

Week 8 Assignment 2: Network Security Groups and Application Security Groups

Course: **Cloud and Network Security C3-2024**

Student Name: **Loise Murugi Murage**

Student No: **CS-CNS07-24115.**

Thursday, November 14, 2024

Week 8 Assignment 2:

Class Exercise: Network Security Groups and Application Security

Week 8 Assignment 2: Network Security Groups and Application Security Groups

Contents

Class Exercise: Network Security Groups and Application Security.....	1
Introduction.....	3
Instructions	3
Exercise 1: Create the virtual networking infrastructure	3
Task 1: Create a virtual network.....	3
Task 2: Create application security groups.....	8
Task 3: Create a network security group and associate the NSG to the subnet	10
Task 4: Create inbound NSG security rules to all traffic to web servers and RDP to the servers.....	15
Exercise 2: Deploy virtual machines and test network filters.....	19
Task 1: Create a virtual machine to use as a web server	19
Task 2: Create a virtual machine to use as a management server.	26
Task 3: Associate each virtual machines network interface to its application security group.	
.....	31
Task 4: Test the network traffic filtering.....	35
Clean up resources	41
Conclusion	42

Week 8 Assignment 2: Network Security Groups and Application Security Groups

Introduction

In this lab activity we will be using Microsoft Azure to implement a virtual networking infrastructure to configure Network Security Groups and Application Security Groups and test to ensure they are working correctly. Network security group (NSG) contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, we will specify source and destination, port, and protocol. Application security groups (ASG) enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups.

We will then create a web server and a management server and configure an Application Security Group for each of the servers.

We will then Remote desktop to the Management server and use the web server to display the IIS webpage from the internet.

We will use West US as the region.

Instructions

Exercise 1: Create the virtual networking infrastructure

Task 1: Create a virtual network

In this task, you will create a virtual network to use with the network and application security groups.

1. Sign-in to the Azure portal <https://portal.azure.com/>.

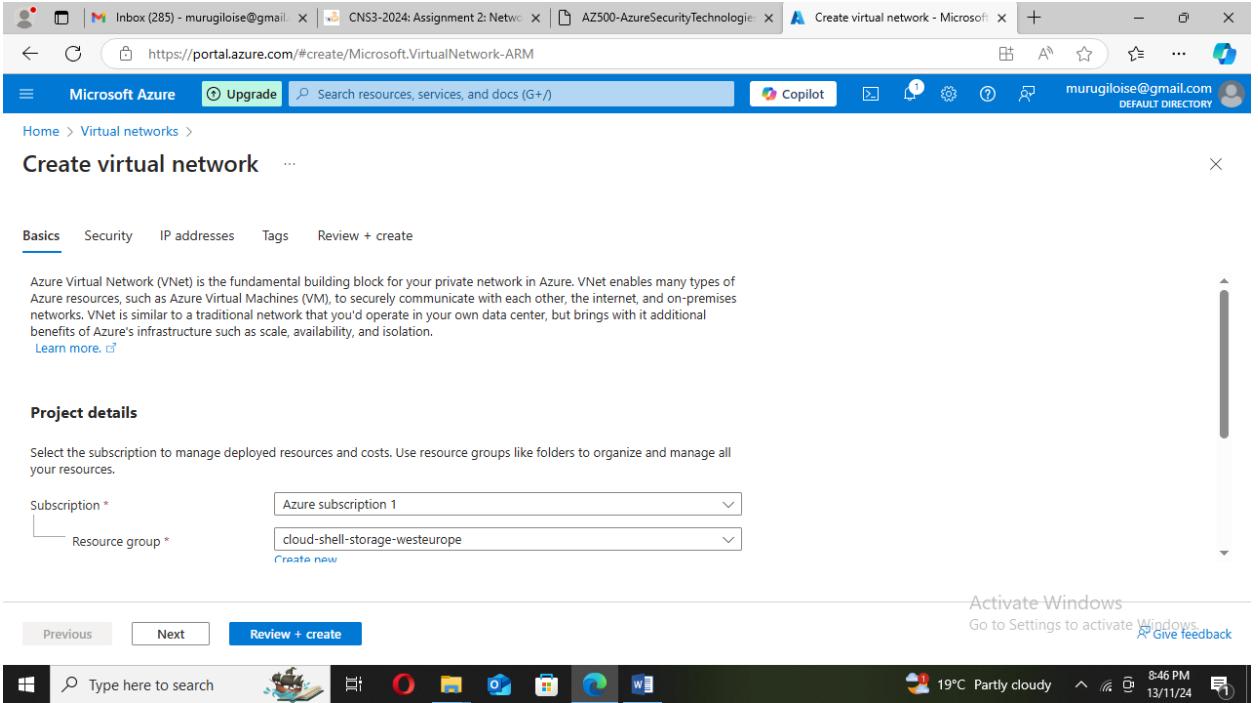
Week 8 Assignment 2: Network Security Groups and Application Security Groups

The screenshot shows the Microsoft Azure portal homepage. At the top, there are four cards: "Take a free online course on Microsoft Learn", "Watch a demo and attend a live Q&A", "Start a project with Quickstart Center", and "Explore support resources". Below these is a section titled "Azure services" with icons for "Create a resource", "Route tables", "Resource groups", "Firewalls", "Deploy a custom...", "Advisor", "Virtual machines", "SQL databases", and "App registrations". A "Private Windows" link is also present. The bottom part of the screenshot shows the Windows taskbar with various pinned icons.

2. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Virtual networks** and press the **Enter** key.

The screenshot shows the "Virtual networks" page in the Microsoft Azure portal. The top navigation bar includes "Home > Virtual networks". The main area displays search filters for "Subscription equals all", "Resource group equals all", "Location equals all", and "Add filter". It also shows sorting options for "Name", "Resource group", "Location", and "Subscription". Below this, a message states "Showing 0 to 0 of 0 records." and features a "Create virtual network" button. The bottom part of the screenshot shows the Windows taskbar.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

3. 

4. On the **Basics** tab of the **Create virtual network** blade, specify the following settings (leave others with their default values) and click **Next: IP Addresses**:

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	click Create new and type the name AZ500LAB07
Name	myVirtualNetwork
Region	East US

Week 8 Assignment 2: Network Security Groups and Application Security Groups

The screenshot shows the Microsoft Azure portal interface for creating a virtual network. The 'Basics' tab is active. Subscription is set to 'Azure subscription 1' and Resource group is '(New) AZ500LAB07'. In the 'Instance details' section, the Virtual network name is 'myVirtualNetwork' and the Region is '(US) West US'. Navigation buttons 'Previous', 'Next', and 'Review + create' are visible at the bottom.

5. On the **IP addresses** tab of the **Create virtual network** blade, set the **IPv4 address space** to **10.0.0.0/16**, and, if needed, in the **Subnet name** column, click **default**, on the **Edit subnet** blade, specify the following settings and click **Save**:

Setting	Value
Subnet name	default
Subnet address range	10.0.0.0/24

Week 8 Assignment 2: Network Security Groups and Application Security Groups

10.0.0.0/16
10.0.0.0 /16
10.0.0.0 - 10.0.255.255 65,536 addresses

Subnets	IP address range	Size	NAT gateway
default	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-

Add IPv4 address space | ↴

Activate Windows
Go to Settings to activate Windows
Give feedback

Previous Next Review + create

6. Back on the IP addresses tab of the Create virtual network blade, click Review + create.

Azure subscription 1
AZ500LAB07
myVirtualNetwork
West US

Azure Bastion: Disabled
Azure Firewall: Disabled

Activate Windows
Go to Settings to activate Windows
Give feedback

Previous Next Create

7. On the Review + create tab of the Create virtual network blade, click Create. We have successfully created a virtual network myVirtualNetwork as seen below.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

The screenshot shows the Microsoft Azure portal interface. At the top, there are several tabs open, including 'Inbox (285) - murugiloise@gmail.com', 'CNS3-2024: Assignment 2: Netwo...', 'AZ500-AzureSecurityTechnologie...', and 'myVirtualNetwork-1731520658072'. The main content area is titled 'myVirtualNetwork-1731520658072 | Overview'. A prominent message says 'Your deployment is complete'. Below it, deployment details are listed: Deployment name: myVirtualNetwork-1731520658072, Start time: 11/13/2024, 8:58:04 PM, Subscription: Azure subscription 1, Correlation ID: 980d45c5-c95d-4b4f-a4c7-742..., and Resource group: AZ500LAB07. There are sections for 'Deployment details' and 'Next steps', with a 'Go to resource' button. On the right side, there are promotional cards for 'Cost management', 'Microsoft Defender for Cloud', and 'Free Microsoft tutorials'. The bottom of the screen shows the Windows taskbar with various pinned icons.

Task 2: Create application security groups

In this task, you will create an application security group.

1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Application security groups** and press the **Enter** key.

The screenshot shows the Microsoft Azure portal interface. The title bar includes tabs for 'Inbox (285) - murugiloise@gmail.com', 'CNS3-2024: Assignment 2: Netwo...', 'AZ500-AzureSecurityTechnologie...', and 'Application security groups - Mic...'. The main content area is titled 'Application security groups'. It features a search bar and filter options: '+ Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'. Below these are buttons for 'Filter for any field...', 'Subscription equals all', 'Resource group equals all', 'Location equals all', and 'Add filter'. A message states 'Showing 0 to 0 of 0 records.' At the bottom, there are columns for 'Name', 'Network interfaces count', 'Type', 'Resource group', 'Location', and 'Subscription'. A large shield icon with a computer monitor inside is centered, and the text 'No application security groups to display' is shown. To the right, there are links for 'Activate Windows', 'Give feedback', and 'Create application security group'. The bottom of the screen shows the Windows taskbar.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

2. On the **Application security groups** blade, click **+ Create**.

The screenshot shows the 'Create an application security group' blade in the Azure portal. The 'Basics' tab is selected. In the 'Project details' section, 'Subscription' is set to 'Azure subscription 1' and 'Resource group' is set to 'AZ500LAB07'. In the 'Instance details' section, 'Name' is empty and 'Region' is set to 'East US'. At the bottom, there are 'Review + create' and 'Next : Tags >' buttons.

3. On the **Basics** tab of the **Create an application security group** blade, specify the following settings:

Setting	Value
Resource group	AZ500LAB07
Name	myAsgWebServers
Region	East US

Note: This group will be for the web servers.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

Activate Windows
Go to Settings to activate Windows.

4. Click **Review + create** and then click **Create**.

We have successfully created **myAsgWebServers** application security group

Activate Windows
Go to Settings to activate Windows.

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

In this task, you will create a network security group.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the

The screenshot shows the Microsoft Azure portal interface. The title bar includes tabs for 'Inbox (285) - murugiloise@gmail.com', 'CNS3-2024: Assignment 2: Netwo...', 'AZ500-AzureSecurityTechnologie...', and 'Network security groups - Micro...'. The main content area is titled 'Network security groups' and shows a shield icon. Below it, the text 'No network security groups to display' is centered. A blue button labeled 'Create network security group' is located below the text. The bottom of the screen shows the Windows taskbar with various pinned icons like File Explorer, Edge, and Mail.

2. On the **Network security groups** blade, click **+ Create**

The screenshot shows the 'Create network security group' blade. The 'Basics' tab is selected. Under 'Project details', 'Subscription' is set to 'Azure subscription 1' and 'Resource group' is set to 'Create new'. Under 'Instance details', 'Name' is empty and 'Region' is showing 'Loading...'. At the bottom, there are buttons for 'Review + create', '< Previous', 'Next : Tags >', and 'Download a template for automation'. The Windows taskbar is visible at the bottom.

3. On the **Basics** tab of the **Create network security group** blade, specify the following settings:

Week 8 Assignment 2: Network Security Groups and Application Security Groups

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	AZ500LAB07
Name	myNsg
Region	East US

The screenshot shows the Azure portal interface for creating a Network Security Group (NSG). The URL in the browser is <https://portal.azure.com/#create/Microsoft.NetworkSecurityGroup-ARM>. The page title is "Create network security group".

Project details:

- Subscription: Azure subscription 1
- Resource group: AZ500LAB07

Instance details:

- Name: myNsg
- Region: West US

At the bottom of the form, there are two buttons: "Review + create" and "Next : Tags >".

Week 8 Assignment 2: Network Security Groups and Application Security Groups

4.

Microsoft Network Security Group - Overview

Your deployment is complete

Deployment name : Microsoft.NetworkSecurityGro... Start time : 11/13/2024, 9:18:07 PM

Subscription : Azure subscription 1 Correlation ID : 0de89c12-d7fa-41f6-9880-415...

Resource group : AZ500LAB07

Deployment details

Next steps

Go to resource

Give feedback

Tell us about your experience with deployment

Cost management

Get notified to stay within your budget and prevent unexpected charges on your bill.

Set up cost alerts >

Microsoft Defender for Cloud

Secure your apps and infrastructure

Go to Microsoft Defender for Cloud >

Free Microsoft tutorials

Start learning today >

Activate Windows

Go to Settings to activate Windows.

Work with an expert

Azure experts are service provider partners

5. In the Azure portal, navigate back to the **Network security groups** blade and click the **myNsg** entry.

Network security groups

Showing 1 to 1 of 1 records.

Name ↑	Resource group ↑↓	Location ↑↓	Subscription ↑↓	Flow log ↑↓
<input type="checkbox"/> myNsg	AZ500LAB07	West US	Azure subscription 1	

< Previous Page 1 of 1 Next >

Activate Windows

Go to Settings to activate Windows.

Give feedback

Week 8 Assignment 2: Network Security Groups and Application Security Groups

6. On the myNsg blade, in the **Settings** section, click **Subnets** and then click **+ Associate**.

The screenshot shows the Azure portal interface for managing a Network Security Group (Nsg). The left sidebar lists various options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Inbound security rules, Outbound security rules, Network interfaces, Subnets, Properties, Locks, Monitoring), and Monitoring. The 'Subnets' option is selected. The main content area is titled 'myNsg | Subnets' and shows a table with the heading 'Search subnets'. The table has columns for Name, Address range, Virtual network, and a sorting arrow for each. A message at the bottom of the table says 'No results.' There is also a 'Give feedback' link. The status bar at the bottom right shows 'Activate Windows' and the system clock '19°C Mostly cloudy 9:24 PM 13/11/24'.

7. On the **Associate subnet** blade, specify the following settings and click **OK**:

Setting	Value
Virtual network	myVirtualNetwork
Subnet	default

Week 8 Assignment 2: Network Security Groups and Application Security Groups

The screenshot shows the Microsoft Azure portal interface. On the left, there's a navigation pane for 'Network security groups' with a search bar and filter options. The main area displays the 'myNsg | Subnets' blade, which includes sections for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Inbound security rules, Outbound security rules, Network interfaces, Subnets), Properties, Locks, Monitoring, and Automation. A context menu is open over the 'Subnets' section. On the right, a modal dialog titled 'Associate subnet' is displayed, prompting the user to select a virtual network and a subnet. The 'Virtual network' dropdown is set to 'myVirtualNetwork (AZ500LAB07)' and the 'Subnet' dropdown is set to 'default'. At the bottom right of the dialog is an 'OK' button.

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

- On the myNsg blade, in the **Settings** section, click **Inbound security rules**.

The screenshot shows the 'myNsg | Inbound security rules' blade. The left sidebar has the same structure as the previous screenshot. The main area shows a table of security rules:

	Priority	Name	Port	Protocol	Source	Destination
<input type="checkbox"/>	65000	AllowVnetInBound	Any	All	Virtual network	Azure
<input type="checkbox"/>	65001	AllowAzureLoadBalancedInbound	Any	All	Azure	Virtual network
<input type="checkbox"/>	65500	DenyAllInbound	Any	All	Any	Any

At the bottom right of the blade, there's an 'Activate Windows' message with a link to 'Go to Settings to activate Windows.'

Week 8 Assignment 2: Network Security Groups and Application Security Groups

2. Review the default inbound security rules and then click + Add.

The screenshot shows the Microsoft Azure portal interface. The left sidebar shows 'Network security groups > myNsg'. The main area displays the 'myNsg | Inbound security rule' blade. The blade has a title 'Add inbound security rule' and a sub-section 'myNsg'. It contains the following fields:

- Source:** Any
- Source port ranges:** *
- Destination:** Any
- Destination port ranges:** 8080
- Protocol:** Any (radio button selected)

Below these fields are buttons for 'Add' and 'Cancel'. At the bottom right of the blade, there is an 'Activate Windows' link and a 'Give feedback' button. The taskbar at the bottom of the screen shows various pinned icons and the system status bar indicates it's 19°C, mostly cloudy, 9:30 PM, and the date is 13/11/24.

3. On the **Add inbound security rule** blade, specify the following settings to allow TCP ports 80 and 443 to the **myAsgWebServers** application security group (leave all other values with their default values):

Setting	Value
Destination	in the drop-down list, select Application security group and then click myAsgWebServers
Destination port ranges	80,443
Protocol	TCP
Priority	100
Name	Allow-Web-All

Week 8 Assignment 2: Network Security Groups and Application Security Groups

The screenshot shows the Microsoft Azure portal interface. The left sidebar shows a 'Network security groups' list with 'myNsg' selected. The main area displays the 'Inbound security rule' configuration for 'myNsg'. The 'Service' dropdown is set to 'Custom'. The 'Destination port ranges' field contains '80,443'. The 'Protocol' section has 'TCP' selected. The 'Action' section has 'Allow' selected. The 'Priority' is set to '100'. A status message at the bottom right says 'Activate Windows Go to Settings to activate Windows.'

- On the Add inbound security rule blade, click Add to create the new inbound rule

This screenshot is similar to the previous one, showing the 'Add inbound security rule' blade for 'myNsg'. The configuration is identical: custom service, destination port range 80,443, TCP protocol, allow action, and priority 100. However, a progress message 'Creating security rule 'Allow-Web-All''. is visible in the top right corner of the blade.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

Network security group: myNsg | Inbound security rules

Priority	Name	Port	Protocol	Source
100	Allow-Web-All	80,443	TCP	Any
65000	AllowVnetInBound	Any	Any	Virtua
65001	AllowAzureLoadBalanc...	Any	Any	AzureI
65500	DenyAllInBound	Any	Any	Any

5. On the **myNsg** blade, in the **Settings** section, click **Inbound security rules**, and then click **+ Add**.
6. On the **myNsg** blade, in the **Settings** section, click **Inbound security rules**, and then click **+ Add**.

Add inbound security rule

myNsg

TCP

UDP

ICMPv4

Action

Allow

Deny

Priority *

110

Name *

Allow-RDP-All

Description

Add Cancel

7. On the **Add inbound security rule** blade, click **Add** to create the new inbound rule.

Result: You have deployed a virtual network, network security with inbound security rules, and two application security groups.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

An inbound security rule has been added successfully and the port 3389 is exposed to the internet

myNsg | Inbound security rules

Priority	Name	Port	Protocol	Source	Action
100	Allow-Web-All	80,443	TCP	Any	
110	Allow-RDP-All	3389	TCP	Any	
65000	AllowVnetInBound	Any	Any	Virtua	
65001	AllowAzureLoadBalanc...	Any	Any	AzureI	
65500	DenyAllInBound	Any	Any	Any	

Exercise 2: Deploy virtual machines and test network filters

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

In this task, you will create a virtual machine to use as a web server.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the

The screenshot shows the 'Virtual machines' blade in the Azure portal. At the top, there are several filter options: 'Subscription equals all', 'Type equals all', 'Resource group equals all', 'Location equals all', and 'Add filter'. Below the filters, it says 'Showing 0 to 0 of 0 records.' A large central message says 'No virtual machines to display' with a small icon of a computer monitor. Below this, it says 'Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.' There is a blue 'Create' button. On the right side, there is an 'Activate Windows' section with a link to 'Go to Settings to activate Windows.' and a 'Give feedback' button. The bottom of the screen shows the Windows taskbar with various pinned icons like File Explorer, Edge, and Mail.

2. On the **Virtual machines** blade, click **+ Create** and, in the dropdown list, click **+ Azure virtual machine**.

The screenshot shows the 'Create a virtual machine' blade on the 'Basics' tab. At the top, there are three help buttons: 'Help me create a low cost VM', 'Help me create a VM optimized for high availability', and 'Help me choose the right VM size for my workload'. Below these are tabs for 'Basics', 'Disks', 'Networking', 'Management', 'Monitoring', 'Advanced', 'Tags', and 'Review + create'. The 'Basics' tab is selected. A note says 'Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)'.

In the 'Project details' section, there is a note: 'This subscription may not be eligible to deploy VMs of certain sizes in certain regions.' Below this, there are fields for 'Subscription' (set to 'Azure subscription 1') and 'Resource group' (set to '(New) Resource group'). There is also a 'Create new' button. At the bottom of the blade, there are navigation buttons: '< Previous', 'Next : Disks >', and 'Review + create'.

On the right side, there is an 'Activate Windows' section with a link to 'Go to Settings to activate Windows.' and a 'Give feedback' button. The bottom of the screen shows the Windows taskbar with various pinned icons.

3. On the **Basics** tab of the **Create a virtual machine** blade, specify the following settings (leave others with their default values):

Week 8 Assignment 2: Network Security Groups and Application Security Groups

Setting	Value
Subscription	the name of the Azure subscription you will be using
Resource group	AZ500LAB07
Virtual machine name	myVmWeb
Region	(US)East US
Image	Windows Server 2022 Datacenter: Azure Edition
Size	Standard D2s v3
Username	Student
Password	Please create your own password and record it for subsequent labs
Confirm password	Retype your password
Public inbound ports	None
Would you like to use an existing Windows Server License	No

Note: For public inbound ports, we will rely on the precreated NSG.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The user is currently on the 'Inbound port rules' configuration page. In the 'Public inbound ports' section, the 'None' option is selected. A note below states: 'All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.' Navigation buttons at the bottom of the form include '< Previous', 'Next : Disks >', and 'Review + create'. The top of the screen shows the Azure navigation bar and a Copilot button.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * None Allow selected ports

Select inbound ports

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

< Previous Next : Disks > Review + create

- Click **Next: Disks >** and, on the **Disks** tab of the **Create a virtual machine** blade, set the **OS disk type** to **Standard HDD** and click **Next: Networking >**.

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

VM disk encryption

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host

Encryption at host is not registered for the selected subscription. [Learn more](#)

OS disk

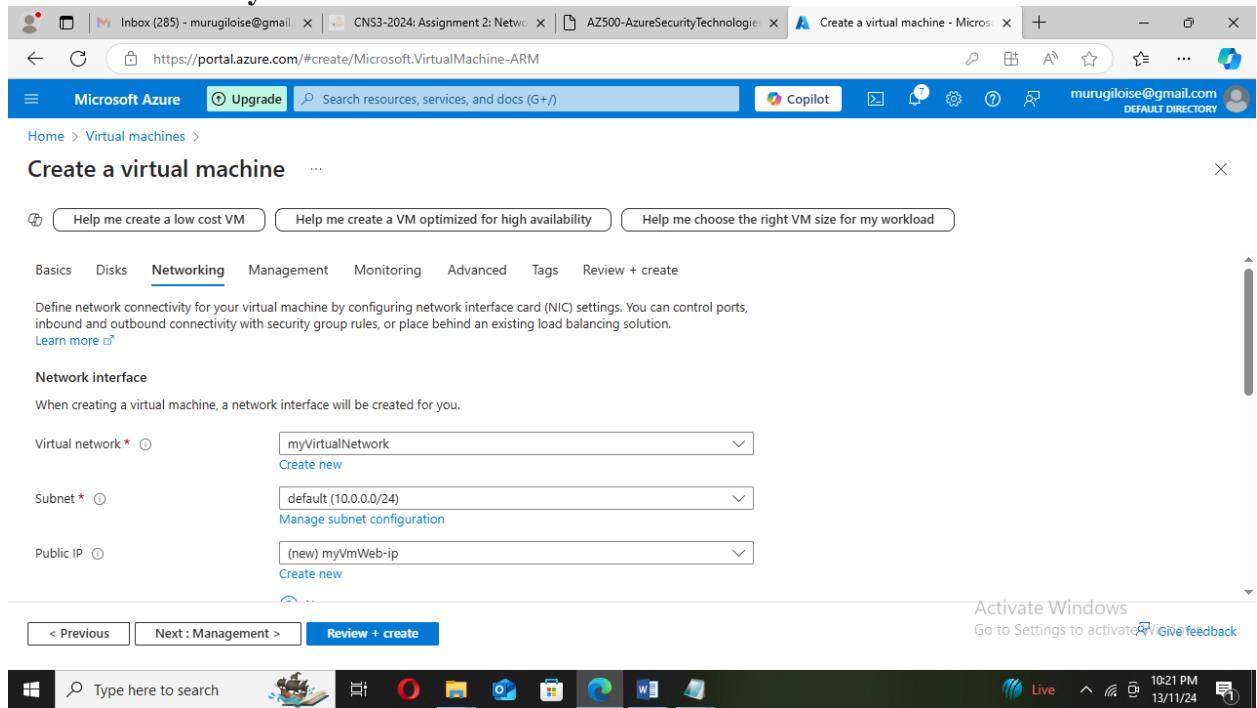
OS disk size Image default (127 GiB)

OS disk type * Standard HDD (locally-redundant storage)

< Previous Next : Networking > Review + create

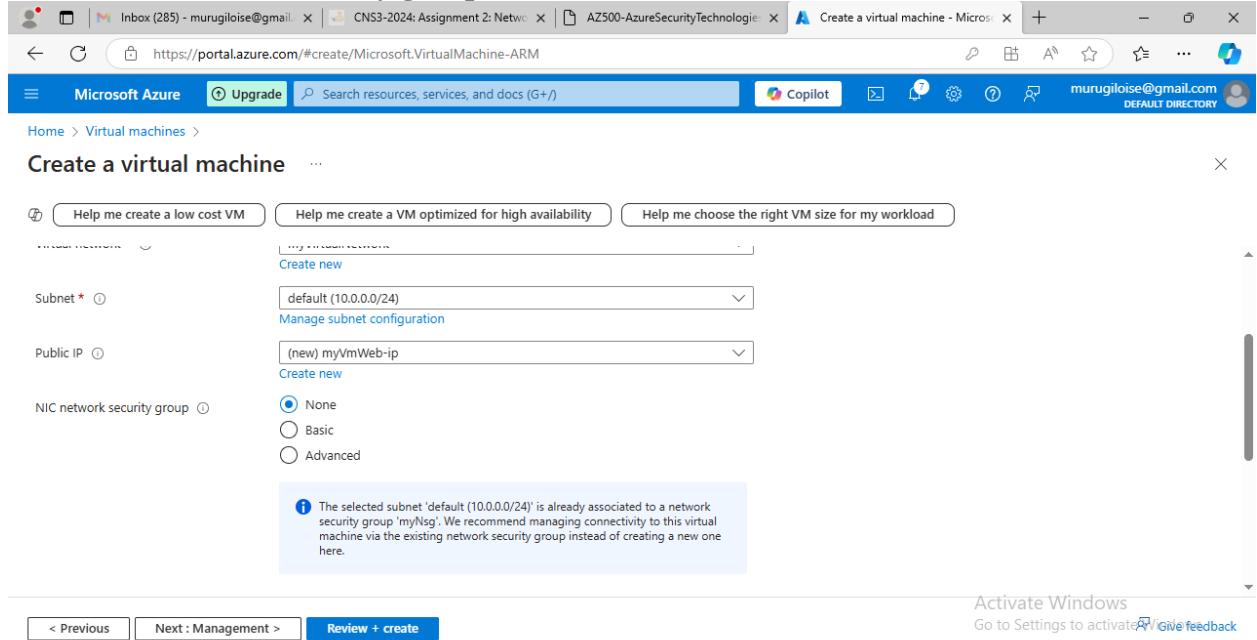
Week 8 Assignment 2: Network Security Groups and Application Security Groups

5. On the Networking tab of the Create a virtual machine blade, select the previously created network myVirtualNetwork.



The screenshot shows the 'Create a virtual machine' blade in the Azure portal. The 'Networking' tab is active. Under 'Network interface', the 'Virtual network' dropdown is set to 'myVirtualNetwork'. The 'Subnet' dropdown is set to 'default (10.0.0.0/24)'. The 'Public IP' dropdown is set to '(new) myVmWeb-ip'. In the 'NIC network security group' section, the 'None' radio button is selected. A tooltip message at the bottom right of this section states: 'The selected subnet 'default (10.0.0.0/24)' is already associated to a network security group 'myNSg'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.' At the bottom of the blade, there are 'Review + create' and 'Next : Management >' buttons.

6. Under NIC network security group select None.



The screenshot shows the 'Create a virtual machine' blade in the Azure portal. The 'Networking' tab is active. Under 'Network interface', the 'Virtual network' dropdown is set to 'myVirtualNetwork'. The 'Subnet' dropdown is set to 'default (10.0.0.0/24)'. The 'Public IP' dropdown is set to '(new) myVmWeb-ip'. In the 'NIC network security group' section, the 'None' radio button is selected. A tooltip message at the bottom right of this section states: 'The selected subnet 'default (10.0.0.0/24)' is already associated to a network security group 'myNSg'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.' At the bottom of the blade, there are 'Review + create' and 'Next : Management >' buttons. The status bar at the bottom shows 'Activate Windows Go to Settings to activate' and 'Give feedback'.

7. Click Next: Management >, then click Next: Monitoring >. On the Monitoring tab of the Create a virtual machine blade, verify the following setting:

Week 8 Assignment 2: Network Security Groups and Application Security Groups

Setting	Value
Boot diagnostics	Enabled with managed storage account (recommended)

The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The user is on the 'Monitoring' step of the wizard. In the 'Diagnostics' section under 'Boot diagnostics', the radio button for 'Enable with managed storage account (recommended)' is selected. Other options like 'Enable with custom storage account' and 'Disable' are available but not selected. The portal header shows the user's email (murugiloise@gmail.com) and the title 'Create a virtual machine - Microsoft Virtual Machine - ARM'. The bottom of the screen shows the Windows taskbar with various pinned icons and system status information.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

- Click **Review + create**, on the **Review + create** blade, ensure that validation was successful and click **Create**. VM has been successfully deployed.

The screenshot shows the Azure portal interface for a completed VM deployment. The main title is "CreateVm-MicrosoftWindowsServer.WindowsServer-202-20241113220802 | Overview". A summary message says "Your deployment is complete". Deployment details include a name, subscription, start time, and correlation ID. Below are sections for "Deployment details" (auto-shutdown, monitor health, run a script) and "Next steps". Buttons for "Go to resource" and "Create another VM" are present. On the right, there are promotional cards for "Cost Management", "Microsoft Defender for Cloud", and "Free Microsoft tutorials". The taskbar at the bottom shows various icons and the date/time as 10:29 PM, 13/11/24.

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

In this task, you will create a virtual machine to use as a management server.

- In the Azure portal, navigate back to the **Virtual machines** blade, click **+ Create**, and, in the dropdown list, click **+ Azure virtual machine**.

The screenshot shows the "Create a virtual machine" blade in the Azure portal. The title is "Create a virtual machine". It includes tabs for "Help me create a low cost VM", "Help me create a VM optimized for high availability", and "Help me choose the right VM size for my workload". The "Basics" tab is selected. A note says "This subscription may not be eligible to deploy VMs of certain sizes in certain regions." The "Project details" section allows selecting a subscription and resource group. At the bottom, buttons for "< Previous", "Next : Disks >", "Review + create", and "Activate Windows" (with a link to settings) are visible. The taskbar at the bottom shows various icons and the date/time as 10:32 PM, 13/11/24.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

2. On the **Basics** tab of the **Create a virtual machine** blade, specify the following settings (leave others with their default values):

Setting	Value
Subscription	the name of the Azure subscription you will be using in the lab
Resource group	AZ500LAB07
Virtual machine name	myVMMgmt
Region	(US)East US
Image	Windows Server 2022 Datacenter: Azure Edition - x64
Size	Standard D2s v3
Username	Student
Password	Please use your personal password created in Lab 02 > 3.
Public inbound ports	None
Already have a Windows Server license	No

Note: For public inbound ports, we will rely on the precreated NSG.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

The screenshot shows the Microsoft Azure portal interface for creating a virtual machine. The top navigation bar includes links for 'Inbox (285) - murugiloise@gmail.com', 'CNS3-2024: Assignment 2: Netwo...', 'AZ500-AzureSecurityTechnologie...', 'Create a virtual machine - Microsoft...', and several other tabs. The main content area is titled 'Create a virtual machine'. It has three buttons at the top: 'Help me create a low cost VM', 'Help me create a VM optimized for high availability', and 'Help me choose the right VM size for my workload'. Below these are fields for 'Size' (selected: 'Standard_D2s_v3 - 2 vcpus, 8 GiB memory (\$152.57/month)'), 'Administrator account' (username: 'Student'), and 'Inbound port rules'. At the bottom, there are buttons for '< Previous', 'Next : Disks >', and 'Review + create'.

- Click Next: Disks > and, on the Disks tab of the Create a virtual machine blade, set the OS disk type to Standard HDD and click Next: Networking >.

This screenshot continues from the previous one, showing the 'Networking' tab of the 'Create a virtual machine' blade. The 'Networking' tab is highlighted with a blue underline. Below it, there's a note about defining network connectivity. The 'Network interface' section shows the configuration: 'Virtual network' is set to 'myVirtualNetwork' (with a 'Create new' option), 'Subnet' is 'default (10.0.0.0/24)' (with a 'Manage subnet configuration' link), and 'Public IP' is '(new) myVMVmgt-ip' (with a 'Create new' link). At the bottom, there are buttons for '< Previous', 'Next : Management >', and 'Review + create'.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

4. On the **Networking** tab of the **Create a virtual machine** blade, select the previously created network **myVirtualNetwork**.

The screenshot shows the Azure portal's 'Create a virtual machine' blade. The 'Networking' tab is active. In the 'Network interface' section, the 'Virtual network' is set to 'myVirtualNetwork'. The 'Subnet' is set to 'default (10.0.0.0/24)'. The 'Public IP' is set to '(new) myVMmgmt-ip'. Under 'NIC network security group', 'None' is selected. A tooltip at the bottom left of the blade says: 'The selected subnet 'default (10.0.0.0/24)' is already associated to a network'.

5. Under **NIC network security group** select **None**.

The screenshot shows the Azure portal's 'Create a virtual machine' blade. The 'Networking' tab is active. In the 'Network interface' section, the 'Virtual network' is set to 'myVirtualNetwork'. The 'Subnet' is set to 'default (10.0.0.0/24)'. The 'Public IP' is set to '(new) myVMmgmt-ip'. Under 'NIC network security group', 'None' is selected. A tooltip at the bottom left of the blade says: 'The selected subnet 'default (10.0.0.0/24)' is already associated to a network'.

6. Click **Next: Management >**, then click **Next: Monitoring >**. On the **Monitoring** tab of the **Create a virtual machine** blade, verify the following setting:

Week 8 Assignment 2: Network Security Groups and Application Security Groups

Setting	Value
Boot diagnostics	Enabled with managed storage account (recommended)

The screenshot shows the Microsoft Azure portal interface for creating a virtual machine. The URL in the address bar is <https://portal.azure.com/#create/Microsoft.VirtualMachine-ARM>. The top navigation bar includes 'Microsoft Azure', 'Upgrade', a search bar, and various icons. The main content area is titled 'Create a virtual machine' with tabs for Basics, Disks, Networking, Management, Monitoring (which is selected), Advanced, Tags, and Review + create. Under the Monitoring tab, there's a section for 'Configure monitoring options for your VM'. It shows 'Alerts' (checkbox for 'Enable recommended alert rules') and 'Diagnostics' (radio buttons for 'Boot diagnostics'): 'Enable with managed storage account (recommended)' (selected), 'Enable with custom storage account', and 'Disable'. Below that is 'Enable OS guest diagnostics'. At the bottom of the blade are buttons for '< Previous', 'Next : Advanced >', and 'Review + create' (which is highlighted in blue).

- Click **Review + create**, on the **Review + create** blade, ensure that validation was successful and click **Create**.

Note: Wait for both virtual machines to be provisioned before continuing.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

The screenshot shows the Microsoft Azure portal interface. At the top, there are several tabs: 'Inbox (285) - murugiloise@gmail.com', 'CNS3-2024: Assignment 2: Netwo...', 'AZ500-AzureSecurityTechnologie...', 'CreateVm-MicrosoftWindowsServ...', and others. The main title is 'CreateVm-MicrosoftWindowsServer.WindowsServer-201-20241113223418 | Overview'. The left sidebar has 'Deployment' selected, with sub-options 'Overview', 'Inputs', 'Outputs', and 'Template'. The main content area displays a green checkmark icon and the message 'Your deployment is complete'. Deployment details include: Deployment name: CreateVm-MicrosoftWindowsServer.Wi..., Start time: 11/13/2024, 10:45:41 PM; Subscription: Azure subscription 1; Resource group: AZ500LAB07. Below this are sections for 'Deployment details' and 'Next steps', which include links to 'Setup auto-shutdown', 'Monitor VM health, performance and network dependencies', and 'Run a script inside the virtual machine', all marked as 'Recommended'. At the bottom are buttons for 'Go to resource' and 'Create another VM', along with links to 'Give feedback' and 'Tell us about your experience with deployment'.

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

In this task, you will associate each virtual machines network interface with the corresponding application security group. The myVMWeb virtual machine interface will be associated to the myAsgWebServers ASG. The myVMMgmt virtual machine interface will be associated to the myAsgMgmtServers ASG.

1. In the Azure portal, navigate back to the **Virtual machines** blade and verify that both virtual machines are listed with the **Running** status. Both the machines are running successfully.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

The screenshot shows the Microsoft Azure portal interface. The user is on the 'Virtual machines' blade. There are two records listed:

Name	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address
myVMMgmt	Azure subscription 1	AZ500LAB07	West US	Running	Windows	Standard_D2s_v3	40.112.251.105
myVmWeb	Azure subscription 1	AZ500LAB07	West US	Running	Windows	Standard_D2s_v3	40.85.150.192

- In the list of virtual machines, click the **myVmWeb** entry.

The screenshot shows the detailed view of the 'myVmWeb' virtual machine. On the left, there's a navigation menu with options like Overview, Activity log, Tags, Diagnose and solve problems, Connect, Bastion, Windows Admin Center, Networking, Network settings, Load balancing, and Application security groups. The main pane displays the 'Essentials' section with various properties:

- Resource group: AZ500LAB07
- Operating system: Windows (Windows Server 2022 Datacenter)
- Size: Standard D2s v3 (2 vcpus, 8 GiB memory)
- Public IP address: 40.85.150.192
- Virtual network/subnet: myVirtualNetwork/default
- DNS name: Not configured
- Health state: -
- Time created: 11/13/2024, 7:28 PM UTC

- On the **myVMWeb** blade, in the **Networking** section, click **Network settings** and then, on the **myVMWeb | Networking settings** blade, click the **Application security**

Week 8 Assignment 2: Network Security Groups and Application Security Groups

groups tab.

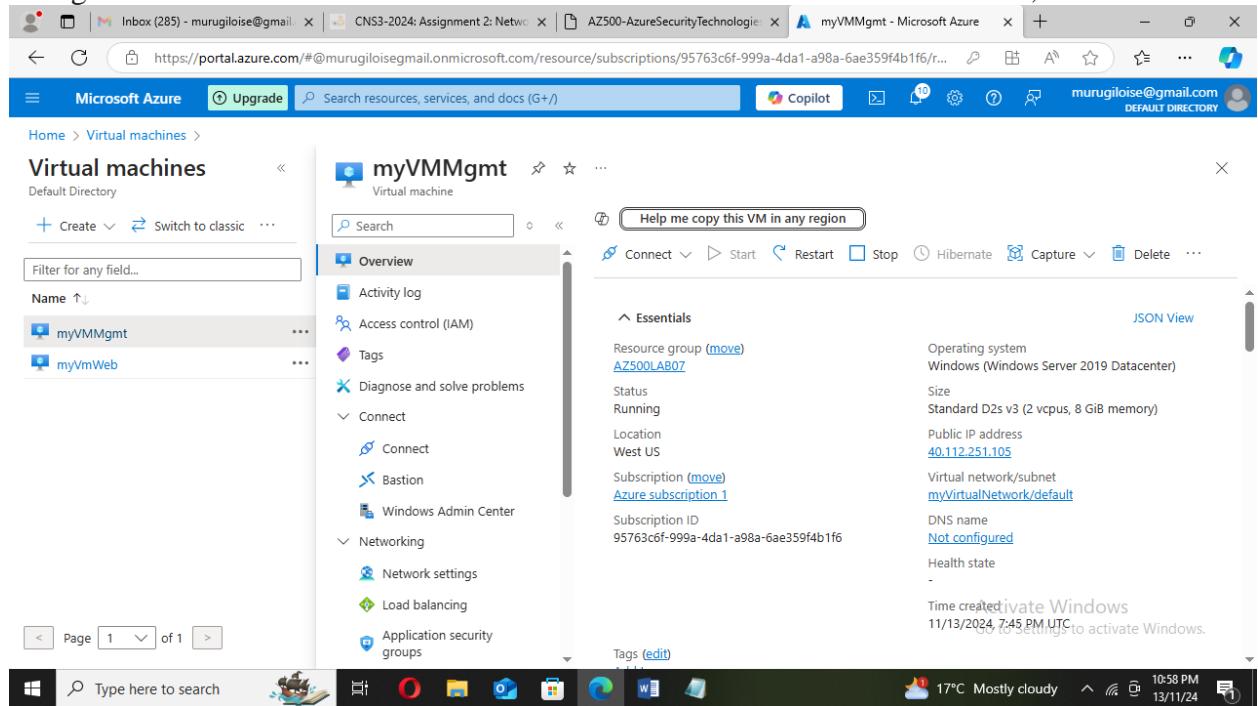
The screenshot shows the Microsoft Azure portal interface. The left sidebar lists 'Virtual machines' with two items: 'myVMgmt' and 'myVmWeb'. The main content area is titled 'myVmWeb | Application security groups'. It features a search bar and a sidebar with options like 'Tags', 'Diagnose and solve problems', 'Connect', 'Networking', and 'Application security groups'. The 'Application security groups' option is currently selected. Below it, there's a message: 'This is a new experience. Please provide feedback'. A section titled 'Network interface / IP configuration' shows 'myvmweb780 (primary) / ipconfig1 (primary)'. A large shield icon is present, and a message states 'No application security groups to display'. A note explains how application security groups can be used to configure network security policies based on VMs. The bottom right corner shows the date and time: '10:52 PM 13/11/24'.

- Click + Add application security groups, in the Application security group list, select myAsgWebServers, and then click Save. We haave successfully added myAsgWebServers .

The screenshot shows the Microsoft Azure portal interface, similar to the previous one but with changes in the application security group list. The 'Application security groups' section now contains a list with one item: 'myAsgWebServers'. To the right, there's a 'Resource group' dropdown set to 'AZ500LAB07'. A message at the bottom right encourages activating Windows: 'Activate Windows Go to Settings to activate Windows.' The bottom right corner shows the date and time: '10:54 PM 13/11/24'.

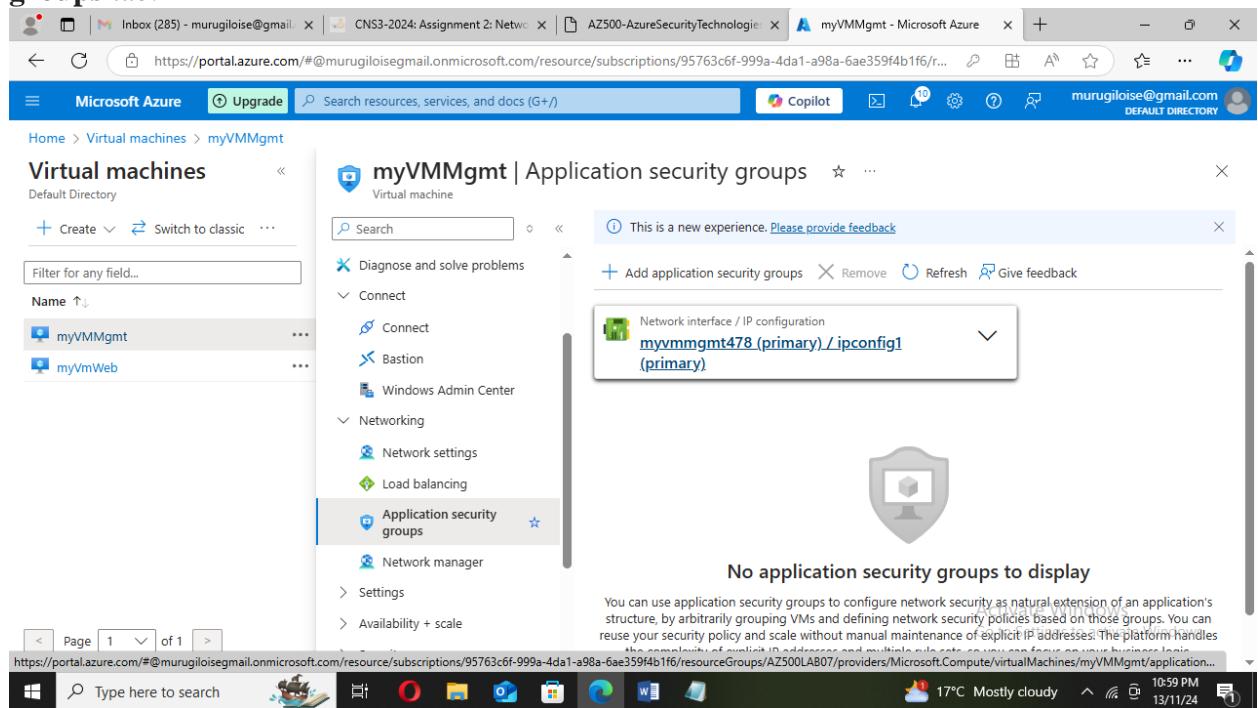
Week 8 Assignment 2: Network Security Groups and Application Security Groups

5. Navigate back to the **Virtual machines** blade and in the list of virtual machines, click



The screenshot shows the Microsoft Azure portal interface. The left sidebar lists 'Virtual machines' under 'Default Directory'. In the main area, a 'myVMMgmt' VM is selected. A context menu is open, and the 'Networking' section is expanded, showing options like 'Connect', 'Bastion', 'Windows Admin Center', 'Networking', 'Network settings', 'Load balancing', and 'Application security groups'. The 'Application security groups' option is highlighted.

6. On the **myVMMgmt** blade, in the **Networking** section, click **Networking settings** and then, on the **myVMMgmt | Networking settings** blade, click the **Application security groups** tab.



The screenshot shows the Microsoft Azure portal interface. The left sidebar lists 'Virtual machines' under 'Default Directory'. In the main area, the 'myVMMgmt' VM is selected. The 'Networking' section is expanded, and the 'Application security groups' tab is selected. A single item, 'myvmmgmt478 (primary) / ipconfig1 (primary)', is listed under 'Network interface / IP configuration'. Below the list, a message states 'No application security groups to display'.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

7. Click + Add application security groups, in the Application security group list, select myAsgMgmtServers, and then click Save.

The screenshot shows the Microsoft Azure portal interface. The user is navigating through the 'Virtual machines' section under 'myVMMgmt'. On the right, a detailed view of an 'Application security group' is displayed. The group is named 'myvmmgmt478 (primary) / ipconfig1 (primary)'. It lists two entries: 'Name' and 'myAsgWebServers'. The 'Resource group' is specified as 'AZ500LAB07'. A message at the top right says 'This is a new experience. Please provide feedback'. Below the main view, there's a search bar and a navigation menu with items like 'Connect', 'Networking', 'Application security groups', and 'Network manager'. The bottom of the screen shows the Windows taskbar with various icons and system status information.

Task 4: Test the network traffic filtering

In this task, you will test the network traffic filters. You should be able to RDP into the myVMMgmt virtual machine. You should be able to connect from the internet to the myVMWeb virtual machine and view the default IIS web page.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

1.

The screenshot shows the Microsoft Azure portal interface. The left sidebar lists 'Virtual machines' with two items: 'myVMMgmt' and 'myVmWeb'. The main content area is titled 'myVMMgmt' and shows the 'Overview' tab selected. The details pane on the right provides information such as the resource group (AZ500LAB07), status (Running), location (West US), subscription (Azure subscription 1), and tags. The public IP address is listed as 40.112.251.105. The 'Connect' button is visible in the top navigation bar and also in the left sidebar under the 'Connect' section.

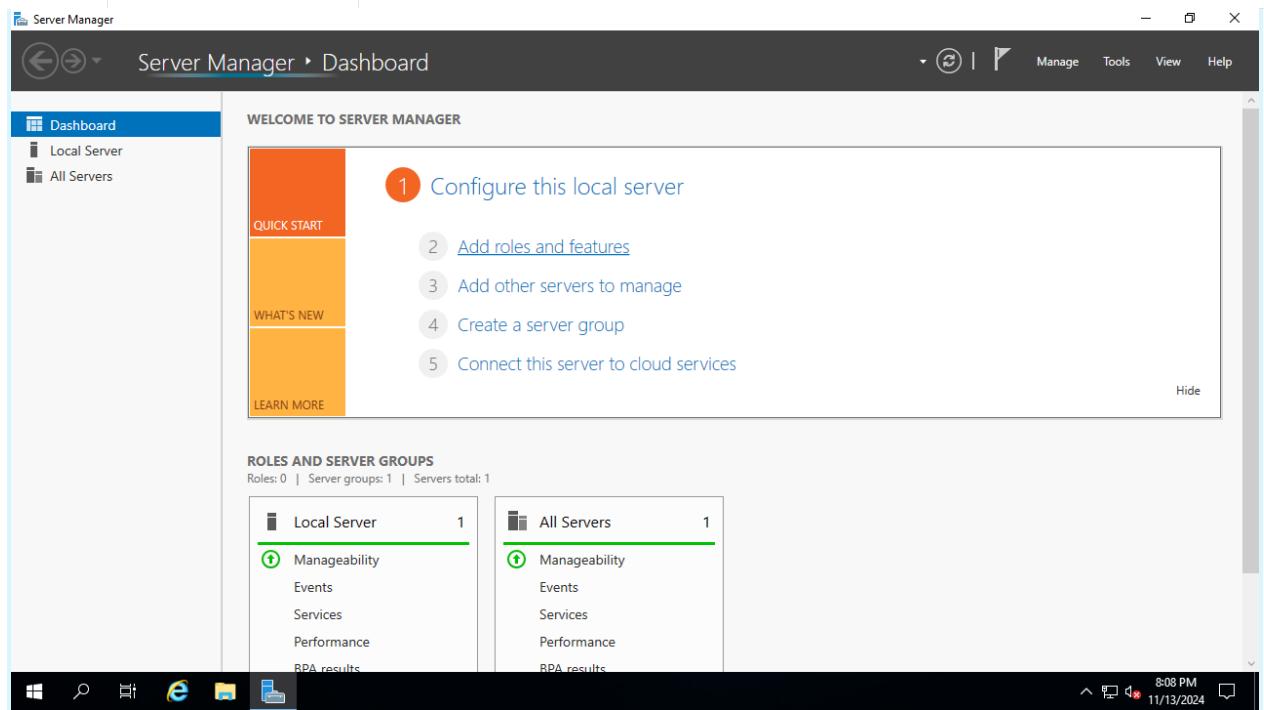
2. On the **myVMMgmt** blade, click **Connect** and, in the drop down menu, click **RDP**.

The screenshot shows the 'myVMMgmt | Connect' blade. The 'Connect' option is selected in the dropdown menu. The 'Native RDP' option is highlighted, showing the connection details: Admin username (Student), Port (3389), and Public IP address (40.112.251.105). The 'Activate Windows' link is visible at the bottom right.

3. Click **Download RDP File** and use it to connect to the **myVMMgmt** Azure VM via Remote Desktop. When prompted to authenticate, provide the following credentials:

Week 8 Assignment 2: Network Security Groups and Application Security Groups

Setting	Value
User name	Student
Password	Please use your personal password created in Lab 02 > Exercise 1 > Task 1 > Step 1



Week 8 Assignment 2: Network Security Groups and Application Security Groups

4.

The screenshot shows the Microsoft Azure portal interface. The left sidebar lists 'Virtual machines' with items 'myVMMgmt' and 'myVmWeb'. The main content area is titled 'myVmWeb | Connect' and shows a 'Search' bar. Under 'Connect', 'Native RDP' is listed as the most common option, with a note: 'Connect via native RDP without any additional software needed. Recommended for testing only.' A public IP address (40.85.150.192) is also provided. The status bar at the bottom shows the date and time as 13/11/24 11:10 PM.

5. On the **myVMWeb** blade, in the **Operations** section, click **Run command** and then click **RunPowerShellScript**.

The screenshot shows the 'Run Command Script' pane for the 'myVmWeb' virtual machine. The left sidebar shows 'Operations' with 'Run command' selected. The main area has a 'PowerShell Script' editor containing the command: 'Install-WindowsFeature -name Web-Server -IncludeManagementTools'. A 'Run' button is visible below the editor. The status bar at the bottom shows the date and time as 13/11/24 11:11 PM.

6. On the **Run Command Script** pane, run the following to install the Web server role on **myVmWeb**:

The command was successfully executed as seen on the image below.

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

Week 8 Assignment 2: Network Security Groups and Application Security Groups

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Virtual machines' blade is open, displaying two VMs: 'myVMMgmt' and 'myVmWeb'. On the right, a 'Run Command Script' blade is active, showing the PowerShell command 'Install-WindowsFeature -name Web-Server -IncludeManagementTools' was run successfully. The output pane shows the results of the command execution.

- In the Azure portal, navigate back to the myVmWeb blade.

The screenshot shows the Microsoft Azure portal interface. The 'Virtual machines' blade is open, and the 'myVmWeb' VM is selected. The 'Overview' tab is active, providing detailed information about the VM, including its resource group, operating system, size, public IP address, virtual network, DNS name, and creation time. The 'Essentials' section also lists these key details.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

8. On the myVMWeb blade, identify the **Public IP address** of the myVmWeb Azure VM.
The Public IP address is 40.85.150.192

The screenshot shows the Microsoft Azure portal interface. The left sidebar lists 'Virtual machines' with two items: 'myVMMgmt' and 'myVmWeb'. The main content area is focused on 'myVmWeb', which is identified as a 'Virtual machine'. A tooltip 'Help me copy this VM in any region' is visible. The 'Essentials' section provides detailed information about the VM, including its Resource group (AZ500LAB07), Operating system (Windows Server 2022 Datacenter), Size (Standard D4s_v3, 8 GiB memory), and Public IP address (40.85.150.192). Other details include Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect (with options for Connect, Bastion, Windows Admin Center), Networking (Network settings, Load balancing, Application security groups), and Subscription information.

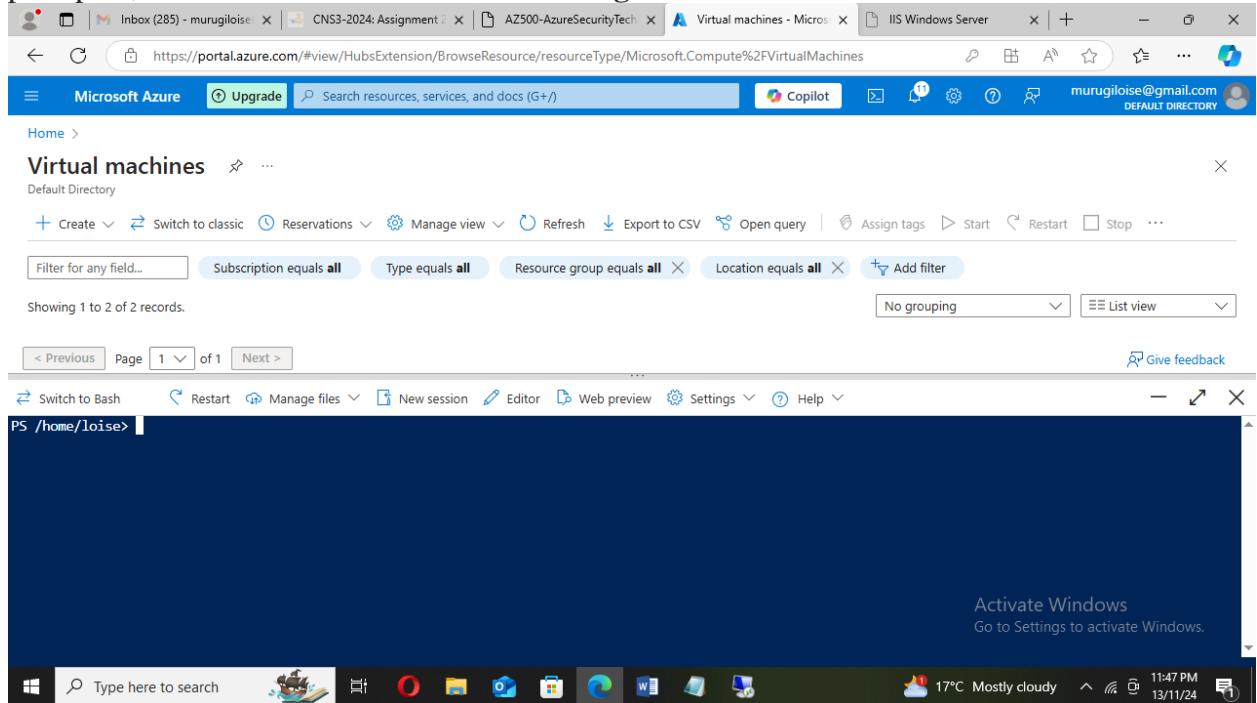
9. Open another browser tab and navigate to IP address you identified in the previous step. From the screenshot below, we were able to access the address 40.85.150.192 of IIS welcome page.

The screenshot shows a web browser window with the URL '40.85.150.192' in the address bar. The page title is 'Windows Server' and the main content is 'Internet Information Services'. The page features a large grid of colored squares, each containing a different language's greeting for 'Welcome' (e.g., 'Welcome', 'Bienvenue', 'Tervetuloa', etc.). At the bottom right, there is a link to 'Activate Windows' with the sub-instruction 'Go to Settings to activate Windows.' The browser's taskbar at the bottom shows other open tabs related to the assignment.

Week 8 Assignment 2: Network Security Groups and Application Security Groups

Clean up resources

1. Open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, select **PowerShell** and **Create storage**.



2. Ensure **PowerShell** is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.
3. In the PowerShell session within the Cloud Shell pane, run the following to remove the resource group you created in this lab:

```
Remove-AzResourceGroup -Name "AZ500LAB07" -Force -AsJob
```

Week 8 Assignment 2: Network Security Groups and Application Security Groups

The screenshot shows the Microsoft Azure portal interface. At the top, there are several tabs: 'Inbox (285) - murugiloise', 'CNS3-2024: Assignment 2', 'AZ500-AzureSecurityTech', 'Virtual machines - Micros', and 'IIS Windows Server'. Below the tabs, the URL is https://portal.azure.com/#view/HubsExtension/BrowseResource/resourceType/Microsoft.Compute%2FVirtualMachines. The main navigation bar includes 'Microsoft Azure', 'Upgrade', a search bar ('Search resources, services, and docs (G+)'), and various icons for Copilot, Mail, Notifications, Settings, and Help. The user 'murugiloise@gmail.com' is logged in.

The main content area is titled 'Virtual machines' with a 'Default Directory' dropdown. It features a toolbar with 'Create', 'Switch to classic', 'Reservations', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', 'Assign tags', 'Start', 'Restart', and 'Stop' buttons. Below the toolbar are filter options: 'Filter for any field...', 'Subscription equals all', 'Type equals all', 'Resource group equals all', 'Location equals all', and 'Add filter'. A message 'Showing 1 to 2 of 2 records.' is displayed. On the right, there are buttons for 'No grouping' and 'List view'.

At the bottom of the main area, there are links for '< Previous', 'Page 1 of 1', and 'Next >'. To the right of these links is a 'Give feedback' button.

Below the main content area is a PowerShell session window. The command PS /home/loise> Remove-AzResourceGroup -Name "AZ500LAB07" -Force -AsJob is run. The output table shows one resource group:

ID	Name	PSJobTypeName	State	HasMoreData	Location	Command		
1	Long	Running	0...	AzureLongRunni...	Running	True	localhost	Remove-AzResourceGroup

The PowerShell session ends with PS /home/loise> [REDACTED]

The bottom of the screen shows the Windows taskbar with icons for File Explorer, OneDrive, Mail, Photos, Edge, Microsoft Store, Word, Excel, and Powerpoint. The system tray shows the date (13/11/24), time (11:47 PM), and a notification for USD/RUB +0.25%. An 'Activate Windows' message is also visible.

Conclusion

In this lab activity we have been able to create a virtual network with one subnet, the virtual network is myVirtualNetwork, and set the IPv4 address space to 10.0.0.0/16, with a Subnet default, under the resource group AZ500LAB07 with West US as the region. We then created Application security groups myAsgWebServers and myAsgMgmtServers under the same region AZ500LAB07. We then created network security groups (myNsg) and associated it with myVirtualNetwork. We then created inbound security rules with TCP ports 80 and 443 to the myAsgWebServers application security group, then added another inbound security rule to the myAsgMgmtServers for port 3389 and TCP as the protocol.

We then created a virtual machine to use a web server myVmWeb and management server myVMMgmt under the resource group AZ500LAB07, then associated the virtual machines to the Application security group. Then we successfully did a remote desktop into the myVMMgmt virtual machine. On the myVMWeb we installed the web server role to be able to access myVMWeb via HTTP/HTTPS. On the web browser we were able to access the Public IP which displayed IIS welcome page. From this lab we were able to validate that the NSG and ASG configuration is working and traffic was correctly managed.