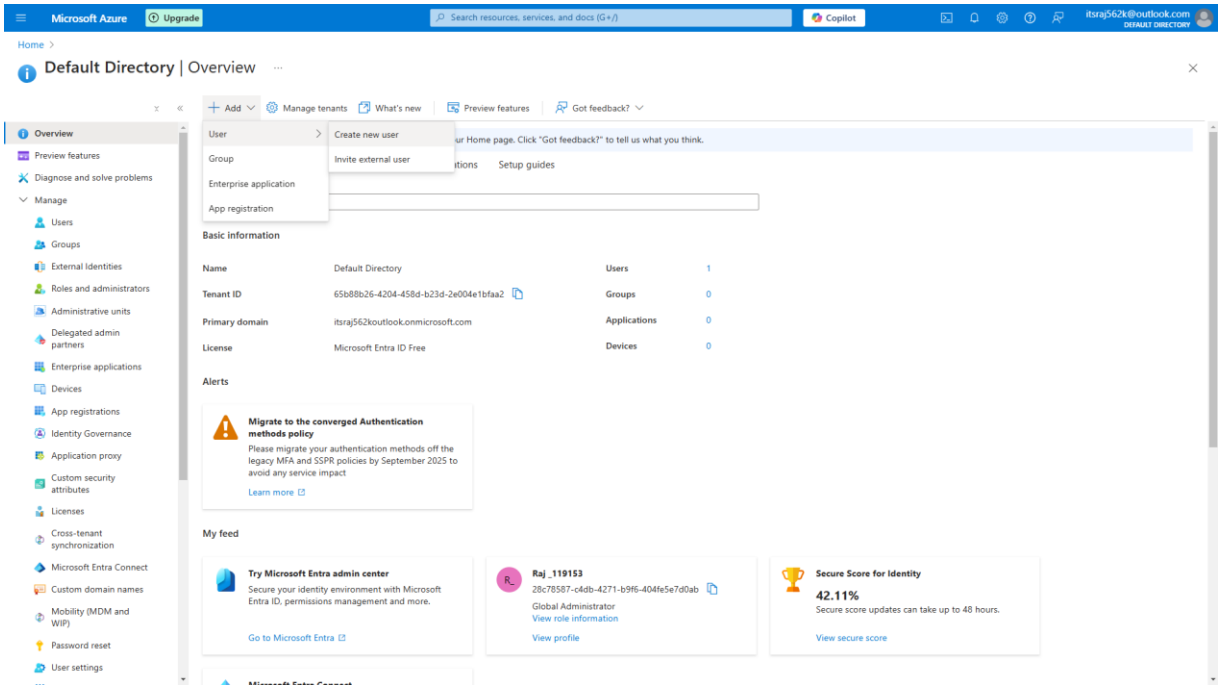
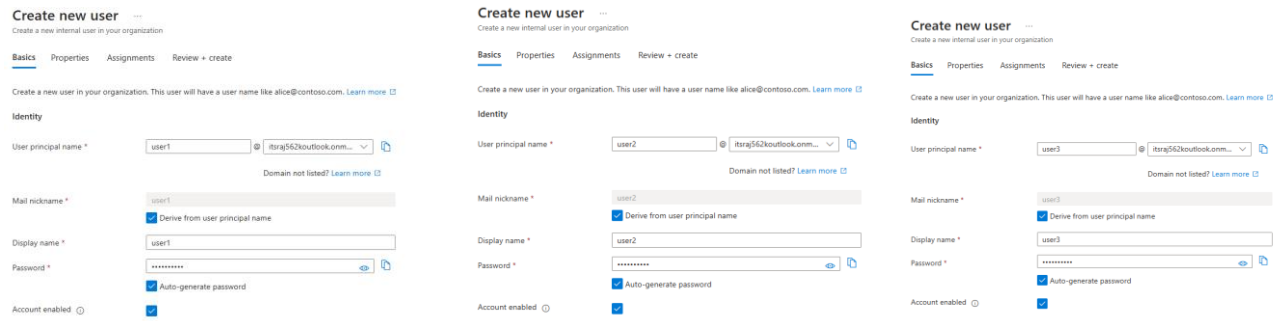
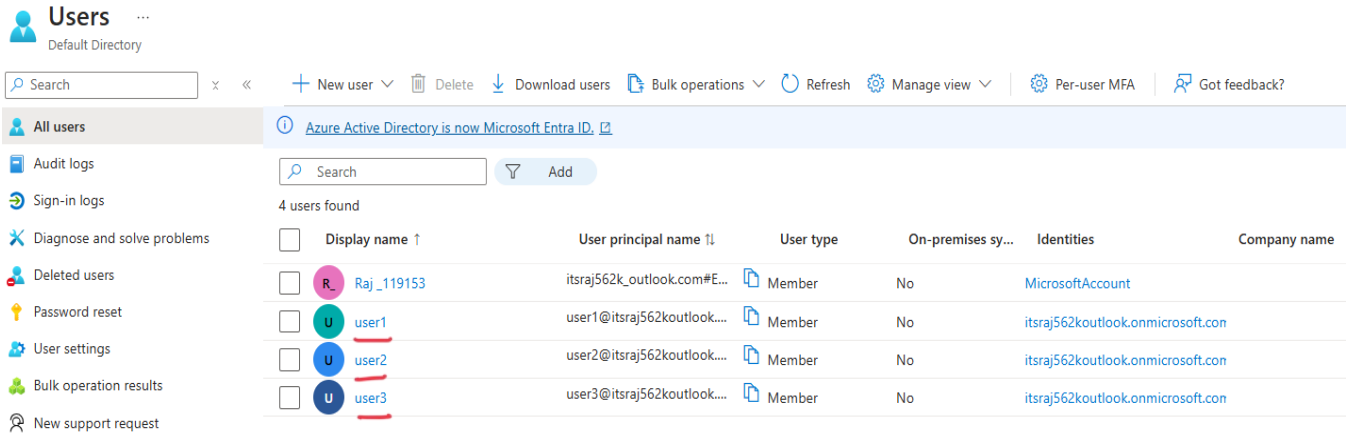
AZURE Project

Task 1

Create 3 users in Entra Id.



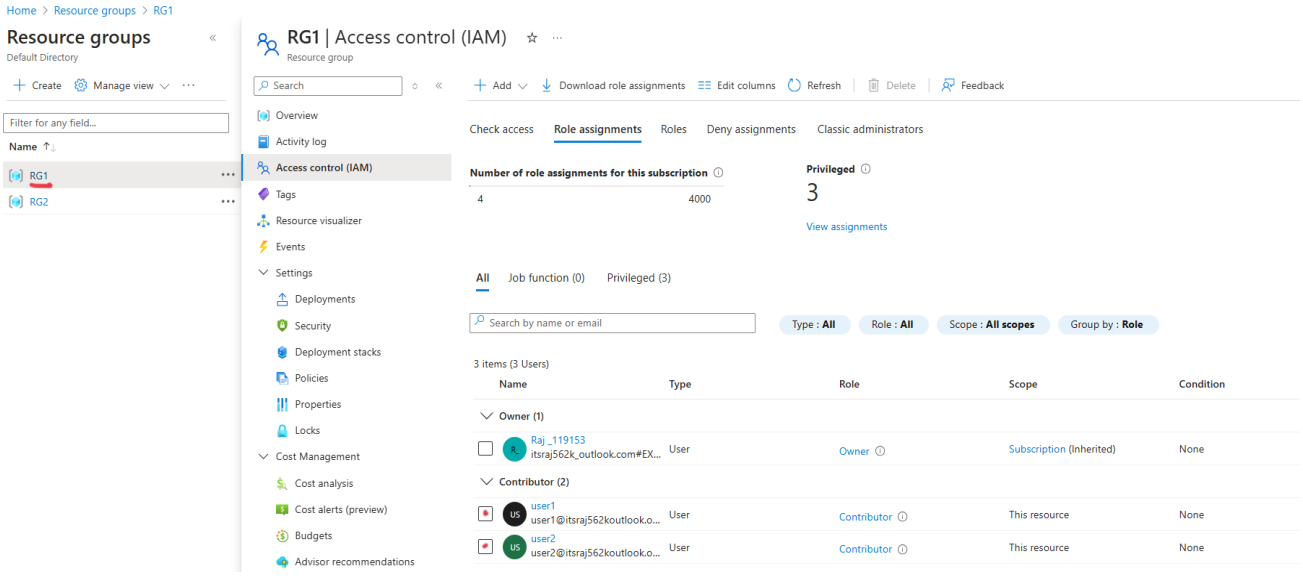


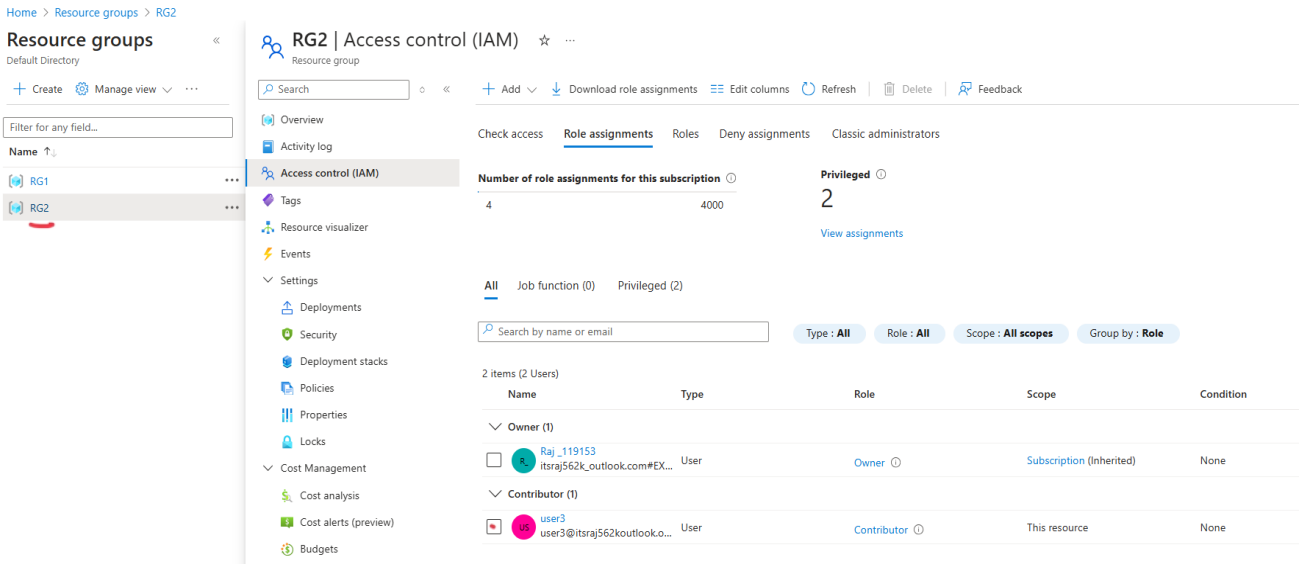


Task 2

➔ Assigning contributor access to user1 and user2 in RG1 Resources Group level.

➔ Assigning contributor access to user3 in RG2 Resources Group. Why because, User3 should not have access to VM of user1 and user2.





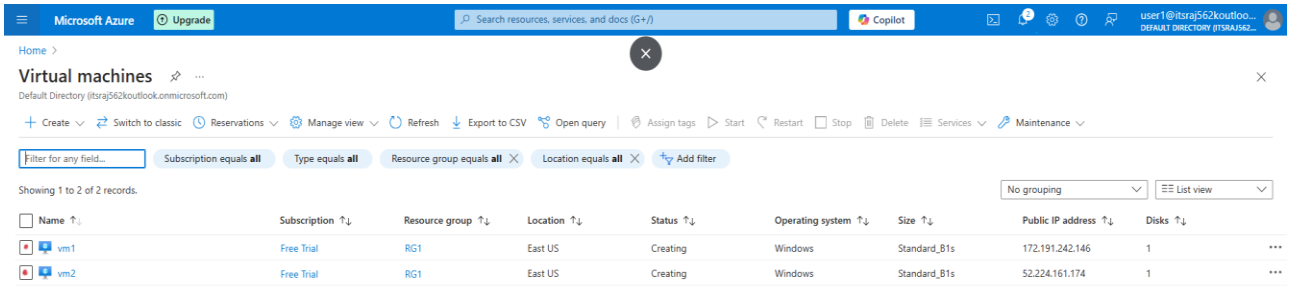
Task 3

user1 → Create virtual Machine1

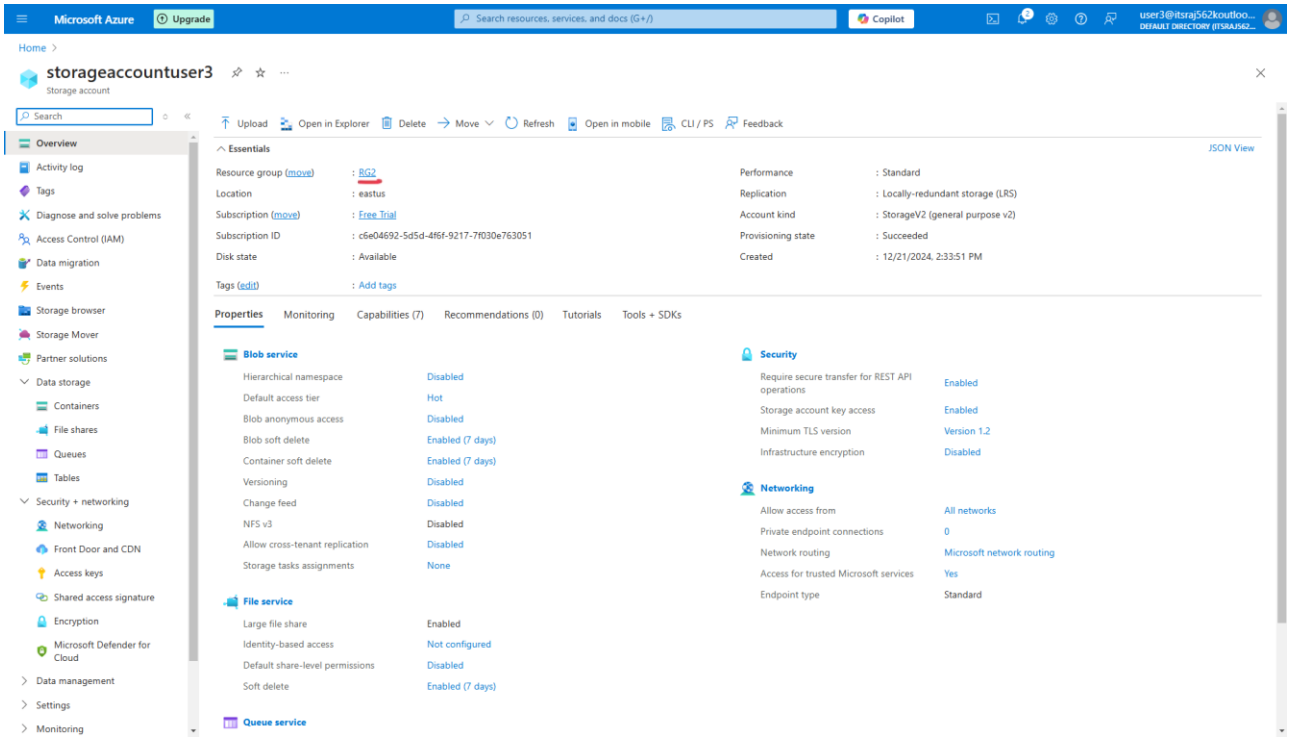
user2 → Create virtual Machine2

user3 → Create Storage Account

➔ User1, user2 virtual machine.

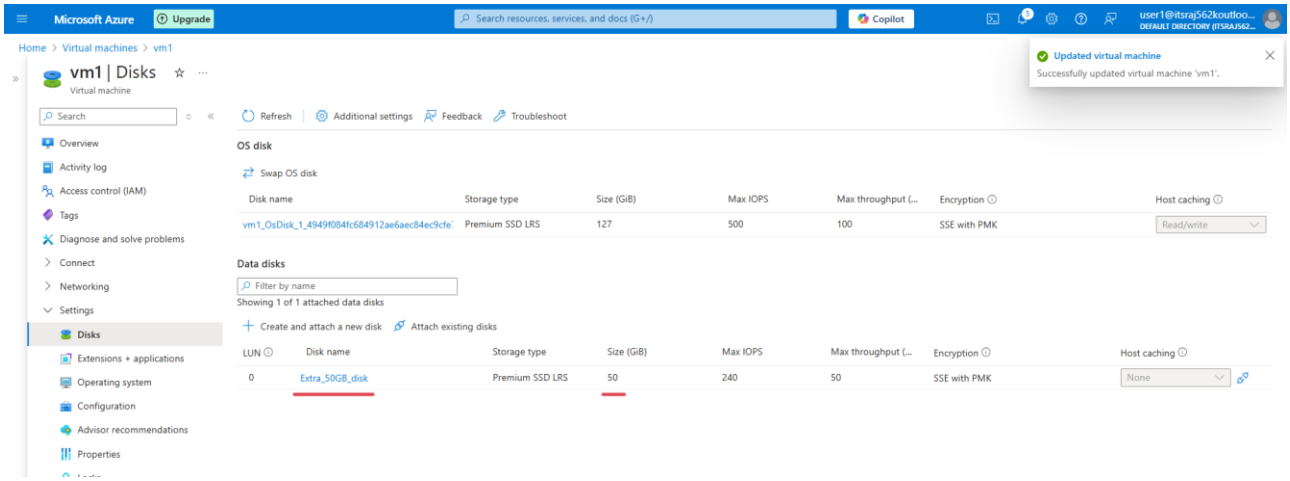


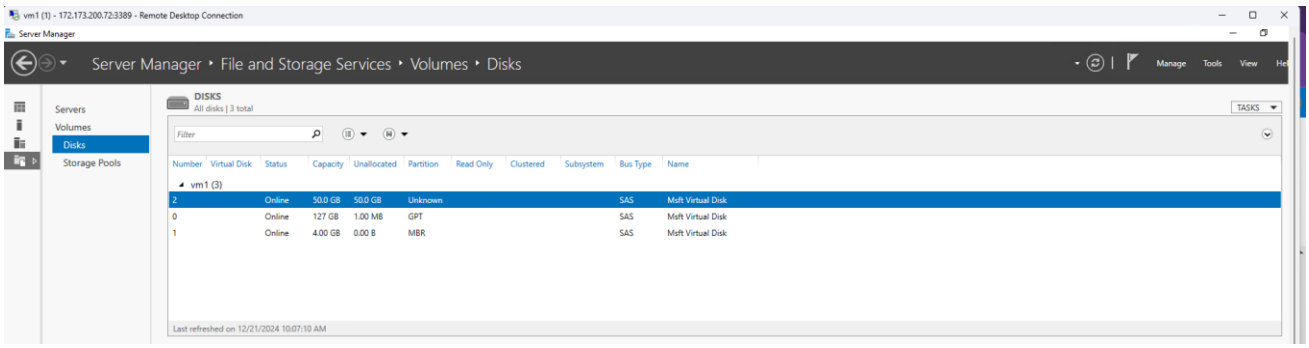
➔ User3 storage account.



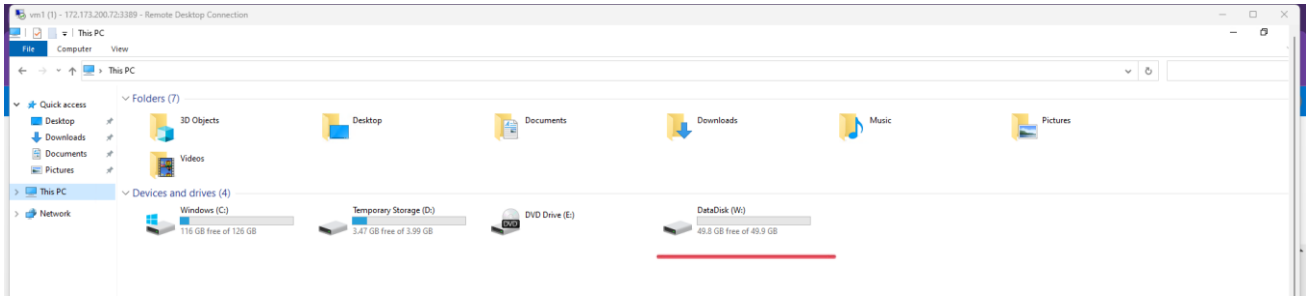
Task 4

In vm1 add extra 50GB DataDisk.



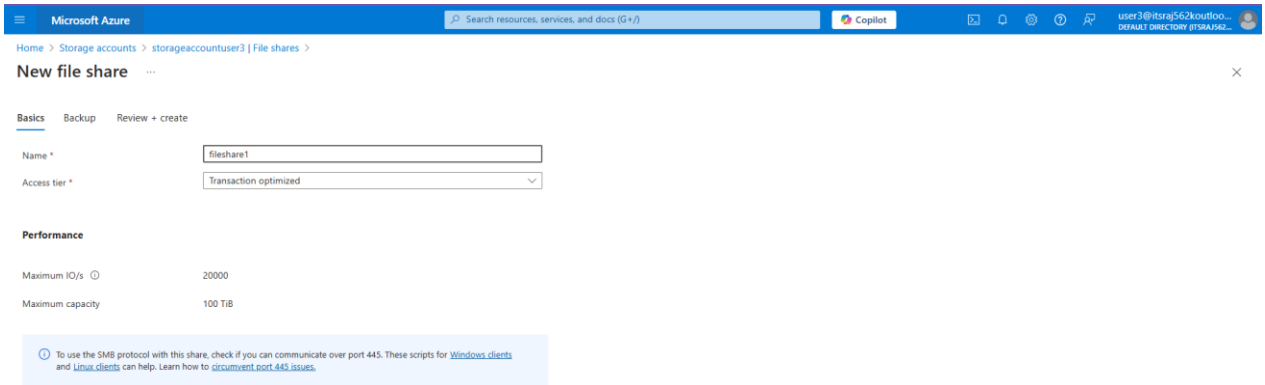


➔ 50GB DataDisk has been created.

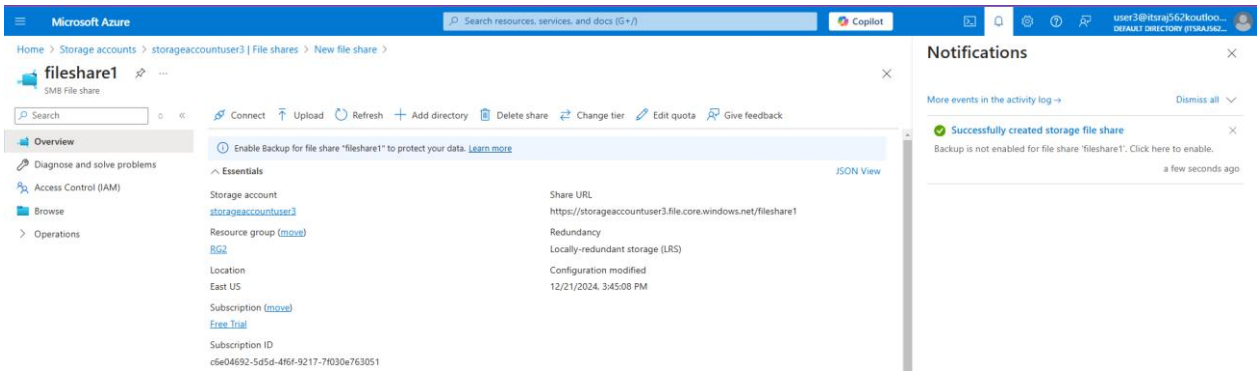


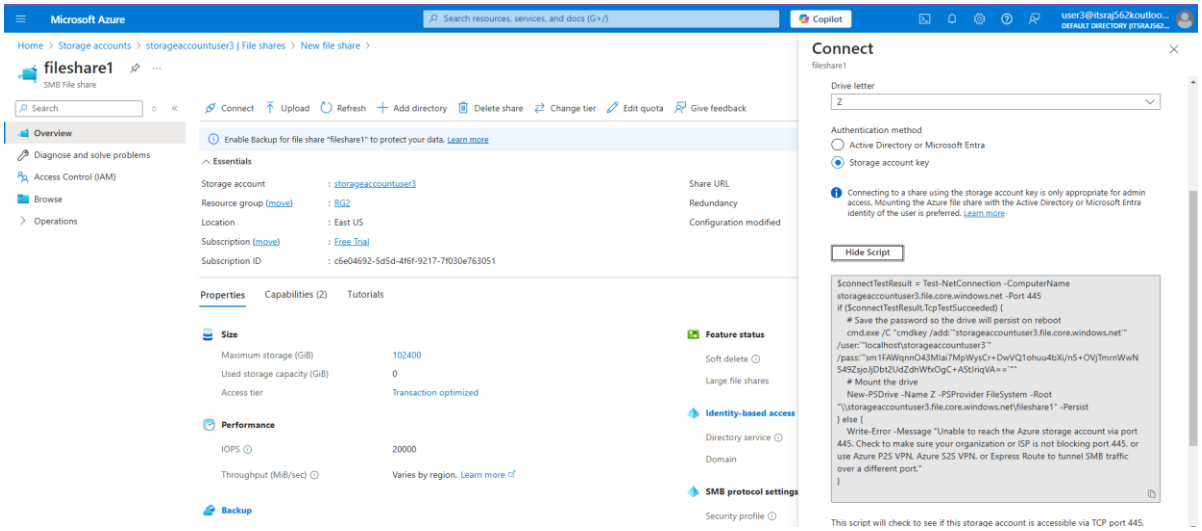
Task 5

Create fileshare in user3 account and mount it in the vm2 machine.

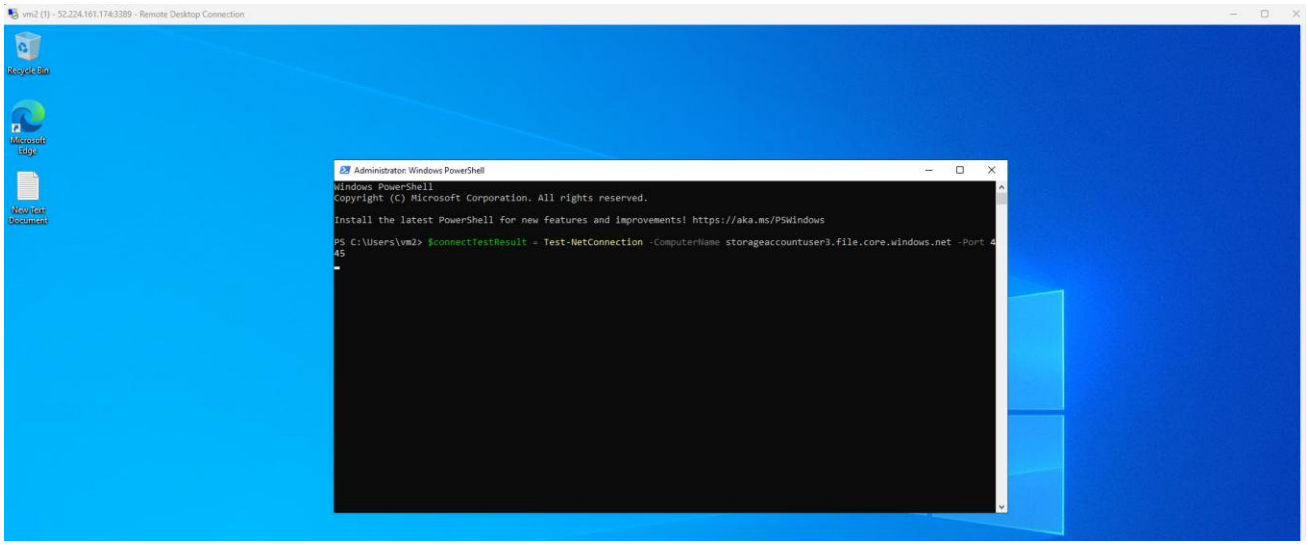


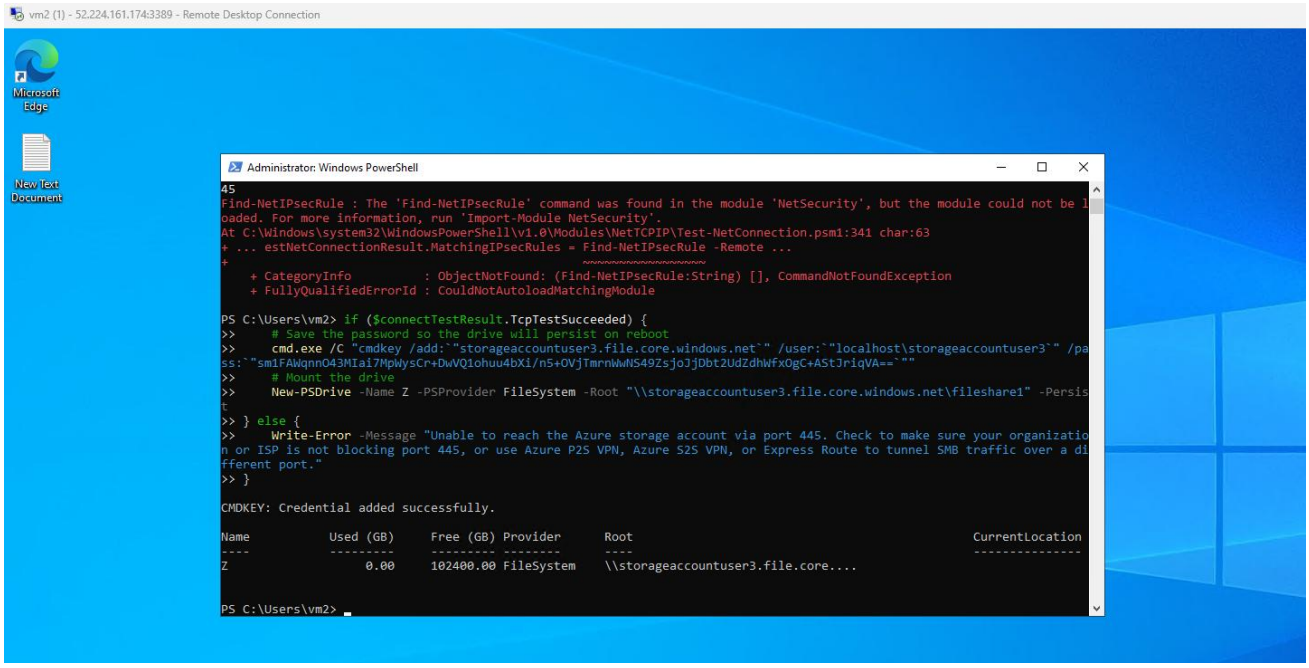
→Fileshare1 created in user3 account.



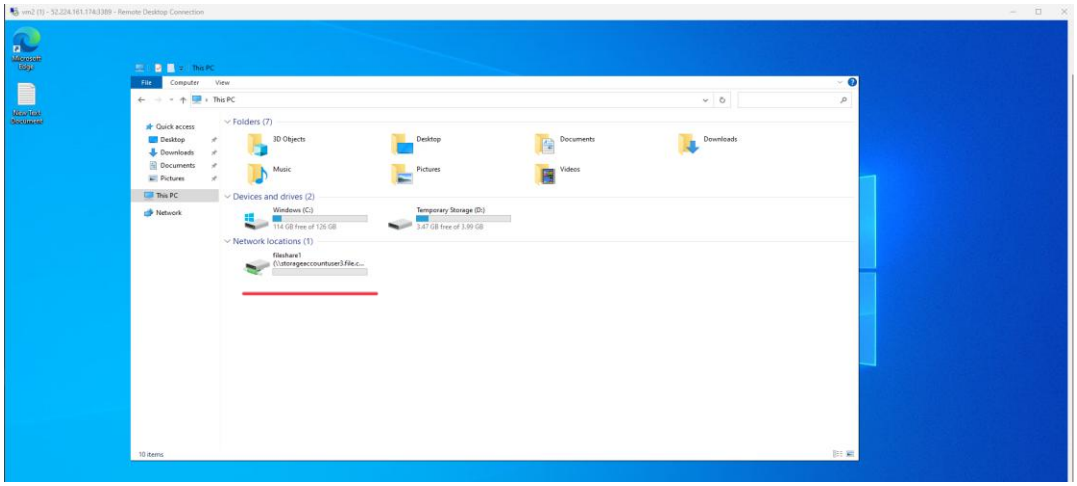


➔ Copying the script from fileshare1 and paste it in the vm2 PowerShell.

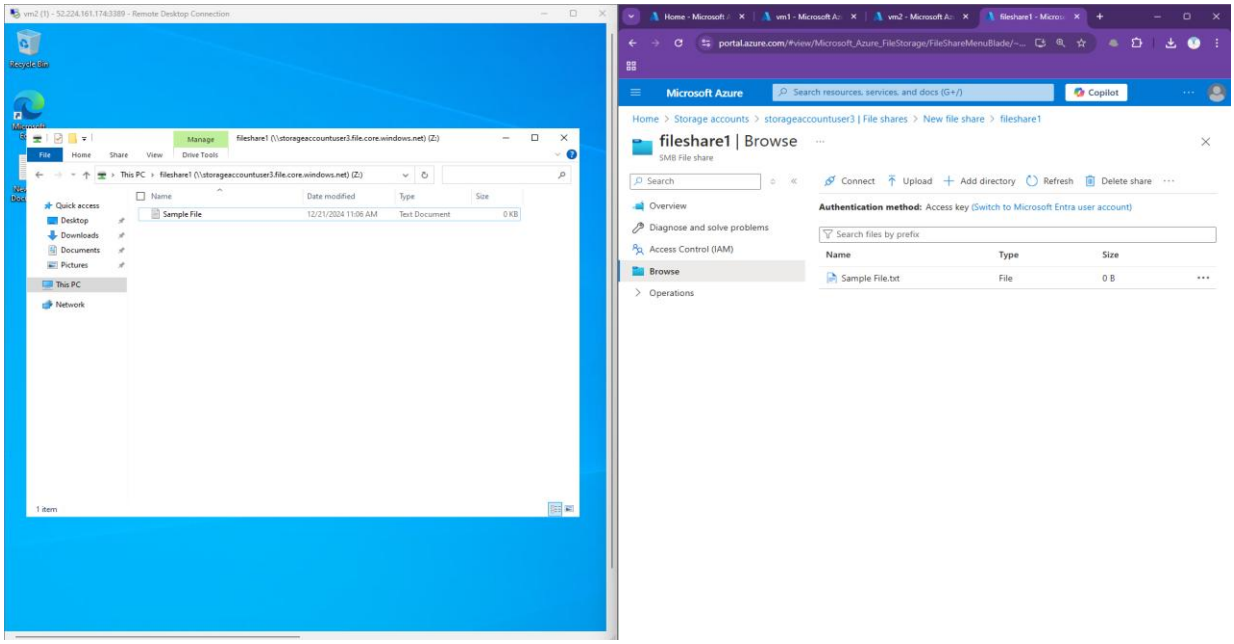




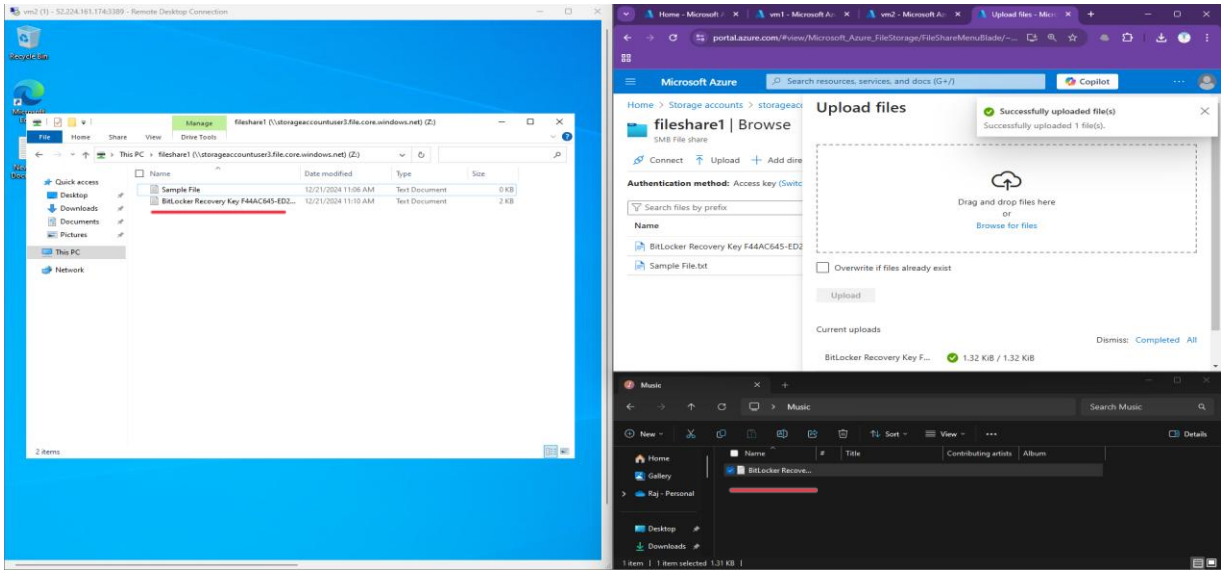
➔ Successfully mounted Fileshare1 in the vm2.



➔ If I create Sample File in the vm2 it will be reflected in fileshare1 which is in user3 storage account.



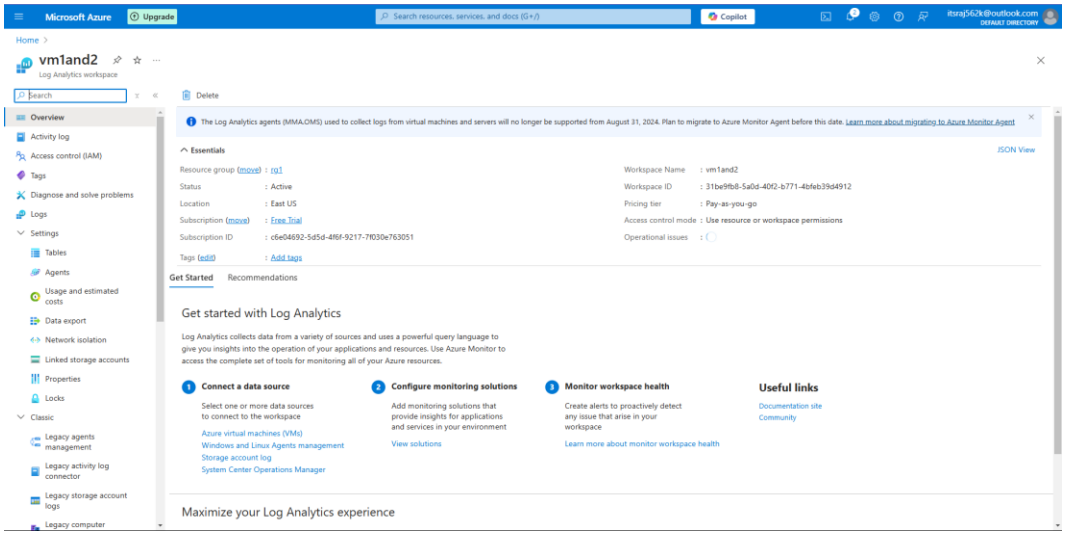
➔ If I upload BitLocker key in the fileshare1 which it will reflect in vm2 fileshare1.



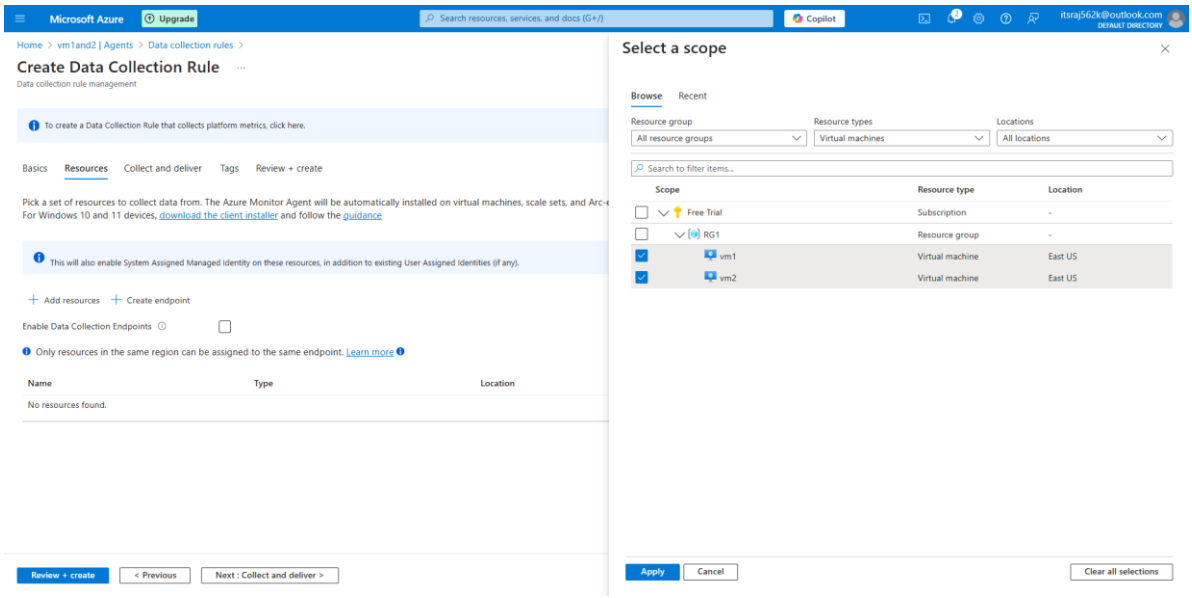
Task 6

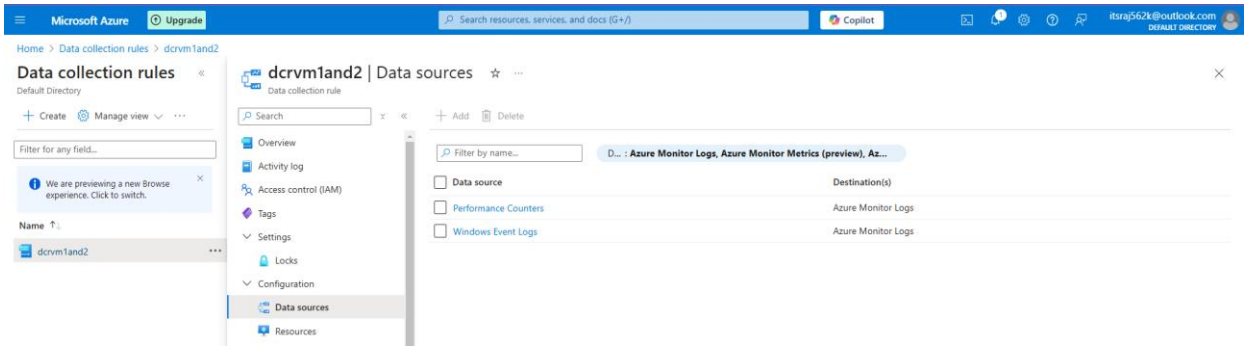
Sending vm1 and vm2 logs to log analysis workspace using DCR.

➔ Log Analysis Workspace was created.

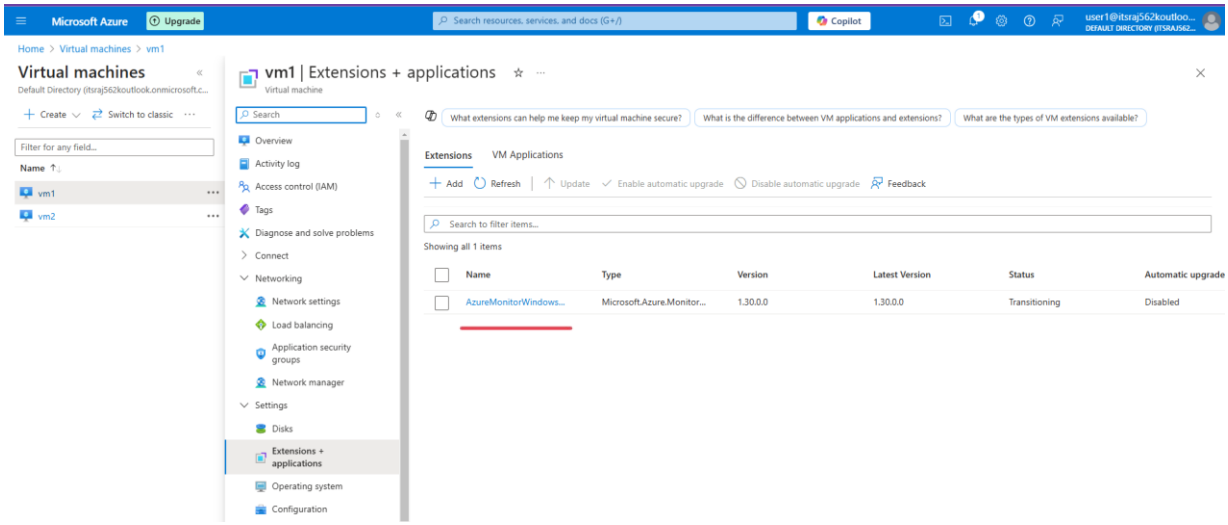


➔ In DCR adding vm1 and vm2 resources, including the destination, which is LAW.

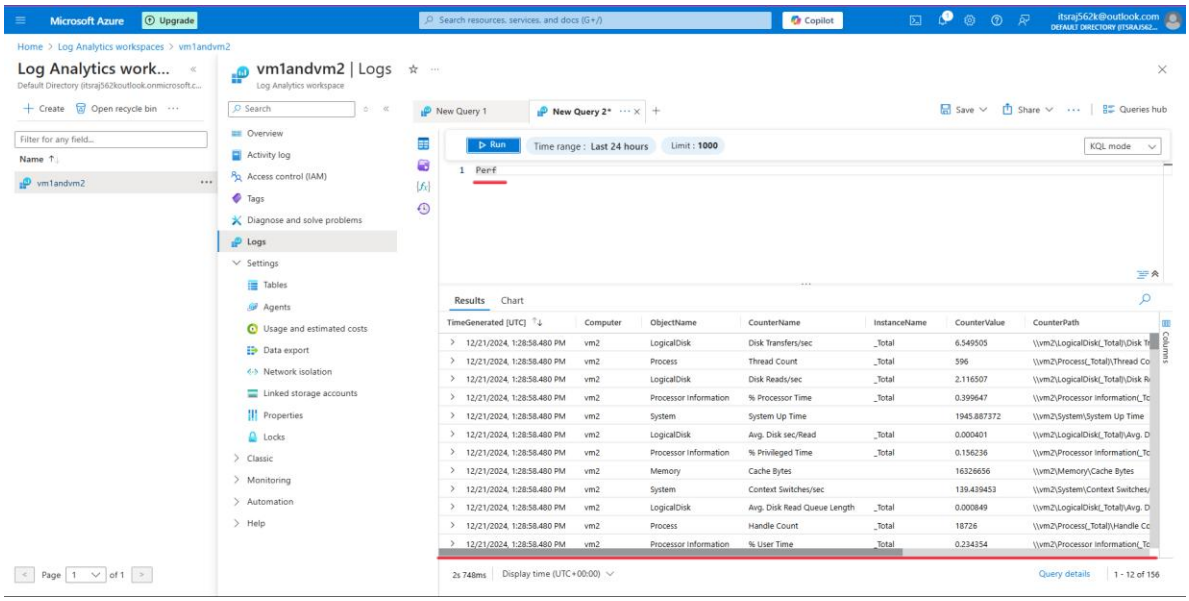


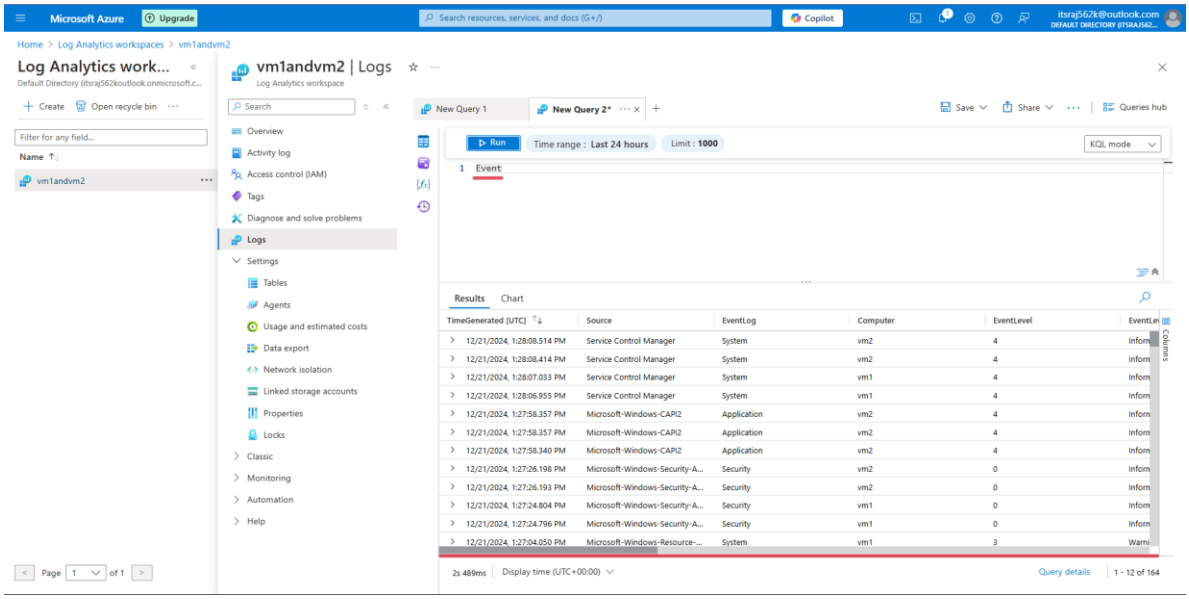


➔ Agent was created in both vm1 and vm2.



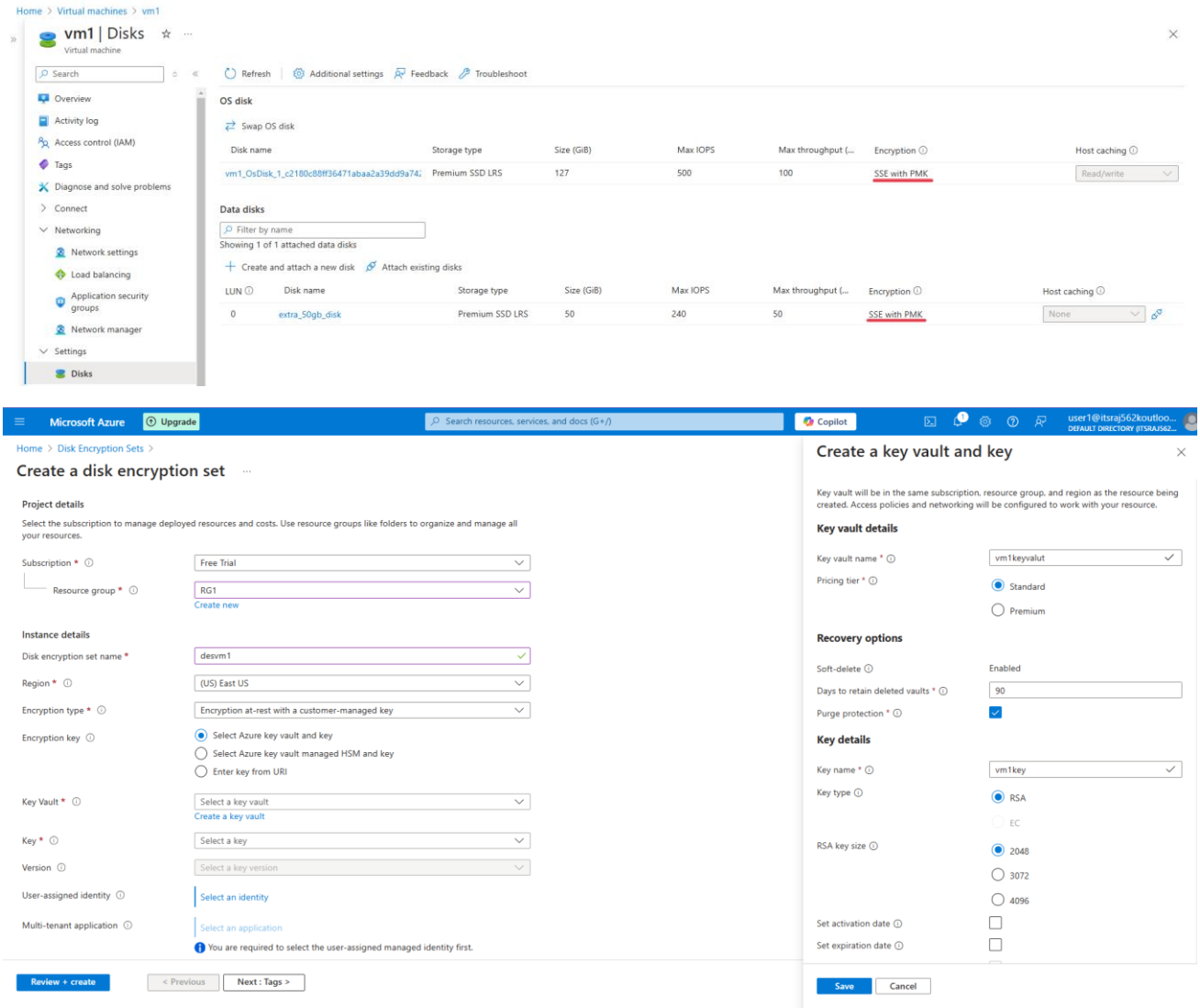
➔ When I type “perf” and “Event”, It shows all the results of vm1 and vm2.



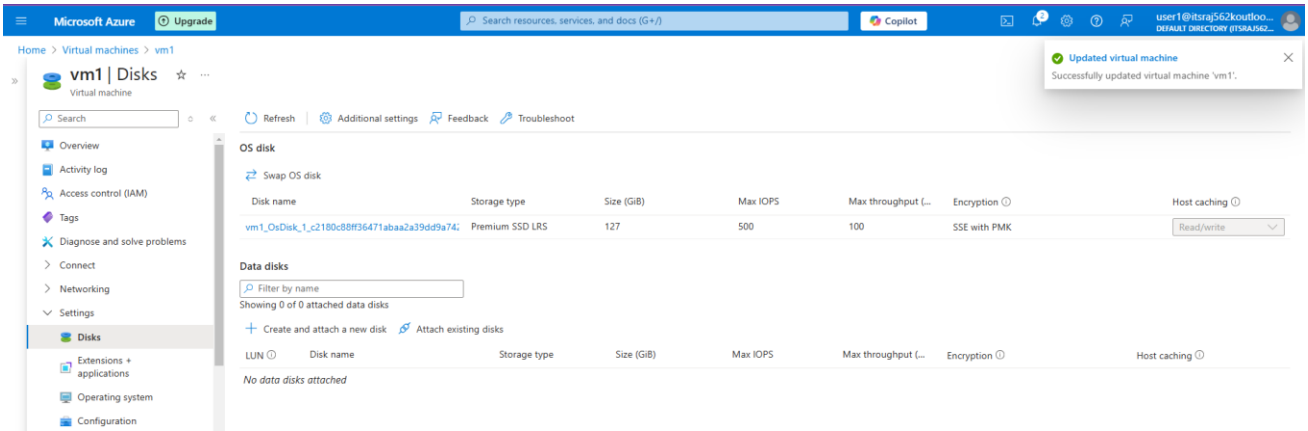


Task 7

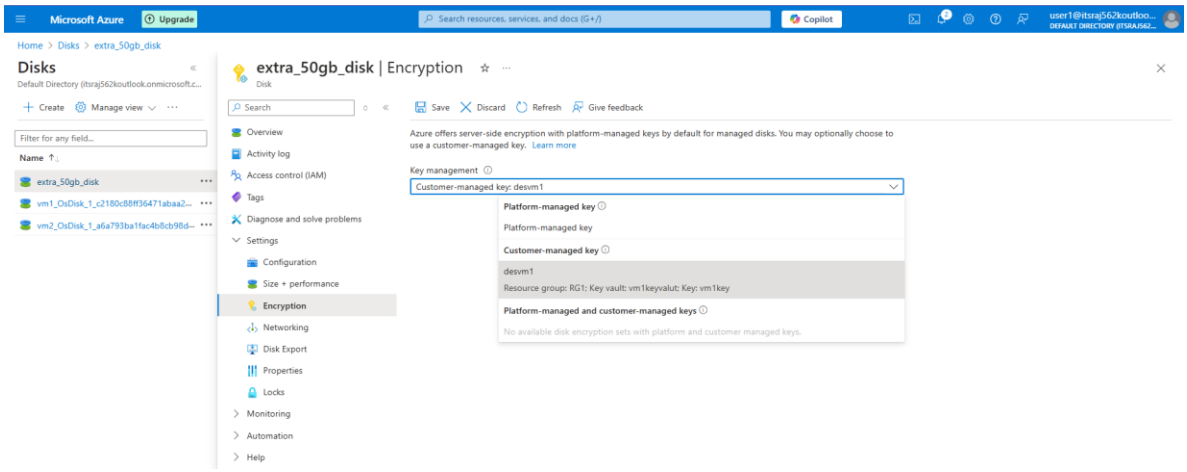
Converting VM1 OS Disk & Data Disk Encryption from PMK to CMK Using Azure Key Vault.



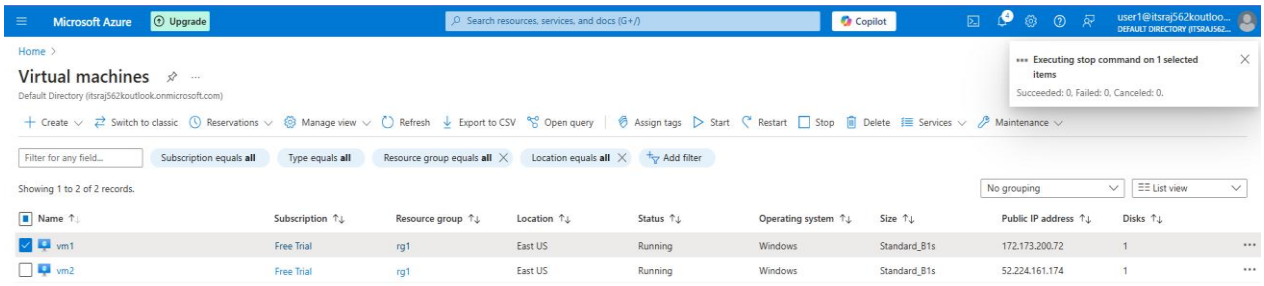
NOTE: Changes to encryption settings can only be made when the Data Disk is unattached.



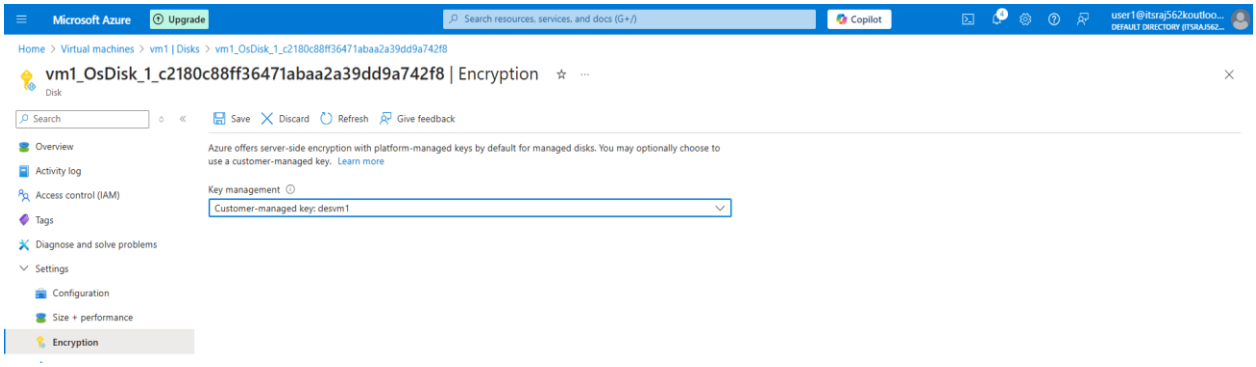
→Changed Data Disk encryption from PMK to CMK.



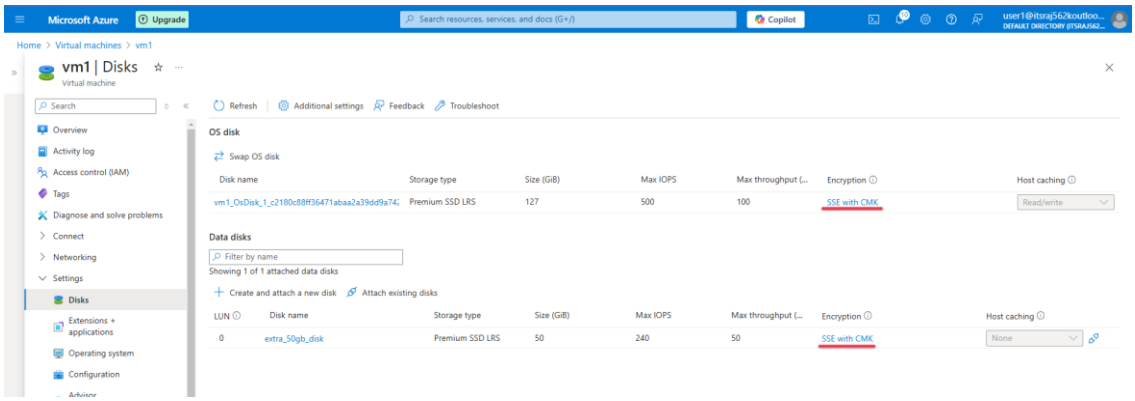
→Changing OS Disk Encryption to CMK is possible after Stopping the Instance.



→Changed OS Disk encryption from PMK to CMK.



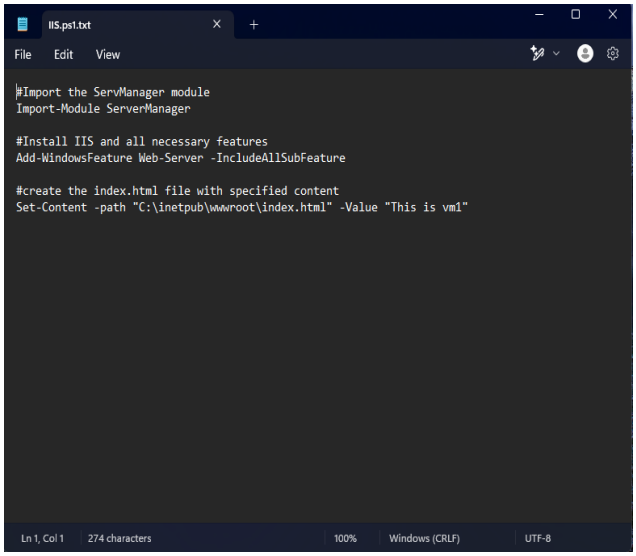
➔ Now both OS Disk and Data Disk encryption was changed to CMK.

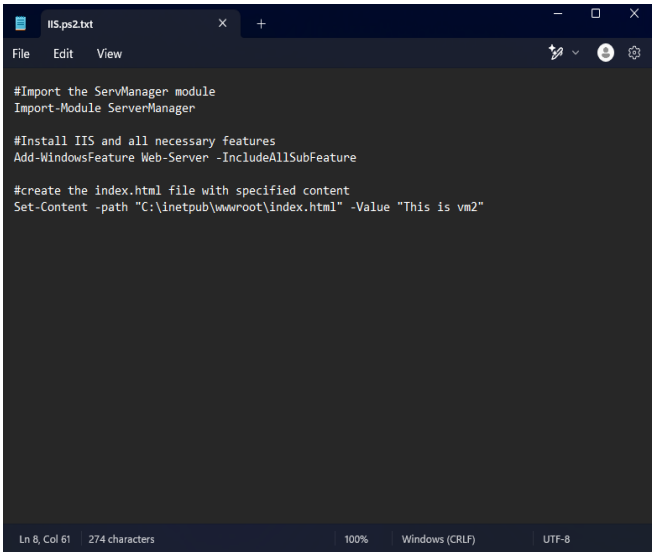


Task 8

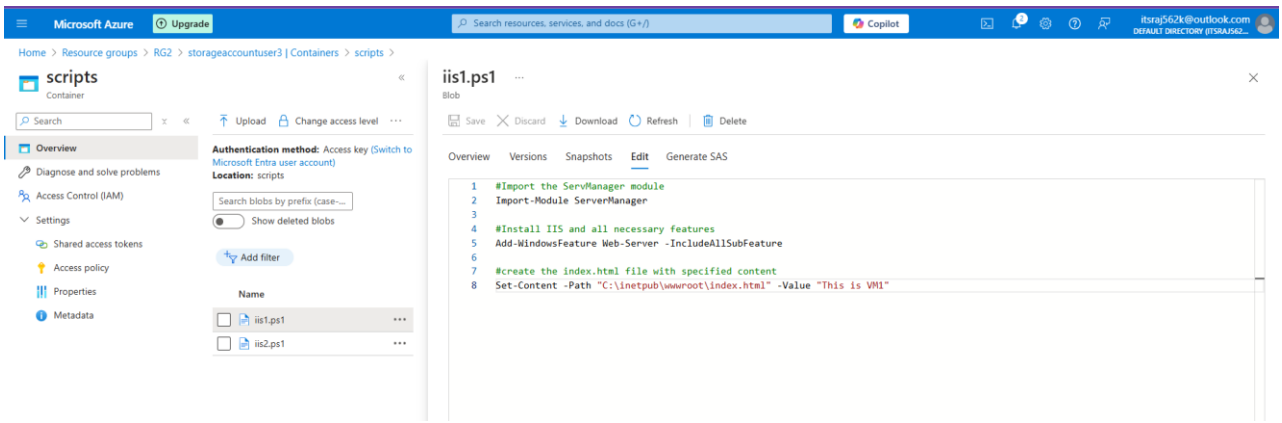
Automating IIS Installation on VM1 and VM2.

➔ I have 2 PowerShell script for Automating IIS.

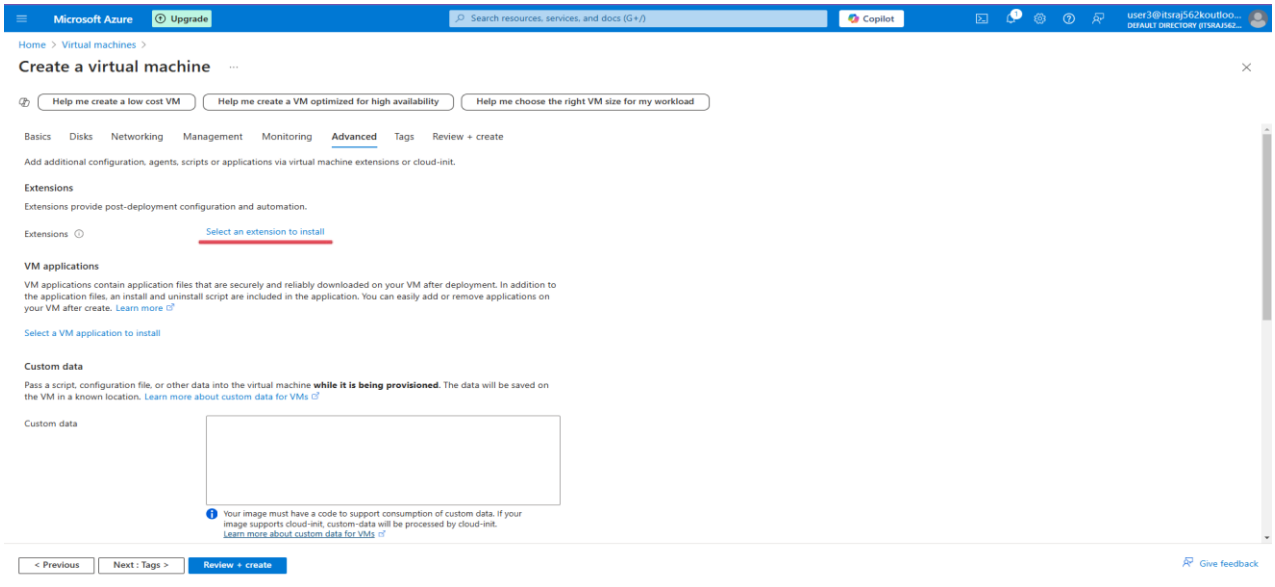


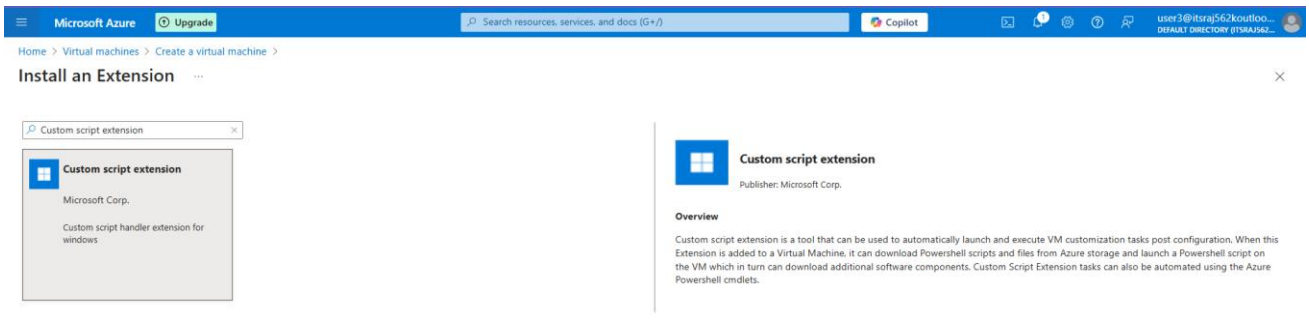


➔ Uploaded script into the storage account.

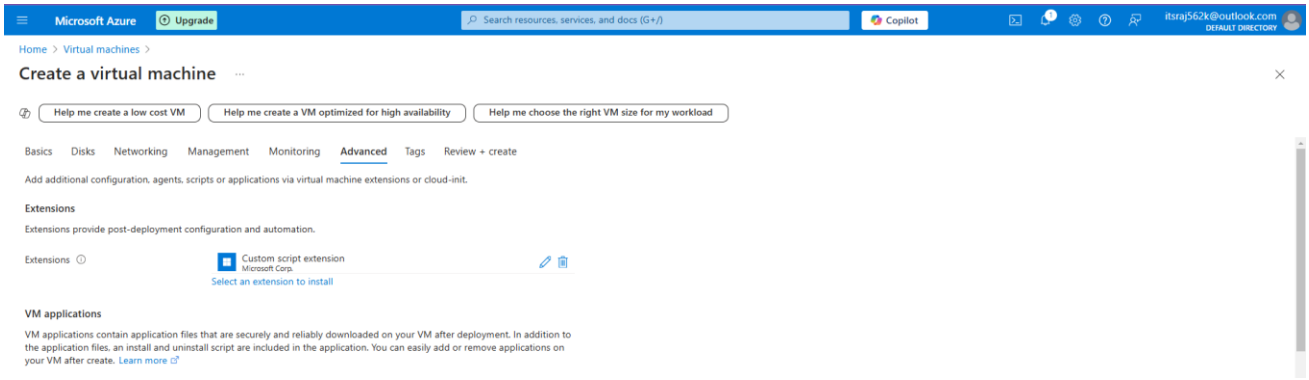


➔ Creating vm1 and adding the extension.

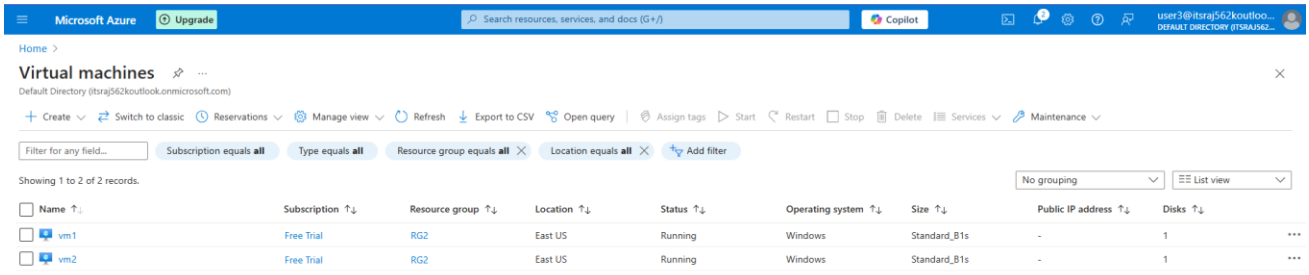




➔ PowerShell Script was added.

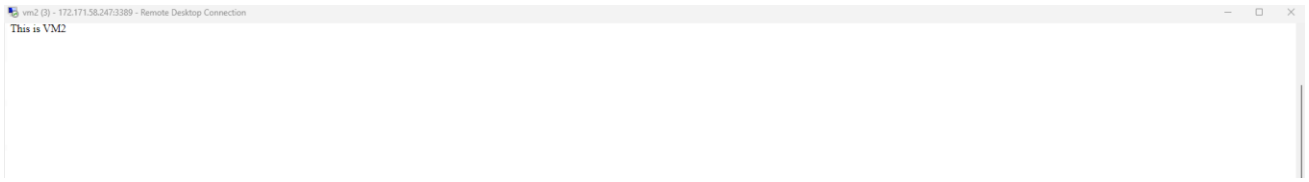


→ Created 2vm's with custom script.



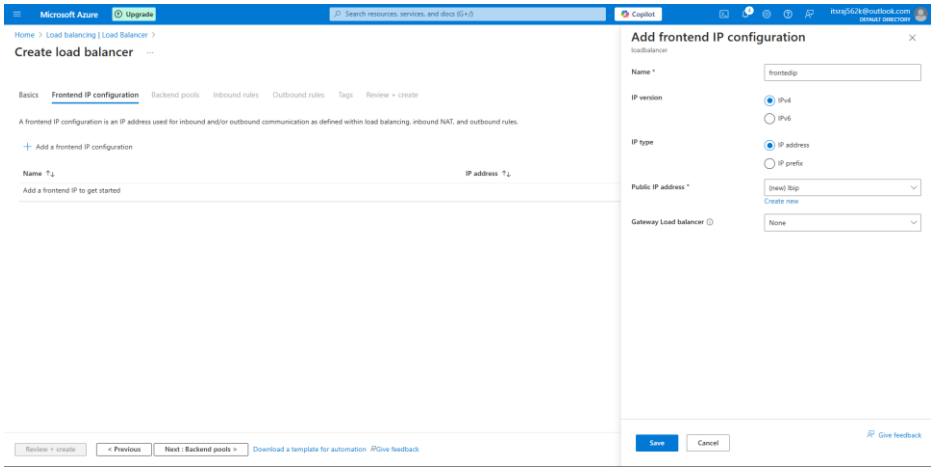
→vm1

→vm2

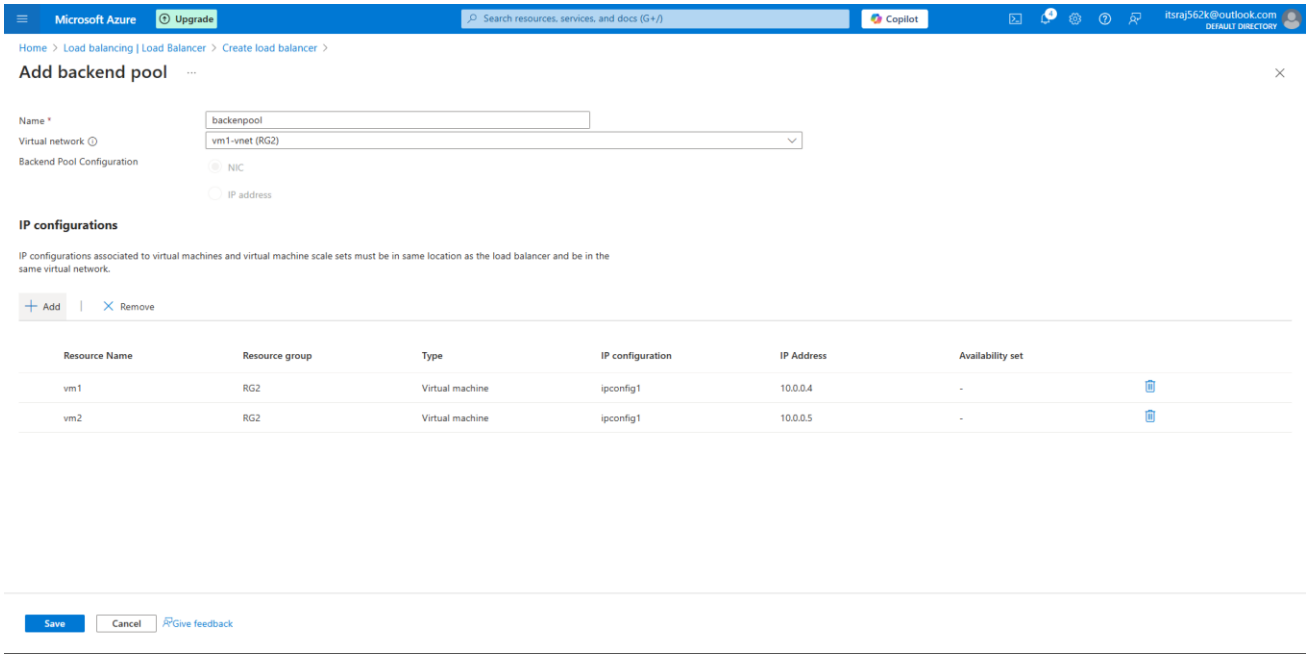


Task 9

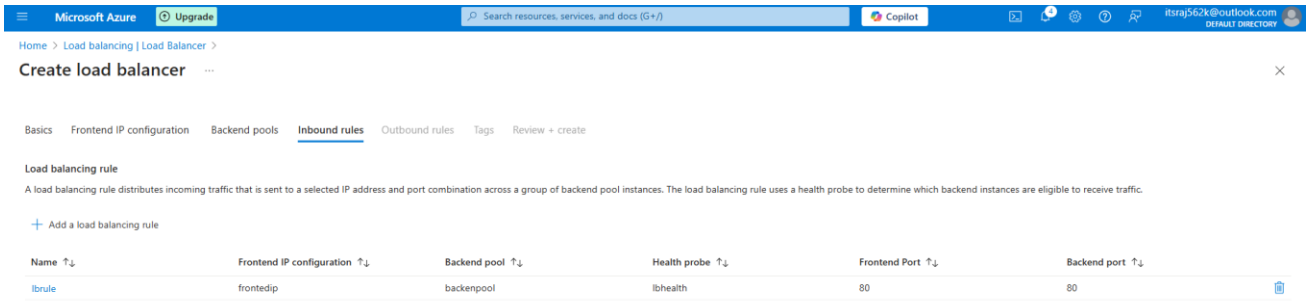
Adding Load Balancer to the vm's.



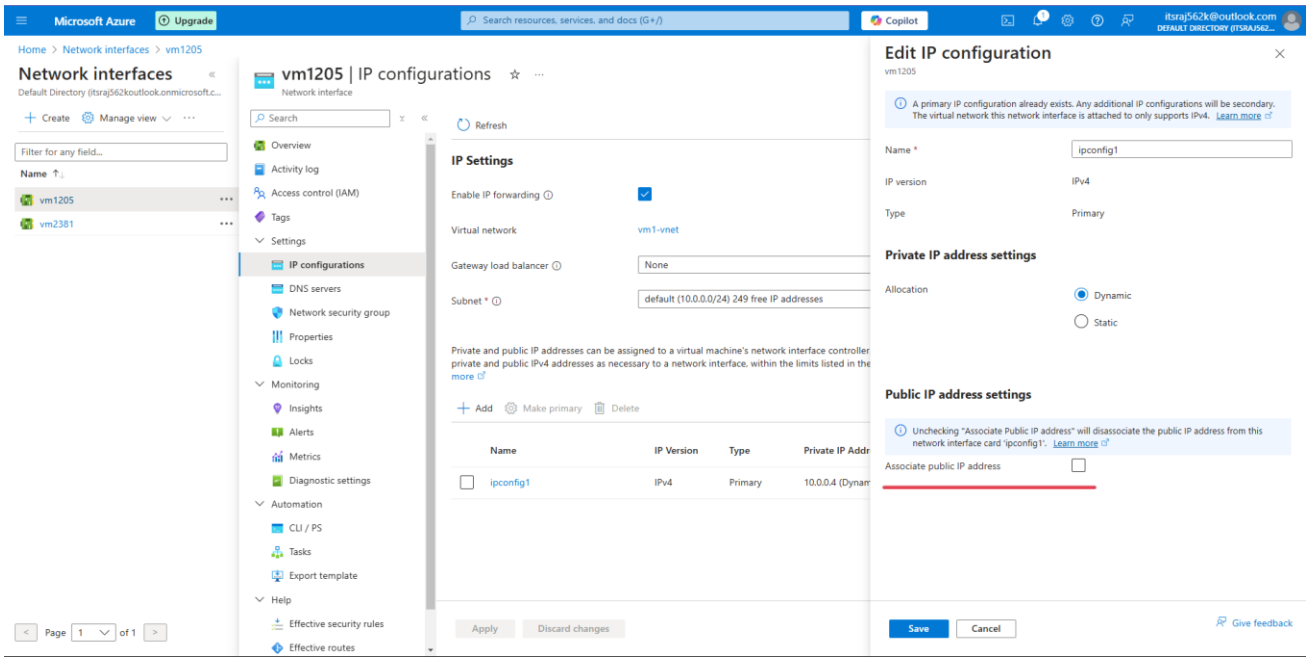
➔ Added Backend Pool.



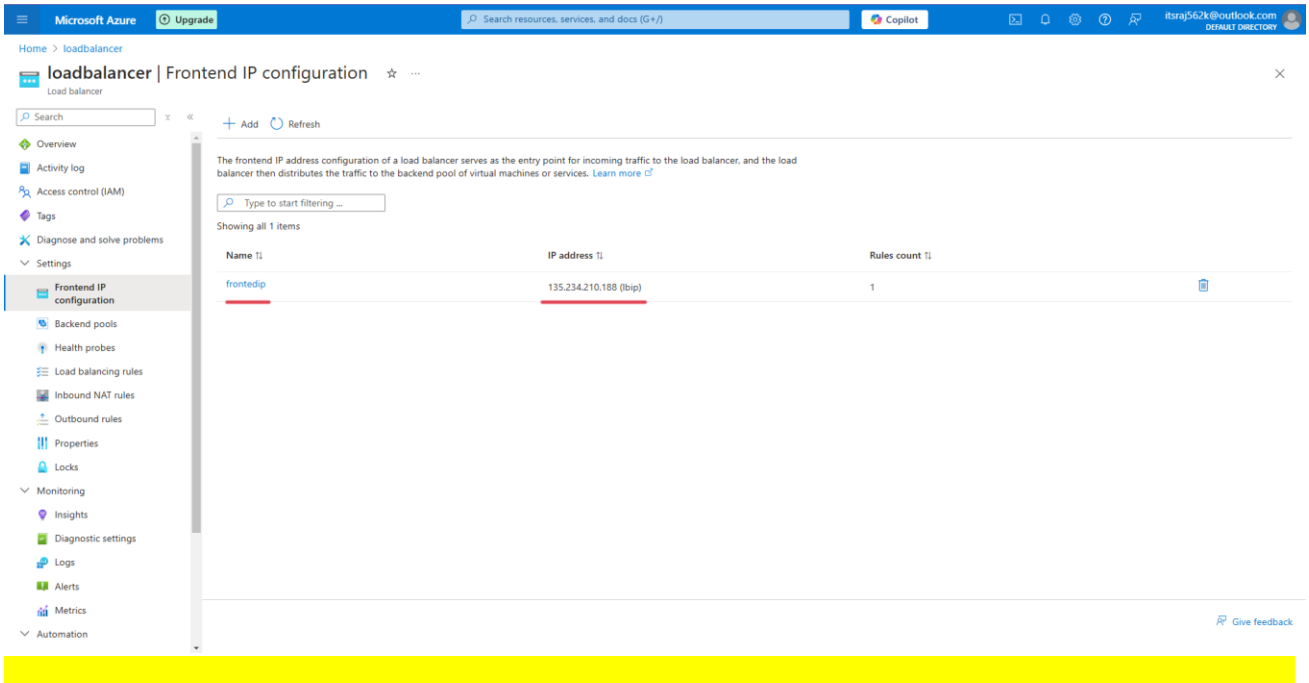
➔Added Inbound Rules.



➔ Removing Public IP from vm1 and vm2.



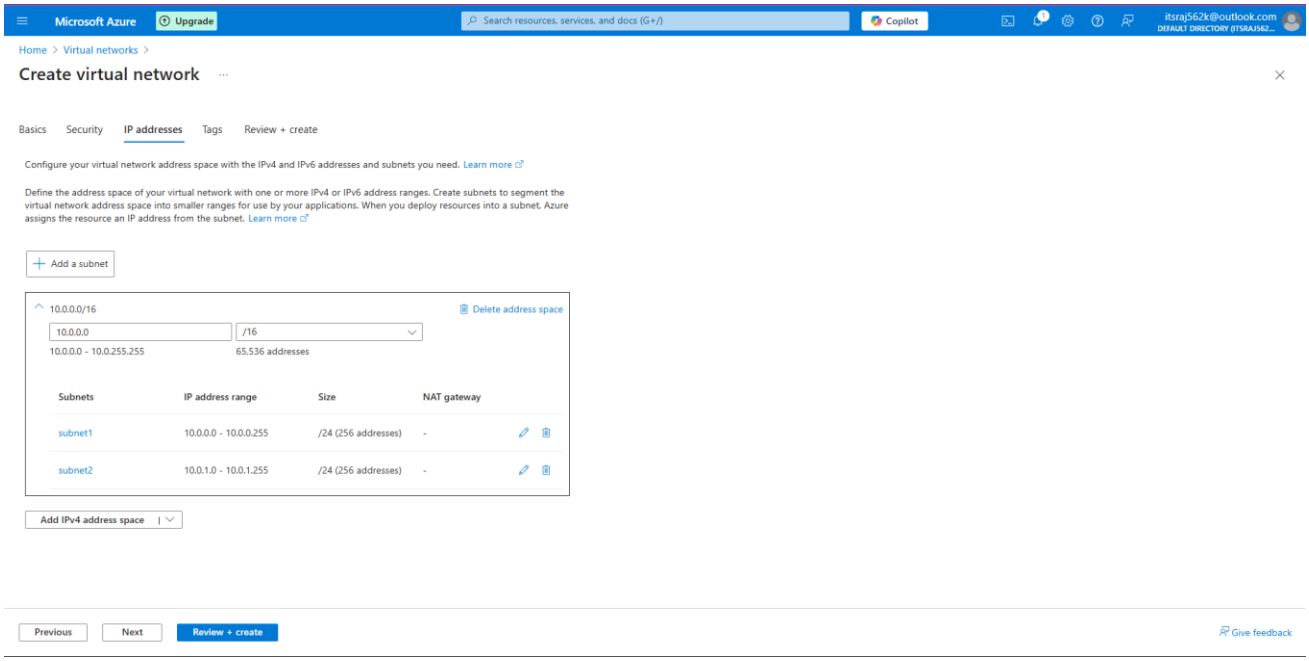
➔Finally Load Balancer was created.

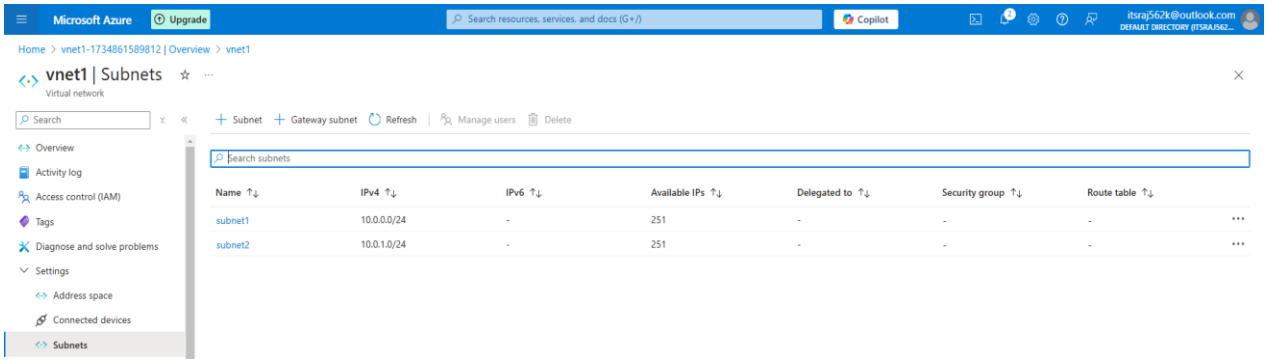


Task 10

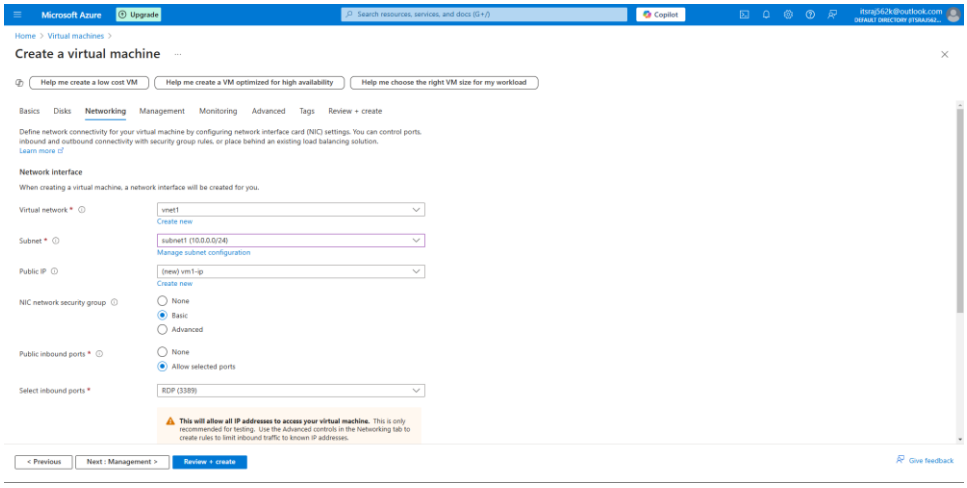
Subtask: 1 → Creating 2 subnet inside a Virtual Network (vnet) and establish RDP connection.

→ Creating 2 subnets.

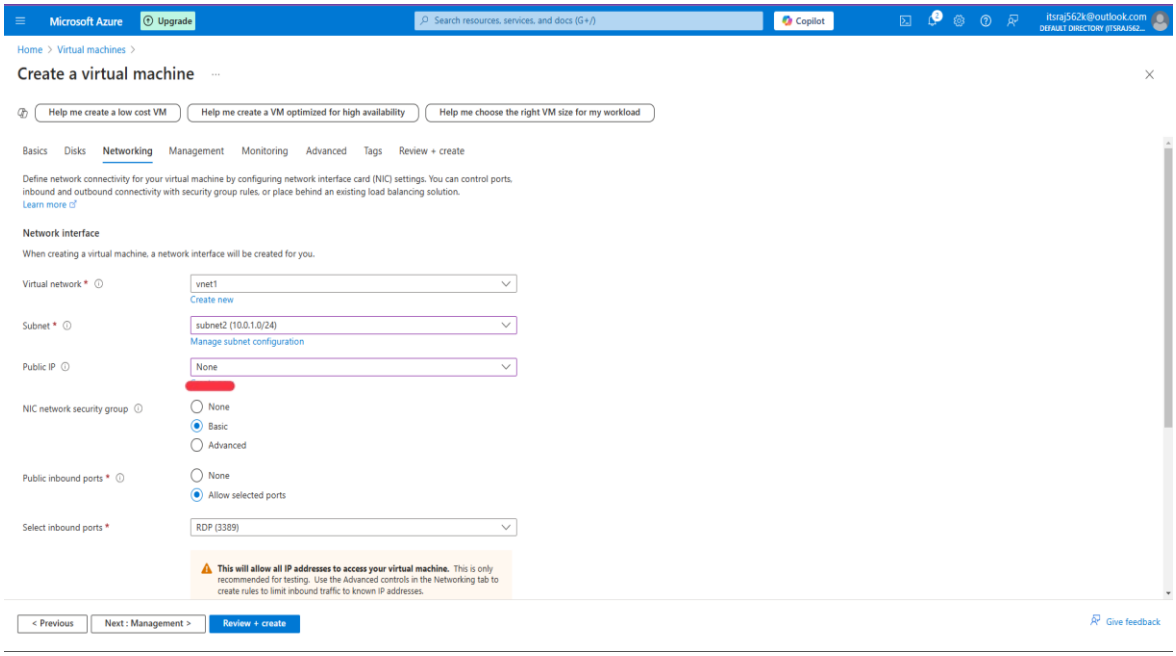




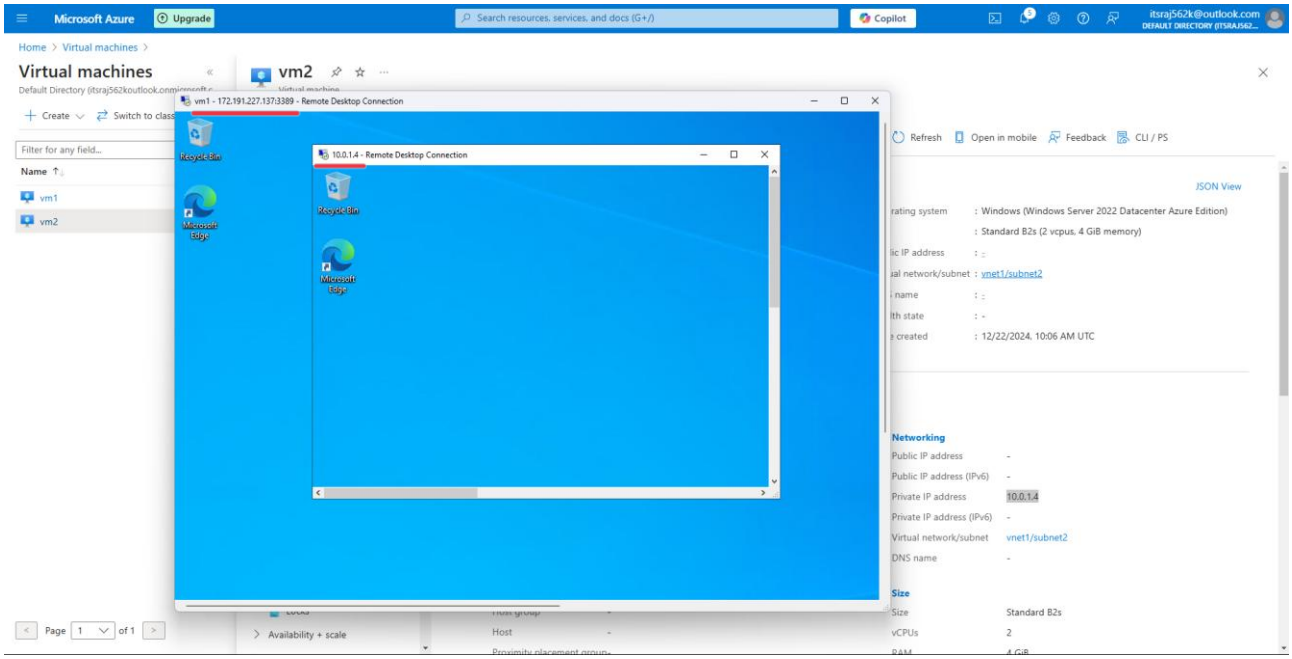
→ Vm1 in subnet1 with public IP.



➔ Vm2 in subnet2 without public IP.

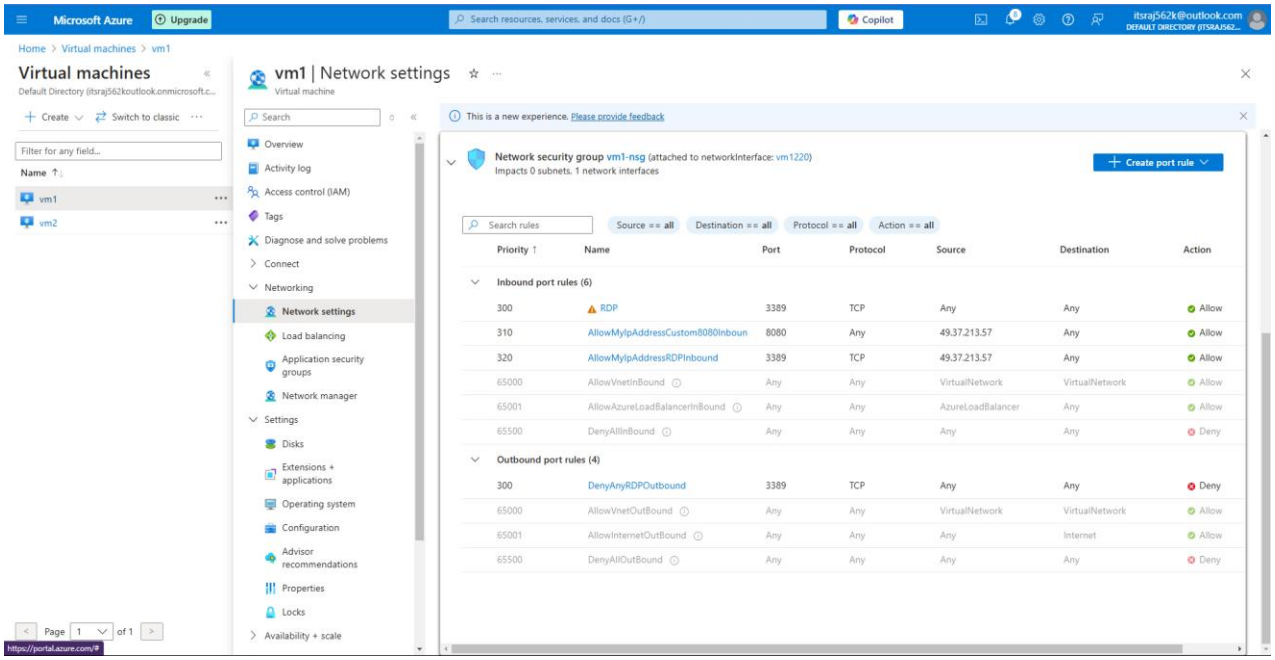


➔ RDP connection was established b/w two 2 vm's in the separate subnet.

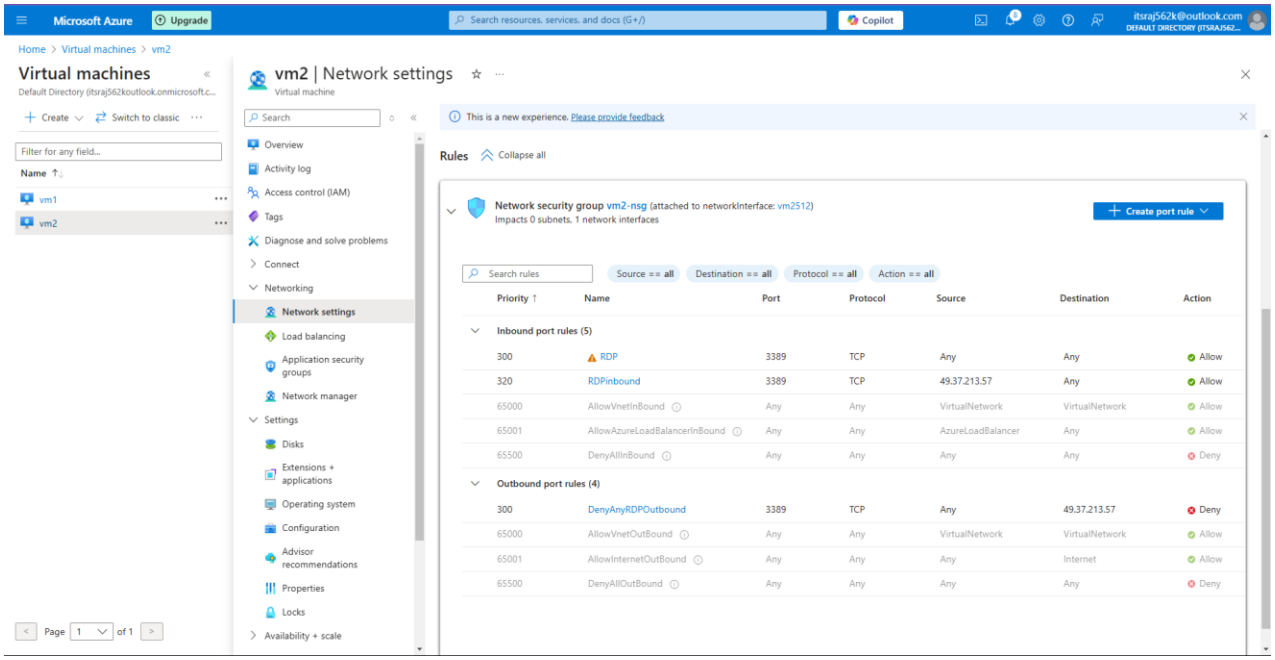


Subtask: 2 → Block RDP connection between Subnets, Allow Inside Each Subnet.

➔ Subnet1 NSG rules.



➔ Subnet2 NSG rules.



➔ If I connect vm2 in the subnet2 using subnet1 vm by RDP, it should not connect.

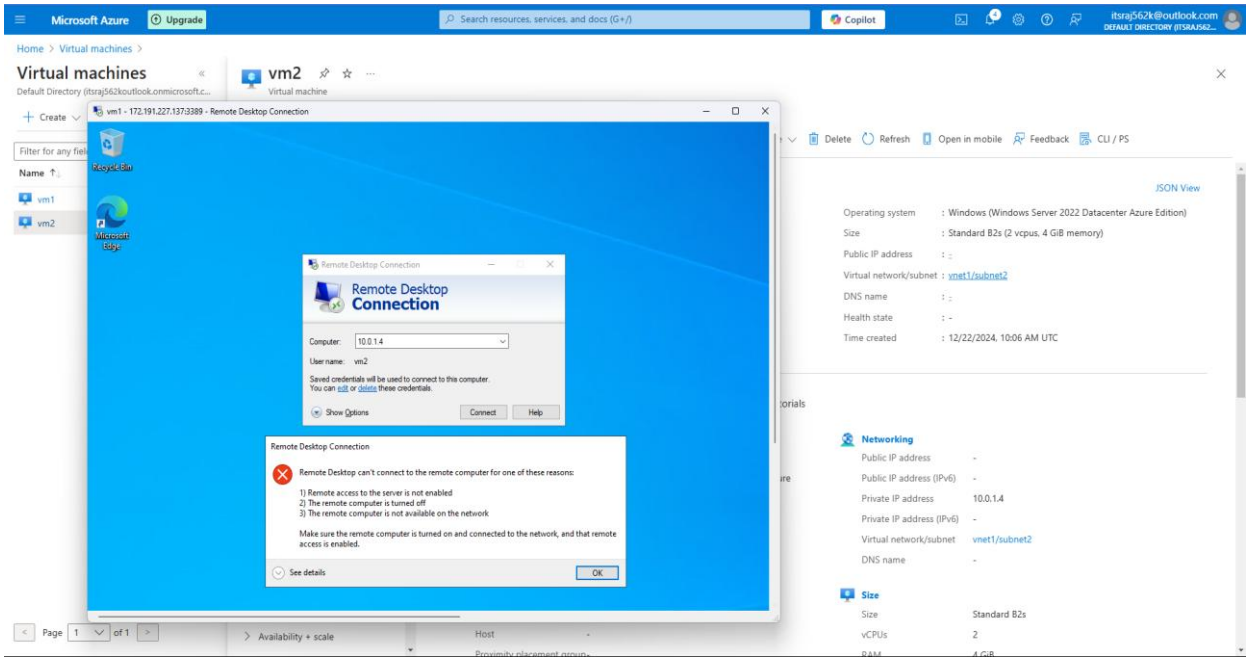


Figure 1 RDP connection was not established

➔ If I removed the NSG rules it should work.

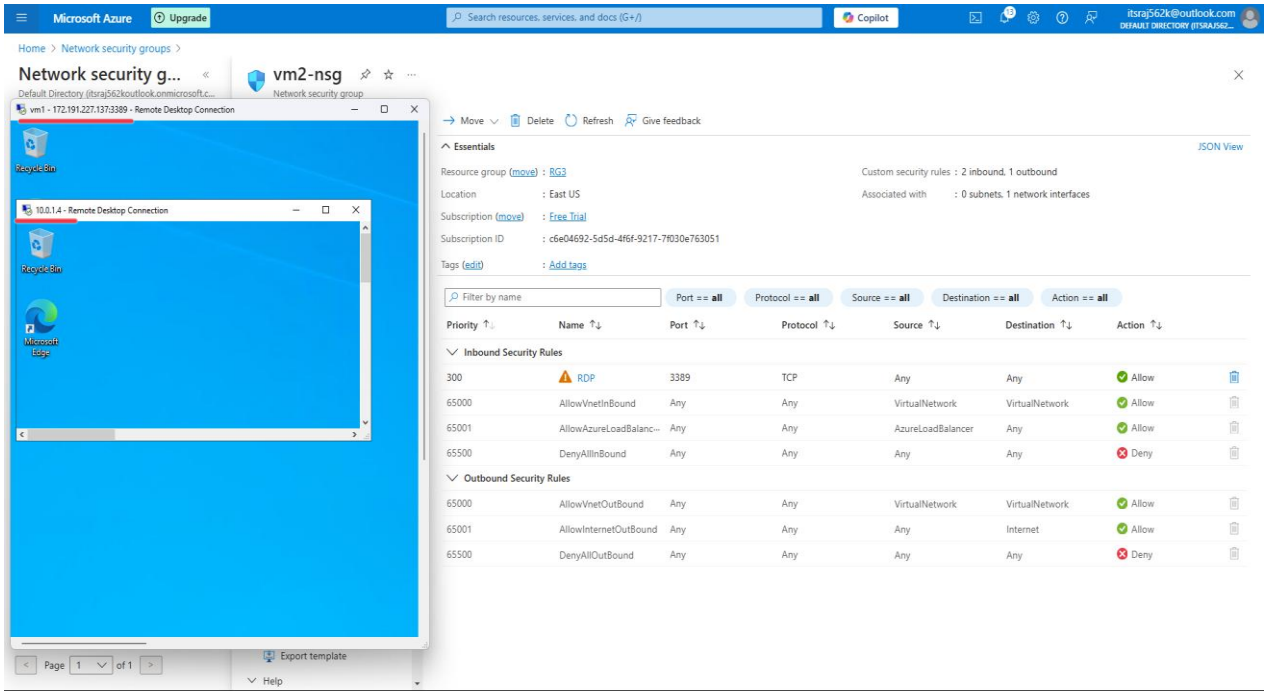
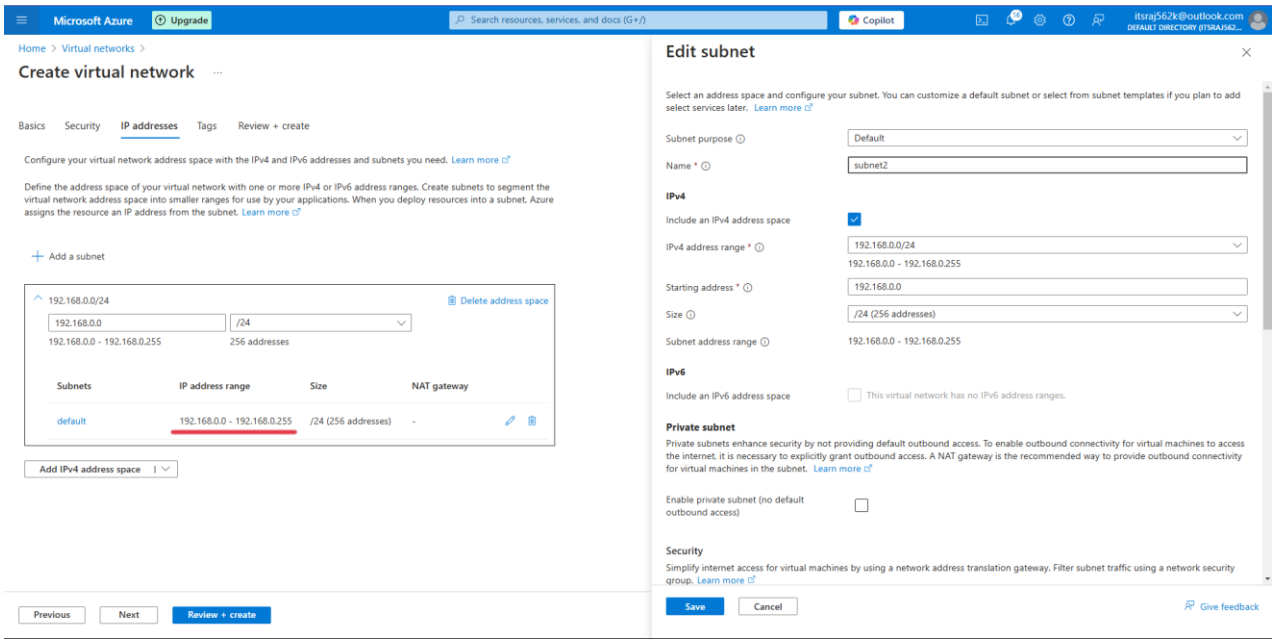


Figure 2 RDP connection was established sucessfully

Subtask: 3 → Peering connection.

➔ Creating another vnet with different IP range.

NOTE: If 2 vnet has same IP range peering will not establish.



➔ Creating vm2 in the above subnet without public IP.

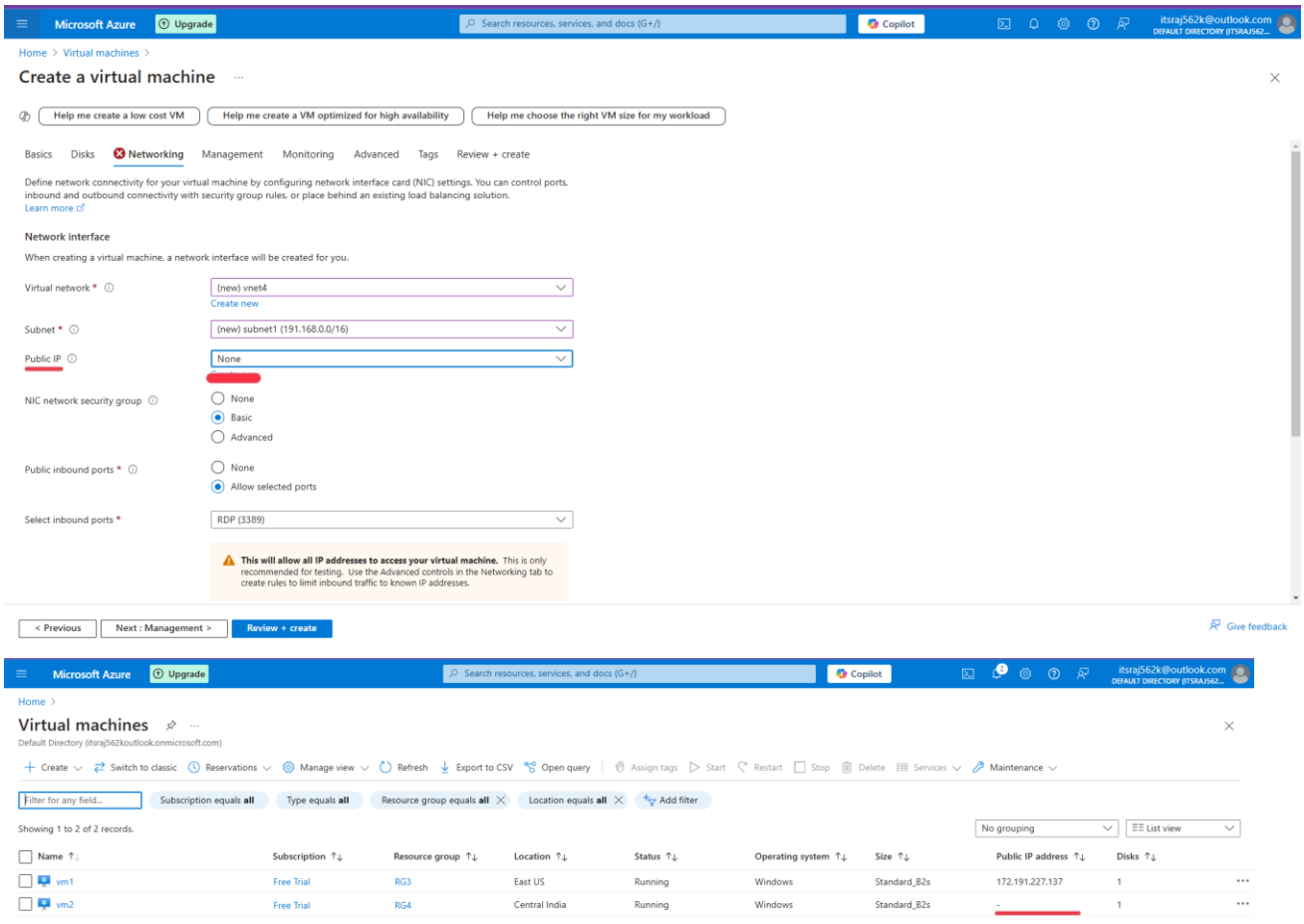
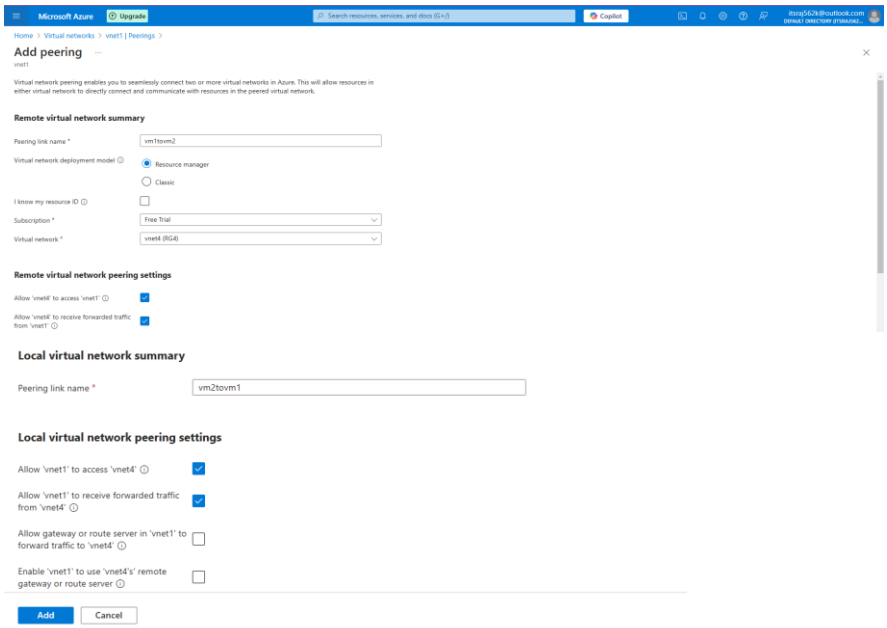
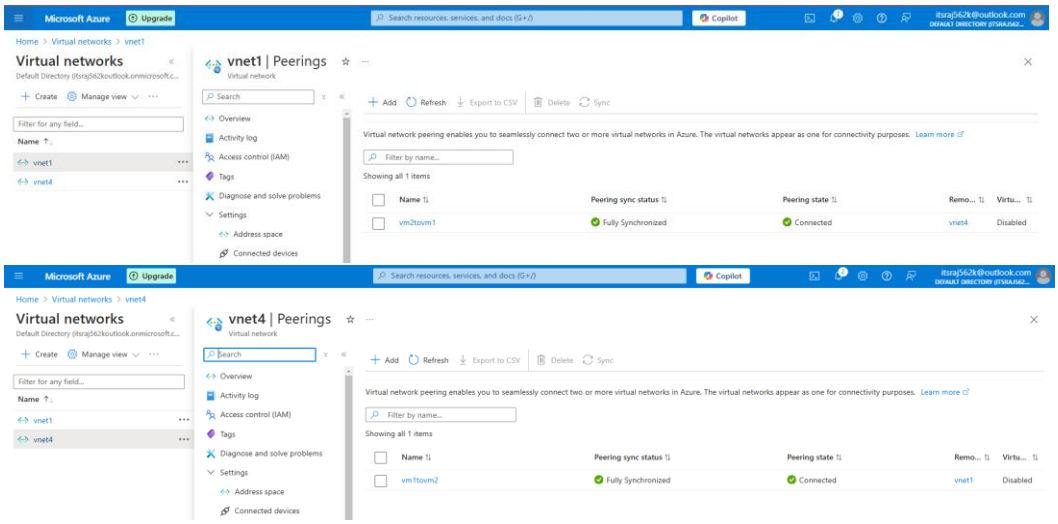


Figure 3 Vm2 in diff region without public IP

➔ Creating peering connection between 2 different vnet's.





➔ In Vm1, RDP connection was established to vm2 in another region vnet without public IP.