



Microsoft ADC Cybersecurity Skilling Program

Week 6 Lab Assignment

Student Name: ALEX EVANS NJIRU MBOGO

Student ID: adc-css02-25064

AZ-500

Lab 02: Network Security Groups and Application Security Groups

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.

For all the resources in this lab, we are using the **East US** region. Verify with your instructor this is the region to use for class.

Lab objectives

In this lab, you will complete the following exercises:

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

Exercise 1: Create the virtual networking infrastructure

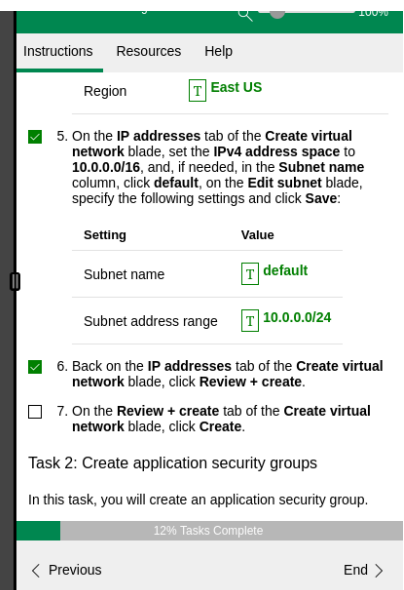
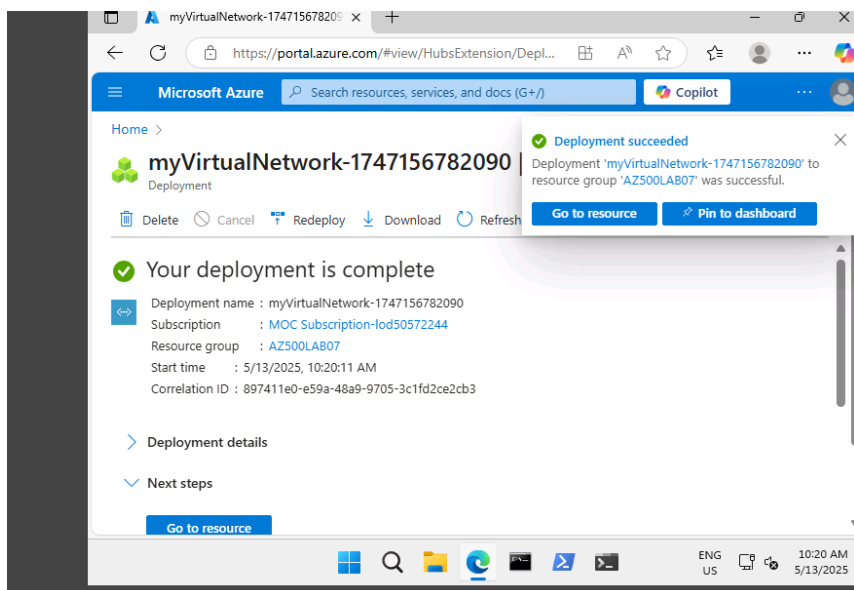
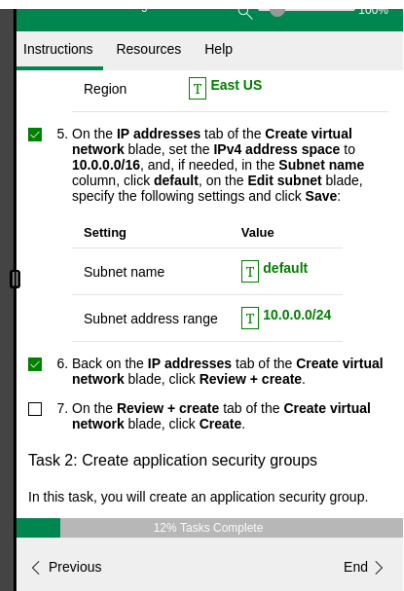
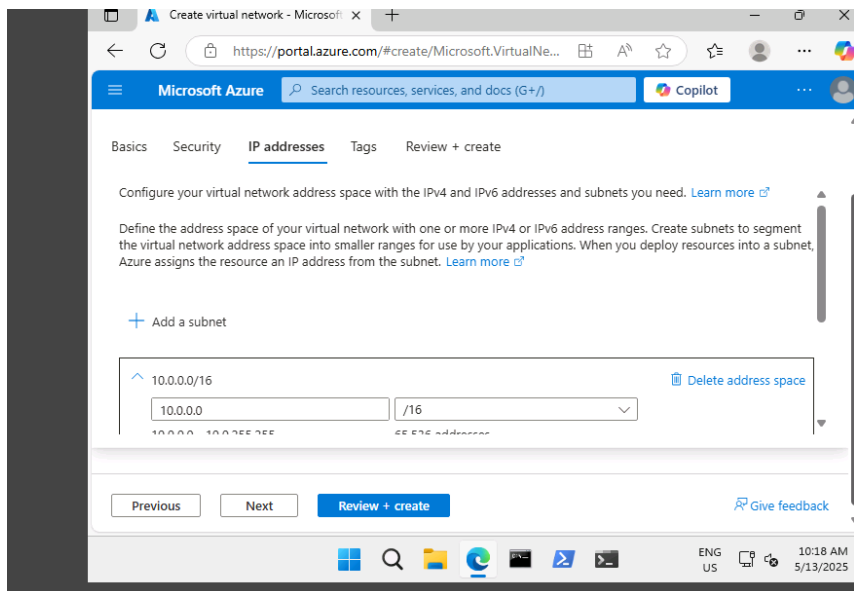
Estimated timing: 20 minutes

In this exercise, you will complete the following tasks:

- Task 1: Create a virtual network with one subnet.
- Task 2: Create two application security groups.
- Task 3: Create a network security group and associate it with the virtual network subnet.
- Task 4: Create inbound NSG security rules to all traffic to web servers and RDP to the management servers.

Task 1: Create a virtual network

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



Task 2: Create application security groups

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

Microsoft Azure

Search resources, services, and docs (G+J)

Copilot

Home > Application security groups >

Create an application security group

Validation passed

Basics Tags Review + create

Summary

Basics

SubscriptionMOC Subscription-Iod50572244

Resource groupAZ500LAB07

LocationEast US

NamemyAsgWebServers

Create

< Previous

Next >

Download a template for automation

InstructionsResourcesHelp

Resource groupAZ500LAB07

NamemyAsgWebServers

RegionEast US

This group will be for the web servers.

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

5. Navigate back to the **Application security groups** blade and click **+ Create**.

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

Setting	Value
Resource group	AZ500LAB07
Name	myAsgMgmtServers

20% Tasks Complete

< Previous

End >

Microsoft Azure

Search resources, services, and docs (G+J)

Copilot

Home >

Microsoft.ApplicationSecurityGroup | Overview

Deployment

Delete Cancel Redeploy Download Refresh

Your deployment is complete

Deployment name : Microsoft.ApplicationSecurityGroup

Subscription : MOC Subscription-Iod50572244

Resource group : AZ500LAB07

Start time : 5/13/2025, 10:22:44 AM

Correlation ID : 25a6e0ab-21f2-4d46-9c9a-121d054f60b3

> Deployment details

> Next steps

Go to resource

InstructionsResourcesHelp

RegionEast US

This group will be for the web servers.

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

5. Navigate back to the **Application security groups** blade and click **+ Create**.

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

Setting	Value
Resource group	AZ500LAB07
Name	myAsgMgmtServers
Region	East US

This group will be for the management servers.

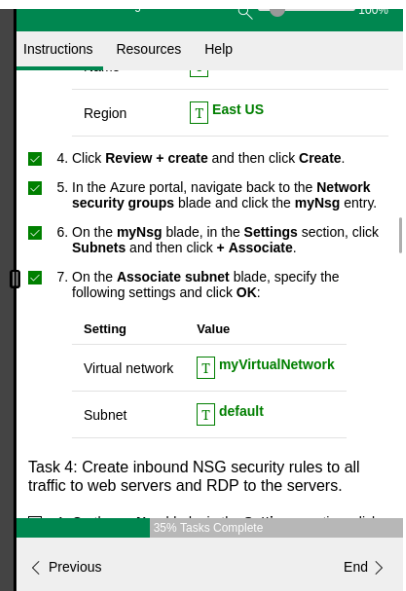
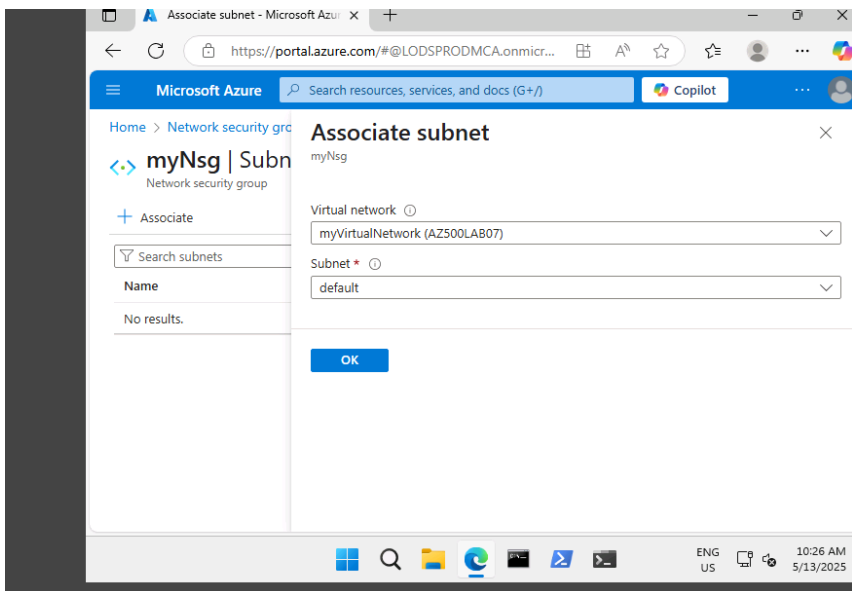
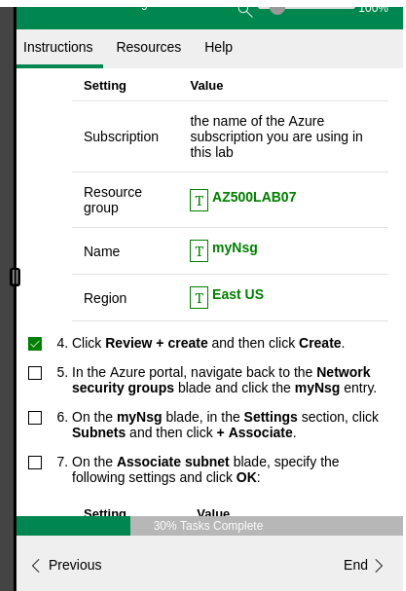
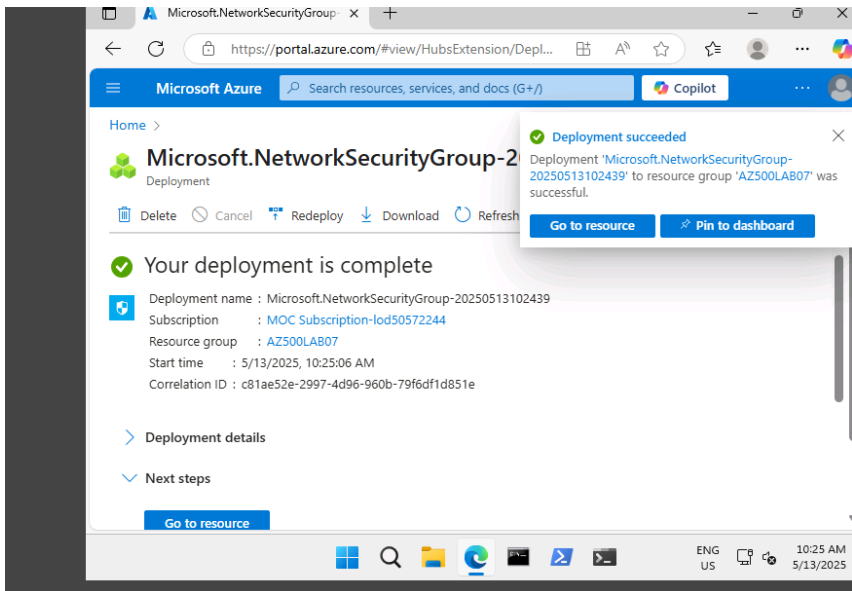
23% Tasks Complete

< Previous

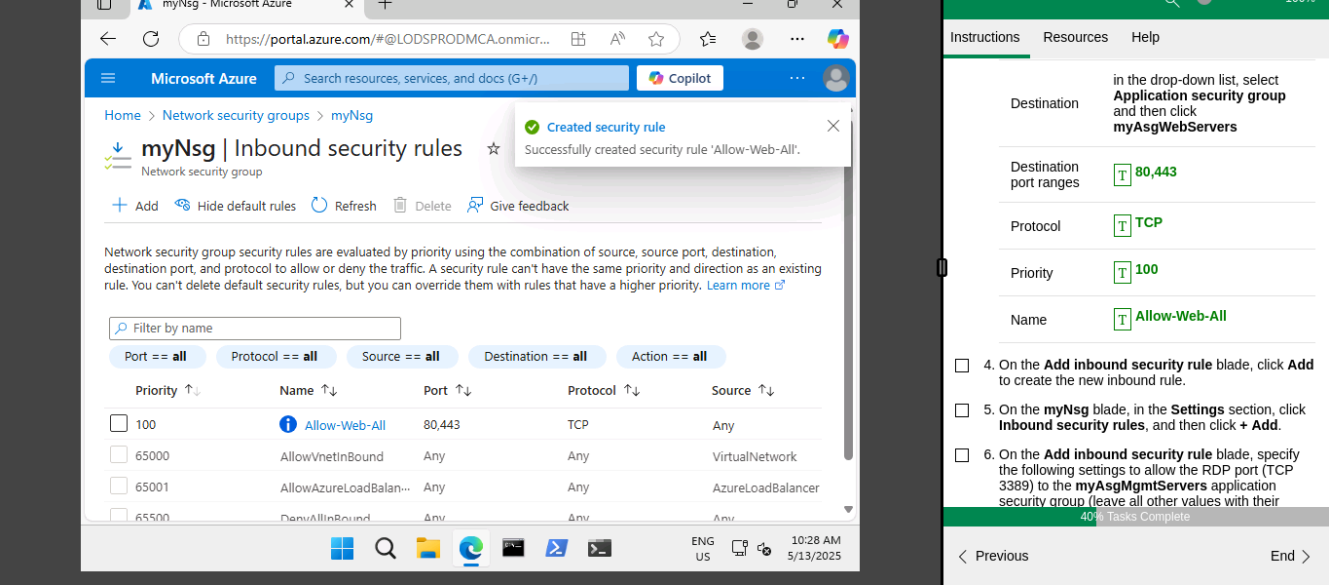
End >

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

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



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



The screenshot shows the Microsoft Azure portal interface for the 'myNsg' Network Security Group. The 'Inbound security rules' section is active, displaying a list of rules. A notification indicates that a security rule named 'Allow-Web-All' has been successfully created. The 'Add inbound security rule' blade is open on the right, showing the configuration for the 'Allow-Web-All' rule.

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

Allow-Web-All Rule Configuration:

- Destination: myAsgWebServers
- Destination port ranges: 80,443
- Protocol: TCP
- Priority: 100
- Name: Allow-Web-All

Instructions:

- On the **Add inbound security rule** blade, click **Add** to create the new inbound rule.
- On the **myNsg** blade, in the **Settings** section, click **Inbound security rules**, and then click **Add**.
- On the **Add inbound security rule** blade, specify the following settings to allow the RDP port (TCP 3389) to the **myAsgMgmtServers** application security group (leave all other values with their default values):

Allow-RDP-All Rule Configuration:

- Destination port ranges: 3389
- Protocol: TCP
- Priority: 110
- Name: Allow-RDP-All

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

Exercise 2: Deploy virtual machines and test network filters

Estimated time: 25 minutes

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

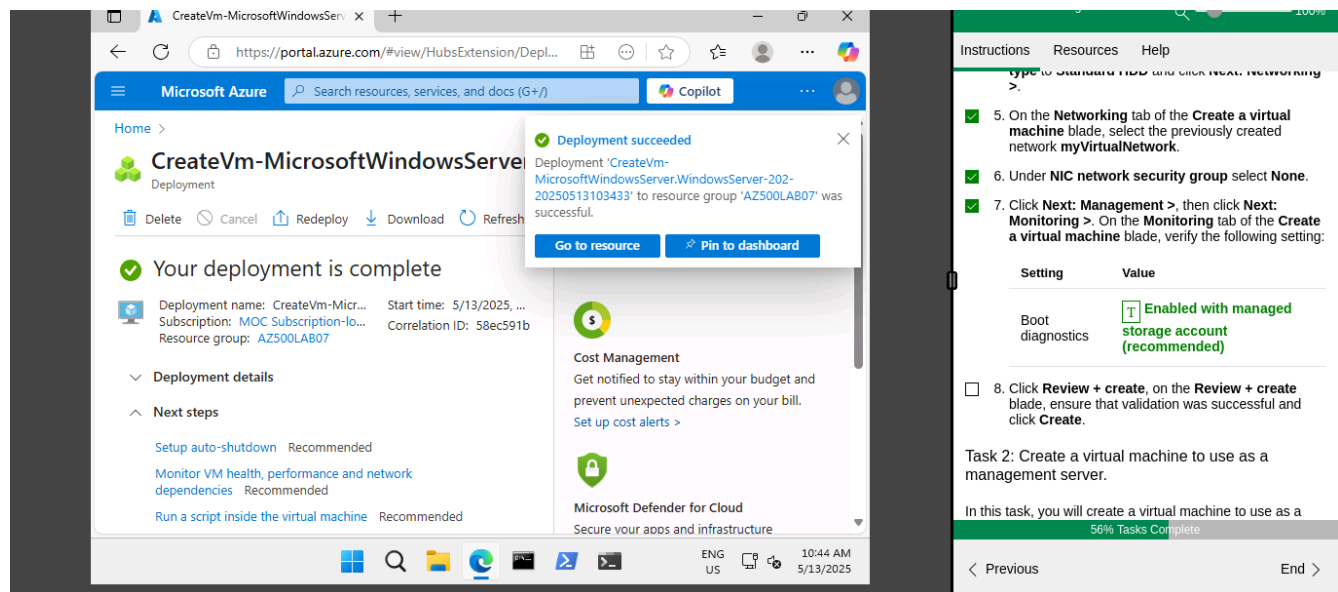
Exercise 2: Deploy virtual machines and test network filters

you will complete the following tasks:

- Task 1: Create a virtual machine to use as a web server.
- Task 2: Create a virtual machine to use as a management server.
- Task 3: Associate each virtual machines network interface to it's application security group.
- Task 4: Test the network traffic filtering.

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.



The screenshot displays the Microsoft Azure portal interface. On the left, a deployment blade for 'CreateVm-MicrosoftWindowsServer' is shown, indicating that the deployment is complete. A notification banner at the top right states 'Deployment succeeded' for the deployment 'CreateVm-MicrosoftWindowsServer-202-20250513103433' to resource group 'AZ500LAB07'. The main content area shows deployment details and next steps. On the right, a sidebar contains a list of tasks and a table of settings.

Deployment Details:

- Deployment name: CreateVm-Mic...
- Subscription: MOC Subscription-Lo...
- Resource group: AZ500LAB07
- Start time: 5/13/2025, ...
- Correlation ID: 58ec591b

Next steps:

- Setup auto-shutdown Recommended
- Monitor VM health, performance and network dependencies Recommended
- Run a script inside the virtual machine Recommended

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

Tasks:

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

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

56% Tasks Complete

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

< Previous End >

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

The screenshot shows the Microsoft Azure portal interface. The main content area displays the 'CreateVm-MicrosoftWindowsServer.WindowsServer...' deployment page. The deployment is complete, with a green checkmark and the message 'Your deployment is complete'. Below this, there are sections for 'Deployment details' and 'Next steps'. The right sidebar shows a task list for 'Network Security Groups and Application Security' with 67% completion. The task list includes instructions for clicking 'Review + create' and clicking 'Create'.

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.

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.

The screenshot shows the Microsoft Azure portal interface. The main content area displays the 'myVmWeb | Application security groups' page. The page shows the 'myVmWeb' virtual machine and its network interface 'myvmweb173 (primary) / ipconfig1 (primary)'. The right sidebar shows a task list for 'Network Security Groups and Application Security' with 75% completion. The task list includes instructions for navigating back to the 'Virtual machines' blade, clicking the 'myVMWeb' entry, and clicking 'Add 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.

myVMMgmt - Microsoft Azure

https://portal.azure.com/#@LODSPRODMCA.onmicr...

Microsoft Azure

Search resources, services, and docs (G+J)

Copilot

Home > Compute infrastructure > Virtual machines > myVMMgmt

myVMMgmt | Application security groups

Virtual machine

This is a new experience. [Please provide feedback](#)

+ Add application security groups X Remove Refresh Give feedback

Network interface / IP configuration

myvmgmt722_z1 (primary) / ipconfig1 (primary)

☐ Name

Resource group

☐ myAsgMgmtServers

AZ500LAB07

ENG US

10:58 AM

5/13/2025

Network Security Groups and Application Security ...

37 Minutes Remaining

100%

Instructions Resources Help

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**.

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

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 myVMMgmt virtual machine. You should be able to connect from the internet to the myVMWeb virtual machine and view the default IIS web page.

78% Tasks Complete

< Previous End >

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.

myVMMgmt - Microsoft Azure

https://portal.azure.com/#@LODSPRODMCA...

Microsoft Azure

Search resou

Downloads

Just-in-time policy
Unsupported by plan

Most common

Native RDP

Connect via native RD
needed. Recommended

Public IP address (135.

Select

Do

More ways to con

Windows Security

Enter your credentials

These credentials will be used to connect to 135.222.40.111.

Student

Password

BASE22C\Student

☐ Remember me

More choices

OK Cancel

ENG US

11:01 AM

5/13/2025

Network Security Groups and Application Security ...

35 Minutes Remaining

100%

Instructions Resources Help

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 myVMMgmt virtual machine. You should be able to connect from the internet to the myVMWeb virtual machine and view the default IIS web page.

83% Tasks Complete

< Previous End >

135.222.40.111

Student

Please wait for the User Profile Service

Network Security Groups and Application Security ...

34 Minutes Remaining

Instructions Resources Help

Password **Please use your personal password created in Lab 02 > Exercise 1 > Task 1 > Step 9.**

Verify that the Remote Desktop connection was successful. At this point you have confirmed you can connect via Remote Desktop to myVMMgmt.

- ☐ 4. In the Azure portal, navigate to the **myVMWeb** virtual machine blade.
- ☐ 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**:

```
powershell  
Install-WindowsFeature -name Web-Se
```

Wait for the installation to complete. This

84% Tasks Complete

< Previous End >

https://labclient.labondemand.com/LabClient/74f2913c-84ec-45e1-a83c-450e65f175c9

Run Command Script x Script - Search x IIS Windows Server x

Not secure | 20.169.162.42

IIS

ENG US 11:13 AM 5/13/2025

Network Security Groups and Application Security ...

22 Minutes Remaining

Instructions Resources Help

- ☒ 8. On the **myVMWeb** blade, identify the **Public IP address** of the myVmWeb Azure VM.
- ☒ 9. Open another browser tab and navigate to IP address you identified in the previous step.

The browser page should display the default IIS welcome page because port 80 is allowed inbound from the internet based on the setting of the **myAsgWebServers** application security group. The network interface of the myVMWeb Azure VM is associated with that application security group.

Result: You have validated that the NSG and ASG configuration is working and traffic is being correctly managed.

Clean up resources

Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs.

- ☐ 1. Open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, select

93% Tasks Complete

< Previous End >

Result: You have validated that the NSG and ASG configuration is working and traffic is being correctly managed.

Summary

This week I went through the following :

- Create a virtual network with one subnet.
- Task 2: Create two application security groups.
- Task 3: Create a network security group and associate it with the virtual network subnet.
- Task 4: Create inbound NSG security rules to all traffic to web servers and RDP to the management servers.