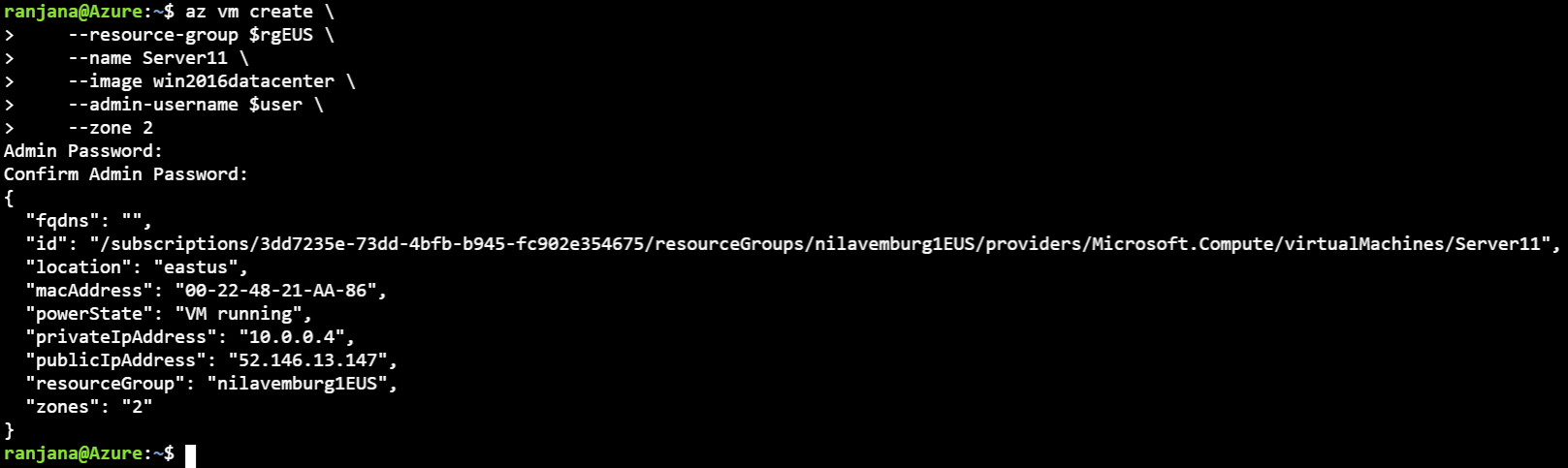
* EastUS server (Server11) should be accessible from internet via public IP
* Establish secure Connection to SEA-EUS Azure sites
* All servers should be reachable with internal ip addresses

EastUS server (Server11) should be accessible from internet via public IP

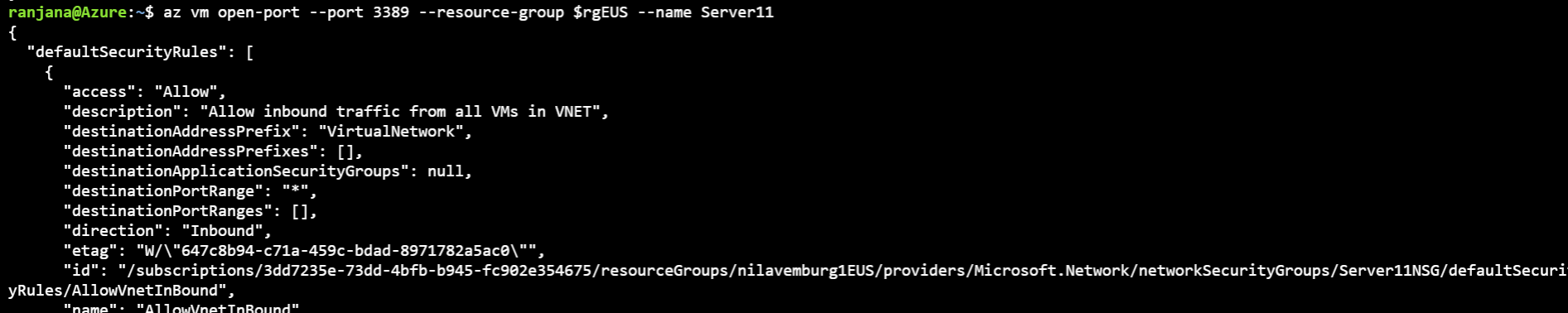
We will now set up our EUS resources. To create the VM as mentioned, we are first creating our resource group in EUS location.



Creating Virtual machine (Server11) in the resource group created above.



As the server should be RDP’able from internet, we will open port 3389 on the VM.

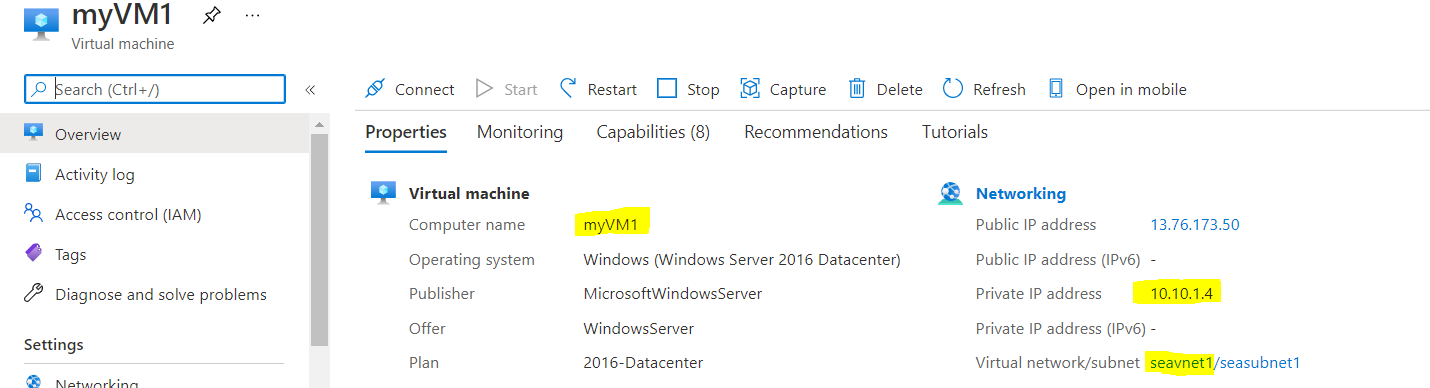


Establish secure Connection to SEA-EUS Azure sites

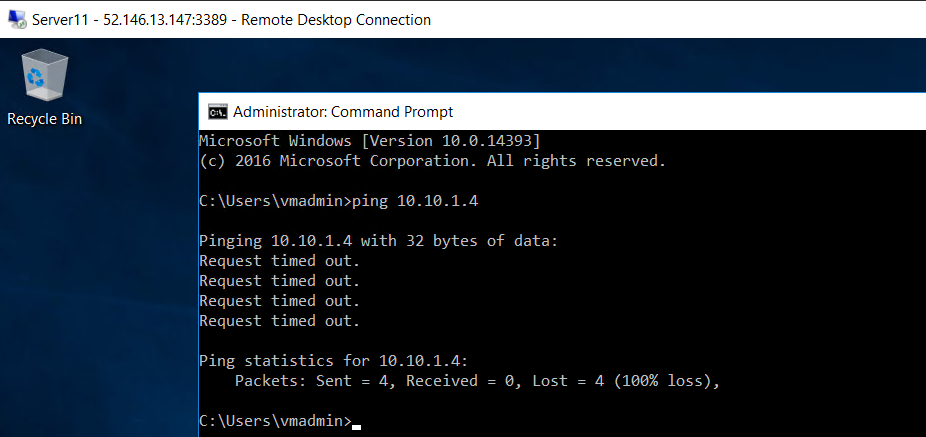
All servers should be reachable with internal ip addresses

**As we have to Establish secure Connection between EUS and SEA Azure sites, we will create vNet peering between both these regions-**

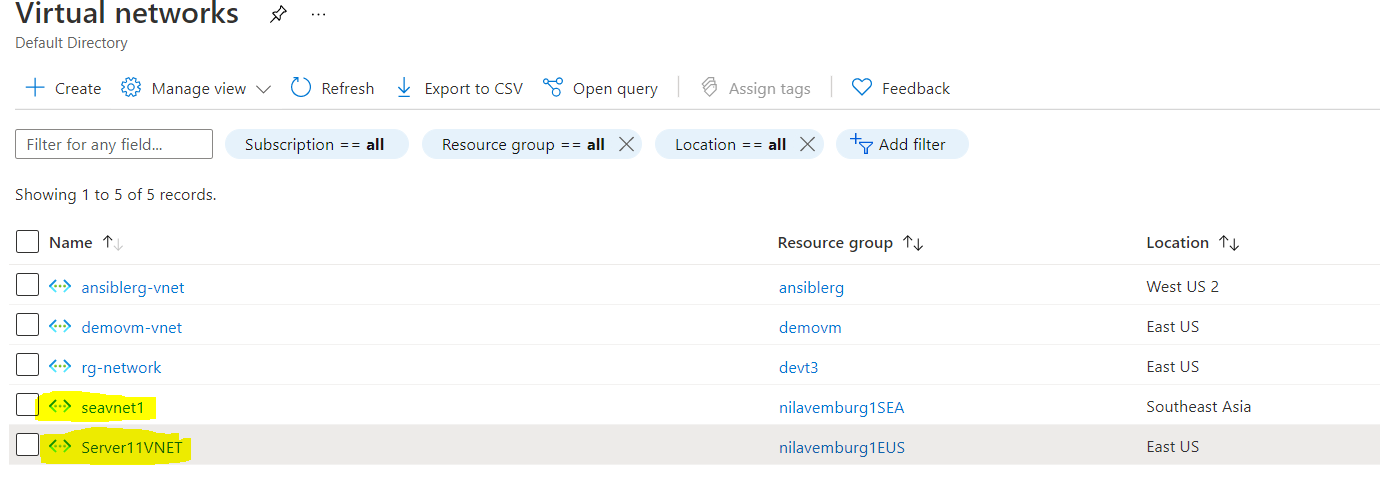
Firstly, we will try to ping the Private IP of oner VM (in one reqion) from another VM (in another region). Here I am taking the Private IP of the VM (myVM1) that is in SEA region.



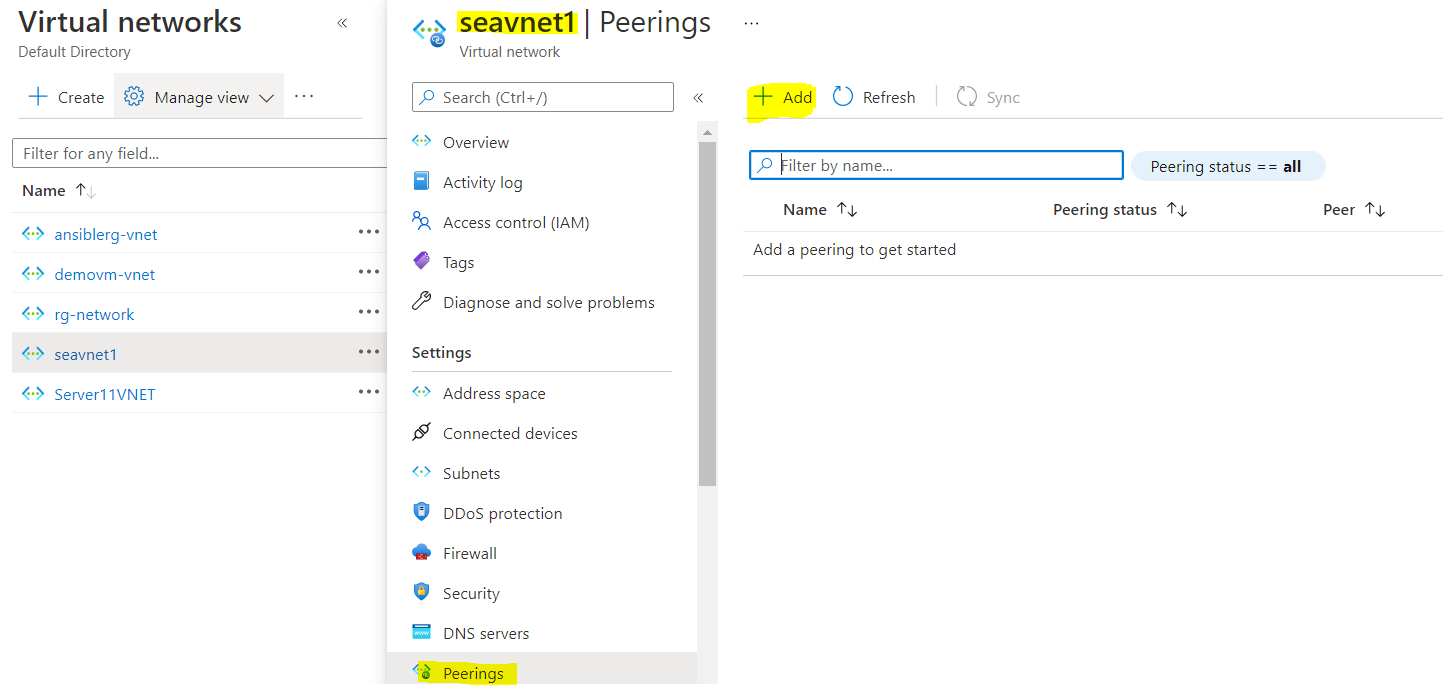
Now on trying to ping the SEA VM from EUS VM, we can see that -by default the VM is not reachable via private IP from another region VM.



We will now take a note of the Virtual network in both the regions and will create a Bidirectional peering between both the VMs.



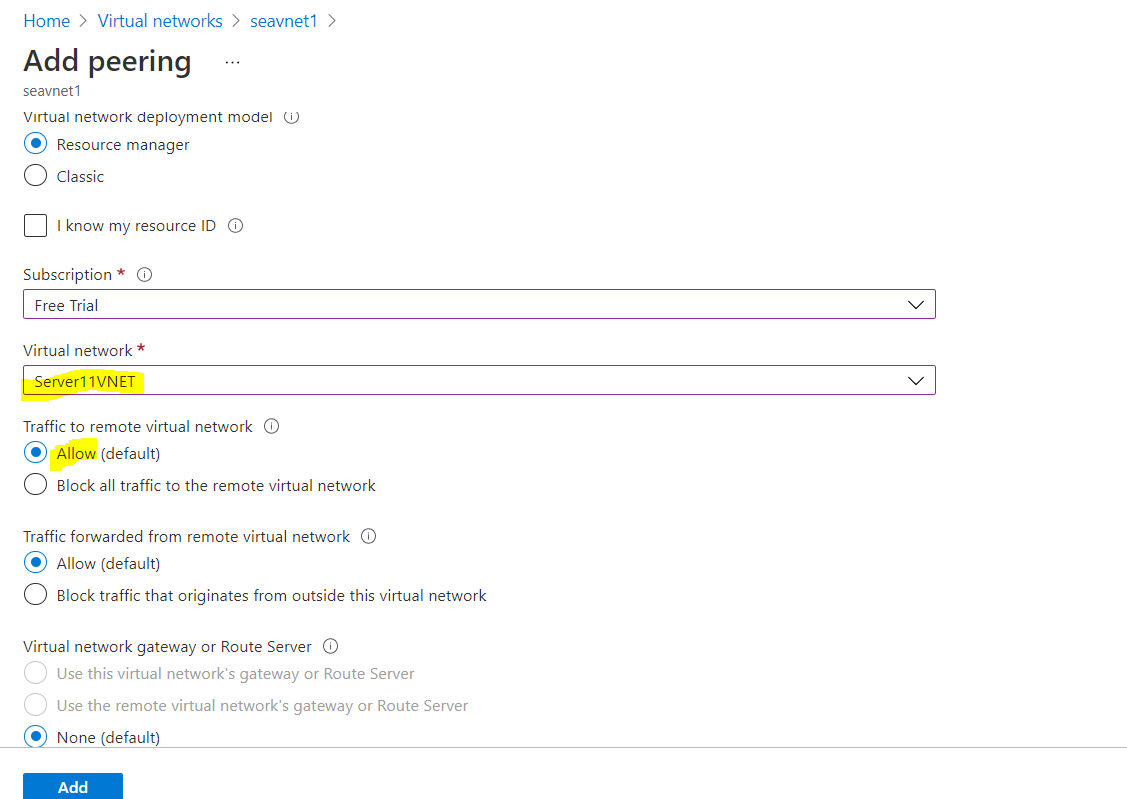
From SEA vNet, we can create a peering using ‘Peerings’ under Settings option. And click on +Add to proceed for setting up the peering connection.



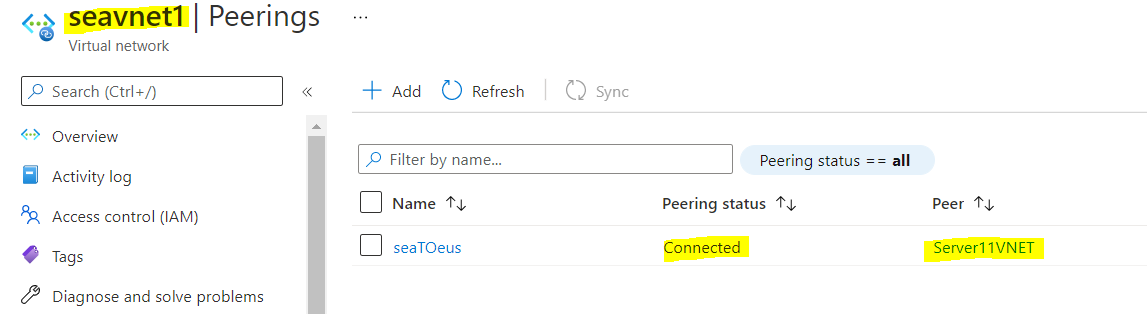
Add below details as required. Also we can observe that we can create a Bidirectional peering from peeing option of either of the vNets.

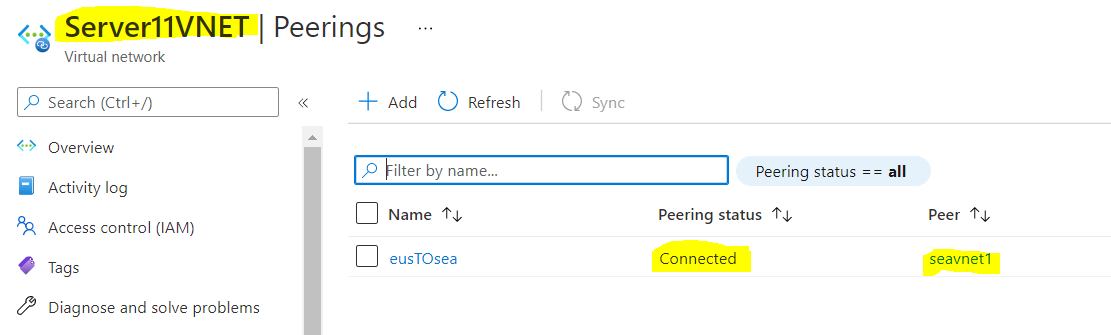


Once the required details have been filled, Click on Add to submit the settings.

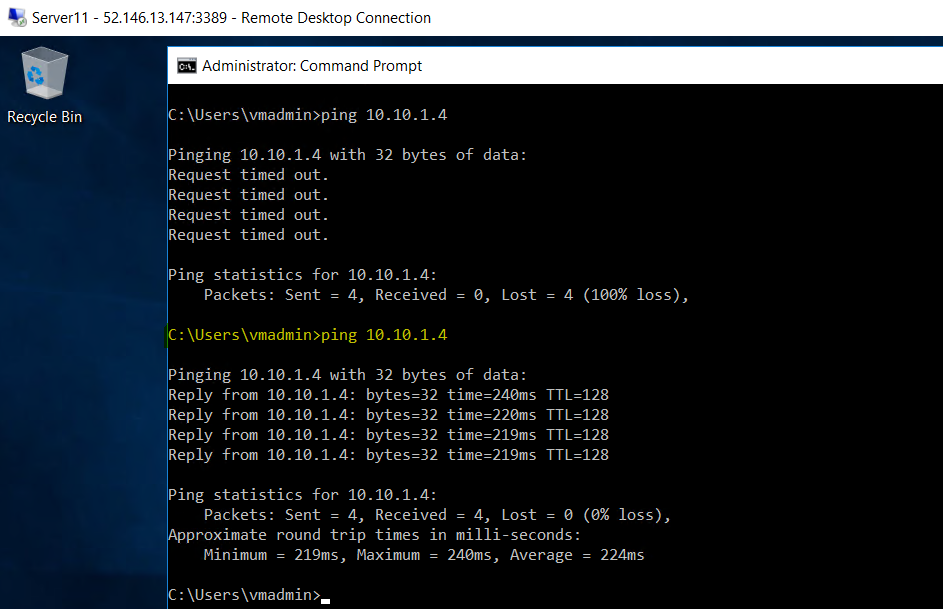


Now we can see that the Peering have been configured for both the vNets.





Now if I try to ping the SEA VM from EUS region, we can see that the VM is accessible via Private IP-



**Resource creation using Terraform -**

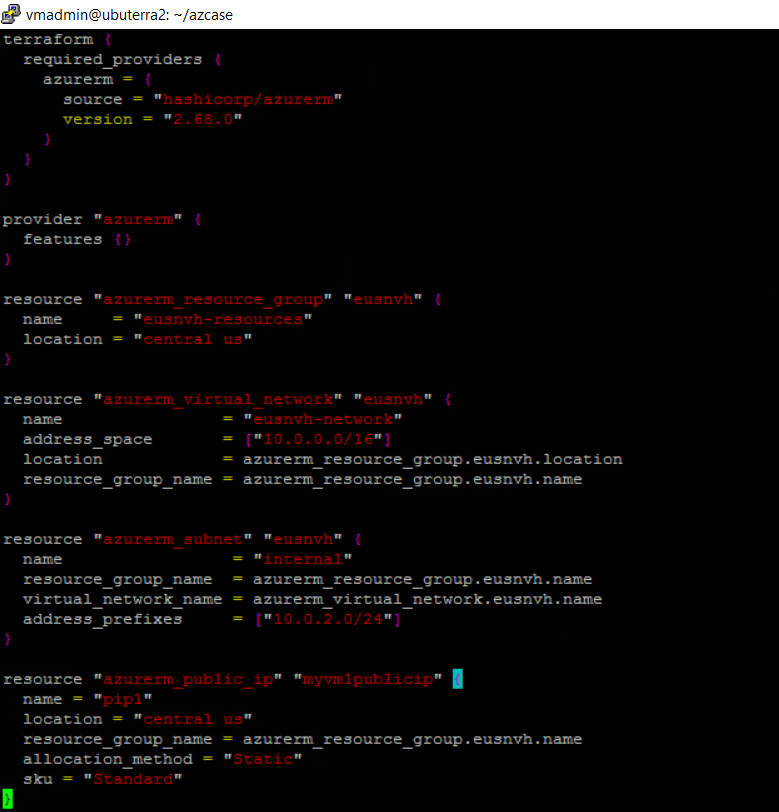
Also, I tried creating Virtual machine using Terraform along with Storage account and

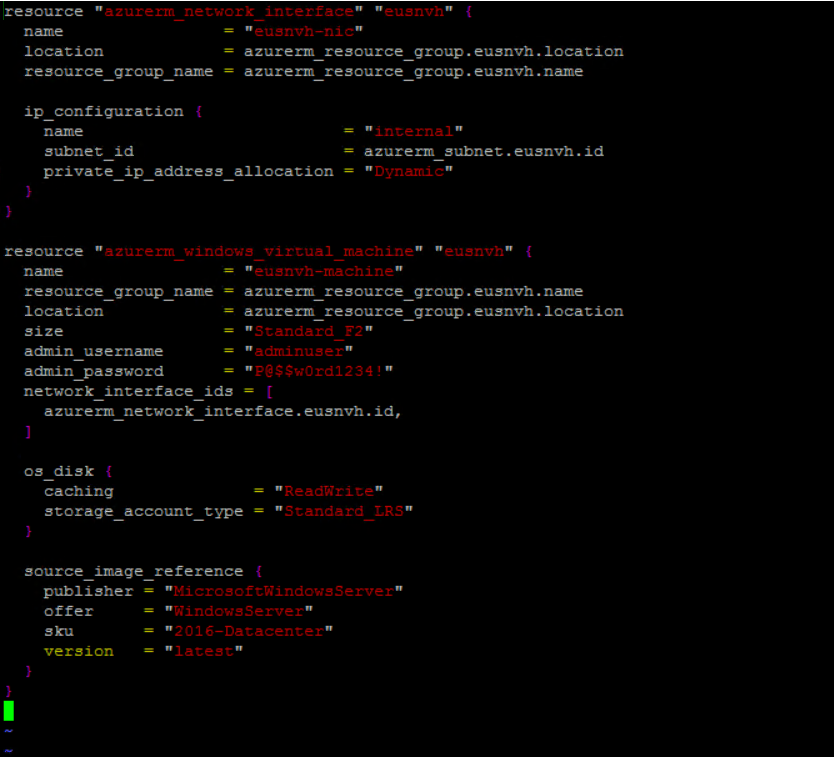
File share-

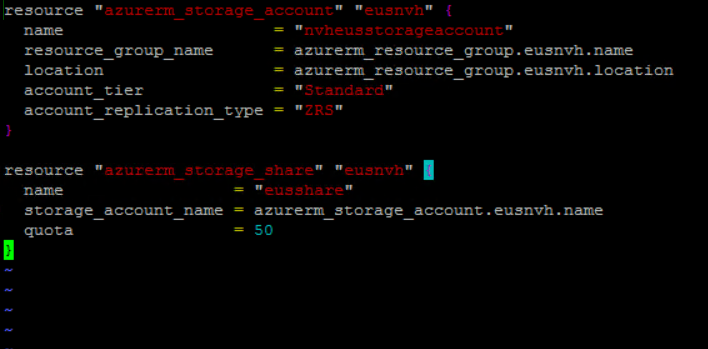
**Resources created using Terraform-**

* Resource group
* Virtual Machine with Public IP address
* Storage account
* File share

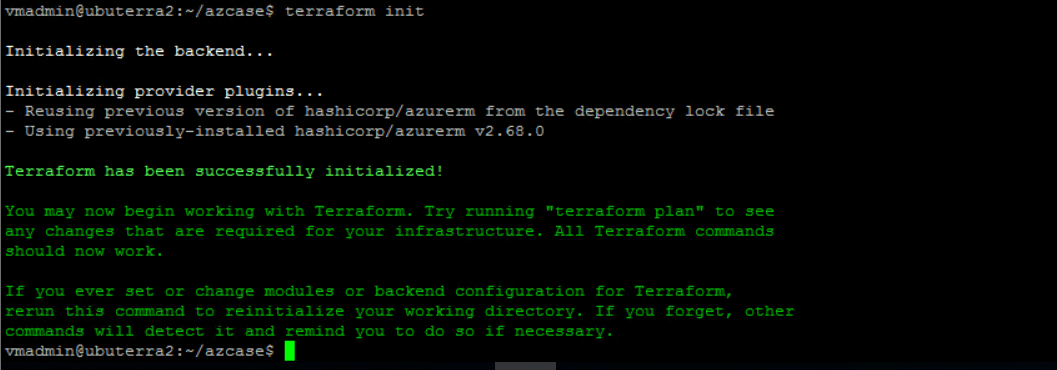
Created directory ‘**azcase’,** created rg.tf with belowIAAS**-**



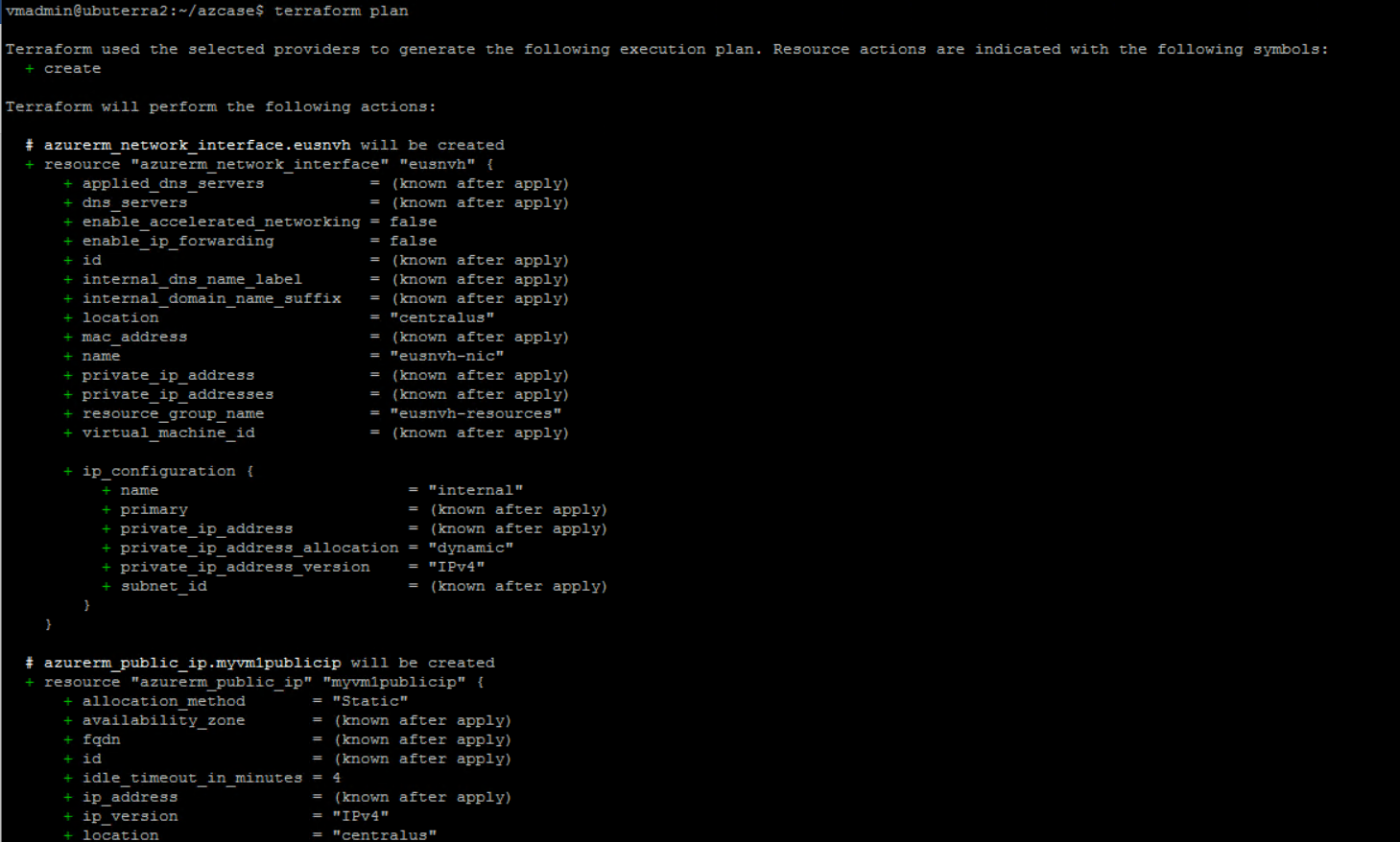




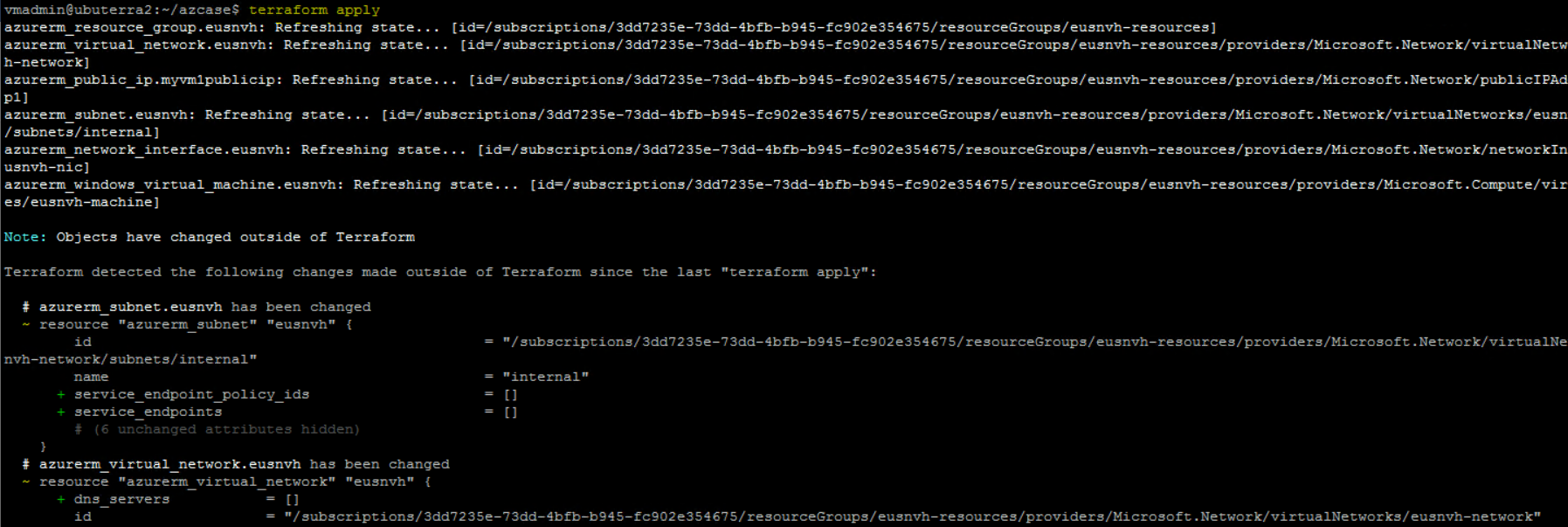
**Terraform init -**



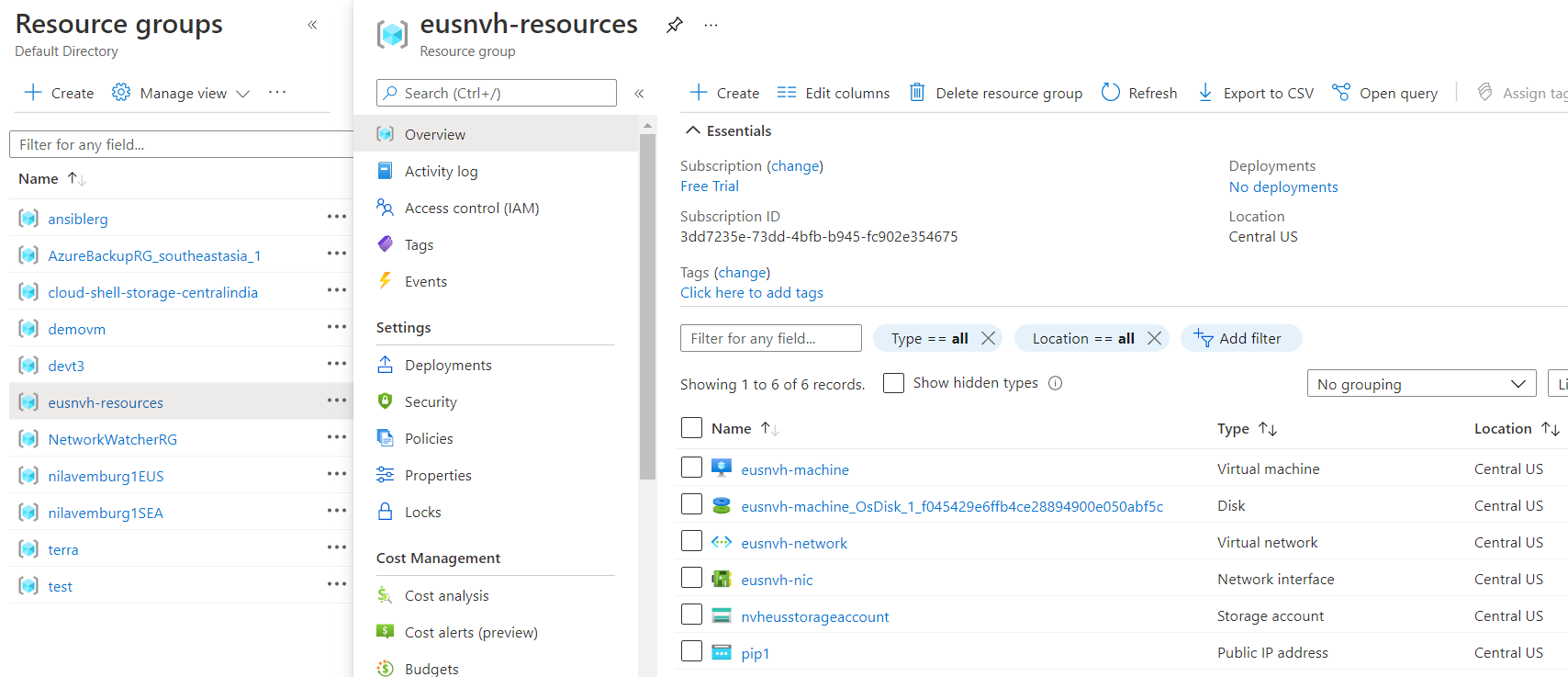
**Terraform plan -**



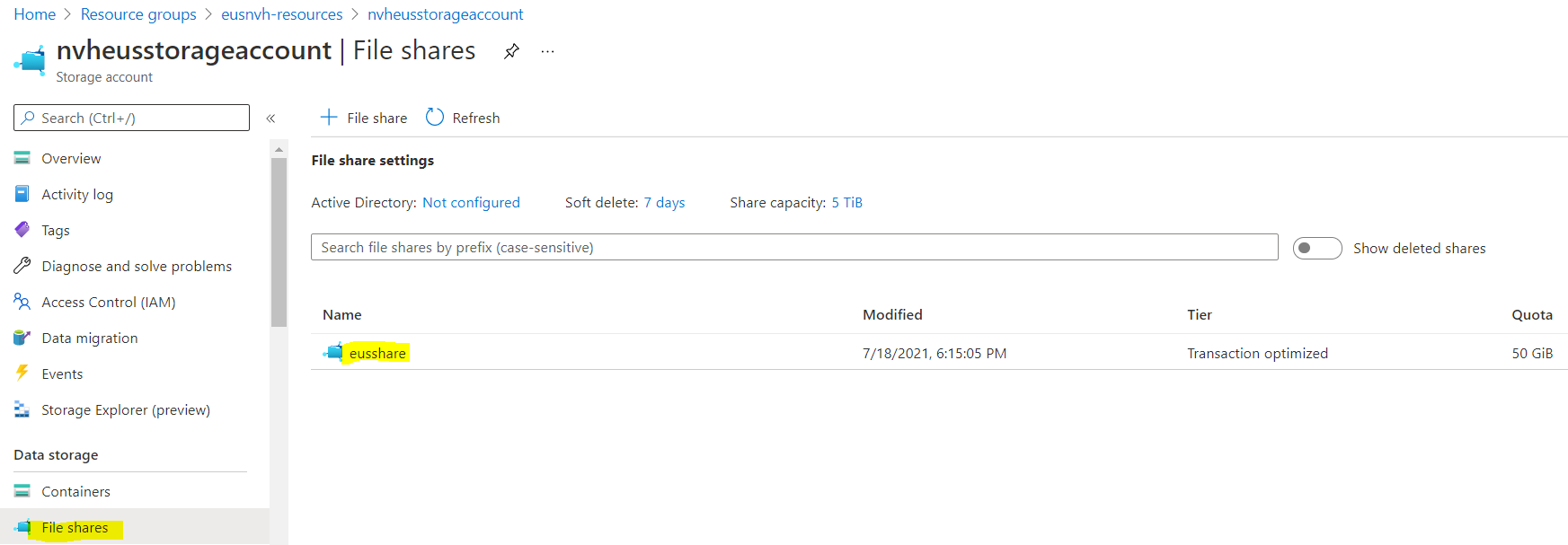
**Terraform apply -**



Hence the resources have been created-



Storage account with file share have also been created-



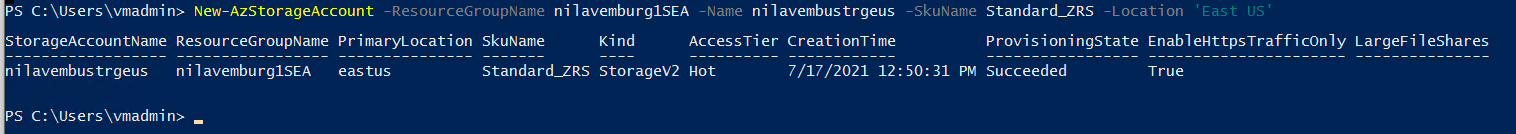
**Storage requirements-**

* EUS based resources should provide data resiliency in case of azure datacentre failure.
* The storage should be accessible by applications with secure access. Provide access urls and keys.
* Sales manager should access his resource from windows explorer.
* SEA data resources must provide high resiliency in case of even multiple azure data center failures

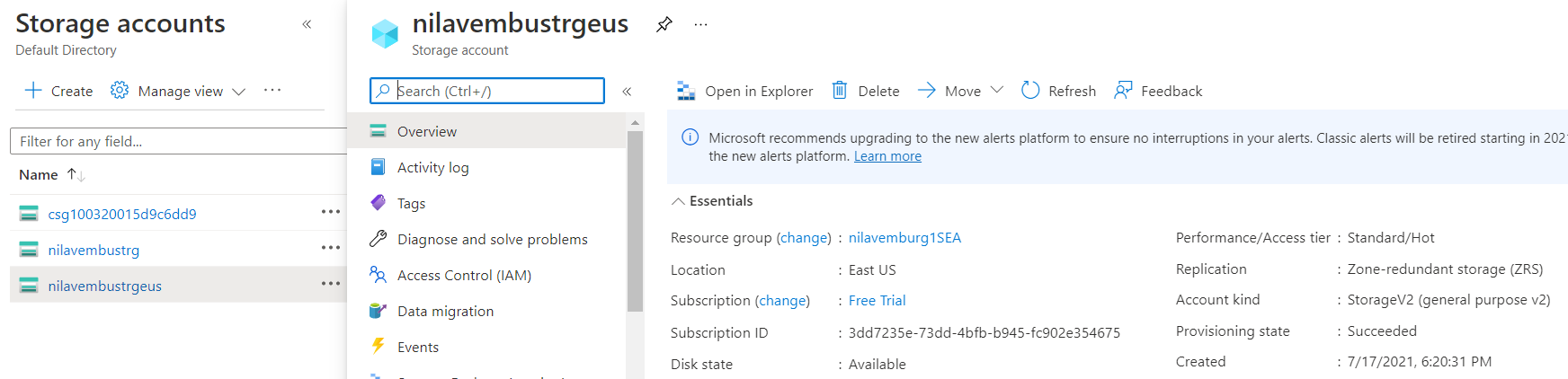
EUS based resources should provide data resiliency in case of azure datacentre failure.

**Creating Storage account for EUS region-**

Creating Storage account -

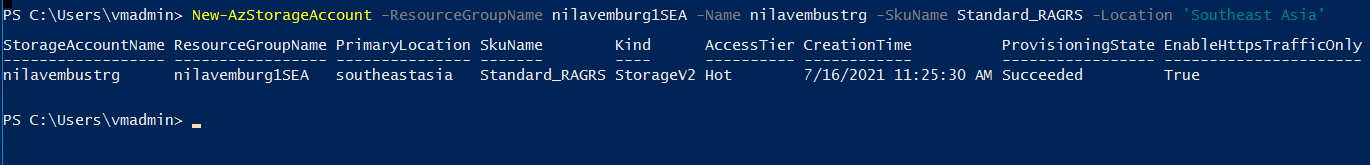


Storage account has been created for EUS region now-

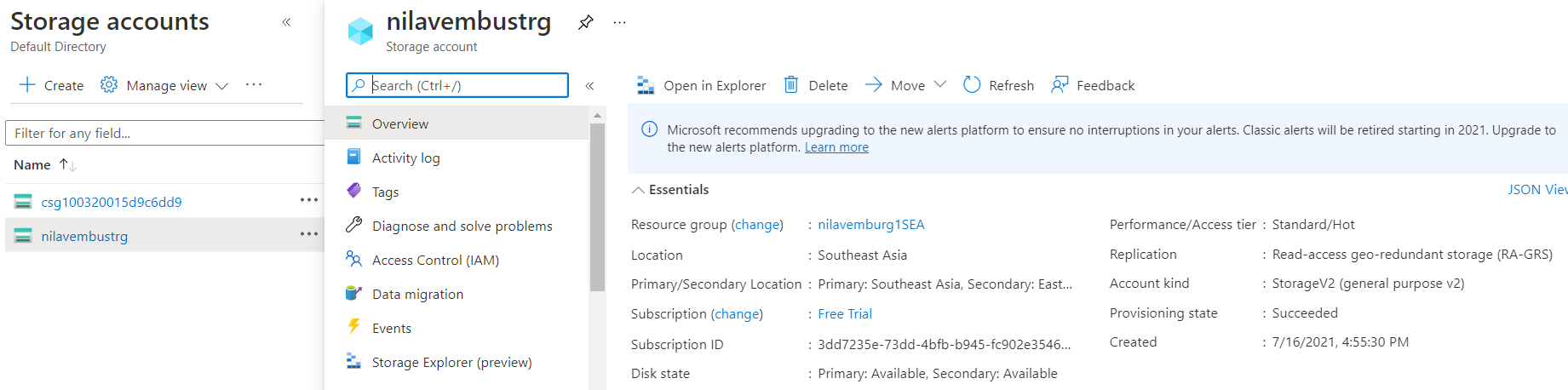


**Creating Storage account for SEA region-**

Creating Storage account -



Storage account has been created for SEA now-

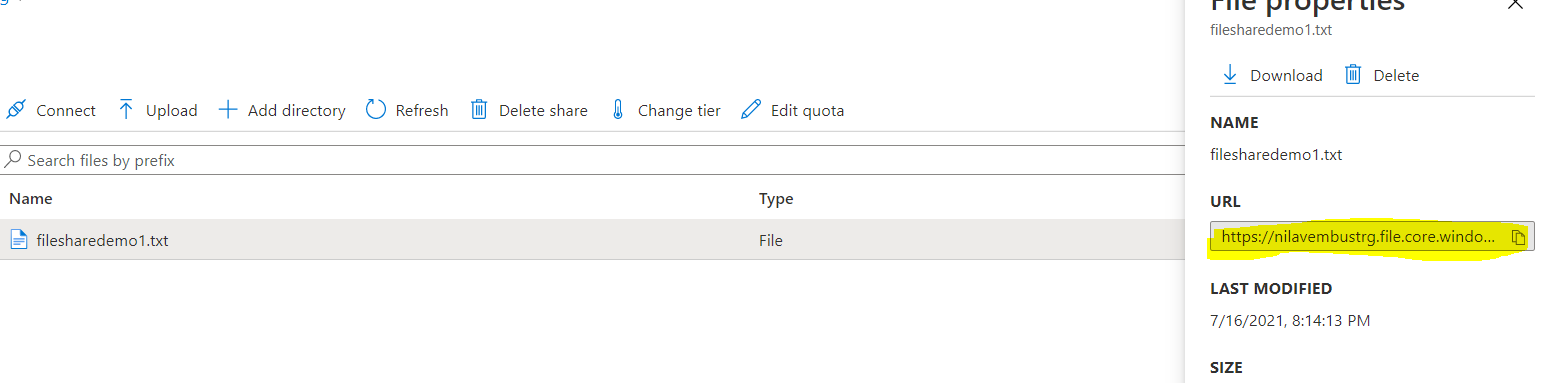


The storage should be accessible by applications with secure access. Provide access urls and keys.

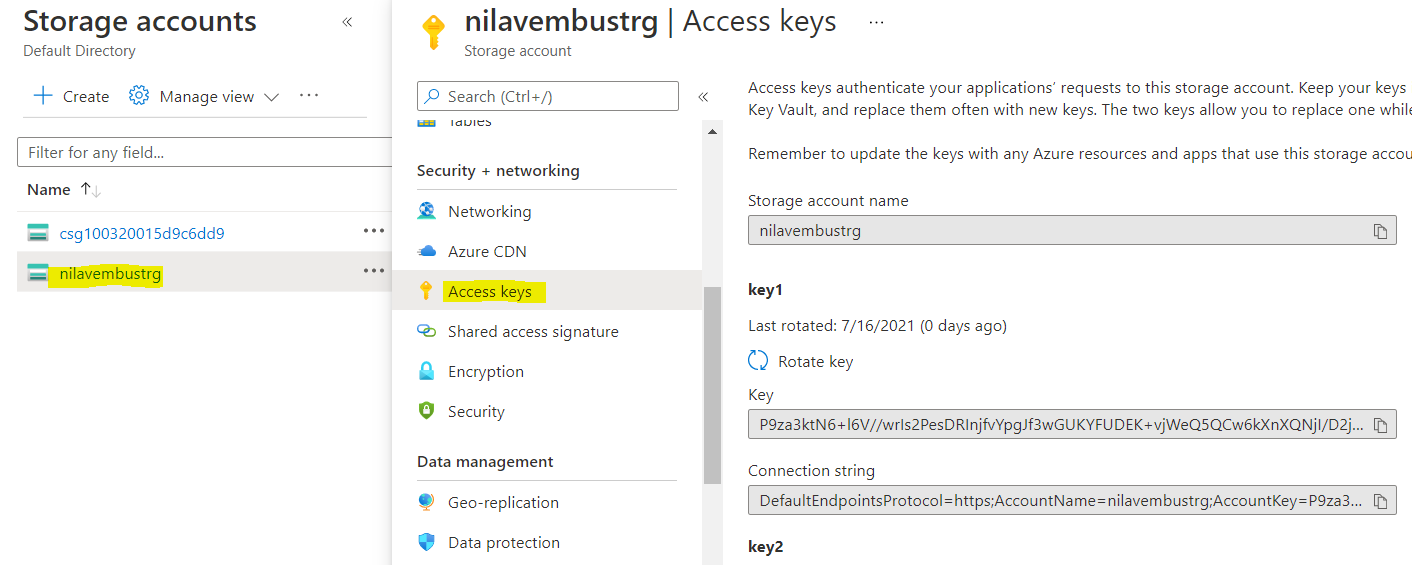
**“Provide access urls and keys.”**

As the storage account has been created now, we can create the required service (table/blob/ fileshare/queue) as per our requirement and can provide the resource URL along with the Access keys(as per current requirement) to the appropriate user.

We can get URL from the file/contents of the Storage resources (in our case:fileshare)



And about Storage keys, we can get from the **Access keys** section under **Security + Networking** in the Storage account.

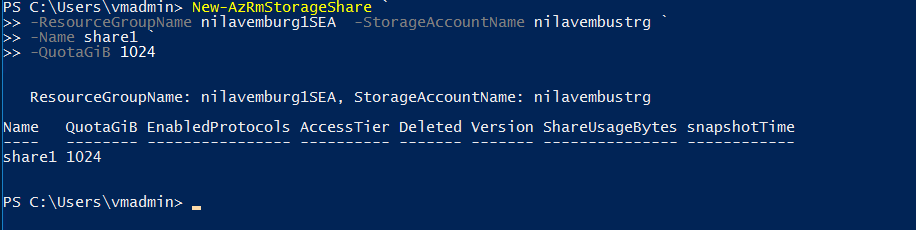


Sales manager should access his resource from windows explorer.

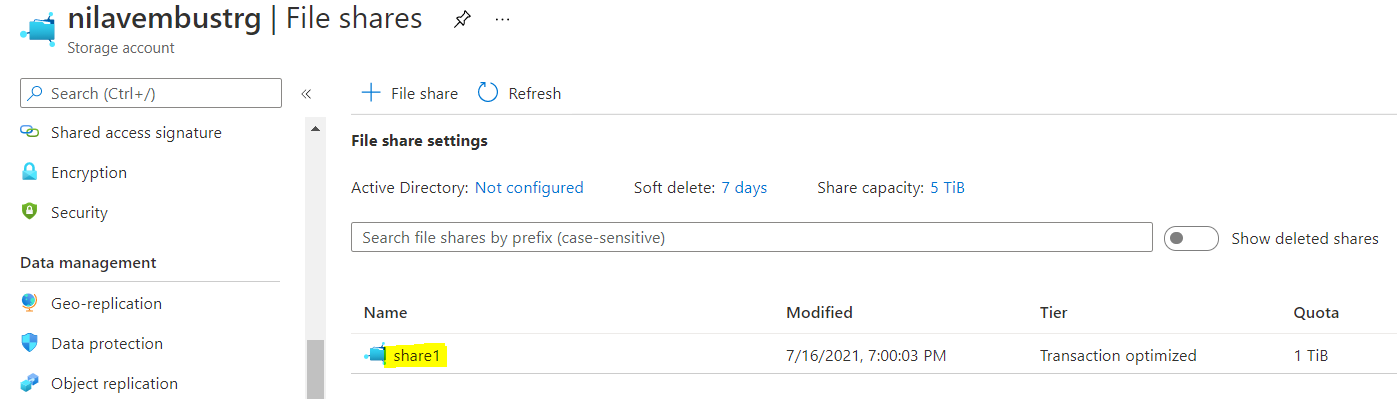
According to the requirement here,

* “Sales manager should access his resource from windows explorer.”

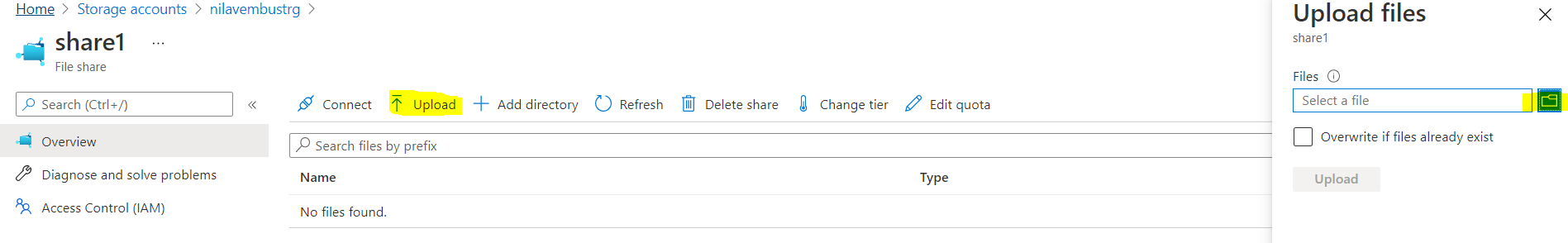
As the resource is to be accessible via Windows Explorer, we will be creating a File share resource-



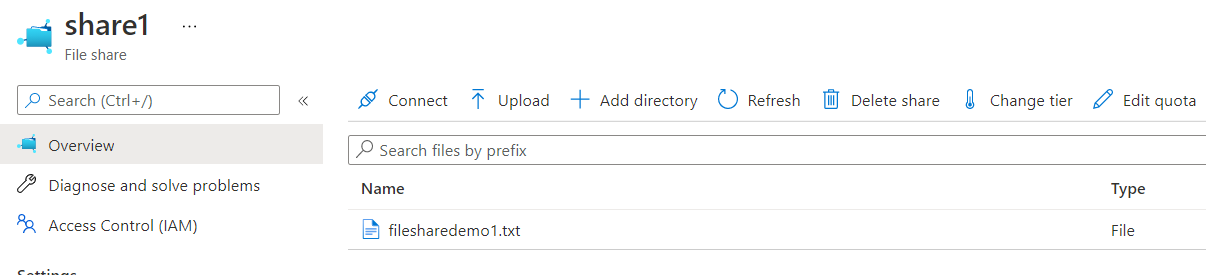
We can see that the File share ‘share1’ has been created now-



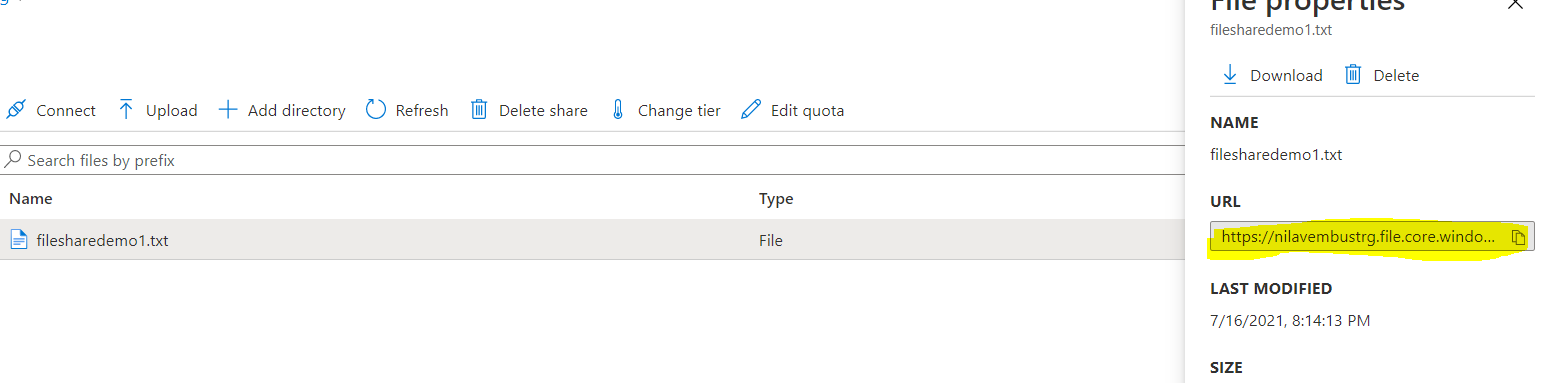
As file share has been created now, open it and click on ‘Upload’ to upload files into the file share.



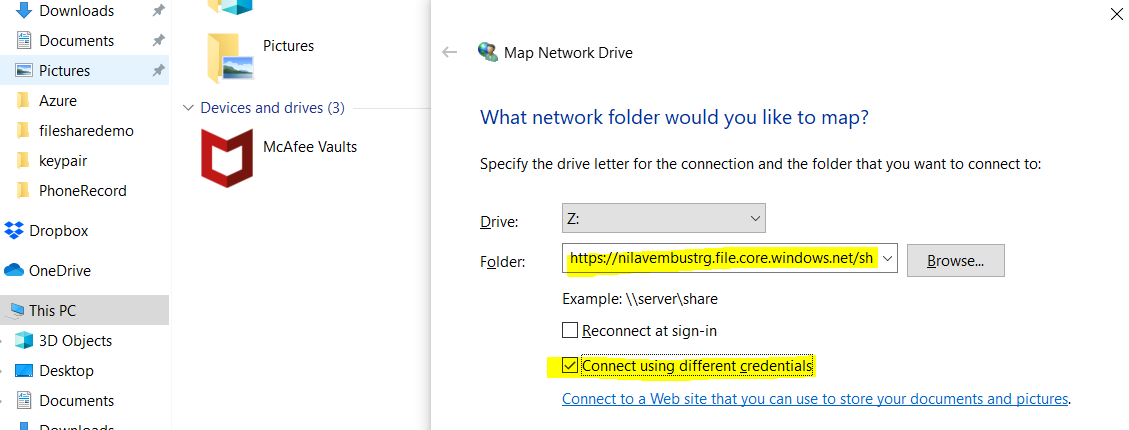
Below selected file has been uploaded in the File share.



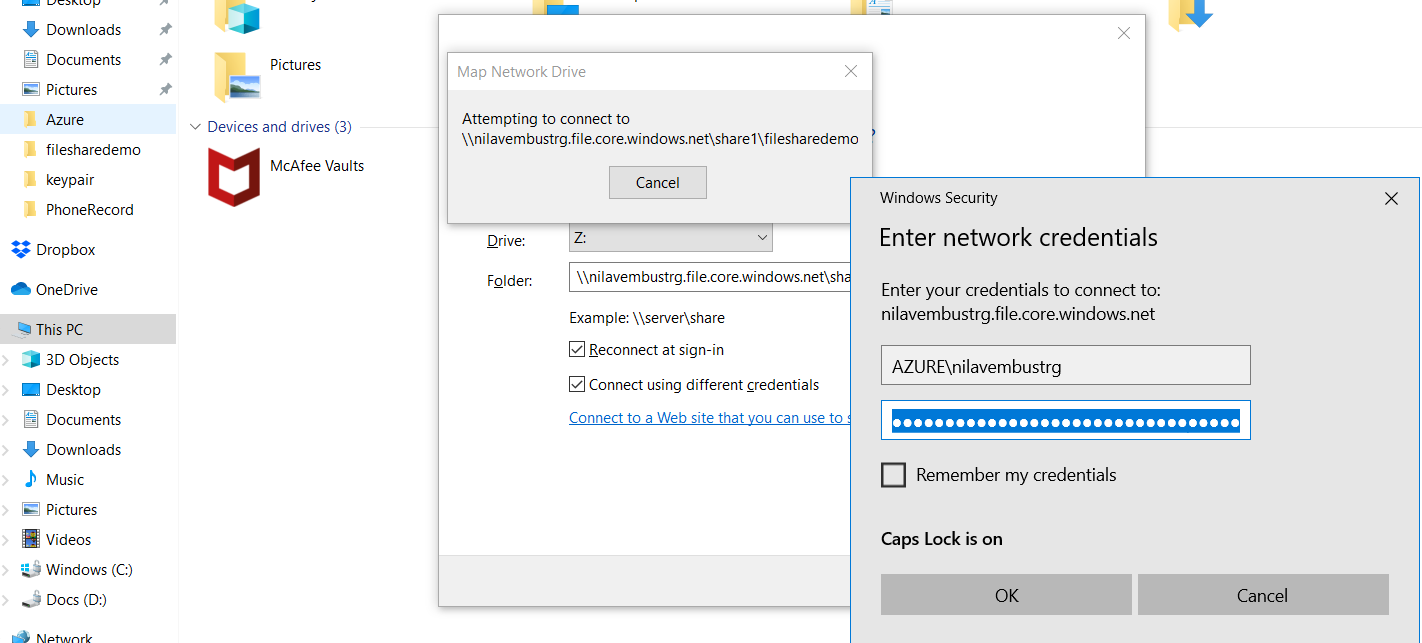
Now, to enable users to use the File share from Windows Explorer, we will copy the File URL so that we can use it to map the share as s drive to user’s local machine.



We can map it through Windows Explorer using Map Network Drive option



However, the same doesn’t work for me currently while trying demo after entering the access key as password and below username(AZURE\file share name) due to port issue-

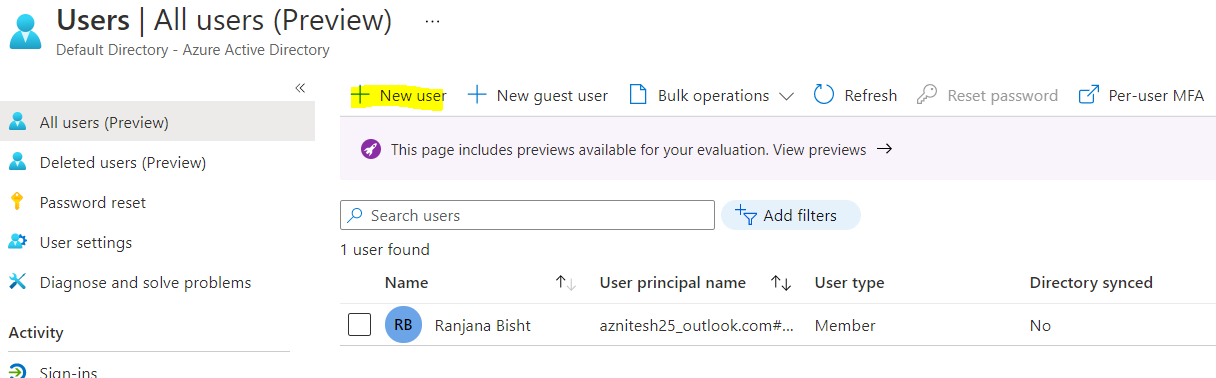


**Resource management-**

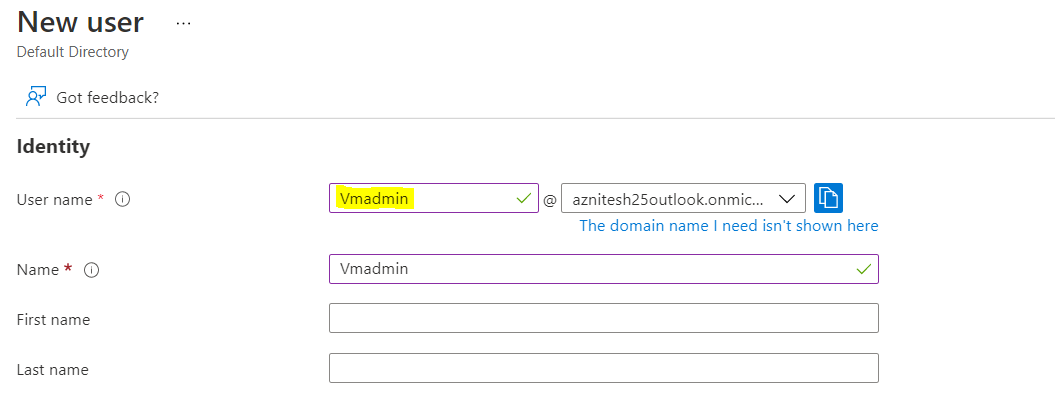
* Create Vmadmin user who can manage all VM in the subscription
* Create Backup\_admin user who can manage backup only in EUS servers in EURG

Create Vmadmin user who can manage all VM in the subscription

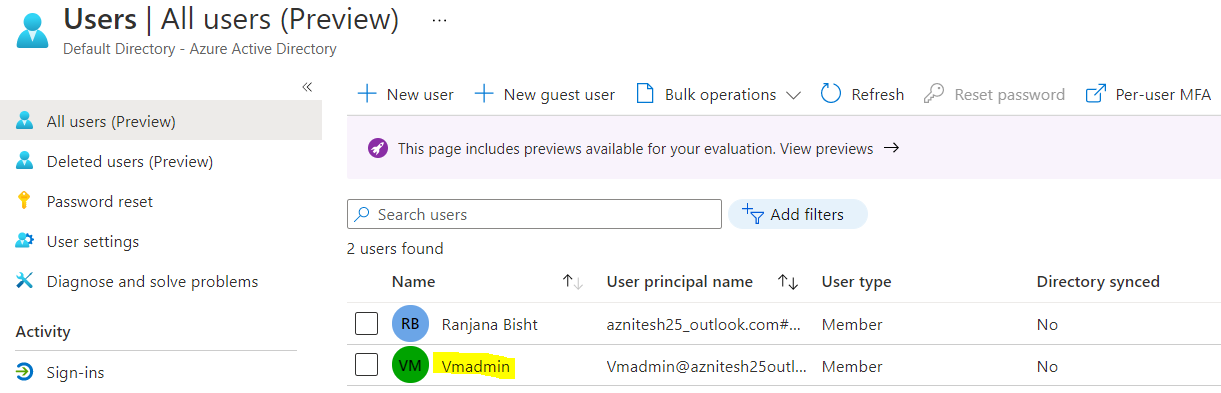
To create a new user, we will go to Azure active Directory service, add ‘New user’.



We will create a new user, **Vmadmin** as per our requirement as mentioned and add the user to AAD.



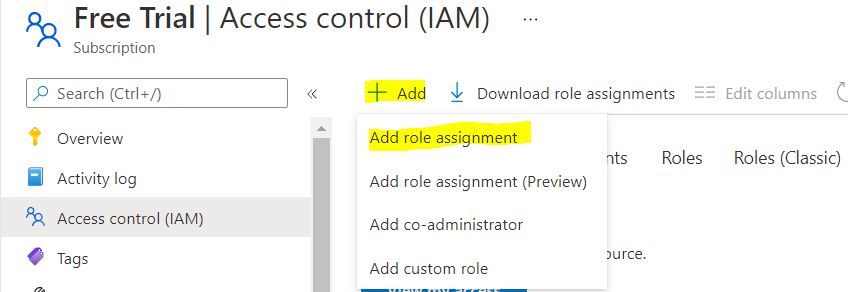
User ‘Vmadmin’ has been created now.



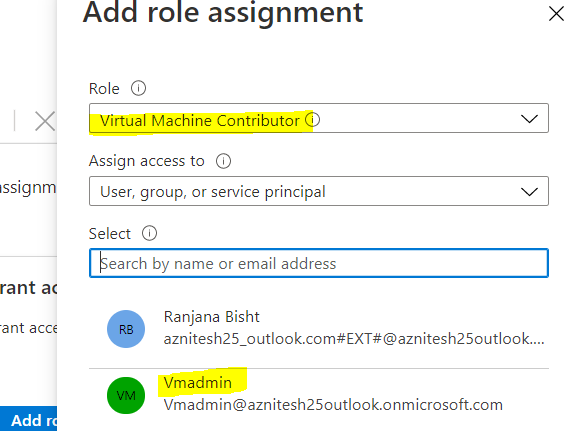
As we need user **Vmadmin** to manage all the VMs in the **Subscription**, we will assign appropriate role to the user at **Subscription** level.

Go Subscription -> Click on the Subscription -> Access control (IAM)

Click on **+ Add** and select **‘Add role assignment’**

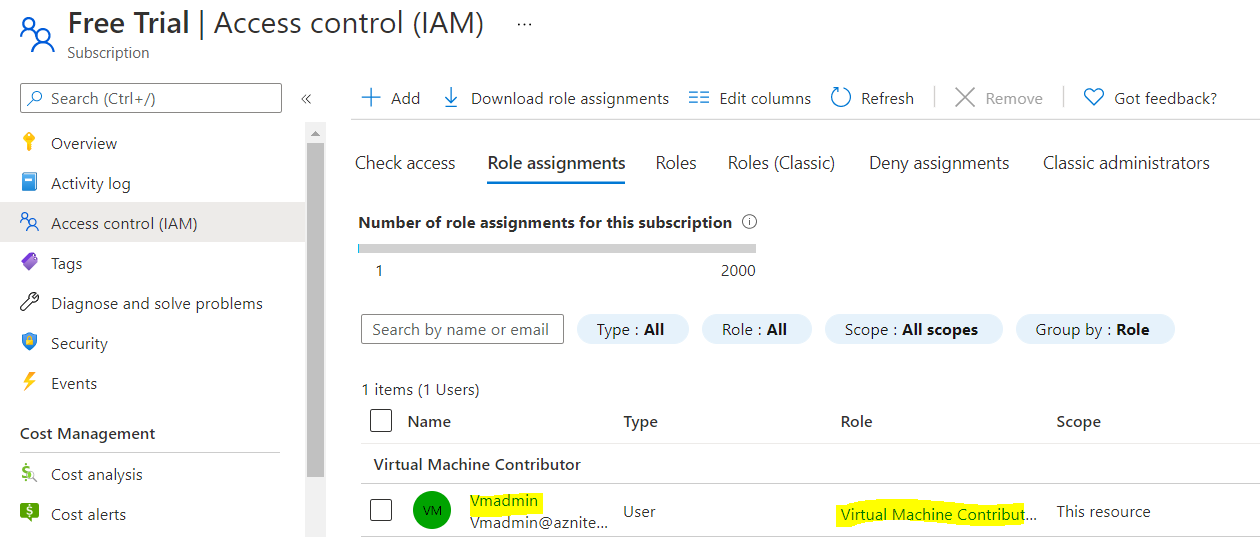


As suitable for the specified task, we will select **Virtual Machine Contributor** role and will select the user **Vmadmin**.



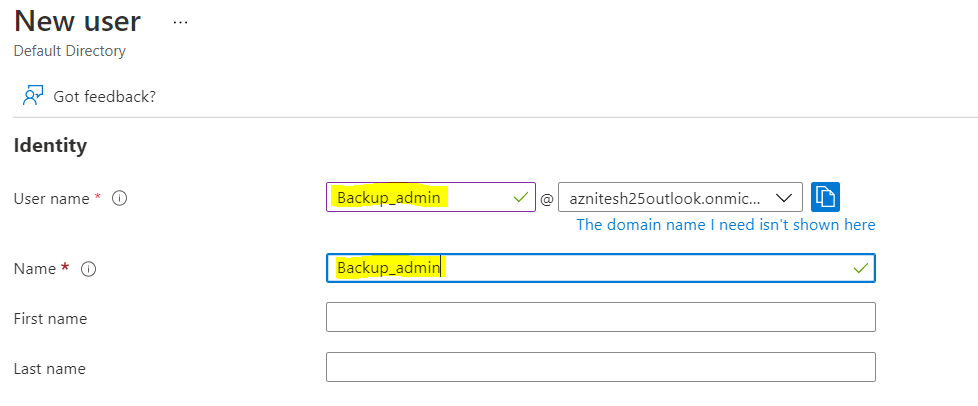
Access has been set up now for user Vmadmin.

This user can now mange all the virtual machines in the Subscription.

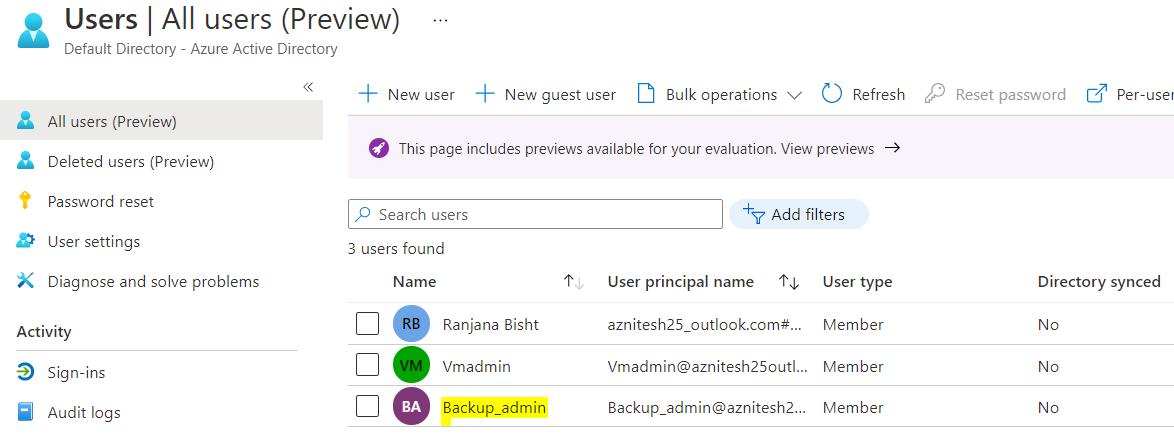


Create Backup\_admin user who can manage backup only in EUS servers in EURG

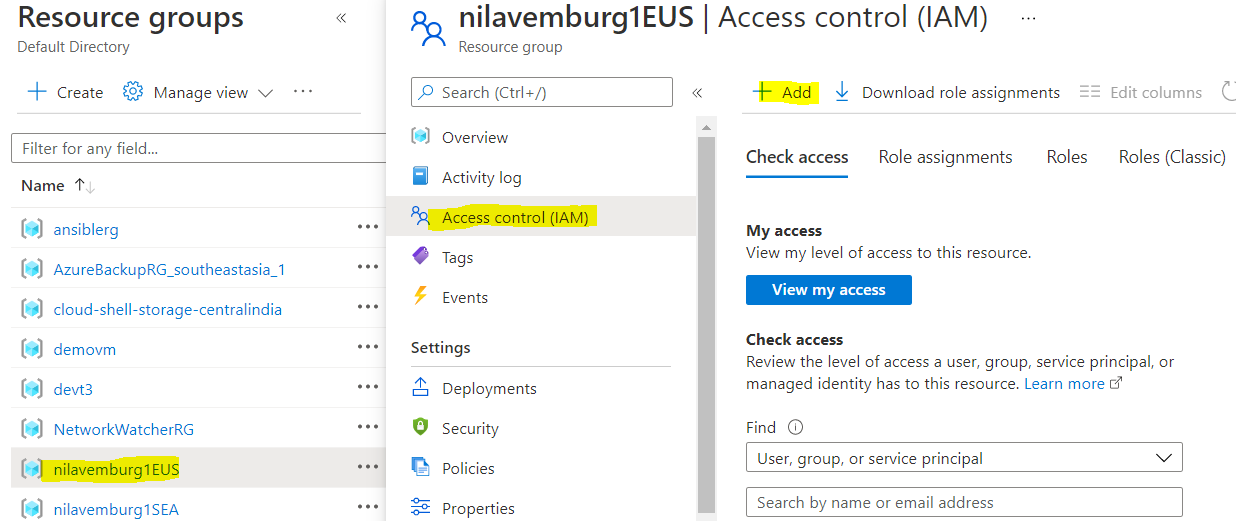
As we need another user Backup\_admin for backup related tasks, we will create the user as below-



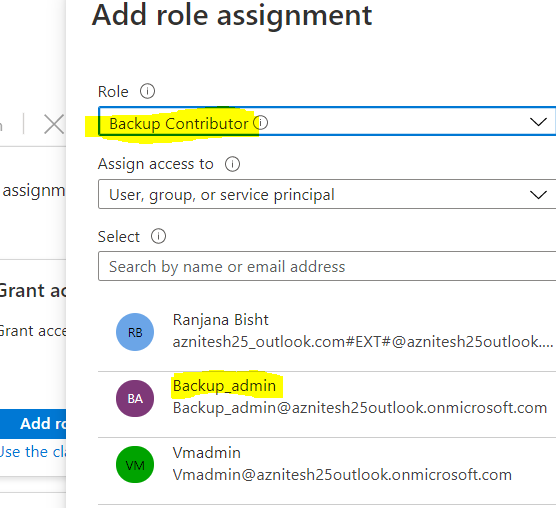
User Backup\_admin has been created now.



As the Backup\_admin need to manage the Backup tasks for **EUS** resource group VMs only, we will provide relevant access at **Resource group level**.



We will choose **Backup Contributor** role and will select the required user.



User Backup\_admin have been created now as specified. And this user can manage all the Backup tasks for EUS created RG.

