COURSE: CLOUD AND NEWTORK SECURITY
NAME: DENISE SOPHY ONDISO MUTAYI
STUDENT NO: CS-CN09-25047

NETWORK SECURITY GROUPS AND APPLICATION SECURITY GROUPS

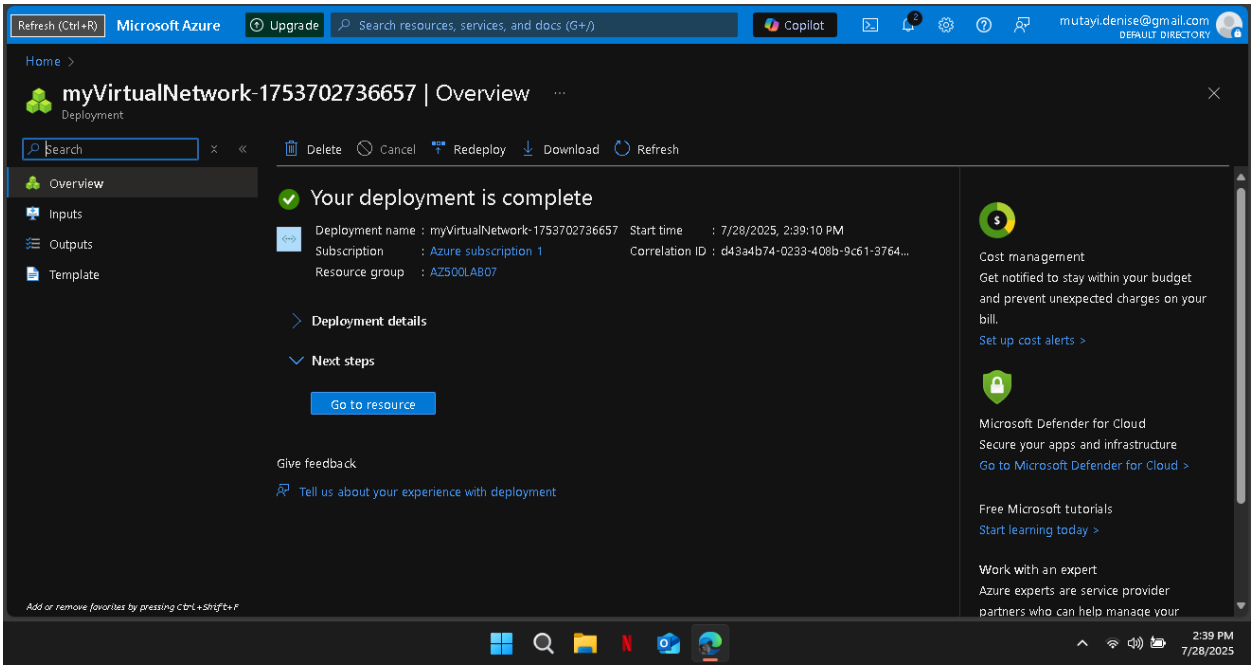
Table of contents

Introduction

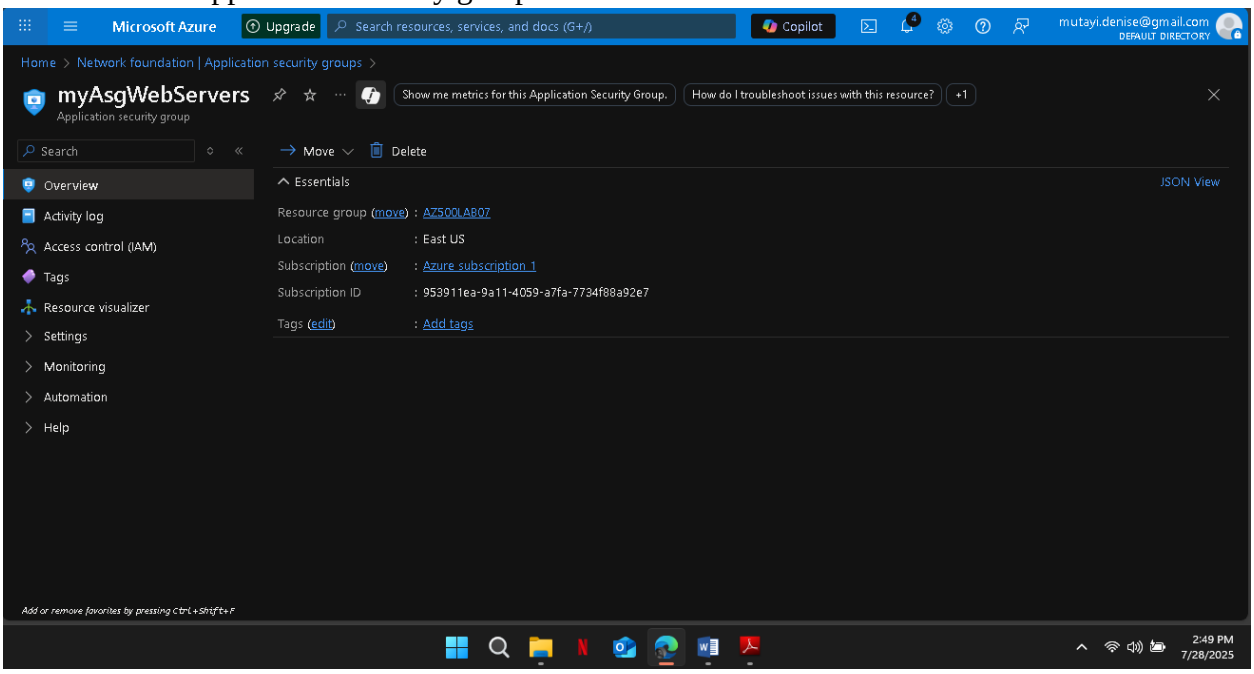
This lab focused on implementing Azure Network Security Groups (NSGs) and Application Security Groups (ASGs) to control and test inbound and outbound traffic to virtual machines deployed within a virtual network. I deployed two VMs (myVMWeb and myVMMgmt) across different subnets and assigned each to a specific ASG—WebASG and MgmtASG. The goal was to ensure that only HTTP (port 80) traffic could reach the web server from the internet, and RDP (port 3389) access was limited to the management server. I configured NSG rules targeting these ASGs to simulate real-world security segmentation. The test included accessing the web server via its public IP and validating successful or blocked traffic based on the rule sets applied. The lab provided practical experience with scoped security controls in a cloud environment, aligning with best practices for least privilege access and network isolation.

Exercise 1: Create the virtual networking infrastructure

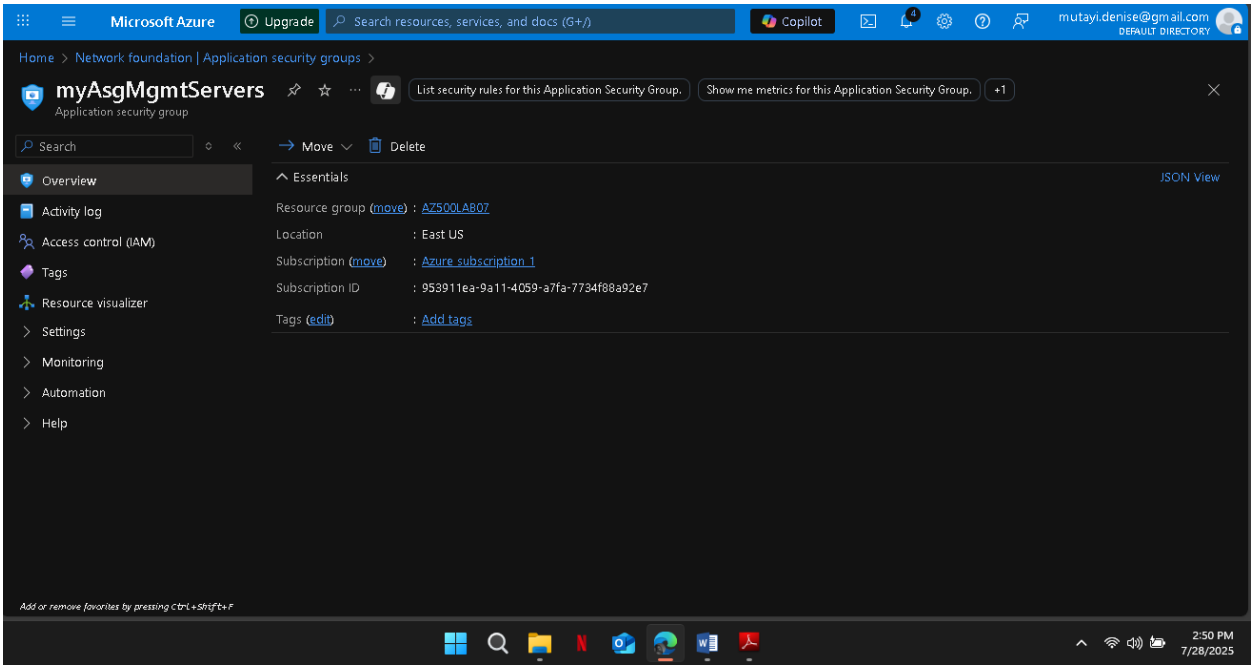
Task 1: Create a virtual network with one subnet.



Task 2: Create application security groups

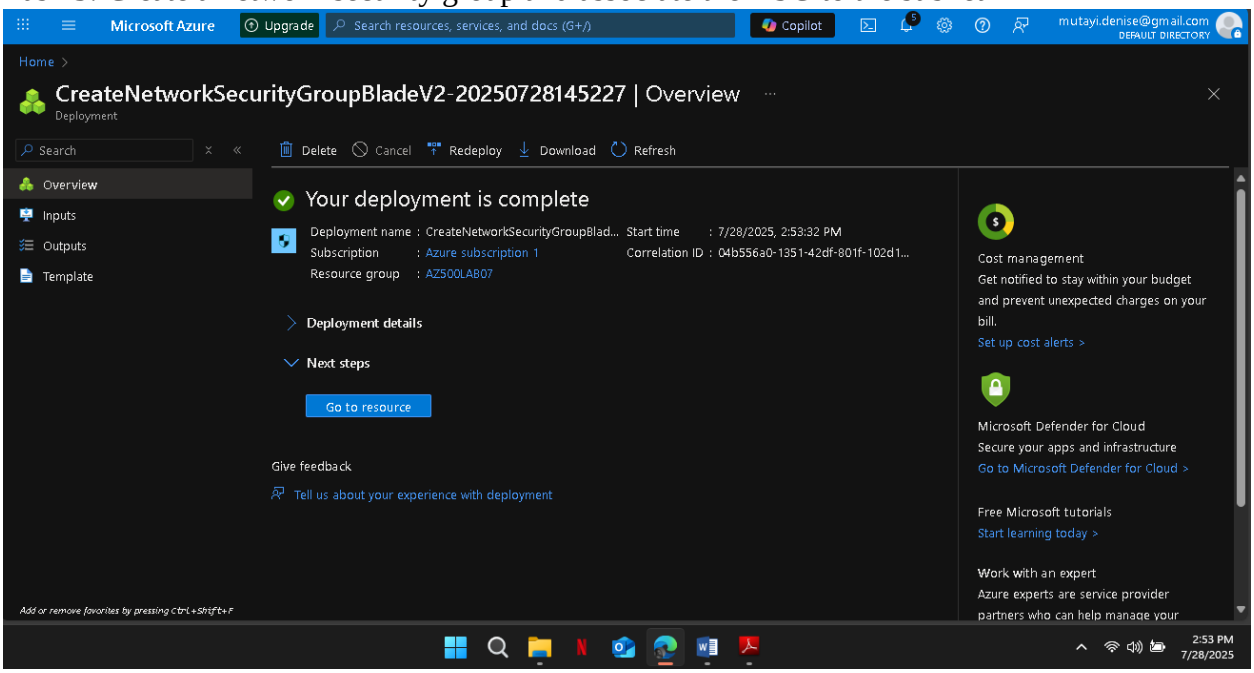


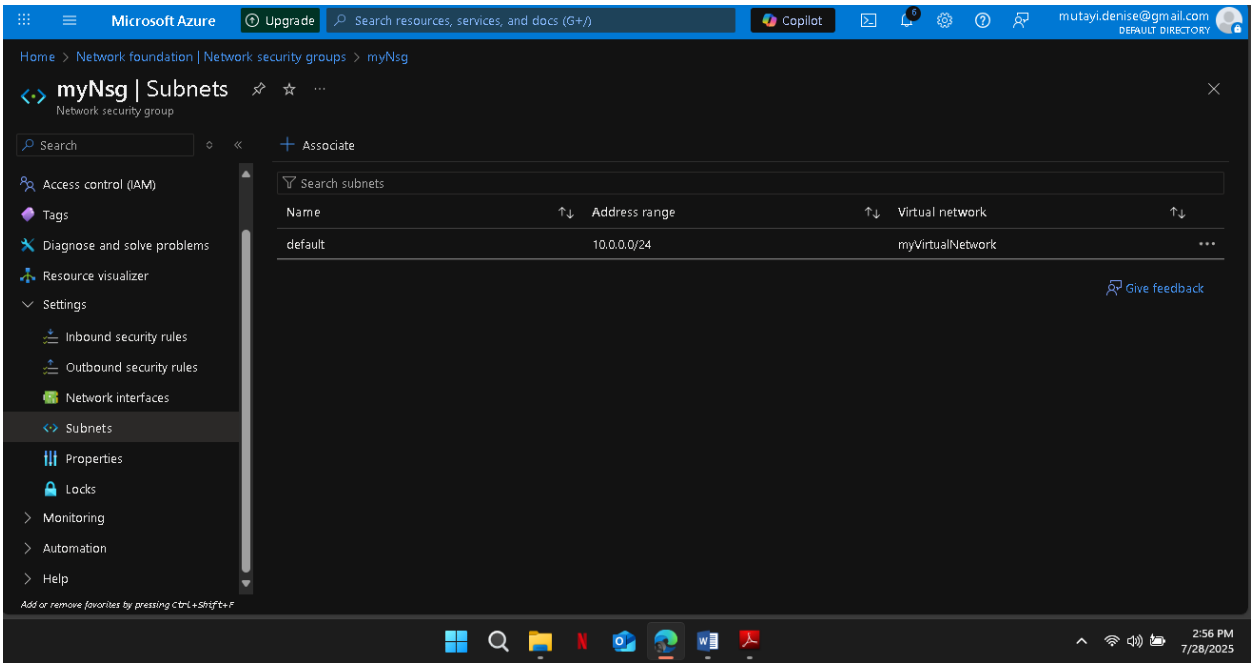
This group will be for the web servers



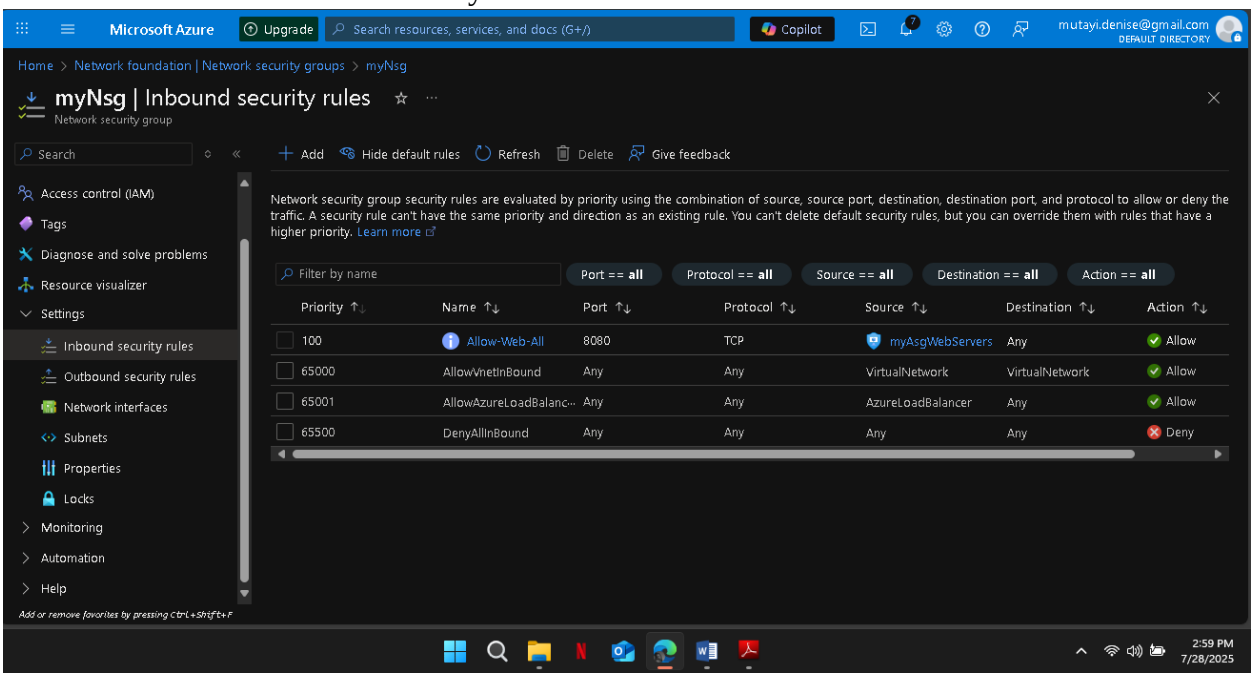
This group will be for the management servers

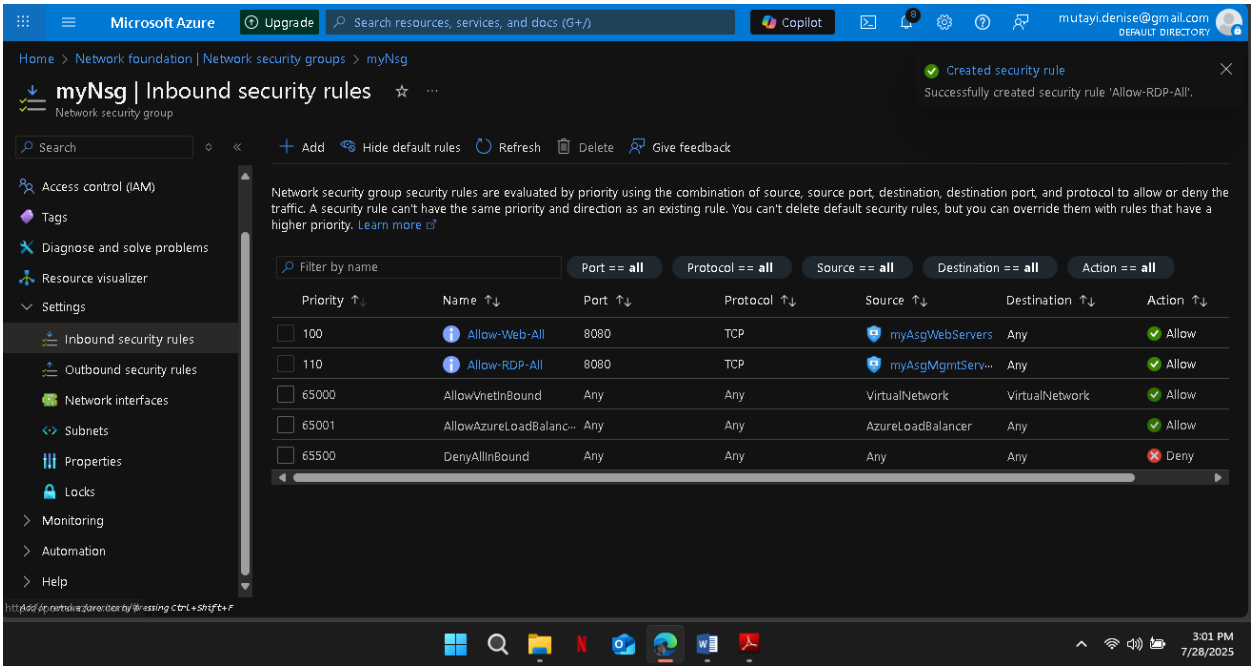
Task 3: Create a network security group and associate the NSG to the subnet





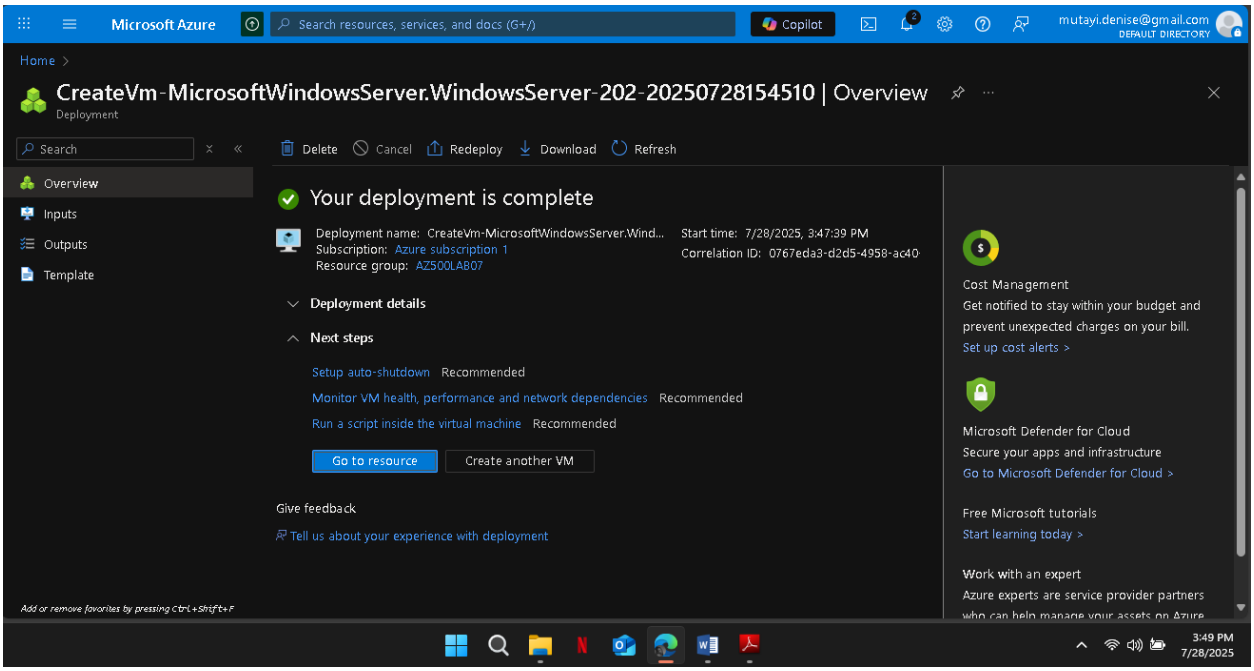
Task 4: Create inbound NSG security rules to all traffic to web servers and RDP to the servers.



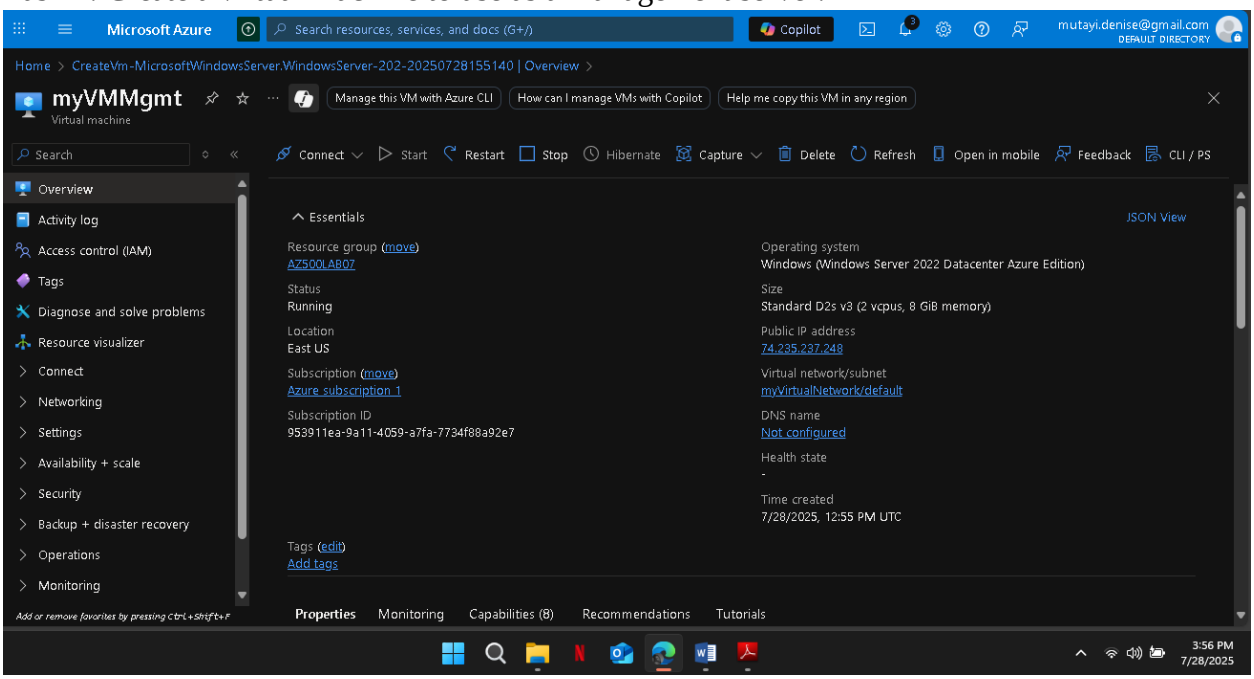


Exercise 2: Deploy virtual machines and test network filters

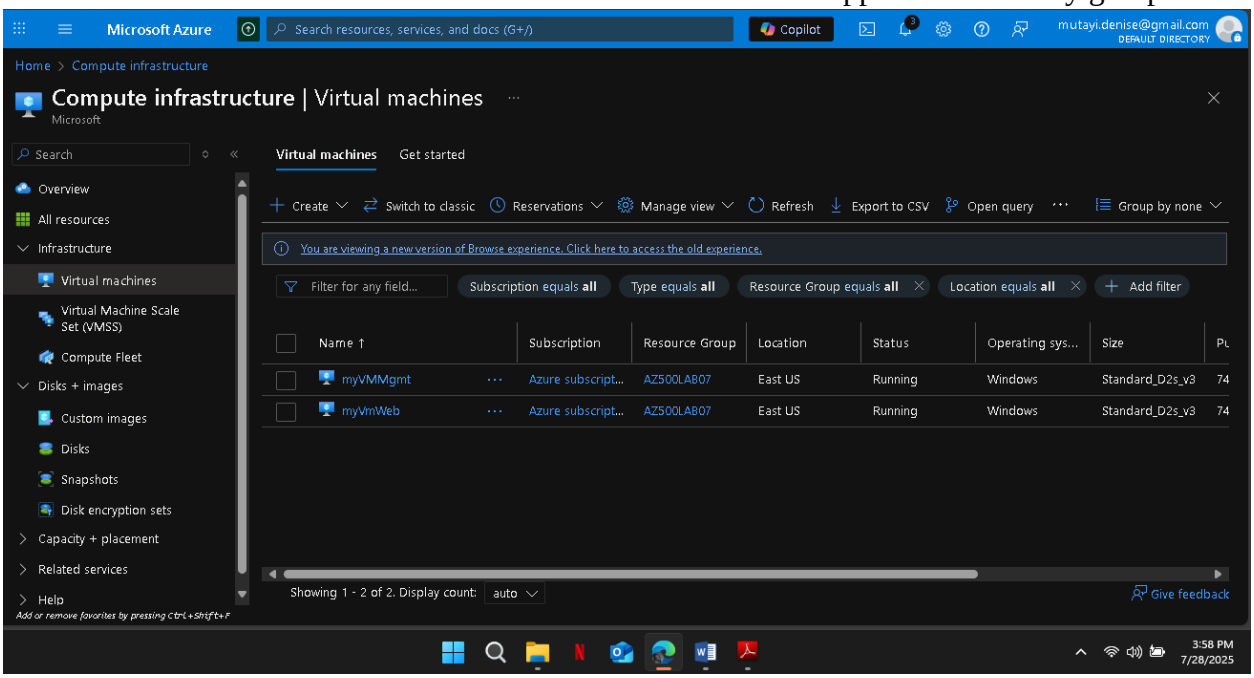
Task 1: Create a virtual machine to use as a web server.



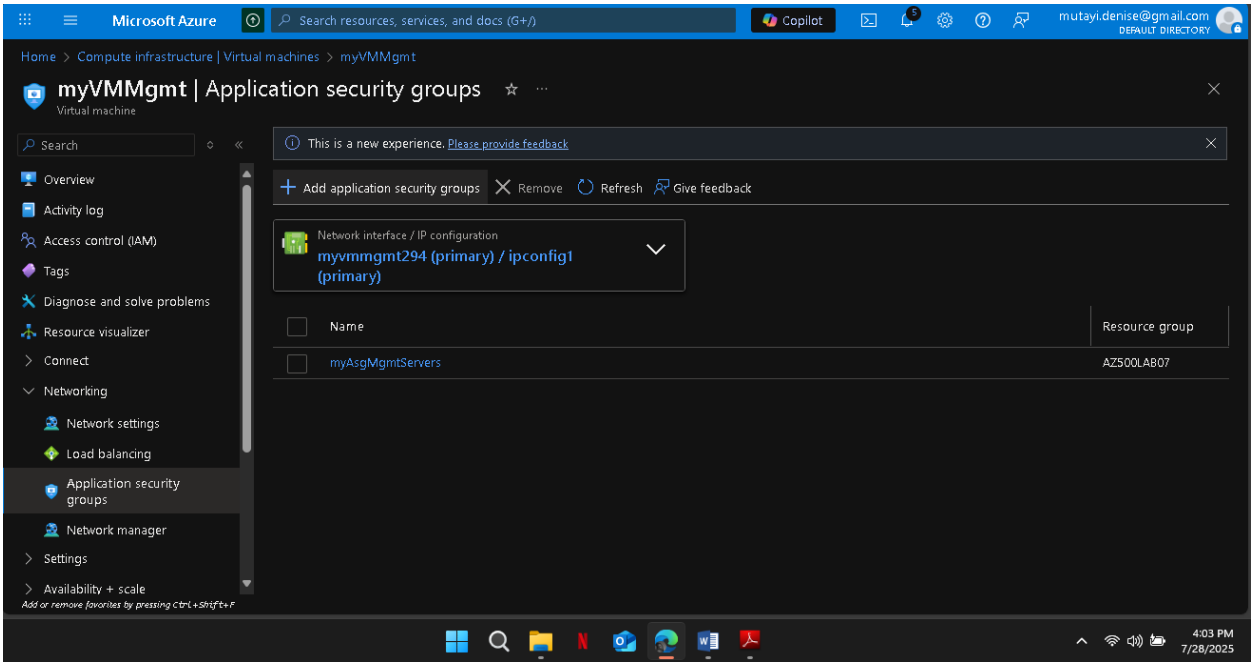
Task 2: Create a virtual machine to use as a management server.

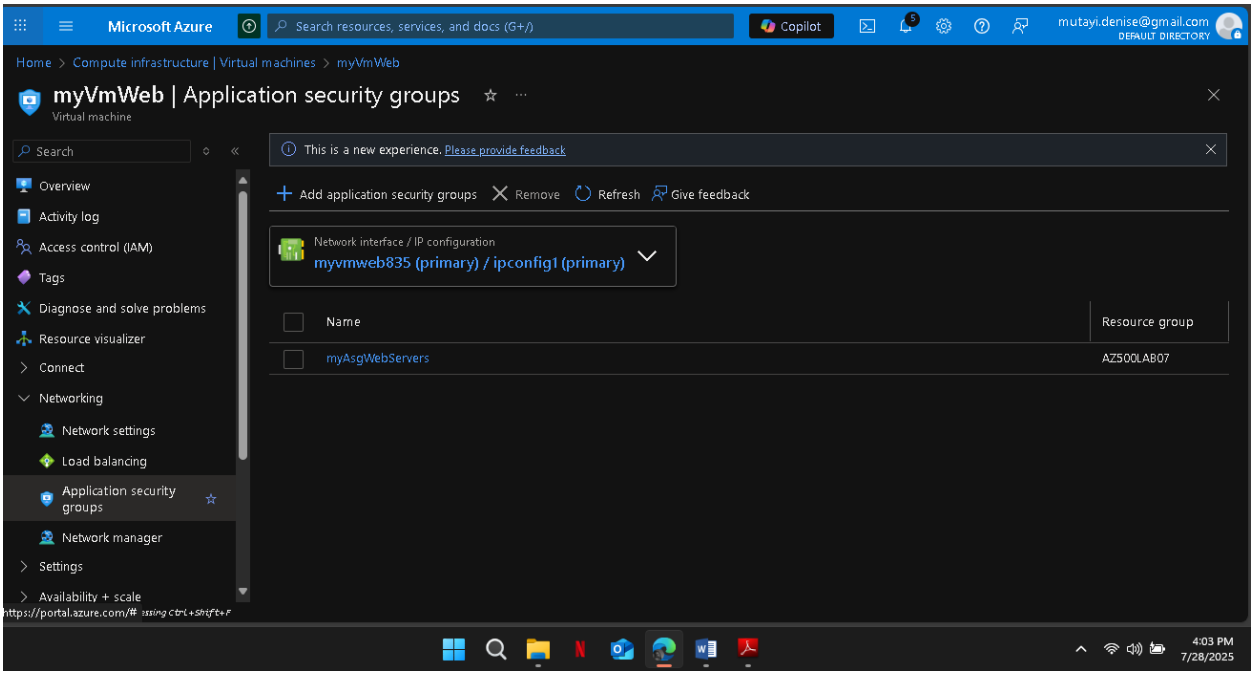


Task 3: Associate each virtual machines network interface to its application security group.

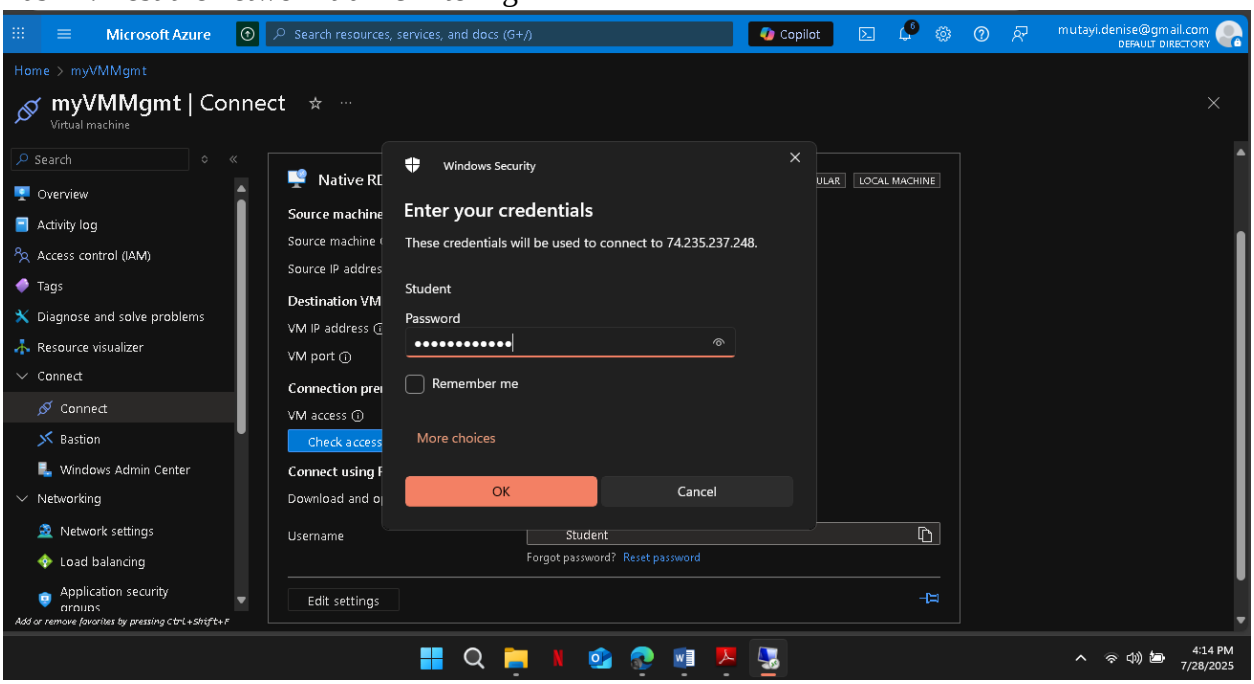


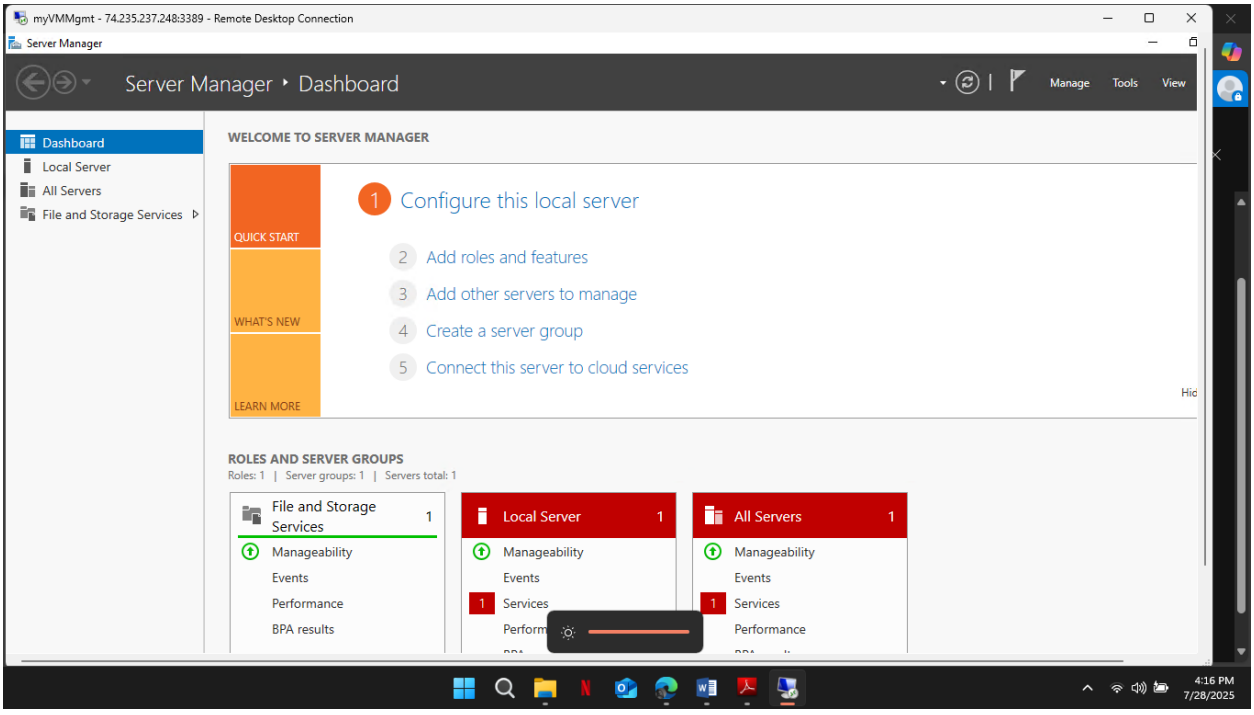
Both are running

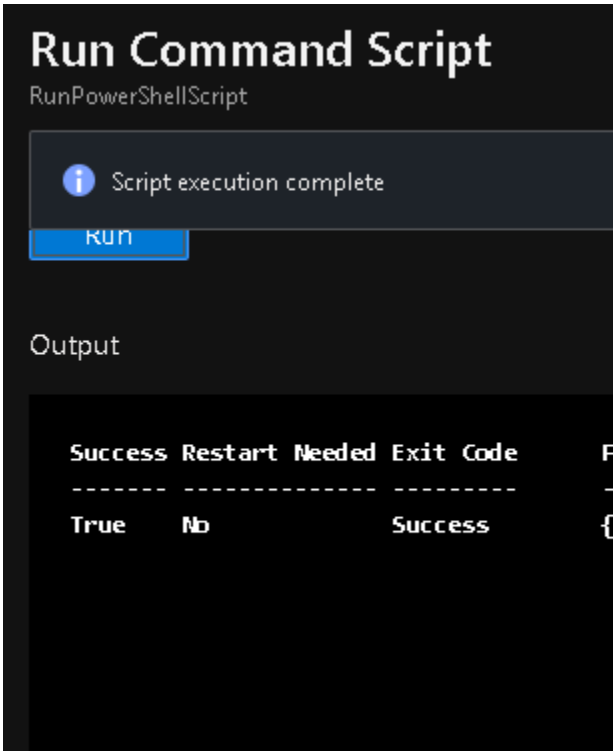

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
mutayi.denise@gmail.com
DEFAULT DIRECTORY
Home > Compute infrastructure | Virtual machines > myVMMgmt
myVMMgmt | Application security groups
Virtual machine
Search
This is a new experience. Please provide feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
Availability + scale
Add or remove favorites by pressing Ctrl+Shift+F
Add application security groups
Remove
Refresh
Give feedback
Network interface / IP configuration
myvmmgmt294 (primary) / ipconfig1 (primary)
Name
Resource group
myAsgMgmtServers
AZ500LAB07
4:03 PM
7/28/2025


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
mutayi.denise@gmail.com
DEFAULT DIRECTORY
Home > Compute infrastructure | Virtual machines > myVmWeb
myVmWeb | Application security groups
Virtual machine
Search
This is a new experience. Please provide feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
Availability + scale
https://portal.azure.com/# ssing Ctrl+Shift+F
Add application security groups
Remove
Refresh
Give feedback
Network interface / IP configuration
myvmweb835 (primary) / ipconfig1 (primary)
Name
Resource group
myAsgWebServers
AZ500LAB07
4:03 PM
7/28/2025

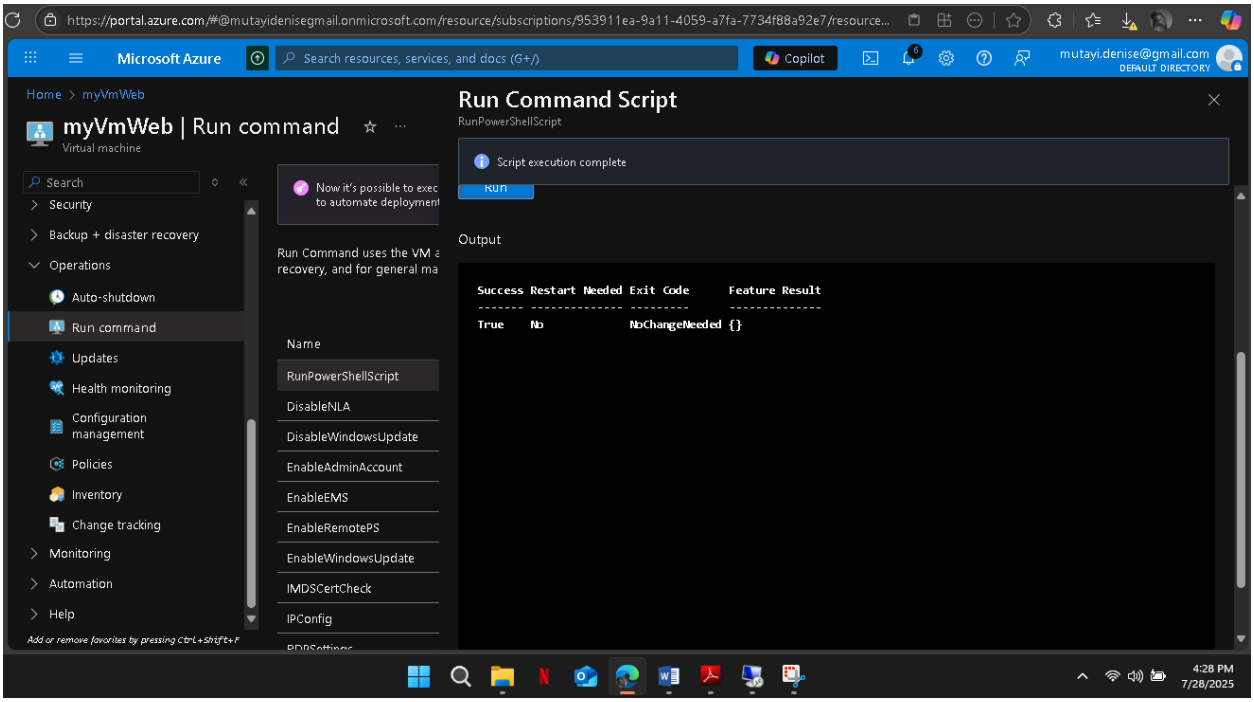
Task 4: Test the network traffic filtering

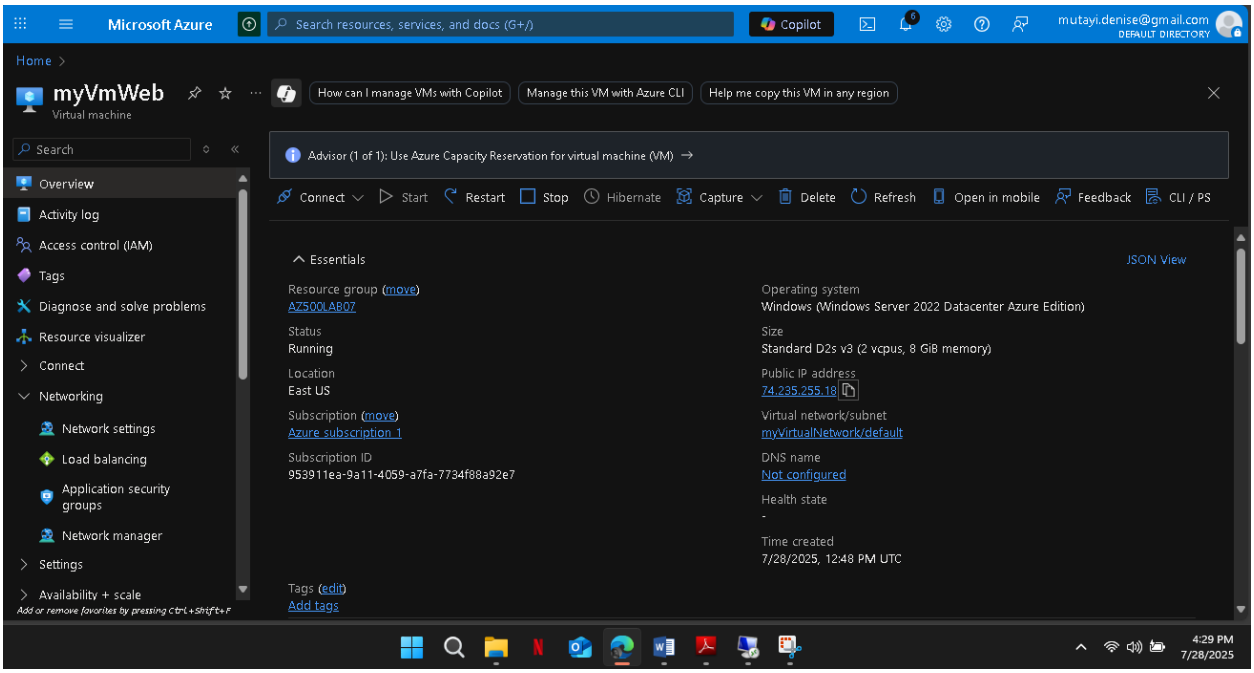






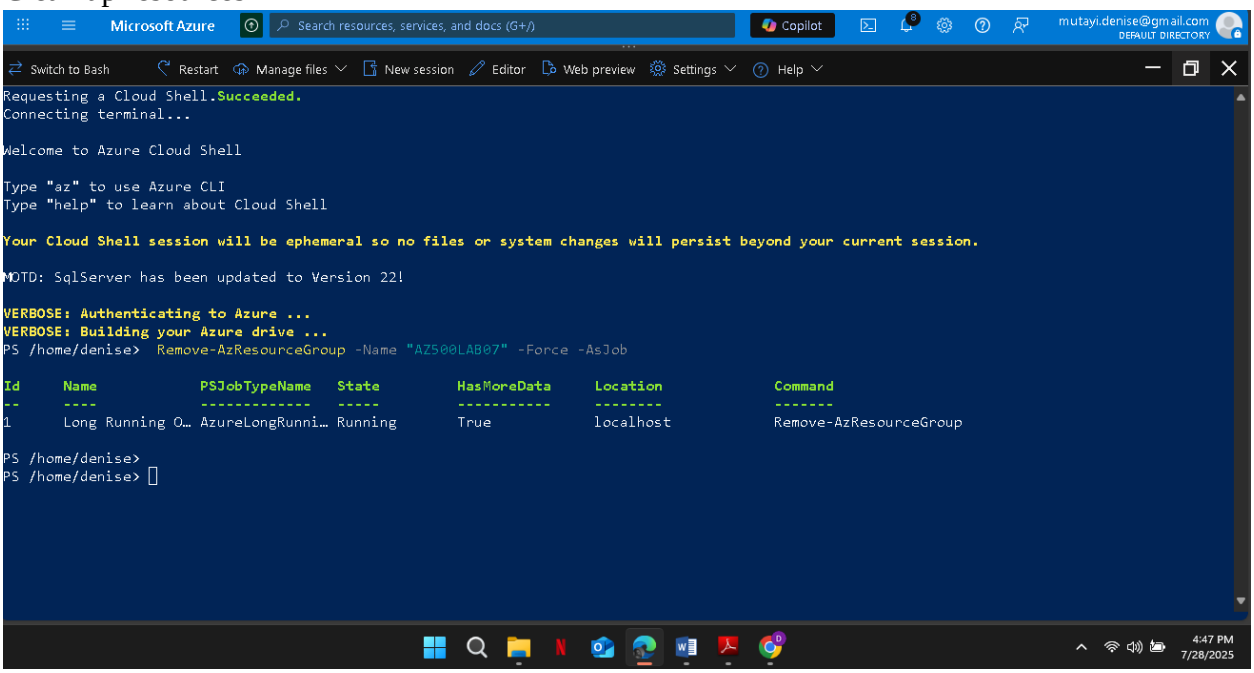
This is a result of re-running the original command. The initial output (now unavailable due to session closure) was identical in status, confirming successful installation.





The public IP address is 74.235.255.18

Clean up resources



Conclusion

At the end of the lab, I successfully verified the security rules applied to the NSG. The HTTP rule allowed access to myVMWeb via its public IP (74.235.255.18), while RDP access was restricted to only the management server. However, when testing the public IP in a browser, the request timed out, likely due to a misconfiguration in the NSG rule, IIS service not running, or VM startup delays. Despite this, the process reinforced the importance of applying NSG rules to ASGs rather than individual IPs, promoting scalable and maintainable cloud network security. Finally, I cleaned up the environment using PowerShell with the Remove-AzResourceGroup command, confirming that automation and good hygiene are integral to responsible Azure resource management. The lab strengthened my skills in applying, testing, and validating security configurations within Azure's virtual networking model.