Microsoft ADC Cybersecurity Skilling Program

Week 6 Lab Assignment

Student Name: Vincent Onchieku Collins

Student ID: ADC-CSS02-25052

Introduction

In today's cloud environments, securing network traffic is a fundamental aspect of infrastructure deployment. This lab focuses on implementing and testing Azure Network Security Groups (NSGs) and Application Security Groups (ASGs) to control and filter network access to virtual machines. The scenario simulates a real-world requirement where an organization needs to separate Web Servers and Management Servers using ASGs, allowing public web access only to the web servers and secure RDP access to management servers. The exercises are designed to guide students through the creation of a virtual network, security groups, and virtual machines, and demonstrate how traffic is filtered based on NSG rules associated with ASGs.
It included the following tasks:

1. Exercise 1: Create the virtual networking infrastructure

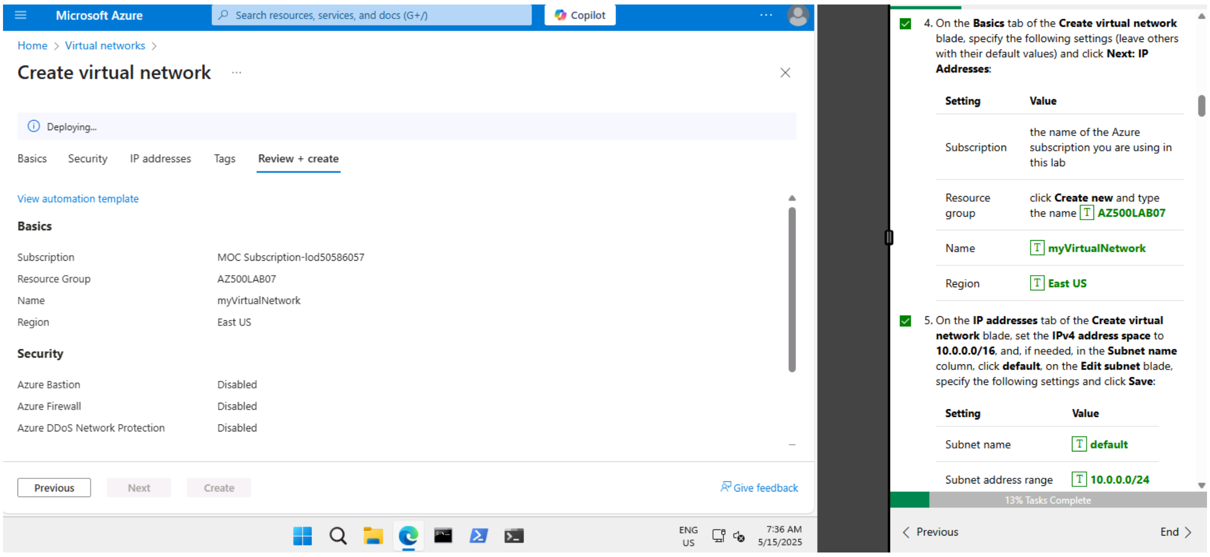
- Task 1: Create a virtual network with one subnet.
- Task 2: Create two application security groups.
- Task 3: Create a network security group and associate it with the virtual network subnet.
- Task 4: Create inbound NSG security rules to all traffic to web servers and RDP to the management servers.

2. Exercise 2: Deploy virtual machines and test the network filters

- 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.

Exercise 1: Create the virtual networking infrastructure

I began by creating a virtual network named myVirtualNetwork with a subnet using the IP address range 10.0.0.0/24. I then created two Application Security Groups (ASGs): myAsgWebServers for the web servers and myAsgMgmtServers for the management servers. Next, I set up a Network Security Group (NSG) called myNsg and associated it with the subnet I had just created. To control traffic, I added inbound rules to the NSG: one rule allowed HTTP and HTTPS traffic (TCP ports 80 and 443) to the web server ASG, and another rule allowed Remote Desktop Protocol (RDP) access (TCP port 3389) to the management server ASG.



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Virtual networks >

Create virtual network

Deploying...

Basics

Subscription	MOC Subscription-lod50586057
Resource Group	AZ500LAB07
Name	myVirtualNetwork
Region	East US

Security

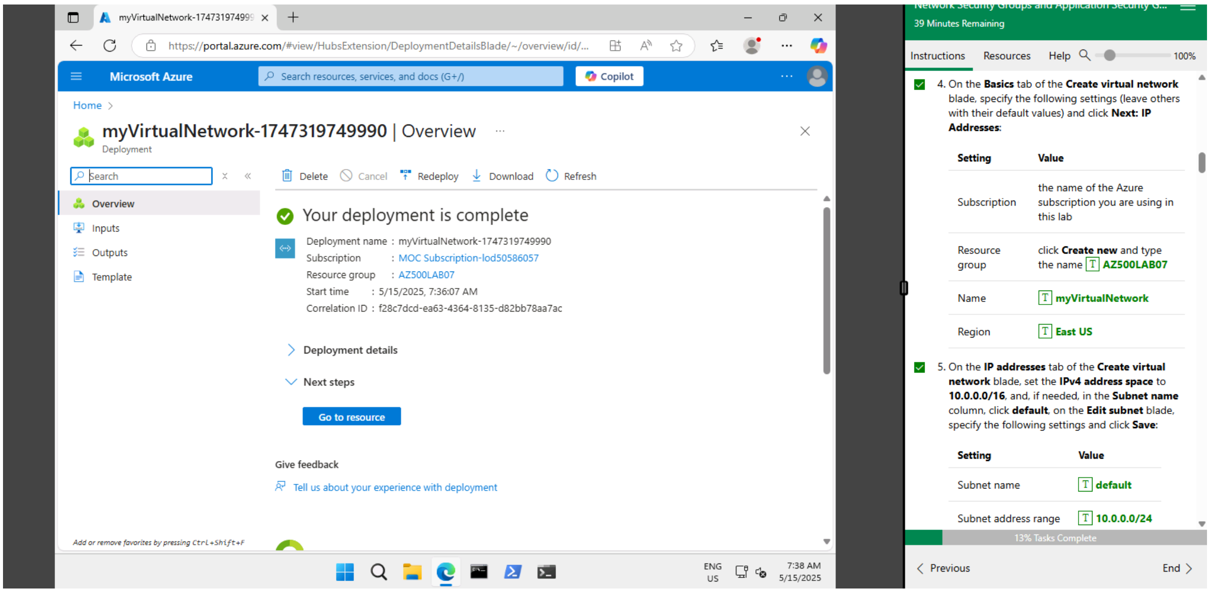
Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

☑ 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 T **AZ500LAB07**
Name	T **myVirtualNetwork**
Region	T **East US**

☑ 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	T **default**
Subnet address range	T **10.0.0.0/24**



myVirtualNetwork-17473197499
https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home >

myVirtualNetwork-1747319749990 | Overview

Deployment

Your deployment is complete

Deployment name : myVirtualNetwork-1747319749990
Subscription : MOC Subscription-lod50586057
Resource group : AZ500LAB07
Start time : 5/15/2025, 7:36:07 AM
Correlation ID : f28c7dcd-ea63-4364-8135-d82bb78aa7ac

Give feedback

Tell us about your experience with deployment

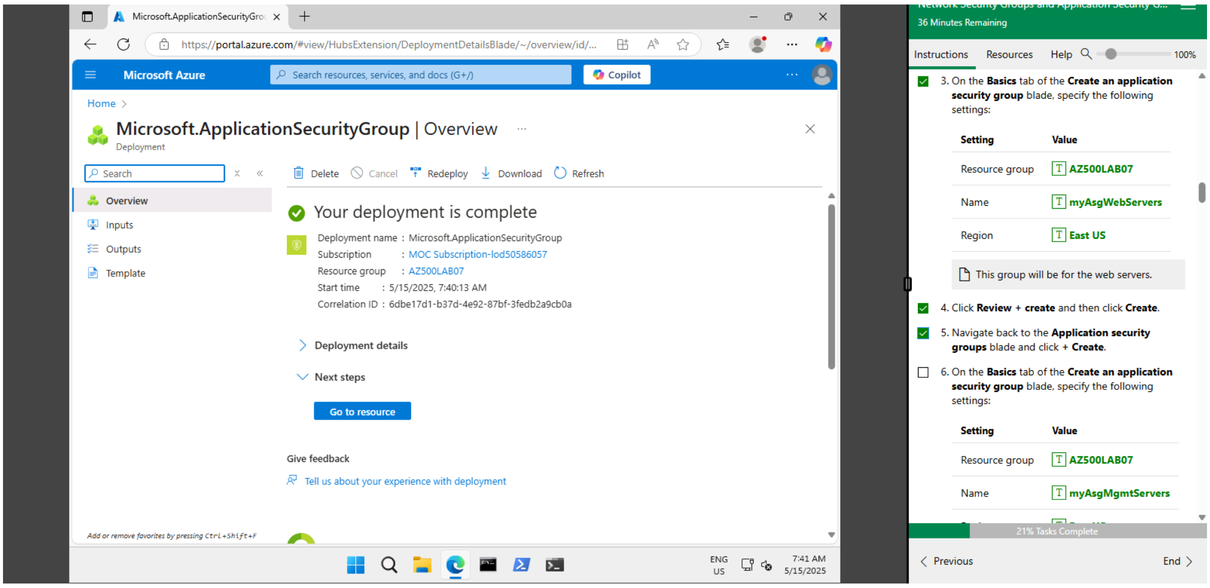
Add or remove favorites by pressing Ctrl+Shift+F

☑ 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 T **AZ500LAB07**
Name	T **myVirtualNetwork**
Region	T **East US**

☑ 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	T **default**
Subnet address range	T **10.0.0.0/24**



Microsoft.ApplicationSecurityGro
https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Add or remove favorites by pressing Ctrl+Shift+F
ENG
US
7:41 AM
5/15/2025
Instructions
Resources
Help
100%
21% Tasks Complete
Previous
End

Microsoft.ApplicationSecurityGroup | Overview

Deployment

Your deployment is complete

Deployment name : Microsoft.ApplicationSecurityGroup
Subscription : MOC Subscription-lod50586057
Resource group : AZ500LAB07
Start time : 5/15/2025, 7:40:13 AM
Correlation ID : 6dbe17d1-b37d-4e92-87bf-3fedb2a9cb0a

Deployment details

Next steps

Go to resource

Give feedback

Tell us about your experience with deployment

Network Security Groups and Application Security G...

36 Minutes Remaining

☑ 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

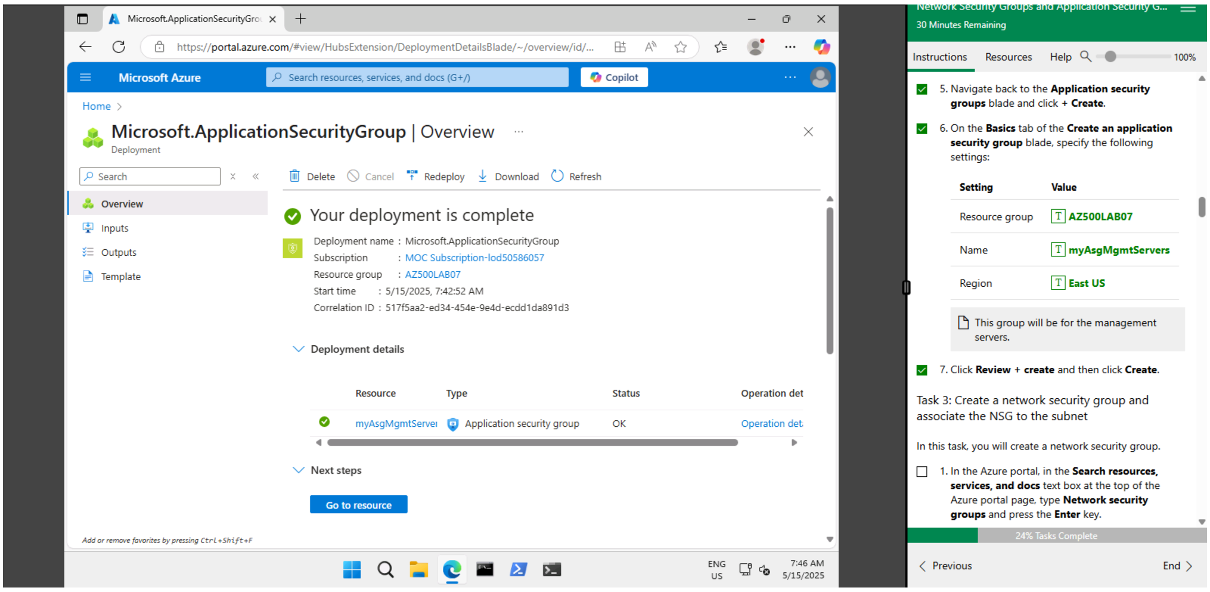
This group will be for the web servers.

☑ 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



Microsoft.ApplicationSecurityGro
https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Add or remove favorites by pressing Ctrl+Shift+F
ENG
US
7:46 AM
5/15/2025
Instructions
Resources
Help
100%
24% Tasks Complete
Previous
End

Microsoft.ApplicationSecurityGroup | Overview

Deployment

Your deployment is complete

Deployment name : Microsoft.ApplicationSecurityGroup
Subscription : MOC Subscription-lod50586057
Resource group : AZ500LAB07
Start time : 5/15/2025, 7:42:52 AM
Correlation ID : 517f5aa2-ed34-454e-9e4d-ecdd1da891d3

Deployment details

Resource	Type	Status	Operation det
myAsgMgmtServe	Application security group	OK	Operation det

Next steps

Go to resource

Network Security Groups and Application Security G...

30 Minutes Remaining

☑ 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

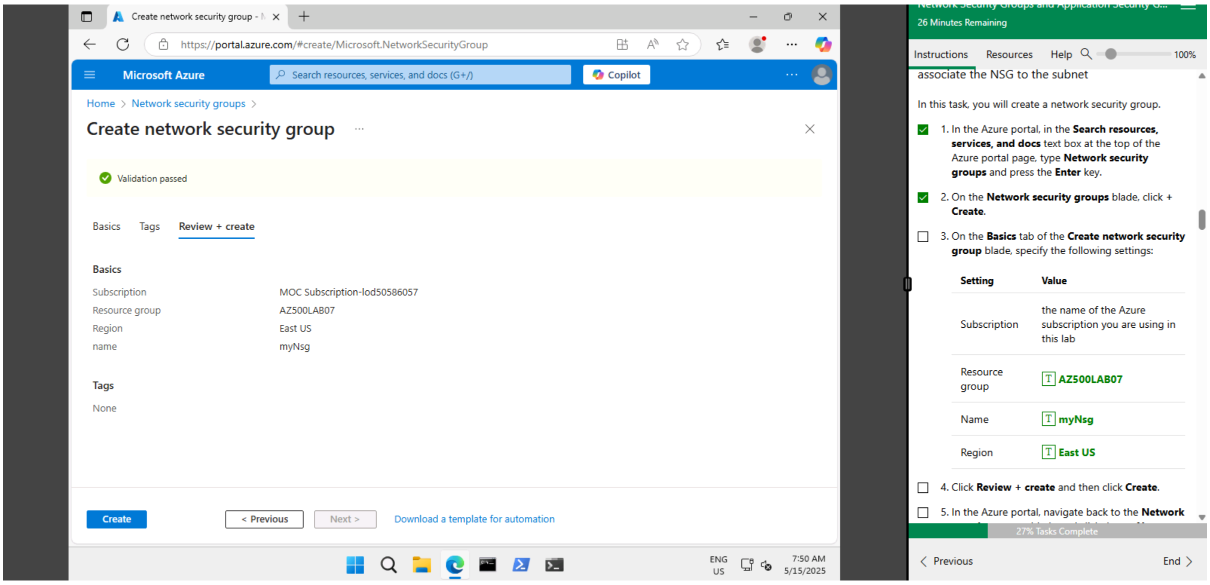
This group will be for the management servers.

☑ 7. Click **Review + create** and then click **Create**.

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

In this task, you will create a network 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 **Network security groups** and press the **Enter** key.


Create network security group - Microsoft Azure
https://portal.azure.com/#create/Microsoft.NetworkSecurityGroup
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Network security groups >

Create network security group

Validation passed

Basics
Tags
Review + create

Basics

Subscription	MOC Subscription-lod50586057
Resource group	AZ500LAB07
Region	East US
name	myNsg

Tags

None

Create
< Previous
Next >
Download a template for automation
ENG US
7:50 AM 5/15/2025
Network Security Groups and Application Security G...
26 Minutes Remaining
Instructions
Resources
Help
100%

associate the NSG to the subnet

In this task, you will create a network 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 **Network security groups** and press the **Enter** key.

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

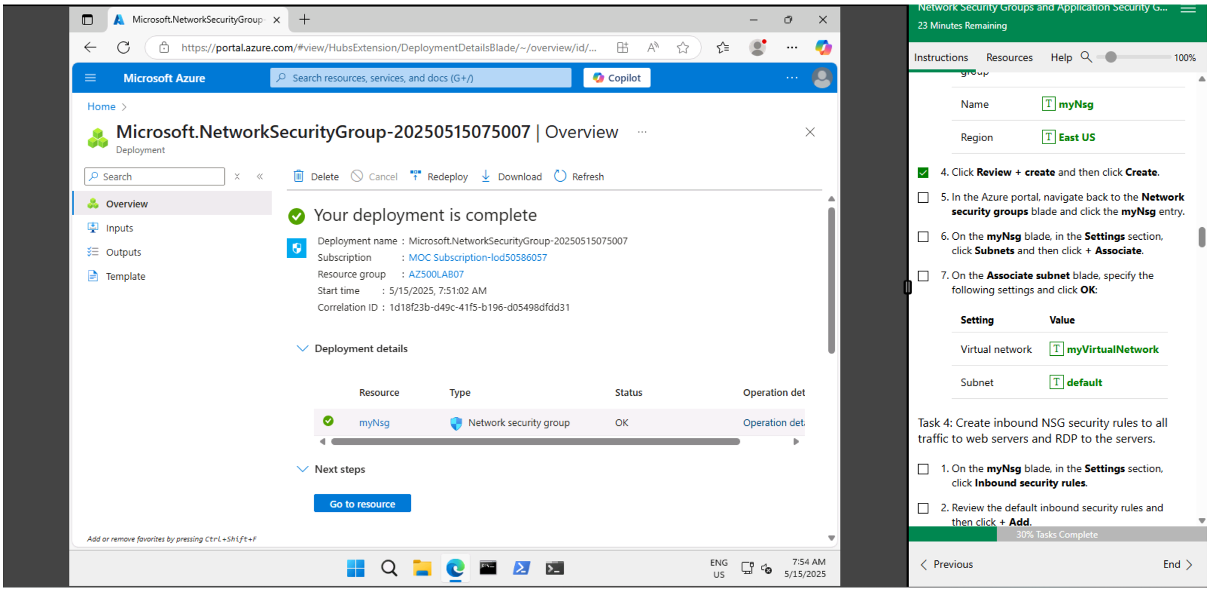
□ 3. On the **Basics** tab of the **Create network security group** blade, specify the following settings:

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

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

□ 5. In the Azure portal, navigate back to the **Network**

27% Tasks Complete
Previous
End


Microsoft.NetworkSecurityGroup-
https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home >

Microsoft.NetworkSecurityGroup-20250515075007 | Overview

Deployment

Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh

Your deployment is complete

Deployment name : Microsoft.NetworkSecurityGroup-20250515075007
Subscription : MOC Subscription-lod50586057
Resource group : AZ500LAB07
Start time : 5/15/2025, 7:51:02 AM
Correlation ID : 1d18f23b-d49c-41f5-b196-d05498dfdd31

Deployment details

	Resource	Type	Status	Operation det
✓	myNsg	Network security group	OK	Operation det

Next steps

Go to resource
Add or remove favorites by pressing Ctrl+Shift+F
ENG US
7:54 AM 5/15/2025
Network Security Groups and Application Security G...
23 Minutes Remaining
Instructions
Resources
Help
100%

Name	myNsg
Region	East US

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

□ 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**.

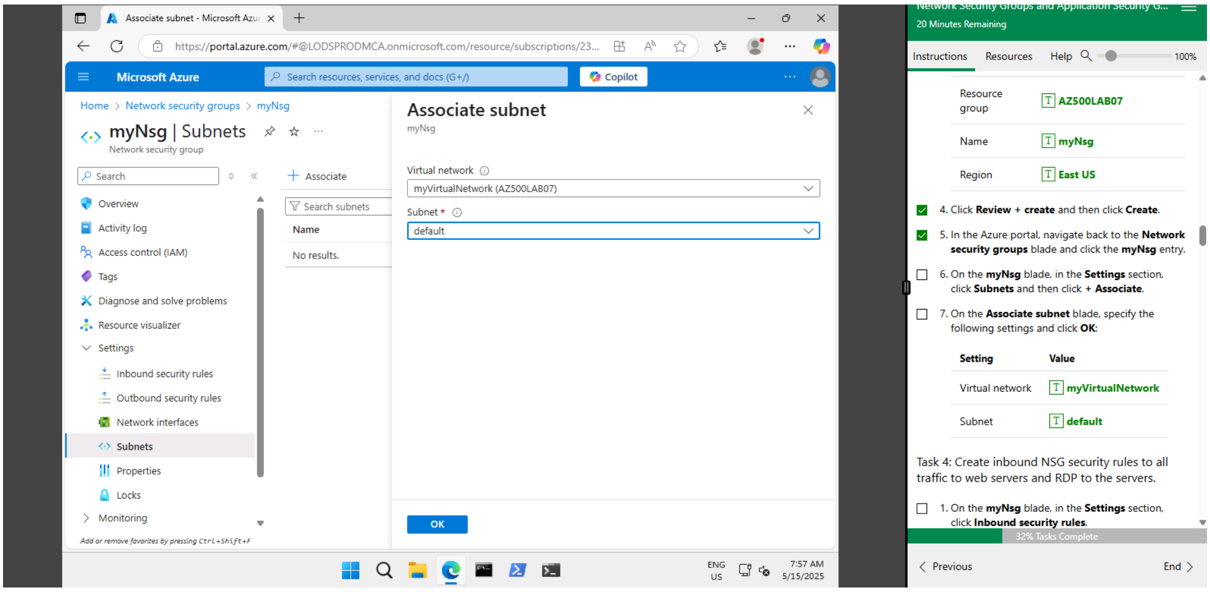
□ 7. On the **Associate subnet** blade, specify the following settings and click **OK**:

Setting	Value
Virtual network	myVirtualNetwork
Subnet	default

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**.

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



Associate subnet

myNsg

Virtual network: myVirtualNetwork (AZ500LAB07)

Subnet *: default

Network Security Groups and Application Security G...

20 Minutes Remaining

Instructions Resources Help 100%

Resource group	AZ500LAB07
Name	myNsg
Region	East US

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

☑ 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**:

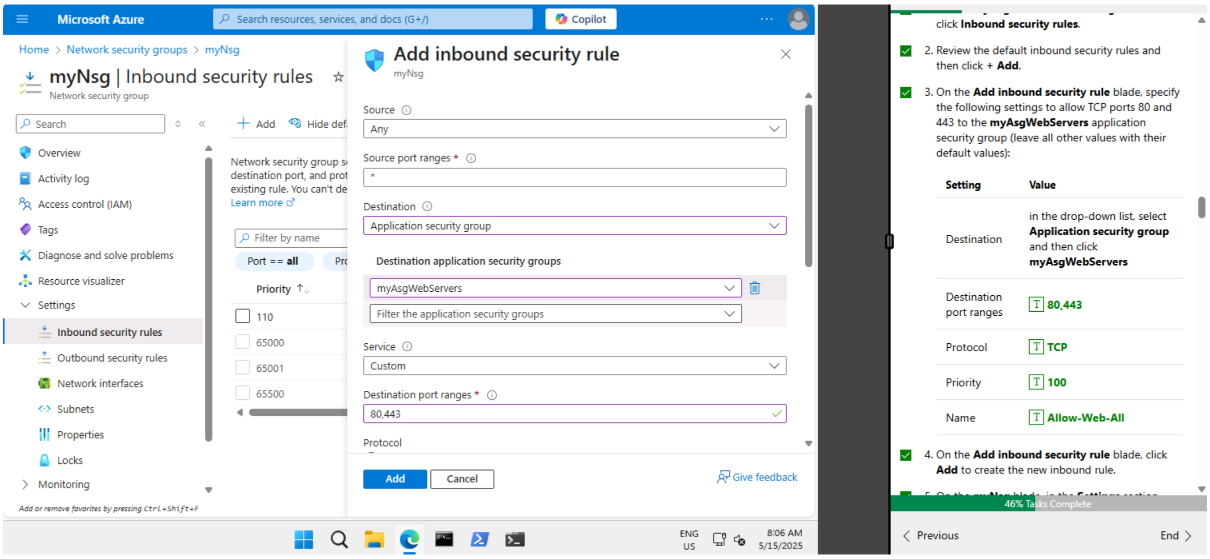
Setting	Value
Virtual network	myVirtualNetwork
Subnet	default

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**.

32% Tasks Complete

< Previous End >



Add inbound security rule

myNsg

Source: Any

Source port ranges *: *

Destination: Application security group

Destination application security groups: myAsgWebServers

Filter the application security groups

Service: Custom

Destination port ranges *: 80,443

Protocol

click **Inbound security rules**.

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

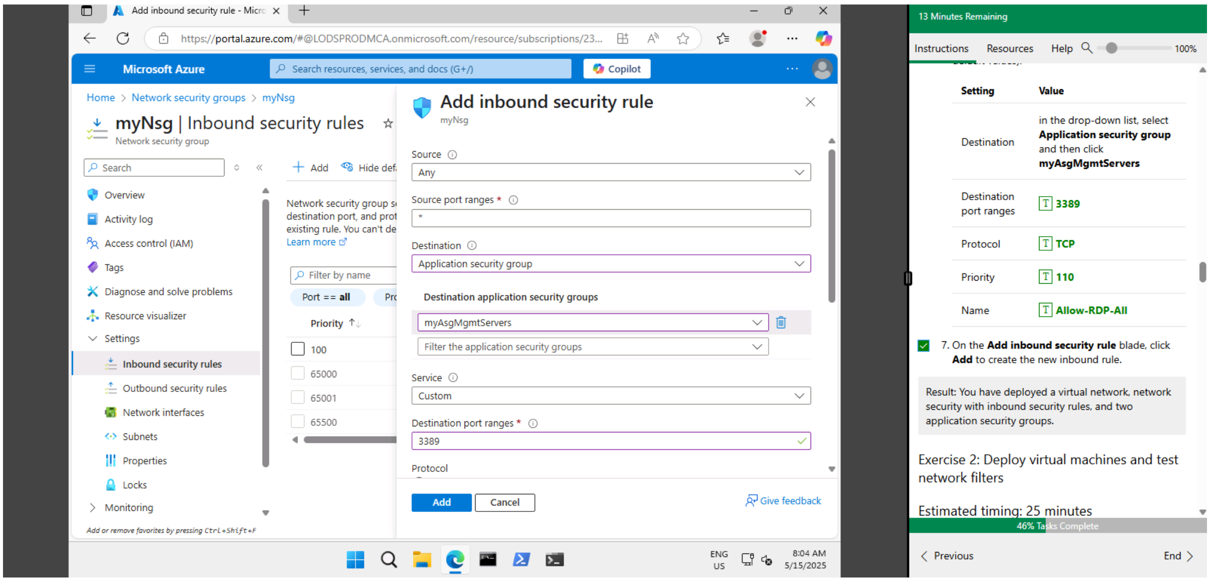
☑ 3. On the **Add inbound security rule** blade, specify the following settings to allow TCP ports 80 and 443 to the **myAsgWebServers** application security group (leave all other values with their default values):

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

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

46% Tasks Complete

< Previous End >


Add inbound security rule - Micro
https://portal.azure.com/#@LODSPRODMCA.onmicrosoft.com/resource/subscriptions/23...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Network security groups > myNsg
myNsg | Inbound security rules
Network security group
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Monitoring
Add or remove favorites by pressing Ctrl+Shift+F
Add
Hide def
Network security group s
destination port, and prot
existing rule. You can't de
Learn more
Filter by name
Port == all
Pr
Priority
100
65000
65001
65500
ENG
US
8:04 AM
5/15/2025

Add inbound security rule

myNsg

Source: Any

Source port ranges *: *

Destination: Application security group

Destination application security groups: myAgsMgmtServers

Filter the application security groups

Service: Custom

Destination port ranges *: 3389

Protocol

13 Minutes Remaining

Setting	Value
Destination	in the drop-down list, select **Application security group** and then click **myAsgMgmtServers**
Destination port ranges	**3389**
Protocol	**TCP**
Priority	**110**
Name	**Allow-RDP-All**

☑ 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.

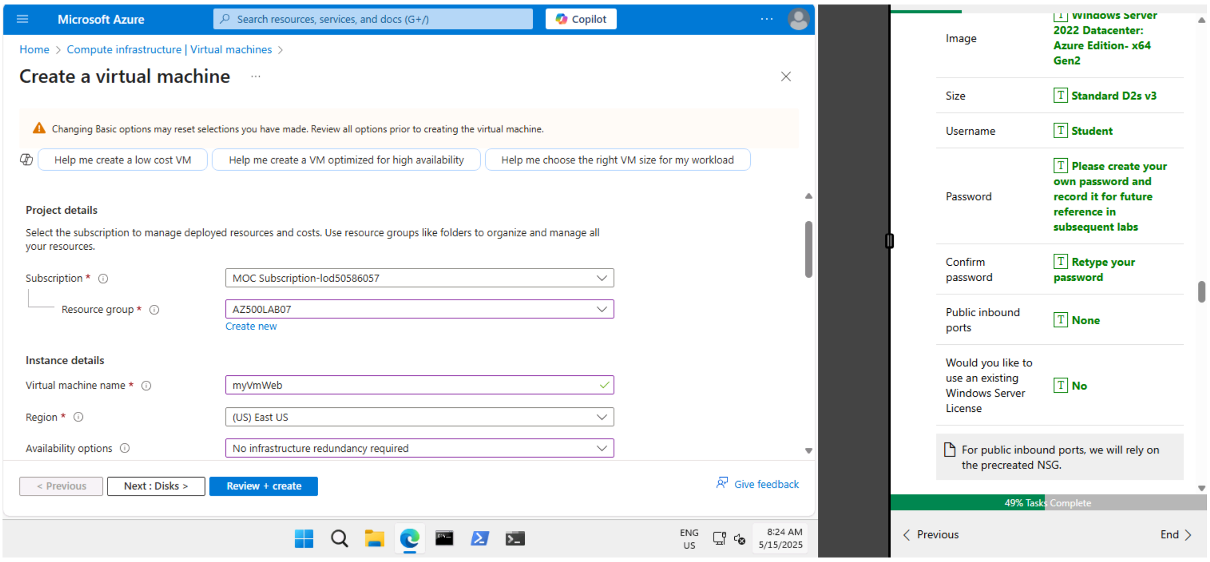
Exercise 2: Deploy virtual machines and test network filters

Estimated timing: 25 minutes

46% Tasks Complete

Exercise 2: Deploy virtual machines and test the network filters

In this lab, I explored the Microsoft Service Trust Portal to understand how Microsoft maintains transparency around its compliance and data protection practices. I accessed the portal via aka.ms/STP, signed in using the provided tenant admin credentials, and accepted the Microsoft Non-Disclosure Agreement to unlock additional compliance content. I navigated to the Certifications, Regulations, and Standards section and selected ISO/IEC to view the related documents. Using the ellipsis menu, I saved a document to My Library and confirmed the action by verifying it appeared in the My Library section. I then explored the Industry and Regional Resources, selecting Financial Services to view region-specific compliance documents. Lastly, I accessed Resources for your Organization to review documents tied to my tenant's subscription. In the second task, I navigated to the Privacy and Data Protection section and followed the Learn more link to visit the Microsoft Trust Center, where I reviewed Microsoft's approach to privacy and data protection across services. This lab provided a comprehensive overview of Microsoft's transparency resources available for compliance assurance.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Compute infrastructure | Virtual machines >

Create a virtual machine

Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.

Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : MOC Subscription-lod50586057

Resource group * : AZ500LAB07

Create new

Instance details

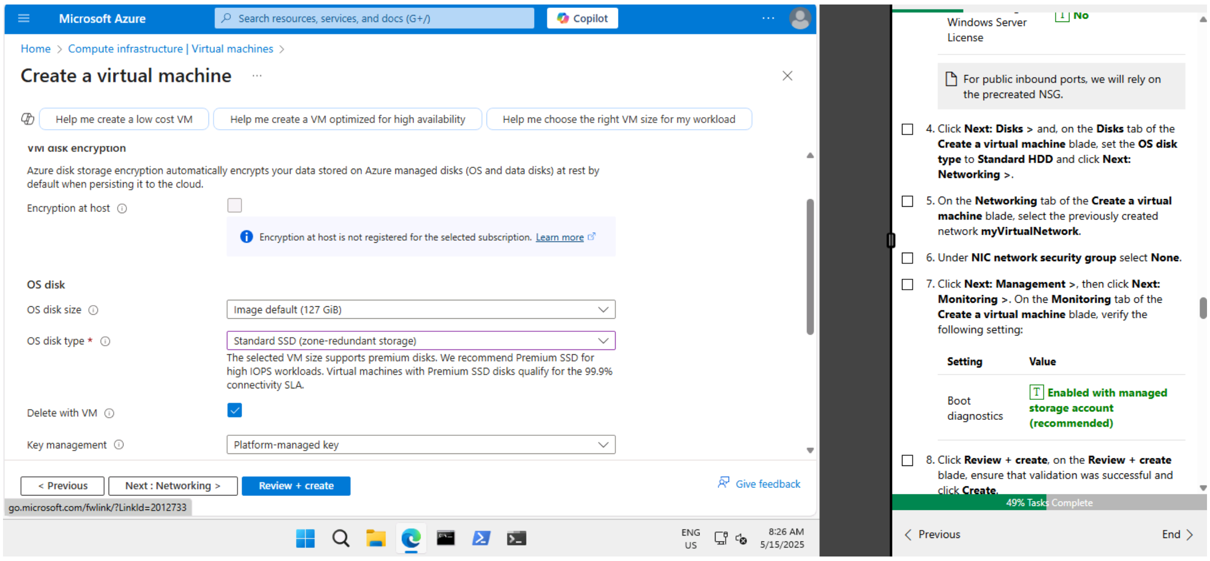
Virtual machine name * : myVmWeb

Region * : (US) East US

Availability options : No infrastructure redundancy required

Image	Windows Server 2022 Datacenter: Azure Edition- x64 Gen2
Size	Standard D2s v3
Username	Student
Password	Please create your own password and record it for future reference in subsequent labs
Confirm password	Retype your password
Public inbound ports	None
Would you like to use an existing Windows Server License	No

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



Microsoft Azure

Home > Compute infrastructure | Virtual machines >

Create a virtual machine

Help me create a low cost VM | Help me create a VM optimized for high availability | Help me choose the right VM size for my workload

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 SSD (zone-redundant storage) The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.
Delete with VM	☑
Key management	Platform-managed key

< Previous | Next : Networking > | Review + create | Give feedback

go.microsoft.com/fwlink/?LinkId=2012733

ENG US 8:26 AM 5/15/2025

Windows Server License	No

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

☐ 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**.

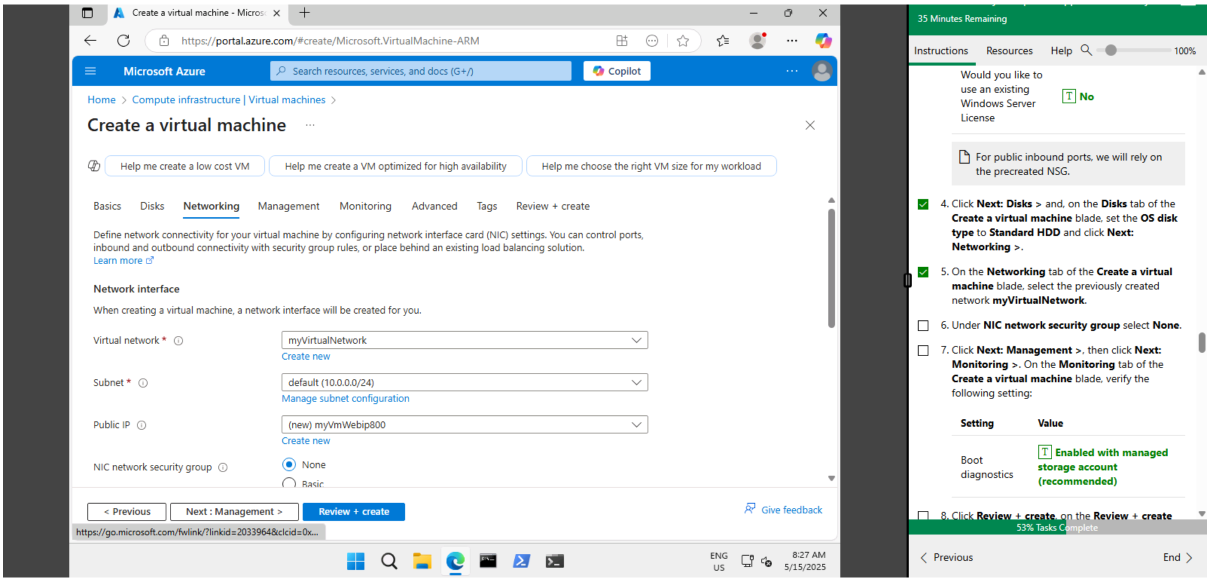
☐ 7. Click **Next: Management >**, then click **Next: Monitoring >**. On the **Monitoring** tab of the **Create a virtual machine** blade, verify the following setting:

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**.

49% Tasks Complete

< Previous | End >



Create a virtual machine - Micros

https://portal.azure.com/#create/Microsoft.VirtualMachine-ARM

Microsoft Azure

Home > Compute infrastructure | Virtual machines >

Create a virtual machine

Help me create a low cost VM | Help me create a VM optimized for high availability | Help me choose the right VM size for my workload

Basics | Disks | **Networking** | Management | Monitoring | Advanced | Tags | Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network *	myVirtualNetwork Create new
Subnet *	default (10.0.0.0/24) Manage subnet configuration
Public IP	(new) myVmWebip800 Create new
NIC network security group	● None ○ Basic

< Previous | Next : Management > | Review + create | Give feedback

https://go.microsoft.com/fwlink/?linkid=2033964&clcid=0x...

ENG US 8:27 AM 5/15/2025

35 Minutes Remaining

Instructions | Resources | Help | 100%

Would you like to use an existing Windows Server License	No

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

☑ 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**.

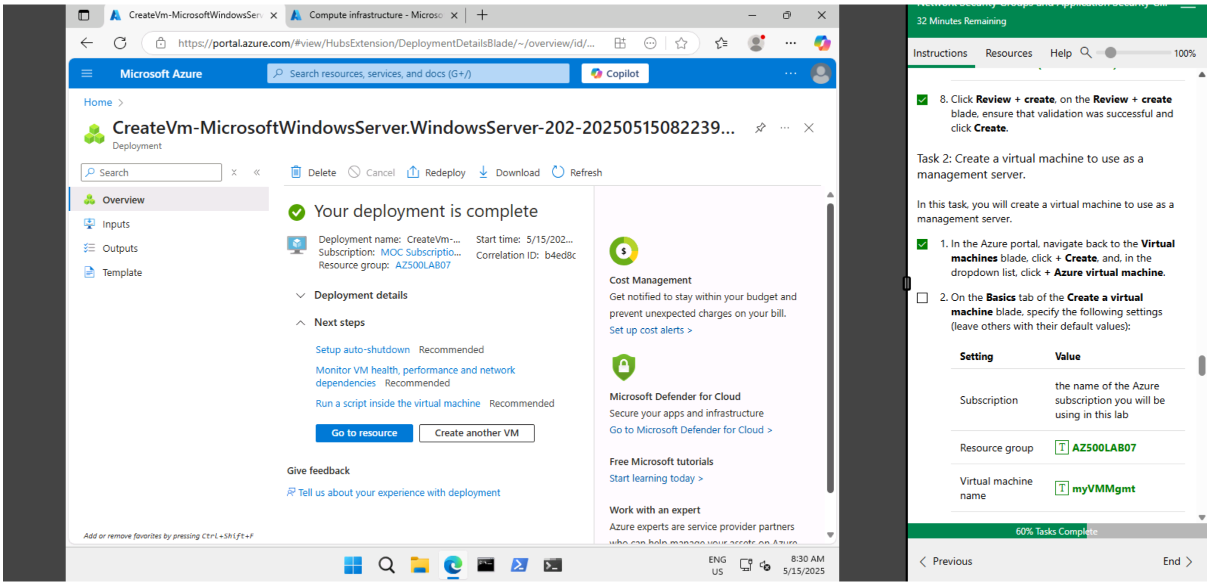
☐ 7. Click **Next: Management >**, then click **Next: Monitoring >**. On the **Monitoring** tab of the **Create a virtual machine** blade, verify the following setting:

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

☐ 8. Click **Review + create**, on the **Review + create**

53% Tasks Complete

< Previous | End >



CreateVm-MicrosoftWindowsServ | Compute infrastructure - Microso

https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/...

Microsoft Azure

Home >

CreateVm-MicrosoftWindowsServer.WindowsServer-202-20250515082239...

Deployment

Overview | Inputs | Outputs | Template

Delete | Cancel | Redeploy | Download | Refresh

Your deployment is complete

Deployment name: CreateVm-...
Subscription: MOC Subscriptio...
Resource group: AZ500LAB07
Start time: 5/15/202...
Correlation ID: b4ed8c

Deployment details

Next steps

Setup auto-shutdown Recommended

Monitor VM health, performance and network dependencies Recommended

Run a script inside the virtual machine Recommended

Go to resource | Create another VM

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 >

Work with an expert

Azure experts are service provider partners who can help manage your assets on Azure

Add or remove favorites by pressing Ctrl+Shift+F

ENG US 8:30 AM 5/15/2025

32 Minutes Remaining

Instructions | Resources | Help | 100%

☑ 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 management server.

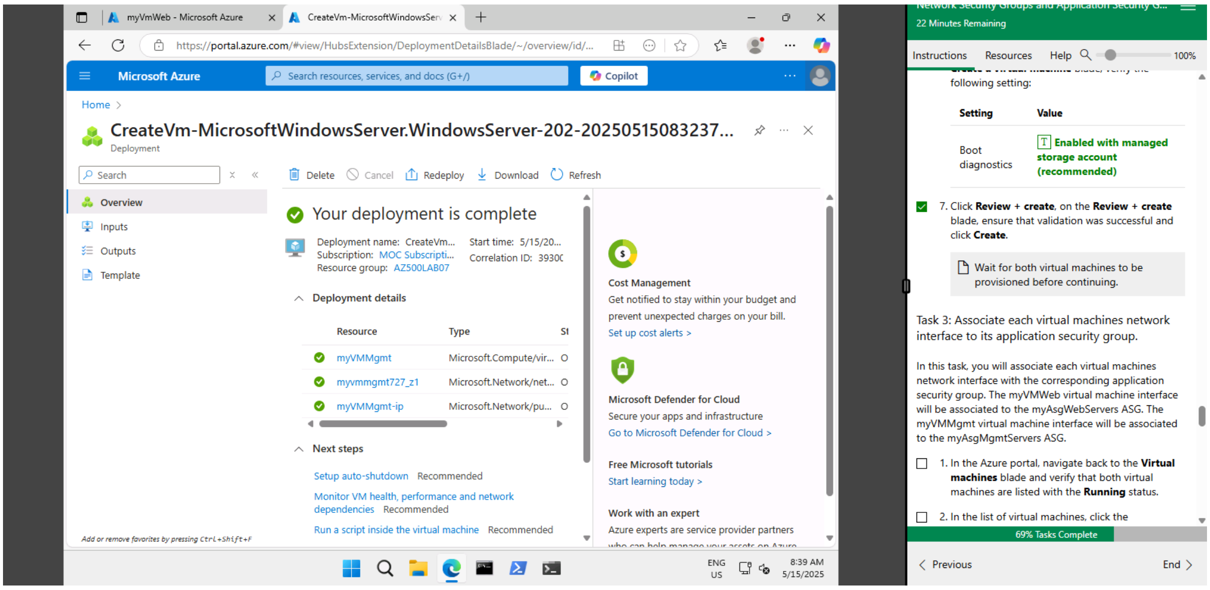
☑ 1. In the Azure portal, navigate back to the **Virtual machines** blade, click **+ Create**, and, in the dropdown list, click **+ Azure virtual machine**.

☐ 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 this lab
Resource group	**AZ500LAB07**
Virtual machine name	**myVMMgmt**

60% Tasks Complete

< Previous | End >


myVmWeb - Microsoft Azure
CreateVm-MicrosoftWindowsSer
https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Add or remove favorites by pressing Ctrl+Shift+F
ENG
US
8:39 AM
5/15/2025

CreateVm-MicrosoftWindowsServer.WindowsServer-202-20250515083237...

Deployment

Your deployment is complete

Deployment name: CreateVm...
Subscription: MOC Subscripti...
Resource group: AZ500LAB07

Start time: 5/15/20...
Correlation ID: 3930(

Deployment details

	Resource	Type	St
✓	myVMMgmt	Microsoft.Compute/vir...	O
✓	myvmmgmt727_z1	Microsoft.Network/net...	O
✓	myVMMgmt-ip	Microsoft.Network/pu...	O

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

Go to Microsoft Defender for Cloud >

Free Microsoft tutorials

Start learning today >

Work with an expert

Azure experts are service provider partners

Network Security Groups and Application Security G...

22 Minutes Remaining

Instructions Resources Help 100%

following setting:

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

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

> Wait for both virtual machines to be provisioned before continuing.

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

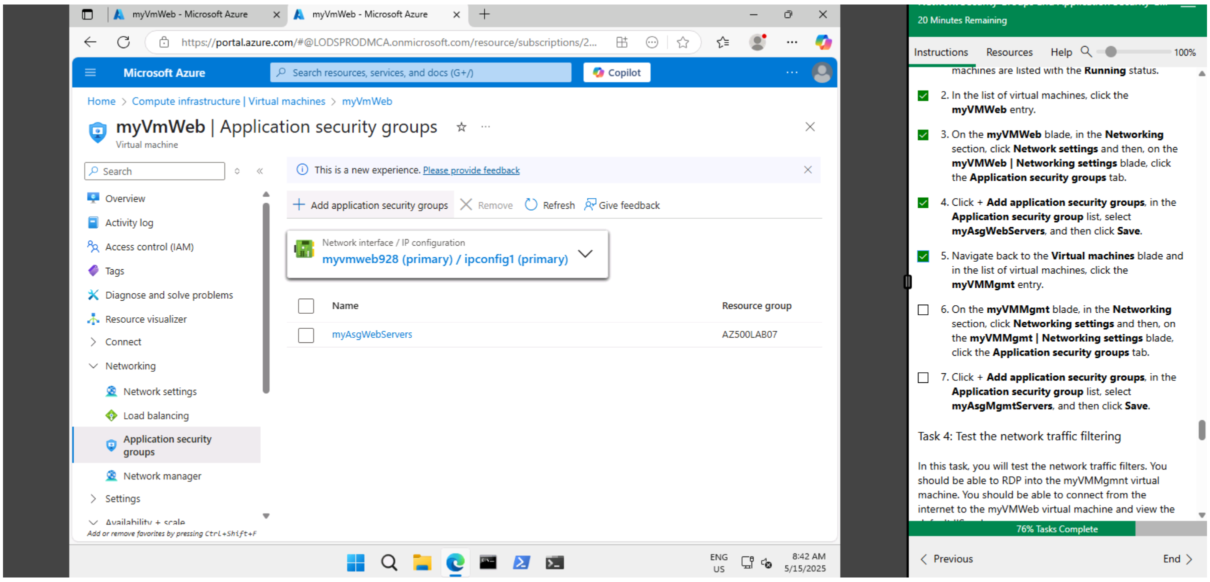
In this task, you will associate each virtual machines network interface with the corresponding application security group. The myVMWeb virtual machine interface will be associated to the myAsgWebServers ASG. The myVMMgmt virtual machine interface will be associated to the myAsgMgmtServers ASG.

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

☐ 2. In the list of virtual machines, click the

69% Tasks Complete

< Previous End >


myVmWeb - Microsoft Azure
myVmWeb - Microsoft Azure
https://portal.azure.com/#@LODSPRODMCA.onmicrosoft.com/resource/subscriptions/2...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home
Compute infrastructure | Virtual machines
myVmWeb
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
Availability + scale
Add or remove favorites by pressing Ctrl+Shift+F
Add application security groups
Remove
Refresh
Give feedback
ENG
US
8:42 AM
5/15/2025

myVmWeb | Application security groups

Virtual machine

This is a new experience. Please provide feedback

Network interface / IP configuration

myvmweb928 (primary) / ipconfig1 (primary)

☐	Name	Resource group
☐	myAsgWebServers	AZ500LAB07

20 Minutes Remaining

Instructions Resources Help 100%

machines are listed with the **Running** status.

☑ 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**.

☑ 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.

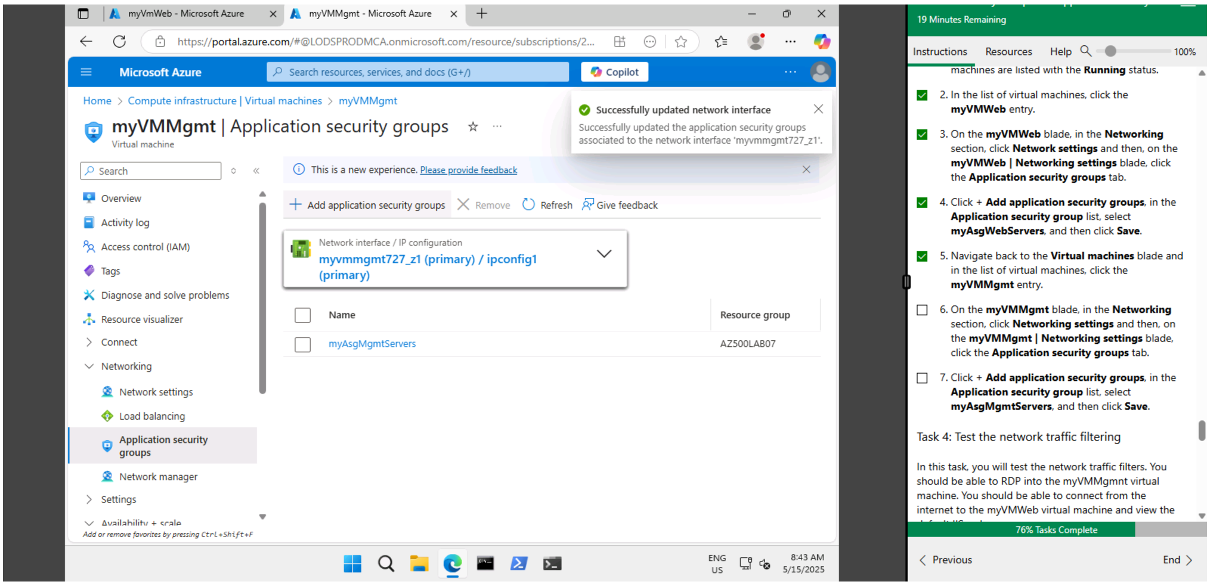
☐ 7. Click + **Add application security groups**, in the **Application security group** list, select **myAsgMgmtServers**, and then click **Save**.

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 myVMMgmnt virtual machine. You should be able to connect from the internet to the myVMWeb virtual machine and view the

76% Tasks Complete

< Previous End >


myVmWeb - Microsoft Azure
myVMMgmt - Microsoft Azure
https://portal.azure.com/#@LODSPRODMCA.onmicrosoft.com/resource/subscriptions/2...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Compute infrastructure | Virtual machines > myVMMgmt
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
Availability + scale
Add or remove favorites by pressing Ctrl+Shift+F
Add application security groups
Remove
Refresh
Give feedback
ENG US
8:43 AM 5/15/2025

myVMMgmt | Application security groups

Virtual machine

Successfully updated network interface

Successfully updated the application security groups associated to the network interface 'myvmmgmt727_z1'.

This is a new experience. Please provide feedback

Network interface / IP configuration
myvmmgmt727_z1 (primary) / ipconfig1 (primary)

□ Name	Resource group
□ myAsgMgmtServers	AZ500LAB07

19 Minutes Remaining

Instructions Resources Help 100%

machines are listed with the **Running** status.

☑ 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**.

☑ 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.

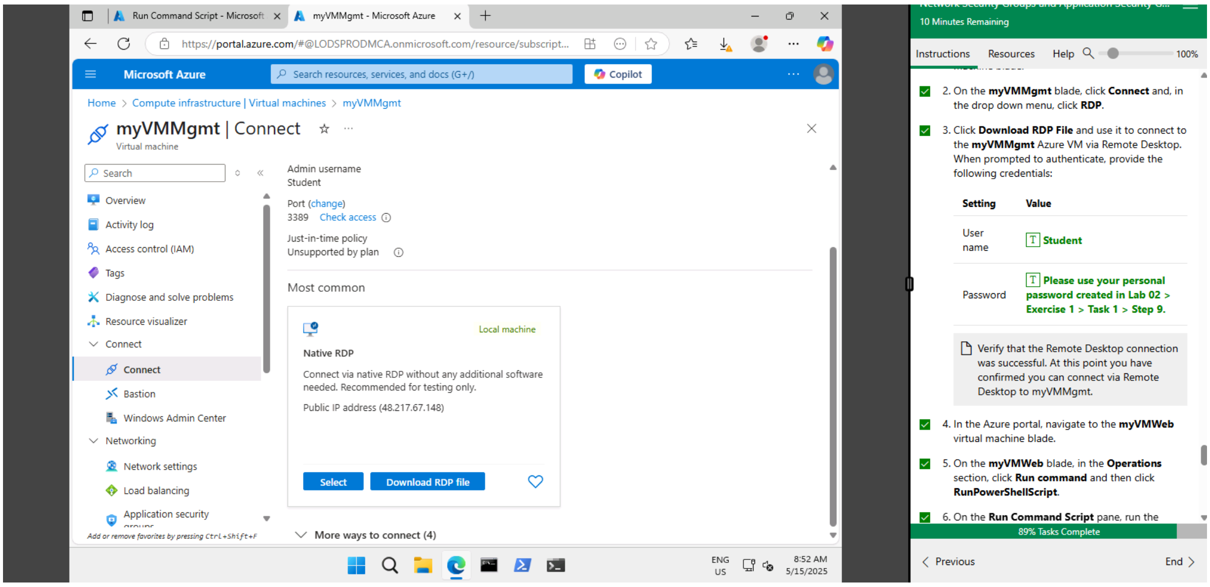
□ 7. Click + **Add application security groups**, in the **Application security group** list, select **myAsgMgmtServers**, and then click **Save**.

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 myVMMgmnt virtual machine. You should be able to connect from the internet to the myVMWeb virtual machine and view the

76% Tasks Complete

< Previous End >


Run Command Script - Microsoft
myVMMgmt - Microsoft Azure
https://portal.azure.com/#@LODSPRODMCA.onmicrosoft.com/resource/subscript...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Compute infrastructure | Virtual machines > myVMMgmt
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Connect
Bastion
Windows Admin Center
Networking
Network settings
Load balancing
Application security groups
Add or remove favorites by pressing Ctrl+Shift+F
Select
Download RDP file
More ways to connect (4)
ENG US
8:52 AM 5/15/2025

myVMMgmt | Connect

Virtual machine

Admin username
Student

Port (change)
3389 Check access

Just-in-time policy
Unsupported by plan

Most common

Local machine

Native RDP

Connect via native RDP without any additional software needed. Recommended for testing only.

Public IP address (48.217.67.148)

Network Security Groups and Application Security G...

10 Minutes Remaining

Instructions Resources Help 100%

☑ 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 credentials:

Setting	Value
User name	T **Student**
Password	T **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.

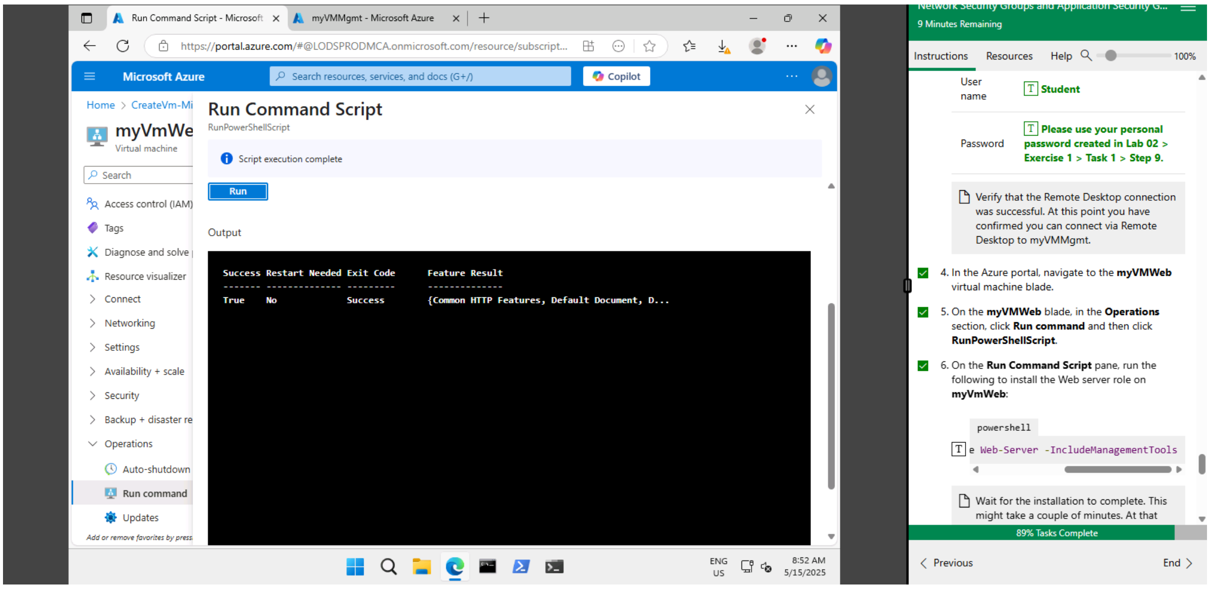
☑ 4. In the Azure portal, navigate to the **myVMWeb** virtual machine blade.

☑ 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

89% Tasks Complete

< Previous End >



Run Command Script

RunPowerShellScript

Script execution complete

Run

Output

```
Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Common HTTP Features, Default Document, D...
```

Network Security Groups and Application Security G...

9 Minutes Remaining

Instructions Resources Help 100%

User name	Student
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**.

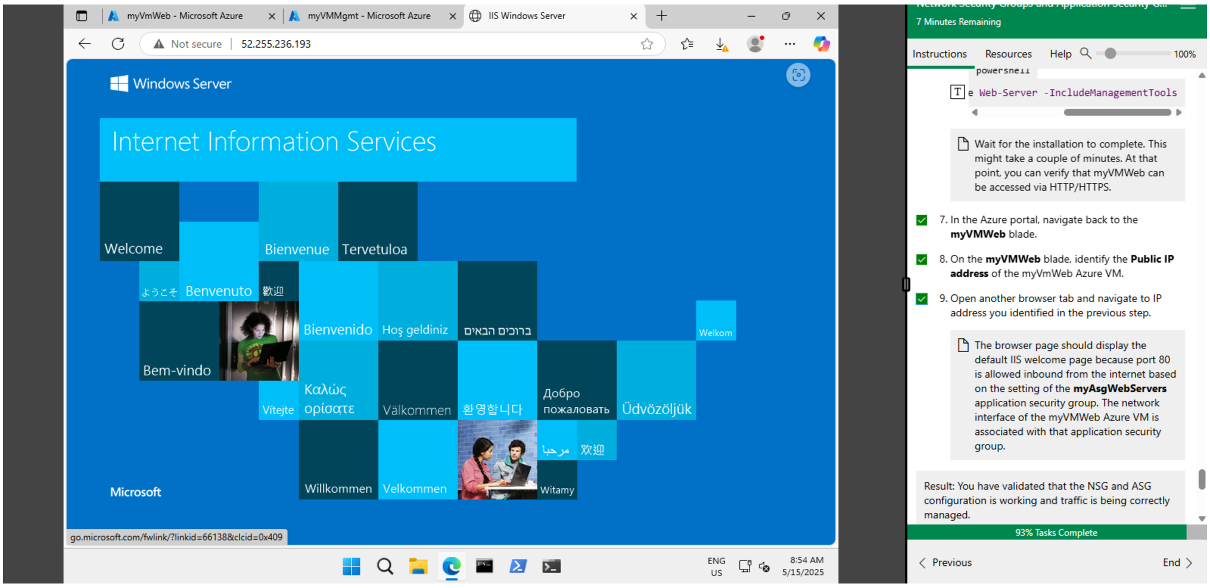
☑ 6. On the **Run Command Script** pane, run the following to install the Web server role on **myVmWeb**:

```powershell
e Web-Server -IncludeManagementTools
```

Wait for the installation to complete. This might take a couple of minutes. At that

89% Tasks Complete

Previous End



Network Security Groups and Application Security G...

7 Minutes Remaining

Instructions Resources Help 100%

```powershell
e Web-Server -IncludeManagementTools
```

Wait for the installation to complete. This might take a couple of minutes. At that point, you can verify that myVMWeb can be accessed via HTTP/HTTPS.

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

☑ 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.

93% Tasks Complete

Previous End

Conclusion

Through this lab, we successfully deployed and tested Azure's virtual networking infrastructure with a focus on NSGs and ASGs. By segmenting traffic and assigning ASGs to appropriate VM roles, we ensured that the web servers were accessible via HTTP/HTTPS while restricting RDP access to only the management servers. This hands-on experience demonstrates how Azure's layered security model can be effectively used to implement network isolation and enforce access control, aligning with best practices for securing cloud resources.