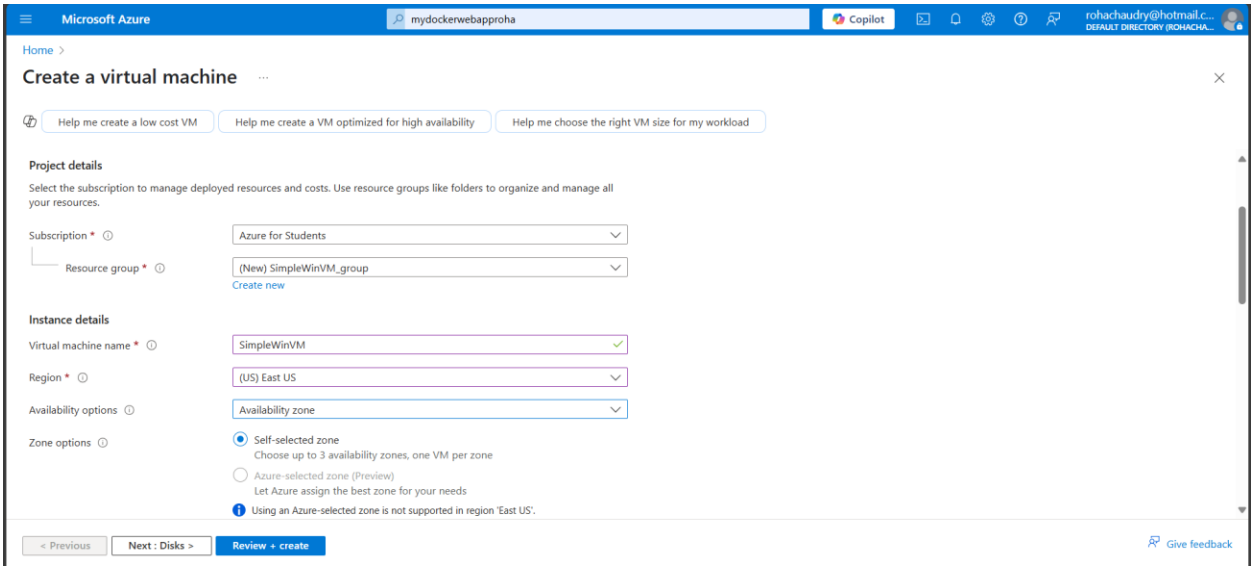
2025

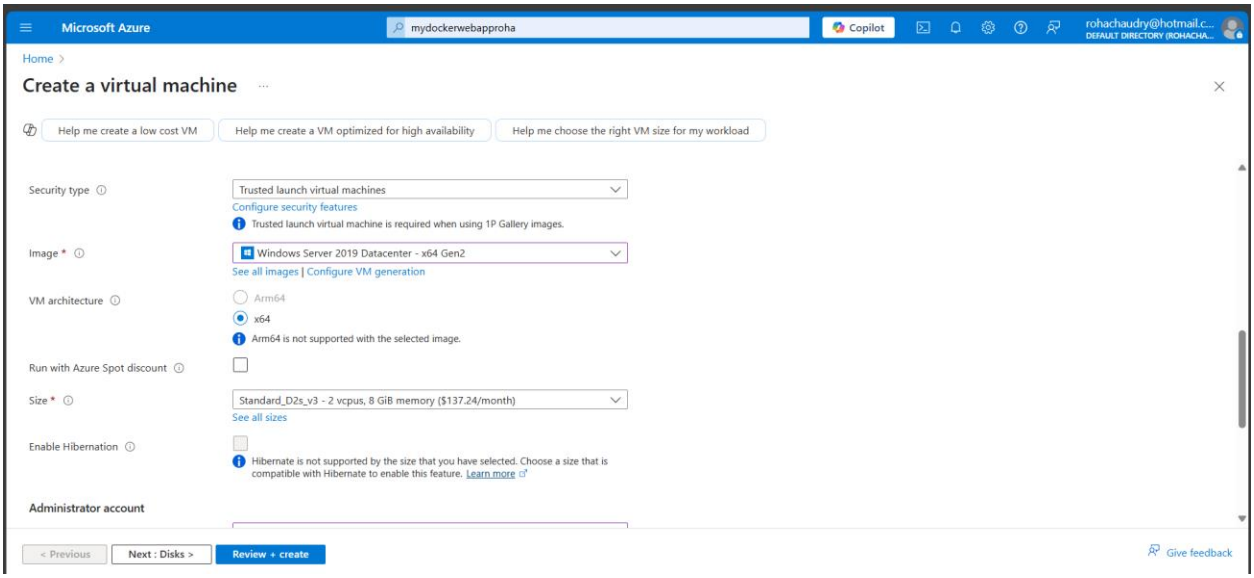
Azure Lab 06

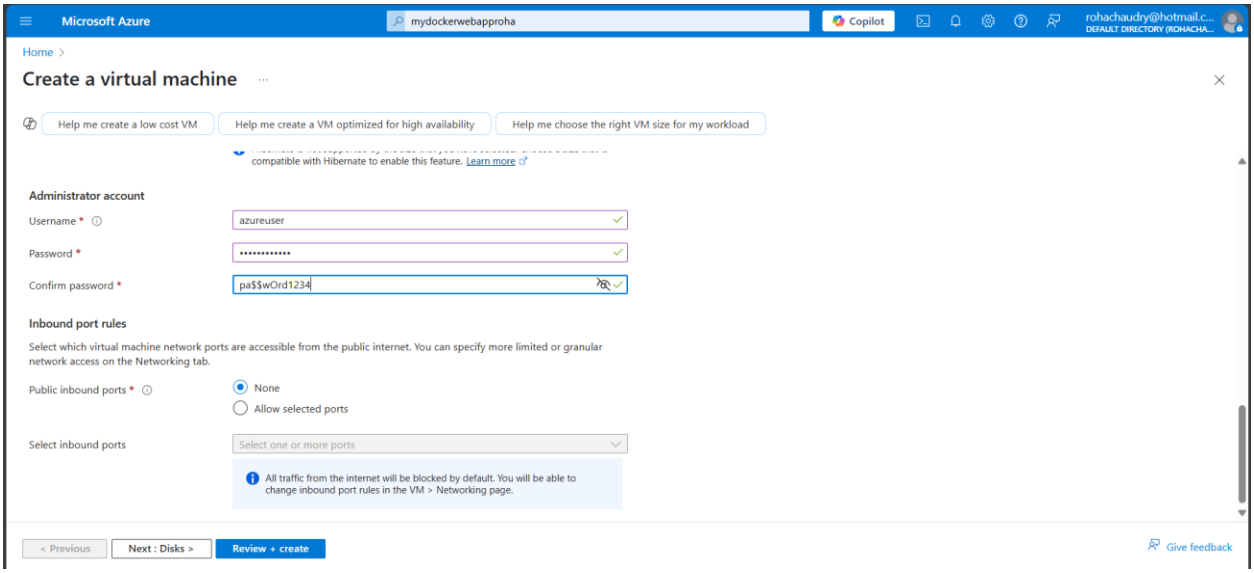
CONFIGURE A NETWORK SECURITY GROUP

ROHA ALI (2112124)

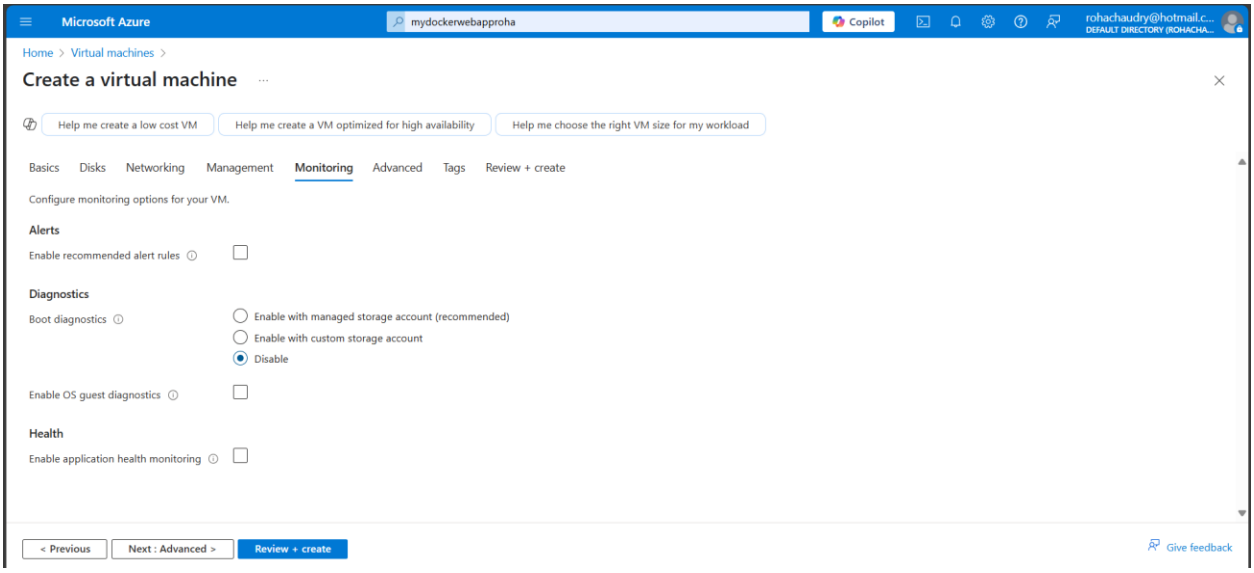
3. On the Basics tab, fill in the following information (leave the defaults for everything else):



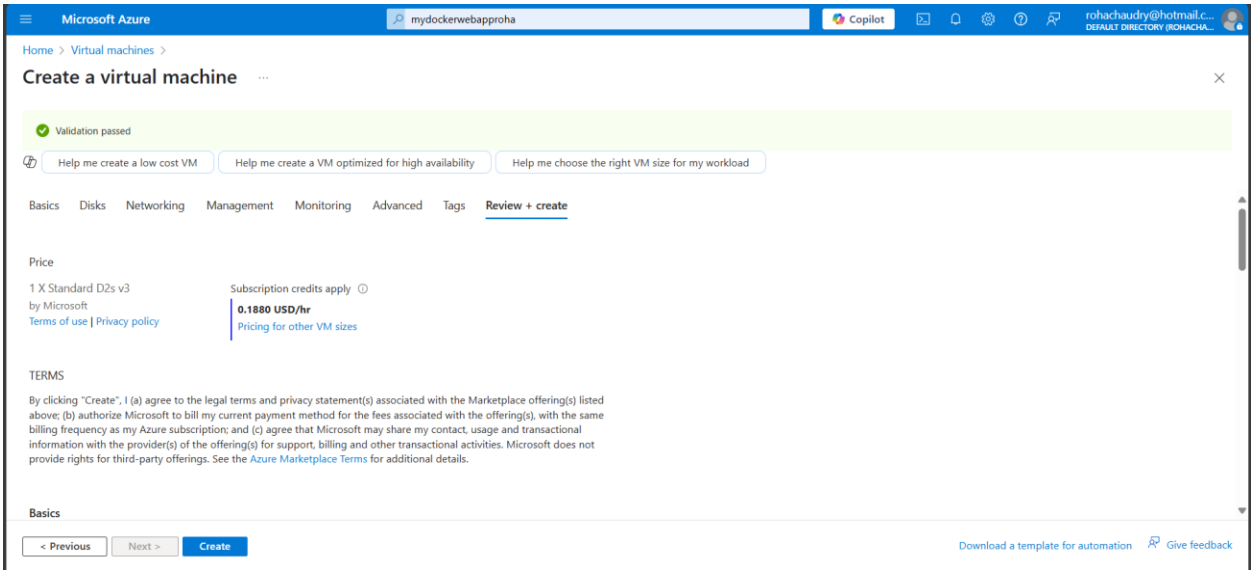




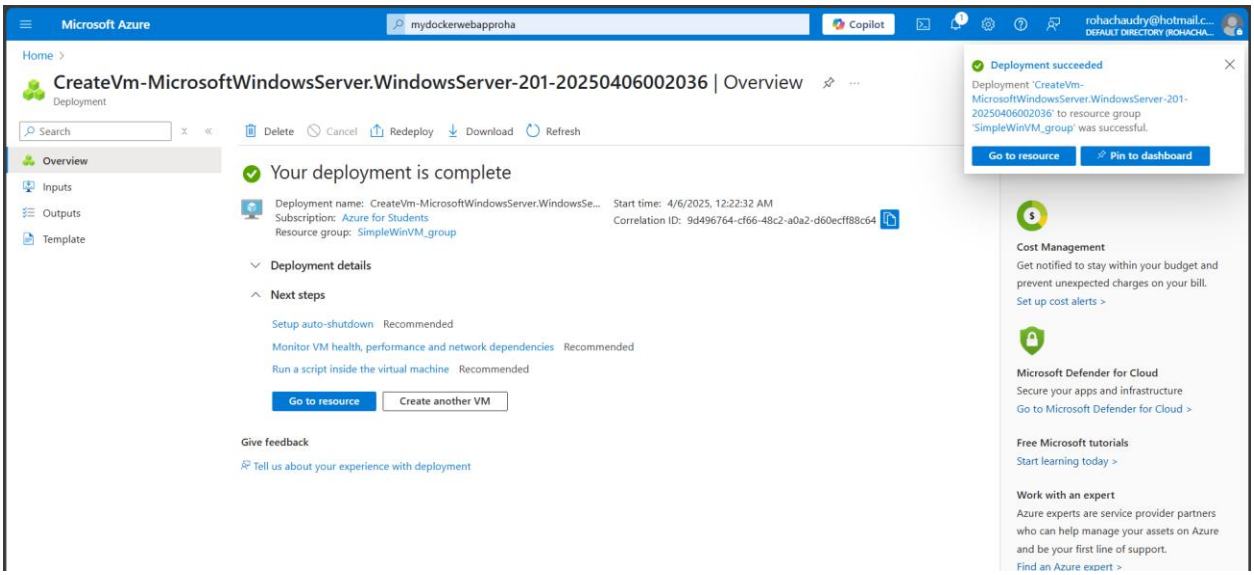
5. Switch to the Management tab, and in its Monitoring section, select the following setting:



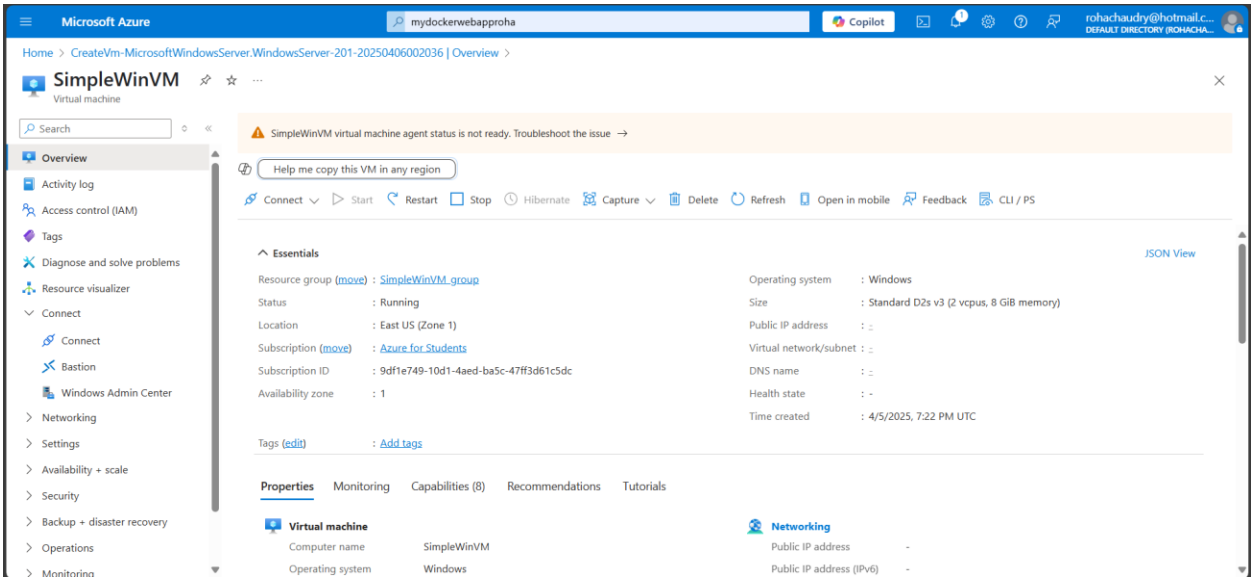
6. Leave the remaining defaults and then click the Review + create button at the bottom of the page.



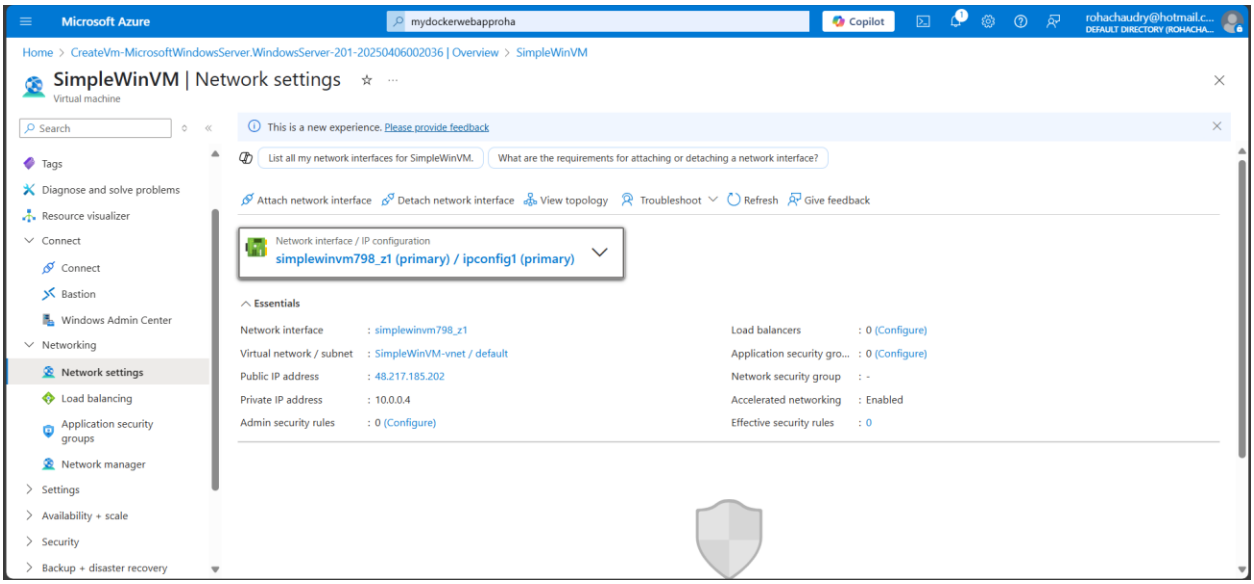
7. Once Validation is passed click the Create button. It can take about five minutes to deploy the virtual machine.



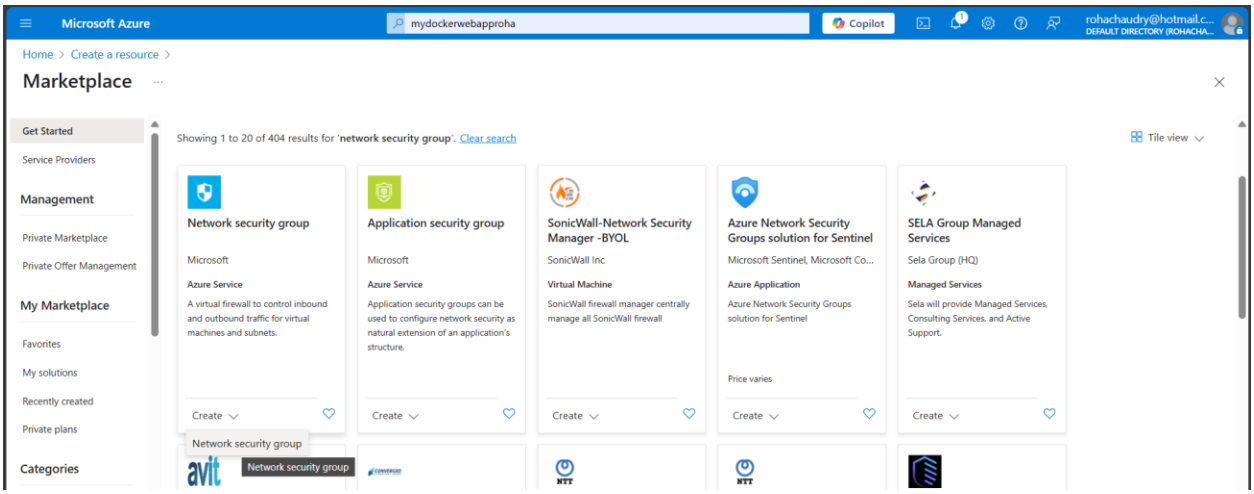
9. From the deployment blade or from the Notification area, click Go to resource.



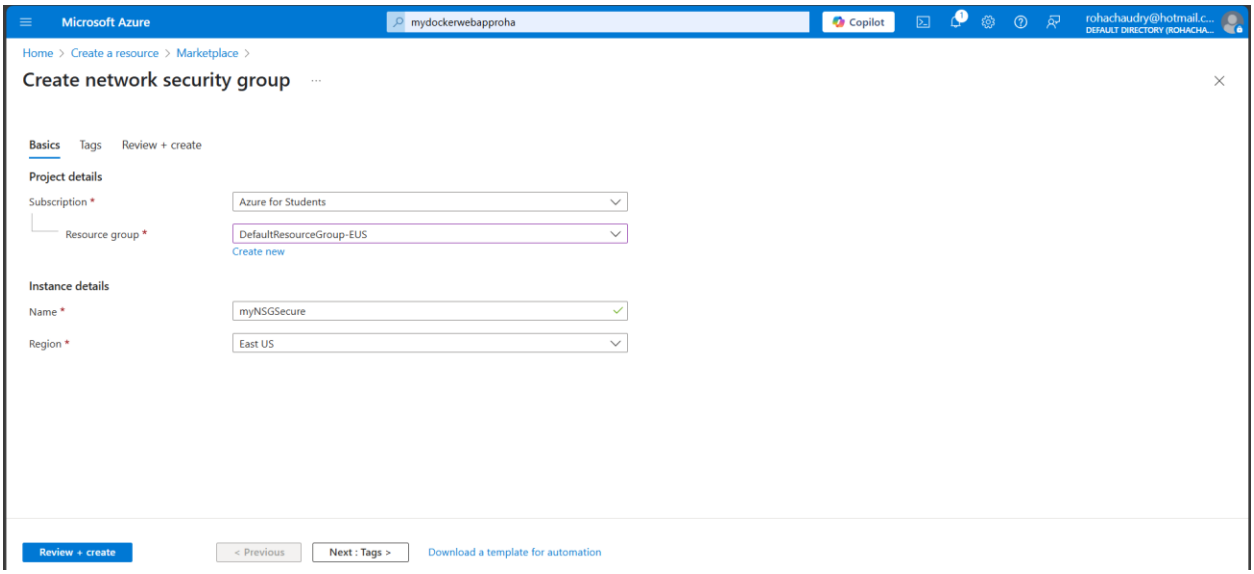
10. On the SimpleWinVM virtual machine blade, click Networking, review the Inbound port rules tab, and note that there is no network security group associated with the network interface of the virtual machine or the subnet to which the network interface is attached.



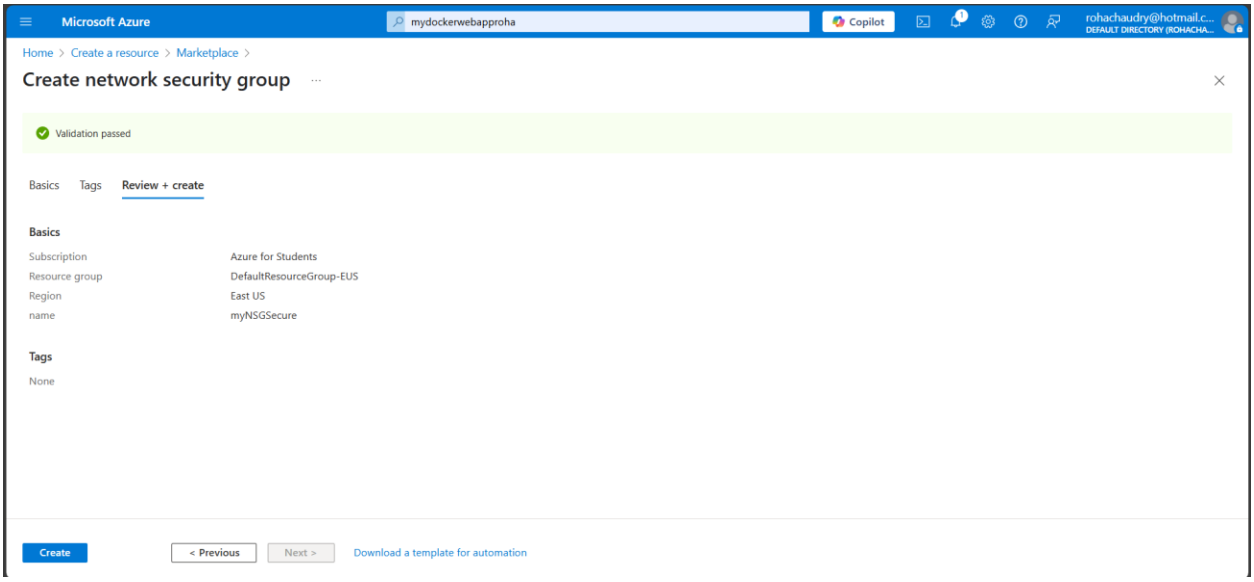
1. From the All services blade, search for and select Network security groups and then click + Add, + Create, + New

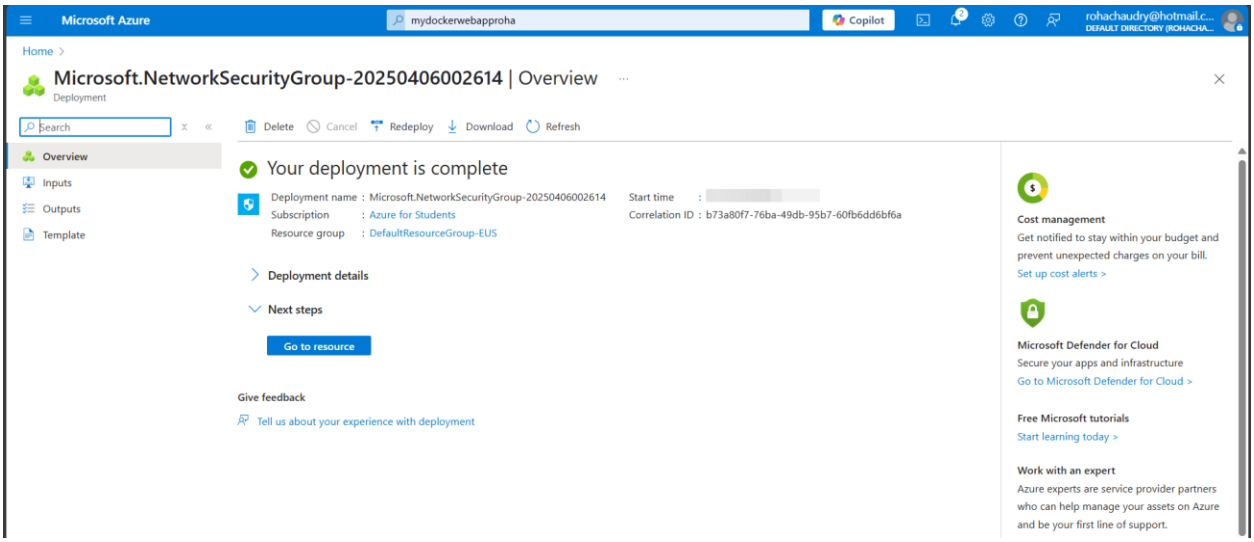


2. On the Basics tab of the Create network security group blade, specify the following settings.

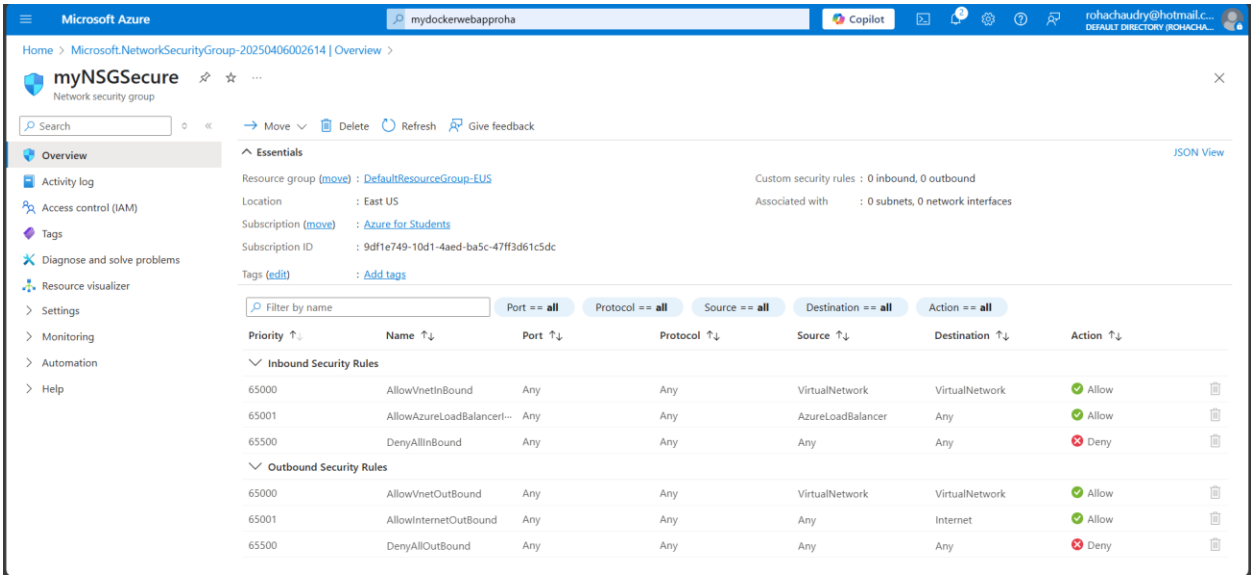


3. Click Review + create and then after the validation click Create.

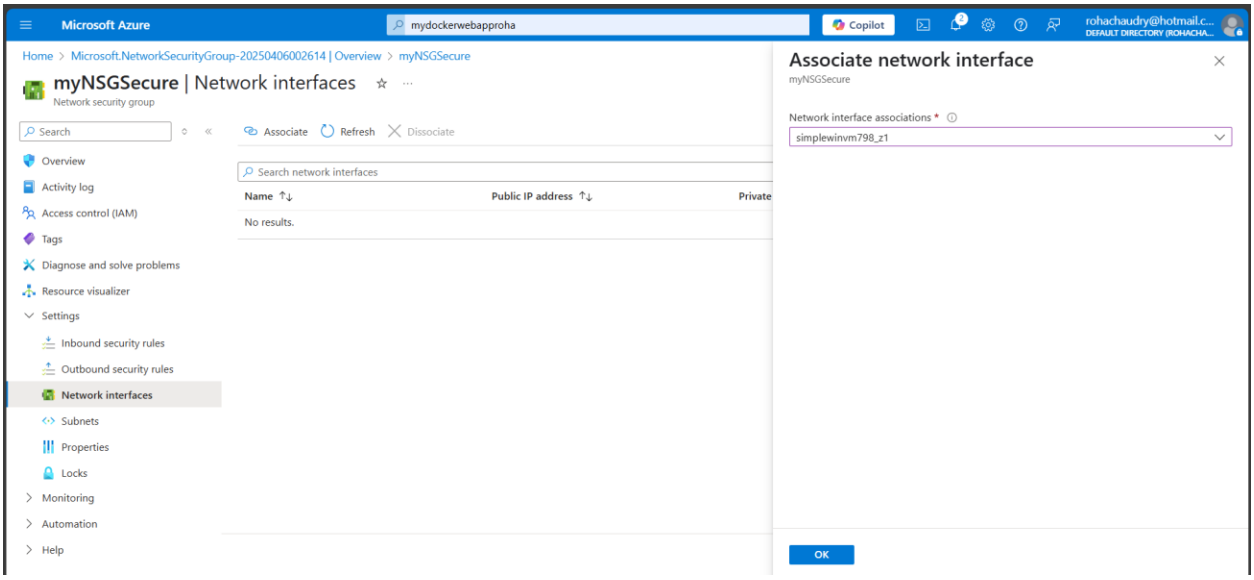




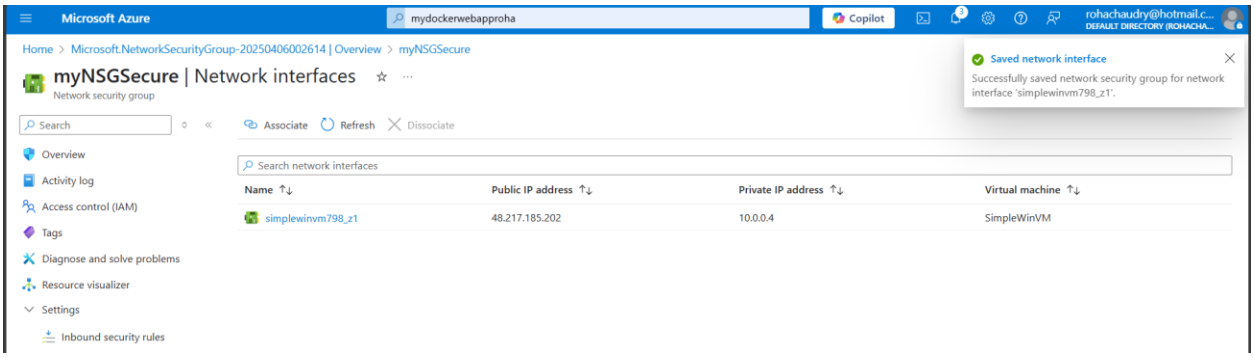
4. After the NSG is created, click Go to resource.



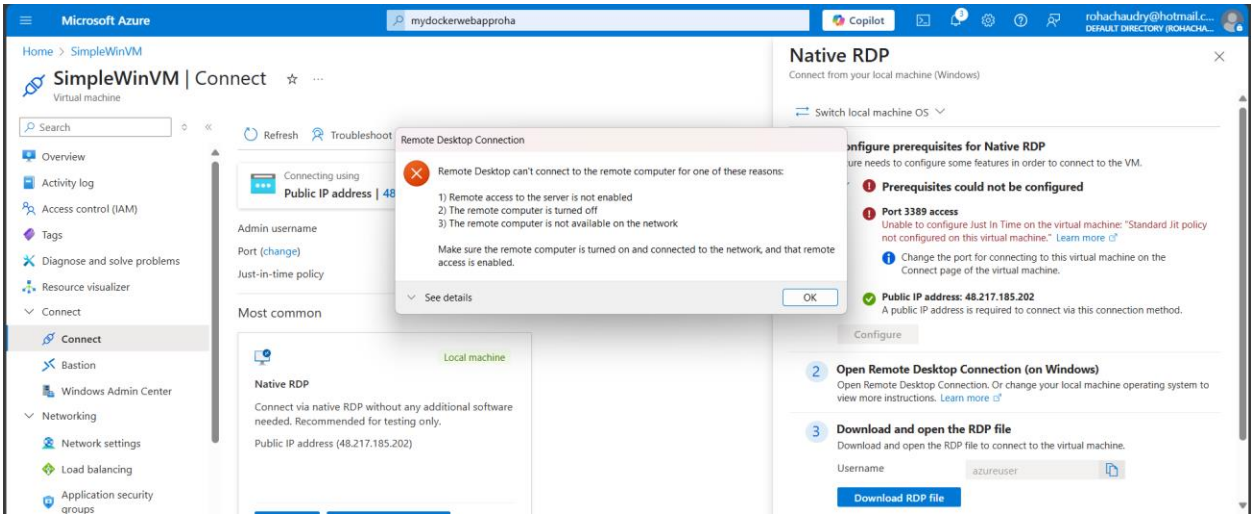
5. Under Settings click Network interfaces and then ** Associate**.



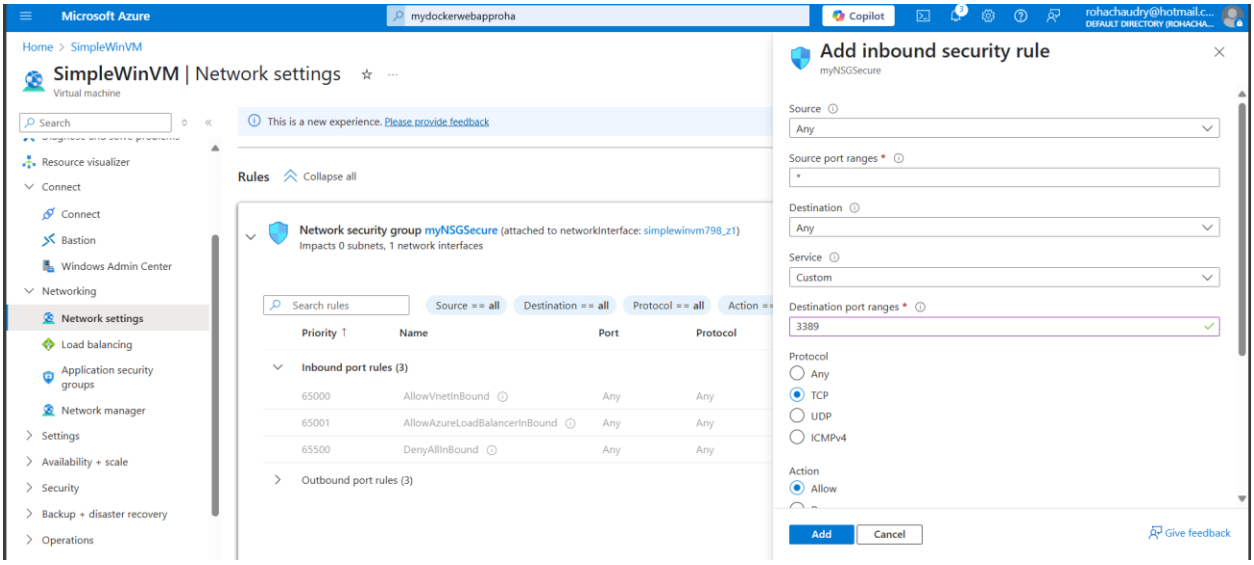
6. Select the network interface you identified in the previous task.

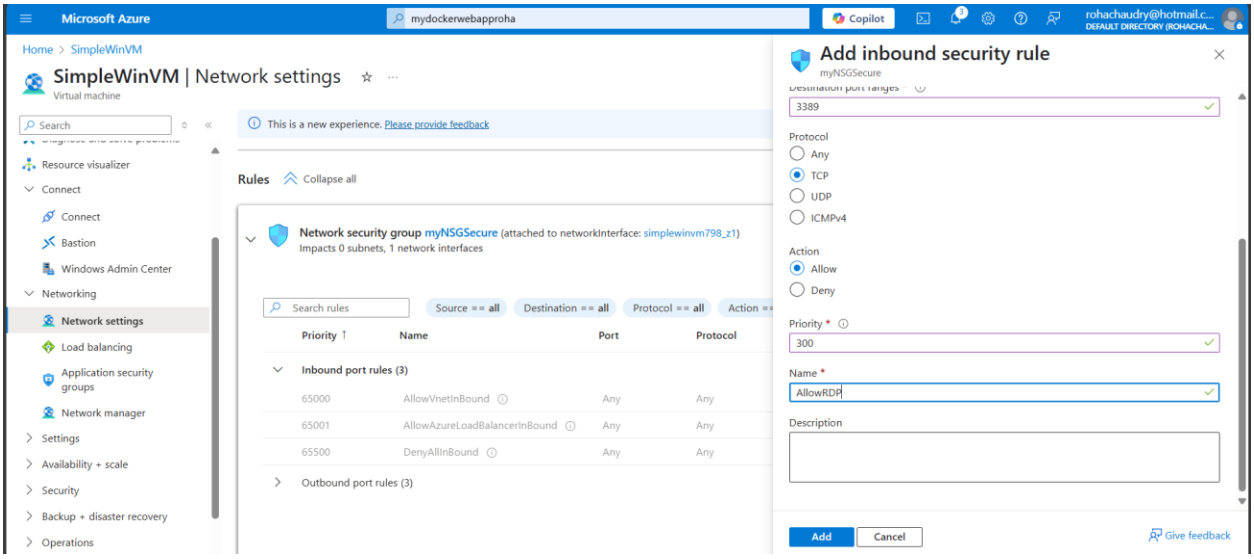


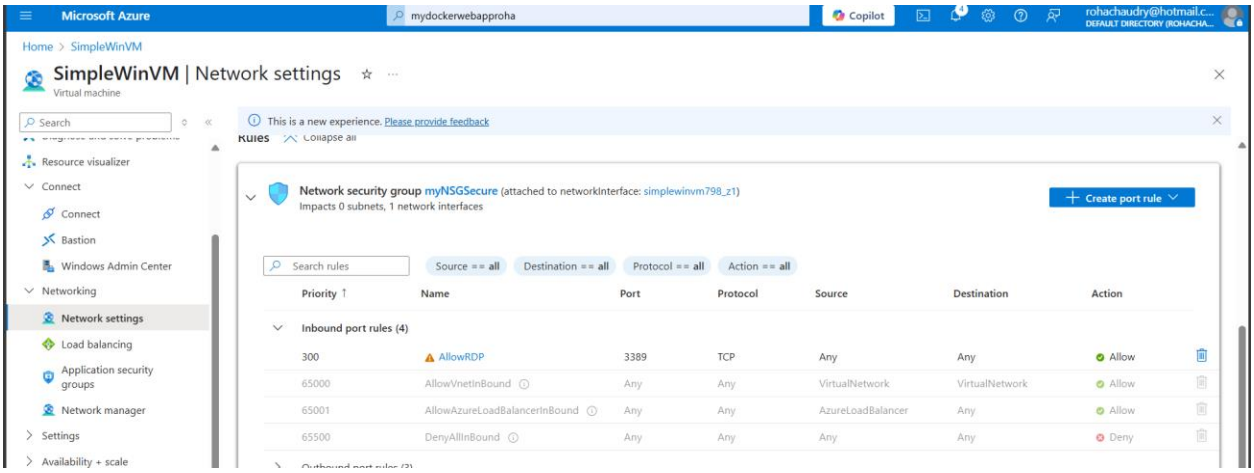
3. Attempt to connect to the virtual machine by selecting RDP and downloading an running the RDP file. By default the network security group does not allow RDP. Close the error window.



5. On the Inbound port rules tab, click Add inbound port rule . Click Add when you are done.





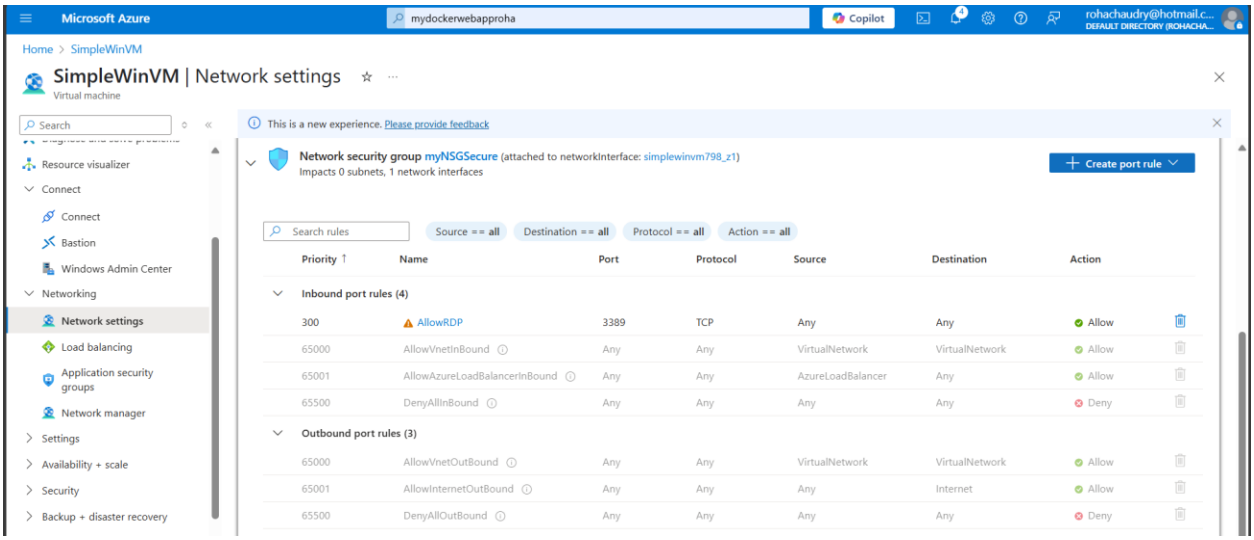


2. After the machine starts, open an Internet Explorer browser.

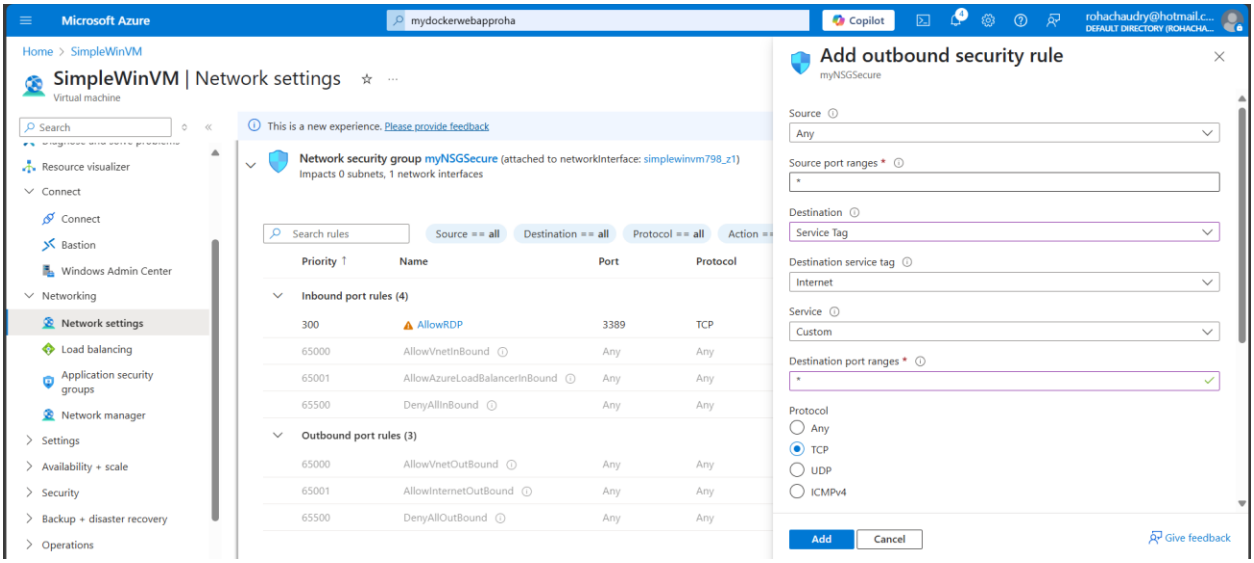
3. Verify that you can access https://www.bing.com and then close Internet Explorer. You will need to work through the IE enhanced security pop-ups.

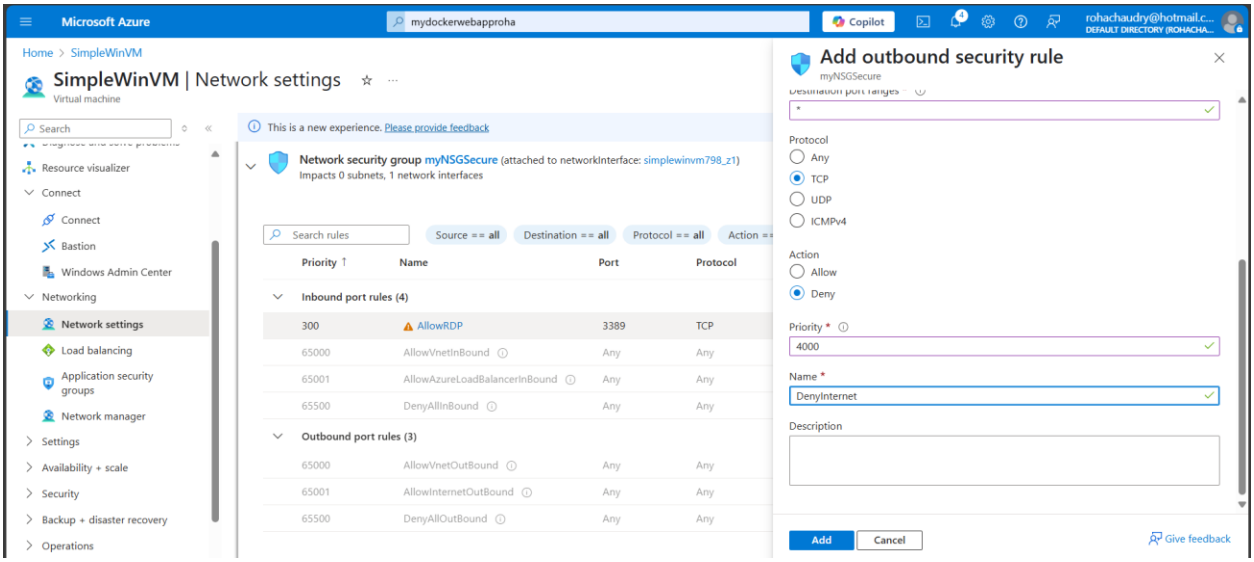
4. Back in the Azure portal, navigate back to the blade of the SimpleWinVM virtual machine.

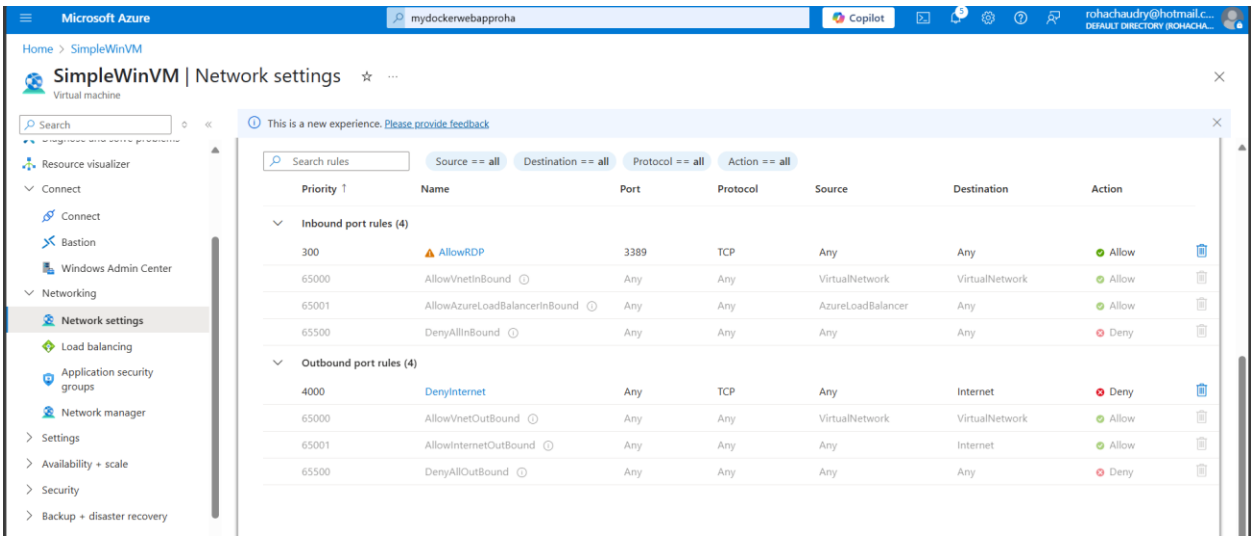
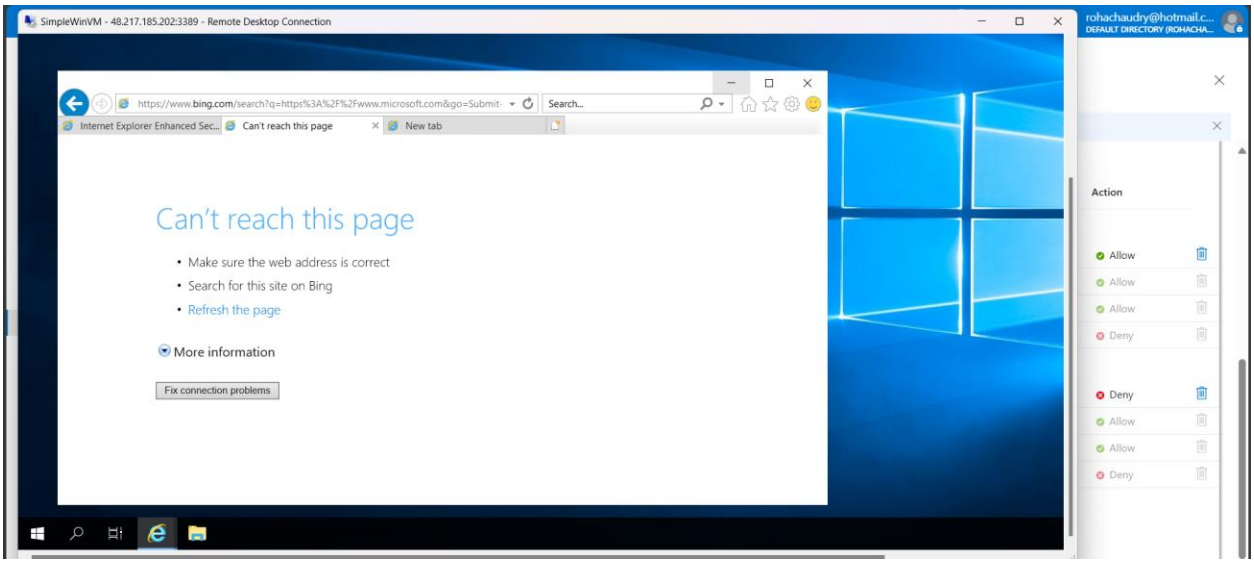
5. Under Settings, click Networking, and then Outbound port rules.



7. Click Add outbound port rule to the right of the myNSGSecure (attached to network interface: myVMNic) network security group and configure a new outbound security rule with a higher priority that will deny internet traffic. Click Add when you are finished.


Microsoft Azure
mydockerwebapproha
Copilot
rohachaudry@hotmail.c...
DEFAULT DIRECTORY (ROHACHA...
Home > SimpleWinVM
SimpleWinVM | Network settings
Virtual machine
Search
This is a new experience. Please provide feedback
Resource visualizer
Connect
Connect
Bastion
Windows Admin Center
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
Availability + scale
Security
Backup + disaster recovery
Operations
Network security group myNSGSecure (attached to networkInterface: simplewinvm798_z1)
Impacts 0 subnets, 1 network interfaces
Search rules
Source == all
Destination == all
Protocol == all
Priority
Name
Port
Protocol
Inbound port rules (4)
300 AllowRDP 3389 TCP
65000 AllowVnetInBound Any Any
65001 AllowAzureLoadBalancerInBound Any Any
65500 DenyAllInBound Any Any
Outbound port rules (3)
65000 AllowVnetOutBound Any Any
65001 AllowInternetOutBound Any Any
65500 DenyAllOutBound Any Any
Add outbound security rule
myNSGSecure
Source
Any
Source port ranges *
*
Destination
Service Tag
Destination service tag
Internet
Service
Custom
Destination port ranges *
*
Protocol
Any
TCP
UDP
ICMPv4
Add
Cancel
Give feedback


Microsoft Azure
mydockerwebapproha
Copilot
rohachaudry@hotmail.c...
DEFAULT DIRECTORY (ROHACHA...
Home > SimpleWinVM
SimpleWinVM | Network settings
Virtual machine
Search
This is a new experience. Please provide feedback
Resource visualizer
Connect
Connect
Bastion
Windows Admin Center
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
Availability + scale
Security
Backup + disaster recovery
Operations
Network security group myNSGSecure (attached to networkInterface: simplewinvm798_z1)
Impacts 0 subnets, 1 network interfaces
Search rules
Source == all
Destination == all
Protocol == all
Priority
Name
Port
Protocol
Inbound port rules (4)
300 AllowRDP 3389 TCP
65000 AllowVnetInBound Any Any
65001 AllowAzureLoadBalancerInBound Any Any
65500 DenyAllInBound Any Any
Outbound port rules (3)
65000 AllowVnetOutBound Any Any
65001 AllowInternetOutBound Any Any
65500 DenyAllOutBound Any Any
Add outbound security rule
myNSGSecure
*
Protocol
Any
TCP
UDP
ICMPv4
Action
Allow
Deny
Priority *
4000
Name *
DenyInternet
Description
Add
Cancel
Give feedback



9. Browse to https://www.microsoft.com. The page should not display. You may need to work through additional IE enhanced security pop-ups.