Microsoft ADC Cybersecurity Skilling Program

Week 9 Lab Assignment

Student Name: Vincent Onchieku Collins

Student ID: ADC-CSS02-25052

Introduction

In Lab 06 of the Azure Security Technologies module, I explored how to secure Azure file shares using virtual networks, subnets, and network security groups (NSGs). This exercise aimed to demonstrate the importance of service endpoints and how restricting access to specific subnets enhances security. The lab was conducted in the East US region and involved creating and configuring Azure infrastructure components including virtual networks, storage accounts, and virtual machines. This hands-on lab provided practical knowledge in network segmentation and storage access control through service endpoints and security rules.
It included the following tasks:

Task 1: Create an Azure Container Registry

Task 2: Create a Dockerfile, build a container and push it to Azure Container Registry

Task 3: Create an Azure Kubernetes Service cluster

Task 4: Grant the AKS cluster permissions to access the ACR

Task 5: Deploy an external service to AKS

Task 6: Verify you can access an external AKS-hosted service

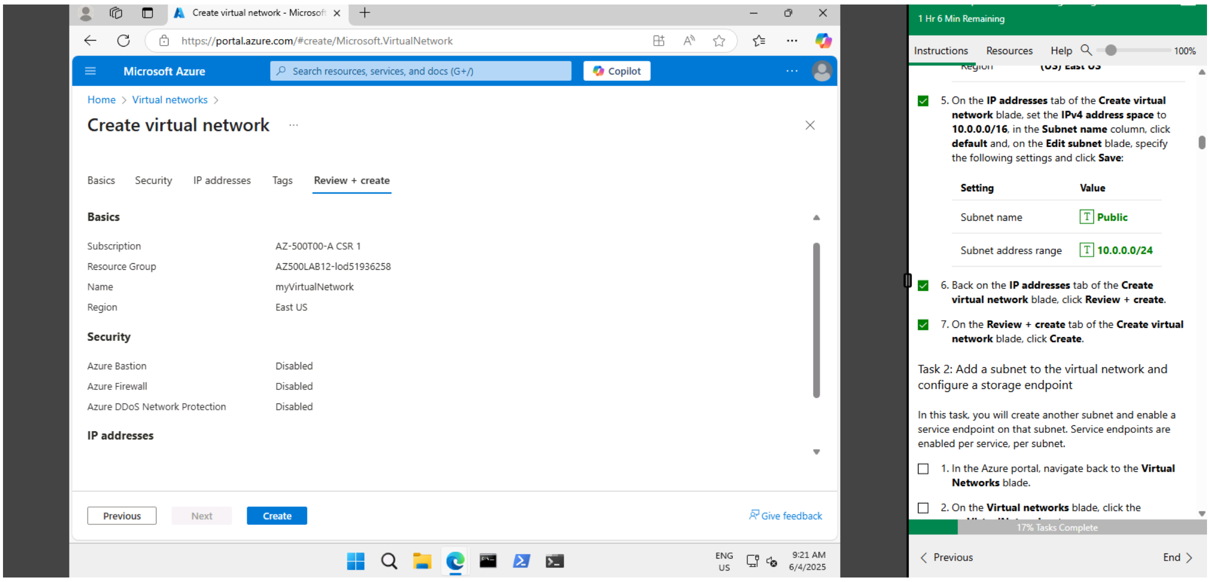
Task 7: Deploy an internal service to AKS

Task 8: Verify the you can access an internal AKS-hosted service

Tasks:

Task 1: Creating a Virtual Network

The first task in the lab involved setting up a virtual network named `myVirtualNetwork` in the East US region under a newly created resource group `AZ500LAB12`. I configured the virtual network with an IPv4 address space of `10.0.0.0/16` and added an initial subnet named `Public` with the address range `10.0.0.0/24`. This foundational step was critical as it established the network environment required for securely connecting various resources in subsequent tasks. By segmenting the network early, I could later enforce granular security rules on a per-subnet basis.



Create virtual network - Microsoft
https://portal.azure.com/#create/Microsoft.VirtualNetwork
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Virtual networks >

Create virtual network

Basics

Subscription	AZ-500T00-A CSR 1
Resource Group	AZ500LAB12-lod51936258
Name	myVirtualNetwork
Region	East US

Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

IP addresses

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

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

☑ 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**.

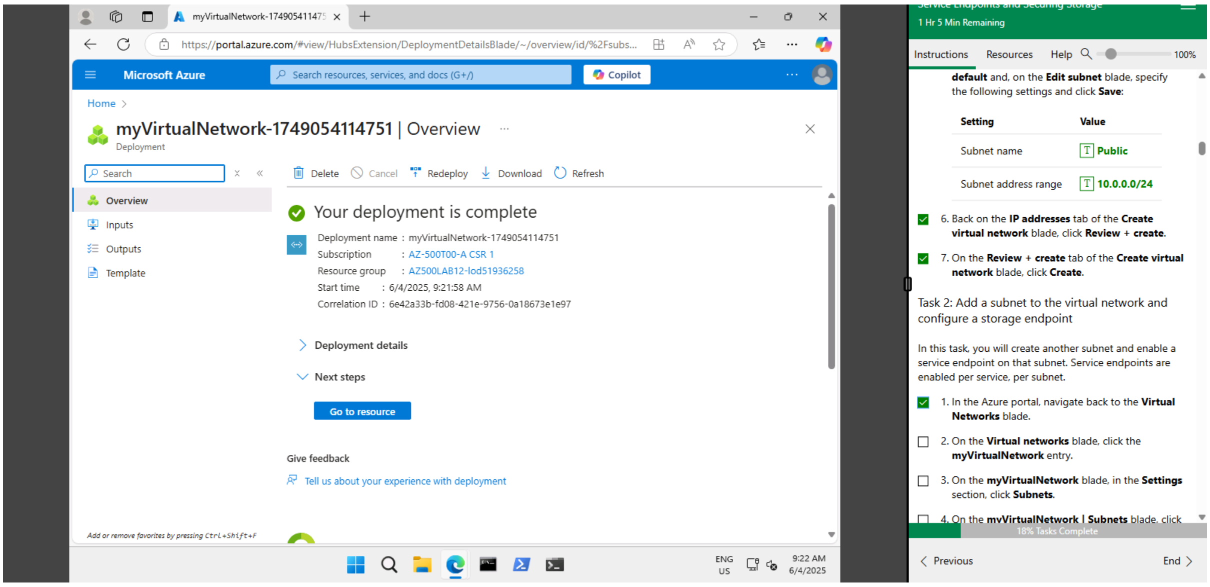
Task 2: Add a subnet to the virtual network and configure a storage endpoint

In this task, you will create another subnet and enable a service endpoint on that subnet. Service endpoints are enabled per service, per subnet.

□ 1. In the Azure portal, navigate back to the **Virtual Networks** blade.

□ 2. On the **Virtual networks** blade, click the

17% Tasks Complete
Previous
End



myVirtualNetwork-1749054114751
https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/%2Fsubs...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home >

myVirtualNetwork-1749054114751 | Overview

Deployment

Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh

Your deployment is complete

```
Deployment name : myVirtualNetwork-1749054114751
Subscription    : AZ-500T00-A CSR 1
Resource group  : AZ500LAB12-lod51936258
Start time      : 6/4/2025, 9:21:58 AM
Correlation ID  : 6e42a33b-fd08-421e-9756-0a18673e1e97
```

Deployment details
Next steps
Go to resource
Give feedback
Tell us about your experience with deployment
Add or remove favorites by pressing Ctrl+Shift+F
ENG US
9:22 AM 6/4/2025
Service Endpoints and Securing Storage
1 Hr 5 Min Remaining
Instructions
Resources
Help
100%

default and, on the **Edit subnet** blade, specify the following settings and click **Save**:

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

☑ 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**.

Task 2: Add a subnet to the virtual network and configure a storage endpoint

In this task, you will create another subnet and enable a service endpoint on that subnet. Service endpoints are enabled per service, per subnet.

☑ 1. In the Azure portal, navigate back to the **Virtual Networks** blade.

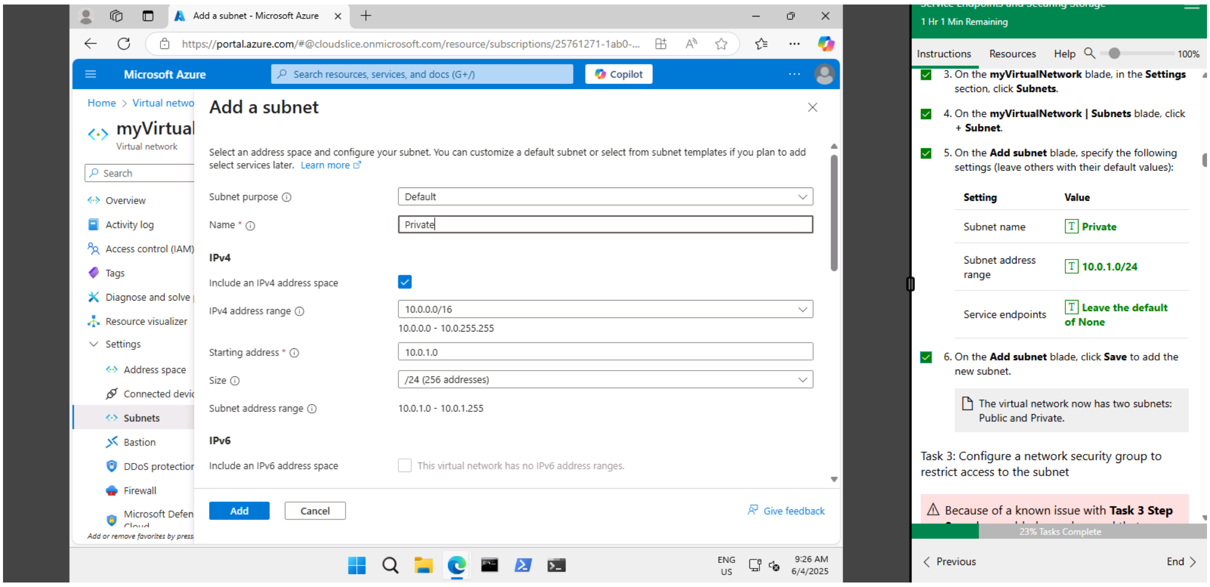
□ 2. On the **Virtual networks** blade, click the **myVirtualNetwork** entry.

□ 3. On the **myVirtualNetwork** blade, in the **Settings** section, click **Subnets**.

□ 4. On the **myVirtualNetwork | Subnets** blade, click

Task 2: Add a subnet to the virtual network and configure a storage endpoint

Next, I added a second subnet named `Private` with the address range `10.0.1.0/24` to the same virtual network. Although service endpoints were not enabled at this stage, the creation of a dedicated private subnet was necessary for isolating resources that would later connect securely to Azure Storage. This logical separation helped enforce strict access policies through subsequent NSG configurations and ensured that only specific parts of the network could interact with sensitive storage resources.



Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. Learn more

Subnet purpose: Default

Name *: Private

IPv4

Include an IPv4 address space: ☑

IPv4 address range: 10.0.0.0/16

10.0.0.0 - 10.0.255.255

Starting address *: 10.0.1.0

Size: /24 (256 addresses)

Subnet address range: 10.0.1.0 - 10.0.1.255

IPv6

Include an IPv6 address space: □ This virtual network has no IPv6 address ranges.

Add | Cancel | Give feedback

1 Hr 1 Min Remaining

Instructions | Resources | Help | 100%

☑ 3. On the **myVirtualNetwork** blade, in the **Settings** section, click **Subnets**.

☑ 4. On the **myVirtualNetwork | Subnets** blade, click **+ Subnet**.

☑ 5. On the **Add subnet** blade, specify the following settings (leave others with their default values):

Setting	Value
Subnet name	Private
Subnet address range	10.0.1.0/24
Service endpoints	Leave the default of None

☑ 6. On the **Add subnet** blade, click **Save** to add the new subnet.

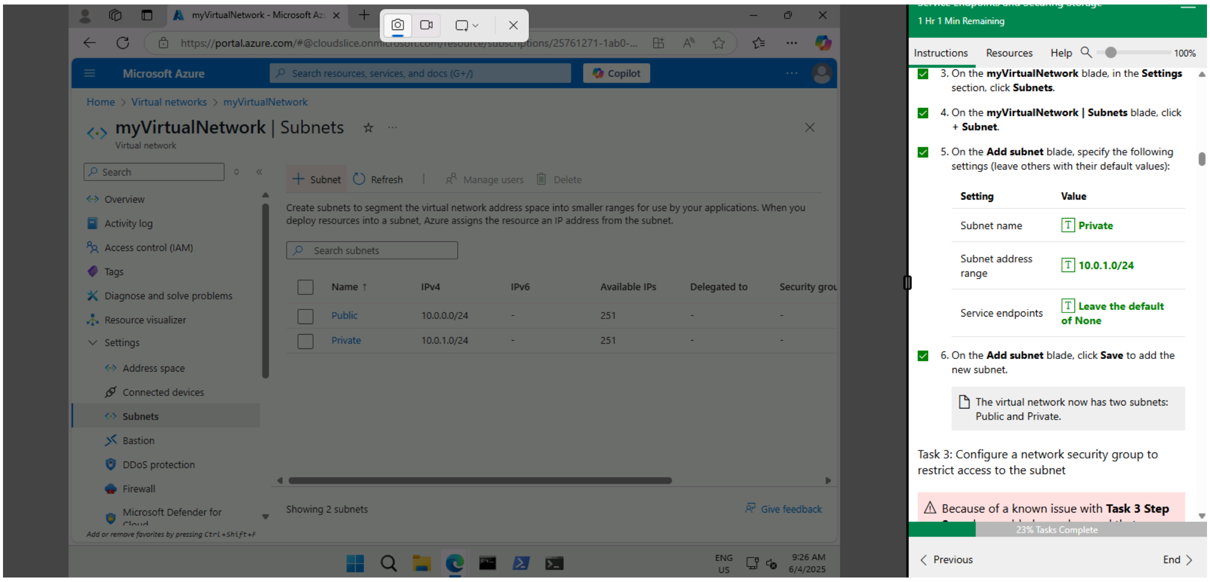
The virtual network now has two subnets: Public and Private.

Task 3: Configure a network security group to restrict access to the subnet

Because of a known issue with **Task 3 Step**

23% Tasks Complete

Previous | End



myVirtualNetwork - Microsoft Az
https://portal.azure.com/#@cloudslice.onmicrosoft.com/resource/subscriptions/25761271-1ab0-...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Virtual networks > myVirtualNetwork
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Address space
Connected devices
Subnets
Bastion
DDoS protection
Firewall
Microsoft Defender for Cloud
Add or remove favorites by pressing Ctrl+Shift+F

myVirtualNetwork | Subnets

Virtual network

+ Subnet | Refresh | Manage users | Delete

Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet.

Search subnets

□	Name ↑	IPv4	IPv6	Available IPs	Delegated to	Security grou
□	Public	10.0.0.0/24	-	251	-	-
□	Private	10.0.1.0/24	-	251	-	-

Showing 2 subnets

Give feedback

1 Hr 1 Min Remaining

Instructions | Resources | Help | 100%

☑ 3. On the **myVirtualNetwork** blade, in the **Settings** section, click **Subnets**.

☑ 4. On the **myVirtualNetwork | Subnets** blade, click **+ Subnet**.

☑ 5. On the **Add subnet** blade, specify the following settings (leave others with their default values):

Setting	Value
Subnet name	Private
Subnet address range	10.0.1.0/24
Service endpoints	Leave the default of None

☑ 6. On the **Add subnet** blade, click **Save** to add the new subnet.

The virtual network now has two subnets: Public and Private.

Task 3: Configure a network security group to restrict access to the subnet

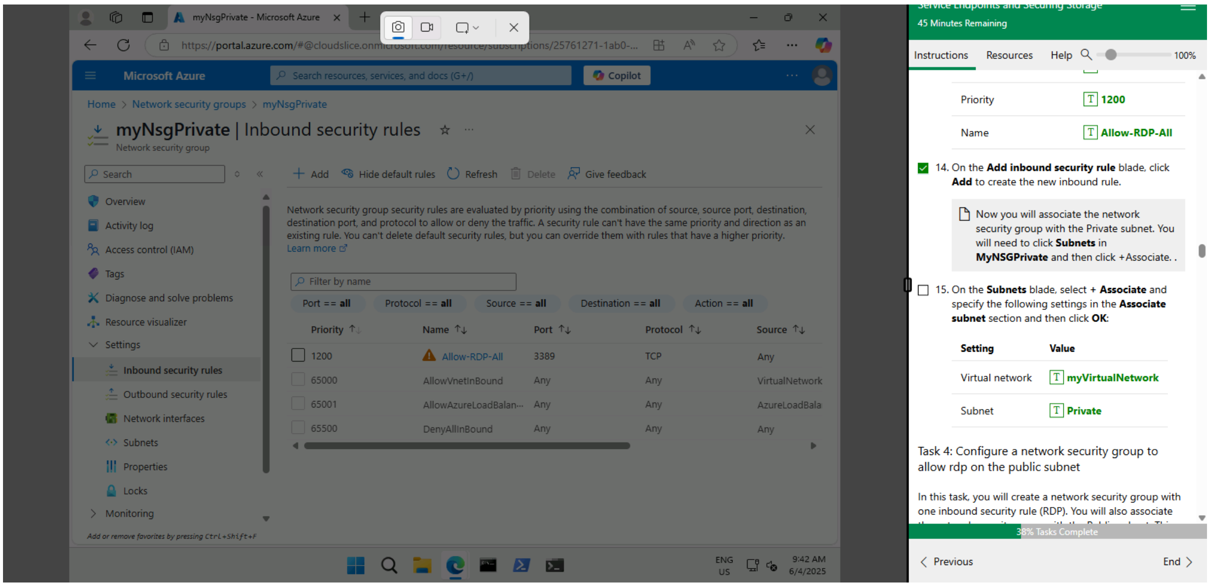
Because of a known issue with **Task 3 Step**

23% Tasks Complete

Previous | End

Task 3: Configure a network security group to restrict access to the subnet

In this task, I created a network security group called `myNsgPrivate` and associated it with the Private subnet. I configured two outbound rules: one to **allow** traffic to Azure Storage (`Allow-Storage-All`) and another to **deny** outbound traffic to the Internet (`Deny-Internet-All`). Additionally, I added an inbound rule to allow Remote Desktop Protocol (RDP) traffic within the virtual network. This setup was essential to restrict data flow strictly to authorized endpoints and mitigate the risk of data exfiltration or unauthorized access from the broader internet.



myNsgPrivate | Inbound security rules
Network security group

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. Learn more

	Priority	Name	Port	Protocol	Source
□	1200	Allow-RDP-All	3389	TCP	Any
□	65000	AllowVnetInBound	Any	Any	VirtualNetwork
□	65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBala
□	65500	DenyAllInBound	Any	Any	Any

Priority	1200
Name	Allow-RDP-All

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

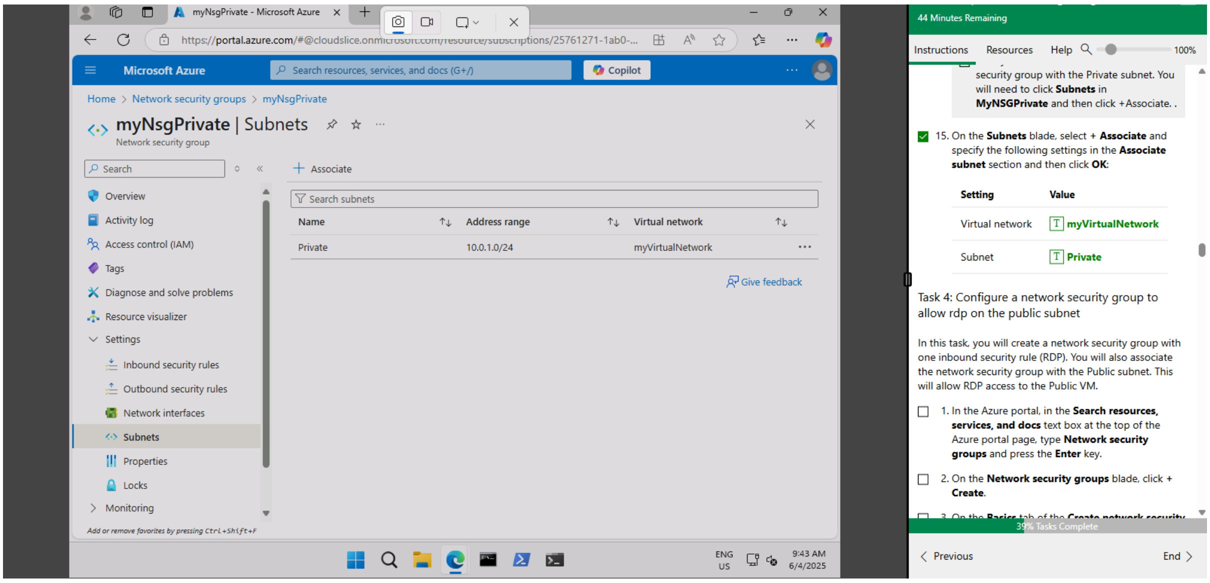
Now you will associate the network security group with the Private subnet. You will need to click **Subnets** in **MyNSGPrivate** and then click +Associate. .

□ 15. On the **Subnets** blade, select + **Associate** and specify the following settings in the **Associate subnet** section and then click **OK**:

Setting	Value
Virtual network	myVirtualNetwork
Subnet	Private

Task 4: Configure a network security group to allow rdp on the public subnet

In this task, you will create a network security group with one inbound security rule (RDP). You will also associate



myNsgPrivate | Subnets
Network security group

Name	Address range	Virtual network
Private	10.0.1.0/24	myVirtualNetwork

security group with the Private subnet. You will need to click **Subnets** in **MyNSGPrivate** and then click +Associate. .

☑ 15. On the **Subnets** blade, select + **Associate** and specify the following settings in the **Associate subnet** section and then click **OK**:

Setting	Value
Virtual network	myVirtualNetwork
Subnet	Private

Task 4: Configure a network security group to allow rdp on the public subnet

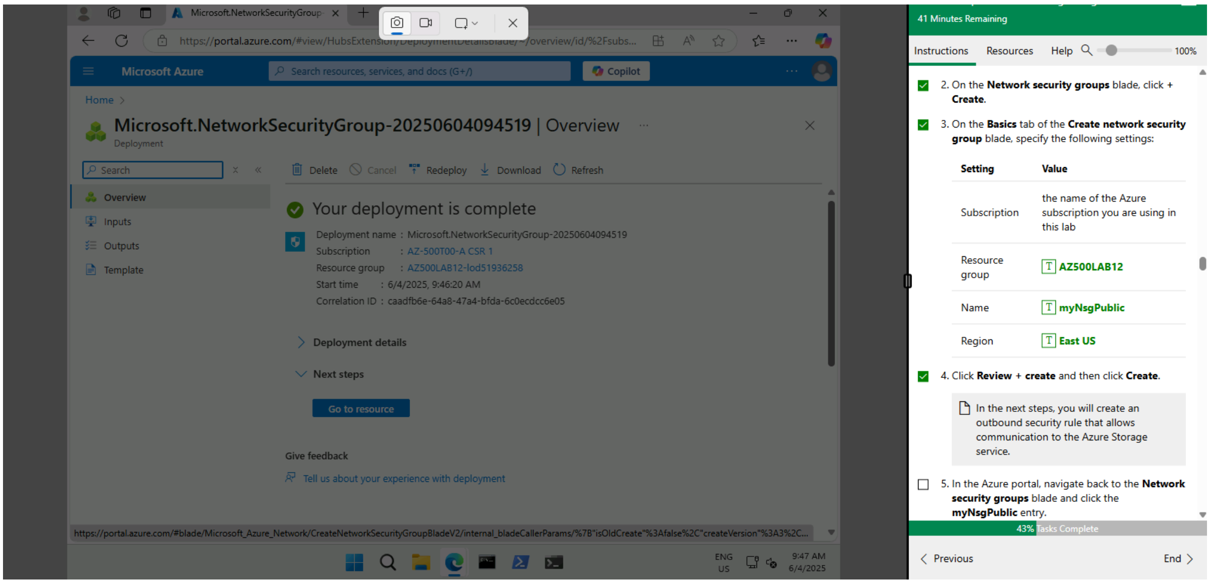
In this task, you will create a network security group with one inbound security rule (RDP). You will also associate the network security group with the Public subnet. This will allow RDP access to the Public VM.

□ 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**.

Task 4: Configure a network security group to allow rdp on the public subnet

For the fourth task, I created another network security group named `myNsgPublic` and applied it to the Public subnet. I then added an inbound rule to allow RDP traffic (`Allow-RDP-All`) on port 3389. This configuration was important for administrative access and testing purposes, as it enabled connectivity to virtual machines deployed in the Public subnet. Ensuring RDP access only from specific locations and subnets is a fundamental security practice that helps reduce the attack surface.



Microsoft.NetworkSecurityGroup-
https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/%2Fsubs...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home
Search
Delete
Cancel
Redeploy
Download
Refresh
Overview
Inputs
Outputs
Template

Microsoft.NetworkSecurityGroup-20250604094519 | Overview

Deployment

Your deployment is complete

Deployment name : Microsoft.NetworkSecurityGroup-20250604094519
Subscription : AZ-500T00-A CSR 1
Resource group : AZ500LAB12-lod51936258
Start time : 6/4/2025, 9:46:20 AM
Correlation ID : caadfb6e-64a8-47a4-bfda-6c0ecdcc6e05

Deployment details
Next steps
Go to resource
Give feedback
Tell us about your experience with deployment
https://portal.azure.com/#blade/Microsoft_Azure_Network/CreateNetworkSecurityGroupBladeV2/internal_bladeCallerParams/%7B"isOldCreate"%3Afalse%2C"createVersion"%3A3%2C...
ENG US
9:47 AM 6/4/2025
41 Minutes Remaining
Instructions
Resources
Help
100%

☑ 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:

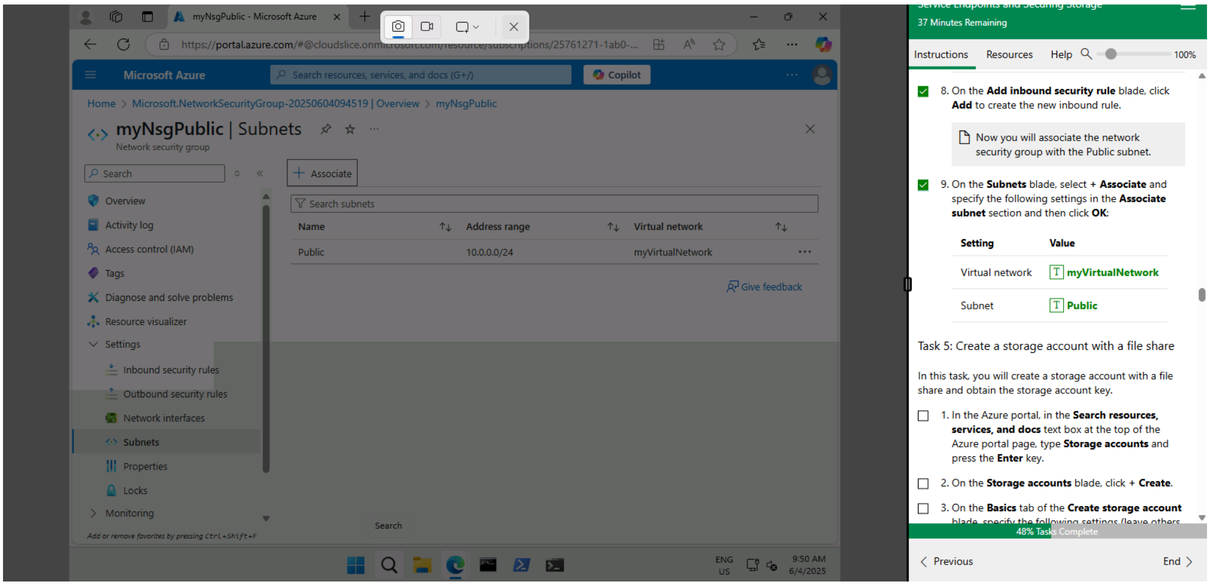
Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	AZ500LAB12
Name	myNsgPublic
Region	East US

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

In the next steps, you will create an outbound security rule that allows communication to the Azure Storage service.

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

43% Tasks Complete
Previous
End



myNsgPublic - Microsoft Azure
https://portal.azure.com/#@cloudslice.onmicrosoft.com/resource/subscriptions/25761271-1ab0-...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft.NetworkSecurityGroup-20250604094519 | Overview > myNsgPublic

myNsgPublic | Subnets

Network security group

Search
Associate
Search subnets
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

Name	Address range	Virtual network
Public	10.0.0.0/24	myVirtualNetwork

Give feedback
Search
ENG US
9:50 AM 6/4/2025
Service Endpoints and Securing Storage
37 Minutes Remaining
Instructions
Resources
Help
100%

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

Now you will associate the network security group with the Public subnet.

☑ 9. On the **Subnets** blade, select + **Associate** and specify the following settings in the **Associate subnet** section and then click **OK**:

Setting	Value
Virtual network	myVirtualNetwork
Subnet	Public

Task 5: Create a storage account with a file share

In this task, you will create a storage account with a file share and obtain the storage account key.

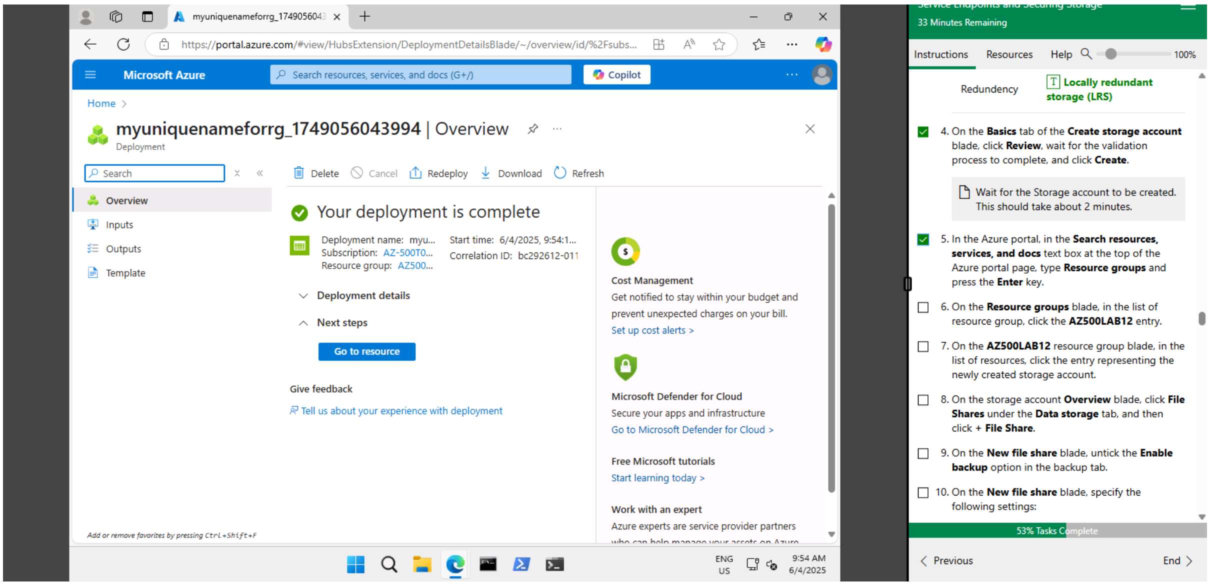
☐ 1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Storage accounts** and press the **Enter** key.

☐ 2. On the **Storage accounts** blade, click + **Create**.

☐ 3. On the **Basics** tab of the **Create storage account** blade, specify the following settings (leave others

Task 5: Creating a Storage Account with a File Share

I proceeded to create a storage account with a globally unique name in the East US region. After choosing standard performance and locally redundant storage (LRS), I deployed the storage account and created a file share within it. This storage resource would later serve as the target for secure file access tests. Acquiring the storage account key was also necessary for authenticating connections from the virtual machines during subsequent tasks.



myuniquenameforrg_1749056043994 | Overview

Deployment

Your deployment is complete

Deployment name: myu...
Subscription: AZ-500T0...
Resource group: AZ500...
Start time: 6/4/2025, 9:54:1...
Correlation ID: bc292612-011

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

Microsoft Defender for Cloud: Secure your apps and infrastructure

Work with an expert: Azure experts are service provider partners

Redundancy	Locally redundant storage (LRS)

☑ 4. On the **Basics** tab of the **Create storage account** blade, click **Review**, wait for the validation process to complete, and click **Create**.

Wait for the Storage account to be created. This should take about 2 minutes.

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

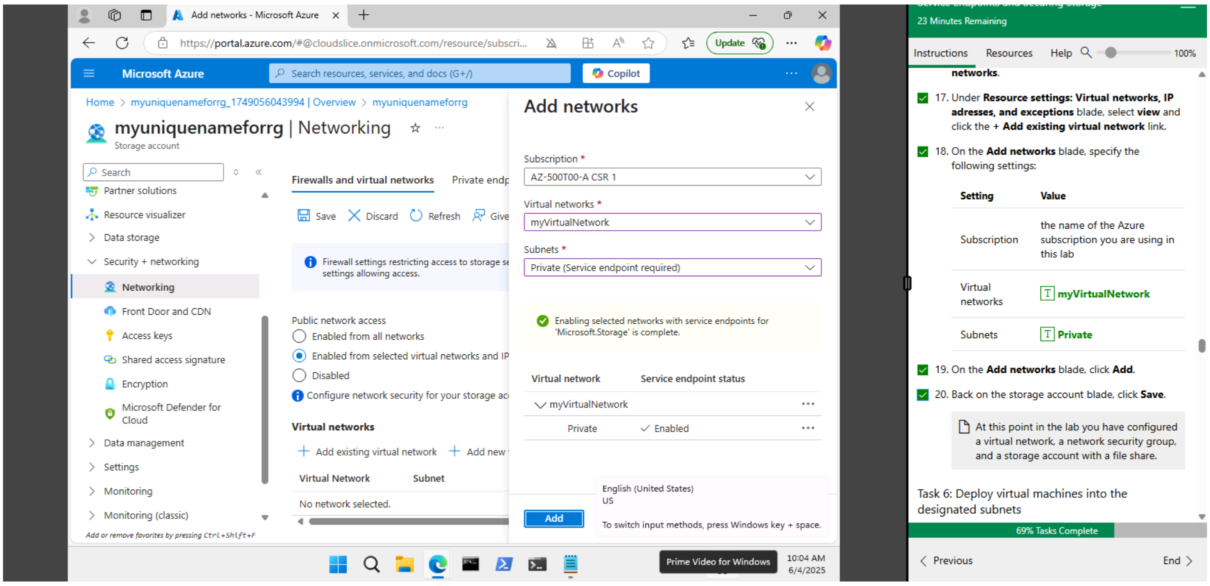
□ 6. On the **Resource groups** blade, in the list of resource group, click the **AZ500LAB12** entry.

□ 7. On the **AZ500LAB12** resource group blade, in the list of resources, click the entry representing the newly created storage account.

□ 8. On the storage account **Overview** blade, click **File Shares** under the **Data storage** tab, and then click + **File Share**.

□ 9. On the **New file share** blade, untick the **Enable backup** option in the backup tab.

□ 10. On the **New file share** blade, specify the following settings:



myuniquenameforrg | Networking

Storage account

Firewall settings restricting access to storage se settings allowing access.

Public network access
○ Enabled from all networks
● Enabled from selected virtual networks and IP
○ Disabled

Add networks

Subscription *: AZ-500T00-A CSR 1

Virtual networks *: myVirtualNetwork

Subnets *: Private (Service endpoint required)

Enabling selected networks with service endpoints for 'Microsoft.Storage' is complete.

Virtual network	Service endpoint status
myVirtualNetwork	
Private	✓ Enabled

Add networks - Microsoft Azure
https://portal.azure.com/#@cloudslice.onmicrosoft.com/resource/subscri...
Update
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > myuniquenameforrg_1749056043994 | Overview > myuniquenameforrg
Search
Partner solutions
Resource visualizer
Data storage
Security + networking
Networking
Front Door and CDN
Access keys
Shared access signature
Encryption
Microsoft Defender for Cloud
Data management
Settings
Monitoring
Monitoring (classic)
Firewalls and virtual networks
Private endp
Save
Discard
Refresh
Give
Configure network security for your storage ac
Virtual networks
Add existing virtual network
Add new
Virtual Network
Subnet
No network selected.
Add
English (United States) US
To switch input methods, press Windows key + space.
Add or remove favorites by pressing Ctrl+Shift+F
Prime Video for Windows
10:04 AM 6/4/2025
23 Minutes Remaining
Instructions
Resources
Help
100%
69% Tasks Complete
Previous
End

networks.

☑ 17. Under **Resource settings: Virtual networks, IP adresses, and exceptions** blade, select **view** and click the + **Add existing virtual network** link.

☑ 18. On the **Add networks** blade, specify the following settings:

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Virtual networks	myVirtualNetwork
Subnets	Private

☑ 19. On the **Add networks** blade, click **Add**.

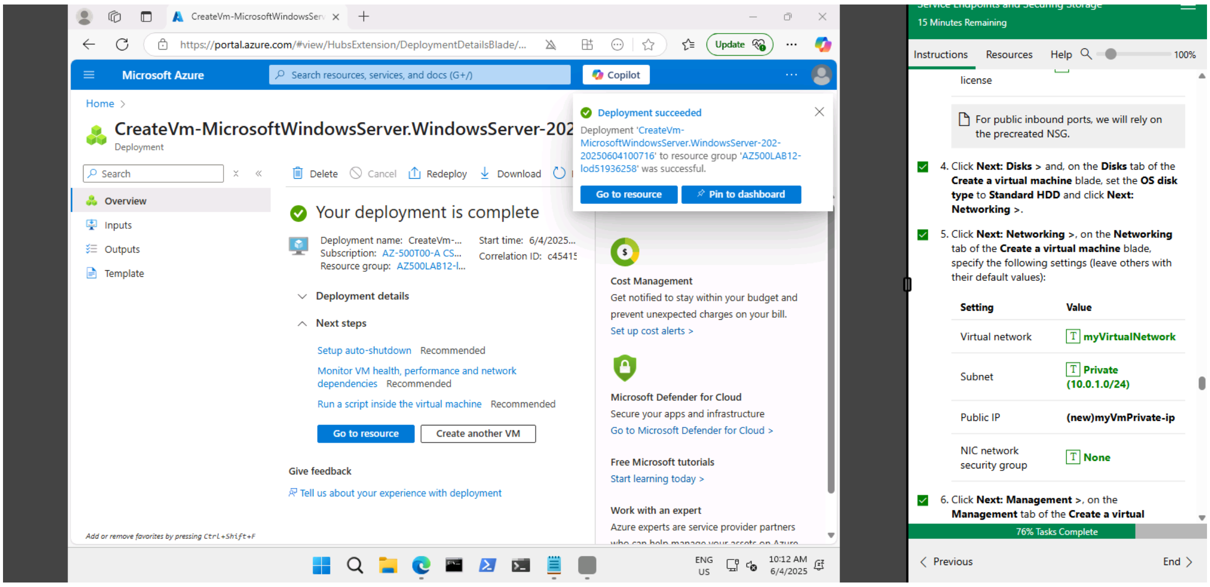
☑ 20. Back on the storage account blade, click **Save**.

At this point in the lab you have configured a virtual network, a network security group, and a storage account with a file share.

Task 6: Deploy virtual machines into the designated subnets

Task 6: Deploy virtual machines into the designated subnets

In this task, I deployed virtual machines into both the Public and Private subnets. These VMs were essential for testing access to the storage account under different security and network configurations. The VM in the Private subnet represented a trusted resource that should be allowed to connect to the file share, while the one in the Public subnet was used to simulate an untrusted source. Deploying VMs in segregated subnets provided a controlled environment to validate network security settings.


CreateVm-MicrosoftWindowsServ
https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/...
Update
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Go to resource
Pin to dashboard
Go to resource
Create another VM
Add or remove favorites by pressing Ctrl+Shift+F
ENG
US
10:12 AM
6/4/2025
Service Endpoints and Securing Storage
Instructions
Resources
Help
100%
Previous
End

CreateVm-MicrosoftWindowsServer.WindowsServer-202
Deployment

Deployment succeeded

Deployment 'CreateVm-MicrosoftWindowsServer.WindowsServer-202-20250604100716' to resource group 'AZ500LAB12-lod51936258' was successful.

Your deployment is complete

Deployment name: CreateVm-...
Subscription: AZ-500T00-A CS...
Resource group: AZ500LAB12-l...
Start time: 6/4/2025...
Correlation ID: c45415

Deployment details

Next steps

Setup auto-shutdown Recommended

Monitor VM health, performance and network dependencies Recommended

Run a script inside the virtual machine Recommended

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

15 Minutes Remaining

license

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

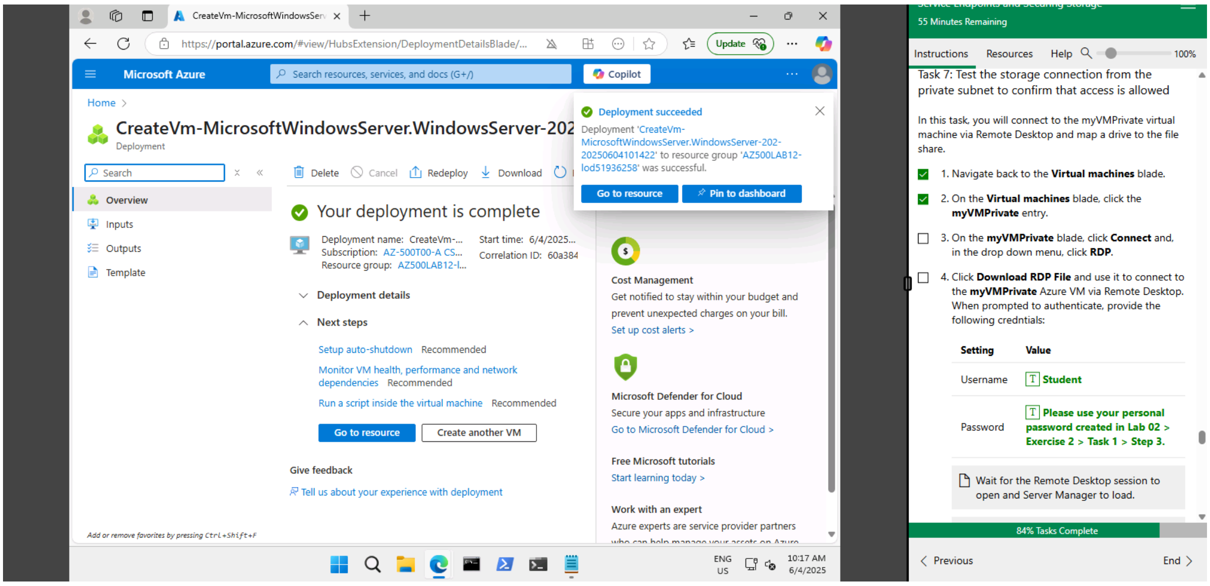
☑ 4. Click **Next: Disks >** and, on the **Disks** tab of the **Create a virtual machine** blade, set the **OS disk type** to **Standard HDD** and click **Next: Networking >**.

☑ 5. Click **Next: Networking >**, on the **Networking** tab of the **Create a virtual machine** blade, specify the following settings (leave others with their default values):

Setting	Value
Virtual network	myVirtualNetwork
Subnet	Private (10.0.1.0/24)
Public IP	(new)myVmPrivate-ip
NIC network security group	None

☑ 6. Click **Next: Management >**, on the **Management** tab of the **Create a virtual**

76% Tasks Complete


CreateVm-MicrosoftWindowsServ
https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/...
Update
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Go to resource
Pin to dashboard
Go to resource
Create another VM
Add or remove favorites by pressing Ctrl+Shift+F
ENG
US
10:17 AM
6/4/2025
Service Endpoints and Securing Storage
Instructions
Resources
Help
100%
Previous
End

CreateVm-MicrosoftWindowsServer.WindowsServer-202
Deployment

Deployment succeeded

Deployment 'CreateVm-MicrosoftWindowsServer.WindowsServer-202-20250604101422' to resource group 'AZ500LAB12-lod51936258' was successful.

Your deployment is complete

Deployment name: CreateVm-...
Subscription: AZ-500T00-A CS...
Resource group: AZ500LAB12-l...
Start time: 6/4/2025...
Correlation ID: 60a384

Deployment details

Next steps

Setup auto-shutdown Recommended

Monitor VM health, performance and network dependencies Recommended

Run a script inside the virtual machine Recommended

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

55 Minutes Remaining

Task 7: Test the storage connection from the private subnet to confirm that access is allowed

In this task, you will connect to the myVMPrivate virtual machine via Remote Desktop and map a drive to the file share.

☑ 1. Navigate back to the **Virtual machines** blade.

☑ 2. On the **Virtual machines** blade, click the **myVMPrivate** entry.

□ 3. On the **myVMPrivate** blade, click **Connect** and, in the drop down menu, click **RDP**.

□ 4. Click **Download RDP File** and use it to connect to the **myVMPrivate** Azure VM via Remote Desktop. When prompted to authenticate, provide the following credntials:

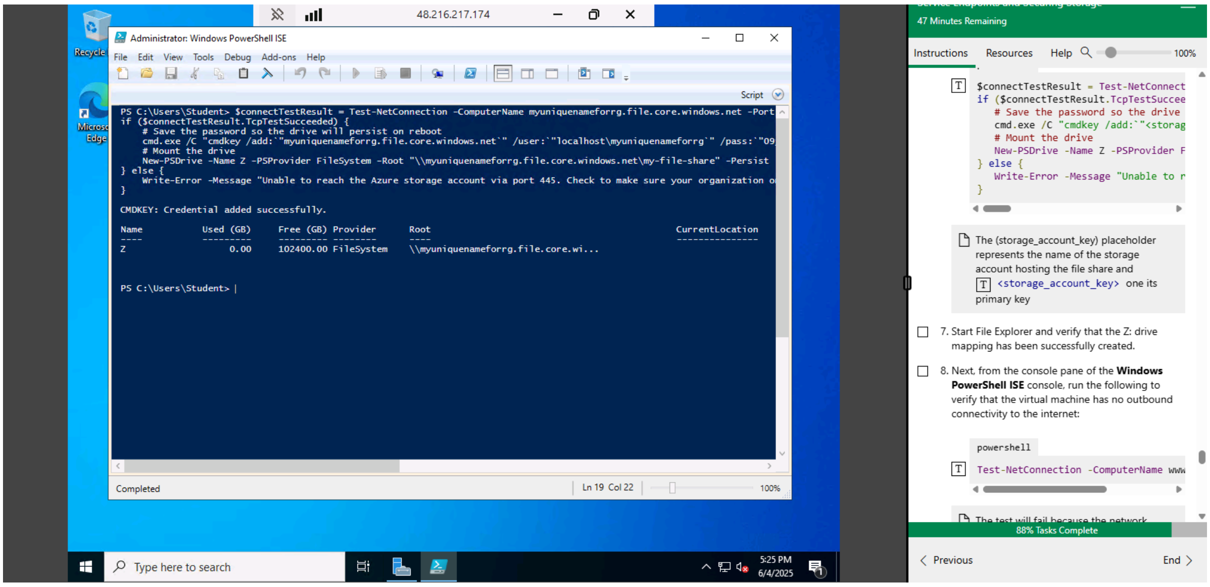
Setting	Value
Username	Student
Password	Please use your personal password created in Lab 02 > Exercise 2 > Task 1 > Step 3.

Wait for the Remote Desktop session to open and Server Manager to load.

84% Tasks Complete

Task 7: Test the storage connection from the private subnet to confirm that access is allowed

Once the VMs were deployed, I accessed the VM in the Private subnet and attempted to connect to the file share using the storage account key. The connection was successful, confirming that the service endpoint and NSG rules were correctly configured to allow secure access to Azure Storage from only the trusted subnet. This step validated that the security architecture supported secure communication over the Azure backbone network without exposing data to the public internet.



48.216.217.174
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Script
Completed
Ln 19 Col 22
100%
Type here to search
5:25 PM
6/4/2025
Service Endpoints and Securing Storage
Instructions Resources Help
100%
88% Tasks Complete
Previous
End

```
PS C:\Users\Student> $connectTestResult = Test-NetConnection -ComputerName myuniquenameforrg.file.core.windows.net -Port
if ($connectTestResult.TcpTestSucceeded) {
    # Save the password so the drive will persist on reboot
    cmd.exe /C "cmdkey /add:`"myuniquenameforrg.file.core.windows.net`" /user:`"localhost\myuniquenameforrg`" /pass:`"09
    # Mount the drive
    New-PSDrive -Name Z -PSProvider FileSystem -Root "\\myuniquenameforrg.file.core.windows.net\my-file-share" -Persist
} else {
    Write-Error -Message "Unable to reach the Azure storage account via port 445. Check to make sure your organization o
}

CMDKEY: Credential added successfully.

Name           Used (GB)     Free (GB) Provider      Root                                               CurrentLocation
----           ---------     --------- --------      ----                                               ---------------
Z                   0.00     102400.00 FileSystem    \\myuniquenameforrg.file.core.wi...


PS C:\Users\Student> |
```

47 Minutes Remaining

```
$connectTestResult = Test-NetConnect
if ($connectTestResult.TcpTestSuccee
   # Save the password so the drive
   cmd.exe /C "cmdkey /add:`"<storag
   # Mount the drive
   New-PSDrive -Name Z -PSProvider F
} else {
   Write-Error -Message "Unable to r
}
```

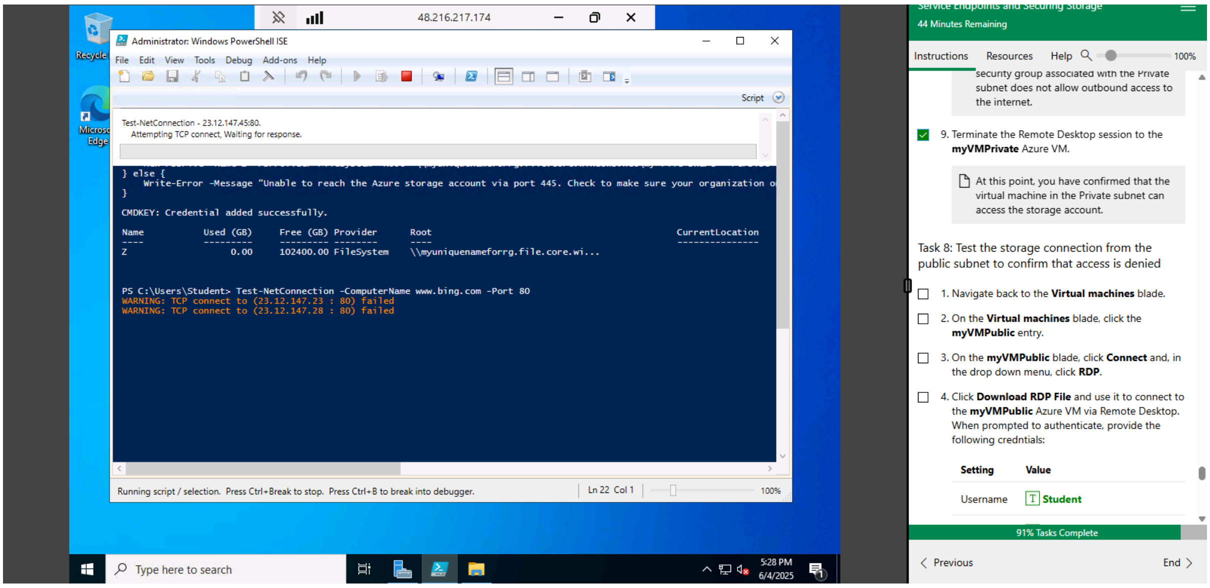
The (storage_account_key) placeholder represents the name of the storage account hosting the file share and <storage_account_key> one its primary key

□ 7. Start File Explorer and verify that the Z: drive mapping has been successfully created.

□ 8. Next, from the console pane of the **Windows PowerShell ISE** console, run the following to verify that the virtual machine has no outbound connectivity to the internet:

```powershell
Test-NetConnection -ComputerName www
```

The test will fail because the network



48.216.217.174
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Script
Ln 22 Col 1
100%
Type here to search
5:28 PM
6/4/2025
Service Endpoints and Securing Storage
Instructions Resources Help
100%
91% Tasks Complete
Previous
End

Test-NetConnection - 23.12.147.45:80.
Attempting TCP connect, Waiting for response.

```
} else {
    Write-Error -Message "Unable to reach the Azure storage account via port 445. Check to make sure your organization o
}

CMDKEY: Credential added successfully.

Name           Used (GB)     Free (GB) Provider      Root                                               CurrentLocation
----           ---------     --------- --------      ----                                               ---------------
Z                   0.00     102400.00 FileSystem    \\myuniquenameforrg.file.core.wi...


PS C:\Users\Student> Test-NetConnection -ComputerName www.bing.com -Port 80
WARNING: TCP connect to (23.12.147.23 : 80) failed
WARNING: TCP connect to (23.12.147.28 : 80) failed
```

Running script / selection. Press Ctrl+Break to stop. Press Ctrl+B to break into debugger.

44 Minutes Remaining

security group associated with the Private subnet does not allow outbound access to the internet.

☑ 9. Terminate the Remote Desktop session to the **myVMPrivate** Azure VM.

At this point, you have confirmed that the virtual machine in the Private subnet can access the storage account.

Task 8: Test the storage connection from the public subnet to confirm that access is denied

□ 1. Navigate back to the **Virtual machines** blade.

□ 2. On the **Virtual machines** blade, click the **myVMPublic** entry.

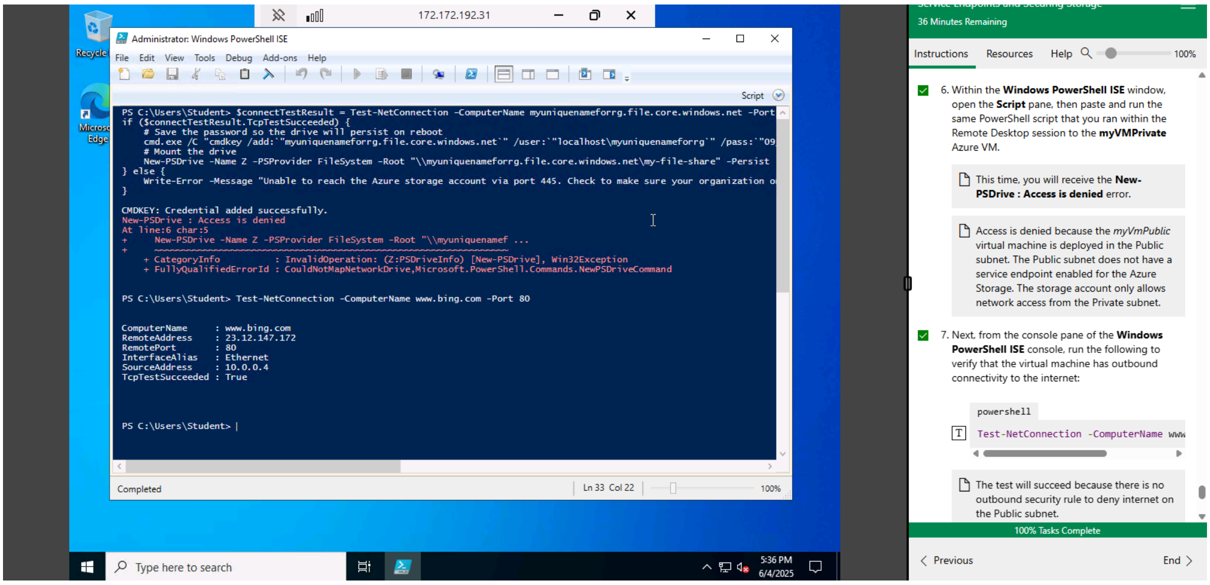
□ 3. On the **myVMPublic** blade, click **Connect** and, in the drop down menu, click **RDP**.

□ 4. Click **Download RDP File** and use it to connect to the **myVMPublic** Azure VM via Remote Desktop. When prompted to authenticate, provide the following credntials:

Setting	Value
Username	**Student**

Task 8: Test the storage connection from the public subnet to confirm that access is denied

Lastly, I tested the same storage connection from the VM deployed in the Public subnet. As expected, the connection attempt failed. This validated that the NSG and service endpoint settings successfully restricted access to the storage account from unauthorized subnets. This task demonstrated the effectiveness of using service endpoints in conjunction with subnet-specific access controls to enforce data access policies.



```
PS C:\Users\Student> $connectTestResult = Test-NetConnection -ComputerName myuniquenameforrg.file.core.windows.net -Port
if ($connectTestResult.TcpTestSucceeded) {
    # Save the password so the drive will persist on reboot
    cmd.exe /C "cmdkey /add:`"myuniquenameforrg.file.core.windows.net`" /user:`"localhost\myuniquenameforrg`" /pass:`"09
    # Mount the drive
    New-PSDrive -Name Z -PSProvider FileSystem -Root "\\myuniquenameforrg.file.core.windows.net\my-file-share" -Persist
} else {
    Write-Error -Message "Unable to reach the Azure storage account via port 445. Check to make sure your organization o
}

CMDKEY: Credential added successfully.
New-PSDrive : Access is denied
At line:6 char:5
+     New-PSDrive -Name Z -PSProvider FileSystem -Root "\\myuniquenamef ...
+     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (Z:PSDriveInfo) [New-PSDrive], Win32Exception
    + FullyQualifiedErrorId : CouldNotMapNetworkDrive,Microsoft.PowerShell.Commands.NewPSDriveCommand


PS C:\Users\Student> Test-NetConnection -ComputerName www.bing.com -Port 80


ComputerName     : www.bing.com
RemoteAddress    : 23.12.147.172
RemotePort       : 80
InterfaceAlias   : Ethernet
SourceAddress    : 10.0.0.4
TcpTestSucceeded : True



PS C:\Users\Student> |
```

36 Minutes Remaining

☑ 6. Within the **Windows PowerShell ISE** window, open the **Script** pane, then paste and run the same PowerShell script that you ran within the Remote Desktop session to the **myVMPrivate** Azure VM.

This time, you will receive the **New-PSDrive : Access is denied** error.

Access is denied because the *myVmPublic* virtual machine is deployed in the Public subnet. The Public subnet does not have a service endpoint enabled for the Azure Storage. The storage account only allows network access from the Private subnet.

☑ 7. Next, from the console pane of the **Windows PowerShell ISE** console, run the following to verify that the virtual machine has outbound connectivity to the internet:

```powershell
Test-NetConnection -ComputerName www
```

The test will succeed because there is no outbound security rule to deny internet on the Public subnet.

100% Tasks Complete

Conclusion

Through this lab, I gained a thorough understanding of securing Azure Storage using service endpoints, subnets, and network security groups. I learned how to isolate traffic within the Azure backbone, restrict access using NSGs, and validate security rules through hands-on testing. These best practices are essential in real-world scenarios where organizations must ensure that sensitive storage resources are only accessible from specific, trusted network segments. The lab reinforced key Azure networking and security concepts that are critical for designing secure cloud architectures