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

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

Introduction

In this lab activity we will be using Microsoft azure to implementing 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 server.

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

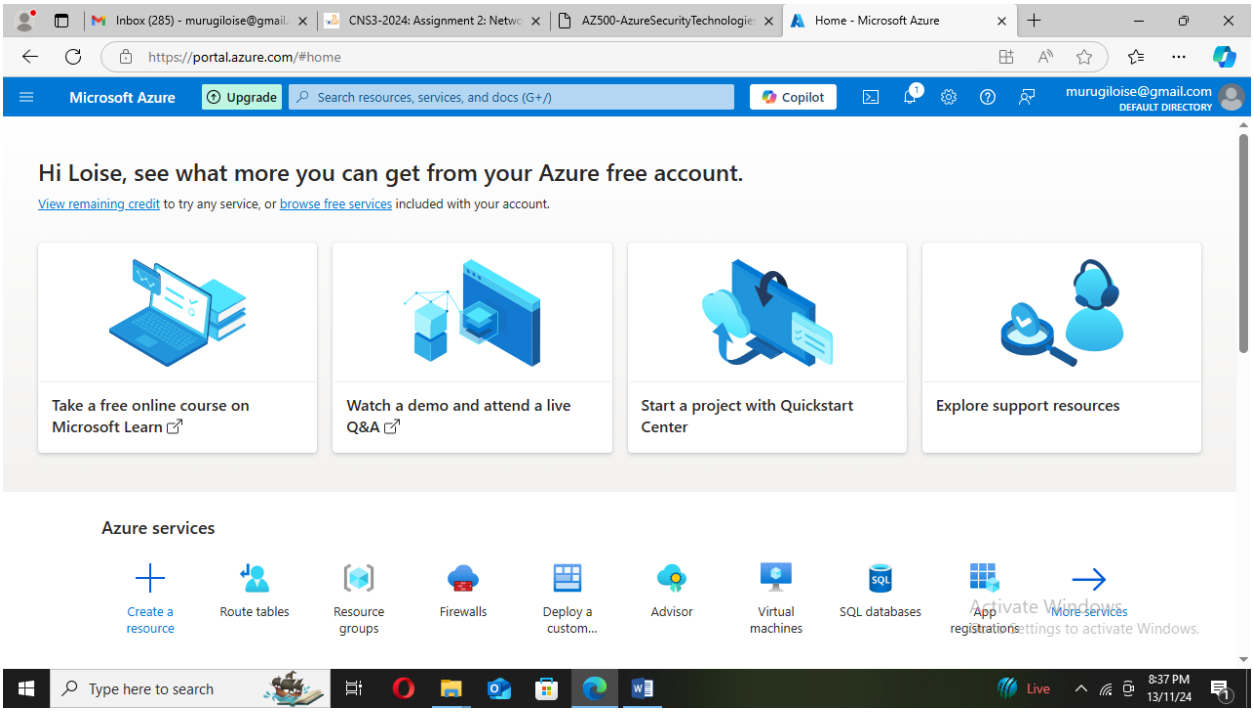
Exercise 1: Create the virtual networking infrastructure

Task 1: Create a virtual network

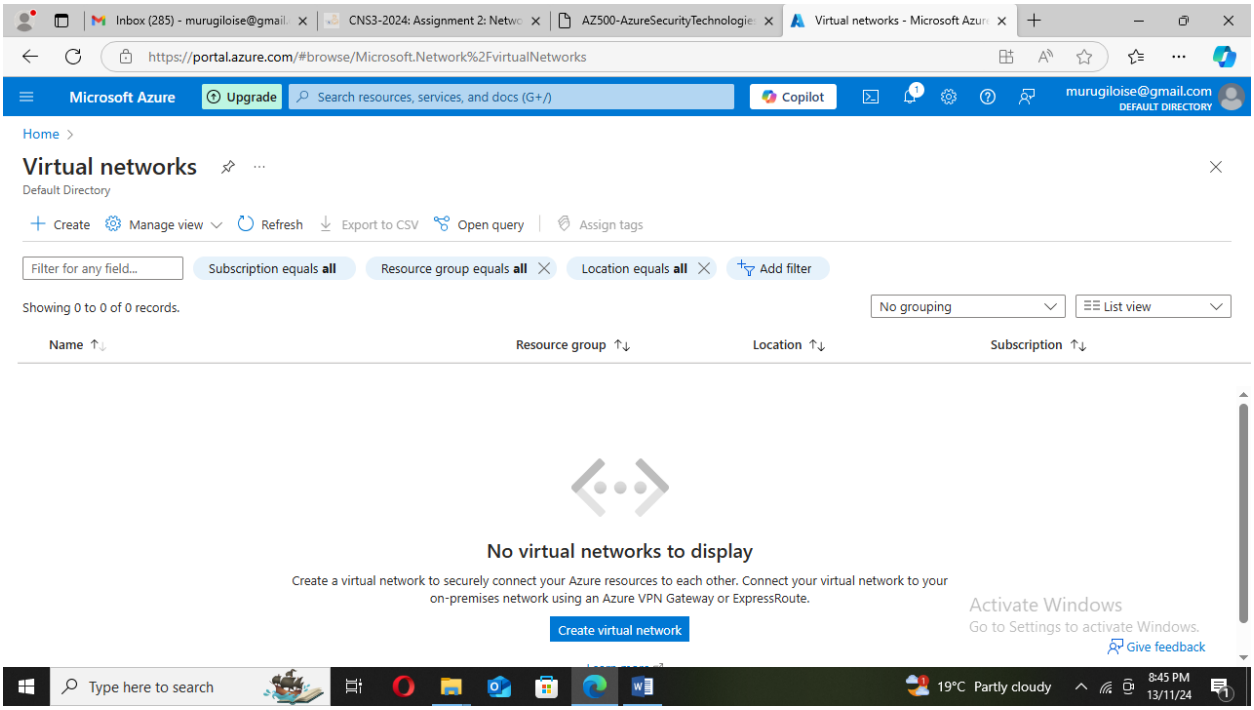
In this task, you will create a virtual network to use with the network and application security groups.

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

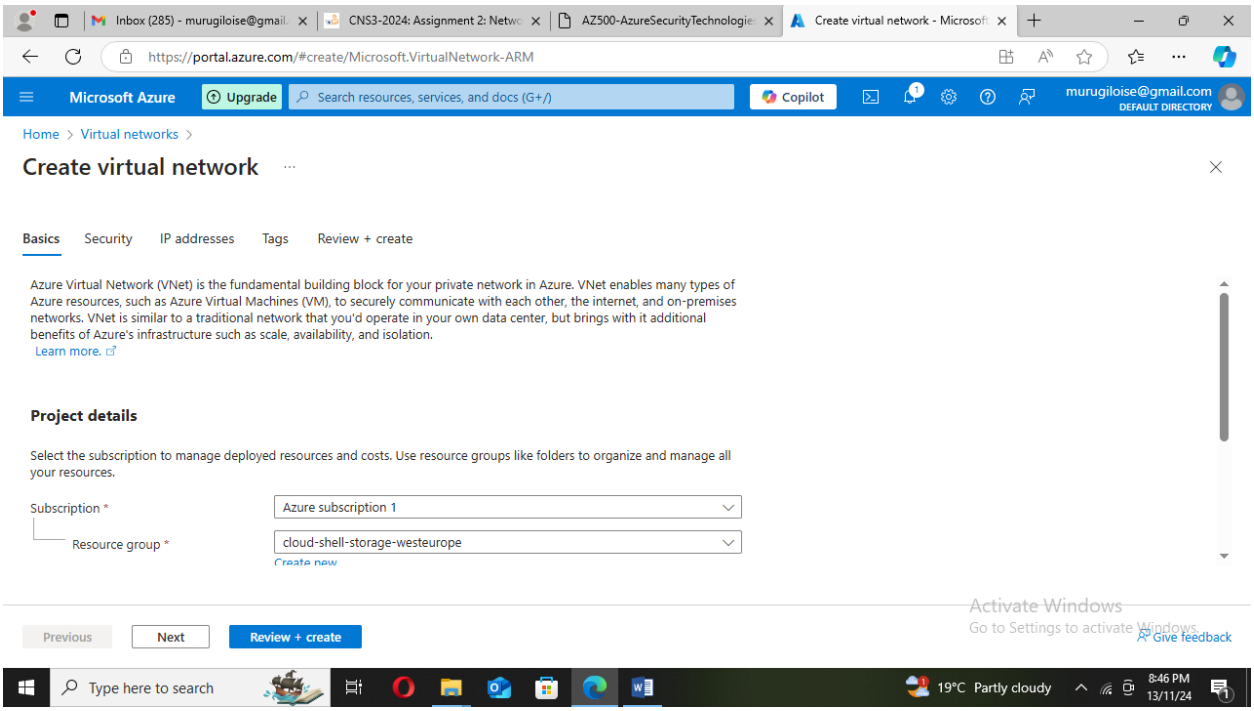
Week 8 Assignment 2: Network Security Groups and Application Security Groups



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.



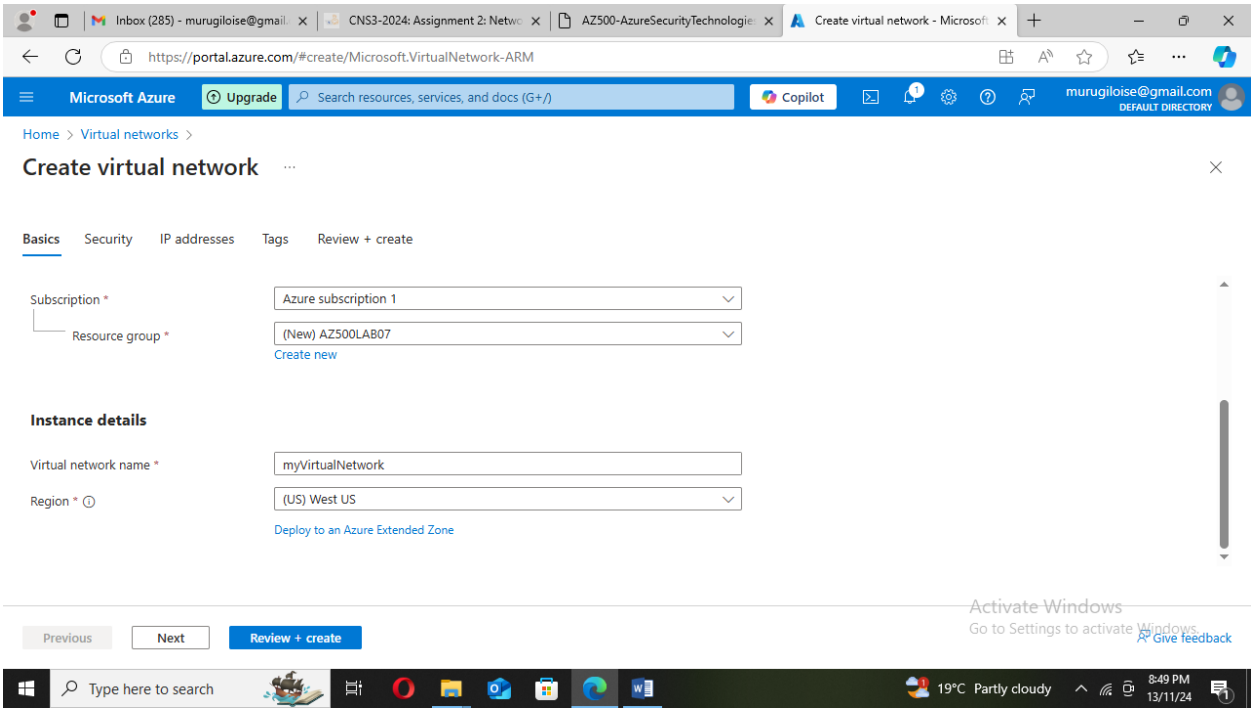
Week 8 Assignment 2: Network Security Groups and Application Security Groups

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**

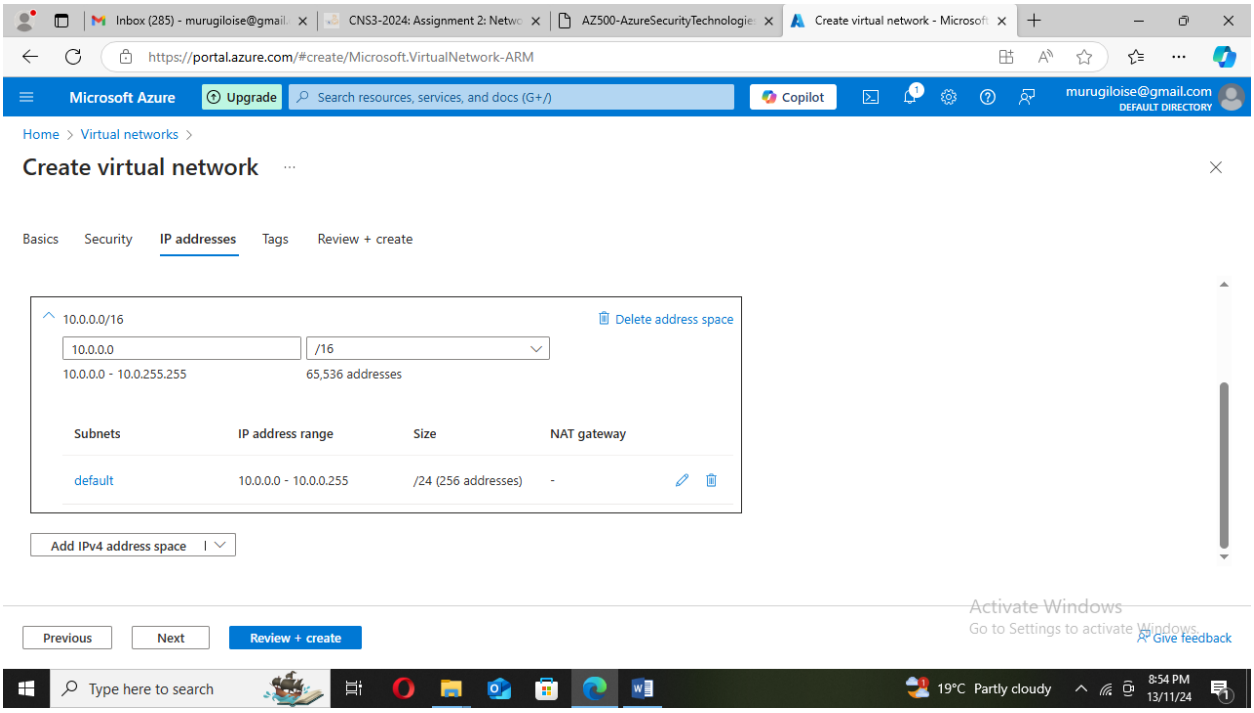
Week 8 Assignment 2: Network Security Groups and Application Security Groups



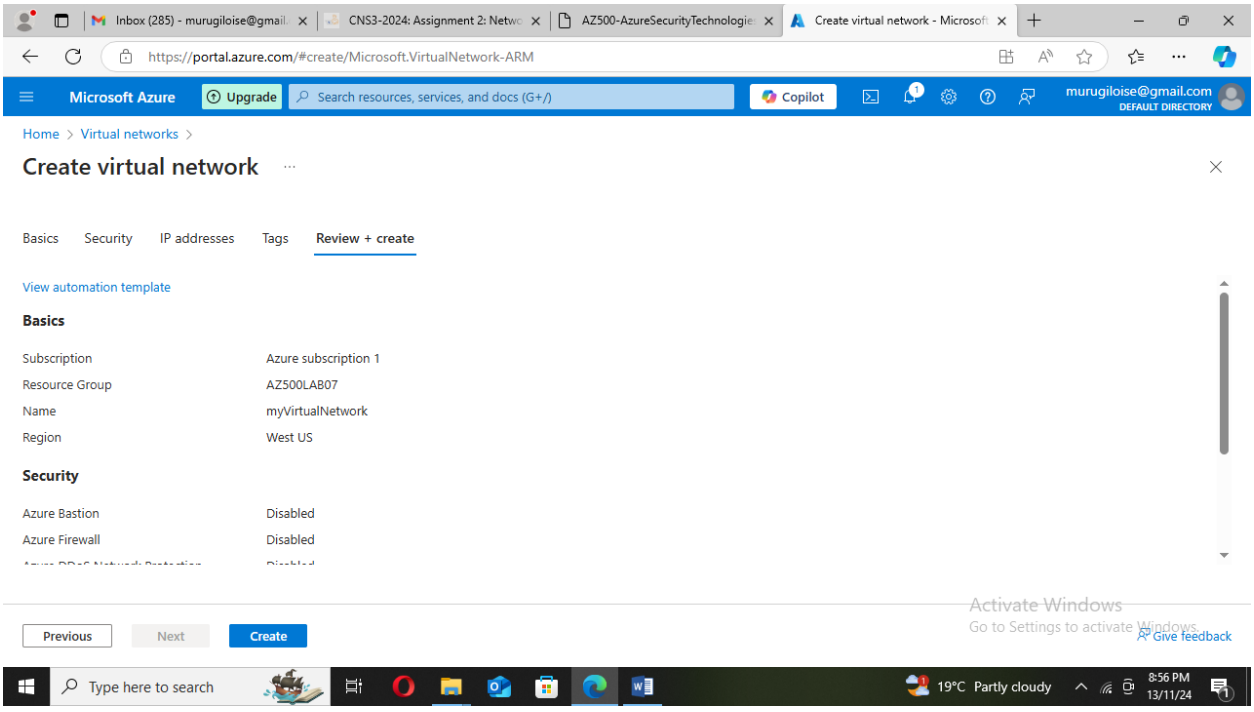
5. On the **IP addresses** tab of the **Create virtual network** blade, set the **IPv4 address space** to **10.0.0.0/16**, and, if needed, in the **Subnet name** column, click **default**, on the **Edit subnet** blade, specify the following settings and click **Save**:

Setting	Value
Subnet name	**default**
Subnet address range	**10.0.0.0/24**

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

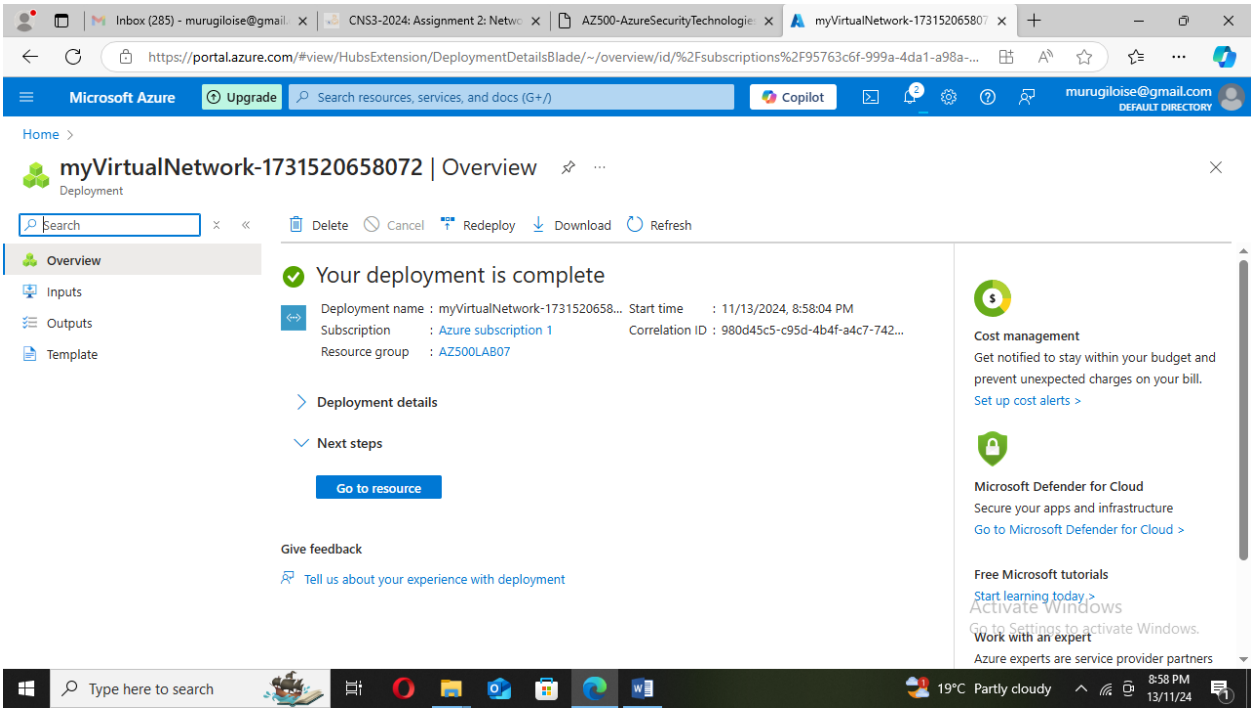


6. Back on the **IP addresses** tab of the **Create virtual network** blade, click **Review + create**.



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.

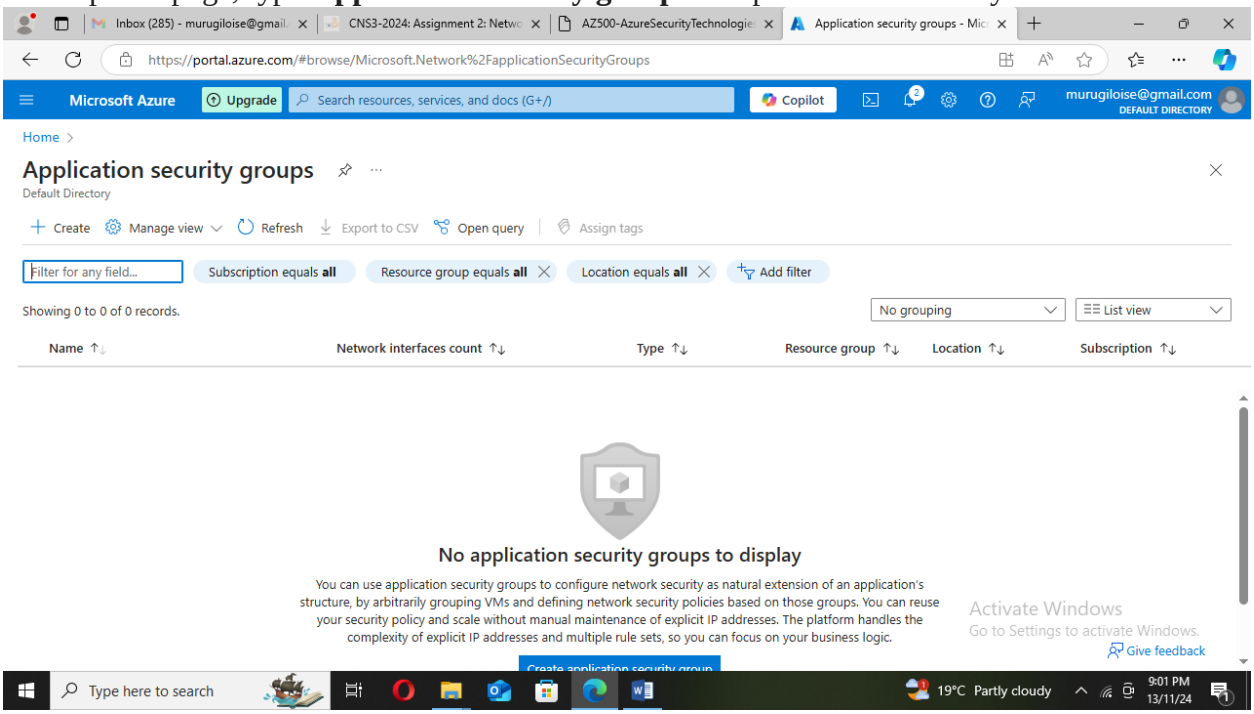
Week 8 Assignment 2: Network Security Groups and Application Security Groups



Task 2: Create application security groups

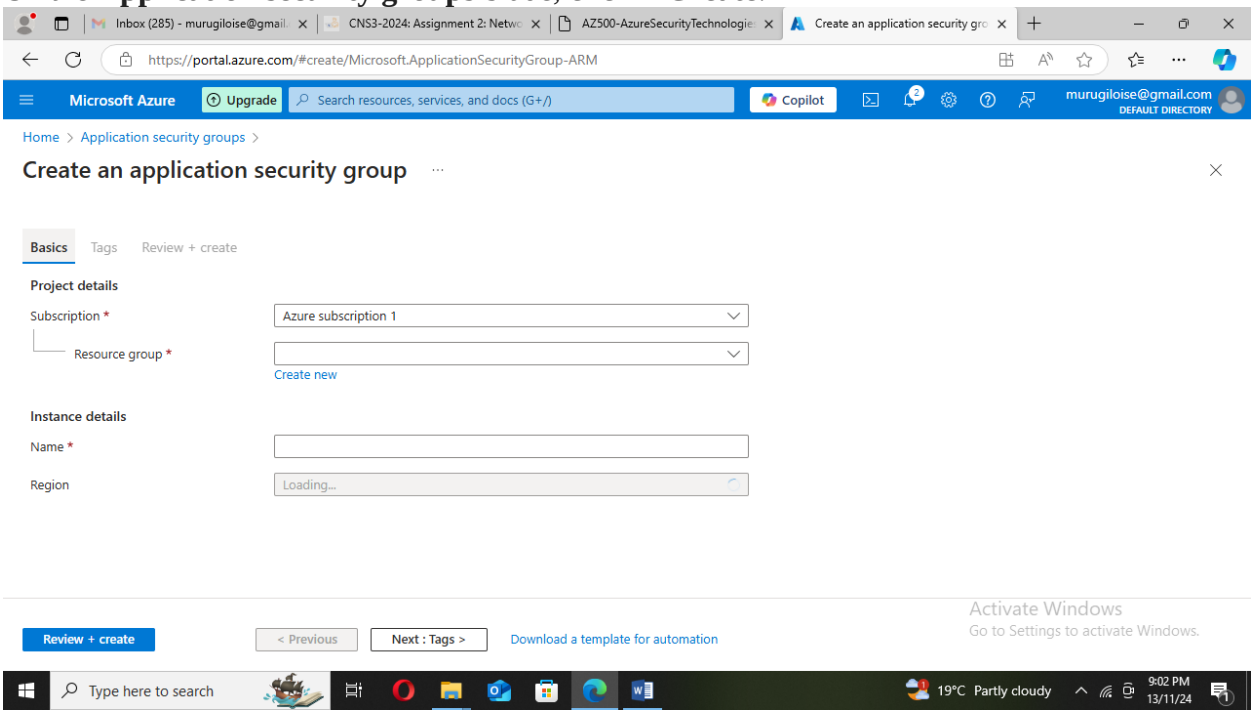
In this task, you will create an application security group.

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.



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

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

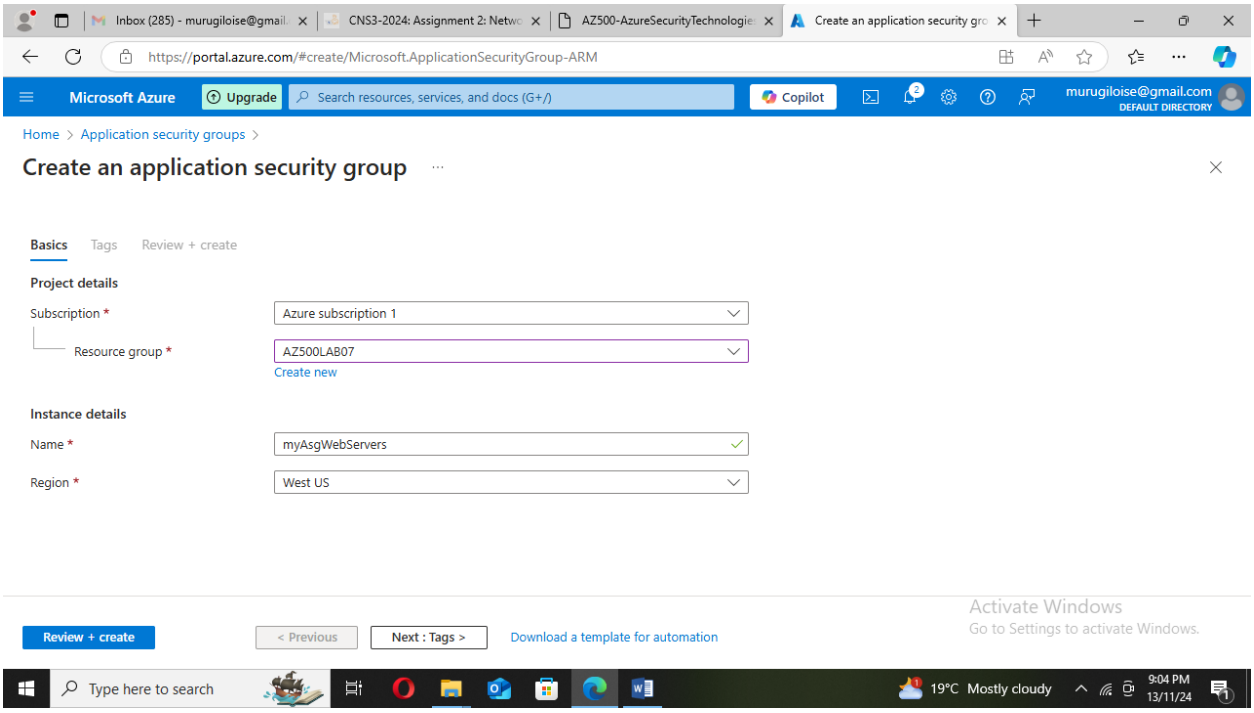


3. On the **Basics** tab of the **Create an application security group** blade, specify the following settings:

Setting	Value
Resource group	**AZ500LAB07**
Name	**myAsgWebServers**
Region	**East US**

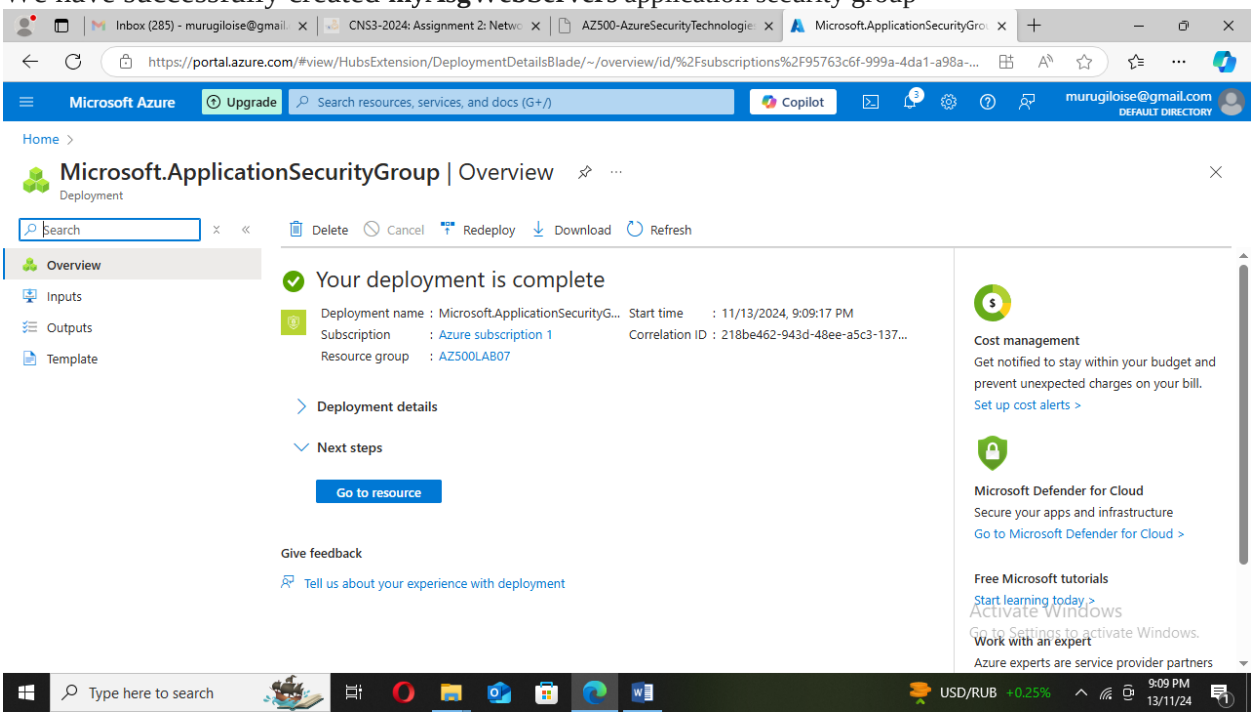
Note: This group will be for the web servers.

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



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

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

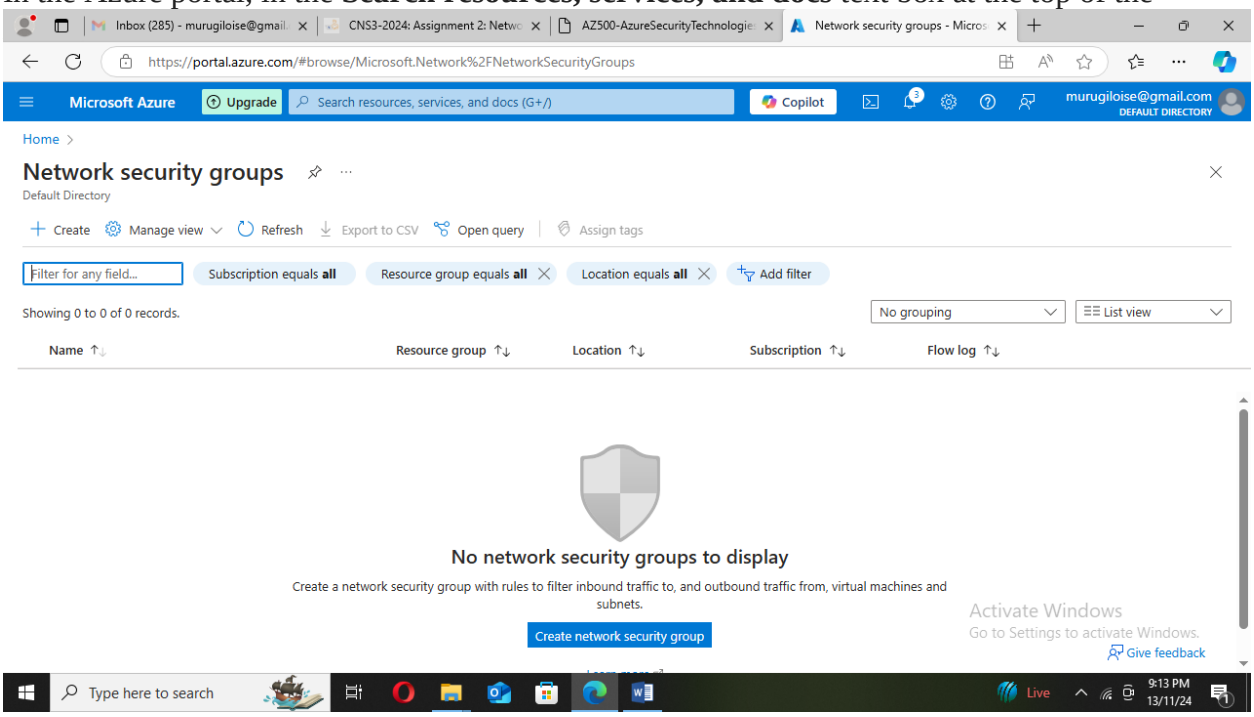


Task 3: Create a network security group and associate the NSG to the subnet

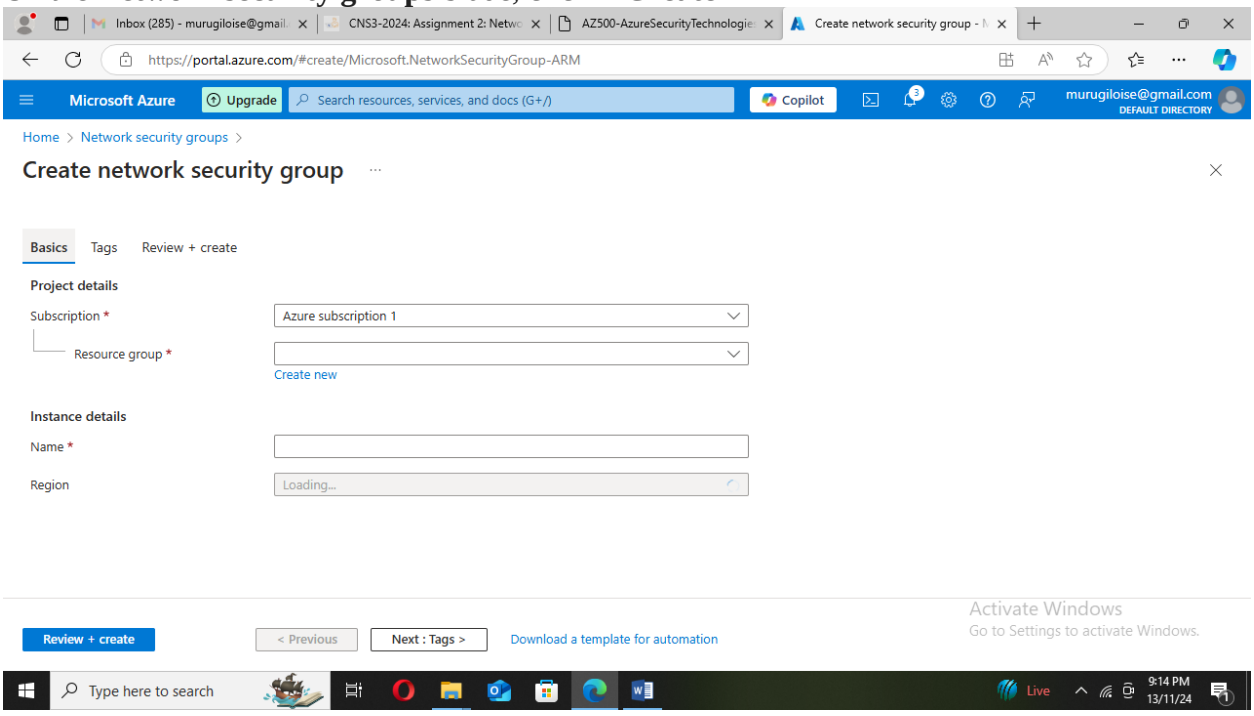
In this task, you will create a network security group.

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



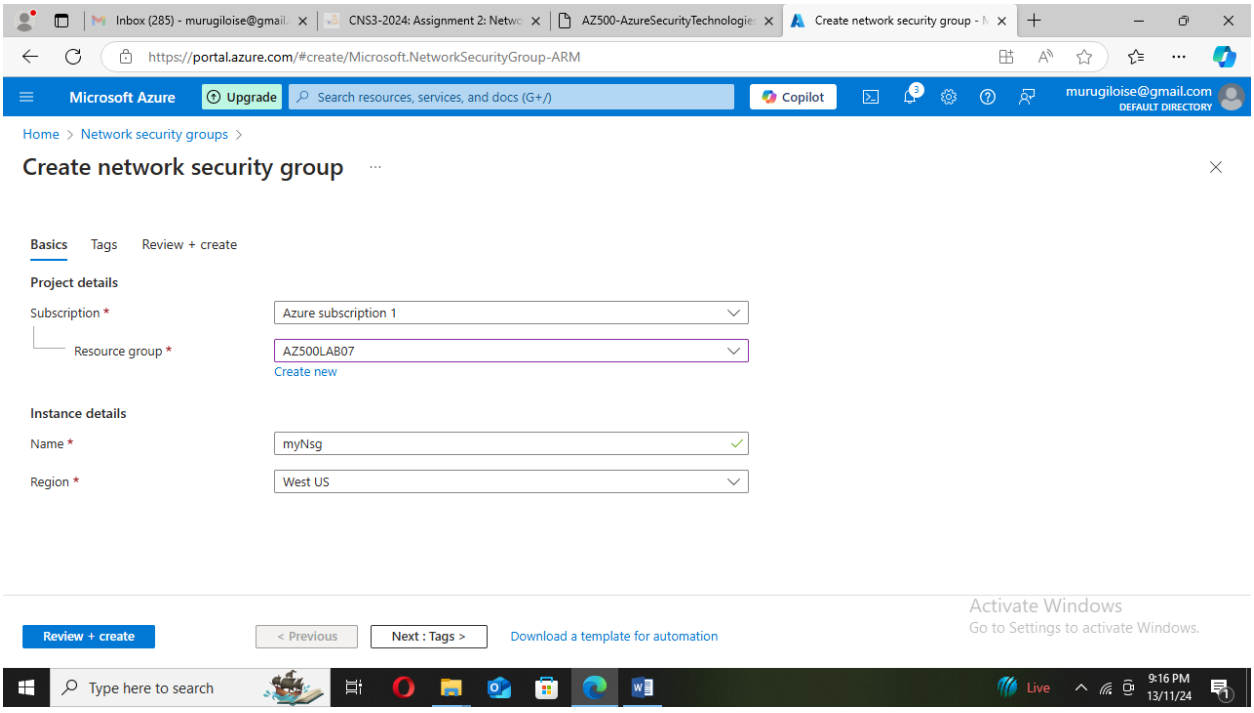
2. On the **Network security groups** blade, click **+ Create**



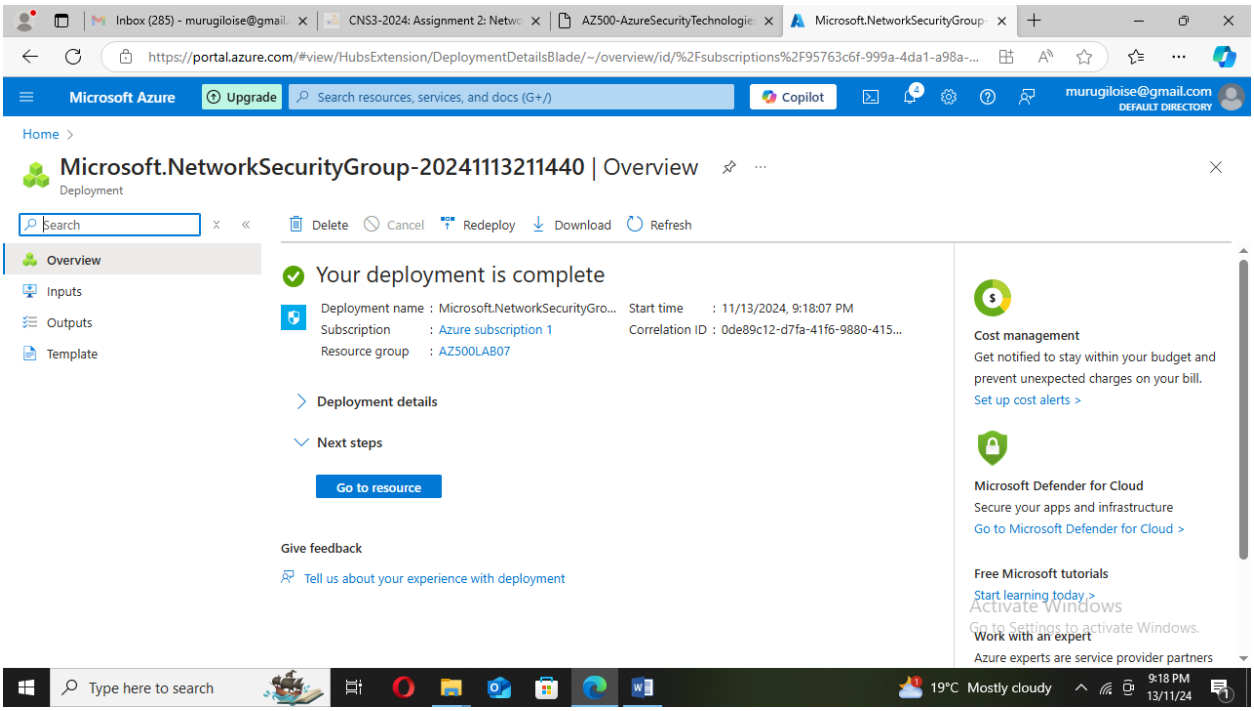
3. On the **Basics** tab of the **Create network security group** blade, specify the following settings:

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

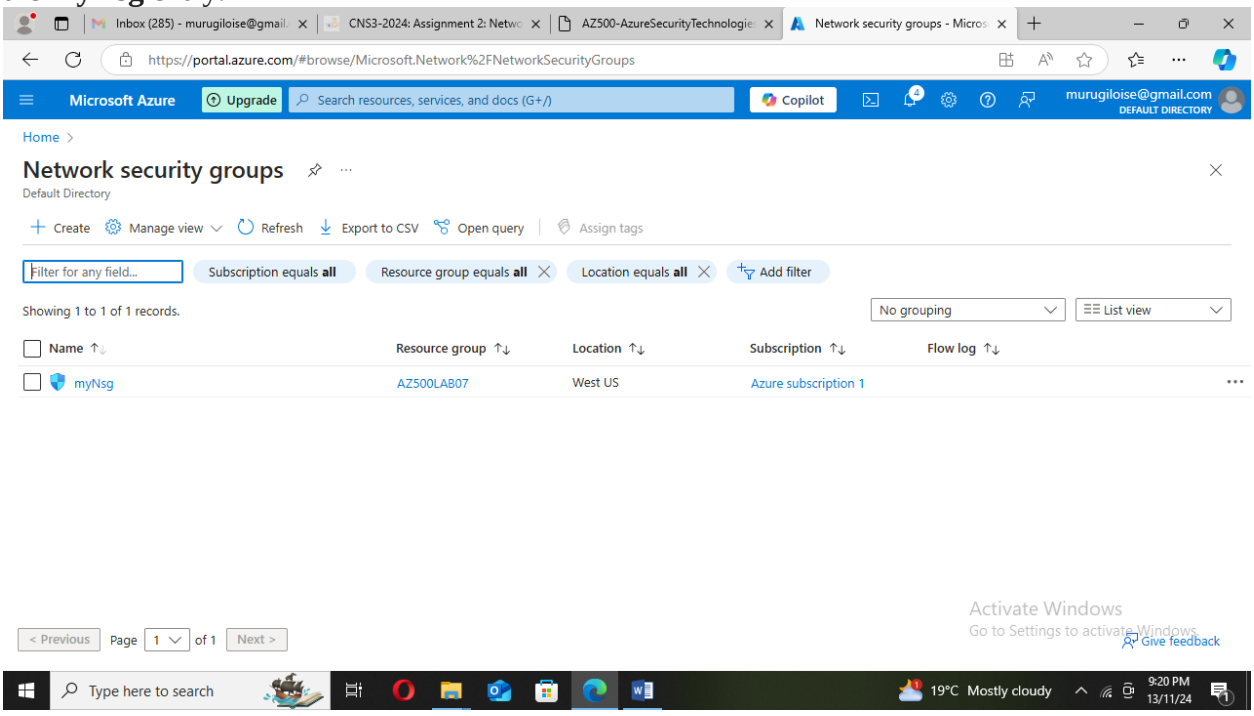
Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	**AZ500LAB07**
Name	**myNsg**
Region	**East US**



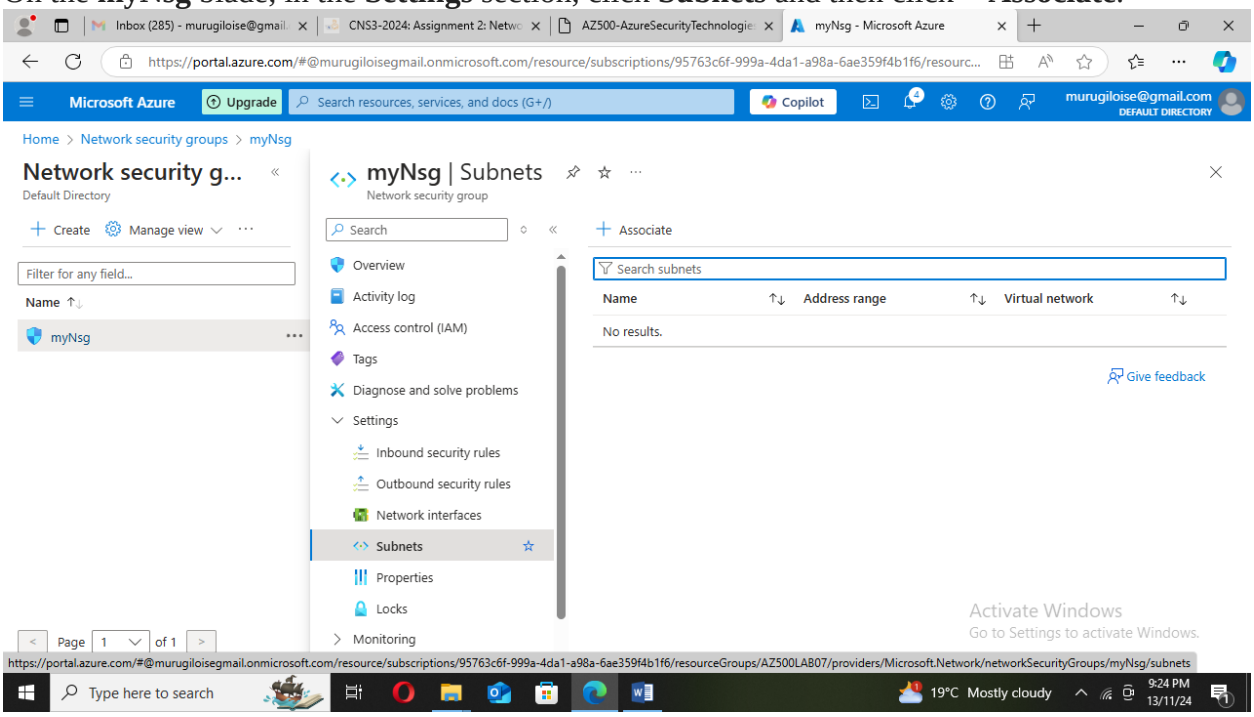
Week 8 Assignment 2: Network Security Groups and Application Security Groups

4. 

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



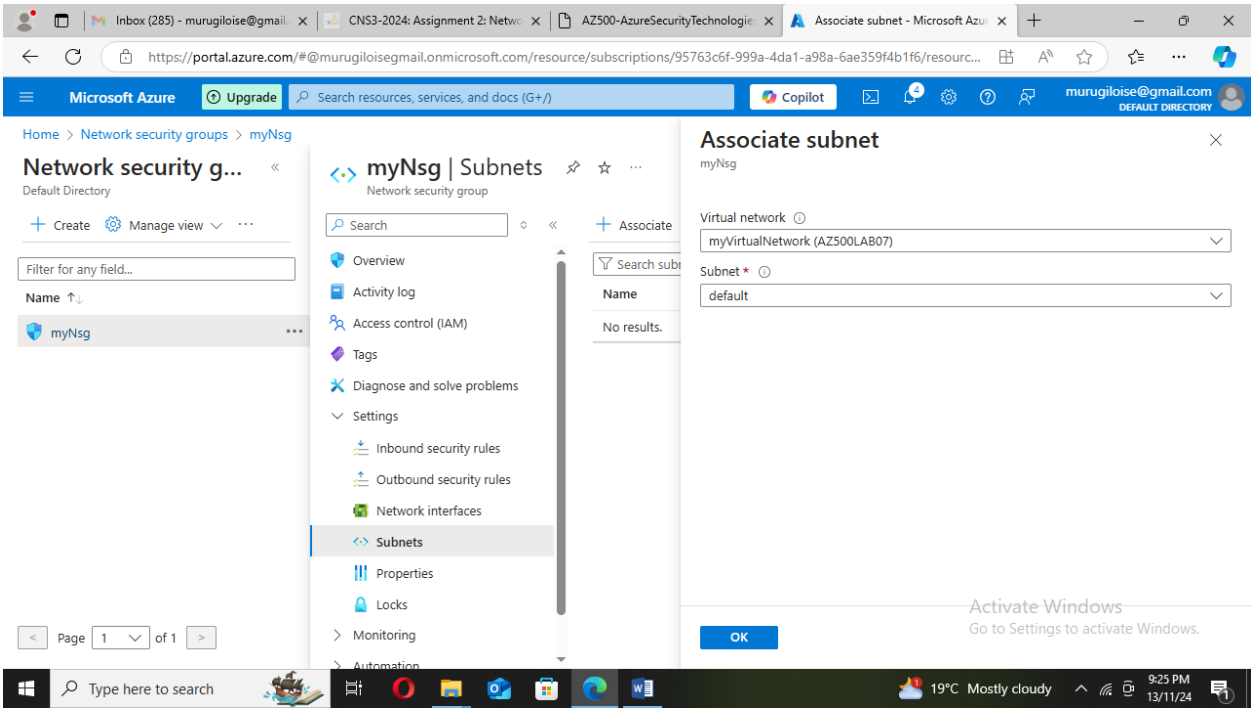
6. On the **myNsg** blade, in the **Settings** section, click **Subnets** and then click **+ Associate**.



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

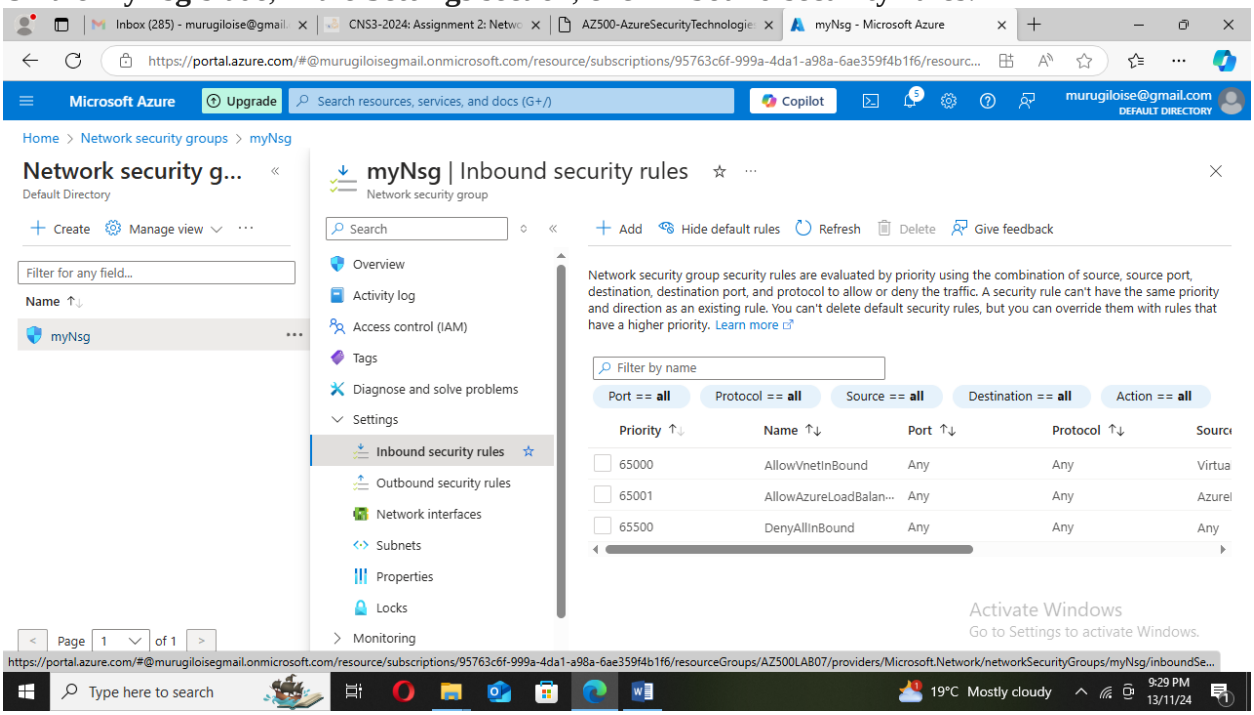
Setting	Value
Virtual network	**myVirtualNetwork**
Subnet	**default**

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



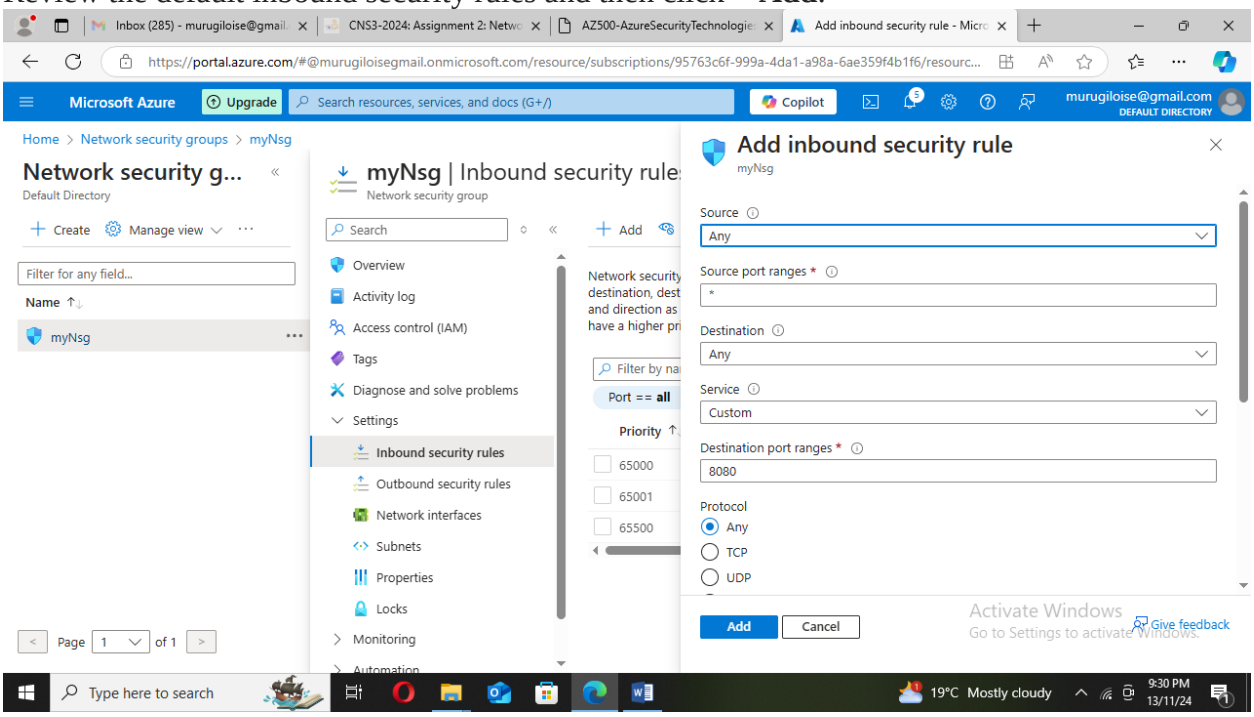
Task 4: Create inbound NSG security rules to all traffic to web servers and RDP to the servers.

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



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

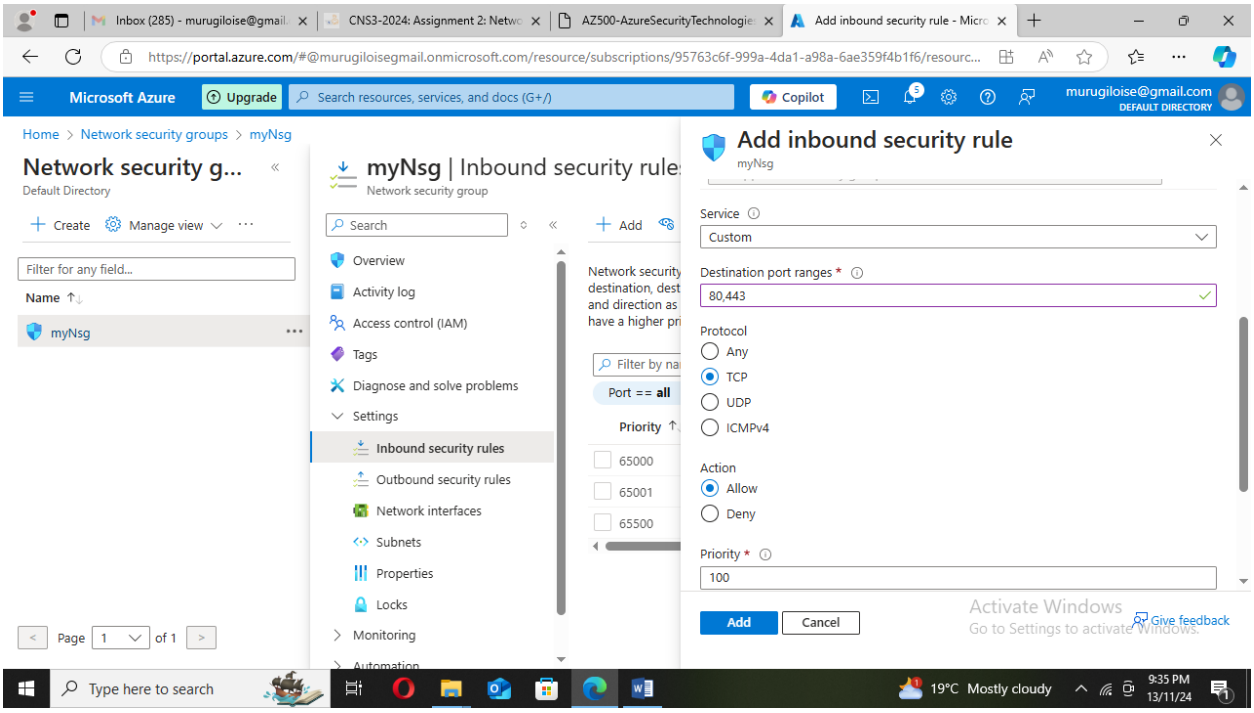
2. Review the default inbound security rules and then click **+ Add**.



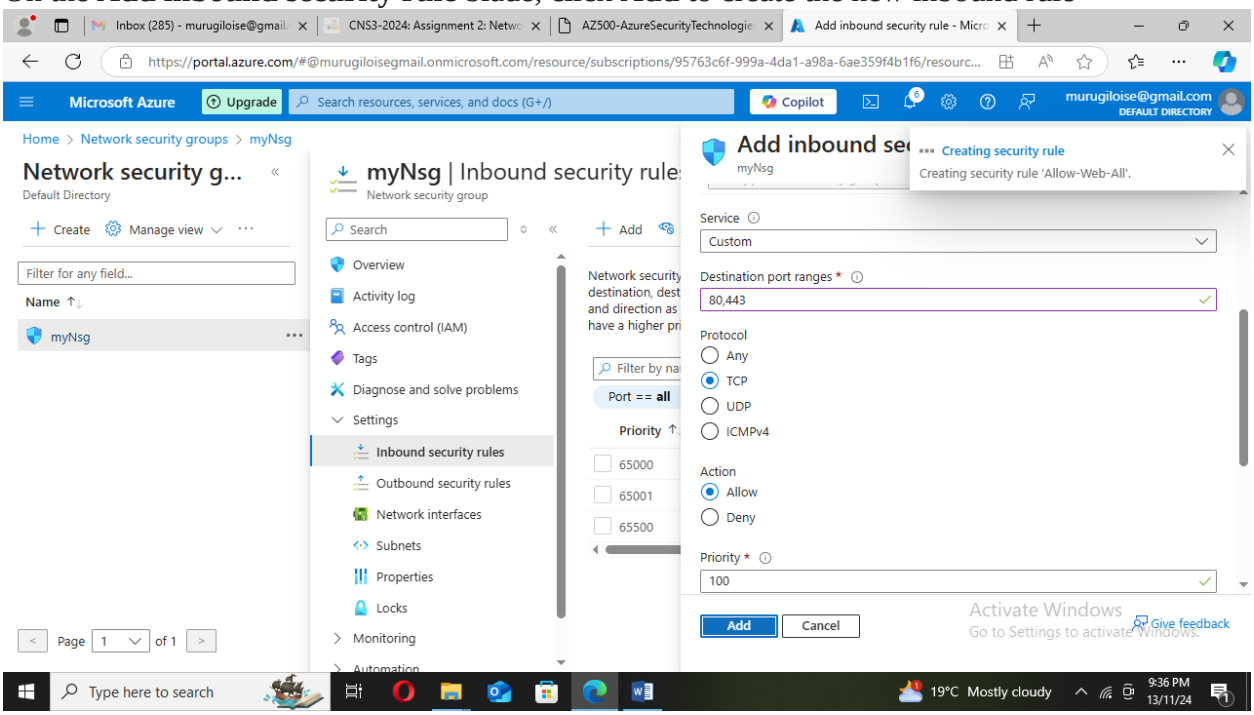
3. On the **Add inbound security rule** blade, specify the following settings to allow TCP ports 80 and 443 to the **myAsgWebServers** application security group (leave all other values with their default values):

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

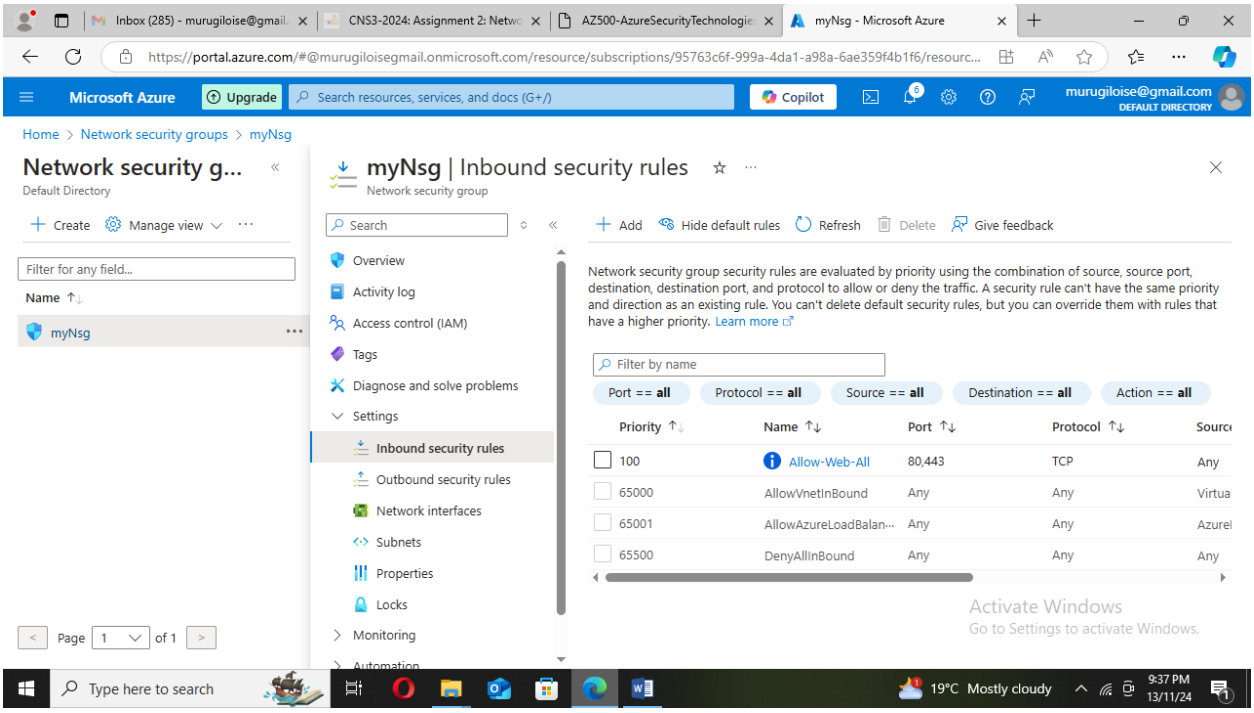
Week 8 Assignment 2: Network Security Groups and Application Security Groups



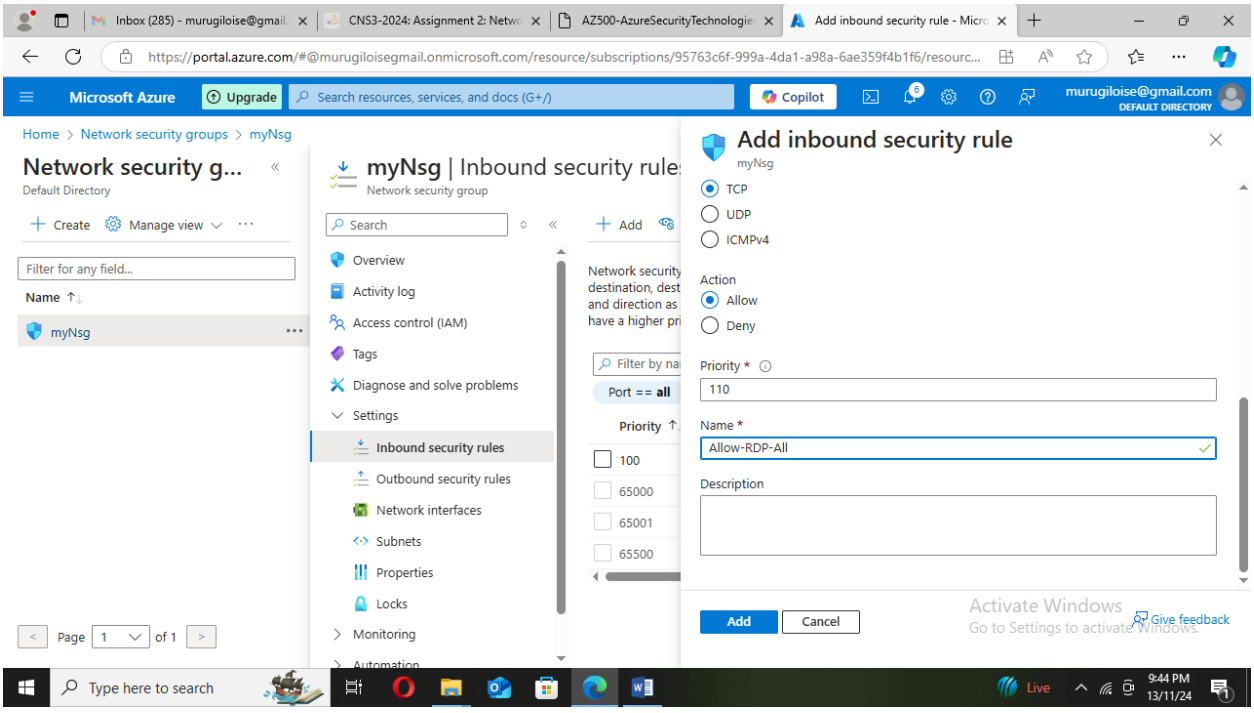
4. On the **Add inbound security rule** blade, click **Add** to create the new inbound rule



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



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**.

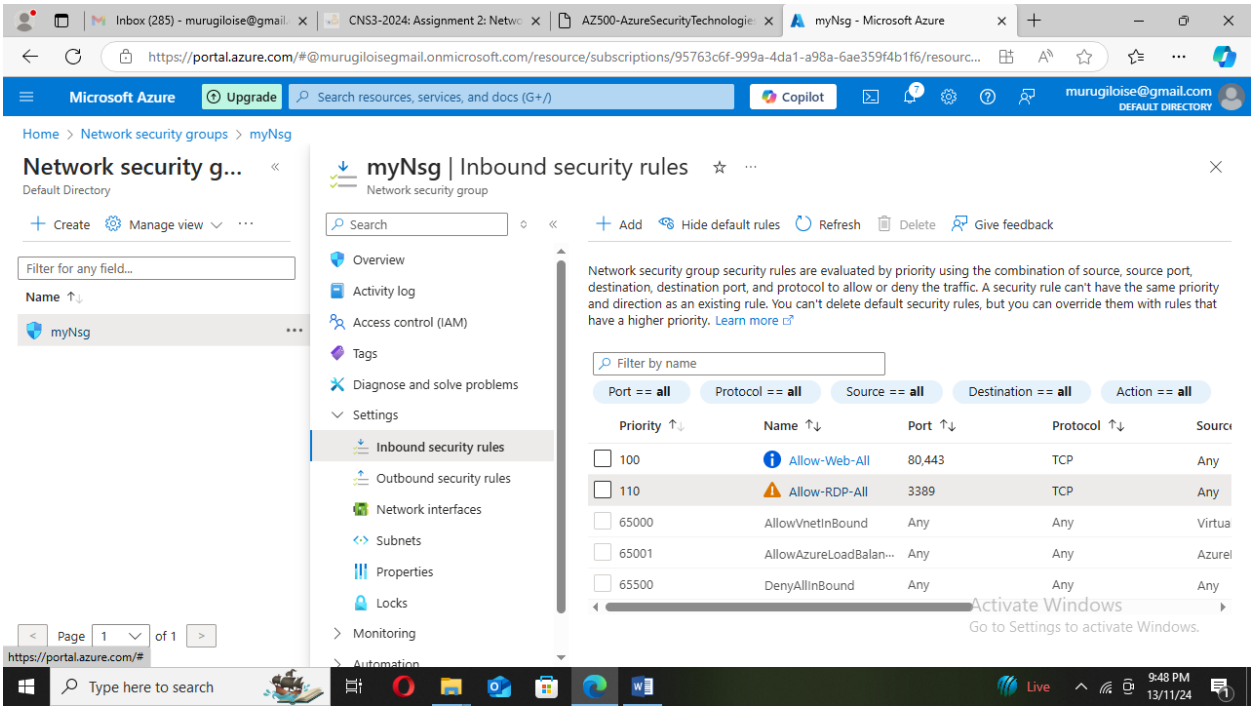


7. On the **Add inbound security rule** blade, click **Add** to create the new inbound rule.

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



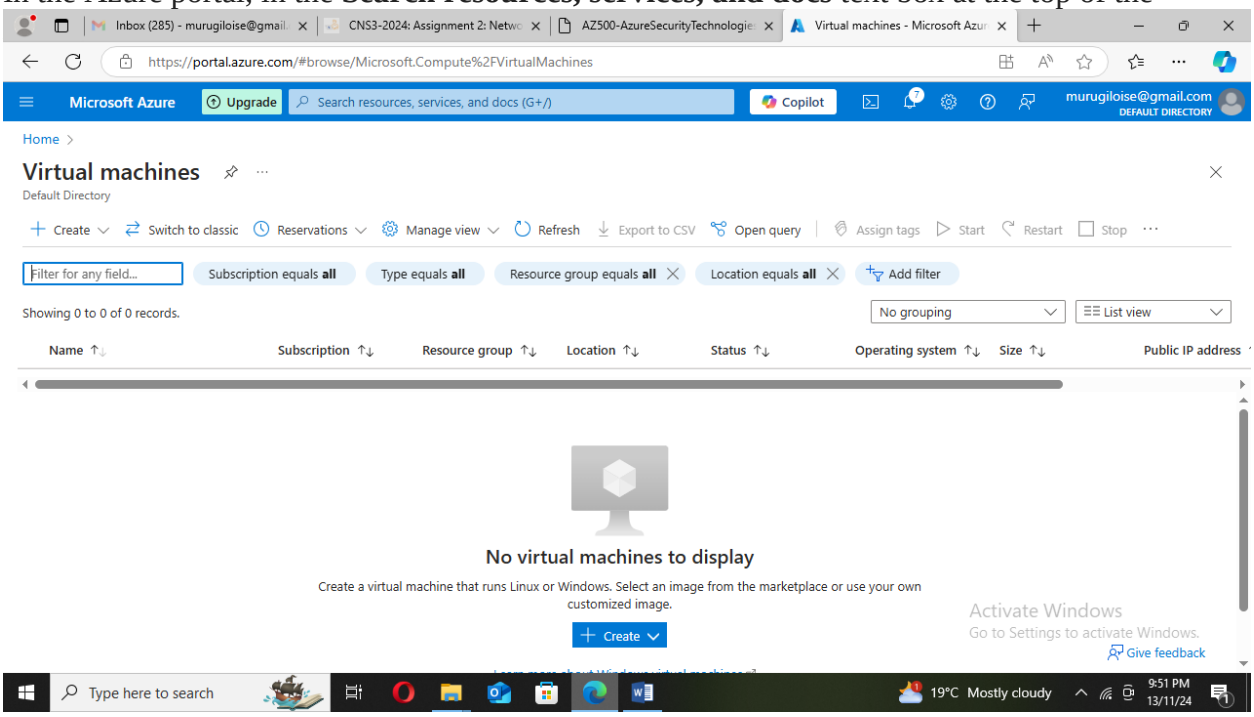
Exercise 2: Deploy virtual machines and test network filters

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

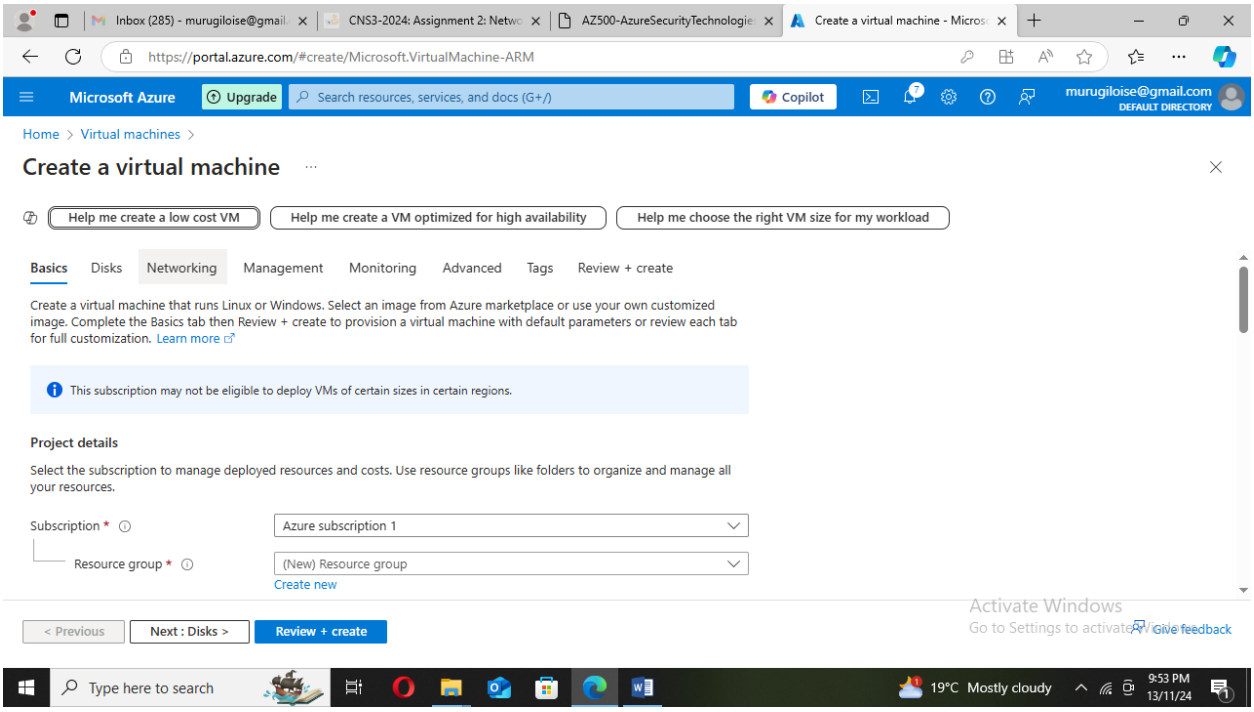
In this task, you will create a virtual machine to use as a web server.

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



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



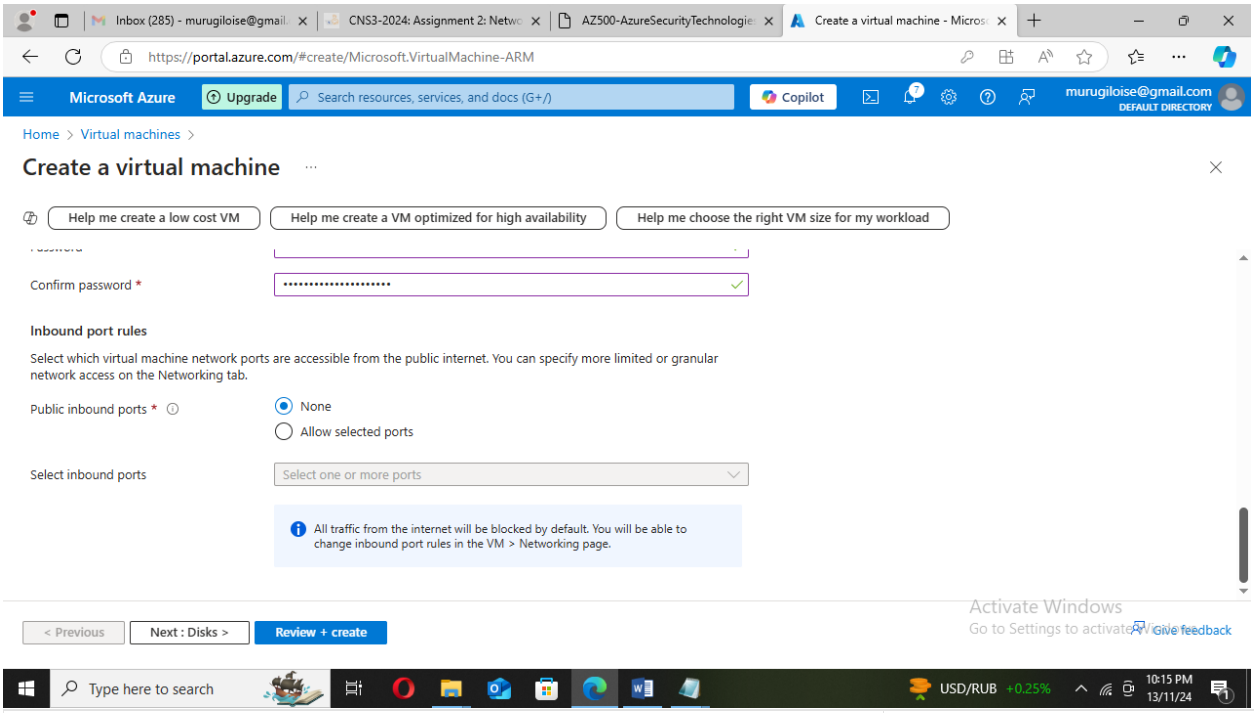
3. On the **Basics** tab of the **Create a virtual machine** blade, specify the following settings (leave others with their default values):

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

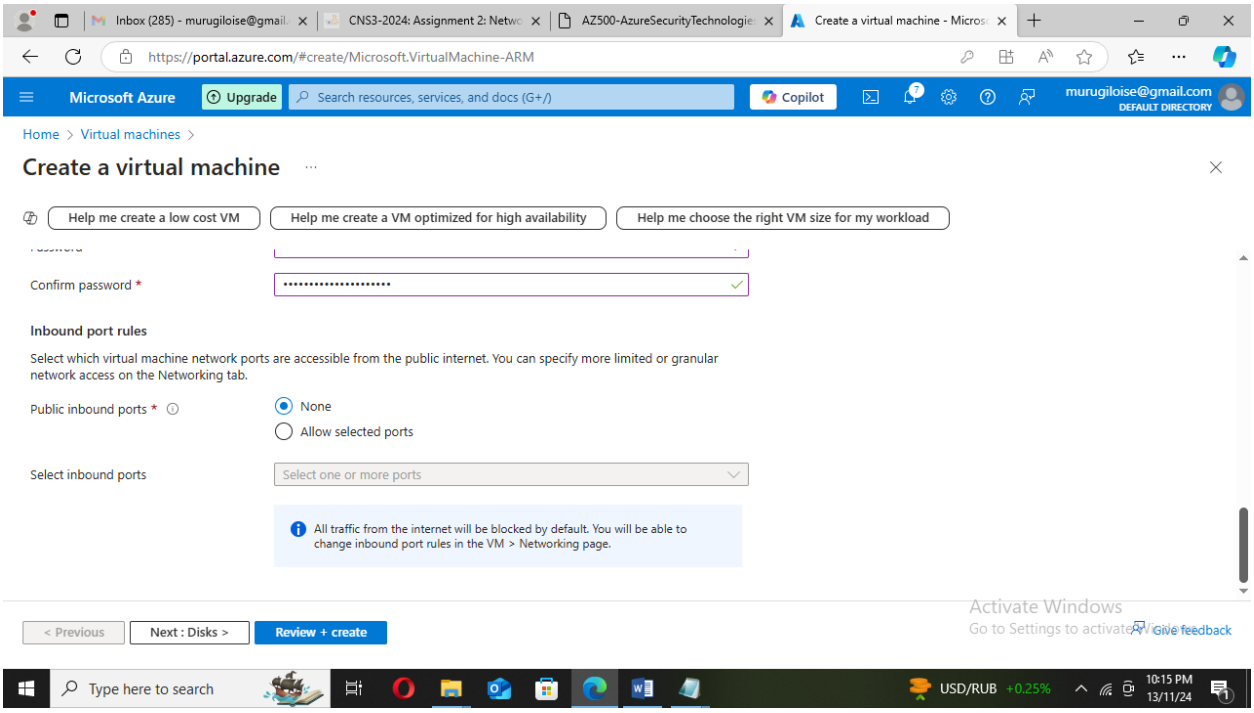
Setting	Value
Subscription	the name of the Azure subscription you will be
Resource group	**AZ500LAB07**
Virtual machine name	**myVmWeb**
Region	**(US)East US**
Image	**Windows Server 2022 Datacenter: Azure Ed**
Size	**Standard D2s v3**
Username	**Student**
Password	**Please create your own password and record 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.

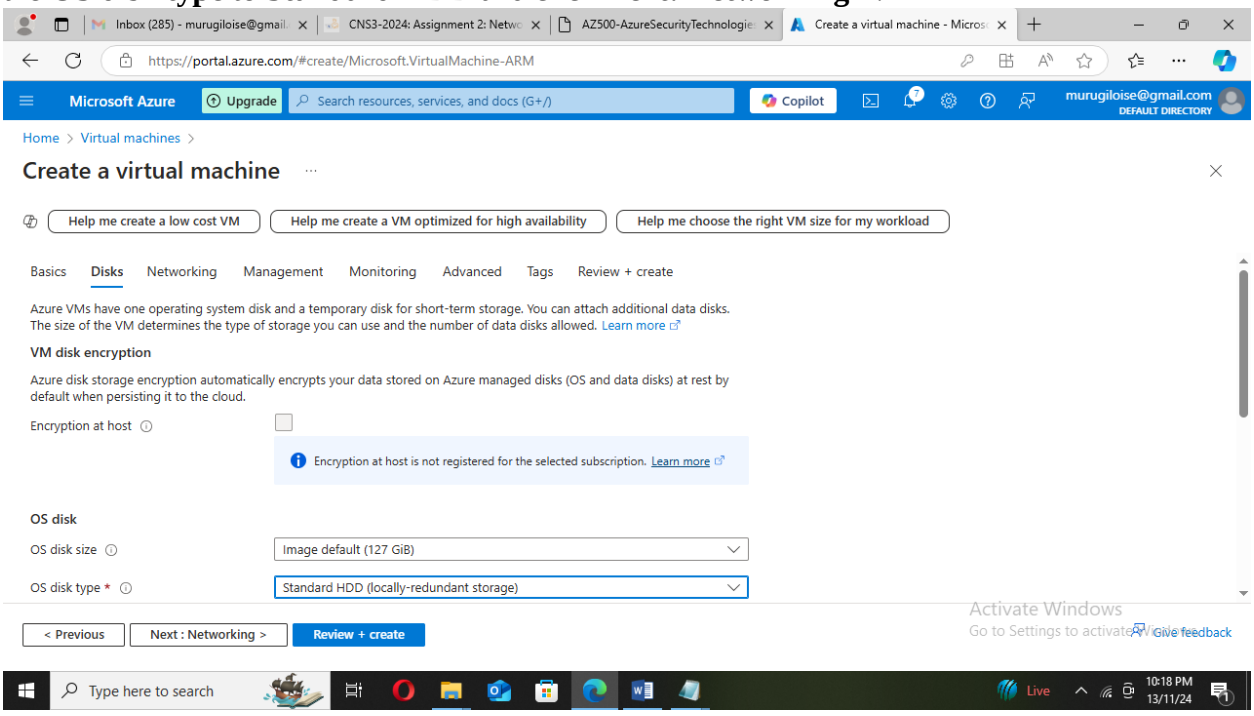
Week 8 Assignment 2: Network Security Groups and Application Security Groups



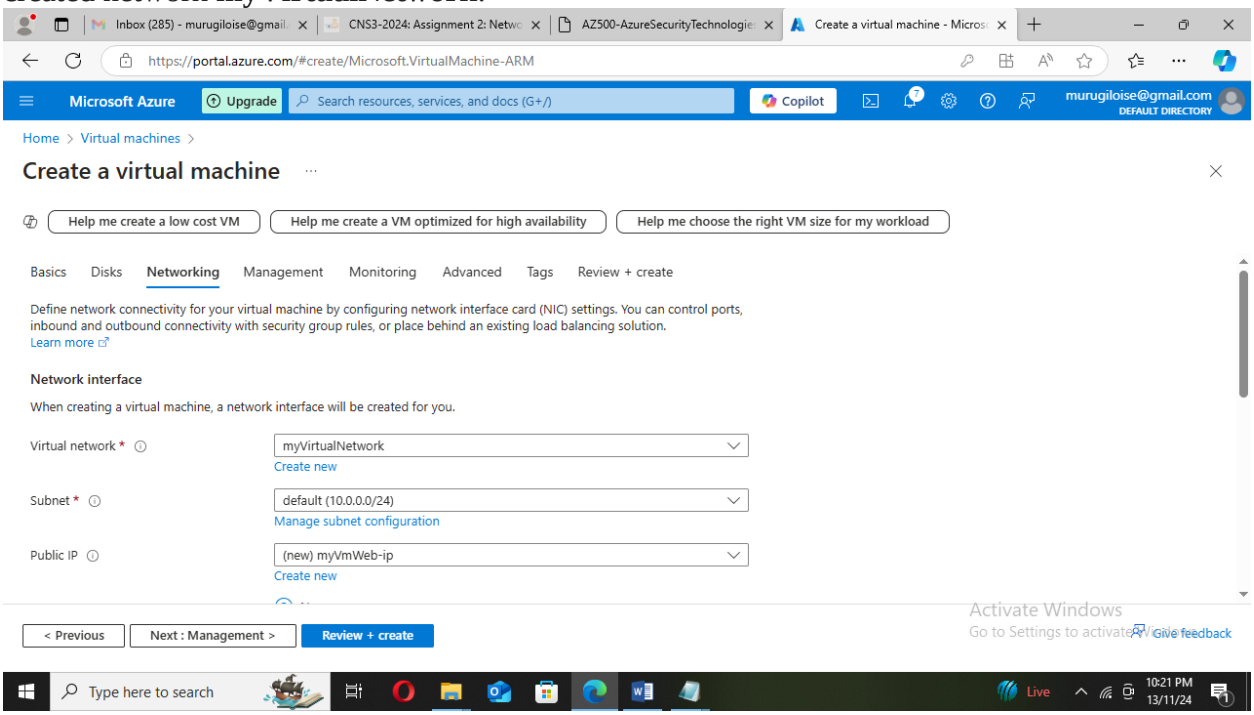
Week 8 Assignment 2: Network Security Groups and Application Security Groups



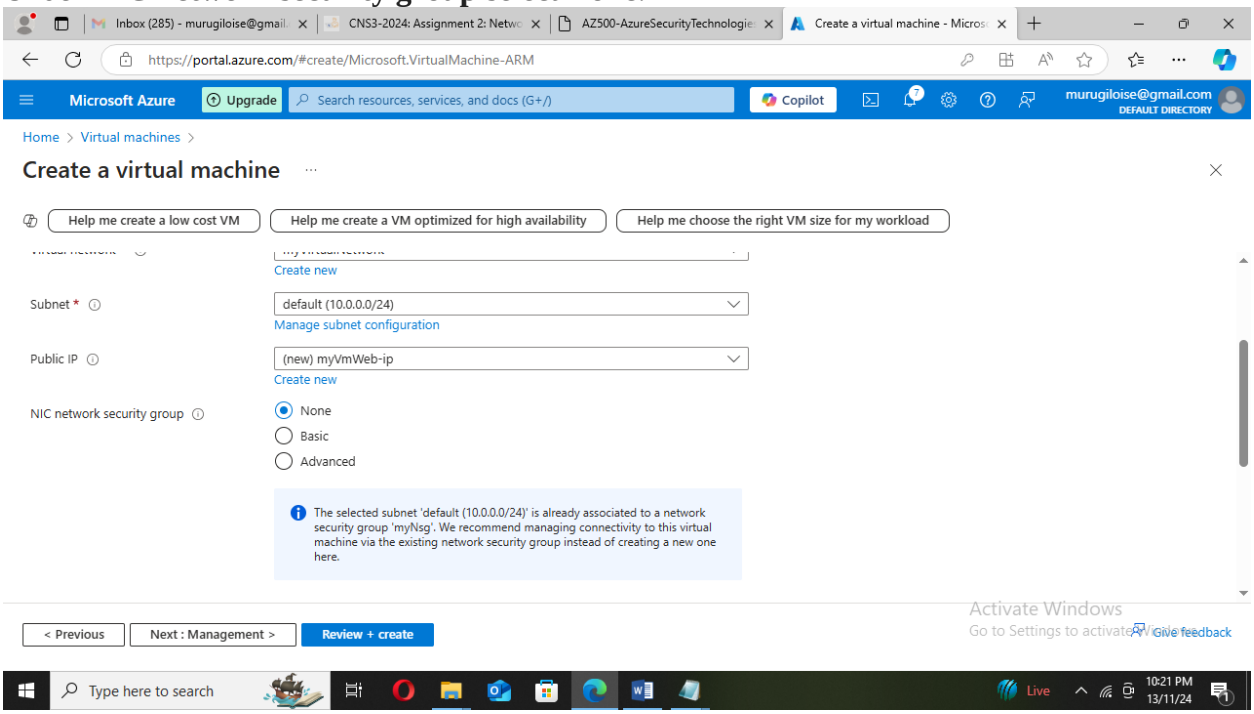
4. Click **Next: Disks >** and, on the **Disks** tab of the **Create a virtual machine** blade, set the **OS disk type** to **Standard HDD** and click **Next: Networking >**.



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



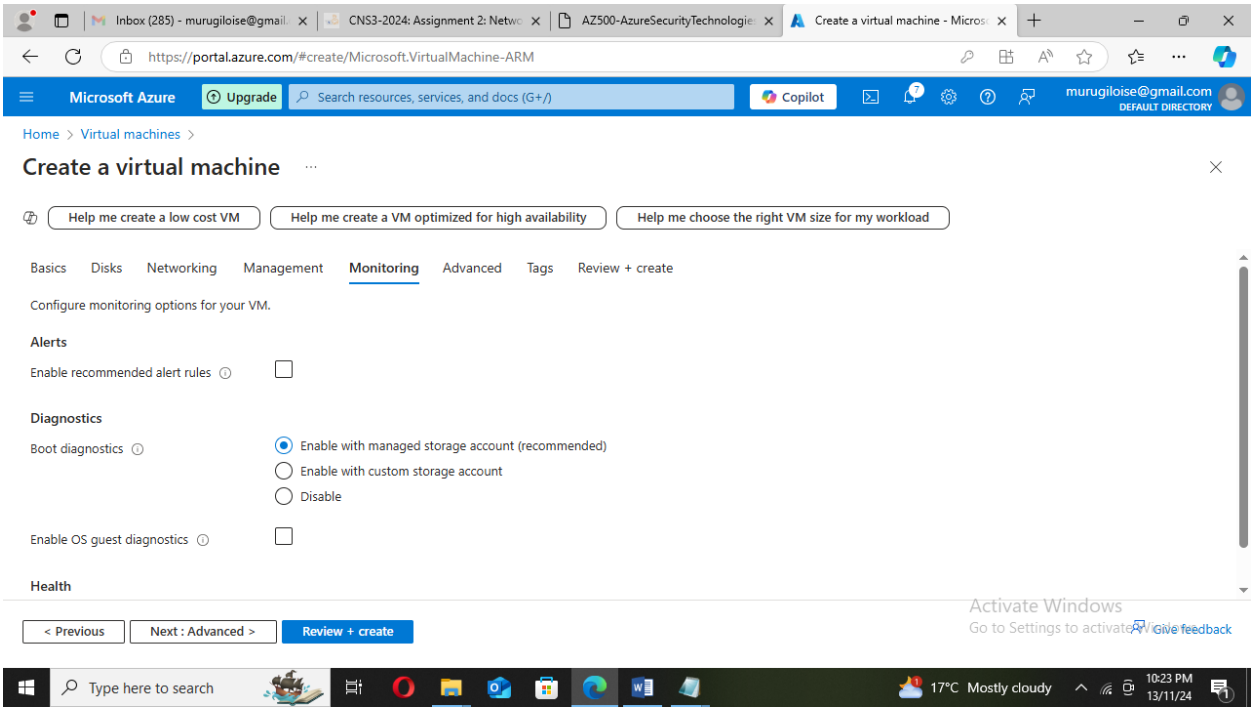
6. Under **NIC network security group** select **None**.



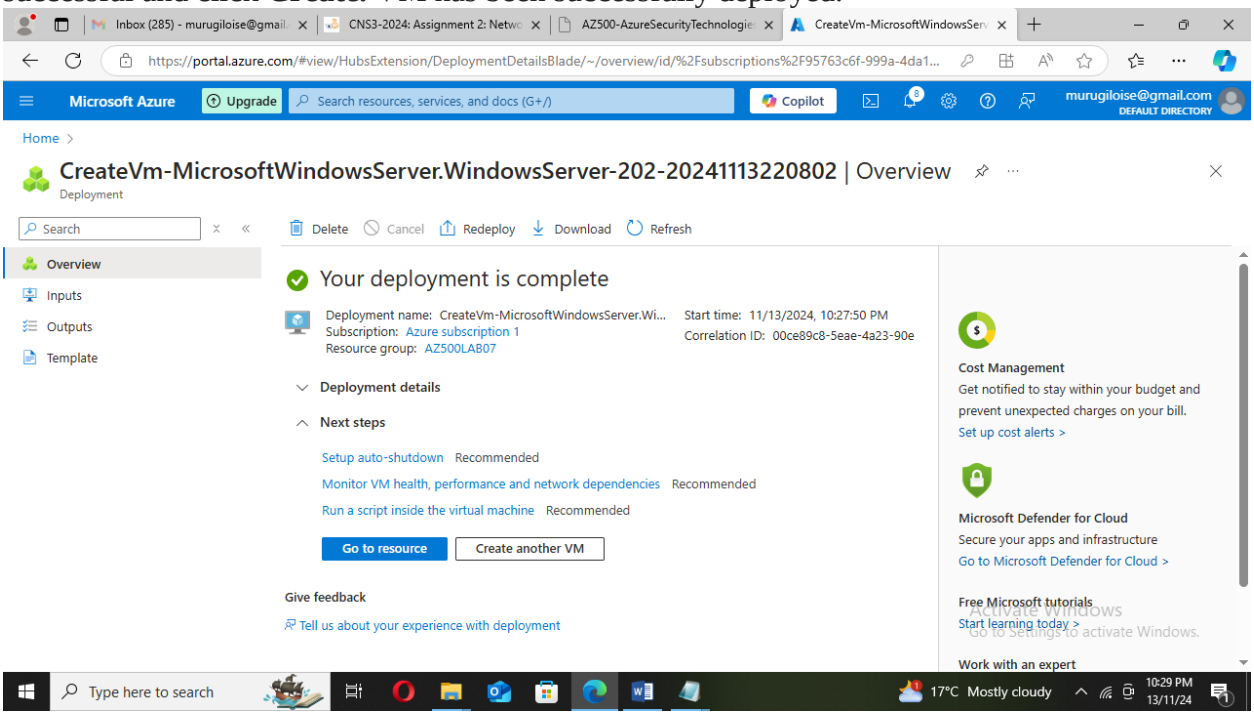
7. Click **Next: Management >**, then click **Next: Monitoring >**. On the **Monitoring** tab of the **Create a virtual machine** blade, verify the following setting:

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

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



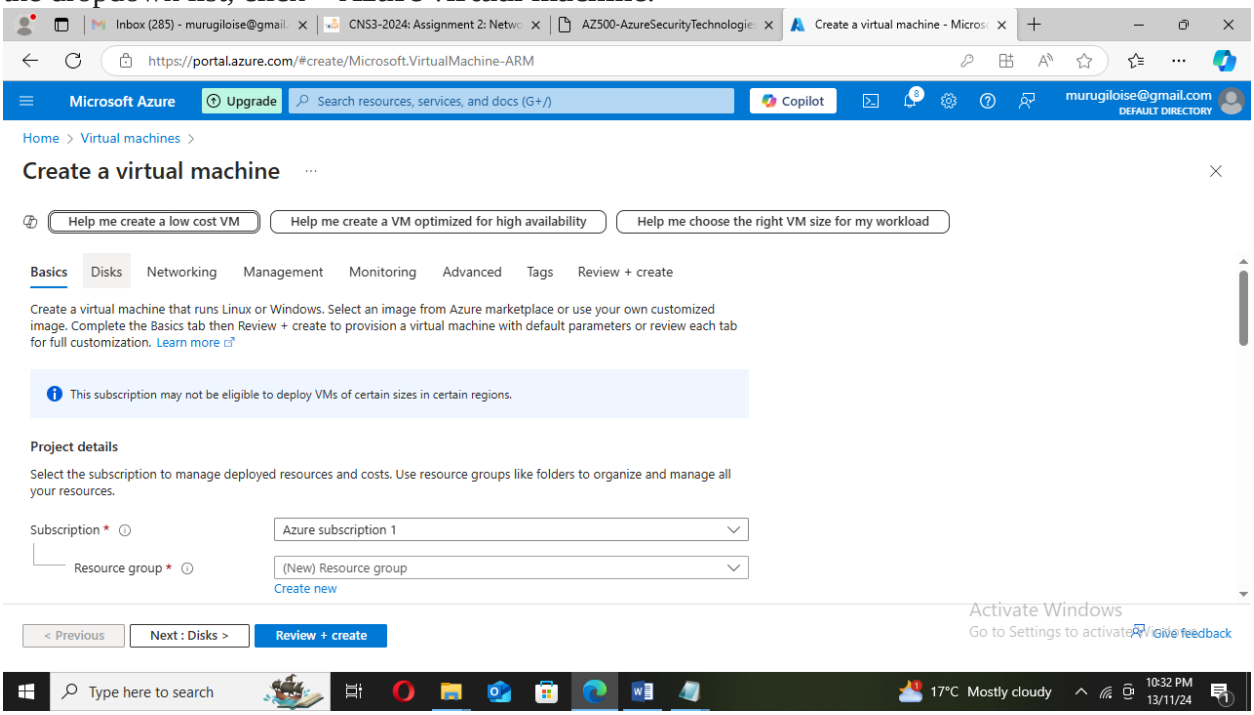
8. Click **Review + create**, on the **Review + create** blade, ensure that validation was successful and click **Create.** VM has been successfully deployed.



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.

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



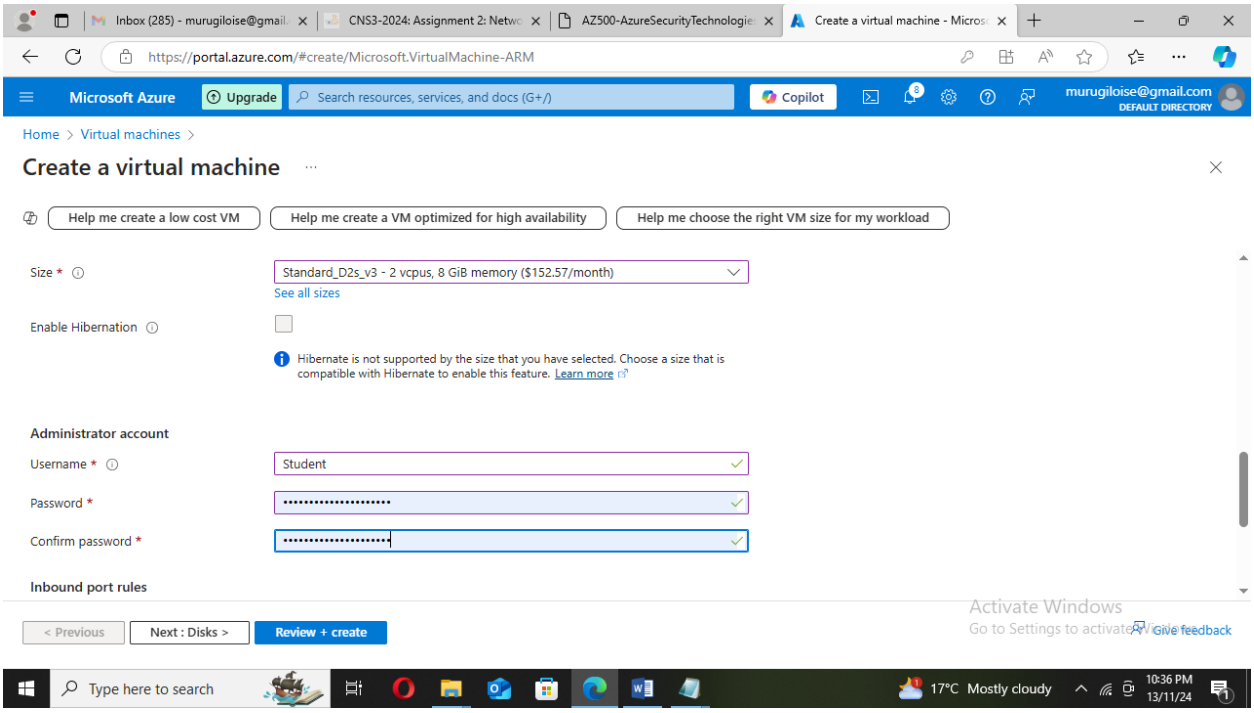
Week 8 Assignment 2: Network Security Groups and Application Security Groups

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

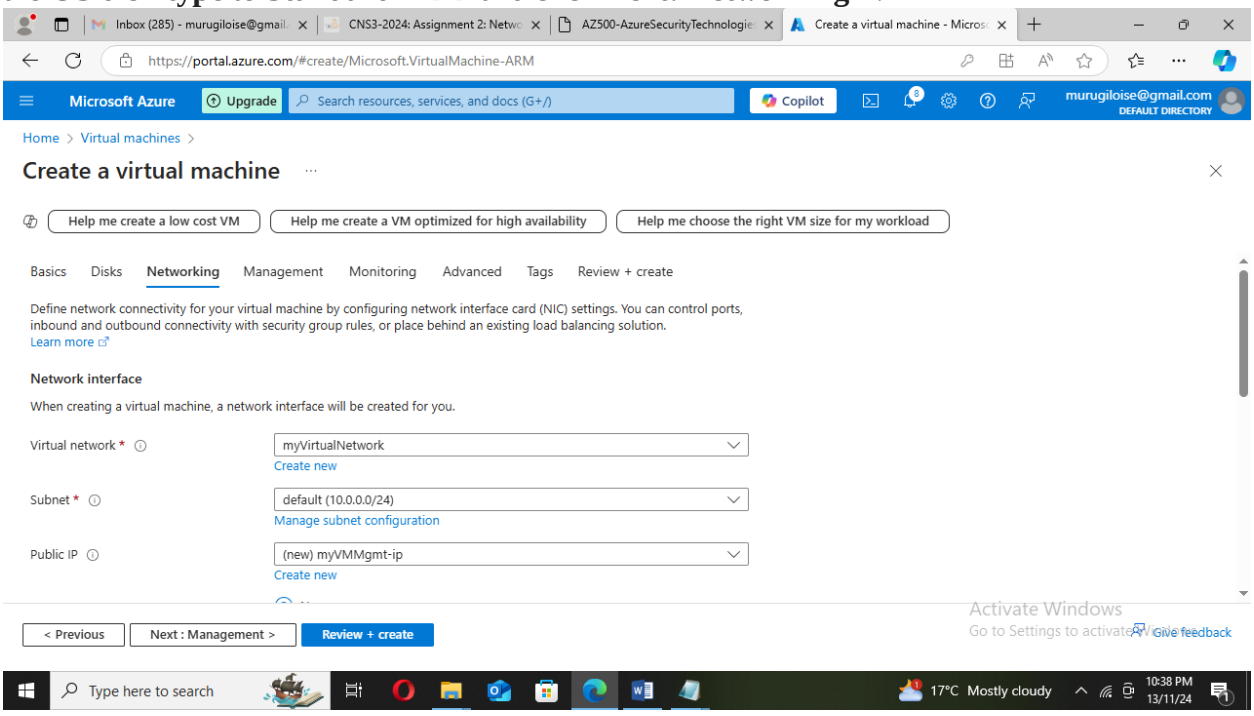
Setting	Value
Subscription	the name of the Azure subscription you will be using in th
Resource group	**AZ500LAB07**
Virtual machine name	**myVMMgmt**
Region	(US)East US
Image	**Windows Server 2022 Datacenter: Azure Edition - x64**
Size	**Standard D2s v3**
Username	**Student**
Password	**Please use your 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

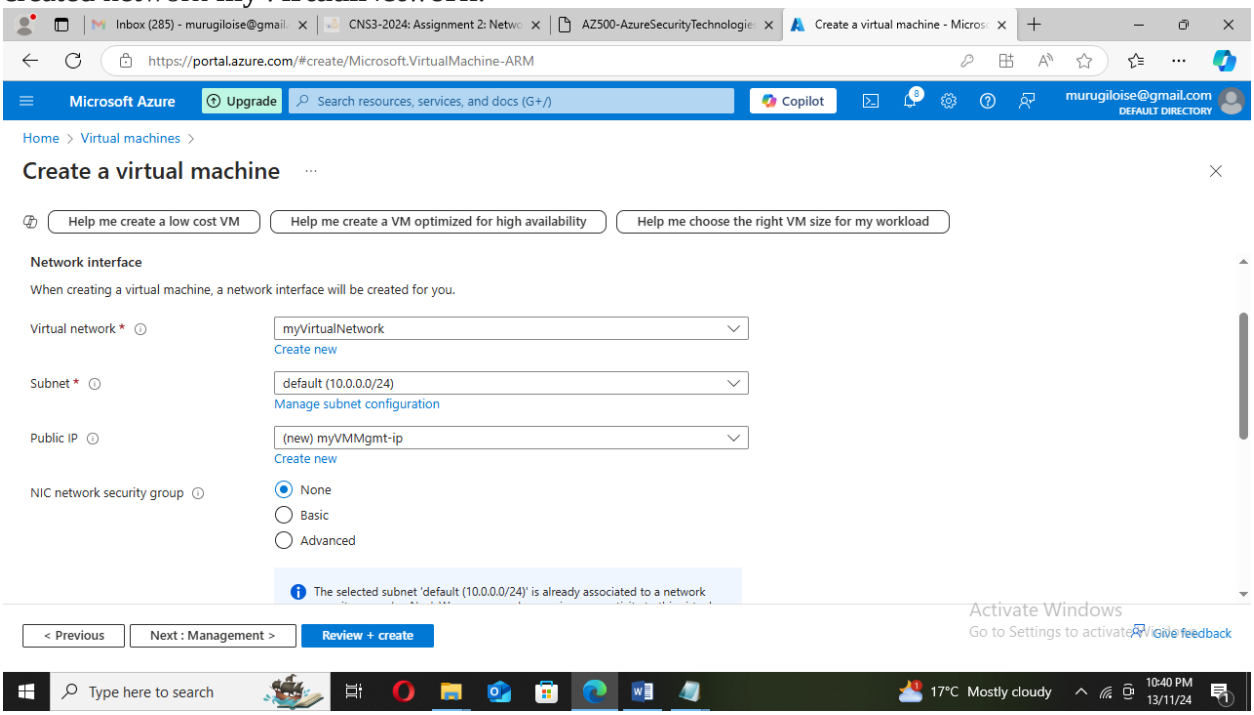


3. Click **Next: Disks >** and, on the **Disks** tab of the **Create a virtual machine** blade, set the **OS disk type** to **Standard HDD** and click **Next: Networking >**.

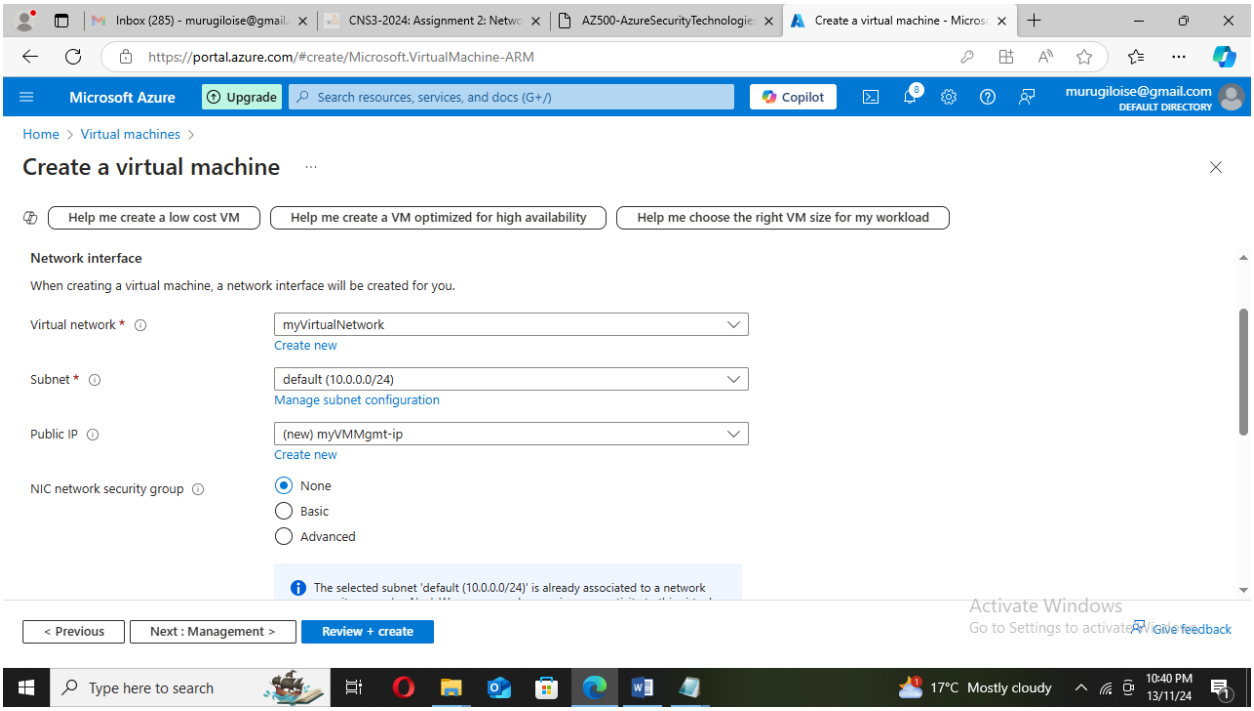


Week 8 Assignment 2: Network Security Groups and Application Security Groups

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

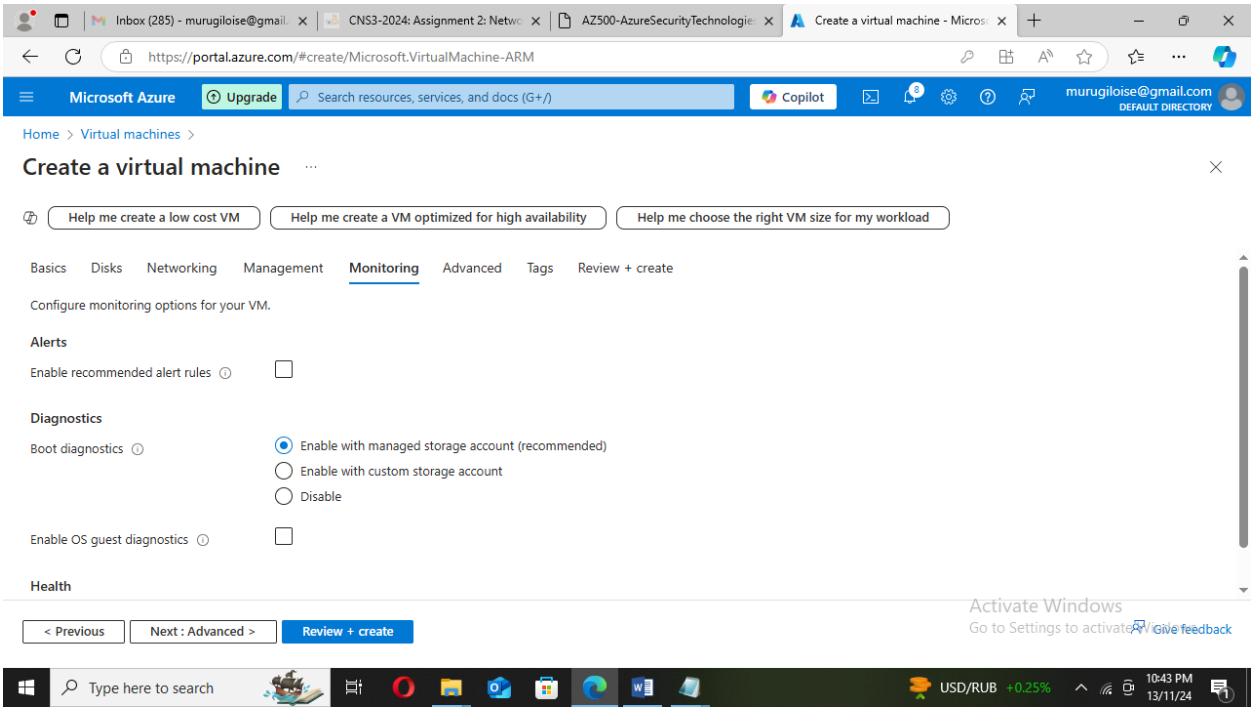


5. Under **NIC network security group** select **None**.



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

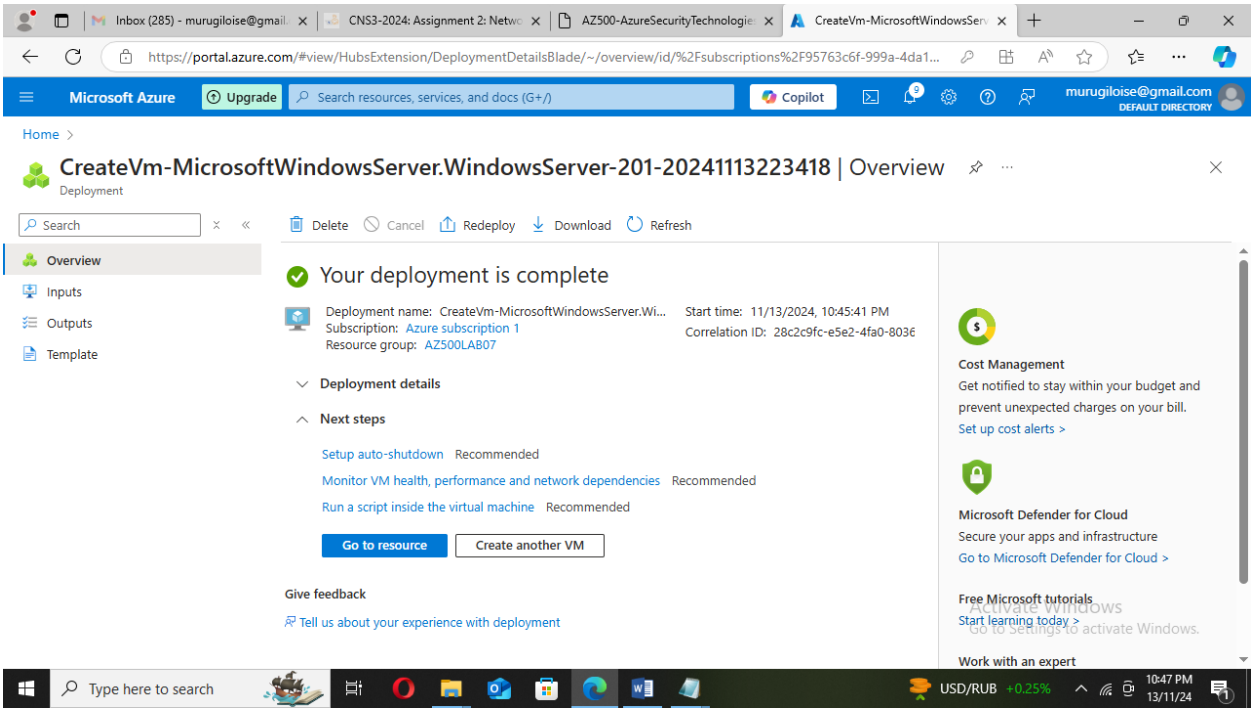
Setting	Value
Boot diagnostics	**Enabled with managed storage account (recommended)**



7. 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

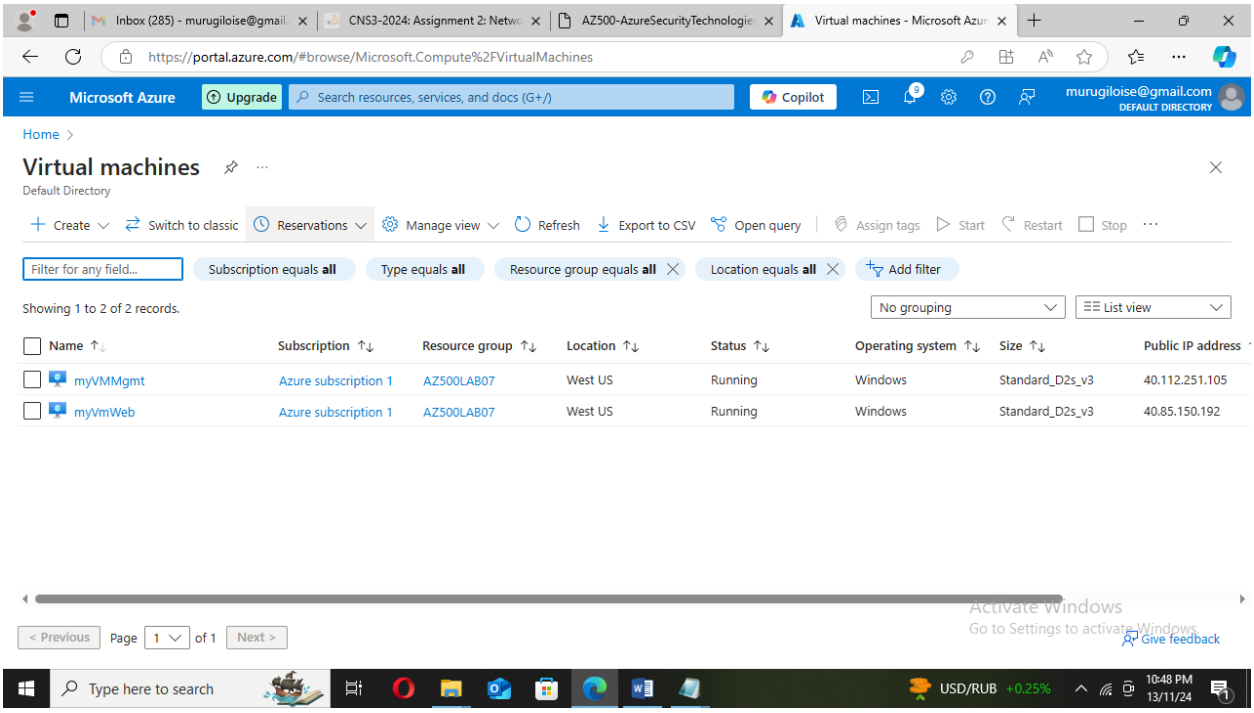


Task 3: Associate each virtual machines network interface to its application security group.

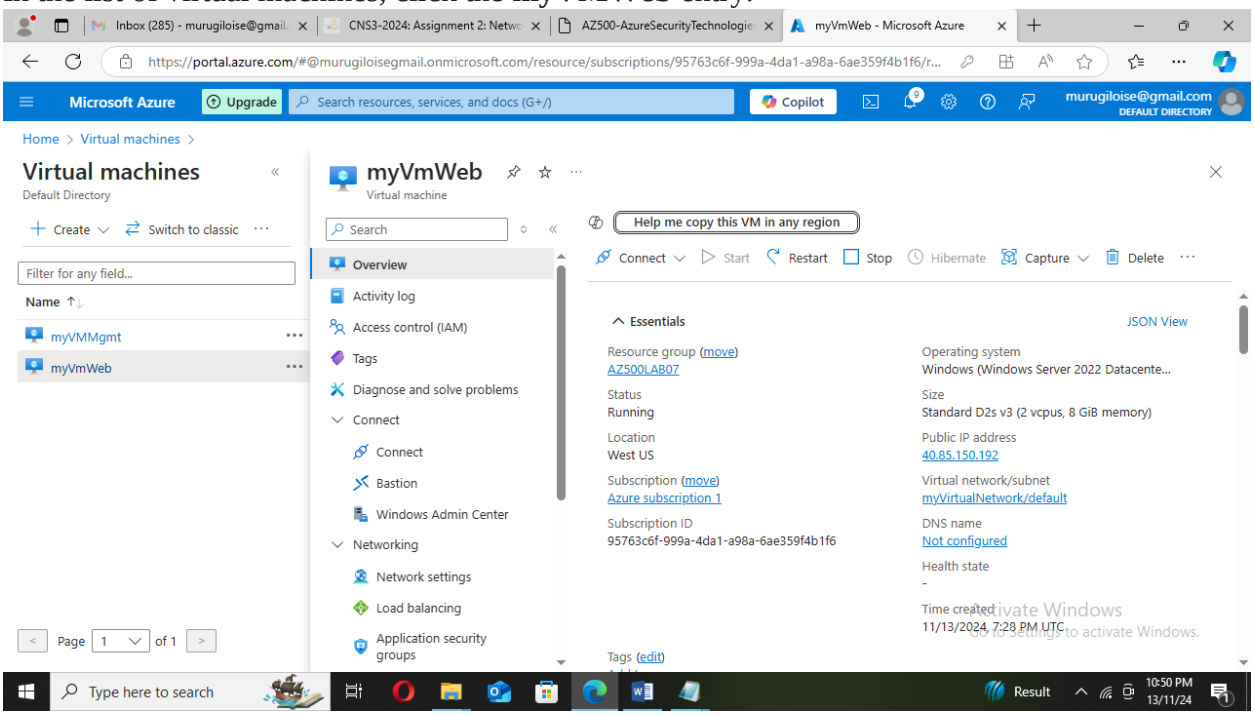
In this task, you will associate each virtual machines network interface with the corresponding application security group. The myVMWeb virtual machine interface will be associated to the myAsgWebServers ASG. The myVMMgmt virtual machine interface will be associated to the myAsgMgmtServers ASG.

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

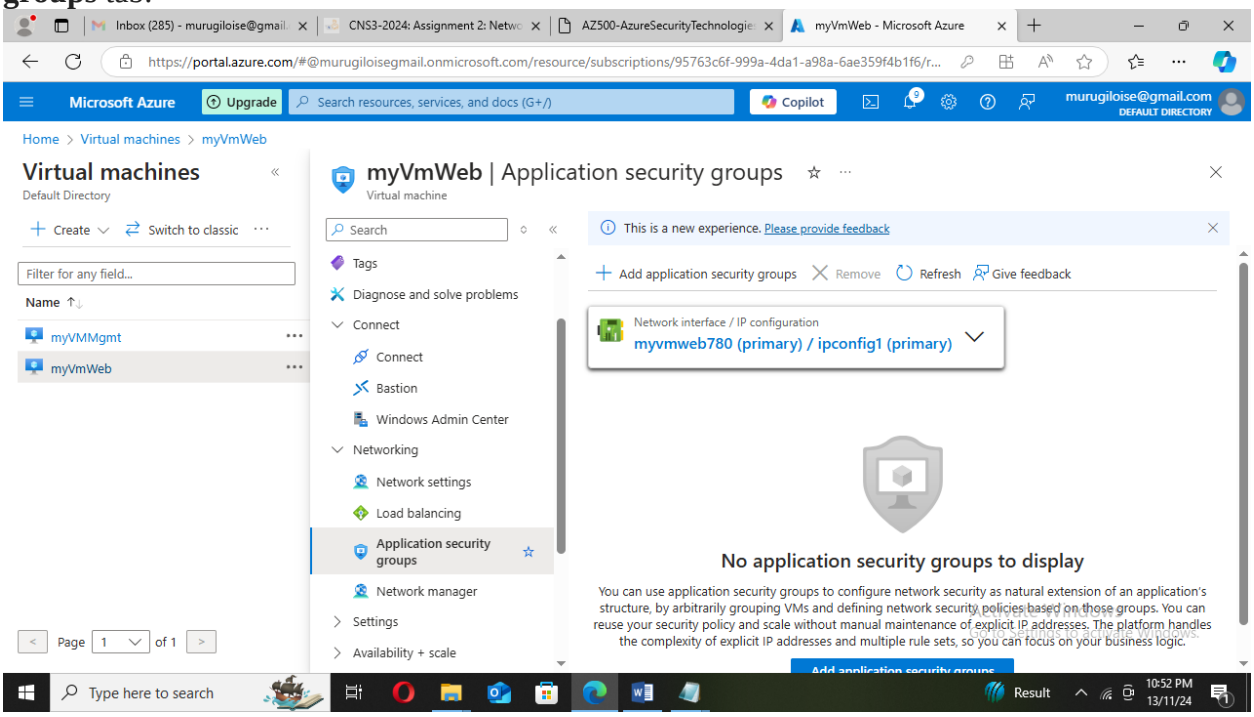


2. In the list of virtual machines, click the **myVMWeb** entry.

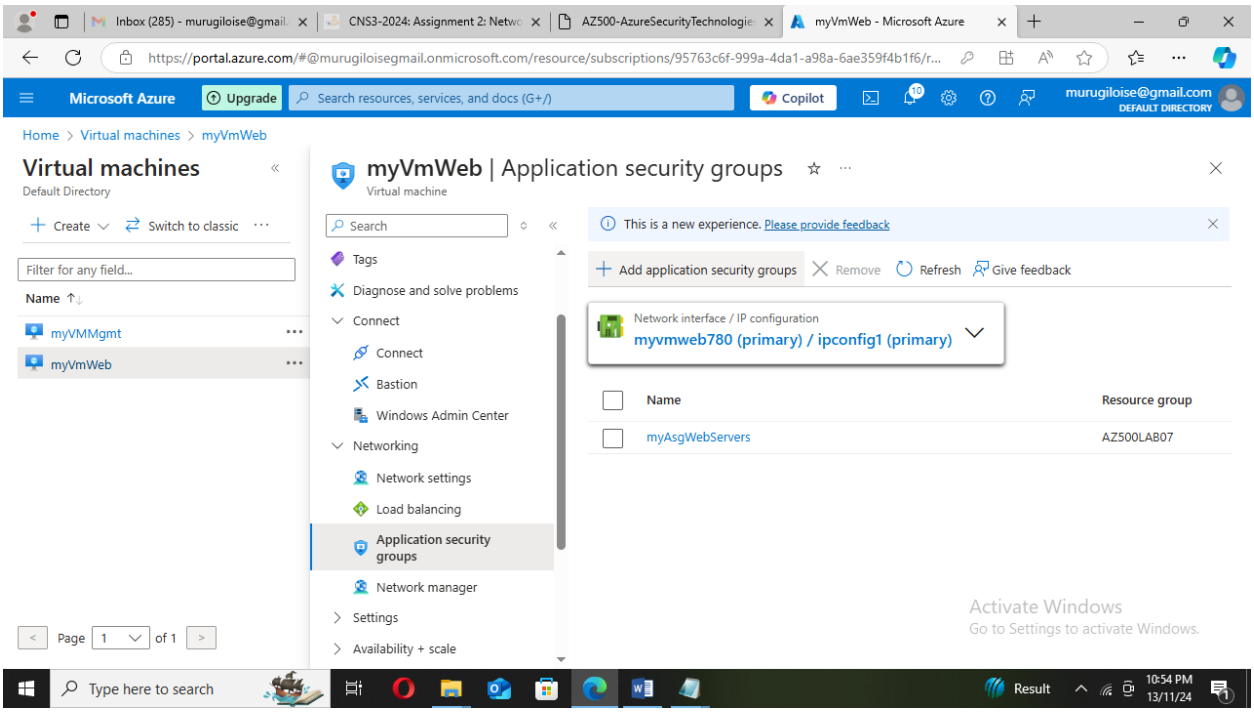


3. On the **myVMWeb** blade, in the **Networking** section, click **Network settings** and then, on the **myVMWeb | Networking settings** blade, click the **Application security**

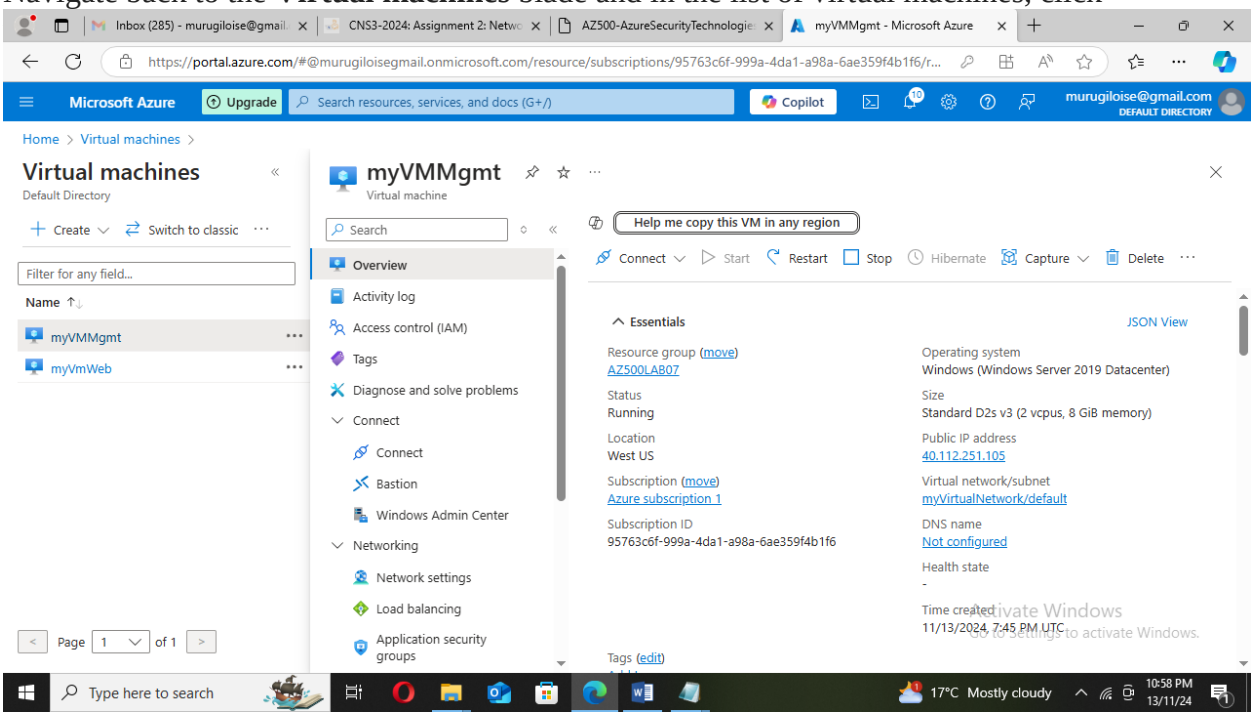
groups tab.



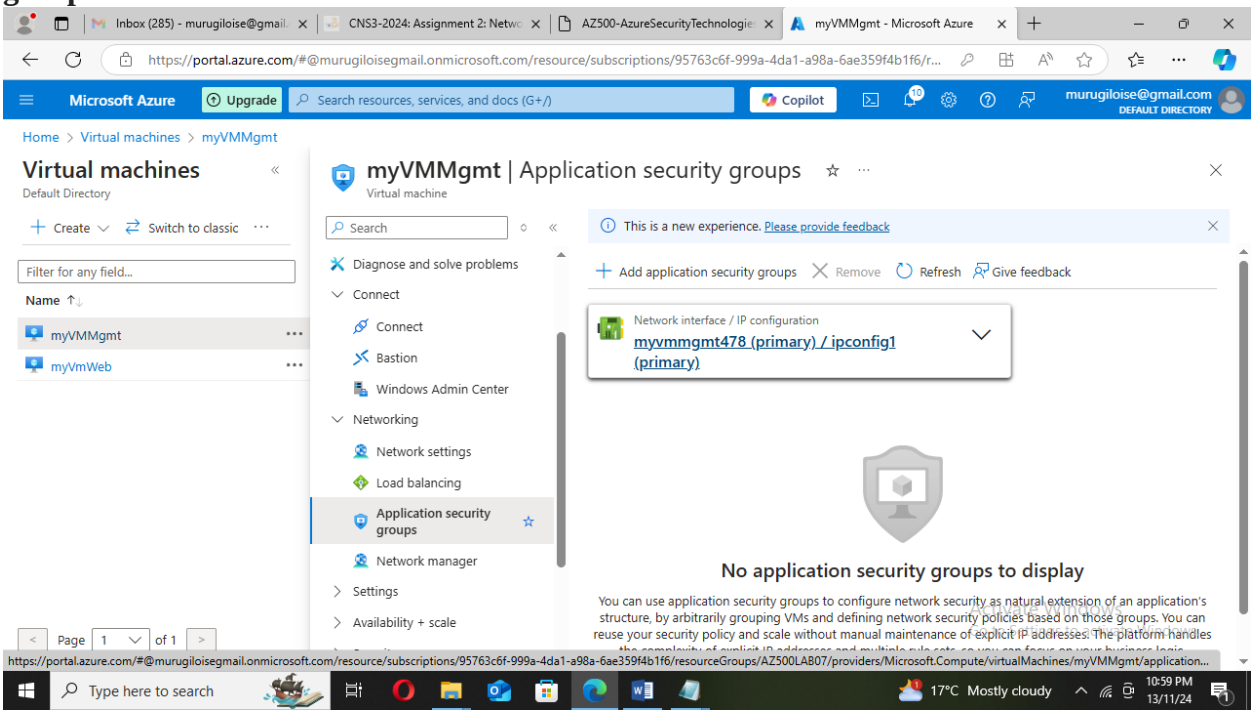
4. Click + **Add application security groups**, in the **Application security group** list, select **myAsgWebServers**, and then click **Save**. We haave successfully added myAsgWebServers .



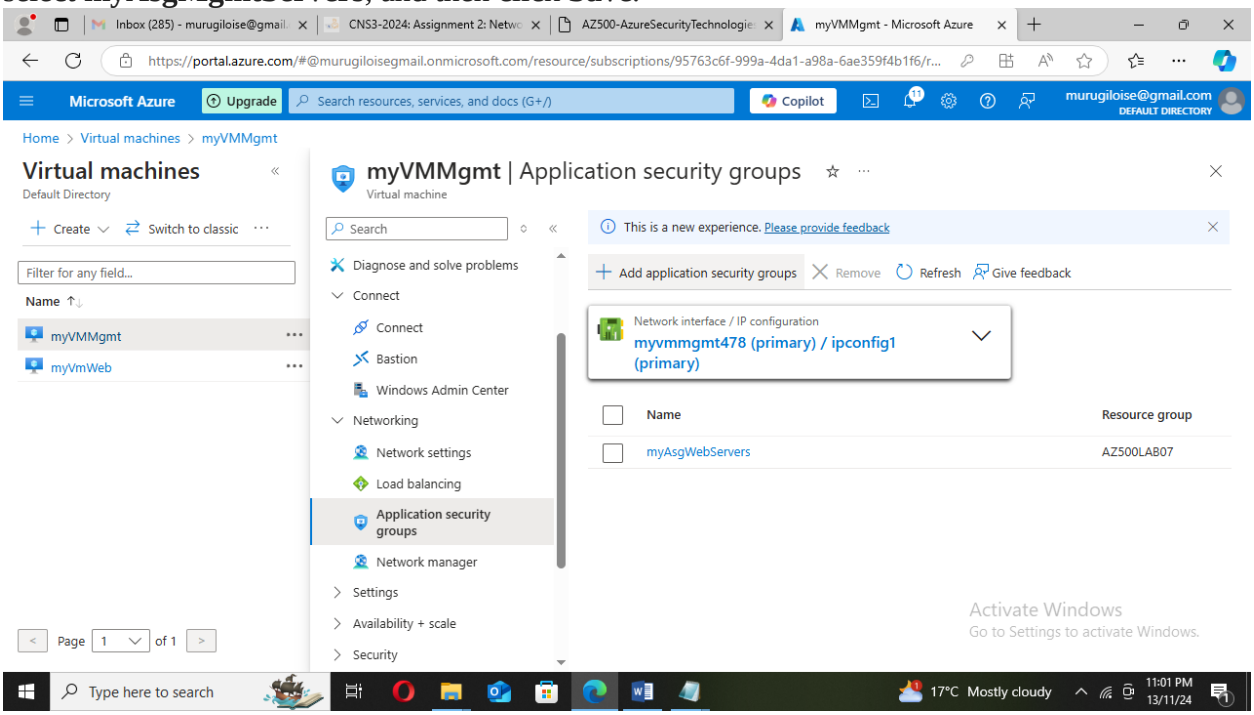
5. Navigate back to the **Virtual machines** blade and in the list of virtual machines, click



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.



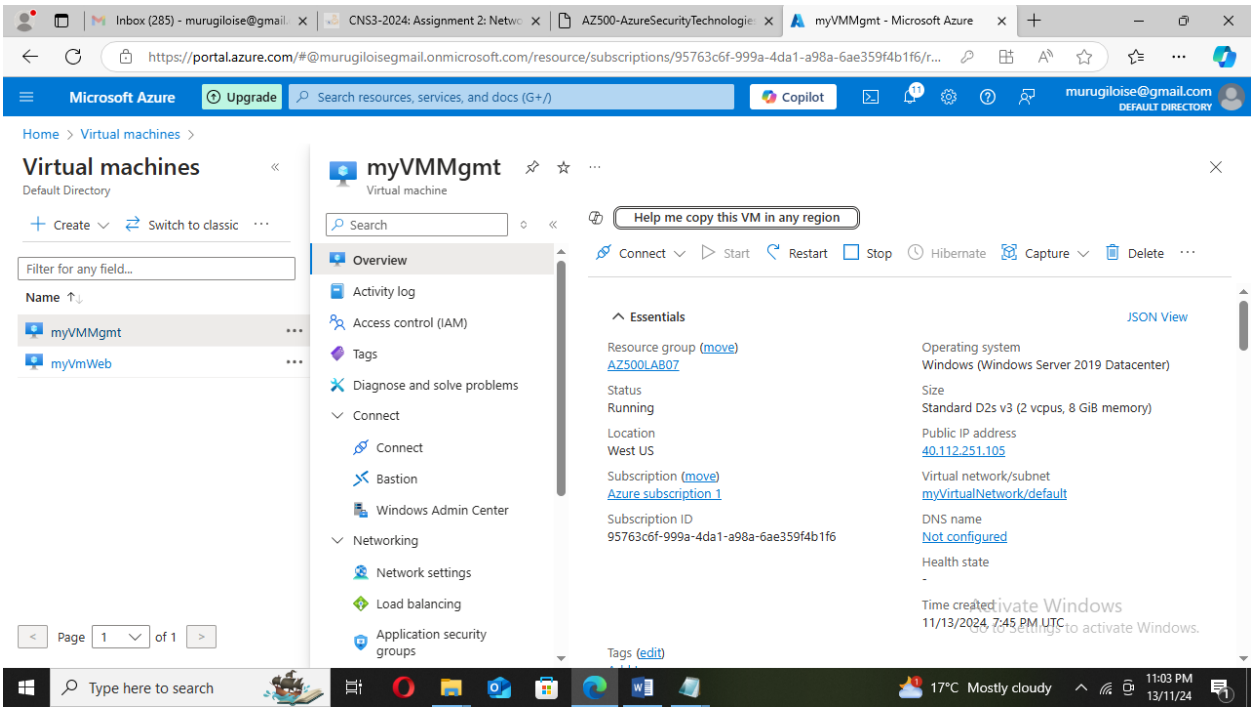
7. Click + **Add application security groups**, in the **Application security group** list, select **myAsgMgmtServers**, and then click **Save**.



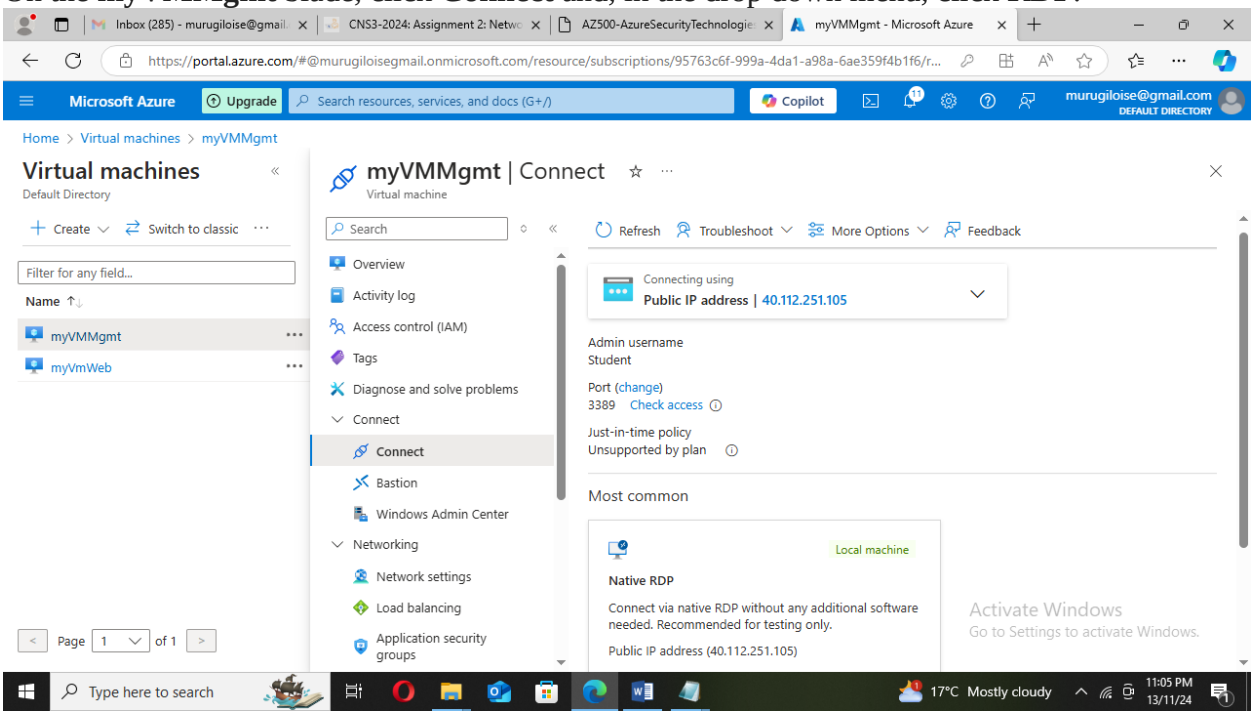
Task 4: Test the network traffic filtering

In this task, you will test the network traffic filters. You should be able to RDP into the myVMMgmnt 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. 

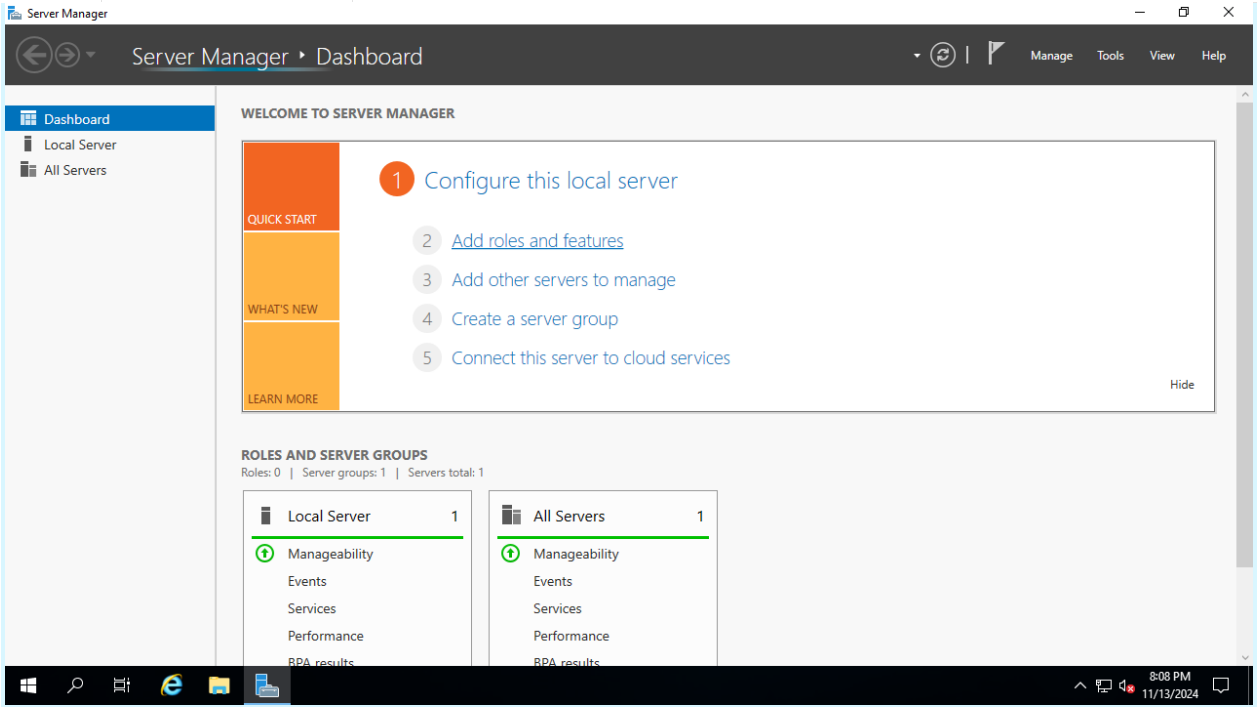
2. On the **myVMMgmt** blade, click **Connect** and, in the drop down menu, click **RDP**.



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 credntials:

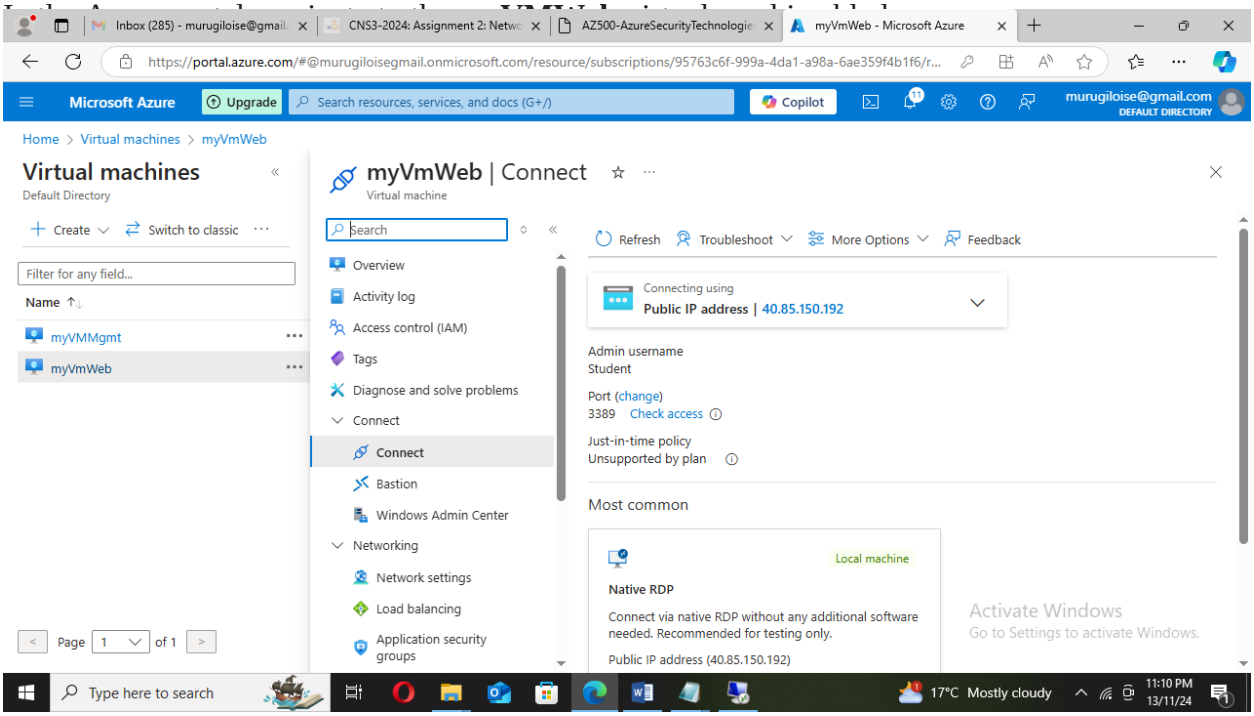
Week 8 Assignment 2: Network Security Groups and Application Security Groups

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

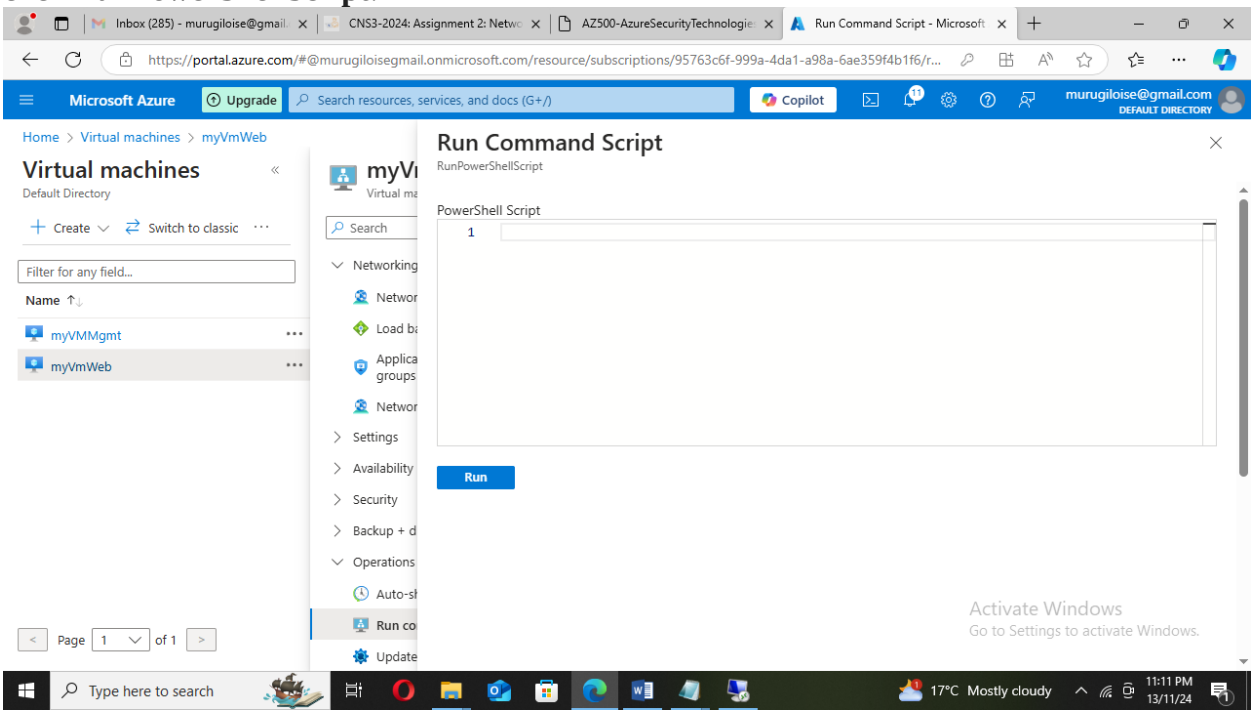


Week 8 Assignment 2: Network Security Groups and Application Security Groups

4.



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

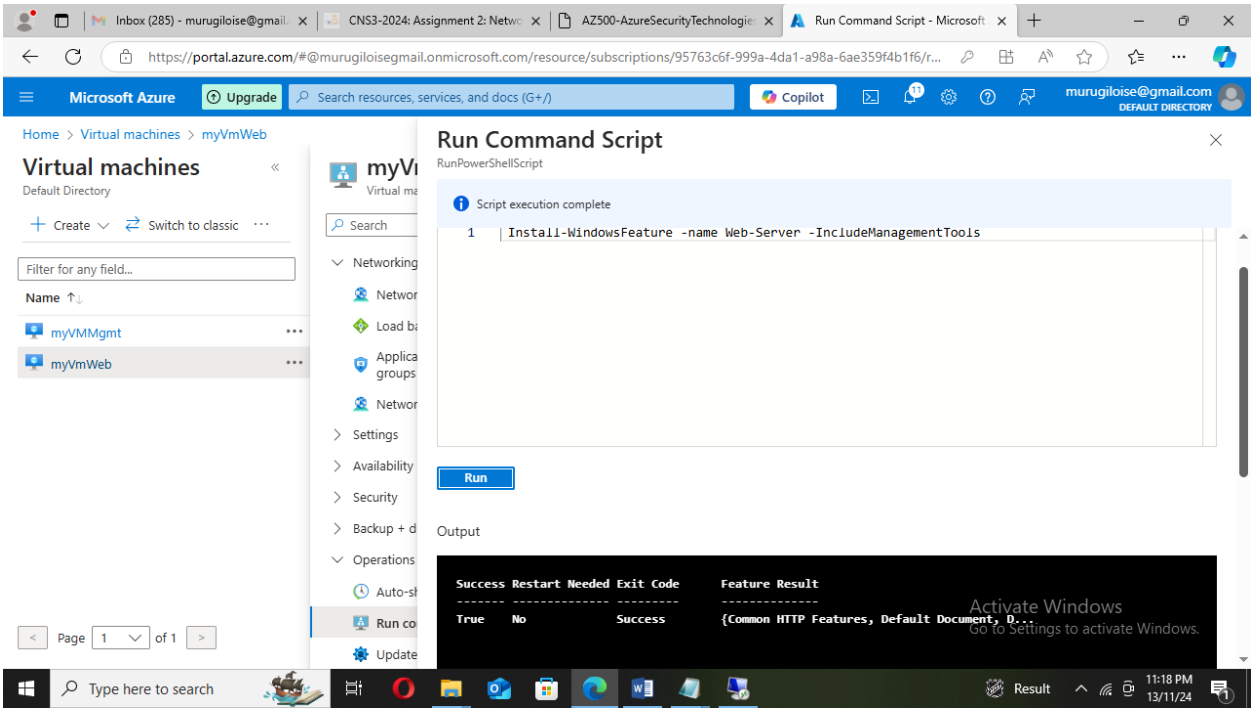


6. On the **Run Command Script** pane, run the following to install the Web server role on **myVmWeb**:

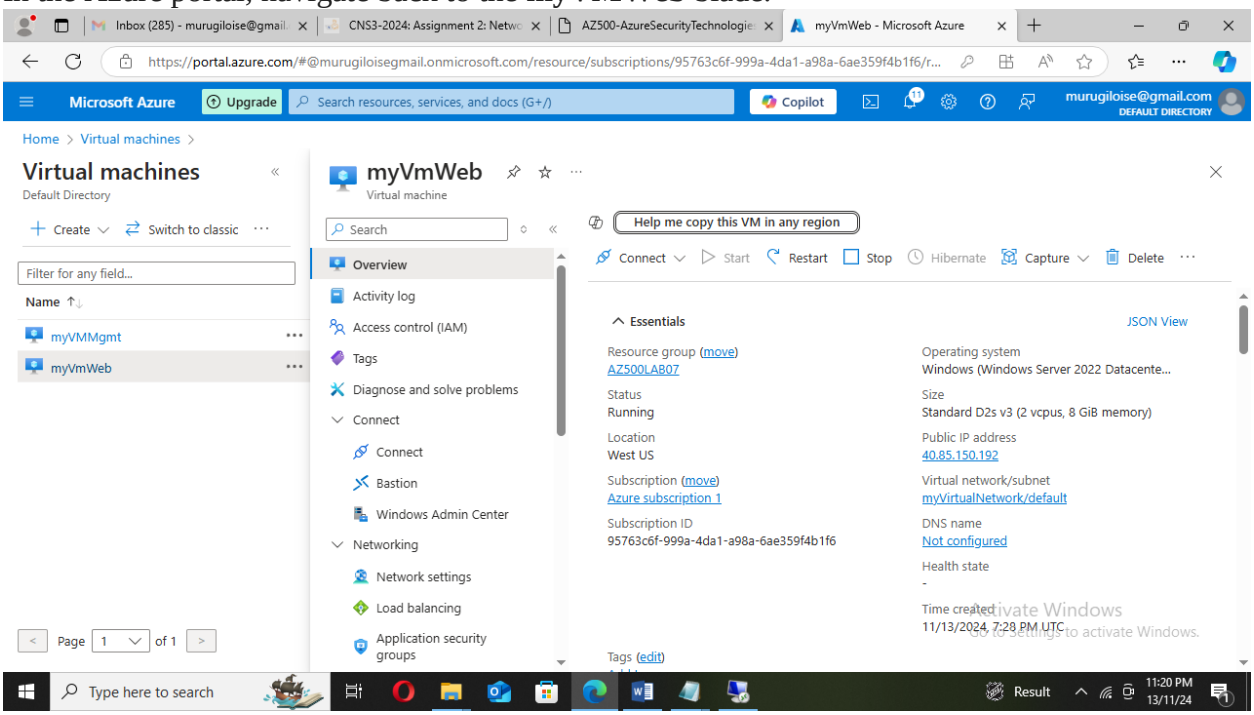
The command was successfully executed as seen on the image below.

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

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

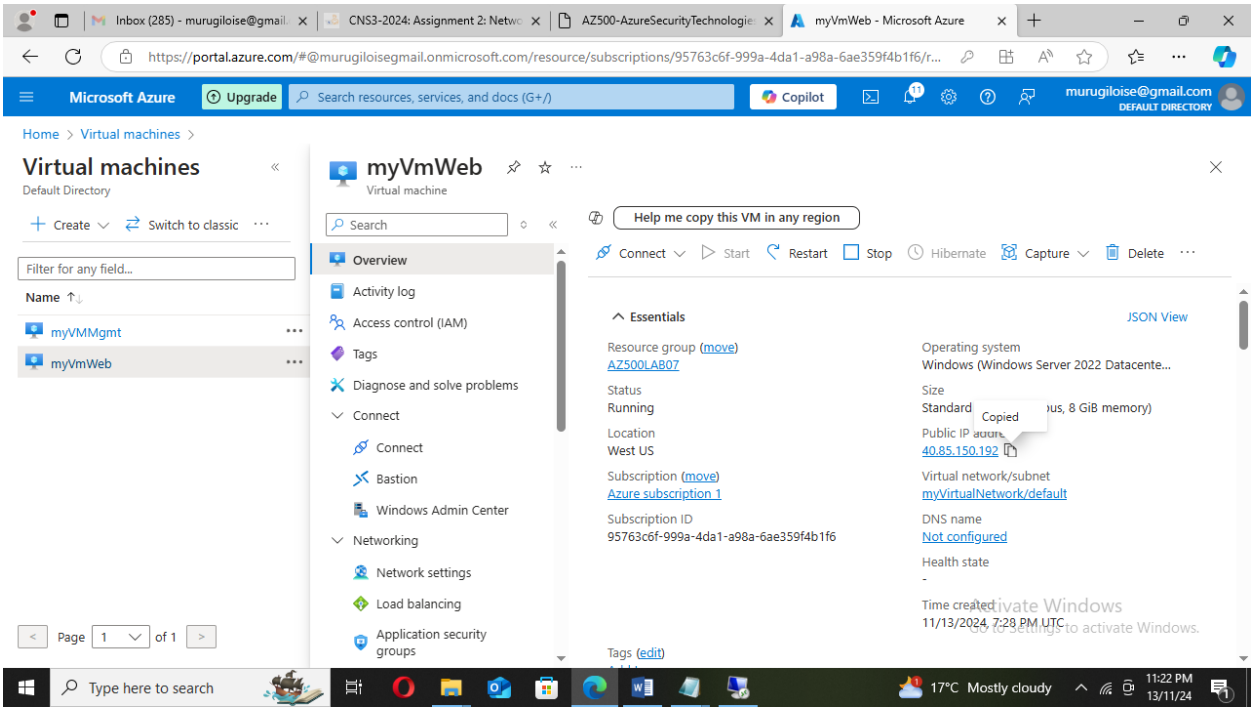


7. In the Azure portal, navigate back to the **myVMWeb** blade.

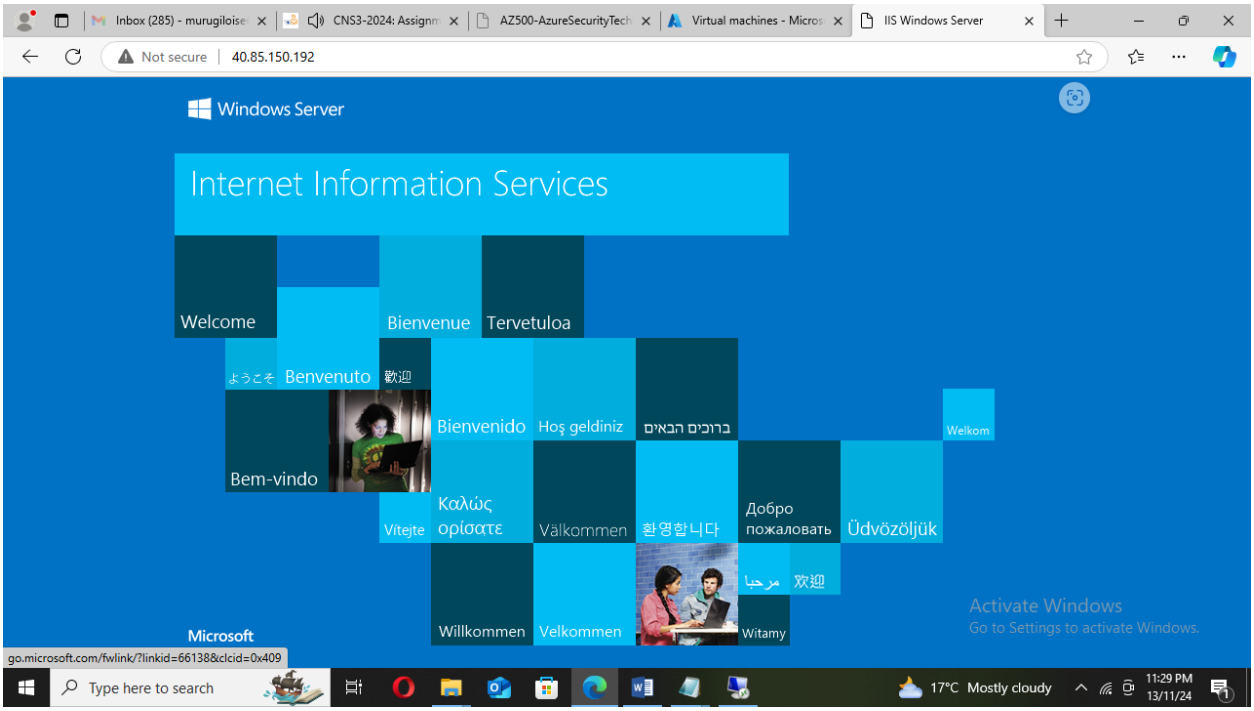


Week 8 Assignment 2: Network Security Groups and Application Security Groups

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



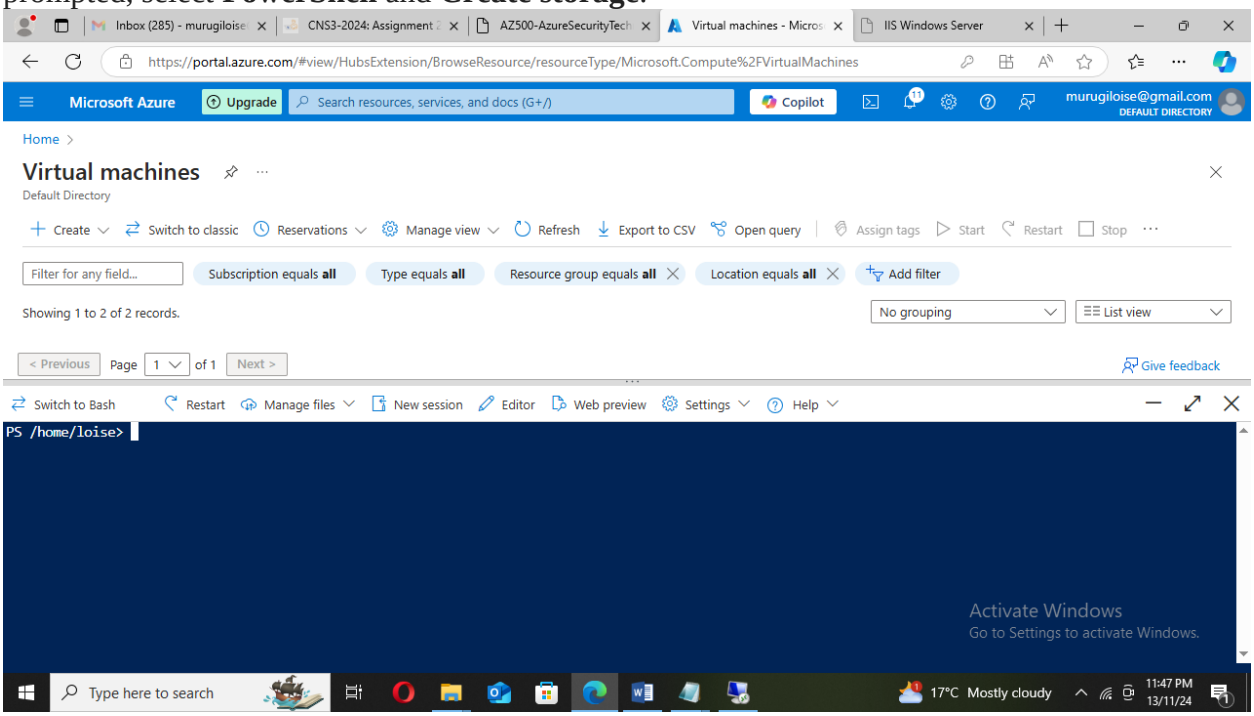
9. Open another browser tab and navigate to IP address you identified in the previous step. From the screenshot below, we were able to access the address 40.85.150.192 of IIS welcome page.



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

Clean up resources

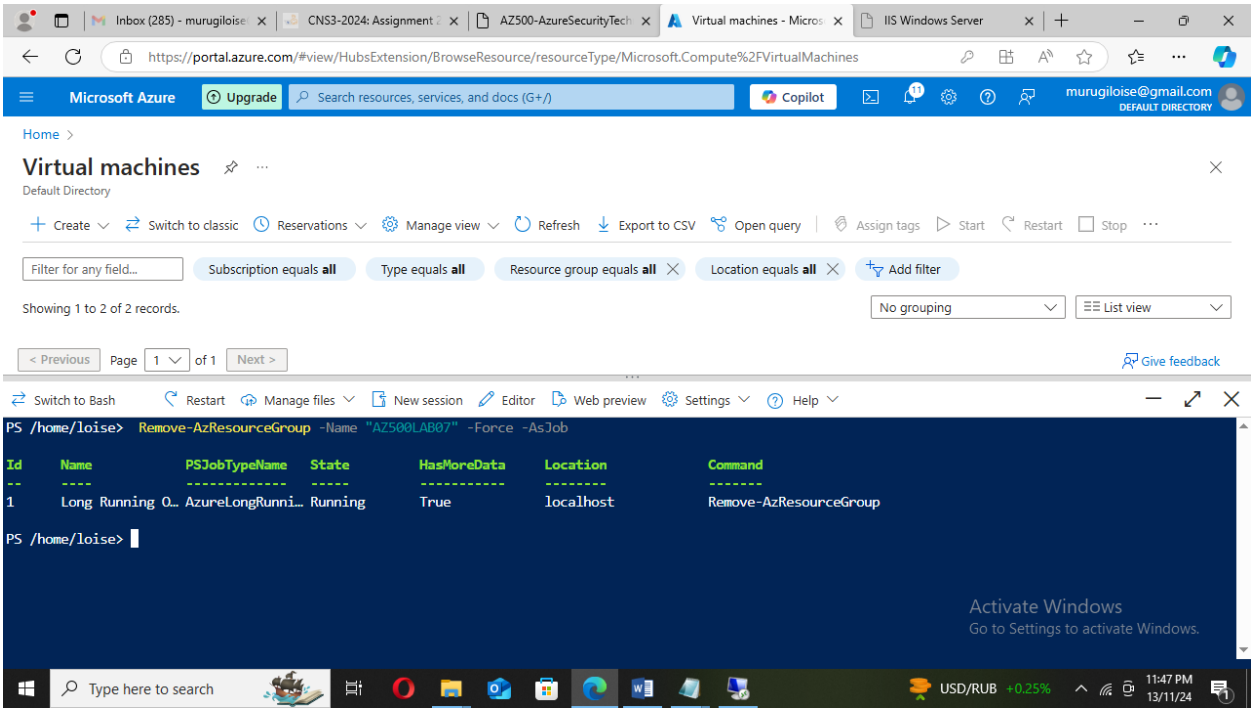
1. Open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, select **PowerShell** and **Create storage**.



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



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 myVMMgmnt 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.