



NETWORK SECURITY GROUPS AND APPLICATION SECURITY GROUPS



Sneha Thankam Varghese

Table of Contents

Exercise 1: Create the virtual networking infrastructure	2
Exercise 2: Deploy virtual machines and test network filters.	6

Lab scenario

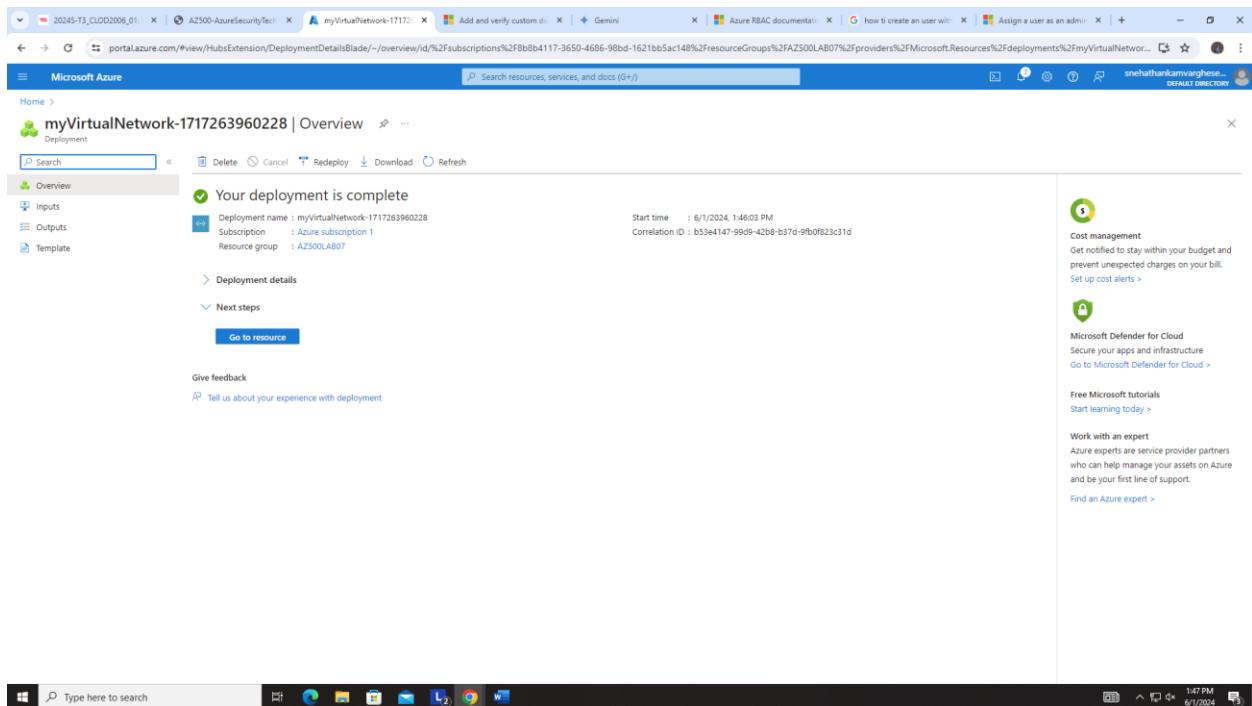
You have been asked to implement your organization's virtual networking infrastructure and test to ensure it is working correctly. In particular:

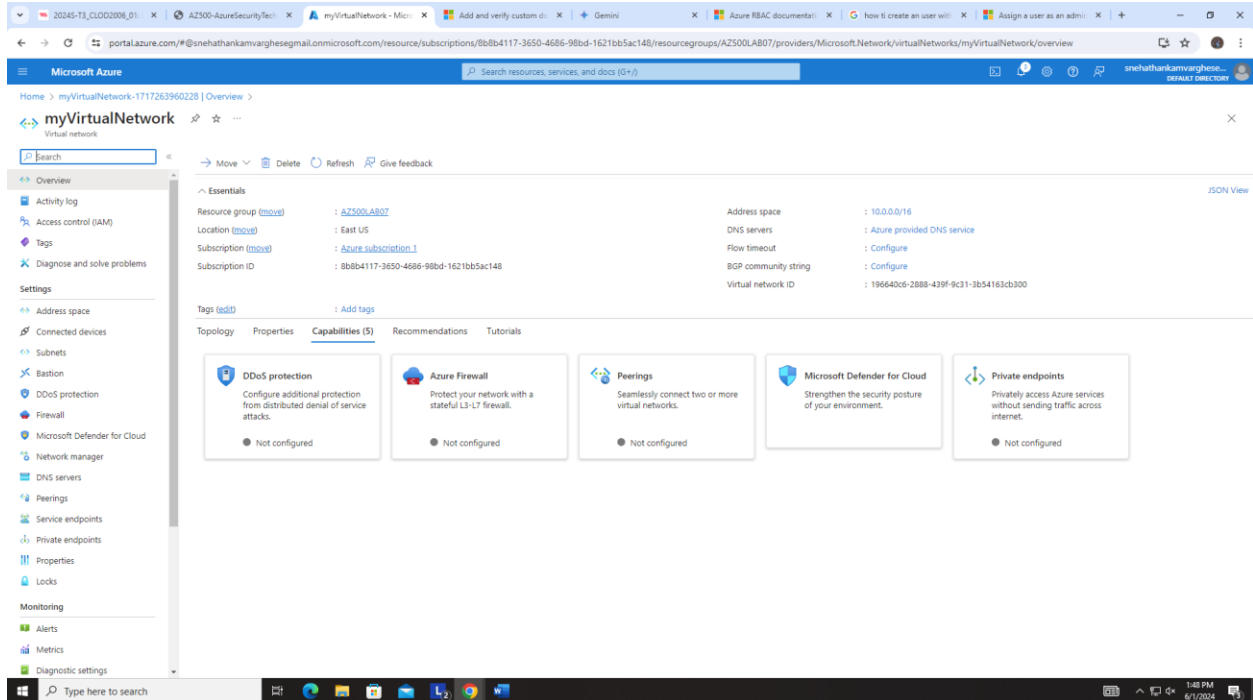
- The organization has two groups of servers: Web Servers and Management Servers.
- Each group of servers should be in its own Application Security Group.
- You should be able to RDP into the Management Servers, but not the Web Servers.
- The Web Servers should display the IIS web page when accessed from the internet.
- Network security group rules should be used to control network access.

Lab Link

Exercise 1: Create the virtual networking infrastructure

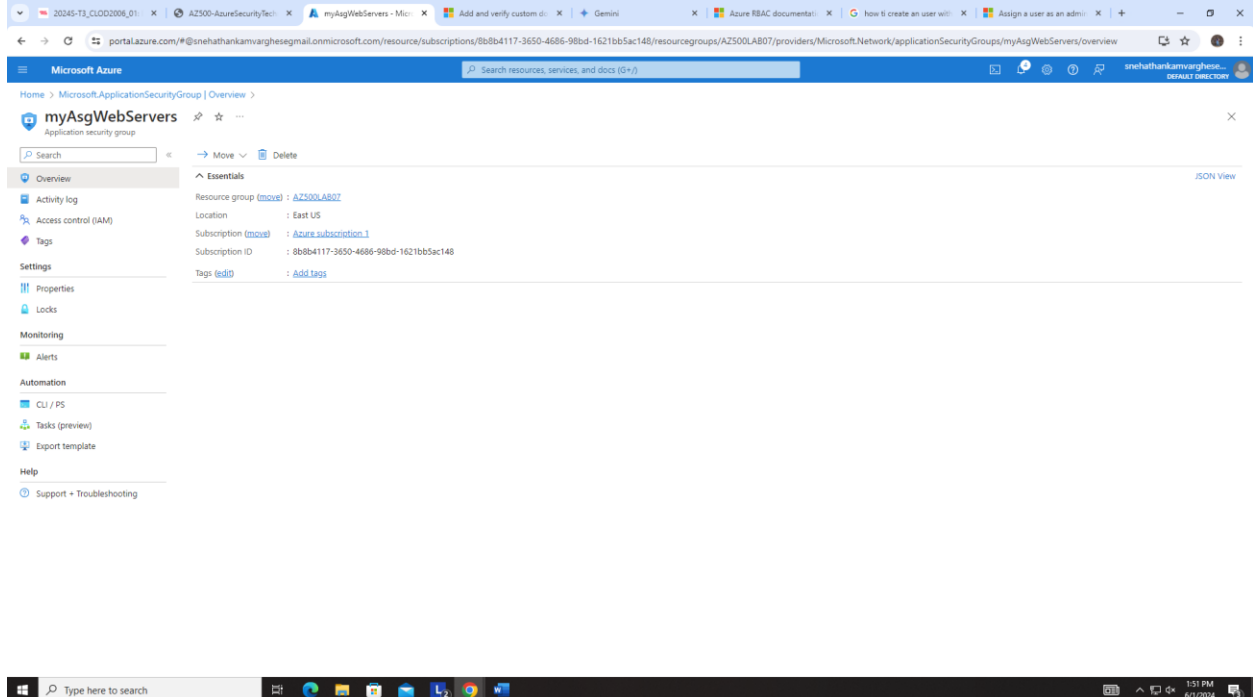
Task 1 : Create a Virtual Network





Task 2: Create application security groups

Application security group will be for the web servers.



The application security group will be for the management servers.

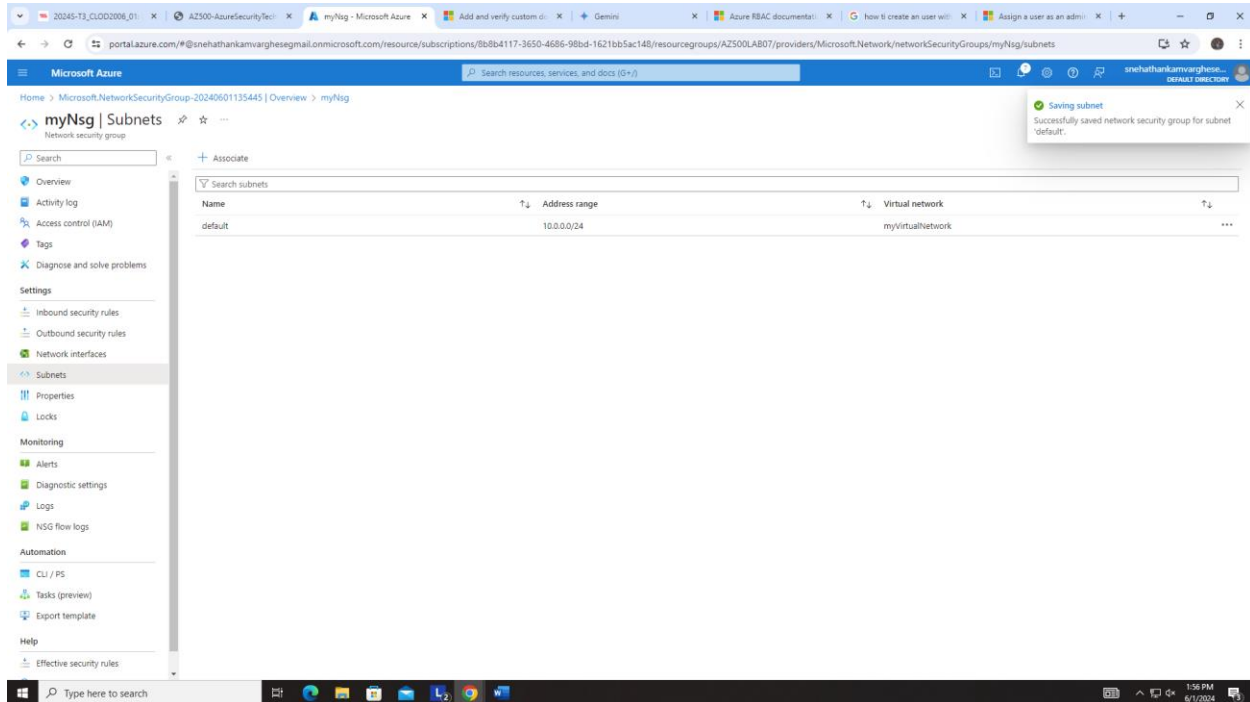
The screenshot displays the Azure portal interface for an Application Security Group (ASG) named 'myAsgMgmtServers'. The left-hand navigation pane includes sections for Overview, Activity log, Access control (IAM), Tags, Settings, Properties, Locks, Monitoring, Alerts, Automation, and Help. The main content area, titled 'Essentials', provides key information about the ASG: Resource group (AZ500LAB07), Location (East US), Subscription (Azure subscription 1), Subscription ID (8b8b4117-3650-4686-98bd-1621bb5ac148), and Tags (Add tags). A 'JSON View' link is visible in the top right corner of the main area.

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

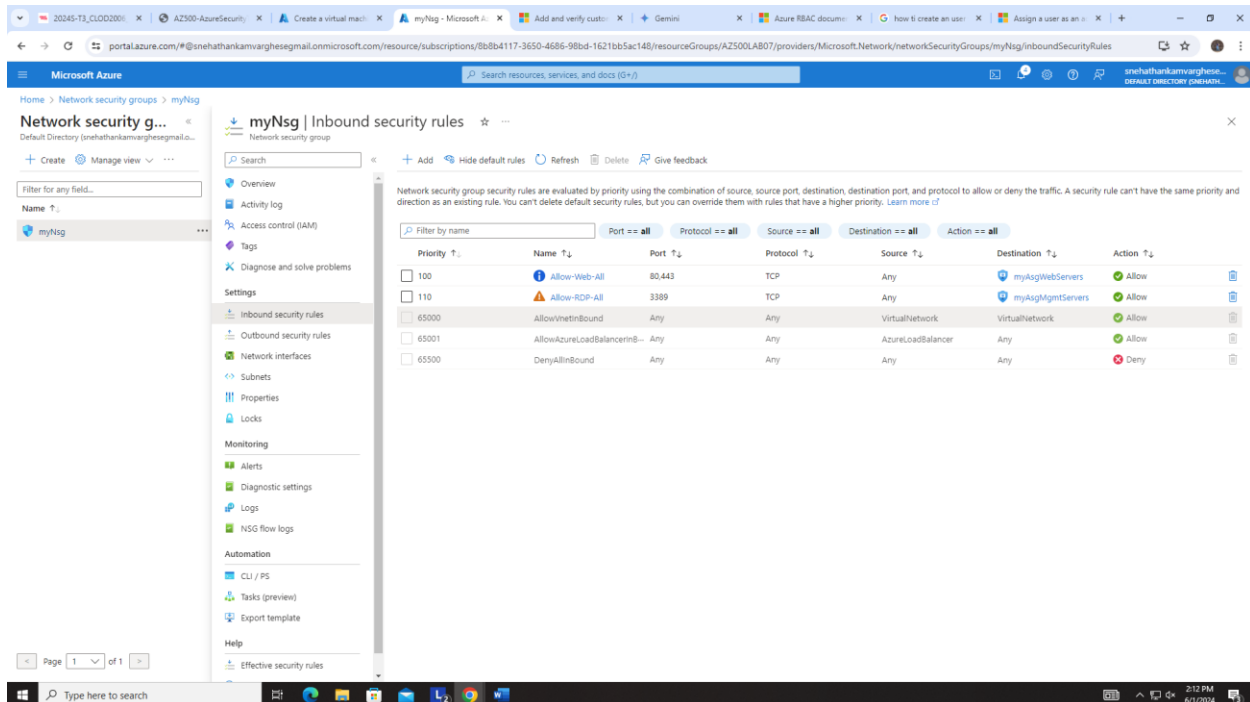
The screenshot shows the Azure portal for a Network Security Group (NSG) named 'myNsg'. The left navigation pane includes Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Network interfaces, Subnets, Properties, Locks, Monitoring, Alerts, Diagnostic settings, Logs, NSG flow logs, Automation, and Help. The main content area, titled 'Essentials', shows the NSG's resource group (AZ500LAB07), location (East US), subscription, and subscription ID. It also indicates 'Custom security rules: 0 inbound, 0 outbound' and 'Associated with: 0 subnets, 0 network interfaces'. Below this is a table of security rules, with filters for Port, Protocol, Source, Destination, and Action. The table is divided into 'Inbound Security Rules' and 'Outbound Security Rules'.

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Associating subnet to the Network Security Group



Task 4: Create inbound NSG security rules for 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.

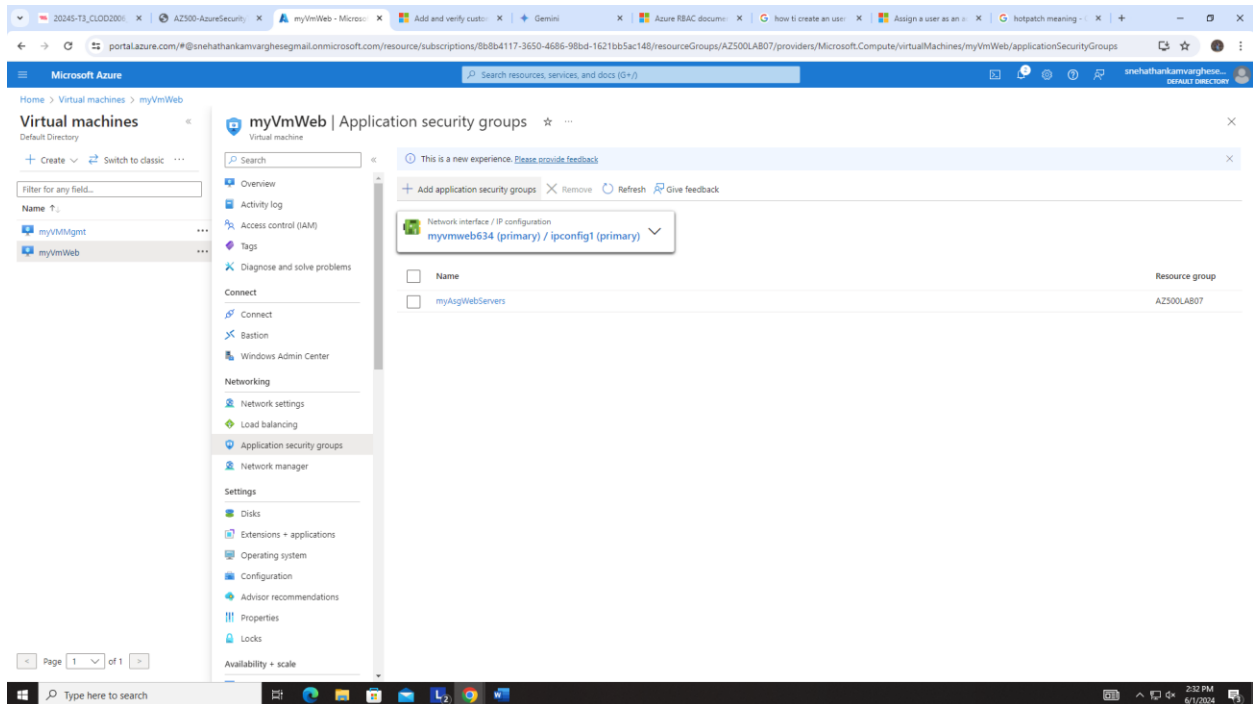
The screenshot displays the Azure portal interface for a virtual machine named 'myVmWeb'. The left sidebar contains navigation options such as Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Network settings, Load balancing, Application security groups, Network manager, Settings, Disks, Extensions + applications, Operating system, Configuration, Advisor recommendations, Properties, Locks, and Availability + scale. The main content area shows the 'Overview' tab for 'myVmWeb'. A warning banner at the top states: 'myVmWeb virtual machine agent status is not ready. Troubleshoot the issue →'. Below this, the 'Essentials' section provides key details: Resource group (AZ500LAB07), Status (Running), Location (East US), Subscription (Azure subscription 1), and Subscription ID (8b8b4117-3650-4686-98bd-1621bb5ac148). To the right, a table lists properties: Operating system (Windows), Size (Standard B1s (1 vcpu, 1 GiB memory)), Public IP address (172.191.2.108), Virtual network/subnet (myVirtualNetwork/default), DNS name (not configured), Health state (-), and Time created (6/1/2024, 6:18 PM UTC). The 'Tags' section is empty. Below the Essentials section are tabs for Properties, Monitoring, Capabilities (8), Recommendations, and Tutorials. The 'Properties' tab is active, showing details for the Virtual machine (Computer name: myVmWeb, Operating system: Windows, VM generation: V2, VM architecture: x64, Agent status: Not Ready, Agent version: Unknown, Hibernation: Disabled, Host group: -, Host: -, Proximity placement group: -, Colocation status: N/A, Capacity reservation group: -, Disk controller type: SCSI) and Networking (Public IP address: 172.191.2.108 (network interface myvmweb634), Private IP address: 10.0.0.4, Virtual network/subnet: myVirtualNetwork/default, DNS name: Configure). The 'Size' section shows Standard B1s with 1 vCPU and 1 GiB RAM. The 'Source image details' section shows the source image publisher as MicrosoftWindowsServer.

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

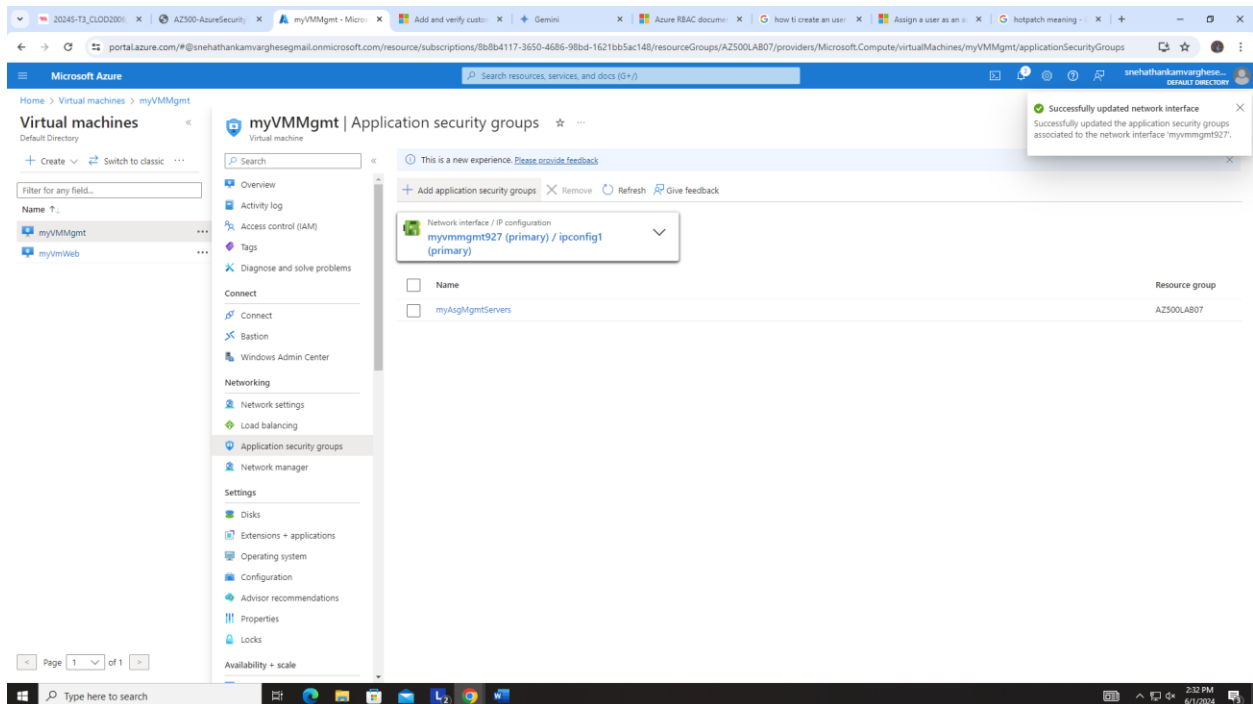
The screenshot displays the Azure portal interface for a virtual machine named 'myVMMgmt'. The left sidebar contains navigation options such as Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Network settings, Load balancing, Application security groups, Network manager, Settings, Disks, Extensions + applications, Operating system, Configuration, Advisor recommendations, Properties, Locks, and Availability + scale. The main content area shows the 'Overview' tab for 'myVMMgmt'. A warning banner at the top states: 'myVMMgmt virtual machine agent status is not ready. Troubleshoot the issue →'. Below this, the 'Essentials' section provides key details: Resource group (AZ500LAB07), Status (Running), Location (East US), Subscription (Azure subscription 1), and Subscription ID (8b8b4117-3650-4686-98bd-1621bb5ac148). To the right, a table lists properties: Operating system (Windows), Size (Standard B1s (1 vcpu, 1 GiB memory)), Public IP address (172.191.3.65), Virtual network/subnet (myVirtualNetwork/default), DNS name (not configured), Health state (-), and Time created (6/1/2024, 6:25 PM UTC). The 'Tags' section is empty. Below the Essentials section are tabs for Properties, Monitoring, Capabilities (8), Recommendations, and Tutorials. The 'Properties' tab is active, showing details for the Virtual machine (Computer name: myVMMgmt, Operating system: Windows, VM generation: V2, VM architecture: x64, Agent status: Not Ready, Agent version: Unknown, Hibernation: Disabled, Host group: -, Host: -, Proximity placement group: -, Colocation status: N/A, Capacity reservation group: -, Disk controller type: SCSI) and Networking (Public IP address: 172.191.3.65 (network interface myvmgmt027), Private IP address: 10.0.0.5, Virtual network/subnet: myVirtualNetwork/default, DNS name: Configure). The 'Size' section shows Standard B1s with 1 vCPU and 1 GiB RAM. The 'Source image details' section shows the source image publisher as MicrosoftWindowsServer.

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

The myVMWeb virtual machine interface associated to the myAsgWebServers ASG

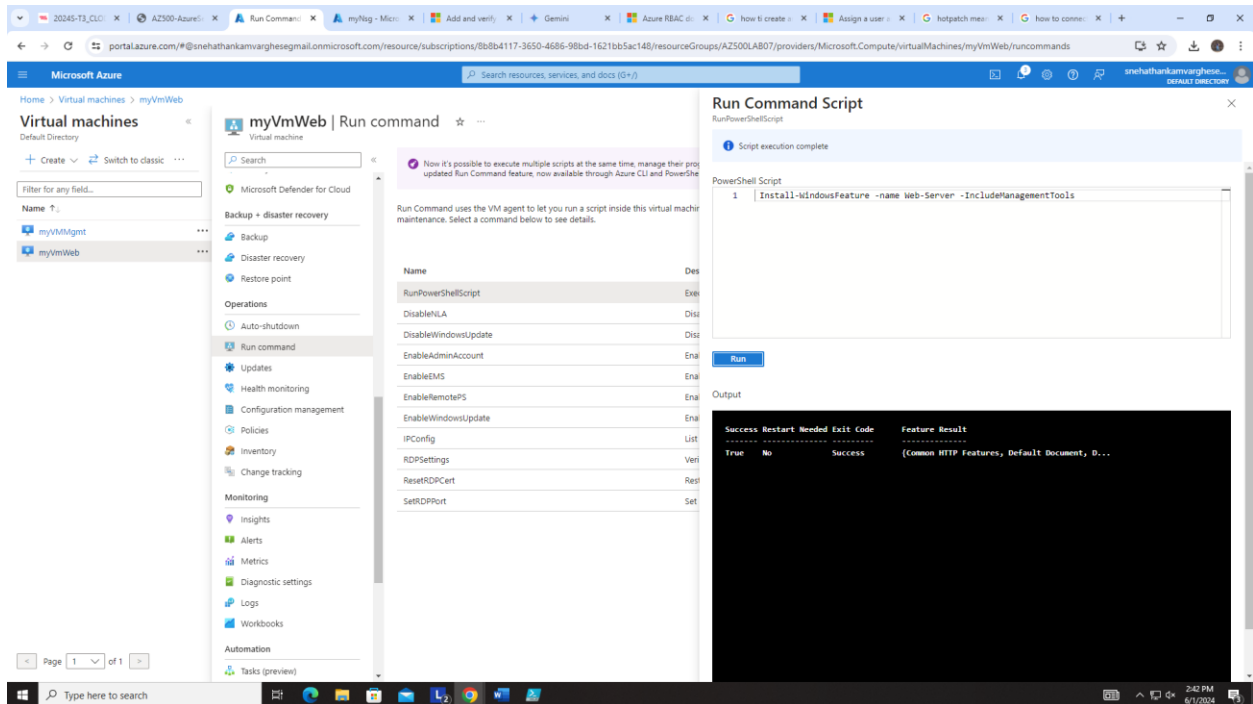


The myVMMgmt virtual machine interface associated to the myAsgMgmtServers ASG.



Task 4: Test the network traffic filtering

Verified myVMWeb can be accessed via HTTP/HTTPS.



Verified the Public IP of WebServer is accessible.

