

Cyber Shujaa

Cloud Security Specialist

Assignment 18 - Lab 6: Service Endpoints and Securing Storage

NAME: WELDON KIPKIRUI KENEI

CS NO: ADC-CSS02-25027

Introduction

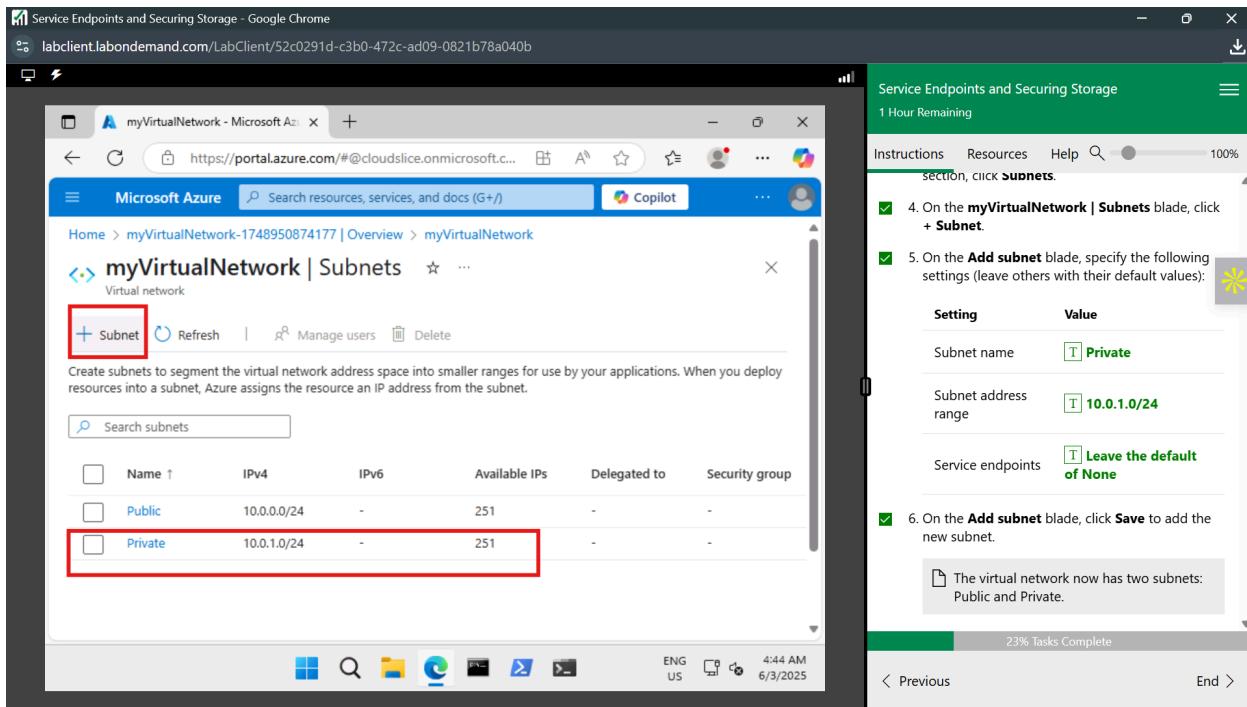
In this lab scenario, we will create a proof of concept to demonstrate securing Azure file shares. Specifically, we want to: Create a storage endpoint so traffic destined to Azure Storage always stays within the Azure backbone network, configure the storage endpoint so only resources from a specific subnet can access the storage, and confirm that resources outside of the specific subnet cannot access the storage.

Service endpoints and security storage

Firstly, we need to create a virtual network using the Azure portal as shown.

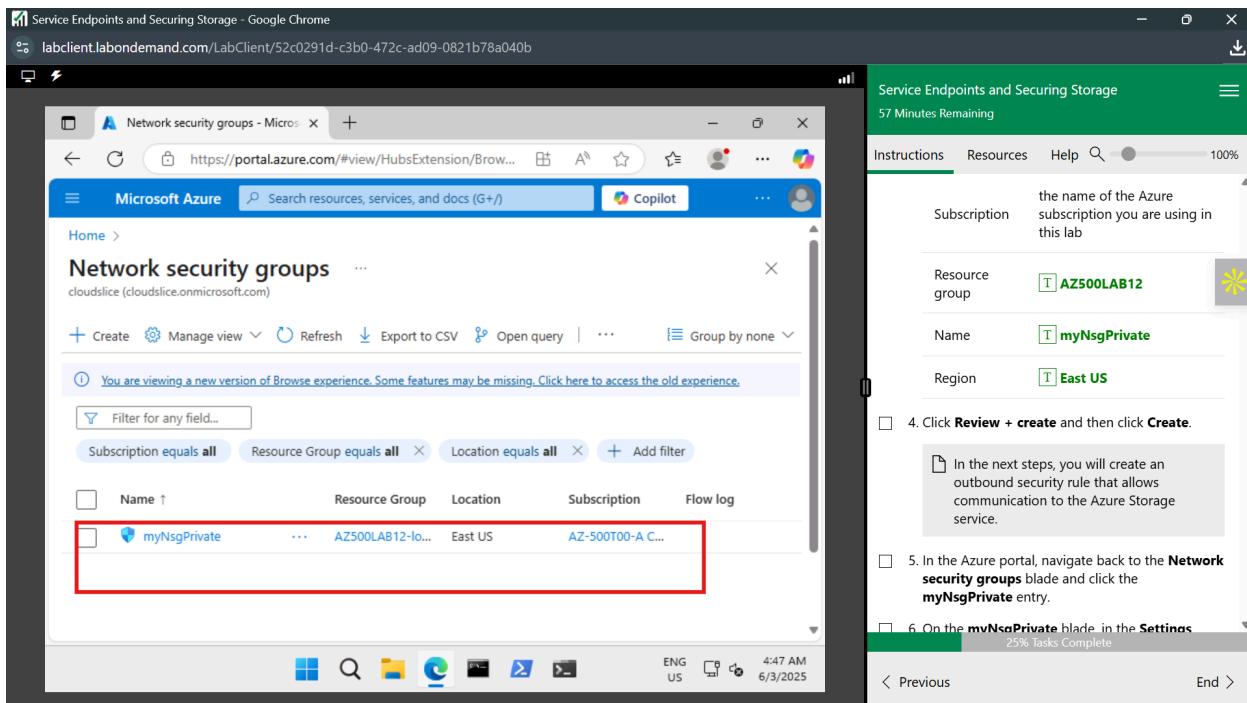
The screenshot shows the Microsoft Azure portal with the URL <https://portal.azure.com/#create/Microsoft.VirtualNetwork>. The 'Create virtual network' blade is open, and the 'Review + create' tab is selected. On the left, there are sections for 'Security' (Azure Bastion: Disabled, Azure Firewall: Disabled, Azure DDoS Network Protection: Disabled), 'IP addresses' (Address space: 10.0.0.0/16 (65,536 addresses), Subnet: Public (10.0.0.0/24) (256 addresses)), and 'Tags'. At the bottom, there are 'Previous' and 'Next' buttons, and a prominent blue 'Create' button which is highlighted with a red box. On the right, a sidebar titled 'Service Endpoints and Securing Storage' shows a progress bar at 16% complete. Task 6 is checked: 'Back on the IP addresses tab of the Create virtual network blade, click Review + create.' Task 7 is unchecked: 'On the Review + create tab of the Create virtual network blade, click Create.' Below the sidebar, a task list for 'Task 2: Add a subnet to the virtual network and configure a storage endpoint' is described, along with a note about creating another subnet and enabling service endpoints per service per subnet.

Next, we will create another subnet and enable a service endpoint on that subnet. Service endpoints are enabled per service, per subnet.



The screenshot shows the Microsoft Azure portal with the URL <https://portal.azure.com/#@cloudslice.onmicrosoft.com>. The page displays the 'myVirtualNetwork | Subnets' blade under the 'Virtual network' section. A new subnet named 'Private' is being created, with the IP range set to 10.0.1.0/24. The 'Service endpoints' setting is set to 'Leave the default of None'. A sidebar on the right provides step-by-step instructions for creating the subnet.

We will then create a network security group with two outbound security rules (Storage and internet) and one inbound security rule (RDP). We will also associate the network security group with the Private subnet. This will restrict outbound traffic from Azure VMs connected to that subnet.



The screenshot shows the Microsoft Azure portal with the URL <https://portal.azure.com/#view/HubsExtension/Browse>. The page displays the 'Network security groups' blade. A new network security group named 'myNsgPrivate' is being created, associated with the 'AZ500LAB12-loc...' resource group and the 'East US' region. A sidebar on the right provides step-by-step instructions for creating the network security group.

Service Endpoints and Securing Storage - Google Chrome
labclient.labondemand.com/LabClient/52c0291d-c3b0-472c-ad09-0821b78a040b

Associate subnet

myNsgPrivate

Virtual network: myVirtualNetwork (AZ500LAB12-1od51890630)

Subnet: Private

OK

Service Endpoints and Securing Storage
45 Minutes Remaining

Instructions Resources Help 100%

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.

39% Tasks Complete

Configure a network security group to allow RDP on the public subnet

Here, we will create a network security group with one inbound security rule (RDP). We will also associate the network security group with the Public subnet. This will allow RDP access to the Public VM.

Service Endpoints and Securing Storage - Google Chrome
labclient.labondemand.com/LabClient/52c0291d-c3b0-472c-ad09-0821b78a040b

Create network security group

Validation passed

Basics Tags Review + create

Basics

Subscription: AZ-500T00-A CSR 3
Resource group: AZ500LAB12-1od51890630
Region: East US
Name: myNsgPublic

Tags

None

Create < Previous Next > Download a template for automation

Service Endpoints and Securing Storage
42 Minutes Remaining

Instructions Resources Help 100%

4. Click Review + create and then click Create.

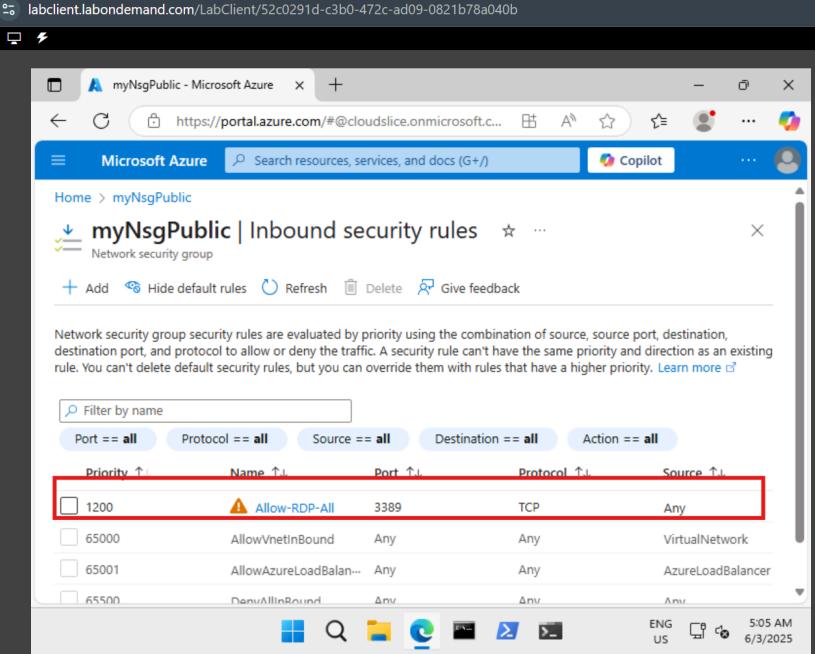
In the next steps, you will create an inbound security rule that allows communication to the Azure Storage service.

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

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

42% Tasks Complete

We then create the rule as follows;

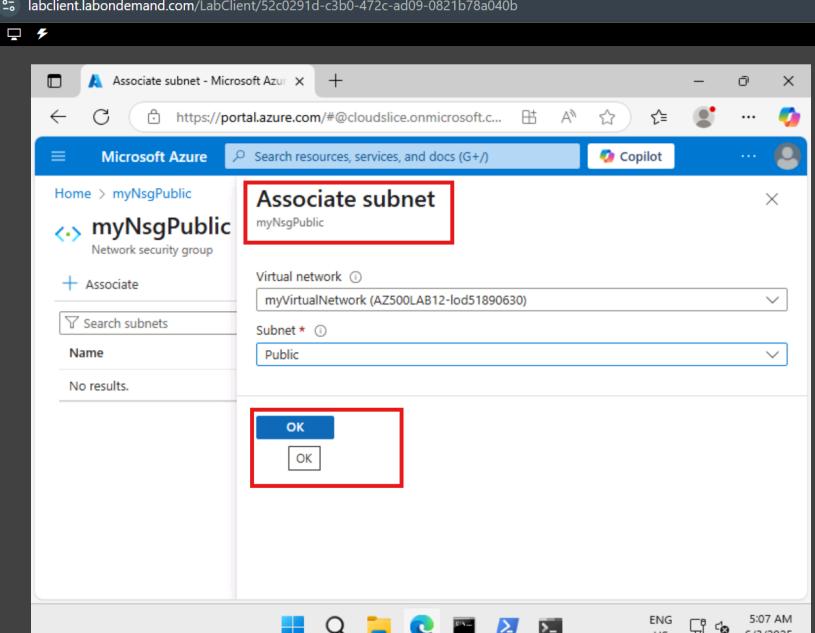


The screenshot shows the 'Inbound security rules' blade for the 'myNsgPublic' network security group. A specific rule is highlighted with a red box:

Priority	Name	Port	Protocol	Source
1200	Allow-RDP-All	3389	TCP	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer
65500	DenyAllInbound	Any	Any	Any

To the right, a task pane displays steps 8 and 9 of a guide. Step 8 instructs to click 'Add' to create a new inbound rule. Step 9 instructs to associate the network security group with the Public subnet.

Then we associate it with our public subnet.



The screenshot shows the 'Associate subnet' dialog for the 'myNsgPublic' network security group. The 'Virtual network' dropdown is set to 'myVirtualNetwork (AZ500LAB12-lod51890630)'. The 'Subnet' dropdown is set to 'Public'. The 'OK' button at the bottom is highlighted with a red box.

To the right, a task pane displays steps 8 and 9 of a guide. Step 8 instructs to click 'Add' to create a new inbound rule. Step 9 instructs to associate the network security group with the Public subnet.

Create a storage account with a file share

Here, we will create a storage account with a file share and obtain the storage account key.

The screenshot shows the Microsoft Azure portal with a lab client interface. On the left, a browser window displays the 'Create a storage account' blade. The 'Basics' tab is selected, showing configuration details: Subscription (AZ-500T00-A CSR 3), Resource group (AZ500LAB12-lod51890630), Location (East US), Storage account name (lab12securestorage), Primary service (Standard), Performance (Standard), and Replication (Read-access geo-redundant storage (RA-GRS)). A red box highlights the configuration area. On the right, the 'Service Endpoints and Securing Storage' lab step is shown with the following details:

Storage account name	any globally unique name between 3 and 24 in length consisting of letters and digits
Location	(US) EastUS
Performance	Standard (general-purpose v2 account)
Redundancy	Locally redundant storage (LRS)

Below these settings, a task list is displayed:

- 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.
- 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 click Search.

The status bar at the bottom indicates 50% Tasks Complete.

We created a file share service under our storage account.

The screenshot shows the Microsoft Azure portal with a lab client interface. On the left, a browser window displays the 'File shares' blade for the 'lab12securestorage' storage account. It shows one file share named 'my-file-share'. On the right, the 'Service Endpoints and Securing Storage' lab step is shown with the following details:

Virtual networks	myVirtualNetwork
Subnets	Private

Below these settings, a task list is displayed:

- On the Add networks blade, click Add.
- Back on the storage account blade, click Save.

A note in a callout box states: "At this point in the lab you have configured a virtual network, a network security group, and a storage account with a file share."

The status bar at the bottom indicates 69% Tasks Complete.

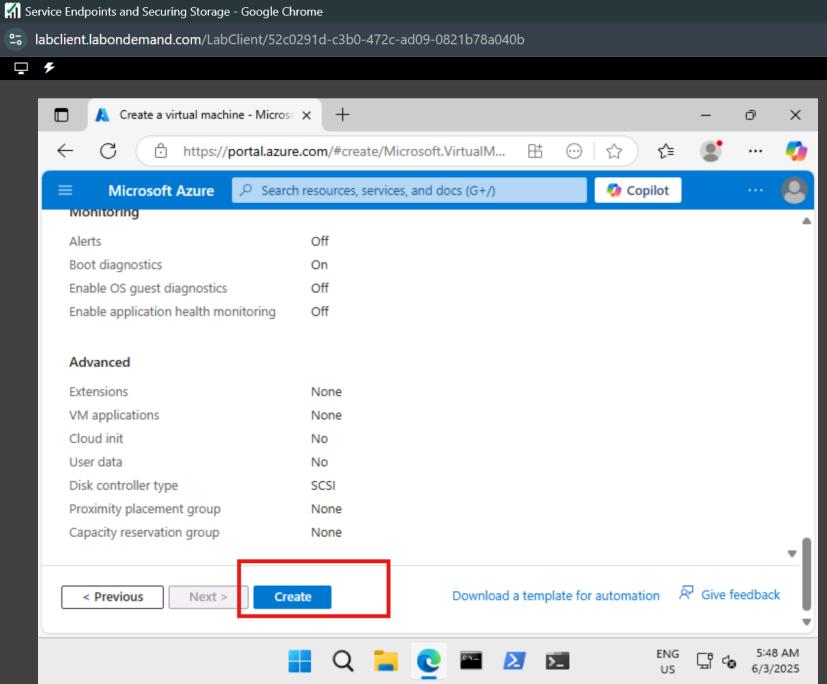
And then we added it to our virtual network

The screenshot shows a Microsoft Azure lab environment titled "Service Endpoints and Securing Storage". On the left, a browser window displays the Azure portal with the URL <https://portal.azure.com/#@cloudslice.onmicrosoft.com>. The browser's address bar also shows the URL <https://labclient.labondemand.com/LabClient/52c0291d-c3b0-472c-ad09-0821b78a040b>. The Azure portal shows the configuration of a storage account named "myVirtualNetwork". The "Virtual networks" section lists "myVirtualNetwork" with a single subnet. A red box highlights this row. To the right, a sidebar titled "Service Endpoints and Securing Storage" provides instructions for the lab, including steps 19 and 20 related to adding networks and saving changes. A note indicates that at this point, a virtual network, a network security group, and a storage account with a file share have been configured.

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

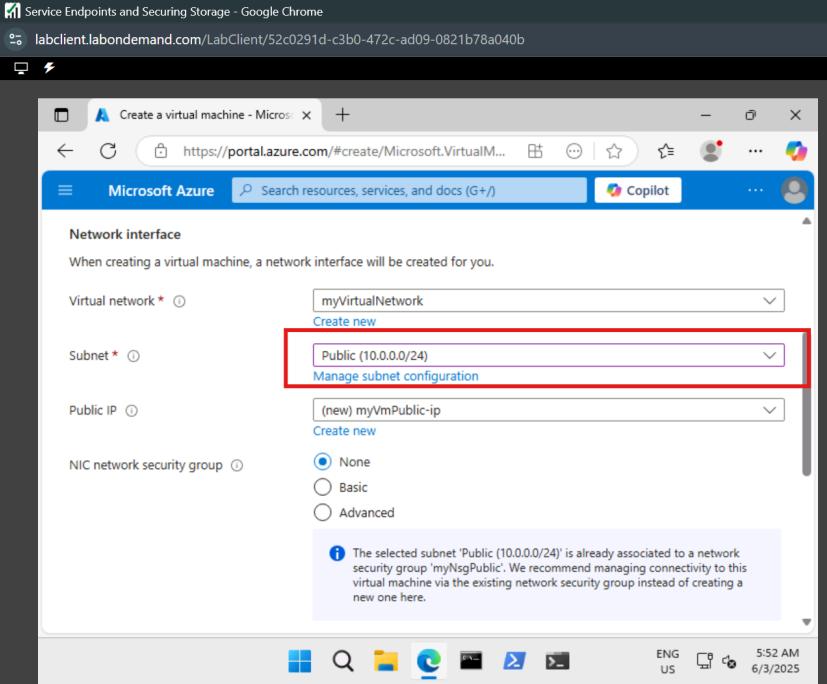
Deploy virtual machines into the designated subnets

Here, we will create two virtual machines, one in the Private subnet and one in the Public subnet.



The screenshot shows the 'Create a virtual machine' blade in the Microsoft Azure portal. On the right, a sidebar titled 'Service Endpoints and Securing Storage' displays configuration details: Virtual network set to 'myVirtualNetwork', Subnet set to 'Private (10.0.1.0/24)', and Public IP set to '(new)myVmPrivate-ip'. A task list on the right indicates steps 6 and 7 have been completed. Step 6: 'Click Next: Management >, on the Management tab of the Create a virtual machine blade, accept the default settings and click Review + create.' Step 7: 'On the Review + create blade, ensure that validation was successful and click Create.' A note below states: 'The second virtual machine will be connected to the Public subnet.'

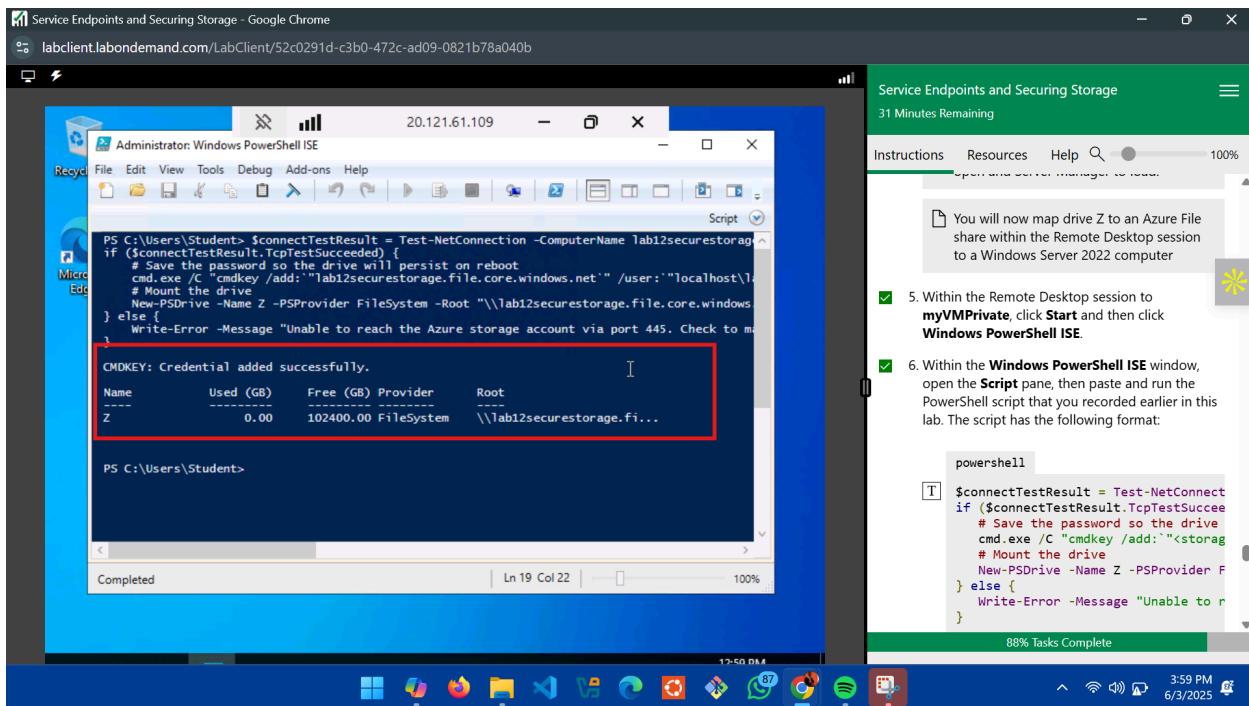
The second virtual machine will be connected to the Public subnet.



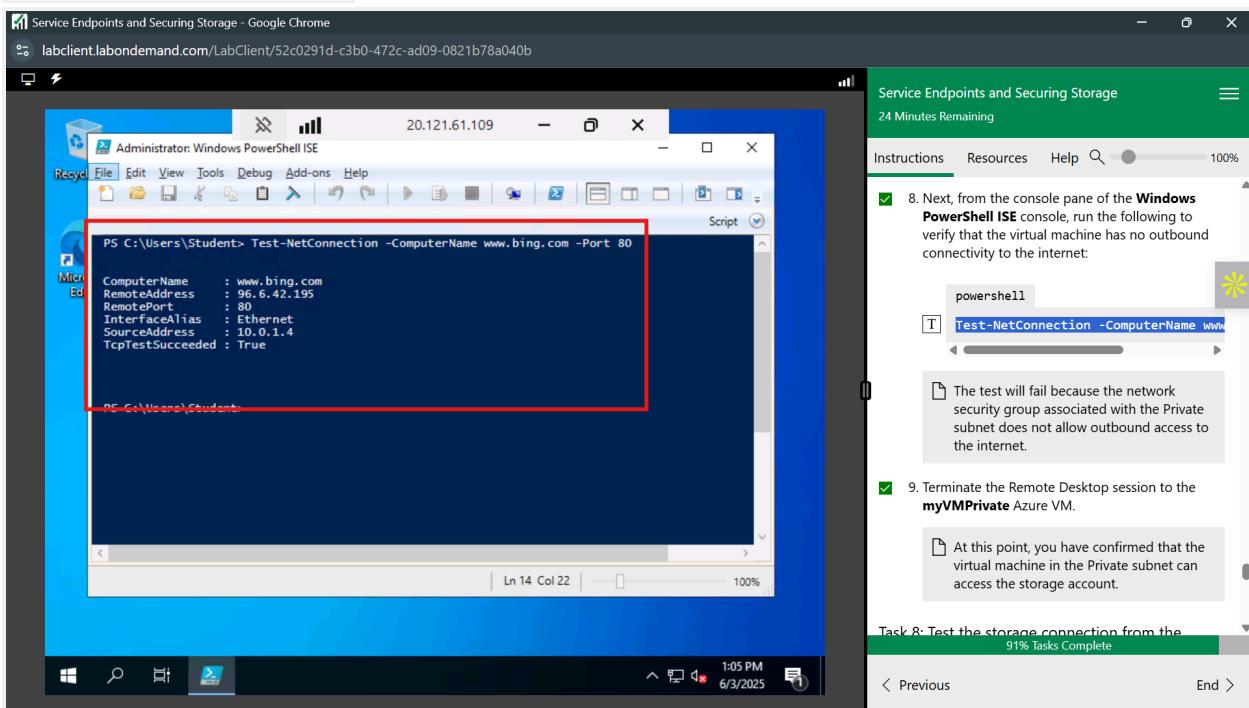
The screenshot shows the 'Create a virtual machine' blade in the Microsoft Azure portal. On the right, a sidebar titled 'Service Endpoints and Securing Storage' displays configuration details: Subnet set to 'Public (10.0.0.0/24)', and Public IP set to '(new)myVmPublic-ip'. A task list on the right indicates steps 12 and 13 have been completed. Step 12: 'Click Next: Management >, on the Management tab of the Create a virtual machine blade, accept the default settings and click Review + create.' Step 13: 'On the Review + create blade, ensure that validation was successful and click Create.' A note below states: 'You can continue to the next task once the deployment of the myVMPublic Azure VM is completed.'

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

We will connect to the myVMPrivate virtual machine via Remote Desktop and map a drive to the file share.

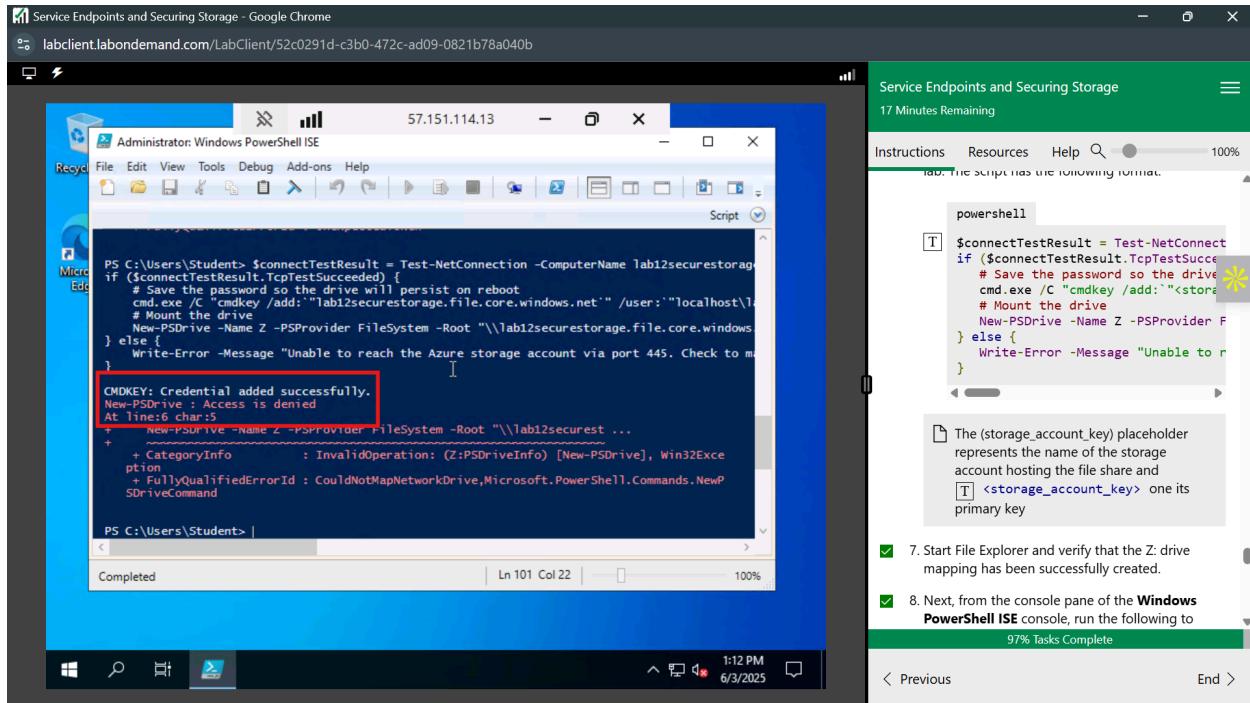


We then test the connection using the `Test-NetConnection -ComputerName www.bing.com -Port 80`



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

We will now map drive Z to an Azure File share within the Remote Desktop session to a Windows Server 2022 computer



The screenshot shows a Windows PowerShell ISE window running on a Windows Server 2022 machine with IP 57.151.114.13. The script in the console pane attempts to connect to an Azure storage account and map a drive. A red box highlights the error message "CMDKEY: Credential added successfully. New-PSDrive : Access is denied At line:6 char:5". The task pane on the right contains instructions for connecting to Azure storage, mentioning a placeholder <storage_account_key>.

```
$connectTestResult = Test-NetConnection -ComputerName lab12securestorage
if ($connectTestResult.TcpTestSucceeded) {
    # Save the password so the drive will persist on reboot
    cmd.exe /C "cmdkey /add:'\\lab12securestorage.file.core.windows.net' /user:'localhost\1$' /password:$storageAccountKey"
    # Mount the drive
    New-PSDrive -Name Z -PSProvider FileSystem -Root '\\\\lab12securestorage.file.core.windows.net\\$'
} else {
    Write-Error -Message "Unable to reach the Azure storage account via port 445. Check to make sure the storage account has port 445 open in its firewall settings and try again."
}

CMDKEY: Credential added successfully.
New-PSDrive : Access is denied
At line:6 char:5
+     New-PSDrive -Name Z -PSProvider FileSystem -Root '\\\\lab12securestorage...
+     + CategoryInfo          : InvalidOperation: (Z:PSDriveInfo) [New-PSDrive], Win32Exception
+     + FullyQualifiedErrorId : CouldNotMapNetworkDrive,Microsoft.PowerShell.Commands.NewPSDriveCommand
```

The storage account only allows network access from the Private subnet.

Service Endpoints and Securing Storage
17 Minutes Remaining

Instructions Resources Help 100%

lab. The script has the following format:

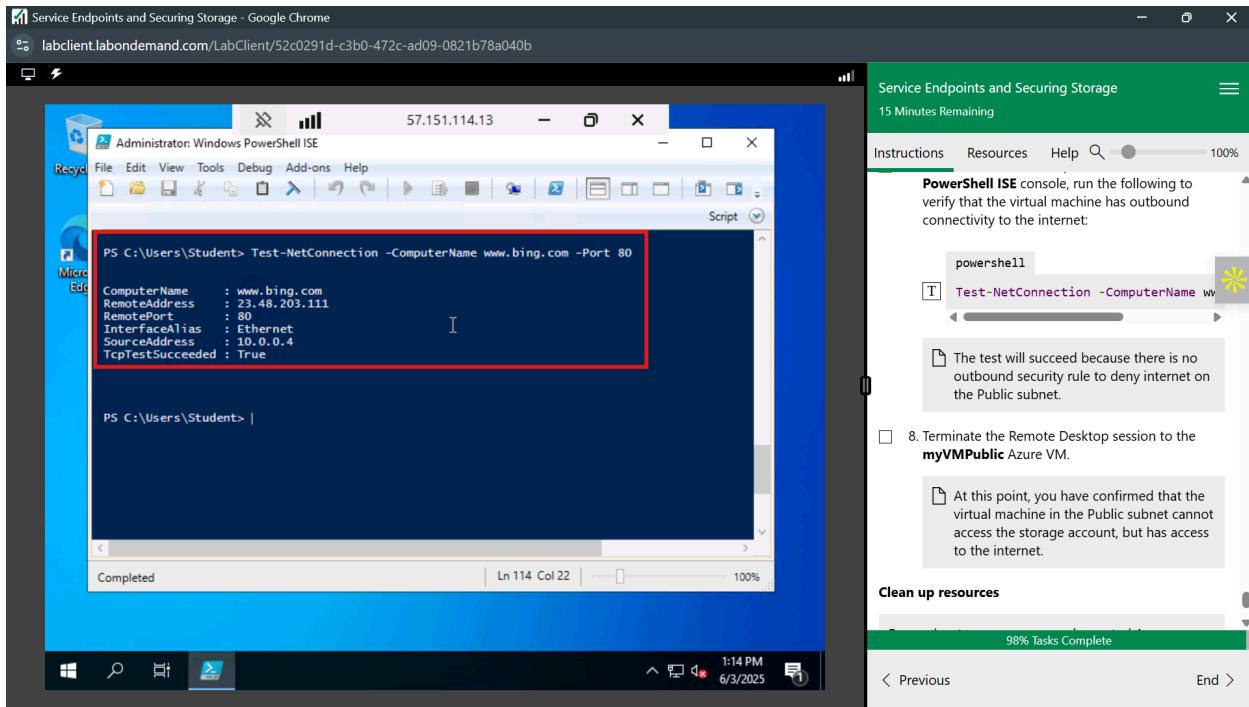
```
powershell
$connectTestResult = Test-NetConnection
if ($connectTestResult.TcpTestSucceeded) {
    # Save the password so the drive will persist on reboot
    cmd.exe /C "cmdkey /add:'<storage_account_key>' /user:'localhost\1$' /password:$storageAccountKey"
    # Mount the drive
    New-PSDrive -Name Z -PSProvider FileSystem -Root '\\\\lab12securestorage.file.core.windows.net\\$'
} else {
    Write-Error -Message "Unable to reach the Azure storage account via port 445. Check to make sure the storage account has port 445 open in its firewall settings and try again."
}
```

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

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.

We then test for outbound connectivity with the `Test-NetConnection -ComputerName www.bing.com -Port 80` command.



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

Conclusion

To conclude, we were able to demonstrate how to secure access of our storage service through network private service endpoints. We were able to keep the traffic of our storage endpoint within the Azure backbone.